# アプリケーションソフトウェアの
# プロテクションプロファイル


バージョン: 1.2

2016-04-22

**National Information Assurance Partnership**

平成 29 年 1 月 13 日 翻訳 暫定第 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

## 改版履歴

| バージョン | 日付 | コメント |
|---|---|---|
| v 1.2 | 2016-04-22 | サーバサイドの TLS 要件を追加 (選択に基づく)<br>NIAP TRRT 問い合わせに基づく複数の明確化<br>FDP_DEC_EXT.1 を別個のコンポーネントにリファクタ |
| v 1.1 | 2014-11-05 | TLS 暗号スイートの選択を追加 |
| v 1.0 | 2014-10-20 | 初版発行 |

## 目次

# 1. 概論

## 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、アプリケーションソフトウェアのセキュリティ機能を [CC] の観点から記述し、そのようなソフトウェアの機能要件及び保証要件を定義することである。近年、ソフトウェアへの攻撃はオペレーティングシステムを標的とするものからアプリケーションを標的とするものへとシフトしている。これは、オペレーティングシステムのセキュリティと開発プロセスにおける改善への、当然の反応である。その結果、セキュリティ侵害のリスクを低減させるためには、アプリケーションのセキュリティを向上させることが最も重要となる。

## 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で用いられるコモンクライテリアの用語と技術用語の両方について説明する。

### 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) | 製品の種別に対するセキュリティ要件についての実装に依存しないセット。 |
| セキュリティターゲット (ST) | 特定の製品に対するセキュリティ要件についての実装に依存するセット。 |
| 評価対象 (TOE) | 評価される製品。ここでは、アプリケーションソフトウェアとその補足証拠資料。 |
| TOE セキュリティ機能 (TSF) | 評価され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 を満たすかについての記述。 |
| セキュリティ機能要件 (SFR) | TOE によるセキュリティ実施の要件。 |
| 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、攻撃者がアプリケーションプロセスのアドレス空間へ導入したコードへ制御をリダイレクトすることがより困難となる。 |
| 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、及びその補足証拠資料。用語 *TOE* と *アプリケーション*は、本文書においては同義である。 |
| アプリケーションプログラミン | ライブラリのような別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 |

| | |
|---|---|
| グインタフェース (API) | 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一連のライブラリ用に提供されることが多い。 |
| クレデンシャル (Credential) | 利用者の本人性を確立するようなデータ、例、暗号鍵またはパスワード。 |
| データ実行防止 (DEP) | 最新のコンピューターハードウェア上で動作する最新の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パーミションを実施するもの。DEP は、メモリのページに、攻撃者がコードの導入と実行をより困難とするようなデータと命令の両方が含まれないようにする。 |
| 開発者 (Developer) | アプリケーション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。 |
| モバイルコード (Mobile Code) | ローカルシステム上の制限された実行環境内で実行されるために、リモートシステムから送信されるソフトウェア。通常は、永続的なインストールは行われず、利用者の同意や通知すらなしに実行が開始される。モバイルコード技術の例としては、JavaScript、Java アプレット、Adobe Flash、及び Microsoft Silverlight が含まれる。 |
| オペレーティングシステム (OS) | ハードウェア資源を管理し、アプリケーションへサービスを提供するソフトウェア。 |
| 個人を特定できる情報 (Personally Identifiable Information) (PII) | ある機関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、金融取引、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、生年月日及び出生地、母親の旧姓、バイオメトリック記録等、個人の本人性を区別または追跡するために利用可能な情報であって、個人へ結び付けられた、または個人へ結び付けられ得る、その他の任意の個人情報を含む。[OMB] |
| プラットフォーム (Platform) | アプリケーションソフトウェアが動作する環境。プラットフォームはオペレーティングシステム、またはオペレーティングシステム上で動作する実行環境、これらの組み合わせの可能性がある。 |
| 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企業データが含まれるかもしれない、または電子メール、メッセージ、文書、カレンダー項目、及び連絡先などの特定のアプリケーションデータかもしれない。機微なデータには最小限、PII、クレデンシャル、及び鍵が含まれなければならない (must)。機微なデータは、ST 作成者によってアプリケーションの TSS で特定されなければならない (shall)。 |
| スタッククッキー (Stack Cookie) | 関数呼び出しの開始時にスタック上に値を置き、関数呼び出しの最後にその値が同一であることをチェックするような悪用防止機能。これは、スタックガード (Stack Guard)、またはスタックカナリア (Stack Canaries) とも呼ばれる。 |
| ベンダ (Vendor) | アプリケーションソフトウェアを販売するエンティティ。本文書の目的においては、ベンダと開発者は同一である。ベンダは、アプリケーションソフトウェアの維持管理とアップデートに責任を負う。 |

## 1.3 適合する評価対象

本文書の要件は、デスクトップ及びサーバプラットフォーム上と同様に、モバイルデバイス上で動作するアプリケーションソフトウェア（「アプリ」）に適用される。一部のアプリケーション種別はより具体的な PP によってカバーされるが、これらの PP は本 PP の拡張パッケージとして表現されることがある。このようなアプリケーションは、本 PP 及び規定の機能に対応する拡張パッケージの両方の要件の対象となる。一部の特に専門のアプリケーション用の PP は現時点では拡張パッケージとして表現されないかもしれないが、本文書の要件はこれらの高度に専門のアプリケーションの対策方針としてみなされるべきである (should)。

本文書の要件は幅広いアプリケーションソフトウェアへ適用されるが、規定の種別のアプリケーションに対して正式なコモンクライテリア評価がいつ期待されるかについて決定するにあたっては、関連する国のスキームからのガイダンスを参考にされたい。これは、そのアプリケーションのセキュリティ機能の性質によって異なるかもしれない。

### 1.3.1 TOE 境界

アプリケーションは、そのベンダによって提供されるソフトウェアから構成され、オペレーティングシステムによって提供されるファイルシステム上にインストールされる。アプリケーションは、オペレーティングシステム (図 1) 、オペレーティングシステム上で動作する実行環境、またはこれらの組み合わせ (図 2) かもしれない、プラットフォーム上で動作する。正確性と再現性を提供するため、いくつかの保証アクティビティは、アプリケーションが動作する特定のプラットフォームに特有なものである。テストアクティビティは、プラットフォームにわたるカバレージが可能な限り完全かつ正確であるように、積極的にプラットフォームベンダから求められる。これによって、それらのプラットフォーム上のアプリケーションの認証が可能となる。

アプリケーションには、オフィススイート、シンクライアント、PDF リーダ、及びダウンロード可能なスマートフォンアプリのようなさまざまな幅広いソフトウェアが含まれる。TOE にはアプリケーションインストールパッケージの任意のソフトウェアが含まれ、それらのソフトウェアには、カーネルドライバのような基盤となるプラットフォームの機能を拡張するものもあるかもしれない。多くのプラットフォームには、ウェブブラウザ、電子メールクライアント及びメディアプレイヤのようなアプリケーションがバンドルされており、これらもまた本文書で定義された要件の対象とみなされるべきである (should) が、正式なコモンクライテリア評価の期待は、国のスキームに依存する。BIOS 及びその他のファームウェア、オペレーティングシステムのカーネル、ならびにプラットフォームの一部として提供されるその他のシステムソフトウェア (及びドライバ) は、本文書の適用範囲外である。

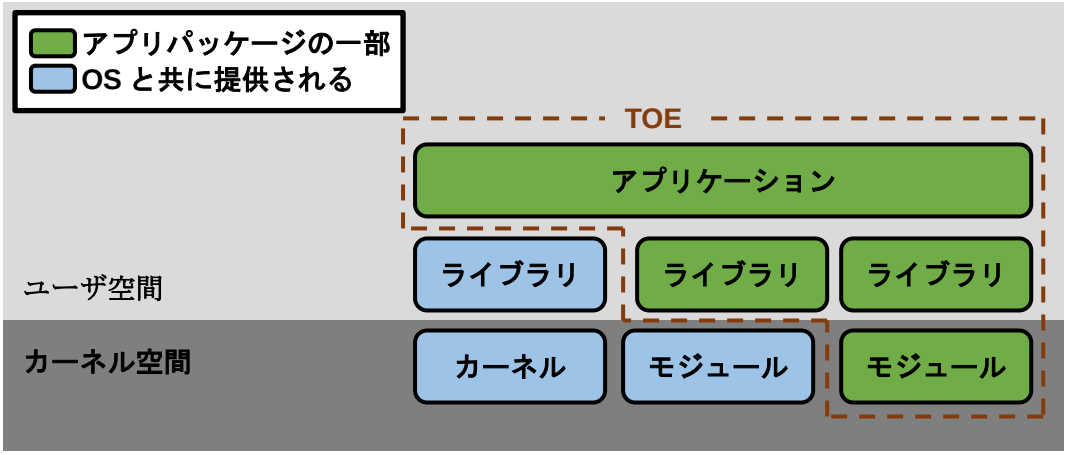


**図 1：オペレーティングシステム上で動作するアプリケーション及びカーネルモジュールとしての TOE**

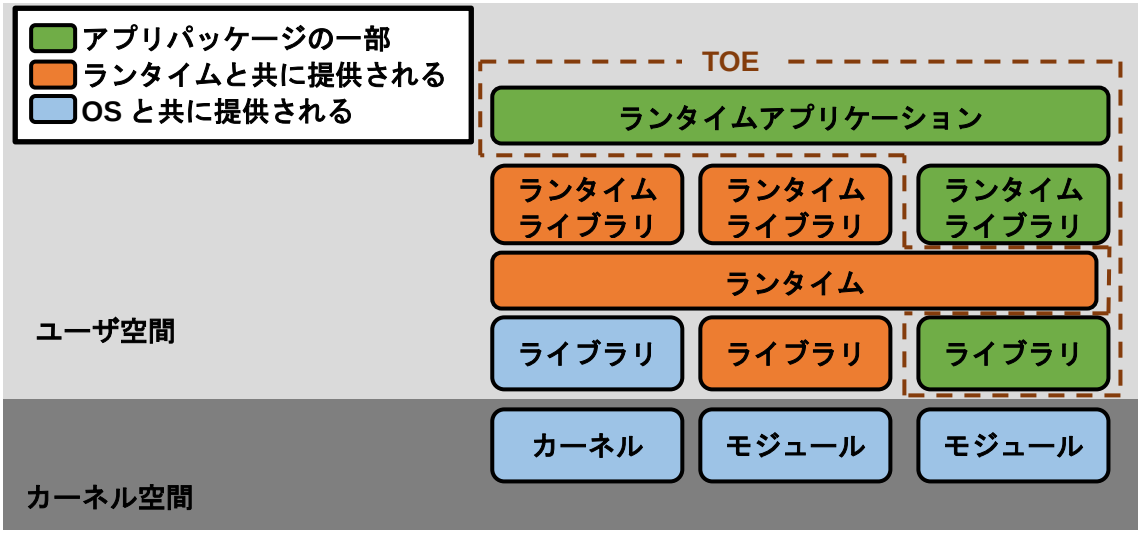


**図 2：実行環境プラスネイティブコード中で動作するアプリケーションとしての TOE**

## 1.4 使用事例

本プロテクションプロファイルの要件は、以下の使用事例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。これらの使用事例は、数多くの具体的な使用事例がアプリケーションソフトウェアに存在するため、意図的に非常に広範なものとなっている。多くのアプリケーションがこれらの幅広い使用事例の組み合わせで用いられることがあり、本 PP の拡張パッケージに適合する評価は、適用可能な場合、いくつかのアプリケーション種別については最も適切であるかもしれない。

**[使用事例 1] コンテンツ作成**

アプリケーションが、利用者にコンテンツを作成してローカルまたはリモートストレージへの格納を可能にする。コンテンツの例には、テキスト文書、プレゼンテーション、及び画像が含まれる。

**[使用事例 2] コンテンツ利用**

アプリケーションが、利用者にローカルまたはリモートストレージからコンテンツを読み出してコンテンツの利用を可能にする。コンテンツの例には、ウェブページ及びビデオが含まれる。

**[使用事例 3] 通信**

アプリケーションが、通信チャネルを介した他の利用者またはアプリケーションとの、対話的または非対話的な通信を可能にする。通信の例には、インスタントメッセージ、電子メール、及び音声が含まれる。

# 2. 適合主張

### 適合ステートメント

本 PP へ適合するため、ST は、 [CC] パート 1 (ASE_CCL) で定義された正確適合(Strict Conformance)のサブセットである完全適合(Exact Conformance)を論証しなければならない (must)。その ST には、以下のような本 PP のすべてのコンポーネントが含まれなければならない (must) :

- 無条件のもの (常に要求される)
- 選択ベースのもの (規定の*選択*が無条件要件で選択されるとき、要求される)

また、以下のようなコンポーネントを含んでもよい

- オプション、または
- オブジェクティブ (訳注：将来、必須となるような新技術に基づく要件)。

無条件の要件は、本文書の本体で見つかり、一方、附属書には選択ベース要件、オプション要件、及びオブジェクティブ要件が含まれる。ST は、これらのコンポーネントのいずれについても繰り返してよいが、本 PP や本 PP に適合する PP で定義されていないような、いかなる追加のコンポーネント (例、CC パート 2 または 3、または本 PP に適合しない PP からのもの、もしくは ST により拡張されたもの) を含んではならない (must not)。本 PP を拡張するかもしれないような、より特化した PP についてはセクション 1.3 を参照されたい。

### 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 [CC] のパート 2 (拡張) 及びパート 3 (拡張) に適合する。

### PP 主張

本 PP は、その他のいかなる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、TOE が対処することが期待されるような脅威、運用環境についての前提条件、及び TOE が強制すると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、通信チャネル上またはネットワーク基盤上の他のどこかに位置する。攻撃者は、アプリケーションソフトウェアを危殆化するために、アプリケーションソフトウェアとの通信に関与したり、アプリケーションソフトウェアと他のエンドポイントとの間の通信を改変したりするかもしれない。

**T.NETWORK_EAVESDROP**

攻撃者は、通信チャネル上またはネットワーク基盤上の他のどこかに位置する。攻撃者は、アプリケーションと他のエンドポイントとの間で交換されるデータをモニターして、そのデータへのアクセスを取得するかもしれない。

**T.LOCAL_ATTACK**

攻撃者は、アプリケーションが動作するのと同じコンピューティングプラットフォーム上の非特権ソフトウェアを介して活動できる。攻撃者は、ファイルや他のローカル通信の形態でアプリケーションに対して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.PHYSICAL_ACCESS**

攻撃者は、機微な保存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**

TOE 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。これには、基盤となるプラットフォームと、それが TOE へ提供するすべての実行環境が含まれる。

**A.PROPER_USER**

アプリケーションソフトウェア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。

**A.PROPER_ADMIN**

アプリケーションソフトウェア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ソフトウェアを管理する。

## 3.3 組織のセキュリティ方針

アプリケーションの組織のセキュリティ方針は存在しない。

# 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.INTEGRITY**

適合 TOE は、そのインストールパッケージ及びアップデートパッケージの完全性を保証し、また実行環境ベースの軽減策を活用する。ソフトウェアはほとんどエラーなしで出荷されることはなく、現場のソフトウェアに対してパッチ及びアップデートを展開して完全性を付与することは企業ネットワークのセキュリティにとって不可欠である。プロセッサ製造業者、コンパイラ開発者、実行環境ベンダ、及びオペレーティングシステムベンダは、システムをセキュリティ侵害す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ような、実行環境ベースの軽減策を開発している。アプリケーションソフトウェアは、ランタイム環境によって提供される API を用いることによって、またはコンパイラまたはリンカオプションを介したメカニズムの有効化によって、これらのメカニズムを利用できる場合が多い。

以下で対処：FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1

**O.QUALITY**

実装の品質を保証するため、適合 TOE は、それ自身のバージョンのサービスと API を実装するよりもむしろ、ランタイム環境によって提供されるサービスと API を活用する。これは、暗号サービス及びファイルとメディアの構文解析のようなその他の複雑な操作に関しては、特に重要である。このプラットフォームのふるまいの活用は、文書化されサポートされている API のみを使用することに依存している。

以下で対処：FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1

**O.MANAGEMENT**

利用者及び企業による管理を容易にするため、適合 TOE は、それらのセキュリティ関連の設定及び維持管理のために一貫したサポートされたインタフェースを提供する。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を通した、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、ならびに設定メカニズムの提供が含まれる。これにはまた、任意の PII の開示に関する制御を利用者へ提供することも含まれる。

以下で対処：FMT_SMF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1.5, FPR_ANO_EXT.1

**O.PROTECTED_STORAGE**

ストレージ媒体の物理的制御の喪失事象において利用者データの機密性の喪失の問題に対処するため、適合 TOE は、保存データ保護を利用する。これには、このデータへの許可されないアクセスを防止するため、TOE によって格納されるデータ及び鍵の暗号化が含まれる。これにはまた、不必要なネットワーク通信であってその結果がデータの喪失となり得るものが含まれる。

以下で対処：FDP_DAR_EXT.1, FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_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処するため、適合 TOE は、機微なデータに高信頼チャネルを使用する。機微なデータには、暗号鍵、パスワード、及びアプリケーション外部へ暴露されるべきでない (should not) アプリケーション特有のその他の任意のデータが含まれる。

以下で対処：FTP_DIT_EXT.1, FCS_TLSC_EXT.1, FCS_DTLS_EXT.1, FCS_RBG_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、TOE がそのセキュリティ機能を正しく提供することを支援する。これらは、環境についての前提条件と対応する。

**OE.PLATFORM**

TOE 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。これには、基盤となるオペレーティングシステムと、TOE へ提供される任意の別個の実行環境が含まれる。

**OE.PROPER_USER**

アプリケーションソフトウェア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。

**OE.PROPER_ADMIN**

アプリケーションソフトウェアの管理者は、不注意、意図的に怠慢、敵対的ではなく、また適用される企業のセキュリティ方針を遵守してソフトウェアを管理する。

## 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提供するものとして O.PROTECTED_COMMS によって対抗される。<br>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提供するものとして O.INTEGRITY によって対抗される。<br>脅威 T.NETWORK_ATTACK は、ネットワーク攻撃に対して防御するようアプリケーションを設定する能力をていきょうするものとして O.MANAGEMENT によって対抗される。 |
| T.NETWORK_EAVESDROP | O.PROTECTED_COMMS, O.QUALITY, O.MANAGEMENT | 脅威 T.NETWORK_EAVESDROP は、送信されるデータの機 |

| | | |
|---|---|---|
| | | 密性を提供するものとして O.PROTECTED_COMMS によって対抗される。<br><br>対策方針 O.QUALITY は、ネットワークベースの攻撃に対する保護を提供するメカニズムの利用を保証する。<br><br>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アプリケーションを設定する能力を提供するものとして O.MANAGEMENT によって対抗される。 |
| T.LOCAL_ATTACK | O.QUALITY | 対策方針 O.QUALITY 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.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 により実現される。 |
| A.PROPER_USER | OE.PROPER_USER | 運用環境の対策方針 OE.PROPER_USER は、A.PROPER_USER により実現される。 |
| A.PROPER_ADMIN | OE.PROPER_ADMIN | 運用環境の対策方針 OE.PROPER_ADMIN は、A.PROPER_ADMIN により実現される。 |

# 5. セキュリティ要件

本章では、TOE によって満たされなければならない (have to) セキュリティ要件を記述する。これらの要件は、 [CC] のパート 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。以下の表記法が用いられる：

- **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、さらに要件を制約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) : 要件の言明中に [CC] によって提供される 1 つ以上のオプション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、パスワードの長さのような、規定されていないパラメタへ具体的な値を割り付けるために用いられる。角括弧内に表す値は割付を示す。
- **繰返し**操作：括弧内の数字で特定される (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 改訂第 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_RBG_EXT.1 乱数ビット生成サービス**

FCS_RBG_EXT.1.1 アプリケーションは、 [**選択**：

*DRBG 機能を一切利用せずに*、

*プラットフォーム提供の DRBG 機能を起動して*、

*DRBG 機能を実装して*

] その暗号操作を行わなければならない (shall)。

**適用上の注釈**：*DRBG 機能を実装して*が選択される場合、追加の FCS_RBG_EXT.2 エレメントが ST に含まれなければならない (shall)。本要件において、暗号操作には、すべての暗号鍵生成／暗号鍵導出／暗号鍵共有、IV (特定のモードに関して) に加えて、プロトコル特有の乱数値が含まれる。

**保証アクティビティ**

***DRBG 機能を一切利用せずに***が選択された場合、評価者は、アプリケーション及びその開発者証拠資料を検査しなければならない (shall) かつそのアプリケーションが一切の乱数ビット生成サービスを必要としないことを検証しなければならない (shall)。

***DRBG 機能を実装して***が選択された場合、評価者は、追加の FCS_RBG_EXT.2 エレメントが ST に含まれていることを保証しなければならない (shall)。

***プラットフォーム提供の DRBG 機能を起動して***が選択された場合、評価者は、以下のアクティビティを行うこと。

*評価者は、プラットフォーム RBG から乱数を取得するすべての機能が (ST に含まれる SFR に記述されるように) 特定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、これらの機能のそれぞれについて、どのプラットフォームインタフェース (API) を利用して乱数の取得が行われるか TSS に言明されていることを決定しなければならない (shall)。評価者は、これらのインタフェースのそれぞれが、以下の各プラットフォームについて列挙された受け入れ可能なインタフェースに対応していることを確認しなければならない (shall)。次に評価者は、アプリケーション (TOE) に適切な逆コンパイラを用いてアプリケーションバイナリを逆コンパイルしなければならない (shall)。評価者は、逆コンパイラの出力を検索し、TSS に列挙される API のそれぞれについて、その API が出力に現れることを決定しなければならない (shall)。API の表現が以下のリストの文字列に直接対応しない場合、評価者は逆コンパイルされたテキストからそれに対応する API への対応を、API テキストが逆コンパイルされたテキストへ直接対応しない理由の記述と、逆コンパイルされたテキストが関連付けられた API に対応する正当化を含めて、提供しなければならない (shall)。*

*TSS で特定された機能に対して API が「正しく」使用されていることの確認を評価者が試行することは一切期待されないことに留意すべきである (should) ; ここでのアクティビティは、利用される API を列挙すること、そして逆コンパイルによって存在チェックを行うことである。*

*以下は、受け入れ可能な API のプラットフォーム毎のリストである :*

***BlackBerry の場合**：評価者は、アプリケーションが Security Builder Crypto GSE を呼び出すことを検証しなければならない (shall)。*

***Android の場合**: 評価者は、javax.crypto.KeyGenerator クラスまたは java.security.SecureRandom クラスもしくは/dev/random または /dev/urandom の少なくとも 1 つをアプリケーションが使用していることを検証しなければならない (shall)。*

***Windows の場合**：評価者は、クラシックデスクトップアプリケーション用に BCryptGenRandom または CryptGenRandom API が用いられることを検証しなければならない (shall)。評価者は、Windows Universal アプリケーション用に System.Random API が用いられることを検証しなければならない (shall)。本文書の将来のバージョンでは、ベンダ証拠資料により、CryptGenRandom は、選択しとしてはもはや望ましい API ではないため、削除されるかもしれない。*

***iOS の場合**：評価者は、乱数を取得するため、アプリケーションが SecRandomCopyBytes を呼び出すか、/dev/random を直接利用することを検証しなければならない (shall)。*

***Linux の場合**：評価者は、アプリケーションが/dev/random または /dev/urandom から乱数を収集することを検証しなければならない (shall)。*

***Solaris の場合**：評価者は、アプリケーションが/dev/random から乱数を収集することを検証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、乱数を取得するため、アプリケーショ*

*ンが/dev/random を用いることを検証しなければならない (shall)。*

*プラットフォームにより提供される機能の呼び出しが別の方法でなされる場合、評価者はこれがどのように行われるか、またそれがここに列挙された手法とどのように等価であるか(例、高レベルの API が同一の低レベル API を呼び出す) について TSS に記述されていることを保証しなければならない (shall)。*

**FCS_STO_EXT.1 クレデンシャルの格納**

FCS_STO_EXT.1.1　アプリケーションは、不揮発性メモリへ [**選択**：

*一切のクレデンシャルを格納しない、*

*プラットフォームによって提供される機能を呼び出して [**割付**：クレデンシャルのリスト] をセキュアに格納する、*

*[**割付**：クレデンシャルのリスト] をセキュアに格納するための機能を実装する、*

] ようにしなければならない (shall)。

**適用上の注釈**：本要件は、永続的なクレデンシャル (秘密鍵、PKI プライベート鍵、またはパスワード) がセキュアに格納されることを保証する。

保証アクティビティは、プラットフォーム毎の原則で、どの選択が可能かを暗黙的に制限している。例えば、プラットフォームがハードウェアに裏付けられた保護をクレデンシャルの格納用に提供する場合、3 番目の選択肢を指示することはできない。

*クレデンシャルをセキュアに格納するための機能を実装する*が選択される場合、以下のコンポーネントが ST に含まれなければならない (must) : FCS_COP.1(1)。その他の暗号操作がクレデンシャルのセキュアな格納を実装するために用いられる場合、対応する要件が ST に含まれなければならない (must)。

**保証アクティビティ**

*評価者は、ST の要件を満たすために必要なすべての永続的なクレデンシャル (秘密鍵、PKI プライベート鍵、またはパスワード) が TSS に列挙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)。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のために用いられるか、そしてどのように格納されるかについて、TSS に列挙されていることを確認しなければならない (shall)。*

*アプリケーションがプラットフォームにより提供される機能を起動するすべてのクレデンシャルについて、評価者はプラットフォーム毎に異なる以下のアクションを実行しなければならない (shall)。*

***BlackBerry の場合**：評価者は、アプリケーションが BlackBerry KeyStore 及び Security Builder API を用いてクレデンシャルを格納することを検証しなければならない (shall)。*

***Android の場合**：評価者は、アプリケーションが Android KeyStore または Android 鍵チェインを用いてクレデンシャルを格納することを検証しなければならない (shall)。*

***Windows の場合**：評価者は、すべての証明書がWindows Certificate Store に格納されることを検証しなければならない (shall)。評価者は、パスワードのような、その他のクレデンシャルが Windows Credential Manager に格納されるか、Data Protection API (DPAPI) を用いて格納されることを検証しなければならない (shall)。Windows Universal アプリケーションについて、評価者はアプリケーションが ProtectData クラスを利用していること、及びクレデンシャルを IsolatedStorage に格納していることを検証しなければならない (shall)。*

***iOS の場合**：評価者は、すべてのクレデンシャルが鍵チェインの中に格納されることを検証しなければならない (shall)。*

***Linux の場合**：評価者は、すべての鍵がLinux keyrings を用いて格納されることを検証しなければならない (shall)。*

***Solaris の場合**：評価者は、すべての鍵が Solaris Key Management Framework (KMF) を用いて格納されることを検証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、すべてのクレデンシャルが鍵チェインの中に格納されることを検証しなければならない (shall)。*

### 5.1.2 利用者データ保護 (FDP)

#### FDP_DEC_EXT.1 プラットフォーム資源へのアクセス

FDP_DEC_EXT.1.1 アプリケーションは、そのアクセスを以下に制限しなければならない [**選択**：

*ハードウェア資源一切なし*、

*ネットワーク接続性*、

*カメラ*、

*マイクロフォン*、

*位置情報サービス*、

*NFC*、

*USB*、

*Bluetooth*、

*[**割付**：追加のハードウェア資源のリスト]*

] 。

**適用上の注釈：** ここでの意図は、アプリケーションがアクセスするすべてのハードウェア資源が選択に取り込まれていること、及びこれらが正当化されたものに制限されていることを評価者が保証することである。プラットフォームによっては、ハードウェア資源へアクセスするためにアプリケーションが明示的にパーミションを求めなければならない (must) 場合もある。そのようなパーミションを求めることは、例え、そのアプリケーションがそのハードウェア資源を後で利用しない場合であっても、アクセスとみなされるべきである (should)。選択は、基盤となるプラットフォームへのアクセスの必要性をアプリケーションが表

現する方法と一貫した形で表現されるべきである (should)。例えば、プラットフォームはさまざまなハードウェア資源 (例えば、衛星受信器、WiFi、携帯電話) を暗黙に利用する可能性のある*位置情報サービス*を提供するかもしれないが、その場合でも*位置情報サービス*が適切な選択である。これは、これらの資源の利用が推測できるためであるが、また実際の利用が規定のプラットフォームに応じて変動するためでもある。明示的に特定される必要のない資源は、中央演算装置、メインメモリ、ディスプレイ、入力デバイス (例えばキーボード、マウス)、及びプラットフォームによって提供される永続的ストレージデバイス等、任意のアプリケーションによって通常利用されるものである。

**保証アクティビティ▼**

*評価者は、以下のプラットフォーム特有のアクションを実行しなければならない(shall)、また、ハードウェア資源へのアプリケーションのアクセスを決定するため、利用者証拠資料を検査しなければならない (shall)。評価者は、これが指示された選択と一貫していることを保証しなければならない (shall)。評価者は、アプリケーション開発者によって提供される文書をレビューしなければならない(shall)、また、アクセスするような資源のリポジトリのそれぞれについて、アクセスが要求される理由についての正当化を特定しなければならない (shall)。*

***BlackBerry の場合：****評価者は、アプリケーションをインストールして、最初に実行しなければならない (shall)。評価者は、それがアクセスを求めようとするすべてのハードウェア資源が選択に取り込まれていることを検証しなければならない (shall)。注記：利用者が App permissions > Settings > Security and Privacy > Application Permissions > Select application in question を選択すると、どのプラットフォーム資源が承認／拒否されているか、そして変更できるか、列挙される。*

***Android の場合：****評価者は、インストール時 (Android 5.1 及びそれ以前) またはアクセス時 (Android 6.0 及びそれ以降) に、アプリがアクセスしようとするハードウェア資源のそれぞれについて提示されるパーミションを検査しなければならない (shall)。*

***Windows の場合：****Windows Universal アプリケーションの場合、評価者は、必須のハードウェア機能のリストについて WMAppManifest.xml ファイルをチェックしなければならない (shall)。評価者は、アプリケーションが最初にインストールされた際、要求されるハードウェア機能を利用者が認識することを検証しなければならない (shall)。これには、ID_CAP_ISV_CAMERA、ID_CAP_LOCATION、ID_CAP_NETWORKING、ID_CAP_MICROPHONE、ID_CAP_PROXIMITY 等のパーミッションが含まれる。Windows アプリのパーミションの完全なリストは、以下で見つけることができる：*

- *http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx*

*Windows デスクトップアプリケーションについて、評価者は、必須の機微な情報のリポジトリのリストを、アプリケーションソフトウェアまたは証拠資料のいずれかで特定しなければならない (shall)。*

***iOS の場合**：評価者は、アプリケーションまたは証拠資料のいずれかがアクセスするハードウェア資源のリストを提供することを検証しなければならない (shall)。*

***Linux の場合**：評価者は、アプリケーションソフトウェアまたは証拠資料のいずれかがアクセスするハードウェア資源のリストを提供することを検証しなければならない (shall)。*

***Solaris の場合**：評価者は、アプリケーションソフトウェアまたは証拠資料のいずれかがアクセスするハードウェア資源のリストを提供することを検証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、アプリケーションソフトウェアまたは証拠資料のいずれかがアクセスするハードウェア資源のリストを提供することを検証しなければならない (shall)。*

FDP_DEC_EXT.1.2　アプリケーションは、以下へのアクセスを制限しなければならない (shall) [**選択**：

*機微な情報リポジトリなし、*

*アドレス帳、*

*カレンダー、*

*電話帳、*

*システムログ、*

*[**割付**：追加の機微な情報のリポジトリのリスト]*

] 。

**適用上の注釈**: *機微な情報のリポジトリ*は、何らかのアプリケーション、利用者、または利用者役割の間で共有されると期待される可能性があるが、これらのすべてが通常はアクセスを要求するとは限らないものであるような、機微なデータの集まりとして定義される。

**保証アクティビティ**

*評価者は、以下のプラットフォーム特有のアクションを実行しなければならない(shall)、また、機微な情報のリポジトリへのアプリケーションのアクセスを決定するため、利用者証拠資料を検査しなければならない (shall)。評価者は、これが指示された選択と一貫していることを保証しなければならない (shall)。評価者は、アプリケーション開発者によって提供される文書をレビューしなければならない(shall)、また、アクセスするような機微な情報のリポジトリのそれぞれについて、アクセスが要求される理由についての正当化を特定しなければならない (shall)。*

***BlackBerry の場合**：評価者は、アプリケーションをインストールして、最初に実行しなければならない (shall)。評価者は、それがアクセスを求めるような機微な情報リポジトリを特定しなければならない (shall)。*

***Android の場合**：評価者は、インストール時 (Android 5.1 及びそれ以前) またはアクセス時 (Android 6.0 及びそれ以降) に、アプリがアクセスしようとする機微な情報リポジトリのそれぞれについて提示*

*されるパーミションを検査しなければならない (shall)。*

***Windows の場合**：Windows Universal アプリケーションの場合、評価者は、要求される機能のリストについてWMAppManifest.xml ファイルをチェックしなければならない (shall)。評価者は、アプリケーションが最初にインストールされた際、要求される情報リポジトリを特定しなければならない (shall)。これには、ID_CAP_CONTACTS、ID_CAP_APPOINTMENTS、ID_CAP_MEDIALIB などのパーミッションが含まれる。Windows アプリのパーミッションの完全なリストは、以下で得られる：*

- *http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx*

*Windows デスクトップアプリケーションの場合、評価者は、それがアクセスする機微な情報リポジトリのリストを、アプリケーションソフトウェアまたは証拠資料のいずれかで特定しなければならない (shall)。*

***iOS の場合**：評価者は、それがアクセスする機微な情報リポジトリのリストがアプリケーションソフトウェアまたは証拠資料のいずれかで提供されることを検証しなければならない (shall)。*

***Linux の場合**：評価者は、それがアクセスする機微な情報リポジトリのリストがアプリケーションソフトウェアまたは証拠資料のいずれかで提供されることを検証しなければならない (shall)。*

***Solaris の場合**：評価者は、それがアクセスする機微な情報リポジトリのリストがアプリケーションソフトウェアまたは証拠資料のいずれかで提供されることを検証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、それがアクセスする機微な情報リポジトリのリストがアプリケーションソフトウェアまたは証拠資料のいずれかで提供されることを検証しなければならない (shall)。*

**FDP_NET_EXT.1 ネットワーク通信**

FDP_NET_EXT.1.1 アプリケーションはネットワーク通信を以下のものに制約しなければならない (shall) [**選択**：

*ネットワーク通信なし、*

*[**割付**：利用者がネットワーク通信を開始できる機能のリスト] のための利用者によって開始される通信、*

*[**割付**：リモートに開始される通信のリスト] への応答、*

*[**割付**：アプリケーションによって開始されるネットワーク通信のリスト]*

]。

**適用上の注釈**：本要件は、内向きと外向きの両方のネットワーク通信を、要求されるもののみに、または利用者によって開始されるネットワーク通信に制限することを意図している。これは、アプリケーションが一般的にファイルシステムをアクセスし得るネットワーク通信であって、リモートマウントされたドライブ／共有へのプラットフォームのアクセスに帰結し得るものには適用されない。

**保証アクティビティ⮟**

*評価者は、以下のテストを実行しなければならない (shall) :*

- ***テスト 1 :*** *評価者は、アプリケーションを実行しなければならない (shall)。アプリケーションが動作している間、評価者はアプリケーションに関連しないトラフィクをすべて無視しながらネットワークトラフィクをスニッフし、検出されたあらゆるネットワーク通信が TSS に文書化されているか、または利用者によって開始されたものであることを検証しなければならない (shall)。*
- ***テスト 2 :*** *評価者は、アプリケーションを実行しなければならない (shall)。アプリケーションの初期化後、評価者はネットワークポートスキャンを実行し、アプリケーションによってオープンされたあらゆるポートが 3 番目の選択及びその割付として ST に取り込まれていることを検証しなければならない (shall)。これには、コネクションベースのプロトコル (例えば TCP、DCCP) に加えて、コネクションレスプロトコル (例えば UDP) も含まれる。*

***Android の場合 :*** *「ネットワーク通信なし」が選択される場合、評価者は android:name="android.permission.INTERNET" を含む <uses-permission> または <uses-permission-sdk-23> タグがアプリケーションの AndroidManifest.xml ファイルに含まれないことを保証しなければならない (shall)。この場合、プラットフォームがアプリケーションにいかなるネットワーク通信を行うことも許可しないため、上記のテスト 1 及び 2 を行う必要はない。*

**FDP_DAR_EXT.1 機微なアプリケーションデータの暗号化**

FDP_DAR_EXT.1.1 アプリケーションは、不揮発性メモリ中に [**選択** :

*プラットフォームによって提供される機能を活用して機微なデータを暗号化する、*

*機微なデータを暗号化するための機能を実装する、*

*一切の機微なデータを保存しない*

] ようにしなければならない (shall)。

**適用上の注釈** : *機微なデータを暗号化するための機能を実装する*が選択される場合には、*アプリケーションソフトウェアのプロテクションプロファイル拡張パッケージ : ファイル暗号化*に対する評価が要求される。

機微なデータを含む可能性のあるあらゆるファイル (一時ファイルを含む) は、保護されなければならない (shall)。唯一の例外は、利用者が意図的に機微なデータを保護されていないファイルへエクスポートした場合である。

**保証アクティビティ⮟**

*評価者は、アプリケーションがデータを書き込み可能なファイルシステムの場所を棚卸ししなければならない (shall)。評価者は、アプリケーションを実行し、機微なデータの格納を試行しなければならない (shall)。次に評価者は、これらのファイルシステムの領域を検査して*

*(もしあれば) データが格納された場所を突き止め、それが暗号化されていることを決定しなければならない (shall)。*

***一切の機微なデータを保存しない**が選択される場合、評価者は、TSS を検査して、機微なデータがどのように不揮発性メモリへ書込不可能とされているかについて TSS に記述されていることを保証しなければならない (shall)。また評価者は、これが上記のファイルシステムのテストと一貫していることを保証しなければならない (shall)。*

***機微なデータを暗号化するための機能を実装する**が選択される場合、**アプリケーションソフトウェアのプロテクションプロファイル拡張パッケージ: ファイル暗号化**に適合した評価が要求される。評価者は、そのような評価が進行中であることを保証しなければならない (shall)。*

***プラットフォームによって提供される機能を活用して機密性のあるデータを暗号化する**が選択される場合、評価アクティビティは、以下のプラットフォームによって異なる要件に記述されるとおり実行されること。*

***BlackBerry の場合**: 評価者は、TSS を検査して、アプリケーションが Advanced Data at Rest Protection API を利用する方法、及びアプリケーションが適切なドメインを用いて各データファイルを保存し保護する方法が、記述されていることを保証しなければならない (shall)。*

***Android の場合**: 評価者は、TSS を検査して、機微なデータを含むファイルが MODE_PRIVATE フラグをセットして保存される方法が、記述されていることを検証しなければならない (shall)。*

***Windows の場合**: Windows プラットフォームは、現在のところ、アプリケーション開発者による呼び出しに依存するような保存データ暗号化サービスを提供していない。評価者は、利用者操作ガイダンスに、BitLocker または Encrypting File System (EFS) などのプラットフォーム暗号化を有効化する必要性が、エンドユーザへ明確に示されていることを検証しなければならない (shall)。*

***iOS の場合**: 評価者は、TSS を検査して、ローカルに保存される各データファイルについてアプリケーションが Complete Protection、Protected Unless Open、または Protected Until First User Authentication Data Protection Class を用いる方法が記述されていることを保証しなければならない (shall)。*

***Linux の場合**: Linux プラットフォームは、現在のところ、アプリケーション開発者による呼び出しに依存する保存データ暗号化サービスを提供していない。評価者は利用者操作ガイダンスに、プラットフォーム暗号化をアクティベートする必要性が、エンドユーザへ明確に示されていることを検証しなければならない (shall)。*

***Solaris の場合**: Solaris プラットフォームは現在のところ、アプリケーション開発者による呼び出しに依存するような保存データ暗号化サービスを提供していない。評価者は、利用者操作ガイダンスに、プラットフォーム暗号化をアクティベートする必要性が、エンドユーザへ明確に示されていることを検証しなければならない (shall)。*

***Mac OS X の場合**: Mac OS X プラットフォームは、現在のところ、*

*アプリケーション開発者による呼び出しに依存するような保存データ暗号化サービスを提供していない。評価者は、利用者操作ガイダンスに、プラットフォーム暗号化を有効化する必要性が、エンドユーザへ明確に示されていることを検証しなければならない (shall)。*

### 5.1.3 セキュリティ管理 (FMT)

#### FMT_MEC_EXT.1 サポートされる設定メカニズム

FMT_MEC_EXT.1.1　アプリケーションは、設定オプションの格納及び設定のためにプラットフォームベンダによって推奨されるメカニズムを呼び出さなければならない (shall)。

**適用上の注釈**：リモートに格納される設定オプションは、本要件の適用範囲外である。

**保証アクティビティ**

*評価者は、アプリケーションの設定オプション (例、設定) を特定し、これらがプラットフォームによってサポートされるメカニズムを用いて格納及び設定されるかどうかを決定するため、TSS をレビューしなければならない (shall)。最低限 TSS には、あらゆる SFR に関連する設定と SFR に対応した操作ガイダンスで義務付けられたあらゆる設定が列挙されなければならない (shall)。そのようにするための方法は、プラットフォームによって異なる。*

***BlackBerry の場合**：評価者は、アプリケーションを実行してその設定にセキュリティ関係の変更を行わなければならない (shall)。評価者は、アプリケーション作業用ディレクトリの app フォルダにある少なくとも 1 つのファイルが変更され、行われた変更を反映していることをチェックしなければならない (shall)。*

***Android の場合**：評価者は、アプリケーションを実行し、その設定に対してセキュリティ関連の変更を行わなければならない (shall)。評価者は、アプリケーションが設定データの保存に SharedPreferences 及び／または PreferenceActivity のクラスを利用したことを検証するため、/data/data/package/shared_prefs/にある少なくとも 1 つの XML ファイルが設定に行われた変更を反映していることをチェックして、しなければならない (shall)、ここで package は、そのアプリケーションの Java パッケージとする。*

***Windows の場合**：評価者は、Windows Universal アプリケーションが Windows.UI.ApplicationSettings 名前空間または IsolatedStorageSettings 名前空間のいずれかをアプリケーション固有設定の保存に利用していることを検証し、決定しなければならない (shall)。Classic Desktop アプリケーションについては、評価者は、SysInternal ツールの ProcMon で監視しながら、アプリケーションを実行し、その設定に対して変更を行わなければならない (shall)。評価者は、ProcMon ログが Windows Registry への対応する変更を示していることを検証しなければならない (shall)。*

***iOS の場合**：評価者は、アプリがすべての設定の保存に user defaults system または key-value store を用いることを検証しなければならない (shall)。*

***Linux の場合**：評価者は、strace ユーティリティで監視しながらアプリケーションを実行しなければならない (shall)。評価者は、その設定にセキュリティ関連の変更を行わなければならない (shall)。評価者は、/etc (システム固有の設定の場合) または利用者のホームディレクトリ (利用者固有の設定の場合) に存在する設定ファイルへの対応する変更を strace がログ出力することを検証しなければならない (shall)。*

***Solaris の場合**：評価者は、dtrace ユーティリティで監視しながらアプリケーションを実行しなければならない (shall)。評価者は、その設定にセキュリティ関連の変更を行わなければならない (shall)。評価者は、/etc (システム固有の設定の場合) または利用者のホームディレクトリ (利用者固有の設定の場合) に存在する設定ファイルへの対応する変更を dtrace がログ出力することを検証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、アプリケーションが NSUserDefaults クラスを用いて設定の保存及び読み出しを行っていることを検証しなければならない (shall)。*

**FMT_CFG_EXT.1 デフォルトでセキュアな設定**

FMT_CFG_EXT.1.1 アプリケーションは、デフォルトのクレデンシャルまたはクレデンシャルなしで設定されるとき、新たなクレデンシャルを設定するために十分な機能のみを提供しなければならない (shall)。

**適用上の注釈**：デフォルトのクレデンシャルは、アプリケーションのインストール中に自動的に (利用者の介入なしに) プラットフォームへロードされるクレデンシャル (例えば、パスワード、鍵) である。FCS_RBG_EXT.1 に列挙される要件を用いてインストール中に生成されるクレデンシャルは、定義によりデフォルトのクレデンシャルではない。

**保証アクティビティ**

*評価者は、アプリケーションが何らかの種類のクレデンシャルを要求するかどうか、そしてアプリケーションがデフォルトのクレデンシャルと共にインストールされるかどうかを決定するため、TSS をチェックしなければならない (shall)。アプリケーションが何らかのデフォルトのクレデンシャルを利用する場合、評価者は以下のテストを実行しなければならない (shall)。*

- ***テスト 1**：評価者は、新たなクレデンシャルを生成したりロードしたりせずにアプリケーションをインストールして実行し、新たなクレデンシャルを設定するために要求される最小限のアプリケーション機能のみが利用可能であることを検証しなければならない (shall)。*
- ***テスト 2**：評価者は、すべてのクレデンシャルのクリアを試行して、新たなクレデンシャルを設定するために要求される最小限のアプリケーション機能のみが利用可能であることを検証しなければならない (shall)。*
- ***テスト 3**：評価者はアプリケーションを実行し、新たなクレデン*

*シャルを確立して元のデフォルトのクレデンシャルがもはやアプリケーションへのアクセスを提供しないことを検証しなければならない (shall)。*

FMT_CFG_EXT.1.2　アプリケーションは、それとそのデータを許可されないアクセスから保護するようなファイルパーミションを用いて、デフォルトで設定されなければならない (shall)。

**適用上の注釈**：ファイルパーミションの正確な期待は。プラットフォームによって異なるが、一般的な意図としては信頼の境界はアプリケーションとそのデータを保護することである。

**保証アクティビティ⮟**

*評価者は、アプリケーションをインストールして実行しなければならない (shall)。評価者は、プラットフォームのファイルシステムを (可能な範囲内で) アプリケーションによって作成されたファイルがあるかどうか検査して、そのパーミションがそれを保護するために十分であることを保証しなければならない (shall)。そのようにするための手法は、プラットフォームによって異なる。*

***BlackBerry の場合**：評価者は、アプリケーションのデータディレクトリの内部で ls -alR|grep -E '^.....(r|-w|--x)' を実行し、すべてのファイルが (読出、書込、または実行のいずれについても) ワールドアクセス可能でないことを保証しなければならない (shall)。このコマンドは、いかなるファイルもプリントすべきではない (should)。また評価者は、他の任意のアプリケーションによって読出／変更可能な外部ストレージへ書き込まれる機微なデータがないことを検証しなければならない (shall)。*

***Android の場合**：評価者は、アプリケーションのデータディレクトリ内部で ls -alR|grep -E '^.....(r|-w|--x)' を実行し、すべてのファイルが (読出、書込、または実行のいずれについても) ワールドアクセス可能でないことを保証しなければならない (shall)。このコマンドは、いかなるファイルもプリントすべきではない (should)。また評価者は、外部ストレージへ書き込まれる機微なデータがないことを検証しなければならない (shall)。そのようなデータは READ_EXTERNAL_STORAGE または WRITE_EXTERNAL_STORAGE あるいはその両方のパーミッションを含む任意のアプリケーションによって読出／変更できるためである。*

***Windows の場合**：評価者は、SysInternals tools、Process Monitor 及び Access Check (または icacls.exe のような、同等の機能のツール) を Classic Desktop アプリケーションについて実行し、アプリケーションのインストール中にディスクへ書き込まれたファイルが正しいファイルパーミションを持ち、標準的な利用者がアプリケーションまたはそのデータファイルを変更できないことを検証しなければならない (shall)。Windows Universal アプリケーションの場合、評価者は AppContainer サンドボックスのため要件が満たされるとみなさなければならない (shall)。*

***iOS の場合**：評価者は、ローカルに保存されるデータファイルのそれ*

*ぞれについて、アプリケーションが適切な Data Protection Class を活用しているかどうか決定しなければならない (shall)。*

***Linux の場合**：評価者は、アプリケーションのデータディレクトリ内部で find . -perm /007 コマンドを実行し、すべてのファイルが (読出、書込、または実行のいずれについても) ワールドアクセス可能でないことを保証しなければならない (shall)。このコマンドは、いかなるファイルもプリントすべきではない (should)。*

***Solaris の場合**：評価者は、アプリケーションのデータディレクトリ内部で find . ¥( -perm -001 -o -perm -002 -o -perm -004 ¥) コマンドを実行し、すべてのファイルが (読出、書込、または実行のいずれについても) ワールドアクセス可能でないことを保証しなければならない (shall)。このコマンドは、いかなるファイルもプリントすべきではない (should)。*

***Mac OS X の場合**：評価者は、アプリケーションのデータディレクトリ内部で find . -perm +007 コマンドを実行し、すべてのファイルが (読出、書込、または実行のいずれについても) ワールドアクセス可能でないことを保証しなければならない (shall)。このコマンドは、いかなるファイルもプリントすべきではない (should)。*

**FMT_SMF.1 管理機能の仕様**

FMT_SMF.1.1 TSF は、以下の管理機能を実行できなければならない (shall) [**選択**：

*管理機能なし、*

*システムのハードウェア、ソフトウェア、または設定を記述する任意の情報の送信の有効化／無効化、*

*任意の PII の送信の有効化／無効化、*

*任意のアプリケーション状態 (例えばクラッシュダンプ) 情報の送信の有効化／無効化、*

*[**割付**:エンタープライズまたは商用クラウドバックアップシステムのリスト] へのネットワークバックアップ機能の有効化／無効化、*

*[**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]*

] 。

**適用上の注釈**：本要件は、アプリケーションが実際に実装している機能のみを有効化／無効化する能力を提供する必要があることを規定している。アプリケーションは、プラットフォームまたは他のアプリケーションのふるまいをコントロールする責任はない。

**保証アクティビティ▼**

*評価者は、PP によって義務付けられる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しなければならない (shall)。評価者は、アプリケーション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アプリケーションの能力をテストしなければならない (shall)。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*

*すべての方法について、これらの機能をテストすることが期待される。*

### 5.1.4 プライバシー

**FPR_ANO_EXT.1 個人を特定可能な情報の送信に関する利用者の同意**

FPR_ANO_EXT.1.1 アプリケーションは、 [**選択**：

*ネットワーク経由で PII を送信してはならない (shall not)*、

*[**割付**：ネットワーク経由で PII を送信する機能のリスト] を実行する前に利用者の承認を要求しなければならない (shall)*

] 。

**適用上の注釈**：本要件は、アプリケーションによって明確に要求される PII にのみ適用される；アプリケーションからのプロンプトなしに一般的な (または不適切な) データフィールド中に利用者が PII を自発的に提供した場合には適用されない。アプリケーションの開始時に利用者へ提示される、PII を送信する意図を宣言するダイアログボックスは、本要件を満たすのに十分である。

**保証アクティビティ**

*評価者は、PII が送信される可能性のあるアプリケーションの機能を特定するため、TSS 証拠資料を検査して、また以下のテストを実行しなければならない (shall)。*

- ***テスト 1**：評価者はアプリケーションを実行し、PII の送信を担当する機能を行使して、PII の送信前に利用者の承認が要求されることを検証しなければならない (shall)。*

### 5.1.5 TSF の保護 (FPT)

**FPT_API_EXT.1 サポートされるサービス及び API の利用**

FPT_API_EXT.1.1 アプリケーションは、文書化されたプラットフォーム API のみを利用しなければならない (shall)。

**適用上の注釈**：*文書化された*の定義は、アプリケーションが (文書化されたプラットフォーム API に依存する) サードパーティによって提供されるか、あるいはプラットフォーム API のサポートが保証できるかもしれないプラットフォームベンダによって提供されるかによって異なるかもしれない。

**保証アクティビティ**

*評価者は、アプリケーションで利用されるプラットフォーム API が TSS に列挙されていることを検証しなければならない (shall)。次に評価者はこのリストを (例えば開発者アカウント、プラットフォーム開発者グループを介して入手可能な) サポートされる API と比較して、TSS に列挙されるすべての API がサポートされていることを保証しなければならない (shall)。*

**FPT_AEX_EXT.1 悪用防止機能**

FPT_AEX_EXT.1.1　アプリケーションは、 [**割付 :** *明示的な例外のリスト*] を除いて、明示的なアドレスにメモリを割り当てることを要求してはならない (shall not)。

**適用上の注釈 :** 明示的なアドレスにメモリの割り当てを要求することは、アドレス空間配置ランダム化 (ASLR) を阻害する。

**保証アクティビティ⮟**

*評価者は、アプリケーションがコンパイルされる際に ASLR を有効化するために用いられるコンパイラフラグが TSS に記述されていることを保証しなければならない (shall)。評価者は静的または動的な分析を行って、メモリ割り当てが明示的かつ一貫したアドレスに配置されないことを決定しなければならない (shall)。そのようにするための手法は、プラットフォームによって異なる。*

***BlackBerry の場合 :*** *評価者は、2 つの異なる BlackBerry システム上で同一のアプリケーションを実行し、そのアプリケーションに割り当てられたすべてのメモリアドレスを列挙するツールを実行しなければならない (shall)。次に評価者は、2 つの異なるインスタンスが割り当てロケーションを共有していないことを検証しなければならない (shall)。*

***Android の場合 :*** *評価者は、2 つの異なる Android システム上で同一のアプリケーションを実行しなければならない (shall)。ADB 経由で接続し、/proc/PID/maps を検査する。2 つの異なるインスタンスが割り当てロケーションを共有していないことを保証する。*

***Windows の場合 :*** *評価者は、2 つの異なる Windows システム上で同一のアプリケーションを実行し、そのアプリケーションに割り当てられたすべてのメモリアドレスを列挙するツールを実行しなければならない (shall)。次に評価者は、2 つの異なるインスタンスが割り当てロケーションを共有していないことを検証しなければならない (shall)。Microsoft の sysinternals ツール VMMap を用いて、実行中アプリケーションのメモリアドレスを閲覧することが可能である。評価者は、Microsoft の BinScope Binary Analyzer などのツールを用いて、アプリケーションが ASLR 有効化されていることを確認しなければならない (shall)。*

***iOS の場合 :*** *評価者は、静的な分析を行ってあらゆる mmap 呼び出し (または mmap を呼び出す API 呼び出し) を検索し、固定アドレスへの割り当てを要求する引数が提供されていないことを保証しなければならない (shall)。*

***Linux の場合 :*** *評価者は、2 つの異なる Linux システム上で同一のアプリケーションを実行しなければならない (shall)。次に評価者は、pmap -x PID を用いてこれらのメモリマップを比較して、2 つの異なるインスタンスが割り当てロケーションを共有していないことを保証しなければならない (shall)。*

***Solaris の場合 :*** *評価者は、2 つの異なる Solaris システム上で同一のアプリケーションを実行しなければならない (shall)。次に評価者は、pmap -x PID を用いてこれらのメモリマップを比較して、2 つの異なるインスタンスが割り当てロケーションを共有していないことを保*

*証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、2 つの異なる Mac OS X システム上で同一のアプリケーションを実行しなければならない (shall)。次に評価者は、vmmap PID を用いてこれらのメモリマップを比較して、2 つの異なるインスタンスが割り当てロケーションを共有していないことを保証しなければならない (shall)。*

FPT_AEX_EXT.1.2　アプリケーションは、 [**選択**：

*書込及び実行の両方のパーミションを持ついかなるメモリ領域も割り付けてはならない (shall not)、*

*[**割付**：実行時 (just-in-time) コンパイルを行う機能のリスト] のみに書込及び実行のパーミションを持つメモリ領域を割り付けなければならない (shall)*

] 。

**適用上の注釈**：書込及び実行の両方のパーミションを持つメモリマッピングを要求することは、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。アプリケーションが実行時コンパイルを実行しない場合、最初の選択が選ばれなければならない (must)。

**保証アクティビティ**

*評価者は、メモリマッピングが書込及び実行パーミションと共に要求されることが一切ないことを検証しなければならない (shall)。そのようにするための方法は、プラットフォームによって異なる。*

***BlackBerry の場合**：評価者は、以下を検証するため、アプリケーションについて静的な分析を実行しなければならない(shall)*

- *PROT_WRITE と PROT_EXEC の両方のパーミションと共に mmap が呼び出されることがなく、また*
- *mprotect が呼び出されることがない。*

***Android の場合**：評価者は、以下を検証するため、アプリケーションについて静的な分析を実行しなければならない(shall)*

- *PROT_WRITE と PROT_EXEC の両方のパーミションと共に mmap が呼び出されることがなく、また*
- *mprotect が呼び出されることがない。*

***Windows の場合**：評価者は、Microsoft の BinScope Binary Analyzer などのツールを用いて、アプリケーションが NXCheck を渡すことを確認しなければならない (shall)。また評価者は、コンパイル中に /NXCOMPAT フラグが使われていることを保証して、アプリケーションに DEP 保護が有効化されていることを検証してもよい。*

***iOS の場合**：評価者は、アプリケーションに静的な分析を行って、PROT_EXEC パーミションと共に mprotect が呼び出されることがないことを検証しなければならない (shall)。*

***Linux の場合**：評価者は、アプリケーションに静的な分析を行って、*

- *PROT_WRITE と PROT_EXEC の両方のパーミションと共に mmap が呼び出されることがなく、また*
- *PROT_EXEC パーミションと共に mprotect が呼び出されることがない*

*ことの両方を検証しなければならない (shall)。*

***Solaris の場合**：評価者は、アプリケーションに静的な分析を行って、*

- *PROT_WRITE と PROT_EXEC の両方のパーミションと共に mmap が呼び出されることがなく、また*
- *PROT_EXEC パーミションと共に mprotect が呼び出されることがない*

*ことの両方を検証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、アプリケーションに静的な分析を行って、PROT_EXEC パーミションと共に mprotect が呼び出されることがないことを検証しなければならない (shall)。*

FPT_AEX_EXT.1.3　アプリケーションは、プラットフォームベンダによって提供されるセキュリティ機能と適合性がなければならない (shall)。

**適用上の注釈**：本要件は、アプリケーションが動作するためにプラットフォームのセキュリティ機能が無効化される必要がないことを保証するようにデザインされている。

**保証アクティビティ⮟**

*評価者は、付与されたようにプラットフォームを設定し、指示されるテストの 1 つを実施しなければならない (shall)：*

***BlackBerry の場合**：評価者は、BlackBerry OS の最新バージョン上でアプリケーションの動作が成功することを保証しなければならない (shall)。*

***Android の場合**：評価者は、Android の最新バージョン上でアプリケーションの動作が成功することを保証しなければならない (shall)。*

***Windows の場合**：クラシックデスクトップと Windows Universal の両方のアプリケーションについて、評価者は Microsoft の Enhanced Mitigation Experience Toolkit (EMET) の最新バージョンを設定してアプリケーションを保護しなければならない (shall)。次に評価者はアプリケーションを動作させ、アプリケーションが EMET によって保護されている間にクラッシュしないことを検証しなければならない (shall)。*

***iOS の場合**：評価者は、iOS の最新バージョン上でアプリケーションの動作が成功することを保証しなければならない (shall)。*

***Linux の場合**：評価者は、SELinux が有効化され実施されたシステム上でアプリケーションの動作が成功することを保証しなければならない (shall)。*

***Solaris の場合**：評価者は、Solaris Trusted Extensions が有効化され実施された状態でアプリケーションが動作することを保証しなけれ*

*ばならない (shall)。*

***Mac OS X の場合**：評価者は、OS X の最新バージョン上でアプリケーションの動作が成功することを保証しなければならない (shall)。*

FPT_AEX_EXT.1.4　アプリケーションは、利用者による明示的な指示がない限り、実行可能ファイルを含むディレクトリへ利用者によって変更可能なファイルを書き込んではならない (shall not)。

**適用上の注釈**：実行可能形式と利用者によって変更可能なファイルは同一の親ディレクトリを共有してはならないが、親の上位のディレクトリを共有してもよい。

**保証アクティビティ⮟**

*評価者はアプリケーションを実行し、どこにそのファイルを書き込むか決定しなければならない (shall)。利用者が書き込み先を選ばなかった場合のファイルについて、評価者は、書き込み先ディレクトリに実行可能ファイルが含まれるかどうかをチェックしなければならない (shall)。これはプラットフォームによって異なる：*

***BlackBerry の場合**：評価者は、アプリケーションがすべてのデータをアプリケーション作業ディレクトリ (サンドボックス) 内へ書き込むことをプラットフォームが強制するため、要件が満たされるとみなさなければならない (shall)。*

***Android の場合**：評価者は、通常の利用方法を模倣してプログラムを実行し、すべてのファイルがどこに書き込まれるか記録しなければならない (shall)。評価者は、/data/data/package/ (ここで package はアプリケーションの Java パッケージ) 配下に格納される実行可能ファイルが存在しないことを保証しなければならない (shall)。*

***Windows の場合**：Windows Universal アプリケーションの場合、アプリケーションがすべてのデータをアプリケーション作業ディレクトリ (サンドボックス) 内へ書き込むことをプラットフォームが強制するため、評価者は要件が満たされるとみなさなければならない (shall)。Windows Desktop アプリケーションの場合、評価者は通常の利用方法を模倣してプログラムを実行し、すべてのファイルがどこに書き込まれるか記録しなければならない (shall)。評価者は、アプリケーションが書き込むのと同一のディレクトリに格納される実行可能ファイルが存在せず、アプリケーションのインストールディレクトリ中にデータファイルが存在しないことを保証しなければならない (shall)。*

***iOS の場合**：評価者は、アプリケーションがすべてのデータをアプリケーション作業ディレクトリ (サンドボックス) 内へ書き込むことをプラットフォームが強制するため、要件が満たされるとみなさなければならない (shall)。*

***Linux の場合**：評価者は、通常の利用方法を模倣してプログラムを実行し、すべてのファイルがどこに書き込まれるか記録しなければならない (shall)。評価者は、アプリケーションが書き込むのと同一のディレクトリに格納される実行可能ファイルが存在しないことを保証しなければならない (shall)。*

***Solaris の場合**：評価者は、通常の利用方法を模倣してプログラムを実行し、すべてのファイルがどこに書き込まれるか記録しなければならない (shall)。評価者は、アプリケーションが書き込むのと同一のディレクトリに格納される実行可能ファイルが存在しないことを保証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、通常の利用方法を模倣してプログラムを実行し、すべてのファイルがどこに書き込まれるか記録しなければならない (shall)。評価者は、アプリケーションが書き込むのと同一のディレクトリに格納される実行可能ファイルが存在しないことを保証しなければならない (shall)。*

FPT_AEX_EXT.1.5　アプリケーションは、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 (shall)。

**保証アクティビティ▼**

*評価者は、アプリケーションにおける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するために用いられるコンパイラフラグが ST の TSS セクションに記述されていることを保証しなければならない (shall)。評価者は静的な分析を行って、スタックベースのバッファオーバーフロー保護が存在することを検証しなければならない (shall)。そのようにするための手法は、プラットフォームによって異なる：*

***BlackBerry の場合**：評価者は、-fstack-protector-strong または-fstack-protector-all フラグが用いられることを保証しなければならない (shall)。-fstack-protector-all フラグが望ましいが、-fstack-protector-strong も受容可能である。*

***Android の場合**：完全に Java のアプリケーションは Java マシン中で動作するため、通常のスタック保護は必要としない。Java Native Interface (JNI) を利用するアプリケーションの場合、評価者は-fstack-protector-strong または-fstack-protector-all フラグが用いられることを保証しなければならない (shall)。-fstack-protector-all フラグが望ましいが、-fstack-protector-strong も受容可能である。*

***Windows の場合**：評価者は TSS をレビューして、コンパイル中に /GS フラグが用いられたことを検証しなければならない (shall)。評価者は、/GS の正しい使い方を検証できる、BinScope のようなツールを実行しなければならない (shall)。*

***iOS の場合**：アプリケーションが GCC または Xcode を用いてコンパイルされる場合、評価者は-fstack-protector-strong または-fstack-protector-all フラグが用いられることを保証しなければならない (shall)。-fstack-protector-all フラグが望ましいが、-fstack-protector-strong も受容可能である。アプリケーションが何らかのその他のコンパイラを用いてビルドされる場合、評価者はビルドプロセス中に適切なスタック保護が用いられたことを決定しなければならない (shall)。*

***Linux の場合**：アプリケーションが GCC を用いてコンパイルされる場合、評価者は-fstack-protector-strong または-fstack-protector-all フラグが用いられることを保証しなければならない (shall)。-fstack-*

*protector-all フラグが望ましいが、-fstack-protector-strong も受容可能である。アプリケーションが clang を用いてビルドされる場合、-fsanitize=address フラグと共にコンパイル及びリンクされなければならない (must)。アプリケーションが何らかのその他のコンパイラを用いてビルドされる場合、評価者はビルドプロセス中に適切なスタック保護が用いられたことを決定しなければならない (shall)。*

***Solaris の場合**：アプリケーションが GCC を用いてコンパイルされる場合、評価者は-fstack-protector-strong または-fstack-protector-all フラグが用いられることを保証しなければならない (shall)。-fstack-protector-all フラグが望ましいが、-fstack-protector-strong も受容可能である。アプリケーションが clang を用いてビルドされる場合、-fsanitize=address フラグと共にコンパイル及びリンクされなければならない (must)。アプリケーションが何らかのその他のコンパイラを用いてビルドされる場合、評価者はビルドプロセス中に適切なスタック保護が用いられたことを決定しなければならない (shall)。*

***Mac OS X の場合**：アプリケーションが GCC または Xcode を用いてコンパイルされる場合、評価者は-fstack-protector-strong または-fstack-protector-all フラグが用いられることを保証しなければならない (shall)。-fstack-protector-all フラグが望ましいが、-fstack-protector-strong も受容可能である。アプリケーションが何らかのその他のコンパイラを用いてビルドされる場合、評価者はビルドプロセス中に適切なスタック保護が用いられたことを決定しなければならない (shall)。*

**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　アプリケーションは、アプリケーションソフトウェアへのアップデート及びパッチをチェックする [**選択**：*能力を提供*、*ためにプラットフォームを活用*] しなければならない (shall)。

**適用上の注釈**：本要件は、アップデートを「チェック」する能力に関する。任意のアップデートの実際のインストールは、プラットフォームによって行われるべきである (should)。本要件は、アップデートがベンダによって提供されていることをアプリケーションがチェックできると保証することを意図している。他のソースによって提供されたアップデートには、悪意のあるコードが含まれるおそれがあるからである。

**保証アクティビティ▼**

*評価者は、文書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、アプリケーションがエラーを発行しないことを検証しなければならない (shall)。アップデートされた場合、またはアップデートが利用できないと報告された場合、本要件は満たされたとみなされる。*

FPT_TUD_EXT.1.2　アプリケーションは、プラットフォームによってサポートされるパッケージマネージャのフォーマットを用いて配付されなければならない (shall)。

**保証アクティビティ▼**

*評価者は、アプリケーションのアップデートがプラットフォームによ*

*ってサポートされるフォーマットで配付されることを検証しなければならない (shall)。これはプラットフォームによって異なる：*

***BlackBerry の場合**：評価者は、アプリケーションが Blackberry (BAR) フォーマットでパッケージされることを保証しなければならない (shall)。*

***Android の場合**：評価者は、アプリケーションが Android アプリケーションパッケージ (APK) フォーマットでパッケージされることを保証しなければならない (shall)。*

***Windows の場合**：評価者は、アプリケーションが標準 Windows Installer (.MSI) フォーマット、Microsoft Authenticode プロセスを用いて署名された Windows Application Software (.EXE) フォーマット、または Windows Universal Application パッケージ (.APPX) フォーマットでパッケージされていることを保証しなければならない (shall)。Authenticode 書名に関する詳細に関しては、https://msdn.microsoft.com/en-us/library/ms537364(v=vs.85).aspx を参照されたい。*

***iOS の場合**：評価者は、アプリケーションが IPA フォーマットでパッケージされることを保証しなければならない (shall)。*

***Linux の場合**：評価者は、選択されたディストリビューションのパッケージ管理インフラストラクチャのフォーマットでアプリケーションがパッケージされることを保証しなければならない (shall)。例えば、Red Hat 及び Red Hat 派生ディストリビューション上で動作するアプリケーションは、RPM フォーマットでパッケージされるべきである (should)。Debian 及び Debian 派生ディストリビューション上で動作するアプリケーションは、deb フォーマットでパッケージされるべきである (should)。*

***Solaris の場合**：評価者は、アプリケーションが PKG フォーマットでパッケージされることを保証しなければならない (shall)。*

***Mac OS X の場合**：評価者は、アプリケーションが DMG フォーマット、PKG フォーマット、または MPKG フォーマットでパッケージされることを保証しなければならない (shall)。*

FPT_TUD_EXT.1.3　アプリケーションはその削除の結果として、設定、出力ファイル、及び監査／ログ事象を例外として、アプリケーションのすべての痕跡が削除されるようにパッケージされなければならない (shall)。

**適用上の注釈**：システム／ファームウェアイメージとバンドルされたアプリケーションは、OS によって提供される手段で利用者がアプリケーションを削除できない場合、本要件に従属しない。

**保証アクティビティ▼**

*評価者は、アプリケーションのインストールに先立って全ファイルシステム上のすべてのファイルのパスを記録し、次にアプリケーションをインストールして実行しなければならない (shall)。その後、評価者はアプリケーションをアンインストールし、結果として得られたファイルシステムを最初の記録と比較して、設定、出力、及び監査／ログファイル以外に、ファイルシステムに追加されたファイルがないこと*

*を検証しなければならない (shall)。*

FPT_TUD_EXT.1.4　アプリケーションは、それ自身のバイナリコードをダウンロードしたり、変更したり、置換したり、アップデートしてはならない (shall not)。

**適用上の注釈**：本要件は、アプリケーションのコードに適用される。これは、アプリケーションによってダウンロードされ実行されるようにデザインされるモバイルコード技術には適用されない。

**保証アクティビティ**

*評価者は、アプリケーションの実行可能ファイルがアプリケーションによって変更されないことを検証しなければならない (shall)。評価者は、以下のテストを完了しなければならない (shall)：*

- ***テスト 1**：評価者はアプリケーションをインストールし、その後その実行ファイルすべての場所を規定しなければならない (shall)。次に評価者は、各ファイルについて、ファイルのハッシュまたはファイルそのもののコピーを別途保存しなければならない (shall)。次に評価者はアプリケーションを実行し、TSS に記述されているようにアプリケーションのすべての機能を行使しなければならない (shall)。次に評価者は各実行可能ファイルをそのファイルの保存されたハッシュまたは保存されたコピーのいずれかと比較しなければならない (shall)。評価者は、これらが同一であることを検証しなければならない (shall)。*

FPT_TUD_EXT.1.5　アプリケーションは、アプリケーションソフトウェアの現バージョンを問い合わせる **[選択、**少なくとも 1 つ：*能力を提供*、*ためにプラットフォームを活用* ] しなければならない (shall)。

**保証アクティビティ**

*評価者は、利用者操作ガイダンス (AGD_OPE.1) に従ってソフトウェアの現バージョンをアプリケーションに問い合わせなければならず (shall)、文書化されインストールされたバージョンと現バージョンが一致することを検証しなければならない (shall)。*

FPT_TUD_EXT.1.6　アプリケーションのインストールパッケージ及びそのアップデートは、そのプラットフォームがそれらをインストール前に暗号技術的に検証できるようにディジタル署名されなければならない (shall)。

**適用上の注釈**：インストールパッケージ及びアップデートの検証の詳細には (アプリケーションに関する要件ではなく) プラットフォームに関する要件が関係するので、これらはここで完全には規定されない。

**保証アクティビティ**

*評価者は、アプリケーションのインストールパッケージ及びそれへのアップデートが正当なソースによってどのように署名されるか、TSS に特定されていることを検証しなければならない (shall)。正当なソースの定義は、TSS に含まれなければならない (must)。また評価者は、アップデート候補がどのように取得されるか、TSS (または操作*

*ガイダンス) に記述されていることを保証しなければならない (shall)。*

**FPT_LIB_EXT.1 サードパーティライブラリの利用**

FPT_LIB_EXT.1.1　アプリケーションは、 [**割付**：*サードパーティライブラリのリスト*] のみとパッケージされなければならない (shall)。

**適用上の注釈**：本要件の意図は、アプリケーションが不必要または予期されないサードパーティライブラリを含んでいるかどうかを評価者が検出及び文書化できることである。これには、プライバシーの脅威を引き起こすおそれのあるアドウェアライブラリや、後に脆弱性が発見された場合のために、そのようなライブラリの文書化を保証することが含まれる。

**保証アクティビティ**

*評価者はアプリケーションをインストールし、そのダイナミックライブラリがインストールされるディレクトリを調査しなければならない (shall)。評価者は、アプリケーションと共にパッケージされている、またはアプリケーションによって利用されることが判明したライブラリが、割付中のものに制限されていることを検証しなければならない (shall)。*

### 5.1.6 高信頼パス／チャネル (FTP)

**FTP_DIT_EXT.1 通過中データの保護**

FTP_DIT_EXT.1.1　アプリケーションは、それ自身と別の高信頼 IT 製品との間で [**選択**：

*あらゆるデータを送信しない*、

*あらゆる機微なデータを送信しない*、

*すべての送信される機微なデータを [**選択**、少なくとも 1 つ：HTTPS、TLS、DTLS、セキュアシェルの拡張パッケージに適合する SSH] で暗号化する*、

*すべての送信されるデータを [**選択**、少なくとも 1 つ:HTTPS、TLS、DTLS、SSH] で暗号化する*

] ようにしなければならない (shall)。

**適用上の注釈**：拡張パッケージは、本要件を上書きしてその他のプロトコルを提供してもよい。暗号化は、機微でないデータを送信するアプリケーションには要求されない。

*TLS* が選択される場合には、FCS_TLSC_EXT.1 からのエレメントの評価が要求される。

*HTTPS* が選択される場合には、FCS_HTTPS_EXT.1 からのエレメントの評価が要求される。

*DTLS* が選択される場合には、FCS_DTLS_EXT.1 からのエレメントの評価が要求される。

*SSH* が選択される場合、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 (shall)。

**保証アクティビティ▼**

*評価者は、以下のテストを実行しなければならない (shall)。*

- ***テスト 1**：評価者は、アプリケーションからのパケットをキャプチャしながらアプリケーションを行使 (例えばリモートシステムまたはウェブサイトへ接続することによって、データの送信を試行) しなければならない (shall)。評価者はパケットキャプチャから、トラフィックが ST 中の選択に従って HTTPS、TLS、DTLS で暗号化されていることを検証しなければならない (shall)。*
- ***テスト 2**：評価者は、アプリケーションからのパケットをキャプチャしながらアプリケーションを行使 (例えばリモートシステムまたはウェブサイトへ接続することによって、データの送信を試行) しなければならない (shall)。評価者はパケットキャプチャをレビューして、機微なデータが平文で送信されていないことを検証しなければならない (shall)。*
- ***テスト 3**：評価者は TSS を検査して、利用者クレデンシャルが送信されるかどうかを決定しなければならない (shall)。クレデンシャルが送信される場合、評価者はクレデンシャルを既知の値に設定しなければならない (shall)。評価者は、TSS 中に記述されるようにクレデンシャルが送信されるようにしながら、アプリケーションからのパケットをキャプチャしなければならない (shall)。評価者はキャプチャされたネットワークパケットの文字列検索を行って、評価者によって先ほど設定された平文のクレデンシャルが見つからないことを検証しなければならない (shall)。*

***Android の場合**：「一切のデータを送信しない」が選択される場合、評価者は android:name="android.permission.INTERNET" を含む <uses-permission> または <uses-permission-sdk-23> タグがアプリケーションの AndroidManifest.xml ファイルに含まれないことを保証しなければならない (shall)。この場合、プラットフォームがアプリケーションにいかなるネットワーク通信を行うことも許可しないため、上記のテスト 1、2 または 3 を行う必要はない。*

***iOS の場合**：「すべての送信されるデータを暗号化する」が選択される場合、評価者はアプリケーションの Info.plist ファイルに NSAllowsArbitraryLoads または NSExceptionAllowsInsecureHTTPLoads キーが含まれないことを保証しなければならない (shall)。これらのキーは、iOS の Application Transport Security 機能を無効化するためである。*

## 5.2 セキュリティ保証要件

セクション 5 の TOE のセキュリティ対策方針は、セクション 3.1 で特定された脅威へ対処するために構築された。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具体化である。本 PP は、評価者が評価に利用可能な証拠資料を評価し、また独立テストを実行するような範囲を設定するために、セキュリティ保証要件 (SAR) を特定する。

本セクションには、本 PP に対する評価に要求される CC パート 3 からの一連の SAR が列挙されている。実行されるべき個別の保証アクティビティ (AA) 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 に適合するために作成された ST に適合する TOE 評価の一般的なモデルは、以下のようなものである：

ST が評価に適していると承認された後、情報技術セキュリティ評価機関 (ITSEF) は、TOE と支援 IT 環境、及び TOE の管理者／利用者ガイドを入手すること。ITSEF は、ASE 及び ALC の SAR に関して共通評価方法 (CEM) によって義務付けられたアクションを実行することが期待されている。また ITSEF は、TOE に具現化された特定の技術に適用される他の CEM 保証要件の解釈として意図されたものであるセクション 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と。セクション 5 で取り込まれた保証アクティビティは、TOE 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説明も提供している。

### 5.2.1 ASE クラス：セキュリティターゲット

[CEM] に定義された ASE アクティビティによる。

### 5.2.2 ADV クラス：開発

TOE に関する情報は、ST の TSS 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。TSS に含まれる製品の記述は機能仕様と関連するため、TOE 開発者はこれに同意しなければならない (must)。セクション 5.1 に含まれる保証アクティビティは、TSS セクションにふさわしい内容を決定するために十分な情報を ST 作成者に提供すべきである (should)。

**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 (shall)。

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 (shall)。

**適用上の注釈**：本セクションの概論で述べたように、機能仕様は AGD_OPR 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。機能要件中の保証アクティビティは、文書及び TSS セクションに存在すべき (should) 証拠資料を参照している。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 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

**内容・提示エレメント：**

ADV_FSP.1.1C 機能仕様には、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 (shall)。

ADV_FSP.1.2C 機能仕様には、SFR 実施、及び SFR 支援の各 TSFI に関連するすべてのパラメタが識別しなければならない (shall)。

ADV_FSP.1.3C 機能仕様には、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 (shall)。

ADV_FSP.1.4C 追跡は、機能仕様での TSF I に対する SFR からへの追跡を実証するものでなければならない (shall)。

**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 (shall)。

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 (shall)。

**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。機能仕様文書はセクション 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。機能仕様情報の内容についての要件は、行われるその他の保証アクティビティの特質により暗黙に評定される。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アクティビティを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いなかったことになる。*

### 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に対する役割を果たすことができることを IT 要員が検証する方法の記述が含まれなければならない (must)。この文書は、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 (should)。ガイダンスは、ST で主張されたとおり製品がサポートしているすべての運用環境に関して提供されなければならない (must)。このガイダンスには、その環境への TSF のインストールを成功させるための指示、及び製品として、またより大規模な運用環境のコンポーネントとして、TSF のセキュリティを管理するための指示が含まれる。規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。そのようなガイダンスに関する要件は、各要件と共に規定された保証アクティビティに含まれている。

**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 (shall)。

**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。必要に応じて、ガイダンス文書はセキュリティの自動化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。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 (should)。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 (shall)。

**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、TOE によって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利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 (shall)。

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 (shall)。

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 (shall)。

AGD_OPE.1.5C 利用者操作ガイダンスは、TOE 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の維持するために必要なことを識別しなければならない (shall)。

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 (shall)。

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 (shall)。

**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 (shall)。

**保証アクティビティ**

*操作ガイダンスの内容の一部は、セクション5.1 の保証アクティビティ、及び [CEM] に従った TOE の評価によって検証されることになる。また、以下の追加情報も必要となる。暗号機能が TOE によって提供される場合、TOE の評価される構成と関連付けられた暗号エンジンを設定するための指示が操作ガイダンスに含まれなければならない (shall)。TOE の CC 評価の中で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、管理者へ与えられなければならない (shall)。文書には、ディ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)。これは TOE によって行われても、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、このプロセスに以下の手順が含まれることを検証しなければならない (shall)：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、規定のディレクトリへの格納) が含まれるべきである (should)。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／ディジタル署名の生成が含まれる。本 PP 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、操作ガイダンスは管理者に対して明確にしなければならない (shall)。*

**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 TOE を提供しなければならない (shall)。

**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 (should)。

**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 TOE のセキュアな受入れに必要なすべてのステップが記述しなければならない (shall)。

AGD_PRE.1.2C 準備手続きには、TOE のセキュアな設置、及び ST に記述される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 (shall)。

**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・提示に関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 (shall)。

AGD_PRE.1.2E 評価者は、TOE が運用に向けてセキュアに準備され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 (shall)。

**保証アクティビティ**

*上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の設定にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST の中で TOE について主張されているすべてのプラットフォームへ十分に対応していることをチェックして保証しなければならない (shall)。*

### 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 TOE 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 TOE 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プラクティスが果たす重要な役割を軽視する意味ではなく、この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、TOE 及び TOE の参照を提供しなければならない (shall)。

**内容・提示エレメント**：

ALC_CMC.1.1C TOE は、その一意な参照でラベル付けされなければならない (shall)。

**適用上の注釈**：一意な参照情報には、以下のものが含まれる：

- アプリケーションの名称
- アプリケーションのバージョン
- アプリケーションの記述
- アプリケーションが動作するプラットフォーム
- 利用可能な場合、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・提示に関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 (shall)。

**保証アクティビティ▼**

*評価者は ST をチェックして、ST の要件を満たすバージョンを具体的に特定する識別情報 (製品名／バージョン番号など) が含まれていることを保証しなければならない (shall)。さらに、評価者は AGD ガイダンス及びテスト用に受け取った TOE サンプルをチェックして、バージョン番号が ST のものと一貫していることを保証しなければならない (shall)。ベンダが TOE を宣伝するウェブサイトを維持管理している場合、評価者はそのウェブサイト上の情報を検査して、ST の情報がその製品を識別するために十分であることを保証しなければならない (shall)。*

**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、TOE の構成リストを提供しなければならない (shall)。

**内容・提示エレメント**：

ALC_CMS.1.1C　構成リストは、TOE 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 (shall)。

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 (shall)。

**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・提示に関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 (shall)。

**保証アクティビティ▼**

*本 PP において「SAR が要求する評価証拠」は、ST 中の情報と、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られる。TOE が具体的に特定され、その識別情報が ST 及び AGD ガイダンスの中で一貫していることを (ALC_CMC.1 に関する評価アクティビティで実行されるとおりに) 保証することによって、評価者はこのコンポーネントによって要求される情報を暗黙に確認する。ライフサイクルサポートは、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の提供者への指示を目的としている。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軽視する意味ではなく、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。*

*評価者は、開発者が (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文書中で) 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において利用に適当な 1 つ以上の開発環境を特定していることを保証しなければならない (shall)。これらの開発環境のそれぞれについて、開発者は 1 つまたは複数の環境におけるバッファオーバーフロー保護メカニズムの発動が保証される*

*ように環境を設定する方法 (例えば、コンパイラのフラグ) に関する情報を提供しなければならない (shall)。評価者は、そのような保護がデフォルトでオンとなっているか、または具体的に有効化されなければならない (have to) のかという指摘もまたこの文書に含まれていることを保証しなければならない (shall)。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 中の要件と関連して開発者から提供される文書が、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しなければならない (shall)。*

**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、TOE にタイムリーなセキュリティアップデートが行われる方法の記述を TSS 中に提供しなければならない (shall)。

**注記**：アプリケーション開発者は、セキュリティ脆弱性を修正する目的で自分の製品へのアップデートをサポートしなければならない (must)。

ALC_TSU_EXT.1.2D 開発者は、アップデートが製品の設定またはセキュリティ特性を変更する際どのように利用者へ通知されるかの記述を TSS に提供しなければならない (shall)。

**内容・提示エレメント**：

ALC_TSU_EXT.1.1C この記述には、TOE ソフトウェアへのセキュリティアップデートを作成し展開するためのプロセスが含まれなければならない (shall)。

ALC_TSU_EXT.1.2C その記述には、脆弱性の公的な開示から TOE 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、日単位の時間の長さとしてタイムウィンドウが明示されなければならない (shall)。

ALC_TSU_EXT.1.3C その記述には、TOE に関連するセキュリティ問題を報告するため公的に利用可能なメカニズムが含まれなければならない (shall)。

**注記**：報告メカニズムには、ウェブサイト、電子メールアドレス、そして報告の機微な性質を保護するための手段 (例えば、悪用の概念実証の詳細を暗号化するために用いることができる公開鍵) が含まれるかもしれない。

**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資料の内容・提示に関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 (shall)*。

**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しなければならない (shall)。評価者は、この記述がアプリケーション全体に対応することを検証しなければならない (shall)。また評価者は、TOE 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の中で対応されていることも検証しなければならない (shall)。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しなければならない (shall)。*

*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 TOE 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 に列挙されていることを検証しなければならない (shall)。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ていることを検証しなければならない (shall)。*

*評価者は、TOE に関連するセキュリティ問題を報告するため公的に利用可能なメカニズム (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しなければならない (shall)。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 (shall)。*

### 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で、テストは、設計情報の利用可能性に依存し、公開されていう r 機能とインタフェースに基づいて行われる。評価プロセスの主要なアウトプットの 1 つは、以下の要件に規定されるような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 TOE を提供しなければならない (shall)。

**内容・提示エレメント**：

ATE_IND.1.1C　TOE は、テストに適していなければならない (shall)。

**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 (shall)*。

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 (shall)。

**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アプリケーションをテストしなければならない (shall)。

**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、システムの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しなければならない (shall)。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 (shall)。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カバーする。*

*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 (must)。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違いに対応し、行われるべきテストにその違いが影響しないという論拠を示さなければならない (must)。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 (must)。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。評価者には、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 (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供されるべきである (should)。*

*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, SSH) によって用いられるものである。テスト計画書には、上位レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も特定される。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 (shall)。つまりテストの実行が失敗し、修正がインストールされ、そして次にテストの再実行が成功したという結果が得られた場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示されるであろう。*

### 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現時点の世代については、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者を超える巧妙さが必要とされる。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 TOE 中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文書を考慮して、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、テストのために TOE を提供しなければならない (shall)。

**内容・提示エレメント**：

AVA_VAN.1.1C　TOE は、テストに適していなければならない (shall)。

**適用上の注釈**：テストに適当とは、評価者による静的または動的な分析を混乱させるような、あいまい化またはパッケージ化が行われていないことを意味する。

**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 (shall)。

AVA_VAN.1.2E　評価者は、TOE の潜在的脆弱性を識別するために、公知の情報源の検索を実行しなければならない (shall)。

**適用上の注釈**：パブリックドメイン情報源には、公知の脆弱性に関する共通脆弱性及び暴露 (CVE) 辞書が含まれる。またパブリックドメイン情報源には、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 TOE 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 (shall)。

**保証アクティビティ▼**

*評価者は報告書を作成し、本要件に関連する自分たちの結論を文書化しなければならない (shall)。この報告書は、物理的には ATE_IND に言及される全体的なテスト報告書の一部であってもよいし、あるいは別個の文書であってもよい。評価者は公開情報の検索を行い、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。また評価者はアプリケーションのファイルに対してウィルススキャナを最新のウィルス定義と共に実行し、どのファイルも悪意があるとフラグされないことを検証しなければならない (shall)。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いであろうから、適切な正当化が策定されることになるであろう。*

# 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 (TOE によって行われなければならない (must) 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 に規定されている。(本附属書中の) 第 1 の種類は、ST に含まれ得る要件であるが、TOE 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 中の) 第 2 の種類は、PP の本体中の選択に基づく要件である。規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 (must)。(附属書 C 中の) 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 (例えば、FMT タイプの要件) もまた、ST へ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_CKM.1(2) 暗号対称鍵生成**

FCS_CKM.1.1(2) アプリケーションは、FCS_RBG_EXT.1 に規定される乱数ビット生成器及び以下に規定される暗号鍵長を用いて対称暗号鍵を生成しなければならない (shall) [**選択**：

*128 ビット*、

*256 ビット*

] 。

**適用上の注釈**：対称鍵は、鍵チェインと共に鍵の生成に用いられるかもしれない。

**保証アクティビティ▼**

***TSS***

*評価者は TSS をレビューして、FCS_RBG_EXT.1 によって記述される機能が呼び出される方法が記述されていることを決定しなければならない (shall)。*

*アプリケーションがホストプラットフォームの乱数ビット生成に依存している場合、評価者は TSS に、その外部 RBG の名称／製造業者が含まれること、及びその外部 DRBG 機能を呼び出す際に用いられる関数呼び出し及びパラメタが記述されていることを検証しなければならない (shall)。異なるプラットフォームに異なる RBG が用いられる場合、評価者は TSS に各プラットフォームの各 RBG が特定されていることを検証しなければならない (shall)。また評価者は、その外部 DRBG にシードを供給するエントロピーの量のベンダの見積もりの短い記述が 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、FCS_RBG_EXT または運用環境で利用可能な文書の中の RBG 機能の記述を用いて、要求されている鍵サイズが利用者データの暗号化／復号に用いられる鍵サイズ及びモードと同一であることを決定する。*

**FCS_TLSC_EXT.2 TLS クライアントプロトコル**

FCS_TLSC_EXT.2.1　アプリケーションは、X.509v3 証明書を用いた相互認証をサポートしなければならない (shall)。

**適用上の注釈**：TLS の X.509v3 証明書の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、TLS 相互認証を行う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 (must) 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しなければならない (shall)。*

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

- ***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)：*
  - *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中の 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、接続が成功しないことを検証しなければならない (shall)。*

# B. 選択ベースの要件

本 PP の概論で示したように、本 PP の本体にはベースライン要件 (TOE 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 (must) もの) が含まれている。これ以外にも PP の本体中の選択に基づく追加的要件が存在し、規定の選択がなされた場合には、以下の追加的要件が含まれることが必要となる。

**FCS_RBG_EXT.2 アプリケーションによる乱数ビット生成**

FCS_RBG_EXT.2.1　アプリケーションは、[**選択**：H*ash_DRBG (任意)* 、*HMAC_DRBG (任意)* 、*CTR_DRBG (AES)*] を用いる NIST Special Publication 800-90A 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 (shall) 。

> ***本要件は、FCS_RBG_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：本要件は、FCS_RBG_EXT.1.1 中で *DRBG 機能を実装して*が選択されている ST に含まれなければならない (shall)。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 (should)。

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。

**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、以下のテストを実行しなければならない (shall)。*
>
> *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 つのテストを実施しなければならない (shall)。「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、可変シードテストを実行しなければならない (shall)。評価者は (Seed, DT) ペアの 128 個のセット (それぞれ 128 ビット) を TSF の RBG 機能に提供しなければならない (shall)。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) 鍵も提供しなければならない (shall)。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 (shall not)。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実行しなければならない (shall)。このテストについては、評価者がシード及び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) 鍵も提供しなければならない (shall)。次に評価者はTSF のRBG を、繰返しのたびにDT の値を1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション3 に規定されるように次回の繰返しの際の新たなシードを作成して、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 回の試行を行わなければならない (shall)。RNG が設定可能な場合、評価者は各設定について 15 回の試行を行わなければならない (shall)。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しなければならない (shall)。*

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

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

  ***エントロピー入力**：エントロピー入力値の長さは、シードの長さ*

*と等しくなければならない (must)。*

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

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

FCS_RBG_EXT.2.2　決定論的 RBG は、プラットフォームベースの DRBG 及び [**選択**：

*ソフトウェアベースのノイズ源*、

*その他のノイズ源なし*

] であって、最小で [**選択**：

*128 ビット*、

*256 ビット*

] の、それが生成する鍵とハッシュの (NIST SP 800-57 による) セキュリティ強度の最も大きいもの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、シードが供給されなければならない (shall)。

***本要件は、FCS_RBG_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：本要件は、FCS_RBG_EXT.1.1 中で *DRBG 機能を実装して*が選択されている ST に含まれなければならない (shall)。本要件中の最初の選択について、アプリケーションの 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。アプリケーションは、その DRBG へのシードを供給するためにプラットフォームの DRBG を用いなければならない (must) ことに注意されたい。

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) 及び AES 256 (セキュリティ強度 256 ビット) が含まれる場合、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 D 及びエントロピーの文書化と評定の明確化附属書に従って、*

*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))。*

*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_CKM_EXT.1 暗号鍵生成サービス**

FCS_CKM_EXT.1.1 アプリケーションは、 [**選択**：

*非対称暗号鍵を生成しない*、

*プラットフォームによって提供される機能を呼び出して非対称鍵を生成する*、

*非対称鍵の生成を実装する*

] ようにしなければならない (shall)。

***本要件は、FCS_TLSC_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：*非対称鍵の生成を実装する*または*プラットフォームによって提供される機能を呼び出して非対称鍵を生成する*が選択される場合には、追加的な FCS_CKM.1(1) エレメントが ST に含まれなければならない (shall)。

**保証アクティビティ**

*評価者はアプリケーション及びその開発者文書を検査して、アプリケーションが非対称鍵生成サービスを必要とするかどうかを決定しなければならない (shall)。必要ない場合、評価者は**非対称暗号鍵を生成しない**選択が ST 中で行われていることを検証しなければならない (shall)。それ以外の場合、評価アクティビティが選択ベースの要件中に言明されるように行われなければならない (shall)。*

**FCS_CKM.1(1) 暗号非対称鍵生成**

FCS_CKM.1.1(1) アプリケーションは、以下に規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 (shall) [**選択**：

***[RSA スキーム] [2048 ビット以上]** の暗号鍵長を用い、以下を満たすもの： **[選択：***

***FIPS PUB 186-4, “Digital Signature Standard (DSS)”、附属書 B.3、***

***ANSI X9.31-1998、セクション 4.1***

*]*,

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

***[FFC スキーム] [2048 ビット以上]** の暗号鍵長を用い、以下を満たすもの： **[FIPS PUB 186-4, “Digital Signature Standard (DSS)”,***

***Appendix B.1]***

] 。

> ***本要件は、FCS_CKM_EXT.1.1 中の選択に依存する。***

**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 (shall)。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 (must)。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。

TOE 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、TOE 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。現状では、モダンな 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、TOE のサポートする鍵長が TSS に特定されていることを保証しなければならない (shall)。ST に 2 つ以上のスキームが規定されている場合、評価者は TSS を検査して各スキームの用途が特定されていることを検証しなければならない (shall)。*
>
> *評価者は、本 PP に定義されるすべての利用について、選択された 1 つまたは複数の鍵生成スキーム及び 1 つまたは複数の鍵長を用いるように TOE を設定する方法が AGD ガイダンスで管理者へ指示されていることを検証しなければならない (shall)。*
>
> *アプリケーションが**プラットフォームによって提供される機能を呼び出して非対称鍵を生成する**場合には、評価者は TSS を検査して鍵生成機能がどのように呼び出されるか記述されていることを検証しなければならない (shall)。*
>
> *アプリケーションが**非対称鍵の生成を実装する**場合には、以下のテストアクティビティが実施されなければならない (shall)。*
>
> *保証アクティビティの注釈 : 以下のテストには、アプリケーションのエンドユーザには通常利用できないツールを評価者へ提供する開発者環境へのアクセスを、開発者が提供することが要求されるかもしれない。*
>
> ***FIPS PUB 186-4 RSA スキームのための鍵生成***
>
> *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、公開鍵検証指数 e、秘密素因数 p 及び q、公開モジュラス (modulus) n 及び秘密署名指数 d の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。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) を規定している。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 (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)*

*ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (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)。*

*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 (should)。それ以外の場合、評価者はサポートされている鍵の長さ nlen のそれぞれについて TSF に 10 個の鍵ペアを生成させ、以下を検証しなければならない (shall)。*

- *n = p*q、*
- *p 及び q が、Miller-Rabin にしたがう確率的素数であること、*
- *GCD(p-1,e) = 1、*
- *GCD(q-1,e) = 1、*
- *2^16 <= e <= 2^256 かつ e は奇整数、*
- *|p-q| > 2^(nlen/2 - 100)、*
- *p >= squareroot(2)*( 2^(nlen/2 -1) )、*
- *q >= squareroot(2)*( 2^(nlen/2 -1) )、*
- *2^(nlen/2) < d < LCM(p-1,q-1)、*
- *e*d = 1 mod 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しなければならない (shall)。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しなければならない (shall)。*

- *TSS には、TOE 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 (shall)。*

- *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 (shall)」でない言明 (すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」) のすべてにおいて、そのようなオプションを TOE 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 (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE 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 (shall)。*
- *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 (shall)」または「すべきである (should)」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 (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*

*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) に生成させなければならない (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)。正しさを決定するため、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) 機能へ提出しなければならない (shall)。*

*FIPS 186-4 公開鍵検証 (PKV) テスト*

*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 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (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***

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

*暗号素数及びフィールド素数 :*

- *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する (shall)*

*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している。*

*暗号群生成元：*

- *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*

*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している。プライベート鍵：*

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

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

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

*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)。*

**FCS_CKM.2 暗号鍵確立**

FCS_CKM.2.1 アプリケーションは、[**選択：** *プラットフォームによって提供される機能を呼び出し、機能を実装し*] て以下に規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 (shall)：

**[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”]***、

***[有限体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*

]。

| ***本要件は、FCS_TLSC_EXT.1.1 中の選択に依存する。*** |
|---|

**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 (shall)。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。TOE 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、TOE 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(1) に規定される曲線と相関しなければならない (shall)。

有限体ベースの鍵確立スキームに用いられるドメインパラメタは、FCS_CKM.1.1(1) に従う鍵生成によって規定される。

**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 で特定された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 に 2 つ以上のスキームが特定されている場合、評価者は TSS を検査して各スキームの用途が識別されていることを検証しなければならない (shall)。*<br><br>*評価者は、選択された 1 つまたは複数の鍵確立スキームを用いるように TOE を設定する方法が AGD ガイダンスで管理者へ指示されていることを検証しなければならない (shall)。*<br><br>*保証アクティビティの注釈 : 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。*<br><br>***鍵確立スキーム***<br><br>*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)。*<br><br>***SP800-56A 鍵確立スキーム***<br><br>*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)。各鍵共有スキーム向けのこれらの検証テストは、勧告中の仕様にしたがった鍵共有スキームのコンポーネントが TOE に実装されていることを検証するものである。これらのコンポーネントには、DLC プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵材料 (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証しなければならない (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***

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

*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)。*

*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)。*

*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、TSF は上記を行わなければならない (shall)。*

***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 TOE の能力を検証する。このテストを実施するため評価者は、SP800-56A 鍵共有実装に含まれるサポートする暗号機能のリストを取得し、どのエラーを TOE が認識可能であるべきか (should) を決定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 認可曲線、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。*

*評価者はテストベクタの一部にエラーを注入し、以下のフィールドが不正であるために生じる無効な鍵共有結果を TOE が認識することをテストしなければならない (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、公開鍵検証機能または部分的な鍵検証機能 (ECC の*

*み)、 あるいはその両方におけるエラーを TOE が検出でき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 (shall)、したがって有効な鍵共有結果をもたらすべきである (should) (これらのテストベクタは合格すべきである (should))。*

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

***SP800-56B 鍵確立スキーム***

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

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

*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 が使わ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)。*

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

*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、出力された平文の鍵材料 (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)。*

*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 にしたがい、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)。*

**FCS_COP.1(1) 暗号操作—暗号化／復号**

FCS_COP.1.1(1) アプリケーションは、以下の規定された暗号アルゴリズム

- AES-CBC (NIST SP 800-38A に定義) モード；

及び [**選択**：

*AES-GCM (NIST SP 800-38D に定義)、*

*その他のモードなし*

] ならびに暗号鍵長 256 ビット及び [**選択**：*128 ビット、その他の鍵長なし*] に従って暗号化／復号を実行しなければならない (shall)。

***本要件は、FCS_TLSC_EXT.1.1、FCS_STO_EXT.1.1 中の選択に依存する。***

**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 (should)。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 (should)。128 ビットの鍵長は、FCS_TLSC_EXT.1 及び FCS_CKM.1(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AGD 文書をチェックして、要求されるモード及び鍵長に機能を設定するために行われることが必要とされる設定があれば、それが存在することを決定する。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)。*

***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する (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しなければならない (shall)。*

- *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)。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)。*
- *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 (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)。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)。*
- *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 (shall)、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 (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)。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 (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する (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)。*

- *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)。*

*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***

*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)。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*

*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 (shall)、100 個は 256 ビットの鍵を用いるものとする (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]
```

*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)。*

*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 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 の認証済み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*
- *2 つの平文の長さ. 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)。*
- *3 通りの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)。*
- *2 通りの 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)。*

*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。*

*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、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)。*

*各テストの結果は、直接評価者によって、あるいは入力を実装者へ供給しその結果を受領することによって、取得され得る。正しさを決定するため、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)。*

**FCS_COP.1(2) 暗号操作—ハッシュ**

FCS_COP.1.1(2) アプリケーションは、規定されたアルゴリズム [**選択**：

*SHA-1*、

*SHA-256*、

*SHA-384*、

*SHA-512*、

*その他のアルゴリズムなし*

] 及びメッセージダイジェストサイズ [**選択**：

*160*、

*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実行しなければならない (shall)。

| ***本要件は、FCS_TLSC_EXT.1.1 中の選択に依存する。*** |
|---|

**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 に適合するため要求されている。FCS_TLSC_EXT.1.1 が ST に含まれる場合、FCS_COP.1(2) のハッシュアルゴリズムの選択が、FCS_TLSC_EXT.1.1 の必須及び選択された暗号スイートで用いられるハッシュアルゴリズムと一致しなければならない (must)。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、ハッシュ関数を規定することである。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 (must)。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すべきである (should) (例えば、128 ビットの鍵については SHA 256)。

**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 (例えば、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しなければならない (shall)。*<br><br>*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。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)。* |
|---|

*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。*
- ***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。*
- ***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。i 番目のメッセージの長さは 512 + 99*i となる (ここで 1 ≤ i ≤ 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。*
- ***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。i 番目のメッセージの長さは 512 + 8*99*i となる (ここで 1 ≤ i ≤ 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。*
- ***テスト5**：疑似ランダム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。*

**FCS_COP.1(3) 暗号操作—署名**

FCS_COP.1.1(3) アプリケーションは、以下の識別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) を実行しなければならない (shall) [**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*

] 。

***本要件は、FCS_TLSC_EXT.1.1 中の選択に依存する。***

**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 (should)。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規定するために繰り返されるべきである (should)。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規定すべきである (should)。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わなければならない (shall)。*

*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 (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しなければならない (shall)。*
- ***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 (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*

- ***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 TOE による RSA 署名生成の実装を検証しなければならない (shall)。このテストを行うために評価者は、TSF のサポートする*

*法サイズ／SHA の組み合わせのそれぞれについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない (must)。評価者は、TOE に自分のプライベート鍵と法の値を用いてこれらのメッセージへ署名させなければならない (shall)。評価者は、既知の良好な実装及び関連付けられた公開鍵を用いて署名を検証することによって、TSF の署名の正しさを検証しなければならない (shall)。*

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

**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) アプリケーションは、以下の規定された暗号アルゴリズム

- HMAC-SHA-256

及び [**選択**：

*SHA-1*、

*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 256 及び [**選択**：*160*、*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* と 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実行しなければならない (shall)。

***本要件は、FCS_TLSC_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：本要件の意図は、アプリケーションによって用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) 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規定することである。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 (must)。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 (should)。HMAC-SHA256 は、FCS_TLSC_EXT.1 に要求される暗号スイートへ適合するため要求される。

**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わなければならない (shall)。*

*サポートされてい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るものとする (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、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 (shall)。*

**FCS_TLSC_EXT.1 TLS クライアントプロトコル**

FCS_TLSC_EXT.1.1 アプリケーションは、以下の暗号スイートをサポートして [**選択**：*プラットフォームによって提供される TLS 1.2 を呼び出さ、TLS 1.2 (RFC 5246) を実装し*] なければならない (shall)：

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

オプションの暗号スイート：[**選択**：

*RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*、

*RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*、

*RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*、

*RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*、

*RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*、

*RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*、

*RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*、

*RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*、

*RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*、

*RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*、

*RFC 5246 で定義された TLS_RSA_WITH_AES_128_CBC_SHA256*、

*RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA256*、

*その他の暗号スイートなし*

] 。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**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 (should)。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、「なし」が選択されるべきである (should)。テスト環境中のサーバ上で評価される構成において管理的に用いられることが可能な暗号スイートを制限することは必要である。上に列挙した Suite B アルゴリズム (RFC 6460) は、実装に望ましい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要求されている。

これらの要件は、IETF によって新たな TLS バージョンが標準化されるに伴って再検討されることになる。

ECDHE を用いるいずれかの暗号スイートが選択される場合には、FCS_TLSC_EXT.4 が要求される。

*TLS 1.2 (RFC 5246) を実装し*が選択される場合には、FCS_CKM.2、FCS_CKM_EXT.1、FCS_COP.1(1)、FCS_COP.1(2)、FCS_COP.1(3)、及び FCS_COP.1(4) が要求される。

**保証アクティビティ▼**

*評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが規定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、規定された暗号スイートがこのコンポーネントに列挙されたものを含むことを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述と適合するように TOE を設定するための指示が含まれることを保証しなければならない (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)：*

- ***テスト 1**：評価者は、要件に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、EAP セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィクの特徴を検査する必要はない。*
- ***テスト 2**：評価者は、extendedKeyUsage フィールド中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 フィールド中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)。*
- ***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一致しないサーバ証明書を TLS 接続中に送信しなければならな*

*い (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 証明書を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 証明書を送信したりする。) 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) 。*

- ***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)。*
- ***テスト 5**：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)：*
  - ***テスト 5.1**:ServerHello 中のサーバによって選択される TLS バージョンを、サポートされない TLS バージョン (例えば 03 04 の 2 バイトによって表現される 1.3) に変更し、クライアントが接続を拒否することを検証する。*
  - ***テスト 5.2**：ServerHello ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、ServerKeyExchange ハンドシェイクメッセージをクライアントが拒否すること (DHE または ECDHE 暗号スイートの場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。*
  - ***テスト 5.3**：ServerHello ハンドシェイクメッセージ中のサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージ中に提示されない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない (shall) 。*
  - ***テスト 5.4**：サーバの KeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange の受信後に接続を拒否することを検証する。*
  - ***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。*
  - ***テスト 5.6**：クライアントが ChangeCipherSpec メッセージを発行した後にサーバから歪曲されたメッセージを送信し、クライアントが接続を拒否することを検証する。*

FCS_TLSC_EXT.1.2　アプリケーションは、RFC 6125 に従って提示された識別子が参照識別子と一致することを検証しなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：識別子の検証のルールは、RFC 6125 のセクション 6 に記述されている。参照識別子はアプリケーションサービスに応じて、利用者 (例えばウェブブラウザへの URL 入力またはリンクのクリック)

によって、設定 (例えばメールサーバまたは認証サーバの名前の設定) によって、またはアプリケーション (例えば API のパラメタ) によって確立される。単一の参照識別子の生成元ドメイン及びアプリケーションサービス種別 (例えば、HTTP、SIP、LDAP) に基づき、クライアントは受容可能なすべての参照識別子、例えば証明書のサブジェクト名 (Subject Name) フィールドの共通名 (Common Name) ならびにサブジェクトの別名 (Subject Alternative Name) 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 (Service Name) を確立する。次にクライアントはこのすべての受容可能な参照識別子のリストを、TLS サーバの証明書中に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るサブジェクトの別名である。共通名を用いる検証は、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の別名中の 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 (should)。しかし、提示された識別子がワイルドカードを含む場合、クライアントはマッチングに関するベストプラクティスに従わなければならない (must)。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、どの種類の参照識別子がサポートされているか (例えば共通名、DNS 名、URI 名、サービス名、またはその他のアプリケーション特有のサブジェクトの別名) ならびに IP アドレス及びワイルドカードがサポートされているかどうかを含め、アプリケーションに設定された参照識別子からすべての参照識別子を確立するクライアントの手法が TSS に記述されていることを保証しなければならない (shall)。評価者はこの記述に、TOE によって Certificate Pinning がサポートされるか、または利用されるかどうか、及びその方法が規定されていることを保証しなければならない (shall)。*

*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)。*

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

- ***テスト 1** : 評価者は、参照識別子に一致する識別子をサブジェクトの別名 (SAN) にも共通名 (CN) にも含まないサーバ証明書を提示しなければならない (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)。*
- ***テスト 2** : 評価者は、参照識別子に一致する CN を含み、SAN 拡張を含むが、参照識別子に一致する識別子を 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)。*
- ***テスト 3** : 評価者は、参照識別子に一致する 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)。*

- ***テスト 4****:評価者は、参照識別子に一致しない CN を含むが、SAN には一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)。*
- ***テスト 5****:評価者は、参照識別子のサポートされる種別のそれぞれについて、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):*
  - ***テスト 5.1****: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)。*
  - ***テスト 5.2****:評価者は、左端のラベル中だ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、証明書中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.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)。*
  - ***テスト 5.3****:評価者は、パブリックなサフィックスの直前の左端のラベルにワイルドカードを含む (例えば、*.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.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.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)。*
- ***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 フィールド中に正しい 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)。*
- ***テスト 7****: [条件付き] Pinning された証明書がサポートされている場合、評価者は Pinning された証明書に一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 アプリケーションは、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 (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**: 有効性は RFC 5280 に従って、識別子の検証、認証パス、有効期限、及び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 のために行われるテストに従ってテストされなければならない (shall)。

TLS 接続に関しては、ピア証明書が無効である場合にこのチャネルが確立されてはならない (shall not)。HTTPS は TLS 上に実装されるが、HTTPS プロトコル (FCS_HTTPS_EXT.1) では異なるふるまいが要求される。本エレメントは、HTTPS 以外の TLS 接続に対応する。

**保証アクティビティ**

*評価者は TLS を機能として用いて FIA_X509_EXT.1.1 中の証明書有効性確認ルールが遵守されることを検証しなければならず (shall)、また以下の追加的テストを実行しなければならない (shall)。*

- ***テスト 1**: 評価者は、有効な認証パスのない証明書を使用すると、認証が失敗することを論証しなければならない (shall)。次に評価者は管理ガイダンスを用いて、ピアの証明書の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、接続が成功することを論証しなければならない (shall)。次に評価者は、CA 証明書の 1 つを削除して、接続が失敗することを示さなければならない (shall)。*

### FCS_TLSC_EXT.4 TLS クライアントプロトコル

FCS_TLSC_EXT.4.1 アプリケーションは、Client Hello 中の Supported Elliptic Curves Extension に以下の NIST 曲線を提示しなければならない (shall) : [**選択**：*secp256r1*、*secp384r1*、*secp521r1*] 及びその他の曲線なし。

***本要件は、FCS_TLSC_EXT.1.1、FCS_TLSS_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：本要件は、認証及び鍵共有のために許可される楕円曲線を、FCS_COP.1(3) 及び FCS_CKM.1(1) ならびに FCS_CKM.2 からの NIST 曲線に制限する。この拡張は、楕円曲線暗号スイートをサポートするクライアントについて要求される。

**保証アクティビティ**

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

*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) :*

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

**FCS_TLSS_EXT.1 TLS サーバプロトコル**

FCS_TLSS_EXT.1.1 アプリケーションは、以下の暗号スイートをサポートして [**選択**：*プラットフォームによって提供される TLS 1.2 を呼び出さ、TLS 1.2 (RFC 5246) を実装し*] なければならない (shall)：

必須の暗号スイート：

RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA

オプションの暗号スイート： [**選択**：

*RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256、*

*RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256、*

*RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256、*

*RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256、*

*RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384、*

*RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、*

*RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256、*

*RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256、*

*RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384、*

*RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、*

*RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256、*

*RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256、*

*その他の暗号スイートなし*

] 。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**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 (should)。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、「なし」が選択されるべきである (should)。テスト環境中のサーバ上で評価される構成において管理的に用いられることが可能な暗号スイートを制限することは必要である。上に列挙した 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要求されている。

これらの要件は、IETF によって新たな TLS バージョンが標準化されるに伴って再検討されることになる。

ECDHE を用いるいずれかの暗号スイートが選択される場合には、FCS_TLSC_EXT.4 が要求される。

TLS 1.2 (RFC 5246) を実装しが選択される場合には、FCS_CKM.2.1、FCS_COP.1.1(1)、FCS_COP.1.1(2)、FCS_COP.1.1(3)、及び FCS_COP.1.1(4) が要求される。

**保証アクティビティ**

*評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが規定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、規定された暗号スイートがこのコンポーネントに列挙されたものを含むことを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述と適合するように TOE を設定するための指示が含まれることを保証しなければならない (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)：*

- ***テスト 1**：評価者は、要件に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、EAP セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィクの特徴を検査する必要はない。*
- ***テスト 2**：評価者は、サーバの ST 中の暗号スイートのいずれをも含まない暗号スイートのリストと共に Client Hello をサーバへ送信し、サーバが接続を拒否することを検証しなければならない (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)。*
- ***テスト 3**：評価者は、クライアントを用いてサーバによって選択された暗号スイートと一致しない鍵交換メッセージを TLS 接続中に送信しなければならない (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 鍵交換を送信したり、ECDSA 暗号スイート*

*のいずれかを使用しているのに RSA 鍵交換を送信したりする。)*
*評価者は、アプリケーションが鍵交換メッセージを受信した後に切断することを検証しなければならない (shall) 。*

- ***テスト 4**：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)：*
  - ***テスト 4.1**:ServerHello 中のサーバによって選択される TLS バージョンを、サポートされない TLS バージョン (例えば 03 04 の 2 バイトによって表現される 1.3) に変更し、クライアントが接続を拒否することを検証する。*
  - ***テスト 4.2**:Client Hello ハンドシェイクメッセージ中のクライアントのノンス中の少なくとも 1 バイトを改変して、クライアントの Certificate Verify ハンドシェイクメッセージをサーバが拒否すること (相互認証を用いる場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。*
  - ***テスト 4.3**：クライアントの Key Exchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントの Certificate Verify ハンドシェイクメッセージをサーバが拒否すること (相互認証を用いる場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。*
  - ***テスト 4.4**：Client Finished ハンドシェイクメッセージ中の 1 バイトを改変して、サーバが接続を拒否しアプリケーションデータを全く送信しないことを検証する。*
  - ***テスト 4.5**:クライアントが ChangeCipherSpec メッセージを送信する前にクライアントから Finished メッセージを送信することによって fatal alert を生成させた後、先ほどのテストからのセション識別子と共に Client Hello を送信し、サーバが接続を拒否することを検証する。*
  - ***テスト 4.6**:クライアントが ChangeCipherSpec メッセージを発行した後にクライアントから歪曲されたメッセージを送信し、サーバが接続を拒否することを検証する。*

FCS_TLSS_EXT.1.2 アプリケーションは、SSL 1.0、SSL 2.0、SSL 3.0、TLS 1.0、TLS 1.1、及び [**選択**：*TLS 1.2、なし*] を要求するクライアントからの接続を拒否しなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：SSL のすべてのバージョンと TLS 1.0 及び 1.1 は拒否される。FCS_TLSS_EXT.1.1 において選択されなかったあらゆる TLS のバージョンが、ここで選択されるべきである (should)。

**保証アクティビティ**

*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、また本要件を満たすために必要な設定があればそれは*

*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)。*

- ***テスト 1：評価者は、バージョン SSL 2.0 での接続を要求する Client Hello を送信し、サーバが接続を拒否することを検証しなければならない (shall)。評価者はこのテストを SSL 3.0、TLS 1.0、TLS 1.1、及び TLS 1.2 が選択された場合はそれについて繰り返さなければならない (shall)。***

FCS_TLSS_EXT.1.3 アプリケーションは、サイズ 2048 ビット及び [**選択**：*3072 ビット、4096 ビット、その他のサイズなし*] の RSA 及び [**選択**：*NIST 曲線 [**選択**：secp256r, secp384r] 及びその他の曲線なし、 サイズ 2048 ビット及び [**選択**：3072 ビット、その他のサイズなし] の Diffie-Hellman パラメタ、その他なし*] を用いて鍵確立パラメタを生成しなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：ST で DHE 暗号スイートが FCS_TLSS_EXT.1.1 に列挙されている場合、ST には本要件中の Diffie-Hellman の選択が含まれなければならない (must)

**保証アクティビティ**

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

*評価者は、要件を満たすために必要な任意の設定ガイダンスが 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)。*

- ***テスト 1：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 メッセージ中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)。(サイズが、設定された曲線に期待されるサイズと一致することを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 NIST 楕円曲線のそれぞれとサポートされる Diffie-Hellman 鍵長のそれぞれについて、繰り返さなければならない (shall)。***

FCS_TLSS_EXT.1.4 アプリケーションは、X.509v3 証明書を用いた TLS クライアントの相互認証をサポートしなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

FCS_TLSS_EXT.1.5 アプリケーションは、ピア証明書が無効である場合に高信頼チャネルを確立してはならない (shall not)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**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、この利用に TLS 相互認証のためのクライアント側証明書のサポートが含まれなければならない (must) ことを追加する。有効性は RFC 5280 に従って、認証パス、有効期限、及び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 のために行われるテストに従ってテストされなければならない (shall)。

**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しなければならない (shall)。*

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

- ***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)、そしてクライアントから証明書を送信することなく接続を試行しなければならない (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)。*
- ***テスト 2**：評価者は、クライアントの証明書によって用いられる supported_signature_algorithm なしで証明書要求をクライアントへ送信するようサーバを設定しなければならない (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)。*
- ***テスト 3**：評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを論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論証しなければならない (shall)。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 (shall)。*
- ***テスト 4**：評価者は、サーバの Certificate Request メッセージ中の認証局 (ルートまたは CA のいずれか) の 1 つへ連鎖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)。*
- ***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)。*
- ***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サーバを設定し、次*

*にクライアントの証明書中の 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中の 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.1.6 アプリケーションは、証明書に含まれる識別名 (DN) またはサブジェクトの別名 (SAN) がピアに期待される識別子に一致しない場合、高信頼チャネルを確立してはならない (shall not)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：ピア識別子は、証明書の Subject フィールドまたは Subject Alternative Name 拡張に存在し得る。期待される識別子は、設定されてもよいし、あるいはピアによって用いられるドメイン名、IP アドレス、利用者名、または電子メールアドレスと比較されたり、あるいは比較のためディレクトリサーバへ渡されたりしてもよい。マッチングは、ビットごとの比較によって行われるべきである (should)。

**保証アクティビティ**

*TOE が相互認証を実装する場合、評価者は証明書中の DN 及び 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)。*

*DN が自動的にドメイン名または IP アドレス、利用者名、もしくは電子メールアドレスと比較されない場合、評価者はその接続に期待される識別子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)。*

- ***テスト 1**：評価者は、期待される識別子と一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)。*

**FCS_DTLS_EXT.1 DTLS の実装**

FCS_DTLS_EXT.1.1 アプリケーションは、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 (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**保証アクティビティ**

- ***テスト 1**：評価者は、DTLS サーバとの接続を試行し、パケットアナライザでトラフィクを確認し、そして接続が成功しトラフィクが DTLS として特定されることを検証しなければならない (shall)。*

  *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　アプリケーションは、DTLS 1.2 (RFC 6347) に従った変動が許可される場合を除き、DTLS の実装には TLS (FCS_TLSC_EXT.1) 中の要件を実装しなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**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。したがって、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 の実装に適用される。

**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行わなければならない (shall)。*

FCS_DTLS_EXT.1.3　アプリケーションは、ピア証明書が無効とみなされる場合には高信頼チャネルを確立してはならない (shall not)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：有効性は RFC 5280 に従って、認証パス、有効期限、及び失効状態によって決定される。

**保証アクティビティ▼**

*証明書の有効性は FIA_X509_EXT.1 のために行われるテストに従ってテストされなければならず (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)。*

- ***テスト 1**:評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを論証しなければならない (shall)。次に評価者は、管理ガイダンスを利用して、その機能で使われる証明書の有効性確認に必要とされるトラストアンカーデータベースへ 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しなければならない (shall)。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 (shall)。*

**FCS_HTTPS_EXT.1 HTTPS プロトコル**

FCS_HTTPS_EXT.1.1アプリケーションは、RFC 2818 に適合する HTTPS プロトコルを実装しなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**保証アクティビティ▼**

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

FCS_HTTPS_EXT.1.2アプリケーションは、TLS (FCS_TLSC_EXT.1) を用いて HTTPS を実装しなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**保証アクティビティ▼**

*その他のテストは、FCS_TLSC_EXT.1 と組み合わせて行われる。*

FCS_HTTPS_EXT.1.3アプリケーションは、ピア証明書が無効とみなされる場合には利用者に通知すると共に [**選択**：*接続を確立しない、アプリケーションが接続を確立するための認可を要求する、その他のアクションなし*] を行わなければならない (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：有効性は RFC 5280 に従って、認証パス、有効期限、及び失効状態によって決定される。

**保証アクティビティ▼**

*証明書の有効性は FIA_X509_EXT.1 のために行われるテストに従ってテストされなければならず (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)：*

- ***テスト 1：****評価者は、有効な認証パスのない証明書を使用すると、アプリケーション通知が発生することを論証しなければならない (shall)。次に評価者は、管理ガイダンスを利用して、その機能で使われる証明書の有効性確認に必要とされるトラストアンカーデータベースへ 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しなければならない (shall)。次に評価者は、これらの証明書の 1 つを削除して、有効性確認の失敗がアプリケーションへ通知されることを示さなければならない (shall)。*

**FIA_X509_EXT.1 X.509 証明書有効性確認**

FIA_X509_EXT.1.1　アプリケーションは、以下のルールに従って証明書の有効性確認を行うため [**選択**: *プラットフォームによって提供される機能を呼び出さ、機能を実装し*] なければならない (shall)：

- RFC 5280 証明書有効性確認及び認証パス検証。

- 認証パスは、信頼済み CA 証明書で終わらなければならない (must)。
- アプリケーションは、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、認証パスを検証しなければならない (shall)。
- アプリケーションは、[**選択**：*RFC 2560 に規定されるオンライン証明書状態プロトコル (OCSP)*、*RFC 5759 に規定される証明書失効リスト (CRL)*、*RFC 6066 に規定される OCSP TLS Status Request Extension (すなわち、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 (shall)。
- アプリケーションは、以下のルールに従って extendedKeyUsage フィールドを検証しなければならない (shall) :
    - 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 (shall)。
    - 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 (shall)。
    - TLS に提示されるクライアント証明書は、extendedKeyUsage フィールドに Client Authentication 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 (shall)。
    - 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 (shall)。
    - 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 (shall)。
    - EST 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 (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**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ルールが列挙されている。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 (shall)。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。この利用には、extendedKeyUsage ルールが検証されることが要求される。

*機能を実装*または*プラットフォームによって提供される機能を呼び出さ*の選択にかかわらず、証明書の有効性確認はプラットフォームによって管理されるルートストア中の信頼済みルート CA 証明書に至ることが期待される。

**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しなければならない (shall)。また評価者は、認証パス検証アルゴリズムの記述も 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 (must)。extendedKeyUsage ルールのテストは、これらのルールを要求する用途と組み合わせて行われる。アプリケーションが長さ 4 以上の連鎖をサポートする場合、評価者は少なくとも 4 つの証明書の連鎖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、2 つの中間 CA、及び自己署名されたルート CA である。アプリケーションが最大信頼深度 2 をサポートする場合には、その代わりに中間 CA を持たない連鎖が作成されるべきである (should)。*

- ***テスト 1***：*評価者は、有効な認証パスのない証明書の有効性を確認すると、その機能が失敗することを論証しなければならない (shall)。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しなければならない (shall)。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 (shall)。*
- ***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しなければならない (shall)。*
- ***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、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)；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以下のテストが行われなければならない (shall)：*
  - *評価者は、ノード証明書の失効をテストしなければならない (shall)。*
  - *中間 CA 証明書がサポートされる場合、評価者は中間 CA 証明書の失効も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、失効した証明書 (選択において選ばれた手法のそれぞれについて) 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 鍵使用ビットがセットされていない証明書を持つCRL に CA が署名するよう設定し、CRL の有効性確認が失敗することを検証しなければならない (shall)。*

- ***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。)*
- ***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。)*
- ***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。)*

FIA_X509_EXT.1.2　アプリケーションは、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 (shall)。

***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**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約する。

**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 (must)。アプリケーションが長さ 4 以上の連鎖をサポートする場合、評価者は少なくとも 4 つの証明書の連鎖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、2 つの中間CA、及び自己署名されたルートCA である。アプリケーションが最大信頼深度 2 をサポートする場合には、その代わりに中間CA を持たない連鎖が作成されるべきである (should)。*

- ***テスト 1**：評価者は、TOE の証明書を発行する CA の証明書に basicConstraints 拡張が含まれないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗する。*
- ***テスト 2**：評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグがセットされていないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗する。*
- ***テスト 3**：評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグが TRUE にセットされているような認証パスを構築しなければならない (shall)。この認証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　アプリケーションは、RFC 5280 に定義される X.509v3 証明書を用いて、 [**選択**：*HTTPS*、*TLS*、*DTLS*] の認証をサポートしなければならない (shall)。

> ***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：ST 作成者の選択は、FTP_DIT_EXT.1.1 の選択と一致しなければならない (shall)。

FIA_X509_EXT.2.2　アプリケーションが証明書の有効性を決定する接続を確立できないとき、アプリケーションは [**選択**：*このような場合には証明書を受容するかどうかの選択を管理者に許可する*、*証明書を受容する*、*証明書を受容しない*] ようにしなければならない (shall)。

> ***本要件は、FTP_DIT_EXT.1.1 中の選択に依存する。***

**適用上の注釈**：CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態の検証を行うために接続を確立しなければならない (must) 場合は多々生ずる。この選択は、(例えば、ネットワークエラーのため) そのような接続が確立できない場合のふるまいを記述するために用いられる。TOE が、証明書は FIA_X509_EXT.1 中の他の全てのルールに従って有効であると決定した場合、選択に示されるふるまいによって有効性が決定されなければならない (shall)。証明書が FIA_X509_EXT.1 中の他の有効性確認ルールのいずれかに失敗する場合、TOE はその証明書を受容してはならない (must not)。

**保証アクティビティ▼**

> *評価者は TSS をチェックして、TOE がどの証明書を利用するか選ぶ方法が記述されていること、及び TOE がその証明書を利用できるように運用環境を設定するために必要な指示があれば、それが管理ガイダンスに記述されていることを保証しなければならない (shall)。*
>
> *評価者は TSS を検査して、高信頼チャネルの確立に用いられる証明書の有効性確認中に接続が確立できなかった際の TOE のふるまいが記述されていることを確認しなければならない (shall)。評価者は、高信頼チャネル間の相違があれば、それが記述されていることを検証しなければならない (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には、この設定アクションを行う方法に関する指示が操作ガイダンスに含まれていることを評価者は保証しなければならない (shall)。*
>
> *評価者は、高信頼チャネルのそれぞれについて、以下のテストを実行しなければならない (shall)：*
>
> - ***テスト 1**：評価者は、有効な証明書の使用には TOE 以外の IT エンティティとの通信による少なくとも一部の証明書有効性確認のチェック実行が必要とされることを論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行われることを確認しなければならない (shall)。選択された*

*アクションが管理者によって設定可能である場合には、評価者は操作ガイダンスに従って、サポートされているすべての管理者設定可能オプションが、文書化されているようにふるまうことを決定しなければならない (shall)。*

- ***テスト 2：評価者は、TOE 以外の IT エンティティとの通信による少なくとも一部の証明書有効性確認のチェック実行が必要とされる無効な証明書が受容不可であることを論証しなければならない (shall)。***

# 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、TOE 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　アプリケーションは、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 (shall)：[**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しなければならない (shall)。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 (must) 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しなければならない (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)：*

- ***テスト 1**：評価者は、signature_algorithms 中のクライアントの HashAlgorithm 一覧表に従ってサポートされていない証明書を TLS 接続中に送信する (例えば、SHA-1 署名を持つ証明書を送信する) ようにサーバを設定しなければならない (shall)。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) 。*

**FPT_API_EXT.2 サポートされるサービス及び API の利用**

FPT_API_EXT.2.1　アプリケーションは、[**割付**：*IANA MIME メディアタイプに含まれる解析されるフォーマットのリスト*] を解析するために [**選択**：*プラットフォームによって提供されるライブラリを使用しなければならない (shall)*、*機能を実装しない*] 。

**適用上の注釈**：IANA MIME タイプは http://www.iana.org/assignments/media-types に列挙されており、多数の画像、音声、ビデオ、及びコンテンツのファイルフォーマットが含まれる。本要件は、解析サービスの提供がアプリケーションの目的である場合には適用されない。

**保証アクティビティ**

*評価者はTSS に、(http://www.iana.org/assignments/media-types によって記述されるような) IANA MIME メディアタイプがアプリケーションの処理するすべてのフォーマットについて列挙されていること、そしてこれらのフォーマットとプラットフォームによって提供される解析サービスが関連付けられていることを検証しなければならない (shall)。*

**FPT_IDV_EXT.1 ソフトウェア識別情報とバージョン**

FPT_IDV_EXT.1.1 アプリケーションは、ISO/IEC 19770-2:2009 標準の SWID タグに関する最小要件に適合する SWID タグを含まなければならない (shall)。

**適用上の注釈**：有効な SWID タグには、ソフトウェア識別エレメント及び Entity エレメントが、ISO/IEC 19770-2:2009 標準に定義されるように含まれなければならない (must)。SWID タグはファイル拡張子.swidtag と共に、ISO/IEC 19770-2:2009 に定義されるように保存されなければならない (must)。

**保証アクティビティ**

*評価者はアプリケーションをインストールし、その後 SWID タグが.swidtag ファイルに存在することをチェックしなければならない (shall)。評価者は、そのファイルをオープンし、少なくともソフトウェア識別エレメント及び Entity エレメントが含まれることを検証しなければならない (shall)。*

# D. エントロピー証拠資料と評定

本附属書では、TOE によって使用されるエントロピー源に要求される補足情報を記述する。

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 (should)。本証拠資料には、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 (should)。本証拠資料は、TSS の一部である必要はない。

## D.1 設計記述

証拠資料には、すべてのエントロピー源の構成要素の相互作用を含め、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 (shall)。また、製品に含まれるサードパーティ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 (should)。

本証拠資料には、どのようにエントロピーが作り出されるのか、そして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。本証拠資料では、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、生の出力に対する後処理 (ハッシュ、XOR など) があれば、それについて保存されるのか (保存されるとすればどこに)、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 (should)。処理に課される条件があれば (例えばブロッキング)、それについてもエントロピー源の設計の中で記述されるべきである (should)。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 (must)。

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 (shall)。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 (shall)。

## D.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、また (この特定の TOE による) RBG 出力の作成に用いられる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確信できる理由についての技術的な説明が存在すべきである (should)。この説明には、期待される最小エントロピー割合 (すなわち、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)) の記述が含まれ、TOE の攪拌シード生成プロセスへ十分なエントロピーが投入されることを説明することになる。この説明は、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することが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割合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ている。

サードパーティによって提供されるエントロピー源について、TOE 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、本証拠資料にはこのサードパーティ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た証拠資料に明確に記述されなければならない (must)。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 (must)、その想定が ST に含まれなければならない(must)。

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いて期待されるエントロピーの割合が明示的に示され統計学的な割合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い、または計算された割合が明示的にシードと関連付けられていない場合には、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 (shall not)。

## D.3 運用条件

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。そ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について、明確に記述されること。同様に、証拠資料には、エントロピー源が誤動作または不整合となることが判っている条件についても記述されなければならない (shall)。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 (shall)。

## D.4 ヘルステスト

さらに具体的に、すべてのエントロピー源ヘルステストとその根拠が、文書化されること。これには、ヘルステストの記述、それぞれのヘルステストが行われる頻度及び条件 (例えば、起動時、連続的、またはオンデマンド)、それぞれのヘルステストで期待される結果、そしてそれぞれの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信じられる理由を示す根拠が含まれること。

# E. 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—<br>● 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。<br>● 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。<br>● 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-0619, July 12, 2006. |

# F. 略語

| 略語 | 意味 |
|---|---|
| ADB | Android Debug Bridge |
| AES | Advanced Encryption Standard |
| ANSI | 米国規格協会 (American National Standards Institute) |
| API | アプリケーションプログラミングインタフェース (Application Programming Interface) |
| APK | Android Application Package |
| APPX | Windows Store Application Package |
| API | アプリケーションプログラミングインタフェース (Application Programming Interface) |
| ASLR | アドレス空間配置ランダム化 (Address Space Layout Randomization) |
| BAR | Blackberry Application Package |
| BIOS | 基本入出力システム (Basic Input/Output System) |
| CDSA | Common Data Security Architecture |
| CESG | Communications-Electronics Security Group |
| CMC | Certificate Management over CMS |
| CMS | Cryptographic Message Syntax |
| CN | 共通名 (Common Names) |
| CRL | 証明書失効リスト (Certificate Revocation List) |
| CSA | Computer Security Act |
| DEP | データ実行防止 (Data Execution Prevention) |
| DES | Data Encryption Standard |
| DHE | Diffie-Hellman Ephemeral |
| DMG | Apple Disk Image |
| DNS | ドメイン名システム (Domain Name System) |
| DPAPI | Data Protection Application Programming Interface |
| DRBG | 決定論的乱数ビット生成器 (Deterministic Random Bit Generator) |

| | |
|---|---|
| DSS | Digital Signature Standard |
| DT | Date/Time Vector |
| DTLS | データグラムトランスポート層セキュリティ (Datagram Transport Layer Security) |
| EAP | 拡張認証プロトコル (Extensible Authentication Protocol) |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral |
| ECDSA | 楕円曲線ディジタル署名アルゴリズム (Elliptic Curve Digital Signature Algorithm) |
| EMET | Enhanced Mitigation Experience Toolkit |
| EST | Enrollment over Secure Transport |
| FIPS | 連邦情報処理規格 (Federal Information Processing Standards) |
| DSS | Digital Signature Standard |
| GPS | Global Positioning System |
| HMAC | Hash-based Message Authentication Code |
| HTTP | ハイパーテキスト転送プロトコル (Hypertext Transfer Protocol) |
| HTTPS | Hypertext Transfer Protocol Secure |
| DSS | Digital Signature Standard |
| IANA | Internet Assigned Number Authority |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| IP | インターネットプロトコル (Internet Protocol) |
| IPA | iOS Package archive |
| IR | Intermediate Integer |
| ISO | 国際標準化機構 (International Organization for Standardization) |
| IT | 情報技術 (Information Technology) |
| ITSEF | 情報技術セキュリティ評価機関 (Information Technology Security Evaluation Facility) |
| JNI | Java Native Interface |
| LDAP | Lightweight Directory Access Protocol |
| MIME | Multi-purpose Internet Mail Extensions |

| | |
|---|---|
| MPKG | Meta Package |
| MSI | Microsoft Installer |
| NFC | Near Field Communication |
| NIAP | National Information Assurance Partnership |
| NIST | 国立標準技術研究所 (National Institute of Standards and Technology) |
| OCSP | オンライン証明書状態プロトコル (Online Certificate Status Protocol) |
| OID | オブジェクト識別子 (Object Identifier) |
| OMB | Office of Management and Budget |
| OS | オペレーティング システム (Operating System) |
| PDF | ポータブル文書フォーマット (Portable Document Format) |
| PID | プロセス識別子 (Process Identifier) |
| PII | 個人情報 (Personally Identifiable Information) |
| PKG | Package file |
| PKI | 公開鍵基盤 (Public Key Infrastructure) |
| PP | プロテクションプロファイル (Protection Profile) |
| IT | 情報技術 (Information Technology) |
| RBG | 乱数ビット生成器 (Random Bit Generator) |
| RFC | Request for Comment |
| RNG | 乱数生成器 (Random Number Generator) |
| RNGVS | Random Number Generator Validation System |
| SAN | サブジェクトの別名 (Subject Alternative Name) |
| SAR | セキュリティ保証要件 (Security Assurance Requirement) |
| SE | Security Enhancements |
| SFR | セキュリティ機能要件 (Security Functional Requirement) |
| SHA | セキュアハッシュアルゴリズム (Secure Hash Algorithm) |
| S/MIME | Secure/Multi-purpose Internet Mail Extensions |
| SIP | セション確立プロトコル (Session Initiation Protocol) |

| | |
|---|---|
| SP | Special Publication |
| SSH | セキュアシェル (Secure Shell) |
| SWID | ソフトウェア識別情報 (Software Identification) |
| TLS | トランスポート層セキュリティ (Transport Layer Security) |
| UI | ユーザインタフェース (User Interface) |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| USB | ユニバーサルシリアルバス (Universal Serial Bus) |
| XCCDF | セキュリティ設定チェックリスト記述形式 (eXtensible Configuration Checklist Description Format) |
| XOR | 排他的論理和 (Exclusive Or) |