モバイルデバイス基盤の
プロテクションプロファイル

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_md_v2.0.pdf

バージョン 2.0　2014 年 9 月 17 日

平成 27 年 7 月 21 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

謝辞

本プロテクションプロファイルは、産業界、米国政府機関、コモンクライテリア評価機関、及び国際コモンクライテリアスキームからの代表者とともに、Mobility Technical Community によって開発された。National Information Assurance Partnership は、このグループのメンバーへ謝辞を送り感謝したい。彼らの真摯な取り組みが、この刊行へ大きく寄与している。参加した組織名は以下のとおりである：

米国政府

Defense Information Systems Agency (DISA)

Information Assurance Directorate (IAD)

National Information Assurance Partnership (NIAP)

National Institute of Standards and Technology (NIST)

国際コモンクライテリアスキーム

Australasian Information Security Evaluation Program (AISEP)

Canadian Common Criteria Evaluation and Certification Scheme (CSEC)

独立行政法人 情報処理推進機構、日本 (IPA)

UK IT Security Evaluation and Certificate Scheme (CESG)

産業界

Apple, Inc.

BlackBerry

LG Electronics, Inc.

Microsoft Corporation

Motorola Solutions

Samsung Electronics Co., Ltd.

Mobility Technical Community のその他のメンバー

コモンクライテリア評価機関

EWA-Canada, Ltd.

Gossamer Security Solution

0. 前書き

0.1 文書の目的

本書は、モバイルデバイスの基盤となるセキュリティ及び評価要件を表現するコモンクライテリア (CC) のプロテクションプロファイル (PP) を提示する。

0.2 文書の適用範囲

開発及び評価プロセスにおけるプロテクションプロファイルの適用範囲は、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 [CC] に記述されている。中でも、PP は TOE の一般的な種別に対する IT セキュリティ要件を定義し、言明された要件を満たすためにその TOE によって提供されるべき機能及び保証のセキュリティ対策を特定する [CC1, Section C.1]。

0.3 意図される読者

本 PP が意図する読者は、モバイルデバイス開発者、CC 利用者、評価者及びスキームである。

0.4 関連する文書

コモンクライテリア[1]

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

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

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

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

[1]詳細については、http://www.commoncriteriaportal.org/を参照されたい。

0.5 改版履歴

バージョン	日付	内容
1.0	2013 年 10 月 21 日	初版発行
1.1	2014 年 2 月 12 日	誤字修正、適用上の注釈の追加説明。 FCS_TLS_EXT.1 からの割付及び FCS_TLS_EXT.1 と FCS_TLS_EXT.2 における暗号スイートの限定されたテストを削除。
2.0	2014 年 9 月 17 日	Technical Rapid Response Team Decisions に基づく改変の追記。 数多くの要件と保証アクティビティを明確化。 オブジェクティブ要件を義務化： ● アプリケーションのアクセス制御 (FDP_ACF_EXT.1.2) ● VPN 情報フロー制御 (FDP_IFC_EXT.1) 新たなオブジェクティブ要件を追加： ● IEEE 802.11 のスイート B 暗号 ● 証明書の登録 ● 追加的鍵材料種別の保護 ● ヒープオーバーフロー保護 ● Bluetooth 要件 ● アプリケーションのための暗号操作サービス ● リモートアテステーション (FPT_NOT_EXT.1) いくつかのオブジェクティブ要件に移行期日を追加。 ハードウェア分離された REK と鍵ストレージの選択を追記。 REK による鍵導出を許可。 FTP_ITC_EXT.1 を明確化し FDP_UPC_EXT.1 を追加。 アプリケーションの使用に HTTPS と TLS を義務化。(FDP_UPC_EXT.1) 承認済み DRBG から Dual_EC_DRBG を削除。 新たな TLS 要件を採択。 認証失敗制限回数到達時の TSF のワイプを義務化し、リブート前後で認証失敗回数が保持されることを要求。 管理クラスを明確化。 より多くのドメイン分離の議論とテストを追記。 監査要件を更新し監査対象事象の表を追加。 SFR カテゴリ対応表を追加。 使用事例テンプレートを更新。 用語集を概論へ移動。

内容

図 / 表

1. PP 概論

1.1 PP 参照識別

PP 参照： モバイルデバイス基盤のプロテクションプロファイル

PP バージョン： 2.0

PP の日付： 2014 年 9 月 17 日

1.2 用語集

用語	意味
アドレス空間配置ランダム化 (ASLR)	メモリマッピングを予測不可能なロケーションにロードする、悪用防止機能。ASLR によって、攻撃者がプロセスまたはカーネルのアドレス空間へ導入したコードへ制御を渡すことがより困難となる。
管理者 (Administrator)	管理者は、エンタープライズによってモバイルデバイスへ適用されるポリシーの設定を含めた、管理アクティビティに責任を負う。この管理者はリモートから操作を行うと考えられ、また MDM エージェントを介して操作を行うモバイルデバイス管理 (MDM) 管理者であるかもしれない。デバイスが登録解除されている場合、利用者が管理者となる。
保証 (Assurance)	TOE が SFR を満たしているという確信の根拠 [CC1]。
予備ブートモード (Auxiliary Boot Modes)	予備ブートモードは、デバイスが 1 つ以上のコンポーネントへ電源を供給し、デバイスの完全に認証された運用状態以外に存在する特定のコンポーネントと不許可利用者が対話できるようなインタフェースを提供する状態。 開発者モードは予備ブートモードのサブセットであるが、特に開発者を対象とし平均的な利用者との対話を意図したものではない点が異なる。
CC	コモンクライテリア (Common Criteria)
共通アプリケーション開発者 (Common Application Developer)	アプリケーション開発者 (またはソフトウェア会社) は、同一の名前の下に多数のアプリケーションを作成することが多い。モバイルデバイスは、通常は共有されることのないリソースが、そのようなアプリケーションによって共有されることを許可することが多い。
データ (Data)	サーバまたはモバイルデバイス (MD) によって格納または送信されるプログラム／アプリケーションまたはデータファイル。
データ暗号化鍵 (DEK)	保存データを暗号化するために使用される鍵。
開発者モード (Developer Modes)	開発者モードは、ソフトウェアのデバッグの目的で高度なシステムアクセスを提供するため利用者に追加的なサービスが利用可能となる状態である。開発者モードは、ソフトウェアのデバッグの目的で高度なシステムアクセスを提供するため利用者に追加的なサービスが利用可能となる状態である。本プロファイルの目的では、これらのモードには **FPT_TUD_EXT.2** に従って検証されていないブートモードも含まれる。
登録状態 (Enrolled state)	モバイルデバイスが管理者からのアクティブなポリシー設定と共に管理されている状態。
エンタープライズアプリケーション (Enterprise Applications)	エンタープライズによって提供され管理されるアプリケーション。
エンタープライズデータ (Enterprise Data)	エンタープライズデータは、エンタープライズサーバに常駐する、

用語	意味
	またはモバイルデバイス上に一時的に格納される任意のデータであって、それに対するモバイルデバイス利用者のアクセスは、エンタープライズによって定義され管理者によって実装されるセキュリティポリシーに従って許可される。
ファイル暗号化鍵 (FEK)	ファイル暗号化が使用される場合、ファイルの暗号化に使用される DEK。FEK は、暗号化されるファイルごとに一意である。
鍵のチェイン (Key Chaining)	複数層の暗号化鍵を用いて、データを保護する方法。最上位層の鍵はより下位の層の鍵を暗号化し、これによってデータが暗号化される。この方法は、任意の数の層を持つことができる。
鍵暗号化鍵 (KEK)	別の鍵、例えば DEK や鍵を含むストレージなどを暗号化するために使用される鍵。
ロック状態 (Locked State)	電源は入っているが、大部分の機能が利用できない。機能へのアクセスには、利用者認証が要求される (そのように設定されている場合)。
MD	モバイルデバイス (Mobile Device)
MDM エージェント (MDM Agent)	MDM エージェントは、アプリケーションとしてモバイルデバイス上にインストールされるか、またはモバイルデバイスの OS の一部である。MDM エージェントは、管理者によってコントロールされる MDM サーバへのセキュアな接続を確立する。
モバイルデバイス利用者 (利用者)	モバイルデバイスの物理的なコントロールと操作を行う権限のある個人。使用事例によって、これはデバイスの所有者の場合もあれば、デバイスの所有者によって許可された個人の場合もある。
オペレーティングシステム (OS)	最も高い特権レベルで実行されるソフトウェアであって、ハードウェア資源を直接コントロールできるもの。モダンなモバイルデバイスは、少なくとも 2 つの主要なオペレーティングシステムを持つ。ひとつは携帯電話ベースバンドプロセッサ上で動作するもの、もうひとつはアプリケーションプロセッサ上で動作するものである。アプリケーションプロセッサの OS は、大部分の利用者との対話をつかさどり、アプリの実行環境を提供する。携帯電話ベースバンドプロセッサの OS は、携帯電話ネットワークとの通信をつかさどり、またその他の周辺機器をコントロールすることもある。OS という用語は、文脈が指定されない場合には、アプリケーションプロセッサの OS を指すものと想定されることがある。
パスワード認証ファクタ (Password Authentication Factor)	利用者がアクセスを得るために秘密の文字のセットを提供することが要求される、認証ファクタの一種。
電源切断状態 (Powered-Off State)	一切の TOE 機能が実行できないようにデバイスがシャットダウンされている。
PP	プロテクションプロファイル (Protection Profile)
保護データ (Protected Data)	保護データは、すべての非 TSF データであり、すべての利用者またはエンタープライズデータを含む。保護データには、ソフトウェアベースのセキュアな鍵ストレージ中のすべての鍵が含まれる。このデータの一部または全部は機微なデータともみなされ得る。
リッチなオペレーティングシステム (Rich OS)	この用語は、上記「オペレーティングシステム (OS)」に定義されるアプリケーションプロセッサの主要オペレーティングシステムを指して使われる同義語である。この用語は、プロセッサ上に存在する可能性のあるより小さな分離された実行環境で実行されるオペレーティングシステムから、主要オペレーティングシステムを区別するために使用される。

用語	意味
ルート暗号化鍵 (REK)	他の鍵の暗号化に使用される、デバイスと結び付けられた鍵。
SAR	セキュリティ保証要件 (Security Assurance Requirement)
機微なデータ (Sensitive data)	機微なデータは、ST 作成者によってセキュリティターゲット (ST) の TSS セクションで特定されなければならない (shall)。機微なデータにはすべての利用者またはエンタープライズデータが含まれてもよく、また電子メール、メッセージ、文書、カレンダー項目、及び連絡先など特定のアプリケーションデータであってもよい。機微なデータは、ロック状態の間保護される (FDP_DAR_EXT.2)。機微なデータには、少なくともソフトウェアベースの鍵ストレージ中の鍵の一部または全部が含まれなければならない (must)。
SFR	セキュリティ機能要件 (Security Functional Requirement)
ST	セキュリティターゲット
評価対象	ソフトウェア、ファームウェア、またはハードウェアからなるセットで、ガイダンスが伴うことがある。[CC1]
TOE	評価対象
TOE セキュリティ機能 (TSF)	TOE のすべてのハードウェアとソフトウェア、そしてファームウェアから構成されるセットであって、SFR の正しい実施のために信頼されなければならない (must) もの。[CC1]
トラストアンカーデータベース (Trust Anchor Database)	信頼されたルート認証局証明書のリスト。
TSF データ (TSF Data)	TSF の運用のためのデータであって、要件の実施が依存するもの。
未登録状態 (Unenrolled state)	モバイルデバイスが管理されていない状態。
ロック解除状態 (Unlocked State)	電源が入っていて、デバイスの機能が利用できる。利用者認証が行われていることを暗黙に意味する (そのように設定されている場合)。

その他のコモンクライテリアの略号及び用語については、 [CC1] を参照されたい。

1.3 TOE 概要

本保証標準は、エンタープライズで使用されるモバイルデバイスの情報セキュリティ要件を特定する。本保証標準の文脈におけるモバイルデバイスとは、ハードウェアプラットフォームとそのシステムソフトウェアから構成されるデバイスである。このデバイスは、保護されたエンタープライズネットワークやエンタープライズデータ及びアプリケーションへのアクセス、及び他のモバイルデバイスとの通信を行うため、無線接続性を提供するのが普通であり、またセキュアメッセージング、電子メール、ウェブ、VPN 接続、及び VoIP (ボイスオーバーIP) のような機能を持つソフトウェアが含まれる。

図 1 に、モバイルデバイスのネットワーク運用環境を示す。

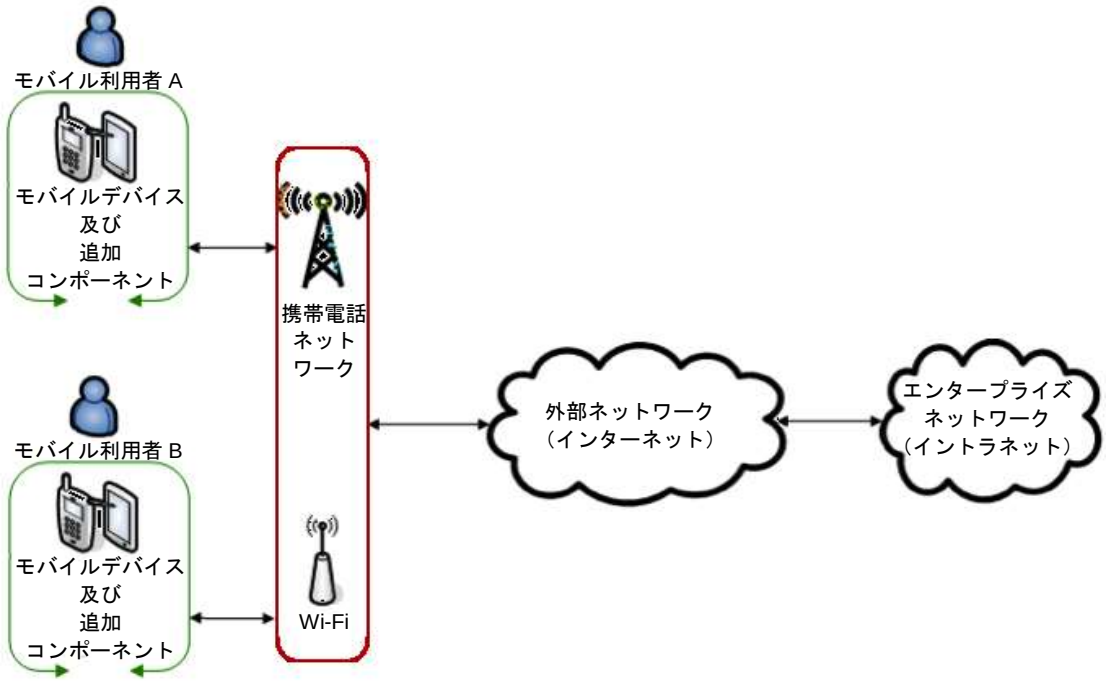

図 1：モバイルデバイスのネットワーク環境

本プロテクションプロファイルへの適合を主張すべき (should) 「モバイルデバイス」の例としては、スマートフォン、タブレットコンピュータ、及び同様の機能を持つ他のモバイルデバイスが挙げられる。

モバイルデバイスは、暗号サービス、保存データの保護、及び鍵ストレージサービスなどの基本的なサービスを提供して、デバイス上のアプリケーションのセキュアな運用をサポートする。セキュリティポリシーの実施、アプリケーション実施アクセス制御、悪用防止 (Anti-Exploitation) 機能、利用者認証、及びソフトウェア完全性保護などの追加的なセキュリティ機能が、脅威に対抗するために実装される。

本保証標準は、モバイルデバイスによって提供されるこれらの不可欠なセキュリティサービスを記述し、セキュアなモバイルアーキテクチャの基礎としての役割を果たす。図 2 に示すように、典型的な展開には、サードパーティの、またはバンドルされたコンポーネントもまた含まれることになるであろう。これらのコンポーネントが製造業者によってモバイルデバイスの一部としてバンドルされていた場合であっても、またはサードパーティによって開発された場合であっても、これらはモバイルデバイス管理システムのプロテクションプロファイル、IPsec 仮想プライベートネットワーク (VPN) クライアントのプロテクションプロファイル、そしてボイスオーバーIP (VoIP) アプリケーションのプロテクションプロファイルなど、関連する保証標準に対して別個に検証されなければならない (must)。これらのコンポーネントを確実に検証することは、セキュアなモバイルアーキテクチャ全体のアーキテクトの責任である。モバイルデバイスにあらかじめインストールされている追加的アプリケーションであって検証されていないものは、潜在的に欠陥を持つが悪意は持たないとみなされる。例としては、VoIP クライアント、電子メールクライアント、そしてウェブブラウザが挙げられる。

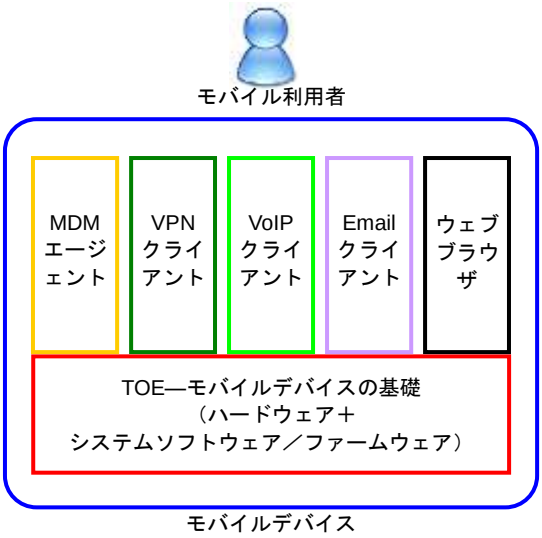

図 2：オプションの追加的モバイルデバイスコンポーネント

1.4 TOE の用途

モバイルデバイスは、さまざまな使用事例で運用される可能性がある。附属書 G には、本プロテクションプロファイルによって特定される使用事例を最もよくサポートする選択、割付、及びオブジェクティブ要件を列挙した使用事例テンプレートが提供されている。不可欠なセキュリティサービスを提供する以外にも、モバイルデバイスにはこれらのさまざまな使用事例のための構成をサポートするために必要なセキュリティ機能が含まれる。各使用事例には、望ましいセキュリティを達成するために追加的な設定やアプリケーションが要求されるかもしれない。これらの使用事例のいくつかを、以下に説明する。

使用事例テンプレートのいくつかには、提示された使用事例に強く望まれるオブジェクティブな要件が含まれている。読者は、これらの要件が本プロテクションプロファイルの次期の版では必須とされると期待してよい。また業界は、短期のうちにそのセキュリティ機能を製品へ含めることを目指すべきである (should)。

このバージョンのプロテクションプロファイルの刊行時点では、セクション 5 中の要件を満たすことが、すべての使用事例について必要とされる。

[使用事例 1] 汎用エンタープライズ用途及び制限された個人的用途のエンタープライズ所有デバイス

汎用業務用途のエンタープライズ所有デバイスは、一般的に「企業所有デバイスの私的利用 (COPE)」と呼ばれる。この使用事例には、高度なエンタープライズのコントロールが、設定と (おそらくは) ソフトウェアインベントリに関して必要とされる。エンタープライズは、利用者のエンタープライズデータのコントロールと利用者のネットワークのセキュリティを維持するため、利用者へモバイルデバイスと追加的アプリケーション (VPN または電子メールクライアントなど) の提供を選択する。利用者は、インターネット接続を用いてウェブをブラウズしたり会社のメールへアクセスしたりエンタープライズアプリケーションを実行する可能性があるが、この接続はエンタープライズの高度なコントロール下にあるかもしれない。

[使用事例 2] 特化した高セキュリティ用途のエンタープライズ所有デバイス

ネットワーク接続性が意図的に制限され、設定が厳密にコントロールされ、そしてソフト

ウェアインベントリが制限されたエンタープライズ所有デバイスは、特化した高セキュリティの使用事例に適切である。例えば、デバイスには、いかなる外部周辺機器への接続も許可されないかもしれない。WiFi または携帯電話を介してエンタープライズ所有のネットワークと通信することのみが可能であるかもしれず、またインターネットとの接続性すら許可されないかもしれない。デバイスの使用には、いかなる汎用使用事例におけるものよりも制約的な、しかし高度に機密性のある情報へのリスクを低減し得るような、ポリシーの遵守が要求されるかもしれない。前述の事例と同様に、エンタープライズはエンタープライズへの接続性を提供する追加的なアプリケーションや、プラットフォームと同様なレベルの保証を持つサービスを追求することになる。

[使用事例 3] 個人的及びエンタープライズ用途の個人所有デバイス

個人的な活動とエンタープライズデータの両方に使用される個人所有デバイスは、一般に私的デバイスの業務利用 (BYOD) と呼ばれる。エンタープライズ所有のケースとは異なり、利用者が主に個人的な利用のためにデバイスを購入するため、エンタープライズがデバイスへ実施できるセキュリティポリシーの点でエンタープライズの役割は限定されており、デバイスの機能を限定するようなポリシーが受容されることは考えづらい。しかし、エンタープライズは利用者にエンタープライズネットワークへの完全な (またはほぼ完全な) アクセスを許可するのであるため、アクセスを許可する前にエンタープライズは例えばパスワードや画面ロックポリシーなど一定のセキュリティポリシーを要求することになり、また、例えば VPN クライアントなどの保証されたエンタープライズソフトウェアを要求するかもしれない。デバイスは、大幅な個人的利用が行われた後に、エンタープライズ資源へのアクセスのために配備されるかもしれない。エンタープライズの運用環境と受容可能なリスクレベルに基づけば、本 PP のセクション 5 に概説されるセキュリティ機能要件は、本 BYOD 使用事例のセキュアな実装に十分である。

[使用事例 4] 個人的及び制限されたエンタープライズ用途の個人所有デバイス

個人所有のデバイスもまた、エンタープライズ電子メールなどの制限されたエンタープライズサービスへのアクセスを与えられるかもしれない。利用者はエンタープライズまたはエンタープライズデータへの完全なアクセスを持たないため、エンタープライズはデバイス上に何らかのセキュリティポリシーを実施する必要はないかもしれない。しかしエンタープライズは、モバイルデバイスによってこれらのクライアントへ提供されようとしているサービスが危殆化していないことを保証できる、セキュアな電子メール及びウェブブラウジングを望むかもしれない。エンタープライズの運用環境と受容可能なリスクレベルに基づけば、本 PP のセクション 5 に概説されるセキュリティ機能要件は、本 BYOD 使用事例のセキュアな実装に十分である。

2. CC への適合

[CC1]、[CC2] 及び [CC3] に定義されるとおり、本 cPP はコモンクライテリア v3.1 改定第 4 版へ適合する。PP の評価へ適用される方法論は、 [CEM] に定義される。

本 cPP は、以下の保証ファミリを満たす：APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.1, APE_REQ.1 及び APE_SPD.1。

3. セキュリティ課題定義

3.1 脅威

モバイルデバイスは、伝統的なコンピュータシステムの脅威とともに、そのモバイルとしての特性によって課される脅威の対象となる。以降のセクションで詳述するとおり、本プロテクションプロファイル中で考慮される脅威は、ネットワークの盗聴、ネットワーク攻撃、物理的アクセス、及び悪意または欠陥のあるアプリケーションである。

3.1.1 T.EAVESDROP ネットワークの盗聴

攻撃者は、無線通信チャネル上またはネットワーク基盤上のどこかに位置する。攻撃者は、モバイルデバイスと他のエンドポイントとの間で交換されるデータの監視やアクセスの獲得ができてしまうかもしれない。

3.1.2 T.NETWORK ネットワーク攻撃

攻撃者は、無線通信チャネル上またはネットワーク基盤上のどこかに位置する。攻撃者は、モバイルデバイスを危殆化するために、モバイルデバイスとの通信の開始や、モバイルデバイスと他のエンドポイントとの間の通信の改変ができてしまうかもしれない。これらの攻撃には、デバイス上の何らかのアプリケーションまたはシステムソフトウェアの、悪意のあるソフトウェアアップデートが含まれる。また、これらの攻撃には、通常はネットワーク上でデバイスへ配付される悪意のあるウェブページや電子メールの添付ファイルが含まれる。

3.1.3 T.PHYSICAL 物理的アクセス

モバイルデバイスの紛失や盗難によって、認証情報を含む利用者データの機密性の損失が引き起こされるかもしれない。このような物理的アクセスの脅威には、外部ハードウェアポートを介した、利用者インタフェースを介した、及びストレージ媒体への直接的な (そして破壊的であるかもしれない) アクセスを介した、デバイスへのアクセスを試行する攻撃が伴うかもしれない。そのような攻撃の目標は、所有者への返還が期待できない紛失または盗難されたモバイルデバイスのデータへアクセスすることである。

注釈：物理的に危殆化された後のデバイスの再利用に対する防御は、本プロテクションプロファイルの適用範囲外である。

3.1.4 T.FLAWAPP 悪意や欠陥のあるアプリケーション

モバイルデバイスへロードされるアプリケーションには、悪意のある、または悪用可能なコードが含まれるかもしれない。このようなコードは、その開発者によって意図的に、または、もしかするとソフトウェアライブラリの一部として開発者によって知らないうちに含まれるかもしれない。悪意のあるアプリは、アクセス権のあるデータの漏出を試行するおそれがある。またそのようなアプリは、プラットフォームのシステムソフトウェアへの攻撃を実施し、それによって追加的な特権と、さらに悪意のあるアクティビティを実施する能力が提供されることになるかもしれない。悪意のあるアプリケーションはデバイスのセンサ (GPS、カメラ、マイクロフォン) をコントロールして利用者周囲の情報収集活動を、たとえこれらの活動にデータの常駐やデバイスからの送信が伴わなくても、行うことができるかもしれない。欠陥のあるアプリケーションは、それがなければ防げたであろうネットワークベースまたは物理的な攻撃を行う手段を、攻撃者に与えてしまうかもしれない。

3.1.5 T.PERSISTENT 永続的プレゼンス

攻撃者によるデバイスへの永続的プレゼンスは、そのデバイスの完全性が失われたこと、そして再び取り戻すことができないことを意味する。デバイスは、何らかの他の脅威ベクタを原因として、このように完全性を失ったと考えられるが、攻撃者によって引き続きアクセスされることは、それ自体脅威が継続していることになる。この場合、デバイスとそのデータは敵対者によって、少なくとも合法的な所有者と同程度に、コントロールされるかもしれない。

3.2 前提条件

モバイルデバイスの前提条件は、附属書 A.1.1 に定義される。

3.3 組織のセキュリティ方針

モバイルデバイスの OSP 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

モバイルデバイスのセキュリティ対策方針は、以下のとおり定義される。

4.1.1 O.COMMS 保護された通信

TOE とリモートネットワークエンティティとの間のエンタープライズ及び利用者データならびに設定データの無線送信に関して、セクション 3.1 に記述されたネットワークの盗聴及びネットワーク攻撃の脅威に対抗するため、適合 TOE は高信頼通信パスを利用する。TOE は、以下の標準プロトコルの 1 つ (以上) を用いて通信することができる：IPsec、DTLS、TLS、HTTPS、または Bluetooth。これらのプロトコルは、さまざまな実装上の選択を提供する RFC によって特定される。相互運用性と暗号攻撃への耐性を提供するための要件が、これらの選択の一部 (特に、暗号プリミティブに関するもの) に課されている。

適合 TOE は ST に特定されたすべての選択をサポートしなければならない (must) が、追加的なアルゴリズムやプロトコルをサポートしてもよい。そのような追加的メカニズムが評価されない場合、それらが評価されなかったという事実が明確になるよう、管理者へガイダンスが提供されなければならない (must)。

FCS_CKM.1(*), FCS_CKM.2(*), FCS_CKM_EXT.7, FCS_COP.1(*), FCS_DTLS_EXT.1, FCS_HTTPS_EXT.1 FCS_RBG_EXT.1, FCS_SRV_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FDP_BLT_EXT.1, FDP_IFC_EXT.1, FDP_STG_EXT.1, FDP_UPC_EXT.1, FIA_BLT_EXT.1, FIA_BLT_EXT.2, FIA_PAE_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, FIA_X509_EXT.4, FPT_BLT_EXT.1, FTA_WSE_EXT.1, FTP_ITC_EXT.1

4.1.2 O.STORAGE 保護されたストレージ

モバイルデバイスの紛失の際の利用者データの機密性の損失の問題に対処するため (T.PHYSICAL)、適合 TOE は保存データ保護を利用する。TOE は、デバイス上に格納されるデータ及び鍵を暗号化することができ、また暗号化されたデータへの不許可アクセスを防止する。

FCS_CKM_EXT.1, FCS_CKM_EXT.2, FCS_CKM_EXT.3, FCS_CKM_EXT.4, FCS_CKM_EXT.5, FCS_CKM_EXT.6, FCS_COP.1(*), FCS_IV_EXT.1, FCS_RBG_EXT.1, FCS_STG_EXT.1, FCS_STG_EXT.2, FCS_STG_EXT.3, FDP_DAR_EXT.1, FDP_DAR_EXT.2, FIA_UAU_EXT.1, FPT_KST_EXT.1, FPT_KST_EXT.2, FPT_KST_EXT.3

4.1.3 O.CONFIG モバイルデバイスの設定

モバイルデバイスが保存または処理する可能性のある利用者及びエンタープライズデータを確実に保護するため、適合 TOE は利用者及びエンタープライズ管理者によって定義されたセキュリティポリシーを設定し適用する能力を提供する。エンタープライズセキュリティポリシーが設定される場合、それは利用者によって特定されるセキュリティポリシーよりも優先して適用されなければならない (must)。

FMT_MOF_EXT.1.1, FMT_MOF_EXT.1.2, FMT_SMF_EXT.1, FMT_SMF_EXT.2, FTA_TAB.1

4.1.4 O.AUTH 許可と認証

モバイルデバイスの紛失の際の利用者データの機密性の損失の問題に対処するため (T.PHYSICAL)、利用者には保護された機能及びデータへのアクセスに先立ってデバイスへ

認証ファクタを入力することが要求される。機密性のない機能の一部 (例えば、緊急通話、テキスト通知) は、認証ファクタの入力前にアクセスすることができる。デバイスは、デバイスが紛失または盗難された場合に認証が要求されることを保証するために、設定された非アクティブ時間間隔後に自動的にロックされる。

高信頼通信パスのエンドポイントの認証は、デバイスの完全性を侵食する不許可ネットワーク接続を確立する攻撃ができないことを保証するため、ネットワークアクセスに関して要求される。

利用者による TSF への認証試行の繰返し回数は、不成功の試行間に遅延時間が実施されるよう制限または抑制 (throttle) される。

FCS_CKM.2(1), FIA_AFL_EXT.1, FIA_BLT_EXT.1, FIA_BLT_EXT.2, FIA_PMG_EXT.1, FIA_TRT_EXT.1, FIA_UAU_EXT.1, FIA_UAU_EXT.2, FIA_UAU_EXT.3, FIA_UAU.7, FIA_X509_EXT.2, FIA_X509_EXT.4, FTA_SSL_EXT.1

4.1.5 O.INTEGRITY　モバイルデバイスの完全性

モバイルデバイスの完全性が保たれていることを保証するため、適合 TOE は自己テストを行って、重要な機能、ソフトウェア／ファームウェア及びデータの完全性が保たれていることを保証する。これらの自己テストに何らかの失敗があれば、利用者に通知されなければならない (shall)。(これは、脅威 T.PERSISTENT に対する保護となる。)

悪意または欠陥のあるコードを含むアプリケーションの問題 (T.FLAWAPP) に対処するため、ソフトウェア／ファームウェアへのダウンロードされたアップデートの完全性は、モバイルデバイス上のそのオブジェクトのインストール／実行に先立って検証される。さらに TOE は、アプリケーションが対話することを許可されたシステムサービス及びデータへのアクセスのみを許可するよう、アプリケーションを制限する。その上 TOE は、メモリレイアウトをランダム化することによって、悪意のあるアプリケーションがアクセス権限を持たないデータへのアクセスを得ることのないように、さらに保護する。

FAU_GEN.1, FAU_SAR, FAU_SEL.1, FAU_STG.1, FAU_STG.4, FCS_COP.1(2), FCS_COP.1(3), FDP_ACF_EXT.1, FPT_AEX_EXT.1, FPT_AEX_EXT.2, FPT_AEX_EXT.3, FPT_AEX_EXT.4, FPT_BBD_EXT.1, FPT_NOT_EXT.1, FPT_STM.1, FPT_TST_EXT.1, FPT_TST_EXT.2, FPT_TUD_EXT.1, FPT_TUD_EXT.2

4.2 運用環境のセキュリティ対策方針

TOE の運用環境によって満たされることが要求される対策方針は、附属書 A.2.2 に定義される。

5. セキュリティ機能要件

個別のセキュリティ保証要件は、以下のセクションに特定されている。要件の完全なリストについては、附属書 A.3「セキュリティ機能要件カテゴリの対応付け」を参照されたい。

5.1 表記法

以下の表記が、操作の完了に使用される。

- [*大括弧中のイタリック体テキスト*] は、ST 作成者によって完了されるべき操作を示す。
- 下線付きテキストは詳細化として追加テキストが提供されることを示す。
- [**大括弧中の太字テキスト**] は、割付の完了を示す。
- [***大括弧中の太字イタリック体テキスト***] は、選択の完了を示す。

5.2 クラス：暗号サポート (FCS)

5.2.1 暗号鍵管理 (FCS_CKM)

本セクションでは、どのように鍵が生成され、導出され、結合(combined)され、そして破棄されるのかを記述する。鍵には、DEK と KEK という、大別して 2 つの種別が存在する。(REK は、KEK の一種とみなされる。) DEK は、 (セクション 0 に記述される DAR 保護のように) データを保護するために使用される。KEK は、DEK、他の KEK、及び利用者またはアプリケーションによって格納される他の種別の鍵など、他の鍵を保護するために使用される。以下の図に、本プロファイルの概念を説明するため、鍵に関する階層構造の例を示す。この例は承認済みのデザインを意味するものではないが、ST 作成者は、本プロファイルの要件を満たしていることを論証するために、彼らの鍵階層構造を説明する図を提供することが期待される。

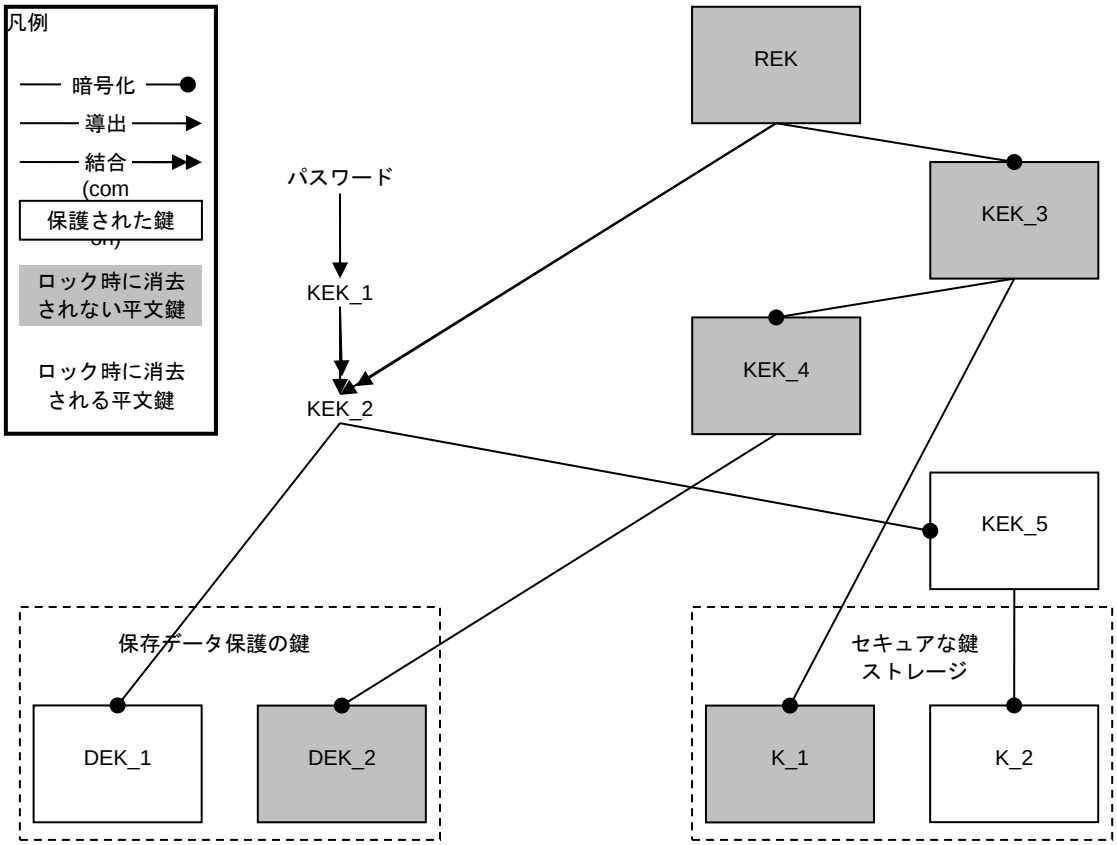

図 3：鍵階層構造の例

5.2.1.1 暗号鍵生成

FCS_CKM.1(1)	**暗号鍵生成**

FCS_CKM.1.1(1): TSF は、以下に特定される暗号鍵生成アルゴリズム [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)”, Appendix B.3;***
  - ***ANSI X9.31-1998, Section 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**]*

] に従って、非対称暗号鍵を生成しなければならない (shall)。

適用上の注釈：ST 作成者は、鍵確立及びエンティティ認証に使用さ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)。鍵生成が鍵確立に使用される場合、FCS_CKM.2.1(1) のスキーム及び選択された暗号プロトコルが選択とマッチしなければならない (must)。鍵生成がエンティティ認証に使用される場合、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ける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。

ECC スキームは、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

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特定されている場合、評価者は TSS を調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)。

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)。

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。

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*、プライベート素因数 *p* 及び *q*、モジュラス (modulus) *n* 及びプライベート署名指数 *d* の計算を含めた鍵コンポーネントの値を正しく求める TSF の能力を検証する。

鍵ペア生成では、素数 *p* 及び *q* を生成するための 5 つのやり方 (または方法) を特定している。これには、以下のものが含まれる。

1. ランダム素数：
   - 証明可能素数
   - 確率的素数
2. 条件付き素数：
   - 素数 *p1*、*p2*、*q1*、*q2*、*p* 及び *q* を、すべて証明可能素数としなければならない (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法とすべての条件付き素数法の鍵生成方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 が準拠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、承認済みランダムビット生

成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 関数へ投入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 個の公開鍵を不許可値となるように改変し、5 個を未改変の (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、並びにプライベート鍵 x と公開鍵 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 つのやり方 (または方法) :

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しなければならない (shall)

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

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 とおりの方法を特定している。

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)。

証明可能素数法の暗号素数及びフィールド素数生成法、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)。

5.2.1.2 暗号鍵生成 (WLAN)

FCS_CKM.1(2)	暗号鍵生成

FCS_CKM.1.1(2) TSF は、以下の [***IEEE 802.11-2012***] に合致する、特定された暗号鍵生成アルゴリズム [***PRF-384***] と特定された暗号鍵長 [***128 ビット***] に従って、FCS_RBG_EXT.1 に特定されるようなランダムビット生成器を用いて、対称暗号鍵を生成しなければならない (shall)。

適用上の注釈：本要件は FTA_WSE_EXT.1 をサポートする。これは、モバイルデバイスが設定済み無線 LAN に接続できることを要求するものである。IEEE 802.11-2012 (セクション 11.6.1.2) によって要求され WPA2 の認定において検証される暗号鍵導出アルゴリズムは、HMAC-SHA-1 関数を用いて 384 ビットを出力する PRF-384 である。

本要件は、クライアントが認証された後にアクセスポイントとクライアントとの間の通信のために生成／導出される鍵にのみ適用される。これは PMK からの PTK の導出を指すものであり、本 PP に特定される RBG によって生成される乱数値、本 PP に特定されるように SHA-1 を用いる HMAC 関数、そしてその他の情報を用いて行われる。これは、IEEE 802.11-2012 の主に第 11 章に特定されている。

保証アクティビティ：

暗号プリミティブは、本 PP の別の場所で特定される保証アクティビティによって検証されることになる。評価者は、本 PP によって定義され実装されるプリミティブが無線クライアントへのセキュアな接続性を確立し維持するために TOE によって使用される方法が TSS に記述されていることを検証しなければならない (shall)。また TSS には、開発者の実装が暗号標準に準拠していることを保証する開発者の 1 つまたは複数の方法の記述が提供されなければならない (shall)。これには、開発組織によって行われたテストだけではなく、行われたサードパーティテスト (例えば WPA2 認定) も含まれる。評価者は、テスト方法論の記述が十分に詳細であって、プロトコル特定の詳細がテストされた範囲を判断できることを保証しなければならない (shall)。

また評価者は、無線アクセスポイントと TOE との間のフレームを収集するためのパケットスニフィングツールを用いて以下のテストを実行しなければならない (shall) :

ステップ 1 : 評価者はアクセスポイントを未使用チャネルに設定し、そのチャネルのみをスニッフするよう WLAN スニファを設定しなければならない (shall) (すなわち、スニファをその選択されたチャネルにロックする)。またスニファは、TOE またはアクセスポイント、あるいはその両方の MAC アドレスをフィルタするよう設定されるべきである (should)。

ステップ 2 : 評価者は、IEEE 802.11-2012 及び 256 ビット (64 個の 16 進値 0-9 または a-f) の事前共有鍵を用いてアクセスポイントと通信するよう TOE を設定し、操作ガイダンス中に記述されるように接続をセットアップしなければならない (shall)。この事前共有鍵は、テストのためにのみ使用される。

ステップ 3：評価者はスニフィングツールを起動し、TOE とアクセスポイントとの間の接続を開始し、そして TOE にアクセスポイントとの認証を行わせ、関連付け (associate) させ、そして 4 ウェイハンドシェイクの完了を成功させなければならない (shall)。

ステップ 4：評価者はタイマーを 1 分に設定しなければならず (shall)、その終了時に評価者は TOE をアクセスポイントから切り離しスニファを停止させなければならない (shall)。

ステップ 5：評価者は 4 ウェイハンドシェイクのフレーム (Wireshark のキャプチャでは EAPOL をキーとして示される) を特定し、IEEE 802.11-2012 に特定されるように 4 ウェイハンドシェイクのフレーム及び事前共有鍵から PTK を導出しなければならない (shall)。

ステップ 6：評価者は、キャプチャされたパケットから 4 ウェイハンドシェイクの完了が成功した後にアクセスポイントと TOE との間で送信された、そしてフレーム制御値が 0x4208 (最初の 2 バイトが 08 42) 以外の、最初のデータフレームを選択しなければならない (shall)。評価者は IEEE 802.11-2012 に特定されるように PTK を用いてパケットのデータ部分を復号しなければならず (shall)、そして復号されたデータに ASCII 可読なテキストが含まれていることを検証しなければならない (shall)。

ステップ 7：評価者は、フレーム制御値が 0x4208 以外の、TOE とアクセスポイントとの間の次の 2 つのデータフレームについてステップ 7 を繰り返さなければならない (shall)。

5.2.1.3 暗号鍵確立

FCS_CKM.2.1(1)	**暗号鍵確立**

FCS_CKM.2.1(1) TSF は、以下に特定される鍵確立方法に従って、暗号鍵確立を実行しなければならない (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*

]。

適用上の注釈：

ST 作成者は、選択された暗号プロトコルに使用さ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.2 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ける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。

鍵確立スキームに使用される楕円曲線は、FCS_CKM.1.1(1) に特定される曲線と相関しなければならない (shall)。楕円曲線ベースのスキームは、2015 年の第 3 四半期以降に評価に

入る製品について必須となる。

有限体ベースの鍵確立スキームに使用されるドメインパラメタは、FCS_CKM.1.1(1) にしたがった鍵生成によって特定される。

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(1) に特定される鍵生成スキームと対応していることを保証しなければならない (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 を調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、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)。

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。

鍵確立スキーム

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

SP800-56A 鍵確立スキーム

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 承認曲線 (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 において使用さ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、実装されている承認 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) を判断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 承認曲線、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 において使用さ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(static)公開鍵、両者の短期(ephemeral)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改変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 が送信側として動作する場合、RSA ベースの鍵確立スキームの TOE のサポートするすべての組み合わせについて正しい動作を保証するため、以下の保証アクティビティが実行されなければならない (shall) :

本テストを実行するため、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 (鍵確認がサポートされている場合はその有りまたは無し、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、通常の操作で使用さ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 が受信側として動作する場合、RSA ベースの鍵確立スキームの TOE のサポートするすべての組み合わせについて正しい動作を保証するため、以下の保証アクティビティが実行されなければならない (shall) :

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またはなし、鍵確認がサポートされている場合にはサポートされている鍵確認 MAC 関数のそれぞれ、そして KTS-OAEP がサポートされている場合にはサポートされているマスク生成関数のそれぞれ) の組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない (shall)。各テストベクタには RSA プライベート鍵、平文の鍵材料 (KeyData)、該当する場合は任意の追加入力パラメタ、鍵確認が組み込まれている場合には MacTag、そして出力された暗号文が含まれなければならない (shall)。テストベクタのそれぞれについて、評価者は TOE 上で鍵確立復号操作を行い、出力された平文鍵材料 (KeyData) がテストベクタ中の平文鍵材料と同等であることを保証しなければならない (shall)。鍵確認が組み込まれている場合、評価者は鍵確認ステップを行い、出力された MacTag がテストベクタ中の MacTag と同等であることを保証しなければならない (shall)。

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

5.2.1.4 暗号鍵配送 (WLAN)

FCS_CKM.2.1(2)	暗号鍵配送

FCS_CKM.2.1 (2) TSF は、以下の[***NIST SP 800-38F***、***IEEE 802.11-2012 for the packet format and timing considerations***]に合致する、指定された暗号鍵配送方法 [***EAPOL 鍵フレーム内の AES 鍵ラップ***]、かつ暗号鍵を暴露しないものに従って、グループ一時鍵 (GTK) を復号しなければならない (shall)。

適用上の注釈：本要件は FTA_WSE_EXT.1 をサポートする。これは、モバイルデバイスが設定済み無線 LAN に接続できることを要求するものである。本要件は、TOE が接続しているアクセスポイントからのブロードキャスト及びマルチキャストメッセージを復号するために TOE によって受信される GTK に適用される。IEEE 802.11-2012 には送信のフォーマットと、それが NIST SP 800-38F に特定される AES 鍵ラップ方法によってラップされなければならない (must) という事実が特定されている。TOE は、そのような鍵を解くことができなければならない (must)。

保証アクティビティ：

評価者は TSS をチェックして、GTK が TOE 上で利用されるためにインストールされる前に、本 PP に特定される AES 実装を用いて解く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)。また評価者は、無線アクセスポイントと TOE との間のフレームを収集するためのパケットスニフィングツールを用いて以下のテストを実行しなければならない (shall) (このテストは、FCS_CKM.1.1(2) の保証アクティビティと組み合わせて行われてもよい :

ステップ 1 : 評価者はアクセスポイントを未使用チャネルに設定し、そのチャネルのみをスニッフするよう WLAN スニファを設定しなければならない (shall) (すなわち、スニファをその選択されたチャネルにロックする)。またスニファは、TOE またはアクセスポイント、あるいはその両方の MAC アドレスをフィルタするよう設定されるべきである (should)。

ステップ 2 : 評価者は、IEEE 802.11-2012 及び 256 ビット (64 個の 16 進値 0-9 または a-f) の事前共有鍵を用いてアクセスポイントと通信するよう TOE を設定し、操作ガイダンス中に記述されるように接続をセットアップしなければならない (shall)。この事前共有鍵は、テストのためにのみ使用される。

ステップ 3 : 評価者はスニフィングツールを起動し、TOE とアクセスポイントとの間の接続を開始し、そして TOE にアクセスポイントとの認証を行わせ、関連付け (associate) させ、そして 4 ウェイハンドシェイクの完了を成功させなければならない (shall)。

ステップ 4 : 評価者はタイマーを 1 分に設定しなければならず (shall)、その終了時に評価者は TOE をアクセスポイントから切り離しスニファを停止させなければならない (shall)。

ステップ 5 : 評価者は 4 ウェイハンドシェイクのフレーム (Wireshark のキャプチャでは EAPOL をキーとして示される) を特定し、IEEE 802.11-2012 に特定されるように 4 ウェイハンドシェイクのフレーム及び事前共有鍵から PTK 及び GTK を導出しなければならない (shall)。

ステップ 6 : 評価者は、キャプチャされたパケットから 4 ウェイハンドシェイクの完了が成功した後にアクセスポイントと TOE との間で送信された、そしてフレーム制御値が 0x4208 (最初の 2 バイトが 08 42) の、最初のデータフレームを選択しなければならない (shall)。評価者は IEEE 802.11-2012 に特定されるように GTK を用いてパケットのデータ部分を復号しなければならず (shall)、そして復号されたデータに ASCII 可読なテキストが含まれていることを検証しなければならない (shall)。

ステップ 7 : 評価者は、フレーム制御値が 0x4208 の次の 2 つのデータフレームについてステップ 7 を繰り返さなければならない (shall)。

5.2.1.5 暗号鍵サポート (REK)

FCS_CKM_EXT.1	**拡張 : 暗号鍵サポート**

FCS_CKM_EXT.1.1: TSF は、[選択 : *128 ビット*、*256 ビット*] 長の鍵を持つ [選択 : *ハードウェア的に分離された*、*ハードウェア的に保護された*] REK をサポートしなければならない (shall)。

FCS_CKM_EXT.1.2: TSF 上のシステムソフトウェアは、鍵による [選択 : *AES 暗号化／復号*、*NIST SP 800-108 鍵導出*] を要求することのみが可能でなければならず (shall)、REK を読み出したり、インポートしたり、あるいはエクスポートすることが可能であってはならない (shall not)。

FCS_CKM_EXT.1.3: REK は、FCS_RBG_EXT.1 に従う RBG により生成されなければならない (shall)。

適用上の注釈：128 ビットまたは 256 ビットのいずれか (または両方) が許可される；ST 作成者は、デバイスに適切な選択を行う。256 ビットの鍵長の使用は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

本要件に関して、「ハードウェア的に分離された」と「ハードウェア的に保護された」は両方とも、REK が高機能 OS から分離されなければならず (must) 、OS のカーネルがこの鍵の操作を要求することのみが許され生の鍵材料をアクセスすることは許されないような設計を意味する。これら 2 つの違いは、生の鍵材料がアクセスされる場所に関するものである。「ハードウェア的に分離された」REK（1 つ以上）の生の鍵材料は、処理とメモリの両方に関して OS から分離された、分離したプロセッサ実行環境中においてのみ利用できる。「ハードウェア的に保護された」REK（１つ以上）の生の鍵材料は、いかなるソフトウェアからも利用できず、ハードウェアによって計算機的 (computationally) に処理される。「ハードウェア的に保護された」が選択される場合、FCS_CKM_EXT.1.4 (訳注：Appendix C.1) が ST に含まれなければならない (must)。

インポートやエクスポートを行うための公開／文書化された API が存在しないことは、プライベートな／文書化されていない API が存在する場合、本要件を満たすには十分ではない。

要件は、AES 暗号化／復号または REK による SP800-108 からのモードによる鍵導出の、いずれかを許している。

REK の生成に使用される RBG は、ハードウェア鍵コンテナにネイティブな RBG であってもよいし、またはデバイス外部 (off-device) の RBG であってもよい。デバイス外部の RBG によって行われる場合、デバイスの製造業者は製造プロセスの完了後に REK にアクセスできてはならない (shall not)。これらの 2 つの場合について、保証アクティビティは異なる。

保証アクティビティ：

評価者は TSS をレビューして、REK が製品によってサポートされていること、その製品によって REK に対して提供される保護の記述が TSS に含まれていること、そして REK の生成方法の記述が TSS に含まれることを判断しなければならない (shall)。

評価者は、REK の保護の記述に、その REK のいかなる読み出し、インポート、及びエクスポートも防止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)。(例えば、REK を保護しているハードウェアがリムーバブルである場合、その記述には他のデバイスによる REK からの読み出しが防止される方法が含まれるべきである (should)。) 評価者は、暗号化／復号アクションが分離されており、鍵による暗号化／復号が可能である一方で、アプリケーションやシステムレベルプロセスによる REK の読み出しが防止されていることが TSS に記述されていることを検証しなければならない (shall)。

「ハードウェア分離された」が選択され 1 つまたは複数の REK が別個のプロセッサ実行環境によってリッチ OS から分離されている場合、評価者はその記述に、リッチ OS による REK 鍵材料を含むメモリのアクセスがどのように防止されているか、どのソフトウェアが REK へのアクセスを許されているか、実行環境中の任意の他のソフトウェアによるその鍵材料の読み出しがどのように防止されているか、そしてどの他のメカニズムがリッチ OS と別個の実行環境との間の共有メモリの場所へ REK 鍵材料が書き込まれることを防止するのか、含まれていることを検証しなければならない (shall)。

鍵導出が REK を用いて行われる場合、評価者は鍵導出関数の記述が TSS 記述に含まれていることを保証しなければならず (shall)、また承認済み導出モード及び SP 800-108 に従う鍵拡張アルゴリズムが鍵導出に使用されることを検証しなければならない (shall)。(追加的な鍵拡張アルゴリズムは、他の NIST Special Publications に定義されている。)

評価者は、REK の生成が FCS_RBG_EXT.1.1 及び FCS_RBG_EXT.1.2 要件を満たしていることを検証しなければならない (shall) :

- 1 つまたは複数の REK がデバイス上で生成される場合、何が生成を引き起こすのか、FCS_RBG_EXT.1 によって記述される機能がどのように起動されるのか、そして 1 つまたは複数の REK に RBG の別個のインスタンスが使用されるのかどうかの記述が、TSS に含まれなければならない (shall)。
- 1 つまたは複数の REK がデバイス外部で生成される場合、TSS には RBG が FCS_RBG_EXT.1.2 を満たしているという証拠資料が含まれなければならない (shall)。これは、RBG 保証アクティビティに提供される文書と同等の、RBG 文書の 2 番目のセットであると考えられる。さらに TSS には、デバイス製造業者によるあらゆる REK へのアクセスが防止される製造プロセスが記述されなければならない (shall)。

5.2.1.6 暗号データ暗号化鍵

FCS_CKM_EXT.2	拡張 : 暗号鍵ランダム生成

FCS_CKM_EXT.2.1 すべての DEK は、[選択 : *128*、*256*] ビットの AES 鍵長のセキュリティ強度に対応するエントロピーを持つようにランダムに生成されなければならない (shall)。

適用上の注釈 : 本要件の意図は、AES の鍵空間の総当たりよりも少ない労力で DEK が復元できないことを保証することである。TOE の鍵生成機能は、TOE デバイス上に実装された RBG を利用する (FCS_RBG_EXT.1)。128 ビットまたは 256 ビットのいずれか (または両方) が許可される。ST 作成者は、デバイスに適切な選択を行う。DEK は、デバイス上の利用者データをすべて再暗号化する必要なく認証ファクタ (特に、パスワード認証ファクタ) が改変できるよう、KEK に加えて使われる。

256 ビットの鍵長の使用は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ :

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て DEK が生成される方法が記述されていることを判断しなければならない (shall)。評価者は、FCS_RBG_EXT.1 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、要求されている鍵長がデータの暗号化／復号に使用される鍵長及びモードと同一であることを判断する。

5.2.1.7 暗号鍵暗号化鍵

FCS_CKM_EXT.3	拡張 : 暗号鍵生成

FCS_CKM_EXT.3.1 すべての KEK は、少なくとも KEK によって暗号化される鍵のセキュリティ強度に対応する [選択 : *128 ビット*、*256 ビット*] の鍵でなければならない (shall)。

適用上の注釈 :

256 ビットの鍵長の使用は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

FCS_CKM_EXT.3.2 TSF は、以下の方法の 1 つを用いて、すべての KEK を生成しなければならない (shall) :

a) PBKDF を用いたパスワード認証ファクタから KEK を導出する、及び

[選択：

b) *本プロファイルを満たす RBG (FCS_RBG_EXT.1 に特定される) を用いて KEK を生成する*

c) *[選択 : XOR 操作を用いる、複数の鍵を連結し KDF を用いる (SP 800-108 に記述される)、別の鍵を用いて暗号化する] ことによって各ファクタの実効エントロピーを維持するように他の KEK から結合(combined) する]*

]。

適用上の注釈：

PBKDF は、FCS_COP.1(5) に従って行われる。

これらの方法のそれぞれは、本文書に特定される要件を満たすために必要となることが期待される。特に、図 3 には各種類の KEK が存在している。KEK_3 は生成され、KEK_1 はパスワード認証ファクタから導出され、KEK_2 は 2 つの KEK から結合されている。結合される場合、ST 作成者は各ファクタの実効エントロピーが維持されることを正当化するためにどの結合方法が使用されるかを記述しなければならない (shall)。

保証アクティビティ：

評価者は、鍵階層構造 TSS を検査して、すべての KEK の形成が記述されていること、そして鍵長が ST 作成者によって記述されているものと一致していることを保証しなければならない (shall)。

- 評価者は TSS をレビューして、PBKDF を用いて KEK が導出されるという記述が含まれることを検証しなければならない (shall)。この記述には、ソルトのサイズとストレージの場所が含まれなければならない (must)。このアクティビティは、FCS_COP.1(5) のアクティビティと組み合わせて行われてもよい。
- KEK が生成される場合、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判断しなければならない (shall)。評価者は、FCS_RBG_EXT.1 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、要求されている鍵長がデータの暗号化／復号に使用される鍵長及びモードと同一であることを判断する。
- KEK が結合によって形成される場合、評価者は TSS に結合(combination)の方法が記述され、またその方法が XOR、KDF、または暗号化のいずれかであることを検証しなければならない (shall)。KDF が使用される場合、評価者は鍵導出関数の記述が TSS 記述に含まれていることを保証しなければならず (shall)、また承認済み導出モード及び SP 800-108 に従う鍵拡張アルゴリズムが鍵導出に使用されることを検証しなければならない (shall)。(追加的な鍵拡張アルゴリズムは、他の NIST Special Publications に定義されている。)

5.2.1.8 暗号鍵の破棄

FCS_CKM_EXT.4	**拡張：鍵の破棄**

FCS_CKM_EXT.4.1 TSF は、以下の特定された暗号鍵破棄方法に従って暗号鍵を破棄しなければならない (shall)：

- *目的の鍵を暗号化する KEK をクリアすることによって、*
- *以下のルールに従って：*

- 揮発性メモリについては、 [選択：*TSF の RBG を用いた疑似ランダムパターンからなる*、*ゼロからなる*] 単一の直接上書きと、それに引き続く読み出し検証によって破棄が実行されなければならない (shall)。
- 不揮発性 EEPROM については、TSF の RBG (FCS_RBG_EXT.1 に規定されるように) を用いた疑似ランダムパターンからなる単一の直接上書きと、それに引き続く読み出し検証によって破棄が実行されなければならない (shall)。
- 不揮発性フラッシュメモリについては、 [選択：*ゼロからなる単一直接上書きとそれに引き続く読み出し検証によって*、*ブロック消去とそれに引き続く読み出し検証によって*] 破棄が実行されなければならない (shall)。
- EEPROM とフラッシュメモリ以外の不揮発性メモリについては、毎回書き込み前に改変されるランダムパターンで 3 回以上上書きすることによって破棄が実行されなければならない (shall)。

適用上の注釈：上述のクリアは、平文鍵／暗号クリティカルセキュリティパラメタの各中間ストレージ領域 (すなわち、メモリバッファなど任意のストレージであって、そのようなデータの経路中に含まれるもの) に、その鍵／暗号クリティカルセキュリティパラメタが別の場所へ転送された際、適用される。

平文鍵材料は不揮発性メモリへの書き込みが許されないため (FPT_KST_EXT.1)、第 2 の選択は揮発性メモリへ書き込まれる鍵材料にのみ適用される。

FCS_CKM_EXT.4.2 TSF は、すべての平文鍵材料とセキュリティパラメタを、もはや必要とされなくなった際に破棄しなければならない (shall)。

適用上の注釈：本要件の目的においては、平文鍵材料とは認証データ、パスワード、秘密／プライベート対称鍵、鍵の導出に使用されたデータなどを指す。鍵破棄手続きは、FCS_CKM_EXT.4.1 に従って行われる。

2015 年の第 3 四半期以降に評価に入る製品については、平文鍵材料はパスワードから導出された値を意味することになる。

例えば TOE の電源が切られている際、ワイプ機能が行われた際、高信頼チャネルが切断された際、鍵材料がもはや高信頼チャネルのプロトコルによって必要とされなくなった際、及びロック状態へ移行した際など、平文鍵材料がもはや必要とされない状況は複数存在する (パスワード認証ファクタから導出された値または FCS_STG_EXT.2 に従ってパスワードから導出された KEK によって保護される鍵材料に関しては、図 3 を参照のこと)。ロック状態で受信された機微なデータを保護する鍵 (またはこれらの鍵を導出するために使用される鍵材料) については、「もはや必要なくなった際」には「ロック状態にある間」が含まれる。

高信頼チャネルには、TLS、HTTPS、DTLS、IPsec VPN、IEEE 802.11、EAP-TLS、Bluetooth BR/EDR、及び Bluetooth LE が含まれる可能性がある。これらのチャネルの平文鍵材料には、マスター秘密、セキュリティアソシエーション (SA)、事前共有鍵 (PSK)、ペアごとのマスター鍵 (PSK)、リンク鍵、及び長期鍵 (LTK) などが含まれる (が、これらには限定されない)。

リッチ OS と同一のアプリケーションプロセッサ上の別個の実行環境内で 1 つまたは複数の REK が処理される場合、REK 鍵材料は使用直後に RAM からクリアされなければならず (must)、また少なくとも、デバイスがロックされた際にはワイプされなければならない (must)。REK は、機微なデータを保護する鍵階層構造の一部だからである。

さらに、IEEE 802.11-2012 では無線 LAN クライアントの PMK の寿命を定めていない (IEEE

802.11-2012 Section 11.6.1.3 に記述されている) が、この寿命は制限されるべきであり (should)、また PMKSA は、同一の PMK が 24 時間を超えて連続して使われないようにクリアされるべきである。したがって、PMK については、「もはや必要とされなくなった際」は 24 時間後である。

保証アクティビティ：

評価者は、平文鍵材料の各種別 (DEK、ソフトウェアベースの鍵ストレージ、KEK、高信頼チャネル鍵、パスワードなど) が、その生成元 (origin) 及びストレージの場所を含めて TSS に列挙されていることをチェックして保証しなければならない (shall)。

評価者は、鍵材料の各種別がいつクリアされるのか (例えば、システムの電源断の際、ワイプ機能の際、高信頼チャネルの切断の際、高信頼チャネルのプロトコルによってもはや必要とされなくなった際、ロック状態への移行の際、及び、場合によっては使用直後、ロック状態にいる間など) TSS に記述されていることをチェックして検証しなければならな い (shall)。

また評価者は、鍵の種別のそれぞれについて、行われる消去処理の種別 (暗号学的消去、ゼロで上書き、ランダムパターンで上書き、またはブロック消去) が列挙されていることも検証しなければならない (shall)。異なる種類のメモリが保護されるべき材料の格納に使用される場合、評価者はデータが格納されるメモリに応じた消去処理 (例えば、「フラッシュメモリに格納される秘密鍵はゼロで 1 度上書きすることによってクリアされるが、内部永続的ストレージデバイス上に格納される秘密鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってクリアされる」) が TSS に記述されていることを保証するためチェックしなければならない (shall)。ブロック消去について、評価者は使用されるブロック消去コマンドが列挙されていることも保証しなければならず (shall)、また使用されるコマンドが平文鍵材料の任意のコピー及びフラッシュメモリの使用を最適化するために作成されるかもしれないコピーにも対応していることを検証しなければならない (shall)。

保証アクティビティの注釈：以下のテストには、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。

ソフトウェア及びファームウェア鍵クリア状況のそれぞれ (システムの電源断の際、ワイプ機能の際、高信頼チャネルの切断の際、高信頼チャネルのプロトコルによってもはや必要とされなくなった際、ロック状態への移行の際、及び、場合によっては使用直後、ロック状態にいる間を含む) について、評価者は以下のテストを繰り返さなければならない (shall)。この時点で、ハードウェアに束縛された鍵はテストから明示的に除外されることに注意されたい。

*テスト 1：*評価者は、TOE 及び計測機能を備えた TOE ビルドに適切な専用の運用環境と開発ツール (デバッガ、シミュレータなど) の組み合わせを利用して、鍵 (その鍵に関する通常の暗号処理中に TOE によって内部的に作成される可能性のある鍵の中間コピーの *すべて*を含む) が正しくクリアされることをテストしなければならない (shall)。

ソフトウェア中の暗号 TOE 実装は、デバッガの下でロード及び行使され、そのようなテストが行われなければならない (shall)。評価者は、TOE によって永続的に暗号化される鍵の中間コピーを含め、クリア対象となる鍵のそれぞれについて、以下のテストを実行しなければならない (shall)：

1. 計測機能を備えた TOE ビルドをデバッガへロードする。
2. クリア対象となる TOE 内の鍵の値を記録する。

3. #1 の鍵に関する通常の暗号処理を TOE に行わせる。
4. TOE に鍵をクリアさせる。
5. TOE に実行を停止させるが、終了はさせない。
6. TOE に、TOE の全メモリフットプリントをバイナリファイルへダンプさせる。
7. #4 で作成されたバイナリファイルの内容から、#1 の既知の鍵の値のインスタンスを検索する。

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

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

*テスト 2：*TOE がファームウェアに実装されておりデバッガを用いることができない制限された運用環境で動作している場合、評価者は汎用オペレーティングシステム上で TOE のシミュレータを利用しなければならない (shall)。評価者は、シミュレートされたテスト環境という計測設備を説明し、得られたテスト結果を正当化する根拠を提供しなければならない (shall)。

5.2.1.9 TSF のワイプ

FCS_CKM_EXT.5	**拡張：TSF のワイプ**

FCS_CKM_EXT.5.1 TSF は、以下によってすべての保護されたデータをワイプしなければならない (shall)： [選択：

- *FCS_CKM_EXT.4.1 中の要件にしたがうことによって、不揮発性メモリ中の暗号化された DEK または KEK、あるいはその両方を暗号学的に消去する；*
- *以下のルールに従ってすべての保護されたデータを上書きする：*
  - *EEPROM については、TSF の RBG (FCS_RBG_EXT.1 に特定されるような) を用いた疑似ランダムパターンからなる単一の直接上書きと、それに引き続く読み出し検証によって破棄が実行されなければならない (shall)。*
  - *フラッシュメモリについては、[ゼロからなる単一直接上書きとそれに引き続く読み出し検証によって、ブロック消去とそれに引き続く読み出し検証によって] 破棄が実行されなければならない (shall)。*
  - *EEPROM とフラッシュメモリ以外の不揮発性メモリについては、毎回書き込み前に改変されるランダムパターンを用いて 3 回以上上書きすることによって破棄が実行されなければならない (shall)。*]

FCS_CKM_EXT.5.2 TSF は、ワイプ手続きの終了時に、電源が再投入されなければならない (shall)。

適用上の注釈：ST 作成者は、TSF が行うワイプの方法を選択しなければならない (shall)。

保証アクティビティ：

評価者は、デバイスがワイプされる方法、そして行われる消去処理の種類 (暗号学的消去または上書き) と、上書きが行われる場合には、上書き手続き (ゼロで上書き、異なる交番パターンで 3 度以上上書き、ランダムパターンで上書き、またはブロック消去) が 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)。保護されるべきデータ

の保存に異なる種類のメモリが使用される場合、評価者はデータが保存されるメモリに応じた消去処理 (例えば、「フラッシュメモリ上に保存されるデータはゼロで 1 度上書きすることによってクリアされるが、内部永続的ストレージデバイス上に保存されるデータは書き込みごとに変化するランダムパターンを 3 度上書きすることによってクリアされる」) が TSS に記述されていることをチェックして保証しなければならない (shall)。

保証アクティビティの注釈：以下のテストは、消費者向けモバイルデバイス製品には通常含まれないツールを評価者へ提供するようなテストプラットフォームへのアクセスをベンダが提供することが必要とされる。

評価者は、以下のテストの 1 つを行わなければならない (shall)。ワイプコマンドの前及び後のテストは同一でなければならない (shall)。このテストは、保護されるべきデータの保存に使用されるメモリの種類それぞれについて、繰り返されなければならない (shall)。

ファイルベースの方法のための方法 1：

*テスト：*評価者は、AGD ガイダンスに従って暗号化を有効化しなければならない (shall)。評価者は、例えばアプリケーションを用いることによって、利用者データ (保護データまたは機微なデータ) を作成しなければならない (shall)。評価者は、開発者によって提供されるツールを利用して、メモリ中に保存されたこのデータを検査しなければならない (shall) (例えば、復号されたファイルを検査することによって)。評価者は、FMT_SMF_EXT.1 に提供される AGD ガイダンスに従って、ワイプコマンドを開始しなければならない (shall)。評価者は、開発者によって提供されるツールを利用してメモリの同一データロケーションを調査し、TSS 中に記述される方法に従ってこのデータがワイプされていることを検証しなければならない (shall) (例えば、ファイルがいまだに暗号化されておりアクセスできない)。

ボリュームベースの方法のための方法 2：

*テスト：*評価者は、AGD ガイダンスに従って暗号化を有効化しなければならない (shall)。評価者は、例えばアプリケーションを用いることによって、一意のデータ文字列を作成しなければならない (shall)。評価者は、開発者によって提供されるツールを利用して、復号されたデータから一意の文字列を検索しなければならない (shall)。評価者は、FMT_SMF_EXT.1 に提供される AGD ガイダンスに従って、ワイプコマンドを開始しなければならない (shall)。評価者は、開発者によって提供されるツールを利用して復号されたメモリ中で同一の一意の文字列を検索し、TSS 中に記述される方法に従ってこのデータがワイプされていることを検証しなければならない (shall) (例えば、ファイルがいまだに暗号化されておりアクセスできない)。

5.2.1.10 暗号ソルト生成

FCS_CKM_EXT.6	拡張：ソルト生成

FCS_CKM_EXT.6.1 TSF は、FCS_RBG_EXT.1 を満たす RBG を用いてすべてのソルトを生成しなければならない (shall)。

適用上の注釈：暗号ソルトは、以下を含むさまざまな利用のために生成される：

- RSASSA-PSS 署名生成
- DSA 署名生成
- ECDSA 署名生成
- DH 静的鍵共有スキーム
- PBKDF

- NIST SP 800-56B 中の鍵共有スキーム

保証アクティビティ：

評価者は、TOE 上のどのアルゴリズムがソルトを要求するかを含め、ソルト生成に関する記述が 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、ソルトが FCS_RBG_EXT.1 に記述される RBG を用いて生成されることを確認しなければならない (shall)。KEK の PBKDF 導出については、この保証アクティビティは FCS_CKM_EXT.3.2 と組み合わせて行われてもよい。

5.2.2 暗号操作 (FCS_COP)

5.2.2.1 機密性アルゴリズム

FCS_COP.1(1)	**暗号操作**

FCS_COP.1.1(1) TSF は、以下の特定された暗号アルゴリズム

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

[選択：

- *AES 鍵ラップ (KW) (NIST SP 800-38F に定義)*、
- *パディング付 AES 鍵ラップ (KWP) (NIST SP 800-38F に定義)*、
- *AES-GCM (NIST SP 800-38D に定義)*、
- *AES-CCM (NIST SP 800-38C に定義)*、
- *AES-XTS (NIST SP 800-38E に定義) モード*、
- *AES-CCMP-256 (NIST SP800-38C 及び IEEE 802.11ac-2013 に定義)*、
- *AES-GCMP-256 (NIST SP800-38D 及び IEEE 802.11ac-2013 に定義)*、
- *その他のモードなし*]

ならびに暗号鍵長 128 ビットの鍵長及び [選択 : *256 ビットの鍵長、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)。

適用上の注釈 : FCS_COP.1.1(1) の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)。2 番目の選択については、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 CBC 及び CCMP は、FCS_TLSC_EXT.1 及び FCS_CKM.1.1(2) への適合のため要求される。

IEEE 802.11-2012 への適合には、AES CCMP (これには SP 800-38C に特定される CCM での AES が使用される) と 128 ビットの暗号鍵長が実装されなければならない (must) ことに注意されたい。オプションとして、256 ビットの暗号鍵長を持つ AES-CCMP-256 または AES-GCMP-256 が IEEE 802.11ac 接続のために実装されてもよい。将来は、これらのモードのうち 1 つが要求されるかもしれない。

256 ビットの鍵長のサポートは、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

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。

AES-CBC テスト

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、または入力を実装者へ供給しその結果を受領することによって、取得され得る。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることによって得られた値と比較しなければならない (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 10 個の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを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、評価者はすべてゼロの暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを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なければならず (shall)、第 2 のセットは 256 個の 256 ビットの鍵／暗号文のペアからなるものとしなければならない (shall)。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 としなければならない (shall)。各ペアの暗号文の値は、それに対応する鍵で復号された際にすべてゼロの平文が得られるような値としなければならない (shall)。

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、評価者は暗号化テストにおける平文と同一の形式の暗号文の値を入力として 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、選んだ鍵及び IV によって、試験すべきモードを用いてメッセージを暗号化しなければならない (shall)。暗号文は、同一の平文メッセージを同一の鍵と IV によって既知の良好な実装を用い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、選んだ鍵及び IV によって、試験すべきモードを用いてメッセージを復号しなければならない (shall)。平文は、同一の暗号文メッセージを同一の鍵と IV によって既知の良好な実装を用いて復号した結果と比較されなければならない (shall)。

AES-CBC モンテカルロテスト

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 ビットの鍵を用いなければならない (shall)。平文と IV の値は、128 ビットのブロックとしなければならない (shall)。3 つ組のそれぞれについて、以下のように 1000 回の反復処理が実行されなければならない (shall)。

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

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-CCM テスト

評価者は、以下の入力パラメタ長とタグ長のそれぞれについて、AES-CCM の生成—暗号化及び復号—検証機能をテストしなければならない (shall)。

128 ビット及び 256 ビットの鍵

2 つのペイロード長. **1 つ**のペイロード長は、ゼロバイト以上のサポートされる最も短いペイロード長としなければならない (shall)。他のペイロード長は、32 バイト (256 ビット) 以下のサポートされる最も長いペイロード長としなければならない (shall)。

2 つまたは 3 つの関連データ長。1 つの関連データ長は 0 としなければならない (shall) (サポートされる場合)。1 つの関連データ長は、ゼロバイト以上でサポートされる最も短い関連データ長としなければならない (shall)。1 つの関連データ長は、32 バイト (256 ビット) 以下でサポートされる最も長い関連データ長としなければならない (shall)。実装が 2^{16} バイトの関連データ長をサポートする場合、2^{16} バイトの関連データ長がテストされなければならない (shall)。

ノンス長。7 バイトから 13 バイトまで (上端及び下端を含む) のサポートされるすべてのノンス長がテストされなければならない (shall)。

タグ長。4、6、8、10、12、14 及び 16 バイトのサポートされるすべてのタグ長がテストされなければならない (shall)。

AES-CCM の生成—暗号化機能をテストするために、評価者は以下の 4 つのテストを実行しなければならない (shall)。

テスト 1. サポートされる鍵及び関連データ長の**それぞれ**について、またサポートされるペイロード、ノンス、及びタグ長の**いずれか**について、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得しなければならない (shall)。

テスト 2. サポートされる鍵及びペイロード長の**それぞれ**について、またサポートされる関連データ、ノンス、及びタグ長の**いずれか**について、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得しなければならない (shall)。

テスト 3. サポートされる鍵及びノンス長の**それぞれ**について、またサポートされる関連データ、ペイロード、及びタグ長の**いずれか**について、評価者は 1 つの鍵の値及び 10 個の関連データ、ペイロード及びノンスの値の 3 つ組を供給し、得られた暗号文を取得しなければならない (shall)。

テスト 4. サポートされる鍵及びタグ長の**それぞれ**について、またサポートされる関連データ、ペイロード、及びノンス長の**いずれか**について、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得しなければならない (shall)。

上記のテストそれぞれの正しさを判断するため、評価者は暗号文を、既知の良好な実装を用いた同一の入力の生成—暗号化の結果と比較しなければならない (shall)。

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

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

AES-GCM テスト

評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、AES-GCM の認証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 通りの IV 長の一方を 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、または入力を実装者へ供給しその結果を受領することによって、取得することができる。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ与えることによって得られた値と比較しなければならない (shall)。

XTS-AES テスト

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

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

3 通りのデータユニット (すなわち、平文) の長さ. データユニット長の 1 つは、128 ビットのゼロ以外の整数倍としなければならない (shall) (サポートされる場合)。データユニット長の 1 つは、128 ビットの整数倍としなければならない (shall) (サポートされる場合)。データユニット長の 3 番目は、サポートされる最も長いデータユニット長か 2^{16} ビットの、いずれか小さいほうとしなければならない (shall)。

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

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

評価者は、暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、XTS-AES 暗号化を XTS-AES 復号と置き換えて、XTS-AES 復号機能をテストしなければならない (shall)。

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

評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、AES-KW の認証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 ビットの鍵暗号化鍵 (KEK)

3 通りの平文の長さ. 平文の長さの 1 つは、セミブロック 2 個 (128 ビット) としなければならない (shall)。平文の長さの 1 つは、セミブロック 3 個 (192 ビット) としなければならない (shall)。データユニット長の 3 番目は、セミブロック 64 個 (4096 ビット) 以下でサポートされる最も長い平文の長さとしなければならない (shall)。

100 個の鍵と平文のペアのセットを用いて、AES-KW 認証済み暗号化から得られた暗号文を取得する。正しさを判断するため、評価者は既知の良好な実装の AES-KW 認証済み暗号化機能を利用しなければならない (shall)。

評価者は、認証済暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、AES-KW 認証済み暗号化を AES-KW 認証済み復号と置き換えて、AES-KW の認証済み復号機能をテストしなければならない (shall)。

評価者は、AES-KW の認証済み暗号化と同一のテストを用い、以下の改変を 3 通りの平文の長さに行って、AES-KWP 認証済み暗号化機能をテストしなければならない (shall)。

平文の長さの 1 つは、1 オクテットとする (shall)。平文の長さの 1 つは、20 オクテット (160 ビット) としなければならない (shall)。

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

評価者は、AES-KWP 認証済暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、AES-KWP 認証済み暗号化を AES-KWP 認証済み復号と置き換えて、AES-KWP の認証済み復号機能をテストしなければならない (shall)。

5.2.2.2 ハッシュアルゴリズム

FCS_COP.1(2)	暗号操作

FCS_COP.1.1(2) TSF は、以下の[***FIPS Pub 180-4***] に合致する、特定された暗号アルゴリズム SHA-1 及び [選択：*SHA-256*、*SHA-384*、*SHA-512*、*その他のアルゴリズムなし*] であって、メッセージダイジェスト長が 160 及び [選択：*256*、*384*、*512 ビット*、*その他のメッセージダイジェストサイズなし*] に従って、[***暗号ハッシュ***] を実行しなければならない (shall)。

適用上の注釈：NIST SP 800-131A に従い、SHA-1 によるデ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。ベンダには SP 800-131A に従って SHA-2 アルゴリズムを実装することが期待され、また 2015 年の第 3 四半期以降に評価に入る製品には SHA-2 ア

ルゴリズムが含まれることが要求されることになる。

SHA-1 は現在、FCS_TLSC_EXT.1 及び FCS_CKM.1.1(2) に適合するため要求されている。ベンダには、SHA-2 ファミリをサポートする更新されたプロトコルの実装が強く推奨される。更新されたプロトコルがサポートされるまで、本 PP は SP 800-131A に適合した SHA-1 の実装を許す。

本要件の意図は、ハッシュ関数を特定することである。ハッシュの選択は、メッセージダイジェスト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、使用さ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 AGD 文書をチェックして、必要とされるハッシュのサイズ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判断する。評価者は、ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連が TSS に文書化されていることをチェックしなければならない (shall)。

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使用さ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)。

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。

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。

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。

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 $1 \le i \le m$)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、

それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—バイト指向モード

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。

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。

5.2.2.3 署名アルゴリズム

FCS_COP.1(3)	**暗号操作**

FCS_COP.1.1(3) TSF は、以下の特定された暗号アルゴリズムに従って、[***暗号署名サービス (生成及び検証)***] を実行しなければならない (shall)

- [**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： [**FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 4**]

及び [選択：

- ***[ECDSA 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)”, Section 5**]；*
- *その他のアルゴリズムなし*

]。

適用上の注釈：ST 作成者は、デ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特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特定すべきである (should)。RSA 署名生成及び検証は現在、FCS_TLSC_EXT.2 に適合するため要求されている。

ECDSA スキームは、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

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。

ECDSA アルゴリズムテスト

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)。正しさを判断するため、評価者は既知の良好な実装の署名検証機能を利用しなければならない (shall)。

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) を改変しなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

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)。

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。

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

5.2.2.4 鍵付きハッシュアルゴリズム

FCS_COP.1(4)	暗号操作

FCS_COP.1.1(4) TSF は、以下の [***選択：FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code、及びFIPS Pub 180-4, "Secure Hash Standard***] に合致する、特定された暗号アルゴリズム HMAC-SHA-1 及び [*選択:HMAC-SHA-256、HMAC- SHA-384、HMAC- SHA-512、その他のアルゴリズムなし*] と暗号鍵長 [割付 : *HMAC に使用される (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 160 及び [選択 : *256、384、512、その他なし*] ビットに従って、[***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)。

適用上の注釈：本要件における選択は、鍵付きハッシュメッセージ認証と関連して使用される鍵のサイズに特定される鍵長と一貫していなければならない (must)。HMAC-SHA-1 は現在、FCS_TLSC_EXT.1 及び FCS_CKM.1.1(2) に適合するため要求されている。

HMAC-SHA-256 及び HMAC-SHA-384 は、FCS_TLS_EXT.2.1 の暗号スイートをサポート

するため 2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

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

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。

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、同一の鍵と IV によって既知の良好な実装を用いて生成された HMAC タグと比較されなければならない (shall)。

5.2.2.5 パスワードベースの鍵導出関数

FCS_COP.1(5)	暗号操作

FCS_COP.1.1(5) TSF は、以下の[**NIST SP 800-132**] に合致する、特定された暗号アルゴリズム [*HMAC-[選択：SHA-1、SHA-256、SHA-384、SHA-512]*] であって、[割付：*整数*] 回の反復処理と出力暗号鍵長 [選択 : *128, 256*] ビットを伴う、[***パスワードベースの鍵導出関数***] を実行しなければならない (shall)。

適用上の注釈: 2 番目の選択の中の暗号鍵長は、FCS_CKM_EXT.3 において選択された KEK 鍵長に対応して行われるべきである (should)。256 ビットの鍵長の使用は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

このパスワードは、KEK への入力として使用されるサブマスクを形成するビット列へ調整されなければならない (must)。調整は、特定されたハッシュ関数のいずれか、または NIST SP 800-132 に記述されるプロセスを用いて行うことができる。使用される方法は ST 作成者によって選択される。NIST SP 800-132 では、HMAC と承認済ハッシュ関数からなる疑似ランダム関数 (PRF) の使用が要求される。ST 作成者は、使用されるハッシュ関数を選択するとともに、HMAC 及びハッシュ関数の適切な要件が含まれるようにする。

NIST SP 800-132 の附属書 A では、パスワードから鍵を導出するために必要とされる計算量を増加させるため、またそれによって辞書攻撃を行うための労力を増加させるため、反復回数を設定することを推奨している。

保証アクティビティ：

評価者は、パスワードがまずエンコードされてそれから SHA アルゴリズムへ供給される方法が TSS に記述されていることをチェックしなければならない (shall)。アルゴリズムの設定 (パディング、ブロック化など) が記述されていなければならず (shall)、またこれらがこのコンポーネントと共にハッシュ関数そのものに関する選択によってサポートされていることを評価者は検証しなければならない (shall)。評価者は、この機能へ入力されるサブマスクの形成にハッシュ関数の出力がどのように使用され、そしてそれが FCS_CKM_EXT.3 に特定される KEK と同一の長さであるという記述が TSS に含まれることを検証しなければならない (shall)。

NIST SP 800-132 ベースのパスフレーズの調整については、要求される保証アクティビティは適切な要件 (FCS_COP.1.1(4)) の保証アクティビティを行う際に実施されることにな

る。KEK の形成に使用されるサブマスクの形成にあたって何らかの鍵の操作が行われる場合、そのプロセスは TSS に記述されなければならない (shall)。

入力されるパスワードからのサブマスクの形成の明示的なテストは、要求されない。

評価者は、TOE によって行われる PBKDF の反復回数が NIST SP 800-132 に適合していることを、パスワードから鍵材料を導出するために必要とされる予想時間の記述と、TOE がパスワードベースの鍵導出のための計算時間を増加させている方法 (反復回数の増加を含むが、それに限定されない) が TSS に含まれることを保証することによって、検証しなければならない (shall)。

5.2.3 HTTPS プロトコル (FCS_HTTPS)

FCS_HTTPS_EXT.1	拡張：HTTPS プロトコル

FCS_HTTPS_EXT.1.1 TSF は、RFC 2818 に準拠する HTTPS プロトコルを実装しなければならない (shall)。

FCS_HTTPS_EXT.1.2 TSF は、TLS (FCS_TLSC_EXT.2) を用いて HTTPS を実装しなければならない (shall)。

FCS_HTTPS_EXT.1. 3 TSF は、ピア証明書が無効とみなされる場合にはアプリケーションに通知すると共に [選択 : 接続を確立しない、接続を確立するための認証をアプリケーションに要求する、その他のアクションなし] を行わなければならない (shall)。

適用上の注釈：有効性は認証パス、有効期限、及び RFC 5280 にしたがう失効状態によって判断される。

保証アクティビティ：

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

その他のテストは、FCS_TLSC_EXT.2 と組み合わせて行われる。

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 2 : 評価者は、有効な認証パスのない証明書を使用すると、アプリケーション通知が発生することを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)。

5.2.4 初期化ベクタ生成 (FCS_IV)

FCS_IV_EXT.1	拡張：初期化ベクタ生成

FCS_IV_EXT.1.1 TSF は、表 14 :「NIST 承認暗号利用モードの参照情報と IV 要件」に従って IV を生成しなければならない (shall)。

適用上の注釈：表 14 には、暗号利用モードのそれぞれについて、対応する NIST Special Publications にしたがった IV の作成に関する要件が列挙されている。暗号プロトコルにしたがった暗号化のために生成される IV の作成は、そのプロトコルによって対応される。したがって、本要件は鍵ストレージ及びデータストレージ暗号化のために生成される IV にの

み対応する。

保証アクティビティ：

評価者は、TSS の鍵階層構造セクションを検査して、すべての鍵の暗号化が記述されていること、そして同一の KEK によって暗号化される鍵のそれぞれについて IV の形成が FCS_IV_EXT.1 を満たしていることを保証しなければならない (shall)。

5.2.5 ランダムビット生成 (FCS_RBG)

FCS_RBG_EXT.1	**拡張：暗号操作 (ランダムビット生成)**

FCS_RBG_EXT.1.1: TSF は、[選択、*1 つを選択:*[選択：*Hash_DRBG (任意)* 、*HMAC_DRBG (任意)* 、*CTR_DRBG (AES)] を用いる NIST Special Publication 800-90A*、*AES を用いる FIPS Pub 140-2 附属書 C： X9.31 附属書 2.4*] に従って、すべての決定論的ランダムビット生成サービスを行わなければならない (shall) 。

FCS_RBG_EXT.1.2 決定論的 RBG は、鍵とそれが生成するハッシュとの (NIST SP 800-57 による) セキュリティ強度の大きいほうと少なくとも等しい、 [選択：*128 ビット*、*256 ビット*] の最小エントロピーを持つ、 [選択：*ソフトウェアベースのノイズ源*、*TSF ハードウェアベースのノイズ源*] 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を供給されなければならない (shall)。

FCS_RBG_EXT.1.3: TSF は、ランダムなビットを要求する TSF 上で動作中のアプリケーションへ RBG の出力を供給できなければならない (shall)。

適用上の注釈：NIST Special Pub 800-90B の附属書 C には、最小エントロピーの測定について記述されており、これは直ちに使用されるべき (should) であり、また本 PP の将来の版では必須となる。

FCS_RBG_EXT.1.1 の最初の選択に関しては、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方法が含まれる。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 に使用さ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。識別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 については許されているが、CTR_DRBG については AES ベースの実装のみが許されている。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4, Section 3 に記述される方法のみが有効であることに注意されたい。ここで使用される AES 実装の鍵の長さが利用者データの暗号化に使用されるものと異なる場合には、FCS_COP.1 を調整するか繰り返して異なる鍵の長さを反映する必要があるかもしれない。このオプションは、2016 年 1 月 1 日以降に評価に入る製品については、もはや許可されない。

また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に確実に含まれるようにしなければならない (must)。

DRBG のヘルステストは、FPT_TST_EXT.1.1 に要求される自己テストと組み合わせて行われる。

FCS_RBG_EXT.1.2 の選択については、ST 作成者は ST に含まれるアルゴリズムの中で最も大きなセキュリティ強度に対応するエントロピーの適切なビット数を選択する。セキュ

リティ強度は、NIST SP 800-57A の表 2 及び 3 に定義されている。例えば、実装に 2048 ビット RSA (セキュリティ強度 112 ビット)、AES 128 (セキュリティ強度 128 ビット)、そして HMAC-SHA-256 (セキュリティ強度 256 ビット) が含まれている場合、ST 作成者は 256 を選択することになる。256 ビットのシード供給は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

ST 作成者は、ソフトウェアまたはハードウェアのノイズ源のどちらかを選択してよい。ハードウェアノイズ源は、その物理的特性により、決定論的ルールでは説明できないデータを作成するコンポーネントである。別の言い方をすれば、ハードウェアベースノイズ源は、予測不可能な物理プロセスから乱数列を生成する。例えば、ループ状に接続された奇数のインバータゲートからなるリングオシレータをサンプリングすることが考えられる。ここで電気的パルスはインバータからインバータへ、ループを周回しながら伝播する。インバータにはクロックが与えられていないので、ループを周回するために必要な正確な時間は、さまざまな物理的効果によって各インバータから次に接続されたインバータへの遅延時間が変わるため、わずかに変動することになる。この変動が、概略固有振動数のまわりで時間とともにドリフトとジッタを引き起こす結果となる。この、バイナリ値を振動するリングオシレータの出力が、ひとつのインバータから一定周期 (オシレータの固有周波数よりもはるかに遅い周期) でサンプリングされる。

保証アクティビティ：

附属書 E 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))。

評価者は、セクション 6.2.1 に従って提供される API 文書に、FCS_RBG_EXT.1.3 に記述されるセキュリティ機能が含まれることを検証しなければならない (shall)。

保証アクティビティの注釈：以下のテストには、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。

評価者は、RBG が準拠する標準に従って、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 に準拠する実装

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。

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。

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 に特

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 に準拠する実装

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 SP800-90A に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

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。

5.2.6 暗号アルゴリズムサービス (FCS_SRV)

FCS_SRV_EXT.1	**拡張：暗号アルゴリズムサービス**

FCS_SRV_EXT.1.1 TSF は、アプリケーションが以下の暗号操作の実施を TSF に要求するメカニズムを提供しなければならない (shall) :

- FCS_CKM.2(1) におけるすべての必須及び選択済みアルゴリズム
- FCS_COP.1(1) における以下のアルゴリズム : AES-CBC、[選択 : AES 鍵ラップ、パディング付 AES 鍵ラップ、AES-GCM、AES-CCM、その他のモードなし]
- FCS_COP.1(3) におけるすべての必須及び選択済みアルゴリズム
- FCS_COP.1(2) におけるすべての必須及び選択済みアルゴリズム
- FCS_COP.1(4) におけるすべての必須及び選択済みアルゴリズム

[選択 :

- *FCS_CKM.1(1) におけるすべての必須及び選択済みアルゴリズム*、
- *FCS_COP.1(5) における選択済みアルゴリズム*、
- *その他の暗号操作なし*]。

適用上の注釈：丸印付きのリストに列挙された FCS コンポーネントのそれぞれについて、TOE が ST 中でそのコンポーネントに関して特定されたすべてのアルゴリズムを利用できるようにすることが意図されている。例えば、FCS_COP.1(2) に関して ST 作成者が SHA-256 を選択する場合には、TOE は SHA-1 (FCS_COP.1.1(2) の「必須」部分) 及び SHA-256 (FCS_COP.1.1(2) の「選択済み」部分) を行うためのインタフェースを利用できるようにしなければならない (have to) であろう。例外は FCS_COP.1(1) に関するものであり、ここでは TOE が AES_CCMP、AES_XTS、AES_GCMP-256、または AES_CCMP_256 を利用できるようにすることは、たとえこれらが TSF 関連機能を行うために実装されていたとしても、要求されない。しかし、ST 作成者は FCS_COP.1(1) コンポーネントに関して ST 中で選択されているものとマッチするアルゴリズムを選択することが期待される (本コンポーネント中の FCS_COP.1(1) の選択に応じて)。

保証アクティビティ：

評価者は、セクション 6.2.1 に従って提供される API 文書に、これらの要件に記述されるセキュリティ機能 (暗号アルゴリズム) が含まれることを検証しなければならない (shall)。

評価者は、TSF による暗号操作を要求するアプリケーションを書かなければならない (shall)。または、開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。評価者は、操作から得られた結果が API 文書に従って期待される結果と一致することを検証しなければならない (shall)。このアプリケーションは、他のアルゴリズムサービス要件の暗号操作保証アクティビティを検証する補助として用いることもできる。

5.2.7 暗号鍵ストレージ (FCS_STG)

本セクションでは、どのように鍵が保護されるのかを記述する。すべての鍵は最終的に REK によって保護されなければならず (must)、またオプションとして利用者のパスワードによって保護されてもよい。それぞれの鍵の機密性と完全性は、保護されなければならない (must)。また本セクションでは、アプリケーション及び利用者による利用のためモバイルデバイスによって提供されるべきセキュアな鍵ストレージサービスについても記述する。これらの鍵には、OS 内部の鍵と同一のレベルの保護が適用される。

5.2.7.1 セキュアな鍵ストレージ

FCS_STG_EXT.1	**拡張：暗号鍵ストレージ**

FCS_STG_EXT.1.1 TSF は、非対称プライベート鍵及び [選択：*対称鍵*、*永続的秘密*、*その他の鍵なし*] に [選択：*ハードウェアの*、*ハードウェア分離された*、*ソフトウェアベースの*] セキュアな鍵ストレージを提供しなければならない (shall)。

適用上の注釈：このセキュアな鍵ストレージが完全にハードウェアで実装されている場合、ST 作成者は「ハードウェア」を選択しなければならない (shall)。鍵ストレージは、、OS が鍵による操作を要求することしか許されないように、鍵の生のバイトが TSF 上のいかなるソフトウェアにも利用できない場合、完全にハードウェアで実装されているとみなされる。ハードウェアの鍵ストアは、USB、microSD、及び Bluetooth を含む、さまざまなインタフェースを通して TSF へ公開され得る。

セキュアな鍵ストレージが、処理とメモリの両方でリッチ OS から分離された、別個のプロセッサ実行環境で実装されている場合、ST 作成者は「ハードウェア分離された」を選択しなければならない (shall)。

セキュアな鍵ストレージが FCS_STG_EXT.2 によって要求されるように保護されたソフトウェアで実装されている場合、ST 作成者は「ソフトウェアベースの」を選択しなければならない (shall)。「ソフトウェアベースの」が選択される場合、ST 作成者は FCS_STG_EXT.2 中の「すべてのソフトウェアベースの鍵ストレージ」を選択しなければならない (shall)。

すべての対称鍵及び永続的秘密のためのセキュアな鍵ストレージのサポートは、将来の版で要求されることになる。

FCS_STG_EXT.1.2 TSF は、[選択：*利用者*、*管理者*] 及び [選択：*TSF 上で動作中のアプリケーション*、*その他のサブジェクトなし*] の要求により、鍵／秘密をセキュアな鍵ストレージへインポートできなければならない (shall)。

適用上の注釈：ST 作成者が利用者のみを選択した場合、ST 作成者は FMT_MOF_EXT.1.1 中の機能 11 もまた選択しなければならない (shall)。

FCS_STG_EXT.1.3 TSF は、[選択：*利用者*、*管理者*] の要求により、セキュアな鍵ストレージの中の鍵／秘密を破棄できなければならない (shall)。

適用上の注釈：ST 作成者が利用者のみを選択した場合、ST 作成者は FMT_MOF_EXT.1.1 中の機能 12 もまた選択しなければならない (shall)。

FCS_STG_EXT.1.4 TSF は、鍵／秘密をインポートしたアプリケーションにのみ、その鍵／秘密の利用を許可することができなければならない (shall)。例外は、[選択：*利用者*、*管理者*、*共通アプリケーション開発者*] により明示的に許可された場合のみかもしれない。

適用上の注釈：ST 作成者が利用者または管理者を選択した場合、ST 作成者は FMT_SMF_EXT.1.1 中の機能 34 もまた選択しなければならない (must)。ST 作成者が利用者のみを選択した場合、ST 作成者は FMT_MOF_EXT.1.1 中の機能 34 もまた選択しなければならない (shall)。

FCS_STG_EXT.1.5 TSF は、鍵／秘密をインポートしたアプリケーションにのみ、その鍵／秘密の破棄を要求することを許可しなければならない (shall)。例外は、[選択：*利用者*、*管理者*、*共通アプリケーション開発者*] により明示的に許可された場合のみかもしれない。

適用上の注釈：ST 作成者が利用者または管理者を選択した場合、ST 作成者は FMT_SMF_EXT.1.1 中の機能 35 もまた選択しなければならない (must)。ST 作成者が利用者のみを選択した場合、ST 作成者は FMT_MOF_EXT.1.1 中の機能 35 もまた選択しなければならない (must)。

保証アクティビティ：

このコンポーネントの保証アクティビティには、ST の TSS を検査して、要求されるセキュアな鍵ストレージを TOE が実装していることを判断することが必要とされる。評価者は、「ハードウェアの」、「ハードウェア分離された」、または「ソフトウェアベースの」の選択を正当化する鍵ストレージメカニズムの記述が 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 AGD ガイダンスををレビューして、鍵／秘密をインポートまたは破棄するために必要な手順が記述されていることを判断しなければならない (shall)。また評価者は、セクション 6.2.1 に従って提供される API 文書に、これらの要件に記述されるセキュリティ機能 (インポート、利用、及び破棄) が含まれることを検証しなければならない (shall)。API 文書には、FCS_STG_EXT.1.4 を満たすためにアプリケーションへ鍵／秘密へのアクセスを制限するための方法が含まれなければならない (shall)。

評価者は、各セキュリティ機能の機能をテストしなければならない (shall)。

テスト 1 : 評価者は、AGD に従ってサポートされるそれぞれの種類の鍵／秘密をインポートしなければならない (shall)。評価者は、サポートされるそれぞれの種類の鍵／秘密を生成しインポート機能を呼び出すアプリケーションを書かなければならない (shall)。または、開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。評価者は、インポート中に何のエラーも発生しないことを検証しなければならない (shall)。

テスト 2 : 評価者は、インポートされた種類の鍵／秘密を利用するアプリケーションを書かなければならない (shall)。または、開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。

- RSA については、秘密はデータの署名に使用されなければならない (shall)。
- ECDSA については、秘密はデータの署名に使用されなければならない (shall)

将来は、これ以外の種類もテストが要求されることになる。

- 対称アルゴリズムについては、秘密はデータの暗号化に使用されなければならない (shall)。
- 永続的秘密については、秘密はインポートされた秘密と比較されなければならない (shall)。

評価者は、アプリケーションによってインポートされた鍵／秘密及び異なるアプリケーションのインポートされた鍵／秘密と共にこのテストを繰り返さなければならない (shall)。評価者は、利用者によって、または異なるアプリケーションによってインポートされた鍵／秘密の使用をアプリケーションに許可する前に、TOE が承認を必要とすることを検証しなければならない (shall)。

- 評価者は承認を拒否し、記述されたとおりアプリケーションがその鍵／秘密を使用できない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繰り返し、承認を許可してアプリケーションがその鍵／秘密を使用できることを検証しなければならない (shall)。

ST 作成者が「共通アプリケーション開発者」を選択した場合、このテストは異なる開発者からのアプリケーションを使用するか、 (API 文書に従って) 適切に共有を承認しないか、いずれかによって行われる。

テスト 3 : 評価者は、AGD ガイダンスに従ってサポートされるそれぞれの種類の鍵／秘密を破棄しなければならない (shall)。評価者は、インポートされた種類の鍵／秘密を破棄するアプリケーションを書かなければならない (shall)。または、開発者がそのようなアプリ

ケーションへのアクセスを提供しなければならない (shall)。

評価者は、アプリケーションによってインポートされた鍵／秘密及び異なるアプリケーションのインポートされた鍵／秘密と共にこのテストを繰り返さなければならない (shall)。評価者は、管理者によって、または異なるアプリケーションによってインポートされた鍵／秘密の破棄をアプリケーションに許可する前に、TOE が承認を必要とすることを検証しなければならない (shall)。

- 評価者は承認を拒否し、記述されたとおりアプリケーションがその鍵／秘密を引き続き使用でき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繰り返し、承認を許可してアプリケーションがもはやその鍵／秘密を使用できないことを検証しなければならない (shall)。

ST 作成者が「共通アプリケーション開発者」を選択した場合、このテストは異なる開発者からのアプリケーションを使用するか、 (API 文書に従って) 適切に共有を承認しないか、いずれかによって行われる。

5.2.7.2 保存された鍵の暗号化

FCS_STG_EXT.2	**拡張：暗号化された暗号鍵のストレージ**

FCS_STG_EXT.2.1 TSF は、DEK 及び KEK ならびに [選択：*長期高信頼チャネル鍵材料*、*すべてのソフトウェアベースの鍵ストレージ*、*その他の鍵なし*] を、以下の KEK によって保護しなければならない (shall) [*選択：*

1) *以下によってREK に保護されるもの [選択：*
   a. *REK による暗号化*、
   b. *REK へチェインする KEK による暗号化]*、
2) *以下によってREK 及びパスワードに保護されるもの [選択：*
   a. *REK 及びパスワードから導出された KEK による暗号化*、
   b. *REK へチェインする KEK 及びパスワードから導出された KEK による暗号化]*

]。

適用上の注釈：FCS_STG_EXT.1.1 において「ソフトウェアベースの」が選択される場合、ST 作成者は「すべてのソフトウェアベースの鍵ストレージ」を選択しなければならない (must)。FCS_STG_EXT.1.1 において ST 作成者が「ハードウェアの」または「ハードウェア分離された」を選択する場合、セキュアな鍵ストレージは本要件の対象とはならない。

REK は、本要件の対象とはならない。

REK 及びパスワードから導出された KEK は、本要件を満たすために結合されて結合 KEK を形成してもよい (FCS_CKM_EXT.3 に記述されるように)。

機微なデータは、REK 及びパスワードによって保護される。本体に FDP_DAR_EXT.2 が含まれる場合、この機微なデータには利用者またはエンタープライズデータの一部または全部が含まれる。ソフトウェアベースの鍵ストレージは、すべて機密性がある (REK 及びパスワードによって保護される) か、FDP_DAR_EXT.2.1 に従って鍵を機密性がある (REK 及びパスワードによって保護される) とマークすることを利用者及びアプリケーションに許可するか、いずれかでなければならない (shall)。

すべての鍵は最終的に REK によって保護されなければならない (must)。機微なデータは、

パスワードによって保護されなければならない (must) (選択 2)。特に、図 3 にはこれらの要件に従って保護された KEK が含まれている。DEK_1 は 2a を満たし機微なデータに適当であり、DEK_2 は 1b を満たし機微なデータに適当ではなく、K_1 は 1a を満たし機密性のある鍵とはみなされず、そして K_2 は 2b を満たし機密性のある鍵とみなされる。

長期高信頼チャネル鍵材料には、IPsec や WiFi の事前共有鍵並びにリンク鍵、長期鍵 (LTK)、コネクション署名解決鍵 (CSRK)、識別情報解決鍵 (IRK)、及び汎用 AMP リンク鍵などの Bluetooth 鍵が含まれる。これらの鍵は、ロック状態においても必要とされる可能性があるため、パスワードによって保護されてはならない (shall not)。長期高信頼チャネル鍵材料の暗号化は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

評価者は、保存データ用の各 DEK、ソフトウェアベースの鍵ストレージ、長期高信頼チャネル鍵、及び DEK、長期高信頼チャネル鍵とソフトウェアベースの鍵ストレージの保護に関連する KEK についての保護における鍵の階層構造の記述が TSS に含まれていることを決定するために TSS をレビューしなければならない (shall)。この記述には、実装が FCS_STG_EXT.2 を満たすことを論証するために TOE によって実装された鍵階層構造を説明する図が含まれなければならない (must)。その記述には、FCS_RBG_EXT.1 によって記述される機能が DEK (FCS_CKM_EXT.2)を生成するために起動される方法、それぞれの鍵の鍵長 (FCS_CKM_EXT.2 及び FCS_CKM_EXT.3)、それぞれの KEK が形成される方法 (FCS_STG_EXT.3 に従って生成、導出、または結合される(combined))、暗号化された鍵のそれぞれについて完全性の保護方法 (FCS_STG_EXT.3)、そして同一の KEK によって暗号化される鍵のそれぞれについての IV 生成 (FCS_IV_EXT.1) が示されなければならない (shall)。各タスクのさらなる詳細は、関連する要件に従う。

FCS_STG_EXT.2.2 DEK 及び KEK ならびに [選択：*長期高信頼チャネル鍵材料、すべてのソフトウェアベースの鍵ストレージ、その他の鍵なし*] は、[選択: *鍵ラップ (KW) モード、パディング付きの鍵ラップ (KWP) モード、GCM、CCM、CBC モード*] の AES を用いて暗号化されなければならない (shall)。

適用上の注釈：128 ビットまたは 256 ビットのいずれか (または両方) が許可される。ST 作成者は、デバイスに適切な選択を行う。本要件は、本 PP で定義される KEK にのみ適用され、その他の規格で特定される KEK には適用されない。

保証アクティビティ：

評価者は、それぞれの鍵 (DEK、ソフトウェアベースの鍵ストレージ、及び KEK) が、選択されたモードの一つを用いたセキュリティ強度以上の鍵によって暗号化されることを保証するために TSS に鍵階層構造のセクションを検査しなければならない (shall)。

評価者は、それぞれの DEK とソフトウェア保存鍵が FCS_STG_EXT.2 に従って暗号化されることを検証するために TSS 中の鍵階層構造の記述を検査しなければならない (shall)。

5.2.7.3 保存された鍵の完全性

FCS_STG_EXT.3	**拡張：暗号化鍵ストレージの完全性**

FCS_STG_EXT.3.1 TSF は、任意の暗号化された DEK 及び KEK ならびに [選択 : *長期高信頼チャネル鍵材料、すべてのソフトウェアベースの鍵ストレージ、その他の鍵なし*] の完全性を以下によって保護しなければならない (shall) [選択：

- *FCS_STG_EXT.2 に従う暗号化の* [*選択 : GCM、CCM、鍵ラップ、パディング付*

き鍵ラップ] *暗号利用モード*;

- *FCS_STG_EXT.2 により保護された鍵により暗号化される保存された鍵のハッシュ (FCS_COP.1(2))*;
- *FCS_STG_EXT.2 により保護された鍵を用いる鍵付きハッシュ(FCS_COP.1(4))*;
- *FCS_STG_EXT.2 に従い保護された非対称鍵を用いる保存された鍵のデジタル署名*]。

FCS_STG_EXT.3.2 TSF は、保存された鍵の [選択：*ハッシュ*、*デジタル署名*、*MAC*] の完全性をその鍵の使用前に検証しなければならない (shall)。

適用上の注釈：本要件は、保存されない導出された鍵には適用されない。

1 つの鍵がこれらの方法を複数使うことによって破損から保護されることは期待されていない。しかし、製品はある種別の鍵にはある完全性保護方法を使い、別の種別の鍵には別の方法を用いてもよい。選択肢のそれぞれについての明示的な保証アクティビティは、要件 (FCS_COP.1.1(2), FCS_COP.1.1(4)) のそれぞれにおいて記述されている。

保証アクティビティ：

評価者は、暗号化された鍵のそれぞれが、FCS_STG_EXT.3 中の選択肢のひとつに従って完全性が保護されることを検証するため、TSS 中の鍵階層構造の記述を検査ししなければならない(shall)。

5.2.8 TLS クライアントプロトコル (FCS_TLS)

5.2.8.1 EAP-TLS クライアントプロトコル

FCS_TLSC_EXT.1	**拡張：EAP TLS プロトコル**

FCS_TLSC_EXT.1.1 TSF は、TLS 1.0 及び [選択: *TLS 1.1 (RFC 4346)*、*TLS 1.2 (RFC 5246)*、*その他の TLS バージョンなし*] を、以下の暗号スイートをサポートしするよう、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
- [選択：オプションの暗号スイート：
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
  - *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*
  - *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_256_CBC_SHA384*
- *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_GCM_SHA384*
- *その他の暗号スイートなし*]]。

適用上の注釈：評価される構成においてテストされるべき暗号スイートは、本要件により制限される。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)。もし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使用可能な暗号スイートを制限することは必要である。上記の Suite B アルゴリズム (RFC 6460) は、実装上望ましいアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への準拠を保証するため要求されている。

もし楕円曲線暗号スイートが選択される場合、FCS_TLSC_EXT.1.5 が ST に含まれなければならない (shall)。

TLS 1.2 は望ましいプロトコルである。しかし、TLS 1.0 は現在 RFC 5216 への適合を保証するため必要とされている。TLS 1.0 及び TLS 1.1 は、TLS 1.2 のサポートの欠如のため現在のところ許容されている。TLS 1.0 及び TLS 1.1 は、112 ビット以上のセキュリティ強度を持つ接続を保証するために必要な拡張を有していない。

TLS 1.2 は、2015 年の第 3 四半期以降に評価に入る製品について EAP-TLS が必須となる。これらの要件は、IETF により新しい TLS のバージョンが規格化された際に再検討されることになる。

保証アクティビティ：

評価者は、サポートされる暗号スイートが特定されていることを保証するため、TSS 中の本プロトコル実装の記述をチェックしなければならない (shall)。 評価者は、特定された暗号スイートが本コンポーネントに列挙されたものを含むことを保証するため、TSS をチェックしなければならない (shall)。 評価者は、TLS が TSS の記述と適合するように TOE の設定に関する指示が操作ガイダンスに含まれることを保証するため、操作ガイダンスについてもチェックしなければならない (shall)。

評価者は、以下のテストについても実施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、例えば、EAP セションの一部として確立されてもよい。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、使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 ではないこと) を見極めようとして暗号化されたトラフィックの特徴を検査する必要はない。

テスト 2 : 評価者は、extendedKeyUsage フィールド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 (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、または ECDSA 暗号スイートのひとつを使用しているのに RSA 証明書を送信) を TLS 接続中に送信しなければならない (shall)。評価者は、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 TOE が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、トラフィックに以下の改変を行わなければならない (shall) :

- Server Hello 中のサーバにより選択された TLS バージョンを非サポートの 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) に改変し、クライアントが接続を拒否することを検証する。
- Server Hello ハンドシェイクメッセージ中のサーバのノンスの少なくとも 1 バイトを改変して、クライアントが Server Key Exchange ハンドシェイクメッセージを拒否すること (DHE または ECDHE 暗号スイートの場合) またはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。
- Server Hello 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、Client Hello ハンドシェイクメッセージ中に存在しない暗号スイートに改変する。評価者は、Server Hello を受信した後に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) 。
- サーバの 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、Server Key Exchange メッセージの受信後にクライアントが接続を拒否することを検証する。
- Server Finished ハンドシェイクメッセージの 1 バイトを改変して、受信するとクライアントが fatal alert を送信し、アプリケーションデータを一切送信しないことを検証する。
- サーバが ChangeCipherSpec メッセージを発行した後にサーバから歪曲されたメッセージを送信し、クライアントが接続を拒否することを検証する。

FCS_TLS_EXT.1.2 TSF は、EAP-TLS に提示されたサーバ証明書が [選択 : *特定の CA のひとつへチェーンする*、*受容可能な認証サーバ証明書の特定の FQDN を含む*] ことを検証しなければならない (shall)。

適用上の注釈：CA または FQDN は、FMT_SMF_EXT.1 の機能 7.a に従って特定される。

保証アクティビティ：

評価者は、証明書への署名が許可される認証局のリストを設定するため、または EAP-TLS 交換において TOE が受け入れる認証サーバ証明書の FQDN を設定するための、管理者への指示が AGD ガイダンスに含まれていることをチェックしなければならない (shall)。

RFC 5246 への適合性をテストするため、将来さらにテストが追加されるかもしれない。評価者は、以下のテストについても実行しなければならない (shall)。

テスト 1 : AGD ガイダンスにより提供されるガイダンスにしたがい、CA または FQDN が認証サーバ証明書として「受け入れ可能」と設定され、次に評価者は無線接続を開始し、

無線クライアントが接続に成功することを検証すること。次に評価者は、証明書が TOE により許可されていない CA により署名されるか、または TOE により許可されてない FQDN を証明書が提示する、それ以外は有効であるようにシステムを設定する。このような証明書を提示する認証サーバへの認証の試行は、接続において拒否される結果となるべきである (should)。TOE が受け入れ可能な認証サーバを制限する両方の方法をサポートする場合、評価者はこのテストを 2 回、各方法について 1 回ずつ、繰り返さなければならない (shall)。

FCS_TLSC_EXT.1.3 TSF は、ピア証明書が無効である場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注釈：有効性は識別子の検証、証明書パス、有効期限、及び RFC 5280 にしたがう失効状態により決定される。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、本チャネルは確立されてはならない (shall not)。TLS 上に HTTPS が実装されるが、HTTPS プロトコル (FCS_HTTPS_EXT.1) は、異なるふるまいを要求する。本エレメントは、非 HTTPS の TLS 接続に対処する。

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、有効な認証パスを持たない証明書の使用が、機能しない結果をもたらうことを実証しなければならない (shall)。管理ガイダンスを用いて、評価者は、次にその機能で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、その機能がうまく動作することを実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、うまく機能しないことを示さなければならない (shall)。

FCS_TLSC_EXT.1.4 TSF は、X.509v3 証明書を用いる相互認証をサポートしなければならない (shall)。

適用上の注釈：TLS での X.509v3 証明書の使用は、FIA_X509_EXT.2.1 で対処されている。本要件は、クライアントが TLS 相互認証用に TLS サーバへ証明書を提示可能でなければならない (must) ことをこの使用に含まれなければならない (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 で要求される TSS 記述に、TLS 相互認証用のクライアント証明書の使用が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、FIA_X509_EXT.2.1 で要求される AGD ガイダンスに、TLS 相互認証用のクライアント証明書を設定するための指示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、以下のテストについても実行しなければならない (shall)：

*テスト 1：*評価者は、トラフィックに対して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にサーバを設定し、次にサーバの CertificateRequest ハンドシェイクメッセージの CA フィールドにある 1 バイトを改変する。改変された CA フィールドは、クライアント証明書に署名するために使用された 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)。

5.2.8.2 TLS クライアントプロトコル

FCS_TLSC_EXT.2	拡張：TLS プロトコル

FCS_TLSC_EXT.2.1 TSF は、TLS 1.2 (RFC 5246) を実装し、下記の暗号スイートをサポートしなければならない (shall)：[

- 必須暗号スイート：
  - RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
- [選択：オプションの暗号スイート：
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
  - *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*
  - *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_SHA 256*
  - *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_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *その他の暗号スイートなし*]]。

適用上の注釈：評価構成でテストされるべき暗号スイートは、本要件により制限される。ST 作成者は、サポートされた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)。テスト環境のサーバ上で評価構成において管理的に使用可能な暗号スイートを制限する必要がある。上記の Suite B アルゴリズム (RFC 6460) は、実装上の推奨アルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への準拠を保証するため要求されている。

楕円曲線暗号スイートが選択される場合、FCS_TLSC_EXT.2.5 が ST に含まれなければならない (shall)。

これらの要件は、IETF により新たな TLS バージョンが標準化される際に再検討される。

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 は、2015 年の第 3 四半期以降に評価に入る製品について必須となるだろう。

保証アクティビティ：

評価者はて、サポートされた暗号スイートが指定されていることを保証するため、TSS における本プロトコル実装の記述をチェックししなければならない (shall)。評価者は指定さ

れた暗号スイートが本コンポーネントに列挙されたものを含むことを保証するため、TSS をチェックしなければならない (shall)。また評価者は、TLS が TSS の記述に適合するように TOE を設定するための指示が操作ガイダンスに含まれることを保証するため、操作ガイダンスをチェックしなければならない (shall)。

評価者は、TLS のテストを目的とするアプリケーションを書くか、または ST 作成者が提供するかしなければならない (shall)。評価者は、以下のテストについても実行しなければならない (shall) :

テスト 1 : 評価者は、要件で特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない (shall)。本接続は、上位プロトコルの確立の一部として、例えば EAP セションの一部として、確立されてもよい。テストの意図を満たすために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 であり、256 ビット AES ではないこと) を判別するために暗号化されたトラフィックの特徴を検査する必要はない。

テスト 2 : 評価者は、extendedKeyUsage フィールドにサーバ認証目的が含まれるサーバ証明書を持ったサーバを用いて接続の確立を試行し、接続が確立されることを検証しなければならない (shall)。次に評価者は、extendedKeyUsage フィールドにサーバ認証目的が含まれ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、サーバ選択の暗号スイートと一致しないサーバ証明書を TLS 接続において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、サーバの証明書ハンドシェイクメッセージ受信後、TOE が接続を切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、トラフィックに以下の改変を行わなければならない (shall) :

- ServerHello においてサーバにより選択された TLS バージョンを、非サポートの 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) に改変し、クライアントが接続を拒否することを検証する。
- ServerHello ハンドシェイクメッセージにおけるサーバのノンスの少なくとも 1 バイトを改変して、ServerKeyExchange ハンドシェイクメッセージをクライアントが拒否すること (DHE または ECDHE 暗号スイートの場合) あるいはクライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。
- ServerHello ハンドシェイクメッセージにおけるのサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージに存在しない暗号スイートに改変する。評価者は、ServerHello 受信後に、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) 。
- (条件付き) ECDHE または DHE 暗号スイートがサポートされた場合、サーバの Key Exchange ハンドシェイクメッセージにおける署名ブロックを改変して、ServerKeyExchange 受信後に、クライアントが接続を拒否することを検証する。
- Server Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検

証する。

- サーバが ChangeCipherSpec メッセージを発行した後、サーバから文字化けしたメッセージを送信し、クライアントが接続を拒否することを検証する。

FCS_TLSC_EXT.2.2 TSF は、提示された識別子が RFC 6125 に従って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)。

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) により、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) により、またはアプリケーション(例えば、API のパラメタ) により確立される。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、クライアントは受け入れ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) フィールドのコモン名 (Common Name) 及び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) 等を確立する。クライアントは、次にすべての受け入れ可能な参照識別子の本リストを、TLS サーバの証明書における提示された識別子と比較する。

推奨される検証方法は、DNS 名、URI 名、またはサービス名を用いたサブジェクトの別名 (Subject Alternative Name) である。コモン名を用いた検証は、バックワード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(Subject Alternative Name) 中の IP アドレス使用のサポートは、ベストプラクティスに反するため推奨されないが、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 (例えばコモン名、DNS 名、URI 名、サービス名、またはその他のアプリケーション特有のサブジェクトの別名 (Subject Alternative Name)) 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)。評価者はこの記述に、TOE によって Certificate Pinning がサポートされるか、または利用されるかどうか、及びその方法が特定されていることを保証しなければならない (shall)。

評価者は、TLS における証明書有効性確認の目的に使用さ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)。特に、AGD ガイダンスには参照識別子を設定するためアプリケーションによって利用される API が記述されるべきである (should)。

評価者は、AGD ガイダンスに従って参照識別子を設定し、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、参照識別子と一致する識別子をサブジェクトの別名(Subject Alternative Name) (SAN) にもコモン名 (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、参照識別子と一致する CN を含み、SAN 拡張を含むが、参照識別子と一致する識別子を SAN に含まないサーバ証明書を提示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、参照識別子と一致する CN を含み、SAN 拡張を含まないサーバ証明書を提示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、参照識別子と一致しない CN を含むが、SAN と一致する識別子を含むサーバ証明書を提示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す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) :

- 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)。
- 評価者は、左端のラベル中にワイルドカードを含むがパブリックなサフィックスに先立たない (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)。
- 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 された証明書と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.2.3 TSF は、ピア証明書が無効である場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注釈：有効性は識別子の検証、認証パス、有効期限、及び RFC 5280 に従う失効状態によって判断される。証明書の有効性は FIA_X509_EXT.1 用に実行されるテストに従い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、非 HTTPS の TLS 接続に対処する。

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、有効な認証パスのない証明書を使用すると、その機能が失敗することを実証しなければならない (shall)。管理ガイダンスを利用して、評価者は、その際、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なければならず、その機能が成功することを実証しなければならない (shall)。評価者は、次にこれらの証明書のうち 1 つを削除し、その機能が失敗することを示さなければならない (shall)。

FCS_TLSC_EXT.2.4 TSF は、X.509v3 証明書を用いる相互認証をサポートしなければならない (shall)。

適用上の注釈：TLS での X.509v3 証明書の使用は、FIA_X509_EXT.2.1 で対処される。本要件は、クライアントが TLS 相互認証を行うために TLS サーバへ証明書を提示できなければならない (must) ことが、この証明書の使用に含まれなければならない (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 により要求される TSS 記述に、TLS 相互認証のためのクライアント証明書の使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、以下のテストについても実行しなければならない (shall)：

*テスト 1：*評価者は、トラフィックに以下の改変を行わなければならない (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における CA フィールドの 1 バイトを改変する。改変された CA フィールドは、クライアント証明書に署名するために使用された 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)。

5.3 クラス：利用者データ保護 (FDP)

5.3.1 アクセス制御 (FDP_ACF)

FDP_ACF_EXT.1	拡張：セキュリティアクセス制御

FDP_ACF_EXT.1.1 TSF は、あるアプリケーションからアクセス可能であるようなシステムサービスを制限するメカニズムを提供しなければならない (shall)。

適用上の注釈：本要件が適用されるシステムサービスの例には、以下が含まれる。

- カメラとマイクロフォン入力デバイスからのデータを取得する
- 現在の GPS 位置情報を取得する
- システムワイドなクレデンシャル保存からのクレデンシャルを読み出す
- 連絡先リスト／アドレス帳を読み出す
- 保存された写真を読み出す
- テキストメッセージを読み出す
- 電子メールを読み出す
- デバイス ID 情報を読み出す
- ネットワークアクセスを取得する

保証アクティビティ：

評価者は、アプリケーションによる利用が可能なシステムサービスがすべて TSS に列挙されていることを保証しなければならない (shall)。評価者は、アプリケーションがこれらのシステムサービスとインタフェースする方法、及びこれらのシステムサービスが TSF により保護される手段についても TSS に記述されていることを保証しなければならない (shall)。

TSS は、以下のどのカテゴリにそれぞれのシステムサービスが分類されるかを記述しなければならない (shall)：

1) アクセスが許可されるアプリケーションなし
2) 特権アプリケーションがアクセスを許可される
3) 利用者の権限付与によりアプリケーションがアクセスを許可される
4) すべてのアプリケーションがアクセスを許可される

特権アプリケーションには、TSF 開発者により開発された任意のアプリケーションが含まれる。TSS は、サードパーティのアプリケーションへ特権が付与される方法を記述しなければならない (shall)。特権アプリケーションの両方の種別について、TSS は、特権がいつどのように検証されるか、及び TSF が特権のないアプリケーションがそれらのサービスへのアクセスを防止する方法を記述しなければならない (shall)。

利用者がアクセスを承諾してもよい任意のアプリケーションについて、評価者は、そのアプリケーションがインストールされる時または実行時に、利用者が認証を求めるプロンプト表示されるかどうかを TSS が識別していることを保証しなければならない (shall)。評価者は、アプリケーションがシステムサービスへアクセスするのを制限するための指示が利用者操作ガイダンスに含まれていることを保証しなければならない (shall)。

保証アクティビティの注釈：以下のテストは、消費者向けモバイルデバイス製品には通常

含まれないツールを評価者へ提供するようなテストプラットフォームへのアクセスをベンダが提供することが必要とされる。

評価者は、以下のテストを目的とするアプリケーションを書かくか、または、開発者がそのようなアプリケーションを提供しなければならない (shall)。

テスト1 : アプリケーションがアクセスを許可されることがないようなシステムサービスのそれぞれについて、評価者はテストアプリケーションによってシステムサービスへのアクセスを試行し、そのアプリケーションがシステムサービスへアクセスできないことを検証しなければならない (shall)。

テスト2 : 特権を持つアプリケーションのみがアクセスを許可されるようなシステムサービスのそれぞれについて、評価者は特権を持たないアプリケーションによってシステムサービスへのアクセスを試行し、そのアプリケーションがシステムサービスへアクセスできないことを検証しなければならない (shall)。評価者は、特権を持つアプリケーションによってシステムサービスへのアクセスを試行し、そのアプリケーションがシステムサービスへアクセスできることを検証しなければならない (shall)。

テスト3 : 利用者がアクセスを得るようなシステムサービスのそれぞれについて、評価者はテストアプリケーションによってシステムサービスへのアクセスを試行しなければならない (shall)。評価者は、そのようなアクセスをシステムがブロックするか、または利用者の権限付与を求めるプロンプトを表示するかのどちらかであることを保証しなければならない (shall)。利用者の権限付与を求めるプロンプト表示はランタイム時またはインストール時のどちらで行われてもよいが、TSS に記述されたふるまいと一貫しているべきである (should)。

テスト4 : すべてのアプリケーションによってアクセス可能であるとして TSS に列挙されたシステムサービスのそれぞれについて、評価者はアプリケーションがシステムサービスへアクセスできることをテストしなければならない (shall)。

FDP_ACF_EXT.1.2 TSF は、 [選択 : *アプリケーションプロセス*、*アプリケーションプロセスのグループ*] が、他の [選択 : *アプリケーションプロセス*、*アプリケーションプロセスのグループ*] によって保存された [選択 : *すべての*、*プライベートな*] データへアクセスすることを防止するアクセス制御ポリシーを提供しなければならない (shall)。例外として、[選択 : *利用者*、*管理者*、*共通アプリケーション開発者*]による共有のための明示的な場合のみ権限付与されることがある。

適用上の注釈 : アプリケーションプロセスのグループは、エンタープライズ、管理された、作業環境、個人、管理されていない、または個人環境のいずれかに特定することができる。プライベートなデータは、それを書き込んだアプリケーションによってのみアクセス可能なデータと定義される。プライベートなデータは、アプリケーションが設計によって共有ストレージ領域へ書き込み可能なデータとは区別される。

保証アクティビティ :

評価者は、どのデータ共有がアプリケーション間で許可されるか、どのデータ共有が許可されないか、及び不許可共有がどのように防止されるかについて記述されていることを検証するため、TSS を検査しなければならない (shall)。

テスト : 評価者は、2 つのアプリケーションを書くか、または開発者がそれらを提供するかしなければならない、ひとつは一意の文字列を含むデータを保存し、他方がそのデータへのアクセスを試行するものである(shall)。「アプリケーションのグループ」が選択された場合、2 つのアプリケーションは異なるグループに配置されなければならない (shall)。「プラ

イベートなデータ」が選択される場合、アプリケーションは指定された共有ストレージ領域へ書き込んではならない (shall not)。評価者は、保存された一意の文字列へ 2 番目のアプリケーションがアクセスできないことを検証しなければならない (shall)。評価者は、利用者、または管理者として、または最初のアプリケーションとの共通アプリケーション開発者による 3 番目のアプリケーションを用いることのいずれかによってアクセスを得て、そのアプリケーションが保存された一意の文字列へアクセスできることを検証しなければならない (shall)。

5.3.2 保存データの保護 (FDP_DAR)

FDP_DAR_EXT.1	拡張：保護データの暗号化

FDP_DAR_EXT.1.1 暗号化は、すべての保護データを網羅しなければならない (shall)。

適用上の注釈：1.2「用語集」に定義されるように、保護データはすべての非 TSF データであり、すべての利用者またはエンタープライズデータを含む。

FDP_DAR_EXT.1.2 暗号化は、[選択：*XTS*、*CBC*、*GCM*] モードの AES で鍵長 [選択：*128*、*256*] ビットにより、DEK を用いて実行されなければならない (shall)。

適用上の注釈：256 ビットの鍵長の使用は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

評価者は、どのデータが DAR 実装によって保護されるか、そしてどのデータが TSF データとみなされるかを ST の TSS セクションが示していることを検証しなければならない (shall)。評価者は、このデータがすべての保護データを含むことを保証しなければならない (shall)。

評価者は、設定の記述及び DAR 保護の利用が利用者に対して認証クレデンシャルの設定及び提供を越えたいかなるアクションも行うことを要求しないことを決定するため、AGD ガイダンスをレビューしなければならない (shall)。 評価者は、設定が利用者に対してファイルごとに暗号化を識別することを要求しないことを決定するため、AGD ガイダンスについてもレビューしなければならない (shall)。

保証アクティビティの注釈：以下のテストは、消費者向けモバイルデバイス製品では通常見られないようなツールを提供するテストプラットフォームへのアクセスを評価者に提供するよう開発者に要求する。

*テスト 1:*評価者は、AGD ガイダンスに従って暗号化を有効化しなければならない (shall)。評価者は、ファイルの作成またはアプリケーションの使用のいずれかにより、利用者データ (非システムデータ) を作成しなければならない (shall)。 評価者は、FIA_UAU_EXT.1 のテスト 1 と組み合わせて、製品の電源が切られる際に本データが暗号化されていることを検証するため、開発者により提供されるツールを利用しなければならない (shall)。

5.3.3 サブセット情報フロー制御—VPN (FDP_IFC)

FDP_IFC_EXT.1	拡張：サブセット情報フロー制御

FDP_IFC_EXT.1.1 TSF は、 [選択：*すべての IP トラフィック (VPN 接続を確立するために要求される IP トラフィックを除く) が IPsec VPN クライアントを流れることを可能とする VPN クライアントへのインタフェースを提供; すべての IP トラフィック (VPN 接続を確立するために要求される IP トラフィックを除く) が IPsec VPN クライアントを流れることを有効化*] しなければならない (shall)。

適用上の注釈：典型的には、VPN 接続を確立するために要求されるトラフィックは「制御プレーン」トラフィックと呼ばれる； 一方、IPsec VPN によって保護される IP トラフィックは「データプレーン」トラフィックと呼ばれる。すべての「データプレーン」トラフィックは VPN 接続を介して流れなければならず (must)、VPN はスプリットトンネルを行ってはならない (must not)。(訳注：VPN Tunnel。どのデータを VPN トンネルに通すかを管理者が制御すること)

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

ST 作成者は、TSF がネイティブな VPN クライアントを提供する場合には 2 番目のオプションを選択しなければならない (IPsec が FTP_ITC_EXT.1 で選択されている場合) (shall)。ネイティブな VPN クライアントが検証されている場合、ST 作成者は VPN クライアントのプロテクションプロファイルから FDP_IFC_EXT も含めなければならない (FTP_ITC_EXT.1 において IPsec が選択され、TSF が「IPsec 仮想プライベートネットワーク (VPN) クライアントのプロテクションプロファイル」に適合した認証を受けている場合) (shall)。

将来的には、本要件は、現在の要件 (IPsec 高信頼チャネルが有効化される時、TSF からのすべてのトラフィックがそのチャネルを経由してルーティングされることを要求している) と TSF による任意の通信を許可する IPsec 高信頼チャネルの確立を実施する選択肢を持つことを区別させるかもしれない。

保証アクティビティ：

評価者は、VPN クライアントが有効化される時に TSF 上のプロセスを通る IP トラフィックのルーティングが ST の TSS セクションに記述されていることを検証しなければならない (shall)。 評価者は、どのトラフィックが VPN を通過せず、どのトラフィックが通過するのかについて、及び ST 作成者によって VPN 接続の確立に必要であると識別したトラフィックのみ (IKE トラフィック及びおそらくは HTTPS または DNS トラフィック) が VPN プロトコル (IPsec) によりカプセル化されないような設定が各ベースバンドプロトコルについて存在することについて、記述に示されていることを保証しなければならない (shall)。評価者は、任意のサポートされたベースバンドプロトコル (例えば WiFi または LTE) を用いた際の IP トラフィックのルーティングにおける何らかの違いについて TSS セクション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、以下の選択肢の 1 つ (または複数) が、文書によって対処されていることを検証しなければならない (shall)：

- 上記の記述には、VPN クライアントが有効化された場合、すべての設定がすべてのデータプレーントラフィックを VPN クライアントによって確立されたトンネルインタフェースを介してルーティングすることが示されている。
- AGD ガイダンスに、利用者及び／または管理者が本要件を満たすように TSF を設定可能な方法が記述されている。
- API 文書は、VPN クライアントがこのルーティングの指定を許可するセキュリティ機能を含んでいる。

*テスト 1：*ST 作成者は、WiFi と携帯電話プロトコルとの間のルーティングに何らかの違いを識別している場合、評価者は識別された携帯電話プロトコルの 1 つを実装する基地局を

用いて本テストを繰り返さなければならない (shall)。

ステップ 1 - 評価者は、AGD ガイダンスに記述された WiFi 設定を有効化しなければならない (FTP_ITC_EXT.1 による要求のとおり) (shall)。 評価者は、無線アクセスポイントとインターネット接続されたネットワークの間でパケットスニフィングツールを使用しなければならない (shall)。 評価者は、スニフィングツールを起動し、ウェブサイトのナビゲーション、提供されたアプリケーションの使用、及び他のインターネット資源のアクセス等、デバイスを用いたアクションを行わなければならない (shall)。 評価者は、これらのアクションにより生成されたトラフィックをスニフィングツールがキャプチャし、スニフィングツールを終了し、セションデータを保存することを検証しなければならない (shall)。

ステップ 2 - 評価者は、本要件で特定されたルーティングをサポートするに IPsec VPN クライアントを設定しなければらず、必要な場合、デバイスが AGD ガイダンスに記述されるとおり特定されたルーティングを行うように設定しなければならない (shall)。 評価者は、スニフィングツールを起動し、VPN 接続を確立し、そして最初のステップで実行したとおりデバイスを用いて同じアクションを実行しなければならない (shall)。 評価者は、これらのアクションによって生成されたトラフィックをスニフィングツールがキャプチャしていることを検証し、スニフィングツールを終了し、セションデータを保存しなければならない (shall)。

ステップ 3 - 評価者は、すべてのデータプレーントラフィックが IPsec によってカプセル化されていることを検証するため、ステップ 1 及びステップ 2 の両方からのトラフィックを検査しなければならない(shall)。 評価者は、ステップ 2 でキャプチャされた TOE からゲートウェイへのカプセル化されたパケット中に存在する Security Parameter Index (SPI) 値を検査しなければならず (shall)、この値が VPN を通過するトラフィックを生成するために使用されたすべてのアクションで同じであることを検証しなければならない (shall)。ゲートウェイから TOE へのパケットの SPI 値は、TOE からゲートウェイへのパケットの SPI 値と異なっていることが期待されていることに注意されたい。 評価者は、IPsec トンネル外の携帯電話ベースバンド上の IP トラフィックが、ベースバンドプロセッサから発出される可能性があることをよく認識していなければならず (shall)、また任意の特定されたトラフィックがアプリケーションプロセッサから発出されないことを製造事業者と共に検証しなければならない (shall)。

ステップ 4 - 評価者は、TOE からローカルな無線ネットワーク上の別のデバイスの IP アドレスへの ICMP echo を実行しなければならず (shall)、また、一切のパケットが送信されないことをスニフィングツール使用により検証しなければならない (shall)。 評価者は、ローカルな無線ネットワークからのものを含めて、VPN トンネルの外へのパケットパケットの送信を試行しなければならず(すなわち、VPN ゲートウェイを通過しない) (shall)、そして TOE がそれらを廃棄することを検証しなければならない (shall)。

5.3.4 証明書データストレージ (FDP_STG)

FDP_STG_EXT.1	**拡張：利用者データストレージ**

FDP_STG_EXT.1.1 TSF は、トラストアンカーデータベース用の保護されたストレージを提供しなければならない (shall)。

保証アクティビティ：

評価者は、本 PP の要件を満たすために使われる証明書を含むように実装されたトラストアンカーデータベースについて TSS に記述されていることを保証しなければならない (shall)。本記述は、証明書がストレージへロードされる方法と、FMT_SMF_EXT.1 及び FMT_MOF_EXT.1.1 で確立されたアクセス権限に従ってストレージが不許可アクセスから

保護される方法 (例えば、unix パーミッション) に関する情報を含まなければならない (shall)。

5.3.5 TSF 間利用者データ保護チャネル (FDP_UPC)

FDP_UPC_EXT.1	拡張：TSF 間利用者データ転送保護

FDP_UPC_EXT.1.1 TSF は、他の通信パスとは論理的に異なり、端点の保証された識別を提供し、チェネルデータを暴露から保護し、チャネルデータの改変を検知するような、非 TSF アプリケーションと別の IT 製品との間の通信チャネルを提供するため、TLS、HTTPS、Bluetooth BR/EDR、及び [選択：*DTLS*、*Bluetooth LE*、*その他のプロトコルなし*] を用いて、TOE 上で動作している非 TSF アプリケーション用の手段を提供する。

適用上の注釈：本要件の意図は、選択されたプロトコルのひとつが、必ずしも企業インフラの一部ではない遠端サービスへの接続用のデバイス上で動作する利用者アプリケーションにより利用可能であることである。すべての TSF 通信 (デバイスからゲートウェイへの通信を意味する) が当該要件に示されるプロトコルを用いて保護されることを FTP_ITC_EXT が要求するため、本コンポーネントにより要求されるプロトコルは FTP_ITC_EXT で列挙されたものの「最上位に」掲載することに注意すべきである (should)。

いくつかのアプリケーションは TSF の一部であり、TSF アプリケーションが FTP_ITC_EXT.1 の最初の選択でのプロトコルのうち少なくとも 1 つによって保護されることを FTP_ITC_EXT が要求していることにも注意すべきである (should)。特定されたサービスが提供されている限り、本要件 (非 TSF アプリ用) と FTP_ITC_EXT (TSF アプリ用) の両方を満たすため、あるプロトコルの 2 つの異なった実装、または 2 つの異なるプロトコルを有することは必須ではない。

ST 作成者は、非 TSF アプリ用として、どの高信頼チャネルプロトコルがモバイルデバイスによって実装されているのかを列挙しなければならない (shall)。 ST 作成者が IPsec を選択する場合、TSF は「IPsec 仮想プライベートネットワーク (VPN) クライアントのプロテクションプロファイル」に適合して認証されなければならない (shall)。附属書 B には、その他のオプションの高信頼チャネルプロトコルのそれぞれを実装するための要件が含まれている。ST 作成者は、**FDP_UPC_EXT.1** で選択された高信頼チャネルプロトコル用のセキュリティ機能要件を ST の本体に含めなければならない (must)。

FDP_UPC_EXT.1.2 TSF は、非 TSF アプリケーションが高信頼チャネルを介して通信を開始することを許可しなければならない (shall)。

保証アクティビティ：

評価者は、セクション 6.2.1 に従って提供される API 文書が、これらの要件に記述されるセキュリティ機能 (保護チャネル) を含むことを検証しなければならず、かつ本要件をサポートするために実装された API が、適切な設定／パラメタが含むので、本コンポーネントにより要求されるように通信の両端点の相互識別を保証するために必要な情報の提供と取得の両方をアプリケーションに可能であることを検証しなければならない (shall)。 評価者が書くか、または、開発者が TSF による保護チャネルサービスを要求するアプリケーションへのアクセスを提供するかしなければならない (shall)。評価者は、保護チャネルから得られた結果が API 文書に従って期待される結果と一致することを検証しなければならない (shall)。本アプリケーションは、プロトコル要件の保護チャネル保証アクティビティを検証する補助として用いてもよい。

評価者は、TSS で列挙されたすべてのプロトコルが特定され ST に要件として含まれていることが記述されていることを決定するため、TSS を検査しなければならない (shall)。評価

者は、アプリケーションによって利用されるために選択された 1 つまたは複数のプロトコルを設定するために必要な指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。評価者は、以下のテストについても実行しなければならない (shall) :

テスト 1 : 評価者は、操作ガイダンスに記述されたように接続を設定し、通信が成功することを保証するとともに、アプリケーションが要件で特定された各プロトコルを用いて外部 IT エンティティとの通信を開始できることを保証しなければならない (shall)。

テスト 2 : 評価者は、許可された IT エンティティとの各通信チャネルについて、チャネルデータが平文では送信されないことを保証しなければならない (shall)。

5.4 クラス : 識別と認証 (FIA)

5.4.1 認証失敗 (FIA_AFL)

FIA_AFL_EXT.1	認証失敗時の取り扱い

FIA_AFL_EXT.1.1 TSF は、当該利用者による最後の認証の成功に関連する [割付 : *受容可能な値の範囲*] 以内の設定可能な正の整数回の認証試行の不成功がいつ発生したがを検出しなければならない (shall)。

適用上の注釈 : 正の整数は、FMT_SMF_EXT.1.1 の機能 2.c に従って設定される。TOE が複数のパスワード認証ファクタインタフェース (例えば、DAR 復号インタフェース、画面ロックインタフェース、予備ブートモードインタフェース) を実装する場合、本コンポーネントは利用可能なすべてのインタフェースに適用される。

FIA_AFL_EXT.1.2 認証試行の不成功が定義された回数を超過したとき、TSF はすべての保護データのワイプを行わなければならない (shall)。

適用上の注釈 : ワイプは、FCS_CKM_EXT.5 に従って行われる。

FIA_AFL_EXT.1.3 TSF は、電源を切る際に、発生した認証試行の不成功の回数を保持しなければならない (shall)。

適用上の注釈 : TOE は、利用者がデバイスへアクセスできるようになる前のブートシーケンス中で他のパスワード認証ファクタインタフェースに先立つパスワード認証ファクタインタフェースを実装してもよい (例えば、画面ロックインタフェースに先立つボリューム DAR 復号インタフェース)。この状況では、利用者が 2 番目のインタフェースへアクセスするには最初のインタフェースへの認証を成功させなければならない (must) ため、2 番目のインタフェースについて認証試行の不成功の回数が保持される必要はない。

保証アクティビティ :

評価者は、各パスワード認証ファクタインタフェースについて利用者ごとに最後の認証の成功以降の認証試行不成功の回数に対応した値が保持されていることが、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、TOE が電源オフの際にこの値が保持されるかどうか、及びどのように保持されるかについてもこの記述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、値が保持されていない場合、そのインタフェースが値を保持するブートシーケンス中の別のインタフェースの後にあることを保証しなければならない (shall)。

評価者は、認証試行の不成功回数の上限を管理者が設定する方法が AGD ガイダンス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、利用可能な認証ファクタインタフェース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、認証試行の不成功回数の上限について AGD ガイダンスに従ってデバイスを設定しなければならない (shall)。 評価者は、ロック状態に入り、ワイプが発生するまで不許可パスワードを入力しなければならない (shall)。 評価者は、パスワードの入力回数が設定された上限一致していること、かつワイプが実行されることを検証しなければならない (shall)。

テスト 2 : 評価者はテスト 1 を繰り返さなければならない (shall) が、認証試行の不成功のたびに TOE の電源をオフにしなければならない (可能であれば、バッテリーを取り外すことによって) (shall)。 評価者は、パスワード入力の合計回数が設定された上限と一致していること、かつワイプが実行されることを検証しなければならない (shall)。もしくは、認証失敗の回数がテスト対象インタフェースについて保持されていない場合、評価者は認証試行の不成功のたびに TOE をブートする際にテスト対象インタフェースの前に他の認証ファクタインタフェースが提示されることを検証しなければならない (shall)。

5.4.2 Bluetooth の許可と認証 (FIA_BLT)

FIA_BLT_EXT.1	**拡張：Bluetooth 利用者許可**

FIA_BLT_EXT.1.1 TSF は、リモート Bluetooth デバイスとのペアリング前に、明示的な利用者の許可を要求しなければならない (shall)。

適用上の注釈：利用者の許可には、リモートデバイス名の確認、リモートデバイスへ接続する意図の表明、及び関連するペアリング情報 (例えば PIN、数値コード、または「はい／いいえ」の応答) の入力などの明示的アクションが含まれる。 利用者は、ボンディングが行われない場合であっても、すべてのペアリング試行を明示的に許可しなければならない (must have to)。

明示的な利用者のアクションがペアリングを許可するためには要求されなければならない (must) ので、ペアリングプロセス中にアプリケーションがプログラム的にペアリング情報 (例えば PIN、数値コード、あるいは「はい／いいえ」の応答) を入力することが可能であってはならない (must not)。プログラム的な許可を行う公開 API が存在しないことでは、本要件を満たすには不十分である；隠蔽されたまたはプライベートな API も同様に存在してはならない (must)。

保証アクティビティ：

評価者は、いつ利用者の許可が Bluetooth ペアリングに必要とされるかの記述が TSS に含まれていること、そして本記述が、Bluetooth 高信頼チャネルのアプリケーションの利用及び一時的な (ボンディングされない) 接続が形成される状況を含め、すべての Bluetooth ペアリングに手入力による明示的な利用者の許可を義務付けていることを保証するため、TSS を検査しなければならない (shall)。 評価者は、セクション 6.2.1 に従って提供される API 文書を検査しなければならず、ペアリング中の利用者の手入力をバイパスすることを意図したペアリング情報 (例えば PIN、数値コード、あるいは「はい／いいえ」の応答) をプログラム的に入力するためのいかなる API もこの API 文書に含まれていないことを検証しなければならない (shall)。

評価者は、これらの利用者許可画面が明確に識別され、Bluetooth ペアリングを許可するための指示が与えられていることを検証するため、AGD ガイダンスを検査しなければならない (shall)。

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、以下のステップを行わなければならない (shall) :

ステップ 1 - 中間者保護やボンディングを一切要求せず、かつ NoInputNoOutput 入出力 (IO) capability を有すると主張するようなリモート Bluetooth デバイスからの TOE とのペアリングを開始する。(そのようなデバイスは、ペアリング中に TOE がサポートする最低レベルの利用者対話を提示する TOE からふるまいを起こそうと試行するであろう。) ステップ 2 - TOE が、いかなる Bluetooth ペアリングも利用者からの明示的な許可なしでは許可しないことを検証する (例えば、利用者はプロンプトに対して最低限「はい」または「許可」と答えなければならない (must have to))。

5.4.3 ポートアクセスエンティティの認証 (FIA_PAE)

FIA_PAE_EXT.1	拡張：PAE 認証

FIA_PAE_EXT.1 TSF は、「サプリカント」役割のポートアクセスエンティティ (PAE) について、IEEE Standard 802.1X に適合しなければならない (shall)。

適用上の注釈：本要件は、802.1X 認証交換におけるサプリカントとしての TSF の役割を網羅する。この交換が成功して完了した場合、TSF は EAP-TLS (またはその他の適切な EAP の交換) の結果として PMK を導出し、無線アクセスシステム (認証子) との 4 ウェイハンドシェイクを行って 802.11 通信を開始する。

先ほど示した通り、交換の間には少なくとも 2 つの通信経路が存在する。ひとつは無線アクセスシステムとのもの、もうひとつは無線アクセスシステムを中継として用いる認証サーバとのものである。TSF は、802.1X-2010 に特定されるように無線アクセスシステムと LAN 上の EAP (EAPOL) 接続を確立する。TSF と認証サーバは、EAP-TLS セション (RFC 5216) を確立する。

802.1X 認証を行うポイントは、ネットワークへのアクセスを取得することである (認証が成功し、すべての 802.11 ネゴシエーションが成功して行われたことを前提として)。802.1X の言葉で言えば、無線アクセスシステムによって維持管理される「コントロールされたポート」へのアクセスを TSF が得ることを意味する。

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、TOE がテストネットワークへのアクセスを有さないことを実証しなければならない (shall)。無線アクセスシステムを介した認証サーバとの認証成功の後、評価者は TOE がテストネットワークへのアクセスを有することを実証しなければならない (shall)。
- *テスト 2：*評価者は、TOE がテストネットワークへのアクセスを有さないことを実証しなければならない (shall)。評価者は、EAP-TLS ネゴシエーションが失敗するような、無効なクライアント証明書を用いた認証を試行しなければならない (shall)。この結果として、TOE は依然としてテストネットワークへアクセスできない状態であるべきである (should)。
- *テスト 3：*評価者は、TOE がテストネットワークへのアクセスを有さないことを実証しなければならない (shall)。評価者は、EAP-TLS ネゴシエーションが失敗するような、無効な認証サーバ証明書を用いた認証を試行しなければならない (shall)。この結果として、TOE は依然としてテストネットワークへアクセスできない状態であるべきである (should)。

5.4.4 パスワード管理 (FIA_PMG)

FIA_PMG_EXT.1	拡張：パスワード管理

FIA_PMG_EXT.1.1 TSF は、パスワード認証ファクタについて以下をサポートしなければならない (shall)：

1. パスワードは、 [選択：*大文字及び小文字、 [割付：少なくとも 52 文字の文字セット*]]、数字、ならびに特殊文字： [選択：*"!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("、")"、割付：その他の文字*] の任意の組み合わせによって構成できなければならない (shall)；
2. [割付：*14 以上の整数*] 文字までの長さのパスワードがサポートされなければならない (shall)。

適用上の注釈：一部の会社の方針では 14 文字またはそれ以上のパスワードが要求される一方で、DAR 保護及び鍵ストレージ保護への REK の利用及び耐破壊性 (anti-hammer) 要件 (FIA_TRT_EXT.1) は、はるかに短く複雑性の少ないパスワードを使って物理的アクセスを行う攻撃者の脅威に対抗する。

ST 作成者は、文字セット：基本ラテン文字の大文字及び小文字、または少なくとも 52 文字を含む別の割付けられたのいずれかを選択する。 割付けられた文字セットは、明確に定義されたもの：国際エンコーディング標準 (Unicode など) に従うか、または ST 作成者により割付で定義されたもののいずれか、でなければならない (must)。 ST 作成者は、TOE によってサポートされる特殊文字についても選択する；それらは割付を用いてサポートされる追加の特殊文字をオプションとして列挙できる。

保証アクティビティ：

評価者は、操作ガイダンスが強いパスワードの生成に関するセキュリティ管理者へのガイダンスを提供していること、及び最小パスワード長の設定に関する指示を提供していることを決定するため、操作ガイダンスを検査しなければならない (shall)。評価者は、以下のテストについても実行しなければならない (shall)。これらのテストの 1 つまたは複数が、単一のテストケースで実施可能であることに注意されたい。

*テスト 1：*評価者は、要件を満たすパスワードか、何らかの形で要件を満たすことのできないパスワードの、いずれかを作成しなければならない (shall)。 パスワードのそれぞれについて、評価者は TOE がそのパスワードをサポートすることを検証しなければならない (shall)。 評価者はパスワードのすべてのあり得る組み合わせをテストすることは要求されない (または実現不可能か) が、評価者は要件に列挙されたすべての文字、ルールの特性、及び最小の長さがサポートされていることを保証しなければならず、テスト用に選択されたそれらの文字のサブセットを正当化しなければならない (shall)。

5.4.5 認証の抑制 (FIA_TRT)

FIA_TRT_EXT.1	**拡張：認証の抑制**

FIA_TRT_EXT.1.1 TSF は、 [選択：*外部ポートを介した認証を防止する、不許可認証試行のたびに遅延時間を実施する*] ことによって、自動化された利用者の認証試行を制限しなければならない (shall)。最小遅延時間は、500 ミリ秒につき試行可能な回数が 10 回以下となるようなものでなければならない (shall)。

適用上の注釈：本要件における利用者認証試行は、パスワード認証ファクタを推測する試行である。開発者は、不均等または均等な遅延時間を用いることによって、要件における遅延時間のタイミングを実装することができる。

本要件で特定される最小遅延時間は、パスワードの総当たり攻撃に対する防御を提供する：例えば、ランダムに生成された 4 文字のパスワードを見つけ出すために期待時間 (63

文字の最小文字セットを利用して) は 4 日半であり、5 文字の場合その時間は 287 日を超える。

保証アクティビティ：

評価者は、認証試行が自動化され得ないようにする手段が 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、TSF が (通常の利用者インタフェース以外の) 外部インタフェースを介した認証を無効化する方法、または自動化された入力を遅らせるために認証試行を遅延させる方法のいずれかについて TSS に記述されていることを保証しなければならず (shall)、また 10 回の試行に課される遅延が合計で少なくとも 500 ミリ秒となることを保証しなければならない (shall)。

5.4.6 利用者認証 (FIA_UAU)

5.4.6.1 保護された認証フィードバック

FIA_UAU.7	保護された認証フィードバック

FIA_UAU.7.1 TSF は、認証を行っている間、[***デバイスの画面上へ見えなくされたフィードバック***] だけを利用者に提供しなければならない (shall)。

適用上の注釈：TSF は、それぞれの文字を短時間 (1 秒またはそれ未満) 表示したり、パスワードのマスクを解除できる選択肢を利用者に提供したりしてもよい；しかし、パスワードはデフォルトで見えなくしなければならない (must)。

保証アクティビティ：

評価者は、パスワードの入力を見えなくする手段が 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、本要件の任意の設定が AGD ガイダンスで取り上げあられていること、そしてパスワードがデフォルトで見えなくされていることを検証しなければならない (shall)。

*テスト：*評価者は、少なくとも画面ロックでのパスワード認証ファクタを含め、デバイス上でパスワードを入力しなければならず、かつそのパスワードがデバイス上で表示されないことを検証しなければならない (shall)。

5.4.6.2 暗号操作のための認証

FIA_UAU_EXT.1	拡張：暗号操作のための認証

FIA_UAU_EXT.1.1 TSF は、起動時に、保護データ及び暗号化された DEK、KEK 及び [選択：*長期高信頼チャネル鍵材料*、*すべてのソフトウェアベースの鍵ストレージ*、*その他の鍵なし*] の復号に先立って、利用者にパスワード認証ファクタの提示を要求しなければならない (shall)。

適用上の注釈：本要件の意図は、パスワード認証ファクタを用いて利用者がデバイスへ許可される前の保護データの復号を防止することである。パスワード認証ファクタは、機微なデータ(1.2「用語集」及び附属書 D.3.3 参照)を復号するために使用される鍵を導出するためにも要求される。これにはソフトウェアベースのセキュアな鍵ストレージが含まれる。

ST 作成者は、FCS_STG_EXT.2.1 と一致する長期高信頼チャネル鍵材料またはソフトウェアベースの鍵ストレージを選択しなければならない (shall)。

保証アクティビティ：

評価者は、ST の TSS セクションに、保護データ及び鍵を復号するためのプロセスが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、このプロセスが利用者に対し

てパスワード認証ファクタの入力を要求することと、FCS_CKM_EXT.3 に従い、ソフトウェアベースのセキュアな鍵ストレージを保護するために使用される KEK、及び (オプションとして) 機微なデータのために使用される DEK(s)が FCS_STG_EXT.2 に従って導出されることを保証しなければならない (shall)。

以下のテストは､FDP_DAR_EXT.1 及び FDP_DAR_EXT.2 と組み合わせて行われてもよい。

保証アクティビティの注釈：以下のテストは、開発者がテストプラットフォームへのアクセスを評価者に対して提供することが必要であり、それにより、消費者向けモバイルデバイス製品には通常含まれないようなツールを提供する。

*テスト 1：*評価者は、保護データの暗号化を有効化しなければならず、AGD ガイダンスに従い利用者に認証を要求しなければならない (shall)。 評価者が、保護データとして取り扱われる一意の文字列を含むアプリケーションを書くか、または開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。

評価者は、デバイスを再起動し、開発者により提供されたツールを用いてアプリケーションデータの中から一意の文字列を検索し、そして一意の文字列が発見されないことを検証しなければならない (shall)。 評価者は、デバイスの全機能へアクセスするためのパスワード認証ファクタを入力し、開発者により提供されたツールを用いてアプリケーションデータの中から一意の文字列へアクセスし、そして一意の文字列が発見されることを検証しなければならない (shall)。

テスト2： [条件付き] 評価者は、AGD ガイダンスに従い利用者に認証を要求しなければならない (shall)。 評価者は、鍵をソフトウェアベースのセキュアな鍵ストレージに保存しなければならない (shall)。

評価者は、デバイスをロックし、開発者により提供されたツールを用いて保存されたデータの中の鍵へアクセスし、そして鍵の読み出しやアクセスができないことを検証しなければならない (shall)。 評価者は、デバイスの全機能へアクセスするためのパスワード認証ファクタを入力し、開発者により提供されたツールを用いて鍵へアクセスし、そして鍵の読み出しやアクセスができることを検証しなければならない (shall)。

テスト3: [条件付き] 評価者は、機微なデータの暗号化を有効化し、AGD ガイダンスに従い利用者に認証を要求しなければならない (shall)。 評価者が機微なデータとして取り扱われる一意の文字列を含むアプリケーションを書くか、または、開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。

評価者は、デバイスをロックし、開発者により提供されたツールを用いてアプリケーションデータの中の一意の文字列へのアクセスを試行し、そして一意の文字列が発見できないことを検証しなければならない (shall)。 評価者は、デバイスの全機能へアクセスするためのパスワード認証ファクタを入力し、開発者により提供されたツールを用いてアプリケーションデータの中の一意の文字列へアクセスし、そして一意の文字列が読み出せることを検証しなければならない (shall)。

5.4.6.3 認証のタイミング

FIA_UAU_EXT.2	**拡張：認証のタイミング**

FIA_UAU_EXT.2.1 TSF は、利用者が認証される前に、利用者を代行して行われる [選択：[割付：*アクションのリスト*]、*アクションなし*]を許可しなければならない (shall)。

FIA_UAU_EXT.2.2 TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に。各利用者に認証が成功することを要求しなければならない(shall)。

保証アクティビティ：

評価者は、ロック状態で不許可利用者に許可されるアクションが 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、デバイスがロック状態にある間に選択に列挙されていないアクションの実行を試行し、そのアクションが成功しないことを検証しなければならない (shall)。

5.4.6.4 再認証

FIA_UAU_EXT.3	拡張：再認証

FIA_UAU_EXT.3.1: TSF は、利用者がパスワード認証ファクタを改変する時、及びロック解除状態へ移行するための TSF 起動ロック及び利用者起動ロックの後、及び [選択 : [割付 : *その他の条件*]、*その他の条件なし*] において、正しいパスワード認証ファクタの入力を利用者に要求しなければならない (shall)。

適用上の注釈 : TSF 起動ロック及び利用者起動ロックは、FTA_SSL_EXT.1 に記述されている。

保証アクティビティ：

テスト 1 : 評価者は、AGD ガイダンスに従いパスワード認証ファクタを利用するよう TSF を設定しなければならない (shall)。 評価者は、AGD ガイダンスに従いパスワード認証ファクタを改変し、TSF がファクタの改変を許可する前にパスワード認証ファクタの入力を要求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、AGD ガイダンスに従い非アクティブ時間 (FMT_SMF_EXT.1) の後にロック状態へ移行するよう TSF を設定しなければならない (shall)。 評価者は、TSF がロックするまで待ち、そして TSF がロック解除状態へ移行する前に、パスワード認証ファクタの入力を要求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、AGD ガイダンスに従い利用者起動ロックを設定しなければならない (shall)。 評価者は、TSF をロックし、そして TSF がロック解除状態へ移行する前に、パスワード認証ファクタの入力を要求することを検証しなければならない (shall)。

5.4.7 X509 証明書 (FIA_X509)

5.4.7.1 証明書の有効性確認

FIA_X509_EXT.1	拡張：証明書の有効性確認

FIA_X509_EXT.1.1 TSF は、以下の規則に従い、証明書の有効性を確認しなければならない (shall) :

- RFC 5280 証明書有効性確認及び証明書パス検証。
- 証明書パスは、トラストアンカーデータベース中の証明書で終わらなければならない (must)。
- TSF 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り、証明書パスを検証しなければならない (shall)。
- TSF は、[選択 : *RFC 2560 で特定されるオンライン証明書状態プロトコル (OCSP)*、*RFC 5759 で特定される証明書失効リスト (CRL)*] 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)。
- TSF は、以下の規則に従い 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使用される証明書は、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 で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)。
- (条件付き) EST(訳注：Enrollment over Secure Tranport, RFC 7030)で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)。

適用上の注釈：FIA_X509_EXT.1.1 には、証明書有効性確認を行うための規則が列挙されている。ST 作成者は、OCSP か CRL のどちらを用いて失効状態が検証されるかを選択しなければならない (shall)。 FIA_X509_EXT.2 は、証明書が EAP-TLS 用に利用されることを要求する；本利用は、extendedKeyUsage 規則が検証されることが要求する。証明書は、オプションとして、システムソフトウェア及びモバイルアプリケーションの高信頼アップデート (FPT_TUD_EXT.2) 及び完全性検証 (FPT_TST_EXT.2) 用として利用してもよく、また実装されている場合は、コード署名目的 extendedKeyUsage を含んでいることが検証されなければならない (must)。

FIA_X509_EXT.1.1 は TOE プラットフォームが TLS サーバにより提示される証明書に関して特定のチェックを実行することを要求しているが、認証サーバがクライアントにより提示される証明書に関して実行しなければならない (have to) 同様のチェックも存在する；すなわち、クライアント証明書の extendedKeyUsage フィールドが "Client Authentication" を含むこと、及び鍵共有ビット (Diffie-Hellman 暗号スイートの場合) または鍵暗号化ビット (RSA 暗号スイートの場合) がセットされていること。 TOE により使用されるために取得される証明書は、企業で使用されるためのこれらの要件に適合しなければならない (have to)。 このチェックは、WLAN 高信頼チャネル用の EAP-TLS をサポートするために要求される。

EAP-TLS での WLAN 証明書の有効性確認の場合、TOE が CRL を利用して証明書失効状態を検証する時、TOE は利用可能な保存され、有効な CRL のいずれかを利用すべきである (should)。 TOE が OCSP を利用して証明書失効状態を検証する時、WLAN 高信頼チャネルを確立する前に証明書失効状態は検証できない。

FIA_X509_EXT.1.2 TSF 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、証明書を CA 証明書としてのみ取り扱わなければならない (shall)。

適用上の注釈：本要件は、TSF により使用され、処理される証明書に適用され、トラストアンカーデータベースへ追加されてもよい証明書を制限する。

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)。 評価者は、証明書パス検証アルゴリズムの記述についても TSS が提供していることを保証する。

記述されたテストは、FIA_X509_EXT.2.1 及び FIA_X509_EXT.3 の使用事例を含めて、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実行されなければならない (must)。 extendedKeyUsage 規則のテストは、それらの規則を要求する用途と組み合わせて実行される。 評価者は、少なくとも 4 つの証明書のチェインを作成しなければならない (shall)：テ

ストされるノードの証明書、2 つの中間 CA、及び自己署名されたルート CA である。

テスト 1： 評価者は、その機能 (例えばアプリケーションの検証、高信頼チャネルの設定、または高信頼ソフトウェアアップデート) で利用される証明書の検証に必要とされるトラストアンカーデータベースへの 1 つまたは複数の証明書をロードし、その機能が成功することを実証しなければならない (shall)。 評価者は、次に証明書の 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、有効期限切れの証明書の有効性確認を行い、その機能が失敗することを実証しなければならない (shall)。

テスト 3： 評価者は、CRL または OCSP のいずれかが選択されているかに応じて -失効した証明書を TOE が適切に処理できることをテストしなければならない (shall) : 両方が選択される場合、タスとはそれぞれの方法について実行されなければならない (shall)。 評価者は、ノード証明書の失効及び中間 CA 証明書の失効をテスト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 により失効されるべきである (should))。 WLAN 使用事例のテストについては、事前に保存された CRL のみが利用される。 評価者は、次に有効な証明書が使用され、証明書の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)。評価者は、次に失効された証明書 (選択において選ばれた各方法について) を利用してテストを試行し、もはや証明書が有効でない場合には有効性確認機能が失敗することを保証する。

テスト 4： 評価者は、TOE の証明書を発行する CA の証明書が basicConstraints 拡張を含まないように証明書パスを構築しなければならない (shall)。この証明書パスの検証は失敗すること。

テスト 5： 評価者は、TOE の証明書を発行する CA の証明書が basicConstraints 拡張に cA フラグがセットされないように証明書パスを構築しなければならない (shall)。この証明書パスの検証は失敗する。

テスト 6： 評価者は、TOE の証明書を発行する CA の証明書が basicConstraints 拡張に cA フラグが TRUE にセットされるように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。

テスト 7： 評価者は、証明書の最初の 8 バイト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実証しなければならない (shall)。(証明書が正しく構文解析されないこと。)

テスト 8： 評価者は、証明書の最終バイト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実証しなければならない (shall)。(証明書の署名が検証されないこと。)

テスト 9： 評価者は、証明書の公開鍵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実証しなければならない (shall)。(証明書の署名が検証されないこと。)

5.4.7.2 X509 証明書認証

FIA_X509_EXT.2	**拡張：X509 証明書認証**

FIA_X509_EXT.2.1 TSF は、EAP-TLS 交換、及び [選択 : *IPsec*、*TLS*、*HTTPS*、*DTLS*] 、及び [選択 : *システムソフトウェアアップデートのコード署名*、*モバイルアプリケーションのコード署名*、*完全性検証のためのコード署名*、*[割付 : その他の用途]*、*追加用途なし*] 用の認証をサポートするため、RFC 5280 により定義された X.509v3 証明書を利用しなければならない (shall)。

適用上の注釈： ST 作成者の選択は、FTP_ITC_EXT.1.1 の選択と一致しなければならない (shall)。 証明書は、オプションとして、システムソフトウェア (FPT_TUD_EXT.2.3) 及びモバイルアプリケーション (FPT_TUD_EXT.2.5) の高信頼アップデート、及び完全性検証 (FPT_TST_EXT.2) 用に利用してもよい。 FPT_TUD_EXT.2.5 が ST に含まれている場合、「モバイルアプリケーション用のコード署名」が選択に含まれなければならない (must)。

FIA_X509_EXT.2.2 TSF が証明書の有効性を決定するための接続を確立できない時、TSF は、 [選択：*このような場合に証明書を受け入れるかどうかの選択を管理者に許可する*、*このような場合に証明書を受け入れるかどうかの選択を利用者に許可する*、*証明書を受け入れる*、*証明書を受け入れない*] ようにしなければならない (shall)。

適用上の注釈： しばしば接続は証明書の失効状態の検討を実行するために確立されなければならない(must) – CRL をダウンロードするにせよ、OCSP を実行するにせよ。このような接続が確立できない事象 (例えば、ネットワークエラーのため) におけるふるまいを記述するために選択が利用される。TOE が FIA_X509_EXT.1 のその他の全ての規則に従い証明書が有効であると決定した場合、2 番目の選択に示されるふるまいが有効性を決定しなければならない (shall)。 FIA_X509_EXT.1 のその他の有効性確認規則のいずれかに失敗する場合、TOE はその証明書を受け入れてはならない (must not)。 ST 作成者により管理者設定または利用者設定オプションが選択される場合、ST 作成者は FMT_SMF_EXT.1 の機能 30 についても選択しなければならない (must)。

TOE は、高信頼チャネルにより異なるふるまいをしてもよい； 例えば、接続が確立されることがありそうにない WLAN の場合、証明書がその他のチャネル用に受け入れられていない場合であっても、TOE はその証明書を受け入れるかもしれない。 ST 作成者は、すべての適用可能なふるまいを選択すべきである (should)。

保証アクティビティ：

評価者は、TOE がどの証明書を利用するか選ぶ方法、及び TOE がその証明書を利用できるように運用環境を設定するための管理者ガイダンスにおける必要な指示が TSS に記述されていることを保証するため、TSS をチェックしなければならない (shall)。

評価者は、高信頼チャネルの確立で利用される証明書の有効性チェック中に接続が確立できない時の TOE のふるまいが TSS に記述されていることを確認するため、TSS を検査しなければならない (shall)。 評価者は、複数の高信頼チャネル間の区別について記述されていることを検証しなければならない(shall)。 管理者がデフォルトのアクションを特定できるという要件が存在する場合、評価者は、この設定アクションをが実行される方法についての指示が操作ガイダンスに含まれていることを保証しなければならない (shall)。

評価者は、各高信頼チャネルについて、以下のテストを実行しなければならない (shall)：

テスト： 評価者は、有効な証明書の利用には、TOE 以外の IT エンティティと通信することにより、少なくとも一部の証明書有効性確認のチェックの実行が要求されることを実証しなければならない (shall)。 評価者は、次に TOE が証明書の有効性を検証できないように環境を操作し、FIA_X509_EXT.2.2 で選択されたアクションが実行されることを観測しなければならない(shall)。 選択されたアクションが管理者により設定可能である場合、評価者は、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それらが文書化されたとおりにふるまうことを決定するため、操作ガイダンスに従わなければならない (shall)。

5.4.7.3 証明書の有効性確認要求

FIA_X509_EXT.3	拡張：証明書の有効性確認要求

FIA_X509_EXT.3.1 TSF は、アプリケーションに対して証明書有効性確認サービスを提供

しなければならない (shall)。

FIA_X509_EXT.3.2 TSF は、有効性確認の成功または失敗により、アプリケーションの要求へ対応しなければならない (shall)。

適用上の注釈： FIA_X509_EXT.1 の規則のすべてに適合するため、複数の API 呼び出しが要求されるかもしれない；このような呼び出しのすべてが、明確に文書化されるべきである (should)。

保証アクティビティ：

評価者は、本要件で記述されたセキュリティ機能 (証明書有効性確認) がセクション 6.2.1 に従って提供される API 文書に含まれることを検証しなければならない(shall)。本文書は、成功と失敗を示す結果について明確でなければならない (shall)。

評価者は、TSF による証明書有効性確認を要求するアプリケーションを書くか、または開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。評価者は、有効性確認から得られた結果が API 文書に従い期待される結果と一致することを検証しなければならない(shall)。本アプリケーションは、FDP_STG_EXT.1、FDP_ITC_EXT.1、FMT_SMF_EXT.1.1、及び FIA_X509_EXT.1 により要求されるテストに従いインポート、削除、改変、及び有効性確認が正しく実行されることを検証するために利用してもよい。(may)

5.5 クラス：セキュリティ管理 (FMT)

利用者と管理者の両方 (セクション 1.2 の用語集の定義のとおり) が TOE を管理してよい (may)。本管理者は、リモートから操作を行うことが多く、MDM エージェントを介して操作を行うモバイルデバイス管理 (MDM) の管理者であるかもしれない。

管理者は、企業によってモバイルデバイスに適用されるポリシーの設定を含めた、管理アクティビティに責任を負う。これらの管理機能群は、利用者に提供される管理機能とは異なるものとなる。利用者に提供され、管理者には提供されない管理機能群は、FMT_MOF_EXT.1.1 に列挙されている。利用者が機能の実行を制限されるようなポリシーを管理者が適用するような管理機能群は、FMT_MOF_EXT.1.2 に列挙されている。

表 1 は、以下の 3 つの要件 (FMT_MOF_EXT.1.1、FMT_MOF_EXT.1.2、FMT_SMF_EXT.1) にて本プロテクションプロファイルにより要求された管理機能群を比較している。

5.5.1 TSF における機能の管理 (FMT_MOF)

FMT_MOF_EXT.1	**拡張：セキュリティ機能のふるまいの管理**

FMT_MOF_EXT.1.1 TSF は、表 1 の列 3 の機能を実行する能力を利用者に制限しなければならない (shall)。

適用上の注釈： 3 番目の列に「M」とある機能は、本コンポーネントについて必須である；3 番目の列に「O」とある機能は、オプションであり選択してもよい；3 番目の列に「-」とある機能は該当せず、選択することはできない。ST 作成者は、利用者が実行できるようなセキュリティ管理機能のみを選択すべきである (should)。

ST 作成者は、FMT_MOF_EXT.1.1 と FMT_MOF_EXT.1.2 の両方で同一の機能を選択することはできない。

ST 作成者は、管理者が実行しないセキュリティ管理機能群を選択すべきである (should)。ST 作成者は、管理者用の API が実装されておらず利用者に限定された機能 (列 2 のとおり) を明確な区分により (インデックスとともに) 示すような表を ST において利用してもよい。ST 作成者は、選択可能なサブ機能群または列の値についての割付けられた値におけるバリ

エーションを示すために、行を繰り返すべきである (should)。

必須の機能については、選択中にないサブ機能群もまた必須であり、割付には少なくとも 1 つの割付けられた値を含まなければならない (must)。オプション機能における選択不可のサブ機能群については、選択外のすべてのサブ機能群は列挙された機能のために実装されなければならない (must)。

保証アクティビティ：

評価者は、管理者によりのみ実行される管理機能群が TSS に記述されていることを検証し、これらの管理機能群用の管理者 API が TSS に含まれないことを確認しなければならない (shall)。 本アクティビティは、FMT_SMF_EXT.1 と組み合わせて行われることになる。

FMT_MOF_EXT.1.2 TSF は、デバイスが登録され、管理者設定済みのポリシーに従う時、表 1 の列 5 の機能群を実行する能力を管理者に限定しなければならない (shall)。

適用上の注釈：デバイスが登録されている限り、企業の最小限のセキュリティ機能が実施されていることを (企業の) 管理者が保証しなければならない (must)。さらに制約的なポリシーは、利用者または管理者を代行して利用者によりいつでも適用可能である。

5 番目の列に「M」とある機能は、本コンポーネントについて必須である；5 番目の列に「O」とある機能は、オプションであり選択可能である；そして 5 番目の列に「-」とある機能は該当せず、選択することはできない。

ST 作成者は、FMT_MOF_EXT.1.1 と FMT_MOF_EXT.1.2 の両方で同一の機能を選択することはできない。

ST 作成者は、管理者が制限できるセキュリティ管理機能群を選択すべきである (should)。ST 作成者は、管理者用の API が実装されている機能群および実装されていない機能群(列 4 のとおり) を明確な区分により(インデックスとともに) 示すような表を ST において利用してもよい。ST 中に表を利用して、(列 4 にあるように) 管理者のための API を伴って実装されていない機能に明確な区分を (インデックスを伴って) 示してもよい。 さらに、ST 作成者は、利用者がアクセスまたは実行できない機能がどれかを (列 5 にあるように) 区分すべきである (should)。 ST 作成者は、選択可能なサブ機能群または列の値についての割付けられた値におけるバリエーションを示すために、行を繰り返すべきである (should)。

必須の機能については、選択中にないサブ機能群もまた必須であり、割付には少なくとも 1 つの割付けられた値を含まなければならない (must)。オプション機能における選択不可のサブ機能群については、選択外のすべてのサブ機能群は列挙された機能のために実装されなければならない (must)。

保証アクティビティ：

評価者は、利用者がその機能へのアクセス、実行、または緩和 (該当する場合) が防止されている方法と、アプリケーション／API による管理者設定の改変が防止されている方法を含めて、管理者により実行される管理機能について TSS に記述されていることを検証しなければならない(shall)。 TSS は、管理者設定済みのポリシーにより影響を受ける機能とその影響について記述される。本アクティビティは、FMT_SMF_EXT.1 と組み合わせて実行される。

テスト 1： 評価者は、モバイルデバイスへポリシーを配備するために*テスト環境*を利用しなければならない (shall)。

テスト 2： 評価者は、FMT_MOF_EXT.1.1 に定義されるように (企業の) 管理者により管理され、利用者により上書き／緩和できない、すべての管理機能群を一括して含むポリシ

ーを作成しなければならない (shall)。 評価者は、デバイスへこれらのポリシーを適用し、利用者として (設定が利用可能な場合) 及びアプリケーションとして (API が利用可能な場合) の両方について、各設定の上書き／緩和を試行し、そして TSF がこれを許可しないことを保証しなければならない (shall)。 利用者は、管理者のものよりもさらに制約的なポリシーを適用できることに注意されたい。

テスト 3： 管理者へ提供される機能群の追加的なテストは、FMT_SMF_EXT.1.1 のテストアクティビティと組み合わせて実行される。

5.5.2 管理機能の仕様 (FMT_SMF)

5.5.2.1 管理機能の仕様

FMT_SMF_EXT.1	**拡張：管理機能の仕様**

FMT_SMF_EXT.1.1 TSF は、以下の管理機能群を実行できなければならない (shall)：

管理機能 **状態マーカー：** M — 必須 O — オプション／オブジェクティブ	**FMT_SMF_EXT.1**	**FMT_MOF_EXT.1.1**	**管理者**	**FMT_MOF_EXT.1.2**
1. パスワードポリシーの設定： a. 最小のパスワード長 b. 最小のパスワード複雑性 c. 最大のパスワードライフタイム	M	-	M	M
2. セションロックのポリシー： a. 画面ロックの有効化／無効化 b. 画面ロックのタイムアウト c. 認証失敗の回数	M	-	M	M
3. VPN 保護の有効化／無効化： a. デバイス全体にわたって [選択： *b. アプリごとに (per-app basis)* *c. その他の方法なし*]	M	O	O	O
4. [割付：*無線のリスト*] の有効化／無効化	M	O	O	O
5. [割付：*オーディオまたは映像収集デバイスのリスト*] の有効化／無効化： a. デバイス全体にわたって [選択： *b. アプリごとに (per-app basis)* c. *その他の方法なし*]	M	-	M	M
6. TSF が接続できる無線ネットワーク (SSID) の特定	M	-	M	O
7. 各無線ネットワークのセキュリティポリシーの設定： a. [選択：*TSF が受容する WLAN 認証サーバ証明書から CA を特定*、*受容可能な WLAN 認証サーバ証明書の FQDN を特定*] b. セキュリティタイプ	M	-	M	O

c. 認証プロトコル d. 認証に使用されるべきクライアントのクレデンシャル				
8. ロック状態への移行	M	-	M	-
9. 保護データの TSF ワイプ	M	-	M	-
10. 以下によるアプリケーションのインストール方針の設定 [選択： *a. アプリケーションの生成元を制約*、 *b. 許可されるアプリケーションを [割付：アプリケーション特性] に基づいて特定 (アプリケーションのホワイトリスト)*、 c. *アプリケーションのインストールを拒否*]	M	-	M	M
11. セキュアな鍵ストレージへの鍵／秘密のインポート	M	O	O	-
12. セキュアな鍵ストレージにあるインポートされた鍵／秘密及び [選択：*その他の鍵／秘密なし*、 *[割付：鍵／秘密のその他のカテゴリのリスト]*] の破棄	M	O	O	-
13. トラストアンカーデータベースへの X.509v3 証明書のインポート	M	-	M	O
14. トラストアンカーデータベースにあるインポートされた X.509v3 証明書及び [選択：*その他の X.509v3 証明書なし*、 *[割付：X.509v3 証明書のその他のカテゴリのリスト]*] の削除	M	O	O	-
15. 管理への TOE の登録	M	M	O	-
16. アプリケーションの削除	M	-	M	O
17. システムソフトウェアのアップデート	M	-	M	O
18. アプリケーションのインストール	M	-	M	O
19. エンタープライズアプリケーションの削除	M	-	M	-
20. Bluetooth 高信頼チャネルの設定： a. 検出可能 (Discoverable) モードの無効化 (BR/EDR について) b. Bluetooth デバイス名の改変 [選択： *c. Bluetooth と共に使用される追加的無線技術の有効化／無効化*、 *d. アドバタイジングの有効化／無効化 (LE について)*、 *e. コネクション可能 (Connectable) モードの有効化／無効化* *f. デバイス上で利用できる Bluetooth サービスまたはプロファイルあるいはその両方の有効化／無効化*、 *g. 各ペアリングのセキュリティの最低レベルの指定*、 *h. アウトオブバンド (Out of Band) ペアリングの許可される方法の設定*、 i. *その他の Bluetooth 設定なし*]	M	O	O	O
21. 以下のロック状態での通知表示の有効化／無効化： [選択： *a. 電子メール通知*、 *b. カレンダーの予定*、 *c. 電話呼出し通知と関連付けられた連絡先*、 *d. テキストメッセージ通知*、 *e. その他のアプリケーションベースの通知*、 f. *すべての通知*]	M	O	O	O
22. [割付：*外部アクセス可能なハードウェアポートのリスト*] 上のすべてのデータシグナリングの有効化／無効化	O	O	O	O
23. [割付：*デバイスがサーバとしてふるまうプロトコルのリスト*] の有効化／無効化	O	O	O	O
24. 開発者モードの有効化／無効化	O	O	O	O

25. 保存データ保護の有効化	O	O	O	O
26. リムーバブルメディアの保存データ保護の有効化	O	O	O	O
27. ローカル利用者認証のバイパスの有効化／無効化	O	O	O	O
28. エンタープライズデータのワイプ	O	O	O	-
29. トラストアンカーデータベースにある X.509v3 証明書のアプリケーションによる [選択：*インポート*、*削除*] の承認	O	O	O	O
30. TSF が証明書の有効性を判断するための接続を確立できなかった場合に、高信頼チャネルを確立するか、または確立を許可しないかの設定	O	O	O	O
31. 携帯電話基地局への接続に使用される携帯電話プロトコルの有効化／無効化	O	O	O	O
32. TSF によって記録された監査ログの読み出し	O	O	O	-
33. アプリケーション上のデジタル署名の検証に使用される [選択：*証明書*、*公開鍵*] の設定	O	O	O	O
34. 複数のアプリケーションによる鍵／秘密の共有利用の例外の承認	O	O	O	O
35. 鍵／秘密をインポートしなかったアプリケーションによる鍵／秘密の破棄の例外の承認	O	O	O	O
36. ロック解除バナーの設定	O	-	O	O
37. 監査対象項目の設定	O	-	O	O
38. TSF ソフトウェア完全性検証値の読み出し	O	O	O	O
39. 以下の有効化／無効化 [選択： *a. USB マスストレージモード*、 *b. 利用者認証なしの USB データ転送*、 c. *接続しているシステムの認証なしの USB データ転送*]	O	O	O	O
40. [選択：*ローカルに接続されたシステム*、*リモートシステム*] へのバックアップの有効化／無効化	O	O	O	O
41. 以下の有効化／無効化 [選択： *a. [選択：事前共有鍵、パスコード、認証なし] によって認証されたホットスポット機能*、 b. *[選択：事前共有鍵、パスコード、認証なし] によって認証された USB テザリング*]	O	O	O	O
42. [選択：*アプリケーションプロセス*、*アプリケーションプロセスのグループ*] 間のデータ共有の例外の承認	O	O	O	O
43. [割付：*アプリケーション特性*] に基づいたアプリケーションプロセスグループへのアプリケーションの配置	O	O	O	O
44. 位置情報サービスの有効化／無効化： a. デバイス全体にわたって [選択： *b. アプリごとに (per-app basis)* c. *その他の方法なし*]	M	O	O	O
45. [割付：*TSF によって提供されるべきその他の管理機能のリスト*]	O	O	O	O

表 1：管理機能

適用上の注釈：

表 1 は、このプロテクションプロファイルに要求される管理機能を比較したものである。

最初の列には、PP で識別された管理機能が列挙されている。

以下の列において：

- 『M』は必須を意味し、
- 『O』はオプション／オブジェクティブ(訳注：将来的に追加される)を意味する、

2 番目の列 (FMT_SMF_EXT.1) は、その機能が実装されるべきかどうかを示している。ST 作成者は、実装されるオプションの機能を選択すべきである (should)。

3 番目の列 (FMT_MOF_EXT.1.1) は、利用者に対して制限されるべきか機能を示している。

4 番目の列 (管理者) は、管理者が常に利用可能であるべき機能を示している。これらは、2 番目及び 3 番目の列から導き出される。 したがって、TOE は、これらの機能が FMT_SMF_EXT.1 に含まれる場合、管理者が実行できるよう提供しなければならない (must)。

5 番目の列 (FMT_MOF_EXT.1.2) は、そのデバイスが登録され、管理者が示されたポリシーを適用する場合、その機能が管理者に制限されるべきかどうかを示している。

ST 作成者は、ST において表を利用して、実装される機能のみを列挙してもよい。必須の機能については、選択にない任意のサブ機能もまた必須であり、割付には少なくとも 1 つの割付けられた値を含まなければならない (must)。オプションであり割付または選択を含む機能については、少なくとも 1 つの値が割付／選択されて ST に含まれなければならない (must)。オプションの機能における選択不可のサブ機能については、その機能が含まれるためにはすべてのサブ機能が実装されなければならない (must)。「アプリごとの原則で (per-app basis)」のサブ機能及び割付を持つ機能について、ST 作成者は、割付けられた特性がアプリごとに管理可能であるもの及びそうでないものについて、行を繰り返して示さなければならない (must)。

機能特有の適用上の注釈：

機能 3、 5 及び 44 について、機能はデバイスワイドの原則で実装されなければならない (must) が、アプリごとの原則 (per-app basis) で、有効化／無効化が適用されるアプリケーションのリストを含む設定に実装してもよい。

機能 3 は、IPsec VPN のみの有効化／無効化に対応する。VPN クライアント自身の設定 (VPN ゲートウェイ、証明書、及びアルゴリズム等の情報を含む) は、IPsec VPN クライアントのプロテクションプロファイルにより対処される。管理者オプションは、管理者がリモートから VPN 接続を有効化／無効化できる場合にのみ列挙されるべきである (should)。

機能 4 の割付は、Wi-Fi、GPS、携帯電話、NFC、Bluetooth BR/EDR、及び Bluetooth LE 等、すべて無線であり、有効化及び無効化が可能なものから構成される。 将来は、Bluetooth BR/EDR と Bluetooth LE の両方がサポートされる場合、それらを別個に有効化及び無効化できることが要求される。 携帯電話無線の無効化は、緊急通話を行うために無線が有効化されてはならないことを意味しない；しかし、「機内モード」のデバイス、つまりすべての無線が無効化されているデバイスが、緊急通話を行うために自動的に (許可なしに) 携帯電話無線を起動することは期待されていない。

機能 5 の割付は、カメラやマイクロフォン等、すべてのオーディオ及び映像デバイスであり、利用者または管理者のいずれかにより有効化及び無効化が可能なものから構成される。マイクロフォンの無効化は、緊急通話を行うためにマイクロフォンが有効化されてはならないことを意味しない。

機能 4 及び 5 に関しては、特定の無線またはオーディオ／映像デバイスの無効化は、TOE の電源が入った直後に実施されなければならない (must)。 無効化は、例えばアップデートまたはバックアップに伴い、TOE が補助ブートモードにブートされた際にも適用されなければならない (must)。TOE が、セキュリティ管理ポリシーがアクセス不可能な状態を、例

えば保存データ保護のために、サポートする場合、これらの状態に入っている間はデフォルトでこれらのデバイスが無効化されることを保証することによって、本要件を満たすことは受容可能である。 補助ブートモードの間これらのデバイスが無効化されていることは、緊急通話を行うためにそのデバイス (特に携帯電話無線) が有効化できないことを意味しない。

機能 7 のセキュリティポリシーは、WPA2 エンタープライズ等のセキュリティタイプ、及び EAP-TLS 等の認証プロトコルに対応する。CA または FQDN は、FCS_TLSC_EXT.1.2 に従い比較のために特定される。

TSF のワイプ (機能 9) は、FCS_CKM_EXT.5 に従い実行されわれる。

機能 10 での選択は、利用者がインストールしてもよいアプリケーションを制限するために MDM エージェントを通して管理者が利用可能なメカニズムを ST 作成者が選択することを可能とする。

- インストール可能なアプリケーションの生成元を管理者が制約できる場合、ST 作成者はオプション a を選択する。
- 許可されたアプリケーションのホワイトリストを管理者が指定できる場合、ST 作成者はオプション b を選択する。ST 作成者は、作成できたホワイトリストに基づいて任意のアプリケーションの特徴 (例えば、名称、バージョン、または開発者) を列挙すべきである (should)。
- 利用者がアプリケーションを追加インストールすることを管理者が防止できる場合、ST 作成者は c を選択する。

将来、機能 14 は、開発者の証明書等、TSF の継続的な運用に必要な CA 証明書を除き、任意のデフォルト高信頼 CA 証明書の破棄または無効化を要求されるかもしれない。 現時点では、ST 作成者は、割付において、事前にインストールされた、または他のカテゴリーの X.509v3 証明書をトラストアンカーデータベースから削除できるかどうかを示さなければならない (shall)。

機能 15 について、登録機能は、MDM エージェントをインストールしようとしてもよく、またデバイスへ適用されるべきポリシーを含む。 利用者承認通知が、その通知の中にポリシーをすべて列挙するよりもむしろ、ポリシーを閲覧するための (例えば、「閲覧」アイコンを「押す」することによで) 利用者が意図して選択することを要求することは受け入れられる。

機能 17 について、システムソフトウェアをアップデートするための管理者機能は、アップデートそのものを開始する能力ではなく、アップデートするために利用者へプロンプトを表示させることに限定されてもよい。管理者はリモートから操作を行うと考えられるため、低電力状態等、アップデートを失敗させデバイスを動作不能としてしまうような不適当な状況を、彼／彼女は認識していないかもしれない。このような状況では、利用者はアップデートの許容を拒否できる。システム設計者がこの制限を認識し、企業にとって重要なアップデートを実施するためにネットワークアクセス制御を実施すると期待されている。

機能 18 は、インストールとアップデートの両方に対応する。 本プロテクションプロファイルは、アプリケーションのインストールとアップデートを区別していない、なぜなら、モバイルデバイスは、通常アプリケーションのアップデート中に新たなインストールによって過去のインストールを完全に上書きするからである。

機能 19 について、「企業アプリケーション」は企業の管理者によってインストールされるアプリケーションである。

機能 20 について、検出可能 (Discoverable) モードの管理と Bluetooth デバイス名の管理は両方とも必須である。 Bluetooth に関するその他すべての管理機能は、現在オブジェクティブ (将来の目標) である：

- 機能 20.c には、Bluetooth High Speed の一部として利用される WiFi の無効化及び Bluetooth のアウトオブバンドペアリング方法としての NFC の無効化が含まれる。
- 無効化されるかもしれない Bluetooth サービス及び／またはプロファイル (機能 20.f) は、サービス及び／またはプロファイルの名称、もしくは利用されるサービス及び／またはプロファイル用のアプリケーション種別のいずれかによって、利用者／管理者が列挙するべきである (should)。
- 機能 20.g のセキュリティのレベルの例としては、レガシーなペアリングの使用及びさまざまな種類の Secure Simple Pairing（BR/EDR 用は、確認なし（Just Works）、6 桁の認証コードを表示しての一致確認（Numeric Comparison）、6 桁の認証コード入力による確認（Passkey Entry）、Bluetooth 以外の通信による確認（Out-Of-Band）； LE 用は、確認なし（Just Works）、6 桁の認証コード入力による確認（Passkey Entry）、Bluetooth 以外の通信による確認（Out-Of-Band））の使用がある。 セキュリティのレベルは、各個別のペアリングまたはすべての Bluetooth ペアリングについて設定可能であってもよい。

  2015 年の第 3 四半期以降に評価に入る製品については、TSF が Security Mode 4/Level 3 以上 (BR/EDR について) または Security Mode 1/Level 3 (LE について) 以外の任意のセキュリティモードをサポートする場合、ペアリングプロセス中に特定のデバイスへ実施されるセキュリティの最低レベルを利用者が選ぶためのメカニズムを TSF は提供しなければならない (shall)。

  BR/EDR については、Security Mode 4/Level 3 は Secure Simple Pairing (SSP) に暗号化要件とペアリング中の中間者 (MiTM) 保護の要件を付け加えたものに対応する。LE については、Security Mode 1/Level 3 は暗号化を伴う認証済みペアリングを利用する要件に対応する。本要件は、レガシー及び／または確認なし SSP を無効化する方法 (BR/EDR について) 及び認証済みペアリングと暗号化を要求する (LE について) 方法を利用者へ提供するメニューの利用により満たすことができるかもしれない。
- Bluetooth 以外の通信による確認（Out-Of-Band）のペアリング方法がサポートされる場合、機能 20.h が選択されるべきである (should)。

ロック状態での通知の表示がサポートされる場合、これらの通知の設定 (機能 21) が選択に含まれなければならない (must)。

機能 22 の割付は、USB、SD カード、そして HDMI 等、すべての外部アクセス可能なハードウェアポートから構成され、そのデータ転送機能は、利用者または管理者のいずれかにより有効化及び無効化できる。 外部ポート上のデータ転送の無効化は、デバイスの通常動作モードへのブート中及びブート後に有効となっていなければならない (must)。 TOE が、設定済みセキュリティ管理ポリシーがアクセス不可能な状態を、例えば保存データ保護のためにサポートする場合、これらの状態に入っている間はデフォルトでデータ転送が無効化されることを保証することにより、本要件を満たすことは受容可能である。 各ポートは、別個に有効化または無効化されてもよい。設定ポリシーは、すべてのポートをまとめて無効化する必要はない。

機能 23 の割付は、WiFi テザリング (パーソナルホットスポット) 等、TSF がサーバとして動作するすべてのプロトコルから構成され、利用者または管理者のいずれかにより有効化

及び無効化することができる。

機能 24 は、開発者モードが TSF によりサポートされる場合、選択に含まれなければならない (must)。

機能 25 は、保存データ保護が元々有効化されていない場合、選択に含まれなければならない (must)。

機能 26 は、デバイスがリムーバブルメディアをサポートする場合、選択に含まれるべきである (should)。

機能 27 は、パスワードのヒントやリモート認証を含めた「パスワードを忘れた場合」の機能等、ローカル利用者認証のバイパスがサポートされる場合、選択に含まれなければならない (must)。

機能 29 は､TSF がアプリケーションにトラストアンカーデータベースから X.509v3 証明書をインポートまたは削除することを許可している場合、選択に含まれなければならない (must)。 これらのアプリケーションは、MDM エージェントを含まない。 本機能は、自身の検証用証明書を信頼するアプリケーションには適用されない。 本機能は、アプリケーションがデバイスワイドなトラストアンカーデータベースを改変し、他のアプリケーションについて TSF により実行される検証に影響を及ぼすような状況にのみ適用される。利用者または管理者は、本要件を満たすために任意のアプリケーションからの要求をグローバルに許可または拒否する能力の提供を受けてもよい。

機能 30 は、FIA_X509_EXT.2.2 において「管理者による設定オプション」が選択される場合、選択に含まれなければならない (must)。

機能 33 は、FPT_TUD_EXT.2.5 が ST に含まれ、設定可能オプションが選択される場合、選択に含まれるべきである (should)。

機能 34 は、FCS_STG_EXT.1.4 において利用者または管理者が選択される場合、選択に含まれるべきである (should)。

機能 35 は、FCS_STG_EXT.1.5 において利用者または管理者が選択される場合、選択に含まれるべきである (should)。

機能 36 は、FTA_TAB.1 が ST に含まれる場合、選択に含まれなければならない (must)。

機能 37 は、FAU_SEL.1 が ST に含まれる場合、選択に含まれなければならない (must)。

機能 41 について、ホットスポット機能は外部ホットスポットへの TOE の接続ではなく、モバイルデバイスが他のデバイスへのアクセスポイントとしてサービスを提供している状態を指す。

機能 42 及び 43 は、FDP_ACF_EXT.1.2 に対応する。

機能 44 について、位置情報サービスには GPS、携帯電話、及び WiFi から収集された位置情報が含まれる。デバイス全体にわたる位置情報サービスの無効化は、緊急通話を行うためにマイクロフォンが有効化されないかもしれないことを意図しない。

保証アクティビティ：

評価者は、すべての管理機能、どの役割がそれぞれの機能を実行可能か、これらの機能が FMT_MOF_EXT.1 により識別される役割を限定する (または限定できる) 方法について、TSS に記述されていることを検証しなければならない (shall)。

以下のアクティビティは、表中の機能番号に従い書かれている。これらのアクティビティ

には、TSS 保証アクティビティ、AGD 保証アクティビティ、そしてテストアクティビティが含まれる。

以下で特定されるテストアクティビティは、FPT_TUD_EXT.1.1、FPT_TUD_EXT.1.2、及び FPT_TUD_EXT.1.3 の保証アクティビティで記述される*テスト環境*において、実行されなければならない (shall)。 評価者は、利用者及び管理者の両方がその機能を実行できる場合は必要に応じてそれぞれテストを繰返しつつ、特定されたテストのそれぞれを実行するため、AGD ガイダンスを調べなければならない (shall)。 評価者は、設定の詳細を含め、各管理機能を実行する方法が AGD ガイダンスに記述されていることを検証しなければならない (shall)。 テストされる特定された各管理機能について、評価者は、基盤となるメカニズムが構成された設定を示していることを確認しなければならない (shall)。

機能 1

評価者は、許容可能なポリシーオプションを TSS が定義していることを検証しなければならない (shall) : パスワード長とライフタイムの両方についての値の範囲、及び文字セットと複雑さのポリシーを含めた複雑さの記述 (例えば、パスワードあたりの大文字、小文字、及び特殊文字の数の設定及び実施)。

テスト 1 : 評価者は、以下のそれぞれについて、改変可能な設定のそれぞれについて少なくとも 2 つの値を設定し、ポジティブ及びネガティブテストを実行し、管理者として TSF 設定を行使しなければならない (shall)。

- 最小のパスワード長
- 最小のパスワード複雑性
- 最大のパスワードライフタイム

機能 2

評価者は、タイムアウト時間間隔と認証失敗回数の両方の値の範囲が TSS に定義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、利用者及び管理者として TSF 設定を行使しなければならない (shall)。評価者は、以下のそれぞれについて、改変可能な設定のそれぞれについて少なくとも 2 つの値を設定し、ポジティブ及びネガティブテストを実行しなければならない (shall)。

- 画面ロックの有効化／無効化
- 画面ロックのタイムアウト
- 認証失敗の回数 (FIA_AFL.1 のテストと組み合わせてもよい)

機能 3

テスト 3 : 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 3a : 評価者は、VPN 保護を有効化するために、TSF 設定を行使しなければならない (shall)。 これらの設定アクションは、FDP_IFC.1.1 要件のテスト用に利用されなければならない (must)。

テスト 3b : [条件付き] 「アプリごとに (per-app basis)」が選択されている場合、評価者は 2 つのアプリケーションを作成し、一方は VPN を利用可能とし、他方は VPN を利用しないものとしなければならない (shall)。 評価者は、TOE からのパケットをキャプチャし手いる間、各アプリケーションを(ネットワーク資源へのアクセスを試行して；例えば異なるウェブサイトをブラウズすることにより) 個別に行使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、VPN 利用可能なアプリケーションからのトラフィックが IPsec でカプセル化されていること、及び VPN 利用不可のアプリケーションからのトラフィックが IPsec でカプセル化されていないことを検証しなければならない (shall)。

機能 4

評価者は、各無線の記述と、無線が有効化／無効化できるかどうかの表示及びそれを行うことができる役割について TSS に含まれていることを検証しなければならない (shall)。さらに評価者は、各無線が動作する周波数範囲が TSS 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、有効化／無効化機能を実行する方法について AGD ガイダンスに記述されていることを確認しなければならない (shall)。 この試験に使用されるスペクトラムアナライザ及び Ramsey (訳注 : 電波シールド) ボックスは、NVLAP 認定され校正されなければならない (shall)。

テスト 4 : 評価者は、ST 作成者によって列挙された無線 (例えば Wi-Fi、GPS、携帯電話、NFC、Bluetooth) それぞれの状態を有効化及び無効化するために、利用者及び管理者の両方として TSF 設定を行使しなければならない (shall)。 さらに、評価者は、デバイスによってサポートされる任意の補助ブートモードでブートし、以下のステップを繰り返さなければならない (shall)。各無線について、評価者は、以下を実行しなければならない (shall) :

ステップ 1 - 試験される無線の望まれている周波数範囲 (TSS に提供される範囲に基づいて) をスイープするため、スペクトラムアナライザを設定し、他のすべての RF トラフィックから分離するため、ハンドセットを Ramsey ボックス (またはその他の電波暗室環境) に入れなければならない。

ステップ 2 - 評価者は、RF 信号の期待されるふるまいのベースラインを作成しなければならない (shall)。特定の無線周波数帯でアップリンクチャネルの RF アクティビティのスパイクが確認された場合、無線が有効化されているとみなされる。評価者はデバイスの電源を投入し、テスト対象の無線が有効化されていることを保証し、デバイスの電源を切断し、スペクトラムアナライザの「マックスホールド」を有効化して、デバイスの電源を投入しなければならない (shall)。 評価者は、何らかの RF スパイクが存在するかどうかを確認しなければならない (shall)。 評価者は、ブートプロセスを完了するために必要なパスワードを入力し、2 分待つと共に各ステップの間にスペクトラムアナライザをリセットしなければならない (shall)。

ステップ 3 - 評価者は、テスト対象の無線を無効化し、無線ごとに 5 回ずつ上記のテストを完了しなければならない (shall)。 評価者は、デバイスのリブートと一時的な使用の間、アップリンクチャネルで RF アクティビティが観測できないことを検証しなければならない (shall)。

機能 5

評価者は、各収集デバイスの記述と、それが有効化／無効化できるかどうかの表示及びそれを実行することができる役割について、TSS 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、有効化／無効化機能を実行する方法について AGD ガイダンスに記述されていることを確認しなければならない (shall)。

テスト 5 : 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 5a : 評価者は、ST 作成者により列挙されたオーディオまたは映像収集デバイス (例えばカメラ、マイクロフォン) のそれぞれの状態を有効化及び無効化するため、利用者及び管理者の両方として TSF 設定を行使しなければならない (shall)。 それぞれの収集デバイスについて、評価者は、デバイスを無効化し、その後その機能の利用を試行しなければな

らない (shall)。 評価者は、TOE をリブートし、無効化された収集デバイスがブートプロセス中またはその初期に利用できないことを検証しなければならない (shall)。 さらに、評価者は、利用可能な補助ブートモードのそれぞれでデバイスをブートし、収集デバイスが利用できないことを検証しなければならない (shall)。

テスト 5b : [条件付き] 「アプリごとに (per-app basis)」が選択されている場合、評価者は 2 つのアプリケーションを作成し、一方は A/V デバイスの使用アクセスを有効化し、他方は A/V デバイスへアクセスしないようにしなければならない (shall)。 評価者は、A/V デバイスへのアクセスを個別に試行するため、各アプリケーションを行使しなければならない (shall)。 評価者は、有効化されたアプリケーションが A/V デバイスへアクセスでき、無効化されたアプリケーションが A/V デバイスへアクセスできないことを検証しなければならない (shall)。

機能 6

評価者は、機能 6 及び 7 に関連するテストを目的とした無線アクセスシステム及び認証サーバからなるテスト環境を作成しなければならない (shall)。

テスト 6 : 評価者は、管理者及び利用者として、AGD ガイダンスに従って無線ネットワーク及び無線ネットワーク設定を特定しなければならない (shall)。 評価者は、テストネットワークの設定に従って、管理機能のそれぞれについて値を特定しなければならない (shall)。最低限、評価者は、2 つの SSID を構築し、一方は EAP-TLS を用いた WPA2 企業ネットワークに対応し、他方は許容されない SSID に対応するようにしなければならない (shall)。評価者は、TSF が許容された SSID への接続を確立できるが、許容されない SSID へはできないことを検証しなければならない (shall)。

機能 7

評価者は、機能 6 及び 7 に関連するテストを目的とした無線アクセスシステム及び認証サーバからなるテスト環境を作成しなければならない (shall)。

評価者は、WLAN 認証サーバの検証で使用されるさまざまなクレデンシャルオプションの設定及び実施について TSS に記述されていることを検証しなければならない (shall)。 評価者は、TSS に記述されるクレデンシャルオプションのそれぞれについて、セキュリティ種別、プロトコル、及びクライアントクレデンシャルを設定する方法について管理ガイダンスに記述されていることを決定するため、管理ガイダンスをレビューしなければならない (shall)。

テスト 7 : 評価者は、WLAN 認証サーバの不正確な値を無線ネットワークに指定し、モバイルデバイスが WLAN へ接続できないことを検証しなければならない (shall)。 評価者は、セキュリティ種別及び認証プロトコルについてそれぞれ個別に不正確な値を設定し、このテストを繰り返し、モバイルデバイスが WLAN へ接続できないことを検証しなければならない (shall)。次に評価者は、ST で主張されている各クレデンシャルオプションについて、正確なオプションを指定し、TOE が WLAN への接続の確立に成功できることを実証しなければならない (shall)。

機能 8

テスト 8 : 評価者は、管理者及び利用者の両方として、ロック状態への移行をデバイスへ指令するよう TSF に指示するためにテスト環境を用い、デバイスが指令を受けてロック状態へ移行することを検証しなければならない (shall)。

機能 9

テスト 9 : 評価者は、管理者として及び利用者として、保護データのワイプの実行をデバイ

スへ指令するようテスト環境を用いて TSF に指示しなければならない (shall)。評価者は、この管理設定が FCS_CKM_EXT.5 中の保証アクティビティを実施する際に使用されることを保証しなければならない (must)。

機能 10

評価者は、ST に含まれる選択に基づいて許容可能なアプリケーションインストールポリシーオプションについて TSS に記述されていることを検証しなければならない (shall)。 アプリケーションホワイトリストが選択される場合、評価者は、基礎となるホワイトリスト上の各アプリケーションの特徴についての記述が TSS に含まれることを検証しなければならない (shall)。

テスト 10 : 評価者は、AGD ガイダンスに従って特定のアプリケーション、アプリケーションの生成元、またはアプリケーションのインストールを制限するため、管理者として TSF 設定を行使しなければならない (shall)。 評価者は、不許可アプリケーションのインストールを試行し、これが不可能であることを保証しなければならない (shall)。 評価者は、これに関連して以下の具体的なテストを実行しなければならない (shall) :

テスト 10a : [条件付き] 評価者は、アプリケーションをインストールするために不許可リポジトリへの接続を試行しなければならない (shall)。

テスト 10b :[条件付き] 評価者は、2 つのアプリケーション (一方はホワイトリストにあり、他方はない) を既知の良好なリポジトリからインストールすることを試行して、ホワイトリストにないアプリケーションが拒否されることを検証しなければならない (shall)。 評価者は、ホワイトリストが遵守されることを決定するために、USB 接続を介して実行可能形式またはインストールパッケージのサイドロード (side-load) についても試行しなければならない (shall)

機能 11 及び機能 12

評価者は、TSF のセキュアな鍵ストレージへインポート可能な鍵／秘密の各カテゴリーについて TSS に記述されていることを検証しなければならない (shall)。

テスト 11 :
及び
テスト 12 : これらの機能のテストは、FCS_STG_EXT.1 と共に実行される。

機能 13

評価者は、トラストアンカーデータベースにおいて証明書をインポート、改変、または削除するために必要とされる手順が記述されていること、及びそれらの証明書をインポートする権限を持つ利用者 (例えば、管理者のみ、または管理者と利用者の両方) が識別されていることを決定するために、AGD ガイダンスをレビューしなければならない (shall)。

テスト 13 : 評価者は、管理ガイダンスにより決定されるとおり、利用者及び／または管理者として、AGD ガイダンスに従い証明書をインポートしなければならない (shall)。 評価者は、インポート中に何のエラーも発生しないことを検証しなければならない (shall)。 評価者は、インストールが適切に完了したという保証を提供するため、X.509v3 証明書の利用を要求するアクションを実行するべきである (should)。

機能 14

評価者は、X.509 証明書の追加の各カテゴリ及び TSF 内でのそれらの用途について TSS に記述されていることを検証しなければならない (shall)。

テスト 14 : 評価者は、、利用者及び管理者として AGD ガイダンスに従い、管理者がインポ

ートした証明書及び機能 14 の割付に含まれるその他のカテゴリの証明書を、トラストアンカーデータベースから削除しなければならない (shall)。

機能 15

評価者は、デバイスが登録されるにあたって企業により実施される各管理機能についての記述が TSS に含まれることを保証するため、TSS を検査しなければならない (shall)。 評価者は、これと同一の情報が存在することを決定するため、AGD ガイダンスを検査しなければならない (shall)。

テスト 15 : 評価者は、デバイスを管理へ登録するため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)。

機能 16

評価者は、どのアプリケーションが削除可能か (例えば、利用者によりインストールされたアプリケーション、管理者によりインストールされたアプリケーション、または企業アプリケーション)、及びそれを行うことができる役割についての表示が 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、削除可能なアプリケーションの各種別について、それらのアプリケーション及び関連データを削除するために必要な手順が詳述されていることを決定するため、AGD ガイダンスを検査しなければならない (shall)。 本保証アクティビティの目的について、「関連データ」とは、アプリによりその動作中に作成されたデータであって、そのアプリの存在と独立に存在しないもの、例えば、設定データ、または電子メールクライアントの一部である電子メール情報を指す。 反面、ワープロ文書 (ワープロアプリ用) または写真 (写真またはカメラアプリ用) 等のデータは、これには当たらない。

テスト 16 : 評価者は、AGD ガイダンスに従いアプリケーションの削除を試行し、TOE がもはやそれらのアプリケーションまたはそれらに関連するデータへのアクセスを利用者に許可しないことを検証しなければならない (shall)。

機能 17

テスト 17 : 評価者は、AGD ガイダンスの手順に従い TSF システムソフトウェアのアップデートを試行し、アップデートが正しくインストールされシステムソフトウェアのバージョン番号が増加することを検証しなければならない (shall)。

機能 18

テスト 18 : 評価者は、AGD ガイダンスの手順に従いモバイルアプリケーションのインストールを試行し、モバイルアプリケーションがインストールされ TOE 上で利用可能であることを検証しなければならない (shall)。

機能 19

評価者は、どの企業アプリケーションが削除可能か、どのアクションが本削除を開始するか、及びどの役割が実行可能かについての指示が TSS に含まれることを検証しなければならない (shall)。本アクティビティは、機能 16 に定義される TSS アクティビティと組み合わせて行うことができる。 評価者は、企業アプリケーションをデバイスから削除するために必要なステップが AGD ガイダンスに記述されていることを決定するため、AGD ガイダンスをレビューしなければならない (shall)。

テスト 19 : 評価者は、管理者ガイダンスに従うことにより、企業アプリケーションをデバイスから削除するため、試行しなければならない (shall)。 評価者は、TOE がもはやそれらのアプリケーションまたはそれらに関連するデータへのアクセスを利用者に許可しない

ことを検証しなければならない (shall)。

機能 20

評価者は、サポートされる Bluetooth プロファイル及び TOE によりサポートされる Bluetooth セキュリティモード及びレベルについての記述が TSS に含まれることを保証しなければならない (shall)。 機能 c が選択された場合、評価者は、Bluetooth と共に使用してもよい追加の無線技術が、Out of Band（Bluetooth 以外の）ペアリングメカニズムとしての Bluetooth 高速通信用 WiFi 及び NFC（訳注 : Near Field radio Communication）を含め、TSS に記述されていることを検証しなければならない (shall)。 機能 f が選択された場合、評価者は、すべてのサポートされる Bluetooth サービスが管理可能なものとして TSS に列挙されていること、そして TOE がサービス名よりむしろアプリケーションによる無効化を許容する場合、各アプリケーション用のサービスのリストについても列挙されていることを検証しなければならない (shall)。 機能 g が選択された場合、評価者は、ペアリング用セキュリティレベルの管理方法について、各ペアリングについて設定が行われるかまたはグローバルな設定かを含め、TSS に記述されていることを検証しなければならない (shall)。機能 h が選択された場合、評価者は、Out of Band（Bluetooth 以外の）ペアリング方法がいつ許容されるか、及びどれが設定可能なのかについて、TSS に記述されていることを検証しなければならない (shall)。

テスト 20 : 評価者は、以下の各サブ機能についてのテストを実行するため、Bluetooth 特有のプロトコルアナライザを用いなければならない (shall) :

*テスト 20a :*評価者は、検出可能 (Discoverable) モードを無効化しなければならず (shall)、他の Bluetooth BR/EDR デバイスが TOE を検出できないことを検証しなければならない (shall)。 評価者は、Bluetooth デバイスを検索している他のデバイスからの問い合わせに TOE が応答しないことを検証するため、プロトコルアナライザを用いなければならない (shall)。 評価者は、検出可能 (Discoverable) モードを有効化し、他のデバイスが TOE を検出できること、及び検索中のデバイスからの問い合わせに TOE が応答パケットを送信することを検証しなければならない (shall)。

テスト 20b : 評価者は、現在の Bluetooth デバイス名を決定するため TOE からの Bluetooth トラフィックを検査し、Bluetooth デバイス名の改変を行い、そのデバイスからの Bluetooth トラフィックが新しい名前を列挙していることを検証しなければならない (shall)。

テスト 20c : [条件付き] 評価者は、TOE の追加の無線技術を無効化し、Bluetooth トラフィックが Bluetooth High Speed を用いて WiFi 上で送信不可であること、及び NFC がペアリングで利用できないことを検証しなければならない (shall)。評価者は追加的無線技術を有効化し、Bluetooth High Speed に WiFi が利用されること、またはデバイスが NFC を利用してペアリングできることを検証しなければならない (shall)。

テスト 20d : [条件付き] 評価者は、Bluetooth LE 用のアドバタイジングを有効化しアドバタイズメントがプロトコルアナライザによりキャプチャされることを検証し、アドバタイジングを無効化しデバイスからのアドバタイズメントがプロトコルアナライザにより一切キャプチャされないことを検証しなければならない (shall)。

テスト 20e : [条件付き] 評価者は、接続可能 (Connectable) モードを有効化し、他の Bluetooth デバイスが TOE とペアリングできること、及び (デバイスがボンディングされていた場合) ペアリングと切断した後に再接続することを検証しなければならない (shall)。BR/EDR デバイスについて : 評価者は、TOE が他のデバイスからのページングに応答し、ペアリング及び再接続を許可することを検証するため、プロトコルアナライザを用いなければならない (shall)。 評価者は、接続可能 (Connectable) モードを無効化し、TOE がリ

モート Bluetooth デバイスからのページングに応答しないこと、その結果ペアリングも再接続も許可しないことを検証しなければならない (shall)。 LE について：評価者は、TOE が接続可能なアドバタイジングイベントを送信し、接続要求に応答することを検証するため、プロトコルアナライザを用いなければならない (shall)。 評価者は、接続可能 (Connectable) モードを無効化し、TOE が接続可能なアドバタイジングイベントの送信を停止し、リモート Bluetooth デバイスからの接続要求への応答を停止することを検証しなければならない (shall)。

テスト 20f : [条件付き] 評価者は、TOE 上で低セキュリティモード／レベルを許容しなければならず (shall)、かつセキュリティモード 4／レベル 3 またはセキュリティモード 4／レベル 4 (BR/EDR 用)、またはセキュリティモード 1／レベル 3 (LE 用) 以外のもののみを許容するリモートデバイスから TOE とのペアリングを開始しなければならない (shall)。 (例えば、リモート BR/EDR デバイスは Input/Output 能力「NoInputNoOutput」を主張してもよく、中間者 (MiTM) 保護が要求されないことを言明してもよい。 リモート LE デバイスは暗号化をサポートしなくてよい。) 評価者は、TOE が低セキュリティモード／レベルへフォールバックするため、本ペアリング試行が成功することを検証しなければならない (shall) 。 そのとき評価者は、2 つのデバイスのペアリングを解除し、TOE における低セキュリティモード／レベルの使用を禁止し、再度接続を試行しなければならない (shall)。 評価者は、ペアリング試行が失敗することを検証しなければならない (shall)。 低セキュリティモード／レベルが無効化された状態で、評価者は、TOE から、セキュリティモード 4／レベル 3 またはセキュリティモード 4／レベル 4 (BR/EDR 用) またはセキュリティモード 1／レベル 3 (LE 用) をサポートするリモートデバイスへのペアリングを開始しなければならない (shall)。 評価者は、本ペアリングが成功し、高セキュリティモード／レベルを利用することを検証しなければならない (shall)。

テスト 20g : [条件付き] 評価者は、Out of Band（Bluetooth 以外の）ペアリング方法のそれぞれを用いてペアリングを試行し、そのペアリング方法が動作することを検証し、反復的に各ペアリング方法を無効化し、そのペアリング方法が失敗することを検証しなければならない (shall)。

機能 21

評価者は、少なくとも機能 21 にて選択された情報のカテゴリそれぞれについて、ロック状態でその種別の情報について、情報の表示を有効化及び無効化する方法が特定されていることを決定するため、AGD ガイダンスを検査しなければならない (shall)。

テスト 21 : AGD ガイダンスに列挙された情報の各カテゴリについて、評価者は、TSF が AGD に従い情報を制限するよう設定されている時、ロック状態において情報がもはや表示されないことを検証しなければならない (shall)。

以下の機能がオプションの機能であり、その機能が実装されている場合、以下の保証アクティビティは実行されなければならない (shall) ことに注意すべきである (should)。 機能番号の隣の [条件付き] という表記は、その機能が ST に含まれない場合、その保証アクティビティが実行されると期待されないことを示している。

機能 22 [条件付き]

評価者は、外部アクセス可能な各ハードウェアポートのリストと、そのポート上のデータ転送が有効化／無効化できるかどうかの表示が TSS に含まれることを検証しなければならない (shall)。 AGD ガイダンスは、有効化／無効化機能を実行する方法を記述すること。

テスト 22 : 評価者は、ST 作成者により列挙された外部アクセス可能なハードウェアポート (例えば USB、SD カード、HDMI) のそれぞれのデータ転送機能を有効化及び無効化するた

め、TSF 設定を行使しなければならない (shall)。 評価者は、特定のインタフェースについて、それらが無効化されている時、データ転送用のすべてのピンで低レベルのシグナリングが発生していないことを保証するため、テスト機器を使用しなければならない (shall)。無効化された各データ転送機能について、評価者は、デバイスを通常の動作モードでリブートしブート中及びデバイスの初期実行段階を通してその機能が無効化されていることを検証することにより、本テストを繰り返さなければならない (shall)。

機能 23 [条件付き]

評価者は、ST に列挙した各プロトコルにおいて TSF がサーバとしてどのようにふるまうか、及びサーバとしてふるまう理由について、TSS に記述されていることを検証しなければならない (shall)。

テスト 23 : 評価者は、割付に列挙された各プロトコルの無効化、ここではテザリングの利用が含まれるべきである (should)、を試行しなければならない (shall)。 評価者は、リモートデバイスが、無効化されたプロトコルを用いて、TOE または TOE リソースへアクセスすることが、もはやできないことを検証しなければならない (shall)。

機能 24 [条件付き]

テスト 24 : 評価者は、開発者モードを有効化及び無効化するため、利用者及び管理者の両方として TSF 設定を行使しなければならない (shall)。 評価者は、開発者モードの設定が無効化されている時、開発者モードアクセスが利用不可であることをテストしなければならない (shall)。 評価者は、デバイスのリブート中に開発者モードが無効化されたままであることを検証しなければならない (shall)。

機能 25 [条件付き]

テスト 25 : 評価者は、AGD ガイダンスに従いシステムワイドの保存データ保護を有効化するため、利用者及び管理者の両方として TSF 設定を行使しなければならない (shall)。 評価者は、DAR(訳注：Data at Rest 保存データ)に関するすべての保証アクティビティ (セクション 0 参照) が、本設定のデバイスを用いて実行されることを保証しなければならない (shall)。

機能 26 [条件付き]

テスト 26 : 評価者は、AGD ガイダンスに従いリムーバブルメディアの保存データ保護を有効化するため、利用者及び管理者の両方として TSF 設定を行使しなければならない (shall)。評価者は、DAR に関するすべての保証アクティビティ (セクション 0 参照) が、本設定のデバイスを用いて実行されることを保証しなければならない (shall)。

機能 27 [条件付き]

評価者は、任意の「パスワードを忘れた場合」、パスワードのヒント、または (ローカルな認証メカニズムをバイパスするための) リモート認証機能を有効化及び無効化する方法が記述されていることを決定するため、AGD ガイダンスを検査しなければならない (shall)。

テスト 27 :「パスワードを忘れた場合」機能またはローカル認証プロセスがバイパス可能となるような他の手段を提供するような AGD ガイダンスに列挙されている各メカニズムについて、評価者は、その機能を無効化し、それらがローカル認証プロセスをバイパスすることができないことを保証しなければならない (shall)。

機能 28 [条件付き]

テスト 28 : 評価者は、管理者ガイダンスに従いデバイス上に残存する企業データのワイプを試行しなければならない (shall)。 評価者は、そのデータがもはや利用者によってアクセ

スできないことを検証しなければならない (shall)。

機能 29 [条件付き]

評価者は、トラストアンカーデータベースにおける証明書に関する選択されたアクション (インポート、削除) をアプリケーションが実行するための承認が達成される方法 (例えば、ポップアップ、ポリシー設定等) について TSS に記述されていることを検証しなければならない (shall)。

評価者は、アプリケーションにより許容されるセキュリティ機能 (トラストアンカーデータベースのインポート、改変、または破棄) について、セクション 6.2.1 に従って提供される API 文書に含まれることについても検証しなければならない (shall)。

テスト 29 : 評価者は、以下のテストの 1 つを実行しなければならない (shall) :

テスト 29a :[条件付き] アプリケーションがトラストアンカーデータベースへ証明書をインポートできる場合、評価者は、証明書をトラストアンカーデータベースへインポートするアプリケーションを書くか、または開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。 評価者は、アプリケーションが証明書をインポートすることを許可する前に、TOE が承認を要求することを検証しなければならない (shall)。

- 評価者は、アプリケーションが証明書をインポートできないことを検証するため、承認を拒否しなければならない (shall)。 インポートの失敗は、インポートが試行された証明書へチェインする証明書の有効性確認を試行することによりテストされなければならない (FIA_X509_EXT.1 の保証アクティビティに記述されているとおり) (shall)。
- 評価者は、アプリケーションが証明書をインポートできること、及び有効性確認が発生することを検証するため、承認を許可することでテストを繰り返さなければならない (shall)。

テスト 29b :[条件付き] アプリケーションがトラストアンカーデータベースの証明書を削除できる場合、評価者は、トラストアンカーデータベースから証明書を削除するアプリケーションを書かくか、または開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。 評価者は、証明書を削除するアプリケーションを許可する前に、TOE が承認を要求することを検証しなければならない (shall)。

- 評価者は、アプリケーションが証明書を削除できないことを検証するため、承認を拒否しなければならない (shall)。 削除の失敗は、削除が試行された証明書へチェインする証明書の有効性確認を試行することによりテストされなければならない (FIA_X509_EXT.1 の保証アクティビティに記述されているとおり) (shall)。

評価者は、アプリケーションが証明書を削除／改変することができ、もはや有効性確認が行われないことを検証するため、承認を許可することによりこのテストを繰り返さなければならない (shall)。

機能 30 [条件付き]

テスト 30 : この機能のテストは、FIA_X509_EXT.2.2 と組み合わせて実行される。

機能 31 [条件付き]

評価者は、どの携帯電話プロトコルが無効化できるかについて TSS に記述されていることを保証しなければならない (shall)。 評価者は、TSS で識別された各携帯電話プロトコルを無効化するための手続きについて AGD ガイダンスに記述されていることを確認しなければならない (shall)。

テスト 31 : 評価者は、管理ガイダンスに従い各携帯電話プロトコルの無効化を試行しなければならない (shall)。 評価者は、デバイスを携帯電話ネットワークへ接続することを試行し、ネットワーク解析ツールを用いて、そのデバイスが無効化されたプロトコルのネゴシエーションを許可しないことを検証しなければならない (shall)。

機能 32 [条件付き]

テスト 32 : 評価者は、管理者ガイダンスに従い任意のデバイス監査ログの読み出しを試行し、そのログが読み出し可能であることを検証しなければならない (shall)。 本テストは、FAU_GEN.1 の保証アクティビティと組み合わせて実行してもよい。

機能 [条件付き]

テスト 33 : この機能のテストは、FPT_TUD_EXT.2.5 と組み合わせて実行される。

機能 34 [条件付き]

評価者は、複数アプリケーションによる鍵／秘密の共有された利用についての例外の承認がどのように達成されるか (例えば、ポップアップ、ポリシー設定等) について TSS に記述されていることを検証しなければならない (shall)。

テスト 34 : 本機能のテストは、FCS_STG_EXT.1 と組み合わせて実行される。

機能 35 [条件付き]

評価者は、鍵／秘密をインポートしなかったアプリケーションによるその鍵／秘密の破棄についての例外の承認がどのように達成されるか (例えば、ポップアップ、ポリシー設定等) について TSS に記述されていることを検証しなければならない (shall)。

テスト 35 : 本機能のテストは、FCS_STG_EXT.1 と組み合わせて実行される。

機能 36 [条件付き]

評価者は、バナー設定における任意の制約 (例えば、文字の制限) について TSS に記述されていることを検証しなければならない (shall)。

テスト 36 : 本機能のテストは、FTA_TAB.1 と組み合わせて実行される。

機能 37 [条件付き]

テスト 37 : 本機能のテストは、FAU_SEL.1 と組み合わせて実行される。

機能 38 [条件付き]

テスト 38 : 本機能のテストは、FPT_NOT_EXT.1.2 と組み合わせて実行される。

機能 39 [条件付き]

評価者は、USB 上のデータ転送が管理される方法の記述が TSS に含まれることを検証しなければならない (shall)。

テスト 39 : 評価者は、0 における選択に基づいて以下のテストを実行しなければならない (shall)。

テスト 39a : [条件付き] 評価者は、USB マスストレージモードを無効化し、デバイスをコンピュータへ接続し、そしてコンピュータが TOE をデバイスとしてマウントできないことを検証しなければならない (shall)。 評価者は TOE をリブートし、このテストを他のサポートされている補助ブートモードで繰り返さなければならない (shall)。

テスト 39b : [条件付き] 評価者は、利用者認証なしでの USB データ転送を無効化し、デ

バイスをコンピュータへ接続し、そしてコンピュータが TOE データへアクセスできるようになる前に TOE が利用者認証を要求することを検証しなければならない (shall)。 評価者は、TOE をリブートし、このテストを他のサポートされている補助ブートモードで繰り返さなければならない (shall)。

テスト 39c : [条件付き] 評価者は、接続システム認証なしでの USB データ転送を無効化し、デバイスをコンピュータへ接続し、そしてコンピュータが TOE データへアクセスできるようになる前に TOE が接続システム認証を要求することを検証しなければならない (shall)。次に評価者は、TOE を別のコンピュータへ接続し、そのコンピュータが TOE データへアクセスできないことを検証しなければならない (shall)。 次に評価者は、TOE を元のコンピュータへ接続し、そのコンピュータが TOE データへアクセスできることを検証しなければならない (shall)。

機能 40 [条件付き]

評価者は、利用できるバックアップ方法であって有効化／無効化可能なものの記述が TSS に含まれることを検証しなければならない (shall)。

テスト 40 : 評価者は、サポートされているバックアップの場所をそれぞれ順番に無効化し、TOE がバックアップを完了できないことを検証しなければならない (shall)。 次に評価者は、サポートされているバックアップの場所をそれぞれ順番に有効化し、TOE がバックアップを行えることを検証しなければならない (shall)。

機能 41 [条件付き]

評価者は、ホットスポット機能及び USB テザリングの記述が、それらの認証を含めて TSS に含まれることを検証しなければならない (shall)。

テスト 41 : 評価者は、0 における選択に基づいて以下のテストを実行しなければならない (shall)。

テスト 41a : [条件付き] 評価者は、サポートされている認証方法のそれぞれと共に、ホットスポット機能を有効化しなければならない (shall)。 評価者は、別のデバイスを用いてホットスポットへ接続し、ホットスポット機能が設定された認証方法を必要とすることを検証しなければならない (shall)。

テスト 41b : [条件付き] 評価者は、サポートされている認証方法のそれぞれと共に、USB テザリング機能を有効化しなければならない (shall)。 評価者は、別のデバイスを用いて USB 経由で TOE へ接続し、テザリング機能が設定された認証方法を必要とすることを検証しなければならない (shall)。

機能 42 [条件付き]

テスト 42 : 本機能のテストは、FDP_ACF_EXT.1.2 と組み合わせて実行される。

機能 43 [条件付き]

テスト 43 : 本機能のテストは、FDP_ACF_EXT.1.2 と組み合わせて実行される。

機能 44 [条件付き]

テスト 44 : 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 44a : 評価者は、デバイスワイドに位置情報サービスを有効化しなければならず (shall)、アプリケーション (地図表示アプリケーション等) が TOE の位置情報にアクセス不可能なことを検証しなければならない (shall)。

テスト 44b : [条件付き] 「アプリごとに (per-app basis)」が選択されている場合、評価者は、2 つのアプリケーションを作成し、一方は位置情報サービスの使用アクセスを有効化し、他方は位置情報サービスへアクセスしないようにしなければならない (shall)。 評価者は、位置情報サービスへのアクセスを個別に試行するため、各アプリケーションを行使しなければならない (shall)。 評価者は、有効化されたアプリケーションが位置情報サービスへアクセスでき、無効化されたアプリケーションが位置情報サービスへアクセスできないことを検証しなければならない (shall)。

機能 45 [条件付き]

評価者は、すべての割付けられたセキュリティ管理機能及びそれらの意図されたふるまいが TSS に記述されていることを検証しなければならない (shall)。

テスト 45 : 評価者は、その機能が設定可能であること、またその機能の意図されたふるまいが TOE により遂行されることを実証するためのテストを設計し実行しなければならない (shall)。

5.5.2.2 修正アクションの特定

FMT_SMF_EXT.2	拡張：修正アクションの特定

FMT_SMF_EXT.2.1 TSF は、[選択：*保護データのワイプ*、*機微なデータのワイプ*、*管理者への警報*、*企業アプリケーションの削除*、 [割付：*その他の利用可能な修正アクションの列挙*]] を、登録解除及び [選択： [割付：*その他の管理者によって設定されたトリガー*]、*その他のトリガーなし*] の際に、提供しなければならない (shall)。

適用上の注釈：登録解除は、MDM エージェントの削除、または管理者のポリシーの削除により構成してよい。選択における機能は、TOE が (おそらく MDM エージェントを介して) 管理者へ (おそらく API を介して) 提供する修正アクションであり、登録解除の際に行われるものである。

保証アクティビティ：

評価者は、すべての利用できる修正アクション、いつそれらが利用できるか、そして任意のその他の管理者により設定されたトリガーについて、TSS に記述されていることを検証しなければならない (shall)。

評価者は、登録解除の際に選択における各修正アクションを実行するために、デバイスを繰り返し設定するため、テスト環境を用いなければならない (shall)。 評価者は、AGD ガイダンスに従いデバイスを登録解除し、設定された修正アクションが実行されることを検証しなければならない (shall)。

5.6 クラス：TSF の保護 (FPT)

5.6.1 悪用防止 (Anti-Exploitation) サービス (FPT_AEX)

5.6.1.1 アドレス空間配置ランダム化

FPT_AEX_EXT.1	拡張：悪用防止サービス (ASLR)

FPT_AEX_EXT.1.1 TSF は、アドレス空間配置ランダム化 (ASLR) をアプリケーションへ提供しなければならない (shall)。

FPT_AEX_EXT.1.2 任意の利用者空間メモリマッピングのベースアドレスは、少なくとも 8 個の予測不可能なビットから構成されること。

適用上の注釈：この 8 個の予測不可能なビットは、TSF RBG によって (FCS_RBG_EXT.1

に特定されるように) 提供されてもよいが、要求はされない。

保証アクティビティ：

評価者は、ST の TSS セクションに 8 ビットが生成される方法が記述され、これらのビットが予測不可能である理由の正当化が提供されていることを保証しなければならない (shall)。

保証アクティビティの注釈：以下のテストでは、開発者に対して、消費者向けのモバイルデバイス製品には通常含まれないようなツールを評価者へ提供するような、テストプラットフォームへのアクセスを提供することを要求している。

*テスト 1：*評価者は、TSF に含まれる 3 つのアプリを選択しなければならない (shall)。 これらは、TSF に含まれるウェブブラウザまたはメールクライアントが含まれなければならない (must)。 これらの各アプリについて、評価者は、同じ種別の 2 つの別個のモバイルデバイス上で同じアプリを起動し、すべてのメモリマップ上のロケーションを比較する。 評価者は、両方のデバイス上で、どのメモリマップも同じロケーションに配置されていないことを保証しなければならない (must)。

2 つのマッピングが 1 つのアプリについて同一となり、他の 2 つのアプリでは同一でないというまれな (たかだか 1/256) 事象が発生した場合、評価者は、そのアプリについてテストを繰り返し、2 回目のテストでマッピングが異なることを検証しなければならない (shall)。

5.6.1.2 メモリページのパーミッション

FPT_AEX_EXT.2	拡張：悪用防止サービス (メモリページのパーミッション)

FPT_AEX_EXT.2.1 TSF は、物理メモリの毎ページにおける読み出し、書き込み、及び実行パーミッションを実施できなければならない (shall)。

保証アクティビティ：

評価者は、TSS にメモリ管理ユニット (MMU) の記述があることを保証し、本記述に仮想メモリのすべてのページにおける読み出し、書き込み、及び実行パーミッションを実施する MMU の能力について文書化されていることを保証しなければならない (shall)。

5.6.1.3 オーバーフロー保護

FPT_AEX_EXT.3	拡張：悪用防止サービス (オーバーフロー保護)

FPT_AEX_EXT.3.1 アプリケーションプロセッサ上の非特権実行ドメインで実行する TSF プロセスは、スタックベースのバッファオーバーフロー保護を実装しなければならない (shall)。

適用上の注釈：

「非特権実行ドメイン」とは、プロセッサのユーザモード (例えば、カーネルモードとの対語として) を指す。すべての TSF プロセスがこのような保護を実装しなければならない (must) わけではないが、大部分のプロセス (TSF プロセスによって利用されるライブラリを含む) がバッファオーバーフロー保護を実装すると期待されている。

保証アクティビティ：

評価者は、アプリケーションプロセッサの非特権実行モードで実行される TSF ソフトウェアに実装されるスタックベースのバッファオーバーフロー保護の記述が TSS に含まれることを決定しなければならない (shall)。 スタックベースのバッファオーバーフロー保護の正確な実装は、プラットフォームにより異なる。 実装の例としては、"-fstack-protector-all"、

“-fstack-protector”、及び“/GS”フラグ等のコンパイラオプションを通してアクティベートされる。

評価者は、スタックベースのバッファオーバーフロー保護を実装しているものとしていないものを示す、TSF バイナリ及びライブラリのインベントリが TSS に含まれることを保証しなければならない (shall)。TSS には、この方法で保護されないバイナリ及びライブラリの根拠が提供されなければならない (must)。

5.6.1.4 ドメイン分離

FPT_AEX_EXT.4	拡張：ドメイン分離

FPT_AEX_EXT.4.1 TSF は、信頼されないサブジェクトによる改変から自分自身を保護しなければならない (shall)。

FPT_AEX_EXT.4.2 TSF は、アプリケーション間のアドレス空間の分離を実施しなければならない (shall)。

適用上の注釈：ストレージ中に常駐する TSF ソフトウェア (例えば、カーネルイメージ、デバイスドライバ、高信頼アプリケーション) に加えて、プロセッサの特権モードで動作するソフトウェア (例えば、カーネル) の実行コンテキスト (例えば、アドレス空間、プロセッサのレジスタ、プロセス毎の環境変数)、及び高信頼アプリケーションのコンテキストが保護される。 ソフトウェアに加えて、TSF のふるまいをコントロールする、またはそれへ影響を与える設定情報があれば、それもまた信頼できないサブジェクトによる改変から保護される。

設定情報には、利用者及び管理者の管理機能の設定、WLAN プロファイル、及びサービスレベルセキュリティ要件データベース等の Bluetooth データが含まれるが、これらに限定されない。

信頼されないサブジェクトとして、以下を含む、信頼されないアプリケーション；電源オフ、画面ロック状態の間、または補助ブートモードへのブート時にデバイスへアクセスする不許可利用者；及び、不許可利用者または信頼されないソフトウェアまたはハードウェアで、デバイスが画面ロック状態か、または補助ブートモードへブートされるかのいずれかの時に、有線インタフェースを介してデバイスへのアクセスを有するもの。

保証アクティビティ：

評価者は、非 TSF ソフトウェアが TSF のふるまいを管理する TSF ソフトウェアまたは TSF データを改変から防止するために用意されているメカニズムが TSS に記述されていることを保証しなければならない (shall)。 これらのメカニズムが網羅する範囲は、ハードウェアベースの手段 (例えば「実行リング」及びメモリ管理機能) から；ソフトウェアベースの手段 (例えば API への入力に対する境界値チェック) までである。 評価者は、記述されたメカニズムが TSF を改変から保護するために妥当とみなされることを決定する。

評価者は、TSF がどのようにアプリケーションのアドレス空間が互いに分離を保っているかについて TSS に記述されていることを保証しなければならない (shall)。

評価者は、ロック状態において、または TSF のふるまいを改変できるような補助ブートモード中に、ダイアラから利用可能な USSD 及び MMI コードが TSS に詳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、コード、TSF により実行される行われるアクション、及び実行されるアクションが利用者または TSF データを改変しないという正当化が本記述に含まれることを保証しなければならない (shall)。 USSD も MMI コードも利用可能でない場合、評価者は、これらのコードにより規定されたアクションが防止される

方法についての記述を TSS が提供することを保証しなければならない (shall)。

評価者は、補助ブートモードにおいて有線インタフェースを介してアクセス及び改変できるような TSF データ (ソフトウェア、実行コンテキスト、設定情報、及び監査ログを含む) について TSS に文書化されることを保証しなければならない (shall)。 評価者は、デバイスのアップデートまたはリストアをサポートするために改変されるデータがこの記述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、データが改変され得る補助ブートモード、補助ブートモードへ入る方法、データのロケーション、データがどのように改変されるか、改変をサポートするために必要なデータのフォーマット及びパッケージング、ならびに (もしあれば) データの改変に必要なソフトウェアまたはハードウェアあるいはその両方のツールが、この文書に含まれることを保証しなければならない (shall)。

評価者は、補助ブートモードにおける有線インタフェースを介した TSF データの不正かつ未検出の改変 (すなわち、FPT_TUD_EXT.2 による暗号技術的に検証済みのアップデートは除外される) が防止される手段の記述を TSS が提供することを保証しなければならない (shall)。 (公的に入手可能なツールの欠如は十分な正当化ではない。十分な正当化の例としては、改変の監査、デジタル署名またはハッシュの形態での暗号技術的検証、補助ブートモードの無効化、及びファイルへの書き込みまたはパーティションのフラッシングを防止するアクセス制御メカニズムなどが挙げられる。)

保証アクティビティの注釈：以下のテストでは、ベンダに対して、消費者向けのモバイルデバイス製品には通常含まれないようなツールを評価者へ提供するような、テストプラットフォームへのアクセスを提供することを要求している。 加えて、ベンダは TSF を構成するファイル (例えば、システムファイル、ライブラリ、設定ファイル、監査ログ) のリストを提供する。このリストは、フォルダ／ディレクトリ (例えば、/usr/sbin、/etc) と、特定されたディレクトリの外部に存在するかもしれない個別ファイルによって分類されてもよい。

*テスト 1：*評価者は、ベンダの提供した TSF を構成するファイルのリストの中の各ファイルについて「パーミッション設定」をチェックして、信頼されないアプリケーションによる書き込みを防止するための設定が適切であることを保証しなければならない (shall)。評価者は、彼らの選んだファイルの改変を試行し、メカニズムによってパーミッション設定が実施され、改変が防止されることを保証しなければならない (shall)。

*テスト 2:*評価者は、アプリを作成し、モバイルデバイスへロードしなければならない (shall)。本アプリは、全ファイルシステムに対するトラバースを試行し、データが書き込みまたは上書きできるロケーションがあればそれを報告しなければならない (shall)。 評価者は、これらのロケーションはいずれも、OS ソフトウェア、デバイスドライバ、システム及びセキュリティ設定ファイル、鍵材料、または他のアプリケーションのイメージ／データの一部でないことを保証しなければならない (must)。

*テスト 3：*利用可能な各補助ブートモードについて、評価者は TSS に記述されるソフトウェアまたはハードウェアあるいはその両方のツールを用いて彼らの選んだ TSF ファイルの改変を試行しなければならない (shall)。評価者は、TSS における記述に従い期待されるとおり、改変が失敗すること、または TSF が変更を監査することを検証しなければならない (shall)。

5.6.2 鍵の格納 (FPT_KST)

5.6.2.1 平文鍵格納

FPT_KST_EXT.1	**拡張：鍵の格納**

FPT_KST_EXT.1.1 TSF は、いかなる平文の鍵材料も読み出し可能な不揮発性メモリへ格納してはならない (shall not)。

適用上の注釈：本要件の意図は、TOE が平文の鍵材料を永続的ストレージへ書き込まないことである。本要件の目的に関して、平文の鍵材料とは、認証データ、パスワード、秘密／プライベート対称鍵、プライベート非対称鍵、鍵の導出に使用したデータ等を指す。 これらの値は、暗号化されて格納されなければならない (must)。

さらに、2015 年の第 3 四半期以降に評価に入る製品については、本要件は、パスワードから導出されるあらゆる値にも適用されることになる。つまり、TOE は、比較の目的で平文のパスワードハッシュを保護データが復号される前に格納することはできず、TOE は、パスワード認証ファクタを検証するため、鍵の導出及び復号を使用すべきである (should)。

保証アクティビティ：

評価者は、本要件の保証アクティビティを実行するにあたり、ST の TSS セクションを調べなければならない (shall)。

それらのレビューを実行するにあたり、評価者は、DEK、格納された鍵、及びデータの復号に関連するパスワード認証及び電源投入の際に発生するアクティビティの記述を TSS が含んでいることを決定しなければならない (shall)。

評価者は、平文が不揮発性ストレージへ書き込まれることを防止するために、KEK、DEK、及び格納された鍵が TOE によりアンラップされ、保存され、利用される方法を含め、暗号化機能を実行するために FCS 要件における暗号化機能が利用される方法についても記述が網羅していることを保証しなければならない (shall)。 評価者は、電源断の各シナリオについて、不揮発性ストレージにおけるすべての鍵が KEK でラップされることをどのように TOE が保証するかについて TSS が記述していることを保証しなければならない (shall)。

評価者は、システムで利用可能なその他の機能 (例えば、鍵の再生成) が永続的ストレージにおいて暗号化されてない鍵材料が存在しないことをどのように保証するのかについて TSS が記述していることを保証しなければならない (shall)。

評価者は、鍵材料が暗号化されずに永続的ストレージへ書き込まれることがないことを TSS が論証していることを決定するため、TSS をレビューしなければならない (shall)。

5.6.2.2 鍵の送信禁止

FPT_KST_EXT.2	拡張：鍵の送信禁止

FPT_KST_EXT.2.1 TSF は、いかなる平文の鍵材料も TOE のセキュリティ境界の外へ送信してはならない (shall not)。

適用上の注釈：本要件の目的において、鍵材料は、鍵、パスワード、及び鍵の導出に使用されるその他の材料を指す。本要件の意図は、デバイス外部へ情報を送信するサービスへの平文の鍵情報のログ出力を防止することである。

将来、本要件は、アプリケーションが TOE の境界の外にある状況で、TOE のセキュアな鍵ストレージに格納される対称鍵及び非対称プライベート鍵に適用される。つまり、TSF は、それらの鍵へのアクセスを有するアプリケーションを代行して暗号鍵操作 (署名、暗号化、及び復号) を提供すること (FCS_SRV_EXT.1.2) が要求される。

保証アクティビティ：

評価者は、本要件の保証アクティビティを実行するにあたり、ST の TSS セクションを調べなければならない (shall)。 評価者は、TSS が TOE のセキュリティ境界について記述して

いることを保証しなければならない (shall)。 暗号モジュールは、特定のカーネルモジュール、オペレーティングシステム、アプリケーションプロセッサ、またはモバイルデバイス全体まで含まれるかもしれない。

レビューを実行にあたり、評価者は、DEK、保存された鍵、及びデータの復号に関連するパスワード認証及び電源投入の際に発生するアクティビティの記述が TSS に含まれていることを決定しなければならない (shall)。

評価者は、システムで利用可能なその他の機能 (例えば、鍵の再生成) が、暗号化されてない鍵材料がセキュリティ境界の外部へ送信されないことをどのように保証するかについて TSS に記述されていることを保証しなければならない (shall)。

評価者は、鍵材料が TOE のセキュリティ境界の外部へ送信されないことを論証していることを決定するため、TSS をレビューしなければならない (shall)。

5.6.2.3 平文での鍵のエクスポート禁止

FPT_KST_EXT.3	拡張：平文での鍵のエクスポート禁止

FPT_KST_EXT.3.1 TSF は、TOE の利用者が平文の鍵をエクスポートすることが不可能であることを保証しなければならない (shall)。

適用上の注釈：平文の鍵には、DEK、KEK、及びセキュアな鍵ストレージに格納されたすべての鍵が含まれる (FCS_STG_EXT.1)。 本要件の意図は、TOE の利用者または管理者により許可されたバックアップの最中に平文の鍵のエクスポートを防止することである。

保証アクティビティ：

ST 作成者は､鍵の取り扱いと保護に関する自身のポリシーステートメントを提供すること。評価者は、平文の DEK、KEK、またはセキュアな鍵ストレージに格納された鍵のいずれかをエクスポートしないというポリシーについて TSS に記述されていることを保証するため、チェックしなければならない (shall)。

5.6.3 自己テスト通知 (FPT_NOT)

FPT_NOT_EXT.1	拡張：自己テスト通知

FPT_NOT_EXT.1.1 TSF は、以下の種別の失敗が発生した時、非動作モードへの移行及び [選択：*監査記録への失敗のロギング*、*管理者への通知*、 *[割付：その他のアクション]*、*その他のアクションなし*] を実行しなければならない (shall)：

- 自己テストの失敗
- TSF ソフトウェア完全性検証の失敗
- [選択：*その他の失敗なし*、 *[割付：その他の失敗]*]。

保証アクティビティ：

評価者は、起こり得る重要な失敗と、これらの重要な失敗の際に取られるべきアクションについて TSS に記述されていることを検証しなければならない (shall)。

保証アクティビティの注釈：以下のテストには、開発者に対して、消費者向けのモバイルデバイス製品には通常含まれないようなツールを評価者へ提供するような、テストプラットフォームへのアクセスを提供することを要求している。

*テスト 1：*評価者は､､2 番目のリストに特定される重要な失敗に対応するシステム中のファイル及びプロセスを改変するため、開発者により提供されるツールを利用しなければならない (shall)。 評価者は、それらの重要な失敗を作成することが、デバイスに最初のリス

トで特定される修正アクションを取らせる結果となることを検証しなければならない (shall)。

5.6.4 高信頼タイムスタンプ (FPT_STM)

FPT_STM.1	高信頼タイムスタンプ

FPT_STM.1.1 TSF は、自分自身で使用するために高信頼タイムスタンプを提供できなければならない (shall)。

保証アクティビティ：

評価者は、時刻を利用させる各セキュリティ機能が列挙されていることを保証するため、TSS を検査しなければならない (shall)。 TSS は、時刻に関連する各機能の文脈において、どのように時刻が維持管理され信頼性があるとみなされるかについての記述を提供する。本文書は、TSF が NTP サーバまたはキャリアのネットワーク時刻を主要な時刻のソースとして利用するかどうか識別しなければならない (must)。

評価者は、時刻を設定する方法が操作ガイダンスに記述されていることを保証するため、操作ガイダンスを検査する。

テスト 1 : 評価者は、操作ガイドを用いて時刻を設定する。次に評価者は、時刻が正しく設定されたことを観測するため、利用可能なインタフェースを利用しなければならない (shall)。

5.6.5 TSF 機能テスト (FPT_TST)

5.6.5.1 TSF 暗号機能テスト

FPT_TST_EXT.1	拡張：TSF 暗号機能テスト

FPT_TST_EXT.1.1 TSF は、すべての暗号機能の正しい動作を実証するため、初期の起動中 (電源投入時) に一連の自己テストを実行しなければならない (shall)。

適用上の注釈：本要件は、既知解テスト及び／またはペアワイズ一貫性テスト (pair-wise consistency tests)を実行することにより満たされてもよい。 自己テストは、暗号機能が行使される前に (例えば、その機能を利用するプロセスの初期化中に) 実行されなければならない (must)。

暗号機能には、FCS_COP の暗号操作、FCS_CKM の鍵生成機能、及び FCS_RBG_EXT のランダムビット生成が含まれる。

保証アクティビティ：

評価者は、起動時に行われる自己テストを TSS が特定されていることを保証するため、TSS を検査しなければならない (shall)。本記述には、TSF により実施されるテスト手続の概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを保証することによりメモリがテストされる」のような記述が使用されなければならない (shall)) が含まれなければならない (must)。 TSS には、自己テスト失敗の際に TSF が入り得る任意のエラー状態、及びそのエラー状態を抜けて通常動作を再開するために必要な条件とアクションが含まれなければならない (must)。評価者は、これらの自己テストが起動時に自動的に実行されること、そして利用者またはオペレータからの入力やアクションは一切必要とされないことが TSS に示されていることを検証しなければならない (shall)。

評価者は、TSS 中の自己テストのリストを検査して、これにアルゴリズム自己テストが含

まれることを検証しなければならない (shall)。アルゴリズム自己テストは、通常、既知解テストを用いて実施されることになる。

5.6.5.2 TSF 完全性テスト

FPT_TST_EXT.2	拡張：TSF 完全性テスト

FPT_TST_EXT.2.1 TSF は、可換 (mutable) メディアに保存された、アプリケーションプロセッサ OS カーネル、及び [選択：*可換メディアに保存されたすべての実行可能コード*、*[割付：その他の実行可能コードのリスト]*、*その他の実行可能コードなし*] でのブートチェインの完全性を、 [選択：*ハードウェア保護された非対称鍵を用いたデジタル署名*、*ハードウェア保護されたハッシュ*] を用いて実行する前に、検証しなければならない (shall)。

適用上の注釈：TSF のブートチェインは、ROM、ブートローダ、及びカーネルを含むファームウェア及びソフトウェアのシーケンスであって、どのプロセッサがそのコードを実行するかに関わらず、最終的にアプリケーションプロセッサ上のカーネルのロードに帰結するものである。

本要件を満たすために、ハードウェア保護は元来過渡的なものであってもよく：ハードウェア保護された公開鍵またはハッシュは、可換ブートローダコードを検証するために使用され、そのブートローダコードには可換 OS カーネルコードを検証するためにブートローダによって使用される鍵またはハッシュが含まれ、その可換 OS カーネルコードには次のレイヤーの実行可能コードを検証するための鍵またはハッシュが含まれる、などとなっていてもよい。

(最初の) 可換実行可能コードを検証するために使用される暗号メカニズムは、ハードウェアまたは読み出し専用メモリ (ROM) に実装されるなどして、保護されなければならない (must)。「可換メディア内のすべての実行可能コード」が検証される場合、ハードウェア内または読み出し専用メモリ内の実装は、当然の論理的帰結である。

現時点では、可換メディアに保存された、他のプロセッサ上で実行されるソフトウェアの検証は、要求されない；しかし、最初の割付で追加されてもよい。すべての実行可能コード (ブートローダ、カーネル、デバイスドライバ、プリロードされたアプリケーション、利用者によってロードされたアプリケーション、及びライブラリを含む) が検証される場合、「可換メディアに保存されたすべての実行可能コード」が選択されるべきである (should)。

本要件の文脈において、「ハードウェア保護された」とは、ソフトウェアをデジタル署名するために使用されるプライベート鍵が製造業者のプライベート鍵である場合、公開鍵を用いる署名の検証が成功するように、暗号技術的な値 (例えば、公開鍵またはハッシュ) がデバイスハードウェアにより不変の方法で 保存されることを意味する。この値は不許可暴露に対して保護される必要はなく、不許可改変に対してのみ保護されればよい。

保証アクティビティ：

評価者は、ST の TSS セクションに、TSF のアプリケーションプロセッサ用のソフトウェアの、ブートチェイン全体の記述を含め、ブート手続きの記述が含まれていることを検証しなければならない (shall)。 評価者は、オペレーティングシステム及びカーネル用のブートローダ及びカーネルをロードする前に、すべてのブートローダ及びカーネルソフトウェアそのものが暗号技術的に検証されることを保証しなければならない (shall)。 実行前に検証される追加の各カテゴリの実行可能コードについて、評価者は、TSS における記述が、そのソフトウェアが暗号学的に検証される方法について記述していることを検証しなければならない (shall)。

評価者は、検証されていない、または許可されていないソフトウェアによる改変を防止す

る暗号鍵またはハッシュの保護に対する正当化が TSS 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、暗号技術的な検証を行うメカニズムに与えられる保護の記述が TSS 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、ブート手順中に TOE 上で利用可能な補助ブートの各モードが 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、補助ブートの各モードについて、カーネル経由で実行されるコードの暗号技術的な完全性がそれぞれ実行前に検証されることの記述を検証しなければならない (shall)。

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、TSF ソフトウェアをロードさせるアクションを実行し、完全性メカニズムがいずれの実行可能形式も完全性エラーを含むフラグを立てず、TOE が正しくブートすることを観測しなければならない (shall)。

保証アクティビティの注釈 : 以下のテストは、消費者向けモバイルデバイス製品には通常含まれないツールを評価者へ提供するようなテストプラットフォームへのアクセスをベンダが提供することが必要とされる。

テスト 2 : 評価者は、完全性保護された TSF 実行可能形式を改変し、その実行可能形式の TSF によるロードを成功させようしなければならない (shall)。 評価者は、完全性違反が引き起こされ、TOE がブートしないことを観測する。(完全性違反が、そのモジュールが改変されたことでフォーマットが破損したために実行不可能となった事実によるものではなく、モジュールのロード失敗が原因であることを決定するために、十分に注意しなければならない (must))。

[条件付き] テスト 3 : ST 作成者が、完全性検証が公開鍵を用いて実行されると示している場合、評価者は、アップデートメカニズムが FIA_X509_EXT.1 に従い証明書の有効性確認を含むことを検証しなければならない (shall)。 評価者は、extendedKeyUsage フィールドにコード署名目的を持たない証明書を用いて TSF 実行可能形式をデジタル署名しなければならず、完全性違反が引き起こされることを検証しなければならない (shall)。 評価者は、コード署名目的を含む証明書を用いてテストを繰り返さなければならず、完全性検証が成功することを検証しなければならない (shall)。理想的には、その 2 つの証明書は、extendedKeyUsage フィールド以外は同一であるべきである (should)。

5.6.6 高信頼アップデート (FPT_TUD)

5.6.6.1 高信頼アップデート : TSF バージョン問い合わせ

FPT_TUD_EXT.1	拡張 : 高信頼アップデート : TSF バージョン問い合わせ

FPT_TUD_EXT.1.1 TSF は、TOE ファームウェア／ソフトウェアの現在のバージョンを問い合わせる能力を許可利用者へ提供しなければならない (shall)。

FPT_TUD_EXT.1.2 TSF は、デバイスのハードウェアモデルの現在のバージョンを問い合わせる能力を許可利用者へ提供しなければならない (shall)。

適用上の注釈 : デバイスのハードウェアモデルの現在のバージョンは、デバイスを構成するハードウェアを (製造業者の文書と連携して) 示すために十分な識別子である。

FPT_TUD_EXT.1.3 TSF は、インストールされたモバイルアプリケーションの現在のバージョンを問い合わせる能力を許可利用者へ提供しなければならない (shall)。

適用上の注釈 : モバイルアプリケーションの現在のバージョンは、インストールされた各モバイルアプリケーションの名称と公開されたバージョン番号である。

保証アクティビティ：

評価者は、モバイルデバイス、及び管理機能の利用方法を示す任意の支援ソフトウェアから構成される*テスト環境*を確立しなければはならない (shall)。 これは、開発者からのテストソフトウェア、開発者からの管理ソフトウェアの参照実装、または他の商用ソフトウェアであってもよい。 評価者は、提供されたガイダンス文書に従い管理機能を行使するためモバイルデバイスとその他のソフトウェアを設定しなければならない (shall)。

*テスト1：*提供された AGD ガイダンスを用いて、評価者は、管理者及び利用者が以下を問い合わせることができることをテストしなければならない (shall)：

- TSF オペレーティングシステム及び個別にアップデート可能なファームウェアの現在のバージョン
- TSF のハードウェアモデル
- すべてのインストールされたモバイルアプリケーションの現在バージョン

評価者は、ハードウェアモデルの識別子がデバイスを構成するハードウェアを特定するために十分であることを保証するため、製造業者の文書をレビューしなければならない (must)。

5.6.6.2 高信頼アップデート検証

FPT_TUD_EXT.2	**拡張：高信頼アップデート検証**

FPT_TUD_EXT.2.1 TSF は、アプリケーションプロセッサのシステムソフトウェア及び [選択： *[割付：その他のプロセッサのシステムソフトウェア]*、*その他のプロセッサのシステムソフトウェアなし*] へのアップデートを、それらのアップデートのインストール前に、製造業者によるデジタル署名を用いて、検証しなければならない (shall)。

適用上の注釈：デジタル署名メカニズムは、FCS_COP.1.1(3) に従い実装される。

現時点では、本要件は、アプリケーションプロセッサの外部で動作するソフトウェアへのソフトウェアアップデートの検証を要求していない。

サポートされるメカニズムを介した、不揮発性ストレージに常駐するソフトウェアへの任意の変更は、ソフトウェアアップデートとみなされる。つまり、ソフトウェアがデバイスへ届く方法または配付される方法に関わらず、本要件は TSF ソフトウェアアップデートに適用される。 これには、有線インタフェース経由でデバイスへ配付され得るソフトウェアを含むパーティションイメージと同様に無線経由 (OTA) のアップデートも含まれる。

FPT_TUD_EXT.2.2 TSF は、TSF ブート完全性 [選択：*鍵*、*ハッシュ*] を [選択：*絶対にアップデートしない*、*検証済みソフトウェアによってのみアップデートする*]ようにしなければならない(shall)。

適用上の注釈： 本要件によるアップデートされた鍵またはハッシュは、FPT_TST_EXT.2 での実行前にソフトウェアを検証するために使用される。 鍵またはハッシュは、アップデートにおけるデジタル署名の一部として検証され、また鍵またはハッシュのアップデートを実行するソフトウェアは FPT_TST_EXT.2 により検証される。

FPT_TUD_EXT.2.3 TSF は、TSF アップデート用に使用されるデジタル署名検証の鍵が [選択： *トラストアンカーデータベースにおける公開鍵に対して検証される*、*ハードウェア保護された公開鍵と一致する*] ことを検証しなければならない (shall)。

適用上の注釈：ST 作成者は、システムソフトウェアのアップデート用署名鍵が制限される

方法を示さなければならず (shall)、また FPT_TUD_EXT.2.3 で選択されている場合、この署名鍵がハードウェアでどのように保護されるかを示さなければならない (shall)。

証明書が使用される場合、証明書は、FIA_X509_EXT.1 に従いソフトウェアアップデートの目的のために検証され、また FIA_X509_EXT.2.1 で選択されるべきである (should)。さらに、FPT_TUD_EXT.2.6 が ST に含まれなければならない (must)。

本要件の文脈では、「ハードウェア保護された」は、ソフトウェアに署名するために使用されるプライベート鍵が製造業者のプライベート鍵である場合には公開鍵を用いた署名の検証が成功しないように、暗号技術的な値 (例えば、公開鍵またはハッシュ) がデバイスハードウェアにより変更不可能に保存されることを意味する。この値は、不許可暴露に対して保護される必要はなく、不許可改変に対してのみ保護されればよい。

保証アクティビティ：

評価者は、システムソフトウェアをアップデートするための TSF ソフトウェアアップデートメカニズムが ST の TSS セクションに記述されていることを検証しなければならない (shall)。 評価者は、その記述にインストール前のソフトウェアのデジタル署名検証が含まれることと、検証が失敗した場合にインストールが失敗することを検証しなければならない (shall)。 評価者は、TSF のアップデートに関わるすべてのソフトウェア及びファームウェアが記述されていること、また複数の段階とソフトウェアが示されている場合、各段階に関与するソフトウェア／ファームウェアが示され、アップデートの署名検証を実行する段階が識別されていることを検証しなければならない (shall)。

評価者は、デジタル署名が検証される方法と、署名の検証に使用される公開鍵がハードウェア保護されたものであるか、またはトラストアンカーデータベースの公開鍵へのチェインに対して検証されるたものかいずれかであることが TSS に記述されていることを検証しなければならない (shall)。 ハードウェア保護が選択された場合、評価者は、ハードウェア保護の方法が記述され、ST 作成者が不許可者により公開鍵が改変されない理由について正当化していることを検証しなければならない (shall)。

[条件付き] ST 作成者が、その他のプロセッサ上で実行中のシステムソフトウェアへのソフトウェアアップデートが検証されることを示している場合、評価者は、これらの他のプロセッサが TSS に列挙されていること、及びその記述が、アプリケーションプロセッサ上で実行中のソフトウェア用のアップデートメカニズムと異なる場合、これらのプロセッサ用のソフトウェアアップデートメカニズムを含むことを検証しなければならない (shall)。

[条件付き] ST 作成者が、ソフトウェアアップデートのデジタル署名検証用に公開鍵が使用されることを示している場合、評価者は、アップデートメカニズムが FIA_X509_EXT.1 に従い証明書の有効性確認を含み、extendedKeyUsage のコード署名目的のチェックを含むことを検証しなければならない (shall)。

評価者は、利用可能な各アップデートメカニズムについて以下のテストが実行された証拠資料を開発者が提供したことを検証しなければならない (shall) :

テスト 1 : 試験者は、デジタル署名のないアップデートのインストールを試行しなければならず (shall)、またインストールが失敗することを検証しなければならない (shall)。 試験者は、デジタル署名のあるアップデートのインストールを試行しなければならず、またインストールが成功することを検証しなければならない (shall)。

テスト 2 : 試験者は、デバイスにより許可されない鍵でアップデートに対してデジタル署名し、インストールが失敗することを検証しなければならない (shall)。 試験者は、許可された鍵でアップデートに対してデジタル署名し、インストールが成功することを検証しなけ

ればならない (shall)。

テスト 3: [条件付き] 試験者は、無効な証明書を用いてアップデートに対してデジタル署名しなければならず、アップデートのインストールが失敗することを検証しなければならない (shall)。 試験者は、コード署名目的を持たない証明書でアップデートに対してデジタル署名し、アプリケーションのインストールが失敗することを検証しなければならない (shall)。 試験者は、有効な証明書とコード署名目的を含む証明書を用いてテストを繰り返し、アプリケーションのインストールが成功することを検証しなければならない (shall)。

テスト 4 : [条件付き] 試験者は、最初の選択中に列挙された各プロセッサの上で実行されるソフトウェアについてこのテストを繰り返さなければならない (shall)。 試験者は、デジタル署名のないアップデートのインストールを試行しなければならず (shall)、そしてインストールが失敗することを検証しなければならない (shall)。 試験者は、デジタル署名のあるアップデートのインストールを試行し、インストールが成功することを検証しなければならない (shall)。

FPT_TUD_EXT.2.4 TSF は、モバイルアプリケーションソフトウェアをインストール前にデジタル署名メカニズムを用いて検証しなければならない (shall)。

適用上の注釈：本要件は、X.509v3 証明書または証明書の有効性確認を強制はしない。X.509v3 証明書と証明書有効性確認は、FPT_TUD_EXT.2.5 において対処される。

保証アクティビティ：

評価者は、モバイルアプリケーションソフトウェアがインストール時に検証される方法について TSS が記述していることを検証しなければならない (shall)。 評価者は、この方法がデジタル署名を使用していることを保証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書かくか、または開発者がアプリケーションを提供しなければならない (shall)。 評価者は、デジタル署名を持たないこのアプリケーションのインストールを試行し、インストールが失敗することを検証しなければならない (shall)。評価者は、デジタル署名されたアプリケーションのインストールを試行し、インストールが成功することを検証しなければならない (shall)。

5.7 クラス：TOE アクセス (FTA)

5.7.1 セションロック (FTA_SSL)

5.7.1.1 TSF 及び利用者起動によるロックされた状態

FTA_SSL_EXT.1	拡張：TSF 及び利用者起動によるロックされた状態

FTA_SSL_EXT.1.1 TSF は、非アクティブ時間間隔の後、ロックされた状態へ遷移しなければならない (shall)。

FTA_SSL_EXT.1.2 TSF は、利用者または管理者のいずれかによる起動の後、ロックされた状態へ遷移しなければならない (shall)。

FTA_SSL_EXT.1.3 TSF は、ロックされた状態への遷移に際して、以下の操作を実行しなければならない (shall) :

a) 表示デバイスの消去または上書きを行い、直前の内容を不可視化すること、

b) [割付：*ロックされた状態への遷移の際に実行されるその他のアクション*]。

適用上の注釈：非アクティブ時間間隔は、FMT_SMF_EXT.1 の機能 2.b を用いて設定され

る。 利用者／管理者起動によるロックは、FMT_SMF_EXT.1 の機能 8 で特定される。

保証アクティビティ：

評価者は、ロックされた状態への遷移の際に実行されるアクションについて TSS が記述していることを検証しなければならない (shall)。 評価者は、非アクティブ時間間隔の設定方法及びロックの指示方法について AGD ガイダンスが記述していることを検証しなければならない (shall)。 評価者は、不許可利用者に対して表示が許可されている情報について TSS が記述していることを検証しなければならない (shall)。

*テスト 1：*評価者は、AGD ガイダンスに従い、非アクティブ時間 (FMT_SMF_EXT.1) の経過後にロックされた状態へ遷移するよう TSF を設定しなければならない (shall)。 評価者は、TSF がロックするまで待ち、表示が消去または上書きされること、またロックされた状態で許可されるアクションのみがセションのロック解除されており、それらのアクションが FIA_UAU_EXT.2 に特定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、利用者と管理者の両方として、AGD ガイダンスに従い、TSF がロックされた状態への遷移するよう指示しなければならない (shall)。 評価者は、TSF がロックするまで待ち、表示が消去または上書きされること、ロックされた状態で許可されるアクションのみがセションのロック解除されており、それらのアクションが FIA_UAU_EXT.2 に特定されていることを検証しなければならない (shall)。

5.7.2 無線ネットワークアクセス (FTA_WSE)

FTA_WSE_EXT.1	拡張：無線ネットワークアクセス

FTA_WSE_EXT.1.1 TSF は、FMT_SMF_EXT.1 にて管理者により設定されるとおり、受け入れ可能なネットワークとして特定された無線ネットワークへの接続を試行できなければならない (shall)。

適用上の注釈：本要件の意図は、TSF が接続してもよいアクセスポイントを利用者及び管理者設定することを許可すること、及び利用者または管理者による明示的な許可なしに TSF が無線ネットワークへ接続することを防止することである。デバイスが登録される際、利用者が企業管理者により特定されたもの以外の無線ネットワークへの接続を禁止される場合､本管理機能が FMT_MOF_EXT.1.2 要件の選択に列挙されているべきである (should)。本管理機能が FMT_MOF_EXT.1.2 要件の選択に列挙されていない場合、利用者は、無線ネットワークの設定及び接続を行うため、管理者として管理機能を実行してもよい(may)。

保証アクティビティ：

本要件の保証アクティビティは、FMT_SMF_EXT.1 の保証アクティビティと組み合わせて実行される。

5.8 クラス：高信頼パス／チャネル (FTP)

5.8.1 高信頼チャネル通信 (FTP_ITC)

FTP_ITC_EXT.1	拡張：高信頼チャネル通信

FTP_ITC_EXT.1.1 TSF は、他の通信チャネルと論理的に分離され、そのエンドポイントの保証された識別を提供し、チャネルデータを暴露から保護し、チャネルデータの改変を検知するような、自身と他の高信頼 IT 製品との間の通信チャネルを提供するために、802.11-2012、802.1X、及び EAP-TLS、ならびに [選択、*少なくとも 1 つを選択： IPsec*、*TLS*、*DTLS*、*HTTPS プロトコル*] を利用しなければならない (shall)。

適用上の注釈：上記要件の必須部分の意図は、TOE とアクセスポイント、VPN ゲートウェイ、または他の高信頼 IT 製品との間の高信頼チャネルを確立し維持するため、要件で特定された暗号プロトコルを用いることである。

ST 作成者は、どの高信頼チャネルプロトコルがモバイルデバイスによって実装されているのかを列挙しなければならない (shall)。ST 作成者が IPsec を選択した場合、TSF は「IPsec 仮想プライベートネットワーク (VPN) クライアントのプロテクションプロファイル」に適合して認証されなければならない (shall)。附属書 B (訳注：「附属書 C 選択ベースの要件」が正しい。) には、その他のオプションの高信頼チャネルプロトコルのそれぞれを実装するための要件が含まれている。ST 作成者は、**FTP_ITC_EXT.1** において選択された高信頼チャネルプロトコルのセキュリティ機能要件を ST の本文中に含めなければならない (must)。

エンドポイントの保証された識別は、列挙された高信頼チャネルプロトコルによって使用される認証メカニズムに従って行われる。

FTP_ITC_EXT.1.2　TSF は、TSF が高信頼チャネルを介して通信を起動することを許可しなければならない (shall)。

FTP_ITC_EXT.1.3　TSF は、無線アクセスポイントへの接続、管理者としての通信、設定済みの企業接続、及び [選択：*OTA アップデート*、*その他の接続なし*] について、高信頼チャネルを介した通信を起動しなければならない (shall)。

適用上の注釈：将来的に、OTA アップデートについて高信頼チャネルが要求されることになる。

保証アクティビティ：

評価者は、要件で特定された暗号プロトコルの観点から、アクセスポイント、VPN ゲートウェイ、及び他の高信頼 IT 製品へ接続する TOE の詳細と、仕様に反映されていないかもしれない TOE 特有のオプションまたは手続きが記述されていることを決定するため、TSS を検査しなければならない (shall)。 評価者は、TSS に列挙されたすべてのプロトコルが ST の要件において特定され、含まれていることについても確認しなければならない (shall)。評価者は、アクセスポイント、VPN ゲートウェイ、及び他の高信頼 IT 製品への接続を確立するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。

OTA アップデートが選択される場合、TSS は、どの高信頼チャネルプロトコルが TOE によって開始されアップデートに利用されるかについて記述しなければならない (shall)。

また評価者は、列挙された各プロトコル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、操作ガイダンスに記述されるように接続を設定し、通信が成功することを保証することにより、TOE が 802.11-2012 及び事前共有鍵を用いて、アクセスポイントとの通信を起動できることを保証しなければならない (shall)。

*テスト 2：*評価者は、操作ガイダンスに記述されるように接続を設定し、通信が成功することを保証することにより、TOE が 802.11-2012、802.1x、及び EAP-TLS を用いてアクセスポイントとの通信を起動できることを保証しなければならない (shall)。

テスト 3：[条件付き] IPsec が選択される (及び TSF にネイティブな VPN クライアントが含まれる) 場合、評価者は、操作ガイダンスに記述されるように接続を設定し、通信が成功することを保証することにより、TOE が VPN ゲートウェイとの通信を起動できることを保証しなければならない (shall)。

*テスト 4：*その他の任意の選択されたプロトコル (かつ、テスト 1、2、または 3 でテスト

されていないもの) について、評価者は、操作ガイダンスに記述されるように接続を設定し、通信が成功することを保証することにより、TOE がそのプロトコルを用いて高信頼 IT 製品との通信を起動できることを保証しなければならない (shall)。

テスト 5 : OTA アップデートが選択される場合、評価者は、操作ガイダンスに従いアップデート要求を引き起こさなければならず (shall)、そしてその通信が成功することを保証しなければならない (shall)。

テスト 6 : 評価者は、正当な IT エンティティとの各通信チャネルについて、チャネルデータが平文では送信されないこと、そしてテスト対象のトラフィックとしてそのトラフィックがをプロトコルアナライザが特定することを保証しなければならない (shall)。

6. セキュリティ保証要件

セクション 4 の TOE のセキュリティ対策方針は、セクション 0 で識別された脅威に対抗するために構築された。セクション 5 のセキュリティ機能要件 (SFR) は、セキュリティ対策方針の形式的な実体化である。PP は、評価者が評価のために適用可能な文書を評定し、独立テストを実行する範囲を設定するため、セキュリティ保証要件 (SAR) を特定する。

本セクションには、本 PP に対する評価に必要とされる CC パート 3 の SAR 一式が列挙されている。 実行すべき個別の保証アクティビティ (保証アクティビティ) は、本セクションとセクション 5 の両方に特定されている。

本 PP に適合するよう作成された ST に対して、TOE の評価のための一般的モデルは、以下のとおりである：

評価用にとして ST が承認された後、ITSEF は、TOE と支援 IT 環境、及び TOE の管理者／利用者ガイドを取得する。ITSEF は､ASE 及び ALC の SAR に関して共通評価方法 (CEM) により義務付けられたアクションを実行すると期待されている。 ITSEF は、TOE において具体化される特定の技術に適用するため、他の CEM 保証要件の解釈として意図された、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。 セクション 5 で取り上げられた保証アクティビティは、TOE が PP に適合していることを実証するために開発者が何を提供する必要があるかについての明確化も提供している。

TOE のセキュリティ保証要件は、表 2 に識別される。

保証クラス	**保証コンポーネント**
セキュリティターゲット (ASE)	適合主張 (ASE_CCL.1)
	拡張コンポーネント定義 (ASE_ECD.1)
	ST 概説 (ASE_INT.1)
	運用環境のセキュリティ対策方針 (ASE_OBJ.1)
	主張されたセキュリティ要件 (ASE_REQ.1)
	セキュリティ課題定義 (ASE_SPD.1)
	TOE 要約仕様 (ASE_TSS.1)
開発 (ADV)	基本機能仕様 (ADV_FSP.1)
ガイダンス文書 (AGD)	利用者操作ガイダンス (AGD_OPE.1)
	準備手続き (AGD_PRE.1)
ライフサイクルサポート (ALC)	TOE のラベル付け (ALC_CMC.1)
	TOE CM 範囲 (ALC_CMS.1)
	タイムリーなセキュリティアップデート (ALC_TSU_EXT)
テスト (ATE)	独立テスト-サンプル(訳注：「独立テスト-適合」) (ATE_IND.1)
脆弱性評定 (AVA)	脆弱性調査 (AVA_VAN.1)

表 2：セキュリティ保証要件

6.1 ASE：セキュリティターゲット

ST は、CEM で定義される ASE アクティビティごとに評価される。さらに、TSS に含めるべき TOE の技術種別に特有の必要な記述を要求するような保証アクティビティがセクション 5 にて特定されているかもしれない。

6.2 ADV：開発

TOE に関する設計情報は、ST の TSS 部分、及び本 PP により要求される追加の情報であり公知とするべきでないもの (例えば、Entropy Essay) と同様に、エンドユーザに利用可能なガイダンス文書に含まれる。

6.2.1 基本機能仕様 (ADV_FSP)

機能仕様は、TOE のセキュリティ機能インタフェース (TSFI) を記述するものである。これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者により直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、そのようなインタフェースは間接的なテストしかできないことから、そのようなインタフェース自体を特定することにはあまり意味がない。本 PP では、このファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示されるインタフェースと、AGD 文書に提示されるインタフェースを理解することに焦点を絞る。セクション 5 に特定された保証アクティビティを満たすために、追加の「機能仕様」文書は必要とされない。

評価される必要のあるインタフェースは、独立した抽象的なリストよりむしろ、列挙された保証アクティビティを実行するために必要な情報を通して特徴づけされる。

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_OPE、AGD_PRE、及び起動に特権が要求されるような API を含め、アプリケーション開発者へ提供される API 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がアクセス可能なウェブサイトを参照してもよい。

API 文書には、本プロファイルで要求されるそれらのインタフェースが含まれなければならない (shall)。

API 文書には、利用可能な各機能がどの製品とバージョンに適用されるかを明示されなければならない (shall)。

機能要件における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) 証拠を示している；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 の追跡は、暗黙的にすでになされており、追加の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 機能仕様は、SFR 実施及び SFR 支援の各 TSFI に関連するすべてのパラメ

タを識別しなければなければならない (shall)。

ADV_FSP.1.3C 機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を提供しなければならない (shall)。

ADV_FSP.1.4C 追跡は、機能仕様での TSFI に対する SFR の追跡を実証するものでなければならない (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 に関連付けられた特定の保証アクティビティはない。 機能仕様書は、セクション 5 に記述された保証アクティビティ、及び AGD、ATE、及び AVA の SAR について記述されたその他のアクティビティを支援するために提供される。 機能仕様情報の内容に関する要件は、実施されるその他の保証アクティビティに基づいて暗黙的に評価される；評価者が、不十分なインタフェース情報のためにアクティビティを実施できない場合、適切な機能仕様が提供されなかったことになる。

6.3 AGD：ガイダンス文書

ガイダンス文書は、ST と共に提供される。 ガイダンスは、その運用環境がセキュリティ機能に関する役割を満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)。 その文書は、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、以下が含まれる：

- その環境において TSF を正常にインストールするための指示；及び
- 製品として、かつ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；及び
- 保護された管理者機能を提供するための指示。

特定のセキュリティ機能に関するガイダンスもまた、提供されなければならない (must)；そのようなガイダンスに関する要件は、各要件において特定された保証アクティビティに含まれている。

6.3.1 利用者操作ガイダンス (AGD_OPE)

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、単一の文書である必要はない。利用者、管理者及びアプリケーション開発者のためのガイダンスは、複数の文書またはウェブページに分散していてもよい。 必要に応じて、ガイダンス文書はセキュリティ自動化（訳注：SCAP）をサポートするためのセキュリティ設定チェックリスト記述形式 (XCCDF：eXtensible

Configuration Checklist Description Format) で表現される。

ここで情報を繰り返すのではなく、開発者は、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るため、本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するべきである (should)。これによって、受け入れ可能なガイダンスの準備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、管理者（例えば、MDM エージェント）、アプリケーション開発者が、利用者役割の定義において考慮されるべきである。

AGD_OPE.1.2C 利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごとに記述しなければならない (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を維持するために必要なことを識別しなければならない (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 の保証アクティビティ、及び CEM にしたがった TOE の評価により検証されることになる。以下の追加の情報についても必要となる。

操作ガイダンスには、最初からインストールされているアプリケーションと任意の関連するバージョン番号のリストが含まれなければならない (shall)。 任意のサードパーティベンダが、エンドユーザまたはエンタープライズによる購入前にアプリケーションをインストールすることが許可されるならば、このようなアプリケーションもまた列挙されなければならない (shall)。

操作ガイダンスには、TOE の評価された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含まれなければならない (shall)。TOE の CC 評価中に、評価もテストもされな

かった他の暗号エンジンの使用という警告が、管理者へ提供されなければならない (shall)。

その文書には、デジタル署名の検証により 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ていなければならない (must)。 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) :

46. アップデートそのものを取得するための指示。これには、アップデートが TOE へアクセス可能とするための指示 (例えば、特定のディレクトリへの格納) が含まれるべきである (should)。
47. アップデートプロセスを起動するための指示、及び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も。これには、ハッシュ／デジタル署名の生成が含まれる。

TOE が、本 PP での評価の適用範囲に含まれないセキュリティ機能を含むこともあるだろう。操作ガイダンスは、どのセキュリティ機能が保証アクティビティにより網羅されているかを管理者に対して明確にしなければならない (shall)。

6.3.2 準備手続き (AGD_PRE)

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、準備手続きに関して必要とされる内容を決定するために保証アクティビティを検査するべきである (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を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 に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない (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)*。

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：

上記概論で述べたように、特に TOE の機能要件を支援する運用環境の設定にあたり、その文書に関して多大な期待が存在する。 評価者は、TOE に関して提供されたガイダンスが、ST における TOE について主張されたすべてのプラットフォームに適切に対処していることを保証するため、チェックしなければならない (shall)。

6.4 ALC クラス：ライフサイクルサポート

本 PP に適合する TOE に関して提供される保証レベルにおいて、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よりもむしろ、ライフサイクルのエンドユーザの目に映る観点に限定される。 これは、製品の全般的な信頼度に寄与する開発者の実践が果たす重要な役割を軽減しようとするものではない；むしろ、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へ反映したものである。

6.4.1 TOE のラベル付け (ALC_CMC)

本コンポーネントは、TOE を同一ベンダの他の製品またはバージョンから区別でき、またエンドユーザにより調達される際に容易に指定できるように、TOE を識別することを目標としている。

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、その一意の参照でラベル付けされなければならない (shall)。.

評価者アクションエレメント：

ALC_CMC.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

保証アクティビティ：

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

6.4.2 TOE の CM 範囲 (ALC_CMS)

TOE の適用範囲とそれに関連した評価証拠の要件を考慮して、本コンポーネントの保証アクティビティは ALC_CMC.1 に関して列挙された保証アクティビティにより網羅される。

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：

本 PP において「SAR が要求する評価証拠」は、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 ST の情報との組み合わせに限定される。 TOE が具体的に識別され、その識別情報が ST 及び AGD ガイダンスの内容と一貫していることを (ALC_CMC.1 の保証アクティビティで行われるように) 保証することにより、評価者は、本コンポーネントにより要求される情報を暗黙的に確認する。

ライフサイクルサポートは、TSF 製造業者の開発及び構成管理プロセスの徹底した検査よりもむしろ、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対象としている。 これは、製品の全般的な信頼度寄与する開発者の実践が果たす重要な役割を軽減しようとするものではない；むしろ、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。

保証アクティビティ：

評価者は、開発者が (彼らのプラットフォーム用の公開の開発文書において) 開発者のプラットフォーム用アプリケーションの開発において利用に適した 1 つ以上の開発環境を識別していることを保証しなければならない (shall)。 これらの各開発環境について、開発者は、環境におけるバッファオーバーフロー保護メカニズムが確実に起動されることを保証するため、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、または明確に有効化されなければならないかについての指示についても本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 が一意に認識されること (その TSF ベンダからの他の製品との関連で)、及び ST 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)。

6.4.3 タイムリーなセキュリティアップデート (ALC_TSU_EXT)

本コンポーネントは、タイムリーな形でセキュリティ上の課題に対処するためエンドユーザデバイスがアップデートされる方法について、TOE 開発者が、他の必要な人々と協力して、情報を提供する必要がある。 その文書には、セキュリティ欠陥が報告／発見された時点からアップデートがリリースされる時点までのアップデートを公開提供するプロセスを記述する。 本記述には、関係者 (例えば、開発者、通信事業者) 、及びワーストケースの時間の長さを含めて、アップデートが公的に利用できる前に、実行される手順 (例えば、開発者のテスト、通信事業者のテスト) が含まれる。

開発者アクションエレメント：

ALC_TSU_EXT.1.1D 開発者は、TOE に対してタイムリーにセキュリティアップデートが行われる方法について、TSS に記述を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 記述には、TOE ソフトウェア／ファームウェアに対する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)。

適用上の注釈：記述されるべきソフトウェアには、アプリケーションプロセッサ及びベースバンドプロセッサのオペレーティングシステム、並びに任意のファームウェア及びアプリケーションが含まれる。 プロセス記述には、TOE 開発者のプロセスとともに、任意のサードパーティ (通信事業者) のプロセスが含まれる。 プロセス記述には、各展開メカニズム (例えば、無線経由のアップデート、通信事業者ごとのアップデート、ダウンロードされたアップデート) が含まれる。

ALC_TSU_EXT.1.2C 記述には、脆弱性の公開から TOE へのセキュリティアップデートの公開までの間の、日単位の時間の長さの期間を表明しなければならない (shall)。

適用上の注釈：全体の時間の長さは、クリティカルパス上の各当事者 (例えば、TOE 開発者、モバイル通信事業者) が消費する時間の長さの合計として提示されてもよい。 展開メカニズムごとに公的に利用可能となるまでの時間の長さは、異なるかもしれない；その場合、それぞれについて記述されること。

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)。

適用上の注釈：報告メカニズムには、ウェブサイト、電子メールアドレス、そして報告の機密性のある性質を保護するための手段（例えば、概念を実証するためだけのエクスプロイト（訳注：脆弱性を突いた攻撃プログラム））の詳細を暗号化するために用いることができる公開鍵) が含まれてもよい。

評価者アクションエレメント：

ALC_TSU_EXT.2.1E 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：

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、開発者により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、本記述が TOE の OS、ファームウェア、及びバンドルされたアプリケーションのそれぞれに対応していることを検証しなければならない (shall)。 評価者は、また、TOE 開発者のプロセスに加えて、任意のキャリアまたはその他

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)。 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について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各展開メカニズムについて、TSS が、脆弱性の公開から本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の公開利用可能までの時間を列挙し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明されていることを検証しなければならない (shall)。

評価者は、本記述に、TOE に関連するセキュリティ上の課題を報告するための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) が含まれることを検証しなければならない (shall)。 評価者は、本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用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方法が含まれることを検証しなければならない (shall)。

6.5 ATE クラス：テスト

テストは、システムの機能的側面、及び設計または実装の弱点を利用する側面とについて特定される。 前者は、ATE_IND ファミリにより行われるが、後者は、AVA_VAN ファミリにより行われる。 本 PP で指定された保証レベルにおいては、テストは宣伝された機能及びインタフェースに基づき、設計情報の可用性に依存して行われる。 評価プロセスの主要なアウトプットのひとつは、以下の要件において特定されるようなテスト報告書である。

API の多くは利用者インタフェース (例えば、タッチスクリーン) に露出されないため、必要なインタフェースを刺激する能力として、開発者のテスト環境が要求される。本テスト環境は、評価者が、例えば、API へアクセスし、消費者向けモバイルデバイス上では利用不可能なファイルシステム情報の閲覧を許可するものとなる。

6.5.1 独立テスト—適合 (ATE_IND)

テストは、TSS に記述された機能と提供された管理者文書 (設定及び操作を含む)に記述された機能とを確認するために実行される。 テストの焦点は、セクション 5 で特定された要件が満たされていることの確認であるが、いくつかの追加のテストがセクション 6 の SAR において特定されている。 保証アクティビティは、これらのコンポーネントに関連する追加のテストアクティビティを特定する。 評価者は、テスト計画及びテスト結果、ならびに本 PP への適合を主張するプラットフォーム／TOE の組み合わせに焦点を絞った範囲の論拠を文書化したテスト報告書を作成する。

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)*。

保証アクティビティ：

評価者は、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)。 テスト計画書は、CEM と本 PP の保証アクティビティ部分に含まれるすべてのテストアクションを網羅すること。保証アクティビティに列挙されたテストごとに 1 つのテストケースを用意する必要はないが、評価者は、ST において該当する各テスト要件が網羅されていることをテスト計画書において文書化しなければならない (must)。

テスト計画書は、テストされるプラットフォームが識別し、テスト計画書に含まれないが 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と。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、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 で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、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、それも記述されること。テストの一部として、または標準的なテスト前の条件のいずれかとして、各プラットフォームのインストレーション及び設定を評価者が AGD 文書に従って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が含まれてもよい。 各ドライバまたはツールについて、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論拠（単なる主張ではなく）が提供されるべきである (should)。 また、これには、使用さ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 によって特定され、評価される暗号プロトコル (IPsec, TLS/HTTPS, SSH) によって使用されるものである。

テスト計画書には、高レベルのテスト目的とそ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バージョンであってもよい）には、テスト手順が実行された際に行われたアクティビティが詳述され、また実際のテスト結果が含まれること。これは、累積的な記述でなければならず (shall)、したがって結果が失敗となったテスト実行があった場合；修正版がインストールされ；次に、テストの再実行が成功し、報告書には、単なる「成功」結果だけではなく、「失敗」と「成功」の結果 (及びその詳細説明) が示されることになる。

6.6 AVA クラス：脆弱性評定

本プロテクションプロファイルの第一世代については、評価機関は、これらの種別の製品にどのような脆弱性が発見されているのかを見付けるために公知の情報源を探索することを期待されている。 多くの場合、これらの脆弱性は、基本的な攻撃者を超えた高度な知識が要求される。 侵入テストツールが作成され、評価機関へ広く配付されるまでは、評価者は、TOE のこれらの脆弱性についてテストすることは期待されない。 評価機関は、ベンダが提供した文書から得られたこれらの脆弱性の可能性についてコメントすることを期待される。 この情報は、侵入テストツールの開発において、将来のプロテクションプロファイルの開発用に使用されることになる。

6.6.1 脆弱性調査 (AVA_VAN)

開発者アクションエレメント：

AVA_VAN.1.1D 開発者は、テストのための 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)。

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、公知の情報源の探索を*実行しなければならない (shall)*。

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：

ATE_IND と同様に、評価者は、本要件に関連する所見を文書化した報告書を作成しなければならない (shall)。 本報告書は、物理的に ATE_IND で言及された全般的なテスト報告書の一部であってもよいし、別文書であってもよい。 評価者は、ネットワーク基盤デバイス及び実装された一般的な通信プロトコルで発見されている脆弱性と、特定の TOE に関する脆弱性を決定するために公知の情報源の探索を実行する。 評価者は、報告書において、調べた情報源と発見された脆弱性を文書化する。 発見された各脆弱性について、評価者は、それが適用されないことを示す根拠を提供するか、または評価者が脆弱性を確認するためのテストを考案する（ATE_IND で提供されたガイドラインを利用）かのいずれか、適切な方を実行する。 適切さは、その脆弱性を利用するために必要とされる攻撃ベクトルを評定して決定される。 例えば、脆弱性の悪用が、専門的なスキル及び電子顕微鏡を必要とする場合、テストは適当ではなく、適切な正当化が系統的に説明されることになる。

A. 根拠

本 PP において、本文書の最初のセクションでは、モバイルデバイスによって対処される脅威；及び適合 TOE により達成される軽減の程度についての全般的な理解の向上を達成しようとして、物語調での説明を用いている。この説明のスタイルは、形式化された評価アクティビティにはそのまま適用できないため、本セクションでは表形式に加工して、本文書に関連付けられる保証アクティビティを説明する。

A.1 セキュリティ課題記述

A.1.1 前提条件

以下に列挙する具体的な条件が、TOE の運用環境に存在することが前提となる。これらには、TOE セキュリティ要件の開発における実質的な事実と TOE の使用における基本的環境条件の両方が含まれている。

前提条件の名称	前提条件の定義
A.CONFIG	接続されたネットワーク間を流れるすべての該当するネットワークトラフィックに TOE セキュリティポリシーが実施されるように、TOE のセキュリティ機能が正しく設定されることが前提となる。
A.NOTIFY	モバイル利用者は、モバイルデバイスが紛失または盗難にあった場合、即ちに管理者へ通知することが前提となる。
A.PRECAUTION	モバイル利用者は、モバイルデバイスの紛失または盗難のリスクを軽減するための予防措置を講ずることが前提となる。

表 3：TOE の前提条件

A.1.2 脅威

以下に列挙する脅威はモバイルデバイスによって対処され、またすべてのモバイルデバイスへ適用される。

脅威の名称	脅威の定義
T.EAVESDROP	無線通信チャネル上やネットワーク上のどこかに位置する場合、攻撃者は、モバイルデバイスと他のエンドポイントとの間で交換されるデータの監視やアクセスの取得ができるかもしれない
T.NETWORK	攻撃者は、モバイルデバイスを用いて通信を起動し、またはモバイルデバイスと他のエンドポイントとの間の通信を改変できるかもしれない。
T.PHYSICAL	利用者データ及びクレデンシャルの機密性の喪失は、攻撃者がモバイルデバイスへの物理的なアクセスを取得した結果として生じるかもしれない。
T.FLAWAPP	悪意のある、または悪用可能なコードが、開発者により意図的または意図せずに使用され、プラットフォームのシステムソフトウェアに対する攻撃の可能性を生じさせてしまうかもしれない。
T.PERSISTENT	攻撃者がデバイスへのアクセスを獲得し、持ち続けることによって、完全性の喪失と、敵対者と正当な所有者の両方による管理の可能性が生じる。

表 4：脅威

A.1.3 組織のセキュリティ方針

モバイルデバイスに特有の組織のセキュリティ方針は特定されていない。

A.1.4 セキュリティ課題定義の対応付け

以下の表は、本 PP で定義された脅威及び前提条件を、本 PP で定義または識別されたセキュリティ対策方針へマッピングしている。

脅威または前提条件	セキュリティ対策方針
A.CONFIG	OE.CONFIG
A.NOTIFY	OE.NOTIFY
A.PRECAUTION	OE.PRECAUTION
T.EAVESDROP	O.COMMS, O.CONFIG, O.AUTH
T.NETWORK	O.COMMS, O.CONFIG, O.AUTH
T.PHYSICAL	O.STORAGE, O.AUTH
T.FLAWAPP	O.COMMS, O.CONFIG, O.AUTH, O.INTEGRITY
T.PERSISTENT	O.INTEGRITY

表 5：セキュリティ課題定義の対応付け

A.2 セキュリティ対策方針

A.2.1 TOE のセキュリティ対策方針

以下の表には、モバイルデバイスに特有のセキュリティ対策方針が含まれている。

セキュリティ対策方針の名称	セキュリティ対策方針の定義
O.COMMS	TOE は、TOE の外部へ送信されるデータの機密性を保つ手段として、1 つ (または複数) の標準プロトコルを用いて通信を行う能力を提供する。
O.STORAGE	TOE は、TOE が保存するデータの機密性を保証するため、すべての利用者データ、企業データ及び認証鍵を暗号化する能力を提供する。
O.CONFIG	TOE は、セキュリティポリシーを設定し、適用する能力を提供する。これにより、モバイルデバイスが TOE が保存または処理する利用者データ及び企業データを保護できることを保証する。
O.AUTH	TOE は、適切な特権を持つ許可されたエンティティと通信していることを保証するため、利用者及び高信頼パスのエンドポイントを認証する能力を提供する。
O.INTEGRITY	TOE は、重要な機能、ソフトウェア／ファームウェア及びデータの完全性が保たれていることを保証するため、自己テストを実行する能力を提供する。TOE は、ダウンロードされたアップデートの完全性を検証する手段についても提供する。

表 6：TOE のセキュリティ対策方針

A.2.2 運用環境のセキュリティ対策方針

以下の表には、モバイルデバイスの運用環境に特有のセキュリティ対策方針が含まれている。

セキュリティ対策方針の名称	セキュリティ対策方針の定義
OE.CONFIG	TOE 管理者は、意図されたセキュリティポリシーを作成するため、モバイルデバイスのセキュリティ機能を正しく設定する。
OE.NOTIFY	モバイル利用者は、モバイルデバイスが紛失または盗難にあった場合、即ちに管理者へ通知する。
OE.PRECAUTION	モバイル利用者は、モバイルデバイスの紛失または盗難のリスクを軽減するための予防措置を講じる。

表 7：運用環境のセキュリティ対策方針

A.2.3 セキュリティ対策方針の対応付け

本 PP で特定または定義されたセキュリティ機能要件 (SFR) とセキュリティ対策方針との対応付けは、セクション 4 で提供される。

A.3 セキュリティ機能要件とカテゴリの対応付け

表 9 には、プロテクションプロファイルの使用を容易とするため、SFR の要約とカテゴリが含まれ、表 8 には、これらのカテゴリが定義されている。

表 8：カテゴリの定義

カテゴリ	定義
アルゴリズム	基本的な暗号アルゴリズム。
RBG	ランダムビット生成。
鍵	暗号鍵の管理、ストレージ、及び生成。
DAR 保護	保存データの保護及びワイプ。
認証	パスワード認証ファクタの利用とロック状態。
証明書	証明書有効性確認。
完全性	ソフトウェア完全性検証。
アクセス制御	ファイルアクセス制御。
悪用防止サービス	悪用を防止する TOE サービス。
監査	監査の生成及び格納。
管理	設定、ポリシー、コマンド、及びリモート管理。
高信頼チャネル	認証及び暗号化されたプロトコル及びネットワーキング。
Bluetooth 高信頼チャネル	Bluetooth ネットワーキングセキュリティ。
WLAN 高信頼チャネル	WLAN セキュリティ。

表 9：SFR とカテゴリの対応付け

要件	要約	カテゴリ
FCS_CKM.1(1)	鍵生成	アルゴリズム
FCS_CKM.2(1)	鍵確立	アルゴリズム
FCS_COP.1(1)	Advanced Encryption Standard	アルゴリズム
FCS_COP.1(2)	ハッシュ	アルゴリズム
FCS_COP.1(3)	デジタル署名	アルゴリズム
FCS_COP.1(4)	鍵付きハッシュ	アルゴリズム
FCS_COP.1(5)	パスワードベースの鍵導出関数	アルゴリズム
FCS_SRV_EXT.1	暗号サービス及びアプリ	アルゴリズム
FPT_TST_EXT.1	暗号自己テスト	アルゴリズム
FCS_RBG_EXT.1	ランダムビット生成	RBG
FCS_CKM_EXT.1	ルート暗号化鍵	鍵
FCS_CKM_EXT.2	データ暗号化鍵生成	鍵
FCS_CKM_EXT.3	鍵暗号化鍵生成	鍵
FCS_CKM_EXT.4	鍵の破棄	鍵
FCS_CKM_EXT.6	ソルト生成	鍵
FCS_IV_EXT.1	初期化ベクタ生成	鍵
FCS_STG_EXT.1	鍵ストレージ	鍵
FCS_STG_EXT.2	保存された鍵の暗号化	鍵
FCS_STG_EXT.3	保存された鍵の完全性	鍵
FPT_KST_EXT.1	平文鍵のストレージなし	鍵
FPT_KST_EXT.2	平文鍵の送信なし	鍵
FPT_KST_EXT.3	平文鍵のエクスポートなし	鍵
FCS_CKM_EXT.5	TSF のワイプ	DAR 保護
FDP_DAR_EXT.1	保存データ暗号化	DAR 保護
FDP_DAR_EXT.2	画面ロック保存データ暗号化	DAR 保護
FIA_UAU_EXT.1	復号に要求されるパスワード	DAR 保護
FIA_AFL_EXT.1	認証失敗時の取り扱い	認証
FIA_PMG_EXT.1	パスワード長／複雑性サポート	認証
FIA_TRT_EXT.1	認証の抑制	認証
FIA_UAU.7	あいまい化されたパスワード	認証
FIA_UAU_EXT.2	認証のタイミング	認証
FIA_UAU_EXT.3	再認証条件	認証
FTA_SSL_EXT.1	利用者及び TSF 手動のロック	認証
FTA_TAB.1	バナー	認証
FDP_STG_EXT.1	トラストアンカーデータベース	証明書
FIA_X509_EXT.1	証明書有効性確認のルール	証明書
FIA_X509_EXT.3	アプリへの証明書有効性確認サービス	証明書
FIA_X509_EXT.4	証明書の登録	証明書
FPT_NOT_EXT.1	自己テスト通知と失敗時のふるまい	完全性
FPT_TST_EXT.2	セキュアなブート	完全性
FPT_TUD_EXT.2	高信頼ソフトウェアアップデート	完全性
FDP_ACF_EXT.1	システムサービス及びファイルのアクセス制御	アクセス制御
FPT_AEX_EXT.1	アドレス空間配置ランダム化	悪用防止サービス

要件	要約	カテゴリ
FPT_AEX_EXT.2	メモリページのアクセス権限	悪用防止サービス
FPT_AEX_EXT.3	オーバーフロー保護	悪用防止サービス
FPT_AEX_EXT.4	ドメイン分離	悪用防止サービス
FPT_BBD_EXT.1	BP の AP 仲介	悪用防止サービス
FPT_STM.1	タイムスタンプ	監査
FAU_GEN.1	監査ログの生成	監査
FAU_SAR	監査レビュー	監査
FAU_SEL.1	選択的監査	監査
FAU_STG.1	監査格納の保護	監査
FAU_STG.4	監査データ損失の防止	監査
FMT_MOF_EXT.1.1	管理者の管理機能	管理
FMT_SMF_EXT.1	すべての管理機能	管理
FMT_SMF_EXT.2	登録解除の修正アクション	管理
FPT_TUD_EXT.1	TSF バージョン問い合わせ	管理
FCS_HTTPS_EXT.1	HTTPS プロトコル	高信頼チャネル
FCS_TLSC_EXT.2	TLS クライアントプロトコル	高信頼チャネル
FDP_IFC_EXT.1	VPN のスプリットトンネリングなし	高信頼チャネル
FDP_UPC_EXT.1	利用者データ高信頼チャネル通信	高信頼チャネル
FIA_X509_EXT.2	証明書の用途に関する要件	高信頼チャネル
FTP_ITC_EXT.1	TSF 高信頼チャネル通信	高信頼チャネル
FCS_DTLS_EXT.1	DTLS	高信頼チャネル
FIA_BLT_EXT.1	Bluetooth 利用者許可	Bluetooth 高信頼チャネル
FCS_CKM_EXT.7	Bluetooth 鍵生成	Bluetooth 高信頼チャネル
FDP_BLT_EXT.1	アプリによる Bluetooth デバイスアクセス	Bluetooth 高信頼チャネル
FIA_BLT_EXT.2	Bluetooth 認証	Bluetooth 高信頼チャネル
FPT_BLT_EXT.1	Bluetooth プロファイル制限	Bluetooth 高信頼チャネル
FCS_CKM.1(2)	WLAN 鍵生成 (PTK)	WLAN 高信頼チャネル
FCS_CKM.2(2)	WLAN 鍵配付 (GTK)	WLAN 高信頼チャネル
FCS_TLSC_EXT.1	EAP-TLS クライアントプロトコル	WLAN 高信頼チャネル
FIA_PAE_EXT.1	802.1x プロトコル	WLAN 高信頼チャネル
FTA_WSE_EXT.1	WLAN アクセス	WLAN 高信頼チャネル
FCS_CKM.1(3)	スイート B　WLAN 鍵生成 (PTK)	WLAN 高信頼チャネル

B. オプションの要件

本 PP の概論で示したように、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り実施されなければならない (must) もの）が本 PP の本文に含まれている。さらに、これ以外に 3 つの種別の要件が、附属書 B、C、及び D に特定されている。

最初の種別（本附属書）は、ST に含むことのできる要件であるが、TOE が本 PP への適合を主張するためには必須ではないものである。2 番目の種別（附属書 C）は、PP の本文の選択に基づく要件である； 特定の選択がなされた場合、当該附属書の追加の要件が含まれることが必須となる。3 番目の種別（附属書 D）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でのベースライン要件に含まれるであろうコンポーネントであり、モバイルデバイスのベンダによる採用が推奨される。 ST 作成者には、附属書 B、附属書 C、及び／または附属書 D に含まれる要件と関連するかもしれないが、列挙されていない要件（例えば、FMT 種別の要件）についても 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。

現時点では、オプションの要件は特定されていない。

C. 選択に基づいた要件

本 PP の概論で示したように、本 PP の本文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 の本文の選択に基づく追加の要件が存在し、特定の選択がなされた場合には、以下の追加の要件が含まれることが必須となる。

C.1 暗号鍵サポート (REK)

FCS_CKM_EXT.1	拡張：暗号鍵サポート

FCS_CKM_EXT.1.2： REK は、ハードウェアから読み出し、またはエクスポートできたりしてはならない (shall not)。

適用上の注釈：FCS_CKM_EXT.1.1 で「ハードウェア保護された」が選択される場合、FCS_CKM_EXT.1.4 が ST に含まれなければならない (must)。

インポートまたはエクスポート用の公開／文書化された API が存在しないことは、プライベートな／文書化されていない API が存在する場合、本要件を満たすには十分ではない。

保証アクティビティ：

本エレメントの保証アクティビティは、本コンポーネントの他のエレメントの保証アクティビティと組み合わせて実行される。

C.2 DTLS プロトコル (FCS_DTLS)

FCS_DTLS_EXT.1	DTLS プロトコル

FCS_DTLS_EXT.1.1 TSF は、DTLS 1.2 (RFC 6347) に従い、DTLS プロトコルを実装しなければならない (shall)。

FCS_DTLS_EXT.1.2： TSF は、DTLS 1.2 (RFC 6347) に従い、パリエーションが許可される場合を除き、DTLS の実装には TLS (FCS_TLSC_EXT.2) の要件を実装しなければならない (shall)。

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。

FCS_DTLS_EXT.1.3 TSF 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)。

適用上の注釈：有効性は、認証パス、有効期限、及び RFC 5280 に従う失効状態により決定される。

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ックを観測し、接続が成功しトラフィックが DTLS として識別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.2 に列挙された保証アクティビティと組み合わせて実行される。

証明書の有効性は、FIA_X509_EXT.1 のために実行されるテストに従い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わなければならない (shall)。

テスト 2 : 評価者は、有効な認証パスのない証明書の利用が当該機能の失敗という結果となることを実証しなければならない (shall)。 管理ガイダンスを用いて、評価者は、次にその機能で使われる証明書の有効性確認に必要な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実証しなければならない (shall)。 評価者は、次にこれらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない (shall)。

C.3 TLS クライアントプロトコル (FCS_TLSC)

C.3.1 EAP-TLS プロトコル

FCS_TLSC_EXT.1	**拡張 : EAP-TLS プロトコル**

FCS_TLSC_EXT.1.5 TSF は、Client Hello 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。

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) 並びに FCS_CKM.2(1) からの NIST 曲線に制限する。本拡張は、楕円曲線暗号スイートをサポートするクライアントについて必須である。

保証アクティビティ :

評価者は、Supported Elliptic Curves Extension、及び要求されるふるまいがデフォルトで実行されるかまたは設定可能のいずれであるかについて TSS に記述されていることを検証しなければならない (shall)。 本要件を満たすために Supported Elliptic Curves Extension が設定されなければならない (must) ことが TSS に示されている場合、評価者は、AGD ガイダンスに Supported Elliptic Curves Extension の設定が含まれていることを検証しなければならない (shall)。

評価者は、以下のテストについても実行しなければならない (shall) :

テスト : 評価者は、サポートされない ECDHE 曲線（例えば、P-192）を用いて TLS 接続中に ECDHE 鍵交換メッセージを実行するようにサーバを設定しなければならず (shall)、そして TOE がサーバの鍵交換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)。

C.3.2 TLS クライアントプロトコル

FCS_TLSC_EXT.2	拡張：TLS プロトコル

FCS_TLSC_EXT.2.5 TSF は、Client Hello 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。

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) 並びに FCS_CKM.2(1) からの NIST 曲線に制限する。本拡張は、楕円曲線暗号スイートをサポートするクライアントについて必須である。

保証アクティビティ：

評価者は、Supported Elliptic Curves Extension、及び要求されるふるまいがデフォルトで実行されるかまたは設定可能のいずれであるかについて TSS に記述されていることを検証しなければならない (shall)。 本要件を満たすために Supported Elliptic Curves Extension が設定されなければならない (must) ことが TSS に示されている場合、評価者は、AGD ガイダンスに Supported Elliptic Curves Extension の設定が含まれることを検証しなければならない (shall)。

評価者は、以下のテストについても実行しなければならない (shall)：

*テスト 1：*評価者は、サポートされない ECDHE 曲線 (例えば、P-192) を用いて TLS 接続中に ECDHE 鍵交換メッセージを実行するようサーバを設定しなければならず (shall)、そして TOE がサーバの鍵交換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) 。

C.4 TSF 完全性テスト (FPT_TST)

FPT_TST_EXT.2	拡張：TSF 完全性テスト

FPT_TST_EXT.2.2 TSF は、コード署名証明書が無効とみなされる場合、コードを実行してはならない (shall not)。

適用上の注釈：証明書は、オプションとして完全性検証のためのコード署名 (FPT_TST_EXT.2.1) に利用することができる。「完全性検証のためのコード署名」が FIA_X509_EXT.2.1 で選択されている場合、FPT_TST_EXT.2.2 が ST へ含まれなければならない (must)。

有効性は認証パス、有効期限、及び RFC 5280 に従う失効状態により決定される。

保証アクティビティ：

本エレメントのテストは、FPT_TST_EXT.2.1 の保証アクティビティと組み合わせて実行される。

C.5 高信頼アップデート (FPT_TUD)

FPT_TUD_EXT.2	拡張：高信頼アップデート検証

FPT_TUD_EXT.2.6 TSF は、コード署名証明書が無効とみなされる場合、そのコードをインストールしてはならない (shall not)。

適用上の注釈：証明書は、オプションとしてシステムソフトウェアアップデート (FPT_TUD_EXT.2.3) 及びモバイルアプリケーション (FPT_TUD_EXT.2.5) のコード署名に利用することができる。本エレメントは、いずれかのアップデートエレメントに証明書が利用される場合、ST に含まれなければならない (must)。 「システムソフトウェアアップデートのコード署名」または「モバイルアプリケーションのコード署名」が FIA_X509_EXT.2.1 で選択されている場合、FPT_TUD_EXT.2.6 が ST へ含まれなければならない (must)。

有効性は、認証パス、有効期限、及び RFC 5280 に従う失効状態により決定される。

保証アクティビティ：

このエレメントのテストは、FPT_TUD_EXT.2.3 及び FPT_TUD_EXT.2.5 の保証アクティビティと組み合わせて実行される。

D. オブジェクティブな要件

本附属書には、脅威に対抗するセキュリティ機能についても特定する要件が含まれている。これらの要件は、まだ商用化された技術において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。

D.1 クラス：セキュリティ管理 (FAU)

D.1.1 監査データの生成 (FAU_GEN)

FAU_GEN.1	監査データの生成

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない (shall)：

1. 監査機能の起動と終了；
2. すべての管理者アクション；
3. OS 及びカーネルの起動と終了；
4. リムーバブルメディアの挿入または取り出し；
5. 同期接続の確立；
6. 表 10 で具体的に定義された監査対象事象；
7. [選択：*監査記録が監査容量の [割付：100 未満の整数値] パーセントに到達したこと、 [割付：本プロファイルから導出されるその他の監査対象事象]*]。

適用上の注釈：監査データの生成は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない (shall)：

1. 事象の日付・時刻、
2. 事象の種別、
3. サブジェクト識別情報、
4. 事象の結果 (成功または失敗)；及び
5. 表 10 の追加情報。

適用上の注釈：サブジェクトの識別情報は、通常プロセス名／ID である。事象の種別は、例えば「info (情報) 」、「warning (警告) 」、または「error (エラー) 」などの、深刻度レベルにより示されることが多い。

保証アクティビティ：

評価者は、管理者ガイドをチェックし、管理者ガイドにすべての監査対象事象が列挙されており、また監査記録のフォーマットが提供されていることを保証しなければならない (shall)。 監査記録のフォーマットの各種別が、各フィールドの簡潔な記述とともに、網羅されなければならない (must)。 評価者は、PP により義務づけられたすべての監査事象の種別が記述され、またフィールドの記述には FAU_GEN.1.2 で要求される情報が含まれてい

ることを確実にするため、チェックしなければならない (shall)。

評価者は、管理セクションに列挙されるものを含め、本 PP の文脈において関連する管理者アクションの決定についても行わなければならない (shall)。 評価者は、管理者ガイドを検査し、本 PP で特定された要件を実施するために必要な TOE に実装されるメカニズムの設定（有効化及び無効化を含む）に、どの管理者コマンドが関連しているかの決定を行わなければならない (shall)。 評価者は、本 PP に関して管理者ガイドにおけるどのアクションがセキュリティ関連なのかを決定する際に採用した方法またはアプローチを文書化しなければならない (shall)。 評価者は、本アクティビティを、AGD_OPE ガイダンスが要件を満たしていることの保証と関連付けられたアクティビティの一部として実行してもよい (may)。

評価者は、提供された表に列挙された事象と管理者アクションに関する監査記録を TOE に生成させることにより、正しく監査記録を生成するための TOE の能力をテストしなければならない (shall)。これには、事象のすべてのインスタンスが含まれるべきである (should)。評価者は、ST に含まれる暗号プロトコルのそれぞれについて、チャネルの確立と終了に関して監査記録が生成されることをテストしなければならない (shall)。 管理者アクションについて、評価者は、本 PP の文脈においてセキュリティ関連であると上記のように評価者により決定された各アクションが監査対象であることをテストしなければならない (shall)。テスト結果を検証する際に、評価者は、テスト中に生成された監査記録が管理者ガイドで特定されたフォーマットと一致すること、及び各監査記録のフィールドが適切なエントリを有することを保証しなければならない (shall)。

評価者は、サポートされる補助モードのそれぞれにおける監査記録を正しく生成する TOE の能力を、そのモードにおいて利用可能な、できるだけ多くの TOE 機能を行使し、監査記録が正しく生成されることを保証することによって、テストしなければならない (shall)。

ここでのテストは、セキュリティメカニズムを直接テストすることと組み合わせて達成できることに注意されたい。 例えば、提供された管理者ガイダンスが正しいことを保証するために行われるテストは、AGD_OPE.1 が満たされることを検証し、監査記録が期待どおり生成されたことの検証に必要な管理者アクションの呼出しに対応するべきである (should)。

表 10：監査対象事象

要件	監査対象事象	追加監査記録の内容
FAU_GEN.1	なし。	
FAU_SAR.1	なし。	
FAU_SEL.1	監査収集機能が動作している間に生じた監査設定へのすべての改変。	追加の情報なし。
FAU_STG.1	なし。	
FAU_STG.4	なし。	
FCS_CKM_EXT.1	[選択：REK の生成、なし]	追加の情報なし。
FCS_CKM_EXT.2	なし。	
FCS_CKM_EXT.3	なし。	
FCS_CKM_EXT.4	なし。	
FCS_CKM_EXT.5	ワイプ（訳注：完全消去）の成功または失敗。	追加の情報なし。
FCS_CKM_EXT.6	なし。	
FCS_CKM_EXT.7	なし。	
FCS_CKM.1(1)	認証鍵の鍵生成の失敗。	追加の情報なし。
FCS_CKM.1(2)	なし。	

要件	監査対象事象	追加監査記録の内容
FCS_CKM.1(3)	なし。	
FCS_CKM.2(1)	なし。	
FCS_CKM.2(2)	なし。	
FCS_COP.1	なし。	
FCS_DTLS_EXT.1	証明書の有効性確認の失敗。	証明書の発行者名及びサブジェクト名。
FCS_HTTPS_EXT.1	証明書の有効性確認の失敗。	証明書の発行者名及びサブジェクト名。 [選択：利用者の許可判断、追加情報なし]。
FCS_IV_EXT.1	なし。	
FCS_RBG_EXT.1	ランダム化プロセスの失敗。	追加の情報なし。
FCS_SRV_EXT.1	なし。	
FCS_STG_EXT.1	鍵のインポートまたは破棄。 [選択：利用及び破棄ルールの例外、その他の事象なし]	鍵の識別情報。要求者の役割及び識別情報。
FCS_STG_EXT.2	なし。	
FCS_STG_EXT.3	保存された鍵の完全性検証の失敗。	検証されている鍵の識別情報。
FCS_TLSC_EXT.1	EAP-TLS セション確立の失敗。	失敗の理由。
	EAP-TLS セションの確立／終了。	接続の非 TOE エンドポイント。
FCS_TLSC_EXT.2	TLS セションの確立失敗。	失敗の理由。
	提示された識別子の検証の失敗。	提示された識別子及び参照識別子。
	TLS セションの確立／終了。	接続の非 TOE エンドポイント。
FDP_ACF_EXT.1	なし。	
FDP_BLT_EXT.1	なし。	
FDP_DAR_EXT.1	データの暗号化／復号の失敗。	追加の情報なし。
FDP_DAR_EXT.2	データの暗号化／復号の失敗。	追加の情報なし。
FDP_IFC_EXT.1	なし。	
FDP_STG_EXT.1	トラストアンカーデータバースへの証明書の追加または削除。	証明書のサブジェクト名。
FDP_UPC_EXT.1	アプリケーションによる高信頼チャネルの開始。	アプリケーション名。高信頼チャネルプロトコル。接続の非 TOE エンドポイント。
FIA_AFL_EXT.1	認証失敗回数の超過。	追加の情報なし。
FIA_BLT_EXT.1	Bluetooth デバイスの利用者による許可。 ローカルな Bluetooth サービスの利用者による許可。	利用者の許可判断。 デバイスの Bluetooth アドレス及び名称。 Bluetooth プロファイル。 ローカルサービスの識別情報。
FIA_BLT_EXT.2	Bluetooth 接続の開始。	デバイスの Bluetooth アドレス及び名称。
	Bluetooth 接続の失敗。	失敗の理由。
FIA_PAE_EXT.1	なし。	

要件	監査対象事象	追加監査記録の内容
FIA_PMG_EXT.1	なし。	
FIA_TRT_EXT.1	なし。	
FIA_UAU_EXT.1	なし。	
FIA_UAU_EXT.2	認証前に行われたアクション。	追加の情報なし。
FIA_UAU_EXT.3	パスワード認証ファクタの利用者による改変。	追加の情報なし。
FIA_UAU.7	なし。	
FIA_X509_EXT.1	X.509v3 証明書有効性確認の失敗。	有効性確認失敗の理由。
FIA_X509_EXT.2	失効状態を判断するための接続確立の失敗。	追加の情報なし。
FIA_X509_EXT.3	なし。	
FIA_X509_EXT.4	証明書登録要求の生成。	EST サーバの発行者及びサブジェクト名。認証の方法。認証に使用された証明書の発行者及びサブジェクト名。証明書要求メッセージの内容。
	登録の成功または失敗。	追加された証明書の発行者及びサブジェクト名または失敗の理由。
	EST トラストアンカーデータベースのアップデート。	追加されたルート CA のサブジェクト名。
FMT_MOF_EXT.1.1	なし。	
FMT_MOF_EXT.1.2	なし。	
FMT_SMF_EXT.1	設定の変更。	設定を変更した利用者の役割。新たな設定の値。
	機能の成功または失敗。	機能を実行した利用者の役割。行われた機能。失敗の理由。
	ソフトウェアアップデートの開始。	アップデートのバージョン。
	アプリケーションのインストールまたはアップデートの開始。	アプリケーションの名称及びバージョン。
FMT_SMF_EXT.2	登録解除。	管理者の識別情報。実行された修正アクション。
FPT_AEX_EXT.1	なし。	
FPT_AEX_EXT.2	なし。	
FPT_AEX_EXT.3	なし。	
FPT_AEX_EXT.4	TSF データ改変試行のブロック。	サブジェクトの識別情報。TSF データの識別情報。
FPT_BBD_EXT.1	なし。	
FPT_BLT_EXT.1	なし。	
FPT_KST_EXT.1	なし。	
FPT_KST_EXT.2	なし。	
FPT_KST_EXT.3	なし。	
FPT_NOT_EXT.1	[選択：TSF ソフトウェアの測定、なし]。	[選択：完全性検証の値、追加のデータなし]。
FPT_STM.1	なし。	
FPT_TST_EXT.1	自己テスト開始。自己テスト失敗。	失敗を生じたアルゴリズム。

要件	監査対象事象	追加監査記録の内容
FPT_TST_EXT.2	TOE の起動。	ブートモード。
	[選択：検出された完全性違反、なし]。	[選択：完全性違反を生じた TSF コードファイル、追加の情報なし]。
FPT_TUD_EXT.1	なし。	
FPT_TUD_EXT.2	ソフトウェアアップデートの署名検証の成功または失敗。	
	アプリケーションの署名検証の成功または失敗。	
FTA_SSL_EXT.1	なし。	
FTA_TAB.1	バナー設定の改変。	追加の情報なし。
FTA_WSE_EXT.1	アクセスポイントへ接続しようとするすべての試行。	アクセスポイントの識別情報。
FTP_ITC_EXT.1	高信頼チャネルの開始及び終了。	高信頼チャネルプロトコル。接続の TOE 以外のエンドポイント。

D.1.2 セキュリティ監査レビュー (FAU_SAR)

FAU_SAR.1	監査レビュー

FAU_SAR.1.1 TSF は、[**管理者**] が、[**すべての監査事象及び記録内容**] を監査記録から読み出せるようにしなければならない (shall)。

適用上の注釈：管理者は、監査記録の読み出しアクセスを有しなければならず (shall)、その読み出しアクセスはおそらく API を介して、または TOE 上に保存されたローカルな記録を企業の管理者がその記録を閲覧できる MDM サーバへ転送する MDM エージェントを経由して提供される。 本要件が ST に含まれる場合、FMT_SMF_EXT.1 の選択に機能 32 が含まれなければならない (shall)。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない (shall)。

保証アクティビティ：

本要件の保証アクティビティは､FMT_SMF_EXT.1 のテスト 32 と組み合わせて実行される。

D.1.3 セキュリティ監査事象選択 (FAU_SEL)

FAU_SEL.1	選択的監査

FAU_SEL.1.1 TSF は、以下のような属性に基づいて、すべての監査対象事象のセットから監査されるべき事象のセットを選択できなければならない (shall)：

a) 事象種別、

b) 監査対象セキュリティ事象の成功、

c) 監査対象セキュリティ事象の失敗、及び

d) [割付：*その他の属性*]。

適用上の注釈：本要件の意図は、監査事象を引き起こすために選択可能なすべての基準を

識別することである。 これは、利用者／管理者が呼び出す TSF 上のインタフェースを介して設定することができる。 ST 作成者は、割付を用いて任意の追加基準を列挙するか、または「なし」とする。

保証アクティビティ：

評価者は、ガイダンスにすべての事象の種別が列挙されていることと、要件に従って選択可能であるべきすべての属性が、割付中に列挙された属性を含め、記述されていることを保証するため、管理者ガイダンスをレビューしなければならない (shall)。 管理ガイダンスには、事前選択を設定する方法に関する指示についても含まれると共に、（存在する場合）複数の値の事前選択を行うための方法が説明されなければならない (shall)。 管理者ガイダンスには、現在実施されている選択基準に関わらず、常に記録されるそれらの監査記録についても識別されなければならない (shall)。

評価者は、以下のテストについても実行しなければならない (shall)：

*テスト 1：*本要件に列挙される各属性について、評価者は、その属性の選択が、記録されるべき属性を持つ監査事象（または、管理者ガイダンスで識別されるとおり、常に記録される監査事象）のみを生ずることを示すテストを考案しなければならない (shall)。

テスト 2：[条件付き] TSF がさらに複雑な監査事前選択基準（例えば、複数の属性、属性を用いた論理式）をサポートしている場合、評価者は、この機能が正しく実装されていることを示すテストを考案しなければならない (shall)。 評価者は、テスト計画書において、そのテストのセットが代表的なものであり、その機能を実行するのに十分であることを正当化する簡潔な説明を提供しなければならない (shall)。

D.1.4 セキュリティ監査格納 (FAU_STG)

FAU_STG.1	監査格納の保護

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない (shall)。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を防止できなければならない (shall)。

適用上の注釈：監査格納は、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

評価者は、不正な改変及び削除が防止されるように、すべてのログのロケーション及びこれらのファイルのアクセス制御が、TSS に列挙されていることを保証しなければならない (shall)。

*テスト 1：*評価者は、不正な利用者として監査証跡の削除を試行しなければならず (shall)、かつその試行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、不正なアプリケーションとして監査証跡の改変を試行しなければならず (shall)、かつその試行が失敗することを検証しなければならない (shall)。

FAU_STG.4	監査データ損失の防止

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、最も古くに格納された監査記録への上書きを行わなければならない (shall)。

適用上の注釈：監査格納は、2015 年の第 3 四半期以降に評価に入る製品について必須とな

る。

保証アクティビティ：

評価者は、監査記録のサイズ制限、監査証跡が満杯になったことの検出、及び監査証跡が満杯になったとき TSF によって取られる 1 つまたは複数のアクションが記述されていることを保証するため､TSS を検査しなければならない (shall)。評価者は､そのアクションが、最も古くに格納された記録の削除または上書きを起こすことを保証しなければならない (shall)。

D.2 クラス：暗号サービス (FCS)

D.2.1 暗号鍵の管理 (FCS_CKM)

D.2.1.1 暗号鍵生成 (WLAN)

FCS_CKM.1(3)	暗号鍵生成

FCS_CKM.1.1(3) TSF は、以下の[***IEEE 802.11ac-2013***]に合致する FCS_RBG_EXT.1 で特定されたランダムビット生成器を用いて、指定された暗号鍵生成アルゴリズム [***PRF-704***] 及び指定された暗号鍵長 [***256 ビット***] に従い、対称暗号鍵を生成しなければならない (shall)

適用上の注釈：IEEE 802.11ac-2013 (セクション 11.6.1.2) によって要求され WPA2 認定で検証される暗号鍵導出アルゴリズムは､HMAC-SHA-384 関数を用いて 704 ビットを出力する PRF-704 である。

本要件は、クライアントが認証された後にアクセスポイントとクライアントとの間の通信のために生成／導出される鍵にのみ適用される。これは PMK からの PTK の導出を指すものであり、本 PP で特定される RBG によって生成される乱数値、本 PP で特定される SHA-384 を用いた HMAC 関数、及びその他の情報を用いて行われる。これは、IEEE 802.11ac-2013 の主に 11 章に特定されている。

保証アクティビティ：

暗号プリミティブは､本 PP の別の場所で特定される保証アクティビティによって検証されることになる。評価者は、本 PP によって定義され実装されるプリミティブが無線クライアントへのセキュアな接続性を確立し維持するために TOE によって使用される方法が TSS に記述されていることを検証しなければならない (shall)。また TSS には、開発者の実装が暗号標準に準拠していることを保証する開発者の 1 つまたは複数の方法の記述が提供されなければならない (shall)。これには、開発組織によって行われたテストだけではなく、行われたサードパーティテスト (例えば WPA2 認定) が含まれる。評価者は、テスト方法論の記述が十分に詳細であって、プロトコル規定の詳細がテストされた範囲を判断できることを保証しなければならない (shall)。

評価者は、以下のテストについても実行しなければならない (shall) :

ステップ 1 - 評価者は、無線アクセスポイントと TOE との間にパケットスニフィングツールを用いなければならない (shall)。評価者は､パケットスニフィングツールをオンにして、アクセスポイントへの TOE の接続を成功させなければならない (shall)。

ステップ 2 - 評価者は､キャプチャされた 802.11 ビーコン及びプローブ応答メッセージ中で、サポートされている Authentication and Key Management (AKM) スイートとして 00-0F-AC:12 をアドバタイズし、またサポートされている暗号スイートとして 00-0F-AC:9 または 00-0F-AC:10 のいずれかを TOE がアドバタイズしていることを検証しなければなら

ない (shall)。

D.2.1.2 暗号鍵生成 (Bluetooth)

FCS_CKM_EXT.7	拡張：Bluetooth 鍵生成

FCS_CKM_EXT.7.1 TSF は、[割付：*新たな鍵ペア生成の頻度またはその基準あるいはその両方*] ごとに公開／プライベート ECDH 鍵ペアをランダムに生成しなければならない (shall)。

適用上の注釈：ECDH 鍵ペアを適切にフレッシュに保つための受け入れ可能な方法は、例えば 24 時間を超えて同一の鍵ペアが使われないような時間ベースのアプローチを含め、複数存在することだろう。あるいは、その基準は合格または失敗した認証試行の回数と関連しているかもしれない。合理的な認証試行ベースの置換基準を判断する出発点として、Bluetooth 規格 (v4.1, Vol. 2, 5.1) では、任意の BD_ADDR からの 3 回の認証試行失敗後、任意の BD_ADDR からの 10 回のペアリング成功後、または任意の 3 回のペアリング成功を 1 回のペアリング失敗と数えてこれらの組み合わせの後にデバイスのプライベート鍵を変更することによって、認証試行の繰返しを低減することを推奨している。

本要件は、セクション 5 に移動される予定であり、また 2015 年の第 3 四半期以降に評価に入る製品については、必須とされることになる。

保証アクティビティ：

評価者は、新たな ECDH 公開／プライベート鍵ペアを生成する頻度を決定するために使用される基準が TSS に記述されていることを保証しなければならない (shall)。特に、評価者はその実装が静的な ECDH 鍵ペアの使用を許可しないことを保証しなければならない (shall)。

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、以下の手順を実行しなければならない (shall) :

ステップ 1 - TOE をリモート Bluetooth デバイスとペアリングし、TOE によってその時点で使用中の公開鍵を記録する。(この公開鍵は、Bluetooth プロトコルアナライザを用いてペアリング中に交換されるパケットを検査することによって取得できる。)

ステップ 2 - 新たな ECDH 公開／プライベート鍵ペアを生成するために必要なアクションを行う。(このテストの手順は、新たな ECDH 公開／プライベート鍵ペアを生成する頻度を決定するために使用される基準がどのように TSS に記述されているかに依存することに注意されたい。)

ステップ 3 - TOE をリモート Bluetooth デバイスとペアリングし、TOE によってその時点で使用中の公開鍵を再び記録する。

ステップ 4 - ステップ 1 の公開鍵が、ステップ 3 の公開鍵と異なっていることを検証する。

D.2.2 ランダムビット生成 (FCS_RBG)

FCS_RBG_EXT.1	拡張：暗号操作 (ランダムビット生成)

FCS_RBG_EXT.1.4 TSF は、アプリケーションが SP 800-90A に定義される Personalization String を用いて決定論的 RBG へデータを追加することを許可しなければならない (shall)。

適用上の注釈：SP 800-90A で指定されるように、TSF はアプリケーションから入力されたデータを、FCS_RBG_EXT.1 によって要求されるエントロピーにカウントしてはならない

(shall not)。したがって、TSF は RBG シードへの唯一の入力がアプリケーションからのものとなることを許可してはならない (shall not)。

保証アクティビティ：評価者は、この機能が RBG へのインタフェースとして附属書 E によって要求される文書に含まれていること、及びこのインタフェースの呼び出しに続く RBG のふるまいが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、SP 800-90A が指定する DRBG への Personalization String の入力に関して、利用の条件と取り得る値が RBG の文書に記述されていることについても検証しなければならない (shall)。評価者は、以下のテストについても実行しなければならない (shall)。

*テスト 1：*評価者は、Personalization String を介して RBG へデータを追加するアプリケーションを書くか、または、開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。 評価者は、その要求が成功することを検証しなければならない (shall)。

FCS_RBG_EXT.1.5 TSF は、電源断時に決定論的 RBG の状態を保存しなければならず (shall)、また起動時にこの状態を決定論的 RBG への入力として用いなければならない (shall)。

適用上の注釈：電源断時に保存された状態を RBG への入力として追加する機能は、エントロピーの収集が低速な RBG が、リブートのたびに同一の出力を作成することを防止する。状態が保存される際に保護が提供されるという保証はない (あるいは、そのような保護に関する要件もない) ため、その状態は「既知」であるとみなされ、したがって RBG へのエントロピーには寄与できないが、RBG の初期値が予測できず悪用できないようにするために十分な変動を導入することはできる。

保証アクティビティ：

本要件の保証アクティビティは、附属書 E の RBG 文書中に取り込まれる。評価者は、次回起動時に利用できるようにするべくその状態を生成する方法、その状態が DRBG への入力としての利用方法、そして TOE が電源断の間にその状態に対して使用されるあらゆる保護対策が、その文書に記述されていることを検証しなければならない (shall)。

D.2.3 暗号アルゴリズムサービス (FCS_SRV)

FCS_SRV_EXT.1	**拡張：暗号アルゴリズムサービス**

FCS_SRV_EXT.1.2 TSF は、アプリケーションが、セキュアな鍵ストレージに保存された鍵によって、TSF が以下の暗号操作を実行するよう要求するメカニズムをアプリケーションに提供しなければならない(shall)：

- FCS_COP.1(1) におけるアルゴリズム
- FCS_COP.1(3) におけるアルゴリズム

これらは、セキュアな鍵ストレージに格納された鍵によるものとする。

適用上の注釈：将来、TOE は、TOE 上で動作するアプリケーションを含め、TOE 以外へ平文鍵材料を送信することが許されなくなる。 したがって TOE は、TOE のセキュアな鍵ストレージに格納された鍵を用い、アプリケーションを代行して暗号操作を行うことが要求されることになる。

保証アクティビティ：

評価者は、セキュアな鍵ストレージに関する API 文書に、格納された鍵による暗号操作が含まれることを検証しなければならない (shall)。

評価者は、TSF による格納された鍵の暗号操作を要求するアプリケーションを書くか、または、開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。 評価者は、操作から得られた結果が API 文書に従って期待される結果と一致することを検証しなければならない (shall)。 評価者は、FCS_STG_EXT.1 中の保証アクティビティに従ってセキュアな鍵ストレージの機能をテストするため、これらの API を利用しなければならない (shall)。

D.2.4 TLS クライアントプロトコル (FCS_TLSC)

D.2.4.1 EAP-TLS クライアントプロトコル

FCS_TLSC_EXT.1	拡張：EAP-TLS プロトコル

FCS_TLSC_EXT.1.6 TSF 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。

signature_algorithms 拡張のサポートは、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

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は signature_algorithm 拡張が設定されなければならない (must) ことが TSS に示されている場合、評価者は AGD ガイダンスに signature_algorithm 拡張の設定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：*評価者は、signature_algorithms 拡張のクライアント HashAlgorithm 一覧にしたがってサポートされていない TLS 接続において証明書を送信するようサーバを設定しなければならない (例えば、SHA-1 署名を持つ証明書を送信する) (shall)。 評価者は、サーバの証明書ハンドシェイクメッセージの受信後、TOE が接続を切ることを検証しなければならない (shall) 。

FCS_TLSC_EXT.1.7 TSF は、RFC 5746 に従って「renegotiation_info」TLS 拡張を使ってセキュアな再ネゴシエーションをサポートしなければならない (shall)。

FCS_TLSC_EXT.1.8 TSF は、ClientHello メッセージで [選択：以下より 1 つのみ選択：*renegotiation_info 拡張*、*TLS_EMPTY_RENEGOTIATION_INFO_SCSV 暗号スイート*] を含めなければならない (shall)。

適用上の注釈： RFC 5746 は、再ネゴシエーションのハンドシェイクを最初のハンドシェイクの暗号にバインドするような TLS への拡張を定義している。

選択に含まれる暗号スイートは、クライアントがその拡張をサポートしないサーバと互換性を持つための手段である。 クライアント実装が暗号スイートと拡張の両方をサポートすることが推奨されている。

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、2 つの TLS エンドポイント間のトラフィックをキャプチャするため、ネットワークパケットアナライザ／スニファを利用しなければならない (shall)。 評価者は、「renegotiation_info」フィールドまたは SCSV 暗号スイートのいずれかが、最初のハンドシェイク中の ClientHello パケットに含ま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、「renegotiation_info」拡張を含む最初のハンドシェイク中に受信された ServerHello メッセージのクライアントの取り扱いを検証しなければならない (shall)。 評価者は、ServerHello メッセージ中のこのフィールドの長さ部分を非ゼロとなるように改変し、クライアントが失敗を送信し接続を終了することを検証しなければならない (shall)。 評価者は、適切にフォーマットされたフィールドにより TLS 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 3 : 評価者は、セキュアな再ネゴシエーション中に受信された ServerHello メッセージに「renegotiation_info」拡張が含まれることを検証しなければならない (shall)。 評価者は、「client_verify_data」または「server_verify_data」のいずれかの値を改変し、クライアントが接続を終了することを検証しなければならない (shall)。

D.2.4.2 TLS クライアントプロトコル

FCS_TLSC_EXT.2	**拡張 : TLS プロトコル**

FCS_TLSC_EXT.2.6 TSF は、以下のハッシュアルゴリズムを含むような supported _signature_algorithms 値を伴う Client Hello の signature_algorithms 拡張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 によってのみサポートされている。

signature_algorithms 拡張のサポートは、2015 年の第 3 四半期以降に評価に入る製品について必須となる。

保証アクティビティ：

評価者は、signature_algorithm 拡張及び要求されるふるまいがデフォルトで実行されるかまたは設定可能かのいずれかであることが TSS に記述されていることを検証しなければならない (shall)。本要件を満たすように signature_algorithm 拡張が設定されなければならない (must) ことが TSS に示されている場合、評価者は、signature_algorithm 拡張の設定が AGD ガイダンスに含まれていることを検証しなければならない (shall)。

評価者は、以下のテストについても実行しなければならない (shall) :

- *テスト :* 評価者は、評価者は、signature_algorithms 拡張のクライアント HashAlgorithm 一覧にしたがってサポートされていない TLS 接続において証明書を送信するようサーバを設定しなければならない (例えば、SHA-1 署名を持つ証明書を送信する) (shall)。 評価者は、サーバの証明書ハンドシェイクメッセージの受信後、TOE が接続を切ることを検証しなければならない (shall) 。

FCS_TLSC_EXT.2.7 TSF は、RFC 5746 に従って「renegotiation_info」TLS 拡張の使用によるセキュアな再ネゴシエーションをサポートしなければならない (shall)。

FCS_TLSC_EXT.2.8 TSF は、ClientHello メッセージで [選択 : 以下より 1 つのみ選択 :

renegotiation_info 拡張、*TLS_EMPTY_RENEGOTIATION_INFO_SCSV 暗号スイート*] を含めなければならない (shall)。

適用上の注釈： RFC 5746 は、再ネゴシエーションのハンドシェイクを最初のハンドシェイクの暗号にバインドするような TLS への拡張を定義している。

選択に含まれる暗号スイートは、クライアントがその拡張をサポートしないサーバと互換性を持つための手段である。 クライアント実装が暗号スイートと拡張の両方をサポートすることが推奨されている。

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、2 つの TLS エンドポイント間のトラフィックをキャプチャするため、ネットワークパケットアナライザ／スニファを利用しなければならない (shall)。 評価者は、「renegotiation_info」フィールドまたは SCSV 暗号スイートのいずれかが、最初のハンドシェイク中の ClientHello パケットに含ま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、「renegotiation_info」拡張を含む最初のハンドシェイク中に受信された ServerHello メッセージのクライアントの取り扱いを検証しなければならない (shall)。 評価者は、ServerHello メッセージ中のこのフィールドの長さ部分を非ゼロとなるように改変し、クライアントが失敗を送信し接続を終了することを検証しなければならない (shall)。 評価者は、適切にフォーマットされたフィールドにより TLS 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 3：*評価者は、セキュアな再ネゴシエーション中に受信された ServerHello メッセージに「renegotiation_info」拡張が含まれることを検証しなければならない (shall)。 評価者は、「client_verify_data」または「server_verify_data」のいずれかの値を改変し、クライアントが接続を終了することを検証しなければならない (shall)。

D.3 クラス：利用者データ保護 (FDP)

D.3.1 アクセス制御 (FDP_ACF)

FDP_ACF_EXT.1	拡張：セキュリティ属性に基づいたアクセス制御

FDP_ACF_EXT.1.3 TSF は、アプリケーションがデバイス上のファイルへ書き込みと実行の両方のアクセス権限を与えることを禁止するアクセス制御ポリシーを実施しなければならない (shall)。

保証アクティビティ：

保証アクティビティの注釈：以下のテストは、消費者向けモバイルデバイス製品には通常含まれないツールを評価者へ提供するような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を必要としている。

*テスト 1：*評価者は、書き込みと実行の両方のアクセス権限を持つファイルの保存を試行するアプリケーションを書くか、または開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。評価者は、このアクションが失敗すること、及びファイル上のアクセス権限が同時に書き込み及び実行とならないことを検証しなければならない (shall)。

*テスト 2：*評価者は、書き込みと実行の両方のアクセス権限が設定されたファイルが全くないことを検証するため、各 TSF ファイル上のアクセス権限を検査して、ファイルシステムをトラバースしなければならない (shall)。

D.3.2 アプリケーション Bluetooth デバイスアクセス (FDP_BLT)

FDP_BLT_EXT.1	拡張：Bluetooth デバイスアクセスの制限

FDP_BLT_EXT.1.1 TSF は、特定のペアリング済み Bluetooth デバイスとの通信をできるアプリケーションを制限しなければならない (shall)。

適用上の注釈：Bluetooth を利用する特権を持つすべてのアプリケーションに対して、ペアリング済みすべての Bluetooth デバイスとの通信を許可すべきではない (should not)。 例えば、TSF は、現在の接続を開始したアプリケーションのみがそのデバイスとの通信を行えるか、またはペアリング済みデバイスを最初のペアリングに引き続いてそのデバイスへのソケット接続を行った最初のアプリケーションへ厳密に結合させるか、について要求するよう選択してもよい。さらに、より柔軟性を増すため、TSF は、そのデバイス上のどのアプリケーションがペアリング済みの各 Bluetooth デバイスと通信したり、通信を確認したりできるかを選択する方法を利用者へ提供することを選択してもよい。

保証アクティビティ：

評価者は、TOE 上の Bluetooth システムサービスへのアクセスを有するすべてのアプリケーション (FDP_ACF_EXT.1 に列挙されるように) による、ペアリング済み Bluetooth デバイス (またはそれらの通信データあるいはその両方) への無制限のアクセスを防止するメカニズムが TSS に記述されることを保証しなければならない (shall)。 評価者は、この方法が、アクセスを単一のアプリケーションに制約するか、またはペアリング済み Bluetooth デバイスと通信し得るアプリケーションの明示的なコントロールを提供するかのいずれかであることを検証しなければならない (shall)。

D.3.3 保存データの保護 (FDP_DAR)

現バージョンのセクション 0 にある必須要件では、保存データ保護の 2 つのレベルのみに対処している：TSF データと保護データ (及び鍵)。 2015 年の第 3 四半期以降に評価に入る製品については、保存データ保護の追加レベルが追加される：機微なデータ。 表 11 に、各レベルの保存データ保護について、要求される保護のレベルを示す。 FDP_DAR_EXT.2 要件が本体に含まれない場合、本要件が本体に含まれたとすれば機微なデータとみなされ得るデータを含め、すべての非 TSF データが保護データレベルで取り扱われる。これらのデータレベルに関する追加情報は、用語集 (セクション 1.2) に記載されている。

データレベル	要求される保護
TSF データ (TSF Data)	TSF データは機密性を要求しないが、完全性保護 (FPT_TST_EXT.2) は要求する。
保護データ (Protected Data)	保護データは、電源断の間、暗号化される。(FDP_DAR_EXT.1)
機微なデータ (Sensitive Data)	機微なデータは、ロック状態の間、暗号化される。(FDP_DAR_EXT.2)

表 11：データの保護レベル

すべての鍵、保護データ、及び機微なデータは、最終的に REK によって保護されなければならない (must)。 機微なデータは、REK に加えてパスワードによって保護されなければならない (must)。 特に、図 3 には、これらの要件に従って保護された KEK が含まれている：DEK_1 は、機微なデータに適しており、DEK_2 は、機微なデータに適していない、K_1 は、機微な鍵とはみなされず、そして K_2 は、機微な鍵とみなされる。

これらの要件は、ロック状態の間に受信された機微なデータを暗号化する機能が含まれる、ここで、機微なデータの別のサブカテゴリとみなされてもよい。 本機能は、パスワードから導出された KEK を用いて関連するプライベート鍵を保護しつつ、DEK を暗号化するために公開鍵を用いた鍵配送スキーム (RSA) により満たされてもよい。

本機能は、鍵共有スキームによって満たされてもよい。これを行うには、デバイスはデバイスワイドな機微なデータの非対称ペア (訳注：鍵ペア) (そのプライベート鍵は、パスワードから導出された KEK により保護される) 及び受信された機微なデータを保存するための非対称ペア (訳注：鍵ペア) を生成する。機微なデータを保存するため、デバイスワイドな公開鍵及びデータプライベート鍵が、KEK または DEK として利用可能な共有秘密の生成に使用される。データプライベート鍵と共有秘密は、データが暗号化され、データ公開鍵が保存された後、消去される。したがって、ロック状態では、新たに保存されたデータを復号するために鍵材料は利用できない。ロック解除時に、デバイスワイドプライベート鍵が復号され、これをデータ公開鍵と共に用いて共有秘密が再生成され、保存されたデータが復号される。下の図 4 で、この方式が説明されている。

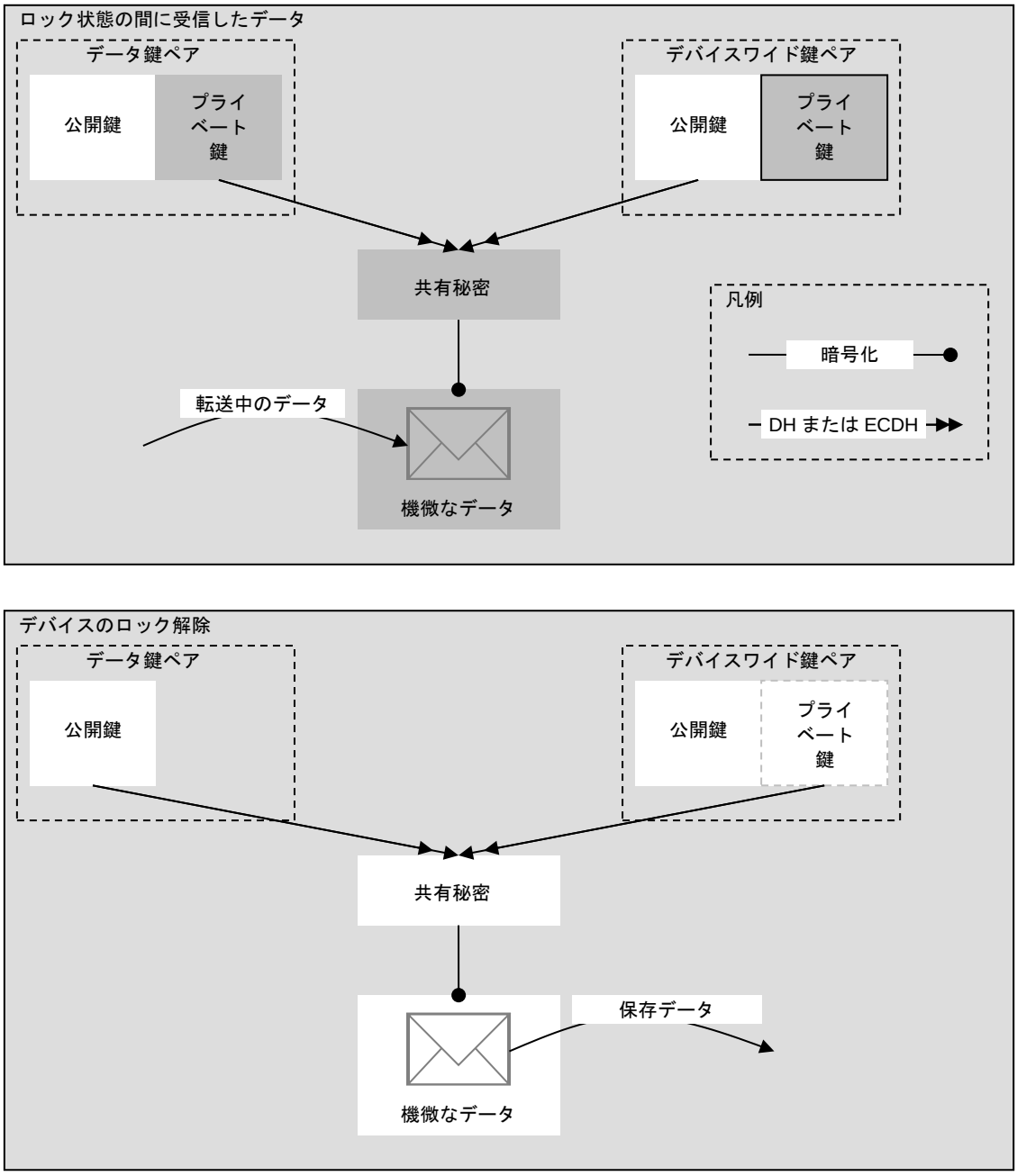

図 4：ロック状態で受信された機微なデータを暗号化するための鍵共有スキーム

FDP_DAR_EXT.2	**拡張：機微なデータの暗号化**

FDP_DAR_EXT.2.1 TSF は、データ及び鍵を機微としてマークするためのメカニズムをアプリケーションに提供しなければならない (shall)。

適用上の注釈：機微とマークされたデータ及び鍵は、モバイルデバイスのロック状態とロック解除状態の両方において、(他の要件によって) 一定の制約対象となる。 本メカニズムにより、アプリケーションは自分の制御下でこれらのデータ及び鍵を、それらの要件の対象として選択できるようになる。

将来、本 PP ではアプリケーションによって作成されたすべてのデータ及び鍵がデフォルト

で「機微」マーキングされることを要求し、明示的な「機微」マーキングではなく明示的な「機微でない」マーキングを要求するかもしれない。

保証アクティビティ：

評価者は、TSF により保存されるどのデータが (純正アプリケーション等によって) 機微と取り扱われるかの記述が TSS に含まれることを検証しなければならない (shall)。本データは、利用者またはエンタープライズデータの全部または一部が含まれるかもしれず、また電子メール、連絡先、カレンダー項目、メッセージ、及び文書の保護レベルに関して具体的でなければならない (must)。

評価者は、データ及び鍵を機微とマークするために使用するアプリケーションに提供されるメカニズムが TSS に記述されていることを決定するため、TSS を検査しなければならない (shall)。 本記述は、このような方法でマークされたデータ及び鍵がマークされないデータ及び鍵とどのように区別されるのか (例えば、タグ付け、メモリまたはコンテナの「特別」領域での分離、等) を反映した情報についても含まれていなければならない (shall)。

*テスト 1：*評価者は、AGD ガイダンスに従って機微なデータの暗号化を有効化し、利用者認証を要求しなければならない (shall)。 評価者は、その他の利用者との対話が要求されないことを検証するために、 (ST で定義されるとおりに、かつファイルの作成または機微なデータを生成するアプリケーションの利用のいずれかにより) 機微なデータの生成とアクセスを試行しなければならない (shall)。

FDP_DAR_EXT.2.2　TSF は、製品がロックされている間に受信された機微なデータを暗号化し保存するため、非対称鍵スキームを使用しなければならない (shall)。

適用上の注釈：機微なデータは、FDP_DAR_EXT.1.2 に従って暗号化される。非対称鍵スキームは、FCS_CKM.2(1) に従って実行されなければならない (must)。

本要件の意図は、デバイスがロックされている間に機微なデータを受信でき、ロック状態にある間に権限のない人物が復号できないような形で受信したデータを保存できるようにすることである。機微なデータのサブセットのみがロック状態で受信し得る場合、このサブセットが TSS に記述されなければならない (must)。

鍵材料は、FCS_CKM_EXT.4 に従ってもはや必要なくなったときに消去されなければならない (must)。ロック状態で受信された機微なデータを保護する鍵 (またはこれらの鍵を導出するために使用される鍵材料) については、「もはや必要なくなったとき」には「ロック状態にある間」が含まれる。例えば、最初の鍵スキームでは、これには受信したデータを保護する DEK が、データが暗号化され次第、含まれる。2 番目の鍵スキームでは、これにはデータ非対称ペアのプライベート鍵、生成された共有秘密、及び生成された任意の DEK が含まれる。もちろん、両方のスキームで非対称ペアのプライベート鍵 (それぞれ、RSA プライベート鍵及びデバイスワイドプライベート鍵) は、ロック状態への移行の際に消去されることが必要とされる。

保証アクティビティ：

評価者は、デバイスがロック状態にある間に機微なデータを受信するプロセスの記述が TSS に含まれていることを決定するため、ST の TSS セクションをレビューしなければならない (shall)。評価者はその記述に、ロック状態中に受信され得る機微なデータが、ロック状態中に受信できない機微なデータと異なって取り扱われるかどうか示されていることについても検証しなければならない (shall)。本記述は、受信されたデータの暗号化及び保存に使用される鍵スキームが含まなければならず (shall)、その鍵スキームは非対称鍵を含むものでなければならず (must) 、また (適用上の注釈に記述されるように) データの導出

または暗号化に使用されるすべての鍵材料をワイプすることによって機微な保存データが復号されることを防止するものでなければならない (must)。本セクションの導入部で要件を満たす 2 つの異なるスキームを提供したが、その他のソリューションによって本要件へ対処してもよい。

評価者は、ロック状態にある間に、もはや不要となったすべての鍵材料についてFCS_CKM_EXT.4 のテストを実行しなければならず (shall)、また非対称スキームの鍵はロック状態への移行の際に実行されるテストにおいて対処されることを保証しなければならない (shall)。

FDP_DAR_EXT.2.3 TSF は、FCS_STG_EXT.2.1 の選択 2 に従って、機微なデータの保護に使用された非対称鍵の任意の保存されたプライベート鍵及び任意の保存された対称鍵を暗号化しなければならない (shall)。

適用上の注釈：TSF がロック解除状態にある間に機微なデータの暗号化に使用される対称鍵は、REK 及びパスワードから導出された KEK によって暗号化され (または、それらによって暗号化された KEK へチェインし) なければならない (must)。ロック状態でデータの暗号化に使用される非対称鍵スキームの保存されたプライベート鍵は、REK 及びパスワードから導出された KEK によって暗号化され (または、それらによって暗号化された KEK へチェインし) なければならない (must)。

保証アクティビティ：

評価者は、FCS_STG_EXT.2.1 のために要求される TSS の鍵階層構造セクションに、機微なデータの暗号化に使用される対称暗号鍵 (DEK) 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、これらの DEK が REK 及びパスワードから導出された KEK によって暗号化され (または、それらによって暗号化された KEK へチェインし) た鍵によって暗号化されることを保証しなければならない (shall)。

評価者は、非対称鍵スキームを記述する ST の TSS セクションに、非対称ペアの任意のプライベート鍵の保護が含まれることを検証しなければならない (shall)。 評価者は、ワイプされず TSF によって保存される任意のプライベート鍵が、REK 及びパスワードから導出された KEK によって暗号化され (または、それらによって暗号化された KEK へチェインし) た鍵によって暗号化されて保存されることを保証しなければならない (shall)。

FDP_DAR_EXT.2.4 TSF は、ロック状態にある間に受信された機微なデータを、ロック解除状態への移行の際に、非対称鍵スキームを用いて復号しなければならず (shall)、また対称鍵スキームを用いてその機微なデータを再度暗号化しなければならない (shall)。

保証アクティビティ：

評価者は、非対称鍵スキームを記述する ST の TSS セクションに、ロック解除状態への移行の際に TSF によって DAR の目的で取られるアクションの記述が含まれることを検証しなければならない (shall)。これらのアクションには少なくとも、非対称鍵スキームを用いてすべての受信されたデータの復号が行われること、及びデバイスがロック解除状態にある間にデータの保存に使用される対称鍵スキームを用いて再度暗号化が行われることが含まれなければならない (shall)。

D.4 クラス：識別と認証 (FIA)

D.4.1 Bluetooth の許可と認証 (FIA_BLT)

D.4.1.1 Bluetooth 利用者許可

FIA_BLT_EXT.1	拡張：Bluetooth 利用者許可

FIA_BLT_EXT.1.2 TSF は、以下の Bluetooth プロファイル： [割付：*Bluetooth プロファイルのリスト*] と関連付けられたサービスへの高信頼リモートデバイスのアクセスを許可する前に明示的な利用者許可を要求しなければならず (shall)、また以下の Bluetooth プロファイル： [割付：*Bluetooth プロファイルのリスト*] と関連付けられたサービスへの信頼できないリモートデバイスのアクセスを許可する前に明示的な利用者の許可を要求しなければならない (shall)。

適用上の注釈：ペアリングに加えて、特定のリモートデバイスによる特定の Bluetooth サービスへのアクセスを許可する明示的な利用者のアクションを要求することが適切であるかもしれない。TSF は、この追加のアクションをすべてのデバイスについて要求するか、または要求される信頼のレベルを有しないデバイスにのみ要求するか、選んでもよい。

TSF は、特定のデバイスを TOE との高信頼デバイス関係を持つものとして指定し、それらにすべてのサービスへの「包括的 (blanket)」アクセスを許可するかもしれない。しかし、そうではなく、それぞれのサービスについてその特定のサービスを利用することが信頼されたデバイスのリストを TSF が維持管理することが強く推奨される。

さらに、TSF は特定のサービスについてデバイスを、利用者がそのデバイスにそのサービスを利用する明示的な許可を与えた後で、信用されないカテゴリから高信頼カテゴリへ移動させることもあるかもしれない。例えば、初めてオブジェクト転送のためにリモートデバイスが OBEX サービスを使う前に、利用者が明示的で手作業での許可を与えるよう要求することが適切であるかもしれない。利用者には、その特定のデバイスによるそのサービスへの将来の接続を、毎回明示的な許可を要求せずに許可するオプションが提示されるかもしれない。

ST 作成者は、リモートデバイスがアクセスを取得する前に明示的な利用者の許可が必要とされるすべての Bluetooth プロファイル及びサービスを列挙しなければならない (shall)。そのサービスについてデバイスが TOE との信頼関係を有するかどうかに応じてふるまいの違いが存在する場合には、それが特定されなければならない (must)。

保証アクティビティ：

評価者は、本要件に従って保護されるサービス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、サービスが TOE 上のアプリケーションによってアクティブに使用中である間に、そのサービスを利用するために要求される信頼のレベルを有さないリモートデバイスから (要件の 2 番目のリストにある) 「保護された」Bluetooth サービスへのアクセスの取得を試行しなければならない (shall)。 評価者は、TOE によって利用者へ、その特定のリモートデバイスにサービスへのアクセスを許すための許可が明示的に求められることを検証しなければならない (shall)。 評価者は、TOE 上で許可を拒否し、サービスへアクセスするためのリモート試行が許可の欠如のため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、テスト 1 を繰り返し、権限付与を許可し、リモートデバイスがサービスへのアクセスに成功することを検証しなければならない (shall)。(信頼されないリモートデバイスが TOE とまだペアリングされたことがない場合、本接続はペアリングを要求してもよいことに注意されたい。)

*テスト 3：*利用者の許可が要求されるかどうか決定するにあたり、TSF の実装が信頼されたデバイスと信頼されないデバイスとを区別している場合、要件の 2 番目のリスト中に表れる (最初のリストではなく) サービスと、そのサービスを利用するために要求される信頼のレベルを有するデバイスを用いて、テスト 1 を繰り返す。評価者は、利用者が明示的な許

可のためにプロンプト表示されないこと、及びサービスへの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 : 利用者の許可が要求されるかどうか決定するにあたり、TSF の実装が信頼されたデバイスと信頼されないデバイスとを区別している場合、要件の最初のリスト中に表れるサービスと、そのサービスを利用するために要求される信頼のレベルを有するデバイスを用いて、テスト 1 を繰り返す。 評価者は、利用者がその特定のリモートデバイス用のサービスへのアクセスを許すために、TOE による許可が明示的に求められることを検証しなければならない (shall)。 評価者は、TOE 上で許可を拒否し、許可がないためにサービスへアクセスするためのリモートからの試行が失敗することを検証しなければならない (shall)。

テスト 5 : 利用者の許可が要求されるかどうか決定するにあたり、TSF の実装が信頼されたデバイスと信頼されないデバイスとを区別している場合、要件の最初のリスト中に表れるサービスと、そのサービスを利用するために要求される信頼のレベルを有するデバイスを用いて、テスト 2 を繰り返す。 評価者は、利用者が明示的に許可を提供した場合、そのリモートデバイスがサービスへのアクセスに成功することを検証しなければならない (shall)。

D.4.1.2 Bluetooth 認証

FIA_BLT_EXT.1	**拡張：Bluetooth 認証**

FIA_BLT_EXT.2.1 TSF は、Bluetooth リンク上でのあらゆるデータ転送の前に、デバイス間の Bluetooth 相互認証を要求しなければならない (shall)。

適用上の注釈：デバイスがペアリング済みでない場合、ペアリング処理が開始されなければならない (must)。デバイスがペアリング済みの場合、あらゆるデータがリンク上を通過する前に現在のリンク鍵に基づく相互認証が成功しなければならない (must)。

保証アクティビティ：

評価者は、Bluetooth ペアリングが完了する前に、任意の種別のデータ転送が防止される方法について TSS に記述されていることを保証しなければならない (shall)。 TSS には、任意のサポートされる RFCOMM 及び L2CAP データ転送メカニズムが明確に記述されなければならない (shall)。 評価者は、Bluetooth デバイスがペアリングされ相互認証された後にのみデータ転送が完了されることを保証しなければならない (shall)

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、OBEX Object Push サービスを用いた TOE ファイルへのアクセスを試行するために Bluetooth ツールを利用し、アクセスが許される前に TOE によりペアリングと相互認証が要求されることを検証しなければならない (shall)。 (OBEX Object Push サービスが TOE 上でサポートされない場合、Bluetooth L2CAP 及び／または RFCOMM 上でデータを転送する異なるサービスが本テストで使用されてもよい。)

FIA_BLT_EXT.2.2 TSF は、現在の接続がすでに存在する Bluetooth デバイスアドレス (BD_ADDR) からの接続試行を破棄しなければならない (shall)。

適用上の注釈：TOE がすでにリモート Bluetooth デバイスとの接続を有する場合、同じ Bluetooth デバイスアドレスを主張するデバイスからの新たな接続試行は悪意のある可能性があり、拒否／無視されるべきである (should)。 単一のリモート BD_ADDR へは、同時に 1 つの接続のみがサポートされる。

本要件は、セクション 5 に移動される予定であり、また 2015 年の第 3 四半期以降に評価に入る製品については、必須とされることになる。

保証アクティビティ：

評価者は、同じ Bluetooth デバイスアドレスを持つ 2 つのデバイスが同時に接続されることなく、また最初の接続が任意の後続の接続試行により上書きされることなく、Bluetooth 接続が維持管理される方法について TSS に記述されていることを保証しなければならない (shall)。

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、以下のステップを実行しなければならない (shall) :

ステップ 1 - TOE と既知のアドレス (BD_ADDR1) に対応するリモート Bluetooth デバイスとの間で Bluetooth 接続を行う。

ステップ 2 - BD_ADDR1 と一致する Bluetooth デバイスアドレスを持つと主張する第 2 のリモート Bluetooth デバイスからの同じ TOE への接続を試行する。

ステップ 3 - Bluetooth プロトコルアナライザを用いて、第 2 の接続試行が TOE により無視され、BR_ADDR1 を持つデバイスへの最初の接続が影響されないことを検証する。

D.4.2 X509 証明書認証 (FIA_X509)

D.4.2.1 X509 証明書認証

FIA_X509_EXT.2	**拡張 : X509 証明書認証**

FIA_X509_EXT.2.3 TSF は、RFC 2986 に指定されるように証明書要求メッセージを生成し、その要求に以下の情報を提供できなければならない (shall) : 公開鍵及び [選択 : デバイス固有情報、コモン名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country)]。

適用上の注釈 : FIA_X509_EXT.2.3 で参照される公開鍵は、FCS_CKM.1(1) で特定されるように TOE により生成された公開鍵・プライベート鍵ペアの公開鍵の部分である。 高信頼チャネルの要件は、証明書要求／応答メッセージ用の CA との通信には適用されない。

Enrollment over Secure Transport (EST) は、まだ広く採用されていない新しい規格なので、本要件は、開発者が証明書要求メッセージを生成する能力を持つがいまだ EST を実装していない製品を区別できるように、暫定的なオブジェクティブ（訳注 : 将来必須となるべき）要件として含まれる。

FIA_X509_EXT.2.4 TSF は、CA 証明書応答の受領の際、ルート CA からの証明書のチェインの有効性を確認しなければならない (shall)。

保証アクティビティ :

ST 作成者が「デバイス固有情報」を選択する場合、評価者は、証明書要求で使用されるデバイス固有フィールドの記述について 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、操作ガイダンスに証明書要求メッセージの生成に関する指示が含まれていることを保証するためチェックしなければならない (shall)。 ST 作成者が「コモン名 (Common Name)」、「組織 (Organization)」、「組織単位 (Organizational Unit)」、または「国 (Country)」を選択する場合、評価者は、本ガイダンスに証明書要求メッセージを作成する前にこれらのフィールドを確立するための指示が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、TOE に証明書要求メッセージを生成させるため、操作ガイダンスを用いなければならない (shall)。 評価者は、生成されたメッセージをキャプチャし、指定さ

れるフォーマットに適合していることを保証しなければならない (shall)。 評価者は、証明書要求が、任意の必要とされる利用者入力情報を含め、公開鍵やその他の要求される情報を提供することを確認しなければならない (shall)。

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

D.4.2.2 X509 証明書の登録

FIA_X509_EXT.4	拡張：X509 証明書登録

FIA_X509_EXT.4.1 TSF は、RFC 7030 Section 4.2 に記述されたシンプル登録方法を用いて、証明書登録を要求するため、RFC 7030 に特定されるような Enrollment over Secure Transport (EST) プロトコルを使用しなければならない (shall)。

FIA_X509_EXT.4.2 TSF は、RFC 7030 Section 3.3.2 により特定されるように、既存の証明書及びそれに対応するプライベート鍵を用いて、EST 要求の認証ができなければならない (shall)。

FIA_X509_EXT.4.3 TSF は、RFC 7030 Section 3.2.3 により特定されるように、利用者名及びパスワードによる HTTP ベーシック認証を用いて、EST 要求の認証ができなければならない (shall)。

FIA_X509_EXT.4.4 TSF は、RFC 7030, section 3.6.1 に記述されたルールに従う Explicit Trust Anchor を用いて、EST サーバの認証を実行しなければならない (shall)。

適用上の注釈： EST は、EST サーバへのセキュアな接続を確立するため、FCS_HTTPS_EXT.1 に特定されるように HTTPS も使用する。EST 運用に特化した別個のトラストアンカーデータベースは、Explicit Trust Anchors として RFC 7030 に記述されている。

FIA_X509_EXT.4.5 TSF は、RFC 7030 Section 4.4 に特定されるように、サーバが提供するプライベート鍵を要求できなければならない (shall)。

FIA_X509_EXT.4.6 TSF は、RFC 7030 Section 4.1.3 に記述された「ルート CA 鍵アップデート」処理を用いて、その EST 固有トラストアンカーデータベースのアップデートができなければならない (shall)。

FIA_X509_EXT.4.7 TSF は、RFC 2986 で特定されるように、EST への証明書要求メッセージを生成し、その要求に以下の情報を提供できなければならない (shall) : 公開鍵及び [選択：デバイス固有情報、コモン名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country)]。

FIA_X509_EXT.4.8 TSF は、CA 証明書応答の受領の際、トラストアンカーデータベースのルート CA から EST サーバ CA 証明書への証明書のチェインの有効性を確認しなければならない (shall)。

適用上の注釈：FIA_X509_EXT.4.7 で参照される公開鍵は、FCS_CKM.1(1) で特定されるように TOE により生成された公開鍵・プライベート鍵ペアの公開鍵の部分である。

保証アクティビティ：

評価者は、操作ガイダンスが、証明書要求メッセージの生成を含め、EST サーバから証明

書を要求することに関する指示について含むを保証するため、チェックしなければならない (shall)。

評価者は、以下のテストについても実行しなければならない (shall)。その他のテストは、FCS_TLSC_EXT.2 用に列挙された保証アクティビティと組み合わせて実行される。

テスト 1 : 評価者は、RFC 7030 Section 4.2 に記述されたシンプル登録方法を用い、RFC 7030 Section 3.3.2 により記述されたように既存の証明書及びプライベート鍵を用いて証明書要求を認証することによって、TOE に対して EST サーバからの証明書登録を要求させるため、操作ガイダンスを使用しなければならない (shall)。 評価者は、証明書の取得が成功した結果として、TOE の鍵ストアへインストールされることを確認しなければならない (shall)。

テスト 2 : 評価者は、RFC 7030 Section 4.2 に記述されたシンプルな登録方法を用い、RFC 7030 により記述されたように利用者名及びパスワードを用いて証明書要求を認証することによって、TOE に対して EST サーバからの証明書登録を要求させるため、操作ガイダンスを使用しなければならない (shall)。 評価者は、証明書の取得が成功した結果として、TOE の鍵ストアへインストールされることを確認しなければならない (shall)。

テスト 3 : 評価者は、TOE の証明書要求に含まれる鍵とは異なる公開鍵を含む証明書を返すよう、EST サーバを改変しなければならない (shall)。 評価者は、TOE に対して EST サーバからの証明書登録を要求させるため、操作ガイダンスを使用しなければならない (shall)。 評価者は、発行された証明書の公開鍵と証明書要求の公開鍵が一致しないため、結果として得られた証明書を TOE が受け入れないことを確認しなければならない (shall)。

テスト 4 : 評価者は、TOE の一般的なトラストアンカーデータベースには存在するがその EST 固有トラストアンカーデータベースには存在しないサーバ証明書を提示するため、EST サーバを設定するか中間者ツールを使用しなければならない (shall)。 評価者は、TOE に対してその EST サーバからの証明書登録を要求させなければならない (shall)。 評価者は、この要求が成功しないことを検証しなければならない (shall)。

テスト 5 : 評価者は、無効な証明書を提示するため、EST サーバを設定するか中間者ツールを使用しなければならない (shall)。 評価者は、TOE に対してその EST サーバからの証明書登録を要求させなければならない (shall)。 評価者は、この要求が成功しないことを検証しなければならない (shall) 。 評価者は、CMC RA 目的を持たない証明書を提示するため EST サーバを設定するか中間者ツールを使用し、その EST への要求が失敗することを検証しなければならない (shall)。 試験者は、有効な証明書及び CMC RA 目的を含む証明書を用いてテストを繰り返し、その証明書の登録要求が成功することを検証しなければならない (shall)。

テスト 6 : 評価者は、TOE と EST サーバとの間でパケットスニフィングツールを使用しなければならない (shall)。 評価者は、TOE に対して EST サーバからの証明書登録を要求させるため、パケットスニフィングツールを電源オンにしなければならない (shall)。 評価者は、EST プロトコルの対話がトランスポート層セキュリティ (TLS) 保護された接続を介して行われることを検証しなければならない (shall)。 評価者は、その接続を復号することは期待されないが、パケットが TLS プロトコルフォーマットに適合していることを観測することが期待されている。

テスト 7 : 評価者は、TOE に対してサーバ提供のプライベート鍵及び証明書を EST サーバから要求させるため、操作ガイダンスを使用しなければならない (shall)。 評価者は、結果としてプライベート鍵及び証明書の取得が成功すること、そして TOE 鍵ストアへインストールされることを確認しなければならない (shall)。

テスト 8 : 評価者は、サーバ提供のプライベート鍵及び証明書要求への応答として、返される証明書の公開鍵とは対応しないプライベート鍵を返すように EST を改変しなければならない (shall)。 評価者は、TOE に対してサーバ提供のプライベート鍵及び証明書を要求させるため、操作ガイダンスを使用しなければならない (shall)。 評価者は、プライベート鍵と公開鍵が対応しないため、結果として得られたプライベート鍵及び証明書を TOE が受け入れられないことを確認しなければならない (shall)。

テスト 9 : 評価者は、RFC 7030 Section 4.1.3 に記述されたとおり「ルート CA 鍵アップデート」を提供するよう EST サーバを設定しなければならない (shall)。 評価者は、TOE に対してその EST サーバから CA 証明書を要求させなければならず (shall)、また EST 固有トラストアンカーデータベースが新たなトラストアンカーにアップデートされることを確認しなければならない (shall)。

テスト 10 : 評価者は、RFC 7030 Section 4.1.3 に記述されたとおり「ルート CA 鍵アップデート」を提供するよう EST サーバを設定しなければならない (shall) が、NewWithOld 証明書の生成された署名の部分を改変しなければならない (shall)。 評価者は、TOE に対してその EST サーバから CA 証明書を要求させなければならず (shall)、また署名が検証されないため EST 固有トラストアンカーデータベースが新たなトラストアンカーにアップデートされないことを確認しなければならない (shall)。

テスト 11 : 評価者は、TOE に対して証明書要求メッセージを生成させるため、操作ガイダンスを使用しなければならない (shall)。 評価者は、生成されたメッセージをキャプチャして、RFC 2986 により特定されたフォーマットに適合していることを保証しなければならない (shall)。 評価者は、証明書要求が、任意の必要とされる利用者入力情報を含め、公開鍵やその他の要求される情報を提供することを確認しなければならない (shall)。

D.5 クラス：TSF の保護 (FPT)

D.5.1 悪用防止 (Anti-Exploitation) サービス (FPT_AEX)

D.5.1.1 アドレス空間配置ランダム化

FPT_AEX_EXT.1	**拡張：悪用防止サービス (ASLR)**

FPT_AEX_EXT.1.3 TSF は、[***アドレス空間配置ランダム化 (ASLR) をカーネルへ***] 提供しなければならない (shall)。

FPT_AEX_EXT.1.4 任意のカーネル空間メモリマッピングのベースアドレスは、少なくとも 4 個の予測不可能なビットから構成されること。

適用上の注釈：この 4 個の予測不可能なビットは、TSF RBG (FCS_RBG_EXT.1 で特定されるとおり) により提供されてもよい。

保証アクティビティ：

評価者は、ST の TSS セクションが、その 4 ビットが生成される方法について記述し、それらのビットが予測不可能である理由の正当化について提供していることを保証しなければならない (shall)。

保証アクティビティの注釈：以下のテストは、通常は消費者向けモバイルデバイス製品には含まれないツールを評価者へ提供するようなテストプラットフォームへのアクセスを提供することを開発者に要求している。

テスト 1 : 評価者は、少なくとも 5 回 TOE をリブートしなければならない (shall)。 これらの各リブートについて、評価者は、カーネルのメモリマッピングのロケーションを検査

しなければならない (shall)。 評価者は、どのメモリマッピングも両方のデバイス上で同じのロケーションに配置されないことを保証しなければならない (must)。

D.5.1.2 メモリページのパーミション

FPT_AEX_EXT.2	拡張：悪用防止サービス (メモリページのパーミション)

FPT_AEX_EXT.2.2 TSF は、 [選択：*一切の例外なく*、*割付：[特定の例外]*] 物理メモリのいかなるページに対しても、書き込みと実行パーミションが同時に与えられることを防止しなければならない (shall)。

適用上の注釈：実行時 (JIT : just-in-time) コンパイルに使用されるメモリが、本要件の例外として予想される；その場合、ST 作成者は、この例外がどのように許可されるかについて対処しなければならない (must)。メモリ管理ユニットには、何らかの違反がカーネルメモリ空間で検出された場合、システムを非運用状態へ移行させると期待されている。

保証アクティビティ：

評価者は、非特権実行ドメインにおいて実行中のすべてのプロセスが、メモリの任意のページへの書き込みと実行パーミションを得ることを (特定された例外を除き) アプリケーションプロセッサのオペレーティングシステムが、どのように防止するかについて、TSS に記述されていることを保証しなければならない (shall)。 評価者は、このようなプロセスがそのようなパーミションを持つメモリのページを要求することを不可能にする方法、またそれらのプロセスへすでに割り当てられた任意のページに書き込みと実行の両方もパーミションを変更できなくする方法について、TSS に記述されていることを保証しなければならない (shall)。

D.5.1.3 オーバーフロー保護

FPT_AEX_EXT.3	拡張：悪用防止サービス (オーバーフロー保護)

FPT_AEX_EXT.3.2 TSF は、アプリケーションプロセッサ上で実行するプロセスへ提供する実行環境においてヒープベースのバッファオーバーフロー保護を含めなければならない (shall)。

適用上の注釈：これらのヒープベースのバッファオーバーフロー保護は、メモリブロックを管理するためにヒープの実装により記録されるメモリアドレスまたはオフセット等のヒープメタデータの完全性を保証することが期待されている。これには、チャンクヘッダ、ルックアサイドリスト、及びヒープによって管理されるメモリブロックの状態やロケーションを追跡するために使用されるその他のデータ構造が含まれる。

保証アクティビティ：

評価者は、ユーザ空間プロセスへ提供されるヒープの実装が TSS に列挙していることを検証しなければならない (shall)。 評価者は、TSS がヒープメタデータのすべての種別を列挙し、またメタデータの各種別について完全性を保証する方法について、識別されていることを保証しなければならない (shall)。 評価者は、TSS がメタデータの各種別に含まれるすべてのメモリアドレスまたはオフセットフィールドを識別し、またこれらのアドレスまたはフィールドの完全性が保証される方法について識別していることを保証しなければならない (shall)。 評価者は、TSF によりヒープオーバーフローが検出されて、その結果としてアクションが取られた際に、エラー条件に入る方法を TSS が識別していることを検証しなければならない (shall)。

各ヒープ実装について、評価者は、ヒープからメモリを割り当て、その後割り当てられたバッファの終端を大きく超えた場所へ恣意的なデータを書き込むようなアプリケーション

を書くか、または開発者がそのようなアプリケーションへのアクセスを提供しなければならない (shall)。 評価者は、このアプリケーションの実行を試行し、書き込みが許可されないことを検証しなければならない (shall)。

D.5.2 ベースバンドの分離 (FPT_BBD)

モバイルデバイスは、次第に複雑となり、リッチなオペレーティングシステムとユーザアプリケーションを実行する*アプリケーションプロセッサ*と、それとは別に*携帯電話やその他の無線*ネットワーク接続性を取り扱う*ベースバンドプロセッサ*を一つ以上持つようになってきている。

- 最新のモバイルデバイス内のアプリケーションプロセッサは、例えば CPU/GPU コアやメモリインタフェースの電子回路を単一の、電力効率のよいパッケージに統合した*システム・オン・チップ* (SoC。訳注：日本では ASIC と呼んでいる) である。
- ベースバンドプロセッサは、それ自体次第に複雑となっており、複数の CPU や DSP を含む単一のパッケージで、音声エンコーディングに加えて*複数の*独立した無線 (LTE, WiFi, Bluetooth, FM, GPS) を提供するようになってきている。

したがって、これらの要件におけるベースバンドプロセッサには、このような統合された複数の SoC が含まれ、かつ、モバイルデバイス上のあらゆる無線プロセッサ (統合またはそうでない場合) が含まれる。

他の全ての要件は、特に注記のない限り、ほとんどがアプリケーションプロセッサ上のファームウェア／ソフトウェアに適用されるが、将来の要件 (特に、すべての完全性、アクセス制御、及び悪用防止に関する要件) については、アプリケーションプロセッサ及びベースバンドプロセッサに適用されることになる。

FPT_BBD_EXT.1	**アプリケーションプロセッサによる仲介**

FPT_BBD_EXT.1.1 TSF は、アプリケーションプロセッサ (AP) により仲介される場合を除き、任意のベースバンドプロセッサ (BP) 上で実行されるコードが AP のリソースへアクセスすることを防止しなければならない (shall)。

適用上の注釈：これらのリソースには、以下のものが含まれる：

- 揮発性及び不揮発性メモリ
- 統合及び非統合の周辺機器 (例えば USB コントローラ、タッチスクリーンコントローラ、LCD コントローラ、コーデック) の制御とそれらからのデータ
- 統合及び非統合の入出力センサ (例えばカメラ、ライト、マイクロフォン、GPS、加速度計、地球磁場センサ) の制御とそれらからのデータ

保証アクティビティ：

評価者は、ST の TSS セクションに、モバイルデバイス上のプロセッサが対話する方法が、どのバスプロトコルを用いて通信するか、そのバス上で動作する他のデバイスが存在するか (周辺機器及びセンサ)、そして共有リソースがあればその識別情報を含め、高水準 (訳注：概要レベル) で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 に記述されている設計があらゆる BP に、あらゆる周辺機器やセンサへのアクセスも、そして AP によって使用されるメインメモリ (揮発性及び不揮発性) へのアクセスも許さないことを検証しなければならない (shall)。 特に、評価者は、その設計が BP による AP の実行可能メモリの改変を防止することを保証しなければならない (shall)。

D.5.3 Bluetooth プロファイル制限 (FPT_BLT)

FPT_BLT_EXT.1	拡張：Bluetooth プロファイルサポートの制限

FPT_BLT_EXT.1.1 TSF は、現在モバイルデバイス上のアプリケーションにより使用されていない [割付：*Bluetooth プロファイルのリスト*] Bluetooth プロファイルへのサポートを無効化しなければならず (shall)、またこれらを有効化するためには明示的な利用者アクションを要求しなければならない (shall)。

適用上の注釈： 一部の Bluetooth サービスは、不許可リモートデバイスがそれらへのアクセスを取得した場合、より深刻な結果を招くことになる。そのようなサービスは、モバイルデバイス上のアプリケーションによりアクティブに使用されていない限り関連する Bluetooth プロファイルのサポートを無効化し (Service Discovery Protocol 検索による検出を防止するため)、その後そのサービスを利用するためにそれらのプロファイルを有効化するには明示的な利用者アクションを要求する等の手段により、保護されるべきである (should)。そのサービスへのリモートデバイスのアクセスを許可する前に、追加の利用者アクションを要求することが、さらに適切であるかもしれない (FIA_BLT_EXT.1.2)。

(例えば、モバイルデバイスの利用者が、オブジェクトの転送の準備ができたことを示すようなアプリケーションにおけるボタンを押すまで、OBEX Push Profile を無効化することが適切であるかもしれない。オブジェクト転送の完了後、OBEX プロファイルのサポートは、次回利用者がその使用を要求するまで中断されるべきである(should))

ST 作成者は、アプリケーションによって利用されていない間に無効化され、かつ有効化されるためには明示的な利用者アクションを必要とする、すべての Bluetooth プロファイルを列挙しなければならない (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: サービスが TOE 上のアプリケーションによりアクティブに利用されていない間、評価者は、TOE 上で (要件によって特定されるように) 「保護された」Bluetooth プロファイルと関連付けられたサービスの検出を Service Discovery Protocol 検索により試行しなければならない (shall)。 評価者は、そのサービスが Service Discovery Protocol 検索結果において見つからないことを検証しなければならない (shall)。 次に、評価者は、TOE との高信頼デバイス関係を現在有していないデバイスからそのサービスへのリモートアクセスの取得を試行しなければならない (shall)。 評価者は、この試行がサービス及びプロファイルの利用不可のために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、TOE との高信頼デバイス関係を現在有するデバイスを用いて、テスト 1 を繰り返し、同じふるまいを示すことを検証しなければならない (shall)。

D.5.4 自己テスト通知 (FPT_NOT)

FPT_NOT_EXT.1	拡張：自己テスト通知

FPT_NOT_EXT.1.2 TSF は、TSF ソフトウェア完全性検証の値を [選択：*ログ出力*、*管理者へ提供*] しなければならない (shall)。

適用上の注釈：これらの通知は、通常リモート証明 (attestation) と呼ばれ、これらの完全性の値は測定値 (measurements) と呼ばれるのが通常である。 完全性の値は、実行可能コードを含む、重要なメモリ及び値のハッシュから計算される。ST 作成者は、これらの値が FAU_GEN.1.1 の一部としてログ出力されるか、管理者へ提供されるかのいずれかを選択し

なければならない (shall)。

保証アクティビティ：

評価者は、どの重要なメモリについてその完全性の値が測定されるか、そして (どの TOE ソフトウェアがこれらの値の生成を行うか、そのソフトウェアがどのように重要なメモリへアクセスするか、及びどのアルゴリズムが使用されるかを含め) どのように測定が行われるか、TSS に記述されていることを検証しなければならない (shall)。

完全性の値が管理者へ提供される場合、評価者は、これらの値を読み出すための指示とそれらを解釈するための情報が 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)。(例えば、複数の測定値が取得される場合、それらの測定値が何であるか、そしてそれらの値の変化がデバイス状態の変化とどのように関係するか。)

保証アクティビティの注釈：以下のテストは、消費者向けモバイルデバイス製品には通常含まれないツールを評価者へ提供するようなテストプラットフォームへのアクセスをベンダが提供することが必要とされる。

評価者は、各測定値について以下のテストを繰り返さなければならない (shall)：

*テスト：*評価者は、承認された状態でデバイスをブートし、(ログから、または管理者ガイダンスを用いて MDM エージェント経由で値を読み出すかのいずれかの方法で) 取得された測定値を記録しなければならない (shall)。 評価者は、重要なメモリまたは測定された値を改変しなければならない (shall)。 評価者は、デバイスをブートし、測定値が変わったことを検証しなければならない (shall)。

FPT_NOT_EXT.1.3 TSF は、すべての完全性検証の値に暗号技術的に署名しなければならない (shall)。

適用上の注釈：本要件の意図は、提供された応答が TOE からのものであり、ネットワークベースの敵対者または悪意のある MDM エージェント等の中間者により、改変も詐称もされていないという保証を管理者に提供することである。

保証アクティビティ：

評価者は、TSF が問い合わせへの応答に署名するためにどの鍵を使うのか、そしてその鍵の所有権を証明するために使用される証明書について、TSS に記述されていることを検証しなければならない (shall)。 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： 評価者は、監査ログまたは測定値のいずれかを問い合わせる管理アプリケーションを書くか、または開発者がそのようなアプリケーションを提供しなければならない (shall)。 評価者は、これらの問い合わせへの返答が署名されていることを検証し、またその署名を TOE の証明書にて検証しなければならない (shall)。

D.5.5 高信頼アップデート (FPT_TUD)

FPT_TUD_EXT.2	**拡張：高信頼アップデート検証**

FPT_TUD_EXT.2.5 TSF は、デフォルトで [選択：*組み込まれた X.509v3 証明書*、*設定された X.509v3 証明書*] により、暗号技術的に検証されたモバイルアプリケーションのみをインストールしなければならない (shall)。

適用上の注釈：組み込まれた証明書は、製造時、またはシステムアップデートの一部として、製造業者によりインストールされる。 署名を検証するために使用される設定された証明書は、FMT_SMF_EXT.1 の機能 33 に従って確定される。

保証アクティビティ：

評価者は、TSS に、モバイルアプリケーションソフトウェアがインストール時にどのように検証されるがについて記述されていることを検証しなければならない (shall)。 評価者は、この方法がコード署名証明書によるデジタル署名を使用することを保証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書くか、または開発者がアプリケーションへのアクセスを提供しなければならない (shall)。 評価者は、このアプリケーションのデジタル署名なしでのインストールを試行しなければならず (shall)、そしてインストールが失敗することを検証しなければならない (shall)。 評価者は、適切な証明書を用いてデジタル署名されたアプリケーションのインストールを試行し、インストールが成功することを検証しなければならない (shall)。

テスト 2 : 評価者は、無効な証明書を用いてアプリケーションにデジタル署名し、アプリケーションのインストールが失敗することを検証しなければならない (shall)。 評価者は、コード署名目的を持たない証明書を用いてアプリケーションにデジタル署名し、アプリケーションのインストールが失敗することを検証しなければならない (shall)。 このテストは、FIA_X509_EXT.1 の保証アクティビティと組み合わせて実行されてもよい。

テスト 3 : 必要な場合、評価者は、AGD ガイダンスに従って、アプリケーションソフトウェアに署名できる公開鍵を制限するようデバイスを設定しなければならない (shall)。 評価者は、デバイス又は設定により許可されない証明書を用いてアプリケーションにデジタル署名し、アプリケーションのインストールが失敗することを検証しなければならない (shall)。 評価者は、正当な証明書を用いてデジタル署名されたアプリケーションのインストールを試行し、アプリケーションのインストールが成功することを検証しなければならない (shall)。

FPT_TUD_EXT.2.7 TSF は、TSF へのソフトウェアアップデートが、TSF の現在のバージョンであるか、または現在のバージョンよりも新しいバージョンであることを検証しなければならない (shall)。

適用上の注釈：新しいバージョンは、より大きいバージョン番号を持つ。 新しいソフトウェアバージョンを以前のバージョンと区別する方法は、製造業者によって決定される。

保証アクティビティ：

評価者は、TSS に、現在インストールされているバージョンよりも古いバージョンのソフトウェアアップデートを TSF がインストールすることを防止するメカニズムについて記述されていることを検証しなければならない (shall)。

評価者は、TSS に記述されたとおり、すべての許可されたソフトウェアアップデートメカニズムを網羅するため、以下のテストを繰り返さなければならない (shall)。 例えば、アップデートメカニズムが数多くの別々のコードファイルを含むパーティション全体を置き換える場合、評価者は、個別の各ファイルについてテストを繰り返す必要はない。

テスト 1 : 評価者は、(製造業者により決定されるとおり) 以前のバージョンのソフトウェアのインストールを試行しなければならない (shall)。 評価者は、特権を持つソフトウェアのバージョン識別子または暗号ハッシュを以前に記録されたものに対してチェックして、その値が改変されていないことをチェックすることにより、この試行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、現在のバージョンまたはそれよりも新しいバージョンのインストールを試行しなければならず (shall)、またそのアップデートが成功することを検証しなければならない (shall)。

D.6 Class: TOE アクセス (FTA)

D.6.1 デフォルト TOE アクセスバナー (FTA_TAB)

FTA_TAB.1	デフォルト TOE アクセスバナー

FTA_TAB.1.1 利用者セション確立前に、TSF は、TOE の不正な使用に関する勧告的警告メッセージを表示しなければならない (shall)。

適用上の注釈：本要件は、テキストまたは望ましいメッセージのテキストを含む画像のいずれかの設定によって満たすことができる。 TSF は、最低限、この情報を起動時に表示しなければならない (shall) が、ロック解除のたびにこの情報を表示してもよい。バナーは、FMT_SMF_EXT.1 の機能 36 に従って設定される。

保証アクティビティ：

TSS は、いつバナーが表示されるかについて記述しなければならない (shall)。 評価者は、以下のテストについても実行しなければならない (shall)：

テスト 1：評価者は、操作ガイダンスに従って、通知及び同意警告メッセージを設定する。次に、評価者は、TSF を起動またはロック解除しなければならない (shall)。 評価者は、TSS に記述された各インスタンスにおいて、通知及び同意警告メッセージが表示されることを検証しなければならない (shall)。

E. エントロピーに関する文書と評定

エントロピー源に関する文書は、それを読んだ後、評価者が完全にエントロピー源を理解し、それがエントロピーを提供すると信頼できる理由を理解できるように、十分に詳細であるべきである (should)。本文書には、設計の記述、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)。本文書が、TSS の一部である必要はない。

E.1 設計記述

文書には、すべてのエントロピー源コンポーネントの相互作用を含め、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)。これには、エントロピー源がどのように動作するのか、どのようにエントロピーが作り出されるのか、そして未処理 (生の) データをエントロピー源の内部からテスト目的でどのように取り出せるかを含め、エントロピー源の運用が記述されることになる。文書には、ランダム性がどこに由来し、次にどこへ渡されるのか、生の出力の後処理 (ハッシュ、XOR 等) が存在すれば、それが (どこに) 保存されるか、そして最後にどのようにエントロピー源から出力されるのかを示しながら、エントロピー源の設計についてのウォークスルー (段階的な説明) が行われるべきである (should)。 処理に課される条件 (例えば、ブロッキング) があれば、それ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量に影響を与えられないことをセキュリティ境界がどのように保証しているかの記述も含まれなければならない (must)。

第三者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、設計の記述には、その記述が含まれなければならない (shall)。電源オフから電源オンまでの間に保存される RBG 状態があれば、その記述が含まれなければならない (shall)。

E.2 エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、エントロピー源が確率的なふるまいを示すことがなぜ確信できるのか (確率分布の説明と、その分布が特定のエントロピー源によって得られるという正当化を行うことは、これを記述する一つの方法である) という、技術的な議論が存在すべきである (should)。 この議論は、期待されるエントロピー量の記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられることをどのように保証するかを説明することになる。この議論は、エントロピー源がエントロピーを含むビットを生成すると信頼できる理由の正当化の一部となる。

エントロピーの正当化は、第三者アプリケーションからのデータも、再起動までの間の状態保存から追加されるデータも、一切含まれてはならない (shall not)。

E.3 運用条件

文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。これには、これらの条件の下でエントロピー源が動作し続けることを保証するために、システムの設計に取り入れられた対策が明確に記述されることになる。同様に、文書にはエントロピー源が動作不良または矛盾した動作となることがわかっている条件も記述されなければならない (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)。

E.4 ヘルステスト

さらに具体的には、すべてのエントロピー源ヘルステストとその根拠が文書化されることになる。これには、ヘルステストの記述、各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)、各ヘルステストに期待される結果、及び各テストがエントロピー源において 1 つ以上の故障を検出するために適切であると信じられる理由を示す根拠が含まれることになる。

F. 略語

F.1 略語

略語	意味
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
ANSI	米国規格協会(American National Standards Institute)
AP	アプリケーションプロセッサ(Application Processor)
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)
BP	ベースバンドプロセッサ(Baseband Processor)
BR/EDR	(Bluetooth) Basic Rate/Enhanced Data Rate
CA	認証局(Certificate Authority)
CBC	Cipher Block Chaining
CCM	Counter with CBC-Message Authentication Code
CCMP	CCM プロトコル(CCM Protocol)
CMC	Certificate Management over Cryptographic Message Syntax (CMS)
CPU	中央処理装置(Central Processing Unit)
CRL	証明書失効リスト (Certificate Revocation List)
CSP	クリティカルセキュリティパラメタ(Critical Security Parameters)
DAR	保存データ (Data At Rest)
DEK	データ暗号化鍵(Data Encryption Key)
DEP	データ実行防止(Data Execution Prevention)
DH	Diffie-Hellman
DNS	ドメイン名システム (Domain Name System)
DSA	デジタル署名アルゴリズム(Digital Signature Algorithm)
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)
EAPOL	EAP Over LAN
ECDH	Elliptic Curve Diffie Hellman
ECDSA	楕円曲線デジタル署名アルゴリズム(Elliptic Curve Digital Signature Algorithm)
EEPROM	電気的消去可能プログラマブル読み出し専用メモリ(Electrically Erasable Programmable Read-Only Memory)
EST	Enrollment over Secure Transport
FIPS	連邦情報処理規格(Federal Information Processing Standards)
FM	周波数変調(Frequency Modulation)
FQDN	完全修飾ドメイン名 (Fully Qualified Domain Name)
GCM	Galois Counter Mode
GPS	Global Positioning System
GPU	Graphics Processing Unit
GTK	グループ一時鍵 (Group Temporal Key)
HDMI	High Definition Multimedia Interface
HMAC	Keyed-Hash Message Authentication Code
HTTPS	HyperText Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	インターネットプロトコル (Internet Protocol)
IPC	プロセス間通信 (Inter-Process Communication)
IPsec	インターネットプロトコルセキュリティ (Internet Protocol Security)

略語	意味
KEK	鍵暗号化鍵 (Key Encryption Key)
LE	(Bluetooth) Low Energy
LTE	Long Term Evolution
MD	モバイルデバイス (Mobile Device)
MDM	モバイルデバイス管理 (Mobile Device Management)
MMI	マンマシンインタフェース (Man-Machine Interface)
MMS	Multimedia Messaging Service
NFC	Near Field Communication
NIST	国立標準技術研究所(National Institute of Standards and Technology)
NX	実行禁止 (Never Execute)
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)
OS	オペレーティング システム (Operating System)
OTA	無線経由の (Over the Air)
PAE	ポートアクセスエンティティ (Port Access Entity)
PBKDF	Password-Based Key Derivation Function
PMK	Pairwise Master Key
PP	プロテクションプロファイル (Protection Profile)
PTK	Pairwise Temporal Key
RA	Registration Authority
RBG	ランダムビット生成器 (Random Bit Generator)
REK	ルート暗号化鍵 (Root Encryption Key)
ROM	読み出し専用メモリ (Read-only memory)
RSA	Rivest Shamir Adleman
SHA	セキュアハッシュアルゴリズム (Secure Hash Algorithm)
SMS	Short Messaging Service
SPI	Security Parameter Index
SSH	セキュアシェル (Secure Shell)
SSID	Service Set Identifier
ST	セキュリティターゲット(Security Target)
TLS	トランスポート層セキュリティ (Transport Layer Security)
TOE	評価対象 (Target of Evaluation)
TSF	TOE セキュリティ機能 (TOE Security Functions)
TSS	TOE 要約仕様 (TOE Summary Specification)
URI	Uniform Resource Identifier
USB	ユニバーサルシリアルバス (Universal Serial Bus)
USSD	Unstructured Supplementary Service Data
VPN	仮想プライベートネットワーク (Virtual Private Network)
WiFi	Wireless Fidelity
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)
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

G. 使用事例テンプレート

以下の使用事例テンプレートには、本プロテクションプロファイルによって特定された使用事例を最もよくサポートする選択、割付、及びオブジェクティブな要件が列挙されている。これらのテンプレートは、そのテンプレートに列挙されたものだけではなく、セクション 5 に列挙されたすべての SFR が ST に含まれることを前提としていることに注意されたい。これらのテンプレート及びテンプレートからの逸脱は、顧客がリスクに基づいた購入判断を行うことを助けるため、セキュリティターゲット中に特定されるべきである (should)。これらのテンプレートを満たさない製品が、本プロテクションプロファイルによって特定されるシナリオにおける使用から除外されることはない。

使用事例テンプレートのいくつかには、提示された使用事例に強く望まれるオブジェクティブな要件が含まれている。読者は、これらの要件が本プロテクションプロファイルの次期の改訂版では必須とされると期待してよい。また業界は、短期のうちにそのセキュリティ機能を製品へ含めることを目指すべきである (should)。

特定の要件についての選択が使用事例テンプレートに特定されていない場合、すべての利用可能な選択が同等にその使用事例に適用可能である。

G.1 [使用事例 1] 汎用エンタープライズ用途のエンタープライズ所有デバイス

要件	アクション
FCS_STG_EXT.1.4	「利用者」を選択しない。
FMT_MOF_EXT.1.2 の機能 4	GPS を割り付ける。
FMT_MOF_EXT.1.2 の機能 23	ST に含める。パーソナルホットスポット接続を割り付ける。
FMT_MOF_EXT.1.2 の機能 36	ST に含める。
FMT_MOF_EXT.1.2 の機能 39	ST に含める。「USB マスストレージモード」を選択する。
FMT_MOF_EXT.1.2 の機能 41	選択に含める。「USB テザリング」を選択する。
FMT_SMF_EXT.1.1 の機能 4	GPS を割り付ける。
FMT_SMF_EXT.1.1 の機能 23	ST に含める。パーソナルホットスポット接続を割り付ける。
FMT_SMF_EXT.1.1 の機能 36	ST に含める。
FMT_SMF_EXT.1.1 の機能 39	ST に含める。「USB マスストレージモード」を選択する。
FMT_SMF_EXT.1.1 の機能 41	ST に含める。両方の選択肢を選択する。
FPT_BBD_EXT.1.1	ST に含める。
FPT_TST_EXT.2.1	「可換メディアに保存されたすべての実行可能コード」を選択する。
FPT_TUD_EXT.2.5	ST に含める。
FTA_TAB.1.1	ST に含める。

表 12：エンタープライズ所有のテンプレート

G.2 [使用事例 2] 特化した高セキュリティ用途のエンタープライズ所有デバイス

要件	アクション
FCS_CKM.1.1(1)	ECC スキームを選択する。

要件	アクション
FCS_CKM.2.1(1)	ECC スキームを選択する。
FCS_CKM_EXT.1.1	256 ビットを選択する。
FCS_CKM_EXT.2.1	256 ビットを選択する。
FCS_CKM_EXT.3.1	256 ビットを選択する。
FCS_COP.1.1(1)	256 ビットを選択する。
FCS_COP.1.1(2)	SHA-256 及び SHA-384 を選択する。
FCS_COP.1.1(3)	ECDSA スキームを選択。
FCS_COP.1.1(5)	256 ビットを選択する。
FCS_RBG_EXT.1.2	256 ビットを選択する。
FCS_TLSC_EXT.2.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 を選択する。
FCS_TLSC_EXT.2.5	ST に含める。secp384 を選択する。
FCS_TLSC_EXT.2.6	ST に含める。SHA-384 を選択する
FDP_DAR_EXT.1.2	256 ビットを選択する。
FIA_X509_EXT.2.2	「…管理者に許可する」または「証明書を受容しない」のいずれかを選択する。
FMT_MOF_EXT.1.2 の機能 3	ST に含める。
FMT_MOF_EXT.1.2 の機能 6	ST に含める。
FMT_SMF_EXT.1.1 の機能 4	TSF 上のすべての無線を割り付ける。
FMT_SMF_EXT.1.1 の機能 5	TSF 上のすべてのオーディオまたは映像収集デバイスを割り付ける。
FMT_SMF_EXT.1.1 の機能 14	トラストアンカーデータベース中のすべての X.509v3 証明書を割り付ける。
FMT_SMF_EXT.1.1 の機能 23	ST に含める。TSF がサーバとしてふるまうすべてのプロトコルを割り付ける。
FMT_SMF_EXT.1.1 の機能 36	ST に含める。
FPT_BBD_EXT.1	ST に含める。
FTA_TAB.1.1	ST に含める。

表 13：高セキュリティのテンプレート

G.3 [使用事例 3] 個人的及びエンタープライズ用途の個人所有デバイス

現時点で、本使用事例に推奨される要件や選択は存在しない。しかし、FDP_ACF_EXT.1.2 ならびに FMT_SMF_EXT.1 の機能 19 及び 28 が、本使用事例において利用者の個人的データからエンタープライズデータを分離する重要な役割を演じることには注意すべきである (should)。

G.4 [使用事例 4] 個人的及び制限されたエンタープライズ用途の個人所有デバイス

現時点で、本使用事例に推奨される要件や選択は存在しない。

H. NIST 承認暗号利用モードの初期化ベクタの要件

暗号利用モード	参照情報	IV 要件
Electronic Codebook (ECB)	SP 800-38A	IV なし
Counter (CTR)	SP 800-38A	「初期カウンタ (Initial Counter)」は、非循環でなければならない (shall)。いかなるカウンタ値も、同一の秘密鍵が使用される複数のメッセージにわたって循環してはならない (shall not)。
Cipher Block Chaining (CBC)	SP 800-38A	IV は、予測不可能でなければならない (shall)。循環する IV は、2 つのメッセージの間で最初の 1 つ以上のブロックが共有されているかどうかという情報を漏らしてしまうため、そのような状況において IV は非循環であるべきである (should)。
Output Feedback (OFB)	SP 800-38A	IV は非循環でなければならず (shall)、また別の IV に暗号を適用することによって生成されたものであってはならない (shall not)。
Cipher Feedback (CFB)	SP 800-38A	循環する IV は、最初の平文ブロックに関する情報や、メッセージ間で共有される共通プリフィックスに関する情報を漏らしてしまうため、IV は非循環であるべきである (should)。
XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing (XTS)	SP 800-38E	IV なし。Tweak 値は非負の整数であって、連続的に割り当てられ、そして任意の非負の整数からスタートするものでなければならない (shall)。
Cipher-based Message Authentication Code (CMAC)	SP 800-38B	IV なし
鍵ラップ及びパディング付き鍵ラップ	SP 800-38F	IV なし
Counter with CBC-Message Authentication Code (CCM)	SP 800-38C	IV なし。ノンスは非循環でなければならない (shall)。
Galois Counter Mode (GCM)	SP 800-38D	IV は非循環でなければならない (shall)。GCM の呼び出し回数は、実装が 96 ビットの IV (デフォルトの長さ) のみを利用する場合を除き、所与の秘密鍵について 2^32 を越えてはならない (shall not)。

表 14：NIST 承認暗号利用モードの参照情報と IV 要件