モバイルデバイス基盤のための
プロテクションプロファイル

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_v1.1.pdf

バージョン 1.1　2014 年 2 月 12 日

平成 26 年 10 月 10 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

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、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)

UK IT Security Evaluation and Certificate Scheme (CESG)

産業界

Apple, Inc.

BlackBerry

Microsoft Corporation

Motorola Solutions

Samsung Electronics Co., Ltd.

Mobility Technical Community のその他のメンバー

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、特定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、適用上の注意の追加説明。 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。

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プロテクションプロファイル

PP バージョン： 1. 1

PP の日付： 2014 年 2 月 12 日

1.2 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、ワイヤレス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。

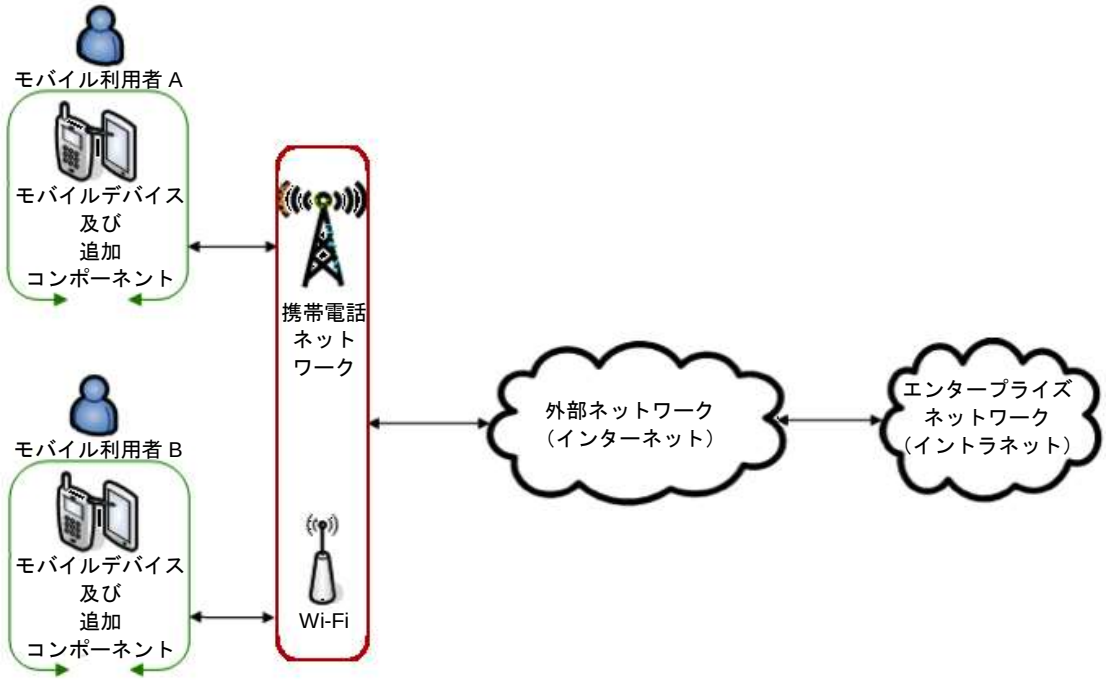

図 1：モバイルデバイスのネットワーク環境

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強制、アプリケーション強制アクセス制御、アンチエ

クスプロイト (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基本的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、以下を提供するサードパーティの、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。

- 通過中のデータの保護 (例えば VPN クライアント、VoIP クライアント、ウェブブラウザ)
- セキュリティポリシー管理 (例えば MDM システム)

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)。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。

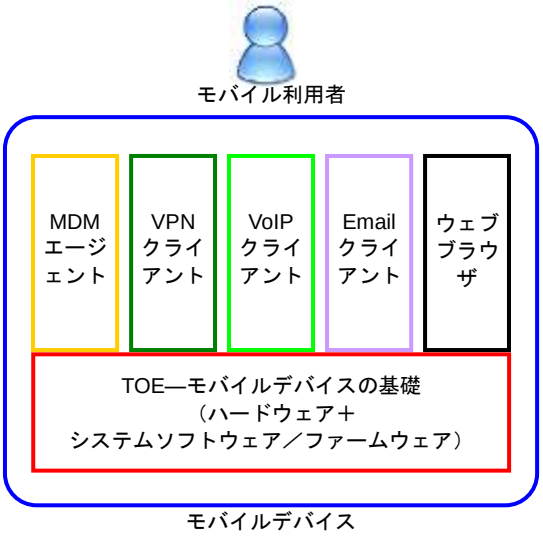

図 2：オプションの追加的モバイルデバイスコンポーネント

1.3 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かもしれない。必須の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構成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。

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、及び客観的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。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、本体中の要件を満たしていれば、すべての使用事例について十分である。

[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いても現実的とはみなされないような、しかし高度に機密性のある情報へのリスクを軽減し得るような、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用いら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強制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。

[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強制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。

2. CC への適合

[CC1]、[CC2] 及び [CC3] に定義されるとおり、本 PP 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。

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、ワイヤレス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、ワイヤレス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。

注意：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 永続的アクセス

攻撃者によるデバイスへの永続的アクセスは、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トルを原因として、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構成データのワイヤレス送信に関して、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、または HTTPS。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_COP.1(*), FCS_DTLS_EXT.1, FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_SRV_EXT.1, FCS_TLS_EXT.1, FCS_TLS_EXT.2, FDP_STG_EXT.1, FIA_PAE_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, 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、デバイス上に保存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正な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.1(*), FMT_POL_EXT.1, FMT_SMF.1, FMT_SMF_EXT.1, FTA_TAB_EXT.1

4.1.4 O.AUTH 認可と認証

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正な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強制されるよう制限または抑制 (throttle) される。

FCS_CKM.1(2), FIA_AFL_EXT.1, FIA_BLT_EXT.1, FIA_PMG_EXT.1, FIA_TRT_EXT.1, FIA_UAU.7, FIA_UAU_EXT.1, FIA_UAU_EXT.2, FIA_UAU_EXT.3, FIA_X509_EXT.2, 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 はセルフテストを行って、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。これらのセルフ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、TOE 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。さらにオペレーティングシステムは、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。その上オペレーティングシステムは、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_SEL.1, FAU_STG_EXT.1, FCS_COP.1(2), FCS_COP.1(3), FCS_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。

5.1 表記法

以下の表記が、操作の完了に用いられる。

- [*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。
- ~~取り消し線~~は詳細化としてテキストが削除されることを、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、合成され、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 5.3.2 に記述される DAR 保護のように) データを保護するために用いられる。KEK は、DEK、及び利用者またはアプリケーションによって保存される他の種別の鍵など、他の鍵を保護するために用いられる。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。

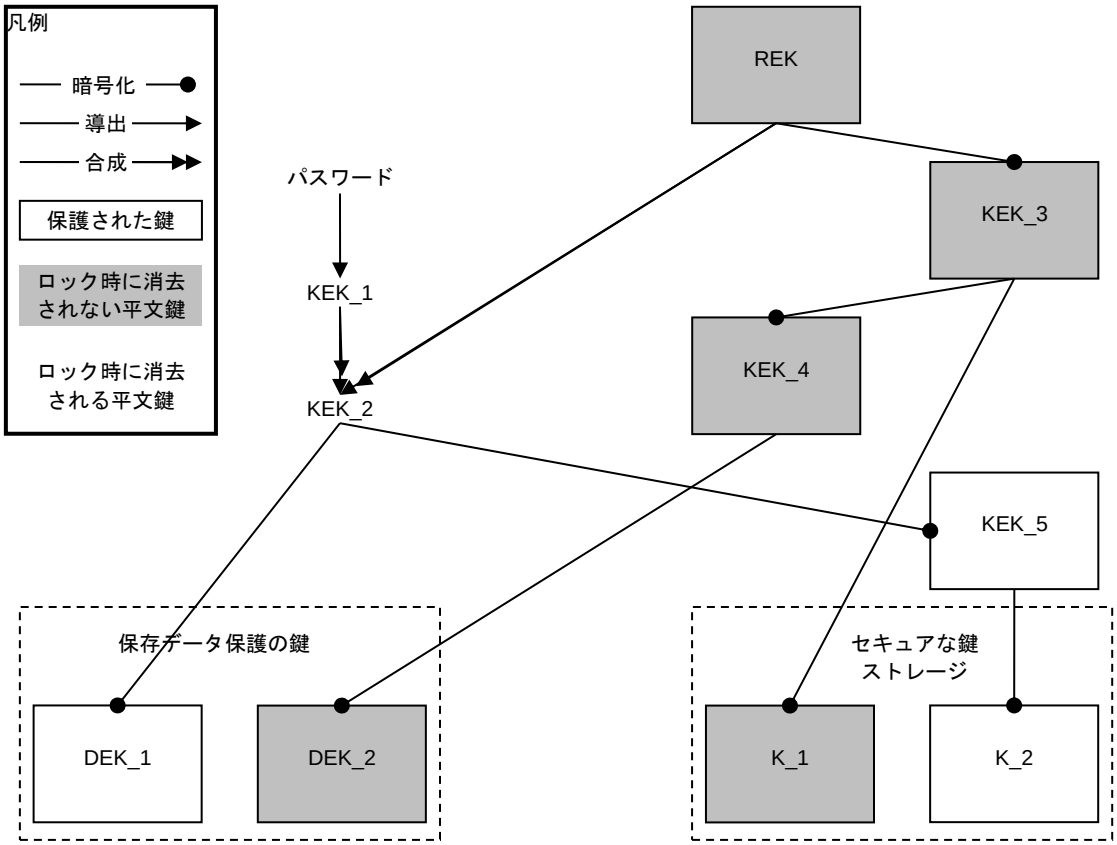

図 3：鍵階層構造の例

5.2.1.1 暗号鍵生成 (鍵確立)

FCS_CKM.1(1)	**詳細化：暗号鍵生成**

FCS_CKM.1.1(1): TSF は、以下の標準のリスト：

- RSA ベースの鍵確立スキームについては、NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”、及び

[***選択：***

- ***有限体ベースの鍵確立スキームについては、NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”、***
- ***楕円曲線ベースの鍵確立スキームならびに「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] (FIPS PUB 186-4, “Digital Signature Standard” の定義による) の実装については、NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”***
- ***その他のアルゴリズムなし***]

及び、特定された暗号鍵長 112 ビットの対称鍵強度と同等、またはそれよりも大きく に合致する、鍵確立のために使用される非対称暗号鍵を生成しなければならない (shall)。

(訳注) 標準のリストの第一段落（必須）において、RSA ベースの鍵確立スキームについては、NIST SP800-56B 及び FIPS PUB 186-4 と記述するのが正しい。また、第二段落（選択肢１）において、NIST SP800-56A ではなく、FIPS PUB 186-4,"Digital Signature Standard" for finite field-based key establishment schemes とするのが正しい。さらに、第三段落 (選択肢２) において、記述を「FIPS PUB 186-4, "Digital Signature Standard" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard") 」とするのが正しい。

適用上の注意：このコンポーネントは、TOE によって用いられるさまざまな暗号プロトコル (例えば、EAP-TLS、高信頼チャネル) 及び画面ロック時の保存データ保護の鍵確立の目的で用いられる公開鍵／プライベート鍵ペアを TOE が生成できることを要求する。複数のスキームがサポートされている場合には、ST 作成者はこの要件を繰り返してこの機能を取り込むべきである (should)。用いられるスキームは、ST 作成者によって選択の中から選ばれることになる。RSA 鍵確立は、**FCS_TLS_EXT.1** にしたがうために要求されている。

用いられるべきドメインパラメタは、本 PP 中のプロトコルの要件によって特定されるかもしれない。一般的には、TOE がドメインパラメタを生成することは期待されておらず、したがって本 PP に特定されたプロトコルやその他の要件に TOE が準拠する際には追加的なドメインパラメタの検証は必要とされない。

2048 ビットの DSA 及び RSA 鍵の生成鍵強度は、112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。同等の鍵強度に関する情報については、NIST Special Publication 800-57, "Recommendation for Key Management" を参照されたい。

将来は、楕円曲線に関する NIST SP 800-56A が要求されることになる。

保証アクティビティ：

この保証アクティビティは、TOE 上で用いられる鍵生成及び鍵確立方式を検証する。

鍵生成：

評価者は、以下から該当するテストを用いて、サポートされるスキームの鍵生成ルーチンの実装を検証しなければならない (shall)。

RSA ベースの鍵確立スキームのための鍵生成

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

鍵ペア生成では、素数 *p* 及び *q* を生成するための 5 とおりの方法 (または手法) を特定している。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手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (must)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF によって生成された値を既知の良好な実装から生成された値と比較することによって、TSF の実装の正しさを検証しなければならない (shall)。

有限体暗号 (FFC) ベースの 56A スキームのための鍵生成

FFC ドメインパラメタ及び鍵生成テスト

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

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

暗号素数及びフィールド素数 :

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

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

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

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

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

楕円曲線暗号 (ECC) ベースの 56A スキームのための鍵生成

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-284 (訳注：P-384 の間違い) 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) 機能へ提出しなければならない (shall)。

ECC 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-284 及び P-521 のそれぞれについて、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

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

機能テスト

機能テストは、鍵共有スキームを正しく実装する TOE の能力を検証する。このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクタを生成または取得しなければならない (shall)。サポートされている鍵共有スキーム・鍵共有役割の組み合わせ、KDF タイプと (サポートされてい

る場合には) 鍵確認役割・鍵確認タイプの組み合わせのそれぞれについて、試験者は 10 セットのテストベクタを生成しなければならない (shall)。このデータセットは、10 セットの公開鍵あたり 1 セットのドメインパラメタ値 (FFC) または NIST 認可曲線 (ECC) からなる。これらの鍵は、テストされるスキームにより静的鍵であるか、短期鍵であるか、またはその両方である。

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

(訳注) 上記のパラグラフは、TLS において SP800-56A で定める KDF は使用されず、SP800-135 に定められた KDF が使用されるため、意味がない。将来このパラグラフは削除される。

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

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

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

検証テスト

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

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

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

SP800-56B 鍵確立スキーム

現時点では、RSA ベースの鍵確立スキームのための詳細なテスト手順は利用できない。行われた選択に応じて TSF が 800-56A 及び／または 800-56B に適合していることを示すため、評価者は TSS に以下の情報が含まれることを保証しなければならない (shall)。

- TSS には、TOE が適合する適切な 800-56 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)。

800-56A 及び 800-56B (選択に応じて) 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)。

5.2.1.2 暗号鍵生成 (認証用非対称鍵)

FCS_CKM.1(2)	**暗号鍵生成**

FCS_CKM.1.1(2) TSF は、以下の特定された暗号鍵生成アルゴリズム[***選択：***

- ***RSA スキームについては、FIPS PUB 186-4, “Digital Signature Standard (DSS)” の附属書 B.3、***
- ***ECDSA スキームならびに「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] の実装については、FIPS PUB 186-4, “Digital Signature Standard (DSS)” の附属書 B.4、***
- ***AES を用いる RSA スキームについては、ANSI X9.31-1998 の附属書 A.2.4***]

及び特定された暗号鍵長 [***112 ビットの対称鍵強度と同等、またはそれよりも大きく***] に従って認証のために使用される非対称暗号鍵を生成しなければならない (shall)。

(訳注) 上記 3 番目の選択肢 ANSI X9.31-1998 は、単にランダムビット生成に関するものであり、RSA スキームについての鍵生成アルゴリズムではないため、本 SFR としては不適当である。以下の適用上の注意にあるとおり、将来削除される。

適用上の注意: 生成された公開鍵は X509v3 証明書の識別情報と関連付けられることが期待されるが、この関連付けは TOE によって行われる必要はなく、運用環境の認証局によって行われることが期待される。

楕円曲線ベースの方式に関しては、鍵サイズは基点の位数の 2 の対数を示す。

ANSI X9.31-1998 の選択肢は、本文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。暗号署名に関する好ましいアプローチとして、本 PP の将来の版では楕円曲線が要求されることになる。

同等の鍵強度に関する情報については、NIST Special Publication 800-57, “Recommendation for Key Management”を参照されたい。

保証アクティビティ：

TSF が FIPS 186-4 署名スキームを実装する場合、この要件は **FCS_COP.1.1(3)** の下で検証される。

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)。

5.2.1.3 暗号鍵生成 (WLAN)

FCS_CKM.1(3)	**暗号鍵生成**

FCS_CKM.1.1(3) TSF は、特定された暗号鍵生成アルゴリズム [***PRF-384***] 及び特定された暗号鍵サイズ [***128 ビット***] にしたがい、**FCS_RBG_EXT.1** に特定されるランダムビット生成器であって以下： [***IEEE 802.11-2012***] を満たすものを用いて、対称暗号鍵を生成しなければならない (shall)。

適用上の注意：この要件は **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ワイヤレス 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。

この要件は、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 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 で後に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ワイヤレス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 によって用いられる方法が 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 つまたは複数の手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)。

5.2.1.4 暗号鍵配付 (WLAN)

FCS_CKM.2	暗号鍵配付

FCS_CKM.2.1 TSF は、指定された暗号鍵配付方法 [***EAPOL 鍵フレーム内の AES 鍵ラップ***] であって、以下： [***NIST SP 800-38F、IEEE 802.11-2012 for the packet format and timing considerations***] を満たし、かつ暗号鍵を暴露しない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)。

適用上の注意：この要件は **FTA_WSE_EXT.1** をサポートする。これは、モバイルデバイスが構成済みワイヤレス LAN に接続できることを要求するものである。この要件は、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 鍵ラップ手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、以下のテストを行わなければならない (shall)。

*テスト 1：*評価者は、TOE のアクセスポイントへの接続を成功させなければならない (shall)。TOE が接続されている状態で、評価者は GTK が TOE とアクセスポイントとの間で平文で送信されていないことを確認しなければならない (shall)。

*テスト 2：*評価者は、TOE が接続しているアクセスポイントによってブロードキャストメッセージが送信されるようにしなければならない (shall)。評価者は、そのメッセージが暗号化されていて通過中に読むことができないこと、そして TOE が送信されたメッセージを復号して読むことができることを保証しなければならない (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、サイズ [選択：*128 ビット*、*256 ビット*] の AES 鍵によってハードウェア保護された REK をサポートしなければならない (shall)。

FCS_CKM_EXT.1.2: REK は、ハードウェアから読み出せたり、エクスポートできたりしてはならない (shall not)。

FCS_CKM_EXT.1.3: TSF 上のシステムソフトウェアは、鍵による暗号化／復号を要求することのみができなければならず (shall)、REK を読み出したり、インポートしたり、またはエクスポートすることができてはならない (shall not)。

FCS_CKM_EXT.1.4: REK は、**FCS_RBG_EXT.1** にしたがう RBG によって生成されなければならない (shall)。

適用上の注意：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。

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、この要件を満たすには十分ではない。

REK の生成に用いられる 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 の生成手法の記述が 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／復号アクションが隔離されており、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)。

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用いら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 鍵強度に対応するエントロピーと共にランダムに生成されなければならない (shall)。

適用上の注意：この要件の意図は、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) が変更できるよう、KEK に加えて使われる。

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、要求されている鍵サイズがデータの暗号化／復号に用いられる鍵サイズ及びモードと同一であることを判断する。

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*] でなければならない (shall)。

FCS_CKM_EXT.3.2 TSF は、PBKDF 及び [**選択**：

a) 本プロファイルを満たす RBG (FCS_RBG_EXT.1 に特定されるように)

b) [選択：XOR 操作を用いる、鍵を連結し KDF を用いる (SP 800-108 に記述されるように)、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保存するように他の KEK から合成される]

を用いてパスワード認証ファクタから KEK を導出することによって、KEK を生成しなければならない (shall)。

適用上の注意：

PBKDF は、**FCS_COP.1(5)** に従って行われる。

これらの手法のそれぞれは、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 から合成されている。合成される場合、ST 作成者はどの結合手法が用いられるかを記述しなければならず (shall)、また各ファクタの実効エントロピーが保存されることを正当化しなければならない (shall)。

保証アクティビティ：

評価者は、パスワード階層構造 TSS を検査して、すべての KEK の形成が記述されていること、そして鍵サイズが 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)。

- 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、要求されている鍵サイズがデータの暗号化／復号に用いられる鍵サイズ及びモードと同一であることを判断する。
- KEK が結合によって形成される場合、評価者は TSS に結合の手法が記述され、実効エントロピーを保存する正当化が含まれていることを検証しなければならない (shall)。

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手法に従って暗合鍵を破棄しなければならない (shall)： [選択：

- *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 EEPROM については、TSF の RBG (FCS_RBG_EXT.1 に特定されるように) 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)。*
- *揮発性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、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)。*]

適用上の注意：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。

FCS_CKM_EXT.4.2 TSF は、すべての平文鍵材料と暗号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)。

適用上の注意：この要件の目的においては、平文鍵材料とは認証データ、秘密／対称鍵、鍵の導出に用いられたデータなどを指し、REK は意味しない。鍵破棄手続きは、**FCS_CKM_EXT.4.1** に従って行われる。

例えば TOE の電源が切られている際、抹消機能が行われた際、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 (**FCS_STG_EXT.2** に従ってパスワードから導出された KEK によって保護された鍵材料に関しては、図 3 を参照のこと)。将来は、「もはや必要とされない」には、ロック状態の間に受信された機密性のあるデータを保護するために生成された鍵が含まれることになる (**FDP_DAR_EXT.2**)。

保証アクティビティ：

評価者は、平文鍵 (DEK、ソフトウェアベースの鍵ストレージ、及び KEK) のそれぞれが、システムの電源断の際、抹消機能の際、高信頼チャネルの切断の際、高信頼チャネルのプロトコルによってもはや必要とされなくなった際、ロック状態への移行 (及び、場合によっては使用直後、ロック状態にいる間など) を含め、いつクリアされるのか、そして行われるクリア手続きの種類 (暗号学的消去、ゼロで上書き、異なる交番パターンで 3 度以上上書き、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)。保護されるべきマテリアルの保存に異なる種類のメモリが用いられる場合、評価者はデータが保存されるメモリに応じたクリア手続き (例えば、「フラッシュメモリ上に保存される共通鍵はゼロで 1 度上書きすることによってクリアされるが、内部永続的ストレージデバイス上に保存される共通鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってクリアされる」) が TSS に記述されていることをチェックして保証しなければならない (shall)。

保証アクティビティの注意：以下のテストには、通常消費者のための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必要とされる。

システムの電源断の際、抹消機能の際、高信頼チャネルの切断の際、高信頼チャネルのプロトコルによってもはや必要とされなくなった際、ロック状態への移行 (及び、場合によっては使用直後、ロック状態にいる間など) を含めた鍵クリア状況のそれぞれについて、評価者は以下のテストを繰り返さなければならない (shall)。

*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、以下のテストを行わなければならない (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 の抹消

FCS_CKM_EXT.5	**拡張：TSF の抹消**

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抹消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：

- ***揮発性であろうと不揮発性であろうと、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)。***
- ***揮発性であろうと不揮発性であろうと、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、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、毎回異なる交番データパターンを用いて 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、抹消手続きの終了時に、電源が再投入されなければならない (shall)。

適用上の注意：ST 作成者は、TSF が行う抹消の手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、デバイスが抹消される方法、そして行われるクリア手続きの種類 (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用いられる場合、評価者はデータが保存されるメモリに応じたクリア手続き (例えば、「フラッシュメモリ上に保存されるデータはゼロで 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意：以下のテストには、通常消費者のための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必要とされる。

2 つの抹消手法について、保証アクティビティは異なる。

*手法 1 のテスト：*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、**FCS_CKM_EXT.4** に概要が示されるテストを用いて、**FMT_SMF.1** に提供される AGD ガイダンスに従って、また以下の **FCS_CKM_EXT.4** に特定される保証アクティビティのテスト 1、ステップ 4 に定義されるように、抹消コマンドを実行しなければならない (shall)。

*手法 2 のテスト：*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) 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)。評価者は、**FMT_SMF.1** に提供される AGD ガイダンスに従って、抹消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検査し、TSS 中に記述される手法に従ってこのデータが抹消されていることを検証しなければならない (shall)。このテストは、保護されるべきデータの保存に用いら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).

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)。

保証アクティビティ：ST 作成者は、ソルト生成に関して TSS に記述を提供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)。

(訳注) ソルト生成に関する SFR が導入されているが、どこで生成したソルトを使用するか

の記述がなく、SFR の内容が不明確である。「適用上の注意」として、どこでソルトが使用されるかを記述する必要がある：

- RSASSA-PSS signature generation
- DSA signature generation
- ECDSA signature generation
- DH static key agreement scheme
- PBKDF
- Key Agreement Scheme in NIST SP 800-56B

以上のような例が想定される。

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(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、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***] を行わなければならない (shall)。

(訳注) 上記選択肢 1 は、「AES-CBC(FIPS PUB 197、及び NIST SP800-38A) モード」とするべきである。

適用上の注意 : **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_TLS_EXT.1** 及び **FCS_CKM.1.1(3)** 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 が用いられる) 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。将来は、この標準がアップデートされ新たな暗号モードが NIST によってレビューされ承認されるのに伴い、この要件には追加的な／新たな暗号モード及び鍵長の要件が含まれるかもしれない。

保証アクティビティ：

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行わなければならない (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行わなければならない (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行わなければならない (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 つのテストを行わなければならない (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 ペアの関連付けられた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 モンテカルロテスト

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

128 ビット及び 256 ビットの鍵

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

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

2 通りの IV 長。96 ビットの IV がサポートされる場合、テストされる 2 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)。

(訳注) 上記テストは GCMVS で定義されたモンテカルロテストということになっているが、GCMVS ではモンテカルロテストは定義されておらず、上記テスト内容もモンテカルロテストではない。将来正しい記述に修正が必要である。

XTS-AES モンテカルロテスト

評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、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)。

(訳注) 上記テストは XTSVS で定義されたモンテカルロテストということになっているが、XTSVS ではモンテカルロテストは定義されておらず、上記テスト内容もモンテカルロテストではない。将来正しい記述に修正が必要である。

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

評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、AES-KW の認証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、以下の変更を 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、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のサイズが 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***] の、以下： [***FIPS Pub 180-4***] に従って [***暗号ハッシュ***] を行わなければならない (shall)。

適用上の注意:本 PP の将来の版では、SHA-1 は選択肢から削除されるかもしれない。SHA-1 によるデジタル署名の生成は 2013 年 12 月以降には許可されず、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存在する可能性のあるリスクのため、強く非推奨とされる。SHA-1 は現在、**FCS_TLS_EXT.1** 及び **FCS_CKM.1.1(3)** に適合するため要求さ

れている。

この要件の意図は、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、用いられるアルゴリズムの全体的な強度と一貫すべきである (should) (例えば、128 ビットの鍵については SHA 256)。

保証アクティビティ：

評価者は 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構成するために行われることが必要とされる構成があれば、それが存在することを判断する。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用いられるハッシュアルゴリズムのそれぞれについて、以下のテストをすべて行わなければならない (shall)。

ショートメッセージテスト—ビット指向モード

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 $1 \leq i \leq m$)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—バイト指向モード

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 $1 \leq i \leq m/8$)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF

へ提供された際に正しい結果が得られることを保証する。

疑似ランダム的に生成されたメッセージテスト

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)	**詳細化：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)***] を行わなければならない (shall)

- RSA スキームについては、FIPS PUB 186-4, “Digital Signature Standard (DSS)” のセクション 4

[選択：

- ***ECDSA スキームについては、FIPS PUB 186-4, “Digital Signature Standard (DSS)” のセクション 5 で「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] を実装***
- ***その他のアルゴリズムなし***]。

また、暗号鍵長は [***112 ビットの対称鍵強度と、同等、またはそれよりも大きく***] なければならない。

適用上の注意：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、この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_TLS_EXT.1** に適合するため要求されている。本プロファイルの将来のバージョンでは、ECDSA スキームが要求されるだろう。

保証アクティビティ：

鍵生成：(訳注) 本 SFR は署名及び署名検証であり、以下の RSA 及び ECDSA の 2 つのスキームに関する鍵生成テストは、本 SFR のテストではない。将来削除が必要である。

RSA 署名スキームの鍵生成

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

鍵ペア生成では、素数 *p* 及び *q* を生成するための 5 とおりの方法 (または手法) を特定している。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手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (must)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF によって生成された値を既知の良好な実装から生成された値と比較することによって、TSF の実装の正しさを検証しなければならない (shall)。

ECDSA 鍵生成テスト

FIPS 186-4 ECDSA 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-284 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) 機能へ提出しなければならない (shall)。

FIPS 186-4 公開鍵検証 (PKV) テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライベート鍵／公開鍵ペアを生成し、5 個の公開鍵を不正な値となるように変更し、5 個を未変更の (すなわち、正しい) 値のままにしなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

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-284 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-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージ、公開鍵及び署名の組のセットを生成し、10 組のうち 5 組で値のいずれか (メッセ

ージ、公開鍵または署名) を変更しなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

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、またはこれらのうち 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)	**詳細化：暗号操作**

FCS_COP.1.1(4) TSF は、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***] であって、暗号鍵長が [**割付：HMAC に用いられる (ビット単位の) 鍵長**]、そしてメッセージダイジェストのサイズが 160 及び [***選択：256、384、512、その他なし***] ビットの、以下：[***選択：FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code、及び FIPS Pub 180-4, "Secure Hash Standard***] を満たすものに従って [*鍵付きハッシュによるメッセージ認証*] を行わなければならない (shall)。

適用上の注意：この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用いら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_TLS_EXT.1** 及び **FCS_CKM.1.1(3)** に適合するため要求されているが、本文書の将来の版では削除されるかもしれない。

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、用いられるハッシュ関数、ブロックサイズ、及び用いられる出力 MAC 長。

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機能

FCS_COP.1(5)	詳細化：暗号操作

FCS_COP.1.1(5) TSF は、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、出力暗号鍵のサイズが [選択：***128, 256***] ビットの、以下：[NIST SP 800-132] を満たすものに従って [***パスワードベースの鍵導出機能***] を行わなければならない (shall)。

適用上の注意：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)。将来の要件では、少なくとも 1000 回の PBKDF 反復処理が要求されることになる。

このパスワードは、KEK への入力として用いら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。用いられる手法は ST 作成者によって選択される。800-132 では、HMAC と認可済み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、用いら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を含む。

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手法が 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用いられ、そしてそれが **FCS_CKM_EXT.2** に特定される DEK 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 の形成に用いら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。

5.2.3 初期化ベクトル生成 (FCS_IV)

FCS_IV_EXT.1	拡張：初期化ベクトル生成

FCS_IV_EXT.1.1 TSF は、表 11：「NIST 認可暗号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)。

適用上の注意：表 11 には、暗号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、この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)。

5.2.4 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)***、***Dual_EC_DRBG (任意)***] を用いる ***NIST Special Publication 800-90A***、***FIPS Pub 140-2 附属書 C：AES を用いる 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) 。

(訳注：***Dual_EC_DRBG*** は、NIST SP 800-90A から削除される予定である)

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、最小で [選択：***128 ビット***、***256 ビット***] の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)。

適用上の注意: NIST Special Pub 800-90B の附属書 C には、直ちに用いるべき (should) であり、また本 PP の将来の版で要求されることになる、最小エントロピー量が記述されている。

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、4 つの異なる乱数生成手法が含まれる。これらはそれぞれ、基盤となる暗号プリミティブ (ハッシュ関数／暗号) に依存している。ST 作成者は利用される関数を選択し (SP 800-90A が選択されている場合)、要件または TSS に用いられる具体的な基盤となる暗号プリミティブを含む。特定されたハッシュ関数 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) はいずれも Hash_DRBG または HMAC_DRBG に許可されるが、CTR_DRBG には AES ベースの実装のみが許可される。SP800-90A に定義された任意の曲線が Dual_EC_DRBG に許可される一方で、ST 作成者は選択された曲線だけではなく、利用されるハッシュアルゴリズムも含めなければならない (must)。

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 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に記述される手法のみが有効であることに注意されたい。ここで用いられる AES 実装の鍵の長さが利用者データの暗号化に用いら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。FCS_RBG_EXT.1.2 の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

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)。

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-512 (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。

将来、本プロファイルでは少なくとも 1 つのハードウェアベースのノイズ源が要求されることになる。ST 作成者は、追加的なノイズ源を選択してもよい。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。

同様に、正確かつ予測可能な規則では説明できない変動的なふるまいをするハードウェアコンポーネントであれば、ハードウェアベースのノイズ源として用いることができる。また、少なくともひとつのノイズ源がハードウェアベースである限り、複数の独立したノイズ源を用いて発生するエントロピーを増大させ、攻撃の可能性を減少させる (攻撃者が複数のランダムビットストリームを攻略しなければならないため) ことも可能である。機械的な入出力デバイスやシステムカウンタによって引き起こされる割り込みのタイミングは、この要件の目的では*ハードウェアベース*のノイズ源とみなされないことに注意すべきである (should)。

保証アクティビティ：

附属書 E 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)。

評価者は、RBG が準拠する標準に従って、以下のテストを行わなければならない (shall)。

FIP 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行わなければならない (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行わなければならない (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 が構成可能な場合、評価者は各構成について 15 回の試行を行わなければならない (shall)。また評価者は、RNG 機能を構成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。
>
> **Additional Input**：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。

5.2.5 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_COP.1(1)
- FCS_COP.1(3)
- FCS_COP.1(2)
- FCS_COP.1(4)
- FCS_COP.1(5)
- FCS_CKM.1(1)

[選択：

- ***FCS_CKM.1(2),***
- ***その他の暗号操作なし***]。

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、検証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。

5.2.6 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。

5.2.6.1 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)。

適用上の注意：このセキュアな鍵ストレージは、**FCS_STG_EXT.2** によって要求されるように保護されるハードウェア内またはソフトウェア内で完全に実装されてもよい。対称鍵、永続的秘密、及び ECDSA のセキュアな鍵ストレージのサポートは、将来の版でテストされることになる。

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)。

適用上の注意：ST 作成者が利用者のみを選択した場合、ST 作成者は **FMT_MOF.1.1(1)** 中の機能 14 もまた選択しなければならない (must)。

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)。

適用上の注意：ST 作成者が利用者のみを選択した場合、ST 作成者は **FMT_MOF.1.1(1)** 中の機能 15 もまた選択しなければならない (must)。

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***] のみが明示的に認可することができる。

適用上の注意: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.1.1** 中の機能 39 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.1.1(1)** 中の機能 25 もまた選択しなければならない (must)。

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***] のみが明示的に認可することができる。

適用上の注意: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.1.1** 中の機能 40 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.1.1(1)** 中の機能 26 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 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手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用いら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。

- ECDSA については、秘密はデータの署名に用いられなければならない (shall)
- 対称アルゴリズムについては、秘密はデータの暗号化に用いら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。

保証アクティビティの注意：以下のテストには、通常消費者のための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必要とされる。

*テスト 5:*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、**FCS_CKM_EXT.4** に概要が示されるテストを用いて、**FMT_SMF_EXT.1** に提供される AGD ガイダンスに従って、また以下の **FCS_CKM_EXT.4** に特定される保証アクティビティのテスト 1、ステップ 4 に定義されるように、鍵／秘密を破棄しなければならない (shall)。

5.2.6.2 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：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 へ連鎖する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 へ連鎖するKEK 及びパスワードから導出されたKEK による暗号化]***

]。

適用上の注意：

REK 及びパスワードから導出されたKEK は、この要件を満たすために合成されて合成KEK を形成してもよい (**FCS_CKM_EXT.3** に記述されるように)。

機密性のあるデータは、REK 及びパスワードによって保護されなければならない (shall)。本体に **FDP_DAR_EXT.2** 及び **FCS_DAR_EXT.3** が含まれる場合、この機密性のある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)。機密性のあるデータは、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 を満たし機密性のあるデータに適当であり、DEK_2 は 1b を満たし機密性のある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。

保証アクティビティ：

評価者はTSS をレビューして、保存データ保護に用いられる各DEK、ソフトウェアベースの鍵ストレージ、そして DEK 及び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 の保護の鍵階層構造の記述がTSS に含まれることを判断しなければならない (shall)。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)。この記述には、**FCS_RBG_EXT.1** によって記述される機能が呼び出されて DEK を生成する方法 (**FCS_CKM_EXT.2**)、鍵のそれぞれについて鍵のサイズ (**FCS_CKM_EXT.2** 及び **FCS_CKM_EXT.3**)、各 KEK が形成される方法 (生成、導出、または **FCS_STG_EXT.3** による合成)、暗号化された鍵のそれぞれについて完全性保護メカニズム (**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 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、対応する要件にしたがう。

FCS_STG_EXT.2.2 すべての鍵は、 [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)。

適用上の注意：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。この要件は、本 PP で定義される KEK にのみ適用され、他の標準中で特定される KEK には適用されない。

保証アクティビティ：

評価者は、TSS の鍵階層構造セクションを検査して、鍵のそれぞれ (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いずれかを用いて、セキュリティ強度が同一またはより大きい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 TSS 中の鍵階層構造の記述を検査して、DEK とソフトウェアによって保存された鍵のそれぞれが **FCS_STG_EXT.2** に従って暗号化されることを検証しなければならない (shall)。

5.2.6.3 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 KEK 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** にしたがう暗号化の [**選択：GCM、CCM、鍵ラップ、パディング付き鍵ラップ**] 暗号モード*、
- ***FCS_STG_EXT.2** によって保護される鍵によって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** によって保護される鍵を用いる鍵付きハッシュ (**FCS_COP.1(4)**)*、
- ***FCS_STG_EXT.2** に従って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***] 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)。

適用上の注意：1 つの鍵が、これらの手法の複数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、製品はある種類の鍵には 1 つの完全性保護手法を使い、別の種類の鍵には別の手法を用いるかもしれない。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、要件のそれぞれにおいて対処される (**FCS_COP.1.1(2), FCS_COP.1(4), FCS_CKM.1**)。

保証アクティビティ：

評価者は TSS 中の鍵階層構造の記述を検査して、暗号化された鍵のそれぞれが、**FCS_STG_EXT.3** 中の選択肢のいずれかに従って完全性保護されることを検証しなければならない (shall)。

5.2.7 TLS プロトコル (FCS_TLS)

(訳注) TLS は、特定の鍵導出関数の適用が求められており、NIST SP800-135 rev.1 が鍵導出関数 KDF として考慮されなければならない。

5.2.7.1 EAP-TLS プロトコル

FCS_TLS_EXT.1	拡張：EAP TLS プロトコル

FCS_TLS_EXT.1.1 TSF は、RFC 5216 に特定される EAP-TLS プロトコルを、TLS 1.0 (RFC 2246) 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***] を実装し、以下の暗号スイートをサポートすることによって、実装しなければならない (shall) [

- *RFC 3268 による必須暗号スイート：*
  - *TLS_RSA_WITH_AES_128_CBC_SHA*
- *[**選択：オプションの暗号スイート：***

- ***TLS_RSA_WITH_AES_256_CBC_SHA***
- ***TLS_DHE_RSA_WITH_AES_128_CBC_SHA***
- ***TLS_DHE_RSA_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_GCM_SHA256***
- ***RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384***
- ***RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256***
- ***RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384***
- ***その他の暗号スイートなし***]]

適用上の注意：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、この要件によって制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである (should)。必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである (should)。テスト環境中のサーバ上で評価される構成において管理的に用いられることが可能な暗号スイートを制限することは必要である。

TLS 1.2 は望ましいプロトコルであり、将来は EAP-TLS に要求されることになるかもしれない。しかし、TLS 1.0 は現在 RFC 5216 へ確実に準拠するため必要とされている。TLS 1.2 は、**FCS_TLS_EXT.2** のために必要とされる。上に列挙した Suite B アルゴリズム (RFC 6460) は、実装に望ましいアルゴリズムである。

FCS_TLS_EXT.1.2 TSF は、EAP-TLS に提示されたサーバ証明書が [選択：***特定された CA のいずれかへ連鎖する、受容可能な認証サーバ証明書の特定された FQDN を含む***] ことを検証しなければならない (shall)。

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

保証アクティビティ：

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが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 TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述に適合するように TOE を構成するための指示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、証明書への署名が許可される認証局のリストを構成するための、または EAP-TLS 交換において TOE によって受容される認証サーバ証明書の FQDN を構成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 への準拠をテストするため、将来はさらにテストが追加されるかもしれない。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 :* 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、EAP セッションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分で

あり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。

- *テスト 2 :* 以下のテストは、サポートされている証明書署名アルゴリズムのそれぞれについて、繰返し行われる。評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含む認証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 :* AGD ガイダンスによって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「受容可能」と設定され、次に評価者はワイヤレス接続を開始し、ワイヤレスクライアントの接続が成功することを検証する。次に評価者は、証明書が TOE によって許可されない CA によって署名される、または TOE によって許可されない FQDN を提示するが、それ以外の点では有効であるようにシステムを設定する。そのような証明書を提示する認証サーバへの認証試行は、接続が拒否される結果となるべきである (should)。TOE が受容可能な認証サーバを制限する両方の手法をサポートする場合、評価者はこのテストを 2 回 (各手法について 1 回ずつ) 繰り返さなければならない (shall)。
- *テスト 4 :* 評価者は、サーバによって選択された暗号スイートとマッチしない証明書を TLS 接続中に送信する (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) よう認証サーバを設定しなければならない (shall)。評価者は、TOE が サーバの証明書ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- *テスト 5 :* 評価者は、TOE と認証サーバとの間に中間者ツールを設定しなければならず (shall) 、また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 ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、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中のサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージ中に存在しない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない (shall) 。
    - *(条件付き)* DHE または ECDHE 暗号スイートがサポートされる場合、ServerKeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange を受信した後に接続を拒否することを検証する。
    - サーバの CertificateRequest ハンドシェイクメッセージ中の CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない (must not)。評価者は、サーバがクライアントの Finished ハンドシェイクメッセージを受信した後に接続を拒

否することを検証しなければならない (shall) 。

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

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)。

適用上の注意：この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の取得
- 現在の GPS 位置情報の取得
- システムワイドな認証情報ストアからの認証情報の読み出し
- 連絡先リスト／アドレス帳の読み出し
- 保存された写真の読み出し
- テキストメッセージの読み出し
- 電子メールの読み出し
- デバイス ID 情報の読み出し
- ネットワークアクセスの取得

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)。また評価者は、これらのシステムサービスとアプリケーションがインタフェースする方法、そしてこれらのシステムサービスが TSF によって保護される手段が、TSS に記述されていることも保証しなければならない (shall)。

TSS には、各システムサービスが以下のどのカテゴリに分類されるのか記述されなければならない (shall)。

1) 一切のアプリケーションにアクセスが許可されないもの
2) 特権を持つアプリケーションにアクセスが許可されるもの
3) 利用者認証によってアプリケーションにアクセスが許可されるもの
4) すべてのアプリケーションにアクセスが許可されるもの

特権を持つアプリケーションには、TSF 開発者によって開発された任意のアプリケーションが含まれる。TSS には、サードパーティアプリケーションへ特権が付与される方法が記述されなければならない (shall)。両方の種類の特権を持つアプリケーションについて、この特権がどのように、いつ検証されるのか、そして TSF が特権を持たないアプリケーションによるこれらのサービスのアクセスを防止する方法が TSS に記述されなければならない (shall)。

利用者がアクセスを付与できる任意のアプリケーションについて、利用者に認証を求めるプロンプトが表示されるのはそのアプリケーションがインストールされたときか、またはランタイム中なのか、TSS に特定されていることを評価者は保証しなければならない (shall)。

保証アクティビティの注意：以下のテストには、通常消費者のための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)。

*テスト 1：*一切のアプリケーションにアクセスが許可されない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り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その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にアクセスが許可される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り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その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り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その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付与できる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り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、または利用者認証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)。利用者認証を求めるプロンプトの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 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その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)。

5.3.2 保存データの保護 (FDP_DAR)

FDP_DAR_EXT.1	**拡張：保存データの保護**

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

適用上の注意：F.1「用語集」に定義されるように、保護データはすべての利用者またはエンタープライズデータを含む、すべての非 TSF データである。

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

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のか、そしてどのデータが TSF データのみなされるのか、ST の TSS セクション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、このデータにすべての保護データが含まれることを保証しなければならない (shall)。

評価者は AGD ガイダンスをレビューして、設定の記述と DAR 保護の利用によって、利用者に設定及び認証情報の提供以外のいかなるアクションも行うことが要求されないことを判断しなければならない (shall)。また評価者は AGD ガイダンスをレビューして、設定によって利用者にファイルごとに暗号化を特定することが要求されないことを判断しなければならない (shall)。

保証アクティビティの注意：以下のテストには、通常消費者のための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必要とされる。

*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、ファイルの作成によって、またはアプリケーションを用いることによって、利用者データ (非システム) 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、製品の電源がオフの際にこのデータが暗号化されていることを、**FIA_UAU_EXT.1** のテスト 1 と組み合わせて、検証しなければならない (shall)。

5.3.3 証明書データストレージ (FDP_STG)

FDP_STG_EXT.1(1)	**拡張：利用者データストレージ**

FDP_STG_EXT.1.1(1) TSF は、トラストアンカーデータベースに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、実装されたトラストアンカーデータベースが TSS に記述されていることを保証しなければならない (shall)。この記述には、証明書がストレージへロードされる方法と、**FMT_SMF.1**、**FMT_MOF.1(1)**、及び **FMT_MOF.1(2)** で確立されたアクセス権限に従ってストレージを不正なアクセスから保護する方法 (例えば、unix パーミッション) に関する情報が含まれなければならない (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、 [***その利用者による最後の認証の成功***] に関連して [[**割付：受容可能な値の範囲**] ***以内の管理者によって設定可能な正の整数***] 回の認証試行の不成功が発生した際に、これを検出できなければならない (shall)。

適用上の注意：正の整数は、**FMT_SMF.1.1** の機能 2c に従って設定される。

FIA_AFL_EXT.1.2 認証試行の不成功が定義された回数 [選択：***に達した、を超えた***] 際、TSF は [[選択：***すべての保護データの完全な抹消、管理者によって設定される修正アクション***] ***を行わ***] なければならない (shall)。

適用上の注意：完全な抹消は、**FCS_CKM_EXT.5** に従って行われる。ST 作成者が 2 番目の選択で管理者によって設定される修正アクションを選択した場合、ST 作成者は認証失敗を **FMT_SMF_EXT.1** 中の管理者によって設定されるトリガーの 1 つとして列挙しなければならない (must)。

保証アクティビティ：

評価者は、最後の認証の成功からの不成功認証試行の回数に対応した値が利用者ごとに記録されていることが、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、不成功認証試行の回数の上限と、その上限に達するか超えた際に行われるべき修正アクション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)。

テスト1: 評価者はAGDガイダンスに従って不成功認証試行の回数の上限と、その上限に達するか超えた際に行われるべき修正アクションをデバイスに設定しなければならない (shall)。評価者はロック状態に入り、修正アクションが発生するまで正しくない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に対応していること、そして修正アクションが実装されていることを検証しなければならない (shall)。

5.4.2 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***] に準拠しなければならない (shall)。

適用上の注意：この要件は、802.1X認証のやり取りにおけるサプリカントとしてのTSFの役割をカバーする。このやり取り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のやり取り) の結果としてPMKを導出し、ワイヤレスアクセスシステム (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、やり取りの間には少なくとも2つの通信経路が存在する。ひとつはワイヤレスアクセスシステムとのもの、もうひとつはワイヤレス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ワイヤレス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セッション (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、ワイヤレス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、以下のテストを行わなければならない (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論証しなければならない (shall)。ワイヤレス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論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論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論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)。

5.4.3 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)。

適用上の注意：一部の会社のポリシーでは 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 の利用と耐破壊性 (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用いた物理アクセスを行う攻撃者の脅威に対抗する。

ST 作成者は、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 文字を含む割付けられた別の文字セットのいずれかの文字セットを選択する。割付けられた文字セットは、国際エンコーディング標準 (Unicode など) にしたがうか、または ST 作成者による割付中で定義されることによって、明確に定義されなければならない (must)。また ST 作成者は、TOE によってサポートされる特殊文字も選択する。これらには、割付を用いてサポートされる追加的な特殊文字が、オプションとして列挙されてもよい。

保証アクティビティ：

評価者は操作ガイダンスを検査して、強いパスワードの構成に関してセキュリティ管理者へガイダンスが提供されていること、そして最小パスワード長の設定に関して指示が提供されていることを判断しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。これらのテストの 1 つ以上が、単一のテストケースによって実施でき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と、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、両方を作成しなければならない (shall)。パスワードのそれぞれについて、評価者は TOE がそのパスワードをサポートすることを検証しなければならない (shall)。評価者にはパスワードのすべてのあり得る組み合わせをテストすることは要求されない (または、それは不可能でもある) 一方で、評価者は要件に列挙されたすべての文字、ルールの特徴、及び最小の長さがサポートされていることを保証し、テストのために選ばれたこれらの文字のサブセットを正当化しなければならない (shall)。

5.4.4 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、正しくない認証試行間に遅延時間を強制する***] 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***] 回未満となるようなものでなければならない (shall)。

適用上の注意：この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タイミングの遅延時間を用いることによって、要件中の遅延時間のタイミングを実装することができる。

この要件に特定される最小遅延時間は、パスワードのブルートフォース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される時間 (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、認証試行を自動化不可能とする手段が 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か、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が 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)。

5.4.5 利用者認証 (FIA_UAU)

5.4.5.1 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、認証が行われている間に利用者へ [***デバイスの画面上で見えなくされたフィードバック***] のみを提供しなければならない (shall)。

適用上の注意：TSF は、各文字を短時間 (1 秒未満) 表示したり、利用者にパスワードのマスクを解除する選択肢を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あいまい化する手段が 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、この要件の設定が存在する場合、それが AGD ガイダンス中で対処されていること、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、少なくともロックスクリーン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、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)。

5.4.5.2 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、起動時の際、保護されたデータ及び鍵の復号を行う前に、利用者に対して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)。

適用上の注意：この要件の意図は、パスワード認証ファクタを用いて利用者がデバイスへ認証される以前の保護データの復号を防止することである。またパスワード認証ファクタは、機密性のあるデータの復号に用いられる鍵を導出するためにも必要とされる (F.1「用語集」及び D.3.2「保存データの保護 (FDP_DAR)」参照)。これには少なくとも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。

保証アクティビティ：

評価者は、保護データ及び鍵を復号するプロセスが 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、このプロセスによって利用者にパスワード認証ファクタの入力が要求されること、そして **FCS_CKM_EXT.3** に従って、ソフト

ウェア鍵ストレージ及び (オプションとして) **FCS_STG_EXT.2** に従って機密性のあるデータの 1 つまたは複数の DEK を保護するために用いられる KEK が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** 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意：以下のテストには、通常消費者のための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必要とされる。

*テスト 1：*評価者は、AGD ガイダンスに従って保護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、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)。

評価者はデバイスをリブートし、開発者によって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を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、デバイスの機能全て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、開発者によって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を発見でき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 ガイダンスに従って利用者認証を要求しなければならない (shall)。評価者は、鍵を生成しソフトウェアベースのセキュアな鍵ストレージ中に保存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)。

評価者はデバイスをロックし、開発者によって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鍵を検索し、そして鍵を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、デバイスの機能全て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、開発者によって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鍵を検索し、そして一意の文字列 (訳注：鍵の間違いか) を発見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、AGD ガイダンスに従って機密性のある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、機密性のあるデータ (これはデータまたは鍵であってもよい) 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)。

評価者はデバイスをロックし、開発者によって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を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、デバイスの機能全て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、開発者によって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を発見できることを検証しなければならない (shall)。

5.4.5.3 認証のタイミング

FIA_UAU_EXT.2	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、利用者に代わって [***選択：[割付*：*アクションのリスト***]、***アクションなし***] が行われることを許可しなければならない (shall)。

FIA_UAU_EXT.2.2 TSF は、あらゆる利用者に代わってそれ以外の任意の TSF 仲介アクションを許可する前に、その利用者の認証の成功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、ロック状態で不正な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何らかのアクションを行うことを試行し、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)。

5.4.5.4 再認証

FIA_UAU_EXT.3	拡張：再認証

FIA_UAU_EXT.3.1: TSF は、利用者が自分のパスワード認証ファクタを変更する際、ロック解除状態へ移行するための TSF 及び利用者主導のロックの後、そして [***選択：[割付：その他の条件***]、***その他の条件なし***] に、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)。

適用上の注意：TSF 及び利用者主導のロックは、**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 ガイダンスに従って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 ガイダンスに従ってパスワード認証ファクタを変更し、TSF がファクタの変更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 ガイダンスに従って非アクティブ時間 (**FMT_SMF.1**) の経過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 ガイダンスに従って利用者主導の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)。

5.4.6 X509 証明書 (FIA_X509)

5.4.6.1 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、以下のルールに従って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認証パス検証。
- 認証パスは、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って、認証パスを検証しなければならない (shall)。
- TSF は、 [選択：***RFC 2560 に特定されるオンライン証明書状態プロトコル (OCSP)、RFC 5759 に特定される証明書失効リスト (CRL)***] 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、以下のルールに従って extendedKeyUsage フィールドを検証しなければならない (shall)。
  - 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、コード署名目的 (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) を持たなければならない (shall)。
  - TLS に提示されるサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) を持たなければならない (shall)。

適用上の注意：**FIA_X509_EXT.1.1** には、証明書有効性確認を行うためのルールが列挙されている。ST 作成者は、失効状態が OCSP か CRL のどちらを用いて検証されるか選択しなければならない (shall)。**FIA_X509_EXT.2** は、証明書が EAP-TLS に利用されることを要求している。この利用によって、extendedKeyUsage ルールが検証されることが要求される。証明書は、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**) にオプションとして用いてもよく、また実装されている場合には、コード署名目的 extendedKeyUsage を含むことが検証されなければならない (must)。

FIA_X509_EXT.1.1 は TOE プラットフォームに、TLS サーバによって提示される証明書に関して一定のチェックを行うことを要求しているが、クライアントによって提示される証明書に関して認証サーバが行わなければならない (have to) これに対応するチェックも存在する。すなわち、クライアント証明書の extendedKeyUsage フィールドに "Client Authentication" が含まれ、また鍵共有 (key agreement) ビット (Diffie-Hellman 暗号スイートの場合) または鍵暗号化 (key encipherment) ビット (RSA 暗号スイートの場合) がセットされていることである。TOE による使用のため取得される証明書がエンタープライズ内で使用されるためには、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 高信頼チャネルで EAP-TLS をサポートするために要求される。

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にのみ、証明書を CA 証明書として取り扱わなければならない (shall)。

適用上の注意：この要件は、TSF によって用いられ処理される証明書に適用され、トラストアンカーデータベースに追加され得る証明書を制約する。

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 TSS に記述されていることを保証しなければならない (shall)。また評価者は、認証パス検証アルゴリズムの記述も TSS に提供されていることも確認する。

記述されるテストは、FIA_X509_EXT.2.1 及び FIA_X509_EXT.3 中の使用事例を含め、他の証明書サービス保証アクティビティと組み合わせて行われなければならない (must)。extendedKeyUsage ルールのテストは、これらのルールを要求する用途と組み合わせて行われる。

テスト 1 : 評価者は、有効な認証パスのない証明書の有効性確認を行うと、その機能 (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) が失敗することを論証しなければならない (shall)。次に評価者は、その機能で使われる証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを論証しなければならない (shall)。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない (shall)。

テスト 2 : 評価者は、有効期限を過ぎた証明書の有効性確認を行うと、その機能が失敗する

ことを論証しなければならない (shall)。

テスト 3 : 評価者は、CRL と OCSP のどちらが選択されているかに応じて、TOE が失効した証明書を適切に処理できることをテストしなければならない (shall)。両方とも選択されている場合には、それぞれの手法についてテストが行われる。評価者は信頼の連鎖の 1 つ上位のみをテストする必要がある (将来の版では、上位の連鎖全体について検証が行われることを保証することが要求されるかもしれない)。評価者は、有効な証明書が用いられること、そして証明書有効性確認機能が成功することを保証しなければならない (shall)。次に評価者は、失効するはずの証明書 (選択において選択された手法のそれぞれについて) を用いてテストを試行し、もはや証明書が有効ではない場合には証明書有効性確認機能が失敗することを保証する。

テスト 4 : 評価者は、TOE の証明書を発行する CA の証明書に basicConstraints 拡張が含まれないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗する。

テスト 5 : 評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグがセットされていないような認証パスを構築しなければならない (shall)。この認証パスの検証は失敗する。

テスト 6 : 評価者は、TOE の証明書を発行する CA の証明書の basicConstraints 拡張中の cA フラグが TRUE にセットされているような認証パスを構築しなければならない (shall)。この認証パスの検証は成功する。

5.4.6.2 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、RFC 5280 によって定義される X.509v3 証明書を用いて EAP-TLS のやり取りの認証、及び [***選択：IPsec、TLS、HTTPS、DTLS***] 、ならびに [***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***] をサポートしなければならない (shall)。

適用上の注意：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、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、ならびに完全性検証 (**FPT_TST_EXT.2**) にオプションとして用いてもよい。これらのコード署名用途のいずれかが選択される場合、**FIA_X509_EXT.2.4** が本体へ含まれなければならない (must)。**FPT_TUD_EXT.2.5** が本体へ含まれる場合、選択に「モバイルアプリケーションのコード署名」が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判断する接続を確立できないとき、TSF は [選択：***このような場合には証明書を受容するかどうかの選択を管理者に許可する、証明書を受容する、証明書を受容しない***] ようにしなければならない (shall)。

適用上の注意：CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態の検証を行うために接続を確立しなければならない (must) 場合は多々生ずる。この選択は、そのような接続が確立できない場合 (例えば、ネットワークエラーのため) のふるまいを記述するために用いられる。TOE が、証明書は **FIA_X509_EXT.1** 中の他の全てのルールに従って有効であると判断した場合、2 番目の選択に示されるふるまいによって有効性が判断されなければならない (shall)。証明書が **FIA_X509_EXT.1** 中の他の有効性確認ルールのいずれかに失敗する場合、TOE はその証明書を受容してはならない (must not)。ST 作成者によって管理者設定オプションが選択された場合、ST 作成者は **FMT_SMF.1** 中の機能 32 もまた

選択しなければならない (must)。

FIA_X509_EXT.2.3 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)。

適用上の注意 : 高信頼通信チャネルには、WLAN 及び TSF によって行われる IPsec、TLS、HTTPS、または DTLS のいずれかが含まれる。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 :

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

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

評価者は、証明書の使用を要求する **FIA_X509_EXT.2.1** に列挙される機能のそれぞれについて、テスト 1 を行わなければならない (shall)。

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

テスト 2 : 評価者は、TOE 以外の IT エンティティとの通信によって、有効な証明書の使用には少なくとも一部の証明書有効性確認のチェック実行が必要とされることを論証しなければならない (shall)。次に評価者は、TOE が証明書の有効性を検証できないように環境を操作し、**FIA_X509_EXT.2.2** で選択されたアクションが行われることを確認しなければならない (shall)。選択されたアクションが管理者によって設定可能である場合には、評価者は操作ガイダンスに従って、サポートされているすべての管理者設定可能オプションが、文書化されているようにふるまうことを判断しなければならない (shall)。

5.4.6.3 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、要求側のアプリケーションに有効性確認の成功または失敗を回答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 文書に、この要件に記述されるセキュリティ機能 (証明書有効性確認) が含まれることを検証しなければならない (shall)。本文書は、結果が成功と失敗のどちらを示すのかに関し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、検証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、**FDP_STG_EXT.1**、**FDP_ITC_EXT.1**、**FMT_SMF.1.1** の機能 14、及び **FIA_X509_EXT.1** によって要求されるテストに従ってインポート、削除、変更、及び有効性確認が正しく行われることを検証するために用いてもよい。

5.5 クラス：セキュリティ管理 (FMT)

利用者と管理者のどちらも TOE を管理し得る。しかし、管理者はデバイス上で分離された役割ではない。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。

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。これらの管理機能は、利用者に提供される管理機能とは異なるセットになるであろう。管理者ではなく、利用者に提供される管理機能は、**FMT_MOF.1(1)** に列挙される。利用者がその機能を行うことを制約するポリシーを管理者が採用し得る管理機能は、**FMT_MOF.1(2)** に列挙される。

表 12 に、以下の 3 つの要件 (**FMT_MOF.1(1)**、**FMT_MOF.1(2)**、及び **FMT_SMF.1**) 中で本プロテクションプロファイルによって要求される管理機能の比較を示す。

5.5.1 TSF 内の機能の管理 (FMT_MOF)

FMT_MOF.1	**セキュリティ機能のふるまいの管理**

FMT_MOF.1.1(1) TSF は、[

1. TOE を以下について管理させる

[***選択：***

2. VPN 保護の有効化／無効化、

3. [割付：無線のリスト] の有効化／無効化、

4. [割付：外部アクセス可能なハードウェアポートのリスト] 上のデータ転送機能の有効化／無効化、

5. [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、

6. 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. なし]***

7. 開発者モードの有効化／無効化、

8. 保存データ保護の有効化、

9. リムーバブルメディアの保存データ保護の有効化、

10. ローカル認証バイパスの有効化／無効化、

11. *携帯電話ネットワークとその他のネットワークとの通信に用いられるアクセスポイント名及びプロキシの設定*
12. *Bluetooth 高信頼チャネルの設定*
    a. *ディスカバリーモードの無効化*
    b. *Bluetooth のバージョン1.0、1.1、1.2、2.0、及び [割付：その他の Bluetooth バージョン番号] を用いた接続の禁止*
    c. *[選択：Bluetooth プロファイルの制限、レガシーペアリング及び Just Works ペアリングの無効化、及び [選択： [割付：その他のペアリング手法]、その他のペアリング手法なし]]、*
13. *機密性のあるデータの抹消*
14. *セキュアな鍵ストレージへの鍵／秘密のインポート、*
15. *セキュアな鍵ストレージにある、利用者によって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]] の破壊*
16. *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、*
17. *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インポート及び削除の承認、*
18. *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、*
19. *携帯電話音声機能の有効化／無効化、*
20. *デバイスメッセージング機能の有効化／無効化、*
21. *携帯電話基地局への接続に用いられる携帯電話プロトコルの有効化／無効化、*
22. *デバイス機能の音声コマンドコントロールの有効化／無効化、*
23. *TSF によって記録された監査ログの読み出し、*
24. *アプリケーション上のデジタル署名の検証に用いられる [選択：証明書、公開鍵] の設定、*
25. *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*
26. *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／秘密の破壊の例外の承認*
27. *[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]、その他の管理機能なし]*
28. *その他の機能なし]*

]] 機能を [実行する] 能力を利用者に対して制限しなければならない (shall)。

適用上の注意：

ST 作成者は、利用者のみが行うことができるセキュリティ管理機能を選択すべきである (should)。

機能 1 について、登録機能にはデバイスへ適用されるべきポリシーも含まれる。利用者承認通知が、その通知中のポリシーをすべて列挙するのではなく、ポリシーの閲覧を (例えば、「View」アイコンを「タップ」することによって) 意図的に選択することを利用者に要求することは許容可能である。

機能 3 の割付は、Wi-Fi、GPS、携帯電話、NFC、そして Bluetooth など、すべての無線であって、有効化及び無効化が可能なものから構成される。

機能 4 の割付は、USB、SD カード、そして HDMI など、すべての外部アクセス可能なハードウェアポートであって、そのデータ転送機能が有効化及び無効化可能なものから構成される。

機能 5 の割付は、WiFi テザリングなど、TSF がサーバとしてふるまうすべてのプロトコルであって、有効化及び無効化が可能なものから構成される。

機能 6 の通知の表示の設定は、**FTA_SSL_EXT.1** の選択で許可された機能であってもよい。

機能 17 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の X.509v3 証明書のインポートまたは削除を許可し、また利用者のみが要求を承認し得る場合に含まれることがある。これらのアプリケーションには、MDM エージェントは含まれない。この機能は、証明書を信頼して自分自身を検証するアプリケーションには適用されない。この機能は、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変更し、それが他のアプリケーションについて TSF によって行われる検証に影響するような状況にのみ適用される。利用者または管理者には、この要件を満たすために任意のアプリケーション要求をグローバルに許可または拒否する能力が提供されてもよい。

機能 19 を行う能力には、(緊急ダイヤルを除いて) 完全に音声呼を無効化する能力が含まれる。

機能 20 を行う能力には、(キャリアによって要求されるもの及び緊急 SMS を除いて) 完全にデバイスメッセージングを無効化する能力が含まれる。デバイスメッセージング機能には、SMS、MMS、そしてボイスメールが含まれる。

保証アクティビティ：

評価者は、**FMT_SMF.1** の TSS 記述と関連して、利用者によってのみ行われ得る管理機能が TSS に記述されていることを検証しなければならない (shall)。

FMT_MOF.1.1(2) TSF は、以下の機能を行う能力を [

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
2. セッ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
3. [**割付：音声または映像収集デバイスのリスト**] の有効化／無効化
4. 以下によるアプリケーションのインストールの設定：

a. 1 つまたは複数の正当なアプリケーションリポジトリの特定、

b. 許可されるアプリケーション及びバージョンのセットの特定 (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の拒否]、

[*選択：*

5. VPN 保護の有効化／無効化

6. [割付：無線のリスト] の有効化／無効化

7. [割付：外部アクセス可能なハードウェアポートのリスト] 上のデータ転送機能の有効化／無効化、

8. [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、

9. TSF が接続できるワイヤレスネットワーク (SSID) の特定、

10. 各ワイヤレスネットワークのセキュリティポリシーの設定：

a. [選択：1 つまたは複数の CA を特定してそこからの 1 つまたは複数の WLAN 認証サーバ証明書を TSF が受容する、1 つまたは複数の FQDN を特定してその 1 つまたは複数の WLAN 認証サーバ証明書を受容可能とする]

b. セキュリティの種類を特定する能力

c. 認証プロトコルを特定する能力

d. 認証に用いられるべきクライアント認証情報の特定

e. [割付：任意の追加的な WLAN 管理機能]

11. 開発者モードの有効化／無効化、

12. 保存データ保護の有効化、

13. リムーバブルメディアの保存データ保護の有効化、

14. ローカル認証バイパスの有効化／無効化、

15. 携帯電話ネットワークとその他のネットワークとの通信に用いられるアクセスポイント名及びプロキシの設定

16. Bluetooth 高信頼チャネルの設定

a. 検出可能 (Discoverable) モードの無効化

b. Bluetooth のバージョン 1.0、1.1、1.2、2.0、及び [割付：その他の Bluetooth バージョン番号] を用いた接続の禁止

c. [選択：Bluetooth プロファイルの制限、レガシーペアリング及び JustWorks ペアリングの無効化、及び [選択： [割付：その他のペアリング手法]、その他のペアリング手法なし]]、

17. 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. なし]

18. トラストアンカーデータベースへの／からの X.509v3 証明書のインポート及び削除、

19. 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、または確立を禁止するかの設定、

20. トラストアンカーデータベース中の X.509v3 証明書のアプリケーションによるインポート及び削除の承認、

21. 携帯電話音声機能の有効化／無効化、

22. デバイスメッセージング機能の有効化／無効化、

23. 携帯電話基地局への接続に用いられる携帯電話プロトコルの有効化／無効化、

24. デバイス機能の音声コマンドコントロールの有効化／無効化、

25. アプリケーション上のデジタル署名の検証に用いられる [選択：証明書、公開鍵] の設定、

26. アプリケーションの削除

27. システムソフトウェアのアップデート

28. アプリケーションのインストール

29. 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

30. 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

31. [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***]、その他の管理機能なし]*

] を、デバイスが登録された際、及び管理者によって設定されるポリシーに従って、管理者に制限しなければならない (shall)。

適用上の注意：

デバイスが登録されている限り、(エンタープライズの) 管理者にはエンタープライズの最小限のセキュリティ機能が強制されていることが保証されなければならない (must)。さらに制約的なポリシーは、追加的な管理者の代理として利用者によって任意の時点で適用可能である。

機能 3 の割付は、カメラやマイクロフォンなど、すべての音声及び視覚的デバイスであって、有効化及び無効化が可能なものから構成される。

機能 6 の割付は、Wi-Fi、GPS、携帯電話、NFC、そして Bluetooth など、すべての無線であって、有効化及び無効化が可能なものから構成される。

機能 7 の割付は、USB、SD カード、そして HDMI など、すべての外部アクセス可能なハードウェアポートであって、そのデータ転送機能が有効化及び無効化可能なものから構成される。

機能 8 の割付は、WiFi テザリングなど、TSF がサーバとしてふるまうすべてのプロトコル

であって、有効化及び無効化が可能なものから構成される。

機能 10 のセキュリティポリシーは、WPA2 エンタープライズなどのセキュリティの種類、及び EAP-TLS などの認証プロトコルに対応する。

機能 17 の通知の表示の設定は、**FTA_SSL_EXT.1** の選択で許可された機能であってもよい。

機能 20 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の X.509v3 証明書のインポートまたは削除を許可し、また管理者が要求を承認し得る場合に含まれ得る。これらのアプリケーションには、MDM エージェントは含まれない。この機能は、証明書を信頼して自分自身を検証するアプリケーションには適用されない。この機能は、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変更し、それが他のアプリケーションについて TSF によって行われる検証に影響するような状況にのみ適用される。利用者または管理者には、この要件を満たすために任意のアプリケーション要求をグローバルに許可または拒否する能力が提供されてもよい。

機能 21 を行う能力には、(緊急ダイヤルを除いて) 完全に音声呼を無効化する能力が含まれる。

機能 22 を行う能力には、(キャリアによって要求されるもの及び緊急 SMS を除いて) 完全にデバイスメッセージングを無効化する能力が含まれる。デバイスメッセージング機能には、SMS、MMS、そしてボイスメールが含まれる。

保証アクティビティ：

テスト 1 : 評価者は、*テスト環境*を用いてモバイルデバイスへポリシーを展開しなければならない (shall)。

テスト 2 : 評価者は、**FMT_MOF.1.1(2)** に定義される (エンタープライズ) 管理者によってコントロールされ、利用者によって上書きできない、すべての管理機能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、利用者として各設定の上書きを試行し、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)。

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.1	**管理機能の仕様**

FMT_SMF.1.1 TSF は、以下の管理機能を行えなければならない (shall)： [

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
2. セッ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
3. VPN 保護の有効化／無効化

4. [**割付：無線のリスト**] の有効化／無効化
5. [**割付：音声または視覚的収集デバイスのリスト**] の有効化／無効化
6. TSF が接続できるワイヤレスネットワーク (SSID) の特定
7. 各ワイヤレスネットワークのセキュリティポリシーの設定：
    a. [***選択：1 つまたは複数の CA を特定してそこからの 1 つまたは複数の WLAN 認証サーバ証明書を TSF が受容する、1 つまたは複数の FQDN を特定してその 1 つまたは複数の WLAN 認証サーバ証明書を受容可能とする***]
    b. セキュリティの種類を特定する能力
    c. 認証プロトコルを特定する能力
    d. 認証に用いられるべきクライアント認証情報の特定
    e. [**割付：任意の追加的な WLAN 管理機能**]
8. ロック状態への移行
9. 保護データの完全な抹消
10. 以下によるアプリケーションのインストールの設定 [***選択：***
    a. ***1 つまたは複数の正当なアプリケーションリポジトリの特定、***
    b. ***許可されるアプリケーション及びバージョンのセットの特定 (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の拒否***]、
11. セキュアな鍵ストレージへの鍵／秘密のインポート、
12. セキュアな鍵ストレージ中の、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、
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、
14. トラストアンカーデータベース中の、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、
15. 管理への TOE の登録
16. アプリケーションの削除
17. システムソフトウェアのアップデート
18. アプリケーションのインストール

[***選択：***

19. ***[割付：外部アクセス可能なハードウェアポートのリスト] 上のデータ転送機能の有効化／無効化、***
20. ***[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、***
21. ***開発者モードの有効化／無効化、***
22. ***保存データ保護の有効化、***

23. リムーバブルメディアの保存データ保護の有効化、
24. ローカル認証バイパスの有効化／無効化、
25. 携帯電話ネットワークとその他のネットワークとの通信に用いられるアクセスポイント名及びプロキシの設定
26. Bluetooth 高信頼チャネルの設定：
    a. 検出可能 (Discoverable) モードの無効化
    b. Bluetooth のバージョン1.0、1.1、1.2、2.0、及び [割付：その他の Bluetooth バージョン番号] を用いた接続の禁止
    c. [選択：Bluetooth プロファイルの制限、レガシーペアリング及び JustWorks ペアリングの無効化、及び [選択： [割付：その他のペアリング手法]、その他のペアリング手法なし]]、
27. 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. なし]
28. 機密性のあるデータの抹消、
29. 管理者への警報、
30. エンタープライズアプリケーションの削除、
31. トラストアンカーデータベース中の X.509v3 証明書のアプリケーションによるインポート及び削除の承認、
32. 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、または確立を禁止するかの設定、
33. 携帯電話音声機能の有効化／無効化、
34. デバイスメッセージング機能の有効化／無効化、
35. 携帯電話基地局への接続に用いられる携帯電話プロトコルの有効化／無効化、
36. デバイス機能の音声コマンドコントロールの有効化／無効化、
37. TSF によって記録された監査ログの読み出し、
38. アプリケーション上のデジタル署名の検証に用いられる [選択：証明書、公開鍵] の設定、
39. 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、
40. 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、
41. ロック解除バナーの設定、

42. [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*]、[その他の管理機能なし]

]。

適用上の注意：

機能 4 の割付は、Wi-Fi、GPS、携帯電話、NFC、そして Bluetooth など、すべての無線であって、利用者または管理者のいずれかによって有効化及び無効化が可能なものから構成される。

機能 5 の割付は、カメラやマイクロフォンなど、すべての音声及び視覚的デバイスであって、利用者または管理者のいずれかによって有効化及び無効化が可能なものから構成される。

機能 7 のセキュリティポリシーは、WPA2 エンタープライズなどのセキュリティの種類、及び EAP-TLS などの認証プロトコルに対応する。CA または FQDN は、**FCS_TLS_EXT.1.2** にしたがった比較のために特定される。

TSF の完全な抹消は、**FCS_CKM_EXT.5** に従って行われる。

将来、機能 14 には、例えば開発者の証明書など TSF の継続的な運用に必要な CA 証明書を除いた、任意のデフォルト高信頼 CA 証明書の破棄が要求されるかもしれない。現時点では、ST 作成者は割付中で、事前にインストールされた、またはその他の任意のカテゴリの X.509v3 証明書が、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、登録機能にはデバイスへ適用されるべきポリシーも含まれる。利用者承認通知が、その通知中のポリシーをすべて列挙するのではなく、ポリシーの閲覧を (例えば、「View」アイコンを「タップ」することによって) 意図的に選択することを利用者に要求することは許容可能である。

機能 19 の割付は、USB、SD カード、そして HDMI など、すべての外部アクセス可能なハードウェアポートであって、そのデータ転送機能が利用者または管理者のいずれかによって有効化及び無効化可能なものから構成される。

機能 20 の割付は、WiFi テザリングなど、TSF がサーバとしてふるまうすべてのプロトコルであって、利用者または管理者のいずれかによって有効化及び無効化可能なものから構成される。

機能 21 は、開発者モードが TSF によって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 22 は、保存データ保護がネイティブに有効化されない場合、選択に含まれなければならない (must)。

機能 23 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 24 は、ローカル認証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)。

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 (機能 27) が選択に含まれなければならない (must)。

機能 28 は、オプションの機密性のある保存データの要件 **FDP_DAR_EXT.2** に関連し、**FDP_DAR_EXT.2** が PP の本体に含まれる場合、含まれるべきである (should)。

機能 31 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には、MDM エージェントは含まれない。この機能は、証明書を信頼して自分自身を検証するアプリケーションには適用されない。この機能は、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変更し、それが他のアプリケーションについて TSF によって行われる検証に影響するような状況にのみ適用される。利用者または管理者には、この要件を満たすために任意のアプリケーション要求をグローバルに許可または拒否する能力が提供されてもよい。

機能 32 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 を行う能力には、(緊急ダイヤルを除いて) 完全に音声呼を無効化する能力が含まれる。

機能 34 を行う能力には、(キャリアによって要求されるもの及び緊急 SMS を除いて) 完全にデバイスメッセージングを無効化する能力が含まれる。デバイスメッセージング機能には、SMS、MMS、そしてボイスメールが含まれる。

機能 38 は、**FPT_TUD_EXT.2.5** が本体に含まれ、設定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 39 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 40 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 41 は、**FTA_TAB.1** が本体に含まれる場合、選択に含まれなければならない (must)。

保証アクティビティ：

以下のアクティビティは、**FPT_TUD_EXT.1.1**、**FPT_TUD_EXT.1.2**、**FPT_TUD_EXT.1.3**、及び **FPT_TUD_EXT.1.4** の保証アクティビティに記述される*テスト環境*において、行われなければならない (shall)。評価者は AGD ガイダンスを参照して以下のテストのそれぞれを行い、利用者及び管理者の両方がその機能を行い得る場合には各テストを繰返さなければならない (shall)。以下のテスト番号は、機能番号に対応する。

テスト 1 : 評価者は、以下のそれぞれについて、変数設定のそれぞれについて少なくとも 2 つの割付を行い、管理者として TSF を行使してポジティブ及びネガティブテストを行わなければならない (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

テスト 2 : 評価者は、利用者及び管理者として TSF 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、変数設定のそれぞれについて少なくとも 2 つの割付を行い、ポジティブ及びネガティブテストを行わなければならない (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)

テスト 3 : 評価者は、TSF 設定を行使して VPN 保護を有効化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** 要件のテストに用いられなければならない (must)。

テスト 4 : 評価者は、利用者及び管理者の両方として TSF を行使して、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しなければならない (shall)。それぞれの無線について、評価者はスペクトラムアナライザ及び電波暗室環境 (RF-shielded environment) を用いて、無線が有効化された際の信号の存在と無線が無効化された際の信号の不在を検証しなければならない (shall)。評価者は、デバイスのリブート及び通常使用中に信号の不在を検証しなければならない (shall)。

テスト 5 : 評価者は、利用者及び管理者の両方として TSF 設定を行使して、ST 作成者によって列挙された音声または視覚的収集デバイス (例えばカメラ、マイクロフォン) それぞれの状態を有効化及び無効化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、その後その機能の使用を試行しなければならない (shall)。

テスト 6 : 評価者は、テスト 6 及び 7 を目的としたワイヤレス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はならない (shall)。評価者は、管理者として及び利用者として、AGD ガイダンスに従ってワイヤレスネットワーク及びワイヤレス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 EAP-TLS を用いる WPA2 エンタープライズネットワークをテストしなければならない (shall)。評価者は、TSF がネットワークへの接続を確立できることを検証しなければならない (shall)。

テスト 7 : 評価者は、WLAN 認証サーバの正しくない値をワイヤレスネットワークに指定して、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、セキュリティの種類と認証プロトコルにそれぞれ個別に正しくない値を設定してこのテストを繰り返し、WLAN 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)。

テスト 8 及び 9 : 評価者は、デバイスへ以下を指令するよう、管理者として、テスト環境を用いて TSF に指示しなければならない (shall)。

- ロック状態への移行
- 全データの抹消

評価者は、指令に応じてデバイスがロック状態へ移行することを保証しなければならない (must)。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確実に用いられるようにしなければならない (must)。

テスト 10 : 評価者は管理者として TSF 設定を行使して、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ソース、またはアプリケーションのインストールを制限しなければならない (shall)。評価者は拒否された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)。

テスト 11 及び 12 : これらの機能のテストは、**FCS_STG_EXT.1** と関連して行われる。

テスト 13 : 評価者は AGD ガイダンスををレビューして、トラストアンカーデータベースへ証明書をインポート、変更、または削除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)。評価者は、利用者として、または管理者として、AGD ガイダンスに従って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)。

テスト 14 : 評価者は、利用者として、及び管理者として、AGD ガイダンスに従ってトラストアンカーデータベースから管理者によってインポートされた証明書、及び機能 15 (訳注 : 機能 14 が正しい) の割付に含まれる証明書のその他のカテゴリが存在する場合には、それを削除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、また強制される管理機能の種類のそれぞれの記述が含まれることを検証しなければならない (shall)。

テスト 16 : 評価者は AGD ガイダンスに従ってアプリケーションの削除を試行し、もはや TOE がこれらのアプリケーションまたはこれらに関連付けられた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)。

テスト 17 及び 18 : 評価者は、TSF システムソフトウェアのアップデート (アップデートが利用可能な場合) 及びモバイルアプリケーションのインストールを試行して、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及びモバイルアプリケーション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)。

テスト 19 : [条件付き] 評価者は TSF 設定を行使して、ST 作成者によって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) それぞれのデータ転送機能を有効化及び無効化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テスト機器を使用して、無効化されている際にはデータ転送に用いられるすべてのピンで低レベルのシグナリングが行われないことを保証しなければならない (shall)。

テスト 20 : [条件付き] 評価者は、割付中に列挙されたプロトコルのそれぞれの無効化を試行しなければならない (shall)。これには、テザリングの利用が含まれるべきである (should)。評価者は、無効化されたプロトコルを用いてリモートデバイスが 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)。

テスト 21 : [条件付き] 評価者は、利用者及び管理者の両方として TSF を行使して、開発者モードが存在する場合にはそれを有効化及び無効化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際には開発者モードのアクセスが利用できない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)。

テスト 22、23、及び 24 : [条件付き] 評価者は、利用者及び管理者の両方として TSF を行使して、AGD ガイダンスに従ってシステムワイドの保存データ保護を有効化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 5.3.2 参照) が、この設定におけるデバイスを用いて確実に実施されるようにしなければならない (shall)。評価者は、「パスワードを忘れた場合」の機能が存在する場合にはそれを無効化し、デバイスが一切のパスワードのヒントを提供しないことを保証しなければならない (shall)。

テスト 25 : [条件付き] : 評価者は、テストネットワークの APN を確立し、デバイス上へプライベートな APN を設定しなければならない (shall)。次に評価者は (おそらく開発者によって提供されるツールを利用して) 公共ルーティング可能なインターネットへパケットを送信しなければならない (shall)。評価者は、これらのパケットが APN 終端ポイントへ届いていること、そしてキャリアのインターネットアクセスゲートウェイを経由して到達していないことを確認しなければならない (shall)。評価者は、デバイス上に異なる、または無効な APN を設定してこのテストを繰り返し、パケットが APN 終端ポイントへ届かないことを検証しなければならない (shall)。

テスト 26：[条件付き] 評価者は検出可能 (Discoverable) モードを無効化し、一切の新たな Bluetooth 周辺機器がデバイスへ接続できないことを検証しなければならない (shall)。評価者は各 Bluetooth バージョンを禁止して、Bluetooth 周辺機器のデバイスへの接続を試行しなければならない (shall)。評価者は、Bluetooth プロトコル分析ツールを用いて、Bluetooth 周辺機器とのペアリングネゴシエーション中に TOE が無効化されたバージョンを利用したり、無効化されたバージョンを TOE がサポートしているものとして列挙したりしないことを検証しなければならない (shall)。評価者は、選択に応じて、TOE によって許可されるペアリングメカニズムを (Bluetooth プロファイルまたは特定のペアリングプロトコルによって) 制限しなければならない (shall)。評価者は、Bluetooth プロトコル分析ツールを用いて、Bluetooth 周辺機器とのペアリングネゴシエーション中に TOE が無効化されたペアリングメカニズムを利用したり、無効化されたペアリングメカニズムを TOE がサポートしているものとして列挙したりしないことを検証しなければならない (shall)。

テスト 27：[条件付き] AGD ガイダンスに列挙された情報のカテゴリそれぞれについて、評価者は TSF が AGD に従って情報を制限するよう設定されている際、ロック状態でもはや情報が表示されないことを検証しなければならない (shall)。

テスト 28：[条件付き] 評価者は、管理者ガイダンスに従ってデバイス上に残存する機密性のあるデータの抹消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から利用できないことを検証しなければならない (shall)。

テスト 29：[条件付き] 評価者は、管理者ガイダンスに従って管理者へ警報を行うようデバイスを設定しなければならない (shall) (例えば、MDM への警報を引き起こすトリガーを設定することによって)。評価者は、管理者がデバイスの警報を受け取ることを検証しなければならない (shall)。

テスト 30：[条件付き] 評価者は、管理者ガイダンスにしたがうことによって、デバイスから任意のエンタープライズアプリケーションの削除を試行しなければならない (shall)。評価者は、もはや TOE がこれらのアプリケーションまたはこれらに関連付けられた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)。

テスト 31：[条件付き] 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、アプリケーションによって許可される任意のセキュリティ機能 (トラストアンカーデータベースのインポート、変更、または破棄) が含まれることを検証しなければならない (shall)。

アプリケーションがトラストアンカーデータベースへ証明書をインポートし得る場合。評価者は、トラストアンカーデータベースへ証明書をインポート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、証明書のインポート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、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連鎖する証明書の有効性確認を試行することによって、テストされなければならない (shall) (**FIA_X509_EXT.1** の保証アクティビティに記述されているように)。
- 評価者はこのテストを繰り返し、承認を許可することによってアプリケーションが証明書をインポートすることができ、有効性確認が行われることを検証しなければならない (shall)。

アプリケーションがトラストアンカーデータベース中の証明書を削除し得る場合、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、証明書の削除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、アプリケーションが証明書を削除できないことを検証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連鎖する証明書の有効性確認を試行することによって、テストされなければならない (shall) (**FIA_X509_EXT.1** の保証アクティビティに記述されている通り)。

評価者はこのテストを繰り返し、承認を許可することによってアプリケーションが証明書を削除／変更することができ、もはや有効性確認が行われないことを検証しなければならない (shall)。

テスト32：[条件付き] この機能のテストは、**FIA_X509_EXT.2.2** と組み合わせて行われる。

テスト33：[条件付き] 評価者は、管理者ガイダンスに従ってすべての携帯電話音声機能の無効化を試行しなければならない (shall)。次に評価者は、利用者として TOE 上で発呼を試行し、この機能が失敗することを検証しなければならない (shall)。また評価者は、TOE への発呼を試行し、この呼が完了できないことを検証しなければならない (shall)。

テスト34：[条件付き] 評価者は、管理者ガイダンスに従ってすべてのデバイスメッセージング機能の無効化を試行しなければならない (shall)。次に評価者は、利用者として TOE 上でメッセージの送信を試行し、この機能が失敗することを検証しなければならない (shall)。また評価者は、TOE へのメッセージ送信を試行し、このメッセージが受信されないことを検証しなければならない (shall)。

テスト35：[条件付き] 評価者は、管理ガイダンスに従って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させることを試行し、ネットワーク分析ツールを用いて、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)。

テスト 36：[条件付き] 評価者は音声コントロール機能の無効化を試行しなければならず (shall)、また TOE が音声コマンドを与えられた際にもはや一切のアクションを行わないことを検証しなければならない (shall)。

テスト37：[条件付き] 評価者は、管理者ガイダンスに従って任意のデバイス監査ログの読み出しを試行し、そのログが読み出され得ることを検証しなければならない (shall)。このテストは、**FAU_GEN.1** の保証アクティビティと組み合わせて行われてもよい。

テスト38：[条件付き] この機能のテストは、**FPT_TUD_EXT.2.5** と組み合わせて行われる。

テスト39 及び40：[条件付き] これらの機能のテストは、**FCS_STG_EXT.1** と組み合わせて行われる。

テスト41：[条件付き] この機能のテストは、**FTA_TAB.1** と組み合わせて行われる。

5.5.2.2 修正アクションの仕様

FMT_SMF_EXT.1	**拡張：修正アクションの仕様**

FMT_SMF_EXT.1 TSF は、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、 [**選択：*ロック状態への移行*、*保護データの完全な抹消*、*機密性のあるデータの抹消*、*管理者への警報*、*エンタープライズ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]***] を提供しなければならない (shall)。

適用上の注意：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って成立し得る。

保証アクティビティ：

評価者は、テスト環境を用いてデバイスを繰り返し構成し、登録解除の際の選択中の修正アクションのそれぞれを行わなければならない (shall)。評価者は、AGD ガイダンスに従ってデバイスを登録解除し、構成された修正アクションが行わ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_EXT)

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 任意のユーザ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。

適用上の注意：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、この 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意：以下のテストには、通常消費者のための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必要とされる。

*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)。これには、TSF に含まれる任意のウェブブラウザまたはメールクライアントが含まれなければならない (must)。これらのアプリのそれぞれについて、評価者は同一の種類の 2 つの別個のモバイルデバイス上で同一のアプリを起動し、すべてのメモリマッピングのロケーションを比較する。評価者は、どのメモリマッピングも両方のデバイス上で同一の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)。

1 つのアプリについて 2 つのマッピングが同一となり他の 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 メモリページのアクセス権限

FPT_AEX_EXT.2	拡張：悪用防止サービス (メモリページのアクセス権限)

FPT_AEX_EXT.2.1 TSF は、物理メモリのすべてのページに読み出し、書き込み、及び実行アクセス権限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、そしてこの記述に仮想

メモリのすべてのページに読み出し、書き込み、及び実行アクセス権限を強制する MMU の能力が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 スタックオーバーフロー保護

FPT_AEX_EXT.3	拡張：悪用防止サービス (スタック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される 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)。

適用上の注意：

「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などではなく) を指す。すべての TSF 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ことが期待される。

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 ソフトウェアにスタックベースのバッファオーバーフロー保護が実装されるという記述が TSS に含まれることを判断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って異なることになる。実装の例としては、"-fstack-protector-all"、“-fstack-protector”、及び“/GS”フラグによってアクティベートされるものが挙げられる。

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 ドメイン隔離

FPT_AEX_EXT.4	拡張：ドメイン隔離

FPT_AEX_EXT.4.1 TSF は、信頼されないサブジェクトによる変更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隔離を強制しなければならない (shall)。

適用上の注意：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、プロセスごとの環境変数)、ならびに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 ソフトウェア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アプリケーションによる変更から保護される。

保証アクティビティ：

評価者は、TSF ソフトウェアまたは TSF のふるまいを支配する TSF データを非 TSF ソフトウェアが変更することを防止するメカニズムが用意されていることが TSS に記述されていることを保証しなければならない (shall)。これらのメカニズムには、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 への入力の境界チェック) まで、さまざまな可能性がある。評価者は、記述されたメカニズムが TSF を変更から保護するために妥当と思われることを判断する。

評価者は、アプリケーションのアドレス空間が互いに分離して保たれていることを TSF が保証する方法が、TSS に記述されていることを保証しなければならない (shall)。

保証アクティビティの注意：以下のテストには、通常消費者のための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。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、構成ファイル) 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「アクセス権限設定」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アクセス権限設定が実施され、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)。このアプリは、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)。

5.6.2 鍵ストレージ (FPT_KST)

5.6.2.1 平文鍵ストレージ

FPT_KST_EXT.1	**拡張：鍵ストレージ**

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

適用上の注意：この要件の意図は、TOE が平文鍵材料を永続的ストレージへ書き込まないことである。

保証アクティビティ：

評価者は、この要件に関する保証アクティビティを行うにあたって、ST の TSS セクションを参照しなければならない (shall)。

レビューを行うにあたって、評価者は DEK、保存された鍵、及びデータの復号に関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判断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、及び保存された鍵が TOE によって解かれ、保存され、そして利用される方法を含め、暗号化機能を行うために FCS 要件中の暗号化機能が用いられる方法もまたこの記述でカバーされていることを保証しなければならない (shall)。評価者は、電源断シナリオのそれぞれについて、不揮発性ストレージ中のすべての鍵が KEK によってラップされることを TOE が保証する方法が、TSS に記述されていることを保証しなければならない (shall)。

評価者は、システム中で利用できるその他の機能 (例えば、鍵の再生成) が、永続的ストレ

ージ中に暗号化されない鍵材料が存在しないことをどうやって保証するのか、TSS に記述されていることを保証しなければならない (shall)。

評価者は TSS をレビューして、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はない、と立証されていることを判断しなければならない (shall)。

5.6.2.2 鍵の送信なし

FPT_KST_EXT.2	拡張：鍵の送信なし

FPT_KST_EXT.2.1 TSF は、いかなる平文鍵材料も暗号モジュールから送信してはならない (shall not)。

適用上の注意：この要件の目的においては、鍵材料とは鍵、パスワード、及び鍵の導出に用いられるその他のマテリアルを指す。この要件の意図は、デバイス外部へ情報を送信するサービスへの平文鍵情報のロギングを防止することである。

保証アクティビティ：

評価者は、この要件に関する保証アクティビティを行うにあたって、ST の TSS セクションを参照しなければならない (shall)。評価者は、暗号モジュールの境界が TSS に記述されていることを保証しなければならない (shall)。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であることがほとんどだろう。

レビューを行うにあたって、評価者は DEK、保存された鍵、及びデータの復号に関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判断しなければならない (shall)。

評価者は、システム中で利用できるその他の機能 (例えば、鍵の再生成) が、暗号化されない鍵材料が暗号モジュール外部へ送信されないことをどうやって保証するのか、TSS に記述されていることを保証しなければならない (shall)。

評価者は TSS をレビューして、鍵材料が暗号モジュール外部へことはないということを判断しなければならない (shall)。

5.6.2.3 平文鍵のエクスポートなし

FPT_KST_EXT.3	拡張：平文鍵のエクスポートなし

FPT_KST_EXT.3.1 TSF は、1 人または複数の TOE 利用者が平文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)。

適用上の注意：平文鍵には、DEK、KEK、及びセキュアな鍵ストレージに保存されたすべての鍵が含まれる (**FCS_STG_EXT.1**)。この要件の意図は、TOE 利用者または管理者によってバックアップ中に平文鍵がエクスポートされることを防止することである。

保証アクティビティ：

ST 作成者は、鍵の取り扱い及び保護についての彼らのポリシーの言明を提供すること。評価者は、平文の DEK、KEK、及びセキュアな鍵ストレージに保存された鍵のいずれもエクスポートしないというポリシーが TSS に記述されていることをチェックし保証しなければならない (shall)。

5.6.3 セルフテスト事象通知 (FPT_NOT)

FPT_NOT_EXT.1	拡張：事象通知

FPT_NOT_EXT.1.1 TSF は、以下の種類の失敗が発生した際、非動作モードへ移行して [***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***] を行わなければならない (shall)：

- セルフテストの失敗
- 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)。

保証アクティビティの注意：以下のテストには、通常消費者のための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必要とされる。

*テスト 1：*評価者は、開発者によって提供されるツールを利用して、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変更しなければならない (shall)。評価者は、これらの重要な失敗の作成によって、デバイスが最初のリストに特定される修正アクションを取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の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 TSS を検査して、時刻を利用する機能のそれぞれが列挙されていることを保証しなければならない (shall)。TSS には、時刻に関連する機能それぞれの文脈において、どのように時刻が維持管理され信頼あるものとみなされるかの記述が提供される。本文書には、TSF が GPS、NTP サーバ、またはキャリアのネットワーク時間を主要な時間のソースとして利用するかどうか、またこれらのソースのいずれかまたはすべてが設定可能かどうか、特定されなければならない (must)。

評価者は操作ガイダンスを検査して、時刻を設定する方法が管理者に指示されていることを保証する。TOE が NTP サーバの利用をサポートする場合、操作ガイダンスには TOE と NTP サーバとの間の通信パスが確立される方法と、この通信をサポートするために TOE 上の NTP クライアントに何らかの設定が必要であれば、それが指示される。

*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、利用できるインタフェースを使って時刻が正しく設定されたことを確認しなければならない (shall)。

テスト 2：[条件付き] TOE が NTP サーバの利用をサポートしている場合、評価者は操作ガイダンスを用いて TOE 上の NTP クライアントを設定し、NTP サーバとの通信パスを設定しなければならない (shall)。評価者は、NTP サーバが期待されるとおり時刻を設定することを確認する。TOE が NTP サーバとの接続を確立するために複数の暗号プロトコルをサポートしている場合、評価者はサポートされているプロトコルのそれぞれを用いてこのテストを行わなければならない (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、[*最初の起動中 (電源投入時)*] に一連のセルフテストを実行し、[*すべての暗号機能*] の正しい動作を論証しなければならない (shall)。

適用上の注意：この要件は、既知解テストを行うことによって満たされてもよい。セルフテストは、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) 行われなければならない (must)。

保証アクティビティ：

評価者は TSS を検査して、起動時に行われるセルフテストが特定されていることを保証しなければならない (shall)。この記述には、TSF によって実施されるテスト手順の概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを保証することによってメモリがテストされる」のような記述が用いられなければならない (shall)) が含まれなければならない (must)。TSS には、セルフテスト失敗の際に 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、これらのセルフ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 中のセルフテストのリストを検査して、これにアルゴリズムセルフテストが含まれることを検証しなければならない (shall)。アルゴリズムセルフテストは、典型的には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のブートローダソフトウェア、アプリケーションプロセッサの OS カーネル、及び [選択: *[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*] の完全性を、その実行前に [***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***] を用いて検証しなければならない (shall)。

適用上の注意：この要件を満たすために、ハードウェア保護は推移的 (transitive) な性質であってもよい。ハードウェア保護された公開鍵またはハッシュが可換ブートローダコードを検証するために用いられ、そのブートローダには可換 OS カーネルコードを検証するためにブートローダによって用いられる鍵またはハッシュが含まれていてもよい。

最初の選択は、**FPT_TST_EXT.2.2** が本体に含まれない場合に追加的な実行可能コードを含むために用いられてもよい。現時点では、可換メディアに保存されたベースバンドプロセッサソフトウェアの検証は必要とされない。しかし、これは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 (ベースバンドプロセッサソフトウェアを含む) が検証される場合、**FPT_TST_EXT.2.2** が ST の本体に含まれるべきである (should)。

保証アクティビティ：

評価者は、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手続きの記述が ST の TSS セクション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、

オペレーティングシステム用のブートローダ及びカーネルをロードする前に、ブートローダとカーネルソフトウェアが暗号学的に検証されることを保証しなければならない (shall)。評価者は、未検証または未認証のソフトウェアによる変更を防止する暗号鍵またはハッシュの保護の正当化が 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、暗号検証を行うメカニズムに与えられる保護の記述が TSS に含まれることを検証しなければならない (shall)。

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***] 能力を正当な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***] 能力を正当な利用者へ提供しなければならない (shall)。

適用上の注意：デバイスのハードウェアモデルの現在のバージョンは、デバイスを設定するハードウェアを (製造業者の文書と連携して) 特定する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***] 能力を正当な利用者へ提供しなければならない (shall)。

適用上の注意：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モバイルアプリケーションそれぞれ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、モバイルデバイスと管理機能の利用方法を論証する任意のサポーティング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、または他の商業的に利用可能なソフトウェアであってもよい。評価者はモバイルデバイスとその他のソフトウェアを設定し、提供されたガイダンス文書に従って管理機能を行使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と、個別にアップデート可能なファームウェアがあれば、その現バージョン
- 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バージョン

評価者は製造業者の文書をレビューして、ハードウェアモデルの識別子がデバイスを設定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、 [***TSF へのソフトウェアアップデート***] をインストールする前に、 [***製造業者によるデジタル署名***] デジタル署名を用いてそれらのアップデートを検証しなければならない (shall)。

適用上の注意：デジタル署名メカニズムは、**FCS_COP.1.1(3)** に従って実装される。

現時点では、この要件はアプリケーションプロセッサ以外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には適用されない。将来、TSF のその他のプロセッサ上で動作するソフトウェアの高信頼ソフトウェアアップデートメカニズムのテストが、保証アクティビティによって要求されることになる。

FPT_TUD_EXT.2.2 ブート完全性 [***選択：鍵、ハッシュ***] は、 [***検証済みソフトウェア***] によってのみアップデートされなければならない (shall)。

適用上の注意：この要件による鍵またはハッシュは、**FPT_TST_EXT.2** において実行前にソフトウェアを検証するために用いられる。鍵またはハッシュはアップデート上の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行うソフトウェアは **FPT_TST_EXT.2** によって検証される。

FPT_TUD_EXT.2.3 デジタル署名検証鍵は、 [***選択：トラストアンカーデータベース中の公開鍵に対して検証され、ハードウェア保護された公開鍵と一致し***] なければならない (shall)。

適用上の注意：ST 作成者はシステムソフトウェアアップデートの署名鍵が制限される手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保護されることを示さなければならない (shall)。証明書が用いられる場合、証明書は **FIA_X509_EXT.1** に従って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** において選択されるべきである (should)。

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と、検証が失敗した場合にインストールが失敗することが含まれ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手法と、署名の検証に用いられる公開鍵がハードウェア保護されるかトラストアンカーデータベース中の公開鍵への連鎖に対して検証される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)。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手法が記述されており、権限のない人物によって公開鍵が変更され得ない理由を ST 作成者が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 作成者がソフトウェアアップデートデジタル署名検証用の公開鍵を示している場合、**FIA_X509_EXT.1** にしたがう証明書有効性確認と extendedKeyUsage 中のコード署名目的のチェックがアップデートメカニズムに含まれることを評価者は検証しなければならない (shall)。

評価者は、以下のテストが行われた証拠資料を ST 作成者が提供している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)、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)。

*テスト 2：*試験者は、デバイスによって許可されない鍵でアップデートにデジタル署名し、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、無効な証明書でアップデートにデジタル署名し、アップデートのインストールが失敗することを検証しなければならない (shall)。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)。

FPT_TUD_EXT.2.4 TSF は、インストール前に [モバイルアプリケーションソフトウェア] を [*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)。

適用上の注意：この要件は、X.509v3 証明書や証明書有効性確認を必要としない。X.509v3 証明書と証明書有効性確認は、**FPT_TUD_EXT.2.5** で対処される。

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、この手法にデジタル署名が用いられることを保証しなければならない (shall)。

テスト 1 : 評価者は、アプリケーションを書くか、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、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 セッションロック (FTA_SSL)

5.7.1.1 TSF 及び利用者主導のロック状態

FTA_SSL_EXT.1	拡張：TSF 及び利用者主導のロック状態

FTA_SSL_EXT.1.1 TSF は、非アクティブ時間間隔及び利用者主導のロックの後にロック状態へ移行しなければならず (shall)、そしてロック状態への移行の際、TSF は以下の操作を行わなければならない (shall)：

a) ディスプレイ装置のクリアまたは上書きを行い、過去の内容をあいまい化すること、

b) [割付：*ロック状態への移行の際に行われるその他のアクション*]。

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

保証アクティビティ：

評価者は、ロック状態への移行の際に行われるアクションが 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、非アクティブ時間間隔を設定しロックを指令する手法が 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、不正な利用者に表示が許可される情報が 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 1：*評価者は、AGD ガイダンスに従って非アクティブ時間 (**FMT_SMF.1**) の経過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、そしてディスプレイがクリアまたは上書きされること、またロック状態で許可されるアクションがセッションのロック解除と **FIA_UAU_EXT.2** に特定されるアクションのみであることを検証しなければならない (shall)。

*テスト 2：*評価者は、利用者と管理者の両方として、AGD ガイダンスに従って TSF にロック状態への移行を指令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、そしてディスプレイがクリアまたは上書きされること、またロック状態で許可されるアクションがセッションのロック解除と **FIA_UAU_EXT.2** に特定されるアクションのみであることを検証しなければならない (shall)。

5.7.2 ワイヤレスネットワークアクセス (FTA_WSE)

FTA_WSE_EXT.1	拡張：ワイヤレスネットワークアクセス

FTA_WSE_EXT.1.1 TSF は、**FMT_SMF.1** において管理者によって設定されたとおり、受容可能なネットワークとして特定されたワイヤレスネットワークへの接続を試行できなければならない (shall)。

適用上の注意：この要件の意図は、TSF が接続し得るアクセスポイントの設定を利用者及び管理者に許可すること、及び利用者または管理者による明示的な認可なしに TSF がワイヤレス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た際、エンタープライズ管理者によって特定されたもの以外のワイヤレスネットワークへ利用者が接続できないようにされる場合には、この管理機能は要件 **FMT_MOF.1.1(2)** の選択の中に列挙されるべきである (should)。この管理機能が **FMT_MOF.1.1(2)** 要件の選択の中に列挙されない場合、利用者はワイヤレスネットワークを設定し接続するために管理者として管理機能を行ってもよい。

保証アクティビティ：

この要件の保証アクティビティは、**FMT_SMF.1** と組み合わせて行われる。

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、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*] を利用して、他の通信パスとは論理的に分離されているとともに、そのエンドポイントの保証された識別とチャネルデータの開示からの保護及びチャネルデータの改変の検出を提供する、それ自身と他の高信頼 IT 製品との間の通信チャネルを提供しなければならない (shall)。

適用上の注意：上記の要件の必須部分の意図は、要件に特定された暗号プロトコルを用いて TOE とワイヤレスアクセスポイントとの間の高信頼チャネルを確立し維持することである。

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」に対して検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、**FTP_ITC_EXT.1** に選択された高信頼チャネルプロトコルのセキュリティ機能要件を ST の本体中に含めなければならない (must)。

FTP_ITC_EXT.1.2 TSF は、TSF 及び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)。

適用上の注意：アプリケーションは IPsec または WLAN を介した通信を直接開始できないが、TSF によって開始された高信頼チャネル内で通信を開始し得ることが期待される。この点で、アプリケーションがこれらのプロトコルの高信頼チャネルを開始していることは意識されなくてもよい。

FTP_ITC_EXT.1.3 TSF は、ワイヤレスアクセスポイントへの接続及び [割付：高信頼チャネルが要求される機能のリスト] について、高信頼チャネルを介した通信を開始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 文書に、これらの要件に記述されるセキュリティ機能 (高信頼チャネル) 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 による高信頼チャネルサービスを要求するアプリケーションを書くか、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、高信頼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)。このアプリケーションは、プロトコル要件の高信頼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ることもできる。

評価者は TSS を検査して、要件に特定される暗号プロトコルの観点からアクセスポイントに接続する TOE の詳細と、仕様に反映されていない可能性のある 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判断しなければならない (shall)。また評価者は、TSS に列挙されたすべてのプロトコルが特定され、ST の要件に含まれていることを確認しなければならない (shall)。評価者は、アクセスポイント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)。また評価者は、以下の

テストを行わなければならない (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ことによって、TOE が要件に特定されたプロトコルを用いてアクセスポイント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、正当な IT エンティティとの通信チャネルのそれぞれについて、チャネルデータが平文で送信されないことを保証しなければならない (shall)。

6. セキュリティ保証要件

セクション 4 の TOE に関するセキュリティ対策方針は、セクション 3 に特定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 EAL1 からセキュリティ保証要件 (SAR) を選び出し、評価者が評価の対象となる文書を評定して独立テストを行う範囲を設定する。

本セクションには CC からの SAR の完全なセットが含まれている一方で、評価者によって行われるべき保証アクティビティは本セクションと共にセクション 5 の両方に詳述されている。

本 PP に適合するよう作成された ST に対して、TOE の評価を行う一般的なモデルは以下のようなものである。

ST の評価が承認されると、ITSEF が TOE とサポーティング IT 環境、及び TOE の管理ガイドを取得する。そして、ST に列挙された保証アクティビティ (これは ITSEF によって ST で、または別個の文書で TOE 特有となるように詳細化される) が、ITSEF によって行われる。また ITSEF は、EAL1 の共通評価方法 (CEM) によって義務付けられたアクションをすべて行うことが期待される。これらのアクティビティの結果は、検証のために (利用された管理ガイダンスと共に) 文書化され提示される。

それぞれのファミリには、(もしあれば) 開発者によって提供される必要のある追加的文書／アクティビティを明確にするため、開発者アクションエレメントについて「開発者への注意」が提供される。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加的アクティビティ (セクション 5 及び EAL 1 の CEM にすでに含まれているものに加えて) が記述されている。さらに、本セクションに記述された保証アクティビティは、セクション 5 に特定されたものとは相補的な関係にある。

TOE のセキュリティ保証要件は表 1 に要約されており、本 PP のセクション 4 に特定された対策方針を満たすために必要とされる管理及び評価アクティビティが特定されている。

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評価 (ASE)	ST 概説 (ASE_INT.1)
	適合主張 (ASE_CCL.1)
	運用環境のセキュリティ対策方針 (ASE_OBJ.1)
	拡張コンポーネント定義 (ASE_ECD.1)
	主張されたセキュリティ要件 (ASE_REQ.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 の 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-適合 (訳注 : 原文は「サンプル」を CC/CEM に基づき訂正)(ATE_IND.1)
脆弱性評定 (AVA)	脆弱性調査 (AVA_VAN.1)

表 1：セキュリティ保証要件

6.1 ASE：セキュリティターゲット

CEM に定義される ASE アクティビティによる。

6.2 ADV：開発

TOE に関する情報は ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。TOE 開発者は TSS に含まれる製品の記述を、機能仕様との関連において一致させなければならない (must)。セクション 5 に含まれる保証アクティビティは､TSS セクションにふさわしい内容を判断するために十分な情報を ST 作成者へ提供すべきである (should)。

6.2.1 基本機能仕様 (ADV_FSP)

機能仕様は、対象となる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 の利用者によって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それ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べきである (should)。特定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とはされない。

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としてではなく、列挙された保証アクティビティを行う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)。

適用上の注意：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、及び行使するために特権が要求される 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に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、本プロファイルに要求される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､利用できる機能のそれぞれが適用される製品とバージョンが明示されなければならない (shall)。

機能仕様の保証アクティビティは、文書及び TSS セクションに存在すべき (should) 証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント **ADV_FSP.1.2D** 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容・提示エレメント：

ADV_FSP.1.1C 機能仕様は、SFR 実施、及び SFR 支援の 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 TSFI のそれぞれについて、関連するすべてのパラメタが特定されなければならない (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 の追跡を論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確認すること以外に、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。機能仕様文書はセクション 5 に記述された評価アクティビティと、AGD、ATE、及び AVA の SAR に関して記述されたその他のアクティビティをサポートするために提供される。機能仕様情報の内容についての要件は、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に評価される。不十分なインタフェース情報のために評価者がアクティビティを実施できなかった場合、十分な機能仕様が提供されてい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。ガイダンスには、運用環境がセキュリティ機能に対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)。本文書は、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：

- その環境へ TSF をインストールできるようにするための指示、及び
- 製品として、またより大規模な運用環境のコンポーネントとして、TSF のセキュリティを管理するための指示、ならびに
- 保護された運用管理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)。

適用上の注意：利用者操作ガイダンスは、単一の文書に含まれる必要はない。利用者、管理者及びアプリケーション開発者のためのガイダンスが、複数の文書またはウェブページに分散されていてもよい。必要に応じて、ガイダンス文書はセキュリティの自動化をサポ

ートするためセキュリティ設定チェックリスト記述形式 (XCCDF) で表現される。

ここで繰返し情報を提示するのではなく、開発者はこのコンポーネントに関する保証アクティビティをレビューして、評価者がチェックすることになるガイダンスの詳細を確認すべきである (should)。これによって、受容可能なガイダンスの作成に必要な情報が提供されることになる。

内容・提示エレメント：

AGD_OPE.1.1C 利用者操作ガイダンスは、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)。

適用上の注意: 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ことになる。

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 の評価によって検証されることになる。また、以下の追加情報も必要となる。

操作ガイダンスには、ネイティブにインストールされ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、そのようなアプリケーションが列挙されなければならない (shall)。

操作ガイダンスには、TOE の評価される構成と関連付けられた暗号エンジンを構成するた

めの指示が含まれなければならない (shall)。TOE の CC 評価の中で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、管理者へ与えられなければならない (shall)。

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

1. アップデートそのものを取得するための指示。これには、アップデートを TOE からアクセス可能とするための指示 (例えば、特定のディレクトリへの格納) が含まれるべきである (should)。
2. アップデートプロセスを開始するための、そしてそのプロセスが成功したか失敗したかを判別するための指示。これには、ハッシュ／デジタル署名の生成が含まれる。

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

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、その準備手続きを含めて TOE を提供しなければならない (shall)。

適用上の注意：操作ガイダンスと同様に、開発者は保証アクティビティを検査して準備手続きに関して必要とされる内容を判断すべきである (should)。

内容・提示エレメント：

AGD_ PRE.1.1C 準備手続きは、開発者の配付手続きに従って配付された TOE のセキュアな受入れに必要なすべてのステップ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 が運用に向けてのためにセキュアに準備できることを確認するために、準備手続きを*適用しなければならない (shall)*。

保証アクティビティ：

上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の設定にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST に TOE について主張されているすべてのプラットフォームへ十分に対応していることを保証するために確認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 に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの調査ではなく、ライフサイクルのエンドユーザに可視の側面に限定される。これは、製品の全体的な信頼度の向上に開発者のプラクティスが果たす重要な役割を減じようとするものではない。そうではなく、この保証レベルにおける評価に関して利用可能とされるべき情報を反映したものである。

6.4.1 TOE のラベル付け (ALC_CMC)

このコンポーネントは、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って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 への参照を提供しなければならない (shall)。

内容・提示エレメント：

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

評価者アクションエレメント：

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

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、この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ってカバーされる。

開発者アクションエレメント：

ALC_CMS.2.1D 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.2.1C 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.2.2C 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.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：

本 PP において「SAR によって要求される評価証拠」は、ST の情報と、AGD 要件の下で管理者及び利用者に提供されるガイダンスとの組み合わせに限られる。TOE が具体的に識別され、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 に関する評価アクティビティ中で行われるように) 保証することによって、評価者はこのコンポーネントによって要求される情報を暗黙に確認する。

ライフサイクルサポートは、TSF 製造業者の開発及び構成管理プロセスの詳細な調査ではなく、開発者のライフサイクルの側面と、開発者のデバイス向けアプリケーションのプロバイダへの指示を目的としている。これは、製品の全体的な信頼度の向上に開発者のプラクティス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の公共向け開発文書中で) 開発者のプラットフォーム向けアプリケーションの開発において利用に適当な 1 つ以上の開発環境を特定していることを保証しなければならない (shall)。これらの開発環境のそれぞれについて、開発者は 1 つまたは複数の環境におけるバッファオーバーフロー保護メカニズムが確実に発動されるように環境を設定する方法 (例えば、コンパイラのフラグ) に関する情報を提供しなければならない (shall)。評価者は、そのような保護がデフォルトでオンとなっているか、または具体的に有効化されなければならない (have to) のかという指摘もまたこの文書に含まれていることを保証しなければならない (shall)。

評価者は、TSF が一意に認識され (その TSF ベンダからの他の製品との関連で)、ST 中の要件と関連して開発者から提供される文書が、この一意の識別情報を用いて TSF と関連付けられることを保証しなければならない (shall)。

6.4.3 タイムリーなセキュリティアップデート (ALC_TSU_EXT)

このコンポーネントは、他の任意の必要とされる当事者との関連において、タイムリーな形でセキュリティ問題に対応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 開発者が情報を提供することを要求する。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、公衆へアップデートを提供するプロセスを記述する。この記述には、対象となる当事者 (例えば、開発者、1 つまたは複数の通信事業者) 、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までに行われる手順 (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、タイムリーにセキュリティアップデートが TOE に行われる方法の記述を TSS に提供しなければならない (shall)。

内容・提示エレメント：

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

適用上の注意：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、なら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 その記述には、脆弱性の公的な開示からセキュリティアップデートが TOE に公的に利用可能となるまでの間の、日単位の時間の長さとしてタイムウィンドウが明示されなければならない (shall)。

適用上の注意：時間の全体の長さは、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。公的に利用可能となるまでの時間の長さは、展開メカニズムによって異なるかもしれない。その場合には、そのそれぞれが記述される。

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)。

適用上の注意：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、悪用の概念を実証する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)*。

6.5 ATE クラス：テスト

テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について特定される。前者は ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 PP に特定された保証レベルにおいては、テストは通知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、以下の要件に特定される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には開発者のテスト環境が要求される。このテスト環境によって評価者は、例えば API へアクセスして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を閲覧することができる。

6.5.1 独立テスト—適合 (ATE_IND)

テストは、TSS と、提供された管理 (設定及び操作を含む) 文書に記述された機能を確認するために行われる。テストで重視されるのは、セクション 5 に特定された要件が満たされていることの確認であるが、いくつかの追加的テストがセクション 6 中の SAR につ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と関連付けられた追加的テストアクティビティを特定する。評価者は、テストの計画及び結果、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カバレージ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、テストに用いられる 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、テストに適当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：

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 が特定されたよう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の本体に含まれるすべてのテストアクションをカバーする。保証アクティビティに列挙されたテストのそれぞれについて 1 つのテストケースを用意する必要はないが、ST の該当するテスト要件のそれぞれがカバーされていることを評価者はテスト計画書中に文書化しなければならない (must)。

テスト計画書にはテストされるプラットフォームが特定され、そしてテスト計画書には含まれていないが ST に含まれているプラットフォームについては、そのプラットフォームをテストしないことについての正当化をテスト計画書が提供する。この正当化には、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 に主張されるすべてのプラットフォームがテストされる場合には、根拠は必要

とされない。

テスト計画書にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。評価者は、テストの一部として、または標準的なテスト前の条件として、AGD 文書に従って各プラットフォームの設置及び設定を行うことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供されるべきである (should)。またこれには、用いられるべき暗号エンジンの設定が含まれる。このエンジンによって実装される暗号アルゴリズムは、本 PP によって特定され、評価される暗号プロトコル (IPsec, TLS/HTTPS, SSH) によって用いられるものである。

テスト計画書には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も特定される。これらの手順には、期待される結果も含まれる。テスト報告書 (テスト計画書へ単に注釈を加えたものであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなければならない (shall)。したがって失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告書には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。

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

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、テストに用いられる 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、テストに適当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：

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 中に潜在する脆弱性を特定するために、パブリックドメインソースの検索を*行わなければならない (shall)*。

AVA_VAN.1.3E 評価者は、基本的な攻撃能力を有する攻撃者によって行われる攻撃に TOE が耐えられることを判断するために、特定された潜在する脆弱性に基づいて、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、評価者は報告書を作成し、この要件に関連する自分たちの結論を文書化しなければならない (shall)。この報告書は、物理的には ATE_IND に言及される全体的なテスト報告書の一部であってもよいし、または別個の文書であってもよい。評価者は、公開情報の検索を行って、ネットワークインフラストラクチャデバイス及び実装された通信プロトコル一般に発見されている脆弱性と、特定の TOE に関する脆弱性を判断する。評価者は、参考としたソースと発見された脆弱性を報告書に文書化する。発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、またはそのほうが適切であれば脆弱性を確認するためのテストを (ATE_IND に提供されるガイドラインを用いて) 策定するかのどちらかを行う。適合性は、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の評定によって判断される。例えば、脆弱性の悪用に専門的なスキルと電子顕微鏡が必要とされる場合には、テストは適当ではなく、適切な正当とする理由が策定されることになるであろう。

A. 根拠

本 PP において、本文書の最初のほうのセクションでは全体的なわかりやすさの向上を重視して、モバイルデバイスによって対処される脅威、これらの脅威を軽減するために用いられる手法、及び適合 TOE によって達成される軽減の程度について、説明文を提示した。この提示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のアーティファクトを用いて、本文書に関連付けられる評価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 の使用にあたって不可欠な環境条件の両方が含まれる。

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強制されるように、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、即座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 2：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	ワイヤレス通信チャネル上やネットワーク基盤上の他のどこかに位置する場合、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獲得ができてしまうかもしれない
T.NETWORK	攻撃者は、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。
T.PHYSICAL	利用者データ及び認証情報の機密性の損失が、モバイルデバイスへの物理的なアクセスを攻撃者が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、開発者によって意図的に、または意図せず用いられ、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能力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、完全性の損失と、敵対者と正当な所有者両方によるコントロールが可能となる。

表 3：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 に定義される脅威及び前提条件を、やはり本 PP に定義または特定されるセキュリティ対策方針と対応付ける役割をしている。

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 4：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 (またはそれ以上) の標準プロトコルを用いて通信を行う能力を提供すること。
O.STORAGE	TOE は、すべての利用者及びエンタープライズデータ及び認証鍵を暗号化する能力を提供し、その保存するデータの機密性を保証すること。
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と。これによってモバイルデバイスが、その保存または処理し得る利用者及びエンタープライズデータを保護できることを保証する。
O.AUTH	TOE は、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し、それらが適切な特権と共に認可されたエンティティと通信していることを保証する。
O.INTEGRITY	TOE はセルフテストを行う能力を提供し、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と。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をも提供すること。

表 5：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に正しくモバイルデバイスのセキュリティ機能を設定すること
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、即座に管理者へ通知すること。
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 6：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。

B. オプションの要件

本 PP の概論で示したように、本 PP の本体にはベースライン要件 (TOE またはその基盤となるプラットフォームによって行われなければならない (must) もの) が含まれている。これに追加して、これ以外の 3 種類の要件が附属書 B、C、及び D に特定されている。

(本附属書の) 第 1 の種類は、ST に含まれ得る要件であるが、TOE が本 PP への適合を主張するためには必要とされないものである。(附属書 C の) 第 2 の種類は、PP の本体中の選択に基づく要件である。特定の選択がなされた場合には、その附属書中の追加的要件が含まれることが必要となる。(附属書 D の) 第 3 の種類は、本 PP へ適合するためには要求されないが、本 PP の将来のバージョンのベースライン要件に含まれることになっているコンポーネントであり、モバイル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、または附属書 D に含まれる要件と関連し得るが列挙されていない要件 (例えば、FMT タイプの要件) もまた、ST へ含まれることを保証する責任があることに注意されたい。

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

C.1. TLS プロトコル (FCS_TLS)

FCS_TLS_EXT.2	**TLS プロトコル**

FCS_TLS_EXT.2.1 TSF は、以下の暗号スイートをサポートする以下の 1 つ以上のプロトコル、TLS 1.2 (RFC 5246) 及び [選択：TLS 1.0 (RFC 2246)、TLS 1.1 (RFC 4346)] を実装しなければならない (shall)：[

- *RFC 3268 による必須暗号スイート：*
  - *TLS_RSA_WITH_AES_128_CBC_SHA*
- *[オプションの暗号スイート：*
  - *TLS_RSA_WITH_AES_256_CBC_SHA*
  - *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *TLS_DHE_RSA_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_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *RFC 6460 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - *その他の暗号スイートなし*]]

適用上の注意：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、この要件によって制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである (should)。必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである (should)。テスト環境中のサーバ上で評価される構成において管理的に用いられることが可能な暗号スイートを制限することは必要である。上に列挙したスイート B アルゴリズム (RFC 6460) は、実装に望ましいアルゴリズムである。

FCS_TLS_EXT.2.2 TSF は、証明書に含まれる識別名 (DN) がピアに期待される DN にマッチしない場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注意：DN は、証明書の Subject Name フィールドまたは Subject Alternative Name 拡張に存在し得る。期待される DN は、設定されてもよいし、またはピアによって用いられるドメイン名または IP アドレスと比較されてもよい。

保証アクティビティ：

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイ

ートが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 TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述に適合するように TOE を設定するための指示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、証明書の DN が期待される DN と比較される方法が TSS に記述されていることを検証しなければならない (shall)。DN が自動的にドメイン名や IP アドレスと比較されない場合、評価者はその接続に期待される DN の設定が AGD ガイダンスに含まれていることを保証しなければならない (shall)。

RFC 5246 への準拠をテストするため、将来はさらにテストが追加されるかもしれない。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 :* 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、EAP セッションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。
- *テスト 2 :* 以下のテストは、サポートされている証明書署名アルゴリズムのそれぞれについて、繰返し行われる。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、設定された期待される DN またはピアのドメイン名／IP アドレスのいずれかに DN がマッチする証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できることを検証しなければならない (shall)。評価者は、設定された期待される DN またはピアのドメイン名／IP アドレスのいずれにも DN がマッチしない証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できないことを検証しなければならない (shall)。
- *テスト 4 :* 評価者は、サーバによって選択された暗号スイートとマッチしない証明書を TLS 接続中に送信する (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) ようサーバを設定しなければならない (shall)。評価者は、TOE が サーバの証明書ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。
- *テスト 5 :* 評価者は、TOE とサーバとの間に中間者ツールを設定しなければならず (shall) 、また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 ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、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中のサーバの選択された暗号スイート

を、ClientHello ハンドシェイクメッセージ中に存在しない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない (shall) 。

- *(条件付き)* DHE または ECDHE 暗号スイートがサポートされる場合、ServerKeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange を受信した後に接続を拒否することを検証する。
- サーバの CertificateRequest ハンドシェイクメッセージ中の CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない (must not)。評価者は、サーバがクライアントの Finished ハンドシェイクメッセージを受信した後に接続を拒否することを検証しなければならない (shall) 。
- サーバの Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。

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、 [選択：DTLS 1.0 (RFC 4347)、DTLS 1.2 (RFC 6347)] の 1 つ以上に従って 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、 [選択：DTLS 1.0 (RFC 4347)、DTLS 1.2 (RFC 6347)] にしたがった変動が許可される場合を除き、DTLS の実装には TLS (**FCS_TLS_EXT.2**) の中の要件を実装しなければならない (shall)。

適用上の注意：DTLS と TLS との違いは、RFC 4347 及び 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意と保証アクティビティは、DTLS の実装に適用される。

保証アクティビティ：

評価者は、TLS に列挙された保証アクティビティを行って、このコンポーネントを検証しなければならない (shall)。

C.3. HTTPS プロトコル (FCS_HTTPS)

FCS_HTTPS_EXT.1	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)。

適用上の注意：ST 作成者は、特定された (1 つまたは複数の) 標準に実装が準拠する方法を判断するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへのエレメントの追加によって、または TSS 中の追加的詳細によって、達成できる。

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

保証アクティビティ：

評価者は TSS をチェックして、HTTPS が TLS を用いて管理セッションを確立する方法に関して明確であることを、TLS プロトコルによって要求されるクライアント認証が存在する場合には、処理スタックの異なるレベルで行われ得るセキュリティ管理者認証と対比してそれに注目しながら、保証しなければならない (shall)。このアクティビティのテストは、TLS テストの一部として行われる。これは、TLS テストが TLS プロトコルレベルで行われる場合、追加的なテストとなるかもしれない。

D. オブジェクティブな要件

本附属書はいくつかの脅威についても対抗するセキュリティ機能を特定する要件を含む。その要件は、商業的な技術においてまだ広く有効でないセキュリティ機能を記述するので、本 PP の本文で必須とは現在なっていない。しかしながら、これらの要件が、ST に含まれてもよい (may)、その場合 TOE が本 PP に依然として適合しているし、かつ、それらはできる限り含まれるべきであると期待されている。

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. 監査機能の開始及び終了、
2. すべての管理者アクション、
3. 利用者認証の試行及び試行の成功／失敗、
4. OS 及びカーネルの開始及び終了、
5. セキュリティ機能の失敗、
6. 完全性検証の失敗、
7. ソフトウェアのアップデート、
8. リムーバブルメディアの挿入または取り出し、
9. 同期接続の確立、
10. 高信頼チャネルの確立、
11. [選択：管理者によって設定可能な監査容量のパーセンテージへ監査記録が到達したこと、 [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]].

FAU_GEN.1.2 TSF は、監査記録のそれぞれに、少なくとも以下の情報を記録しなければならない (shall)：

1. 事象の日付及び時刻、
2. 事象の種類、
3. サブジェクトの識別情報、及び
4. 事象の結果 (成功または失敗)。

適用上の注意：サブジェクトの識別情報は、通常プロセス名／ID である。事象の種類は、例えば「info (情報) 」、「warning (警告) 」、または「error (エラー) 」などの、深刻度レベルによって示されることが多い。

保証アクティビティ：

評価者は、管理ガイドをチェックして、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種類のそれぞれが、各フィールドの簡潔な記述とともに、カバーされなければならない (must)。評価者は、PP によって義務づけられるすべての監査事象の種類が記述され、またフィールドの記述には **FAU_GEN.1.2** に要求される情報が含まれることをチェックして保証しなければならない (shall)。

また評価者は、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判断を行わなければならない (shall)。評価者は管理ガイドを検査して、

PP で指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、どの管理コマンドが関連しているのか判断を行わなければならない (shall)。評価者は、本 PP に関して管理ガイド中のどのアクションがセキュリティ関連なのかを判断する際に採用した方法論または手法を文書化しなければならない (shall)。評価者は、このアクティビティを、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行ってもよい (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して TOE に監査記録を生成させることによって、正しく監査記録を生成するための 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 中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って判断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ガイドに特定されたフォーマットと一致することと、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)。

ここでのテストは、セキュリティメカニズムのテストと直接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するため、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び出しに対応するべきである (should)。

D.1.2. 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]。

適用上の注意：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：

評価者は管理ガイダンスをレビューして、ガイダンスにすべての事象の種類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しなければならない (shall)。また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が含まれると共に、(存在するならば) 複数値の事前選択を行うための構文が説明されなければならない (shall)。また管理ガイダンスには、現在実施されている選択基準に関わらず、常に記録される監査記録も識別されなければならない (shall)。

また評価者は、以下のテストを行わなければならない (shall)。

*テスト1：*要件に列挙される属性のそれぞれについて、評価者は、その属性の選択によってその属性を持つ監査事象(または、管理ガイダンスに手識別されるような、常に記録される監査事象) のみが記録され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には、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)。また評価者は、テスト計画書中に、そのテストのセットが典型的なものであり、その機能を実行するのに十分であることを正当化する短い説明文を提供しなければならない (shall)。

D.1.3. セキュリティ監査格納 (FAU_STG)

FAU_STG_EXT.1	監査格納の保護

FAU_STG_EXT.1.1 TSF は、監査証跡が満杯の場合、最も古く保存された監査記録を上書きしなければならない (shall)。

保証アクティビティ：

管理者は TSS を検査して、監査記録のサイズ制限、監査証跡が満杯であることの検出、及び監査証跡が満杯であるとき 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しなければならない (shall)。評価者は、そのアクションによって、最も古く保存された記録の削除または上書きが引き起こされることを保証しなければならない (shall)。

FAU_STG_EXT.1.2 TSF は、権限のない利用者による監査証跡の不当な改変及び削除を禁止しなければならない (shall)。

保証アクティビティ：

*テスト：*評価者は、権限のない利用者として監査証跡へのアクセスを試行しなければならず (shall)、またその試行が失敗することを検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. 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)。

適用上の注意：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以降の 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)。また評価者は、RBG の文書に、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記述されていることをも検証しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

*テスト1：*評価者は、Personalization String を介して RBG へエントロピーを追加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、こ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)。

適用上の注意：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保証はない (そのような保護に関する要件も存在しない) 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：この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状態を生成する方法、その状態が DRBG への入力として利用される方法、そして TOE が電源断の間にその状態に対して用いられる任意の保護対策が、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.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.1.2 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強制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意：以下のテストには、通常の消費者向けのモバイルデバイス製品には含まれないような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。

*テスト 1：*評価者は、ファイルへ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、各 TSF ファイルを上のアクセス権限を検査しながらファイルシステムをトラバースし、どのファイルにも書き込みと実行の両方のアクセス権限が設定されていないことを検証しなければならない (shall)。

FDP_ACF_EXT.1.3 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実施するよう設定可能でなければならない (shall)。そのような共有への例外は、[選択：利用者、管理者、共通アプリケーション開発者] のみが明示的に認可することができる。

適用上の注意：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、または個人の環境、のいずれかに指定される (may)。

保証アクティビティ：

評価者は、TSS に、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、及び許可されない共有がどのように防止されるか、に関して記述されていることを検証するために、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 (shall)、1 番目のアプリケーションは一意の文字列を含むデータを保存する、他方はそのデータへのアクセスを試行する。評価者は、2 番目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ないことを検証しなければならない (shall)。評価者は、利用者、管理者に対してアクセスを許可するか、または 3 番目のアプリケーションを用いて共通アプリケーション開発者に最初のアプリケーションへのアクセスを許可するかのいずれかによって、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)。

D.3.2. 保存データの保護 (FDP_DAR)

現バージョンの本文の要件では、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)。将来は、保存データ保護の追加レベルが追加される：機密性のあるデータ。表 7 に、各レベルの保存データ保護に要求される保護のレベルを示す。**FDP_DAR_EXT.2** の要件が本文に含まれていない場合、すべての非 TSF データ、すなわち機密性のあるデータとみなされ得るデータを含めて、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 F.1) 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。
機密性のあるデータ (Sensitive Data)	機密性のあるデータは、ロック状態の間､暗号化される。

表 7：データの保護レベル

すべての鍵、保護データ、及び機密性のあるデータは、最終的に REK によって保護されなければならない (must)。機密性のあるデータは、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 は機密性のあるデータに適当であり、DEK_2 は機密性のあるデータに適当ではなく、K_1 は機密性のある鍵とはみなされず、そして K_2 は機密性のある鍵とみなされる。

これらの要件には､ロック状態の間に受信された機密性のあるデータ (これは機密性のあるデータの別個のサブカテゴリとみなされ得る) を暗号化する機能が含まれる。この機能は、公開鍵を用いて DEK を暗号化し、対応するプライベート鍵はパスワード導出の KEK を用いて保護することによって、鍵配送スキーム (RSA) によって満たされてもよい。

またこの機能は、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密性のあるデータの非対称ペア (そのプライベート鍵はパスワード導出の KEK によって保護される) 及び受信された機密性のあるデータを保存するための非対称ペアを生成する。機密性のあるデータの保存には、デバイスワイドの公開鍵とデータのプライベート鍵が用いられ、KEK または DEK として利用可能な共有秘密が生成される。データの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の公開鍵が保存された後でクリアされる。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

の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、これをデータの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。

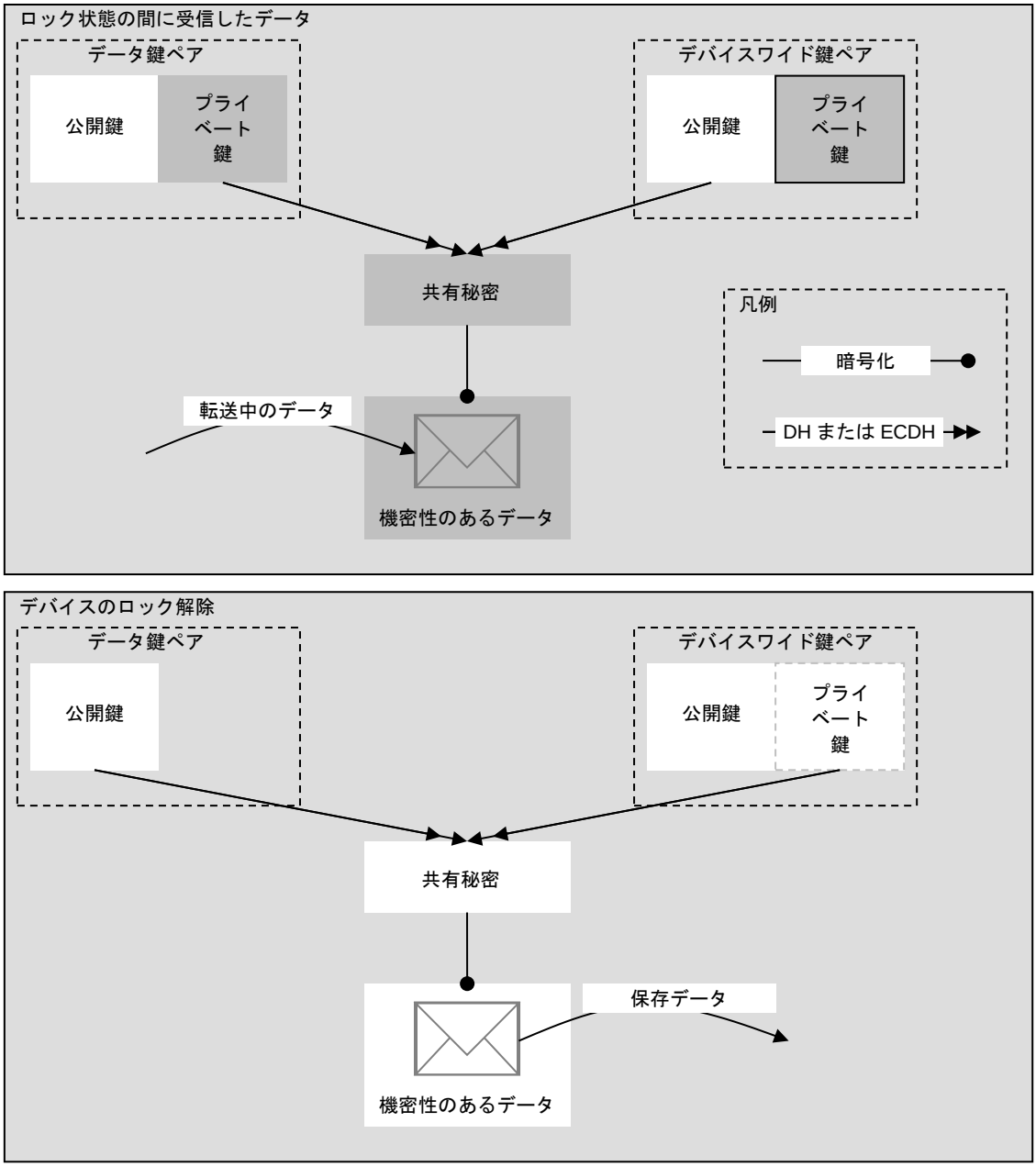

図 4：ロック状態で受信された機密性のあるデータを暗号化するための鍵共有スキーム

FDP_DAR_EXT.2	拡張：機密性のあるデータの暗号化

FDP_DAR_EXT.2.1 TSF は、データ及び鍵を機密性があると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)。

適用上の注意：機密性がある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) 一定の制約下に置かれることになる。このメカニズムによって、アプリケーションは自分の制御下にあるこれらのデータ及び鍵を、これらの要件の対象とすることを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「機密性がある」マーキングされることを要求し、明示的な「機密性がある」マーキングではなく明示的な「機密性がない」マーキングを要求することになる。

保証アクティビティ：

評価者は、TSF によって保存されるどのデータが (ネイティブなアプリケーションなどによって) 機密性がある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)。このデータには、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 TSS を検査して、データ及び鍵を機密性があるとマークするために使われる、アプリケーションに提供されるメカニズムが記述されていることを判断しなければならない (shall)。またこの記述には、このように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」領域への隔離、など) を反映した情報が含まれなければならない (shall)。

*テスト 1：*評価者は、AGD ガイダンスに従って機密性のある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 に定義されるように、またファイルの作成または機密性のある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って) 機密性のあるデータへのアクセスと作成を試行しなければならない (shall)。

FDP_DAR_EXT.2.2 TSF は、非対称鍵方式を用いて製品がロックされている間に受信された機密性のあるデータを暗号化し保存しなければならない (shall)。

適用上の注意：機密性のあるデータは、**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.1(1)** に従って行わ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密性のあるデータを受信でき、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。機密性のある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クリアされなければならない (must)。ロック状態で受信された機密性のある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用いられる鍵材料) 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、両方の方式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クリアされることを必要とする。

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密性のある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に ST の TSS セクションをレビューしなければならない (shall)。また評価者はその記述に、ロック状態中に受信され得る機密性のあるデータが、ロック状態中に受信できない機密性のある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も検証しなければならない (shall)。この記述には、受信データを暗号化し保存するための鍵スキームが含まれなければならず (shall)、この鍵スキームは非対称鍵を含み (must)、また (適用上の注意に記述されるように) データの導出または暗号化に用いられるすべての鍵材料を抹消することによって、機密性のある保存データが復号されることを防止しなければならない (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この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** のテストを行わなければならず (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行わ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** の選択 2 に従って、機密性のあるデータの保護に用いら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)。

適用上の注意：TSF がロック解除状態にある間に機密性のあるデータの暗号化に用いられる対称鍵は、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 へ連鎖し) なければならない (must)。ロック状態でデータの暗号化に用いら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 へ連鎖し) 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** のために要求される TSS の鍵階層構造セクションに、機密性のあるデータの暗号化に用いられる対称暗号鍵 (DEKs) 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 DEKs 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 へ連鎖し) 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、抹消されず 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 へ連鎖し) 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密性のあるデータを、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密性のある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用いら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.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 クライアントを介して流れる*ことを VPN アプリケーションが可能とする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 クライアントを介して流れる*ことを可能と] しなければならない (shall)。

適用上の注意：ネイティブな IPsec クライアントが全く検証されていない場合、またはサードパーティの VPN もまた要求された情報フロー制御を実装し得る場合、2 番目の選択肢が選択されなければならない (shall)。また ST 作成者は、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) を用いた際に IP トラフィックのルーティングに何らかの違いがあれば、それを TSS セクションに特定しなければならない (shall)。

ST 作成者は、TSF がネイティブな VPN クライアントを実装する (**FTP_ITC_EXT.1** において IPsec が選択されている) 場合には 2 番目のオプションを選択しなければならない (shall) この要件が本体に含まれ、ネイティブな VPN クライアントが検証される (**FTP_ITC_EXT.1** において IPsec が選択され、TSF が「IPsec 仮想プライベートネットワーク (VPN) クライアントのプロテクションプロファイル」に対して検証される) 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 (shall)。

次の改訂版では、本要件は本体へ移されることになる。また将来、本要件には現在の要件 (IPsec 高信頼チャネルが有効化される際、TSF からのすべてのトラフィックがそのチャネルを経由してルーティングされることを要求する) と区別して、TSF による任意の通信を許可する IPsec 高信頼チャネルの確立を強制する選択肢を持つことになるかもしれない。

保証アクティビティ：

評価者は、VPN クライアントが有効化されている際の TSF 上のプロセスを介した 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)。評価者はその記述に、どのトラフィックが VPN を通過せずどのトラフィックが通過するのか、そして各ベースバンドプロトコルについて VPN 接続の確立に必要であると ST 作成者によって特定されたトラフィック (IKE トラフィックと、もしかすると HTTPS または DNS トラフィック) のみが VPN プロトコル (IPsec) によってカプセル化されないような設定が存在することが、示されていることを保証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、すべての設定ですべての 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 クライアントを介してルーティングされることが示されている。
- AGD ガイダンスに、利用者または管理者またはその両方が TSF をこの要件を満たすように設定できる方法が記述されている。

- API 文書に、VPN クライアントがこのルーティングを指定することを許可するセキュリティ機能が含まれている。

テスト 1 : ST 作成者が WiFi と携帯電話プロトコルとの間でルーティングに何らかの違いを特定している場合、評価者は特定された携帯電話プロトコルの 1 つを実装する基地局と共にこの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 ガイダンス中の記述により (**FTP_ITC_EXT.1** によって要求されるように) WiFi 設定を有効化しなければならない (shall)。評価者はパケットスニッフィングツールをワイヤレスアクセスポイントとインターネットに接続されたネットワークとの間に用いなければならない (shall)。評価者はスニッフィングツールをオンにして、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、そして他のインターネットリソースのアクセスなど、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って生成されたトラフィックをスニッフィングツールがキャプチャしていることを検証し、スニッフィングツールをオフにして、セッションデータを保存しなければならない (shall)。

ステップ 2 - 評価者は、この要件に特定されたルーティングをサポートする IPsec VPN クライアントを設定し、また必要であれば、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)。評価者はスニッフィングツールをオンにして、VPN 接続を確立し、そしてデバイスを用いて最初のステップで行ったのと同一の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って生成されたトラフィックをスニッフィングツールがキャプチャしていることを検証し、スニッフィングツールをオフにして、セッ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、ステップ 1 及びステップ 2 両方からのトラフィックを検査して、VPN の確立に必要なトラフィック (IKE、DNS、そしてもしかすると HTTPS) を除いてそれ以降のトラフィックが IPsec によってカプセル化されていることを検証しなければならない (shall)。評価者は、IPsec トンネルの外部で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認識しなければならず (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てい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、ローカルなワイヤレスネットワークからのものを含めて、VPN トンネルの外部で (すなわち VPN ゲートウェイを介さずに) パケットの送信を試行しなければならず (shall)、そして TOE がこれらを廃棄することを検証しなければならない (shall)。

D.4. クラス：識別と認証 (FIA)

D.4.1. Bluetooth 認証 (FIA_BLT)

FIA_BLT_EXT.1	**拡張：Bluetooth 認証**

FIA_BLT_EXT.1.1 TSF は、Bluetooth リンク上でいかなるデータも転送される前に、デバイス間の Bluetooth 相互認証を要求しなければならない (shall)。

適用上の注意：相互認証は、ペアリングメカニズムとして Bluetooth 仕様によって定義されている。

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データ転送がどのように防止されるかに関して 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、サポートさ

れる OBEX データ転送メカニズムが明確に述べら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た後にのみ OBEX 転送が完了しないことを保証しなければならない (shall)。

D.4.2. X509 証明書認証 (FIA_X509)

FIA_X509_EXT.2	拡張：X509 証明書認証

FIA_X509_EXT.2.4 TSF は、コード署名証明書が無効とみなされる場合にはそのコードを [選択：*インストール*、*実行*] してはならない (shall not)。

適用上の注意：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**) のコード署名に用いてもよい；これらのいずれの場合でも、ST 作成者は「インストール」を選択しなければならない (must)。証明書は、オプションとして完全性検証 (**FPT_TST_EXT.2**) 用のコード署名に用いてもよい; この場合、ST 作成者は「実行」を選択しなければならない (must)。これらのコード署名用途のいずれかが **FIA_X509_EXT.2.1** 中で選択されている場合、**FIA_X509_EXT.2.4** が本文へ含まれて、適切なアクションが選択されなければならない (must)。

有効性は、RFC 5280 にもとづき、証明書のパス、有効期限、及び失効状態によって判断される。

保証アクティビティ：

本要件の保証アクティビティは、**FIA_X509_EXT.2.1** 及び **FIA_X509_EXT.2.2** の保証アクティビティと組み合わせて実施される。

FIA_X509_EXT.2.5 TSF は、RFC 2986 で指定されるように、証明書要求メッセージを生成しなければならない、かつ、その要求において以下の情報を提供できなければならない (shall) : 公開鍵、共通名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country)。

適用上の注意：**FIA_X509_EXT.2.5** で参照されている公開鍵は、**FCS_CKM.1(2)** で指定されるように TOE によって生成された公開鍵-プライベート鍵の鍵ペアのうちの公開鍵の部分である。

保証アクティビティ：

評価者は、証明書要求メッセージの生成に関する指示が操作ガイダンスに含まれていることをチェックして保証しなければならない (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、操作ガイダンスを用いて TOE に証明書要求メッセージを生成させなければならない (shall)。評価者は、この要求への入力として公開鍵、共通名、組織、組織単位、及び国を提供できることを確認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 によって指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)。

D.5. クラス：セキュリティ管理 (FMT)

D.5.1. ポリシーの管理 (FMT_POL)

FMT_POL_EXT.1 TSF は、管理者が行った強制されているポリシーへのいかなる変更について、利用者へ通知しなければならない (shall)。

適用上の注意：本要件は、変更を含む警報を行うのではなく、現在強制されているポリシーへのアクセス (例えば、メニューを通して) を利用者へ提供することによって満たされてもよい。TSF が登録されると、登録の時点で確立されたポリシーへのすべての変更は利用者の承諾を必要とする。この承諾は、1 回限りの (one-time basis) ものであってもよい (すなわち、「すべて承諾」)。

保証アクティビティ：

*テスト：*評価者は、既存のポリシーを変更し、それを既に登録されているデバイスへ展開しなければならない (shall)。評価者は、最初の登録の合意の下でアップデートを暗黙に許可していない場合、利用者がアップデートを通知されることを保証しなければならない (shall)。

D.6. クラス：TSF の保護 (FPT)

D.6.1. 悪用防止 (Anti-Exploitation) サービス (FPT_AEX)

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。

適用上の注意：この 4 個の予測不可能なビットは、TSF RBG によって (**FCS_RBG_EXT.1** で指定されるように) 提供されてもよい。

保証アクティビティ：

評価者は、ST の TSS セクションに、この 4 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意：以下のテストには、通常消費者のための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必要とされる。

*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)。これらのリブートのそれぞれについて、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一の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)。

FPT_AEX_EXT.2	**拡張：悪用防止サービス (メモリページのアクセス権限)**

FPT_AEX_EXT.2.2 TSF は、物理メモリのすべてのページに書き込みと実行アクセス権限が同時に与えられないようなポリシーを強制できなければならない (shall)。

適用上の注意：Just-in-time (JIT) コンパイルに用いられるメモリは、本要件から除外されてもよい；その場合、ST 作成者はどのようにこの除外が適用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ことが期待されている。

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、かつ、この記述に書き込みと実行の排他的論理和（XOR）のアクセス権限を実施する MMU の能力が書

かれていることを保証しなければならない (shall)。

D.6.2. ベースバンドの隔離 (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ワイヤレス*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。

- 大部分のモダンな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 と呼ぶ) である。
- ベースバンドプロセッサも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 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 (統合されている場合も、そうでない場合も) が含まれる。

特に注記のない限り、他の全ての要件は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とベースバンドプロセッサとに適用されるだろう。

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 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は、アプリケーションプロセッサ (AP) によって仲介される場合を除き、AP のリソースへアクセスが可能であってはならない (shall not)。

適用上の注意：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) のコントロールとそれらからのデータ
- 統合及び非統合入出力センサ (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) のコントロールとそれらからのデータ

本プロテクションプロファイルの将来の改訂版では、本要件は本文へ追加されることになる。

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 について、あらゆる周辺機器やセンサへのアクセス、または AP が使用するメインメモリ (揮発性及び不揮発性) へのアクセスをも許可し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.6.3. 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、可換 (mutable) メディアに保存された実行可能コードの完全性を、それが実行のためにロードされた際に [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] を用いて検証しなければならない (shall)。

適用上の注意：本要件を満たすために、ハードウェア保護は実際には過渡的でもよい。ハードウェア保護された公開鍵またはハッシュが可換ブートローダコードを検証するために用いられ、そのブートローダコードには可換 OS カーネルコードを検証するためにブートローダによって用いられる鍵またはハッシュが含まれ、その可換 OS カーネルコードには次のレイヤーの実行可能コードを検証するため鍵またはハッシュが含まれる、などとなっていてもよい。

実行可能コードには、アプリケーションプロセッサのブートローダ、カーネル、OS、デバイスドライバ、その他のプロセス、アプリケーション、及びライブラリ、ならびにベースバンドプロセッサのブートローダ、カーネル、及び OS が含まれる。

すべての可換実行可能コードは検証されなければならない (must) ため、(最初の) 可換実行可能コードを検証するために用いら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) 中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、ST の TSS セクションに、TSF の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用のソフトウェアのブート処理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、任意の実行可能コードをロードする前に、そのコード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)。評価者は、TSS に、未検証または未認証のソフトウェアによる改変を防止するような、暗号鍵またはハッシュの保護について正当とする理由が含まれていることを検証しなければならない (shall)。

D.6.4. 高信頼アップデート (FPT_TUD)

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.1.4 TSF は、クエリへのすべてのレスポンスを暗号技術的に署名しなければならない (shall)。

適用上の注意：暗号技術的な署名を要求するクエリは、**FPT_TUD_EXT.1.1**、**FPT_TUD_EXT.1.2**、及び **FPT_TUD_EXT.1.3** である。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 エージェントなどといった中間者によって改変または詐称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、TSS に、TSF がクエリへのレスポンスに署名するためにどの鍵を使うか、及びその鍵の所有権を証明するために用いられる証明書について、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、以下のテストを行わなければならない (shall)。

テスト: 評価者は、**FPT_TUD_EXT.1** で要求されるレスポンスのそれぞれについてクエリする管理アプリケーションを書くか、または、開発者が提供しなければならない (shall)。評価者は、これらのクエリへのレスポンスが署名されていること、及び TOE の証明書に基づ

く署名を検証しなければならない (shall)。

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***] によって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承諾なければならない (shall)。

適用上の注意：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、製造事業者によってインストールされる。署名の検証に用いられる設定された証明書は、**FMT_SMF.1** の機能 38 に従って設定される。

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検証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)。評価者は、この手法にコード署名証明書によるデジタル署名が用いられることを保証しなければならない (shall)。

テスト 1 : 評価者は、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を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行われてもよい。

テスト 3 : 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って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.2.6 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、それ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)。

適用上の注意：新しいバージョンは、より大きなバージョン番号を持つ。

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が、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 1 : 評価者は、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ず (shall)、かつ、そのアップデート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.7. Class: TOE アクセス (FTA)

D.7.1. 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 利用者セッションを確立する前に、TSF は TOE の利用に関して管理者によって指定された注意喚起通知及び同意警告メッセージを表示しなければならない (shall)。

適用上の注意：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される (may)。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.1** の機能 41 に従って設定される。

保証アクティビティ：

TSS には、いつバナーが表示されるか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施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、通知及び同意警告メッセージが TSS に記述されているそれぞれのインスタンスにおいて表示されることを検証しなければならない (shall)。

E. エントロピーの文書化と評定

エントロピー源に関する文書化は、読んだ後に評価者が、エントロピー源を理解し、エントロピーを供給することに信頼できるかについての根拠を完全に理解できるように十分に詳細であるべきである (should)。本文書には、設計記述、エントロピーの正当化、運用条件及びヘルステストという、複数の詳細なセクションが含まれるべきである (should)。本文書は、TSS の一部としては要求されない。

E.1. 設計記述

文書化では、エントロピー源のすべての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、どのように動作するのか、どのようにエントロピーが生成されるのか、そしてどのように未処理 (生の) データをエントロピー源の内部からテスト目的で取り出すことができるのか、を含めてエントロピー源の操作について記述することになる。文書化では、ランダム性がどこから由来し、次にどこへ渡されるのか、生の出力の任意の後処理 (ハッシュ、XOR など)、保存されるのであればどこに保存されるのか、そして最後に、どのようにしてエントロピー源から出力されるのか、を示すように、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) を行うべきである(should)。処理における条件等があれば (ブロッキング等)、エントロピー源の設計の中で記述されるべきである (should)。図や例の利用が推奨される。

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に関する記述と、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どのようにしてセキュリティ境界が保証するかに関する記述についても含まれなければならない (must)。

もし、サードパーティのアプリケーションが実装される場合、設計の記述には、サードパーティのアプリケーションがどのようにして RBG へエントロピーを追加できるかに関する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あらゆる RBG の状態に関する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論的なふるまいを示すことがなぜ確信できるのかという技術的な議論が存在するべきである (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、これを記述する方法のひとつである) (should)。この議論には、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に関する説明が含まれることになる。この検討は、エントロピー源がエントロピーを持つ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には、任意のサードパーティアプリケーション、または再起動までの間に保存される任意の状態から、追加される一切のデータが含まれてはならない (shall not)。

E.3. 運用条件

また文書には、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手法が、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、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、またはオンデマンド)、各ヘルステストに期待される結果、そしてそれぞれのテストがエントロピー源の 1 つ以上の故障を検出するために適当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. 用語集と略語

F.1. 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]。
CC	コモンクライテリア (Common Criteria)
CM	構成管理 (Configuration Management)
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) によって保存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用いられる鍵。
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、またはモバイルデバイス上に一時的に保存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)	ファイル暗号化が用いられる場合、ファイルの暗号化に用いられる DEK。FEK は、暗号化されるファイルごとに一意である。
鍵の連鎖 (Key Chaining)	複数層の暗号化鍵を用いて、データを保護する手法。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。この手法は、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用いられる鍵。
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

用語	意味
	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)	これは、モバイルデバイスの物理的なコントロールと操作を利用し、その責任を負う人物である。
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)	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。保護データは、TSF の電源が切断されている間、暗号化される。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密性のあるデータともみなされ得る。
ルート暗号化鍵 (REK)	他の鍵の暗号化に用いられる、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)
機密性のあるデータ (Sensitive data)	機密性のあるデータは、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)。機密性のある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。機密性のあるデータは、ロック状態にある間、オプションとして保護される (**FDP_DAR_EXT.2** 及び **FDP_DAR_EXT.3**)。機密性のあるデータには、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 の正しい強制のために信頼

用語	意味
	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、要件の強制が依存するもの。
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。

F.2. 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)
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)
CPU	中央処理装置(Central Processing Unit)
CSP	クリティカルセキュリティパラメタ(Critical Security Parameters)
DAR	リセット時のデータ(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
DN	識別名 (Distinguished Name)
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)
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)

略語	意味
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)
KEK	鍵暗号化鍵 (Key Encryption Key)
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)
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)
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)
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
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
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)
USB	ユニバーサルシリアルバス (Universal Serial Bus)
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)。

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
FAU_GEN.1	ST に含める。
FDP_DAR_EXT.2	ST に含める。
FMT_MOF.1(2) の機能 9	選択に含める。
FMT_SMF.1.1 の機能 20	選択に含め、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.1.1 の機能 25	選択に含める。
FMT_SMF.1.1 の機能 37	選択に含める。
FMT_SMF.1.1 の機能 41	選択に含める。
FPT_BBD_EXT.1	ST に含める。
FTA_TAB_EXT.1	ST に含める。

表 8：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
FAU_GEN.1	ST に含める。
FCS_CKM.1(1)	楕円曲線ベースの鍵確立スキームを選択する。
FCS_CKM.1(2)	ECDSA スキームを選択する。

FCS_CKM_EXT.1	256 ビットを選択する。
FCS_CKM_EXT.2	256 ビットを選択する。
FCS_CKM_EXT.3	256 ビットを選択する。
FCS_COP.1(1)	256 ビットを選択する。
FCS_COP.1(2)	SHA-384.を選択する。
FCS_COP.1(3)	ECDSA スキームを選択する。
FCS_COP.1(4)	HMAC-SHA-384 を選択する。
FCS_COP.1(5)	HMAC-SHA-384 を選択する。
FCS_DTLS_EXT.1	DTLS 1.2 を選択する。
FCS_RBG_EXT.1.1	256 ビットセキュリティ強度でインスタンス化された SP800-90A DRBG を選択する。
FCS_RBG_EXT.1.2	TSF ハードウェアベースのノイズ源を選択する。256 ビットを選択する。
FCS_STG_EXT.1	対称鍵と永続的秘密を選択する。保証アクティビティには、ECDSA が含まれるべきである (should)。
FCS_TLS_EXT.1	TLS 1.2 を選択する。TLS_ECDHE_ECDSA_WITH AES_256_GCM_SHA384 を選択する。
FCS_TLS_EXT.2	TLS 1.2 を選択する。TLS_ECDHE_ECDSA_WITH AES_256_GCM_SHA384 を選択する。
FDP_DAR_EXT.1	256 ビットを選択する。
FDP_DAR_EXT.2	ST に含める。
FDP_IFC_EXT.1	ST に含める。
FIA_X509.2	「…選択を管理者に許可する」または「高信頼チャネルの確立を禁止する」のいずれかを選択する。
FMT_MOF.1(2) の機能 5	選択に含める
FMT_MOF.1(2) の機能 9	選択に含める。
FMT_MOF.1(2) の機能 10	選択に含める。
FMT_SMF.1.1 の機能 4	TSF 上のすべての無線を割付ける。

FMT_SMF.1.1 の機能 5	TSF 上のすべての音声または映像収集デバイスを割り付ける。
FMT_SMF.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.1.1 の機能 19	選択に含め、すべての外部アクセス可能なハードウェアポートを割り付ける。
FMT_SMF.1.1 の機能 20	選択に含め、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.1.1 の機能 25	選択に含める。
FMT_SMF.1.1 の機能 33	選択に含める。
FMT_SMF.1.1 の機能 34	選択に含める。
FMT_SMF.1.1 の機能 36	選択に含める。
FMT_SMF.1.1 の機能 37	選択に含める。
FMT_SMF.1.1 の機能 41	選択に含める。
FPT_BBD_EXT.1	ST に含める。
FTA_TAB_EXT.1	ST に含める。

表 9：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

要件	**アクション**
FMT_POL_EXT.1	ST に含める。
FMT_SMF.1.1 の機能 12	選択に含める。

表 10：BYOD のテンプレート

H. NIST 承認暗号モードの初期化ベクトルの要件

暗号モード	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、同一の共通鍵が用いら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 上で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、所与の共通鍵について 2^32 を越えてはならない (shall not)。

表 11：NIST 承認暗号モードの参照情報と IV 要件

I. 管理機能

表 12 は、本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 中に特定された管理機能が列挙されている。

2 番目の列は、その機能の TOE による実装 (**FMT_SMF.1** に列挙される) が必須 (M) なのか、オプション／オブジェクティブ (O) なのかを示している。

3 番目の列は、その機能の利用者への制限 (**FMT_MOF.1(1)** に列挙される) が必須 (M) なのか、オプション／オブジェクティブ (O) なのか、または適用されない (-) のかを示している。

4 番目の列は、2 番目及び 3 番目から導出され得るもので、その機能が常に管理者に利用可能であることが必須 (M) なのか、オプション／オブジェクティブ (O) なのか、または適用されない (-) のかを示している。したがって、TOE はこれらの機能が **FMT_SMF.1** に含まれていれば、管理者が行えるように提供しなければならない (must)。

5 番目の列は、そのデバイスが登録され、指示されたポリシーを管理者が適用した場合、その機能の管理者への制限 (**FMT_MOF.1(2)** に列挙されるように) が必須 (M) なのか、オプション／オブジェクティブ (O) なのか、または適用されない (-) のかを示している。

管理機能 **状態のマーカー：** M — 必須 O — オプション／オブジェクティブ - — 適用されない	**FMT_SMF.1**	**FMT_MOF.1(1)**	**管理者**	**FMT_MOF.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. セッ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	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：音声または映像収集デバイスのリスト] の有効化／無効化	M	-	M	M
6. TSF が接続できるワイヤレスネットワーク (SSID) を特定	M	-	M	O
7. 各ワイヤレスネットワークのセキュリティポリシーの設定： a. [選択：TSF が許可する WLAN 認証サーバ証明書から CA を特定、許可可能な WLAN 認証サーバ証明書の FQDN を特定] b. セキュリティタイプを特定する能力 c. 認証プロトコルを特定する能力 d. 認証に用いられるべきクライアント認証情報を特定 e. [割付：任意の追加的な WLAN 管理機能]	M	-	M	O
8. ロック状態への移行	M	-	M	-
9. 保護データの完全な抹消	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. 正当なアプリケーションリポジトリを特定、 b. 許可されたアプリケーションとバージョンの組合せを特定 (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]] の破壊	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	-	-
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. [割付：外部アクセス可能なハードウェアポートのリスト] 上のデータ転送機能の有効化／無効化	O	O	O	O
20. [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
21. 開発者モードの有効化／無効化	O	O	O	O
22. 保存データ保護の有効化	O	O	O	O
23. 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
24. ローカル認証バイパスの有効化／無効化	O	O	O	O
25. 携帯電話ネットワークとその他のネットワークとの通信に用いられるアクセスポイント名及びプロキシの設定	O	O	O	O
26. Bluetooth 高信頼チャネルの設定： a. ディスカバリーモードの無効化 b. Bluetooth のバージョン 1.0、1.1、1.2、2.0、及び [割付：その他の Bluetooth バージョン番号] を用いた接続の禁止 c. [選択：Bluetooth プロファイルの制限、レガシーペアリング及び Just Works ペアリングの無効化、及び [選択： [割付：その他のペアリング手法]、その他のペアリング手法なし]]	O	O	O	O
27. 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. なし]	O	O	O	O
28. 機密性のあるデータの抹消	O	O	O	-
29. 管理者への警報	O	-	O	-
30. エンタープライズアプリケーションの削除	O	-	O	-
31. 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インポート及び削除の承認	O	O	O	O
32. 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
33. 携帯電話音声機能の有効化／無効化	O	O	O	O
34. デバイスメッセージング機能の有効化／無効化	O	O	O	O
35. 携帯電話基地局への接続に用いられる携帯電話プロトコルの有効化／無効化	O	O	O	O
36. デバイス機能の音声コマンドコントロールの有効化／無効化	O	O	O	O
37. TSF によって記録された監査ログの読み出し	O	O	O	-
38. アプリケーション上のデジタル署名の検証に用いられる [選択：証明書、公開鍵] の設定	O	O	O	O
39. 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
40. 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／秘密の破壊の例外の承認	O	O	O	O
41. ロック解除バナーの設定	O	-	O	-

表 12：管理機能