モバイルデバイス管理のプロテクションプロファイル

バージョン：3.0

2016-11-21

National Information Assurance Partnership

平成 29 年 1 月 25 日 翻訳 暫定第 1.0 版

独立行政法人情報処理推進機構

技術本部 セキュリティセンター

情報セキュリティ認証室

改版履歴

バージョン	日付	内容
1.0	2013 年 10 月 21 日	初版発行
1.1	2014 年 2 月 7 日	誤字修正、目次への反映。
2.0	2014 年 12 月 31 日	MDM エージェント SFR の分離 暗号、プロトコル、X.509 要件のアップデート。 MDFPPv2.0 に合致するよう管理機能をアップデート。リモート管理用プロトコルとして SSH を追加。 MDM エージェントと通信するためのプロトコルとして IPsec を削除。X509 登録のオブジェクティブ要件を追加。 オプションのモバイルアプリケーションストア要件を追加。
3.0	2016 年 11 月 11 日	技術的決定に沿ってアップデート。 BYOD 適用例をサポートする要件を追加。 EP（拡張パッケージ）に今、含まれている、IPsec と SSH 要件を削除。

目次

1. 序論

1.1 概要

モバイルデバイス管理 (MDM) 製品は、スマートフォンやタブレットなどのモバイルデバイスへ、企業がセキュリティポリシーを適用することを可能とする。これらのポリシーの目的は、企業データの処理と企業ネットワーク資源への接続をモバイルデバイスに許可するために十分なセキュリティ体制を確立することである。

本文書では、評価対象 (TOE) である MDM システムのセキュリティ機能要件 (SFR) のベースラインセットを提供する。MDM システムは、モバイルデバイスの企業展開の唯一のコンポーネントである。セキュリティポリシーを実施するモバイルデバイスプラットフォームやモバイルアプリケーションのリポジトリを提供するサーバなどの他のコンポーネントは、適用範囲外である。

1.2 用語

以下のセクションは、本 PP で使用されるコモンクライテリアと技術用語の両方を提供する。

1.2.1 コモンクライテリア用語

コモンクライテリア (CC)	情報技術セキュリティ評価のための共通基準（国際標準 ISO/IEC 15408）。
コモンクライテリアテストラボ	コモンクライテリア評価及び認証スキーム（CCEVS）で、米国の国家試験機関認定プログラム(NVLAP)により認定され、コモンクライテリアに基づく表を実施するための認証機関 NIAP により承認された、IT セキュリティ評価機関。
共通評価方法(CEM)	情報技術セキュリティ評価のための共通評価方法。
拡張パッケージ(EP)	ある PP によって記述された製品の特定の部分についての一連の実装依存なセキュリティ要件。
プロテクションプロファイル(PP)	ある分類の製品についての一連の実装依存なセキュリティ要件。
セキュリティ保証要件(SAR)	それらの SFR の TOE の適切な実装が、評価者によってどのように検証されるかについての要件。
セキュリティ機能要件(SFR)	TOE によって実施されるセキュリティについての要件。
セキュリティターゲット(ST)	具体的な製品についての、一連の実装依存なセキュリティ要件。
評価対象(TOE)	評価の対象である製品。
TOE セキュリティ機能(TSF)	評価の対象である製品のセキュリティ機能。
TOE 要約仕様(TSS)	ST における SFR を TOE がどのように満たすかについての記述。

1.2.2 技術用語

管理者	モバイルデバイスについて企業により適用されるポリシーの設定を含めて、管理者アクティビティに責任を持つような要員。この管理者は、モバイルデバイス管理（MDM）管理者であり、MDM エージェントを介して活動する。
データ	サーバまたはモバイルデバイスによって格納され、または伝送されるプログラム／アプリケーションまたはファイル。
開発者モード	ソフトウェアのデバッグのために強化されたシステムアクセスを提供するために、利用者に利用可能であるような追加サービス中の状態。
登録状態	モバイルデバイスが MDM からのポリシーにより管理されている状態。
企業アプリケーション	公開アプリケーションストアとは相対するものとして企業により提供され、管理されるようなアプリケーション。
企業データ	企業サーバ内に存在する、または企業により定義され、管理者により実装されたセキュリティポリシーにしたがってアクセスを許可されたモバイルデバイスへのモバイルデバイス上に一時的に保存された、任意のデータ。
鍵暗号化鍵	データ暗号化鍵(DEK)または鍵を含むストレージリポジトリのような、その他の鍵を暗号化するために使用されるような鍵。
ロック状態	デバイスが電源供給されているが、ほとんどの機能が認証なしには利用不可能なモバイルデバイス状態。
モバイルデバイス利用者	モバイルデバイスを利用し、責任を持っている人。
オペレーティングシステム	最高特権レベルで実行し、直接ハードウェア資源を制御できるソフトウェア。現代的なモバイルデバイスは通常少なくとも 2 つの主たる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、そしてひとつは、アプリケーションプロセッサ上で動作するもの。アプリケーションプロセッサのプラットフォームは、ほとんどの利用者との対話を取り扱い、アプリケーション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プラットフォームは、携帯電話ネットワークとの通信を取り扱い、その他の周辺を制御するかもしれない。用語 OS は、そのような背景なしに、アプリケーションプロセッサのプラットフォームを参照すると思われる。
電源オフ状態	モバイルデバイスのシャットダウン状態。
保護データ	モバイルデバイス上のすべての非 TSF データで、利用者または企業のデータを含む。保護データは、モバイルデバイスが電源オフ状態にある間は暗号化される。これには、ソフトウェアベースのストレージにおける鍵が含まれる。機微なデータと重複するかもしれない。
ルート暗号化鍵	そのデバイスのすべてのその他の鍵を暗号化するために使用されるような、特定のデバイスと結びつけられた鍵。

機微なデータ	モバイルデバイスによって暗号化されるようなデータ。すべての利用者または企業のデータを含むかもしれない、または電子メール、メッセージング、文書、カレンダ項目、または連絡先のような具体的なアプリケーション用のデータであるかもしれない。モバイルデバイスがロック状態にある間、保護されるかもしれない。最小限、スフとウェアベース鍵ストレージにおける何らかの鍵が含まれなければならない。
トラストアンカーデータベース	信頼されるルート認証局の証明書のリスト
TSF データ	セキュリティ要件を実施するために使用されるような TSF の動作のためのデータ。
登録抹消状態	MDM によって管理されないときのモバイルデバイスの状態。
ロック解除状態	電源が投入され、その機能が利用可能であるようなモバイルデバイスの状態。

1.3 適合する評価対象 (TOE)

モバイルデバイス管理 (MDM) システムは、2 つの主要なコンポーネントから構成される：MDM サーバソフトウェアと MDM エージェント。オプションで、MDM システムは、別のモバイルアプリケーションストア(MAS)サーバから構成されるかもしれない。

1.3.1 TOE 境界

MDM システム運用環境は、下図に示すように、MDM エージェントが常駐するモバイルデバイス、MDM サーバが動作するプラットフォーム、及びこれらが通信を行う信頼されない無線ネットワークから構成される。

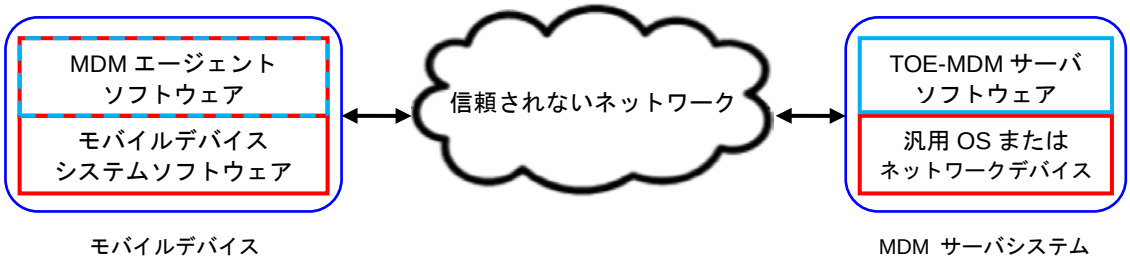

図 1：MDM システムの運用環境

MDM サーバは、高信頼ネットワーク環境中で実行される、汎用プラットフォーム上またはネットワークデバイス上のアプリケーションである。MDM サーバは、モバイルデバイスポリシーの管理と、モバイルデバイスのふるまいに関する報告を提供する。MDM サーバは、デバイスの登録の管理、構成と MDM エージェントへのポリシーの送信、デバイスの状態の報告の収集、及びエージェントへのコマンドの送信を担当する。MDM サーバソフトウェアが動作するプラットフォームは、汎用プラットフォームまたはネットワークデバイスである。

MDM エージェントは、企業管理者により制御される MDM サーバへのセキュアな接続を確立し、管理者のポリシーに従ってモバイルデバイスを構成する。オプションで MDM エージェントは、企業アプリケーションをダウンロードし、インストールするため、MAS サーバ

と対話してもよい。MDM エージェントは、*MDM エージェントの拡張パッケージ*で対処される。MDM エージェントが MDM 開発者によって開発されたアプリケーションとしてモバイルデバイスにインストールされる場合、EP は、本 PP を拡張し、TOE に含まれる。この場合、本 PP で規定される TOE セキュリティ機能は、MDM サーバに追加して、MDM エージェントによって対処されなければならない。さもなければ、MDM エージェントは、モバイルデバイスベンダーによって提供され、本 PP の対象範囲外である；しかし、MDM は、MDM サーバによってサポートされるモバイルプラットフォームを示すことが要求され、それらのプラットフォームのネイティブの MDM エージェントに対してテストされなければならない。

MAS サーバは、信頼されるネットワーク環境で実行するような、汎用プラットフォームまたはネットワークデバイス上のアプリケーションである。MAS サーバは、MDM サーバと別であるか、含まれているかもしれない。MAS サーバは、企業のアプリケーションをホストし、エージェントを認証し、登録されたモバイルデバイスに対してセキュアにアプリケーションを伝送する。

1.4 適用例

本 PP は、4 つの適用例を定義する：

[適用例 1] 汎用企業用途の企業所有デバイス

企業所有デバイスの汎用業務用途は、会社所有個人利用可能（COPE：Corpoately Owned, Personally Enabled）と通常は呼ばれている。この用途には、構成及びソフトウェアインベントリへの高度な企業のコントロールが必要とされる。企業管理者は、利用者へ支給する前にモバイルデバイス上にポリシーを確立するために、MDM 製品を利用する。利用者は、インターネット接続を用い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企業アプリケーションを実行するためにインターネット接続を利用するかもしれないが、この接続は企業の高度なコントロール下にあるかもしれない。利用者は、個人的で非企業用途で、データを保管し、アプリケーションを利用することも想定されるかもしれない。企業管理者は、セキュリティポリシーを展開し、モバイルデバイスの状態を問い合わせるため、MDM 製品を利用する。MDM は、修正アクションのためのコマンドを発行するかもしれない。

[適用例 2] 特化した高セキュリティ用途の企業所有デバイス

ネットワーク接続性が意図的に制限され、構成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企業所有デバイスは、特化した高セキュリティの適用例に適切である。先ほどの適用例と同様に、そのようなポリシーを利用者へ支給する前にモバイルデバイス上に確立するために、MDM 製品が用いられる。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企業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。デバイスの利用には、いかなる汎用の適用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できるような、利用ポリシーの遵守が要求されるかもしれない。

[適用例 3] 個人及び企業用途の個人所有デバイス

個人的な活動と企業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。デバイスは、重要な個人的用途が発生した後、企業資源へのアクセスのために初期設定されるかもしれない。企業所有の事例とは異なり、このシナリオでは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、企業は、利用者が主として個人的に利用するためにデバイスを購入しデバイスの機能を制限するようなポリシーを受け入れる見込みがないので、実施可能なセキュリティ

ポリシーに制限される。

しかし、企業は利用者に企業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から、企業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と、モバイルデバイスのシステムソフトウェアの完全性などの健全性報告を、アクセスを許可する前に要求することになる。MDM の管理者は、非適合デバイスについて、企業データの抹消など、修正アクションを確立することができる。これらの管理策は、企業と個人の行動を区別するためにデバイス自体に組み込まれた分離メカニズム、または企業資源へのアクセスを提供しモバイルデバイスによって提供されるセキュリティ機能を利用するサードパーティアプリケーションによって潜在的に実施可能である。運用環境及び企業の受け入れ可能なリスクレベルに基づき、附属書 E で定義された適用例 3 のテンプレートにある、本プロテクションプロファイルのセクション 5 に概説されたそれらのセキュリティ機能要件は、本 BYOD 適用例のセキュアな実装に十分である。

[適用例 4] 個人及び限定的な企業利用のための個人所有のデバイス

個人所有のデバイスは、企業電子メールのような限定された企業サービスへのアクセスについても得られるかもしれない。利用者は、企業または企業データへの完全なアクセスを持たないので、企業は、デバイス上の任意のセキュリティポリシーを実施する必要はないかもしれない。しかし、企業は、それらのクライアントへモバイルデバイスによって提供されているサービスが危殆化しないような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。運用環境と企業のリスクレベルに基づき、本 PP のセクション 5 で概説されたそれらのセキュリティ機能要件は、この BYOD 適用例のセキュアな実装に十分である。

2. 適合主張

適合ステートメント

本 PP に適合するため、ST は、[CC]パート 1（ASE_CCL）で定義される正確適合（Strict Conformance）のサブセットである、完全適合（Exact Conformance）を実証しなければならない。ST は、以下である本 PP にすべてのコンポーネントを含めなければならない：

- 無条件（常に要求される）
- 選択ベース（特定の選択が無条件の要件で選択されたとき要求される）

以下であるようなコンポーネントを含むこともある：

- オプション
- オブジェクティブ

無条件の要件は、文書の本文（セクション 5）で見つかるが、附属書には、選択ベース、オプション、及びオブジェクティブ要件が含まれる。ST は、これらのコンポーネントのいずれかを繰り返ししてもよいが、本 PP で定義されていない追加のコンポーネント（例、CC パート 2 から）を導入してはならない。

CC 適合主張

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

PP 主張

本 PP は、いかなるプロテクションプロファイルへの適合をも主張しない。

パッケージ主張

本 PP は、いかなるパッケージへの適合も主張しない。

3. セキュリティ課題記述

3.1 脅威

T.MALICIOUS_APPS

モバイルデバイス上にロードされるアプリには、悪意のあるコードまたは悪用可能なコードが含まれる可能性があるため、悪意や欠陥のあるアプリケーションの脅威が存在する。MDM の管理者またはモバイルデバイス利用者は、うっかり悪意のあるコードをインポートするかもしれない、または攻撃者が TOE または TOE データの危殆化を招くような、悪意のあるコードを TOE へ挿入するかもしれない。

T.NETWORK_ATTACK

攻撃者は、MDM サーバとしてなりすましをするかもしれない、また悪意のある管理コマンドを送信することによってモバイルデバイスの完全性の危殆化を試行するかもしれない。

T.NETWORK_EAVESDROP

許可されないエンティティは、リモート管理コマンドを監視し、アクセスを取得し、暴露し、または改変するために、MDM とモバイルデバイスの間の通信を傍受しするかもしれない。許可されないエンティティは、TOE データを監視し、アクセスを取得し、暴露し、または改変するため、モバイルデバイスと企業の間の保護されない無線通信を傍受するかもしれない。

T.PHYSICAL_ACCESS

モバイルデバイスが紛失や盗難にあうかもしれない、また許可されない個人が利用者データのアクセスを試行するかもしれない。これらの攻撃は主としてモバイルデバイスプラットフォームに対するものであり、TOE は、これらの脅威に対処するような機能を設定する。

3.2 前提条件

A.CONNECTIVITY

TOE は、管理アクティビティを行うためのネットワーク接続性に依存している。TOE は、接続性が得られない、または信頼できない場合、確実に運用する。

A.MDM_SERVER_PLATFORM

MDM サーバは、管理機能を提供するような信頼性できるプラットフォームとローカルネットワークに依存している。

MDM サーバは、信頼されるタイムスタンプ、利用者及びグループアカウント管理、ローカルまたはネットワークディレクトリサービス経由でのログオン及びログアウトのサービス、リモートアクセス制御、及びその他のサーバへの監査ログの負荷軽減を含めるための監査ログ管理サービスを含む幅広いセキュリティ関連サービスを提供するため、本プラットフォームに依存している。プラットフォームは、ネットワークの役割を MDM 機能の提供に限定するような、ホストベースファイアウォールのような機能を持った MDM サービスを提供するように、特別に構成されると想定されている。

A.PROPER_ADMIN

不注意、意図的な怠慢、または敵対的であったりしないような、1 人以上の力量のある、信頼された要員が、TOE 管理者として任命され権限付与され、またガイダンス文書を遵守して使用する。

A.PROPER_USER

モバイルデバイス利用者は、意図的な怠慢、敵対的であったりせず、また合理的な企業のセキュリティ方針を遵守してデバイスを使用する。

3.3 組織のセキュリティ方針

P.ACCOUNTABILITY

TOE を操作する要員は、TOE 内の自分のアクションに責任を持たなければならない (shall)。

P.ADMIN

モバイルデバイスのセキュリティ機能の構成は、企業のセキュリティポリシーに忠実でなければならない (must)。

P.DEVICE_ENROLL

モバイルデバイスは、特定の利用者によって企業ネットワーク内で利用される前に、MDM の管理者によってその利用者について登録されなければならない (must)。

P.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、管理者が MDM システムを介して改善アクションを適用できるように、即座に管理者へ通知しなければならない (must)。

4. セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

O.ACCOUNTABILITY

TOE は、その管理者によって取られる管理アクションを記録するようなログ出力設備を提供しなければならない(must)。

O.APPLY_POLICY

TOE は、モバイルデバイス OS と MDM サーバとの対話を介してモバイルデバイス上の企業セキュリティポリシーの設定と実施を促進しなければならない(must)。これには、ポリシーの更新及び起こりうる管理サービスからの登録抹消を含めて、デバイスのライフサイクル全体を通した管理へのデバイスの初期登録が含まれる。

O.DATA_PROTECTION_TRANSIT

MDM サーバと MDM エージェントの間のデータ交換は、監視、アクセス、または改変から保護されなければならない(must)。

O.INTEGRITY

TOE は、重要な機能、ソフトウェア／ファームウェア及び維持されているデータの完全性を保証するための自己テストを実行する機能を提供する。TOE は、ダウンロードされたアップデートの完全性を検証する手段についても提供する。

O.MANAGEMENT

TOE は、その管理機能関連のアクセス制御を提供する。

4.2 運用環境のセキュリティ対策方針

OE.DATA_PROPER_ADMIN

TOE 管理者は、信頼されるやり方ですべての管理者ガイダンスに従い、適用すると信頼されている。

OE.DATA_PROPER_USER

モバイルデバイスの利用者は、信頼されたやり方でモバイルデバイスをセキュアに利用し、すべてのガイダンスを適用するよう訓練される。

OE.IT_ENTERPRISE

企業 IT 基盤は、TOE 及び許可されないアクセスを防止するようなモバイルデバイスに対して利用可能なネットワークのためのセキュリティを提供する。

OE.MOBILE_DEVICE_PLATFORM

MDM エージェントは、暗号サービスとデータ保護と同様なポリシー実施を提供するため、信頼できるモバイルプラットフォームとハードウェアに信頼を置く。モバイルプラットフォームは、MDM エージェントの高信頼アップデートとソフトウェア完全性検証を提供する。

OE.TIMESTAMP

信頼できるタイムスタンプは、TOE の運用環境によって提供される。

OE.WIRELESS_NETWORK

無線ネットワークはモバイルデバイスが利用可能であること。

5. セキュリティ要件

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

5.1 表記法

CC では、割付、選択、選択中の割付、及び詳細化という、セキュリティ機能要件に関する操作を定義している。本文書では、CC によって定義される操作を特定するため、以下のフォント規則を用いる：

- **詳細化**操作（**太字**で表記）は、要件に詳細を追加するために使用される、ゆえに更に要件を制約する。
- **選択**（*イタリック*で表記）：要件を記述している[CC]によって提供される 1 つ以上の選択肢を選択するために使用される。
- **割付**（*イタリック*で表記）は、パスワード長のような、規定されていないパラメタに規定された値を割り付けるために使用される。大かっこ内の値の表示は割付を示す。
- **繰返し**操作：括弧内の数字（例、 (1) ）で識別される。
- **拡張 SFR**：SFR 名の後にラベル”EXT”を付けることで識別される。

5.2 保証アクティビティのテスト環境

以下の保証アクティビティで記述されるとおり、MDM システムの ST は、運用する MDM サーバと共にすべてのサポートされる MDM エージェント／MD プラットフォームを列挙するよう要求される。エージェントの利用を含むテストのための特定された保証アクティビティは、ST において列挙された MDM エージェント／プラットフォームのそれぞれについて完成されるべきである。

エージェントの利用を含むテストのための評価者のアクティビティは、サーバがエージェントと適切に対話することを保証する（即ち、ポリシー更新をエージェントへ送信する）が、エージェントが受信した出たを正しく取り扱いことをは保証しない（即ち、ポリシーをデバイスに適切に適用する）、即ち、これはモバイルデバイス基盤 PP の保証アクティビティまたはモバイルデバイス管理エージェントの拡張パッケージの中で対応される。

5.3 TOE セキュリティ機能要件

5.3.1 セキュリティ監査 (FAU)

FAU_ALT_EXT.1 エージェント警報

FAU_ALT_EXT.1.1 MDM エージェントは、以下のいずれかの事象が発生した際には高信頼チャネルを介して MDM サーバへ警報を提供しなければならない (shall)：

a. 登録状態の変更；
b. モバイルデバイスへのポリシーの適用の失敗、
c. [*選択：[割付：その他の事象]、その他の事象なし*]

適用上の注釈： *MDM エージェントは、管理されたモバイルデバイスに関するポリシーの適用の成功に関して、MDM サーバへ報告するよう要求される、また失敗*

は、このような警告の欠如から推測可能である。本要件は、ポリシーが適切にインストールされないときに MDM サーバが管理者に通知することを保証することを意図している。ポリシーアップデートの適切なインストールの失敗は、モバイルデバイスの登録状態には影響を与えない。

保証アクティビティ：

TSS

評価者は TSS を検査して、どのように警報が実装されているかを検証しなければならない (shall)。評価者は、それぞれの割付された事象の記述が TSS で提供されることについても検証しなければならない(shall)。

テスト

ST でサポートされた、列挙されたそれぞれの MDM エージェント／プラットフォームについて：

テスト 1：評価者は、デバイスを登録し、MDM サーバが登録状態の変更について管理者に警告することを保証しなければならない(shall)。評価者は、デバイスを登録抹消（除去）し、MDM サーバが登録状態の変更を管理者に警告することを保証しなければならない(shall)。

テスト 2：評価者は、MDM エージェントが適用できないような、ポリシーを設定しなければならない(shall)。これらのポリシーは以下を含む：

- *MDM サーバのインタフェース上で設定可能な設定であるが、MDM エージェントが動作するプラットフォームによってサポートされないような設定、もしこのような設定が存在する場合*
- *デバイスへ送信する前にポリシーの手動での改変を要求するような、無効なパラメタを持つ有効な設定*

評価者は、このようなポリシーを展開し、MDM サーバがポリシーの適用に失敗したことについて管理者に警告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）評価者は、列挙されたそれぞれの事象についてトリガーをかけ、MDM サーバが管理者に警告することを保証しなければならない(shall)。

FAU_NET_EXT.1 ネットワーク到達性レビュー

FAU_NET_EXT.1.1 MDM サーバは、登録されたエージェントのネットワーク接続性の状態を読み出す能力を許可された管理者に提供しなければならない (shall)。

適用上の注釈： *MDM サーバは、MDM エージェント EP の FAU_ALT_EXT.2 に従ってエージェントからの定期的な到達可能性事象警告を用いて、登録されたエージェントのネットワーク接続性の状態を確立する。この状態は、エージェントが応答するよう要求される MDM サーバからの「ポーリング」または MDM エージェントによって開始された計画された定期的な接続性の通知を用いて、決定されてもよい。*

保証アクティビティ

TSS

評価者は、サポートされたモバイルプラットフォームのそれぞれに

ついて、到達可能性の事象がどのように実装されているかについて、TSS に記述されていることを保証する。評価者は、この記述に到達可能性の事象を開始するのは誰か（MDM エージェントまたは MDM サーバ）について、明確に示していることを検証する。

ガイダンス

評価者は、ガイダンスが登録されたエージェントのネットワーク接続性の状態を決定する方法について、管理者に指示していることを検証しなければならない(shall)。

テスト

ST でサポートされたとおり、列挙された MDM エージェント／プラットフォームのそれぞれについて：

評価者は、このような接続性を持つ場合と持たない場合の両方について、ネットワーク到達可能性テストを実行するように MDM エージェント／プラットフォームを設定しなければならない(shall)、またガイダンスに従って評価者が両方を反映する結果を決定できることを保証しなければならない(shall)。

5.3.2 識別と認証 (FIA)

FIA_ENR_EXT.1 拡張：モバイルデバイスの管理への登録

FIA_ENR_EXT.1.1 MDM サーバは、モバイルデバイスの登録中、高信頼チャネルを介してリモート利用者を認証しなければならない(shall)。

適用上の注釈： *MDM サーバは、モバイルデバイスのリモート登録を実行するような利用者の認証決定を実行するため、それ自身のディレクトリまたはディレクトリサーバを利用するかもしれない。*

保証アクティビティ：

評価者は TSS を検査し、ST でサポートされるとおり、列挙された MDM エージェント／プラットフォームのそれぞれについて、登録のプロセスが TSS に記述されていることを検証しなければならない (shall)。この記述には、登録のために利用される高信頼パス (FTP_TRP.1(2))、利用者認証の方法 (利用者名／パスワード、トークン等)、認証判断の方法 (ローカルまたはリモート認証サービス)、及び認証の成功時に MDM サーバ上で実行されるアクションが含まれなければならない (shall)。

テスト

テスト 1：評価者は、正しいクレデンシャルを提供せずにデバイスの登録を試行しなければならない (shall)。評価者は、デバイスが登録されないこと、及び記述された登録アクションが実行され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、正しいクレデンシャルを提供してデバイスの登録を試行しなければならない (shall)。評価者は、デバイスが登録されること、及び記述された登録アクションが実行されることを検証しなければならない (shall)。

FIA_ENR_EXT.1.2 MDM サーバは、利用者のデバイス登録を [*選択 : [選択 : IMEI、[割付 : ユニークなデバイス ID]]によって規定されたデバイス、特定のデバイスモデル、デバイスの数、特定の時間間隔*] 及び[*選択 : [割付 : その他の機能]、なし*] に制限しなければならない (shall)。

適用上の注釈 : *本要件は、企業が利用者のデバイスの登録を制限できるよう設計されている。*

本プロテクションプロファイルの次期バージョンで、一意のデバイス ID が利用者登録を制限するために要求されるだろう。一意のデバイス ID は、IMEI または特定のプラットフォーム特有の ID である可能性がある。他のオプションが次期バージョンではまだ選択可能であるが、一意のデバイス ID は要求されるだろう。

保証アクティビティ :

TSS

評価者は TSS を検査し、利用者のデバイスの登録を制限するポリシーが実装されていることを検証しなければならない (shall)。

ガイダンス

評価者は、利用者登録を制限する方法が管理者ガイダンスに記述されていること及びそれが制限の設定方法について管理者に指示を与えていることを保証しなければならない(shall)。

テスト

選択されたポリシーのそれぞれの種別について、評価者は以下のテストを実行しなければならない (shall) :

テスト 1 : 評価者は、登録を防止するため、管理ガイダンスに従って MDM サーバの設定試行しなければならない (shall)。評価者は、設定された制限を超えて利用者がデバイスを登録できないことを検証しなければならない (shall)。(例えば、評価者は、許可されないデバイスの登録を試行してもよいし、許可された数を超えた追加のデバイスの登録を試行してもよい。)

5.3.3 セキュリティ管理 (FMT)

FMT_MOF.1(1) **セキュリティ機能のふるまいの管理**

FMT_MOF.1.1(1) MDM サーバは、以下の機能を実行する能力を[

- *FMT_SMF.1(1) で列挙されたもの*
- *FMT_SMF.1(1) で列挙されたポリシーの有効化、無効化、及び改変*
- *FMT_SMF.1(2) で列挙されたもの*

[*許可された管理者*] *に*制限しなければならない (shall)。

適用上の注釈 : *本要件は、FMT_SMF.1(1) で列挙された機能及びポリシーの有効化、無効化、改変、及び監視を行う権限を管理者が持つ機能の概要を示している。また、MDM サーバ自体を維持し設定するために必要な機能も含まれている。*

保証アクティビティ :

TSS

評価者は、どのようなセキュリティ管理機能が管理者に制限されてい

るか、及びどのようなアクションがそれぞれの管理機能のために取ることが可能かについて、TSS に記述されていることを保証するため、TSS と利用者文書を検査しなければならない (shall)。評価者は、セキュリティ管理機能が許可された管理者に制限され、そして管理者だけが利用者文書で記述されたとおりのアクションを取ることができることを検証しなければならない (shall)。

テスト

評価者は、許可されていない利用者として、FMT_SMF.1(1) の機能及びポリシーへのアクセスを試行し、その試行が失敗することを検証しなければならない (shall)。

FMT_MOF.1(2) **セキュリティ機能のふるまいの管理 (登録)**

FMT_MOF.1.1(2) **MDM サーバ**は、[*登録プロセスを開始する*] 能力を[*許可された管理者及び MD 利用者*]に制限しなければならない (shall)。

適用上の注釈： *本要件は、管理者と MD 利用者の両方が実行してもよい登録機能の概要を概説している。登録アクションは、FIA_ENR_EXT.1 の一部として TSS で特定される。*

許可された管理者は、利用者が所有するようなモバイルデバイスの登録をリモートで開始しないが、管理者が所有しているときにモバイルデバイスを登録してもよい、例えば、利用者にモバイルデバイスを配付する前。

保証アクティビティ：

TSS

評価者は TSS を検査して、許可されていない利用者が MDM サービスでの登録をどのように防止しているかについて TSS に記述されていることを検証しなければならない (shall)。

テスト

この機能のテストは、FIA_ENR_EXT.1 と組み合わせて実行される。

FMT_POL_EXT.1 **高信頼ポリシーアップデート**

FMT_POL_EXT.1.1 MDM サーバは、MDM エージェントに対して、ディジタル署名されたポリシー及びポリシーアップデートを提供しなければならない (shall)。

適用上の注釈： *本要件の意図は、ポリシーを強制するような企業にそのポリシーを暗号学的に結び付けることであり、(FPT_ITT.1 または FTP_ITC.1(2)によってすでにほごされているように) 送信中のポリシーを保護することではない。これは、複数の企業に接続する利用者にとって、特に重要である。*

保証アクティビティ：

TSS

ポリシーは、FCS_COP.183)のアルゴリズムを用いて、その企業によってディジタル署名されなければならない(must)。評価者は、TSS にポリシーが TSF によってディジタル署名される方法が記述されてい

ることを保証しなければならない(shall)。

ガイダンス

評価者は、ポリシーの署名に利用されるその企業の証明書の設定またはそれらを適用する前にポリシーに署名することについて、AGD ガイダンスが管理者に指示していることを検証しなければならない(shall)。

テスト

評価者は、FMT_SMF.1(1) に従ってポリシーアップデートを実行しなければならない(shall)。評価者は、送信中の MDM サーバ、または MDM エージェントのいずれかでのポリシーを検査し、TSF がアップデートに署名し、それを MDM エージェントへ提供することを検証しなければならない(shall)。

FMT_SMF.1(1) **管理機能の特定 (エージェントのサーバ設定)**

FMT_SMF.1.1(1) **MDM サーバ**は、以下の**コマンドを MDM エージェントへ発行**できなければならない (shall) :

1. ロック状態への移行、(MDF 機能 6)
2. 保護データの完全なワイプ(訳注：消去)、(MDF 機能 7)
3. 管理からの登録抹消、
4. ポリシーのインストール、
5. 接続状態の問い合わせ、
6. MD ファームウェア／ソフトウェアの現在のバージョンの問い合わせ、
7. デバイスのハードウェアモデルの現在のバージョンの問い合わせ、
8. 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の問い合わせ、
9. 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、(MD 機能 11)
10. アプリケーションのインストール、(MDF 機能 16)
11. システムソフトウェアのアップデート、(MDF 機能 15)
12. アプリケーションの削除、(MDF 機能 14)

及び MDM エージェントへの以下のコマンド： [*選択：*

13. 企業のアプリケーションの削除、(MDF 機能 17)
14. 企業のデータのワイプ(消去)、(MDF 機能 28)
15. トラストアンカーデータベースにおけ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ーのリスト]]の削除、(MDF 機能 12)
16. 利用者への警報、
17. セキュア鍵ストレージへの鍵／秘密のインポート、(MDF 機能 9)
18. セキュア鍵ストレージにおけ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ーのリスト]]の破壊、(MDF 機能 10)
19. MD により保持される監査ログの閲覧、(MDF 機能 32)
20. MD ソフトウェアの完全性検証値の取り出し、(MDF 機能 38)
21. [選択：アプリケーション処理、アプリケーション処理のグループ]

間のデータ共有の例外の承認、(MDF 機能 42)

22. *[割付：アプリケーションの特徴]に基づくアプリケーション処理グループへのアプリケーションの配置、(MDF 機能 43)*
23. *バイオメトリックテンプレートの廃棄。*
24. *[割付：MD 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]*

並びに以下の MD 設定ポリシー：

25. パスワードポリシー：
    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 (MDF 機能 1)
26. セションロックのポリシー：
    a. 画面ロックの有効化／無効化
    b. 画面ロックのタイムアウト
    c. 認証失敗の回数 (MDF 機能 2)
27. MD が接続してもよい無線ネットワーク(SSID) (WLAN クライアント EP 機能 2)
28. 各無線ネットワークのセキュリティポリシー：
    a. [*選択：MD が WLAN 認証サーバ証明書を受け入れるような CA(訳注：認証局)を規定する、受け入れ可能な WLAN 認証サーバ証明書の FQDN を規定する*]
    b. セキュリティ種別を規定する能力
    c. 認証プロトコルを規定する能力
    d. 認証用に利用されるべきクライアントクレデンシャルを規定
    e. [*割付：任意の追加の WLAN 管理機能*] (WLAN クライアント EP 機能 1)
29. 以下によるアプリケーションのインストールポリシー [*選択：*
    a. 許可されるアプリケーションリポジトリの規定、
    b. 一連の許可されるアプリケーション及びバージョンの規定(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拒否*]、(MDF 機能 8)
30. [*選択：アプリ毎ベースでの、アプリケーション処理グループ毎ベース、その他の方法なし*]での、デバイス全体にわたる[*割付：音声または映像収集デバイスのリスト*] についての有効化／無効化ポリシー、(MDF 機能 5)

及び以下の MD 設定ポリシー： [*選択：*

31. *[選択：アプリ毎ベースでの、アプリケーション処理グループ毎ベース、その他の方法なし]での、MD 全体にあわたる VPN 保護についての有効化／無効化ポリシー、(MDF 機能 3)*
32. *[割付：無線のリスト] についての有効化／無効化ポリシー、(MDF 機能 4)*
33. *[割付：外部アクセス可能なハードウェアポートのリスト] を介したデータ転送についての有効化／無効化ポリシー、(MDF 機能 24)*
34. *[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／無効化ポリシー、(MDF 機能 25)*
35. *開発者モードについての有効化／無効化ポリシー、(MDF 機能 26)*
36. *保存データ保護についての有効化ポリシー、(MDF 機能 20)*
37. *リムーバブルメディアの保存データ保護についての有効化ポリシ*

ー、(MDF 機能 21)

38. ローカル認証の迂回についての有効化／無効化ポリシー、(MDF 機能 27)
39. Bluetooth 高信頼チャネルポリシー：
    a. 検出可能モード(Discoverable mode) の無効化／有効化 (BR/EDR 用)
    b. Bluetooth デバイス名の変更、[選択：
    c. Bluetooth を用いて利用される追加の無線技術の許可／禁止
    d. Advertising の無効化／有効化 (LE 用)
    e. Connection mode の無効化／有効化
    f. Bluetooth サービス及び／またはデバイス上で利用可能なプロファイルの無効化／有効化
    g. それぞれのペアリングのための最小レベルのセキュリティを規定
    h. Out of Band ペアリングの受け入れ可能な方法を設定
    i. その他の Bluetooth 設定なし] (MDF 機能 18)
40. 以下のロック状態での通知表示のポリシーの有効化／無効化：
    [選択：
    a. 電子メール通知、
    b. カレンダの予定、
    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] (MDF 機能 19)
41. MD が証明書の有効性を決定するための接続を確立できなかった場合、高信頼チャネルを確立するか、または確立を禁止するかについてのポリシー、(MDF 機能 30)
42. 携帯電話ネットワーク基地局へ接続するために利用される携帯電話プロトコルについてのポリシーの有効化／無効化、(MDF 機能 31)
43. トラストアンカーデータベースの 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についてのポリシー、 (MDF 機能 29)
44. アプリケーション上のディジタル署名の検証に用いられる [選択：証明書、公開鍵]、(MDF 機能 33)
45. 複数のアプリケーションによる鍵／秘密の共有された利用の例外についてのポリシー、(MDF 機能 34)
46. 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／秘密の破棄の例外についてのポリシー、(MDF 機能 35)
47. ロック解除バナーのポリシー、(MDF 機能 36)
48. 監査可能項目の設定 (MDF 機能 37)
49. 以下の有効化／無効化 [選択：
    a. USB 大容量ストレージモード、
    b. 利用者認証なしの USB データ転送
    c. 接続システムの認証なしの USB データ転送] (MDF 機能 39)
50. [選択：すべてのアプリケーション、選択されたアプリケーション、選択されたアプリケーションのグループ、設定データ]の[選択：ローカル接続されたシステム、リモートシステム]へのバックアップの有効化／無効化 (MDF 機能 40)
51. 以下の有効化／無効化 [選択：

a. *[選択：事前共有鍵、パスコード、認証なし]によって認証されるホットスポット機能、*
b. *[選択：事前共有鍵、パスコード、認証なし]によって認証されるUSB テザリング] (MDF 機能41)*

52. *利用者登録抹消についてのポリシーの有効化委／無効化*
53. *デバイスメッセージング機能の有効化／無効化ポリシー、*
54. *常時オンVPN 保護アクセスデバイスについてのポリシーの有効化／無効化 (MDF 機能45)*
55. *バイオメトリック認証要素の利用についてのポリシーの有効化／無効化 (MDF 機能23)*
56. *接続性タイムアウトポリシー：*
    a. *許可された[選択：喪失した到達可能性イベントの数、サーバ接続性のない時間の長さ]*
    b. *サーバ接続性タイムアウトが超過したとき、エージェントは[選択：利用者パスワードを無効化、デバイスをワイプ]及び[選択：[割付：その他のアクション]、なし]を行わなければならない(shall)。*
57. *[割付：MD によって提供されるべきその他のポリシーのリスト]、その他のポリシーなし*]。

適用上の注釈：

本要件は、MDM エージェントを設定するためにMDM サーバが管理者へ提供するすべての設定機能を取り込むものである。本要件は、MDM エージェントコマンドと MDM エージェントポリシーという、2 つの設定領域に分割されている。ST 作成者は、適切な割付ステートメントを完成させることによって、さらにコマンドや設定ポリシーを追加することができる。

ST 作成者は、モバイルデバイスによって提供されない機能は一切主張してはならない (shall not)。ST 作成者によって本要件中に行われるすべての選択及び割付は、検証済みモバイルデバイス ST の選択及び割付と合致すべきである (should)。

機能特有の適用上の注釈：

機能特有の適用上の注釈は、モバイルデバイス基盤(MDF) PP v3.0 を参照する。

機能 16 は、モバイルデバイスの利用者に対して、警告を表示するようなMDM サーバを提供する。

機能 19 に従って読み出された監査記録は、FAU_STG_EXT.1 に従って外部監査サーバへ転送されるべきである。MDM サーバは、それらのログを保持することは想定されない。

機能56 は、エージェントのFPT_NET_EXT.1.1 に対応する。MDM エージェントが「a」で規定された量の時間内にMDM サーバとの到達可能性事象が成功しなかった場合、エージェントは、「b」で選択されたアクションを実行しなければならない(shall)。実現可能ではあるが、必須ではないが、複数のアクションが「b」で選択された場合、それぞれのアクションが「a」における異なるタイムアウトに対応することが可能である。機能56 がST に含まれる場合、FPT_NET_EXT.1.1 がエージェントST に含まれなければならない(shall)。

保証アクティビティ：

TSS

評価者は、列挙された管理機能のそれぞれが TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。評価者は、サポートされる MDM エージェント／プラットフォームについての管理機能とポリシーの間の違いが列挙されていることを検証するため、TSS を検査しなければならない(shall)。評価者は、TSS の機能及びポリシーにおける選択と割付が、サポートされる MD の機能を超えていないことを検証するため、主張されたモバイルデバイスの ST を検査しなければならない(shall)。

評価者は、MDM サーバ上お管理者が利用可能であるすべての管理機能のサブセットであるような、サポートされる MDM エージェント／プラットフォームのそれぞれについて実装された管理機能が特定されていることを保証するため、TSS を検査しなければならない(shall)。

テスト

ST でサポートされるとおり列挙された MDM エージェント／プラットフォームのそれぞれについて：

評価者は、それぞれの MDM エージェント機能を命令し、上記に列挙されたそれぞれの MDM エージェントポリシーを設定する能力を検証しなければならない (shall)。

FMT_SMF.1(2) **管理機能の特定 (サーバのサーバ設定)**

FMT_SMF.1(2) **MDM サーバ**は、以下の管理機能を実行可能でなければならない (shall)：

a. *MDM サーバ用途のための X.509v3 証明書を選択*

b. *登録のために許可された [選択：[選択：IMEI、[割付：ユニークなデバイス ID]]、特定のデバイスモデル、多くのデバイス、特定の期間]及び[選択：[割付：その他の機能]、その他の機能なし]によって規定されたデバイス]を設定、*

[選択：

c. *管理者に接続が有効性を確立させられないときに証明書を受け入れるかどうかを選択することを許可、*

d. *TOE ロック解除バナーを設定、*

e. *エージェントへ以下のコマンドの周期性を設定：[割付：コマンドのリスト]、*

f. *特定のモバイルデバイスから収集されるもの及び収集されないようなプライバシー的に機微な情報を設定、*

g. *登録認証コードが有効である時間の長さを設定、*

h. *追加の管理機能なし]。*

適用上の注釈： *本要件は、下位の MDM サーバを設定するための MDM サーバのすべての設定機能を取り込んでいる。ST 作成者は、割付ステートメントを完成させることによって、より多くのコマンドや設定ポリシーを追加することが可能である。機能 a は、MDM サーバによって利用され*

る証明書を設定するためのプラットフォームに身体を置くことにより満たされるが、MDM サーバは、管理者に具体的な機能のために利用される証明書を選択することを許可しなければならない(shall)。
b の選択は、FIA_ENR_EXT.1.2 の選択に対応する。d の選択は、FIA_X509_EXT.2.2 の選択に対応するような機能を含む。機能 e は、管理者に割付されたコマンドの周期性を設定することを許可する、例えば、「モバイルデバイスにより保持される監査ログの閲覧」。このやり方で管理者は、ログデータの新鮮さを保証し、監査ログの喪失を最小化するため、日々、周期的にモバイルデバイスから監査ログを取り出すように MDM システムを設定可能である。機能 f は、何らかの情報が収集に適さないかもしれないような個人所有のデバイス利用環境を取り扱うために特定のモバイルデバイスから収集するもの及び収集しないような、プライバシー的に機微な情報を設定することを管理者に許可する。プライバシー的に機微な情報には、デバイスの物理的な位置及びインストールされた個人のアプリケーションのリストのような項目が含まれるかもしれない、また、TOE 及び MDM エージェントの具体的な機能に依存して変わるかもしれない。TOE は、登録されたデバイスを企業所有及び個人所有のようなカテゴリーにグループ化し、それぞれのカテゴリーのデバイスから取集される情報を定義する機能を提供するべきである(should)。機能 g は、FMT_SAE_EXT.1 で有効な登録についての利用者認証コードの時間の長さの設定に対応する。この機能は、FMT_SAE_EXT.1 が ST に含まれる場合に、及びその場合のみに ST に含まれなければならない(shall)。

保証アクティビティ

TSS

評価者は、列挙されたそれぞれの管理機能が TSS に記述されていることを保証するため、TSS を検査しなければならない (shall)。機能 f について、評価者は、登録されたモバイルデバイスから収集するような機能を TOE が持っているプライバシー的に機微な情報について TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、どの選択肢が利用可能であるか及び列挙されたそれぞれの管理機能の設定方法についての詳細な指示が AGD ガイダンスに含まれていることを検証しなければならない(shall)。

テスト

機能 b,c,d 及び g のテストは、その機能用途と組み合わせて実行される。テスト 3 は、機能 f についても網羅する。評価者は、以下のテストを実行しなければならない (shall)。

テスト 1：評価者は、TSF 認証証明書を設定し、確立された信頼された接続(FPT_ITT.1、FTP_ITC.1、及び FTP_PTRP.1)で正しい証明書が利用されることを検証しなければならない(shall)。

テスト 2：(条件付き) 評価者は、いくつかの設定された時間周期についてエージェントへの割り付けられたコマンドのリストについての周期性を設定しなければならない(shall)。

テスト 3：(条件付き) 評価者は、割り付けられた機能が設定され、

機能の意図したふるまいが MDM サーバによって実装されたことを実証するためのテストを設計し実行しなければならない(shall)。

FMT_SMR.1 **セキュリティ管理役割**

FMT_SMR.1.1 MDM サーバは、役割として **管理者、MD 利用者、及び** [*割付：追加の許可された識別された役割*]を維持しなければならない (shall)。

FMT_SMR.1.2 **MDM サーバ**は、利用者を役割に関連付けられなければならない (shall)。

適用上の注釈： *MDM サーバは、異なる利用者役割によって設定され維持されると、想定される。割付には、サポートされる役割を列挙する ST 作成者により利用される。最小限、1 つの管理役割がサポートされなければならない (shall)。追加の役割が 1 つもサポートされない場合には、「追加の役割なし」が記述される。MD 利用者役割は、FIA_ENR_EXT.1 に従って MDM へのモバイルデバイスの登録のために用いられる。*

保証アクティビティ

TSS

評価者は、管理者の役割とその役割に付与された権限及びその役割の制限が TSS に記述されていることを検証するため、TSS を検査しなければならない (shall)。

ガイダンス

評価者は、TOE を管理するための指示とどのインタフェースがサポートされるかが操作ガイダンスに含まれることを保証するため、操作ガイダンスをレビューしなければならない (shall)。

テスト

評価のためテストアクティビティの実行にあたって、評価者は、すべてのサポートされるインタフェースを利用しなければならない (shall) が、各インタフェースを用いて管理者アクションを含むようなそれぞれのテストを繰り返す必要はない。しかし評価者は、本 PP の要件に適合する TOE を管理しているサポートされた方法のそれぞれがテストされることを保証しなければならない(shall)；例えば、TOE がローカルなハードウェアインタフェースまたは TLS/HTTPS を介して管理可能な場合、両方の管理手法が、評価チームのテストアクティビティの間に検査されなければならない (must)。

5.3.4 TSF の保護 (FPT)

FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1 は、コンポーネント FPT_TUD_EXT.1.2 及び FPT_TUD_EXT.1.3 についても含むことに留意されたい。しかし、これらのコンポーネントにより記述される機能は、TSF または運用環境のいずれかによって実装可能である。これらのコンポーネントの定義については、セクション 5.4.4 を参照されたい。

FPT_TUD_EXT.1.1 MDM サーバは、MDM サーバソフトウェアの現在のバージョンを問い合わせる能力を許可された管理者へ提供しなければならない (shall)。

保証アクティビティ

ガイダンス

評価者は、管理者ガイダンスに TOE の現在のバージョンを決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)。

テスト

評価者は、AGD ガイダンスに従ってソフトウェアの現在のバージョンについて TSF に問い合わせなければならず(shall)、また現在のバージョンが文書化されインストールされたバージョンと合致することを検証しなければならない (shall)。

FPT_ITT.1　　内部 TOETSF データ転送

ST 作成者は、少なくとも FPT_ITT.1 または FTP_ITC.1(2)のひとつを ST に含めなければならない(must)。

TOE に MDM エージェントが含まれる場合、エージェントとサーバ間の通信チャネルは、TOE の内部となる。ST 作成者は、FPT_ITT.1 を含めなければならない(shall)。MAS サーバが物理的に MDM サーバと区別されている場合、MAS サーバは、分散型 TOE の別の一部としてみなされ、FPT_ITT.1 が MAS サーバと TSF データを転送するために資料されるすべてのチャネルに適用されなければならない(shall)。

TOE がモバイルデバイスへ組み込まれた評価される MDM エージェントと対話する場合、ST 作成者は、FTP_ITC.1(2)を含めなければならない(shall)。

5.3.5　高信頼パス／チャネル

ST 作成者は、少なくとも FPT_ITT.1 または FTP_ITC.1(2)のひとつを ST に含めなければならない(must)。

TOE がモバイルデバイスへ組み込まれた評価される MDM エージェントと対話する場合、ST 作成者は、FTP_ITC.1(2)を含めなければならない(shall)。MAS サーバが物理的に MDM サーバと区別されている場合、FPT_ITT.1 が ST に含まれなければならない(shall)。

TOE が MDM エージェントを含む場合、ST 作成者は、FPT_ITT.1 を含めなければならない(shall)。

5.4　TOE またはプラットフォームのセキュリティ機能要件

5.4.1　セキュリティ監査 (FAU)

FAU_GEN.1(1)　　監査データの生成

FAU_GEN.1.1(1)　[*選択：TSF、TOE プラットフォーム*] は、以下の監査対象事象を生成できなければなければならない(shall)：

a. **MDM サーバソフトウェア**の起動と終了；
b. すべての管理者アクション；
c. MDM サーバから MDM エージェントへ発行されるコマンド；
d. **表 1** で列挙された特別に定義された監査対象事象；
e. [*割付：その他の事象*]。

適用上の注釈：　*本要件は、MDM サーバソフトウェアまたは TOE プラットフォームの*

いずれかによって生成された監査記録に含まれるべき情報を概説する。これらの監査記録のそれぞれは、MDM サーバによって書かれてもよいし、または実行するオペレーティングシステムへディスパッチされてもよい。ST 作成者は、その他の監査対象事象を割付に含めることができる；それらは、提示されたリストに限定されない。すべての監査は、FAU_GEN.1.2 で述べられた情報を少なくとも含まなければならないが、割付可能なより多くの情報を含むことができる。

上記の項目 b は、監査可能であるべきすべての管理者アクションを要求しているので、これらのアクション監査可能性についての追加の仕様は、追加の記録内容を要求するようなものとは別に表 1 で規定される。管理者アクションは、FMT_MOF.1(1)によって規定される管理者機能を参照する。

項目 c には、トリガーまたは計画に基づいて自動的に実行されてもよいコマンドが含まれる。

ST 作成者によってセキュリティ機能要件、オプションの要件、選択ベースの要件、及びオブジェクティブ要件から選択された特定の要件によって、ST 作成者は、選択された要件について、ST の表 1からの適切な監査対象事象を含めるべきである(should)。

保証アクティビティ

TSS

評価者は TSS をチェックして、TSS に監査対象事象のすべてが列挙されていることを保証しなければならない(shall)。評価者は、本 PP によって必須とされたすべての監査事象種別が TSS に記述されていることを確認するため、チェックしなければならない(shall)。評価者は、TSS に記述されたすべての監査事象について、その記述がどこで監査事象が生成されるか(TSF、TOE プラットフォーム)を示していることを検証しなければならない(shall)。

ガイダンス

評価者は、管理者ガイダンスをチェックし、管理者ガイダンスがすべての監査対象事象を列挙していることを保証しなければならない(shall)。評価者は、本 PP によって必須とされたすべての監査事象種別が記述されていることを確認するためチェックしなければならない(shall)。

評価者は、また、管理セクションで列挙された管理者アクションを含め、本 PP に関連するような管理者アクションの決定を行わなければならない(shall)。評価者は、管理者ガイドを検査し、本 PP で規定された要件を実行するために必要な TOE で実証されたメカニズムの設定(有効化または無効化を含めて)に関連する管理者コマンドがどれかについての決定を行わなければならない(shall)。評価者は、管理者ガイドのどのアクションが本 PP に関してセキュリティ関連であるかを決定する間に取られる方法またはアプローチについて文書化しなければならない(shall)。評価者は、AGD_OPE ガイダンスが本要件を満たすことを保証することに関連するアクティビティの一部として本アクティビティを実行してもよい。

テスト

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ついての監査記録を TOE に生成させることによって、監査記録を正しく生成する TOE の能力をテストしなければならない(shall)。評価者は、ST に含まれる暗号プロトコルのそれぞれのチャネルの確立と終了について、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 でセキュリティ関連であるべき上記評価者によって決定されたそれぞれのアクションが監査可能であることをテストしなければならない(shall)。

ここでのテストが、セキュリティメカニズムのテストと直接に組み合わせて実行可能であることに留意されたい。例えば、提供された管理者ガイダンスが正しいことを保証するために実行されるテストは、AGD_OPE.1 が満たされることを検証し、また、監査記録を検証するために必要な管理者アクションの起動がきたされるとおりに生成されることに対処するべきである。

FAU_GEN.1.2(1) **[*選択：TSF、TOE プラットフォーム*]** は、各 TSF 監査記録内に少なくとも以下の情報を記録しなければならない (shall)：

- 事象の日付及び時刻、
- 事象の種別、
- サブジェクトの識別情報、
- (関連する場合) 事象の結果 (成功または失敗)、
- **表 1 の追加の情報**、
- [*割付：その他の監査関連情報*]。

適用上の注釈： *すべての監査には、少なくとも FAU_GEN.1.2 でもべられた情報が含まれなければならない(must)、しかし、割付可能であるような、より多くの情報を含める可能である。ST 作成者は、TSS において、監査記録のどの情報が、TSF によって実行されたものか、TOE プラットフォームによって実行されたものかを特定しなければならない (shall)。*

保証アクティビティ

TSS

評価者は TSS をチェックして、TSS が監査記録用のフォーマットを提供していることを保証しなければならない(shall)。それぞれの監査記録のフォーマットの種別は、各フィールドの簡潔な記述とともに、網羅されていなければならない (must)。

ガイダンス

評価者は、管理者ガイダンスをチェックして、TSS が監査記録用のフォーマットを提供していることを保証しなければならない(shall)。それぞれの監査記録のフォーマットの種別は、各フィールドの簡潔な記述とともに、網羅されていなければならない (must)。評価者は、フィールドの記述に FAU_GEN.1.2 で要求される情報が含まれていることを確認するためにチェックしなければならない(shall)。

テスト

FAU_GEN.1.1 からのテスト結果を検証するとき、評価者は、テスト中に生成された監査記録が管理者ガイドで規定されたフォーマットと合致すること、及び各監査記録のフィールドが適切なエントリーを持

っていることを保証しなければならない(shall)。

ここでのテストが、セキュリティメカニズムのテストと直接に組み合わせて実行可能であることに留意されたい。例えば、提供された管理者ガイダンスが正しいことを保証するために実行されるテストは、AGD_OPE.1 が満たされることを検証し、また、監査記録を検証するために必要な管理者アクションの起動がきたされるとおりに生成されることに対処するべきである。

監査対象事象の表には、オプション、選択ベース及びオブジェクティブ要件が含まれる。これらの要件の監査は、ST にその要件が含まれている場合にのみ要求される。

要件	**監査対象事象**	**追加の監査記録内容**
FAU_ALT_EXT.1	警告の種別。	警告を送信したモバイルデバイスの識別情報。
FAU_CRP_EXT.1	なし。	
FAU_GEN.1	なし。	
FAU_NET_EXT.1	なし。	
FAU_SAR.1	なし。	
FAU_SEL.1	監査収集機能が動作中に発生する監査設定へのすべての改変。	追加の情報なし。
FAU_STG_EXT.1	なし。	
FAU_STG_EXT.2	なし。	
FCS_CKM_EXT.4	なし。	
FCS_CKM.1	認証鍵用の鍵生成アクティビティの失敗。	追加の情報なし。
FCS_CKM.2	なし。	
FCS_COP.1(*)	なし。	
FCS_DTLS_EXT.1	証明書有効性チェックの失敗。	証明書の発行者名とサブジェクト名。
FCS_HTTPS_EXT.1	証明書有効性チェックの失敗。	証明書の発行者名とサブジェクト名。[*選択：利用者認証の決定、追加の情報なし*]。
FCS_IV_EXT.1	なし。	
FCS_RBG_EXT.1	ランダム化プロセスの失敗。	追加の情報なし。
FCS_STG_EXT.1	なし。	
FCS_STG_EXT.2	なし。	
FCS_TLSC_EXT.1	TLS セション確立の失敗。 提示された識別子の検証失敗。	失敗の理由。提示された識別子と参照識別子。
FCS_TLSS_EXT.1	TLS セション確立の失敗。	失敗の理由。

FIA_ENR_EXT.1	MD 利用者認証の失敗。	提示された利用者名。
FIA_UAU_EXT.4(*)	登録データの再利用の試行。	登録データ。
FIA_UAU.1	なし。	
FIA_X509_EXT.1	X.509 証明書の検証失敗。	失敗の理由。
FIA_X509_EXT.2	失効状態を決定するための接続の確立失敗。	追加の情報なし。
FIA_X509_EXT.3	証明書要求メッセージの生成。検証の成功または失敗。	証明書要求メッセージの内容。 追加された証明書の発行者とサブジェクト名または失敗の理由。
FIA_X509_EXT.4	証明書登録要求の生成。登録の成功または失敗。EST トラスト案が−データベースの更新。	EST サーバの発行者とサブジェクト名。認証の方法。 認証するために利用された証明書の発行者とサブジェクト名。 証明書要求メッセージの内容。 追加された証明書の発行者とサブジェクト名または失敗範湯。 追加されたルート CA のサブジェクト名。
FMT_MOF.1(1)	機能を実行するためのコマンドの発行。ポリシー設定の変更。	送信されたコマンドと MDM エージェント受信者の識別情報。 変更されたポリシーと達または完全なポリシー。
FMT_MOF.1(2)	利用者による登録。	利用者の識別情報。
FMT_MOF.1(3)	なし。	
FMT_MOF.1(4)	なし。	
FMT_POL_EXT.1	なし。	
FMT_SAE_EXT.1	認証データの期限切れ後に試行された登録。	利用者の識別情報。
FMT_SMF.1(1)	なし。	
FMT_SMF.1(2)	機能の成功または失敗。	追加の情報なし。
FMT_SMF.1(3)	なし。	
FMT_SMR.1(*)	なし。	
FPT_ITT.1(*)	高信頼チャネルの開始と終了。	高信頼チャネルプロトコル。開始者と受信者の識別情報。

FPT_TST_EXT.1	自己テストの開始。自己テストの失敗。検知された完全性違反。	失敗を引き起こしたアルゴリズム。完全性違反を引き起こした TSF コードファイル。
FPT_TUD_EXT.1	署名検証の成功または失敗。	追加の情報なし。
FTA_TAB.1	バナー設定の変更。	追加の情報なし。
FTP_ITC.1(*)	高信頼チャネルの開始と終了。	高信頼チャネルプロトコル。接続の非 TOE 端点。
FTP_TRP.1(1)	高信頼チャネルの開始と終了。	高信頼チャネルプロトコル。管理者の識別情報。
FTP_TRP.1(2)	高信頼チャネルの開始と終了。	高信頼チャネルプロトコル。

表 1：監査対象事象

FAU_STG_EXT.1(1) 外部監査証跡ストレージ

FAU_STG_EXT.1.1(1) [*選択：TSF、TOE プラットフォーム*] は、FTP_ITC.1(1)毎に高信頼チャネル及び[*選択：ローカルに格納される、その他の方法なし*]を用いて外部 IT エンティティへ監査データを送信できなければならない(shall)。

適用上の注釈： *TOE は、FTP_ITC.1(1)で規定されたとおりの高信頼チャネルを用いて外部IT エンティティへ監査データを送信できなければならない(shall)、またオプションで監査データをローカルに格納できる。「ローカルに格納される」が選択される場合、FAU_STG_EXT.2.1 が ST に含まれなければならない(shall)。*

TOE は、監査記録の格納とレビューのための非 TOE サーバに信頼を置いてもよい。TOE が監査記録を生成し、管理されるモバイルデバイスからの監査記録を受け取るが、これらの監査記録の格納とこれらの監査記録のレビューを管理者に許可する能力は、運用環境によって提供される。TSF は、本機能について基盤となるオペレーティングシステムに信頼を置くことができ、最初の選択は適切になされるべきである。

TOE が非 TOE 監査サーバに信頼を置き、高信頼チャネルが TLS を実装する場合、監査サーバは TOE の範囲外であるので相互認証は要求されない。

保証アクティビティ

TSS

評価者は TSS をチェックして、監査データが外部監査サーバへ転送される手段と、高信頼チャネルが提供される方法が記述されていることを保証しなければならない (shall)。

ガイダンス

評価者は、ローカル監査データと監査ログサーバへ送信される監査データとの間の関係が操作ガイダンスに記述されていることを決定するため、操作ガイダンスを検査しなければならない(shall)。例えば、監査事象が生成される際、それが外部サーバとローカルストアへ同時に送信されるのか、またはローカルストアがバッファとして用い

られ、監査サーバへデータを送信することによって定期的に「クリア」されるのか、といったことである。

評価者は、監査サーバのあらゆる要件（特定の監査サーバプロトコル、要求されるプロトコルバージョン等）の記述と同様に、また監査サーバと通信するために必要な TOE の設定と同様に、監査サーバへの高信頼チャネルを確立する方法が記述されていることを保証するため、操作ガイダンスについても検査しなければならない(shall)。

テスト

高信頼チャネルメカニズムのテストは、その特定の高信頼チャネルメカニズムの関連する保証アクティビティに特定されるように行われる。

評価者は、本要件に関して以下のテストを行わなければならない(shall)。

評価者は、提供された設定ガイダンスに従って TOE と監査サーバとの間のセションを確立しなければならない(shall) 。次に評価者は、監査サーバへ転送される監査データが生成されるようデザインされた評価者の選択による数回のアクティビティの間、監査サーバと TOE との間を通過するトラフィクを検査しなければならない(shall)。評価者は、これらのデータがこの転送の間平文で閲覧できないこと、そして監査サーバによる受信が成功することを観測しなければならない(shall)。評価者は、テスト中に監査サーバ上で用いられた特定のソフトウェア(名称、バージョン)を記録しなければならない(shall)。

5.4.2 暗号サポート (FCS)

FCS_CKM.1　暗号鍵生成

FCS_CKM.1.1　**[*選択：TSF、TOE プラットフォーム*]** は、以下の暗号鍵生成アルゴリズムに従って、**非対称**暗号鍵を生成しなければならない(shall) [*選択：*

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3** を満たす **2048 ビット以上**の暗号鍵長**を用いた RSA 方式；***
- *以下をみたす「**NIST 曲線**」**P-384 及び [選択：P-256、P-521、その他の曲線なし] を用いた ECC 方式： FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4；***
- *以下をみたす **2048 ビット以上**の暗号鍵長**を用いた FFC 方式：FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1***]。

適用上の注釈： *ST 作成者は、鍵確立と MDM 認証のために利用されるすべての鍵生成方式を選択しなければならない(shall)。鍵生成が鍵確立のために利用されるとき、FCS_CKM.2 の方式と選択された暗号プロトコルがその選択と合致しなければならない(must)。鍵生成が MDM 認証のために利用されるとき、公開鍵は、X.509v3 証明書と関連付けされることが期待される。*

TOE は RSA 鍵確立方式で受信者としてのみ動作する場合、TOE は、RSA 鍵生成を実装する必要はない。

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張される鍵確立に MDM サーバの ST における鍵確立要件が含ま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、MDM サーバの ST の TSS を検査して、 (サポートされるプラットフォームのそれぞれについて) 鍵確立機能が呼び出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) (これは MDM サーバによって実装されないメカニズムによって行われる可能性があることには注意すべきである(should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

TSS

評価者は、鍵長が TOE によってサポートされることを TSS が特定することを保証しなければならない(shall)。ST が複数の方式を規定する場合、評価者は、それぞれの方式についての用途を TSS が特定していることを検証するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、本 PP で定義されたすべての用途について、選択された生成方式と鍵長を利用するために TOE を設定する方法について、管理者に AGD ガイダンスが指示することを検証しなければならない(shall)。

テスト

FIPS PUB 186-4 RSA 方式についての鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない(shall)。このテストは、公開鍵検証指数 e、秘密素因数 p 及び q、公開される法(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：
    a. 証明可能素数
    b. 確率的素数
2. 条件付き素数：
    a. 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)
    b. 素数 p1、p2、q1 及び q2 を証明可能素数とし(shall)、p 及び q を確率的素数としなければならない(shall)
    c. 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値として TSF 鍵生成ルーチンに与えなければならない(must)。これには、1 つまたは複数の乱数シード値、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない(shall)。評価者は、TSF によって生成された値を既知の良好な実装から生成された値と比較することによって、TSF の実装の正しさを検証しなければならない(shall)。

可能な場合、ランダム確率的素数は、上記のとおり既知の良好な実装に対しても検証されるべきである(should)。さもなければ、評価者は、それぞれのサポートされる鍵長 nlen について 10 個の鍵ペアを TSF に生成させ、検証しなければならない(shall) :

• n = p*q,

• p と q は、ミラー・ラビンテストに従う確立的素数である、

• GCD(p-1,e) = 1,

• GCD(q-1,e) = 1,

• 2^16 <= e <= 2^256 及び e は、奇の整数である、

• |p-q| > 2^(nlen/2 - 100),

• p >= squareroot(2)*(2^(nlen/2 -1)),

• q >= squareroot(2)*(2^(nlen/2 -1)),

• 2^(nlen/2) < d < LCM(p-1,q-1),

• e*d = 1 mod LCM(p-1,q-1).

楕円曲線暗号(ECC)のための鍵生成

FIPS 186-4 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 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)。

有限体暗号 (FFC) のための鍵生成

評価者は、パラメタ生成及び鍵生成テストを用いて TOE による FFC のためのパラメタ生成及び鍵生成の実装を検証しなければならない(shall)。このテストは、フィールド素数 p、暗号素数 q (p-1 を割り切る)、

暗号群生成元 g、ならびにプライベート鍵 x 及び公開鍵 y の計算の値を正しく求める TSF の能力を検証する。

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

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 とおりの方法を規定する：

暗号群生成元：

• 検証可能プロセスによって構築された生成元 g

• 検証不可能プロセスによって構築された生成元 g

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

プライベート鍵：

• RBG の len(q) ビットの出力、ここで 1 <=x <= q-1

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

RBG のセキュリティ強度は、少なくとも FFC パラメタセットによって提供されるセキュリティの強度と同じでなければならない (must)。

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

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

• g != 0,1

• q が p-1 を割り切ること

• g^q mod p = 1

• g^x mod p = y

FCS_CKM.2 **暗号鍵確立**

FCS_CKM.2.1 [*選択：TSF、TOE プラットフォーム*] は、以下の規定された暗号鍵**確立**方法に従って、暗号**鍵確立**を**実行し**なければならない(shall) : [*選択：*

- *以下を満たす **RSA ベースの鍵確立方式**： **NIST Special Publication 800-56B, 「Recommendation for Pair-Wise Key***

Establishment Schemes Using Integer Factorization Cryptography」；

- *以下を満たす**楕円曲線ベースの鍵確立方式：** **NIST Special Publication 800-56A, 「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」；***
- *以下を満たす**有限体ベースの鍵確立方式：** **NIST Special Publication 800-56A, 「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」***]。

適用上の注釈： *ST 作成者は、選択された暗号プロトコルのために利用されるすべての鍵確立方式を選択しなければならない(shall)。RSA ベースの鍵確立方式は、NIST SP 800-56B のセクション 9 に記述されている；しかし、*

セクション 9 は、SP 800-5B のその他のセクションの実装に信頼を置いている。TOE が RSA 鍵確立方式において受信者として動作するバイ、TOE は、RSA 鍵生成を実装する必要はない。

鍵確立方式のために利用される楕円曲線は、FCS_CKM.1.1 で規定される曲線と相関しなければならない(shall)。

有限体ベースの鍵確立方式のために利用されるドメインパラメタは、FCS_CKM.1.1 に従って鍵生成により規定される。

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたそれぞれのプラットフォームについて、評価者は、そのプラットフォームの ST において主張された鍵確立が MDM サーバの ST における鍵確立要件を含むことを保証するため、そのプラットフォームの ST を検査しなければならない(shall)。評価者は、鍵確立機能が起動される方法(これには、MDM サーバによって実装されないようなメカニズムを通して行われてもよいことに留意するべきである；それにもかかわらず、メカニズムは、本保証アクティビティの一部として TSS において特定されること)について TSS に記述されていること(それぞれのサポートされるプラットフォームについて)を検証するため、MDM サーバの ST の TSS についても検査しなければならない(shall)。

TOE によって満たされる要件

TSS

評価者は、サポートされた鍵確立方式が FCS_CKM.1.1 で特定された鍵生成方式に対応していることを保証しなければならない(shall)。ST が複数の方式を規定する場合、評価者は、それぞれの方式についての用途が TSS に特定されていることを検証するため、TSS を検査しなければならない(shall)。

評価者は、TOE が復号エラーを取り扱う方法について TSS に記述されていることを保証しなければならない(shall)。NIST Special Publication 800-56B に従って、TOE は、任意の出力されるまたはログ出力されるエラーメッセージの内容を通して、または時間的変化を通して、発生した特定のエラーを明らかにしてはならない(must

not)。KTS-OAEP がサポートされる場合、評価者は、NIST Special Publication 800-56B セクション 7.2.2.3 に記述された 3 つの復号エラーチェックのそれぞれにトリガーをかけるような別々に考案された暗号文の値を作成しなければならない(shall)、それぞれの復号試行がエラーを引き起こすことを保証し、任意の出力されたまたはログ出力されたエラーメッセージがそれぞれ同一であることを保証しなければならない(shall)。KTS-KEM-KWS がサポートされる場合、評価者は、NIST Special Publication 800-56B セクション 7.2.3.3 に記述された 3 つの復号エラーチェックのそれぞれにトリガーをかけるような別々に考案された暗号文の値を作成しなければならない(shall)、それぞれの復号試行がエラーを引き起こすことを保証し、任意の出力されたまたはログ出力されたエラーメッセージがそれぞれ同一であることを保証しなければならない(shall)。

ガイダンス

評価者は、選択された鍵確立方式を利用するために TOE を設定する方法を AGD ガイダンスが管理者に指示していることを検証しなければならない(shall)。

テスト

評価者は、適用可能な以下のテストを用いて TOE によってサポートされた鍵確立方式の実装を検証しなければならない(shall)。

SP800-56A 鍵確立方式

評価者は、以下の機能テストと有効性テストを用いて SP800-56A 鍵共有方式の TOE の実装を検証しなければならない(shall)。それぞれの鍵共有方式についてのこれらの検証テストは、TOE が推奨事項の仕様に従って鍵共有方式の内容を実装していることを検証する。これらのコンポーネントには、プリミティブ (共有秘密の値 Z) の計算及び鍵導出関数 (KDF) を介して導出された鍵材料 (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、以下に記述された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たことについても検証されなければならない(shall)。これには、DKM の改正、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、鍵共有方式を正しく実装するための TOE の能力について検証する。本テストを実行するために、評価者は、TOE がサポートする方式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)。それぞれのサポートされる鍵共有方式－鍵共有役割の組み合わせ、KDF 種別、及びサポートされる場合、鍵確認役割－鍵確認種別の組み合わせについて、テスト者は、10 セットのテストベクタを生成しなければならない(shall)。データセットは、1 セットのドメインパラメタ値(FFC)または 10 セットの公開鍵毎に NIST 承認済み曲線からなる。これらの鍵は、テストされている方式によって、静的、一時的または両方である。

評価者は、DKM、対応する TOE の公開鍵(静的及び／または一時的)、MAC タグ、及びその他の情報フィールド OI 及び TOEid フィールドのような、KDF で利用される任意の入力について取得しなければならない(shall)。

TOE が SP 800-56A で定義される 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された値のみを取得しなければならない(shall)。

評価者は、共有秘密を計算し、鍵材料 DKM を導出し、これらの値から生成されるハッシュまたは MAC タグを比較するため、既知の良好な実装を用いて所与の方式の TSF の実装の正確性を検証しなければならない(shall)。

鍵確認がサポートされる場合、TSF は、それぞれの実装された承認された MAC アルゴリズムについて上記を実行しなければならない(shall)。

有効性テスト

有効性テストは、鍵確認を用いたまたは用いないような、別の団体の有効な及び無効な鍵共有結果を確認するための TOE の能力を検証する。本テストを実行するため、評価者は、TOE が確認可能であるべきエラーを決定するために SP800-56A 鍵共有実装に含まれるサポートしている暗号機能のリストを取得しなければならない。評価者は、ドメインパラメタ値または NIST 承認済み曲線、評価者の公開鍵、TOE の公開・プライベート鍵ペア、MAC タグ、及びその他の情報と TOEid フィールドのような、KDF で利用される任意の入力を含むデータセットからなる一連の 24(FFC)または 20(ECC)個のテストベクタを生成する。

評価者は、TOE が無効な鍵共有結果が以下の不正なフィールドによって引き起こされることをテストするためのテストベクタのいくつかにエラーを注入しなければならない(shall)。TOE が完全なまたは部分的な(ECC のみ)公開鍵検証を含む場合、評価者は、TOE が公開鍵検証機能及び／または部分的鍵検証機能(ECC のみ)においてエラーを検知することを確認するため、両方の者の公開鍵、両方の者の一時的公開鍵及び TOE の静的プライベート鍵にエラーを個別に注入すること。少なくとも 2 つのテストベクタが寒辺されずに残らなければならない(shall)、ゆえに有効な鍵共有結果をもたらすべきである(それらは合格するべきである)。

TOE は、対応するパレメタを用いて鍵共有方式をエミュレートするため、これらの改変されたテストベクタを利用しなければならない(shall)。評価者は、TOE の結果をこれらのエラーを検知することを検証するような既知の良好な実装を用いた結果と比較しなければならない(shall)。

SP800-56B 鍵確立方式

評価者は、TSS に TOE が送信側、受信側、または両方として RSA ベース鍵確立方式について動作するかどうか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)。

TOE が送信側として動作する場合、RSA ベース鍵確立方式のすべての TOE がサポートする組み合わせの適切な動作を保証するため、以下の保証アクティビティが実行されなければならない(shall)。

本テストを実行するため、評価者は、TOE がサポートする方式のテストベクタを既知の良好な実装から生成または取得しなければならない(shall)。サポートされる鍵確立方式とそのオプション(サポート

される場合、鍵確認を用いてまたは用いないで、それぞれのサポートされる確認 MAC 関数については鍵確認がサポートされる場合、またそれぞれのサポートされるマスク生成関数については KTS-OAEP がサポートされる場合) のそれぞれの組み合わせについて、テスト者は、10 セットのテストベクタを生成しなければならない(shall)。それぞれのテストベクタには、RSA 公開鍵、平文の鍵材料、適用可能な場合には任意の追加入力パラメタ、鍵確認が含まれる場合には MacKey と MacTag、及び出力された暗号文が含まれなければならない(shall)、それぞれのテストベクタについて、評価者は、通常の操作で利用されるランダムに生成された MacKey の代わりに鍵確立暗号化操作を同じ入力を用いて TOE 上で実行しなければならず(鍵確認が含まれる場合、テストは、テストベクタからの MacKey を利用しなければならない(shall))、出力された暗号文がテストベクタにおける暗号文と同じであることを保証しなければならない(shall)。

TOE が受信側として動作する場合、すべての TOE がサポートする RSA ベースの鍵確立方式の組み合わせの適切な動作を保証するため、以下の保証アクティビティが実行されなければならない(shall) :

本テストを実行するため、評価者は、TOE のサポートする方式のテストベクタを既知の良好な実装から生成または取得しなければならない(shall)。サポートされる鍵確立方式とそのオプション(サポートされる場合、鍵確認を用いてまたは用いないで、それぞれのサポートされる確認 MAC 関数については鍵確認がサポートされる場合、またそれぞれのサポートされるマスク生成関数については KTS-OAEP がサポートされる場合) のそれぞれの組み合わせについて、テスト者は、10 セットのテストベクタを生成しなければならない(shall)。それぞれのテストベクタには、RSA 公開鍵、平文の鍵材料(KeyData)、適用可能な場合には任意の追加入力パラメタ、鍵確認が含まれる場合には MacTag、及び出力された暗号文が含まれなければならない(shall)。それぞれのテストベクタについて、評価者は、鍵確立復号操作を TOE 上で実行しなければならず、出力された平文鍵材料(KeyData)がテストベクタにおける平文鍵材料と同じであることを保証しなければならない(shall)。鍵確認が含まれる場合、評価者は鍵確認ステップを実行しなければならない(shall)、そして出力された MacTag がテストベクタにおける MacTag と同じであることを保証しなければならない(shall)。

FCS_CKM_EXT.4 暗号鍵の破棄

FCS_CKM_EXT.4.1 [*選択 : TSF、TOE プラットフォーム*] は、以下の規則に従って平文の鍵材料とクリティカルセキュリティパラメタを破壊しなければならない(shall) :

- 揮発性メモリについて、破壊は、[*選択 : TSF の RBG を用いた疑似ランダムパタンからなる、すべてゼロからなる*]1 回の直接上書きによって実行されなければならない(shall)。
- 不揮発性 EEPROM について、破壊は、TSF の RBG (FCS_RBG_EXT.1 で規定されるとおり)を用いた疑似ランダムパタンからなる 1 回の直接上書き、その後の読み出し検証によって実行されなければならない(shall)。

- 不揮発性フラッシュメモリで、ウェアレベリングされたものについて、破壊は、[*選択：すべてゼロからなる 1 回の直接上書きとその後の読み出し検証によって、そのデータ自体と同様なデータをかくのうするメモリへの参照情報を消去するようなブロック消去によって*] 実行されなければならない(shall)。
- 不揮発性フラッシュメモリで、ウェアレベリングされたものについて、破壊は、[*選択：すべてゼロからなる 1 回の直接上書きによって、ブロック消去によって*] 実行されなければならない(shall)。
- EEPROM 及びフラッシュ以外の不揮発性メモリについて、破壊は、毎回書き込みの前に変更されるようなランダムパタンを用いた 1 回に直接上書きによって実行しなければならない(shall)。

適用上の注釈： *MDM サーバが平文の秘密鍵、プライベート暗号鍵、及び CSP を用いた一切の操作を実行しない場合、ST 作成者はそのプラットフォームを選択すべきである (should)。*

任意のセキュリティ関連情報 (鍵や認証データ、及びパスワード等) は、セキュリティ上重要なデータの開示または改変を防止するため、もはや使われなくなった際にはゼロ化されなければならない (must)。

上述のゼロ化は、平文鍵及び暗号サービスプロバイダ (CSP) のすべての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／CSP が別の場所へ転送された際、適用される。

TOE にはホスト IT 環境が含まれないため、必然的にこの機能の範囲はいくぶん限定される。本要件の目的においては、TOE がホストの正しい基盤となる機能を呼び出してゼロ化を行えば十分である。データがゼロ化されることを確実にするため TOE にカーネルモードメモリドライバが含まれなければならない (has to) ことは意味しない。ホストプラットフォームが、その内部プロセス中で鍵材料のゼロ化を適切に行うことが前提とされる。

FCS_CKM_EXT.4.2 TSF は、すべての平文の鍵材料とクリティカルセキュリティパラメタ(CSP)をもはや不要となったときに破壊しなければならない(shall)。

適用上の注釈： *鍵破壊手順は、FCS_CKM_EXT.4.1 に従って実行される。TOE プラットフォームが FCS_CKM.4.1 で選択されたとしても、TSF は、平文の鍵材料と CSP がもはや不要となったときを決定しなければならず (shall)、したがって破壊されるべきである(should)。TSF は、TSF または TOE プラットフォームがその鍵材料と CSP を破壊したかどうかに関わらず、鍵材料と CSP をもはや不要となった時に「解放」しなければならない(shall)。*

本要件の目的のため、平文の鍵材料は、認証データ、許可データ、秘密／プライベート対称鍵、鍵を導出するために利用されるデータ等を指している。

保証アクティビティ

保証アクティビティの注釈：

使用される保証アクティビティは、FCS_CKM_EXT.4.1 でなされた選択に依存している。

TSS

評価者は、TSS にそれぞれの種別の平文の鍵材料と CSP 及びその起源と格納場所を列挙していることを保証するため、チェックしなければならない(shall)。

評価者は、いつそれぞれのタイプの鍵材料と CSｐがもはや不要となるかについて、TSS に記述されていることを検証しなければならない(shall)。

プラットフォームにって満たされる要件

TSS

ST に列挙されたそれぞれのプラットフォームについて、評価者は、上記の列挙された鍵を生成するために使用された秘密鍵、プライベート鍵、及び CSP のそれぞれが網羅されていることを保証するため、そのプラットフォームの ST の TSS を検査しなければならない(shall)。

TOE によって満たされる要件

TSS

評価者は、それぞれの種別について、実行される消去手順の種別が列挙されていることについても検証しなければならない(shall)。異なる種別のメモリが保護されるべき材料を格納するために使用される場合、評価者は、データが格納されるメモリについての消去手順について(例えば、「フラッシュ上に格納される秘密鍵は、ゼロによつ 1 回の上書きによって消去される、一方、内部永続的ストレージデバイス上に格納される秘密鍵は毎回書込みの前に変更されるランダムパタンを用いて 1 回上書きによって消去される」) TSS に記述されていることを保証するためにチェックしなければならない(shall)。ブロック消去について、評価者は、使用されるブロック消去コマンドが列挙されていることも保証しなければならない(shall)、またその使用されるコマンドがフラッシュメモリの利用を最適化するために作成されるかもしれない平文の鍵材料のあらゆる複製についても対処することを検証しなければならない(shall)。

テスト

それぞれのソフトウェアおよびファームウェアの鍵消去状況について、評価者は、以下のテスト繰り返さなければならない(shall)。このときハードウェアに結合された鍵はテストから明示的に除外されることに留意されたい。

テスト 1 : 評価者は、特化した運用環境と TOE 及びその鍵を用いた通常の暗号処理の間に TOE によって内部的に生成されるかもしれない鍵のすべての中間的な複製を含めて、鍵が正しく消去されることをテストするために整えられた TOE のビルドのための開発ツール(デバッガ、シミュレータ、等)の適切な組み合わせを活用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)。

FCS_COP.1(1) 暗号操作 (暗号化及び復号)

FCS_COP.1.1(1) **[*選択 : TSF、TOE プラットフォーム*]** は、以下の規定された暗号アルゴリズム： [***選択 :***

- ***AES-CBC (NIST SP 800-38A で定義される)モード、***
- ***AES-GCM (NIST SP 800-38D で定義される)、***
- ***AES 鍵ラッピング (KW) (NIST SP 800-38F で定義される)、***
- ***AES パディング付き鍵ラッピング (KWP) (NIST SP 800-38F で定義される)、***
- ***AES-CCM (NIST SP 800-38C で定義される)*** **]、**

及び暗号鍵長 **[*選択 : 128 ビット、256 ビット*]** に従って***暗号化／復号***を実行しなければならない(shall)。

適用上の注釈 : *FCS_COP.1.1(1) の最初の選択について、ST 作成者は、高信頼チャネルプロトコルで AES が動作するモードを選択するべきである(should)。2 番目の選択について、ST 作成者は、本機能によってサポートされる鍵長を選択するべきである(should)。*

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたプラットフォームのそれぞれについて、評価者はプ

ラットフォームの ST を検査して、そのプラットフォームの ST に主張される 1 つまたは複数の暗号化／復号機能に MDM サーバの ST における 1 つまたは複数の暗号化／復号機能が含ま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、MDM サーバの ST の TSS を検査して、 (サポートされるプラットフォームのそれぞれについて) 暗号化／復号機能が呼び出される方法が、MDM サーバの ST 中に選択されたモードと鍵長ごとに記述されていることを検証しなければならない (shall) (これは MDM サーバによって実装されないメカニズムによって行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

テスト

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 (shall)、第 2 のセットは 256 個の 256 ビットの鍵／暗号文のペアからなるものとする (shall)。[1,N]の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 とする (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 ビットの鍵を用いるなければならない (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-GCM テスト

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

- 128 ビット及び 256 ビットの鍵
- 2 とおりの平文の長さ。平文の長さの一方は、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)。他方の平文の長さは、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 とおりの AAD の長さ。1 つの AAD の長さは 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 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)。1 つの AAD 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)。
- 2 とおりの IV の長さ。96 ビットの IV がサポートされる場合、テストされる 2 とおりの IV の長さの一方を 96 ビットとしなければならない (shall)。

評価者は、上記のパラメタ長の組み合わせのそれぞれについて、10 個の鍵、平文、AAD、及び IV の組のセットを用いて暗号化機能をテストし、AES-GCM 認証付き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の長さはそれぞれ、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／不合格結果を取得して、合格の場合には平文を復号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)。

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 とおりのペイロードの長さ。片方のペイロードの長さは、ゼロバイト以上でサポートされる最も短いペイロードの長さとしなければならない (shall)。他方のペイロードの長さは、32 バイト (256 ビット) 以下でサポートされる最も長いペイロードの長さとしなければならない (shall)。
- 2 または 3 通りの関連付けられたデータの長さ。1 つの関連付けられたデータの長さは 0 としなければならない (shall) (サポートされる場合)。1 つの関連付けられたデータの長さは、ゼロバイト以上でサポートされる最も短い関連付けられたデータの長さとしなければならない (shall)。1 つの関連付けられたデータの長さは、32 バイト (256 ビット) 以下でサポートされる最も長い関連付けられたデータの長さとしなければならない (shall)。実装が 2^{16} バイトの関連付けられたデータの長さをサポートする場合、2^{16} バイトの関連付けられたデータの長さがテストされなければならない (shall)。
- ノンスの長さ。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の長さがテストされなければならない (shall)。
- タグの長さ。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の長さ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付けられたデータの長さのそれぞれについて、またサポートされるペイロード、ノンス、及びタグの長さ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 2。サポートされる鍵及びペイロードの長さのそれぞれについて、またサポートされる関連付けられたデータ、ノンス、及びタグの長さ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の長さのそれぞれについて、またサポートされる関連付けられたデータ、ペイロード、及びタグの長さのいずれかについて、評価者は 1 つの鍵の値及び 10 個の関連付けられたデータ、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の長さのそれぞれについて、またサポートされる関連付けられたデータ、ペイロード、及びノンスの長さ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)。

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付けられたデータの長さ、ペイロードの長さ、ノンスの長さ、及びタグの長さ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、関連付けられた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)。

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

評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、AES-KW の認証付き暗号化機能をテスト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
- 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) とする (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)。3 番目のデータユニットの長さは、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 認証付き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 認証付き暗号化機能を利用しなければならない (shall)。

評価者は、認証付き暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、AES-KW 認証付き暗号化を AES-KW 認証付き復

号と置き換えて、AES-KW の認証付き復号機能をテストしなければならない (shall)。

評価者は、AES-KW の認証付き暗号化と同一のテストを用い、以下の変更を 3 通りの平文の長さに行って、AES-KWP 認証付き暗号化機能をストしなければならない (shall)。

- 1 つの平文の長さは 1 オクテットとする (shall)。1 つの平文の長さは 20 オクテット (160 ビット) としなければならない (shall)。
- 1 つの平文の長さは、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 認証付き暗号化を AES-KWP 認証付き復号と置き換えて、AES-KWP の認証付き復号機能をテストしなければならない (shall)。

FCS_COP.1(2) **暗号操作 (ハッシュ)**

FCS_COP.1.1(2) **[*選択：TSF、TOE プラットフォーム*]** は、以下：[*FIPS Pub 180-4*]を満たす、規定された暗号アルゴリズム **[*選択：SHA-256、SHA-384、SHA-512*]** と**メッセージダイジェスト**長 **[*選択：256、384、512*] ビット**に従って**暗号ハッシュ**を実行しなければならない(shall)。

適用上の注釈： *本要件の意図は、高信頼アップデート及び高信頼チャネルと関連したディジタル署名生成及び検証に用いられるハッシュ機能を特定することである。ハッシュの選択は、メッセージダイジェスト長の選択をサポートしなければならない(must)。ハッシュの選択は、使用されるアルゴリズムの全体的な強度と一貫しているべきである(should)(例えば、128 ビット鍵については SHA-256)。*

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張される 1 つまたは複数のハッシュ機能に MDM サーバの ST における 1 つまたは複数のハッシュ機能が含ま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、MDM サーバの ST の TSS を検査して、 (サポートされるプラットフォームのそれぞれについて) ハッシュ機能が呼び出される方法が、MDM サーバの ST 中に選択されたダイジェスト長ごとに記述されていることを検証しなければならない (shall) (これは MDM サーバによって実装されないメカニズムによって行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

TSS

評価者は、その他の TSF 暗号機能(例えば、ディジタル署名検証機能)とのハッシュ関数の連携が 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)。評価者は、要求されるハッシュ長についての機能をせっていするために行われるために要求される設定が存在することを決定するために AGD 文書をチェックする。その TSF ハッシュ関数は、2 つのモードの 1 つで実装できる。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。

テスト

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

選択されたロングメッセージテスト—バイト指向モード

評価者は m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 8*99*i となる (ここで $1 \le i \le m/8$)。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。

FCS_COP.1(3) 暗号操作 (ディジタル署名)

FCS_COP.1.1(3) **[*選択：TSF、TOE プラットフォーム*]** は、以下に規定された暗号アルゴリズム **[*選択：_*]**

- ***2048 ビット以上の鍵長を用いる RSA 方式で以下を満たすもの：FIPS PUB 186-2 または FIPS PUB 186-4, "Digital Signature Standard(DSS)"、Section 4；***
- ***「NIST 曲線」P-384 及び [選択：P-256、P-521、その他の曲線なし] を用いる ECDSA 方式で、以下を満たすもの：FIPS PUB 186-4, "Digital Signature Standard(DSS)"、Section 5*]**

に従って**暗号署名サービス(生成と検証)**を実行しなければならない (shall)。

適用上の注釈： *ST 作成者は、ディジタル署名を実行するために実装されたアルゴリズム選択するべきである(should)。MDM サーバは、高信頼チャネルプロトコルに従ってディジタル署名を実行しなければならない(shall)。MDM サーバは、任意の署名されたポリシーと MDM サーバによって送信されたポリシーを検証することが要求される。*

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張されるディジタル署名機能に MDM サーバの ST におけるディジタル署名機能が含ま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、MDM サーバの ST の TSS を検査して、(サポートされるプラットフォームのそれぞれについて) ディジタル署名機能が呼び出される方法が、MDM サーバ中に用いられる操作ごとに記述されていることを検証しなければならない (shall) (これは MDM サーバによって実装されないメカニズムによって行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

テスト

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)。

ECDSAFIPS 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 のサポートするモジュラス長／SHA の組み合わせのそれぞれについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない (must)。評価者は、TOE に自分のプライベート鍵と法の値を用いてこれらのメッセージへ署名させなければならない (shall)。

評価者は、既知の良好な実装及び関連付けられた公開鍵を用いて署名を検証することによって、TSF の署名の正しさを検証しなければならない (shall)。

署名検証テスト

評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない (shall)。評価者は、公開鍵 e、メッセージ、IR フォーマット、または署名、あるいはこれらのうち 2 つ以上にエラーを導入することによって、署名検証テスト中に作成されたテストベクトル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トルを利用して、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)。

FCS_COP.1(4)　暗号操作 (鍵付きハッシュによるメッセージ認証)

FCS_COP.1.1(4)　**[*選択：TSF、TOE プラットフォーム*]** は、以下を満たす規定された暗

号**アルゴリズム HMAC-[*選択：SHA-256*、*SHA-384*、*SHA-512*]**、鍵長 [*割付：HMAC で利用される (ビット単位の) 鍵長*]、**及びメッセージダイジェスト長 [*選択：256*、*384*、*512*]** ビットに従って**鍵付きハッシュによるメッセージ認証を実行し**なければならない(shall) : **[FIPS PUB 198-1, 「*The Keyed-Hash Message Authentication Code*」、及び FIPS PUB 180-4, 「*Secure Hash Standard*」]**。

適用上の注釈： *本要件の意図は、TOE によって用いられるさまざまな暗号プロトコル (例、高信頼チャネル) の鍵確立の目的で用いられるときに用いられる鍵付きハッシュによるメッセージ認証機能を規定することである。ハッシュの選択は、メッセージダイジェスト長の選択をサポートしなければならない(must)。ハッシュの選択は、FCS_COP.1(3) のために用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。*

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたプラットフォームのそれぞれについて、評価者はプラットフォームの ST を検査して、そのプラットフォームの ST に主張される 1 つまたは複数の鍵付きハッシュ機能に MDM サーバの ST における 1 つまたは複数の鍵付きハッシュ機能が含ま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、MDM サーバの ST の TSS を検査して、 (サポートされるプラットフォームのそれぞれについて) 鍵付きハッシュ機能が呼び出される方法が、MDM サーバの ST 中に選択されたモードと鍵長ごとに記述されていることを検証しなければならない (shall) (これは MDM サーバによって実装されないメカニズムによって行われる可能性があることには注意すべきである (should) が、その場合にもそのメカニズムはこの保証アクティビティの一部として TSS に特定されることになる)。

TOE によって満たされる要件

TSS

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、ブロック長、そして用いられる出力 MAC 長。 (訳注：以下の文は、テストの内容と重複するため、取り消し線で削除した) ~~テスト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設定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)。~~

テスト

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設定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)。

FCS_RBG_EXT.1　拡張：乱数ビット生成

FCS_RBG_EXT.1.1　[*選択：TSF、TOE プラットフォーム*] は、[*選択：Hash_DRBG (任意)* 、*HMAC_DRBG (任意)* 、*CTR_DRBG (AES)*] を用いる *NIST Special Publication 800-90A* に従って、すべての決定論的乱数ビット生成サービスを実行しなければならない (shall) 。

適用上の注釈：　*ST 作成者は、そのサーバがそれ自身の DRBG またはプラットフォームの DRBG を提供するか選択すべきである (should)。SP 800-90A には、3 つの異なる乱数生成手法が含まれる；これらはそれぞれ、順番に、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、要件または TSS で用いられる具体的な基盤となる暗号プリミティブを取り込むこと。特定されたハッシュ関数 (SHA-224, SHA-256, SHA-384, SHA-512) のいずれもが Hash_DRBG または HMAC_DRBG 用に許可されるが、CTR_DRBG 用には AES ベースの実装のみが許可される。*

保証アクティビティ

プラットフォームによって満たされる要件

TSS

ST に列挙されたプラットフォームのそれぞれについて、評価者は、そのプラットフォームの ST で主張された RBG 機能に MDM サーバの ST の RBG 機能が含まれていることを保証するため、プラットフォームの ST を検査しなければならない(shall)。評価者は、(サポートされるプラットフォームのそれぞれについて) RBG 機能が呼び出される方法が、MDM サーバにおいて利用されるそれぞれの操作について記述されていることを検証するため、MDM サーバの ST の TSS についても検査しなければならない(shall) (これは MDM サーバによって実装されないメカニズムを介して行われるかもしれないこと；それにもかかわらず、そのメカニズムが本保証アクティビティの一部として TSS で特定されることは留意されるべきである)。

TOE によって満たされる要件

テスト

評価者は、以下のテストを実行しなければならない(shall)。

評価者は、RNG 実装の 15 回の試行を行わなければならない (shall)。RNG が設定可能な場合、評価者は各構成について 15 回の試行を行わなければならない (shall)。また評価者は、RNG 機能を設定するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない (shall)。

RBG が有効な予測耐性を持つ場合、それぞれの試行は、(1) DRBG をインスタンス化、 (2) 乱数ビットの最初のブロックを生成、 (3) 乱数ビットの 2 番目のブロックを生成、 (4) 非インスタンス化、という手順からなる。評価者は、乱数ビットの 2 番目のブロックが予測された

値であることを検証する。評価者は、それぞれの試行に 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 Personlization 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 1 つのブロックを生成」とは、返されるビット数が (NIST SP 800-90A で定義される) 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。

RBG が予測耐性を持たない場合、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 PersonalizationString 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 (df) 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 : Additional Input のビット長は、Personalization String の長さと同一のデフォルトと制約を持つ。

FCS_RBG_EXT.1.2 決定論的 RBG は、[*選択：ソフトウェアベースノイズ源、プラットフォームベースの RBG 、ハードウェアベースノイズ源、その他のノイズ源なし*] で、鍵とそれが生成するハッシュの最大セキュリティ強度 (NIST SP 800-57 にしたがって)と少なくとも等しいような、最小で[*選択：128 ビット、256 ビット*] のエントロピーを持っているもの、からエントロピーを蓄積するエントロピー源によってシード値を供給されなければならない (shall)。

適用上の注釈： *本要件の最初の選択について、ST 作成者は、任意の追加のノイズ源がアプリケーションの DRBG への入力として利用される場合、「ソフ*

トウェアベースノイズ源」を選択する。そのアプリケーションはプラットフォームの DRBG をその DRBG へシード値を供給するために用いなければならない(must)ことに留意されたい。

本要件の 2 番目の選択について、ST 作成者は、ST に含まれるアルゴリズムの最大のセキュリティ強度に対応する適切なエントロピー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 で定義されている。例えば、実装に 2048 ビット RSA(セキュリティ強度 112 ビット)、AES128(セキュリティ強度 128 ビット)及び HMAC-AHS-256(セキュリティ強度 256 ビット)を含む場合、ST 作成者は、256 ビットを選択すること。

保証アクティビティ

証拠資料が作成されなければならない(shall)—そして、評価者は、そのアクティビティを実行しなければならない(shall)—附属書 D：エントロピー証拠資料と評定及び「エントロピー証拠資料と評定の附属書」に従って。

将来的には、具体的な統計学的なテスト(NIST SP 800-90B にあるような)がエントロピー見積を検証するために要求されるだろう。

FCS_STG_EXT.1 暗号化された暗号鍵ストレージ (MDM サーバ)

FCS_STG_EXT.1.1 [*選択：TSF、TOE プラットフォーム*] は、 すべての永続的な秘密とプライベート鍵のために、[*選択：プラットフォームが提供する鍵ストレージ、FCS_STG_EXT.2 で規定される暗号化*]を利用しなければならない(shall)。

適用上の注釈： *本要件は、永続的秘密(クレデンシャル、秘密鍵)及びプライベート鍵が利用されないときにセキュアに格納されることを保証する。何らかの秘密／鍵が TOE によって取り扱われ、その他のものがプラットフォームによって取り扱われる場合、選択の両方が ST 作成者によって規定可能で、ST 作成者は TOE によって取り扱われるそれらの鍵とプラットフォームによるものについて TSS で特定しなければならない(shall)。*

TSF がアプリケーションであい、専用サーバでない場合、それはプラットフォーム提供の鍵ストレージにそのプライベート鍵を格納するべきである(should)。

ST 作成者は、鍵が格納されるやり方の選択と上記選択で格納される場所に責任を持つ。

保証アクティビティ

TSS

本要件が TSF または TOE プラットフォームのいずれによって満たされるかに関わらず、評価者は、ST の要件を満たすために必要なそれぞれの永続的な秘密(クレデンシャル、秘密鍵)及びプライベート鍵が TSS に列挙されていることを保証するため、TSS をチェックすること。これらの項目のそれぞれについて、評価者は、それが利用される目的、格納される方法について TSS に列挙されていることを管区任す

ること。評価者は、以下のアクションを実行すること。

TOE プラットフォームによって取り扱われる永続的な秘密とプライベート鍵

ST で列挙されるそれぞれのプラットフォームについて、評価者は、永続的な秘密とプライベート鍵がそのプラットフォームの ST で保護されているとして特定されている MDM サーバの ST においてプラットフォームによって格納されているものとして列挙されることを保証するためにプラットフォームの ST を検査しなければならない(shall)。

TSF によって取り扱われる永続的な秘密とプライベート鍵

評価者は、TOE によって取り扱われるものとして列挙されるそれぞれの項目について、それが永続的なメモリへ暗号化されずに書き込まれない、及びその項目がプラットフォームによって格納されることを論証していることを決定するため、TSS をレビューする。

5.4.3 識別と認証 (FIA)

FIA_UAU.1 **認証のタイミング**

FIA_UAU.1.1 **[*選択：TSF、TOE プラットフォーム*]** は、利用者が**サーバを用いて**認証される前に利用者を代行して行われる *[割付：TSF 仲介アクションのリスト]*を許可しなければならない (shall)。

FIA_UAU.1.2 **[*選択：TSF、TOE プラットフォーム*]** は、その利用者を代行するほかのすべての TSF 仲介アクションを許可する前に、各利用者に**サーバを用いて**認証が成功することを要求しなければならない (shall)。

適用上の注釈： *本要件は TSF をアクセスしようとするあらゆる利用者が認証されなければならない(must)ことを保証する。これらの利用者は、TOE の管理を試行する管理者かもしれないし、または MDM システムによる管理のため登録を試行する普通の利用者かもしれない。ST 作成者は、この認証前に行われることが可能なアクションのリストの割付を行う責任を負う。TSF または TOE プラットフォームは、本要件を満たすために企業の認証を活用してもよい。*

保証アクティビティ

TSS

評価者は TSS を検査して、認証前に実行可能と実行不可能なアクション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

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、認証前に禁止されたアクションを行うことを試行しなければならない(shall)。評価者は、そのアクションを行うことができ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、認証後に禁止されたアクションを行うことを試行しなければならない (shall)。評価者は、そのアクションを行うことができることを検証しなければならない (shall)。

FIA_X509_EXT.1　証明書の検証

FIA_X509_EXT.1.1　[*選択：TSF、TOE プラットフォーム*] は、以下の規則に従って、証明書の有効性を検証しなければならない(shall)：

- RFC 5280 証明書の検証及び認証パス検証。
- 認証パスは、信頼される CA 証明書で終端しなければならない(shall)。
- 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 で規定されるオンライン証明書状態プロトコル (OCSP)、RFC 5759 で規定される証明書失効リスト (CRL)*] を用いて証明書の失効状態を検証しなければならない(shall)。
- TSF は、以下の規則に従って、extendedKeyUsage フィールドを検証しなければならない(shall)：
  - 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、extendedKeyUsage フィールドにコード署名目的 (id-kp 3 が OID 1.3.6.1.5.5.7.3.3 となる) を持たなければならない(shall)。
  - TLS 用に提示されるクライアント証明書は、extendedKeyUsage フィールドにクライアント認証目的 (id-kp 1 が OID 1.3.6.1.5.5.7.3.2 となる) を持たなければならない(shall)。
  - OCSP レスポンスとして提示される OCSP 証明書は、extendedKeyUsage フィールドに OCSP 署名目的(id-kp 9 が OID 1.3.6.1.5.5.7.3.9 となる)を持たなければならない(shall)。
  - EST ように提示されるサーバ証明書は、extendedKeyUsage フィールドに CMC 登録局(RA)目的(id-kp-cmcRA が OID 1.3.6.1.5.5.7.3.28 となる)を持たなければならない。

適用上の注釈：　*FIA_X509_EXT.1.1 には、証明書の検証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を選択しなければならない (shall)。FIA_X509_EXT.2 は、証明書が高信頼チャネルのために利用されることを要求する；この用途は、extendedKeyUsage 規則が検証されることを要求する。証明書は、オプションで、コード署名とポリシー署名のために利用されてもよい、実装される場合、対応する extendedKeyUsage を含んでいることについて検証されなければならない(shall)。*

TSF か TOE プラットフォーム化の選択に関わらず、検証は、プラットフォームによって管理されるルートストアの信頼されるルート CA 証明書で終端することが期待される。

保証アクティビティ

TSS

評価者は、証明書の有効性のチェックがどこで行われているかについて TSS に記述されていることを保証しなければならない(shall)。評価者は、TSS が認証パス検証アルゴリズムの記述についても提供していることを保証する。

テスト

記述されたテストは、FIA_X509_EXT.2.1 の機能のそれぞれを含めて、その他の証明書サービス保証アクティビティと併せて実行されなければならない(must)。extendedKeyUsage 規則についてのテストは、それらの規則を要求するような用途と併せて実行される。評価者は、少なくとも 4 つの証明書のチェインを作成しなければならない(shall)：テストされるノード証明書、2 つの中間 CA、及び自己署名されたルート CA。

テスト 1：評価者は、その機能において利用されるべき証明書を検証する必要がある、信頼された CA として証明書をロードし、その機能が成功することを実証しなければならない(shall)。評価者は、次に証明書の 1 つを削除し、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、期限切れの証明書の検証が失敗をもたらすことを実証しなければならない(shall)。

テスト 3：評価者は、TOE が失効した証明書を適切に取り扱うことができること—CRL または OCSP が選択されたかの条件でをテストしなければならない(shall)；両方が選択された場合、テストは、それぞれの方法で実行されなければならない(shall)。評価者は、ノード証明書の失効と中間 CA 証明書(即ち、中間 CA 証明書は、るーと CA によって失効されるべきである)の失効をテストしなければならない(shall)。評価者は、有効な証明書が利用されること、及び検証機能が成功したことを保証しなければならない(shall)。評価者は、次に、いつ証明書がもはや検証機能が失敗するような無効となるかを保証するため、(選択において選択されたそれぞれの方法について)失効した証明書を用いてテストを試行すること。

テスト 4：OCSP が選択される場合、評価者は、OCSP 署名目的を持たない証明書を防ぎ、OCSP レスポンスの検証が失敗することを検証するため、OCSP サーバを構成し、中間者攻撃ツールを用いなければならない(shall)。CRL が選択される場合、評価者は、cRLsign 鍵用土ビットがセットされていないような証明書を伴う CRL に署名するため、CA を構成し、CRL の検証が失敗することを検証しなければならない(shall)。

テスト 5：評価者は、証明書の最初の 8 バイトの任意のビットを改変し､証明書が検証に失敗することを実証しなければならない(shall)｡(証明書は、正しく解析できない。)

テスト 6：評価者は、証明書の最後のバイトの任意のビットを改変し、証明書が検証に失敗することを実証しなければならない(shall)。(証明書の署名が検証されない。)

テスト 7：評価者は、証明書の公開鍵の任意のバイトを改変し、証明書が検証に失敗することを実証しなければならない(shall)。(証明書の署名が検証されない。)

FIA_X509_EXT.1.2 [*選択：TSF、TOE プラットフォーム*] 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)。

適用上の注釈： *本要件は、TOE またはプラットフォームによって利用され、処理される証明書に適用され、信頼される CA 証明書として追加されてもよい証明書を制限する。*

保証アクティビティ

テスト

記述されたテストは、FIA_X509_EXT.2.1 の機能を含めて、その他の証明書サービスの保証アクティビティと併せて実行されなければならない(shall)。評価者は、少なくとも 4 つの証明書のチェインを作成しなければならない(shall) : テストされるべきノード証明書、2 つの中間 CA、及び自己署名されたルート CA。

テスト 1 : 評価者は、TOE の証明書を発行している CA の証明書が basicContraints 拡張を含まないように、認証パスを構築しなければならない(shall)。認証パスの検証は失敗する。

テスト 2 : 評価者は、TOE の証明書を発行している CA の証明書が basicContraints 拡張の 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)。認証パスの検証は失敗する。

テスト 3 : 評価者は、TOE の証明書を発行している CA の証明書が basicContraints 拡張の 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)。認証パスの検証は成功する。

FIA_X509_EXT.2 **X509 証明書認証**

FIA_X509_EXT.2.1 [*選択 : TSF、TOE プラットフォーム*] は、[*選択 : IPsec、TLS、HTTPS、DTLS、SSH*] の認証、及び [*選択 : システムソフトウェアのアップデートに対するコード署名、完全性検証に対するコード署名、ポリシー署名、[割付 : その他の用途]、追加の用途なし*] をサポートするため、RFC 5280 によって定義される X.509v3 証明書を利用しなければならない(shall)。

適用上の注釈： *ST 作成者の選択は、FTP_TRP.1、FTP_ITC.1、及び FPT_ITT.1 の選択と合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の高信頼アップデート(FPT_TUD_EXT.1.3) 及びソフトウェア完全性検証 (FPT_TST_EXT.1.2)用にオプションで利用されてもよい。何らかの認証サービスが TOE によって提供され、その他がプラットフォームによる場合、ST 作成者は、どのサービスが TOE によって提供されて、どれがプラットフォームによるかを明確に特定しなければならない(shall)。*

完全性検証に対するコード署名が選択される場合、MDM ベンダが彼らの製品に含まれるほかのベンダからの DLL に対してディジタル署名することは期待されていない。

「IPsec」が選択される場合、IPsec VPN クライアントの拡張パッケージが ST に含まれなければならない(must)。「SSH」が選択される場合、セキュアシェルの拡張パッケージが ST に含まれなければならない(must)。「TLS」、「HTTPS」または「DTLS」が選択される場合、附属書 B からの適切な選択ベースの SFR が ST に含まれなければならない(must)。

FIA_X509_EXT.2.2 [*選択：TSF、TOE プラットフォーム*] が証明書の有効性を判断する接続を確立できないとき、[*選択：TSF、TOE プラットフォーム*] 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)。

適用上の注釈： *CRL のダウンロードするにしても、OCSP の実行するにしても—証明書の失効状態の検証を実行するため、しばしば接続が確立されなければならない(must)。この選択は、こ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。証明書は FIA_X509_EXT.1 の他の全ての規則に従って有効であると TOE が決定した場合、2 番目の選択に示されるふるまいによって有効性が決定されなければならない(shall)。証明書が FIA_X509_EXT.1 の他の検証の規則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る場合、ST 作成者は FMT_SMF.1(2) の機能 d についても選択しなければならない (must)。*

保証アクティビティ

TSS

評価者は、どの証明書を使うかを TOE が選択する方法、及び TOE が証明書を利用できように、運用環境の設定について管理者ガイダンスにおける必要な指示について、TSS に記述されていることを保証するため、TSS をチェックしなければならない(shall)。

評価者は、高信頼チャネルの確立で利用される証明書の有効性チェック中に接続が確立できないときの TOE のふるまいについて TSS に記述されていることを確認するため、TSS を検査しなければならない(shall)。評価者は、高信頼チェネル間のあらゆる区別について記述されていることを検証しなければならない(shall)。

ガイダンス

管理者がデフォルトのアクションを規定できるという要件が選択される場合、次に評価者は、操作ガイダンスにこの設定アクションの実行方法について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)。

テスト

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

評価者は、有効な証明書を用いて、非 TOE のエンティティと通信することによって少なくともいくつかの部分で実行されるためのチェックを行う証明書検証を要求することを実証しなければならない(shall)。評価者は、次に TOE が証明書の有効性を検証できないように環境を操作しなければならない(shall)、また FIA_X509_EXT.2.2 で選択されるアクションが実行されることを観測しなければならない(shall)。選択されるアクションが管理者セー定可能である場合、評価者は、すべてのサポートされる管理者設定可能なオプションがそれらの文書化されたやり方でふるまうことを決定するために、操作ガイダンスに従わなければならない(shall)。

FIA_X509_EXT.2.3 [*選択：TSF、TOE プラットフォーム*] は、それぞれのクライアントデバイスのためのユニークな証明書を要求しなければならない(shall)。

適用上の注釈： *それぞれのクライアントデバイスは、MDM エージェントによって利用されるユニークな X.509v3 証明書を持っているだろう；証明書は、クライアント間で再利用されるべきではない。本要件は、MDM サーバがそれぞれのクライアントの証明書がユニークであることを保証することである。*

保証アクティビティ

テスト

ST でサポートされているとして、列挙されたそれぞれの MDM エージェント／プラットフォームについて：

評価者は、特化した運用環境と開発ツール(TOE のためのデバッガ、シミュレータ等及び本テストを実行するために必要であるものとして整えられた TOE ビルド)の適切な組み合わせを活用しなければならない(shall)。

評価者は、デバイスのユニークな証明書を用いて確立された高信頼チャネルを介して、MDM サーバとクライアントデバイス間の通信を開始し、成功した通信チャネルが確立されたことを検証しなければならない(shall)。評価者は、次に最初のデバイスからのユニークな証明書を用いて確立した高信頼チャネルを介して MDM サーバと 2 番目のクライアントデバイス間の通信の開始を試行し、MDM サーバが通信において本試行を拒否することを検証しなければならない(shall)。

5.4.4 TSF の保護 (FPT)

FPT_TST_EXT.1 **TSF 機能のテスト**

FPT_TST_EXT.1.1 [*選択：TSF、TOE プラットフォーム*] は、TOE の正しい動作を実証するため、初期起動中 (電源投入時) に一連の自己テストを実行しなければならない(shall)。

FPT_TST_EXT.1.2 [*選択：TSF、TOE プラットフォーム*] は、 [*選択：TSF、TOE プラットフォーム*] が提供する暗号サービスを用いて TSF 実行可能形式のコードが実行のためにロードされるとき、格納された TSF 実行可能形式のコードの完全性を検証するための機能を提供しなければならない(shall)。

適用上の注釈： *TOE は通常、IT 環境で動作するソフトウェアパッケージではあるが、上記の要求される自己テストアクティビティを行うことができる。しかし、上記テストにより提供される保証を評定する上で、ホスト環境に大きく依存していること (ホスト環境が危殆化した場合、自己テストは意味がないことを意味する) は理解されるべきである(should)。*

保証アクティビティ

TSS

評価者は、起動時に TSF によって実行される自己テストについて TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)；この記述は、どのテストが実際に行われるのか(例、「メモ

リがテストされる」というよりも、むしろ「ある値をそれぞれのメモリロケーションに書き込み、書き込まれたものとそれが同一であることを保証するため、それを読み出すようなメモリがテストされる」のような記述が用いられるべきである(should))についての概要が含まれるべきである(should)。評価者は、TSF が正しく動作していることを実証するためにテスト十分であることが TSS にて説明されていることを保証しなければならない(shall)。

評価者は、実行時にロードされるときに、格納された TSF 実行可能形式のコードの完全性を検証する方法が TSS に記述されていることを保証するため、TSS を件だしなければならない(shall)。評価者は、格納された TSF 実行可能形式のコードが危殆化していないことを実証する田 m、テストが十分であることについて、TSS にて説明されていることを保証しなければならない(shall)。評価者は、実行されたアクションの成功(例、ハッシュが検証される)及び不成功(例、ハッシュが検証されない)について TSS(または操作ガイダンス)に記述されていることについても保証する。

テスト

評価者は、以下のテストを実行しなければならない(shall) :

テスト 1 : 評価者は、既知の良好な TSF 実行可能形式の完全性チェックを実行し、チェックが成功することを検証する。

テスト 2 : 評価者は、TSF 実行可能形式を改変し、改変された TSF 実行可能形式の完全性チェックを実行し、チェックが失敗する k とを検証する。

FPT_TUD_EXT.1　高信頼アップデート

FPT_TUD_EXT.1.2　[*選択 : TSF、TOE プラットフォーム*] は、TSF ソフトウェアへのアップデートを開始する能力を許可された管理者へ提供しなければならない (shall)。

FPT_TUD_EXT.1.3　[*選択 : TSF、TOE プラットフォーム*] 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、ディジタル署名メカニズムを用いてそれらのアップデートを検証する手段を提供しなければならない (shall)。

適用上の注釈 :　*TSF 上のソフトウェアは、ときどきアップデートが必要となる。本要件は、ベンダによって提供されたアップデートのみを TSF がインストールすることを保証することを意図しており、別の情報源により提供されたアップデートには、悪意のあるコードが含まれているかもしれない。そのサーバがアプライアンスではない場合、アップデートはサーバソフトウェアが動作するプラットフォームによって検証され、サーバがアプライアンスである場合、アップデートは TSF のソフトウェアまたはハードウェアによって検証されなければならない (must)。*

保証アクティビティ

TSS

評価者は、TSS を検査し、アップデートがディジタル署名される規格と署名検証処理がどのように実装されたかについて TSS に記述され

ていることを検証しなければならない(shall)。

ガイダンス

評価者は、TSF ソフトウェアの現在のバージョンを問い合わせる方法、アップデートを開始する方法及びインストールの前にアップデートの完全性をチェックする方法について AGD ガイダンスに記述されていることを検証するため、AGD ガイダンスを検査しなければならない(shall)。

テスト

評価者は、以下のテストを実行しなければならない(shall) :

テスト 1 : 評価者は、ベンダによりディジタル署名されたアップデートの開始を試行し、そのアップデートのインストールが成功することを検証しなければならない(shall)。

テスト 2 : 評価者は、ベンダによりディジタル署名されていないアップデートの開始を試行し、その署名がチェックできるか(アップデートの中止を許可する)またはアップデートがインストールされないことを検証しなければならない(shall)。

5.4.5 高信頼パス／チャネル (FTP)

FTP_ITC.1(1)　TSF 間高信頼チャネル (許可された IT エンティティ)

FTP_ITC.1.1(1)　**[*選択 : TSF、TOE プラットフォーム*]**は、それ自身と**以下の機能をサポートする**許可された IT エンティティの間の高信頼通信チャネルを提供するため**[*選択 : IPsec、SSH、TLS、TLS/HTTPS*]**を利用しなければならない(shall) : **監査サーバ、[*選択 : 認証サーバ、[割付 : その他の機能]*]**で、その他の通信チャネルから論理的に区別され、その端点の保証された識別と改変または暴露からのチャネルデータの保護を提供するもの。

適用上の注釈 :　*上記要件の必須部分の意図は、TOE がその機能を実行するために対話するような、許可された IT エンティティとの高信頼チャネルを確立し、維持するため、要件で特定された暗号プロトコルを利用することである。*

保護(列挙されたプロトコルの 1 つによって)は、少なくとも監査情報を収集するようなサーバとの通信のために要求される。認証サーバ(例、RADIUS)と通信する場合、ST 作成者は、FTP_ITC.1.1(1) で「認証サーバ」を選択し、本接続は、列挙されたプロトコルの 1 つによって保護されなければならない(shall)。その他の許可された IT エンティティ(例、NTP サーバ)が保護される場合、ST 作成者は、適切な割付(それらのエンティティのため)と選択(それらの接続を保護するために利用されるプロトコルのため)を行う。

要約するため、外部監査収集サーバへの接続は、列挙されたプロトコルの 1 つによって保護されることが要求される。外部認証サーバがサポートされる場合、列挙されたプロトコルの 1 つを用いてその接続を保護することが要求される。任意のその他の外部サーバについて、外部通信は、保護されることは要求されないが、保護が主張される場合、特定されたプロトコルの一つを用いて保護されなければならない

(shall)。

高信頼チャネルは、MDM 通信の機密性と完全性を保護するプロトコルとして、IPsec、TLS、DTLS、またはHTTPS を利用する。ST 作成者は、TOE によってサポートされるメカニズムを選択する。「IPsec」が選択される場合、IPsec VPN クライアントの拡張パッケージがST に含まれなければならない(must)。「SSH」が選択される場合、Secure Shell の拡張パッケージがST に含まれなければならない(must)。「TLS」または「TLS/HTTPS」が選択される場合、附属書B の適切な選択ベースのSFR がST に含まれなければならない(must)。

プロトコル、RBG、証明書検証、アルゴリズム、及び同様のサービスは、プラットフォームが提供するサービスと合致することができる。

本要件は、初期に通信が確立されるとき保護される通信であるだけでなく、停電後の再開についても暗黙的に適用される。何らかのTOE セットアップにその他の通信を保護するためのトンネルの手動セットアップを服ような場合があるかもしれない、停電後にTOE が手動の介入と共に(必須)自動的に通信の再確立を試行する場合、攻撃者が重要な情報を取得または接続を危殆化できるかもしれないように作成された窓があるかもしれない。

FTP_ITC.1.2(1) TSF は、高信頼チャネルを介して通信の開始を **MDM サーバまたはその他の許可された IT エンティティ**に許可しなければならない(shall)。

FTP_ITC.1.3(1) TSF は、[*割付：TSF が通信を開始できるようなサービスのリスト*]のための高信頼チャネルを介して通信を開始しなければならない(shall)。

適用上の注釈： *通信を開始する者についての要件はないが、ST 作成者はFTP_ITC.1.3 の割付、TOE が許可された IT エンティティとの通信を開始できるようなサービスに列挙する。*

保証アクティビティ

TSS

評価者は、許可された IT エンティティとの通信方法が通信の保護方法と共に示されていることを決定するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスに MDM サーバと許可された IT エンティティの間の通信チャネルをそれぞれのサポートされる方法について設定する指示が含まれていることを確認しなければならない(shall)。

テスト

テスト 1：評価者は、評価作業中に、操作ガイダンスに記述されるとおりに接続をセットアップし、通信が成功することを保証して、それぞれの (操作ガイダンスにおいて) 規定された通信方法がテスト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、それぞれの通信方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

テスト 3：評価者は、MDM サーバとのそれぞれの通信チャネルについ

て、テスト中のプロトコルとしてプロトコルアナライザがそのトラフィクを特定することを保証しなければならない(shall)。

さらなる保証アクティビティが具体的なプロトコルに関連している。

FTP_TRP.1(1) **高信頼パス (リモート管理)**

FTP_TRP.1.1(1) [***選択：TSF、TOE プラットフォーム***] は、それ自身と他の通信パスとは論理的に区別される**リモート管理者**との間の高信頼通信パスであり、その端点の保証された識別と [*改変、暴露*]からの通信データの保護を提供するような、高信頼通信パスを提供するため、**[*選択：IPsec、TLS、 TLS/HTTPS、SSH*]** を利用しなければならない (shall)。

FTP_TRP.1.2(1) [***選択：TSF、TOE プラットフォーム***] は、**リモート管理者に**高信頼パスを介して通信を開始することを許可しなければならない (shall)。

FTP_TRP.1.3(1) [***選択：TSF、TOE プラットフォーム***] は、[*すべてのリモート管理者アクション*]に高信頼パスの利用を要求しなければならない (shall)。

適用上の注釈： *本要件は、許可されたリモート管理者が高信頼パスを介して TOE とのすべての通信を開始すること、及びリモート管理者による TOE とのすべての通信はこのパスを介して行われることを保証する。本高信頼通信チャネルにおいて通過するデータは、最初の選択で選ばれた定義済のプロトコルで暗号化される。ST 作成者は TOE によってサポートされるメカニズムを選択する。「IPsec」が選択される場合、IPsec VPN クライアントの拡張パッケージが ST に含まれなければならない (must)。「SSH」が選択される場合、Secure Shell の拡張パッケージが ST に含まれなければならない(must)。「TLS」または「TLS/HTTPS」が選択される場合、附属書 B の適切な選択ベースの SFR が ST に含まれなければならない(must)。*

保証アクティビティ

TSS

評価者は、リモート TOE 管理の方法が通信の保護方法と共に示されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、TOE 管理のサポートで TSS に列挙されたすべてのプロトコルが本要件で規定されたものと一貫しており、ST にその要件を含んでいることについても確認しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスにリモート管理セションをそれぞれのサポートされる方法について確立するための指示が含まれていることを確認しなければならない(shall)。

テスト

評価者は、以下のテストについても実行しなければならない(shall) :

テスト 1 : 評価者は、評価作業中に、操作ガイダンスに記述されるとおりに接続をセットアップし、通信が成功することを保証して、それぞれの (操作ガイダンスにおいて) 規定されたリモート管理方法がテスト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、それぞれのリモート管理方法について、高信頼

パスを起動することなくリモート管理セションを確立するためにリモート利用者によって利用できるようなインタフェースが利用可能でないことを保証するため、操作ガイダンスに従わなければならない(shall)。

テスト 3：評価者は、それぞれのリモート管理方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

さらなる保証アクティビティが具体的なプロトコルに関連している。

FTP_TRP.1(2) **高信頼パス (登録用)**

FTP_TRP.1.1(2) [*選択：**TSF**、**TOE プラットフォーム***] は、それ自身と他の通信パスとは論理的に区別される **MD 利用者**との間の高信頼通信パスであり、その端点の保証された識別と暴露からの通信データの保護と[*改変*、*暴露*]からの通信データの改変の検知を提供するような、高信頼通信パスを提供するため、**[*選択： TLS*、 *TLS/HTTPS*]** を利用しなければならない(shall)。

FTP_TRP. 1.2(2) [*選択：**TSF**、**TOE プラットフォーム***] は、高信頼パスを介して、**MD 利用者**に通信の開始を許可しなければならない (shall)。

FTP_TRP.1.3(2) [*選択：**TSF**、**TOE プラットフォーム***] は、[*すべての MD 利用者アクション*]に高信頼パスの利用を要求しなければならない(shall)。

適用上の注釈： *本要件は、許可された MD 利用者が高信頼パスを介して TOE とのすべての通信を開始すること、及び MD 利用者による TOE とのすべての通信がこのパスを介して行われることを保証する。この接続の目的は、MD 利用者による登録のためである。この高信頼通信チャネルにおいて通過するデータは、最初の選択で選ばれた定義済プロトコルにより暗号化される。ST 作成者は TOE によってサポートされたメカニズムを選び、そしてそれらの選択に対応する附属書 B の詳細な要件が、すでに存在していない場合、ST に複写されることを保証する。*

「TLS」が登録用の高信頼通信パスとして利用されるプロトコルとして選択される場合、相互認証は要求されない。

保証アクティビティ

TSS

評価者は、リモート登録の方法が通信の保護方法と共に示されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、登録のサポートで TSS に列挙されたすべてのプロトコルが本要件で規定されたものと一貫しており、ST にその要件を含んでいることについても確認しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスに登録セションをそれぞれのサポートされる方法について確立するための指示が含まれていることを確認しなければならない(shall)。

テスト

ST でサポートされるものとして列挙されたそれぞれの MDM エージェ

ント／プラットフォームについて：

テスト 1：評価者は、評価作業中に、操作ガイダンスに記述されるとおりに接続をセットアップし、通信が成功することを保証して、それぞれの (操作ガイダンスにおいて) 規定された登録方法を用いる通信がテスト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、それぞれのサポートされる登録方法について、高信頼パスを起動することなく登録セションを確立するためにリモート利用者によって利用できるようなインタフェースが利用可能でないことを保証するため、操作ガイダンスに従わなければならない(shall)。

テスト 3：評価者は、それぞれの登録方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

さらなる保証アクティビティが具体的なプロトコルに関連している。

6. セキュリティ保証要件

セクション 4 の TOE のセキュリティ対策方針は、セクション 3.1 で特定された脅威へ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具体化である。本 PP は、評価者が評価に適用可能な証拠資料を評定し、独立テストを実行するような範囲を設定するためのセキュリティ保証要件 (SAR) を特定する。

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

本 PP に適合するよう作成された ST に対する TOE の評価を行う一般的なモデルは以下のようなとおりである：

ST が評価されることが承認された後、ITSEF (訳注：評価機関) は TOE、支援 IT 環境、及び TOE の管理者ガイド／利用者ガイドを入手する。ITSEF は、ASE 及び ALC の SAR について、共通評価方法（CEM）によって義務付けられたアクションを実行することが期待される。ITSEF は、TOE で具体化された具体的な技術に適用される者としてその他の CEM 保証要件の解釈として意図された、セクション 5 に含まれる保証アクティビティについても実行する。セクション 5 で取り込まれた保証アクティビティは、TOE が本 PP に適合することを実証するために開発者が提供する必要があるものとしての明確化を提供する。

TOE のセキュリティ保証要件は、表 2 で特定される。

保証クラス	**保証コンポーネント**
セキュリティターゲット評価 (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)
テスト (ATE)	独立テスト—適合 (ATE_IND.1)
脆弱性評定 (AVA)	脆弱性調査 (AVA_VAN.1)

表 2：TOE セキュリティ保証要件

6.1 ASE クラス：セキュリティターゲット評価

ST は、CEM で定義された ASE アクティビティにより評価される。さらに、セクション 5 で規定された保証アクティビティ､及び TOE 技術種別に特有の TSS で含まれるべき必要な記述について求める関連する附属書があるかもしれない。

6.2 ADV クラス：開発

TOE に関する設計情報は、ST の TSS 部分、及び公開されないような本 PP で要求される追加の情報と同様に、エンドユーザに利用可能なガイダンス証拠資料にも含まれる。

6.2.1 基本機能仕様 (ADV_FSP.1)

機能仕様書には、評価対象のセキュリティ機能インタフェース (TSFI) を記述する。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 証拠資料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「機能仕様書」証拠資料は必要とはされない。

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実行するために必要な情報を通して特徴付けされる。

開発者アクションエレメント：

ADV_FSP.1.1D　開発者は、機能仕様を提供しなければならない (shall)。

ADV_FSP.1.2D　開発者は、機能仕様から SFR への追跡を提供しなければならない (shall)。

適用上の注釈：　*本セクションの序文で述べたように、機能仕様は AGD_OPE 及び AGD_PRE 証拠資料に含まれる情報から構成されている。*

開発者は、アプリケーション開発者及び評価者にアクセス可能なウェブサイトを参照してもよい。

機能仕様の保証アクティビティは、証拠資料及び TSS セクションに存在すべき (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 における追跡は、すでに暗黙的になされており、追加の証拠資料は必要とされない。

内容・提示エレメント：

ADV_FSP.1.1C　機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない (shall)。

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

ADV_FSP.1.3C　機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を提供しなければならない (shall)。

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

評価者アクションエレメント：

ADV_ FSP.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない (shall)。

ADV_ FSP.1.2E　評価者は、機能仕様が、SFR の正確かつ完全な具体化であることを決定しなければならない (shall)。

保証アクティビティ：

情報が提供されていることの保証以外に、これらの SAR に関連する具体的な保証アクティビティはない。機能仕様書証拠資料は、セクション 5 で記述された評価アクティビティ、関連する附属書、及び AGD、ATE 及び AVA の SAR について記述されたその他のアクティ

ビティを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、実行されるその他の保証アクティビティに基づいて暗黙的に評定される；インタフェース情報が不十分である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には、適切な機能仕様が提供されていなかったことになる。

6.3 AGD クラス：ガイダンス証拠資料

ガイダンス証拠資料は、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可能であることを 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)。証拠資料は、非形式的なスタイルかつ IT 要員によって読解可能であるべきである(should)。

ガイダンスは、ST で主張されたとおり製品がサポートする、すべての運用環境について提供されなければならない (must)。このガイダンスには、以下が含まれる：

- その環境において TSF のインストールに成功するための指示、及び
- 製品として、またより大き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
- 保護された管理者機能を提供するための指示。

特定のセキュリティ機能に関するガイダンスもまた、提供されなければならない (must)；このようなガイダンスに関する要件は、各要件で規定された保証アクティビティに含まれる。

6.3.1 利用者操作ガイダンス (AGD_OPE.1)

開発者アクションエレメント：

AGD_OPE.1.1D　開発者は、利用者操作ガイダンスを提供しなければならない (shall)。

適用上の注釈：　*利用者操作ガイダンスは、単一の文書に含まれる必要はない。利用者、管理者及びアプリケーション開発者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、ガイダンス証拠資料はセキュリティ自動化をサポートするために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。*

ここで情報を繰返し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、受け入れ能なガイダンスの作成に必要な情報が提供されることになる。

内容・提示エレメント：

AGD_OPE.1.1C　利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない (shall)。

適用上の注釈：　*利用者及び管理者は、利用者役割の定義において考慮されるべきである。*

AGD_OPE.1.2C　利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごと

に記述しなければならない(shall)。

AGD_OPE.1.3C　利用者操作ガイダンスは、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、必要に応じてセキュアな値を示し、利用者の役割ごとに記述しなければならない(shall)。

AGD_OPE.1.4C　利用者操作ガイダンスは、TSF の制御下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連するセキュリティ関連事象の各タイプについて、利用者の役割ごとに明確に提示しなければならない(shall)。

AGD_OPE.1.5C　利用者操作ガイダンスは、TOE の操作のすべての可能なモード (障害や操作誤りの後の操作を含む)、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない(shall)。

AGD_OPE.1.6C　利用者操作ガイダンスは､ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、利用者の役割ごとに記述しなければならない(shall)。

AGD_OPE.1.7C　利用者操作ガイダンスは、明確で、合理的なものでなければならない(shall)。

評価者アクションエレメント：

AGD_OPE.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

保証アクティビティ：

操作ガイダンスの内容の一部は、セクション 4.2、4.3、及び 4.4 の保証アクティビティと CEM に従った TOE の評価によって検証されることになる。以下の追加情報についても要求される。

暗号機能が TOE によって提供される場合､TOE の評価される構成に関連する暗号エンジンを設定するための指示が操作ガイダンスに含まれていなければならない (shall)。TOE の CC 評価中、その他の暗号エンジンの利用については、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)。

証拠資料には、ディジタル署名を検証することによる TOE へのアップデートを検証する処理が記述されなければならない(must)—これは TOE によって行われても、基盤となるプラットフォームによって行われてもよい。評価者は、この処理に以下の手順が含まれることを検証しなければならない(shall)：

アップデート自体を取得する指示。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、特定のディレクトリへの格納) が含まれるべきである (should)。

アップデート処理を開始するための指示、及び処理が成功したか失敗したかを判別するための指示。これには、ハッシュ／ディジタル署名の生成が含まれる。

TOE には、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を含むこともあり得る。操作ガイダンスは、どのセキュリティ機能が評価アクティビティによって網羅されているのかを管理者に対して明確にしなければならない (shall)。

6.3.2 準備手続き (AGD_PRE.1)

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)。

適用上の注釈：　*操作ガイダンスと同様に、開発者は保証アクティビティを検査して準備手続きに関して必要とされる内容を判断すべきである (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　準備手続きは、TOE のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない (shall)。

評価者アクションエレメント：

AGD_ PRE.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

AGD_ PRE.1.2E　評価者は､TOE が運用に向けてセキュアに準備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：

上記の序文で示すとおり、証拠資料に関する重要な想定がある―特に TOE の機能要件をサポートする運用環境を設定するとき。評価者は、TOE 用に提供されるガイダンスが､ST において 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適切に対処していることを保証するためチェックしなければならない(shall)。

6.4 ALC クラス：ライフサイクルサポート

本 PP に適合する TOE に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.1)

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.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

保証アクティビティ

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

6.4.2 TOE の CM 範囲 (ALC_CMS.1)

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：(訳注：一貫性を保つため ALC_CMS.1 エレメントとした)

ALC_CMS.1.1D　開発者は、TOE の構成リストを提供しなければならない (shall)。

内容・提示エレメント：

ALC_CMS.1.1C　構成リストは、TOE 自体、及び SAR が要求する評価証拠を含まなければならない(shall)。

ALC_CMS.1.2C　構成リストは、構成要素を一意に識別しなければならない (shall)。

評価者アクションエレメント：

ALC_CMS.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

保証アクティビティ：

本 PP において「SAR 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。

評価者は、開発者が (それらのプラットフォームの公共向け開発証拠資料で) 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本証拠資料に含まれていることを保証しなければならない (shall)。

評価者は、TSF が一意に識別され (その TSF ベンダからの他の製品との関連で)、ST の要件と関連して開発者から提供される証拠資料が、この一意の識別情報を用いて TSF と関連付けられることを保証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) に露出しないため、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.1)

テストは、TSS と、提供された管理者証拠資料 (設定及び操作を含む) 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 4.2、4.3 及び 4.4 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、いくつかの追加のテストがセクション 4.4 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の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、テストのための TOE を提供しなければならない (shall)。

内容・提示エレメント：

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

評価者アクションエレメント：

ATE_IND.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

ATE_IND.1.2E　評価者は、TSF が仕様どおりに動作することを確認するために、TSF のサブセットを*テストしなければならない (shall)*。

保証アクティビティ：

評価者は、システムのテストの側面を文書化したテスト計画書とテスト報告書を作成しなければならない (shall)。テスト計画書は、CEM と本 PP の保証アクティビティ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 証拠資料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 証拠資料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証拠資料を考慮して、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.1)

開発者アクションエレメント：

AVA_VAN.1.1D　開発者は、テストのための TOE を提供しなければならない (shall)。

内容・提示エレメント：

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

評価者アクションエレメント：

AVA_VAN.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを*確認しなければならない (shall)*。

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

AVA_VAN.1.3E　評価者は､基本的な攻撃能力を持つ攻撃者からの攻撃に TOE が耐えられることを決定するために、識別された潜在的脆弱性に基づいて侵入テストを*実施しなければならない (shall)*。

保証アクティビティ：

ATE_IND と同様に、評価者は報告書を作成し、本要件に関連する自分たちの結論を文書化しなければならない (shall)。この報告書は、物理的にはATE_INDに言及される全体的なテスト報告書の一部であってもよいし、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中に文書化する。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. オプション要件

本 PP の序論で示したように、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。

第 1 の種類 (本附属書に含まれる) は、ST に取り込むことができる要件であるが、TOE が本 PP への適合を主張するためには必要とされないものである。第 2 の種類 (附属書 C に含まれる) 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取り込まれることが必要となる。第 3 の種類 (附属書 D に含まれる) 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取り込まれることになっているコンポーネントであり、VPN クライアント (訳注：MDM クライアントの間違い) 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する可能性があ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 へ取り込まれることを確実にする責任があることに注意されたい。

本附属書は、TSF によって行われてもよいオプションの要件と、MDM サーバ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てもよいオプションの要件という、2 つのサブセクションに分かれている。

A.1 オプション TSF 要件

A.1.1 セキュリティ監査 (FAU)

FAU_SEL.1 **セキュリティ監査事象の選択 (MDM サーバ)**

FAU_SEL.1.1 **MDM サーバ**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. **事象の種類、**
b. **監査対象セキュリティ事象の成功、**
c. **監査対象セキュリティ事象の失敗、及び**
d. ***[割付：その他の属性]*。**

適用上の注釈： *本要件の意図は、監査事象を引き起こすために選択可能なすべての基準を特定することである。ST 作成者は、MDM サーバとプラットフォームのどちらが監査記録を維持するのか選択しなければならない (must)。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特定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、管理者はその

属性の選択によってその属性を持つ監査事象 (または、管理ガイダンスに特定される、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、その機能を行使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)。

A.1.2 TSF の保護 (FPT)

FPT_ITT.1　　TOE 内 TSF データ転送

FPT_ITT.1.1　TSF は、TOE の別々の部分の間でデータが転送されるとき、**[*選択:IPsec、TLS、HTTPS、DTLS*] の利用を通して** [*暴露及び改変*] からすべてのデータを保護しなければならない(shall)。

適用上の注釈：　*本要件は、分散型 TOE のコンポーネント間のすべての通信(MDM サーバと MAS サーバ間のような)が暗号化された通信チャネルの利用を通して保護されることを保証する。本高信頼通信チャネルにおいて通過するデータは、最初のせんたくで選択された定義されたプロトコルにより暗号化される。*

高信頼チャネルは、MDM 通信の機密性と完全性を保持するようなセキュアなプロトコルを利用する。ST 作成者は、TOE によってサポートされるメカニズムを選択する。「IPsec」が選択される場合、IPsec VPN クライアントの拡張パッケージが ST に含まれなければならない(must)。「SSH」が選択される場合、Secure Shell の拡張パッケージが ST に含まれなければならない(must)。「TLS」または「TLS/HTTPS」が選択される場合、附属書 B の適切な選択ベースの SFR が ST に含まれなければならない(must)。

プロトコル、RBG、証明書検証、アルゴリズム、及び同様のサービスは、プラットフォームが提供するサービスと合致することができる。

保証アクティビティ

TSS

評価者は、分散型 TOE コンポーネントを保護するために利用される方法とプロトコルが記述されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、TOE 管理者の支援で TSS に列挙されたすべてのプロトコルが本要件で規定されたものと一貫していること、及び ST の要件に含まれていることについても確認しなければならない (shall)。

ガイダンス

評価者は、操作ガイダンスにそれぞれのサポートされた方法についての通信パスを確立するための指示が含まれていることを確認しなければならない(shall)。

テスト

テスト 1 : 評価者は、評価作業中に、操作ガイダンスに記述されるとおりに接続をセットアップし、通信が成功することを保証して、それぞれの規定された通信方法を用いて通信がテスト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、それぞれの通信方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

さらなる保証アクティビティが具体的なプロトコルに関連している。

A.1.3 TOE アクセス (FTA)

FTA_TAB.1 TOE アクセスバナー

FTA_TAB.1.1 利用者セッション確立前に、 [*選択 : TSF、TOE ラットフォーム*] は TOE の利用に関する、**管理者が規定する**、勧告的**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)。

保証アクティビティ

TSS

TSS は、バナーがいつ表示されるかについて記述しなければならない (shall)。評価者は、以下のテストについても実行しなければならない (shall) :

テスト

評価者は、通知と同意の警告メッセージを設定するため、操作ガイダンスに従わなければならない(shall)。評価者は、次に 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、通知と同意の警告メッセージが TSS に記述されたそれぞれの場合において表示されることを検証しなければならない(shall)。

A.1.4 高信頼パス／チャネル (FTP)

FTP_ITC.1(2) TSF 間高信頼チャネル (MDM エージェント)

FTP_ITC.1.1(2) TSF は、**[*選択 : TSF、TOE プラットフォーム*]**は、その他の通信チャネルから論理的に区別され、その端点の保証された識別と改変または暴露からのチャネルデータの保護を提供するような、それ自身と IT エンティティの間の高信頼通信チャネルを提供するために**[*選択 : IPsec、SSH、TLS、HTTPS*]**を利用しなければならない(shall)。

適用上の注釈 : *上記要件の必須部分の意図は、TOE と MDM エージェントの間の高信頼チャネルを確立し、維持するため、要件で特定された暗号プロトコルを利用することである。TLS、DTLS または HTTPS のみが本高信頼チャネルにおいて利用される。*

本要件は、任意の監査ログ、モバイルデバイス情報データ(ソフトウェアバージョン、ハードウェアモデル、及びアプリケーションバージョン)、及び MDM エージェントによって収集された、または MDM エージェントから MDM サーバへ送信された設定データの送信が、命令されたとき、または設定可能な感覚で、適切に保護されることを保証することである。MDM エージェントまたは MDM サーバが接続を開始す

ることできる。

高信頼チャネルは、登録された MDM エージェントと MDM サーバ間の通信と登録されていない MDM エージェントと MDM サーバの間の通信の両方を登録操作中に保護する。異なるプロトコルがこれらの２つの接続に利用可能であり、TSS における記述には、この相違について明確化するべきである(should)。

高信頼チャネルは、TLS、DTLS、またはHTTPS をMDM 通信の機密性と完全性を保持するプロトコルとして利用する。ST 作成者は、TOE でサポートされるメカニズムを選択し、次にそれらの選択に対応する附属書 B の詳細な要件がまだ ST に存在していない場合に ST へ複写されることを保証する。

プロトコル、RBG、証明書検証、アルゴリズム、及び同様のサービスは、プラットフォームが提供するサービスと合致することができる。

保証アクティビティ

TSS

評価者は、エージェント-サーバ通信の方法がそれらの通信が保護される方法に沿って、示されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、TSS に列挙されたすべてのプロトコルがリモート TOE 管理者の支援を受けて、要件において規定されたものと一貫していること、及び ST の要件に含まれることについても確認しなければならない(shall)。

ガイダンス

評価者は、MDM エージェントと MDM サーバ間の通信チャネルをそれぞれサポートされる方法について設定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)。

テスト

テスト 1：評価者は、操作ガイダンスに記述されるとおり接続をセットアップし、通信が成功することを保証して、それぞれの規定されたエージェント-サーバ通信方法を用いた通信が、評価作業中に、テストされることを保証しなければならない(shall)。

テスト 2：評価者は、それぞれのエージェント-サーバ通信の方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

テスト 3：評価者は、MDM サーバとのそれぞれの通信チャネルについて、プロトコルアナライザがテストかにあるプロトコルとしてトラフィクを特定することを保証しなければならない(shall)。

A.2 オプション TOE またはプラットフォーム要件

A.2.1 セキュリティ監査 (FAU)

FAU_SAR.1 **監査レビュー**

FAU_SAR.1.1 **[*選択：TSF、TOE プラットフォーム*]** は、監査記録から[*すべての監査データ*]を読み出す能力を[*許可された管理者*]へ提供しなければならない(shall)。

FAU_SAR.1.2 **[*選択：TSF、TOE プラットフォーム*]** は、**許可された管理者**が情報を解釈するために適したやり方で監査記録を提供しなければならない(shall)。

適用上の注釈： *本要件の意図は、管理者が監査記録を閲覧し解釈できることを保証すること、及び許可されない利用者のログへのアクセスを防止することである。*

保証アクティビティ

ガイダンス

評価者は、AGD ガイダンスをチェックして、管理者が監査データへアクセスする方法が記述され、また監査記録のフォーマットが記述されていることを保証しなければならない(shall)。

テスト

評価者は、許可された管理者として監査記録の閲覧を試行し、そのアクションが成功することを検証しなければならない(shall)。評価者は、テスト中に生成された監査記録が管理者ガイドで規定されたフォーマット合致することを保証しなければならない(shall)。

A.2.2 暗号サポート (FCS)

FCS_認証パス.1 TLS クライアントプロトコル

FCS_認証パス.1.1 [*選択：TSF、TOE プラットフォーム*] は、以下の暗号スイートをサポートする TLS 1.2 (RFC 5246) 及び [選択：TLS 1.0 (RFC *3246)*、*TLS1.1 (RFC 4346)*、*その他のバージョンなし*]を実装しなければならない(shall)：

- 必須の暗号スイート：[*選択：*
  - *RFC 5246 で定義される TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 で定義される TLS_RSA_WITH_AES_256_CBC_SHA256*]
- オプションの暗号スイート：[*選択：*
  - *RFC 5246 で定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 で定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *その他の暗号スイートなし*]。

適用上の注釈： *TLS クライアントは、TOE の MDM エージェントに対して要求され、セキュアトランスポートを介して登録をサポートするために MDM サーバに含まれてもよい(附属書 C.2.2)。*

評価される構成でのテストされるべき暗号スイートは、本要件によって限定される。暗号スイート TLS_RSA_WITH_AES_128_CBC_SHA を RFC 5246 が必須としていることが認識されているが、この暗号スイートは、本要件ではテストされない。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るべきである(should)；必須のスイート以外にサポートされる暗号スイートがない場合、「その他の暗号スイートなし」が選択されるべきである(should)。テスト環境のサーバ上で評価される構成で管理者が利用可能な暗号スイートを限定する必要がある。上記の列挙されたスイート B アルゴリズム(RFC6460)は、実装されることが望ましいアルゴリズムである。

これらの要件は、IETF によって規格化される新しい TLS バージョンで見直しが行われる。ECDHE を用いる暗号スイートが選択される場合、FCS_認証パス.3(訳注:FCS_認証パス.1.3 の間違い)が要求される。

保証アクティビティ

TSS

評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS の本プロトコルの実装の記述をチェックしなければならない(shall)。評価者は、規定された暗号スイートが本コンポーネントについて列挙されたものを含むことを保証するため、TSS をチェックしなければならない(shall)。評価者は、TLS が TSS の記述に適合するように TOE の設定についての指示が操作ガイダンスに含まれることを保証するため、操作ガイダンスについてもチェックしなければならない(shall)。エージェントが複数のプラットフォームをサポートする場合、ST は TLS 実装における相違を明確にしなければならない(shall)。

テスト

テスト 1：評価者は、本要件によって規定される暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない(shall)。本接続は、より上位レベルのプロトコルの確立の一部として確立されてもよい、冷、EAP セションの一部として。本テスト意図を満たすために暗号スイートのネゴシエーションに成功したことを観測すれば十分である；利用されている暗号スイートの識別の試行における暗号化トラフィクの特性を検査する必要はない(例えば、暗号アルゴリズムが 128 ビット AES であり 256 ビット AES でないこと)。

テスト 2：評価者は、extendedKeyUsage フィールドにサーバ認証目的を含むようなサーバ証明書を持つサーバを利用して接続の確立を試行し、接続が確立されることを検証しなければならない(shall)。評価者はm次に、extendedKeyUsage フィールドにサーバ認証目的のない別の有効なサーバ証明書をクライアントが拒否すること、及び接続が確立されないことを検証すること。理想的には、2 つの証明書が extendedKeyUsage フィールド以外は同一であるべきである。

テスト 3：評価者は、サーバが選択した暗号スイートと合致しないような(例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを用いる際に ECDSA 証明書を送信するまたは ECDSA 暗号スイートの 1 つを用いる際に RSA 証明書を送信する)TLS 接続におけるサーバ証明書を送信し

なければならない(shall)。評価者は、サーバの証明書ハンドシェイクメッセージを受信した後に、TOE が切断することを検証しなければならない(shall)。

テスト 4：評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートを選択するようサーバを設定し、クライアントが接続を拒否することを検証しなければならない(shall)。

テスト 5：評価者は、トラフィクに対して以下の改変を実行しなければならない(shall)：

- Server Hello でサーバによって選択された TLS バージョンを非サポートの TLS バージョン(例えば 2 バイト 03 04 で表される 1.3)に変更し、クライアントが接続を拒否することを検証する。
- Server Hello ハンドシェイクメッセージでサーバのノンスの少なくとも 1 バイトを改変し、クライアントが Server Key Exchange ハンドシェイクメッセージを拒否すること(DHE または ECDHE 暗号スイートを使用する場合)またはサーバがクライアントの Finished ハンドシェイクを拒否することを検証する。
- サーバの Key Exchange ハンドシェイクメッセージの署名ブロックを改変し、クライアントが Server Key Exchange メッセージを受信後に接続を拒否することを検証する。
- Server Finished ハンドシェイクメッセージで 1 バイトを会は遠視、クライアントが樹脂時に致命的なアラートを送信し、アプリケーションデータを送信しないことを検証する。
- 平文の有効な Server Finished メッセージを送信し、クライアントが致命的なアラートを送信しアプリケーションデータを送信しないことを検証する。サーバの finished メッセージは、有効な検証データを含まなければならなず(shall)、ネットワーク分析ツールを用いて正しく解析しなければならない(shall)。

FCS_認証パス.1.2 [*選択：TSF、TOE プラットフォーム*]は、提示された識別子が RFC 6125 に従う参照識別子と合致することを検証しなければならない(shall)。

適用上の注釈： *識別検証の規則は、RFC6125 のセクション 6 に記述されている。参照識別子は、アプリケーションサービスに依存して、利用者によって(例、ウェブブラウザへの URL 入力またはリンクのクリック)、設定によって(例、メールサーバまたは認証サーバの名前の設定)、またはアプリケーションによって(例、API のパラメタ)確立される。単一の参照識別子のソースドメインとアプリケーションサービスタイプ(例、HTTP、SIP、LDAP) に基づき、クライアントは、証明書の Subject Name フィールドの Common Name 及び(機微でない場合)Subeject Alternative Name フィールドの DNS name、URI name、及び Service name のような、すべての受け入れ可能な参照識別子を確立する。次にクライアントは、このすべての受け入れ可能な参照識別子のリストを TLS サーバの証明書にある提示された識別子と比較する。*

望ましい検証方法は、DNS name、URI name、または Service Name を用いる Subject Alternative Name である。Common Name を用いる検証は、後方互換の目的で要求される。さらに、Subject Name または Subject Alternative Name での IP アドレスの利用のサポートは、ベストプラク

ティスに反するものとして推奨されないが、実装されてもよい。最後に、クライアントは、ワイルドカードを用いる参照識別子を構築することは回避するべきである(should)。しかし、提示された識別子にワイルドカードが含まれる場合、クライアントは、照合に関するベストプラクティスに従わなければならない(must)；これらのベストプラクティスは、保証アクティビティに取り込まれている。ワイルドカードが受け入れられない場合、保証アクティビティで列挙されたワイルドカードシナリオと共に提示されたサーバ証明書が接続を拒否することを実証すれば十分である。

保証アクティビティ

TSS

評価者は、どのタイプの参照識別子がサポートされるか(例、Common Name、DNS Name、URI Name、Service Name、またはその他のアプリケーション特有の Subject Alternative Name)及び IP アドレスとわ瓜度カードがサポートされるかどうかを含めて、利用者／管理者／アプリケーション設定された参照識別子からのすべての参照識別子を確立するクライアントの方法について TSS に記述されていることを保証しなければならない(shall)。評価者は、本記述が TOE によってサポートされるかまたは利用される証明書のピン留めのようなやり方を特定することを保証しなければならない(shall)。

ガイダンス

評価者は、AGD ガイダンスに TLS での証明書検証の目的で利用されるべき参照識別子をセットするための指示が含まれることを検証しなければならない(shall)。

テスト

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

テスト 1：評価者は、参照識別子と合致する ternative Name(SAN)または Common Name(CN) のいずれかにおける識別子を含まないようなサーバ証明書を提示しなければならない(shall)。評価者は、接続が失敗することを検証しなければならない(shall)。

テスト 2：評価者は、参照識別子と合致し、SAN 拡張を含むが、参照識別子にがあ値する SAN 内の識別を含まないような、CN を含むサーバ証明書提示しなければならない(shall)。評価者は、接続が失敗することを検証しなければならない(shall)。評価者は、それぞれのサポートされた SAN タイプについての本テストを繰り返さなければならない(shall)。

テスト 3：評価者は、参照識別子と合致する CN を含み、SAN 拡張を含まないサーバ証明書を提示しなければならない(shall)。評価者は、接続が成功することを検証しなければならない(shall)。

テスト 4：評価者は、参照識別子と合致しない CN を含むが、合致す rSAN における識別を含むサーバ証明書を提示しなければならない(shall)。評価者は接続が成功することを検証しなければならない(shall)。

テスト 5：評価者は、以下のワールドカードテストをそれぞれのサポートされる参照識別子を用いて実行しなければならない(shall)：

- 評価者は、提示された識別子の左端のラベルでないところにワイルドカードを含む(例、foo.*.example.com)サーバ証明書を提示し、接続が失敗することを検証しなければならない(shall)。
- 評価者は、左端にワイルドカードを含むが公開サフィクスに先立っていないような(例、*.example.com)サーバ証明書を提示しなければならない(shall)。評価者は、証明書に単一の左端のラベルを持つ(例、foo.example.com)参照識別子を設定し、接続が成功することを検証しなければならない(shall)。評価者は、証明書の左端のラベルなし(例、example.com)参照識別子を設定し、接続が失敗することを検証しなければならない(shall)。評価者は、左端に 2 つのラベルを持つ(例、bar.foo.example.com)参照識別子を設定し、接続が失敗することを検証しなければならない。
- 評価者は、公開サフィクスの直前の左端ラベルにワイルドカードを含む(例、*.com)サーバ証明書を提示しなければならない(shall)。評価者は、単一の左端ラベルを持つ(例、foo.com)参照識別子を設定し、接続が失敗することを検証しなければならない(shall)。評価者は、２つの左端ラベルを持つ(例、bar.foo.com)参照識別子を設定し、接続が失敗することを検証しなければならない(shall)。

テスト 6 : [条件付き] URI または Service Name 参照識別子がサポートされる場合、評価者は、DNS name とサービス識別子を設定しなければならない(shall)。評価者は、SAN の URI Name または SRV Name フィールドに正しい DNS name 名とサービス識別子を含むサーバ証明書を提示し、接続が成功することを検証しなければならない(shall)。評価者は、間違ったサービス識別子(しかし、正しい DNS name)を用いてこのテストを繰り返し、接続が失敗することを検証しなければならない(shall)。

テスト 7 : [条件付き] ピン留めされた証明書がサポートされる場合、評価者は、ピン留めされた証明書と合致しない証明書を提示し、接続が失敗することを検証しなければならない(shall)。

FCS_認証パス.1.3 [選択：TSF、TOE プラットフォーム]は、ぴあ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。

適用上の注釈： *有効性は識別子検証、認証パス、有効期限、及び RFC 5280 に従う失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1 のために実行されるテストに従ってテストされなければならない(shall)。*

TLS 接続について、本チャネルは、ピア証明書が無効である場合、確立されてはならない(shall)。

保証アクティビティ

テスト

評価者は、FIA_X509_EXT.1.1 の検証規則が忠実に守られることを検証する機能として TLS を利用し、以下の追加のものを実行しなければならない(shall)

テスト 1 : 評価者は、有効な認証パスを持たない証明書を用いるピアが認証失敗をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、評価者は次にピア証明書を検証するために必要とされる信頼された CA 証明書をロードし、接続が成功することを実

証しなければならない(shall)。評価者は、次に CA 証明書の 1 つを削除し、接続が失敗することを示さなければならない(shall)。

FCS_認証パス.1.4 [*選択：TSF、TOE プラットフォーム*] は、X.509v3 証明書を用いて相互認証をサポートしなければならない(shall)。

適用上の注釈： *TLS の X.509v3 証明書の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、クライアントが TLS 相互認証のために TLS サーバへ証明書を提示できなければならないことをこの用途に含まなければならないことを追加する。相互認証は、登録が TLS を利用するとしても、デバイス登録のために要求されない。しかし、登録後の MDM サーバとエージェントの間のすべての通信は相互認証を利用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、FIA_X509_EXT.2.1 毎に要求される TSS 記述に TLS 相互認証のためにクライアント側の証明書の利用が含まれていることを保証しなければならない(shall)。

ガイダンス

評価者は、FIA_X509_EXT.2.1 毎に要求される AGD ガイダンスに TLS 相互認証のためのクライアント側証明書を設定するための指示が含まれ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、トラフィクへの以下の改変を実行しなければならない(shall)：

- 相互認証を要求するためにサーバを構成し、次にサーバの証明書要求ハンドシェイクメッセージの CA フィールドの 1 バイトを改変する。改変された CA フィールドがクライアントの証明書に署名するために資料される CA であってはならない(must not)。評価者は、接続が成功しないことを検証しなければならない(shall)。

A.3 MAS サーバをサポートするためのオプション要件

A.3.1 セキュリティ監査 (FAU)

FAU_GEN.1(2) 監査生成 (MAS サーバ)

FAU_GEN.1.1(2) **MAS サーバ**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)：

a. **管理されたモバイルデバイス上の新しいアプリケーションのプッシュを失敗する；**
b. **管理されたモバイルデバイス上の既存のアプリケーションのアップデートを失敗する。**

適用上の注釈： *MDM エージェントは、アプリケーションの受信の成功、または管理されたモバイルデバイスのアップデートの成功に際して MAS サーバ*

へ報告することが要求され、失敗がこのような警告の欠如から推測される。

保証アクティビティ
TSS

評価者は、TSS をチェックし、TSS が監査記録のフォーマットを提供することを保証しなければならない(shall)。

ガイダンス

評価者は、管理者ガイダンスをチェックし、管理者ガイダンスが監査記録のフォーマットを提供していることを保証しなければならない(shall)。それぞれの監査記録フォーマットタイプがそれぞれのフィールドの概説と共に網羅されなければならない(must)

テスト

評価者は、いつアプリケーションまたはアップデートプッシュが失敗するか、生成された監査記録がガイダンスで規定されたフォーマットと合致すること、及びそれぞれの監査記録のフィールドが正しい辺取りを持っていることを検証しなければならない(shall)。

FAU_GEN.1.2(2) **[*選択：MAS サーバ、MAS サーバプラットフォーム*]**は、少なくとも以下の情報をそれぞれの TSF 監査記録内に記録しなければならない(shall)：

- 事象の日付と時刻、
- 事象の種別、
- **モバイルデバイスの識別、**
- [割付：その他の監査関連情報]。

適用上の注釈： *すべての監査には、少なくとも FAU_GEN.1.2 で述べられた情報を含まなければならない(shall)が、割付可能なさらなる情報を含んでもよい。ST 作成者は、TSS で監査記録のどの情報が TSF によって実行されるか及びどれが TOE プラットフォームによって実行されるものかを特定しなければならない(shall)。*

保証アクティビティ
TSS

評価者は、監査データが会部の監査サーバへ転送される手段、及び高信頼チャネルが提供される方法について記述していることを保証するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、ローカル監査データと監査ログサーバへ送信された監査データの間の関係について操作ガイダンスに記述されていることを決定するため、操作ガイダンスを検査しなければならない(shall)。例えば、いつ監査事象が生成されたか、外部サーバとローカルストアへ同時に

送信されたか、またはローカルストアはバッファとして利用され、監査サーバへデータを送信することによって周期的に「消去」されるか。

テスト

高信頼チャネルのテストは、特定の高信頼チャネルメカニズムの関連する保証策てぃびてぃにおいて規定されるとおり実行される。

評価者は、本要件について、以下のテストを実行しなければならない(shall)：

テスト：評価者は、提供された設定ガイダンスに従って、TOE と監査サーバの間でセションを確立しなければならない(shall)。評価者は、次に、監査サーバへ転送される監査データを生成するよう設計された評価者の選択によるいくつかのアクティビティの間に、監査サーバとTOE の間を通過するトラフィクを検査しなければならない(shall)。評価者は、これらのデータがこの転送中に明確に閲覧できないこと、及びそれらが監査サーバによってうまく受信されることを観測しなければならない(shall)。評価者は、テスト中に監査サーバで利用される特定のソフトウェア(名称、バージョン)を記録しなければならない(shall)。

A.3.2 セキュリティ管理 (FMT)

FMT_MOF.1(3) 機能の管理 (MAS サーバ)

FMT_MOF.1.1(3) **MSA サーバ**は、**利用者アクセスについての利用者グループを設定する**能力を**この機能を実行する管理者だけに許可する具体的なアプリケーション**に制限しなければならない(shall)。

適用上の注釈： *本要件は、MAS サーバが所属するグループに基づいて利用者が度のアプリケーションにアクセスできるかを設定するグループを作成できることを保証するものである。MAS サーバは、MDM によって定義されたグループを利用する場合、それは利用者がアクセスできるアプリケーションを決定するために MDM サーバ(別のサーバの場合)と通信しなければならない(must)。*

保証アクティビティ
TSS

評価者は、MAS サーバが自身のグループを作成するか、MDM サーバによって規定されるグループに頼るかを決定するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスに作成方法について含まれ、利用者グループ及びそのグループによって度のアプリケーションがアクセス可能かを規定する方法を定義することを確認しなければならない(shall)。

テスト

評価者は、MAS クライアントが彼らが登録されているグループに規定

されたアプリケーションのみをアクセスできることを保証しなければならない(shall)。評価者は、利用者グループを作成しなければならない(shall)、そしてその利用者がそのグループの一部として定義しない。そのグループにアクセスできるアプリケーションがアクセスできないことを検証する。評価者は、グループにその利用者を含め、アプリケーションがアクセス可能であることを保証しなければなければならない(shall)。

FMT_MOF.1(4)　機能の管理 (MAS サーバダウンロード)

FMT_MOF.1.1(4)　**MSA サーバ**は、**アプリケーションをダウンロードする**能力を **MDM ポリシーに適合しこの機能を実行するアプリケーションアクセスグループの利用者に指定された登録されたモバイルデバイスのみに許可する許可するよう**に制限しなければならない(shall)。

保証アクティビティ
TSS

評価者は、アプリケーションダウンロードまたはアップデートプッシュを開始するためのすべての方法が規定されることを決定するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスにアプリケーションダウンロードまたはアップデートプッシュの開始方法について含まれていることを確認しなければならない(shall)。

テスト

評価者は、MAS クライアントが、モバイルデバイスが MDM サーバに登録され、適合状態にあることを検証することを保証しなければならない(shall)。評価者は、MDM にデバイスを登録する前に、アプリケーションが MAS サーバからダウンロードできないことを検証しなければならない(shall)。評価者は、デバイスが MDM サーバに接続されるが適合していように、モバイルデバイスを部分的に登録しなければならない(shall)、そしてアプリケーションがダウンロードできないことを検証しなければならない(shall)。

FMT_SMF.1(3)　機能の特定 (MAS サーバ)

FMT_SMF.1.1(3)　**MSA サーバ**は、以下の管理機能を**実行**できなければならない(shall)：

a. アプリケーションアクセスグループを設定する、
b. アプリケーションをダウンロードする、
c. [*選択：[割付：その他の MAS 管理機能]、その他の機能なし*]。

適用上の注釈：　*本要件は、基礎とする MAS サーバを設定するため、MAS サーバにおけるすべての設定機能を取り込む。ST 作成者は、割付ステートメントを完成することによってさらなるコマンドと設定ポリシーを追加できる。*

保証アクティビティ
TSS

評価者は、列挙されたそれぞれの管理機能が TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、どのオプションが利用可能か、及び列挙されたそれぞれの管理機能の能力を設定する方法についての詳細な指示について AGD 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)。

テスト

機能のテストは、FMT_MOF.1 における機能の制限と併せて実行される。

FMT_SMR.1(2)　セキュリティ管理役割 (MAS サーバ)

FMT_SMR.1.1(2)　**MSA サーバ**は、役割 [*管理者、MD 利用者、登録されたモバイルデバイス、アプリケーションアクセスグループ、及び[割付：追加の許可された特定された役割]* を維持しなければならない(shall)。

FMT_SMR.1.2(2)　**MSA サーバ**は、利用者を役割に関連付けられなければならない(shall)。

適用上の注釈：　*MAS サーバが異なる利用者役割によって設定され、維持されることが予見される。サポートされる役割を列挙するために ST 作成者によって割付が利用される。追加の役割なしがサポートされる場合、「追加の役割なし」が記述される。ND 利用者役割が FIA_ENR_EXT.1 に従ってモバイルデバイスの MAS への登録に利用される。*

保証アクティビティ
TSS

評価者は、管理者役割及びその役割に与えられている権限と制限について TSS に記述されていることを検証するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、TOE を管理するための指示及びどのインタフェースがサポートされるかについて操作ガイダンスに含まれていることを保証するため、操作ガイダンスをレビューしなければならない(shall)。

テスト

評価のテストアクティビティの実行において、評価者は、すべてのサポートされるインタフェースを利用しなければならない(shall)、しかし、それぞれのインタフェースに管理者アクションを含めるようなそれぞれのテストを繰り返す必要はない。評価者は、本 PP の要件に適合するような TOE を管理するためのそれぞれのサポートされる方法

がテストされることを保証しなければならない(shall)；例えば、TOE がローカルインタフェースまたは TLS/HTTPS を通して管理可能である場合、管理方法は、評価チームのテストアクティビティ中に検査されなければならない(shall)。

A.3.3 高信頼パス／チャネル (FTP)

FTP_ITC.1(3)　TSF 間高信頼チャネル (MAS サーバ)

FMT_ITC.1.1(3)　**[*選択：MSA サーバ、MAS サーバプラットフォーム*]**は、それ自身と**以下の機能をサポートする許可された IT エンティティ**の間の**高信頼**通信チャネルを提供するため**[*選択：IPsec、SSH、TLS、TLS/HTTPS*]を利用**しなければならない(shall)：**監査サーバ、[*選択：認証サーバ、[割付：その他の機能]*]**で、その他の通信チャネルから論理的に区別され、その端点の保証された識別と改変または暴露からのチャネルデータの保護を提供するもの。

適用上の注釈：　*上記要件の必須部分の意図は、MAS サーバがその機能を実行するために対話するような、許可された IT エンティティとの高信頼チャネルを確立し、維持するために、本要件で特定された暗号プロトコルを利用することである。*

(列挙されたプロトコルの 1 つによる) 保護は、少なくとも監査情報を収集するようなサーバとの通信のために要求される。認証サーバ(例、RADIUS)と通信する場合、ST 作成者は、FTP_ITC.1.1(1) で「認証サーバ」を選択し、本接続は、列挙されたプロトコルの 1 つによって保護されなければならない(shall)。その他の許可された IT エンティティ(例、NTP サーバ)が保護される場合、ST 作成者は、適切な割付(それらのエンティティのため)と選択(それらの接続を保護するために利用されるプロトコルのため)を行う。

要約するため、外部監査収集サーバへの接続は、列挙されたプロトコルの 1 つによって保護されることが要求される。外部認証サーバがサポートされる場合、列挙されたプロトコルの 1 つを用いてその接続を保護することが要求される。任意のその他の外部サーバについて、外部通信は、保護されることは要求されないが、保護が主張される場合、特定されたプロトコルの一つを用いて保護されなければならない(shall)。

高信頼チャネルは、MAS 通信の機密性と完全性を保護するプロトコルとして、IPsec、TLS、DTLS、または HTTPS を利用する。ST 作成者は、TOE によってサポートされるメカニズムを選択する。「IPsec」が選択される場合、IPsec VPN クライアントの拡張パッケージが ST に含まれなければならない(must)。「SSH」が選択される場合、Secure Shell の拡張パッケージが ST に含まれなければならない(must)。「TLS」または「TLS/HTTPS」が選択される場合、附属書 B の適切な選択ベースの SFR が ST に含まれなければならない(must)。

プロトコル、RBG、証明書検証、アルゴリズム、及び同様のサービスは、プラットフォームが提供するサービスと合致することができる。

本要件は、初期に通信が確立されるとき保護される通信であるだけでなく、停電後の再開についても暗黙的に適用される。何らかの TOE セットアップにその他の通信を保護するためのトンネルの手動セットア

ップを服ような場合があるかもしれない、停電後に TOE が(必須の)手動の介入と共に自動的に通信の再確立を試行する場合、攻撃者が重要な情報を取得または接続を危殆化できるかもしれないように作成された窓があるかもしれない。

FTP_ITC.1.2(1) TSF は、高信頼チャネルを介して通信の開始を **MAS サーバまたはその他の許可された IT エンティティ**に許可しなければならない(shall)。

FTP_ITC.1.3(1) TSF は、[*割付：TSF が通信を開始できるようなサービスのリスト*]のための高信頼チャネルを介して通信を開始しなければならない(shall)。

適用上の注釈： *通信を開始する者についての要件はないが、ST 作成者は FTP_ITC.1.3 の割付、TOE が許可された IT エンティティとの通信を開始できるようなサービスに列挙する。*

保証アクティビティ

TSS

評価者は、許可された IT エンティティとの通信方法が通信の保護方法と共に示されていることを決定するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスに MDM サーバと許可された IT エンティティの間の通信チャネルをそれぞれのサポートされる方法について設定する指示が含まれていることを確認しなければならない(shall)。

テスト

テスト 1：評価者は、評価作業中に、操作ガイダンスに記述されるとおりに接続をセットアップし、通信が成功することを保証して、それぞれの (操作ガイダンスにおいて) 規定された通信方法がテスト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、それぞれの通信方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

テスト 3：評価者は、MDM サーバとのそれぞれの通信チャネルについて、テスト中のプロトコルとしてプロトコルアナライザがそのトラフィクを特定することを保証しなければならない(shall)。

さらなる保証アクティビティが具体的なプロトコルに関連している

B. 選択ベース要件

本 PP の序論で示したように、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取り込まれることが必要となる。

B.1 選択ベース TSF 要件

B.1.1 セキュリティ監査 (FAU)

FAU_STG_EXT.2 監査事象ストレージ

FAU_STG_EXT.2.1 [*選択 : TSF、TOE プラットフォーム*] は、監査証跡に保存された監査記録を許可されない改変から保護しなければならない(shall)。

適用上の注釈 : *「ローカルに格納される」が FAU_STG_EXT.1.1(1) で選択される場合、本 SFR は、ST に含まれなければならない(shall)。*

本要件の意図は、監査記録がセキュアに保存されることを確実にすることである。ST 作成者は、監査ストレージまたは故障が発生した際に監査記録が維持されるのかどうかを選択する責任を負う。ST 作成者は、監査記録が保存される手段を選択し、また記録が保存される事象を選択しなければならない (must)。TSF はこの機能を基盤となるオペレーティングシステムに依存してもよく、その場合には最初の選択が適切に行われるべきである (should)。

保証アクティビティ

TSS

評価者は、監査記録が許可されない改変または削除から保護される方法が 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、TOE が監査証跡に特有な保護メカニズムを利用することを保証しなければならない (shall)。

テスト

評価者は、以下のテストを実行しなければならない(shall) :

テスト 1 : 評価者は、許可されない利用者として監査証跡へアクセスし、監査記録の改変及び削除を試行しなければならない(shall)。評価者は、これらの試行が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、許可された利用者として監査証跡へアクセスし、監査記録の改変及び削除を試行しなければならない(shall)。評価者は、これらの試行が成功することを検証しなければならない(shall)。評価者は、改変及び削除を意図した記録のみが改変及び削除されることを検証しなければならない (shall)。

B.1.2 暗号サポート (FCS)

FCS_DTLS_EXT.1 拡張 : DTLS の実装

FCS_DTLS_EXT.1.1 [*選択 : TSF、TOE プラットフォーム*] は、 DTLS 1.2 (RFC 6347)に従

って DTLS プロトコルを実装しなければならない(shall)。

FCS_DTLS_EXT.1.2 [*選択：TSF、TOE プラットフォーム*]は、 DTLS 1.2 (RFC 6347) に従って許容される変形を除き、DTLS の実装については TLS (FCS_TLS_EXT.1) の要件を実装しなければならない(shall)。

適用上の注釈： *DTLS 1.2 と TLS 1.2 との違いは、RFC 6347 に概説されている；それ以外の点では、これらのプロトコルは同じである。特に、TSF のために定義された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 のために列挙されたすべての適用上の注釈と保証アクティビティは、DTLS の実装に適用される。*

FCS_DTLS_EXT.1.3 [*選択：TSF、TOE プラットフォーム*]は、 ピア証明書が無効と思われる場合には、高信頼通信チャネルを確立してはならない(shall not)。

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

保証アクティビティ

テスト

テスト 1：評価者は、DTLS サーバとのコネクションの確立を試行し、パケットアナライザを用いてトラフィクを観測し、接続が成功したこと及びトラフィクが DTLS として特定されることを検証しなければならない(shall)。
その他のテストは、FCS_TLSS_EXT.1 のために列挙された保証アクティビティと併せてテストされなければならない(shall)、また評価者は以下のテストを実行しなければならない(shall)。

テスト 2：評価者は、有効な認証パスを持たない証明書を用いて、機能が失敗をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、評価者は、その機能で利用されるべき証明書を検証する必要があるトラストアンカーデータベースへ証明書をロードし、機能が成功することを実証しなければならない(shall)。評価者は、次に証明書の 1 つを削除し、機能が失敗することを示さなければならない(shall)。

FCS_HTTPS_EXT.1 HTTPS プロトコル

FCS_HTTPS_EXT.1.1 [*選択：TSF、TOE プラットフォーム*]は、RFC 2818 に適合する HTTPS プロトコルを実装しなければならない(shall)。

FCS_HTTPS_EXT.1.2 [*選択：TSF、TOE プラットフォーム*] は、FCS_TLSS_EXT.1 で規定される TLS を用いて HTTPS を実装しなければならない(shall)。

FCS_HTTPS_EXT.1.3 [*選択：TSF、TOE プラットフォーム*] は、ピア証明書が無効と思われる場合、[*選択：接続を確立しない、接続を確立するための許可を要求する、その他のアクションなし*]を実行しなければならない(shall)。

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

保証アクティビティ

テスト

テスト 1：評価者はウェブサーバとの HTTPS 接続の確立を試行し、パケットアナライザを用いてトラフィクを観測し、接続が成功すること及びトラフィクが TLS または HTTPS として特定されることを検証しなければならない(shall)。

その他のテストは、TLS 評価アクティビティと併せて実行される。

証明書有効性は、FIA_X509_EXT.1 のために実行されるテストに従ってテストされなければならない(shall)、また評価者は、以下のテストを実行しなければならない(shall)：

テスト 2：評価者は、認証パスを持たない証明書を用いて、アプリケーション通知をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、次に評価者は、有効な証明書と認証パスをロードし、機能が成功することを実証しなければならない(shall)。評価者は、次に証明書のうち 1 つを削除し、ST に列挙された選択が発生することを示さなければならない(shall)。

FCS_IV_EXT.1　初期化ベクタの生成

FCS_IV_EXT.1.1　[*選択：TSF、TOE プラットフォーム*]は、表 3 に従って IV を生成しなければならない (shall)。

適用上の注釈：　*本要件は、FCS_STG_EXT.2 が ST に含まれる場合、ST に含まれていなければならない(must)、FCS_STG_EXT.1 における選択が TSF がプライベート鍵及び永続的な秘密をプラットフォームが提供する鍵ストレージというよりはむしろ暗号化を用いて保護していることを示していることを意味する。*

表 3 には、それぞれの暗号モードについて、対応する NIST Special Publications に従った IV の作成に関する要件が列挙されている。暗号プロトコルに従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処される。したがって、本要件は鍵ストレージ暗号化のために生成される IV にのみに対処する。

暗号モード	**参照**	**IV 要件**
Electronic Codebook (ECB)	SP 800-38A	IV なし
Counter (CTR)	SP 800-38A	「内部カウンタ」は一切繰り返ししてはならない(shall not)。カウンタの値は、同じ秘密鍵を用いて複数のメッセージで繰り返ししてはならない(shall not)。
Cipher Block Chaining (CBC)	SP 800-38A	IV は予測可能であってはならない(shall not)。IV の繰り返しは、2 つのメッセージの間で最初のブロックまたはそれ以上のブロックが共有されるかどうかについての情報を漏えいするので、IV は、このような場合には繰り返しするべきではない(should not)。

Output Feedback (OFB)	SP 800-38A	IV は繰り返ししてはならない、かつ別の IV で暗号を起動することによって生成されてはならない(shall not)。
Cipher Feedback (CFB)	SP 800-38A	IV は繰り返ししてはならない、IV の繰り返しは、最初の平文ブロックについて及びメッセージの共通の共有プレフィクスについての情報を漏えいする。
XEX (XOR Encrypt XOR)	SP 800-38E	IV なし。Tweak 値は、非負の整数でなければならず、連続的に割り当てられ、任意の非負の整数から始まる。
Cipher-based Message Authentication Code (CMAC)	SP 800-38B	IV なし
Key Wrap and Key Wrap with Padding	SP 800-38F	IV なし
Counter with CBC－Message Authentication Code (CCM)	SP 800-38C	IV なし。ノンスは、繰り返ししてはならない(shall not)。
Galois Counter Mode (GCM)	SP 800-38D	IV は、繰り返ししてはならない(shall not)。GCM の起動回数は、96 ビット IV(デフォルト長)のみを利用することなしに、所与の秘密鍵について 2^32 を超えてはならない(shall not)。

表 3：NIST 承認された暗号モードの参照と IV 要件

保証アクティビティ

TSS

評価者は、利用者クレデンシャル、永続的秘密、及びプライベート鍵の暗号化及びその暗号化のために用いられる IV の生成について記述されていることを保証するため、TSS を検査しなければならない(shall)。

テスト

評価者は、同じ KEK によって暗号化されるそれぞれの鍵の IV の生成が表 3 を満たすことを保証しなければならない(shall)。

FCS_STG_EXT.2　暗号化された暗号鍵ストレージ

FCS_STG_EXT.2.1　[*選択：TSF、TOE プラットフォーム*]は、[*選択：Key Wrap (KW)モード、Key Wrap with Padding (KWP)モード、GCM、CCM、CBC モード*]で AES を用いてすべての鍵を暗号化しなければならない(shall)。

適用上の注釈：　*本要件は、TSF によって利用される鍵は平文で保持されてはならないことを述べている。本要件の意図は、攻撃者に AES 鍵空間を総当たり攻撃することなしに鍵のアクセスを許してしまうような、プライベート鍵、クレデンシャル、永続的な秘密が暗号化されない状態で TOE*

においてアクセスできないことを保証することである。

本要件は、プラットフォームが提供する鍵ストレージでではなく、むしろ、TSF が暗号化を用いてプライベート鍵と永続的な秘密を保護していることを FCS_STG_EXT.1 の選択が示す場合、ST に含まれなければならない(must)。

本要件が ST に含まれる場合 FCS_IV_EXT.1 についても含まれなければならない(must)。

保証アクティビティ

TSS

評価者は、利用者クレデンシャル、永続的秘密、及びプライベート鍵が保存され暗号化される方法が詳細に記述されていることを保証するため、TSS を検査しなければならない (shall)。評価者は、鍵材料が暗号化されずに永続的なメモリに書き込まれないこと及び暗号化のモードが特定されていることを決定するために TSS をレビューしなければならない(shall)。

FCS_認証パス.1 TLS クライアントプロトコル—楕円曲線拡張

FCS_認証パス.1.5 [*選択：TSF、TOE プラットフォーム*]は、以下の NIST 曲線[*選択：secp256r1、secp384r1、secp521r1*]及びその他の曲線なしを用いて Client Hello の Supported Elliptic Curves Extension を提示しなければならない(shall)。

適用上の注釈： *本要件は、認証及び鍵共有のために許可される楕円曲線を FCS_COP.1(3)、FCS_CKM.1、及び FCS_CKM.2 からの NIST 曲線に制限する。本拡張は、クライアントがサポートする楕円曲線暗号スイートのために要求される。*

保証アクティビティ

TSS

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

ガイダンス

Supported Elliptic Curves Extension が要件を満たすために設定されなければならない(must)ことを TSS が示している場合、評価者は、AGD ガイダンスに Supported Elliptic Curves Extension の設定を含んでいることを検証しなければならない(shall)。

テスト

テスト 1：評価者は、サポートされていない ECDHE 曲線(例えば、P-192)を用いた TLS 接続の ECDHE 鍵交換メッセージを実行するようサーバを設定しなければならない(shall)、そして、TOE がサーバの鍵交換ハンドシェイクメッセージを受信した後に、接続を切断すること

を検証しなければならない(shall)。

FCS_TLSS_EXT.1 TLS サーバプロトコル

FCS_TLSS_EXT.1.1 [*選択：MDM サーバ、MDM サーバプラットフォーム*]は、TLS 1.2（RFC 5246）及び[*選択：TLS 1.0 (RFC 2246)、 TLS 1.1 (RFC 4346)、その他のバージョンなし*]を以下の暗号シートをサポートして実装しなければならない(shall)：

- 必須の暗号スイート：[*選択：*
  - o *RFC 5246 で定義される TLS_RSA_WITH_AES_128_CBC_SHA256*
  - o *RFC 5246 で定義される TLS_RSA_WITH_AES_256_CBC_SHA256*]
- オプションの暗号スイート：[*選択：*
  - o *RFC 5246 で定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
  - o *RFC 5246 で定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
  - o *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - o *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - o *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - o *RFC 5289 で定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - o *その他の暗号スイートなし*]。

適用上の注釈： *MDM サーバは、MDM システムでサポートされるとおり、ST に列挙される評価されたエージェントによってサポートされるすべての TLS のバージョンをサポートしなければならない(must)。*

評価される構成でのテストされるべき暗号スイートは、本要件によって限定される。暗号スイート TLS_RSA_WITH_AES_128_CBC_SHA を RFC 5246 が必須としていることが認識されているが、この暗号スイートは、本要件ではテストされない。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るべきである(should)；必須のスイート以外にサポートされる暗号スイートがない場合、「なし」が選択されるべきである(should)。実装によってネゴシエーションされるスイートが本要件にあるものに制限されるように管理者手順がとられる必要がある場合、適切な指示が AGD_OPE によって求められるガイダンスに含まれる必要がある。FMT_SMF.1 は、接続のために利用される暗号スイートの構成に対処する。上記の列挙されたスイート B アルゴリズム(RFC6460)は、実装されることが望ましいアルゴリズムである。

これらの要件は、IETF によって規格化される新しい TLS バージョンで見直しが行われる。

保証アクティビティ
TSS

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

ガイダンス

評価者は、TLS が TSS の記述(例えば、TOE によって公告された一連の暗号スイートが本要件を満たすように制限されなければならないかもしれない)に適合するように、操作ガイダンスに TOE の設定についての指示が含まれていることを保証するために操作ガイダンスをについてもチェックしなければならない(shall)。

テスト

テスト 1：評価者は、本要件によって規定される暗号スイートのそれぞれを用いた TLS 接続を確立しなければならない(shall)。この接続は、上位レベルのプロトコルの確立の一部として確立されてもよい、冷、EAP セションの一部として。テストの意図を満たすために暗号スイートのネゴシエーションに成功することを観測すれば十分である；利用されている暗号スイートの識別を試行するために暗号化されたトラフィクの特徴を検査する必要はない(例えば、暗号アルゴリズムが 128 ビット AES であり、256 ビット AES でないこと)。

テスト 2：評価者は、サーバの ST にある任意の暗号スイートを含まないような暗号スイートのリストを持つサーバへ Client Hello を送信し、サーバ接続を拒否することを検証しなければならない(shall)。さらに、評価者は、TLS_NULL_WITH_NULL_NULL 暗号スイートのみを含むサーバへ Client Hello を送信し、サーバが接続を拒否することを検証しなければならない(shall)。

テスト 3：評価者は、サーバが選択する暗号スイートと合致しないような(例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用している際に、ECDHE 鍵交換を送信する、または ECDSA 暗号スイートの一つを利用している際に RSA 鍵交換を送信する) TLS 接続で鍵交換メッセージをそうしんするためにクライアントを利用しなければならない(shall)。評価者は、TOE がクライアントの change cipher spec メッセージを受信した後、致命的なアラートを送信することを検証しなければならない(shall)。

テスト 4：評価者は以下の改変をトラフィクに対して実行しなければならない(shall)：

- Client Hello ハンドシェイクメッセージにおいてクライアントのノンスにおける 1 バイトを改変し、サーバがクライアントの Certificate Verify ハンドシェイクメッセージを拒否すること、また

はサーバがクライアントの Finished ハンドシェイクメッセージを拒否することを検証する。

- クライアントの Certificate Verify ハンドシェイクメッセージの署名ブロックを改変し、サーバがクライアントの Certificate Verify ハンドシェイクメッセージを拒否することを検証し、サーバがクライアントの Finished ハンドシェイクメッセージを拒否することを検証する。
- Client Finished ハンドシェイクメッセージの 1 バイトを改変し、サーバが接続を拒否し、アプリケーションデータを送信しないことを検証する。
- クライアントが Chenge Cipher Spec メッセージを送信する前に、クライアントから Finished メッセージを送信することによって致命的なアラートを生成した後、以前のテストからのセション ID を用いて Client Hello を送信し、サーバ接続をきょう日することを検証する。
- 平文の有効な Server Finished メッセージを送信し、クライアントが受信に際して致命的なアラートを送信し、アプリケーションデータをそうしんしないことを検証する。サーバの Finished メッセージは、有効なヴぇりｆｙ__だたを含まなければならなず(shall)、ネットワークプロトコル分析ツールを用いて正しく解析しなければならない(shall)。

FCS_TLSS_EXT.1.2 [*選択：TSF、TOE プラットフォーム*]は、SSL 1.0、SSL 2.0、SSL 3.0 及び[*選択：TLS 1.0、TLS 1.1、その他の TLS バージョンなし*]を要求するクライアントからの接続を拒否しなければならない(shall)。

保証アクティビティ

TSS

評価者は、古い SSL と TLS バージョンの拒否の記述、及び AGD ガイダンスに含まれなければならない(must)要件を満たすために必要な設定サポートされる暗号スイートが規定されることを保証するため、TSS に含まれることを検証しなければならない(shall)。

テスト

評価者は、バージョン SSL 1.0 を用いた接続を要求する Client Hello を送信し、サーバが接続の拒否することを検証しなければならない(shall)。評価者は、SSL 2.0 及び SSL 3.0 及び選択された TLS バージョンを用いて本テストを繰り返さなければならない(shall)。

FCS_TLSS_EXT.1.3 [*選択：TSF、TOE プラットフォーム*]は、X.509v3 証明書を用いて TLS クライアントの相互認証をサポートしなければならない(shall)。

FCS_TLSS_EXT.1.4 [*選択：TSF、TOE プラットフォーム*]は、ピア証明書が無効である場合、高信頼チャネルを確立してはならない(shall not)。

適用上の注釈： *TLS のための X.509v3 証明書の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、この用途が TLS 相互認証のためのクライアント側の証明書のためのサポートを含まなければならないことを追加する。*

TLS が利用される場合であっても、相互認証は、デバイス登録で要求されない。しかし、登録後の MDM サーバとエージェント間のすべての通信は、相互認証を利用しなければならない(shall)。
有効性は、RFC 5280 に従って、証明書パス、有効期限も呼び失効状態によって決定される。証明書の有効性は、FIA_X509_EXT.1 のために実行されるテストに従ってテストされなければならない(shall)。

保証アクティビティ

TSS

評価者は、FIA__X509_EXT.2.1 で要求される TSS 記述に TLS 相互認証のクライアント側証明書の利用を含まれることを保証しなければならない(shall)。

ガイダンス

評価者は、FIA__X509_EXT.2.1 で要求される AGD ガイダンスに TLS 相互認証のクライアント側証明書の設定のための指示を含まれることを保証しなければならない(shall)。

テスト

評価者は、以下の相互認証テストを実行しなければならない(shall)：

テスト 1：評価者は、証明書要求をクライアントへ送信するようサーバをせっていしない(shall)、またクライアントから証明書を背負う振することなしに接続を試行しなければならない(shall)。評価者は接続が拒否されることを検証しなければならない(shall)。

テスト 2：評価者は、クライアントの証明書によって利用される supported_signature_algorithm なしにクライアントへ証明書要求を送信するようサーバを設定しなければならない(shall)。評価者は、クライアント証明書を用いて接続を試行し、接続が拒否されることを検証しなければならない(shall)。

テスト 3：評価者は、有効な認証パスを持たない証明書の利用が機能の失敗をもたらすことを実証しなければならない(shall)。管理者ガイダンスを用いて、評価者は、次にその機能で利用されるべき証明書を検証する必要がある証明書をロードし、機能が成功することを実証しなければならない(shall)。評価者は次に証明書の 1 つを削除し、機能が失敗することを示さなければならない(shall)。

テスト 4：評価者は、サーバの証明書要求メッセージにおける認証局(ルートまたは中間 CA のいずれか) の 1 つへチェインしないような証明書を送信するようクライアントを設定しなければならない(shall)。評価者は、試行された接続が拒否されることを検証しなければならない(shall)。

テスト 5：評価者は、extendedKeyUsage フィールドに Client Authentication purpose を持つような証明書をそうしんするようにクライアントを設定し、サーバが施行された接続を受け入れることを検

証しなければならない(shall)。評価者は、このテストを Client Authentication purpose なしに繰り返さなければならない(shall)、そしてサーバが接続を拒否することを検証しなければならない(shall)。理想的には、2 つの証明書は、Client Authentication ぷｒぽせ以外は同一であるべきである(should)。

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

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

FCS_TLSS_EXT.1.5 [*選択：TSF、TOE プラットフォーム*]は、証明書に含まれる distinguished name (DN)または Subject Alternative Name (SAN) がピアに対して期待される識別子と合致しない場合、高信頼チャネルを確立してはならない(shall not)。

適用上の注釈： *ピア識別子は、証明書の Subject フィールドまたは Subject Alternative Name 拡張にあるかもしれない。期待される識別子は、せっていされてもよいし、ピアによって利用されるドメイン名、IP アドレス、利用者名、または電子メールアドレスとひかくされてもよい、または比較のために直接サーバへ渡されてもよい。照合は、ビットワイズ比較によって実行されるべきである。*

保証アクティビティ

TSS

評価者は、証明書の DN 及び SAN が期待される識別子と比較される方法について TSS に記述されていることを検証しなければならない(shall)。

ガイダンス

DN が自動的にドメイン名、IP アドレス、利用者名、または電子メールアドレスと比較されない場合、評価者は、AGD ガイダンスに期待される識別子または接続のディレクトリサーバの設定が含まれていることを保証しなければならない(shall)。

テスト

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

FCS_TLSS_EXT.1.6 [*選択：TSF、TOE プラットフォーム*]は、[*選択：NIST 曲線 [選択：*

secp256r1、secp384r1] 上、及びその他の曲線なし； Diffie-Hellman パラメタで 2048 ビット長のもの及び [選択 3072 ビット、その他のビット長なし]] の鍵共有パラメタを生成しなければならない(shall)。

適用上の注釈： *DHE または ECDHE 暗号スイートが FCS_TLSS_EXT.1.1 で一切選択されない場合、骨れメントは省略されてもよい。*

ST に FCS_TLSS_EXT.1.1 の DHE 暗号スイートが列挙される場合、ST には、本要件の Diffie－Hellman 選択を含まなければならない(must)。FMT_SMF.1 は、TLS 接続のセキュリティ強度を確立するため、鍵共有パラメタの設定を要求する。

保証アクティビティ

TSS

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

ガイダンス

評価者は、本要件を満たす必要があるあらゆる設定ガイダンスが AGD ガイダンスに含まれなければならない(must) ことを検証しなければならない(shall)。

テスト

評価者は、ECDHE 暗号スイートと設定された曲線及び、パケットアナライザを用いて接続を試行し、鍵交換メッセージの鍵共有パラメタが設定されたものであることを検証しなければならない(shall)。(サイズが設定された曲線の期待されるサイズと合致することを決定すれば十分である。) 評価者は、このテストをそれぞれのサポートされる NIST 楕円曲線及びそれぞれの Diffie-Hellman 鍵長について繰り返さなければならない(shall)。

C. オブジェクティブ要件

本 EP の「序論」で示されるとおり、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実行されなければならないようなもの) が本 EP の本文に含まれている。望ましいセキュリティ機能を規定する追加の要件があり、これらの要件は、本附属書に含まれる。これらの要件は、本 EP の将来のバージョンで、オブジェクティブ要件からベースライン要件へ移行することが期待される。

これらは、本 EP へ適合する限りは、いつでも ST に含まれてもよい。

本附属書は、2 つのサブセクションに分けられている : TSF によって実行されてもよいオブジェクティブ要件及び MDM エージェントまたはその基盤となるプラットフォームによって実行されてもよいオブジェクティブ要件。

C.1 オブジェクティブ TOE セキュリティ機能要件

C.1.1 セキュリティ監査 (FAU)

FAU_CRP_EXT.1 モバイルデバイス設定の適合報告のサポート (FAU_CRP)

FAU_CRP_EXT.1.1 MDM サーバは、許可されたエンティティに[*選択 : 登録されたデバイスの設定についての問い合わせに対する応答を提供するインタフェース、登録されたデバイスの設定についてのデータのイクスポートを許可するようなインタフェース*]を認証された[*選択 : TLS/HTTPS、TLS、DTLS、IPsec、SSH*] 高信頼通信チャネルを介して提供しなければならない (shall)。それぞれの登録されたモバイルデバイス用に提供された情報には、以下が含まれる :

a. MD ファームウェア／フソフトウェアの現在のバージョン
b. デバイスのハードウェアモデルの現在のバージョン
c. 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
d. デバイスに適用された MD 設定ポリシーのリスト(FMT_SMF.1.1(1) で定義されたとおり)
e. [*選択 : [割付 : 登録されたデバイスについてのその他の利用可能な情報のリスト]、その他の情報なし*]

適用上の注釈 : *本要件の意図は、MDM サーバが、そのたの企業セキュリティ基盤システムによって利用される登録されたモバイルデバイスについて適合情報を提供できることである。インターネットエンジニアリングタスクフォース(IEFT) セキュリティオートメーションアンドコンティニュアスモニタリング(SACM) ワーキンググループ他によって端点デバイス配置に関するアクセスと報告のプロトコル及び規格を定義するために検討中の規格化作業が行われている。我々は、規格化作業が完了した際に、本要件が本プロテクションプロファイルの将来のバージョンにおいて含まれることを期待している。*

「IPsec」が選択される場合、IPsec VPN クライアントの拡張パッケージが ST に含まれなければならない(must)。「SSH」が選択される場合、セキュアシェルの拡張パッケージが ST に含まれなければならない(must)。「TLS」、「TLS/HTTPS」または「DTLS」が選択される場合、附属書 B からの適切な選択ベースの SFR が ST に含まれなければならない(must)。

保証アクティビティ

ガイダンス

評価者は、MDM サーバの適合性報告インタフェースをアクセスする方法についての指示が操作ガイダンスに含まれることを保証するため、チェックしなければならない(shall)。

テスト

テスト 1：操作ガイダンスを利用して、評価者は許可されたエンティティからの適合性報告インタフェースをアクセスできる能力を実証し、登録されたデバイスについての情報の取得に成功しなければならない(shall)。

テスト 2：評価者は、許可されないエンティティからの適合性報告インタフェースのアクセスを試行し、試行が拒否されることを実証しなければならない(shall)。

C.1.2 識別と認証 (FIA)

FIA_UAU_EXT.4(1) 利用者認証 (再利用の防止)

FIA_UAU_EXT.4.1(1) TSF は、[*割付：特定された認証メカニズム*]に関連する登録認証データの再利用を防止しなければならない(shall)。

適用上の注釈： *本要件は、FIA_ENR_EXT.1.1 での登録のため、利用者を認証するために利用される認証メカニズムを参照する。利用者名とパスワードが登録用に利用者を認証するために利用される場合、パスワードは、再利用されてはならない(shall not)。従って、利用者が管理上 2 台の登録されたデバイス持っている場合または同じデバイスを再登録する必要がある場合(即ち、デバイスワイプ後に)、そのパスワードは、それぞれの登録用に異なっていなければならない(shall)。さらに、２つの異なる利用者が登録しようとする場合、パスワードはそれぞれの利用者について異なっていなければならない(shall)。*

保証アクティビティ

TSS

評価者は、ST でサポートされるとおり列挙されたそれぞれの MDM エージェント／プラットフォームの登録プロセスの記述が TSS に含まれることを検証しなければならない(shall)。本記述が利用者認証の方法(利用者名／パスワード、トークン等) 及び認証データの再利用が防止される方法について含んでいなければならない(shall)。

テスト

テスト 1：評価者は、正しいクレデンシャルを提供するデバイスを登録しなければならない(shall)。評価者は、最初のデバイスを登録するために使用した同じクレデンシャルを用いて 2 番目のデバイスの登録を試行しなければならない(shall)。評価者は、2 番目のデバイスが登録できなかったことを検証しなければならない(shall)。

FIA_UAU_EXT.4(2) 利用者認証 (デバイス登録の再利用の防止)

FIA_UAU_EXT.4.1(2) TSF は、利用者のデバイス登録の制限に関する[*選択：IMEI*、*[割付：*

ユニークなデバイス ID] の再利用を防止しなければならない(shall)。

適用上の注釈： *MDM サーバは、同じユニーク識別子を用いて登録されるような 2 つのデバイスを許可してはならない(shall not)。ユニークな識別子は、FIA_ENR_EXT.1.2 で規定される。*

FIA_UAU_EXT.4.1(2) は、「IMEI によって規定されるデバイス」または「[割付：ユニークなデバイス ID]によって規定されるデバイス」が FIA_ENR_EXT.1.2 で選択される場合にのみ、ST に含まれなければならない(shall)。同じ選択が本要件について完成されなければならない(shall)。

保証アクティビティ

TSS

評価者は、利用者のデバイス登録を制限するようなポリシーの記述が TSS に含まれることを検証しなければならない(shall)。

ガイダンス

評価者は、利用者登録を制限する方法が管理者ガイダンスに記述されていること及びそれが管理者に対して制限の設定方法について指示していることを保証しなければならない(shall)。

テスト

テスト 1：評価者は、MDM サーバが利用者登録を特定のユニークなデバイス ID に制限し、そのデバイス ID を用いてデバイスを登録するよう設定しなければならない(shall)。評価者は、同じユニークなデバイス ID を用いて 2 番目のデバイスの登録を試行しなければならない(shall)。(デバイスが登録抹消されるが、MDM サーバはまたそのデバイスを登録したままであると見なすように、評価者は、ネットワーク接続性なしにデバイスをワイプする必要があるかもしれない。) 評価者は、同じユニークなデバイス ID を用いて 2 番目の登録が失敗することを検証しなければならない(shall)。

C.1.3 セキュリティ管理 (FMT)

FMT_SAE_EXT.1 セキュリティ属性の期限切れ

FMT_SAE_EXT.1.1 TSF は、登録認証データの設定可能な有効期限切れ時刻を規定できなければならない(shall)。

FMT_SAE_EXT.1.2 TSF は、登録認証データの有効期限切れ事項が経過した後、登録を拒否できなければならない(shall)。

適用上の注釈： *本要件は、FIA_ENR_EXT.1.1 で管理上のデバイル登録のために利用される利用者認証コードを参照する。利用者認証コードは、設定可能な時刻制限までの間にのみ有効でなければならない。認証コードが有効期限切れの場合、正しく入力された場合であっても、登録は発生してはならない(shall)。*

認証コードが有効である時間の長さは、FMT_SMF.1(2)における機能 g 毎に設定される。FMT_SAE_EXT.1 が ST に含まれる場合、機能 g は FMT_SMF.1(2) で選択されなければならない(shall)。

保証アクティビティ

TSS

評価者は、ST でサポートされるとおり列挙されたそれぞれの MDM エージェント／プラットフォームについての登録プロセスの記述が TSS に含まれることを検証しなければならない(shall)。本記述は、利用者認証方法(利用者名／パスワード、トークン、等)を含まなければならない(shall)。

ガイダンス

評価者は、TSS に列挙されたそれぞれの利用者認証方法について有効期限切れ時刻を設定するための指示が操作ガイダンスに含まれることを保証するためチェックしなければならない(shall)。

テスト

テスト 1：評価者は、管理者ガイダンスに従って MDM サーバが登録認証データについての有効期限時刻をセットするよう設定しなければならない(shall)。TSS に列挙されたそれぞれの利用者認証法について評価者は、有効期限切れした認証データを用いて登録を試行しなければならない(shall)。評価者は、登録が成功しないことを検証しなければならない(shall)。

C.2 オブジェクティブな TOE またはプラットフォームセキュリティ機能要件

C.2.1 暗号サポート (FCS)

FCS_TLSC_EXT.1　TLS クライアントプロトコル (署名アルゴリズム拡張)

FCS_TLSC_EXT.1.6　[*選択：TSF、TOE プラットフォーム*]は、以下のハッシュアルゴリズムを含む supported_signature_algorithms の値を伴う Client Hello の署名アルゴリズム拡張を提示しなければならない(shall)：[*選択：SHA256、SHA384、SHA512*] 及びその他のハッシュアルゴリズムなし。

適用上の注釈：　*本要件は、クライアントによるディジタル署名検証の目的でサポートされるハッシュアルゴリズムを制限し、サーバに対してサーバによるディジタル署名生成の目的のためのサポートされるハッシュに制限する。署名アルゴリズム拡張は、TLS1.2 によってのみサポートされる。*

保証アクティビティ

TSS

評価者は、署名アルゴリズム拡張及び要求されるふるまいがデフォルトで実行されるかまたは設定されもよいかについて TSS に記述されていることを検証しなければならない(shall)。

ガイダンス

署名アルゴリズム拡張が本要件を満たすように設定されなければならない(must)ことを TSS が示す場合、評価者は、署名アルゴリズム拡張の設定が AGD ガイダンスに含まれることを検証しなければならない(shall)。

テスト

評価者は、署名アルゴリズム拡張の中でクライアントの HashAlgorithm enumeration に従ってサポートされないような TLS 接

続における証明書を送信する (例えば、SHA-1 署名付きの証明書を送信する) ようサーバを設定しなければならない(shall)。評価者は、サーバの証明書ハンドシェイクメッセージを受信した後、TOE が接続を切断することを検証しなければならない(shall)。

FCS_TLSC_EXT.1.7 [*選択：TSF、TOE プラットフォーム*]は、RFC 5746 に従って、「renegotiation_info」TLS 拡張の利用を通してセキュアな再ネゴシエーションをサポートしなければならない(shall)。

FCS_TLSC_EXT.1.8 [*選択：TSF、TOE プラットフォーム*]は、Client Hello メッセージにおける[*選択：以下の 1 つのみを選択：renegotiation_info 拡張、TLS_EMPTY_RENEGOTIATION_INFO_SCSV 暗号スイート*]を含めなければならない(shall)。

適用上の注釈： *RFC 5746 は、再ネゴシエーションのハンドシェイクを元のハンドシェイクでの暗号へバインドするような TLS への拡張を定義する。*

その選択に含まれる暗号スイートは、拡張をサポートしないようなサーバと互換であるようにするためのクライアントのための手段である。クライアント実装は、その暗号スイートとその拡張の両方をサポートすることが推奨される。

保証アクティビティ

テスト

テスト 1：評価者は、2 つの TLS 端点間のトラフィクをキャプチャするためにネットワークパケットアナライザ／スニファを利用しなければならない(shall)。評価者は、初期ハンドシェイク中の ClientHello パケットに「renegotiation_info」フィールドまたは SCSV 暗号スイートのいずれかが含まれることを検証しなければならない(shall)。

テスト 2：評価者は、「renegotiation_info」拡張を含むような初期ハンドシェイク中に受信した SeverHello メッセージのクライアントの取り扱いを検証しなければならない(shall)。評価者は、非ゼロであるような SeverHello メッセージのこのフィールドの長さ部分を改変し、クライアントが失敗を送信し、接続を終了することを検証しなければならない(shall)。評価者は、適切にフォーマットされたフィールドが TLS 接続の成功をもたらすことを検証しなければならない(shall)。

テスト 3：評価者は、セキュアな再ネゴシエーション中に受信した ServerHello メッセージに「renegotiation_info」拡張が含まれることを検証しなければならない(shall)。評価者は、「client_verify_data」または「server_verify_data」のいずれかの値を改変し、クライアントが接続終了することを検証しなければならない(shall)。

FCS_TLSS_EXT.1 TLS サーバプロトコル (署名アルゴリズム拡張)

FCS_TLSS_EXT.1.7 [*選択：TSF、TOE プラットフォーム*] は、以下のハッシュアルゴリズムを用いる証明書要求での supported_signature_algorithms で HashAlgorithm enumeration を提示しなければならない(shall) : [*選択：SHA256、SHA384、SHA512*] 及びその他のハッシュアルゴリズムなし。

適用上の注釈： *本要件は、サーバによるディジタル署名検証の目的でサポートされる*

ハッシュアルゴリズムを制限し、クライアントによるディジタル署名生成の目的でサポートされるハッシュにクライアントを制限する。supported_signature_algorithms は、TLS1.2 のみによってサポートされる。

保証アクティビティ

TSS

(条件付き) 評価者は、証明書要求の supported_signature_algorithms フィールド及び要求されるふるまいがデフォルトで実行されるか、または設定されてもよいかのいずれかについて、TSS に記述されることを検証しなければならない(shall)。TSS に supported_signature_algorithms フィールドが本要件を満たすように設定されなければならない(must)ことを示している場合、評価者は、supported_signature_algorithms フィールドの設定が 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)。

テスト

評価者は、サーバの証明書によって利用されるハッシュアルゴリズムがサポートされないことを示すような署名アルゴリズム拡張をクライアントが送信するように設定しなければならない(shall)。評価者は、接続を試行し、サーバがクライアントの接続を拒否することを検証しなければならない(shall)。

FCS_TLSS_EXT.1.8 [*選択：TSF、TOE プラットフォーム*]は、RFC 5746 に従って、「renegotiation_info」TLS 拡張をサポートしなければならない(shall)。

FCS_TLSS_EXT.1.9 [*選択：TSF、TOE プラットフォーム*]は、ServerHello メッセージに renegotiation_info 拡張を含めなければならない(shall)。

適用上の注釈： *RFC 5746 は、再ネゴシエーションハンドシェイクをオリジナルのハンドシェイクの暗号へバインドするような TLS への拡張を定義する。*

保証アクティビティ

テスト

以下のテストはセキュアな再ネゴシエーションと「renegotiation_info」拡張をサポートするクライアントとの接続を要求する。

テスト 1：評価者は、2 つの TLS 端点間のトラフィクをキャプチャするためにネットワークパケットアナライザ／スニファを利用しなければならない(shall)。評価者は、ServerHello パケットに「renegotiation_info」フィールドが含まれることを検証しなければならない(shall)。

テスト 2：評価者は、非ゼロであるような初期ハンドシェイクの ClientHello メッセージのフィールドの長さ部分を改変し、クライアントが失敗を送信し、接続を終了することを検証しなければならない(shall)。評価者は、適切にフォーマットされたフィールドが TLS 接続の成功をもたらすことを検証しなければならない(shall)。

テスト 3：評価者は、セキュアな再ネゴシエーション中に受信した ClientHello メッセージにおける「client_verify_data」または「server_verify_data」の値を改変し、サーバが接続終了することを検証しなければならない(shall)。

C.2.2 識別と認証 (FIA)

FIA_X509_EXT.3 X.509 登録

FIA_X509_EXT.3.1 [*選択：TSF*、*TOE プラットフォーム*] は、RFC 2986 によって規定されるとおりの証明書要求メッセージを生成し、要求において以下の情報を提供できなければならない：公開鍵及び[*選択：デバイス特有の情報*、*Common Name*、*Organization*、*Organization Unit*、*Country*]。

適用上の注釈： *公開鍵は、FCS_CKM.1.1 で規定されるとおり、TOE によって生成される公開―プライベート鍵ペアの公開鍵部分である。*

Enrollment over Secure Transport(EST)はまだ広く適用されていない新しい規格であるので、本要件は、開発者がまだEST を実装していないような証明書要求メッセージを生成する能力持つようなそれらの製品を区別できるように暫定的にオブジェクティブな要件として含まれる。

FIA_X509_EXT.3.2 [*選択：TSF*、*TOE プラットフォーム*] は、CA 証明書応答の受信に際して、ルート CA からの証明書のチェインを検証しなければならない(shall)。

保証アクティビティ

TSS

ST 作成者が「デバイス特有の情報」を選択する場合、評価者は、証明書要求で利用される device-specific フィールドの記述を TSS に含むことを検証しなければならない(shall)。

ガイダンス

評価者は、証明書要求メッセージの生成を含め、CA からの証明書をの要求に関する指示が操作ガイダンスに含まれていることを保証するためにチェックしなければならない(shall)。ST 作成者が「Common Name」、「Organization」、「Organization Unit」または「Country」を選択する場合、評価者は、証明書要求メッセージを生成する前にこれらのフィールドを確立するための指示が本ガイダンスに含まれることを保証しなければならない(shall)。

テスト

テスト 1：評価者は、TOE に証明書要求メッセージを生成させるために操作ガイダンスを利用しなければならない(shall)。評価者は、生成されたメッセージをキャプチャし、それが規定されたフォーマットに適合することを保証しなければならない(shall)。評価者は、必要なあらゆる利用者入力の情報を含めて、証明書要求が公開鍵及びその他の要求される情報を提供することを確認しなければならない(shall)。

テスト 2：評価者は、有効な認証パスを持たない証明書応答メッセージの検証が機能失敗の結果となることを実証しなければならない(shall)。評価者は、次に、信頼された CA が証明書応答メッセージを検証する必要があるような証明書をロードし、機能が成功することを実証しなければならない(shall)。評価者は、証明書の 1 つを策 s 女子、その機能が失敗することを示さなければならない(shall)。

FIA_X509_EXT.4　代わりの X.509 登録

FIA_X509_EXT.4.1　TSF は、RFC 7030 セクション 4.2 で記述される simple enrollment method を用いて証明書登録を要求するため、RFC 7030 で規定されるとおり、Enrollment over Secure Transport (EST)プロトコルを利用しなければならない(shall)。

FIA_X509_EXT.4.2　TSF は、既存の証明書及び RFC7030 セクション 3.3.2 によって規定されるとおりに対応するプライベート鍵を用いて EST 要求を認証できなければならない(shall)。

FIA_X509_EXT.4.3　TSF は、RFC 7030 セクション 3.2.3 によって規定されるとおりの利用者名とパスワードを用いて HTTP ベーシック認証を用いて EST 要求を認証できなければならない(shall)。

FIA_X509_EXT.4.4　TSF は、RFC7030、セクション 3.6.1 で記述された規則にしたガス Explicit Trust Anchor を用いて、EST サーバの認証を実行しなければならない(shall)。

適用上の注釈：　*EST は、FCS_TLSC_EXT.1 で規定されるとおり、EST サーバとのセキュアな接続を確立するために、HTTPS についても利用する、つえに ST 作成者は、ST の本文に FCS_HTTPS_EXT.1 及び FCS_TLSC_EXT.1 についても含めなければならない(must)。EST 操作専用の別の Trust Anchor Database は、RFC 7030 の Explicit Trust Anchors として記述されている。*

FIA_X509_EXT.4.5　TSF は、RFC 7030 セクション 4.4 で規定されるとおりサーバ提供のプライベート鍵を要求できなければならない(shall)。

FIA_X509_EXT.4.6　TSF は、RFC 7030 セクション 4.1.3 で記述される「Root CA Key Update」処理を用いてその EST 特有の Trust Anchor Database をアップデートできなければならない(shall)。

FIA_X509_EXT.4.7　TSF は、RFC 2986 できていされるとおりの EST に対する証明書要求メッセージを生成し、要求に以下の情報を提供できなければなければならない(shall)：公開鍵及び[*選択：デバイス特有の情報；Common Name*、*Organization*、*Organizational Unit*、*Country*]。

FIA_X509_EXT.4.8　TSF は、CA 証明書応答の受信に際して Trust AnchorDatabase のルート証明 CA 証明書から EST サーバ CA 証明書への証明書のチェインを検証しなければならない(shall)。

適用上の注釈：　*FIA_X509_EXT.4.7 で参照される公開鍵は、FCS_CKM.1(2) で規定される TOE によって生成された公開—プライベート鍵ペアの公開鍵部分である。*

保証アクティビティ

ガイダンス

評価者は、証明書要求メッセージの生成を含め、EST サーバからの証明書をの要求に関する指示が操作ガイダンスに含まれていることを保証するためにチェックしなければならない(shall)。

テスト

評価者は、以下のテストについても実行しなければならない(shall)。その他のテストは、FCS_TLSC_EXT.1 のために列挙された保証アクティビティと併せて実行される。

テスト 1 : 評価者は、RFC7030 セクション 3.3.2 により記述されるとおり、既存の証明書とプライベート鍵を用いてサーバに対する証明書要求を認証し、RFC7030 セクション 4.2 で記述された simple enrollment method を用いて TOE に EST サーバからの証明書登録を要求させるために操作ガイダンスを利用しなければならない(shall)。評価者は、結果としての証明書が TOE 鍵ストア内で取得されインストールされることを確認しなければならない(shall)。

テスト 2 : 評価者は、RFC7030 セクション 3.3.2 により記述されるとおり、利用者名とパスワードを用いてサーバに対する証明書要求を認証し、RFC7030 セクション 4.2 で記述された simple enrollment method を用いて TOE に EST サーバからの証明書登録を要求させるために操作ガイダンスを利用しなければならない(shall)。評価者は、結果としての証明書が TOE 鍵ストア内で取得されインストールされることを確認しなければならない(shall)。

テスト 3 : 評価者は、EST サーバを TOE の証明書要求に含まれる鍵とは異なる公開鍵を含む証明書を返すように改変しなければならない(shall)。評価者は TOE に EST サーバからの証明書登録を要求させるために操作ガイダンスを利用しなければならない(shall)。評価者は、発行された証明書の公開鍵が証明書要求の公開鍵と合致しないので、結果としての証明書を TOE が受け入れないことを確認しなければならない(shall)。

テスト 4 : 評価者は TOE 一般的なトラストアンカーデータベースに存在するが EST 特有のトラストアンカーデータベースには存在しないような、サーバ証明書を TOE に提示するため、EST サーバを設定または中間者攻撃ツールを用いなければならない(shall)。評価者は、TOE に EST サーバからの証明書登録を要求させなければならない。評価者は、その要求さ成功しないことを検証しなければならない(shall)。

テスト 5 : 評価者は、無効な証明書を提示するために、EST サーバを設定または中間者攻撃ツールを用いなければならない(shall)。評価者は、TOE に EST サーバからの証明書登録を要求させなければならない(shall)。評価者は、その要求さ成功しないことを検証しなければならない(shall)。評価者は、CMC RA 目的を持たないような証明書を提示するために、EST サーバを設定または中間者攻撃ツールを利用し、EST サーバへの要求が失敗することを検証しなければならない(shall)。テスト者は、有効な証明書及び CMC RA 目的を持つ証明書を用いてテストを繰り返し、証明書登録要求が成功することを検証しなければならない(shall)。

テスト 6 : 評価者は、TOE と EST サーバ間でパケットスニフィングツールを利用しなければならない(shall)。評価者は、スニフィングツールの電源をオンにし、TOE に EST サーバからの証明書登録を要求させなければならない(shall)。評価者は、EST プロトコル対話が TLS 保護された接続を介して発生することを検証しなければならない(shall)。評価者は、接続を復号することは期待されないが、そのパケットが TLS プロトコルフォーマットに適合することを観測することが期待される。

テスト 7 : 評価者は、EST サーバからサーバ提供のプライベート鍵と証明書を TOE に要求させるために操作ガイダンスを利用しなければならない(shall)。評価者は、結果としてのプライベート鍵と証明書の

取得が成功し TOE 鍵ストアにインストールされることを確認しなければならない(shall)。

テスト 8：評価者は、サーバ提供のプライベート鍵と証明書要求の応答として、返された証明書の公開鍵に対応しないようなプライベート鍵を返すように、EST サーバを改変しなければならない(shall)。評価者は、TOE にサーバ提供のプライベート鍵と証明書を要求させるために、操作ガイダンスを利用しなければならない(shall)。評価者は、プライベート鍵と公開鍵は関連しないので、TOE が結果としてのプライベート鍵と証明書を受け入れないことを確認しなければならない(shall)。

テスト 9：評価者は、RFC 7030 セクション 4.1.3 で記述されるとおりの「Root CA Key Update」を提供するように、EST サーバを設定しなければならない(shall)。評価者は、EST サーバからの CA 証明書を TOE に要求させなければならない、また EST 特有のトラストアンカーデータベースが新しいトラストアンカーを用いてアップデートされることを確認しなければならない(shall)。

D. エントロピー証拠資料と評定

本附属書は、TOE によって利用されるそれぞれのエントロピー源についての要求された補足の情報が記述される。

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

D.1 設計の記述

証拠資料には、すべてのエントロピー源コンポーネントの相互作用を含め、エントロピー源の全体的な設計が含まれなければならない (shall)。設計に関して共有可能な情報は、製品に含まれるような第三者エントロピー源についても含まれるべきである。

証拠資料には、エントロピーの生成方法、及び未処理 (生の) データがエントロピー源の内部からテスト目的でどのように取り出すことができるかを含めて、エントロピー源の動作が記述される。本証拠資料では、エントロピー源の設計の概略が説明され、ランダム性がどこから由来し、次にどこへ渡されるのか、任意の生の出力の後処理 (ハッシュ、XOR など)、保存されるのか (保存されるとすればどこに)、そして最後に、どのようにしてエントロピー源から出力されるのかが示されるべきである(should)。処理に課される条件があれば(例えば、ブロッキング)、それもエントロピー源の設計の中で記述されるべきである(should)。図や例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の記述、及び境界外部の敵対者がエントロピー率に影響を与えられないことをセキュリティ境界がそのように保証するかについての記述についても含まれなければならない(must)。

実装された場合、設計記述には、サードパーティのアプリケーションが RBG へエントロピーを追加できる方法についての記述が含まれなければならない(shall)。電源オフと電源オンの間に保存している RBG 状態の記述が含まれなければならない(shall)。

D.2 エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、エントロピー源が確率的な挙動を示すことがなぜ確信できるのか (確率分布の説明と、その分布が特定のエントロピー源によって得られるという正当化を行うことは、これを記述する方法のひとつである) という、技術的な議論が存在すべきである (should)。この議論には、期待される最小エントロピー率(即ち、ソースデータのビットまたはバイト毎の最小エントロピー(ビット単位))の記述、及び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の説明が含まれる。この議論は、エントロピー源がエントロピーを含むビットを作り出すと信頼できる理由の正当化の一部となる。

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

開発者が提供するエントロピー源について、最小エントロピー率を正当化するため、大量の生のソースビットが収集され、統計学的なテストが実行され、最小エントロピー率が統計学的なテストから決定されることが期待される。現時点では、一切の特定の統計学的テストが要求されていないが、それぞれの出力における最小エントロピーの両を決定するために何等かのテストが必要であると想定される。

サードパーティが提供するエントロピー源について、TOE ベンダはその設計情報及びソー

スの生のエントロピーデータにアクセスを制限されているので、証拠資料がサードパーティソースから得られる最小エントロピーの量の見積を示す。最小エントロピーの量をベンダが「推定」することは受け入れ可能であるが、この前提条件は、提供される証拠資料に明確に述べられなければならない(must)。特に、最小エントロピー見積は、ST において規定されなければならなず(must)、前提条件は ST に含まれる。

エントロピー源の種別に関わらず、正当化は、DRBG が ST で記述されたエントロピーを用いて初期化される方法についても含まれなければならない、例えば最小エントロピー率が DRBG にシード値を供給するために使用されるソースデータの量によって乗算されること及びソースデータに基づいて期待されるエントロピー率が明示的に記述され統計学的な量と比較されることを検証することによって。DRBG にシード値を供給するために利用されるソースデータの両が明確でなくまたは計算された量がシード値に明示的に関連してない場合、証拠資料は、完成したとはみなされない。

エントロピー正当化は、サードパーティアプリケーションから、または再起動の間に保存するあらゆる状態から追加されるあらゆるデータを含んではならない(shall not)。

D.3 運用条件

エントロピー率は、エントロピー源自体の制御外の条件によって影響を受けるかもしれない。例えば、電圧、周波数、温度、及び電源投入後の経過時間は、エントロピー源の動作に影響を与えるかもしれない数少ない要素である。このように、証拠資料には、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確実にするために、システムの設計に取り入れられた対策が明確に記述されることになる。同様に、証拠資料にはエントロピー源が不調または一貫しない動作となることがわかっている条件も記述されなければならない(shall)。エントロピー源の故障または機能低下を検出するための方法が含まれなければならない(shall)。

D.4 ヘルステスト

さらに具体的に、すべてのエントロピー源ヘルステストとその根拠が文書化されることになる。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。

E. 適用例テンプレート

以下の適用例テンプレートは、本プロテクションプロファイルによって特定される利用事例を最もよくサポートするようなそれらの選択、割付、及びオブジェクト要件を列挙する。テンプレートが、テンプレートに列挙されたものだけではなく、セクション 5 で列挙されたすべての SFR が ST に含まれることを想定することに留意されたい。これらのテンプレート及びテンプレートからの逸脱は、リスクベースでの調達の決定を用いて顧客を支援するため、セキュリティターゲットで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は、本プロテクションプロファイルによって特定されてシナリオにおける用途から排除される。

特定の要件についての選択が適用例テンプレートで特定されない場合、すべての利用可能な選択は、適用例に対して等しく適用可能である。

E.1 [適用例 1] 汎用企業用途の企業所有のデバイス

要件	アクション
FMT_SMF.1.1(1) 機能 32	ST に含まれ、GPS を割り付ける。
FMT_SMF.1.1(1) 機能 34	ST に含まれる。個人のホットスポット接続を割り付ける(機能が存在する場合)。
FMT_SMF.1.1(1) 機能 47	ST に含まれる.
FMT_SMF.1.1(1) 機能 49	ST に含まれ、「USB 大容量ストレージモード」を選択する。
FMT_SMF.1.1(1) 機能 51	ST に含まれる。両方のオプションを選択する。

E.2 [適用例 2] 特別に高セキュリティ用途の企業所有のデバイス

要件	アクション
FMT_SMF.1.1(1) 機能 15	ST に含まれる。
FMT_SMF.1.1(1) 機能 16	ST に含まれる。
FMT_SMF.1.1(1) 機能 31	ST に含まれ、「その他の方法なし：を選択する。
FMT_SMF.1.1(1) 機能 32	ST に含まれる。
FMT_SMF.1.1(1) 機能 33	ST に含まれる。少なくとも USB を割り付ける。
FMT_SMF.1.1(1) 機能 34	ST に含まれる。TSF がサーバとして動作するようなすべてのプロトコルを割り付ける。
FMT_SMF.1.1(1) 機能 36	ST に含まれる。
FMT_SMF.1.1(1) 機能 37	ST に含まれる。
FMT_SMF.1.1(1) 機能 40	ST に含まれる。
FMT_SMF.1.1(1) 機能 42	ST に含まれる。
FMT_SMF.1.1(1) 機能 47	ST に含まれる。
FMT_SMF.1.1(1) 機能 52	ST に含まれる。
FMT_SMF.1.1(1) 機能 54	ST に含まれる。
FMT_SMF.1.1(2) 機能 c	ST に含まれる。
FMT_SMF.1.1(2) 機能 d	ST に含まれる。
FCS_CKM.1.1	鍵長 3072 の RSA を選択または ECC 方式を選択する。
FCS_CKM.2.1	「RSA 方式」を選択または「ECC 方式」を選択する。
FCS_COP.1.1(1)	256 ビットを選択する。
FCS_COP.1.1(2)	SHA-384 を選択する。
FCS_COP.1.1(3)	鍵長 3072 の RSA を選択または ECC 方式を選択する。

FIA_X509_EXT.2.2	「管理者に選択することを許可する」または「証明書を受け入れない」のいずれかを選択する。
FCS_TLSC_EXT.1.1	ST に含まれる場合、「TLS 1.2」を選択する。
FCS_TLSC_EXT.1.5	ST に含まれる場合、「secp384r1」を選択する。

E.3 [適用例 3] 個人及び企業用途の個人所有デバイス

要件	アクション
FMT_SMF.1.1(1) 機能 13	ST に含まれる。
FMT_SMF.1.1(1) 機能 14	ST に含まれる。
FMT_SMF.1.1(1) 機能 21	ST に含まれる。
FMT_SMF.1.1(1) 機能 22	ST に含まれる。
FMT_SMF.1.1(1) 機能 30	「アプリ毎ベースで」及び／または「アプロケーションプロセスのグループ毎ベース」を選択する。
FMT_SMF.1.1(1) 機能 31	ST に含まれる場合、「アプリ毎ベースで」及び／または「アプロケーションプロセスのグループ毎ベース」を選択する。
FMT_SMF.1.1(1) 機能 48	ST に含まれる。
FMT_SMF.1.1(1) 機能 52	ST に含まれる場合、「アプリ毎ベースで」及び／または「アプロケーションプロセスのグループ毎ベース」を選択する。
FMT_SMF.1.1(2) 機能 f.	ST に含まれる。

E.4 [適用例 4] 個人及び限定的な企業用途の個人所有デバイス

現時点では一切の要件が本適用例について推奨されていない。

F. 参照文献

識別子	タイトル
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012 • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • 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
[MDF PP]	Protection Profile for Mobile Device Fundamentals, Version 3.0, June 2016
[MDM Agent PP]	Extended Package for Mobile Device Management Agents, Version 3.0, October 2016

G. 頭字語

CSP	Critical Security Parameter
DEK	Data Encryption Key
EST	Enrollment over Secure Transport
KEK	Key Encryption Key
MD	Mobile Device
MDM	Mobile Device Management
OS	Operating System
REK	Root Encryption Key