モバイルデバイス管理エージェントの拡張パッケージ

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。 エージェント監査格納のオブジェクティブ要件を追加。登録抹消防止の新規要件を追加。 MDM エージェント EP の初回リリース。
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。

目次

1. 序論 5
1.1 概要 5
1.2 用語 5
1.2.1 コモンクライテリア用語 5
1.2.2 技術用語 6
1.3 適合する評価対象 6
1.3.1 TOE 境界 7
1.4 本拡張パッケージの使用方法 7
1.5 適用例 7
2. 適合主張 10
3. セキュリティ課題記述 11
3.1 脅威 11
3.2 前提条件 11
3.3 組織のセキュリティ方針 12
4. セキュリティ対策方針 13
4.1 TOE のセキュリティ対策方針 13
4.2 運用環境のセキュリティ対策方針 13
5. セキュリティ要件 14
5.1 表記法 14
5.2 保証アクティビティのテスト環境 14
5.3 MDF PP セキュリティ機能要件の指示 14
5.3.1 暗号サポート(FCS) 14
5.3.2 高信頼パス／チャネル(FTP) 15
5.4 MDM PP セキュリティ機能要件の指示 17
5.4.1 暗号サポート(FCS) 17
5.4.2 TSF の保護 (FPT) 18
5.5 TOE セキュリティ機能要件 18
5.5.1 セキュリティ監査 (FAU) 18
5.5.2 識別と認証 (FIA) 22
5.5.3 セキュリティ管理 (FMT) 22
5.6 TOE またはプラットフォームのセキュリティ機能要件 27
5.6.1 セキュリティ監査 (FAU) 27

5.7 TOE セキュリティ保証要件 27
A. オプション要件 29
B. 選択ベース要件 30
C. オブジェクティブ要件 31
C.1 オブジェクティブ TOE セキュリティ機能要件 31
C.1.1 セキュリティ監査 (FAU) 31
C.1.2 TSF の保護 (FPT) 31
D. エントロピー証拠資料と評定 33
E. 適用例テンプレート 34
F. 参照文献 35
G. 頭字語 36

1. 序論

1.1 概要

本拡張パッケージ(EP)は、モバイルデバイス管理 (MDM) エージェントのセキュリティ要件について記述し、十分定義され、記述された脅威を軽減する際に目標とされる最小限のベースライン要件を提供することを意図している。MDM システムのエージェントは、モバイルデバイスの企業デプロイメントの 1 つのコンポーネントのみである。セキュリティ方針を実行するモバイルデバイスプラットフォームのような、その他のコンポーネント、及びモバイルアプリケーションリポジトリを提供するようなサーバは、適用範囲外である。本概説は、適合する評価対象の機能について記述し、本 EP がどのように MDM プロテクションプロファイル(PP) またはモバイルデバイス基盤(MDF) PP と併せて利用されるべきかについて説明する。

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評価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のセキュリティ要件。
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のセキュリティ要件。
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、一連の実装依存のセキュリティ要件。
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

用語	意味
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。
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。
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。
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。
利用者	モバイルデバイス利用者を参照。

1.3 適合する評価対象

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。

MDM 運用環境は、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。

本 EP の焦点である、MDM エージェントは、モバイルデバイス上の(MDM サーバソフトウェアの開発者により共有される)アプリケーションとしてインストールされ、モバイルデバイスの OS の一部である。MDM エージェントは、MDM サーバへのセキュアな接続を確立する、この接続は企業管理者によって管理される。オプションで、MDM エージェントは、企業ホステッド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のモバイルアプリケーションストア(MAS)サーバと対話する。

MDM エージェントは、モバイルデバイスの OS の一部である場合、MDM エージェントは、モバイルデバイスを設定するための、ローカルインタフェースとリモートインタフェースのような、複数のインタフェースが存在してもよい。本拡張パッケージに適合するエージェントは、少なくとも MDM システムの一部として提供される高信頼チャネルを用いたインタフェースを提供しなければならない(must)。適合 MDM エージェントは、その他のインタフェースについても提供することができる、またこれらの追加のインタフェースの構成の側面は、本 EP の適用範囲内である。

1.3.1 TOE 境界

図 1 は、TOE 境界及びその運用環境の上位レベルの例を示す。上記のとおり、TOE が MDM エージェントに常駐し、モバイルデバイス自体の一部として提供される(赤色で示される)、または MDM サーバソフトウェアの開発者からのサードパーティアプリケーションとして提供される(青色で示される) のいずれかであってもよい。

図 1：MDM システムの運用環境

MDM エージェントは、ポリシーを確立し、デバイスの状態についての問い合わせを実行するために、モバイルデバイスのプラットフォームと密接に対話し、またはその一部でなければならない(must)。モバイルデバイスは言い換えると、MDF PP で規定されたそれ自体のセキュリティ要件を持っている。モバイルデバイスは、MDM エージェントと同時に、または MDM エージェントの評価前のいずれかで、MDF PP に適合する評価を受けなければならない(must)。MDM エージェントがモバイルデバイス OS またはサードパーティアプリケーションの本来一部であるかどうかにかかわらず、真実である。

1.4 本拡張パッケージの使用方法

本 EP は、モバイルデバイス基盤 PP v3.x またはモバイルデバイス管理サーバ PP v3.x に対して拡張可能である：

MDM デバイスを拡張する

TOE は、モバイルオペレーティングシステムの本来の一部である。MDF PP と結合された本 EP の TOE は、モバイルデバイス死体プラス MDM エージェントである。

MDM サーバを拡張する

TOE は、MDM サーバを用いて提供されるサードパーティアプリケーションであり、モバイルデバイスを取得後に利用者によってモバイルデバイス上にインストールされる。MDM サーバと結合された本 EP の TOE は、MDM サーバ及び MDM エージェントの両方を含む MDM 環境全体である。モバイルデバイス自体が TOE の一部でなくとも、そのベースラインセキュリティ機能が存在すると想定可能であるように、MDF PP に適合する評価を受けることが想定される。

1.5 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で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 EP 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(must)。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(must)：

- 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んでもよい：

- 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(must not)。

CC 適合主張

本 EP 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 EP 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。本 EP が MDF PP または MDMPP を拡張する、ここで、本 EP によって拡張される「ベース」機能のいくつかを提供するために MDF PP または MDM PP に信頼を置くことを意味することに留意されたい。しかし、これは、本 EP が MDF PP または MDM PP に適合することを意味するものではない。

パッケージ主張

本 EP 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.BACKUP

攻撃者は、データまたはクレデンシャルのバックアップを標的として、データをこっそりと盗もうと試行するかもしれない。バックアップは、パーソナルコンピュータまたはエンドユーザのバックアップリポジトリ上に格納されるので、企業は、セキュリティ侵害を検知する可能性が低い。

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.MOBILE_DEVICE_PLATFORM

MDM エージェントは、MDFPP に適合評価を受け、暗号サービスとデータ保護と同様にポリシー実施を提供すると想定されている、モバイルプラットフォーム及びハードウェアに依存している。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及びソフトウェア完全性検証を提供する。

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ポリシー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、モバイルデバイスおよび 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)。

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.WIRELESS_NETWORK

無線ネットワークはモバイルデバイスに対して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) ）で特定される。
- **拡張 SFR**：SFR 名の後にラベル”EXT”を付けることで特定される。

5.2 保証アクティビティのテスト環境

MDM エージェントの SFR の保証アクティビティのテスト環境は、エージェント EP が MDM PP または MDF PP を拡張するかどうかによって異なる。

本 EP が MDM PP を拡張する場合、保証アクティビティは、ベース MDM PP に適合する評価における MDM サーバを用いて実行されなければならない(shall)、また本 EP の多くの保証アクティビティは、MDM PP の保証アクティビティと結合されてもよい。

本 EP が MDF PP を拡張する場合、保証アクティビティは、エージェントのすべての機能を検査できるようなテスト用 MDM サーバと共に実行されなければならない(shall)。本テストサーバは、商用製品であることは要求されない、またテストツールとしてのみモバイルデバイスベンダーによって提供されてもよい。本 EP の多くの保証アクティビティは、MDF PP の保証アクティビティと結合されてもよい。

5.3 MDF PP セキュリティ機能要件の指示

本 EP が MDF PP を拡張している場合、MDM エージェントは、モバイルデバイスによって実装され、ベース PP に適合する評価を受けた、多くのセキュリティ機能を活用することが期待される。本セキュリティ機能には、以下が含まれる FCS_CKM.1、FCS_CKM.2(1)、FCS_CKM_EXT.4、FCS_COP.1(*)、FCS_RBG_EXT.1、FCS_TLSC_EXT.1、FIA_X509_EXT.1、FIA_X509_EXT.2、FIA_X509_EXT.3、FPT_TST_EXT.1、FCS_DTLS_EXT.1、及び FCS_HTTPS_EXT.1。

5.3.1 暗号サポート(FCS)

FCS_STG_EXT.4 暗号鍵ストレージ

以下の要件は、名称を除き、MDM PP を拡張する EP の暗号鍵ストレージ要件と同一である。名称は、明確化のために異なり、1 つはベース PP によってエージェントの ST に追加されなければならない(must)。

FCS_STG_EXT.4.1 MDM エージェントは、すべての永続的な秘密及びプライベート鍵について、プラットフォーム提供の鍵ストレージを利用しなければならない(shall)。

適用上の注釈： *本要件は、モバイルプラットフォームによって使用中でないとき、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セキュアに格納されることを保証する。*

保証アクティビティ

TSS

評価者は、ST において本要件を満たす必要がある永続的な秘密(クレデンシャル、秘密鍵)及びプライベート鍵のそれぞれが TSS に列挙されていることを検証すること。これらの項目のそれぞれについて、評価者は、それが使用される目的これが格納される方法について、及び ST でサポートされるとおり列挙されたそれぞれのプラットフォームについて、TSS に列挙されていることを確認すること。評価者は、エージェントが永続的な秘密とプライベート鍵を格納するためのプラットフォーム提供の API を呼び出すことを検証しなければならない(shall)。

5.3.2 高信頼パス／チャネル(FTP)

FTP_ITC_EXT.1 高信頼チャネル通信

本 EP が MDF PP を拡張する場合、エージェントとサーバ間の通信チャネルは、TOE の外部であり、MDF PP の FTP_ITC_EXT.1 が以下のとおり修正されるべきである。

FTP_ITC_EXT.1.1 TSF は、それ自身と他の高信頼 IT 製品間に、他の通信から論理的に区別され、その端点の保証された識別、及び暴露からチャネルデータの保護、及びチャネルデータの改変の検知を提供するため、[*選択：TLS、DTLS、HTTPS*]を利用しなければならない(shall)。

適用上の注釈： *本要件は、ベース PP から継承される：モバイルデバイスは、MDF PP で義務付けられた通信チャネルのためのベース PP と同じく義務付けられた暗号プロトコルを実行することが要求される。ST 作成者は、TLS、DTLS、または HTTPS の一つを選択しなければならない(must)。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、あらゆる監査ログ、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、MDM エージェントから MDM サーバへ送信される設定データの送信が、命令されたとき、または設定可能な周期で適切に保護されることを保証するものである。本高信頼チャネルは、MDM サーバから MDM エージェントへ送信されたあらゆるコマンドとポリシーについても保護する。MDM エージェントまたは MDM サーバのいずれかが接続を開始することができる。

本高信頼チャネルは、登録された MDM エージェント及び 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 サーバ間

の登録操作中の接続の両方に対して保護する。異なるプロトコルは、これらの2 つの接続に対して利用可能であり、TSS における記述はこの相違について明確化するべきである。

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、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し、次にそれらの選択に対応する附属書C における詳細な要件が、まだ存在していない場合には、ST に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なサービスは、プラットフォーム提供サービスを用いて満たされてもよい。

FTP_ITC_EXT.1.2 TSF は、TSF 及び MDM サーバ及び[*選択 : MAS サーバ、その他の IT エンティティなし*] が、高信頼チャネルを介して通信を開始するのを許可なければならない(shall)。

適用上の注釈 : *その他のすべての適用例について、モバイルデバイスは、通信を開始する ; しかし、MDM エージェントについて、MDM サーバも通信を開始してもよい。本要件は、MDF PP の要件を置き換える。*

FTP_ITC_EXT.1.3 TSF は、MDM エージェントと MDM サーバ間のすべての通信及び[*選択 : MAS サーバ及び MDM エージェント間のすべての通信、その他の通信なし*] のために、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 : *本エレメントは、MDF PP から継承される ; モバイルデバイスは、MDM エージェントと MDM サーバ間で高信頼チャネルを管理用通信のために開始し、その他の用途のために、その他の信頼される IT エンティティへその他の高信頼チャネルを開始してもよい。*

保証アクティビティ

以下の追加の保証アクティビティが実行されなければならない(shall)。

TSS

評価者は、それらの通信が保護される方法に沿って、エージェント・サーバ通信の方法が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、リモート 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要件で規定され者と一貫していること、及び ST の要件に含まれていること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 MDM エージェントと MDM サーバ及び条件付きで MAS サーバとの間の通信チャネルの設定についての指示がサポートされるそれぞれの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

それぞれのサポートされる識別子タイプ(DN を除く)について、評価者は、以下のテストを繰り返さなければならない(shall) :

テスト 1 : 評価者は、それぞれの規定された(操作ガイダンスで)エージ

ェント・サーバ通信方式を用いる通信方法が、操作ガイダンスで記述されるとおりの接続をセットアップし、通信が成功することを保証しつつ、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、それぞれの MDM サーバと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されているプロトコルとしてのトラフィクを識別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対応する。

5.4 MDM PP セキュリティ機能要件の指示

本 EP が MDM PP を拡張する場合、エージェントは、MDM TOE の一部であり、あらゆる MDM TOE についての要件も MDM エージェントへ適用される。これらのセキュリティ要件には、以下が含まれる FCS_CKM.1、FCS_CKM.2、FCS_CKM_EXT.4、FCS_COP.1(*)、FCS_RBG_EXT.1、FIA_X509_EXT.1、FIA_X509_EXT.2、FCS_X509_EXT.3、FIA_X509_EXT.4、FCS_DTLS_EXT.1、及び FCS_HTTPS_EXT.1。ST 作成者は、それぞれのエージェントについて適切な選択を行うため、それぞれのエージェントについての MDM PP における要件を繰り返すべきである。

5.4.1 暗号サポート(FCS)

FCS_STG_EXT.4 暗号鍵ストレージ

以下の要件は、名称を除き、MDF PP を拡張する EP の暗号鍵ストレージ要件と同一である。名称は、明確化のために異なり、1 つはベース PP によってエージェントの ST に追加されなければならない(must)。

FCS_STG_EXT.4.1(2) MDM エージェントは、すべての永続的な秘密及びプライベート鍵について、プラットフォーム提供の鍵ストレージを利用しなければならない(shall)。

適用上の注釈： *本要件は、モバイルプラットフォームによって使用中でないとき、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セキュアに格納されることを保証する。*

保証アクティビティ

TSS

評価者は、ST において本要件を満たす必要がある永続的な秘密(クレデンシャル、秘密鍵)及びプライベート鍵のそれぞれが TSS に列挙されていることを検証すること。これらの項目のそれぞれについて、評価者は、それが使用される目的これが格納される方法について、及び ST でサポートされるとおり列挙されたそれぞれのプラットフォームについて、TSS に列挙されていることを確認すること。評価者は、エージェントが永続的な秘密とプライベート鍵を格納するためのプラットフォーム提供の API を呼び出すことを検証しなければならない(shall)。

FCS_TLSC_EXT.1　　TLS クライアントプロトコル

ST 作成者は、MDM PP のオプショナル要件から FCS_TLSC_EXT.1 を含めなければならない(shall)。

5.4.2 TSF の保護 (FPT)

EP が MDM PP を拡張する場合、エージェントとサーバ間の通信チャネルは、TOE の内部であり、MDM PP における FPT_ITT.1 によって対処される。

5.5 TOE セキュリティ機能要件

5.5.1 セキュリティ監査 (FAU)

FAU_ALT_EXT.2 エージェント警報

FAU_ALT_EXT.2.1　MDM エージェントは、以下の監査事象のいずれかの事象において、MDM サーバへの高信頼チャネルを介して警報を提供しなければならない(shall)：

- モバイルデバイスへのポリシーの適用成功、
- 以下の[*選択：受信、生成*] ：周期的な到達可能性の事象の、

[*選択：*

- *登録状態の変更*、
- *MAS サーバからのアプリケーションのインストール失敗*、
- *MAS サーバからのアプリケーションのアップデート失敗*、
- *[割付：その他の事象]*、*その他の事象なし*]

適用上の注釈：　*高信頼チャネルは、エージェントが MDM サーバ(訳注：MDM PP の間違い)を拡張する場合は FPT_ITT.1 で定義され、エージェントが MDF PP を拡張する場合は FTP_ITC_EXT.1 で定義される。本要件の「警告」(“Alert”)は、監査記録または通知と同様に単純なものであってよい。FAU_ALT_EXT.2.2 毎に、キュー(待ち行列)に何らかの以前の警告がある場合、それらの警告は高信頼チャネルが利用可能であるときに送信されなければならない。*

本要件は、MDM エージェントが上記の事象の一つが発生したなら MDM サーバに通知しなければならない(shall)ことを保証するものである。ポリシーのインストール成功の受領がないということは、ポリシーのインストール失敗を示す。

周期的な到達可能性の事象は、デバイスネットワーク到達可能性を決定するための MDM サーバのポーリングに MDM エージェントが応答すること、または到達可能であることをサーバに定期的に通知するように MDM エージェントが設定可能であること、のいずれかを保証する。ST 作成者は、最初の場合に「受信」を選択しなければならなず(must)、2 番目に「生成」を選択しなければならない(must)。MDM サーバに対応する要件は、MDM PP の FAU_NET_EXT.1 である。

ST 作成者は、さらなる事象を割り付けるか、「その他の事象なし」を選択するかのいずれかを行わなければならない(must)。警告は、MDM サーバへ到達するために時間がかかるかもしれないし、または接続性が低いため、到着しないかもしれないことに留意されたい。

保証アクティビティ

TSS

評価者は TSS を検査して、その警報がどのように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、そのポリシーアップデートの候補がどのように入手されるかについて TSS に記述されていることを保証する；また成功する場合(ポリシーアップデートがインストールされる) 及び不成功の場合 (ポリシーアップデートがインストールされない) に取られるアクションについて TSS に記述されていることを保証する。その処理を実行しているソフトウェアコンポーネントについても、TSS で特定されて、評価者により検証されなければならない(must)。

評価者は、到達可能性事象がどのように実装されるかについて、及び FMT_SMF_EXT.3.2 で設定可能が選択されるかどうかについて、TSS に記述されていることを保証する。評価者は、誰(MDM エージェントまたは MDM サーバ) が到達可能性事象を開始するかについて、本記述が明確に示していることを検証する。

テスト

テスト 1 : 評価者は、テスト環境 MDM サーバから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、MDM エージェントがアップデートを受けれ、設定された変更を行い、ポリシーアップデートの成功を MDM サーバへ報告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、FAU_ALT_EXT.1.1 で列挙されたそれぞれのアクションを実行し、その警告が実際に MDM サーバへ到達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、ネットワーク到達可能性テストをこのような接続のある場合とない場合の両方で、実行するよう MDM エージェントを設定し、結果がそれぞれを反映することを保証しなければならない(shall)。

FAU_ALT_EXT.2.2 MDM エージェントは、高信頼チャネルが利用可能でない場合、警告を待ち行列にキューイングしなければならない(shall)。

適用上の注釈： *高信頼チャネルが利用可能でない場合、警告はキューイングされなければならない(shall)。高信頼チャネルが利用可能となるとき、キューイングされた警告は送信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、どのような状況の下で、もしあれば、警告が生成されなくてもよいか(例、デバイスが電源切断または高信頼チャネルからの切断されている)、警告がキューイングされる方法、及びキューイングされたメッセージの最大保存量について、TSS に記述されていることを保証しなければならない(shall)。

テスト

評価者は、MDM エージェントからのネットワーク接続性を無くし、

FAU_ALT_EXT.2.1 で定義されるとおり警告／事象を生成しなければならない(shall)。評価者は、MDM エージェントへのネットワーク接続性を回復し、TOE が切断され間に生成された警告が接続性に再確立に際して、MDM エージェントによって送信されることを検証しなければならない(shall)。

FAU_GEN.1(2) 監査データ生成

以下の要件がFAU_GEN.1.2(2)との関連に沿って列挙されないことに留意されたい。これは、監査データの生成が常に TSF の責任である(即ち、監査対象事象は TOE のふるまいに基づいて発生する)ためであるが、監査データの記録は、TOE 境界の内部、または下層のモバイルデバイスプラットフォームのいずれかによるものである。この理由で、FAU_GEN.1.2(2)は、以下のセクション 5.6.1 で定義される。ST 作成者は、常に FAU_GEN.1.1(2)及びFAU_GEN.1.2(2)の両方を以下に関わらず含む；唯一の相違は、FAU_GEN.1.2(2) が TOE によって実行されるか、または TSF が下層のプラットフォームに依存する場合である。

FAU_GEN.1.1(2) **MDM エージェント**は、以下の監査対象事象の **MDM エージェント**監査記録を生成できなければならない(shall)：

- **MDM エージェントの開始と終了、**
- **MDM ポリシーにおける変更、**
- **MDM サーバによって命令されるあらゆる改変、**
- **表 1 で列挙された具体的に定義された監査対象事象、**
- **[*割付：その他の*事象]**

適用上の注釈： *本要件は、MDM エージェントの監査記録に含まれるべき情報を概説する。ST 作成者は、その他の監査対象事象を直接FAU_GEN.1.1 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。*

MDM ポリシーの変更は、そのポリシーが変更されることを最小限示さなければならない(must)。事象の記録には、以前のポリシーと新しいポリシーの間の相違を含む必要はない。MDM サーバによって命令された改変がFMT_SMF.1.1 に列挙されたそれらのコマンドである。

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)。それぞれの監査記録フォーマットタイプはそれぞれのフィールドの概説に沿って網羅されなければならない(must)。

テスト

評価者は、表 1 で定義される監査対象事象を実行するために TOE を利用しなければならない(shall)、またただし監査記録が TSS に記述されたものと一貫する内容とフォーマットで生成されることを観測しなければならない。本テストが直接セキュリティメカニズムのテストと併せて達成可能であることに留意されたい。

要件	監査対象事象	追加の監査記録内容
FAU_ALT_EXT.2	警告のタイプ	追加の情報なし。
FAU_GEN.1	なし	N/A

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。
FCS_STG_EXT.4/ FCS_STG_EXT.1(1)	なし	N/A
FCS_TLSC_EXT.1	TLS セションの確立失敗。 提示された識別子の検証失敗。 TLS セションの確立／終了。	失敗の理由。 提示された識別子と参照識別子。 接続の非 TOE 端点。
FIA_ENR_EXT.2	管理における登録。	MDM サーバの参照識別子。
FMT_POL_EXT.2	ポリシー検証の失敗。	検証失敗の理由。
FMT_SMF_EXT.3	機能の成功または失敗。	追加の情報なし。
FMT_UNR_EXT.1	登録抹消の試行。	追加の情報なし。
FTP_ITC_EXT.1/ FTP_ITT_EXT.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。

表 1 – 監査対象事象

FAU_SEL.1(2) セキュリティ監査事象選択

FAU_SEL.1.1(2) **TSF** は以下のような属性に基づいて、すべての監査対象事象セットから監査される事象のセットを選択することができなければならない(shall)：

- **事象の種別**；
- **監査対象セキュリティ事象の成功**；
- **監査対象セキュリティ事象の失敗**；**及び**
- **[*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 作成者のために、割付はあらゆる追加の基準または「なし」を列挙するために利用される。本選択は、MDM サーバによって設定されてもよい。*

保証アクティビティ

ガイダンス

評価者は、複数の値を選択する(該当する場合)ための文法を説明するのと同様に、監査対象事象のセットを定義する方法についての指示が操作ガイダンスに含まれていることを決定するため、操作ガイダンスを検査しなければならない(shall)。評価者は、操作ガイダンスが現在実施されている選択基準に関わらず、常に記録されているようなそれらの監査記録を特定しなければならない(shall)。

テスト

テスト 1：本要件に列挙されたそれぞれの属性について、評価者は、属性の選択が記録されるべきその属性と共に監査事象のみを引き起こす(または管理者ガイダンスで特定される常に記録されるようなもの)ことを示すための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 がより複雑な監査の事前選択の基準の特定(例、複数の属性、属性を用いた論理的表現)をサポートする場合、評価者は、この機能が正しく実装されていることを示すテストを考案し

なければならない(shall)。評価者は、テスト計画において、代表的で機能を検査するのに十分なものとしてテストのセットを正当化する解説についても提供しなければならない(shall)。

5.5.2 識別と認証 (FIA)

FIA_ENR_EXT.2 モバイルデバイスの管理への登録

FIA_ENR__EXT.2.1 MDM エージェントは、登録処理中に MDM サーバの参照識別子を記録しなければならない (shall)。

適用上の注釈： *MDM サーバの参照識別子は、MDM サーバの Distinguished Name、Domain Name、及び／または IP アドレスであるかもしれない。本要件は、あるべき情報の特定が MDM サーバと MDM エージェントの間の高信頼チャネル(FPT_ITT.1)を認証するためのネットワーク接続と参照識別子を確立するために利用されることを許可する。*

保証アクティビティ

TSS

評価者は、参照識別子のどの種別が受け入れ可能であるか、及びどのように識別子が規定されるか(例、MDM エージェントで、利用者によって、MDM サーバによって、ポリシーで、事前設定される)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、MDM サーバの参照識別子、ドメイン名、IP アドレス(接続性のため)以外の場合、MDM サーバの証明書の参照識別子の設定方法が操作ガイダンスに記述されていることを検証するため、操作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、MDM エージェントが MDM サーバへ接続できることを検証し、MDM サーバの証明書を検証するその他の保証アクティビティと併せて、MEM エージェント上で MDM サーバの参照識別子を確立するため、操作ガイダンスに従わなければならない(shall)。

5.5.3 セキュリティ管理 (FMT)

FMT_POL_EXT.2 高信頼ポリシーアップデート

FMT_POL_EXT.2.1 MDM エージェントは、企業によっ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のみを受け入れなければならない(shall)。

適用上の注釈： *本要件の意図は、ポリシーを義務付けた企業にそのポリシーを暗号学的に結び付けことであり、移行中のポリシーを保護する(FPT_ITT.1 によって既に保護されているものとして)ことではない。これは、複数の企業に接続するような利用者にとって特に重要である。*

ポリシーは、FCS_COP.1(3)のアルゴリズムを用いて企業によってディジタル署名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、候補のポリシーが MDM エージェントによって取得される方法；ポリシーアップデートのディジタル署名の検証に対応する処理；及び成功するアクション(署名が検証された)と失敗する場合(署名が検証できなかった)が 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しなければならない(shall)。処理を実行しているソフトウェアコンポーネントについても、TSS において特定され、評価者によって検証されなければならない(shall)。

テスト

評価者は、利用可能な設定インタフェース(テスト用 MDM サーバを通して)から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、アップデートが署名され、MDM エージェントへ提供されていることを検証しなければならない(shall)。評価者は、MDM エージェントがディジタル署名されたポリシーを受け付けることを検証しなければならない(shall)。

評価者は、利用可能な設定インタフェース(テスト用 MDM サーバを通して)から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、署名されていないかつ不正に署名されたポリシーを MDM エージェントへ提供しなければならない(shall)。評価者は、MDM エージェントがディジタル署名されたポリシーを受け付けないことを検証しなければならない(shall)。

FMT_POL_EXT.2.2 MDM エージェントは、ポリシー署名証明書が無効と思われる場合、ポリシーをインストールしてはならない(shall not)。

保証アクティビティ

本要件の保証アクティビティは、ベース PP で定義されるとおりに、FIA_X509_EXT.1 及び FIA_X509_EXT.2 の保証アクティビティと併せて実行される。

FMT_SMF_EXT.3 管理機能の特定

FMT_SMF_EXT.3.1 MDM エージェントは、以下の機能を実行するため、そのプラットフォームと対話できなければならない(shall)：[*選択：*

- *MDF PP での管理者提供の管理機能*、
- *MDM PP での管理者提供のデバイス管理機能*]
- MDM エージェント通信の認証に利用されるべき証明書のインポート
- [*選択：[割付：追加の機能]*、*追加の機能なし*]

適用上の注釈： *本要件は、MDM サーバから MDM エージェントへ送られた設定ポリシーを用いて下位のモバイルデバイスを設定するための MDM エージェントにおけるすべての設定機能を取り込んでいる。ST 作成者は、管理機能の情報源としてベース PP(MDF PP または MDM PP)を選択する。*

MDF PP の管理者に提供される管理機能は、MDF PP の表 4 のカラム 4 及び FPT_TUD_EXT.1(バージョン問い合わせ)で規定される。MDM PP の管理者提供のデバイス管理機能は、FMT_SMF1.1(1) で規定される；MDM PP の FMT_SMF.1.1(1) の選択における機能は、MDM エー

ジェントによってサポートされるプラットフォーム上で利用可能な機能に対応して要求される。

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、より多くのコメントと設定ポリシーを追加することができる；モバイルデバイスは、これらの追加コマンドまたは設定ポリシーをサポートしなければならない(must)。

エージェントは、MDM サーバから受信したコメントと設定ポリシーに基づいてそのプラットフォームを設定しなければならない(must)。ST 作成者は、サポートされるモバイルデバイスによって提供されない機能を主張してはならない(shall not)。本要件で ST 作成者によって実行されるすべての選択と割付は、検討されるモバイルデバイスの ST の選択及び割り付けと合致するべきである(should)。

保証アクティビティ

本保証アクティビティは、ベース PP のその他の保証アクティビティと併せて実行されてもよい。

TSS

評価者は、TSS にあらゆる割り付けされた機能が記述されること及びこれらの機能がプラットフォームによってサポートされるとおり文書化され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るモバイルデバイスについて、管理機能とポリシーの間のあらゆる相違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)。

ガイダンス

評価者は、AGD ガイダンスが本要件のそれぞれの機能を設定するための詳細な指示を含むことを検証しなければならない(shall)。

MDM エージェントが MDM システムのコンポーネント(即ち、MDM サーバがベース PP)である場合、評価者は、主張されたモバイルデバイスプラットフォームのための証拠資料を調べることによって、本エージェントのために列挙された設定可能な機能がそのプラットフォームによってサポートされることを検証しなければならない(shall)。

MDM エージェントが設定のために複数のインタフェースをサポートする場合(例えば、リモート設定とローカル設定の両方)、AGD がダンスは、何らかの機能が特定のインタフェースに限定されているかどうかを明確にすること。

テスト

テスト 1：ベース PP の保証アクティビティと併せて、評価者は、それぞれの管理者提供の管理機能の設定を試行しなければならない(shall)、またモバイルデバイスがコマンドを実行し、ポリシーを実施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、設定ガイダンスに従って MDM エージェント認証証明書を設定しなければならない(shall)。評価者は、FPT_ITT.1 のテストの実行においてこの証明書を MDM エージェントが利用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、割り付けられた機能が設定されるこ

と及び機能の意図したふるまいがモバイルデバイスによって起動されることを実証するためのテストを設計し実行しなければならない(shall)。

FMT_SMF_EXT.3.2 MDM エージェントは、以下の機能を実行できなければならない(shall):

- 管理での登録、
- 利用者が管理から登録抹消可能かどうかを設定、
- [*選択:到達可能性事象の周期性を設定*、[*割付:ほかの管理機能*]、*他の管理機能なし*]。

適用上の注釈: *本要件は、それ自身の設定のための MDM エージェントでのすべての設定を取り込んでいる。*

MDM エージェントがモバイルデバイスの一部である場合登録は、エージェントとモバイルデバイスの両方の単一の機能 (FMT_SMF_EXT.3.1) である。

MDM エージェントがモバイルデバイスとは別に開発されたアプリケーションである場合、MDM エージェントは、デバイス管理者として、それ自身をモバイルデバイスへ登録するつ頃によって、機能「管理でのモバイルデバイスの登録」(FMT_SMF_EXT.3.1 に従って) を実行する。エージェント自身は、MDM サーバをどのエージェントに対して応答するか設定することによって管理において登録される。

エージェントが FAU_ALT_EXT.2.1 の周期的な到達可能性事象を生成し、これらの事象の周期性が設定可能である場合、「到達可能性事象の周期性を設定」が選択されなければならない(must)。

保証アクティビティ

TSS

MDM エージェントが登録可能である方法について TSS に記述されていることを検証しなければならない(shall)。

TSS 記述は、MDM エージェントが登録と設定のための複数のインタフェース (例えば、リモート設定とローカル設定の両方) をサポートするかどうか明確化しなければならない(shall)。

さらに、評価者は、割付された場合、MDM エージェントのあらゆる管理機能が TSS に記述されていることを検証しなければならない(shall)。

ガイダンス

評価者は、本要件においてそれぞれの機能を設定するための詳細な指示が 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

テスト 1 : 他の保証アクティビティと併せて、評価者は、TSS で特定されたそれぞれのインタフェースと共に管理において MDM エージェントの登録を試行しなければならない(shall)、また MDM エージェントがそのデバイスを管理でき、MDM サーバと通信できることを検証しなければならない(shall)。

テスト 2 : (条件付き) FAU_ALT_EXT.2.1 の保証アクティビティと併せて、評価者は、いくつかの設定された時間周期で到達可能性事象についての周期性を設定しなければならず(shall)、また MDM サーバがそのスケジュールで警告を受信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、割り付けられた機能が設定されること及び機能の意図したふるまいがモバイルデバイスによって起動されることを実証するためのテストを設計し実行しなければならない(shall)。

FMT_UNR_EXT.1　　利用者登録抹消の防止

FMT_UNR_EXT.1.1　MDM エージェントは、管理からモバイルデバイスの登録抹消の試行に際して以下のふるまいを実施するためのメカニズムを提供しなければならない(shall) :
[*選択 : 登録抹消の発生を防止する、修正アクションを適用する*]。

適用上の注釈 :　*登録抹消は、登録された状態から登録されていない状態へ遷移するアクションである。利用者が登録抹消することの防止が設定可能である場合、管理者は、利用者が MDM サーバを介して登録抹消することを許可されているかどうか設定すること。*

それらの登録抹消が許可される設定について、例えば、BYOD 用途について、MDFPP は、FMT_SMF_EXT.2.1 における企業データのワイプ(訳注 : 完全消去)のような、登録抹消の際に実行される修正アクションについて記述すること ; しかし、MDM エージェントは、エージェントが動作するモバイルデバイスによってサポートされるそれらのアクションに限定される。

保証アクティビティ

TSS

評価者は、利用者が登録抹消することを防止するために利用されるメカニズム、または登録抹消されるときに適用される修正アクションについて、TSS に記述されていることを保証しなければならない(shall)。

ガイダンス

評価者は、管理者ガイダンスがそれぞれの利用可能な設定インタフェースにおいて、登録抹消防止を設定する際に管理者に指示することを保証しなければならない(shall)。任意の設定が利用者に登録抹消を許可する場合、エージェントを登録抹消するようなアクションについても、ガイダンスに記述されていること。

テスト

「登録抹消の発生を防止する」が選択される場合 :

テスト 1 : 評価者は、それぞれの利用可能な設定インタフェースについての管理者ガイダンスに従ってエージェントを設定しなければならない(shall)、デバイスの登録抹消を試行しなければならない(shall)、その試行が失敗することを検証しなければならない(shall)。

「修正アクションを適用する」が選択される場合 :

テスト 2 : 任意の設定が利用者に登録抹消を許可する場合、評価者は、

エージェントが利用者に登録抹消を許可するよう設定し、登録抹消を試行し、修正アクションが適用されることを検証しなければならない(shall)。

5.6 TOE またはプラットフォームのセキュリティ機能要件

5.6.1 セキュリティ監査 (FAU)

FAU_GEN.1(2) 監査データ生成

FAU_GEN.1.2(2) **[選択：TSF、TOE プラットフォーム]**は、それぞれの **MDM エージェント**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)：

- **事象の日付と時刻、**
- **事象の種別、**
- **サブジェクトの本人性、**
- **(関連する場合) 事象の結果 (成功または失敗)、**
- **表 1 における追加の情報、**
- **[*割付：その他の関連監査情報*]。**

適用上の注釈： *すべての監査は、少なくとも FAU_GEN.1.2(2) で述べられた情報を含まなければならない(must)が、割付可能なより多くの情報を含んでもよい。ST 作成者は、MDM エージェントによって実行されるような、及び MDM エージェントのプラットフォームによって実行されるような、監査記録の情報について、TSS において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、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)。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(shall)。

テスト

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)。

ここでのテストが直接セキュリティメカニズムのテストを合わせて達成可能であることに留意されたい。

5.7 TOE セキュリティ保証要件

本 EP に適合した評価が行われる TOE は、同様に、MDF PP または MDM PP に適合した評価が本質的に行われることに留意することが重要である。それらの PP は、SFR とセキュリティ保証要件(SAR)の両方に関連する多くの保証アクティビティを含んでいる。さらに本 EP は、ベース PP で特定される SAR を単に詳細化するような多くの SFR ベースの保証アクティビティを含んでいる。MDF PP または MDM PP によって規定される SAR に関連す

る保証アクティビティは、TOE 全体に対して実行される。

A. オプション要件

セクション 2 で示したように、本 PP の本体にはベースライン要件 (TOE 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 A、附属書 B、及び附属書 C で規定されている。

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 B に含まれる) は、EP 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 C に含まれる) は、本 EP へ適合するためには要求されないが、本 EP 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だろう。ST 作成者には、附属書 A、附属書 B、及び附属書 C の要件と関連するかもしれないが列挙されない(例、FMT-タイプの要件)が ST にも含まれていることを保証する責任があることに留意されたい。

現時点では、オプション要件は特定されていない。

B. 選択ベース要件

本 EP の序論で示したように、ベースライン要件 (TOE またはその基盤となるプラットフォームによって行われなければならない(must)もの) が EP の本文に含まれている。本 EP の本文での選択に基づく追加の要件がある；特定の選択がなされる場合、以下の追加の要件が含まれる必要がある。

現時点では、選択ベースの要件は特定されていない。

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。

いつでも、これらが本 EP へ適合する限りは 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_STG_EXT.1 セキュリティ監査事象ストレージ

FAU_STG_EXT.1.1 MDM エージェントは、プラットフォーム提供の監査ストレージにおける MDM 監査記録を格納しなければならない(shall)。

適用上の注釈 : *FAU_STG_EXT.1 は、モバイルデバイス基盤プロテクションプロファイル バージョン3 に適合するようなMDM エージェントプラットフォーム(即ち、モバイルデバイス)の ST にのみ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、監査記録の TSS 記述がその記録の格納方法を示すことを検証しなければならない(shall)。評価者は、エージェントが監査記録を格納するため、プラットフォーム提供の API を呼び出すことを検証しなければならない(shall)。

C.1.2 TSF の保護 (FPT)

FPT_NET_EXT.1 ネットワーク到達可能性

FPT_NET_EXT.1.1 TSF は、サーバとの最後に成功した接続に関連する設定可能な[*選択 : 正の整数の喪失した到達可能性事象の発生回数、時間制限の超過*]に到達したときを検出しなければならない(shall)。

適用上の注釈 : *本要件は、エージェントがサーバとの接続性が切れてから長すぎる時間が経過したかを決定することを可能とする。喪失した到達可能性事象の許可された回数またはサーバとの最後に成功した接続からの時間制限の設定は、エージェントのサーバ設定ポリシー(FMT_SMF.1.1(1) 機能 56a) で取り扱われ、次に FPT__NET_EXT.1.1 は、MDM サーバ ST に含まれなければならない(shall)。*

長すぎる時間、エージェントのサーバとの接続性が切れた場合、機能 56b で規定される修正アクションが発生しなければならない(shall)。例えば、エージェントがサーバからのコマンドを要求することなしにデバイスをワイプしなければならない(shall)ような許可された時間に

エージェントがサーバと同期しなかった場合。

保証アクティビティ

TSS

評価者は、サーバとの最後に成功した接続からどのくらい時間が経過したか(即ち、喪失した接続可能性の事象の総計または時間)をエージェントがどのような決定するかについての記述が TSS に含まれることを検証しなければならない(shall)。喪失した接続可能性の事象の総計が選択される場合、評価者は、到達可能性事象がどの程度頻繁に送信されるかの記述が TSS に含まれることを検証しなければならない(shall)。

ガイダンス

評価者は、必要な場合、最後に成功したサーバとの接続からの時間がいつ到達したかを検出するために TOE を設定する方法について､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

テスト 1 : 評価者は、FMT_SMF.1.1(1) 機能 56 に従ってエージェントのサーバ設定ポリシーを設定しなければならない(shall)。デバイスは、サーバとの接続を防止するような機内モードに置かれなければならない(shall)。評価者は、設定された時間の後、機能 56 で選択された修正アクションが発生することを検証しなければならない(shall)。

D. エントロピー証拠資料と評定

TOE は、MDF PP 及び MDM PP の「エントロピー証拠資料と評定」セクションで概説される要件を超えたエントロピー源について記述するような追加の補足情報を要求しない。他のベース PP 要件と同様に、唯一の追加の要件は、ベース PP で要求される機能に追加された TOE の具体的な MDM エージェント機能に対しても適用されるエントロピー証拠資料である。

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

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
FAU_ALT_EXT.2.1 機能 c	ST に含まれる。
FMT_UNR_EXT.1.1	「登録抹消の発生を防止する」を選択。

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_UNR_EXT.1.1	「登録抹消の発生を防止する」を選択。

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 PP]	Protection Profile for Mobile Device Management, Version 3.0, November 2016

G. 頭字語

本 EP のすべての関連する頭字語は、MDF PP 及び／または MDM PP で定義される。