モバイルデバイス管理のプロテクションプロファイル

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

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_mdm_v1.1.pdf

2014 年 3 月 7 日

バージョン 1.1

平成 26 年 10 月 10 日　翻訳 暫定第 0.1 版

独立行政法人情報処理推進機構

技術本部 セキュリティセンター

情報セキュリティ認証室

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 3 月 7 日	誤字修正、目次への反映。

目次

内容

改版履歴 2
1. はじめに (イントロダクション) 6
1.1 適合する評価対象 (TOE) 6
1.2 TOE の用途 7
2. セキュリティ課題記述 7
2.1 脅威 8
2.1.1 悪意や欠陥のあるアプリケーション 8
2.1.2 ネットワーク攻撃 8
2.1.3 ネットワークの盗聴 8
2.1.4 物理アクセス 8
2.2 前提条件 8
2.3 組織のセキュリティ方針 8
3. セキュリティ対策方針 9
3.1 TOE のセキュリティ対策方針 9
3.1.1 保護された通信 9
3.1.2 システム報告 9
3.1.3 モバイルデバイスの設定 9
3.1.4 管理機能の運用管理 10
3.2 運用環境のセキュリティ対策方針 10
4. セキュリティ要件 11
4.1 表記法 11
4.2 TOE セキュリティ機能要件 11
セキュリティ監査 (FAU) 11
識別と認証 (FIA) 13
セキュリティ管理 (FMT) 14
TSF の保護 (FPT) 21
4.3 MDM サーバまたはプラットフォームのセキュリティ機能要件 22
セキュリティ監査 (FAU) 22
暗号サポート (FCS) 23
識別と認証 (FIA) 43
TSF の保護 (FPT) 47

高信頼パス／チャネル (FTP) 48
4.4 MDM エージェントまたはプラットフォームのセキュリティ機能要件 50
暗号サポート (FCS) 50
識別と認証 (FIA) 68
TSF の保護 (FPT) 71
4.5 セキュリティ保証要件 72
ASE クラス：セキュリティターゲット評価 73
ADV クラス：開発 73
AGD クラス：ガイダンス文書 74
ALC クラス：ライフサイクルサポート 77
ATE クラス：テスト 78
AVA クラス：脆弱性評定 79
5. 根拠 81
附属書 A： 参考表 82
A.1 前提条件 82
A.2 脅威 83
A.3 組織のセキュリティ方針 83
A.4 TOE のセキュリティ対策方針 84
A.5 運用環境のセキュリティ対策方針 84
附属書 B： オプションの要件 86
B.1 オプションの TSF 要件 86
セキュリティ監査 (FAU) 86
B.2 オプションの MDM サーバまたは MDM サーバプラットフォーム要件 87
セキュリティ監査 (FAU) 87
附属書 C： 選択に基づいた要件 89
C.1 選択に基づいた TSF 要件 89
暗号サポート (FCS) 89
C.2 選択に基づいた MDM サーバまたは MDM サーバプラットフォーム要件 90
暗号サポート (FCS) 90
識別と認証 (FIA) 102
C.3 選択に基づいた MDM エージェントまたは MDM エージェントプラットフォーム要件 102
暗号サポート (FCS) 102
識別と認証 (FIA) 112

C.4　監査対象事象 113
附属書 D：　オブジェクティブな要件 118
D.1　オブジェクティブな TSF 要件 118
セキュリティ監査 (FAU) 118
セキュリティ管理 (FMT) 119
D.2　オブジェクティブな MDM サーバまたは MDM サーバプラットフォーム要件 120
TOE アクセス (FTA) 120
D.3　オブジェクティブな MDM エージェントまたは MDM エージェントプラットフォーム要件 120
セキュリティ監査 (FAU) 120
暗号サポート (FCS) 121
附属書 E：　エントロピーの文書化と評定 123
附属書 F：　用語集 124
技術的定義 124
コモンクライテリア定義 126
附属書 G：　初期化ベクトルの要件 127

表目次

表 1 TOE セキュリティ保証要件 73
表 2 TOE の前提条件 82
表 3 脅威 83
表 4 組織のセキュリティ方針 83
表 5 TOE のセキュリティ対策方針 84
表 6 運用環境のセキュリティ対策方針 84
表 7 TOE セキュリティ機能要件及び監査対象事象サーバ 113
表 8 TOE セキュリティ機能要件及び監視対象事象エージェント 115
表 9 NIST 承認暗号モードの参照情報と IV 要件 127

1. はじめに (イントロダクション)

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、エンタープライズ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、エンタープライズデータの処理とエンタープライズ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エンタープライズ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。

1.1 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、MDM サーバソフトウェアと MDM エージェントという、2 つの主要なコンポーネントから構成される。**MDM** はこれらの構成要素の完全な集合体であるとみなされ、またこれらは協調してふるまわなければならない (must)。このような状況においては、ベンダに関わらず、すべてのコンポーネントを結合して評価にゆだねることが必要となる。

MDM 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ワイヤレスネットワークから構成される。

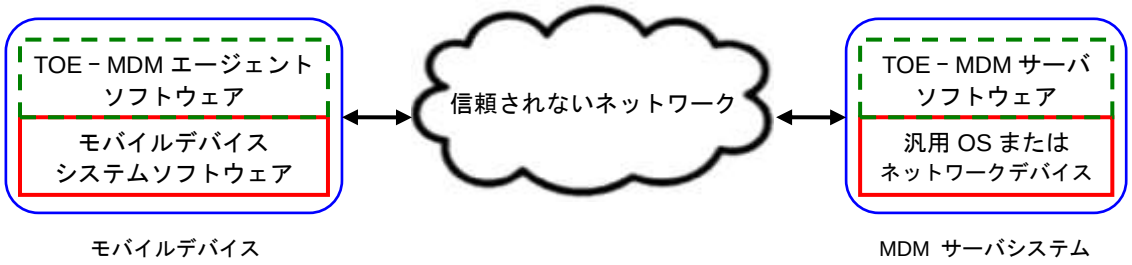

図 1：MDM システムの運用環境

MDM エージェントは、アプリケーションとしてモバイルデバイス上にインストールされるか、またはモバイルデバイスのオペレーティングシステム (OS) の一部である。MDM エージェントは、エンタープライズ管理者によってコントロールされる MDM サーバへのセキュアな接続を確立する。MDM エージェントは (図 1 の緑の点線で示すように) モバイルデバイスのプラットフォームと密接に対話するか、またはその一部として、ポリシーを確立しデバイス状態の問い合わせを受け取らなければならない (must)。一方モバイルデバイスは、*モバイルデバイス基盤のためのプロテクションプロファイル*に特定されるそれ自身のセキュリティ要件を有するため、MDM の評価と並行して、またはそれ以前に、それらの要件に対して評価されなければならない (must)。

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、ポリシーの構成と MDM エージェントへの送信、デバイスの状態に関する報告の収集、及びエージェントへの指令の送信を担当する。MDM サーバソフトウェアが実行され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

であり、*汎用オペレーティングシステムのプロテクションプロファイル*または*ネットワークデバイスのプロテクションプロファイル*においてそれぞれ特定される。

1.2 TOE の用途

本プロテクションプロファイルの要件は、以下の使用事例中のセキュリティ課題へ対処するようにデザインされている。各使用事例には、さまざまなレベル及び種類のリスクの受容が必要とされる。

- **汎用エンタープライズ用途のエンタープライズ所有デバイス**

  エンタープライズ所有デバイスの汎用業務用途には、構成及びソフトウェアインベントリへの高度なエンタープライズのコントロールが必要とされる。エンタープライズ管理者は MDM 製品を用いて、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。利用者は、インターネット接続を用いてウェブをブラウズしたり会社のメールへアクセスしたりエンタープライズアプリケーションを実行する可能性があるが、この接続はエンタープライズの高度なコントロール下にあるかもしれない。利用者は、データを保管し、個人的な、非エンタープライズ用途にアプリケーションを利用することが期待される。エンタープライズ管理者は MDM 製品を用いて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。MDM は、修正アクションのための指令を発行するかもしれない。

- **特化した高セキュリティ用途のセンタープライズ所有デバイス**

  ネットワーク接続性が意図的に制限され、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エンタープライズ所有デバイスは、特化した高セキュリティの使用事例に適切である。先ほどの使用事例と同様に、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エンタープライズ所有のネットワークと通信することのみが可能であるかもしれず、またインターネットとの接続性すら許可されないかもしれない。デバイスの使用には、いかなる汎用の使用事例においても現実的とはみなされないような、しかし高度に機密性のある情報へのリスクを軽減できるような、利用ポリシーの遵守が要求されるかもしれない。

- **個人及びエンタープライズ用途の個人所有デバイス**

  個人的な活動とエンタープライズデータの両方に用いられる個人所有デバイスは、一般に私的デバイスの業務利用 (BYOD) と呼ばれる。エンタープライズ所有のケースとは異なり、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、エンタープライズがデバイスへプッシュできるセキュリティポリシーの点でエンタープライズの役割は限定されており、デバイスの機能を限定するようなポリシーが受容されることは考えづらい。しかし、エンタープライズは利用者にエンタープライズネットワークへの完全な (またはほぼ完全な) アクセスを許可するのであるから、エンタープライズは例えばパスワードや画面ロックポリシーなど一定のセキュリティポリシーと、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、エンタープライズデータの抹消など、修正アクションを確立することができる。

2. セキュリティ課題記述

附属書 A には、セキュリティ課題記述 (SPD) をより「伝統的」な形で提示してある。以下のセクションでは、附属書 A の「伝統的」な言明への参照を含めて、適合 TOE が対処する課題を詳述する。

2.1 脅威

2.1.1 悪意や欠陥のあるアプリケーション

悪意や欠陥のあるアプリケーションの脅威が存在するのは、モバイルデバイスへロードされるアプリケーション (アプリ) に、悪意のある、または悪用可能なコードが含まれている可能性があるためである。このようなコードは、もしかするとソフトウェアライブラリの一部として、開発者によって無意識のうちに取り込まれるかもしれない。悪意のあるアプリは、アクセス権のあるデータの漏出を試行するおそれがある。悪意のあるアプリはデバイスのセンサ (位置情報、カメラ、マイクロフォン等) をコントロールして利用者周囲の情報収集活動を、たとえこれらの活動にデータの常駐やデバイスからの送信が伴わなくても、行うことができるかもしれない。欠陥のあるアプリは、それがなければ防げたであろうネットワークベースまたは物理的な攻撃を行う手段を攻撃者に与えてしまうかもしれない。

[T.MALICIOUS_APPS]

2.1.2 ネットワーク攻撃

攻撃者は、ワイヤレス通信チャネル上またはネットワーク基盤上のどこかに位置を手に入れることができるかもしれない。この有利な立場から、攻撃者はモバイルデバイスとの通信を開始したり、運用環境の構成要素とその他のエンドポイントとの間の通信を改変したりするかもしれない。この通信の改変によって、攻撃者は MDM エージェントや MDM サーバなどのエンドポイントを詐称することができるかもしれない。

[T.NETWORK_ATTACK]

2.1.3 ネットワークの盗聴

ネットワーク攻撃の脅威と同様に、攻撃者はワイヤレス通信チャネル上またはネットワーク基盤上のどこかに位置を手に入れることができるかもしれない。次に攻撃者は、TOE の構成要素間でやり取りされるデータの監視やアクセスの獲得ができてしまうかもしれない。このデータを監視することによって、攻撃者は暗号鍵や人間の利用者の認証データなどを含む、セキュリティ上重要なデータを傍受できてしまうかもしれない。

[T.NETWORK_EAVESDROP]

2.1.4 物理アクセス

基盤となるモバイルデバイスプラットフォームの紛失や盗難により、利用者データ、中でも最も重要なクレデンシャルの損失が引き起こされるかもしれない。物理的な攻撃には、外部ハードウェアポート、利用者インタフェースを通して、またはストレージ媒体への直接的かつ破壊的かもしれないアクセスを介した、デバイスへのアクセスの試行が伴う。そのような攻撃は、所有者への返還が期待できない紛失または盗難されたモバイルデバイスのデータへのアクセスを意図している。このような攻撃は主にモバイルデバイスプラットフォームに対して行われるが、TOE はこの脅威に対抗する機能を提供する。

[T.PHYSICAL_ACCESS]

2.2 前提条件

MDM の前提条件は、附属書 A.1 前提条件 に定義されている。

2.3 組織のセキュリティ方針

MDM の組織のセキュリティ方針は、附属書 A.3 組織のセキュリティ方針 に定義されている。

3. セキュリティ対策方針

3.1 TOE のセキュリティ対策方針

適合 TOE は、TOE への脅威に対抗し、またモバイルデバイスの取り込みによるエンタープライズへの新たな脅威に対抗するセキュリティ機能を提供することになる。以下のセクションでは、適合 TOE へ取り込まれるべく先に議論した脅威に照らして、この機能の記述を提供する。提供されるセキュリティ機能には、TOE のエレメントへの、及びそれらの間の保護された通信、MDM サーバへの管理アクセス、モバイルデバイスのセキュリティポリシーの構成、及びセキュリティ関連事象を検出するためのシステム報告書が含まれる。

3.1.1 保護された通信

セクション 2.1.3 に記述された TOE への、そして TOE 間の機密性のあるデータの送信 (例えば、MDM サーバから MDM エージェントへの通信、及び MDM サーバへのリモート管理) に関する問題へ対処するため、適合 TOE は高信頼通信パスを使用する。MDM サーバと MDM エージェントとの間の高信頼チャネルは、以下の標準プロトコルの 1 つ (以上) を用いて実装される：IPsec、DTLS、または TLS。MDM サーバへのリモート管理が提供される場合、これは以下の標準プロトコルの 1 つ以上を用いて実装される：IPsec または TLS/HTTPS。

セクション 2.1.2 に記述されたネットワーク攻撃の脅威へ対抗するため、本文書に記述されたプロトコルは暗号化と、各エンドポイント間の相互認証を暗号学的にセキュアな方法で提供する。これにより、悪意のある攻撃者が通信パスのいずれかのエンドポイントに対してその相手方として取って代わろうとするいかなる試行も、検出されることになる。

O.DATA_PROTECTION_TRANSIT -> (FCS_CKM.1, FCS_CKM_EXT.2(*), FCS_CKM_EXT.4, FCS_COP.1.(*), FCS_DTLS_EXT.1, FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_IV_EXT.1, FCS_RBG_EXT.1(*), FCS_STG_EXT.1, FCS_TLS_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FPT_ITT.1, FTP_TRP.1, FTP_TRP.2)

3.1.2 システム報告

システムの構成や動作の意図せぬ問題を管理者が発見できるような情報の存在を確実にするため、適合 TOE はそのような問題を指摘する報告を作成する機能を持つ。管理アクティビティの監査によって、修正アクションを促進する情報が提供される。

O.ACCOUNTABILITY -> (FAU_ALT_EXT.1, FAU_ALT_EXT.2, FAU_GEN.1(*), FAU_SAR.1, FAU_SEL.1, FAU_STG_EXT.1, FAU_STG_EXT.2)

3.1.3 モバイルデバイスの設定

モバイルデバイスは、それが保存または処理する可能性のあるエンタープライズデータを確実に保護するため、エンタープライズによって定義されたセキュリティポリシーを受け入れることができる。MDM サーバは、これらのポリシーの設定とデバイス上の MDM エージェントへの送信、MDM エージェントへのコマンドの送信、及びデバイスからの報告の収集を担当する。一方 MDM エージェントは、モバイルデバイスプラットフォームとの対話型のポリシーの確立と MDM からのコマンドの実行、及び MDM サーバへの報告の送信を担当する。

O.APPLY_POLICY -> (FIA_ENR_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FMT_POL_EXT.1, FMT_SMF.1(1), FMT_SMF.1(2))

3.1.4 管理機能の運用管理

MDM サーバソフトウェアが許可された人物によってのみ操作されることを確実にするため、その管理機能に対するアクセス制御が提供される。これには、管理機能の完全性への保護と同様に、管理者アクションの前の認証が含まれる。

O.MANAGEMENT -> (FIA_UAU.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FMT_MOF.1(*), FMT_SMF.1(3), FMT_SMR.1, FPT_TST_EXT.1, FPT_TUD_EXT.1)

3.2 運用環境のセキュリティ対策方針

TOE の運用環境によって満たされることが要求される対策方針は、附属書 A.5「運用環境のセキュリティ対策方針」で定義される。

4. 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。

4.1 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、以下のフォント規則を用いて、CC によって定義される操作を特定する。

- 割付：*イタリック体*のテキストで示す。
- PP 作成者によってなされた詳細化：エレメント番号の後に**太字**で表記された「詳細化」という単語と、**太字**の追加されたテキスト及び必要に応じて取り消し線で表記された削除によって示される。
- 選択：下線付きテキストで示す。
- 選択中の割付：*イタリック体の下線付き*テキストで示す。
- 繰返し：例えば (1), (2), (3) など、繰返し回数を括弧内に付記して示す。

明示的に言明された SFR は、TOE SFR の要件名の後にラベル「EXT」を持つことによって特定される。

4.2 TOE セキュリティ機能要件

本セクションでは、TOE の SFR を特定する。

セキュリティ監査 (FAU)

FAU_ALT_EXT.1 拡張：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. モバイルデバイスへのポリシーの適用の成功、

b. [選択：登録状態の変更、*[割付：その他の事象]*、その他の事象なし]

FAU_ALT_EXT.1.2 MDM サーバは、エージェントのネットワーク接続状態を問い合わせる能力を提供しなければならない (shall)。

適用上の注意：

高信頼チャネルは、FPT_ITT.1 で定義される。本要件における「警報」は、監査記録または通知のように単純なものであってもよい。

本要件は、上記に列挙された事象のいずれかが発生した際にはいつでも MDM エージェントが MDM サーバへ通知しなければならない (shall) ことを確実にするためのものである。ポリシーのインストールが成功したという警報が受け取られないことは、ポリシーのインストールが失敗したことを示す。また、このことは MDM サーバがポーリングによってデバイスのネットワーク到達性を判断できること、または MDM エージェントが到達可能であることをサーバへ定期的に通知を行うよう設定可能であることの、いずれかであることを確実にする。

ST 作成者は追加事象を割り付けるか、「その他の事象なし」オプションを選択するかのいずれかを行わなければならない (must)。接続性が悪いと警報が MDM サーバへ到達するまでに時間がかかったり、到達しなかったりする可能性があることに注意されたい。

保証アクティビティ：

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、そしてもし警報が生成されない可能性のある状況が存在するならばそれは何か (例えば、デバイスの電源が入っていない場合や、高信頼チャネルから切断されている場合) が記述されていることを検証しなければならない (shall)。評価者は、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FAU_ALT_EXT.1.1 に列挙された各アクションを行い、警報が実際に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2：評価者はMDM サーバまたはMDM エージェントを設定して、接続性がある場合とない場合との両方についてネットワーク接続性テストを行い、結果にそれぞれの場合が反映されることを保証しなければならない (shall)。*
- *テスト3：評価者は、接続性の問題のためMDM エージェントへ到達できない事象が、廃棄されるのではなくキューに入れられることを確認しなければならない (shall)。接続性が回復された際には、キューに入れられた事象が再送信されるべきである (should)。*

FAU_ALT_EXT.2 拡張：サーバ警報

FAU_ALT_EXT.2.1 MDM サーバは、以下のいずれかの事象が発生した際には管理者へ警報を行わなければならない (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]

適用上の注意：

MDM エージェントはMDM サーバへ、FMT_POL_EXT.1 中のポリシーのインストール失敗を報告することが要求される。本要件は、ポリシーが適切にインストールされなかった際、MDM サーバが管理者へ確実に通知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へ影響しない。

保証アクティビティ：

評価者はTSS を検査して、警報システムがどのように実装されているかが記述されていることを検証しなければならない (shall)。評価者は、MDM エージェントが適用できるべきでない (should not) ポリシーを複数設定しなければならない (shall)。これらのポリシーには、以下が含まれなければならない (shall)：

- *MDM サーバのインタフェース上で設定可能であるが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ていない設定、 もしそのような設定が存在する場合*
- *無効な設定、これには、デバイスへの送信前にポリシーを手作業で変更することが必要となるかもしれない*
- *無効なパラメタを持つ有効な設定。これにも、デバイスへの送信前にポリシーを手作業で変更することが必要となるかもしれない*

評価者はそのようなポリシーを展開し、適用失敗についてMDM サーバに警告されることを検証しなければならない (shall)。

FAU_GEN.1(1) 監査データ生成 (MDM サーバ)

FAU_GEN.1.1(1) **詳細化：MDM サーバ**は、以下の監査対象事象の **MDM サーバ**監査記録を生成できなければならない (shall)：

a. MDM サーバソフトウェア（訳注：MDM サーバにおける監査機能）の開始及び終了、

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たコマンド、

d. 表 7 に列挙された明確に定義された監査対象事象、及び

e. *[割付：その他の事象]*。

適用上の注意：

本要件は、MDM サーバソフトウェアによって生成される監査記録に含まれるべき情報の概要を示している。これらの監査記録は、MDM サーバソフトウェアによって書き込まれてもよいし、またはそれが動作するオペレーティングシステムへ発行されてもよい。ST 作成者は、その他の監査対象事象を割付中に取り込むことができる。監査対象事象は、提示されたリストには限定されない。すべての監査には、少なくとも FAU_GEN.1.2(1) に言及される情報が含まれなければならない (must) 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 はすべての管理者アクションが監査対象であることを要求しているため、これらのアクションが監査対象であるという追加的な仕様は、追加的な記録内容を要求する管理者アクションを別にして表 7 には特定されていない。管理者アクションは、FMT_MOF.1(1)に特定された管理機能による。

項目 c には、トリガまたはスケジュールに基づいて自動的に行われる可能性のあるコマンドが含まれる。

保証アクティビティ：

評価者は TSS をチェックして、すべての監査対象事象が列挙されていることを確証しなければならない (shall)。評価者は、PP によって義務付けられるすべての監査事象の種類が TSS に記述されていることをチェックして確認しなければならない (shall)。評価者は、すべての要求される監査事象に対応する監査記録を作成するように TOE を設定しなければならない (shall)。

評価者は、列挙された事象及び管理者アクションに対して TOE に監査記録を生成させることによって、TOE の正しく監査記録を生成する能力をテストしなければならない (shall)。管理者アクションについて評価者は、本 PP の文脈においてセキュリティ関連であると上記のように評価者によって判断された各アクションが監査対象であることをテストしなければならない (shall)。

ここでのテストは、セキュリティメカニズムの直接的なテストと組み合わせて達成できることに注意されたい。

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、高信頼チャネル上でリモート利用者を認証しなければならない (shall)。

適用上の注意：

MDM サーバは、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して、モバイルデバイスのリモート登録を行うユーザの認証判断を行うかもしれない。

保証アクティビティ：

評価者は TSS を検査し、登録のプロセスが記述されていることを検証しなければならない (shall)。この記述には、登録に用いられる高信頼パス (FTP_TRP.2)、利用者認証の方法 (利

用者名／パスワード、トークンなど)、認証判断の方法 (ローカルまたはリモート認証サービス)、MDM サーバの DN が記録される方法、そして認証の成功時にモバイルデバイス上及び MDM サーバ上で行われるアクションが含まれなければならない (shall)。評価者は、以下のテストを行わなければならない (shall)。

- *テスト 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 : 特定のデバイス、特定のデバイスモデル、デバイスの数、特定の時間間隔] に制限しなければならない (shall)。

適用上の注意 :

本要件は、エンタープライズ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。

保証アクティビティ :

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)。選択されたポリシーの種類のそれぞれについて、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、登録を行わせないように管理ガイダンスに従って MDM サーバの構成を試行しなければならない (shall)。評価者は、構成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、許可された数以上の追加デバイスの登録を試行してもよい。)*

FIA_ENR_EXT.1.3 MDM エージェントは、登録プロセス中に MDM サーバの DN を記録しなければならない (shall)。

適用上の注意 :

MDM サーバの DN は、MDM サーバのドメイン名または IP アドレスであってもよい。本要件によって、ネットワーク接続の確立に用いられる DN と、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) に期待される DN の特定が可能になる。ST 作成者は、DN が特定される方法 (MDM エージェント中に事前構成される、利用者によって、MDM サーバによって、ポリシー中で、など) を TSS に記述しなければならず (shall)、また適宜操作ガイダンスを提供しなければならない (shall)。

保証アクティビティ :

評価者は TSS と操作ガイダンスを検査して、DN が特定され記録される方法について記述されていることを検証し、また MDM エージェントが MDM サーバのドメイン名または IP アドレスと共に構成されることを検証しなければならない (shall)。評価者は操作ガイダンスに従って、MDM サーバに期待される DN を MDM エージェント上で確立し、その他の保証アクティビティと組み合わせて、MDM エージェントが MDM サーバと接続でき、MDM サーバの証明書の有効性を確認できることを検証しなければならない (shall)。

セキュリティ管理 (FMT)

FMT_MOF.1(1) MDM サーバの機能の管理

FMT_MOF.1.1(1) **詳細化 : MDM サーバ**は、以下の機能

- FMT_SMF.1(1) に列挙されるもの

- FMT_SMF.1(1) に列挙されるポリシーの有効化、無効化、及び変更
- FMT_SMF.1(3) に列挙されるもの

を行う能力を、*正当な管理者*へ制限しなければならない (shall)。

適用上の注意：

本要件は、FMT_SMF.1(1) に列挙される機能及びポリシーの有効化、無効化、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 サーバ自体を維持管理し構成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：

評価者は TSS と利用者文書を検査して、どのセキュリティ管理機能が管理者へ制限されているか、そして各管理機能についてどのアクションを取ることが可能か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、セキュリティ管理機能が正当な管理者に制限され、そして管理者は利用者文書に記述されるアクションのみ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、権限のない利用者として FMT_SMF.1(1) 中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) 登録機能の管理

FMT_MOF.1.1(2) **詳細化：MDM サーバ**は、登録プロセスを開始する能力を*正当な管理者及び MD 利用者*へ制限しなければならない (shall)。

適用上の注意：

本要件は、管理者と MD 利用者の両方が行うことのできる登録機能の概要を示している。登録アクションは TSS 中に、FIA_ENR_EXT.1 の一部として特定される。

保証アクティビティ：

評価者は TSS を検査して、どのように権限のない利用者が MDM サービスへの登録を拒否されるか記述されていることを検証しなければならない (shall)。この機能のテストは、FIA_ENR_EXT.1 と組み合わせて行われる。

FMT_POL_EXT.1 拡張：高信頼ポリシーアップデート (MDM エージェント)

FMT_POL_EXT.1.1 MDM エージェントは、ポリシーアップデートのインストールが成功するごとに、MDM サーバへ報告しなければならない (shall)。

保証アクティビティ：

評価者は、アップデート候補が取得される方法と、成功の (ポリシーアップデートがインストールされた) 場合と不成功の (ポリシーアップデートがインストールなかった) 場合に行われるアクションが、TSS (または操作ガイダンス) に記述されていることを保証する。また、この処理を行うソフトウェアコンポーネントも TSS 中に特定され、評価者によって検証されなければならない (must)。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、FMT_SMF.1(1) に従ってポリシーアップデートを行わなければならない (shall)。評価者は、MDM サーバが MDM エージェントへアップデートを提供することを検証しなければならない (shall)。評価者は、MDM エージェントがアップデートを受け取り、構成された変更を行い、そして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)。*

FMT_SMF.1(1) 管理機能の仕様 (エージェントのサーバ構成)

FMT_SMF.1.1(1) **詳細化：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、
2. 保護データの完全な抹消、
3. 管理からの登録解除、
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、
10. トラストアンカーデータベース中の、管理者によってインポートされた X.509v3 証明書及び [選択：その他の X.509v3 証明書なし、 [*割付：X.509v3 証明書のその他のカテゴリのリスト*]] の削除、

及び MDM エージェントへの以下のコマンド： [選択：

11. 機密性のあるデータの抹消、
12. 管理者への警報、
13. エンタープライズアプリケーションの削除、
14. セキュアな鍵ストレージへの鍵／秘密のインポート、
15. セキュアな鍵ストレージ中の、インポートされた鍵／秘密及び [選択：その他の鍵／秘密なし、 [*割付：鍵／秘密のその他のカテゴリのリスト*]] の削除、
16. アプリケーションの削除、
17. システムソフトウェアのアップデート、
18. アプリケーションのインストール、
19. MD によって記録された監査ログの読み出し、
20. [*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]

ならびに以下の MD 設定ポリシー：

21. 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
22. セッションロックのポリシー：
    a. 画面ロックの有効化／無効化
    b. 画面ロックのタイムアウト
    c. 認証失敗の回数
23. MD が接続できるワイヤレスネットワーク (SSID)
24. 各ワイヤレスネットワークのセキュリティポリシー：

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

b. セキュリティの種類を特定する能力

c. 認証プロトコルを特定する能力

d. 認証に用いられるべきクライアントクレデンシャルの特定

e. [*割付：任意の追加的な WLAN 管理機能*]

25. 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. 1 つまたは複数の正当なアプリケーションリポジトリの特定、

b. 許可されるアプリケーション及びバージョンのセットの特定（アプリケーションのホワイトリスト）

c. アプリケーションのインストールの拒否]、

26. [*割付：音声または映像収集デバイスのリスト*] の有効化／無効化ポリシー、

及び以下の MD 設定ポリシー： [選択：

27. VPN 保護の有効化／無効化ポリシー、

28. [*割付：無線のリスト*] の有効化／無効化ポリシー、

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

30. [*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、

31. 開発者モードの有効化／無効化ポリシー、

32. 保存データ保護の有効化ポリシー、

33. リムーバブルメディアの保存データ保護の有効化ポリシー、

34. ローカル認証バイパスの有効化／無効化ポリシー、

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

36. Bluetooth 高信頼チャネルポリシー：

a. 検出可能（Discoverable）モードの無効化

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

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

37. 以下のロック状態での通知表示の有効化／無効化ポリシー： [選択：

a. 電子メール通知、

b. カレンダーの予定、

c. 電話呼出し通知と関連付けられた連絡先、

d. テキストメッセージ通知、

e. その他のアプリケーションベースの通知、

f. なし]

38. MD が証明書の有効性を判断するための接続を確立できなかった場合に高信頼チャネルを確立するか、または確立を禁止するかのポリシー、
39. 携帯電話音声機能の有効化／無効化ポリシー、
40. デバイスメッセージング機能の有効化／無効化ポリシー、
41. 携帯電話基地局への接続に用いられる携帯電話プロトコルの有効化／無効化ポリシー、
42. デバイス機能の音声コマンドコントロールの有効化／無効化ポリシー、
43. トラストアンカーデータベース中の X.509v3 証明書のアプリケーションによるインポート及び削除ポリシー、
44. アプリケーション上のデジタル署名の検証に用いられる [選択：証明書、公開鍵]、
45. 複数のアプリケーションによる鍵／秘密の共同利用の例外に関するポリシー、
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関するポリシー、
47. ロック解除バナーのポリシー、
48. [*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

]。

適用上の注意：

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 の選択及び割付と一致すべきである (should)。しかし MDM 開発者は、たとえモバイルデバイスがその ST に従って機能をサポートしていたとしても、本プロテクションプロファイル中のオプションの機能／ポリシーの管理を実装しないことを選択してもよい。

将来は、機能 10 には、例えば開発者の証明書など、TSF の継続的な運用に必要な CA 証明書を除いて、任意のデフォルト高信頼 CA 証明書の破棄が要求されるかもしれない。現時点では、ST 作成者は割付中で、事前にインストールされた、またはその他の任意のカテゴリの X.509v3 証明書が、トラストアンカーデータベースから削除できるかどうかを示さなければならない (shall)。

セキュリティポリシーの 24 番は、WPA2 エンタープライズなどのセキュリティの種類、及び EAP-TLS などの認証プロトコルに対応している。CA または FQDN は、MD による比較のために特定される。

ポリシー26 番の割付は、カメラやマイクロフォンなど、すべての音声及び映像デバイスであって、MDM エージェントにより有効化及び無効化が可能なものから構成される。

ポリシー29 番の割付は、Wi-Fi、GPS、携帯電話、NFC、そして Bluetooth など、すべての

無線であって、MDM エージェントにより有効化及び無効化が可能なものから構成される。

ポリシー30 番の割付は、USB、SD カード、そしてHDMI など、すべての外部アクセス可能なハードウェアポートであって、そのデータ転送機能がMDM エージェントにより有効化及び無効化可能なものから構成される。

ポリシー31 番の割付は、WiFi テザリングなど、TSF がサーバとしてふるまうすべてのプロトコルであって、MDM エージェントにより有効化及び無効化が可能なものから構成される。

ポリシー39 番には、(緊急ダイヤルを除いて) 完全に音声呼を無効化する能力が含まれる。

ポリシー40 番には、(キャリアによって要求されるもの及び緊急 SMS を除いて) 完全にデバイスメッセージングを無効化する能力が含まれる。デバイスメッセージング機能には、SMS、MMS、そしてボイスメールが含まれる。

保証アクティビティ：

評価者はTSS を検査して、列挙された管理機能のそれぞれが記述されていることを保証しなければならない (shall)。評価者はTSS を検査して、サポートされている各モバイルデバイスについて管理機能とポリシーに何らかの違いがあれば、それが列挙されていることを検証しなければならない (shall)。また評価者は主張されているモバイルデバイスの ST を検査して、TSS 中の機能及びポリシー中の選択及び割付が、サポートされている MD の機能を超えていないことを検証しなければならない (shall)。

評価者は、列挙されたMDM エージェント機能のそれぞれを設定するための方法と、どのオプションが利用可能かについて詳細な指示が、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)。

評価者は、上に列挙されたMDM エージェントポリシーのそれぞれを設定し、MDM エージェント機能のそれぞれを指令する能力を検証しなければならない (shall)。

FMT_SMF.1(2) 管理機能の仕様 (プラットフォームのエージェント設定)

FMT_SMF.1(2) **詳細化 : MDM エージェント**は、以下の機能を**プラットフォームと対話して行う**ことができなければならない (shall) :

a. *FMT_SMF.1(1) に列挙される機能とFMT_SMF.1(1) に列挙されるMDM 設定ポリシーの実行*
b. *MDM エージェント通信の認証に用いられる証明書の設定*
c. *[割付：追加的な機能]。*

適用上の注意：

本要件は、MDM サーバからエージェントへ送信される設定ポリシーを用いて基盤となるモバイルデバイスを構成するための MDM エージェント中のすべての設定機能を取り込むものである。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、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。これらの追加的なコマンドや設定ポリシーは、モバイルデバイスによってサポートされなければならない (must)。

エージェントは、MDM サーバから受信したコマンド及び設定ポリシーに基づいてプラットフォームを設定しなければならない (must)。可能なコマンド及び設定ポリシーは、FMT_SMF.1(1) に定義される。

保証アクティビティ：

評価者はTSS を検査して、列挙された管理機能のそれぞれが記述されていることを保証しなければならない (shall)。

評価者は、サーバ上でどのオプションが利用可能かについて詳細な指示が、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)。この機能のテストは、

FMT_SMF.1(1) のテストと組み合わせて行われる。

評価者は、以下のテストを行わなければならない (shall)。

- *テスト : 評価者は、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。評価者は、FPT_ITT.1 のテストを行うにあたって MDM エージェントがこの証明書を利用することを検証しなければならない (shall)。*

FMT_SMF.1(3) 管理機能の仕様 (サーバのサーバ構成)

FMT_SMF.1.1(3) **詳細化 : MDM サーバ**は、以下の管理機能を**行う**ことができなければならない (shall) :

a) X.509v3 証明書を MDM サーバが使用するための構成

b) 登録が許可される [選択 : 特定のデバイス、特定のデバイスモデル、デバイスの数、特定の時間間隔] の構成

c) [*割付 : SFR をサポートするために要求される追加的な機能*]、

d) [選択 : 有効性を立証するための接続が行えなかった際に証明書を受容するかどうかの選択を管理者に許可する、その他の管理機能なし]。

適用上の注意 :

本要件は、基盤となる MDM サーバを構成するための MDM サーバ中のすべての構成機能を取り込むものである。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、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。項目 b 中の選択は、FIA_ENR_EXT.1.2 中の選択に対応する。項目 d には、FIA_X509_EXT.2.2 中の選択に対応する機能が含まれる。

保証アクティビティ :

評価者は TSS を検査して、列挙された管理機能のそれぞれが記述されていることを保証しなければならない (shall)。

評価者は、サーバ上でどのオプションが利用可能かについて詳細な指示が、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)。機能 b 及び c のテストは、その機能の利用と組み合わせて行われる。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、1 つまたは複数の MDM サーバ認証証明書を設定し、その証明書が確立された高信頼接続 (FPT_ITT.1, FTP_TRP.1, FTP_TRP.2) に用いられることを検証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 **詳細化 : MDM サーバ**は、*管理者、MD 利用者、及び [割付 : 追加的な権限を持つ特定された役割]* を維持管理しなければならない (shall)。

FMT_SMR.1.2 **詳細化 : MDM サーバ**は、利用者を役割と関連付けることができなければならない (shall)。

適用上の注意 :

MDM サーバは、異なる利用者役割によって設定され維持管理されることが想定される。割付は、サポートされる役割を ST 作成者が列挙するために用いられる。最低でも、1 つの管理役割がサポートされなければならない (shall)。追加的な役割がサポートされない場合には、「その他の追加的役割なし」が言明される。MD 利用者役割は、FIA_ENR_EXT.1 に従って MDM へモバイルデバイスを登録するために用いられる。

保証アクティビティ :

評価者は TSS と利用者文書を検査して、管理者の役割と、役割に付与される権限及び役割

の制限が記述されていることを検証しなければならない (shall)。

評価者は操作ガイダンスをレビューして、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含まれることを保証しなければならない (shall)。評価のためテストアクティビティを行うにあたって、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、各インタフェースについて管理者アクションを伴う各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 管理のサポートされた手法のそれぞれがテストされることを確実に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には、評価チームのテストアクティビティ中で両方の管理手法が行使されなければならない (must)。

TSF の保護 (FPT)

FPT_ITT.1 基本 TSF 内データ転送保護

FPT_ITT.1.1 **詳細化 :** MDM エージェント及び MDM サーバは、**[選択 : IPsec、TLS、DTLS] の利用により、すべてのデータ(訳注：TSF データか)**を、**MDM エージェントと MDM サーバ**との間で送られる場合、暴露及び改変から保護しなければならない (shall)。

適用上の注意：

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) の送信と、MDM エージェントによって収集され、指令された際、または設定可能な時間間隔で MDM エージェントから MDM サーバへ送信される構成データが、適切に保護されることを確実にするためのものである。またこの高信頼チャネルは、MDM サーバによって MDM エージェントへ送信されるあらゆるコマンド及びポリシーをも保護する。MDM エージェントか MDM サーバのいずれかが、接続を開始することができる。

この高信頼チャネルは、MDM 通信の機密性と完全性を保全するセキュアなプロトコルを利用する。ST 作成者は TOE のサポートする 1 つまたは複数のメカニズムを選択し、そしてそれらの選択に対応する附属書 C 中の詳細な要件が、ST に (すでに存在していない場合) コピーされることを確実にする。

プロトコル、RBG、証明書の検証、アルゴリズム、及び同様のサービスは、プラットフォームの提供するサービスによって満たされてもよい。

保証アクティビティ：

評価者は TSS を検査して、エージェント—サーバ間通信の手法が、これらの通信が保護される方法を含めて示されていることを判断しなければならない (shall)。また評価者は、TOE 管理をサポートするものとして TSS に列挙されたすべてのプロトコルが要件中に特定されたものと一貫しており、ST 中の要件に含まれていることを確認しなければならない (shall)。評価者は、サポートされている手法のそれぞれについて、通信チャネルを構成するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 : 評価者は、操作ガイダンスの記述どおりに接続を設定し通信が成功することを保証することによって、(操作ガイダンスに) 特定されたエージェント—サーバ間通信手法のそれぞれを用いた通信が評価中に確実にテストされるようにしなければならない (shall)。*
- *テスト 2 : 評価者は、エージェント—サーバ間通信手法のそれぞれについて、チャネルデータが平文で送信されないことを保証しなければならない (shall)。*
- *テスト 3 : 評価者は、エージェント—サーバ間通信手法のそれぞれについて、チャネルデータの改変が TOE によって検出されることを保証しなければならない*

(shall)。

これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。

FPT_TUD_EXT.1(1) 拡張：高信頼アップデート (MDM サーバ)

FPT_TUD_EXT.1.1(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正当な利用者へ提供しなければならない (shall)。

保証アクティビティ：

評価者は、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、AGD ガイダンスに従って MDM サーバにソフトウェアの現在のバージョンを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一致することを検証しなければならない (shall)。*

4.3 MDM サーバまたはプラットフォームのセキュリティ機能要件

本セクションでは、MDM サーバによって、または MDM サーバのプラットフォームによって行われなければならない (must) SFR を特定する。各要件には、要件中の機能を行うのが MDM サーバなのか、それとも MDM サーバのプラットフォームなのかを ST 作成者が指示するための選択が含まれる。これらの要件の保証アクティビティであってプラットフォームが選択されているものは、ST 作成者によって特定されたプラットフォームがコモンクライテリアで検証されていることを検証するとともに、そのプラットフォームの ST に要件中の機能が含まれることを保証するためのものである。

セキュリティ監査 (FAU)

FAU_GEN.1(1) 監査データの生成 (MDM サーバ)

FAU_GEN.1.2(1) **詳細化：** [選択：MDM サーバ、MDM サーバプラットフォーム] は、**MDM サーバ**監査記録のそれぞれに、少なくとも以下の情報を記録しなければならない (shall)。

- 事象の日付及び時刻、
- 事象の種類、
- サブジェクトの識別情報、
- (意味がある場合には) 事象の結果 (成功または失敗)、
- 表 7 の追加的情報、
- [*割付：その他の監査関連情報*]。

適用上の注意：

すべての監査には、少なくとも FAU_GEN.1.2(1) に言及される情報が含まれなければならない (must) が、割付可能なより多くの情報を含むことができる。ST 作成者は、監査記録のどの情報が MDM サーバによって行われたものか、そしてどれが MDM サーバのプラットフォームによって行われたものかを TSS 中で特定しなければならない (shall)。

保証アクティビティ：

評価者は TSS をチェックして、監査記録のフォーマットが提供されていることを保証しなければならない (shall)。監査記録のフォーマットの種類のそれぞれが、各フィールドの簡潔な記述とともに、カバーされなければならない (must)。

評価者は、列挙された事象及び管理者アクションに対して TOE に監査記録を生成させるこ

とによって、TOE の正しく監査記録を生成する能力をテストしなければならない (shall)。テスト結果を検証する際に、評価者はテスト中に生成された監査記録が管理ガイドに特定されたフォーマットと一致することと、各監査記録のフィールドが適切なエントリを有することを保証しなければならない (shall)。

ここでのテストは、セキュリティメカニズムの直接的なテストと組み合わせて達成できることに注意されたい。

FAU_STG_EXT.1 拡張：外部監査証跡ストレージ

FAU_STG_EXT.1.1 [選択：MDM サーバ、MDM サーバプラットフォーム] は、[選択：IPsec、SSH、TLS、TLS/HTTPS] プロトコルを実装する高信頼チャネルを用いて外部 IT エンティティへ生成された監査データを送信できなければならない (shall)。

適用上の注意：

TOE は、監査記録のストレージ及びレビューを、TOE 以外の監査サーバに依存してもよい。監査記録を生成するのは TOE であるが、これらの監査記録のストレージと、これらの監査記録を管理者がレビューできるようにする能力は、運用環境によって提供される。MDM サーバ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)。

2 番目の選択においては、ST 作成者はこの接続が保護される手段を選択する。また ST 作成者は、選択と一致するサポートプロトコル要件が ST に確実に含まれるようにする。

保証アクティビティ：

また評価者は操作ガイダンスを検査して、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記述されていることを判断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 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)。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。また評価者は操作ガイダンスを検査して、監査サーバへの高信頼チャネルが確立される方法が記述されていること、また監査サーバに関する何らかの要件が存在するならばその要件 (特定の監査サーバプロトコル、要求されるプロトコルのバージョンなど)、さらに監査サーバと通信するために必要とされる TOE の構成が記述されていることを保証しなければならない (shall)。評価者は、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)。

テスト 1：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ッ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ッ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確認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)。

暗号サポート (FCS)

FCS_CKM.1 暗号鍵生成

FCS_CKM.1.1(1) **詳細化：** [選択：MDM サーバ、MDM サーバプラットフォーム] は、以下に従って**鍵確立に用いられる非対称**暗号鍵を生成しなければならない (shall) [選択：

- 有限体ベースの鍵確立スキームについては、NIST Special Publication 800-56A,

“Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”、

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

また、特定された暗号鍵サイズは *112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。*

適用上の注意：

このコンポーネントは、TOE によって用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) の鍵確立の目的で用いられる公開鍵／プライベート鍵ペアを TOE が生成できることを要求する。複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返してこの機能を取り込むべきである (should)。用いられるスキームは、ST 作成者によって選択の中から選ばれることになる。

用いられるべきドメインパラメタは本 PP のプロトコル要件によって特定されているため、TOE がドメインパラメタを生成することは期待されておらず、したがって本 PP に特定されたプロトコルに TOE が準拠する際には追加的なドメインパラメタの検証は必要とされない。

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

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

保証アクティビティ：

プラットフォームによって満たされる要件

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)。

MDM サーバによって満たされる要件

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

鍵生成：

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

RSA ベースの鍵確立スキームのための鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。このテストは、公開鍵検証指数 e、秘密素因数 p 及び q、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。

- *ランダム素数 :*
  - *証明可能素数*
  - *確率的素数*
- *条件付き素数 :*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数としなければならない (shall)*
  - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数としなければならない (shall)*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数としなければならない (shall)*

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

有限体暗号 (FFC) ベースの 56A スキームのための鍵生成

FFC ドメインパラメタ及び鍵生成テスト

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

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

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

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

- *暗号群生成元 :*
  - *検証可能プロセスによって構築された生成元 g*
  - *検証不可能プロセスによって構築された生成元 g*

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

- *プライベート鍵 :*
  - *RBG の len(q) ビットの出力、ここで 1 <=x <= q-1*

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

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

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

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

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

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

楕円曲線暗号 (ECC) ベースの 56A スキームのための鍵生成

ECC 鍵生成テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

ECC 公開鍵検証 (PKV) テスト

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

鍵確立スキーム

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

SP800-56A 鍵確立スキーム

評価者は、以下の機能及び検証テストを用いて、SP800-56A 鍵共有スキームの TOE の実装を検証しなければならない (shall)。各鍵共有スキームのためのこれらの検証テストは、勧告中の仕様に従った鍵共有スキームのコンポーネントが TOE に実装されていることを検証するものである。これらのコンポーネントには、DLC プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵材料 (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証しなければならない (shall)。これには、DKM の解析、MAC データの生成、及び MAC タグの計算が含ま

れる。

機能テスト

機能テストは、鍵共有スキームを正しく実装する TOE の能力を検証する。このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクトルを生成または取得しなければならない (shall)。サポートされている鍵共有スキーム・鍵共有役割の組み合わせ、KDF タイプと (サポートされている場合には) 鍵確認役割・鍵確認タイプの組み合わせのそれぞれについて、試験者は 10 セットのテストベクトルを生成しなければならない (shall)。このデータセットは、10 セットの公開鍵あたり 1 セットのドメインパラメタ値 (FFC) または NIST 認可曲線 (ECC) からなる。これらの鍵は、テストされるスキームにより静的鍵であるか、短期鍵であるか、またはその両方である。

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

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

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

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

検証テスト

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

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

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

SP800-56B 鍵確立スキーム

現時点では、RSA ベースの鍵確立スキームのための詳細なテスト手順は利用できない。

行われた選択に応じてTSF が800-56A 及び／または800-56B に適合していることを示すため、評価者はTSS に以下の情報が含まれることを保証しなければならない (shall)。

- *TSS には、TOE が適合する適切な 800-56 標準のすべてのセクションが列挙されていなければならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなければならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションをTOE が実装している場合には、それがTSS に記述されなければならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠がTSS に提供されなければならない (shall)。*

800-56A 及び800-56B (選択に応じて) の該当するセクションのそれぞれにおいて、「しなければならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それが記述されなければならない (shall)。

FCS_CKM.1.1(2) [選択：*MDM サーバ*、*MDM サーバプラットフォーム*] は、以下の特定された暗号鍵生成アルゴリズムに従って認証に用いられる非対称暗号鍵を生成しなければならない (shall)。 [選択：

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

また、特定された暗号鍵サイズは [***112 ビットの対称鍵強度と、同等、またはそれよりも大きく***] なければならない。

適用上の注意：

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

楕円曲線ベースの方式に関しては、鍵サイズは基点の位数の2 の対数を示す。

ANSI X9.31-1998 の選択肢は、本文書の将来の改訂版では選択から除かれることになる。現状では、モダンなFIPS PUB 186-4 標準への移行を業界が完了するまでにまだ多少時間がかかるため、この選択はFIPS PUB 186-4 のみに限定されてはいない。暗号署名に関する好ましいアプローチとして、本PP の将来の版では楕円曲線が要求されることになる。

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

保証アクティビティ：

プラットフォームによって満たされる要件

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 に主張される鍵生成機能にMDM サーバのST における鍵生成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) 鍵生成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)。

MDM サーバによって満たされる要件

TSF がFIPS 186-4 署名スキームを実装する場合、本要件はFCS_COP.1.1(1)) の下で検証される。

ESF が ANSI X9.31-1998 スキームを実装する場合、評価者は鍵ペアが生成される方法がTSS に記述されていることをチェックして保証しなければならない (shall)。TSF の実装がANSI X9.31-1998 に適合していることを示すため、評価者はTSS に以下の情報が含まれることを保証しなければならない (shall)。

- *TSS には、TOE が準拠する標準のすべてのセクションが列挙されていなければならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなければならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションをTOE が実装している場合には、それがTSS に記述されなければならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠がTSS に提供されなければならない (shall)。*
- *附属書 B の該当するセクションのそれぞれにおいて、「しなければならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それが記述されなければならない (shall)。*

FCS_CKM_EXT.2(1) 暗号鍵ストレージ (MDM サーバ)

FCS_CKM_EXT.2.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、永続的秘密及びプライベート鍵を使用していない際には、[選択：プラットフォームによって提供される鍵ストレージ、FCS_STG_EXT.1 に特定されるよう] に保存しなければならない (shall)。

適用上の注意：

本要件によって、永続的秘密 (クレデンシャル、秘密鍵) とプライベート鍵が使用されていない際、セキュアに保存されることが確実となる。秘密／鍵の一部がTOE によって操作され、その他がプラットフォームによって操作される場合には、両方の選択がST 作成者によって特定されることが可能であり、またST 作成者はTOE によって操作される鍵とプラットフォームによって操作される鍵とをTSS 中に特定しなければならない (must)。

MDM サーバがアプリケーションであって、専用サーバでない場合には、プライベート鍵をプラットフォームによって提供される鍵ストレージへ保存すべきである (should)。

ST 作成者は、鍵が保存される方法、及び保存される場所を、上記の選択中で選択する責任を負う。

保証アクティビティ：

本要件がTOE と TOE プラットフォームのどちらによって満たされる場合であっても、評価者はTSS をチェックして、ST 中の要件を満たすことが必要とされる永続的秘密 (クレデンシャル、秘密鍵) とプライベート鍵のそれぞれが列挙されていることを保証する。これらの項目のそれぞれについて、評価者はそれが何の目的に用いられるか、そしてどのように保存されるかがTSS に列挙されていることを確認する。次に評価者は、以下のアクションを行う。

プラットフォームによって操作される永続的秘密及びプライベート鍵

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、MDM サーバの ST にプラットフォームによって保存されるものとして列挙される永続的秘密及びプライベート鍵が、そのプラットフォームの ST で保護されるものとして特定されていることを保証しなければならない (shall)。

TOE によって操作される永続的秘密及びプライベート鍵

評価者は TSS をレビューして、TOE によって操作されるものとして列挙される項目のそれぞれについて、暗号化されずに永続的メモリへ書き込まれることはなく、またその項目がプラットフォームによって保存される、ということが立証されていることを判断する。

FCS_CKM_EXT.4 暗号鍵の破棄

FCS_CKM_EXT.4.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、すべての平文の秘密及びプライベート暗号鍵ならびに CSP を、もはや必要とされなくなった際にゼロ化しなければならない (shall)。

適用上の注意：

MDM サーバプラットフォームが平文の秘密、プライベート暗号鍵、及び CSP を用いる一切の操作を行わない場合、ST 作成者はプラットフォームを選択すべきである (should)。

あらゆるセキュリティ関連情報 (鍵や認証データ、そしてパスワードなど) 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。

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

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられる CSP であって TOE へ課される FCS_CKM_EXT.4 要件によってカバーされていないもののそれぞれが、TSS に記述されていることをチェックして保証しなければならない (shall)。

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 の TSS を検査して、上記に列挙された秘密鍵、プライベート鍵、及び鍵の生成に用いられる CSP がカバーされていることを保証しなければならない (shall)。

MDM サーバによって満たされる要件

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられる CSP のそれぞれが、それらがゼロ化される時点 (例えば、使用直後、システムのシャットダウン時、など)、及び行われるゼロ化手続きの種類 (ゼロで上書き、ランダムパターンで 3 度上書き、など) と共に TSS に記述されていることをチェックして保証しなければならない (shall)。保護されるべきマテリアルの保存に異なる種類のメモリが用いられる場合、評価者はデータが保存されるメモリに応じたゼロ化手続き (例えば、「フラッシュメモリ上に保存される秘密鍵はゼロで 1 度上書きすることによってゼロ化されるが、内部ハ

ードドライブ上に保存される秘密鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってゼロ化される」) が TSS に記述されていることをチェックして保証しなければならない (shall)。ゼロ化を検証するためにリードバックが行われる場合、このことも記述されなければならない (shall)。

TSS に記述される鍵クリア状況のそれぞれについて、評価者は以下のテストを繰り返さなければならない (shall)。

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

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

- *計測機能を備えた TOE ビルドをデバッガへロードする。*
- *クリア対象となる TOE 内の鍵の値を記録する。*
- *#1 の鍵に関する通常の暗号処理を TOE に行わせる。*
- *TOE に鍵をクリアさせる。*
- *TOE に実行を停止させるが、終了はさせない。*
- *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。*
- *#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 (デジタル署名)

FCS_COP.1.1(1) **詳細化：** [選択：MDM サーバ、MDM サーバプラットフォーム] は、以下に特定された暗号アルゴリズムに従って*暗号署名サービス*を行わなければならない (shall) [選択：

- ***2048 ビット以上の鍵サイズ (法) を用いる RSA デジタル署名アルゴリズム (RSA) であって*FIPS PUB 186-2 または FIPS PUB 186-4, “Digital Signature Standard” *を満たすもの、***
- ***256 ビット以上の鍵サイズを用いる楕円曲線デジタル署名アルゴリズム (ECDSA) であって*FIPS PUB 186-4, “Digital Signature Standard” (FIPS PUB 186-4, “Digital Signature Standard” に定義される) と「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] *を満たすもの、***
- ***2048 ビット以上の鍵サイズ (法) を用いるデジタル署名アルゴリズム (DSA) で***

***あって*FIPS PUB 186-4, “Digital Signature Standard”*を満たすもの、その他の暗号署名サービスなし*]。**

適用上の注意：

MDM サーバと MDM エージェントの両方が、FTP_ITC_EXT.1 のプロトコルに従ってデジタル署名サービスを行わなければならない (must)。また MDM サーバは、デ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モバイルデバイスへ送信してもよい。

複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返してこの機能を取り込むべきである (should)。用いられるスキームは、ST 作成者によって選択の中から選ばれることになる。

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

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 に主張されるデジタル署名機能に MDM サーバの ST におけるデ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)。

MDM サーバによって満たされる要件

鍵生成：

RSA 署名スキームの鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。このテストは、公開鍵検証指数 e、秘密素因数 p 及び q、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。

- *ランダム素数：*
  - *証明可能素数*
  - *確率的素数*
- *条件付き素数：*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数とする (shall)*
  - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数とする (shall)*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数とする (shall)*

ランダム証明可能素数手法とすべての条件付き素数手法の鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシードとして TSF 鍵生成ルーチンに与えなければならない (must)。これには、1 つまたは複数の乱数シード、RSA 鍵の公開鍵指数、及び望ましい鍵の長さが含まれる。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない (shall)。評価者は、TSF によって生成された値を既知の良好な実装から生

成された値と比較することによって、TSF の実装の正しさを検証しなければならない (shall)。

ECDSA 鍵生成テスト

FIPS 186-4 ECDSA 鍵生成テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

FIPS 186-4 公開鍵検証 (PKV) テスト

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

ECDSA アルゴリズムテスト

ECDSA FIPS 186-4 署名生成テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージを生成し、各メッセージについて公開鍵ならびに得られた署名の値 R 及び S を取得しなければならない (shall)。正しさを判断するため、評価者は既知の良好な実装の署名検証機能を利用しなければならない (shall)。

ECDSA FIPS 186-4 署名検証テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージ、公開鍵及び署名の組のセットを生成し、10 組のうち 5 組で値のいずれか (メッセージ、公開鍵または署名) を変更しなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

評価者は、署名生成テストを用いて TOE による RSA 署名生成の実装を検証しなければならない (shall)。このテストを行うために評価者は、TSF のサポートする法サイズ／SHA の組み合わせのそれぞれについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない (must)。評価者は、TOE に自分のプライベート鍵と法の値を用いてこれらのメッセージへ署名させなければならない (shall)。

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

署名検証テスト

評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない (shall)。評価者は、公開鍵 e、メッセージ、IR フォーマット、または署名、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(2) 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(2) [選択：MDM サーバ、MDM サーバプラットフォーム] は、特定された暗号アルゴリズム HMAC-[選択：SHA-1、SHA-256、SHA-384、SHA-512] であって、鍵サイズが [*割付：HMAC に用いられる (ビット単位の) 鍵サイズ*]、メッセージダイジェストのサイズが [選択：160、256、384、512] ビットの、以下：FIPS PUB 198-1, “The Keyed-Hash Message Authentication Code”、及び FIPS PUB 180-3, “Secure Hash Standard” を満たすものに従って鍵付きハッシュによるメッセージ認証を行わなければならない (shall)。

適用上の注意：

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 (例えば高信頼チャネル) の鍵確立の目的で用いられる際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特定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(3) 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

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サイズ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)。

MDM サーバによって満たされる要件

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

サポートされているパラメタセットのそれぞれについて、評価者は 15 セットのテストデータを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_COP.1(3) 暗号操作 (暗号化及び復号)

FCS_COP.1.1(3) [選択：MDM サーバ、MDM サーバプラットフォーム] は、以下の特定された暗号アルゴリズム [選択：

- *(NIST SP 800-38A に定義される) AES-CBC モード、*
- *(NIST SP 800-38D に定義される) AES-GCM、*
- *(NIST SP 800-38C に定義される) AES-CCM、*
- *(NIST SP 800-38F に定義される) AES 鍵ラップ (KW)、*

- *(NIST SP 800-38F に定義される) AES パディング付き鍵ラップ (KWP)*

] 及び暗号鍵サイズ [選択：128 ビット、256 ビット] *の鍵サイズ*に従って [***暗号化／復号***] を行わなければならない (shall)。

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

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サイズ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)。

MDM サーバによって満たされる要件

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-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-GCM モンテカルロテスト

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

- ***128 ビット及び 256 ビットの鍵***
- ***2 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 認証済み暗号化から得られた暗号文とタグを取得しなければならない (shall)。サポートされているタグの長さはそれぞれ、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 鍵ラップ (AES-KW) 及びパディング付き鍵ラップ (AES-KWP) テスト

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

- ***128 ビット及び 256 ビットの鍵暗号化鍵***
- ***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 認証済み暗号化から得られた暗号文を取得する。正しさを判断するため、評価者は既知の良好な実装の AES-KW 認証済み暗号化機能を利用しなければならない (shall)。

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

評価者は、AES-KW の認証済み暗号化と同一のテストを用い、以下の変更を 3 通りの平文の長さに行って、AES-KWP 認証済み暗号化機能を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 認証済み暗号化を AES-KWP 認証済み復号と置き換えて、AES-KWP の認証済み復号機能をテストしなければならない (shall)。

FCS_COP.1(4) 暗号操作 (ハッシュ)

FCS_COP.1.1(4) [選択：MDM サーバ、MDM サーバプラットフォーム] は、特定された暗号アルゴリズム [選択：SHA-1、SHA-256、SHA-384、SHA-512] であって、メッセージダイジェストのサイズが [選択：160、256、384、512] ビットの、以下：FIPS Pub 180-4 を満たすものに従って暗号ハッシュを行わなければならない (shall)。

適用上の注意：

本 PP の将来の版では、SHA-1 は選択肢から削除されるかもしれない。SHA-1 によるデジタル署名の生成は 2013 年 12 月以降には許可されず、また SHA-1 によるデジタル署名の検証は、これらの署名の受容に存在する可能性のあるリスクのため、強く非推奨とされる。

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サイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(1) に用いられるアルゴリズムの全体的な強度と一貫しているべきである (should)。

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

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サイズ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)。

MDM サーバによって満たされる要件

評価者はAGD 文書をチェックして、必要とされるハッシュのサイズに機能を構成するために行われることが必要とされる構成があれば、それが存在することを判断する。評価者は、ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連がTSS に文書化されていることをチェックしなければならない (shall)。

TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。このモードでは、TSF は長さがバイトの整数倍であるメッセージのみを

ハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。このモードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

評価者は、TSF によって実装され、本 PP の要件を満たすために用いられるハッシュアルゴリズムのそれぞれについて、以下のテストをすべて行わなければならない (shall)。

ショートメッセージテスト—ビット指向モード

評価者は m+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から m ビットまでシーケンシャルに変化する。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

ショートメッセージテスト—バイト指向モード

評価者は m/8+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から m/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—ビット指向モード

*評価者は m 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 99*i となる (ここで 1 ≤ i ≤ m)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*

選択されたロングメッセージテスト—バイト指向モード

*評価者は m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 8*99*i となる (ここで 1 ≤ i ≤ m/8)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*

疑似ランダム的に生成されたメッセージテスト

このテストは、バイト指向の実装にのみ行われる。評価者は、n ビットの長さのシードをランダムに生成する。ここで n はテストされるハッシュ関数によって作成されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムに従って 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

FCS_RBG_EXT.1(1) 拡張：ランダムビット生成

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

FCS_RBG_EXT.1.2(1) 決定論的 RBG は、鍵とそれが生成するハッシュとの (NIST SP 800-57 による) セキュリティ強度の大きいほうと少なくとも等しい、最小で [選択：*128 ビ*

ット、256 ビット] のエントロピーを持つ、 [選択 : TSF ハードウェアベースの雑音源、TSF ソフトウェアベースの雑音源、プラットフォームベースの RBG] からエントロピーを蓄積するエントロピー源によってシードを供給されなければならない (shall)。

適用上の注意：

FCS_RBG_EXT.1.1 の最初の選択に関しては、ST 作成者は TOE か TOE のインストールされるプラットフォームのどちらが RBG サービスを提供するか選択すべきである (should)。

NIST Special Pub 800-90B の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり (should)、また本 PP の将来のバージョンでは必要とされることになる。

FCS_RBG_EXT.1.1 の 2 番目の選択に関しては、ST 作成者は RBG サービスが適合する標準 (800-90A または 140-2 附属書 C のいずれか) を選択すべきである (should)。

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

FCS_RBG_EXT.1.2 の 2 番目の選択に関しては、ST 作成者はエントロピー源がソフトウェアベースであるか、ハードウェアベースであるか、プラットフォームベースであるか、またはそれらの何らかの組み合わせであるかを示す。エントロピーの源が複数存在する場合には、ST には各エントロピー源のそれぞれについて、それがハードウェアベースであるか、ソフトウェアベースであるか、またはプラットフォームベースであるかを含めて説明する。プラットフォームベース及びハードウェアベースの雑音源が望ましい。

プラットフォームベースの RBG 源は、プラットフォームによって提供される検証済みの RBG の出力であり、これは FCS_RBG_EXT.1.1 に従って TSF の提供する DRBG のエントロピー源として利用される。このようにして、開発者は NIST SP800-90C に記述されているように RBG を連鎖する。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に記述される手法のみが有効であることに注意されたい。ここで用いられる AES 実装の鍵の長さが利用者データの暗号化に用いられるものと異なる場合には、FCS_COP.1 を調整するか繰り返して異なる鍵の長さを反映する必要があるかもしれない。FCS_RBG_EXT.1.2 の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に確実に含まれるようにする。

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

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 RBG 機能に MDM サーバの ST における RBG 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) RBG 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)。

MDM サーバによって満たされる要件

附属書 E「エントロピーの文書化と評定」に従って、文書が作成されなければならない (shall) (そして評価者はアクティビティを行わなければならない (shall))。

ST 作成者がプラットフォームベースの雑音源を選択した場合、評価者はプラットフォームの ST を検査することによって、プラットフォームの RBG が検証されていることを検証しなければならない (shall)。評価者は、少なくとも本プロファイルに関して ST 作成者によって選択されたエントロピー量が、プラットフォームの RBG に供給されていることを検証しなければならない (shall)。この場合、ST 作成者はプラットフォームの RBG の附属書 E 文書に責任を負わない。

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

FIPS 140-2 の附属書 C に準拠する実装

本セクションに含まれるテストの参照情報は、The Random Number Generator Validation System (RNGVS) である。評価者は、以下の 2 つのテストを実施しなければならない (shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装によって作成されることに注意されたい。正しさの証明は、各スキームに任される。

評価者は、可変シードテストを行わなければならない (shall)。評価者は (Seed, DT) ペア (それぞれ 128 ビット) の 128 個のセットを TSF の RBG 機能に提供しなければならない (shall)。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。DT の値は、各セットについて 1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない (shall not)。評価者は、TSF によって返される値が期待値と一致することを保証する。

評価者は、モンテカルロテストを行わなければならない (shall)。このテストについては、評価者がシード及び DT の初期値 (それぞれ 128 ビット) を TSF の RBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。次に評価者は、繰返しのたびに DT の値を 1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に特定されるように次回の繰返しの際の新たなシードを作成して、TSF の RBG を 10,000 回呼び出す。評価者は、得られた 10,000 番目の値が期待値と一致することを保証する。

NIST Special Publication 800-90A に準拠する実装

評価者は、RBG 実装の 15 回の試行を行わなければならない (shall)。RBG 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、RBG 機能を構成するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない (shall)。

RBG が有効な予測困難性を持つ場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして 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ひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90A に定義される) Output Block Length と等しいランダムなビットを生成すること

を意味する。

RBG が予測困難性を持たない場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) シードを再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして 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。*

識別と認証 (FIA)

FIA_UAU.1 認証のタイミング

FIA_UAU.1.1 **詳細化**： [選択：MDM サーバ、MDM サーバプラットフォーム] は、利用者が**サーバへ**認証される前に、利用者に代わって *[割付：**MDM サーバ**による仲介アクションのリスト]* が行われることを許可しなければならない (shall)。

FIA_UAU.1.2 **詳細化**： [選択：MDM サーバ、MDM サーバプラットフォーム] は、各利用者に代わってそれ以外の **MDM サーバ**による仲介アクションを許可する前に、**サーバへの**その利用者の認証の成功を要求しなければならない (shall)。

適用上の注意：

本要件によって、MDM サーバへのアクセスを試行するあらゆる利用者が認証されなければならない (must) ことが確実となる。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通常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。MDM サーバまたは MDM サーバプラットフォームは、本要件を満たすためにエンタープライズ認証を利用してもよい。

保証アクティビティ：

評価者は TSS を検査して、認証前に行われることが可能なアクションと不可能なアクションとが記述されていることを検証しなければならない (shall)。評価者は、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(1) 拡張 : X509 検証

FIA_X509_EXT.1.1(1) [選択 : MDM サーバ、MDM サーバプラットフォーム] は、以下のルールに従って証明書の有効性を確認しなければならない (shall)。

- RFC 5280 証明書の検証及び証明書パス検証。
- 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、証明書パスを検証しなければならない (shall)。
- TSF は、[選択 : RFC 2560 に特定されるオンライン証明書状態プロトコル (OCSP)、RFC 5759 に特定される証明書失効リスト (CRL)] を用いて証明書の失効状態を検証しなければならない (shall)。
- TSF は、以下のルールに従って extendedKeyUsage フィールドを検証しなければならない (shall)。
  - 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、コード署名目的 (id-kp 3 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 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)。

適用上の注意 :

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)。証明書は、TSF ソフトウェアの高信頼アップデート(FPT_TUD_EXT.1.3) のため、及びソフトウェアの完全性検証(FPT_TST_EXT.1.2) のためにオプションとして用いてもよく、また実装されている場合には、コード署名目的 extendedKeyUsage を含むことが検証されなければならない (must)。FPT_ITT.1 または FTP_TRP.1 もしくは FTP_TRP.2 において TLS、DTLS、または HTTPS が選択されている場合、証明書を利用して認証が行われなければならず (must)、また証明書にクライアント認証目的の extendedKeyUsage が含まれることが検証されなければならない (must)。

証明書の検証は、信頼済みルート証明書に至ることが期待されることに注意すべきである (should)。

FIA_X509_EXT.1.1 は TOE プラットフォームに、TLS クライアントによって提示される証明書に関して一定のチェックを行うことを要求しているが、クライアントが提示する証明書に関してクライアントが行わなければならない関連のチェックが存在する ; すなわち、クライアント証明書の extendedKeyUsage フィールドに "サーバ認証" が含まれ、また鍵共有 (key agreement) ビット (Diffie-Hellman 暗号スイートの場合) または鍵暗号化 (key encipherment) ビット (RSA 暗号スイートの場合) がセットされていることである。TOE が使用するために取得される証明書が、エンタープライズ内で使用されるためには、これらの要件に適合しなければならない (have to)。

FIA_X509_EXT.1.2(1) [選択 : *MDM サーバ、MDM サーバプラットフォーム*] 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)。

適用上の注意：

本要件は、MDM サーバまたはプラットフォームによって用いられ処理される証明書に適用される。

保証アクティビティ：

評価者は、どこで証明書の有効性のチェックが行われるか TSS に記述されていることを保証しなければならない (shall)。また評価者は、証明書パス検証アルゴリズムの記述も TSS に提供されていることも確認する。

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

テスト 1：評価者は、有効な証明書パスのない証明書の検証を行うと、その機能 (アプリケーションの検証、高信頼チャネルの設定、または高信頼ソフトウェアアップデート) が失敗することを論証しなければならない (shall)。次に評価者は、その機能で使われる証明書の検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを論証しなければならない (shall)。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない (shall)。

テスト 2：評価者は、有効期限を過ぎた証明書の検証にてその機能が失敗することを論証しなければならない (shall)。

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

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

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

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

FIA_X509_EXT.2(1) 拡張：X509 認証

FIA_X509_EXT.2.1(1) [選択：*MDM サーバ、MDM サーバプラットフォーム*] は、RFC 5280 によって定義される X.509v3 証明書を用いて [選択：IPsec、TLS、HTTPS、DTLS] の認証、及び [選択：ソフトウェアアップデートのコード署名、ソフトウェア完全性検証のコード署名、ポリシー署名、追加用途なし] をサポートしなければならない (shall)。

適用上の注意：

ST 作成者の選択は、FPT_ITT.1 及び FTP_TRP.1 の選択と一致しなければならない (shall)。

証明書は、システムソフトウェア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) にオプションとして用いてもよい。これらのコード署名用途のいずれかが選択されている場合、FIA_X509_EXT.2.4 が本体へ含まれなければならない (must)。FMT_POL_EXT.1.2 が本体に取り込まれる場合、ポリシー署名が選択されなければならない (must)。一部の認証サービスが TOE によって、その他がプラットフォームによって提供される場合、ST 作成者はどのサービスが TOE によって提供されどのサービスがプラットフォームによって提供されるのか明示しなければならない (shall)。

各クライアントはそれぞれ、MDM エージェントによって使用される一意の X.509v3 証明書を有すること。証明書はクライアント間で再利用されてはならない。

FIA_X509_EXT.2.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] 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：*MDM サーバ、MDM サーバプラットフォーム*] 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)。

適用上の注意：

CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態の検証を行うために接続を確立しなければならない (must) 場合は多々生ずる。この選択は、そのような接続が確立できない場合 (例えば、ネットワークエラーのため) のふるまいを記述するために用いられる。TOE が、証明書は FIA_X509_EXT.1 中の他の全てのルールに従って有効であると判断した場合、2 番目 (訳注：3 番目の間違いか) の選択に示されるふるまいによって有効性が判断されなければならない (shall)。証明書が FIA_X509_EXT.1 中の他の検証ルールのいずれかに失敗する場合、TOE はその証明書を受容してはならない (must not)。ST 作成者によって管理者設定オプションが選択された場合、ST 作成者はまた FMT_SMF.1(3) の機能 d も選択しなければならない (must)。

FIA_X509_EXT.2.3(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、ピア証明書が無効とみなされる場合には高信頼チャネルを確立してはならない (shall not)。

適用上の注意：

高信頼通信チャネルには、TSF によって行われる IPsec、TLS、HTTPS、または DTLS のいずれかが含まれる。有効性は証明書パス、有効期限、及び RFC 5280 にしたがう失効状態によって決定される。

FIA_X509_EXT.2.5(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、RFC 2986 に特定された通り証明書要求メッセージを生成し、またその要求には以下の情報を提供できなければならない (shall)：公開鍵、共通名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country)。

適用上の注意：

FIA_X509_EXT.2.5 に言及される公開鍵は、FCS_CKM.1(2) に特定された通り TOE が生成する公開鍵—プライベート鍵ペアの、公開鍵の部分である。

保証アクティビティ

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

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

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

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

テスト 2 : 評価者は MDM サーバに公開鍵―プライベート鍵ペアを生成させ、CA (TOE 双方から信頼されている) の署名を得るため CA へ CSR (証明書署名要求) を送付させなければならない (shall)。DN (共通名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country)) の値もまた、この要求の中で渡されることになる。

テスト 3 : 評価者は、TOE 以外の IT エンティティとの通信によって、有効な証明書の使用には少なくとも一部の証明書の検証のチェック実行が必要とされることを論証しなければならない (shall)。次に評価者は、TOE が証明書の有効性を検証できないように環境を操作し、FIA_X509_EXT.2.2 で選択されたアクションが行われることを確認しなければならない (shall)。選択されたアクションが管理者によって設定可能である場合には、評価者は操作ガイダンスに従って、サポートされているすべての管理者設定可能オプションが、文書化されているようにふるまうことを判断しなければならない (shall)。

TSF の保護 (FPT)

FPT_TST_EXT.1(1): TSF のテスト

FPT_TST_EXT.1.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、最初の起動中 (電源投入時) に一連のセルフテストを実行し、MDM サーバの正しい動作を論証しなければならない (shall)。

FPT_TST_EXT.1.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、 [選択：MDM サーバ、MDM サーバプラットフォーム] によって提供される暗号サービスの使用により、保存された MDM サーバ実行可能形式コードが実行のためにロードされた際にその完全性を検証する機能を提供しなければならない (shall)。

適用上の注意：

TOE は典型的には IT 環境中で動作するソフトウェアパッケージであるが、それでも上記で求められるセルフテストアクティビティを行うことは可能である。しかし、上述のテストによって提供される保証の評定において、ホスト環境への多大な依存が存在する (ホスト環境が危殆化した場合にはセルフテストは意味をなさなくなることを意味する) ことは理解されるべきである (should)。

保証アクティビティ：

評価者は TSS を検査して、起動時に TSF によって実行されるセルフテストが詳述されていることを保証しなければならない (shall)。この記述には、実際に実施されるテストの概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを保証することによってメモリがテストされる」のような記述が用いられなければならない (shall)) が含まれるべきである (should)。評価者は、TSF が正しく動作していることをテストが十分に論証するという論拠が TSS に示されていることを保証しなければならない (shall)。

評価者は TSS を検査して、保存された TSF 実行可能コードが実行のためにロードされた際にその完全性を検証する方法が記述されていることを保証しなければならない (shall)。評価者は、TSF 実行可能コードの完全性が危殆化されていないことをテストが十分に論証するという論拠が TSS に示されていることを保証しなければならない (shall)。また評価者は、

TSS (または操作ガイダンス) に成功の (例えば、ハッシュが検証された) 場合と不成功の (例えば、ハッシュが検証されなかった) 場合に行われるアクションが記述されていることも検証する。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、既知の良好な TSF 実行可能形式に関する完全性チェックを行い、その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、その改変された TSF 実行可能形式に関する完全性チェックを行い、そのチェックが失敗することを検証する。

FPT_TUD_EXT.1(1) 拡張：高信頼アップデート (MDM サーバ)

FPT_TUD_EXT.1.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、MDM サーバソフトウェアへのアップデートを開始する能力を正当な管理者へ提供しなければならない (shall)。

FPT_TUD_EXT.1.3(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、MDM サーバ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)。

適用上の注意：

MDM サーバは、時折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 MDM サーバがインストールすることを確実にすることを意図している。他のソースによって提供されたアップデートには、悪意のあるコードが含まれるおそれがあるからである。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ることになる。サーバがアプライアンスである場合、アップデートは MDM サーバ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：

評価者は TSS を検査して、アップデートのデジタル署名が準拠する標準と、署名検証プロセスの実装方法が記述されていることを検証しなければならない (shall)。評価者は AGD ガイダンスを検査して、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方法と、アップデートを開始する方法が記述されていることを検証しなければならない (shall)。評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者はベンダによってデジタル署名されたアップデートの開始を試行して、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ってデジタル署名されていないアップデートのインストールを試行して、その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)。*

高信頼パス／チャネル (FTP)

FTP_TRP.1 リモート管理用の高信頼パス

FTP_TRP.1.1 **詳細化：** [選択：**MDM サーバ、MDM サーバプラットフォーム**] は、**[選択：IPsec、 TLS、 TLS/HTTPS] を利用して、**他の通信パスとは論理的に分離されているとともに、そのエンドポイントの保証された識別と通信データの*開示からの*保護*及び通信データの改変の検出*を提供する、それ自身と**リモート管理者**との間の高信頼通信パスを提供しなければならない (shall)。

FTP_TRP.1.2 **詳細化：** [選択：**MDM サーバ、MDM サーバプラットフォーム**] は、**リモート管理者**が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 **詳細化：** [選択：**MDM サーバ、MDM サーバプラットフォーム**] 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)。

適用上の注意：

本要件は、正当な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上で行われることを確実にする。この高信頼通信チャネルを通過するデータは、最初の選択で選ばれたプロトコルの定義により暗号化される。ST 作成者は TOE のサポートする 1 つまたは複数のメカニズムを選び、そしてそれらの選択に対応する附属書 C 中の詳細な要件が、ST に (すでに存在していない場合) 確実にコピーされるようにする。

保証アクティビティ：

評価者は TSS を検査して、リモート TOE 管理の手法が、これらの通信が保護される方法と共に示されていることを判断しなければならない (shall)。また評価者は、TOE 管理をサポートするものとして TSS に列挙されたすべてのプロトコルが要件中に特定されたものと一貫しており、ST 中の要件に含まれていることを確認しなければならない (shall)。評価者は、サポートされている手法のそれぞれについて、リモート管理セッションを確立するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、操作ガイダンスの記述どおりに接続を設定し通信が成功することを保証することによって、(操作ガイダンスに) 特定されたリモート管理手法のそれぞれを用いた通信が評価中に確実にテストされるようにしなければならない (shall)。*
- *テスト 2：サポートされるリモート管理の各手法について、評価者は操作ガイダンスに従って、高信頼パスを伴わずにリモート管理セッションを確立するためにリモート利用者が利用できるインタフェースが存在し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、リモート管理の各手法について、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 4：評価者は、リモート管理の各手法について、TOE チャネルデータの改変が TOE によって検出されることを保証しなければならない (shall)。*

これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。

FTP_TRP.2 登録用の高信頼パス

FTP_TRP.2.1 **詳細化：** [選択：**MDM サーバ、MDM サーバプラットフォーム**] は、**[選択：TLS、 TLS/HTTPS] を利用して**、他の通信パスとは論理的に分離されているとともに、そのエンドポイントの保証された識別と通信データの*開示からの*保護*及び通信データの改変の検出*を提供する、それ自身と **MD 利用者**との間の高信頼通信パスを提供しなければならない (shall)。

FTP_TRP.2.2 **詳細化：** [選択：**MDM サーバ、MDM サーバプラットフォーム**] は、**MD 利用者**が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.2.3 **詳細化：** [選択：**MDM サーバ、MDM サーバプラットフォーム**] 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)。

適用上の注意：

本要件は、正当な 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 とのすべての通信はこのパス上で行われることを確実にする。この接続の目的は、MD 利用者による登録である。この高信頼通信チャネルを通過するデータは、最初の選択で選ばれたプロトコルの定義により暗号化される。ST 作成者は TOE の

サポートする 1 つまたは複数のメカニズムを選び、そしてそれらの選択に対応する附属書 C 中の詳細な要件が、ST に (すでに存在していない場合) 確実にコピーされるようにする。

保証アクティビティ：

評価者は TSS を検査して、リモート登録の手法が、これらの通信が保護される方法を含めて示されていることを判断しなければならない (shall)。また評価者は、登録をサポートするものとして TSS に列挙されたすべてのプロトコルが要件に特定されたものと一貫しており、ST 中の要件に含まれていることを確認しなければならない (shall)。評価者は、サポートされている手法のそれぞれについて、登録セッションを確立するための指示が操作ガイダンスに含まれていることを確認しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 : 評価者は、操作ガイダンスの記述どおりに接続を設定し通信が成功することを保証することによって、(操作ガイダンスに) 特定された登録手法のそれぞれを用いた通信が評価中に確実にテストされるようにしなければならない (shall)。*
- *テスト 2 : サポートされる登録の各手法について、評価者は操作ガイダンスに従って、高信頼パスを伴わずに登録セッションを確立するためにリモート利用者が利用できるインタフェースが存在し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、登録の各手法について、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 4 : 評価者は、登録の各手法について、TOE チャネルデータの改変が TOE によって検出されることを保証しなければならない (shall)。*

これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。

4.4 MDM エージェントまたはプラットフォームのセキュリティ機能要件

本セクションでは、MDM エージェントによって、または MDM エージェントのプラットフォームによって行われなければならない (must) SFR を特定する。各要件には、要件中の機能を行うのが MDM エージェントなのか、それとも MDM エージェントのプラットフォームなのかを ST 作成者が指示するための選択が含まれる。これらの要件の保証アクティビティであってプラットフォームが選択されているものは、ST 作成者によって特定されたプラットフォームがコモンクライテリアで検証されていることを検証するとともに、そのプラットフォームの ST に要件中の機能が含まれることを保証するためのものである。

暗号サポート (FCS)

FCS_CKM.1 暗号鍵生成

FCS_CKM.1.1(3) **詳細化：** [選択：MDM エージェント、MDM エージェントプラットフォーム] は、以下に従って**鍵確立に用いられる非対称**暗号鍵を生成しなければならない (shall) [選択：

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

“Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”]

また、特定された暗号鍵サイズは *112 ビットの対称鍵強度と同等、またはそれよりも大きくなければならない。*

適用上の注意：

このコンポーネントは、TOE によって用いられるさまざまな暗号プロトコル (例えば高信頼チャネル) の鍵確立の目的で用いられる公開鍵／プライベート鍵ペアを TOE が生成できることを要求する。複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返してこの機能を取り込むべきである (should)。用いられるスキームは、ST 作成者によって選択の中から選ばれることになる。

用いられるべきドメインパラメタは本 PP のプロトコル要件によって特定されているため、TOE がドメインパラメタを生成することは期待されておらず、したがって本 PP に特定されたプロトコルに TOE が準拠する際には追加的なドメインパラメタの検証は必要とされない。

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

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

保証アクティビティ：

プラットフォームによって満たされる要件

ST 中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 エージェントの 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 エージェントの 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 エージェント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)。

MDM エージェントによって満たされる要件

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

鍵生成：

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

RSA ベースの鍵確立スキームのための鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。このテストは、公開鍵検証指数 e、秘密素因数 p 及び q、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。

- *ランダム素数：*
  - *証明可能素数*
  - *確率的素数*

- *条件付き素数：*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数としなければならない (shall)*
  - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数となければならない (shall)*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数となければならない (shall)*

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

有限体暗号 (FFC) ベースの 56A スキームのための鍵生成

FFC ドメインパラメタ及び鍵生成テスト

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

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

- *暗号素数及びフィールド素数：*
  - *素数 q 及び p を両方とも証明可能素数となければならない (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なければならない (shall)*

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

- *暗号群生成元：*
  - *検証可能プロセスによって構築された生成元 g*
  - *検証不可能プロセスによって構築された生成元 g*

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

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

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

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

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

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

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

楕円曲線暗号 (ECC) ベースの 56A スキームのための鍵生成

ECC 鍵生成テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

ECC 公開鍵検証 (PKV) テスト

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

鍵確立スキーム

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

SP800-56A 鍵確立スキーム

評価者は、以下の機能及び検証テストを用いて、SP800-56A 鍵共有スキームの TOE の実装を検証しなければならない (shall)。各鍵共有スキームのためのこれらの検証テストは、勧告中の仕様に従った鍵共有スキームのコンポーネントが TOE に実装されていることを検証するものである。これらのコンポーネントには、DLC プリミティブ (共有秘密の値 Z) の計算と、鍵導出関数 (KDF) による導出鍵材料 (DKM) の計算が含まれる。鍵確認がサポートされる場合、評価者はまた以下に記述されるテスト手順を用いて、鍵確認のコンポーネントが正しく実装されていることも検証しなければならない (shall)。これには、DKM の解析、MAC データの生成、及び MAC タグの計算が含まれる。

機能テスト

機能テストは、鍵共有スキームを正しく実装する TOE の能力を検証する。このテストを行うために評価者は、TOE のサポートするスキームの既知の良好な実装からテストベクトルを生成または取得しなければならない (shall)。サポートされている鍵共有スキーム・鍵共有役割の組み合わせ、KDF タイプと (サポートされている場合には) 鍵確認役割・鍵確認タイプの組み合わせのそれぞれについて、試験者は 10 セットのテストベクトルを生成しなければならない (shall)。このデータセットは、10 セットの公開鍵

あたり1 セットのドメインパラメタ値 (FFC) またはNIST 認可曲線 (ECC) からなる。これらの鍵は、テストされるスキームにより静的鍵であるか、短期鍵であるか、またはその両方である。

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

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

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

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

検証テスト

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

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

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

SP800-56B 鍵確立スキーム

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

- *TSS には、TOE が適合する適切な 800-56 標準のすべてのセクションが列挙されていなければならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなければならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションをTOE が実装している場合には、それがTSS に記述され*

なければならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠が TSS に提供されなければならない (shall)。

800-56A 及び 800-56B (選択に応じて) の該当するセクションのそれぞれにおいて、「しなければならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それが記述されなければならない (shall)。

FCS_CKM_EXT.2(2) 暗号鍵ストレージ (MDM エージェント)

FCS_CKM_EXT.2.1(2) [選択:MDM エージェント、MDM エージェントプラットフォーム] は、永続的秘密及びプライベート鍵を使用していない際には、プラットフォームによって提供される鍵ストレージに保存しなければならない (shall)。

適用上の注意：

本要件によって、永続的秘密 (クレデンシャル、秘密鍵) とプライベート鍵が使用されていない際、セキュアに保存されることが確実となる。秘密／鍵の一部が TOE によって操作され、その他がプラットフォームによって操作される場合には、両方の選択が ST 作成者によって特定されることが可能であり、また ST 作成者は TOE によって操作される鍵とプラットフォームによって操作される鍵とを TSS 中に特定しなければならない (must)。

本要件は、MDM エージェントによって用いられる永続的秘密とプライベート鍵がモバイルプラットフォームによって保存されることを前提としている。

保証アクティビティ：

本要件が TOE と TOE プラットフォームのどちらによって満たされる場合であっても、評価者は TSS をチェックして、ST 中の要件を満たすことが必要とされる永続的秘密 (クレデンシャル、秘密鍵) とプライベート鍵のそれぞれが列挙されていることを保証する。これらの項目のそれぞれについて、評価者はそれが何の目的に用いられるか、そしてどのように保存されるかが TSS に列挙されていることを確認する。次に評価者は、以下のアクションを行う。

プラットフォームによって操作される永続的秘密及びプライベート鍵

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、MDM エージェントの ST にプラットフォームによって保存されるものとして列挙される永続的秘密及びプライベート鍵が、そのプラットフォームの ST で保護されるものとして特定されていることを保証しなければならない (shall)。

TOE によって操作される永続的秘密及びプライベート鍵

評価者は TSS をレビューして、TOE によって操作されるものとして列挙される項目のそれぞれについて、暗号化されずに永続的メモリへ書き込まれることはなく、またその項目がプラットフォームによって保存される、ということが立証されていることを判断する。

FCS_CKM_EXT.4 暗号鍵の破棄

FCS_CKM_EXT.4.1(2) [選択:MDM エージェント、MDM エージェントプラットフォーム] は、すべての平文の秘密及びプライベート暗号鍵ならびに CSP を、もはや必要とされなくなった際にゼロ化しなければならない (shall)。

適用上の注意：

MDM エージェントプラットフォームが平文の秘密、プライベート暗号鍵、及び CSP を用いる一切の操作を行わない場合、ST 作成者はプラットフォームを選択すべきである (should)。

あらゆるセキュリティ関連情報 (鍵や認証データ、そしてパスワードなど) 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。

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

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられる CSP であって TOE へ課される FCS_CKM_EXT.4 要件によってカバーされていないもののそれぞれが、TSS に記述されていることをチェックして保証しなければならない (shall)。

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 の TSS を検査して、上記に列挙された秘密鍵、プライベート鍵、及び鍵の生成に用いられる CSP がカバーされていることを保証しなければならない (shall)。

MDM エージェントによって満たされる要件

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられる CSP のそれぞれが、それらがゼロ化される時点 (例えば、使用直後、システムのシャットダウン時、など)、及び行われるゼロ化手続きの種類 (ゼロで上書き、ランダムパターンで 3 度上書き、など) と共に TSS に記述されていることをチェックして保証しなければならない (shall)。保護されるべきマテリアルの保存に異なる種類のメモリが用いられる場合、評価者はデータが保存されるメモリに応じたゼロ化手続き (例えば、「フラッシュメモリ上に保存される秘密鍵はゼロで 1 度上書きすることによってゼロ化されるが、内部ハードドライブ上に保存される秘密鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってゼロ化される」) が TSS に記述されていることをチェックして保証しなければならない (shall)。ゼロ化を検証するためにリードバックが行われる場合、このことも記述されなければならない (shall)。

TSS に記述される鍵クリア状況のそれぞれについて、評価者は以下のテストを繰り返さなければならない (shall)。

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

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

- *計測機能を備えた TOE ビルドをデバッガへロードする。*
- *クリア対象となる TOE 内の鍵の値を記録する。*
- *#1 の鍵に関する通常の暗号化処理を TOE に行わせる。*

- *TOE に鍵をクリアさせる。*
- *TOE に実行を停止させるが、終了はさせない。*
- *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。*
- *#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(5) 暗号操作 (デジタル署名)

FCS_COP.1.1(5) **詳細化：** [選択：MDM エージェント、MDM エージェントプラットフォーム] は、以下に特定された暗号アルゴリズムに従って暗号署名サービスを行わなければならない (shall) [選択：

- **2048 ビット以上の鍵サイズ (法) を用いた RSA デジタル署名アルゴリズム (RSA) であって FIPS PUB 186-2 または FIPS PUB 186-4, “Digital Signature Standard” を満たすもの、**
- **256 ビット以上の鍵サイズを用いた楕円曲線デジタル署名アルゴリズム (ECDSA) であって FIPS PUB 186-4, “Digital Signature Standard” (FIPS PUB 186-4, “Digital Signature Standard” に定義される) と「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] を満たすもの、**
- **2048 ビット以上の鍵サイズ (法) を用いたデジタル署名アルゴリズム (DSA) であって FIPS PUB 186-4, “Digital Signature Standard” *を満たすもの、その他*の暗号署名サービスなし]。**

適用上の注意：

MDM サーバと MDM エージェントの両方が、FTP_ITC_EXT.1 のプロトコルに従ってデジタル署名サービスを行わなければならない (must)。また MDM サーバは、デ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モバイルデバイスへ送信してもよい。MDM には、これらの署名されたポリシーを検証することが要求される。

複数のスキームがサポートされている場合には、ST 作成者は本要件を繰り返してこの機能を取り込むべきである (should)。用いられるスキームは、ST 作成者によって選択の中から選ばれることになる。

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

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 に主張されるデジタル署名機能に MDM エージェントの ST におけるデ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 エージェントの 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) デジタル署名機能が呼び出される方法が、MDM エー

ジェント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 エージェント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)。

MDM エージェントによって満たされる要件

鍵生成：

RSA 署名スキームの鍵生成

評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない (shall)。このテストは、公開鍵検証指数 e、秘密素因数 p 及び q、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。

- *ランダム素数：*
  - *証明可能素数*
  - *確率的素数*
- *条件付き素数：*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて証明可能素数とする (shall)*
  - *素数 p1、p2、q1 及び q2 を証明可能素数とし (shall)、p 及び q を確率的素数とする (shall)*
  - *素数 p1、p2、q1、q2、p 及び q を、すべて確率的素数とする (shall)*

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

ECDSA 鍵生成テスト

FIPS 186-4 ECDSA 鍵生成テスト

サポートされている NIST 曲線、すなわち P-256、P-284 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアを試験対象実装 (IUT) に生成させなければならない (shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない (shall)。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ提出しなければならない (shall)。

FIPS 186-4 公開鍵検証 (PKV) テスト

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

ECDSA アルゴリズムテスト

ECDSA FIPS 186-4 署名生成テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージを生成し、各メッセージについて公開鍵ならびに得られた署名の値 R 及び S を取得しなければならない (shall)。正しさを判断するため、評価者は既知の良好な実装の署名検証機能を利用しなければならない (shall)。

ECDSA FIPS 186-4 署名検証テスト

サポートされている NIST 曲線 (すなわち、P-256、P-284 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットの長さのメッセージ、公開鍵及び署名の組のセットを生成し、10 組のうち 5 組で値のいずれか (メッセージ、公開鍵または署名) を変更しなければならない (shall)。評価者は、これに応じた 10 個の合格/不合格値のセットを取得しなければならない (shall)。

RSA 署名アルゴリズムテスト

署名生成テスト

評価者は、署名生成テストを用いて TOE による RSA 署名生成の実装を検証しなければならない (shall)。このテストを行うために評価者は、TSF のサポートする法サイズ／SHA の組み合わせのそれぞれについて、高信頼リファレンス実装から 10 個のメッセージを生成または取得しなければならない (must)。評価者は、TOE に自分のプライベート鍵と法の値を用いてこれらのメッセージへ署名させなければならない (shall)。

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

署名検証テスト

評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない (shall)。評価者は、公開鍵 e、メッセージ、IR フォーマット、または署名、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(6) 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(6) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、特定された暗号アルゴリズム HMAC-[選択：SHA-1、SHA-256、SHA-384、SHA-512] であって、鍵サイズが *[割付：HMAC に用いられる (ビット単位の) 鍵サイズ]*、そしてメッセージダイジェストのサイズが [選択：160、256、384、512] ビットの、以下：FIPS PUB 198-1, “The Keyed-Hash Message Authentication Code”、及び FIPS PUB 180-3, “Secure Hash Standard” を満たすものに従って鍵付きハッシュによるメッセージ認証を行わなければならない (shall)。

適用上の注意：

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 (例えば高信頼チャネル) の鍵確立の目的で用いられる際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特定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(3) 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

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 エージェントの 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 エージェントの 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 エージェントの ST 中に選択されたモードと鍵サイズ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 エージェント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)。

MDM エージェントによって満たされる要件

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

サポートされているパラメタセットのそれぞれについて、評価者は 15 セットのテストデータを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_COP.1(7) 暗号操作 (暗号化及び復号)

FCS_COP.1.1(7) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、以下の特定された暗号アルゴリズム [選択：

- *(NIST SP 800-38A に定義される) AES-CBC モード、*
- *(NIST SP 800-38D に定義される) AES-GCM*

] 及び暗号鍵サイズ [選択：*128 ビット、256 ビット*] *の鍵サイズ*に従って [**暗号化／復号**] を行わなければならない (shall)。

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

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 エージェントの 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 エージェントの 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 エージェントの ST 中に選択されたモードと鍵サイズ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 エージェント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)。

MDM エージェントによって満たされる要件

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るものとし (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るものとする (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 ビットの鍵とする (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 とする (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する (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 とする (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ものとする (shall)。平文と IV の値は、128 ビットのブロックとする (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るものとする (shall)。

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

1000 回目の反復処理において計算された暗号文 (すなわち、CT[1000]) が、その試行の結果となる。この結果は、既知の良好な実装を用いて同一の値によって 1000 回反復処理を実行した結果と比較されなければならない (shall)。

評価者は、暗号化と同一のテストを用い、CT と PT とを入れ替え、AES-CBC-Encrypt を AES-CBC-Decrypt で置き換えて、復号機能をテストしなければならない (shall)。

AES-CCM テスト

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

- ***128 ビット及び 256 ビットの鍵***
- ***2 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する (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する (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 とする (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する (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する (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-GCM モンテカルロテスト

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

- ***128 ビット及び256 ビットの鍵***
- ***2 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する (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ものとする (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 とする (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する (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ものとする (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 ビットとする (shall)。*

評価者は、上記のパラメタ長の組み合わせのそれぞれについて、10 個の鍵、平文、AAD、及び IV の組のセットを用いて暗号化機能をテストし、AES-GCM 認証済み暗号化から得られた暗号文とタグを取得しなければならない (shall)。サポートされているタグの長さはそれぞれ、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)。

FCS_COP.1(8) 暗号操作 (ハッシュ)

FCS_COP.1.1(8) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、特定された暗号アルゴリズム [選択：*SHA-1*、*SHA-256*、*SHA-384*、*SHA-512*] であって、メッセージダイジェストのサイズが [選択：*160*、*256*、*384*、*512*] ビットの、以下：*FIPS Pub 180-4* を満たすものに従って暗号ハッシュを行わなければならない (shall)。

適用上の注意：

本 PP の将来の版では、SHA-1 は選択肢から削除されるかもしれない。SHA-1 によるデジタル署名の生成は 2013 年 12 月以降には許可されず、また SHA-1 によるデジタル署名の検証は、これらの署名の受容に存在する可能性のあるリスクのため、強く非推奨とされる。

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サイズの選択をサポートしなければならない (must)。ハッシュの選択は、FCS_COP.1(7) 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

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 エージェントの 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 エージェントの 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 エージェントの ST 中に選択されたダイジェストサイズ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 エージェント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)。

MDM エージェントによって満たされる要件

評価者は AGD 文書をチェックして、必要とされるハッシュのサイズに機能を構成するために行われることが必要とされる構成があれば、それが存在することを判断する。評価者は、

ハッシュ機能と他の TSF 暗号機能 (例えば、デジタル署名検証機能) との関連が TSS に文書化されていることをチェックしなければならない (shall)。

TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。このモードでは、TSF は長さがバイトの整数倍であるメッセージのみをハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。このモードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

評価者は、TSF によって実装され、本 PP の要件を満たすために用いられるハッシュアルゴリズムのそれぞれについて、以下のテストをすべて行わなければならない (shall)。

ショートメッセージテスト—ビット指向モード

評価者は m+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から m ビットまでシーケンシャルに変化する。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

ショートメッセージテスト—バイト指向モード

評価者は m/8+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から m/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

選択されたロングメッセージテスト—ビット指向モード

*評価者は m 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 99*i となる (ここで 1 ≤ i ≤ m)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*

選択されたロングメッセージテスト—バイト指向モード

*評価者は m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。i 番目のメッセージの長さは 512 + 8*99*i となる (ここで 1 ≤ i ≤ m/8)。メッセージの本文は、疑似ランダム的に生成されなければならない (shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。*

疑似ランダム的に生成されたメッセージテスト

このテストは、バイト指向の実装にのみ行われる。評価者は、n ビットの長さのシードをランダムに生成する。ここで n はテストされるハッシュ関数によって作成されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムに従って 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

FCS_RBG_EXT.1(2) 拡張：ランダムビット生成

FCS_RBG_EXT.1.1(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、[選択、1 つを選択：[選択：Hash_DRBG (任意) 、HMAC_DRBG (任意) 、CTR_DRBG (AES) 、Dual_EC_DRBG (任意)] を用いる NIST Special Publication 800-90A、FIPS Pub 140-2 附

属書 C：AES を用いる X9.31 附属書 2.4] に従って、すべての決定論的ランダムビット生成サービスを行わなければならない (shall) 。

FCS_RBG_EXT.1.2(2) 決定論的 RBG は、鍵とそれが生成するハッシュとの (NIST SP 800-57 による) セキュリティ強度の大きいほうと少なくとも等しい、最小で [選択：*128 ビット、256 ビット*] のエントロピーを持つ、 [選択：*ソフトウェアベースの雑音源、プラットフォームベースの RBG*] からエントロピーを蓄積するエントロピー源によってシードを供給されなければならない (shall)。

適用上の注意：

FCS_RBG_EXT.1.1 の最初の選択に関しては、ST 作成者は TOE か TOE のインストールされるプラットフォームのどちらが RBG サービスを提供するか選択すべきである (should)。MDM サーバと MDM エージェントのふるまいが異なる場合、ST 作成者は双方を選択すべきである (should)。

NIST Special Pub 800-90B の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり (should)、また本 PP の将来のバージョンでは必要とされることになる。

FCS_RBG_EXT.1.1 の 2 番目の選択に関しては、ST 作成者は RBG サービスが適合する標準 (800-90 または 140-2 附属書 C のいずれか) を選択すべきである (should)。

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

FCS_RBG_EXT.1.2 の 2 番目の選択に関しては、ST 作成者はエントロピー源がソフトウェアベースであるか、プラットフォームベースであるか、またはその両方であるかを示す。エントロピーの源が複数存在する場合には、ST には各エントロピー源のそれぞれについて、それがソフトウェアベースであるかプラットフォームベースであるかを含めて説明する。プラットフォームベースの雑音源が望ましい。

プラットフォームベースの RBG 源は、プラットフォームによって提供される検証済みの RBG の出力であり、これは FCS_RBG_EXT.1.1 に従って TSF の提供する DRBG のエントロピー源として利用される。このようにして、開発者は NIST SP800-90C に記述されているように RBG を連鎖する。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に記述される手法のみが有効であることに注意されたい。ここで用いられる AES 実装の鍵の長さが利用者データの暗号化に用いられるものと異なる場合には、FCS_COP.1 を調整するか繰り返して異なる鍵の長さを反映する必要があるかもしれない。FCS_RBG_EXT.1.2(1) の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に確実に含まれるようにする。

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

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 RBG 機能に MDM エージェントの ST における RBG 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 エージェントの 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) RBG 機能が呼び出される方法が、MDM エージェント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 エージェント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)。

MDM エージェントによって満たされる要件

附属書 E「エントロピーの文書化と評定」に従って、文書が作成されなければならない (shall) (そして評価者はアクティビティを行わなければならない (shall))。

ST 作成者がプラットフォームベースの雑音源を選択した場合、評価者はプラットフォームの ST を検査することによって、プラットフォームの RBG が検証されていることを検証しなければならない (shall)。評価者は、少なくとも本プロファイルに関して ST 作成者によって選択されたエントロピー量が、プラットフォームの RBG に供給されていることを検証しなければならない (shall)。この場合、ST 作成者はプラットフォームの RBG の附属書 E 文書に責任を負わない。

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

FIPS 140-2 の附属書 C に準拠する実装

本セクションに含まれるテストの参照情報は、The Random Number Generator Validation System (RNGVS) である。評価者は、以下の 2 つのテストを実施しなければならない (shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装によって作成されることに注意されたい。正しさの証明は、各スキームに任される。

評価者は、可変シードテストを行わなければならない (shall)。評価者は (Seed, DT) ペア (それぞれ 128 ビット) の 128 個のセットを TSF の RBG 機能に提供しなければならない (shall)。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。DT の値は、各セットについて 1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない (shall not)。評価者は、TSF によって返される値が期待値と一致することを保証する。

評価者は、モンテカルロテストを行わなければならない (shall)。このテストについては、評価者がシード及び DT の初期値 (それぞれ 128 ビット) を TSF の RBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。次に評価者は、繰返しのたびに DT の値を 1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に特定されるように次回の繰返しの際の新たなシードを作成して、TSF の RBG を 10,000 回呼び出す。評価者は、得られた 10,000 番目の値が期待値と一致することを保証する。

NIST Special Publication 800-90A に準拠する実装

評価者は、RBG 実装の 15 回の試行を行わなければならない (shall)。RBG 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、RBG 機能を構成するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない (shall)。

RBG が有効な予測困難性を持つ場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順になる。評価者は、ランダムなビット

の 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そしてPseronalization String である。次の2つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90A に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

RBG が予測困難性を持たない場合、各回の試行は (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) シードを再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。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**：個別化文字列の長さは、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 つの異なる長さの個別化文字列を用いなければならない (shall)。実装が個別化文字列を用いない場合、値を供給する必要はない。*

***追加的入力**：追加的入力のビット長は、個別化文字列の長さと同一のデフォルトと制約を持つ。*

識別と認証 (FIA)

FIA_X509_EXT.1(2) 拡張：X509 検証

FIA_X509_EXT.1.1(2) [選択：*MDM エージェント*、*MDM エージェントプラットフォーム*] は、以下のルールに従って証明書の有効性を確認しなければならない (shall)。

- RFC 5280 証明書の検証及び証明書パス検証。
- 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、証明書パスを検証しなければならない (shall)。
- TSF は、[選択：RFC 2560 に特定されるオンライン証明書状態プロトコル (OCSP)、RFC 5759 に特定される証明書失効リスト (CRL)] を用いて証明書の失効状態を検証しなければならない (shall)。
- TSF は、以下のルールに従って extendedKeyUsage フィールドを検証しなければならない (shall)。
    - 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、コード署名目的 (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) を持たなければならない

(shall)。

- TLS に提示されるクライアント証明書は、extendedKeyUsage フィールドにサーバ認証目的 (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) を持たなければならない (shall)。

適用上の注意：

FIA_X509_EXT.1.1 には、証明書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選択しなければならない (shall)。証明書は、TSF ソフトウェアの高信頼アップデートのため (FPT_TUD_EXT.1.3) 及びソフトウェアの完全性検証のため (FPT_TST_EXT.1.2) にオプションとして用いてもよく、また実装されている場合には、コード署名目的 extendedKeyUsage を含むことが検証されなければならない (must)。TLS、DTLS、または HTTPS が FPT_ITT.1 または FTP_TRP.1 もしくは FTP_TRP.2 において選択されている場合、証明書を利用して認証が行われなければならず (must)、また証明書にサーバ認証目的 extendedKeyUsage が含まれることが検証されなければならない (must)。

証明書の検証は、信頼済みルート証明書に至ることが期待されることに注意すべきである (should)。

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

FIA_X509_EXT.1.2(2) [選択：*MDM エージェント*、*MDM エージェントプラットフォーム*] 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)。

適用上の注意：

本要件は、MDM エージェントまたはプラットフォームによって用いられ処理される証明書に適用される。

保証アクティビティ

評価者は、どこで証明書の有効性のチェックが行われるか TSS に記述されていることを保証しなければならない (shall)。また評価者は、証明書パス検証アルゴリズムの記述も TSS に提供されていることも確認する。

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

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

テスト 1：評価者は、有効な証明書パスのない証明書の検証を行うと、その機能 (アプリケーションの検証、高信頼チャネルの設定、または高信頼ソフトウェアアップデート) が失敗することを論証しなければならない (shall)。次に評価者は、その機能で使われる証明書の

検証に必要とされる 1 つまたは複数の証明書をロードし、その機能が成功することを論証しなければならない (shall)。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなければならない (shall)。

テスト 2 : 評価者は、有効期限を過ぎた証明書の検証を行うと、その機能が失敗することを論証しなければならない (shall)。

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

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

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

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

FIA_X509_EXT.2(2) 拡張 : X509 認証

FIA_X509_EXT.2.1(2) [選択 : *MDM エージェント、MDM エージェントプラットフォーム*] は、RFC 5280 によって定義される X.509v3 証明書を用いて [選択 : *IPsec、TLS、HTTPS、DTLS*]] の認証、及び [選択 : *ソフトウェアアップデートのコード署名、ソフトウェア完全性検証のコード署名、ポリシー署名、追加用途なし*] をサポートしなければならない (shall)。

適用上の注意 :

ST 作成者の選択は、FPT_ITT.1 の選択と一致しなければならない (shall)。証明書は、システムソフトウェア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) にオプションとして用いてもよい。これらのコード署名用途のいずれかが選択されている場合、FIA_X509_EXT.2.4(2) が本体へ取り込まれなければならない (must)。FMT_POL_EXT.1.3 が本体へ取り込まれる場合、ポリシー署名が選択されなければならず (must)、また FIA_X509_EXT.2.6(2) が本体へ取り込まれなければならない (must)。

各クライアントはそれぞれ、MDM エージェントによって使用される一意の X.509v3 証明書を有すること。証明書はクライアント間で再利用されてはならない。

FIA_X509_EXT.2.2(2) [選択 : *MDM エージェント、MDM エージェントプラットフォーム*] 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 : *MDM エージェント、MDM エージェントプラットフォーム*] 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)。

適用上の注意 :

CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態の検証を行うために

接続を確立しなければならない (must) 場合は多々生ずる。この選択は、そのような接続が確立できない場合 (例えば、ネットワークエラーのため) のふるまいを記述するために用いられる。TOE が、証明書は FIA_X509_EXT.1 中の他の全てのルールに従って有効であると判断した場合、2 番目の選択に示されるふるまいによって有効性が判断されなければならない (shall)。証明書が FIA_X509_EXT.1 中の他の検証ルールのいずれかに失敗する場合、TOE はその証明書を受容してはならない (must not)。ST 作成者によって管理者構成オプションが選択された場合、ST 作成者はまた FMT_SMF.1(1) 中の機能 38 も選択しなければならない (must)。

FIA_X509_EXT.2.3(2) [選択：*MDM エージェント、MDM エージェントプラットフォーム*] は、ピア証明書が無効とみなされる場合には高信頼チャネルを確立してはならない (shall not)。

適用上の注意：

高信頼通信チャネルには、TSF によって行われる IPsec、TLS、HTTPS、または DTLS のいずれかが含まれる。有効性は証明書パス、有効期限、及び RFC 5280 にしたがう失効状態によって判断される。

保証アクティビティ

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

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

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

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

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

TSF の保護 (FPT)

FPT_TST_EXT.1(2): TSF のテスト

FPT_TST_EXT.1.1(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、最初の起動中 (電源投入時) に一連のセルフテストを実行し、MDM エージェントの正しい動作を論証しなければならない (shall)。

FPT_TST_EXT.1.2(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、[選択：MDM エージェント、MDM エージェントプラットフォーム] によって提供される暗号サービスの使用により、保存された MDM サーバ実行可能形式コードが実行のためにロー

ドされた際にその完全性を検証する機能を提供しなければならない (shall)。

適用上の注意：

TOE は典型的には IT 環境中で動作するソフトウェアパッケージであるが、それでも上記で求められるセルフテストアクティビティを行うことは可能である。しかし、上述のテストによって提供される保証の評定において、ホスト環境への多大な依存が存在する (ホスト環境が危殆化した場合にはセルフテストは意味をなさなくなることを意味する) ことは理解されるべきである (should)。

保証アクティビティ：

評価者は TSS を検査して、起動時に TSF によって実行されるセルフテストが詳述されていることを保証しなければならない (shall)。この記述には、実際に行われるテストの概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを保証することによってメモリがテストされる」のような記述が用いられなければならない (shall)) が含まれるべきである (should)。評価者は、TSF が正しく動作していることをテストが十分に論証するという論拠が TSS に示されていることを保証しなければならない (shall)。

評価者は TSS を検査して、保存された TSF 実行可能コードが実行のためにロードされた際にその完全性を検証する方法が記述されていることを保証しなければならない (shall)。評価者は、TSF 実行可能コードの完全性が危殆化されていないことをテストが十分に論証するという論拠が TSS に示されていることを保証しなければならない (shall)。また評価者は、TSS (または操作ガイダンス) に成功の (例えば、ハッシュが検証された) 場合と不成功の (例えば、ハッシュが検証されなかった) 場合に行われるアクションが記述されていることも検証する。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、既知の良好な TSF 実行可能形式に関する完全性チェックを行い、その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、その改変された TSF 実行可能形式に関する完全性チェックを行い、そのチェックが失敗することを検証する。*

4.5 セキュリティ保証要件

セクション 3 の TOE に関するセキュリティ対策方針は、セクション 2 に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 4.2、4.3、及び 4.4 のセキュリティ機能要件 (SFR) は、セキュリティ対策方針の形式的な実体化である。PP は EAL1 からセキュリティ保証要件 (SAR) を選び出し、評価者が評価の対象となる文書を評定して独立テストを行う範囲を設定する。

本セクションには CC からの SAR の完全なセットが含まれている一方で、評価者によって行われるべき保証アクティビティは本セクションと共にセクション 4.2、4.3、及び 4.4 の両方に詳述されている。

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

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

それぞれのファミリには、(もしあれば) 開発者によって提供される必要のある追加的文書／アクティビティを明確にするため、開発者アクションエレメントについて「開発者への

注意」が提供される。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加的アクティビティ (セクション 4.2、4.3、及び 4.4 ならびに EAL1 の CEM にすでに含まれているものに加えて) が記述される。さらに、本セクションに記述された保証アクティビティは、セクション 4.2、4.3、及び 4.4 に特定されたものとは相補的な関係にある。

TOE のセキュリティ保証要件は表 1 に要約されており、本 PP のセクション 3 に特定された対策方針を満たすために必要とされる管理及び評価アクティビティが特定されている。

表 1 TOE セキュリティ保証要件

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)

ASE クラス：セキュリティターゲット評価

CEM に定義される ASE アクティビティによる。

ADV クラス：開発

TOE に関する情報は ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。TOE 開発者は TSS に含まれる製品の記述を、機能仕様との関連において一致させなければならない (must)。セクション 4.2、4.3 及び 4.4 に含まれる保証アクティビティは、TSS セクションにふさわしい内容を判断するために十分な情報を ST 作成者へ提供すべきである (should)。

基本機能仕様 (ADV_FSP.1)

機能仕様は、対象となるセキュリティ機能インタフェース (TSFI) を記述するものである。これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、そのようなインタフェースは間接的なテストしかできないことから、そのようなインタフェースそれ自体を特定することにはあまり意味がない。本 PP では、このファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示されるインタフェースと、AGD 文書に提示されるインタフェースを理解することに焦点を絞るべきである (should)。特定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とはされない。

評価される必要のあるインタフェースは、独立した抽象的なリストとしてではなく、列挙された保証アクティビティを行うために必要な情報を通して特徴づけされる。

開発者アクションエレメント：

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

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

適用上の注意：

本セクションの概論で述べたように、機能仕様は AGD_OPR 及び AGD_PRE 文書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、文書及び TSS セクションに存在すべき (should) 証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容・提示エレメント：

ADV_FSP.1.1C 機能仕様は、SFR 実施及び SFR 支援の各 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 の追跡を論証するものでなければならない (shall)。

評価者アクションエレメント：

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

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

保証アクティビティ：

情報が提供されていることを確認すること以外に、これらの SAR に関連付けられた特定の保証アクティビティはない。機能仕様文書はセクション 4.2、4.3 及び 4.4 に記述された評価アクティビティと、AGD、ATE 及び AVA の SAR に関して記述されたその他のアクティビティをサポートするために提供されている。機能仕様情報の内容についての要件は、実施されるその他の保証アクティビティに基づいて暗黙に評価される。不十分なインタフェース情報のために評価者がアクティビティを実施できなかった場合、十分な機能仕様が提供されていなかったことになる。

AGD クラス：ガイダンス文書

ガイダンス文書は、ST と共に提供される。ガイダンスには、運用環境がセキュリティ機能に対する役割を満たすことができることを IT 要員が検証する方法の記述が含まれなければならない (must)。本文書は、非形式的なスタイルかつ IT 要員によって読解可能であるべきである (should)。

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

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

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

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)。

適用上の注意：

利用者操作ガイダンスは、単一の文書に含まれる必要はない。利用者、管理者及びアプリケーション開発者のためのガイダンスが、複数の文書またはウェブページに分散されていてもよい。必要に応じて、ガイダンス文書はセキュリティの自動化をサポートするためセキュリティ設定チェックリスト記述形式 (XCCDF) で表現される。

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

内容・提示エレメント：

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

適用上の注意：

利用者及び管理者は、利用者役割の定義において考慮されることになる。

AGD_OPE.1.2C 利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごとに記述しなければならない(shall)。

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

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

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

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

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

評価者アクションエレメント：

AGD_OPE.1.1E 評価者は、提供された情報が、証拠の内容・提示に対する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。また、以下の追加情報も必要となる。

暗号機能が TOE によって提供される場合、TOE の評価される構成と関連付けられた暗号エンジンを構成するための指示が操作ガイダンスに含まれなければならない (shall)。TOE の CC 評価の中で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、管理者へ与えられなければならない (shall)。

文書には、デジタル署名を検証することによって、TOE へのアップデートを検証するためのプロセスが記述されなければならない (must)。これは TOE によって行われても、基盤となるプラットフォームによって行われてもよい。評価者は、このプロセスに以下の手順が含まれることを検証しなければならない (shall)。

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

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

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)。

適用上の注意：

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

内容・提示エレメント：

AGD_ PRE.1.1C 準備手続きは、開発者の配付手続きに従って配付された TOE のセキュアな受入れに必要なすべてのステップを記述しなければならない (shall)。

AGD_ PRE.1.2C 準備手続きは、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：

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

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。

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

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。

保証アクティビティ：

評価者は、開発者が (彼らのプラットフォームの公共向け開発文書中で) 開発者のプラットフォーム向けアプリケーションの開発において利用に適当な 1 つ以上の開発環境を特定していることを保証しなければならない (shall)。これらの開発環境のそれぞれについて、開発者は 1 つまたは複数の環境におけるバッファオーバーフロー保護メカニズムが確実に発動されるように環境を設定する方法 (例えば、コンパイラのフラグ) に関する情報を提供しなければならない (shall)。評価者は、そのような保護がデフォルトでオンとなっているか、または具体的に有効化されなければならない (have to) のかという指摘もまた本文書に含まれていることを保証しなければならない (shall)。

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

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。

独立テスト—適合 (ATE_IND.1)

テストは、TSS と、提供された管理 (設定及び操作を含む) 文書に記述された機能を確認するために行われる。テストで重視されるのは、セクション 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、いくつかの追加的テストがセクション 4.4 中の SAR について特定されている。保証アクティビティは、これらのコンポーネントと関連付けられた追加的テストアクティビティを特定する。評価者は、テストの計画及び結果、ならびに本 PP への適合を主張するプラットフォーム／TOE の組み合わせに焦点を絞ったカバレージの論拠を文書化した、テスト報告書を作成する。

開発者アクションエレメント：

ATE_IND.1.1D 開発者は、テストのための 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 文書に含まれるもの以外に必要な設定があれば、それも記述される。評価者は、テストの一部として、または標準的なテスト前の条件として、AGD 文書に従って各プラットフォームの設置及び設定を行うことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供されるべきである (should)。またこれには、用いられるべき暗号エンジンの設定が含まれる。このエンジンによって実装される暗号アルゴリズムは、本 PP によって特定され、評価される暗号プロトコル (IPsec, TLS/HTTPS, SSH) によって用いられるものである。

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

AVA クラス：脆弱性評定

本プロテクションプロファイルの第一世代については、オープンソースの調査を行って、これらの種類の製品にどのような脆弱性が発見されているのかを見出すことが評価機関に期待される。多くの場合、これらの脆弱性には基本的な攻撃者を超える巧妙さが必要とされる。侵入テストツールが作成されて評価機関へあまねく配付されるまでは、評価者には TOE のこれらの脆弱性のテストを行うことは期待されない。評価機関には、ベンダによって提供された文書を考慮して、これらの脆弱性の存在する可能性についてコメントすることが期待される。この情報は侵入テストツールの開発と、将来のプロテクションプロファイルの開発のために用いられることになる。

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。

5. 根拠

脅威を対策方針へ、そして対策方針を要件へ追跡する根拠は、セクション 2.0 及び 3.0 の本文に含まれている。未解決となっている対応付けは前提条件と組織のセキュリティ方針についてのもののみであり、これらは以下の附属書 A に含まれている。

附属書A： 参考表

本プロテクションプロファイルにおいて、本文書の冒頭のセクションでは全体的なわかりやすさの向上を重視して、MDM システムへの脅威、これらの脅威を軽減するために用いられる手法、及び適合 TOE によって達成される軽減の程度について、説明文を提示した。この提示のスタイルは形式化された評価アクティビティにはそのまま適用できないため、本附属書では表形式のアーティファクトを用いて、本文書に関連付けられる評価アクティビティを説明する。

A.1 前提条件

以下のサブセクションに列挙された具体的な条件が、TOE の運用環境に存在することが前提となる。これらの前提条件には、TOE セキュリティ要件の開発における実質的な事実と、TOE の使用にあたって基本的な環境条件の両方が含まれる。

ST 作成者は、自身の特有の技術においてもこれらの前提条件が引き続き満たされることを保証すべきである (should)；表は適宜変更されるべきである (should)。

表 2 TOE の前提条件

前提条件の名称	前提条件の名称
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、接続性が利用できない、または信頼できないときは、堅牢に取り扱う。
A.MOBILE_DEVICE_PLATFORM	MDM エージェントは、暗号サービス及びデータ保護と同様にポリシーの実施を、評価済みモバイルプラットフォームとハードウェアに依存している。
A.MDM_SERVER_PLATFORM	MDM サーバは、管理機能を提供する信頼性のあ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、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サービスの提供、及び基本監査ログ管理機能の提供をこのプラットフォームに依存している。プラットフォームは、ネットワーク役割を MDM 機能性の提供に限定する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ための特別な構成が期待されている。
A.PROPER_ADMIN	1 人以上の能力のある信頼された要員であって、不注意、意図的な怠慢、または敵対的であったりしないものが 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、また合理的なエンタープライズのセキュリティ方針を遵守してデバイスを使用する。
A.TIMESTAMP	MDM エージェント及び MDM サーバを運用するプラットフォームは、高信頼タイムスタンプを提供できなければならない (shall)。

A.2 脅威

以下の脅威は、本文書に記述された要件を取り込む際に、ST 作成者によって技術に特有の脅威と統合されるべきである (should)。要件の変更、削除、及び追加はこのリストに影響を与えるかもしれないので、ST 作成者は適宜これらの脅威を変更または削除すべきである (should)。

表 3 脅威

脅威	脅威の説明
T.MALICIOUS_APPS	MDM の管理者またはモバイルデバイスの利用者が、不注意に悪意のあるコードをインポートしたり、または攻撃者が TOE または OE へ悪意のあるコードを挿入したりすることによって、TOE または TOE データの危殆化を招くおそれがある。
T.NETWORK_ATTACK	攻撃者が MDM サーバになりすまし、悪意のある管理コマンドを送信してモバイルデバイスの完全性の侵害しようとするかもしれない。攻撃者が MDM エージェントになりすまし、悪意のある記録を送信して MDM の完全性の侵害しようとするかもしれない。
T.NETWORK_EAVESDROP	権限のないエンティティが MDM とモバイルデバイスとの間の通信を傍受して、リモート管理コマンドを監視したり、アクセスを得たり、暴露したり、または改変するかもしれない。権限のないエンティティがモバイルデバイスとエンタープライズとの間の保護されていないワイヤレス通信を傍受して、TOE データを監視したり、アクセスを得たり、暴露したり、または改変するかもしれない。
T.PHYSICAL_ACCESS	モバイルデバイスが紛失または盗難にあい、権限のない人物が OE データへのアクセスしようとするかもしれない。

A.3 組織のセキュリティ方針

組織のセキュリティ方針は、組織がそのセキュリティニーズへ対処するために課すルール、プラクティス、及び手続きのセットである。以下の OSP は、TOE またはその運用環境によって実施されなければならない (must)。

表 4 組織のセキュリティ方針

方針の名称	方針の定義
P.ADMIN	モバイルデバイスのセキュリティ機能の構成は、エンタープライズのセキュリティ方針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エンタープライズ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

	者向けに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、即座に管理者へ通知しなければならない (must)。
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)。

A.4 TOE のセキュリティ対策方針

以下の表は、TOE のセキュリティ対策方針を特定したものである。

表 5 TOE のセキュリティ対策方針

対策方針	対策方針の説明
O.APPLY_POLICY	TOE は、モバイル OS との対話によって、モバイルデバイス上のエンタープライズセキュリティ方針の設定と実施を可能にしなければならない (must)。これには、管理サービスへのデバイスの初期登録から、ポリシーアップデートを含むライフサイクルを経て、管理サービスからの登録解除が行われるまでが含まれる。
O.ACCOUNTABILITY	TOE は、その管理者によって行われる管理者アクションを記録するロギング機能を提供しなければならない (must)。
O.DATA_PROTECTION_TRANSIT	TOE のエレメントやその運用環境から、またはそれらの間で交換されるデータは、監視、アクセス、及び改変から保護されなければならない (must)。
O.MANAGEMENT	TOE は、その管理機能に対するアクセス制御を提供する。

A.5 運用環境のセキュリティ対策方針

以下の表には、運用環境の対策方針が含まれる。前提条件が PP に追加された際には、これらの対策方針もそのような追加を反映して増補されるべきである (should)。

表 6 運用環境のセキュリティ対策方針

対策方針	対策方針の説明
OE.IT_ENTERPRISE	エンタープライズ IT 基盤は、TOE 及びモバイルデバイスが利用可能なネットワークに対して不正なアクセスを防止する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にポリシーの実施を、信頼性のあるモバイルプラットフォームとハードウェアに依存している。
OE.MDM_SERVER_PLATFORM	MDM サーバは、管理機能を提供する信頼性のあ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。
OE.PROPER_ADMIN	TOE 管理者は、すべての管理ガイダンスを遵守し信頼された方法で適用すると信頼されている。
OE.PROPER_USER	モバイルデバイスの利用者は、モバイルデバイスをセキュアに使用し、すべてのガイダンスを信頼された方法で適用するための教育を受けている。
OE.WIRELESS_NETWORK	ワイヤレスネットワークが、モバイルデバイスにて利用可能である。
OE.TIMESTAMP	高信頼タイムスタンプが、TOE の運用環境によって提供される。

附属書B： オプションの要件

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

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。

B.1 オプションの TSF 要件

セキュリティ監査 (FAU)

FAU_SEL.1(1) セキュリティ監査事象の選択 (MDM サーバ)

FAU_SEL.1.1(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]*。**

適用上の注意：

本要件の意図は、監査事象を引き起こすために選択可能なすべての基準を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管理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)。

B.2 オプションの MDM サーバまたは MDM サーバプラットフォーム要件

セキュリティ監査 (FAU)

FAU_SAR.1 監査レビュー (MDM サーバ)

FAU_SAR.1.1 **詳細化**：[選択：MDM サーバ、MDM サーバプラットフォーム] は、監査記録から**すべての監査データ**を読み出す能力を**正当な管理者**へ提供しなければならない (shall)。

FAU_SAR.1.2 詳細化：[選択：MDM サーバ、MDM サーバプラットフォーム] は、正当な管理者が情報を解釈するために適した形で監査記録を提供しなければならない (shall)。

適用上の注意：

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確実にすること、及び権限のない利用者による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：

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 1：評価者は、正当な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ガイドに特定されたフォーマットと一致することを保証しなければならない (shall)。

FAU_STG_EXT.2 拡張：監査事象ストレージ

FAU_STG_EXT.2.1 [選択：MDM サーバ、MDM サーバプラットフォーム] は、監査証跡の中に保存された監査記録を不正な改変から保護しなければならない (shall)。

適用上の注意：

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管理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)。MDM サーバ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：

評価者は、監査記録が不正な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検証しなければならない (shall)。評価者は、TOE が監査証跡特有の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)。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、権限の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、権限のある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、改変または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)。*

附属書C： 選択に基づいた要件

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

さらに、選択された要件によっては、セクション C.4「監査対象事象」が ST 中の監査対象事象表へ追加される必要もある。

本附属書は、TSF によって行われてもよい選択に基づいた要件、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選択に基づいた要件、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行われてもよい選択に基づいた要件、そして監査対象事象という、4 つのサブセクションに分かれている。

C.1 選択に基づいた TSF 要件

暗号サポート (FCS)

FCS_IV_EXT.1(1) 拡張：初期化ベクトルの生成

FCS_IV_EXT.1.1(1) MDM サーバは、表 9 に従って IV を生成しなければならない (shall)。

適用上の注意：

表 9 には、暗号モードのそれぞれについて、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応される。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 にのみ対応する。

保証アクティビティ：

評価者は TSS を検査して、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と、その暗号化に用いられる IV の生成が詳細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、同一の KEK によって暗号化される鍵のそれぞれに対する IV の生成が、表 9 を満たしていることを保証しなければならない (shall)。

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 MDM サーバは、 [選択：鍵ラップ (KW) モード、パディング付きの鍵ラップ (KWP) モード、GCM、CCM、CBC モード] の AES を用いてすべての鍵を暗号化しなければならない (shall)。

適用上の注意：

本要件は、TSF によって用いられる鍵が平文で保持されてはならない (shall not) ことを言明している。本要件の意図は、プライベート鍵、クレデンシャル、及び永続的秘密が TOE 内で暗号化されない状態で攻撃者に AES 鍵空間の総当りをすることなしにアクセスできないようにすることである 。 本要件は、プラットフォームによって提供される鍵ストレージではなく MDM サーバが暗号化を用いてプライベート鍵と永続的秘密を保護していることを FCS_CKM_EXT.2(1) 中の選択が示している場合、ST 中に取り込まれなければならない (must)。

本要件が ST に取り込まれる場合、FCS_IV_EXT.1 もまた取り込まれなければならない (must)。

保証アクティビティ：

評価者は TSS を検査して、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しなければならない (shall)。

評価者はTSS をレビューして、鍵材料が暗号化されずに永続的メモリへ書き込まれることはないことが立証され、また暗号化のモードが特定されていることを判断しなければならない (shall)。

C.2 選択に基づいたMDM サーバまたはMDM サーバプラットフォーム要件

暗号サポート (FCS)

FCS_DTLS_EXT.1 拡張：DTLS の実装

FCS_DTLS_EXT.1.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、 [選択：DTLS 1.0 (RFC 4347)、DTLS 1.2 (RFC 6347)] の 1 つ以上に従って DTLS プロトコルを実装しなければならない (shall)。

FCS_DTLS_EXT.1.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、 [選択：RFC 4347、RFC 6347] に従った変動が許可される場合を除き、DTLS の実装にはFCS_TLS_EXT.1 の中の要件を実装しなければならない (shall)。

適用上の注意：

DTLS と TLS との違いは、RFC 4347 及びRFC 6347 に概説されている。それ以外の点では、これらのプロトコルは同一である。特に、TOE に定義される適用可能なセキュリティ特性については、2 つのプロトコルに違いはない。したがって、FCS_TLS_EXT.1 に列挙されたすべての適用上の注意と保証アクティビティは、DTLS の実装に適用される。

保証アクティビティ：

評価者は、FCS_TLS_EXT.1 に列挙された保証アクティビティを行って、このコンポーネントを検証しなければならない (shall)。

FCS_HTTPS_EXT.1 拡張：HTTPS の実装

FCS_HTTPS_EXT.1.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、RFC 2818 に準拠する HTTPS プロトコルを実装しなければならない (shall)。

FCS_HTTPS_EXT.1.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、FCS_TLS_EXT.1 に特定される TLS を用いて HTTPS を実装しなければならない (shall)。

適用上の注意：

ST 作成者は、特定された 1 つまたは複数の標準に実装がどのように準拠しているかを判断するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへエレメントを追加することによって、またはTSS 中の追加的詳細によって、達成することができる。

保証アクティビティ：

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

FCS_IPSEC_EXT.1 拡張：インターネットプロトコルセキュリティ (IPsec) 通信

FCS_IPSEC_EXT.1.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、RFC 4301 に特定される IPsec アーキテクチャを実装しなければならない (shall)。

保証アクティビティ：

評価者は操作ガイダンスを検査して、廃棄 (DISCARD)、バイパス (BYPASS)、及び保護 (PROTECT) のルールを特定するエントリを SPD に構築する方法が管理者へ指示されていることを検証しなければならない (shall)。

評価者は、操作ガイダンスを用いて TOE 及びプラットフォームを構成し、以下のテストを行う。

テスト 1：評価者は SPD を、DISCARD、BYPASS、PROTECT のルールが存在するよう設定しなければならない (shall)。各パケットが 3 つのルールのどれか 1 つにマッチするように、パケットヘッダに適切なフィールドを持つ 3 つのネットワークパケットを評価者が送信できるよう、ルールの構築に用いられるセレクタは異なっていなければならない (shall)。評価者は、TOE が期待されたふるまいを示していることを、監査証跡を通して、またパケットキャプチャによって確認する。適切なふるまいとは、適切なパケットが破棄されたり、変更なしに通過したり、IPsec の実装によって暗号化されたりすることである。

テスト 2：評価者は、BYPASS と PROTECT という別の操作を行う、2 つの同一の SPD エントリを作り上げなければならない (shall)。次にこれらのエントリは 2 とおりの異なる順序で展開されるべきであり (should)、どちらの場合についても評価者は、該当するパケットを生成してパケットキャプチャ及びログによって確認を行うことにより、両方の場合で最初のエントリが適用されることを保証しなければならない (shall)。

テスト 3：評価者は、一方が他方の部分集合 (例えば、特定のアドレスとネットワークセグメント) となるように 2 つのエントリを作り上げるべき (should) ことを違いとして、上記の手順を繰り返さなければならない (shall)。ここでも管理者は両方の順序をテストして、ルールの限定性にかかわらず、最初のエントリが適用されることを保証すべきである (should)。

FCS_IPSEC_EXT.1.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、 [選択：トンネルモード、トランスポートモード] を実装しなければならない (shall)。

保証アクティビティ：

評価者は TSS をチェックして、TOE が (選択されたように) トンネルモードまたはトランスポートモード、あるいはその両方で動作できると言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、TOE を選択された各モードに構成する方法が運用ガイドで管理者へ指示されていることを確認しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 (条件付き)：トンネルモードが選択されている場合、評価者は操作ガイダンスを用いて TOE をトンネルモードで動作するように構成し、また VPN GW もトンネルモードで動作するように構成する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いるように TOE 及び VPN GW を構成し、許容される SA がネゴシエーションできることを保証する。評価者は次に、TOE からの接続を開始し、VPN GW ピアへ接続しなければならない (shall)。評価者は、トンネルモードを用いた接続の確立が成功していることを、監査証跡及びキャプチャされたパケットで確認する。*
- *テスト 2 (条件付き)：トランスポートモードが選択されている場合、評価者は操作ガイダンスを用いて TOE をトランスポートモードで動作するように構成し、また VPN GW もトランスポートモードで動作するように構成する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いるように TOE 及び VPN GW を構成し、許容される SA がネゴシエーションできることを保証する。評価者は次に、TOE からの接続を開始し、VPN GW へ接続する。評価者は、トランスポートモードを用いた接続の確立が成功していることを、監査証跡及びキャプチャされたパケットで確認する。*

FCS_IPSEC_EXT.1.3(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、その他のエントリにマッチしなかったものすべてにマッチして廃棄する名目的なエントリを SPD の最後に持たなければならない (shall)。

保証アクティビティ：

評価者は TSS を検査して、SPD に対してパケットが処理される方法と、マッチする「ルール」が存在しない場合には暗黙的または明示的にネットワークパケットを廃棄させる最後のルールが存在することが、TSS に記述されていることを検証しなければならない (shall)。

評価者は、操作ガイダンスに SPD の構築方法に関する指示が提供されていることをチェックし、そのガイダンスを用いて以下のテストのために TOE／プラットフォームを構成する。

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、ネットワークパケットを廃棄 (DISCARD)、バイパス (BYPASS)、及び保護 (PROTECT) する操作が含まれるエントリが存在するように SPD を設定しなければならない (shall)。評価者は、FCS_IPSEC_EXT.1.1 を検証するために作成された SPD を使ってもよい。評価者は BYPASS エントリとマッチするネットワークパケットを構築し、そのパケットを送信しなければならない (shall)。評価者は、ネットワークパケットが変更されずに適切な宛先インタフェースへ通過されることを確認すべきである (should)。評価者は次に、もはや評価者が作成したエントリへはマッチしないようにパケットヘッダのフィールドを変更しなければならない (shall) (それ以前のエントリのどれにもマッチしなかったパケットを廃棄する「TOE／プラットフォームによって作成された」最後のエントリが存在するかもしれない)。評価者はそのパケットを送信し、パケットがどの TOE のインタフェースへの流出も許可されないことを確認する。

FCS_IPSEC_EXT.1.4(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、RFC 4303 に定義される IPsec プロトコル ESP を、RFC 4106 で特定される暗号アルゴリズム AES-GCM-128、AES-GCM-256、[選択：AES-CBC-128、AES-CBC-256 (両者とも RFC 3602 で特定される) と Secure Hash Algorithm (SHA) ベースの HMAC との組み合わせ、その他のアルゴリズムなし] を用いて実装しなければならない (shall)。

保証アクティビティ：

評価者は TSS を検査して、アルゴリズム AES-GCM-128 及び AES-GCM-256 が実装されていることを検証しなければならない (shall)。ST 作成者が AES-CBC-128 または AES-CBC-256 のいずれかを要件に選択している場合には、評価者はそれらもまた TSS に記述されていることを検証する。評価者は操作ガイダンスをチェックして、AES-GCM-128 及び AES-GCM-256 アルゴリズムを使用するように TOE を構成する方法について指示が与えられていること、また AES-CBC-128 または AES-CBC-256 のいずれかが選択されている場合にはこれらについても使用方法がガイダンスに指示されていることを保証しなければならない (shall)。評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は操作ガイダンスの指示により TOE を構成し、TOE が AES-GCM-128 及び AES-GCM-256 アルゴリズムのそれぞれを使用するように構成して、ESP を使用した接続の確立を試行しなければならない (shall)。ST 作成者が AES-CBC-128 または AES-CBC-256 のいずれかを選択している場合には、TOE はこれらのアルゴリズムを使用するよう構成され、評価者は選択されたこれらのアルゴリズムについて ESP を使用した接続の確立を試行する。*

FCS_IPSEC_EXT.1.5(1) TSF は、以下のプロトコルを実装しなければならない (shall)。[選択：RFC 2407、2408、2409、RFC 4109、[選択：拡張シーケンス番号についてその他の RFC なし、拡張シーケンス番号について RFC 4304] 及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義される IKEv1；RFC 5996 (セクション 2.23 に特定される NAT トラバーサルのサポートが必須)、4307、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義される

IKEv2]。

保証アクティビティ：

評価者は TSS を検査して、IKEv1 または IKEv2、あるいはその両方が実装されていることを検証しなければならない (shall)。評価者は操作ガイダンスをチェックして、 (選択されたように) IKEv1 または IKEv2、あるいはその両方を使用するように TOE を構成する方法が管理者へ指示されていることを保証しなければならず (shall)、またガイダンスを利用して NAT トラバーサルを行うよう TOE を構成し、以下のテストを行う。

- *テスト 1：評価者は、TSS 及び RFC 5996 のセクション 2.23 に記述されているように NAT トラバーサル処理を行うよう TOE を設定しなければならない (shall)。評価者は IPsec 接続を開始し、NAT トラバーサルが成功することを判断しなければならない (shall)。*

FCS_IPSEC_EXT.1.6(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、[選択：IKEv1、IKEv2] プロトコルにおける暗号化されたペイロードに暗号アルゴリズムとして RFC 6379 に特定される AES-CBC-128、AES-CBC-256 及び [選択：RFC 5282 に特定される AES-GCM-128、AES-GCM-256、その他のアルゴリズムなし] が用いられることを確実にしなければならない (shall)。

保証アクティビティ：

評価者は、IKEv1 または IKEv2、あるいはその両方のペイロードの暗号化に用いられるアルゴリズムが TSS に特定されていること、及びアルゴリズム AES-CBC-128、AES-CBC-256 が指定されていること、さらに要件の選択においてその他が選択されている場合には、それらが TSS の論拠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、必須のアルゴリズム (要件において選択された追加アルゴリズムがあればそれについても) を使用するよう TOE を構成できる方法が操作ガイダンスに記述されていることを保証しなければならない (shall)。次にガイダンスを用いて TOE を構成し、以下のテストを行う。

- *テスト 1：評価者は、IKEv1 または IKEv2、あるいはその両方のペイロードの暗号化に AES-CBC-128 を使用するよう TOE を構成し、AES-CBC-128 を用いて暗号化されたペイロードのみを受け入れるように構成されたピアデバイスとの接続を確立しなければならない (shall)。評価者は、監査証跡を参照してこのアルゴリズムがネゴシエーションにおいて使用されたものであることを確認すること。*

FCS_IPSEC_EXT.1.7(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、IKEv1 フェーズ 1 交換ではメインモードのみが用いられることを確実にしなければならない (shall)

適用上の注意：

FCS_IPSEC_EXT.1.7 は、IKEv1 が選択されている場合にのみ適用される

保証アクティビティ：

評価者は TSS を検査して、TOE でサポートされている IPsec プロトコルの記述において、IKEv1 フェーズ 1 交換にアグレッシブモードが使用されずメインモードのみが使用されることが言明されていることを保証しなければならない (shall)。これは設定可能なオプションであってもよい。動作前に TOE のモードを構成する必要がある場合には、評価者は操作ガイダンスをチェックしてこの構成の指示がそのガイダンスに含まれていることを保証しなければならない (shall)。評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 (条件付き)：評価者は操作ガイダンスの指示により TOE を構成して、アグレッシブモードで IKEv1 フェーズ 1 接続を使用して接続の確立を試行しなければならない (shall)。この試行は失敗するはずである (should)。評価者は次に、メインモードの交換がサポートされていることを示すべきである (should)。このテ*

ストは、IKEv1 が上記 FCS_IPSEC_EXT.1.5 プロトコル選択において選択されていない場合には適用されない。

FCS_IPSEC_EXT.1.8(1) [選択 : MDM サーバ、MDM サーバプラットフォーム] は、 [選択 : IKEv2 SA ライフタイムを正当な管理者がパケット数／バイト数または経過時間に基づいて構成できるとともにフェーズ 1 SA については 24 時間かつフェーズ 2 SA については 8 時間にその値が制限できる、IKEv1 SA ライフタイムを正当な管理がパケット数／バイト数または経過時間に基づいて構成できるとともにフェーズ 1 SA については 24 時間かつフェーズ 2 SA については 8 時間にその値が制限できる] ことを確実にしなければならない (shall)。

適用上の注意：

ST 作成者は、自分の実装における IKE のバージョンに基づいて選択が与えられる。SA ライフタイムをエージェントにプッシュするよう MDM サーバを管理者が構成できる実装は、両者とも受容可能である。

SA ライフタイムに関する限り、TOE は送信されたバイト数、または送信されたパケット数に基づいてライフタイムを制限できる。パケットベース、またはボリュームベースの SA ライフタイムはいずれも受容可能である。

ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 中の選択によっては両方を) 選択する。IKEv1 要件は、正当な管理者によって設定可能なライフタイムを提供すること (AGD_OPE によって義務付けられる文書中の適切な指示と共に)、または制限を実装に「ハードコーディング」することの、いずれかの手段によって達成することができる。IKEv2 については、ハードコーディングされた制限は存在しないが、この場合には管理者が値を構成できることが必要とされる。一般的には、SA のライフタイムを含む実装のパラメタを設定するための指示が、AGD_OPE に関して作成された管理ガイダンス中に含まれるべきである (should)。同一の鍵によって保護されるトラフィック量 (その鍵によって保護されるすべての IPsec トラフィックの全体量) の制限を TOE が設定できる限り、パケット数の代わりに MB/KB 数によって要件を詳細化することは妥当である。

保証アクティビティ：

ライフタイムの確立及び実施方法については RFC に記述されており、評価者は本セクションの冒頭に述べたように TSS を検査する。評価者は、SA ライフタイムの値が設定可能であり、その指示が操作ガイダンス中に存在することを検証しなければならない (shall)。評価者は、管理者がフェーズ 1 SA の値を 24 時間、フェーズ 2 SA の値を 8 時間に設定できることを保証しなければならない (shall)。現時点ではパケット数またはバイト数に関して義務付けられた値は存在しないため、評価者はこれが構成できることのみを保証する。

このテストにあたって、評価者は双方が適切に構成されていることを保証する必要がある。RFC には以下のように記載されている。「IKEv1 と IKEv2 との違いは、IKEv1 SA のライフタイムがネゴシエーションされることである。IKEv2 においては、SA の両端が独自のライフタイムポリシーを SA に適用し、必要に応じて SA の鍵アップデートを行う責任がある。両端で異なるライフタイムポリシーが採用されている場合、その結果として、より短いライフタイムの側が常に鍵アップデートを要求することになるだろう。両端で同一のライフタイムポリシーが採用されている場合、同時に双方が鍵アップデートを開始することもあり得る (その結果、冗長な SA が生じることになる)。このようなことが起きる確率を減らすため、鍵アップデート要求のタイミングにはジッタを持たせるべきである (SHOULD)。」

以下のテストはそれぞれ、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のバージョンのそれぞれについて行われなければならない (shall)。

- *テスト 1 : 評価者は、操作ガイダンスに従って許容されるパケット数 (またはバイト数) に関して最大のライフタイムを設定しなければならない (shall)。評価者は SA を確立し、この SA の通過が許可されるパケット数 (またはバイト数) を超えた際に接続がクローズされることを判断しなければならない (shall)。*

- *テスト 2：評価者は、フェーズ 1 SA が確立され、再ネゴシエーションまでに 24 時間を超えて維持が試行されるようにテストを構築しなければならない (shall)。評価者は、24 時間以内にこの SA がクローズされるか、再ネゴシエーションされることを確認しなければならない (shall)。そのようなアクションのために TOE が特定の構成を必要とする場合、評価者は TOE の構成機能が操作ガイダンスに文書化されたように動作することを論証するテストを実施しなければならない (shall)。*
- *テスト 3：評価者は、ライフタイムが 24 時間ではなく 8 時間であることを除いて、テスト 1 と同様のテストをフェーズ 2 SA に対して行わなければならない (shall)。*

FCS_IPSEC_EXT.1.9(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、IKE Diffie-Hellman 鍵交換に用いられる秘密の値 x (g^x mod p における「x」) を、FCS_RBG_EXT.1 に特定されるランダムビット生成器を用い、また少なくとも *[割付：NIST SP 800-57, Recommendation for Key Management – Part 1: General の表 2 に掲げるネゴシエーション済み Diffie-Hellman グループに関連付けられた「等価安全性 (bits of security)」の値の少なくとも 2 倍のビット数 (1 つまたは複数)*] のビット長を有するように生成しなければならない (shall)。

FCS_IPSEC_EXT.1.10(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、IKE 交換に用いられるノンスを、特定の IPsec SA のライフタイム内に特定のノンス値が繰り返される確率が 2^[*割付：NIST SP 800-57, Recommendation for Key Management – Part 1: General の表 2 に掲げるネゴシエーション済み Diffie-Hellman グループに関連付けられた「等価安全性 (bits of security)」の値 (1 つまたは複数)*] 分の 1 未満になるように生成しなければならない (shall)。

適用上の注意：

実装によって、異なる Diffie-Hellman グループを SA の形成に用いるようネゴシエーションできるかもしれないため、FCS_IPSEC_EXT.1.9 と FCS_IPSEC_EXT.1.10 中の割付は複数の値を含むかもしれない。サポートされる DH グループのそれぞれについて、ST 作成者は 800-57 の表 2 を参照して、その DH グループに関連付けられる「等価安全性」を判断する。次に、それぞれ一意の値を用いて割付への記入が行われる (1.9 については倍の値を、1.10 については直接その値を割付へ記入する)。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートしている実装を想定してみよう。表 2 から、グループ 14 の等価安全性は 112 であり、グループ 20 については 192 である。したがって FCS_IPSEC_EXT.1.9 の割付は「[224, 384]」となり、FCS_IPSEC_EXT.1.10 の割付は「[112,192]」となるであろう (しかしこの場合には、数学的に意味のある値とするために、おそらく要件を詳細化すべきだろう (should))。

FCS_IPSEC_EXT.1.11(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、すべての IKE プロトコルに DH グループ 14 (2048 ビット MODP)、及び [選択：19 (256 ビットランダム ECP)、5 (1536 ビット MODP)、24 (2048 ビット MODP と 256 ビット POS)、20 (384 ビットランダム ECP)、[*割付：TOE の実装するその他の DH グループ*]、その他の DH グループなし] を確実に実装しなければならない (shall)。

適用上の注意：

この選択は、追加的にサポートされる DH グループを特定するために用いられる。これは、IKEv1 及び IKEv2 鍵交換に適用される。本 PP の将来のバージョンでは、DH グループ 19 及び 20 が要求されることになる。何らかの追加的な DH グループが特定される場合、それは FCS_CKM.1 に列挙される要件に (確立される短期鍵の意味で) 適合しなければならない (must) ことに注意すべきである (should)。

保証アクティビティ：

評価者は、TSF のサポートする DH グループのそれぞれについて、「x」(FCS_IPSEC_EXT.1.9 の定義による) 及び各ノンスを生成するプロセスが TSS に記述され

ていることをチェックし保証しなければならない (shall)。評価者は、本 PP 中の要件を満たす生成された乱数が使われること、及び「x」とノンスの長さが要件中の規定を満たすことが、TSS に示されていることを検証しなければならない (shall)。

評価者は、要件に特定された DH グループがサポートされるものとして TSS に列挙されていることをチェックし保証しなければならない (shall)。1 つよりも多くの DH グループがサポートされる場合、評価者は特定の DH グループをピアとの間で指定／ネゴシエーションする方法が TSS に記述されていることをチェックし保証する。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：サポートされる DH グループのそれぞれについて、評価者はその特定の DH グループを用いてすべての IKE プロトコルの完了が成功することをテストし保証しなければならない (shall)。*

FCS_IPSEC_EXT.1.12(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、すべての IKE プロトコルで RFC 4945 及び [選択：事前共有鍵、その他の手法なし] に準拠する X.509v3 証明書を用いる [選択：RSA、ECDSA] を用いたピア認証が行われることを確実にしなければならない (shall)。

適用上の注意：

適合 TOE には少なくとも 1 つの公開鍵ベースのピア認証手法が必要とされる。TOE による実装を反映して、1 つ以上の公開鍵方式が ST 作成者によって選択される。また ST 作成者は、用いられるアルゴリズム (及び、提供されている場合には鍵生成機能) を反映した適切な FCS 要件が、これらの手法をサポートするものとして列挙されていることも保証する。TSS には、これらのアルゴリズムが用いられる方法も詳述されることになる (例えば、2409 では公開鍵を用いる 3 つの認証手法が特定されており、TSS ではこれらのうちサポートされているものが記述されることになる) ことに注意されたい。

FCS_IPSEC_EXT.1.13(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、証明書に含まれる識別名 (DN) が接続の確立を試行しているエンティティに期待される DN にマッチしない場合、SA を確立してはならない (shall not)。

保証アクティビティ：

評価者は、RSA または ECDSA、あるいはその両方がピア認証を行うために使われるものとして TSS に特定されていることを保証しなければならない (shall)。選択の中で事前共有鍵が選択されている場合、事前共有鍵が確立された IPsec 接続の認証に用いられる方法が TSS に記述されていることを評価者はチェックし保証しなければならない (shall)。評価者は、事前共有鍵が生成され TOE に対して確立される方法が操作ガイダンスに記述されていることをチェックしなければならない (shall)。また TSS と操作ガイダンス中の記述には、事前共有鍵を生成できる TOE と、単純に事前共有鍵を利用するだけの TOE との両方について、事前共有鍵の確立が実現される方法が示されていなければならない (shall)。評価者は、暗号アルゴリズムとして RSA または ECDSA、あるいはその両方を使用するように TOE を設定する方法が操作ガイダンスに記述されていることを保証しなければならない (shall)。

以下のテストのための環境を構築し TOE を構成するため、評価者は信頼できる CA へ接続するように TOE を構成する方法も操作ガイダンスに記述されていることを保証し、またその CA の有効な証明書が TOE にロードされ「信頼できる (trusted)」とマークされることを保証すること。

評価者は、FIA_X509_EXT.2.1 のテストと組み合わせて証明書の検証を検証するテストを行わなければならない (shall)。

- *テスト 1 [条件付き]：評価者は、操作ガイダンスに示されるように事前共有鍵を生成して、それを用いて TOE とそのピアとの間の IPsec 接続を確立させなければならない (shall)。TOE が事前共有鍵の生成をサポートしている場合、鍵を生成する*

TOE のインスタンスだけではなく、単に鍵を受け取り利用するだけの TOE のインスタンスについても、鍵の確立が行われることを評価者は保証しなければならない (shall)。

FCS_IPSEC_EXT.1.14(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、デフォルトで [選択：IKEv1 フェーズ 1、IKEv2 IKE_SA] 接続を保護するためにネゴシエーションされる対称アルゴリズムの強度 (鍵のビット数の意味で) が [選択：IKEv1 フェーズ 2、IIKEv2_CHILD_SA] 接続を保護するためにネゴシエーションされる対称アルゴリズムの強度 (鍵のビット数の意味で) 以上であることを確実にしなければならない (shall)。

適用上の注意：

ST 作成者は、TOE による実装に基づいて IKE に関する選択のいずれか、または両方を選ぶ。もちろん、選ばれた IKE バージョンはこのエレメントだけでなく、このコンポーネント中の他のエレメントの他の選択とも一貫しているべきである (should)。TOE がこの機能を設定可能とすることは受容可能であるが、評価される構成中のデフォルト構成 (「箱から出した状態」または AGD 文書中の設定ガイダンスによる) では、この機能が有効になっていなければならない (must)。

保証アクティビティ：

評価者は、IKE 及び ESP 交換に許可されるアルゴリズムの潜在的な強度 (対称鍵のビット数の意味で) が TSS に記述されていることをチェックしなければならない (shall)。また TSS には、IKEv1 フェーズ 2 または IKEv2 CHILD_SA スイート、あるいはその両方のネゴシエーション時に行われる、ネゴシエーションされたアルゴリズムの強度 (対称アルゴリズムにおける鍵のビット数の意味で) がネゴシエーションを保護する IKE SA の強度以下であることを保証するために行われるチェックについて記述されていなければならない (shall)。

評価者は、単純にガイダンスに従って TOE を構成し、以下のテストを行う。

- *テスト 1：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、要件中に特定されたサポートされるアルゴリズムとハッシュ関数のそれぞれを用いて IPsec 接続のネゴシエーションを成功させなければならない (shall)。*
- *テスト 2：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、IKE SA に用いられるものよりも強度の大きい暗号化アルゴリズム (すなわち、IKE SA に用いられるものよりも大きい鍵サイズの対称アルゴリズム) を選択する ESP について SA の確立を試行しなければならない (shall)。そのような試行は失敗するはずである (should)。*
- *テスト 3：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、要件中に特定されたサポートされるアルゴリズムとハッシュ関数以外のものを用いて IKE SA の確立を試行しなければならない (shall)。そのような試行は失敗するはずである (should)。*
- *テスト 4：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、FCS_IPSEC_EXT.1.4 に特定されない暗号化アルゴリズムを選択する ESP (適切なパラメタが IKE SA の確立に用いられることを前提として) について SA の確立を試行しなければならない (shall)。そのような試行は失敗するはずである (should)。*

FCS_SSH_EXT.1 拡張：SSH の実装

FCS_SSH_EXT.1.1 [選択：MDM サーバ、MDM サーバプラットフォーム] は、RFC 4251、4252、4253、4254、4335、5656、6187 及び 6668.に準拠する SSH プロトコルを実装しなければならない (shall)。

適用上の注意：

ST 作成者は、特定された 1 つまたは複数の標準に実装がどのように準拠しているかを判断するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへエレメントを追加することによって、または TSS 中の追加的詳細によって、達成することができる。

本 PP の次のバージョンでは、鍵アップデートに関して要件が追加されることになる。本要件は、「TSF は、その鍵を用いて 2^{28} 以下のパケットが通過した後に SSH 接続が鍵アップデートされることを確実にしなければならない (shall)」*となる。*

FCS_SSH_EXT.1.2 [選択：MDM サーバ、MDM サーバプラットフォーム] は、SSH プロトコルの実装が RFC 4252 に記述される以下の認証手法をサポートすることを確実にしなければならない (shall)：公開鍵に基づくもの、パスワードに基づくもの。

保証アクティビティ：

評価者は、認証への使用に受容可能な公開鍵アルゴリズムの記述が TSS に含まれること、このリストが FCS_SSH_EXT.1.5 に適合すること、そしてパスワードに基づく認証手法もまた許可されることをチェックして保証しなければならない (shall)。また評価者は、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、サポートされる公開鍵アルゴリズムのそれぞれについて、その公開鍵アルゴリズムを用いた利用者接続の認証を TOE がサポートすることを示さなければならない (shall)。このテストをサポートするために要求される構成アクティビティが存在する場合、それは操作ガイダンス中の指示に従って行われなければならない (shall)。*
- *テスト 2：操作ガイダンスを用いて、評価者はパスワードに基づく認証を受け入れるように TOE を構成し、認証子としてパスワードを用いた SSH 上で TOE への利用者の認証が成功することを論証しなければならない (shall)。*

FCS_SSH_EXT.1.3 [選択：MDM サーバ、MDM サーバプラットフォーム] は、RFC 4253 に記述されるように、SSH トランスポート中の *[割付：バイト数]* を超える大きさのパケットが破棄されることを保証しなければならない (shall)。

適用上の注意：

RFC 4253 は、「大きなパケット (large packets)」の受け入れを、そのパケットが「合理的な長さ (reasonable length)」でなければ破棄されるべき (should) という注意と共に特定している。割付には受け入れられる最大のパケットサイズが ST 作成者によって記入され、これによって TOE の「合理的な長さ (reasonable length)」が定義されるべきである (should)。

保証アクティビティ：

評価者は、RFC 4253 の意味での「大きなパケット (large packets)」がどのように検出され取り扱われるか TSS に記述されていることをチェックしなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、このコンポーネントに特定されたものよりも大きなパケットを TOE が受信すると、そのパケットが破棄されることを論証しなければならない (shall)。*

FCS_SSH_EXT.1.4 [選択：MDM サーバ、MDM サーバプラットフォーム] は、SSH トランスポートの実装が以下の暗号化アルゴリズムを用いることを確実にしなければならない (shall)：AES-CBC-128、AES-CBC-256、[選択：AEAD_AES_128_GCM、AEAD_AES_256_GCM、*その他のアルゴリズムなし*]。

適用上の注意：

割付の中で、ST 作成者はAES-GCM アルゴリズムを選択するか、またはAES-GCM がサポートされない場合には「その他のアルゴリズムなし」を選択することができる。AES-GCM が選択される場合、対応するFCS_COP エントリがST 中に存在すべきである (should)。

保証アクティビティ：

評価者はTSS 中のこのプロトコルの実装の記述をチェックして、オプションの特徴が特定され、またサポートされる暗号スイートも特定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、特定された暗号化アルゴリズムがこのコンポーネントに列挙されたものと同一であることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、SSH がTSS 中の記述に適合するようにTOE を構成するための指示 (例えば、TOE によって通知されるアルゴリズムのセットが、要件に合うよう制限されなければならない (have to) かもしれない) 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、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、要件に特定された暗号化アルゴリズムのそれぞれを用いて、SSH 接続を確立しなければならない (shall)。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。*

FCS_SSH_EXT.1.5 [選択：MDM サーバ、MDM サーバプラットフォーム] は、SSH トランスポートの実装がその 1 つまたは複数の公開鍵アルゴリズムとして SSH_RSA 及び [選択 ： PGP-SIGN-RSA 、 PGP-SIGN-DSS 、 ecdsa-sha2-nistp256 、 ecdsa-sha2-nistp384 、 ecdsa-sha2-nistp521、その他の公開鍵アルゴリズムなし] を用いることを確実にしなければならない (shall)。

適用上の注意：

RFC 4253 は、要求される (required) 公開鍵アルゴリズムと許可できる (allowable) 公開鍵アルゴリズムを特定している。本要件によってSSH-RSA は「要求される (required)」ものとなり、またその他がST 中で主張できるようになる。ST 作成者は、SSH_RSA のみが実装される場合には「その他の公開鍵アルゴリズムなし」を選択して、適切な選択を行うべきである (should)。

保証アクティビティ：

評価者はTSS をチェックして、サポートされる公開鍵アルゴリズムが列挙されていること、またそのリストがこのコンポーネント中のリストと対応していることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、SSH プロトコルに用いられる公開鍵を構成する方法に関する管理者へ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)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は、要件に特定された公開鍵アルゴリズムのそれぞれを用いて、SSH 接続を確立しなければならない (shall)。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。*

FCS_SSH_EXT.1.6 [選択：MDM サーバ、MDM サーバプラットフォーム] は、SSH トランスポート接続に用いられるデータ完全性アルゴリズムが [選択 : hmac-sha1、hmac-sha1-96、hmac-sha2-256、hmac-sha2-512] であることを確実にしなければならない (shall)。

保証アクティビティ：

評価者はTSS をチェックして、サポートされるデータ完全性アルゴリズムが列挙されていること、またそのリストがこのコンポーネント中のリストと対応していることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、許可されたデータ完全性アルゴリズムのみがTOE とのSSH 接続に用いられる (特に、MAC アルゴリズム「なし (none)」が許可されない) ことを確実にする方法に関する管理者へ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)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 : 評価者は、要件に特定されたデータ完全性アルゴリズムのそれぞれを用いて、SSH 接続を確立しなければならない (shall)。テストの意図を満たすには、アルゴリズムのネゴシエーション成功を (通信路上で) 確認すれば十分である。*

FCS_SSH_EXT.1.7 [選択：MDM サーバ、MDM サーバプラットフォーム] は、SSH 鍵交換手法が diffie-hellman-group14-sha1 及び [*選択：ecdh-sha2-nistp256、ecdh-sha2-nistp384、ecdh-sha2-nistp521、その他の鍵交換アルゴリズムなし*] を用いることを確実にしなければならない (shall)。

保証アクティビティ：

評価者は、本要件に列挙された鍵交換手法を用いるようにセキュリティ管理者が TOE を構成できるような構成情報が操作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)。また評価者は操作ガイダンスをチェックして、許可された鍵交換アルゴリズムのみが SSH 接続に用いられることを確実にする方法に関する管理者へ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)。グループ 14 が TOE に「ハードコーディング」されている場合、評価者は TSS をチェックして SSH プロトコルの議論の中でこれが言明されていることを保証しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 : 評価者は、許可されない鍵交換アルゴリズム (例えば、diffie-hellman-group1-sha1) の実行を試行して、この試行が失敗することを確認しなければならない (shall)。次に評価者は要件中の各鍵交換アルゴリズムの実行を試行して、これらの試行が成功することを確認しなければならない (shall)。*

FCS_TLS_EXT.1 拡張：TLS の実装

FCS_TLS_EXT.1.1(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、以下の暗号スイートをサポートする以下の 1 つ以上のプロトコル [選択：TLS 1.0 (RFC 2246)、TLS 1.1 (RFC 4346)、TLS 1.2 (RFC 5246)] を実装しなければならない (shall)：

必須暗号スイート：TLS_RSA_WITH_AES_128_CBC_SHA 及び

オプションの暗号スイート：[選択：なし、TLS_RSA_WITH_AES_256_CBC_SHA、TLS_RSA_WITH_AES_128_CBC_SHA256、TLS_RSA_WITH_AES_256_CBC_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA256、TLS_DHE_RSA_WITH_AES_256_CBC_SHA256、TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256、TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256、TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384、TLS_DHE_RSA_WITH_AES_128_CBC_SHA、TLS_DHE_RSA_WITH_AES_256_CBC_SHA]。

FCS_TLS_EXT.1.2(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、証明書に含まれる識別名 (DN) がピアに期待される DN にマッチしない場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注意：

評価される構成に用いられる暗号スイートは本要件によって制限されるが、その他の暗号スイートが実装されてもよい。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べきである (should)。必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである (should)。実装によってネゴシエーションされるスイートを本要件中のものに制限するために管理手順が取られる必要がある場合、AGD_OPE によって要求されるガイダンス中にその適切な指示が含まれる必要がある。

上に列挙した Suite B アルゴリズム (RFC 6460) は、実装に望ましいアルゴリズムである。

TLS 1.2 は望ましいプロトコルであり、将来は要求されることになるかもしれない。さらに、本 PP の将来のバージョンでは、SSL/TLS プロトコルの特定された古いバージョンを使用したすべての接続試行を拒否するための手段を提供することが TOE に求められることになる。

DN は、証明書の Subject Name フィールドまたは Subject Alternative Name 拡張に存在するかもしれない。期待される DN は、ローカルまたはリモートいずれかのディレクトリサービスを用いて、正当な MD 利用者のリストと比較されなければならない (must)。

保証アクティビティ：

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが特定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述に適合するように TOE を構成するための指示 (例えば、TOE によって通知される暗号スイートのセットが、要件に合うよう制限されなければならない (have to) かもしれない) が含まれていることを保証しなければならない (shall)。

評価者は、証明書中の DN が期待される DN と比較される方法が TSS に記述されていることを検証しなければならない (shall)。DN が自動的にドメイン名や IP アドレスと比較されない場合、評価者はその接続に期待される DN の構成が AGD ガイダンスに含まれていることを保証しなければならない (shall)。

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

- *テスト 1 : 評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、EAP セッションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。*
- *テスト 2 : 以下のテストは、サポートされている証明書署名アルゴリズムのそれぞれについて、繰返し行われる。評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含むサーバ証明書を持ったサーバを用いて接続を確立する試行を行い、接続が確立されることを検証しなければならない (shall)。次に評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含まないこと以外は有効なサーバ証明書をクライアントが拒否し、接続が確立されないことを検証する。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべきである (should)。*
- *テスト 3 : 評価者は、構成された期待される DN またはピアのドメイン名／IP アドレスのいずれかに DN がマッチする証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できることを検証しなければならない (shall)。評価者は、構成された期待される DN またはピアのドメイン名／IP アドレスのいずれにも DN がマッチしない証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できないことを検証しなければならない (shall)。*
- *テスト 4 : 評価者は、サーバによって選択された暗号スイートとマッチしない証明書を TLS 接続中に送信する (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 証明書を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 証明書を送信したりする) ようサーバを設定しなければならない (shall)。評価者は、TOE が サーバの証明書ハンドシェイ*

クメッセージを受信した後に切断することを検証しなければならない (shall) 。

- *テスト 5：評価者は、TOE とサーバとの間に中間者ツールを設定しなければならず (shall) 、またトラフィックに以下の改変を行わなければならない (shall) 。*
    - *ServerHello ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、クライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。*
    - *ServerHello ハンドシェイクメッセージ中のサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージ中に存在しない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない (shall) 。*
    - *(条件付き) DHE または ECDHE 暗号スイートがサポートされる場合、ServerKeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange を受信した後に接続を拒否することを検証する。*
    - *サーバの CertificateRequest ハンドシェイクメッセージ中の CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない (must not)。評価者は、サーバがクライアントの Finished ハンドシェイクメッセージを受信した後に接続を拒否することを検証しなければならない (shall) 。*
    - *サーバの Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。*

識別と認証 (FIA)

FIA_X509_EXT.2(1) 拡張：X509 認証

FIA_X509_EXT.2.4(1) [選択：MDM サーバ、MDM サーバプラットフォーム] は、コード署名証明書が無効とみなされる場合にはそのコードを [選択：インストール、実行] してはならない (shall not)。

適用上の注意：

証明書は、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) にオプションとして用いてもよい。これらのコード署名用途のいずれかが FIA_X509_EXT.2.1 中で選択されている場合、FIA_X509_EXT.2.4 が本体へ取り込まれなければならない (must)。

保証アクティビティ：

本要件の保証アクティビティは、FIA_X509_EXT.1 及び FIA_X509_EXT.2 の保証アクティビティと組み合わせて行われる。

C.3 選択に基づいた MDM エージェントまたは MDM エージェントプラットフォーム要件

暗号サポート (FCS)

FCS_DTLS_EXT.1 拡張：DTLS の実装

FCS_DTLS_EXT.1.1(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、 [選択：DTLS 1.0 (RFC 4347)、DTLS 1.2 (RFC 6347)] の 1 つ以上に従って DTLS プロトコルを実装しなければならない (shall)。

FCS_DTLS_EXT.1.2(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、 [選択：RFC 4347、RFC 6347] に従った変動が許可される場合を除き、DTLS の実装には FCS_TLS_EXT.1 の中の要件を実装しなければならない (shall)。

適用上の注意：

DTLS と TLS との違いは、RFC 4347 及び RFC 6347 に概説されている。それ以外の点では、これらのプロトコルは同一である。特に、TOE に定義される適用可能なセキュリティ特性については、2 つのプロトコルに違いはない。したがって、FCS_TLS_EXT.1 に列挙されたすべての適用上の注意と保証アクティビティは、DTLS の実装に適用される。

保証アクティビティ：

評価者は、FCS_TLS_EXT.1 に列挙された保証アクティビティを行って、このコンポーネントを検証しなければならない (shall)。

FCS_HTTPS_EXT.1 拡張：HTTPS の実装

FCS_HTTPS_EXT.1.1(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、RFC 2818 に準拠する HTTPS プロトコルを実装しなければならない (shall)。

FCS_HTTPS_EXT.1.2(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、FCS_TLS_EXT.1 に特定される TLS を用いて HTTPS を実装しなければならない (shall)。

適用上の注意：

ST 作成者は、特定された 1 つまたは複数の標準に実装がどのように準拠しているかを判断するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへエレメントを追加することによって、または TSS 中の追加的詳細によって、達成することができる。

保証アクティビティ：

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

FCS_IPSEC_EXT.1 拡張：インターネットプロトコルセキュリティ (IPsec) 通信

FCS_IPSEC_EXT.1.1(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、RFC 4301 に特定される IPsec アーキテクチャを実装しなければならない (shall)。

保証アクティビティ：

評価者は操作ガイダンスを検査して、廃棄 (DISCARD)、バイパス (BYPASS)、及び保護 (PROTECT) のルールを特定するエントリを SPD に構築する方法が管理者へ指示されていることを検証しなければならない (shall)。

評価者は、操作ガイダンスを用いて TOE 及びプラットフォームを構成し、以下のテストを行う。

テスト 1：評価者は SPD を、DISCARD、BYPASS、PROTECT のルールが存在するよう設定しなければならない (shall)。各パケットが 3 つのルールのどれか 1 つにマッチするように、パケットヘッダに適切なフィールドを持つ 3 つのネットワークパケットを評価者が送信できるよう、ルールの構築に用いられるセレクタは異なっていなければならない (shall)。評価者は、TOE が期待されたふるまいを示していることを、監査証跡を通して、またパケットキャプチャによって確認する。適切なふるまいとは、適切なパケットが破棄されたり、

変更なしに通過したり、IPsec の実装によって暗号化されたりすることである。

テスト 2：評価者は、BYPASS と PROTECT という別の操作を行う、2 つの同一の SPD エントリを作り上げなければならない (shall)。次にこれらのエントリは 2 とおりの異なる順序で展開されるべきであり (should)、どちらの場合についても評価者は、該当するパケットを生成してパケットキャプチャ及びログによって確認を行うことにより、両方の場合で最初のエントリが適用されることを保証しなければならない (shall)。

テスト 3：評価者は、一方が他方の部分集合 (例えば、特定のアドレスとネットワークセグメント) となるように 2 つのエントリを作り上げるべき (should) ことを違いとして、上記の手順を繰り返さなければならない (shall)。ここでも管理者は両方の順序をテストして、ルールの限定性にかかわらず、最初のエントリが適用されることを保証すべきである (should)。

FCS_IPSEC_EXT.1.2(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、 [選択 : トンネルモード、トランスポートモード] を実装しなければならない (shall)。

保証アクティビティ：

評価者は TSS をチェックして、TOE が (選択されたように) トンネルモードまたはトランスポートモード、あるいはその両方で動作できると言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、TOE を選択された各モードに構成する方法が運用ガイドで管理者へ指示されていることを確認しなければならない (shall)。また評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 (条件付き)：トンネルモードが選択されている場合、評価者は操作ガイダンスを用いて TOE をトンネルモードで動作するように構成し、また VPN GW もトンネルモードで動作するように構成する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いるように TOE 及び VPN GW を構成し、許容される SA がネゴシエーションできることを保証する。評価者は次に、TOE からの接続を開始し、VPN GW ピアへ接続しなければならない (shall)。評価者は、トンネルモードを用いた接続の確立が成功していることを、監査証跡及びキャプチャされたパケットで確認する。*
- *テスト 2 (条件付き)：トランスポートモードが選択されている場合、評価者は操作ガイダンスを用いて TOE をトランスポートモードで動作するように構成し、また VPN GW もトランスポートモードで動作するように構成する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いるように TOE 及び VPN GW を構成し、許容される SA がネゴシエーションできることを保証する。評価者は次に、TOE からの接続を開始し、VPN GW へ接続する。評価者は、トランスポートモードを用いた接続の確立が成功していることを、監査証跡及びキャプチャされたパケットで確認する。*

FCS_IPSEC_EXT.1.3(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、その他のエントリにマッチしなかったものすべてにマッチして廃棄する名目的なエントリを SPD の最後に持たなければならない (shall)。

保証アクティビティ：

評価者は TSS を検査して、SPD に対してパケットが処理される方法と、マッチする「ルール」が存在しない場合には暗黙的または明示的にネットワークパケットを廃棄させる最後のルールが存在することが、TSS に記述されていることを検証しなければならない (shall)。

評価者は、操作ガイダンスに SPD の構築方法に関する指示が提供されていることをチェックし、そのガイダンスを用いて以下のテストのために TOE／プラットフォームを構成する。

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、ネットワークパケットを廃棄 (DISCARD)、バイパス (BYPASS)、及び保護 (PROTECT) する操作が含まれるエントリが存在するように SPD を設定しなければならない (shall)。評価者は、FCS_IPSEC_EXT.1.1 を検証するために作成された SPD を使ってもよい。評価者は BYPASS エントリとマッチするネットワークパケットを構築し、そのパケットを送信しなければならない (shall)。評価者は、ネットワークパケットが変更されずに適切な宛先インタフェースへ通過されることを確認すべきである (should)。評価者は次に、もはや評価者が作成したエントリへはマッチしないようにパケットヘッダのフィールドを変更しなければならない (shall) (それ以前のエントリのどれにもマッチしなかったパケットを廃棄する「TOE／プラットフォームによって作成された」最後のエントリが存在するかもしれない)。評価者はそのパケットを送信し、パケットがどの TOE のインタフェースへの流出も許可されないことを確認する。

FCS_IPSEC_EXT.1.4(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、RFC 4303 に定義される IPsec プロトコル ESP を、RFC 4106 で特定される暗号アルゴリズム AES-GCM-128、AES-GCM-256、[選択：AES-CBC-128、AES-CBC-256 (両者とも RFC 3602 で特定される) と Secure Hash Algorithm (SHA) ベースの HMAC との組み合わせ、その他のアルゴリズムなし] を用いて実装しなければならない (shall)。

保証アクティビティ：

評価者は TSS を検査して、アルゴリズム AES-GCM-128 及び AES-GCM-256 が実装されていることを検証しなければならない (shall)。ST 作成者が AES-CBC-128 または AES-CBC-256 のいずれかを要件に選択している場合には、評価者はそれらもまた TSS に記述されていることを検証する。評価者は操作ガイダンスをチェックして、AES-GCM-128 及び AES-GCM-256 アルゴリズムを使用するように TOE を構成する方法について指示が与えられていること、また AES-CBC-128 または AES-CBC-256 のいずれかが選択されている場合にはこれらについても使用方法がガイダンスに指示されていることを保証しなければならない (shall)。評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1：評価者は操作ガイダンスの指示により TOE を構成し、TOE が AES-GCM-128 及び AES-GCM-256 アルゴリズムのそれぞれを使用するように構成して、ESP を使用した接続の確立を試行しなければならない (shall)。ST 作成者が AES-CBC-128 または AES-CBC-256 のいずれかを選択している場合には、TOE はこれらのアルゴリズムを使用するよう構成され、評価者は選択されたこれらのアルゴリズムについて ESP を使用した接続の確立を試行する。*

FCS_IPSEC_EXT.1.5(2) TSF は、以下のプロトコルを実装しなければならない (shall)。[選択：RFC 2407、2408、2409、RFC 4109、[選択：拡張シーケンス番号についてその他の RFC なし、拡張シーケンス番号について RFC 4304] 及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義される IKEv1；RFC 5996 (セクション 2.23 に特定される NAT トラバーサルのサポートが必須)、4307、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義される IKEv2]。

保証アクティビティ：

評価者は TSS を検査して、IKEv1 または IKEv2、あるいはその両方が実装されていることを検証しなければならない (shall)。評価者は操作ガイダンスをチェックして、 (選択されたように) IKEv1 または IKEv2、あるいはその両方を使用するように TOE を構成する方法が管理者へ指示されていることを保証しなければならず (shall)、またガイダンスを利用して NAT トラバーサルを行うよう TOE を構成し、以下のテストを行う。

- *テスト 1：評価者は、TSS 及び RFC 5996 のセクション 2.23 に記述されているように NAT トラバーサル処理を行うよう TOE を設定しなければならない (shall)。評価者は IPsec 接続を開始し、NAT トラバーサルが成功することを判断しなけれ*

ばならない (shall)。

FCS_IPSEC_EXT.1.6(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、[選択 : IKEv1、IKEv2] プロトコルにおける暗号化されたペイロードに暗号アルゴリズムとして RFC 6379 に特定される AES-CBC-128、AES-CBC-256 及び [選択 : RFC 5282 に特定される AES-GCM-128、AES-GCM-256、その他のアルゴリズムなし] が用いられることを確実にしなければならない (shall)。

保証アクティビティ：

評価者は、IKEv1 または IKEv2、あるいはその両方のペイロードの暗号化に用いられるアルゴリズムが TSS に特定されていること、及びアルゴリズム AES-CBC-128、AES-CBC-256 が指定されていること、さらに要件の選択においてその他が選択されている場合には、それらが TSS の論拠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、必須のアルゴリズム（要件において選択された追加アルゴリズムがあればそれについても）を使用するよう TOE を構成できる方法が操作ガイダンスに記述されていることを保証しなければならない (shall)。次にガイダンスを用いて TOE を構成し、以下のテストを行う。

- *テスト 1：評価者は、IKEv1 または IKEv2、あるいはその両方のペイロードの暗号化に AES-CBC-128 を使用するよう TOE を構成し、AES-CBC-128 を用いて暗号化されたペイロードのみを受け入れるように構成されたピアデバイスとの接続を確立しなければならない (shall)。評価者は、監査証跡を参照してこのアルゴリズムがネゴシエーションにおいて使用されたものであることを確認すること。*

FCS_IPSEC_EXT.1.7(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、IKEv1 フェーズ 1 交換ではメインモードのみが用いられることを確実にしなければならない (shall)

適用上の注意：

FCS_IPSEC_EXT.1.7 は、IKEv1 が選択されている場合にのみ適用される

保証アクティビティ：

評価者は TSS を検査して、TOE でサポートされている IPsec プロトコルの記述において、IKEv1 フェーズ 1 交換にアグレッシブモードが使用されずメインモードのみが使用されることが言明されていることを保証しなければならない (shall)。これは設定可能なオプションであってもよい。動作前に TOE のモードを構成する必要がある場合には、評価者は操作ガイダンスをチェックしてこの構成の指示がそのガイダンスに含まれていることを保証しなければならない (shall)。評価者は、以下のテストを行わなければならない (shall)。

- *テスト 1 (条件付き)：評価者は操作ガイダンスの指示により TOE を構成して、アグレッシブモードで IKEv1 フェーズ 1 接続を使用して接続の確立を試行しなければならない (shall)。この試行は失敗するはずである (should)。評価者は次に、メインモードの交換がサポートされていることを示すべきである (should)。このテストは、IKEv1 が上記 FCS_IPSEC_EXT.1.5 プロトコル選択において選択されていない場合には適用されない。*

FCS_IPSEC_EXT.1.8(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、 [選択 : IKEv2 SA ライフタイムを正当な管理者がパケット数／バイト数または経過時間に基づいて構成できるとともにフェーズ 1 SA については 24 時間かつフェーズ 2 SA については 8 時間にその値が制限できる、IKEv1 SA ライフタイムを正当な管理がパケット数／バイト数または経過時間に基づいて構成できるとともにフェーズ 1 SA については 24 時間かつフェーズ 2 SA については 8 時間にその値が制限できる] ことを確実にしなければならない (shall)。

適用上の注意：

ST 作成者は、自分の実装における IKE のバージョンに基づいて選択が与えられる。SA ライフタイムをエージェントにプッシュするよう MDM サーバを管理者が構成できる実装は、両者とも受容可能である。

SA ライフタイムに関する限り、TOE は送信されたバイト数、または送信されたパケット数に基づいてライフタイムを制限できる。パケットベース、あるいはボリュームベースの SA ライフタイムはいずれも受容可能である。

ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 中の選択によっては両方を) 選択する。IKEv1 要件は、正当な管理者によって設定可能なライフタイムを提供すること (AGD_OPE によって義務付けられる文書中の適切な指示と共に)、または制限を実装に「ハードコーディング」することの、いずれかの手段によって達成することができる。IKEv2 については、ハードコーディングされた制限は存在しないが、この場合には管理者が値を構成できることが必要とされる。一般的には、SA のライフタイムを含む実装のパラメタを設定するための指示が、AGD_OPE に関して作成された管理ガイダンス中に含まれるべきである (should)。同一の鍵によって保護されるトラフィック量 (その鍵によって保護されるすべての IPsec トラフィックの全体量) の制限を TOE が設定できる限り、パケット数の代わりに MB/KB 数によって要件を詳細化することは妥当である。

保証アクティビティ：

ライフタイムの確立及び実施方法については RFC に記述されており、評価者は本セクションの冒頭に述べたように TSS を検査する。評価者は、SA ライフタイムの値が設定可能であり、その指示が操作ガイダンス中に存在することを検証しなければならない (shall)。評価者は、管理者がフェーズ 1 SA の値を 24 時間、フェーズ 2 SA の値を 8 時間に設定できることを保証しなければならない (shall)。現時点ではパケット数またはバイト数に関して義務付けられた値は存在しないため、評価者はこれが構成できることのみを保証する。

このテストにあたって、評価者は双方が適切に構成されていることを保証する必要がある。RFC には以下のように記載されている。「IKEv1 と IKEv2 との違いは、IKEv1 SA のライフタイムがネゴシエーションされることである。IKEv2 においては、SA の両端が独自のライフタイムポリシーを SA に適用し、必要に応じて SA の鍵アップデートを行う責任がある。両端で異なるライフタイムポリシーが採用されている場合、その結果として、より短いライフタイムの側が常に鍵アップデートを要求することになるだろう。両端で同一のライフタイムポリシーが採用されている場合、同時に双方が鍵アップデートを開始することもあり得る (その結果、冗長な SA が生じることになる)。このようなことが起きる確率を減らすため、鍵アップデート要求のタイミングにはジッタを持たせるべきである (SHOULD)。」

以下のテストはそれぞれ、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のバージョンのそれぞれについて行われなければならない (shall)。

- *テスト 1 : 評価者は、操作ガイダンスに従って許容されるパケット数 (またはバイト数) に関して最大のライフタイムを設定しなければならない (shall)。評価者は SA を確立し、この SA の通過が許可されるパケット数 (またはバイト数) を超えた際に接続がクローズされることを判断しなければならない (shall)。*
- *テスト 2 : 評価者は、フェーズ 1 SA が確立され、再ネゴシエーションまでに 24 時間を超えて維持が試行されるようにテストを構築しなければならない (shall)。評価者は、24 時間以内にこの SA がクローズされるか、再ネゴシエーションされることを確認しなければならない (shall)。そのようなアクションのために TOE が特定の構成を必要とする場合、評価者は TOE の構成機能が操作ガイダンスに文書化されたように動作することを論証するテストを実施しなければならない (shall)。*
- *テスト 3 : 評価者は、ライフタイムが 24 時間ではなく 8 時間であることを除いて、テスト 1 と同様のテストをフェーズ 2 SA に対して行わなければならない (shall)。*

FCS_IPSEC_EXT.1.9(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム]

は、IKE Diffie-Hellman 鍵交換に用いられる秘密の値 x (g^x mod p における「x」) を、FCS_RBG_EXT.1 に特定されるランダムビット生成器を用い、また少なくとも [*割付：NIST SP 800-57, Recommendation for Key Management – Part 1: General の表 2 に掲げるネゴシエーション済み Diffie-Hellman グループに関連付けられた「等価安全性 (bits of security)」の値の少なくとも 2 倍のビット数 (1 つまたは複数)*] のビット長を有するように生成しなければならない (shall)。

FCS_IPSEC_EXT.1.10(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、IKE 交換に用いられるノンスを、特定の IPsec SA のライフタイム内に特定のノンス値が繰り返される確率が *2^[割付：NIST SP 800-57, Recommendation for Key Management – Part 1: General の表 2 に掲げるネゴシエーション済み Diffie-Hellman グループに関連付けられた「等価安全性 (bits of security)」の値 (1 つまたは複数)*] 分の 1 未満になるように生成しなければならない (shall)。

適用上の注意：

実装によって、異なる Diffie-Hellman グループを SA の形成に用いるようネゴシエーションできるかもしれないため、FCS_IPSEC_EXT.1.9 と FCS_IPSEC_EXT.1.10 中の割付は複数の値を含むかもしれない。サポートされる DH グループのそれぞれについて、ST 作成者は 800-57 の表 2 を参照して、その DH グループに関連付けられる「等価安全性」を判断する。次に、それぞれ一意の値を用いて割付への記入が行われる (1.9 については倍の値を、1.10 については直接その値を割付へ記入する)。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートしている実装を想定してみよう。表 2 から、グループ 14 の等価安全性は 112 であり、グループ 20 については 192 である。したがって FCS_IPSEC_EXT.1.9 の割付は「[224, 384]」となり、FCS_IPSEC_EXT.1.10 の割付は「[112,192]」となるであろう (しかしこの場合には、数学的に意味のある値とするために、おそらく要件を詳細化すべきだろう (should))。

FCS_IPSEC_EXT.1.11(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、すべての IKE プロトコルに DH グループ 14 (2048 ビット MODP)、及び [選択：19 (256 ビットランダム ECP)、5 (1536 ビット MODP)、24 (2048 ビット MODP と 256 ビット POS)、20 (384 ビットランダム ECP)、[*割付：TOE の実装するその他の DH グループ*]、その他の DH グループなし] を確実に実装しなければならない (shall)。

適用上の注意：

この選択は、追加的にサポートされる DH グループを特定するために用いられる。これは、IKEv1 及び IKEv2 鍵交換に適用される。本 PP の将来のバージョンでは、DH グループ 19 及び 20 が要求されることになる。何らかの追加的な DH グループが特定される場合、それは FCS_CKM.1 に列挙される要件に (確立される短期鍵の意味で) 適合しなければならない (must) ことに注意すべきである (should)。

保証アクティビティ：

評価者は、TSF のサポートする DH グループのそれぞれについて、「x」(FCS_IPSEC_EXT.1.9 の定義による) 及び各ノンスを生成するプロセスが TSS に記述されていることをチェックし保証しなければならない (shall)。評価者は、本 PP 中の要件を満たす生成された乱数が使われること、及び「x」とノンスの長さが要件中の特定を満たすことが、TSS に示されていることを検証しなければならない (shall)。

評価者は、要件に特定される DH グループがサポートされるものとして TSS に列挙されていることをチェックし保証しなければならない (shall)。1 つよりも多くの DH グループがサポートされる場合、評価者は特定の DH グループをピアとの間で指定／ネゴシエーションする方法が TSS に記述されていることをチェックし保証する。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：サポートされる DH グループのそれぞれについて、評価者はその特定の*

DH グループを用いてすべてのIKE プロトコルの完了が成功することをテストし保証しなければならない (shall)。

FCS_IPSEC_EXT.1.12(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、すべての IKE プロトコルで RFC 4945 及び [選択：事前共有鍵、その他の手法なし] に準拠する X.509v3 証明書を用いる [選択：RSA、ECDSA] を用いたピア認証が行われることを確実にしなければならない (shall)。

適用上の注意：

適合 TOE には少なくとも 1 つの公開鍵ベースのピア認証手法が必要とされる。TOE による実装を反映して、1 つ以上の公開鍵方式が ST 作成者によって選択される。また ST 作成者は、用いられるアルゴリズム (及び、提供されている場合には鍵生成機能) を反映した適切な FCS 要件が、これらの手法をサポートするものとして列挙されていることも保証する。TSS には、これらのアルゴリズムが用いられる方法も詳述されることになる (例えば、2409 では公開鍵を用いる 3 つの認証手法が特定されており、TSS ではこれらのうちサポートされているものが記述されることになる) ことに注意されたい。

FCS_IPSEC_EXT.1.13(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、証明書に含まれる識別名 (DN) が接続の確立を試行しているエンティティに期待される DN にマッチしない場合、SA を確立してはならない (shall not)。

保証アクティビティ：

評価者は、RSA または ECDSA、あるいはその両方がピア認証を行うために使われるものとして TSS に特定されていることを保証しなければならない (shall)。選択の中で事前共有鍵が選択されている場合、事前共有鍵が確立された IPsec 接続の認証に用いられる方法が TSS に記述されていることを評価者はチェックし保証しなければならない (shall)。評価者は、事前共有鍵が生成された TOE に対して確立される方法が操作ガイダンスに記述されていることをチェックしなければならない (shall)。また TSS と操作ガイダンス中の記述には、事前共有鍵を生成できる TOE と、単純に事前共有鍵を利用するだけの TOE との両方について、事前共有鍵の確立が実現される方法が示されていなければならない (shall)。評価者は、暗号アルゴリズムとして RSA または ECDSA、あるいはその両方を使用するように TOE を設定する方法が操作ガイダンスに記述されていることを保証しなければならない (shall)。

以下のテストのための環境を構築し TOE を構成するため、評価者は信頼できる CA へ接続するように TOE を構成する方法も操作ガイダンスに記述されていることを保証し、またその CA の有効な証明書が TOE にロードされ「信頼できる (trusted)」とマークされることを保証すること。

評価者は、FIA_X509_EXT.2.1 のテストと組み合わせて証明書の検証を検証するテストを行わなければならない (shall)。

- *テスト 1 [条件付き]：評価者は、操作ガイダンスに示されるように事前共有鍵を生成して、それを用いて TOE とそのピアとの間の IPsec 接続を確立させなければならない (shall)。TOE が事前共有鍵の生成をサポートしている場合、鍵を生成する TOE のインスタンスだけではなく、単に鍵を受け取り利用するだけの TOE のインスタンスについても、鍵の確立が行われることを評価者は保証しなければならない (shall)。*

FCS_IPSEC_EXT.1.14(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、デフォルトで [選択：IKEv1 フェーズ 1、IKEv2 IKE_SA] 接続を保護するためにネゴシエーションされる対称アルゴリズムの強度 (鍵のビット数の意味で) が [選択：IKEv1 フェーズ 2、IIKEv2 CHILD_SA] 接続を保護するためにネゴシエーションされる対称アルゴリズムの強度 (鍵のビット数の意味で) 以上であることを確実にしなければならない (shall)。

適用上の注意：

ST 作成者は、TOE による実装に基づいてIKE に関する選択のいずれか、または両方を選ぶ。もちろん、選ばれた IKE バージョンはこのエレメントだけでなく、このコンポーネント中の他のエレメントの他の選択とも一貫しているべきである (should)。TOE がこの機能を設定可能とすることは受容可能であるが、評価される構成中のデフォルト構成 (「箱から出した状態」または AGD 文書中の設定ガイダンスによる) では、この機能が有効になっていなければならない (must)。

保証アクティビティ：

評価者は、IKE 及び ESP 交換に許可されるアルゴリズムの潜在的な強度 (対称鍵のビット数の意味で) が TSS に記述されていることをチェックしなければならない (shall)。また TSS には、IKEv1 フェーズ 2 または IKEv2 CHILD_SA スイート、あるいはその両方のネゴシエーション時に行われる、ネゴシエーションされたアルゴリズムの強度 (対称アルゴリズムにおける鍵のビット数の意味で) がネゴシエーションを保護する IKE SA の強度以下であることを保証するために行われるチェックについて記述されていなければならない (shall)。

評価者は、単純にガイダンスに従って TOE を構成し、以下のテストを行う。

- *テスト 1：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、要件中に特定されたサポートされるアルゴリズムとハッシュ関数のそれぞれを用いて IPsec 接続のネゴシエーションを成功させなければならない (shall)。*
- *テスト 2：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、IKE SA に用いられるものよりも強度の大きい暗号化アルゴリズム (すなわち、IKE SA に用いられるものよりも大きい鍵サイズの対称アルゴリズム) を選択する ESP について SA の確立を試行しなければならない (shall)。そのような試行は失敗するはずである (should)。*
- *テスト 3：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、要件中に特定されたサポートされるアルゴリズムとハッシュ関数以外のものを用いてIKE SA の確立を試行しなければならない (shall)。そのような試行は失敗するはずである (should)。*
- *テスト 4：このテストは、TOE のサポートする IKE の各バージョンについて行われなければならない (shall)。評価者は、FCS_IPSEC_EXT.1.4 に特定されない暗号化アルゴリズムを選択する ESP (適切なパラメタが IKE SA の確立に用いられることを前提として) について SA の確立を試行しなければならない (shall)。そのような試行は失敗するはずである (should)。*

FCS_TLS_EXT.1 拡張：TLS の実装

FCS_TLS_EXT.1.1(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、以下の暗号スイートをサポートする以下の 1 つ以上のプロトコル [選択：TLS 1.0 (RFC 2246)、TLS 1.1 (RFC 4346)、TLS 1.2 (RFC 5246)] を実装しなければならない (shall)：

必須暗号スイート：TLS_RSA_WITH_AES_128_CBC_SHA 及び

オプションの暗号スイート：[選択：なし、TLS_RSA_WITH_AES_256_CBC_SHA、TLS_RSA_WITH_AES_128_CBC_SHA256、TLS_RSA_WITH_AES_256_CBC_SHA256、TLS_DHE_RSA_WITH_AES_128_CBC_SHA256、TLS_DHE_RSA_WITH_AES_256_CBC_SHA256、TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256、TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256、TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384、

TLS_DHE_RSA_WITH_AES_128_CBC_SHA、
TLS_DHE_RSA_WITH_AES_256_CBC_SHA]。

FCS_TLS_EXT.1.2(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、証明書に含まれる識別名 (DN) がピアに期待される DN にマッチしない場合、高信頼チャネルを確立してはならない (shall not)。

適用上の注意：

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

上に列挙した Suite B アルゴリズム (RFC 6460) は、実装に望ましいアルゴリズムである。TLS 1.2 は望ましいプロトコルであり、将来は要求されることになるかもしれない。さらに、本 PP の将来のバージョンでは、SSL/TLS プロトコルの特定された古いバージョンを使用したすべての接続試行を拒否するための手段を提供することが TOE に求められることになる。

DN は、証明書の Subject Name フィールドまたは Subject Alternative Name 拡張に存在するかもしれない。期待される DN は、登録中にピアによって用いられるドメイン名または IP アドレスである。

保証アクティビティ

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、サポートされる暗号スイートが特定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、特定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TLS が TSS 中の記述に適合するように TOE を構成するための指示 (例えば、TOE によって通知される暗号スイートのセットが、要件に合うよう制限されなければならない (have to) かもしれない) が含まれていることを保証しなければならない (shall)。

評価者は、証明書中の DN が期待される DN と比較される方法が TSS に記述されていることを検証しなければならない (shall)。

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

- *テスト 1：評価者は、要件に特定された暗号スイートのそれぞれを用いて、TLS 接続を確立しなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、EAP セッションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーション成功を確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。*

- *テスト 2：以下のテストは、サポートされている証明書署名アルゴリズムのそれぞれについて、繰返し行われる。評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含むサーバ証明書を持ったサーバを用いて接続を確立する試行を行い、接続が確立されることを検証しなければならない (shall)。次に評価者は、extendedKeyUsage フィールド中にサーバ認証目的を含まないこと以外は有効なサーバ証明書をクライアントが拒否し、接続が確立されないことを検証する。理想的には、2 つの証明書は extendedKeyUsage フィールドを除いて同一であるべ*

きである (should)。

- *テスト 3 : 評価者は、期待される DN に DN がマッチする証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できることを検証しなければならない (shall)。評価者は、期待される DN に DN がマッチしない証明書による接続を試行しなければならない (shall)。評価者は、TSF が接続を成功できないことを検証しなければならない (shall)。*
- *テスト 4 : 評価者は、サーバによって選択された暗号スイートとマッチしない証明書を TLS 接続中に送信する (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用しているのに ECDSA 証明書を送信したり、ECDSA 暗号スイートのいずれかを使用しているのに RSA 証明書を送信したりする) ようサーバを設定しなければならない (shall)。評価者は、TOE が サーバの証明書ハンドシェイクメッセージを受信した後に切断することを検証しなければならない (shall) 。*
- *テスト 5 : 評価者は、TOE とサーバとの間に中間者ツールを設定しなければならず (shall) 、またトラフィックに以下の改変を行わなければならない (shall) 。*
    - *ServerHello ハンドシェイクメッセージ中のサーバのノンス中の少なくとも 1 バイトを改変して、クライアントの Finished ハンドシェイクメッセージをサーバが拒否することを検証する。*
    - *ServerHello ハンドシェイクメッセージ中のサーバの選択された暗号スイートを、ClientHello ハンドシェイクメッセージ中に存在しない暗号スイートに改変する。評価者は、クライアントが ServerHello を受信した後に接続を拒否することを検証しなければならない (shall) 。*
    - *(条件付き) DHE または ECDHE 暗号スイートがサポートされる場合、ServerKeyExchange ハンドシェイクメッセージ中の署名ブロックを改変して、クライアントが ServerKeyExchange を受信した後に接続を拒否することを検証する。*
    - *サーバの CertificateRequest ハンドシェイクメッセージ中の CA フィールド中の 1 バイトを改変する。改変された CA フィールドは、クライアントの証明書の署名に用いられた CA であってはならない (must not)。評価者は、サーバがクライアントの Finished ハンドシェイクメッセージを受信した後に接続を拒否することを検証しなければならない (shall) 。*
    - *サーバの Finished ハンドシェイクメッセージの 1 バイトを改変して、受信後にクライアントが fatal alert を送信しアプリケーションデータを全く送信しないことを検証する。*

識別と認証 (FIA)

FIA_X509_EXT.2(2) 拡張 : X509 認証

FIA_X509_EXT.2.4(2) [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、コード署名証明書が無効とみなされる場合にはそのコードを [選択 : インストール、実行] してはならない (shall not)。

適用上の注意 :

証明書は、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) にオプションとして用いてもよい。コード署名用途が FIA_X509_EXT.2.1 中で選択されている場合、FIA_X509_EXT.2.4 が本体へ取り込まれなければならない (must)。

保証アクティビティ :

本要件の保証アクティビティは、FIA_X509_EXT.1 及び FIA_X509_EXT.2 の保証アクティビティと組み合わせて行われる。

FIA_X509_EXT.2.6(2) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、ポリシー署名証明書が無効とみなされる場合にはそのポリシーをインストールしてはならない (shall not)。

適用上の注意：

証明書は、オプションとしてポリシー署名 (FMT_POL_EXT.1) に用いることができる。ポリシー署名用途が FIA_X509_EXT.2.1 中で選択されている場合、FIA_X509_EXT.2.6 が本体へ取り込まれなければならない (must)。

保証アクティビティ：

本要件の保証アクティビティは、FIA_X509_EXT.1 及び FIA_X509_EXT.2 の保証アクティビティと組み合わせて行われる。

C.4 監査対象事象

ST 作成者によって選択された具体的な要件、附属書 B：オプションの要件、附属書 C：選択に基づいた要件、及び附属書 D：オブジェクティブな要件に応じて、ST 作成者は ST へ選択された要件向けの適切な監査対象事象を取り込むべきである (should)。

表 7 TOE セキュリティ機能要件及び監査対象事象サーバ

要件	監査対象事象	追加監査記録の内容
FAU_ALT_EXT.1	警報の種類。	警報を送信した MDM エージェントの識別情報。
FAU_ALT_EXT.2	警報の種類。	警報を送信した MDM エージェントの識別情報。
FAU_GEN.1(1)	なし。	
FAU_SAR.1	なし。	
FAU_SEL.1	監査収集機能が動作している間に生じたすべての監査構成への変更。	追加的情報なし。
FAU_STG_EXT.1	なし。	
FAU_STG_EXT.2	なし。	
FCS_CKM_EXT.2(1)	なし。	
FCS_CKM_EXT.4	鍵ゼロ化プロセスの失敗。	クリアされようとしていたオブジェクトまたはエンティティの識別情報。
FCS_CKM.1	鍵生成アクティビティの失敗。	追加的情報なし。
FCS_COP.1(1)	暗号署名の失敗。	操作の暗号モード、署名／検証

要件	監査対象事象	追加監査記録の内容
		されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(2)	非データ完全性暗号ハッシュの失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_COP.1(3)	暗号化または復号の失敗。	操作の暗号モード、暗号化／復号されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(4)	ハッシュ機能の失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_DTLS_EXT.1	なし。	
FCS_HTTPS_EXT.1	なし。	
FCS_IPSEC_EXT.1	TOE によって処理されたネットワークパケットを廃棄(DISCARD)、バイパス(BYPASS)、保護 (PROTECT) する判断。 IPsec SA の確立失敗。 IPsec SA の確立／終了。	送信元サブジェクトの想定される識別情報。 送信先サブジェクトの識別情報。 トランスポート層プロトコル(該当する場合)。 発信元サブジェクトのサービス識別子 (該当する場合)。 判断に適用された SPD 中のエンティティ。 失敗の理由。 成功と失敗の両方について、接続の TOE とは反対側のエンドポイント (IP アドレス)。
FCS_IV_EXT.1	なし。	
FCS_RBG_EXT.1(1)	ランダム化プロセスの失敗。	追加的情報なし。
FCS_STG_EXT.1	なし。	
FCS_TLS_EXT.1	TLS セッションの確立失敗。 TLS セッションの確立／終了。	失敗の理由。 接続の TOE とは反対側のエンドポイント (IP アドレス)。
FIA_ENR_EXT.1.1	MD 利用者認証の失敗。	提示されたクレデンシャル。
FIA_ENR_EXT.1.2	登録の失敗。	失敗の理由。
FIA_UAU.1	なし。	

要件	監査対象事象	追加監査記録の内容
FIA_X509_EXT.1	X.509 証明書の検証の失敗。	検証失敗の理由。
FIA_X509_EXT.2	証明書要求メッセージの生成。	証明書要求メッセージの内容。
FMT_MOF.1(1)	機能を実行するコマンドの発行。 ポリシー設定の変更。	送信されたコマンド及び MDM エージェント受信者の識別情報。 変更されたポリシー及び値または全てのポリシー。
FMT_MOF.1(2)	利用者による登録	利用者の識別情報。
FMT_POL_EXT.1	なし。	
FMT_SMF.1(1)	なし。	
FMT_SMF.1(3)	機能の成功または失敗。	追加的情報なし。
FMT_SMR.1	なし。	
FPT_ITT.1	高信頼チャネルの初期化。 高信頼チャネルの終了。 高信頼チャネル機能の失敗。	失敗した高信頼チャネル確立試行のイニシエータ及びターゲットの識別情報。
FPT_TST_EXT.1	TSF セルフテストのこのセットの実行。 検出された完全性違反。	完全性違反については、その完全性違反を引き起こした TSF コードファイル。
FPT_TUD_EXT.1	アップデートの開始。 アップデートの成功または失敗。	アップデートのバージョン。
FTP_TRP.1	高信頼チャネルの初期化。 高信頼チャネルの終了。 高信頼パス機能の失敗。	要求された利用者識別情報の識別。
FTP_TRP.2	高信頼チャネルの初期化。 高信頼チャネルの終了。 高信頼パス機能の失敗。	要求された利用者識別情報の識別。

表 8 TOE セキュリティ機能要件及び監視対象事象エージェント

要件	監査対象事象	追加監査記録の内容
FAU_ALT_EXT.1	警報の種類。	追加的情報なし。
FAU_GEN.1(2)	なし。	
FAU_SEL.1	監査収集機能が動作している間に生じたすべての監査構成への	追加的情報なし。

要件	監査対象事象	追加監査記録の内容
	変更。	
FCS_CKM_EXT.2(2)	なし。	
FCS_CKM_EXT.4	鍵ゼロ化プロセスの失敗。	クリアされようとしていたオブジェクトまたはエンティティの識別情報。
FCS_CKM.1	鍵生成アクティビティの失敗。	追加的情報なし。
FCS_COP.1(5)	暗号署名の失敗。	操作の暗号モード、署名／検証されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(6)	非データ完全性暗号ハッシュの失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_COP.1(7)	暗号化または復号の失敗。	操作の暗号モード、暗号化／復号されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(8)	ハッシュ機能の失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_DTLS_EXT.1	なし。	
FCS_HTTPS_EXT.1	なし。	
FCS_IPSEC_EXT.1	TOE によって処理されたネットワークパケットを廃棄(DISCARD)、バイパス(BYPASS)、保護 (PROTECT) する判断。 IPsec SA の確立失敗。 IPsec SA の確立／終了。	送信元サブジェクトの想定される識別情報。 送信先サブジェクトの識別情報。 トランスポート層プロトコル(該当する場合)。 発信元サブジェクトのサービス識別子 (該当する場合)。 判断に適用された SPD 中のエンティティ。 失敗の理由。 成功と失敗の両方について、接続の TOE とは反対側のエンドポイント (IP アドレス)。
FCS_RBG_EXT.1(2)	ランダム化プロセスの失敗。	追加的情報なし。
FCS_TLS_EXT.1	TLS セッションの確立失敗。 TLS セッションの確立／終了。	失敗の理由。 接続の TOE とは反対側のエン

要件	監査対象事象	追加監査記録の内容
		ドポイント (IP アドレス)。
FIA_X509_EXT.1	X.509 証明書の検証の失敗。	検証失敗の理由。
FIA_X509_EXT.2	なし。	
FMT_POL_EXT.1	ポリシー検証の失敗。	検証失敗の理由。
FMT_SMF.1(2)	機能の成功または失敗。	追加的情報なし。
FPT_ITT.1	高信頼チャネルの初期化。 高信頼チャネルの終了。 高信頼チャネル機能の失敗。	失敗した高信頼チャネル確立試行のイニシエータ及びターゲットの識別情報。
FPT_TST_EXT.1	TSF セルフテストのこのセットの実行。 検出された完全性違反。	完全性違反については、その完全性違反を引き起こした TSF コードファイル。

附属書D： オブジェクティブな要件

本 PP の概論で示したように、本 PP の本体にはベースライン要件 (TOE またはその基盤となるプラットフォームによって行われなければならない (must) もの) が含まれている。これ以外にも望ましいセキュリティ機能を特定する追加的要件が存在し、これらの要件は本附属書に含まれる。これらの要件は、本 PP の将来のバージョンではオブジェクティブな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。

どの時点においても、これらは ST へ取り込むことができ、その場合でも TOE は依然として本 PP に適合する。

本附属書は、TSF によって行われてもよいオブジェクティブな要件と、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行われてもよいオブジェクティブな要件という、2 つのサブセクションに分かれている。

D.1 オブジェクティブな TSF 要件

セキュリティ監査 (FAU)

FAU_GEN.1(2) 監査データ生成 (MDM エージェント)

FAU_GEN.1.1(2) **詳細化：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)：

- 監査機能の起動と終了、
- MDM ポリシーの変更、ならびに
- MDM サーバによって指示された任意の改変。

以下に個別に定義された監査対象事象

- 表 8
- *[割付：その他の事象]*。

適用上の注意：

本要件は、MDM エージェントが監査記録を生成する機能を持つ場合、ST に追加される。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の概要を示している。ST 作成者は、他の監査対象事象を FAU_GEN.1.1 中の表の中に直接取り込むことができる。監査対象事象は、提示されたリストには限定されない。

MDM ポリシーの変更は最低限、ポリシーが変更されたことを示さなければならない (must)。事象記録には、以前のポリシーと新たなポリシーとの間の違いが含まれる必要はない。MDM サーバによって指令される変更は、FMT_SMF.1.1 に列挙される指令である。

保証アクティビティ：

評価者は TSS をチェックして、監査記録のフォーマットが提供されていることを保証しなければならない (shall)。監査記録のフォーマットの種類のそれぞれが、各フィールドの簡潔な記述とともに、カバーされなければならない (must)。

評価者は、列挙された事象及び管理者アクションに対して TOE に監査記録を生成させることによって、TOE の正しく監査記録を生成する能力をテストしなければならない (shall)。テスト結果を検証する際に、評価者はテスト中に生成された監査記録が管理ガイドに特定されたフォーマットと一致することと、各監査記録のフィールドが適切なエントリを有することを保証しなければならない (shall)。

ここでのテストは、セキュリティメカニズムの直接的なテストと組み合わせて達成できることに注意されたい。

FAU_SEL.1(2) セキュリティ監査事象の選択 (MDM エージェント)

FAU_SEL.1.1(2) **MDM エージェント**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) :

e. 事象の種別、

f. 監査対象セキュリティ事象の成功、

g. 監査対象セキュリティ事象の失敗、及び

h. *[割付：その他の属性]*。

適用上の注意：

本要件の意図は、監査事象を引き起こすために選択可能なすべての基準を特定することである。ST 作成者は、割付を用いて任意の追加基準を列挙するか、または「なし」とする。この選択は、MDM サーバによって構成されるかもしれない。

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)。

セキュリティ管理 (FMT)

FMT_POL_EXT.1 拡張：高信頼ポリシーアップデート

FMT_POL_EXT.1.2 MDM サーバは、デ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 MDM エージェントへ提供しなければならない (shall)。

FMT_POL_EXT.1.3 MDM エージェントは、エンタープライズによってデ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)。

適用上の注意：

本要件の意図は、ポリシーとそのポリシーを指令したエンタープライズとを暗号学的に結び付けることであり、通過中のポリシーを保護することではない (これらはすでに FPT_ITT.1 によって保護されている)。これは、複数のエンタープライズへ接続する利用者にとっては、特に重要である。

保証アクティビティ：

ポリシーは、FCS_COP.1(1) のアルゴリズムを用いてエンタープライズによってデジタル署名されなければならない (must)。評価者は、ポリシーが MDM サーバによってデジタル

署名される方法がTSS に記述されていることを保証しなければならない (shall)。該当する場合には、評価者はポリシーの署名に用いられるエンタープライズ証明書の構成または適用前のポリシーへの署名に関してAGD ガイダンスが管理者へ指示を与えていることを検証しなければならない (shall)。

また評価者は、ポリシー候補が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ジタル署名の検証に関連した処理、そして成功の (署名が検証された) 場合と不成功の (署名が検証できなかった) 場合に行われるアクションが、TSS (または操作ガイダンス) に記述されていることも保証する。また、この処理を行うソフトウェアコンポーネントも TSS 中に特定され、評価者によって検証されなければならない (must)。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、FMT_SMF.1(1) に従ってポリシーアップデートを行わなければならない (shall)。評価者は、MDM サーバ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)。評価者は、そのデジタル署名されたポリシーを MDM エージェントが受け入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、FMT_SMF.1(1) に従ってポリシーアップデートを行わなければならない (shall)。評価者は、署名されていない、及び誤って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、そのデジタル署名されたポリシーを MDM エージェントが受け入れないことを検証しなければならない (shall)。*

D.2 オブジェクティブな MDM サーバまたは MDM サーバプラットフォーム要件

TOE アクセス (FTA)

FTA_TAB.1 デフォルト TOE アクセスバナー

FTA_TAB.1.1 利用者セッション確立前に、 [選択 : MDM サーバ、MDM サーバプラットフォーム] は TOE の利用に関する管理者特有の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 には、いつバナーが表示されるかが記述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 : 評価者は操作ガイダンスに従って、通知及び同意警告メッセージを構成する。次に評価者は、TSF を起動またはロック解除しなければならない (shall)。評価者は、TSS に記述されるインスタンスのそれぞれに通知及び同意警告メッセージが表示されることを検証しなければならない (shall)。*

D.3 オブジェクティブな MDM エージェントまたは MDM エージェントプラットフォーム要件

セキュリティ監査 (FAU)

FAU_GEN.1.2(2) **詳細化 :** [選択 : MDM エージェント、MDM エージェントプラットフォーム] は、**MDM エージェント**の各監査記録において少なくとも以下の情報を記録しなければならない (shall)。

- 事象の日付・時刻、
- 事象の種別、

- サブジェクト識別情報、
- (関連する場合) 事象の結果 (成功または失敗)、
- 表 8 における**追加情報**、
- *[割付：その他の監査関連情報]*。

適用上の注意：

すべての監査には、少なくとも FAU_GEN.1.2(2) に言及される情報が含まれなければならない (must) が、割付可能なより多くの情報を含むことができる。ST 作成者は、監査記録のどの情報がMDM エージェントによって行われたものか、そしてどれがMDM エージェントのプラットフォームによって行われたものかをTSS 中で特定しなければならない (shall)。

保証アクティビティ：

評価者はTSS をチェックして、監査記録のフォーマットが提供されていることを保証しなければならない (shall)。監査記録のフォーマットの種類のそれぞれが、各フィールドの簡潔な記述とともに、カバーされなければならない (must)。

テスト結果を検証する際に、評価者はテスト中に生成された監査記録が管理ガイドに特定されたフォーマットと一致することと、各監査記録のフィールドが適切なエントリを有することを保証しなければならない (shall)。

ここでのテストは、セキュリティメカニズムの直接的なテストと組み合わせて達成できることに注意されたい。

FAU_CRP_EXT.1 拡張：モバイルデバイス構成の適合性報告のサポート

FAU_CRP_EXT.1.1 MDM サーバは、 [選択：登録済みデバイスの構成に関する問い合わせへの応答を提供するインタフェース、登録済みデバイスの構成に関するデータをエクスポートすることを許可するインタフェース] を提供しなければならない (shall)。

適用上の注意：

本要件の意図は、利用者操作ガイダンスに定義されるようにセキュリティ監査を完了するために十分な、登録済みデバイスの構成状態に関する情報を MDM が提供することである。これは、MDM サーバに統合された評価及び報告機能の形態を取ってもよいし、またはそれを外部ソフトウェアが行えるようにMDM サーバがデータを提供してもよい。

保証アクティビティ：

評価者はTSS を検査して、デバイス構成に関する問い合わせを処理し結果を報告するインタフェースか、またはすべての登録済みデバイスの構成に関する情報をエクスポートするインタフェースのいずれかが記述されていることを保証しなければならない (shall)。評価者は操作ガイダンスをチェックして、返却／エクスポートされる項目と、これらのデータを取得するための指示が定義されていることを判断しなければならない (shall)。

暗号サポート (FCS)

FCS_CKM.1.1(4) [選択：MDM エージェント、MDM エージェントプラットフォーム] は、以下の特定された暗号鍵生成アルゴリズムに従って認証に用いられる非対称暗号鍵を生成しなければならない (shall)。 [選択：

- RSA スキームについては、FIPS PUB 186-4, “Digital Signature Standard (DSS)” の附属書 B.3、
- ECDSA スキーム及び「NIST 曲線」 P-256、P-384 及び [選択：P-521、その他の曲線なし] の実装については、FIPS PUB 186-4, “Digital Signature Standard (DSS)” の附属書 B.4、

- AES を用いる RSA スキームについては、ANSI X9.31-1998 の附属書 A.2.4]

及び、特定された暗号鍵サイズは [***112 ビットの対称鍵強度と、同等、またはそれよりも大きく***] なければならない。

適用上の注意：

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

楕円曲線ベースの方式に関しては、鍵サイズは基点の位数の 2 の対数を示す。

ANSI X9.31-1998 の選択肢は、本文書の将来の版では選択から除かれることになる。現状では、モダンな FIPS PUB 186-4 標準への移行を業界が完了するまでにまだ多少時間がかかるため、この選択は FIPS PUB 186-4 のみに限定されてはいない。暗号署名に関する好ましいアプローチとして、本 PP の将来の版では楕円曲線が要求されることになる。

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

保証アクティビティ：

プラットフォームによって満たされる要件

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 に主張される鍵生成機能に MDM エージェントの ST における鍵生成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 エージェントの 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) 鍵生成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 エージェント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)。

MDM エージェントによって満たされる要件

TSF が FIPS 186-4 署名スキームを実装する場合、本要件は FCS_COP.1.1(5)) の下で検証される。

TSF が ANSI X9.31-1998 スキームを実装する場合、評価者は鍵ペアが生成される方法が TSS に記述されていることをチェックして保証しなければならない (shall)。TSF の実装が ANSI X9.31-1998 に適合していることを示すため、評価者は TSS に以下の情報が含まれることを保証しなければならない (shall)。

- *TSS には、TOE が準拠する標準のすべてのセクションが列挙されていなければならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなければならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションを TOE が実装している場合には、それが TSS に記述されなければならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠が TSS に提供されなければならない (shall)。*
- *附属書 B の該当するセクションのそれぞれにおいて、「しなければならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それが記述されなければならない (shall)。*

附属書E： エントロピーの文書化と評定

エントロピー源の文書は、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)。本文書には、設計の記述、エントロピーの正当化、運用条件及びヘルステストという、複数の詳細なセクションが含まれるべきである (should)。本文書は、TSSの一部である必要はない。

設計の記述

文書には、すべてのエントロピー源コンポーネントの相互作用を含めた、エントロピー源の全体的な設計が含まれなければならない (shall)。これにはエントロピー源の動作が記述され、どのように動作するのか、どのようにエントロピーが作り出されるのか、そしてどのように未処理 (生の) データをエントロピー源の内部からテスト目的で取り出すことができるのか、などが含まれることになる。本文書では、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。

また、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説明と、境界外部の敵対者がエントロピー量に影響を与えられないことがどのようにしてセキュリティ境界によって確実とされるのかという説明が含まれなければならない (must)。

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、期待されるエントロピー量の記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられると確信できる理由の説明が含まれることになる。この議論は、エントロピー源がエントロピーを含むビットを作り出すと信頼できる理由の正当化の一部となる。

運用条件

また文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。これには、これらの条件の下でエントロピー源が動作し続けることを確実にするために、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、文書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手法が、含まれなければならない (shall)。

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。

附属書F： 用語集

技術的定義

管理者 (Administrator)	管理者は、エンタープライズによってモバイルデバイスへ適用されるポリシーの設定を含めた、管理アクティビティに責任を負う。この管理者は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行動する。
データ (Data)	サーバまたはモバイルデバイス (MD) によって保存または送信されるプログラム／アプリケーションまたはデータファイル。
開発者モード (Developer Modes)	開発者モードは、ソフトウェアのデバッグの目的で高度なシステムアクセスを提供するため利用者に追加的なサービスが利用可能となる状態である。開発者モードは、ソフトウェアのデバッグの目的で高度なシステムアクセスを提供するため利用者に追加的なサービスが利用可能となる状態である。本プロファイルの目的では、これらのモードには FPT_TUD_EXT.2 に従って検証されていないブートモードも含まれる。
登録状態 (Enrolled state)	モバイルデバイスが MDM システムからのポリシーによって管理されている状態。
エンタープライズアプリケーション (Enterprise Applications)	エンタープライズによって提供され管理されるアプリケーション。
エンタープライズデータ (Enterprise Data)	エンタープライズデータは、エンタープライズサーバに常駐する、またはモバイルデバイス上に一時的に保存される任意のデータであって、それに対するモバイルデバイス利用者のアクセスは、エンタープライズによって定義され管理者によって実装されるセキュリティポリシーに従って許可される。
鍵暗号化鍵 (Key Encryption Key) (KEK)	別の鍵、例えば DEK や鍵を含むストレージなどを暗号化するために用いられる鍵。
ロック状態 (Locked State)	電源は入っているが、大部分の機能が利用できない。機能へのアクセスには、利用者認証が要求される (そう構成されている場合)。
MD	モバイルデバイス (Mobile Device)
MDM エージェント (MDM Agent)	MDM エージェントは、アプリケーションとしてモバイルデバイス上にインストールされるか、またはモバイルデバイスの OS の一部である。 MDM エージェントは、管理者によってコントロールされる MDM サーバへのセキュアな接続を確立する。

モバイルデバイス利用者 (Mobile Device User) (利用者)	これは、モバイルデバイスの物理的なコントロールと操作を利用し、その責任を負う人物である。
オペレーティングシステム (Operating System) (OS)	最も高い特権レベルで実行されるソフトウェアであって、ハードウェア資源を直接コントロールできるもの。モダンなモバイルデバイスは、少なくとも 2 つの主要なオペレーティングシステムを持つ。ひとつは携帯電話ベースバンドプロセッサ上で動作するもの、もうひとつはアプリケーションプロセッサ上で動作するものである。アプリケーションプロセッサのプラットフォームは、大部分の利用者との対話をつかさどり、アプリの実行環境を提供する。携帯電話ベースバンドプロセッサのプラットフォームは、携帯電話ネットワークとの通信をつかさどり、またその他の周辺機器をコントロールすることもある。OS という用語は、文脈が指定されない場合には、アプリケーションプロセッサのプラットフォームを指すものと想定されることがある。
電源切断状態 (Powered-Off State)	デバイスがシャットダウンされている。
保護データ (Protected Data)	保護データは、TSF データ以外の MD 上の全データであり、すべての利用者またはエンタープライズデータを含む。保護データは、MD の電源が切断されている間、暗号化される。保護データには、ソフトウェアベースのセキュアな鍵ストレージ中のすべての鍵が含まれる。このデータの一部または全部も、機密性のあるデータとみなされることがある。
ルート暗号化鍵 (Root Encryption Key) (REK)	他の鍵の暗号化に用いられる、デバイスと結び付けられた鍵。
機密性のあるデータ (Sensitive data)	機密性のあるデータは、MD の TSS によって特定されなければならない (shall)。機密性のあるデータにはすべての利用者またはエンタープライズデータが含まれることがあり、また電子メール、メッセージ、文書、カレンダー項目、及び連絡先など特定のアプリケーションデータであるかもしれない。機密性のあるデータは、MD によってロック状態にある間、オプションとして保護される。機密性のあるデータには、少なくともソフトウェアベースの鍵ストレージ中の鍵の一部または全部が含まれなければならない (must)。
トラストアンカーデータベース (Trust Anchor Database)	信頼されたルート認証局証明書のリスト。
TSF データ (TSF Data)	TSF の運用のためのデータであって、要件の実施が依存するもの。
未登録状態 (Unenrolled state)	モバイルデバイスが MDM システムによって管理さ

	れていない状態。
ロック解除状態 (Unlocked State)	電源が入っていて、デバイスの機能が利用できる。利用者認証が行われていることを暗黙に意味する(そう構成されている場合)。

コモンクライテリア定義

保証 (Assurance)	TOE が SFR を満たしているという確信の根拠 [CC1]。
CC	コモンクライテリア (Common Criteria)
CM	構成管理 (Configuration Management)
PP	プロテクションプロファイル (Protection Profile)
SAR	セキュリティ保証要件 (Security Assurance Requirement)
SFR	セキュリティ機能要件 (Security Functional Requirement)
セキュリティターゲット (Security Target) (ST)	具体的な特定された TOE に関する、実装に依存したセキュリティの必要性の言明。
評価対象 (Target of Evaluation) (TOE)	評価にゆだねられるソフトウェア、ファームウェア及びハードウェアのセットで、ガイダンスが伴うことがある。
TOE セキュリティ機能 (TOE Security Functionality) (TSF)	TOE のすべてのハードウェアとソフトウェア、そしてファームウェアの結合した機能であって、SFR の正しい実施のために信頼されなければならない (must) もの。
TOE 要約仕様 (TOE Summary Specification) (TSS)	評価者に、TOE における SFR の実装の記述を提供する文書。

附属書G： 初期化ベクトルの要件

表 9 NIST 承認暗号モードの参照情報と IV 要件

暗号モード	参照情報	IV 要件
Electronic Codebook (ECB)	SP 800-38A	IV なし
Counter (CTR)	SP 800-38A	「初期カウンタ (Initial Counter)」は、非循環でなければならない (shall)。いかなるカウンタ値も、同一の秘密鍵が用いられる複数のメッセージにわたって循環してはならない (shall not)。
Cipher Block Chaining (CBC)	SP 800-38A	IV は、予測不可能でなければならない (shall)。循環する IV は、2 つのメッセージの間で最初の 1 つ以上のブロックが共有されているかどうかという情報を漏らしてしまうため、そのような状況において IV は非循環であるべきである (should)。
Output Feedback (OFB)	SP 800-38A	IV は非循環でなければならず (shall)、また別の IV 上で暗号を適用することによって生成されたものであってはならない (shall not)。
Cipher Feedback (CFB)	SP 800-38A	循環する IV は、最初の平文ブロックに関する情報や、メッセージ間で共有される共通プリフィックスに関する情報を漏らしてしまうため、IV は非循環であるべきである (should)。
XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing (XTS)	SP 800-38E	IV なし。Tweak 値は非負の整数であって、連続的に割り当てられ、そして任意の非負の整数からスタートするものでなければならない (shall)。
Cipher-based Message Authentication Code (CMAC)	SP 800-38B	IV なし
鍵ラップ及びパディング付き鍵ラップ	SP 800-38F	IV なし
Counter with CBC-Message Authentication Code (CCM)	SP 800-38C	IV なし。ノンスは非循環でなければならない (shall)。
Galois Counter Mode (GCM)	SP 800-38D	IV は非循環でなければならない (shall)。GCM の呼び出し回数は、実装が 96 ビットの IV (デフォルトの長さ) のみを利用する場合を除き、所与の秘密鍵について 2^32 を越えてはならない (shall not)。