汎用 OS のプロテクションプロファイル／
モバイルデバイス基盤のプロテクションプロファイル
拡張パッケージ(EP)
無線ローカルエリアネットワーク (WLAN) クライアント

2016 年 2 月 8 日

バージョン 1.0

平成 29 年 9 月 26 日　翻訳 第 1.0 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

目次

表一覧

図一覧

改定履歴

バージョン	日付	説明
1.0	2011 年 12 月	初版発行
2.0	2016 年 2 月	OS PP と MDF PP の両方への拡張を含めるための改訂

1 概説

本拡張パッケージ (EP) は、無線ネットワーク上のデータ保護のための商用製品 (COTS) 無線ローカルエリアネットワーク (WLAN) クライアントに対するセキュリティ要件について記述する。

本概説では、適合評価対象(TOE) の機能について記述し、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 (OS PP) またはモバイルデバイス基盤のプロテクションプロファイル (MDF PP)と併せて本 EP が利用されるべき方法について説明する。

1.1 適合主張

本 EP は、追加の SFR、及び無線 LAN クライアント特有の関連保証アクティビティを用いて、OS PP または MDF PP を補完するために役立つものである。保証アクティビティは、TOE が SFR に適合することを決定するために評価者が実行するアクションである。

本 EP 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 改訂第 4 版に適合する。CC パート 2 拡張、CC パート 3 適合である。

1.2 本拡張パッケージの利用法

本 EP は、PP 適合を評価されたオペレーティングシステム上に WLAN クライアントがインストールされるときに、OS PP を拡張する。本 EP は、PP 適合を評価された自己完結型モバイルデバイス上に WLAN クライアントがインストールされるときに、MDF PP を拡張する。

OS PP または MDF PP のいずれかの EP として、本 EP と選ばれたベース PP の内容がそれぞれの製品特有のセキュリティターゲットとの関係で適切に統合される、と想定される。本 EP が OS PP または MDF PP と共に用いられる場合には、適合 TOE は、後にここで説明される脅威環境に対応して本 EP で定義された追加の機能と共に、それらの PP で要求される機能を実装する義務がある。ST は、その適合主張において、選ばれた PP と本 EP の適用可能なバージョンを識別しなければならない(must)。

1.3 適合評価対象

本書は、WLAN クライアントのセキュリティ機能要件を規定する。本 EP によって定義される TOE は、WLAN クライアントであり、クライアントマシン上で実行するコンポーネント(「リモートアクセスクライアント」と呼ばれる)である。TOE は、クライアントデバイスとすべてのデータが通過する WLAN アクセスシステムの間でセキュアな無線トンネルを確立する。

適合する WLAN クライアントは、IEEE 802.1X ポートベースのネットワークアクセス制御をサポートする。ポートベースのアクセス制御のアーキテクチャフレームワークは、3 つの明確な役割を定義する：サプリカント(TOE)、オーセンティケータ(WLAN アクセスシステム)；及び認証サーバ(AS)。WLAN アクセスシステムは、ネットワークアクセスを提供する前に、TOE を認証する AS を信頼し、TOE の認証成功を要求する。WLAN アクセスシステムは、TOE と AS の間のパス

スルーデバイスとしての役割を果たす。WLAN アクセスシステムは、WLAN クライアントが AS によって認証成功した後にのみ、WLAN クライアントにプライベートネットワークへのアクセスを許可する。TOE と AS は、X.509 v3 証明書と、拡張認証プロトコル – トランスポート層セキュリティ(EAP-TLS)メッセージを用いて、相互のマシン認証を行わなければならない(must)。TOE または AS のいずれかが認証に失敗した場合、WLAN アクセスシステムは WLAN クライアントとの通信を中止する。プライベートネットワークへのセキュアな通信トンネルは、認証が成功した場合にのみ確立されることが可能である。

1.4 TOE の用途と主要なセキュリティ機能

WLAN クライアントは、プライベートネットワークとの無線通信を(WLAN アクセスシステムを介して) 確立するためにリモート利用者がクライアントマシンを利用することを可能にする。プライベートネットワークとリモートアクセス WLAN クライアントの間を通過する IP パケットは暗号化される。WLAN クライアントは、それ自身とプライベートネットワークの間でデータを保護する。通信データが無線コネクションを通過する場合でも、通信データの機密性、完全性及び保護を提供する。

本 EP のセキュリティ機能要件の重点は、次の WLAN クライアントの基本的な観点に置く：

- WLAN クライアントの認証；
- 認証サーバの認証；
- 通信データの暗号学的保護；及び
- サービスの実装。

WLAN クライアントは、EAP-TLS 認証と共に IEEE 802.1X を用いて、クライアントデバイスとネットワーク基盤の間で 802.11 トンネルを確立する。EAP-TLS 交換の一部としてプライベートネットワークの AS との相互認証を実行する。EAP-TLS 交換は、相互認証のために証明書を利用する。WLAN クライアントは、AS から送信されたマシン証明書を検査して、その有効性をチェックし、信用される認証局 (CA) によって署名されていることを保証する。AS は、同時に WLAN クライアント証明書を認証する。EAP-TLS 交換が正常に完了するとき、ネットワークは、WLAN クライアントがプライベートネットワークへのセキュアな通信トンネルの確立を終了することを許可する。WLAN クライアントは、IEEE 802.11 で規定されるとおり、4 ウェイハンドシェイクを用いて WLAN アクセスシステムへの暗号化され、認証されたチャネルをセットアップする。一度チャネルが確立されると、WLAN クライアントと WLAN アクセスシステムの間のすべての通信は、IEEE 802.11 で規定されるとおり、AES の CCMP モードで暗号化され、またオプションで AES は GCMP モードとなる。

本 EP によって定義されるとおり、WLAN クライアント(図 1)は、リモートアクセスのクライアントマシン上で実行されるコンポーネントである。クライアントは、WLAN クライアント「マシン」のごくわずかな部分として描かれていることに留意されたい。このように、TOE は、その実行ドメインと適切な用途のために、TOE の運用環境(ホストプラットフォーム、ネットワークスタッ

ク、及びオペレーティングシステム)に大きく依存しなければならない。TOE は、管理機能に関連するセキュリティ機能の多くに対処するため、IT 環境に依存する。

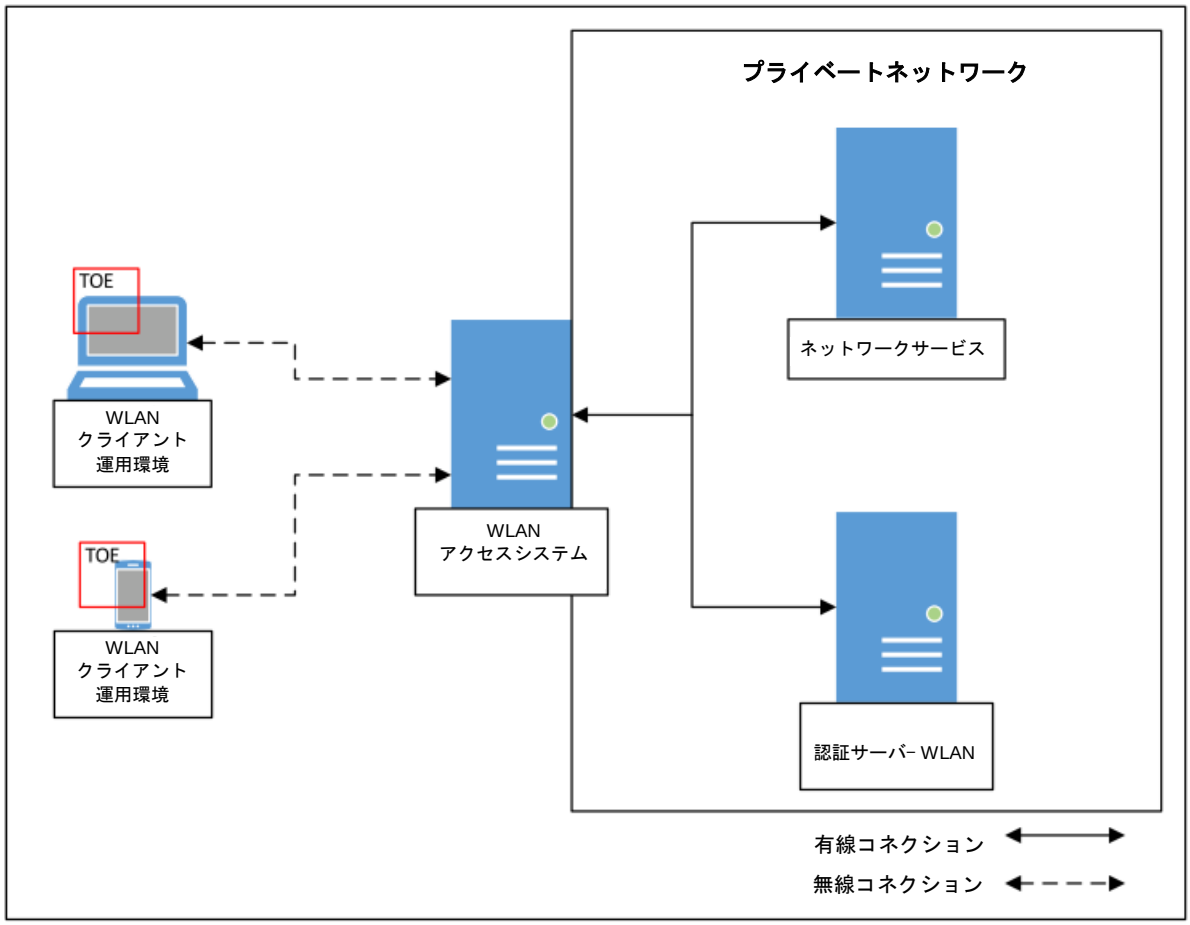

図 1：WLAN クライアント

TOE のセキュリティ機能には、管理、プロトコル適合、暗号学的保護、及び監査生成が含まれる。WLAN クライアントは、以下のクライアントマシンの保護メカニズムと共に、その適切な処理のために IT 環境に依存する：監査レビュー、監査格納、識別と認証、セキュリティ管理、及びセション管理。

2 セキュリティ課題定義

本 EP は、あるエンティティがプライベートネットワークへの無線アクセスを望むときの状況に対処するために書かれている。プライベートネットワークへのアクセスを許可するため、そのエンティティ (マシン) は、セキュア通信チャネルが確立できる前に、認証されなければならない (must)。TOE は、認証されることを要求するエンティティであり、保護されたネットワークによって提供されるサービスへのアクセスを提供され、IEEE 802.1X フレームワークでのサプリカントである。

2.1 脅威

本拡張パッケージは、ベース PP で識別された脅威、前提条件、及び組織のセキュリティ方針を繰り返さないが、それらすべてが所与の適合性に適用され、ゆえに、本 EP はそれらに依存する。ベースPPの脅威、前提条件及び組織のセキュリティ方針と共に、本EPで定義されるそれらは、評価対象としての WLAN クライアントによって対処されるものとして記述される。

本 EP は、ベース PP で記述される脅威、特にネットワーク攻撃とネットワーク盗聴に対して、無線ユースケースに適合した脅威に対処する。無線通信の利用はこのような脅威を増大させる；敵対者は、保護された施設の壁を破壊することなく、またはクライアントデバイスへのアクセスを得ることなく、無線攻撃を開始することができる。信号妨害とサービス妨害攻撃は一般的であり、防ぐのは難しい。このような脅威は本 EP の要件によってカバーされないので、ネットワークの可用性についての前提条件は、これらの脅威に対処するために適当である。しかし、その他のメカニズムが無線通信を保護するために利用できる。セキュリティ方針の不適切なネゴシエーション、または無線通信の確立に弱いプロトコルを実施することは、利用者データとTSFデータの暴露または改変をもたらす可能性があり、懸念事項である。無線トラフィクのキャプチャと保存 (「スニフィング」) から敵対者を防ぐことは不可能であるが、プロトコル相互運用性と強い暗号を要求するセキュリティ方針の相互合意は、無線 LAN 保護の確立に不可欠である。

2.1.1 TSF の障害

TOE のセキュリティメカニズムは一般に、プリミティブなセットのメカニズム (例、メモリ管理、プロセス実行の特権モード) からより複雑なセットのメカニズムへと構築される。プリミティブなメカニズムの障害は、TSF の危殆化を招くような、より複雑なメカニズムでの危始化を招く可能性がある。

(T.TSF_FAILURE)

2.1.2 許可されないアクセス

利用者が TOE データ及び TOE 実行可能コードへの許可されないアクセスを獲得するかもしれない。悪意のある利用者、プロセス、または外部 IT エンティティが、データや TOE 資源への許可

されないアクセスを獲得するため、許可されたエンティティとしてなりすましするかもしれない。悪意のある利用者、プロセスまたは外部 IT エンティティは、識別及び認証データを入手するため、自らを TOE と偽るかもしれない。

(T.UNAUTHORIZED ACCESS)

2.1.3 検出されないアクション

悪意のあるリモート利用者または外部 IT エンティティは、TOE のセキュリティに悪影響を及ぼすようなアクションを取るかもしれない。これらのアクションは、検出されないままになるかもしれず、ゆえにそれらの影響は効果的には、軽減できない。

(T.UNDETECTED_ACTIONS)

2.2 前提条件

WLAN クライアントの前提条件は、附属書 A.1.1 にある。

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

セクション 2 で記述されたセキュリティ課題は、暗号機能の組み合わせによって対処される。適合 TOE は、TOE への脅威に対処するようなセキュリティ機能を提供し、法律または政令によって課される方針を実施する。以下のサブセクションでは、すでに説明された脅威／方針を満たすために要求されるセキュリティ対策方針の記述を提供する。セキュリティ対策方針の記述は、ベース PP で記述されたもの対しての追加である。

注釈：以下の各サブセクションでは、特定のセキュリティ対策方針が識別され (O で強調) 、それらは、対策方針を満たすためのメカニズムを提供するような、対応するセキュリティ機能要件 (SFR) に合致する。

3.1.1 許可された通信

TOE は、許可されたアクセスポイントであると偽るようなその他のエンティティではなく、許可されたアクセスポイントと通信していることを保証する手段を提供し、アクセスポイントに対する TOE の本人性の保証を提供する。

(O.AUTH_COMM -> FCS_TLSC_EXT.1/WLAN, FIA_PAE_EXT.1, FIA_X509_EXT.2, FTP_ITC_EXT.1)

3.1.2 暗号機能

TOE は、機密性を維持し、TOE 及びそのホスト環境の外部で送信されるデータの改変の検出を可能にするため、暗号機能 (即ち、暗号化／復号とデジタル署名の操作) を提供または利用しなければならない。

(O.CRYPTOGRAPHIC_FUNCTIONS -> FCS_CKM.1.1/WLAN, FCS_CKM.2.1/WLAN)

3.1.3 システム監視

TOE は、監査データを生成する機能を提供する。

(O.SYSTEM_MONITORING -> FAU_GEN.1)

3.1.4 TOE 管理

TOE は、管理者が TOE を設定できるようにすることを許容するためのメカニズムを提供する。

(O.TOE_ADMINISTRATION -> FMT_SMF_EXT.1)

3.1.5　TSF 自己テスト

TOE は、TOE が正常に動作していることを保証するため、セキュリティ機能の何らかのサブセットをテストする機能を提供する。

(O.TSF_SELF_TEST -> FPT_TST_EXT.1)

3.1.6　無線アクセスポイントコネクション

TOE は、コネクションする無線アクセスポイントを制限する機能を提供する。

(O.WIRELESS_ACCESS_POINT_CONNECTION -> FTA_WSE_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ような対策方針は、セクション A.2.2 で定義される。

4 セキュリティ要件と根拠

本セクションに含まれるセキュリティ機能要件 (SFR) は、追加の拡張機能コンポーネントと共に、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、改訂第 4 版パート 2 から導出されている。

4.1 表記法

CC では、割付、選択、選択内での割付、及び詳細化というセキュリティ機能要件に関する操作を定義している。本文書では、CC で定義されている操作を識別するために以下の書体表記法を用いる。

- 割付：イタリック体で示される；
- EP 作成者による詳細化：**太字体**と~~取消線~~で示される、必要に応じて；
- 選択：下線付きで示される；
- 選択内の割付：イタリック体及び下線付きで示される；
- 繰り返し：括弧内に繰り返し番号を追加して示される、例：(1), (2), (3)）；及び
- 拡張 SFR は、TOE の SFR についての要件名称の後にラベル「EXT」を付すことで識別される。

4.2 EP セキュリティ機能要件

以下のセクションでは、本 EP に適合主張する TOE によって満たされなければならない(must) SFR について記述される。これらの SFR は、ベース PP が OS PP であるかまたは MDF PP であるかに関わらず主張されなければならない(must)。

表 1：TOE セキュリティ機能要件

機能クラス	機能コンポーネント
セキュリティ監査(FAU)	FAU_GEN.1/WLAN 監査データ生成(無線 LAN)
暗号サポート(FCS)	FCS_CKM.1/WLAN 暗号鍵生成(WPA2 コネクション用の対称鍵)
	FCS_CKM.2/WLAN 暗号鍵配付(GTK)
	FCS_TLSC_EXT.1/WLAN 拡張認証プロトコル-トランスポート層セキュリティ(TLS)
識別と認証(FIA)	FIA_PAE_EXT.1 ポートアクセスエンティティ認証
	FIA_X509_EXT.2/WLAN X.509 証明書の認証(EAP-TLS)
セキュリティ管理(FMT)	MT_SMF_EXT.1/WLAN 管理機能の特定(無線 LAN)
TSF の保護(FPT)	FPT_TST_EXT.1/WLAN TSF 暗号機能のテスト (無線 LAN)
TOE アクセス (FTA)	FTA_ WSE_EXT.1 無線ネットワークアクセス
高信頼パス／チャネル (FTP)	FTP_ITC_EXT.1/WLAN 高信頼チャネル通信(無線 LAN)

4.2.1　クラス：セキュリティ監査(FAU)

FAU_GEN セキュリティ監査データ生成

FAU_GEN.1/WLAN 監査データ生成(無線 LAN)

OS PP と MDF PP の両方にある FAU_GEN.1 の SFR を拡張するための追加の監査対象事象(表 2 に列挙) がある。次の事象は、適合するセキュリティターゲットにおいて OS PP または MDF PP の事象と組み合わせられるべきである(should)。

適用上の注釈：1) 本 EP は複数の PP を拡張するので、本拡張の意図は、両方の PP からの監査対象事象と統合しないことに留意することが重要である。たとえば、MDF PP がベース PP として利用される場合、本 EP の表 **2** に列挙されたものとともに、MDF PP の監査対象事象のみが利用されるべきである(should)。2) ベース PP で監査がオプションの場合、表 **2** の追加の監査対象事象もオプションとなる。3) ベース PP で監査が必須であるがそのベース PP にオプションと必須の監査対象事象が含まれる場合、本 EP の表 **2** にある追加の監査対象事象は必須であると見なされなければならない(must) (オプションと注記されない限り)。

表 2：監査対象事象

要件	監査対象事象	追加の監査記録の内容
FAU_GEN.1/WLAN	なし。	
FCS_CKM.1/WLAN	なし。	
FCS_CKM.2/WLAN	なし。	
FCS_CKM_EXT.4	なし。	
FCS_TLSC_EXT.1/WLAN	EAP-TLS セション確立の失敗。 EAP-TLS セションの確立／終了。	失敗の理由。 コネクションの非 TOE 端点。
FIA_PAE_EXT.1	なし。	
FIA_X509_EXT.2/WLAN	なし。	
FMT_SMF_EXT.1/WLAN	なし。	
FPT_TST_EXT.1/WLAN (注：TOE または TOE プラットフォームにより実行可能)	TSF 自己テストのこのセットの実行。 [選択：検出された完全性違反、なし]。	[選択：完全性違反の原因となる TSF バイナリファイル、追加情報なし]。
FTA_WSE_EXT.1	アクセスポイントへのコネクションのすべての試行。	現在コネクション中のアクセスポイントの識別、成功と失敗(失敗の理由を含む)と共に。
FTP_ITC_EXT.1/WLAN	高信頼チャネル確立のすべての試行。 チャネルデータ改変の検出。	チャネルの非 TOE 端点の識別。

保証アクティビティ	
TSS	本 SFR の TSS 保証アクティビティはない。
AGD	評価者は、操作ガイダンスをチェックし、監査対象事象のすべてが列挙されること、及び監査記録のフォーマットが提供されることを保証しなければならない(shall)。それぞれの監査記録フォーマットの種別が、それぞれのフィールドの簡潔な説明と共に、網羅されなければならない。評価者は、本 EP により義務付けられるすべての監査事象種別が記述されていること、及び FAU_GEN 1.2 で要求される情報、及び表 2 で規定される追加の情報がフィールドの記述に含まれていることを確実にするため、チェックしなければならない(shall)。 評価者は、特に、暗号関連の失敗事象の内容との関連で操作ガイダンスが明確であることを保証しなければならない(shall)。表 2 では、暗号の利用モードを詳述する情報と暗号化されるオブジェクトの名称または識別子が要求される。評価者は、その他の IT システムとの通信に関連する暗号学的障害のあったコネクションの非 TOE 端点と共に、暗号操作 (例えば、鍵ネゴシエーション交換中に実行される、通信データの暗号化のときに実行される) について決定するために、管理者が監査ログをレビュー可能にするために、名称または識別子が十分であることを保証しなければならない。 評価者は、本 EP について関連する管理者アクションの決定についても行わなければならない(shall)。TOE には、機能が SFR で規定されないため、本 EP について評価されないような機能が含まれているかもしれない。この機能は、操作ガイダンスに記述されるような管理者の観点を持っているかもしれない。このような管理者アクションは、TOE の評価された構成では実行されないので、評価者は、操作ガイダンスを検査しなければならず(shall)、本 EP で規定される要件、即ち「すべての管理者アクション」のセットを形作る要件を実施するために必要な TOE に実装されたメカニズムの設定(有効化または無効化を含む) に関連する管理者コマンド、サブコマンド、スクリプト、及び設定ファイル、を決定しなければならない(shall)。評価者は、AGD_OPE ガイダンスが要件を満たすことを保証する、ということに対応するアクティビティの一部として、このアクティビティを実行してもよい。
テスト	評価者は、本 EP の機能要件に関連する保証アクティビティに従って、TOE に監査記録を生成させることにより、監査記録を正しく生成するための TOE の能力をテストしなければならない(shall)。テスト結果の検証に際して、評価者は、テスト中に生成された監査記録が管理者ガイドで規定されたフォーマットと合致していること、及び各監査記録のフィールドに適切なエントリがあることを保証しなければならない(shall)。 ここでのテストは、セキュリティメカニズムのテストと直接併せて達成されることが可能である。例えば、提供された管理ガイダンスが正しいことを保証するために実行されるテストでは、AGD_OPE.1 が満たされることを検証し、監査記録が想定される通りに生成されることを検証するために必要となる管理者アクションの起動に対処するべきである(should)。

4.2.2　クラス：暗号サポート(FCS)

暗号要件は、IEEE 802.11 標準に基づき、WPA2 エンタープライズの Wi-Fi 認証要件の利用を要求するようにも作られている。Wi-Fi Alliance の WPA2 エンタープライズ認証プログラムは、ISO の OSI レイヤー1 と 2 でデータ通信の相互運用性のためにデバイスをテストし、セキュアなコネクションのために Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining (Counter with CBC)-Message Authentication Code (MAC)アルゴリズム(AES-CCMP という) の利用を義務付けている。オプションで AES-GCMP(ガロアカウンタモードプロトコル) が利用可能である。

FCS_CKM 暗号鍵管理

FCS_CKM.1/WLAN 暗号鍵生成 (WPA2 コネクション用対称鍵)

FCS_CKM.1.1/WLAN 詳細化：TSF は、以下の***[IEEE 802.11-2012]*** 及び [選択：IEEE 802.11ac-2014、その他の標準なし]に合致する、特定された暗号鍵生成アルゴリズム ***[PRF-384]*** 及び [選択: PRF-704、その他なし] と特定された暗号鍵長 ***[128 ビット]*** と [選択： 256 ビット、その他の鍵長なし] に従って、**FCS_RBG_EXT.1 で特定される乱数ビット生成器を用いて、対称**暗号鍵を生成しなければならない(shall) 。

適用上の注釈： *IEEE 802.11-2012(セクション 11.6.1.2)によって要求され、WPA2 認証で検証される暗号鍵導出アルゴリズムは、HMAC-SHA-1 関数を用いて 384 ビットを出力する、PRF-384 である。GCMP の利用は、IEEE 802.11ac-2014 (セクション 11.4.5) で定義され、HMAC-SHA-256 (128 ビット対称鍵用)または HMAC-SHA384 (256 ビット対称鍵用) に基づく KDF を要求する。この KDF は 704 ビットを出力する。*

本要件は、アクセスポイントと一回認証された後のクライアントとの間の通信用として生成／導出されるような鍵のみに適用される。それは、本 EP で規定される RBG によって生成された乱数値や、本 EP で規定される SHA-1 を用いる HMAC 関数や、その他の情報と共に利用して行われるような、PMK からの PTK の導出を指す。これは、主に 802.11-2012 のセクション 11.6.1.2 で規定される。

保証アクティビティ	
TSS	評価者は、本 EP により定義され実装されたプリミティブが、無線クライアントへのセキュアなコネクション性を確立し維持する際に、TOE によって使用される方法について、TSS に記述されていることを検証しなければならない(shall)。TSS は、開発者の実装が暗号標準に適合することを保証する開発者の方法についても提供しなければならない(shall)；これには、開発組織によって行われるテストだけでなく、実施されるあらゆる第三者テストについても含まれる。
AGD	本 SFR に対する AGD 保証アクティビティはない。

テスト	評価者は、以下のテストを実行しなければならない(shall)：：

- テスト 1：評価者は、セション鍵の暗号期間が 1 時間となるようアクセスポイントを設定しなければならない(shall)。評価者は、TOE をアクセスポイントへ正常にコネクションし、設定した暗号期間より長い時間でコネクションを維持しなければならない(shall)。評価者は、設定した暗号期間の後、新しいセション鍵を確立するために再ネゴシエーションが開始されることを決定するために、パケットキャプチャツールを利用しなければならない(shall)。最後に、評価者は、ネゴシエーションが成功し、クライアントがアクセスポイントとの通信を継続することを決定しなければならない(shall)。

- テスト 2：評価者は、TOE と無線 LAN アクセスポイントの間でフレームを収集するためのパケットスニフィングツールを用いて、以下のテストを実行しなければならない(shall)。

  ステップ 1：評価者は、アクセスポイントを未使用のチャネルに設定し、WLAN スニファがそのチャネルのみでスニフィングするよう設定しなければならない(shall) (即ち、選択したチャネル上にスニファを固定)。スニファは、TOE 及び／またはアクセスポイントの MAC アドレスでフィルタするようにも設定されるべきである(should)。

  ステップ 2：評価者は、IEEE 802.11-2012 と 256 ビット(16 進値 0-f を 64 個) の事前共有鍵を用いて WLAN アクセスポイントと通信するに TOE を設定しなければならない(shall)。この事前共有鍵は、テスト用でのみ利用される。

  ステップ 3：評価者は、スニフィングツールを起動し、TOE とアクセスポイントの間のコネクションを開始し、TOE がクライアント(訳注：正しくはアクセスポイント)との認証、アソシエーション、及び 4 ウェイハンドシェイクを正常に完了できるようにしなければならない(shall)。

  ステップ 4：評価者は、TOE を無線ネットワークから切断し、スニファを停止させなければならない(shall) ような 終了時刻として、タイマーを 1 分にセットしなければならない(shall)。

  ステップ 5：評価者は、4 ウェイハンドシェイクのフレーム(Wireshark キャプチャで示される EAPOL-key)を識別し、IEEE 802.11-2012 で規定される、4 ウェイハンドシェイクのフレームと事前共有鍵から PTK を導出しなければならない(shall)。

  ステップ 6：評価者は、4 ウェイハンドシェイクが正常に完了した後、アクセスポイントと TOE の間で送信されたキャプチャされたパケットから、フレーム制御値 0x4208 (先頭 2 バイトは 08 42 である) を持たない、先頭のデータフレームを選択しなければならない(shall)。評価者は、IEEE 802.11-2012 で規定されるようにパケットのデータ部分を復号するために PTK を利用しなければならない(shall)、またその復号されたデータに ASCII 可読テキストが含まれていることを検証しなければならない(shall)。

  ステップ 7：評価者は、フレーム制御値は 0x4208 を持たない、TOE とアクセスポイントの間で次の 2 つのデータフレームについて、ステップ 6 を繰り返さなければならない(shall)。

FCS_CKM.2/WLAN 暗号鍵配付(GTK)

FCS_CKM.2.1/WLAN 詳細化：TSF は、以下の[*AES 鍵ラップについて RFC 3394*、*パケットフォーマット及びタイミングの検討について 802.11-2012*] **及び暗号鍵を暴露しない** に合致する、特定された暗号鍵配付方法 [*EAPOL-key フレームでの AES 鍵ラップ*] に従って、**グループ一時鍵** を復号（訳注：配付）しなければならない(shall)。

***適用上の注釈**：本要件は、接続されるアクセスポイントからのブロードキャスト及びマルチキャストメッセージの復号で用いるために TOE によって受信されるグループ一時鍵(GTK)に適用される。802.11-2012 には、送信のフォーマットと RFC 3394 で規定された AES 鍵ラップ方法によってラップされなければならない(must)ことが規定されている。TOE はそのような鍵をラップ解除できなければならない(must)。*

保証アクティビティ	
TSS	評価者は、本 EP で規定される AES 実装を用いて TOE 上での利用のためにインストールされる前に、GTK がラップを解除される方法について TSS に記述されていることを保証するため、TSS をチェックしなければならない(shall)。
AGD	本 SFR に対する AGD 保証アクティビティはない。
テスト	評価者は、TOE と無線アクセスポイントとの間のフレームを収集するためのパケットスニフィングツールを用いて以下のテストを実行しなければならない(shall) (このテストは、FCS_CKM.1.1/WLAN の保証アクティビティと併せて実行されてもよい)。 ステップ 1：評価者は、アクセスポイントを未使用のチャネルに設定し、WLAN スニファがそのチャネルのみでスニフィングするように設定しなければならない(shall) (即ち、選択されたチャネル上にスニファを固定)。スニファは、TOE 及び／またはアクセスポイントの MAC アドレスでフィルタするようにも設定されるべきである(should)。 ステップ 2：評価者は、操作ガイダンスで記述されるとおりにコネクションをセットアップし、IEEE 802.11-2012 と 256 ビット(16 進の値 0-f を 64 個) の事前共有鍵を用いてアクセスポイントと通信するように TOE を設定しなければならない(shall)。事前共有鍵はテスト用のみで使用される。 ステップ 3：評価者は、スニフィングツールを起動し、TOE とアクセスポイントの間のコネクションを開始し、TOE が TOE(訳注：正しくはアクセスポイント)と認証し、アソシエーションし、4 ウェイハンドシェイクを正常に完了できるようにしなければならない(shall)。 ステップ 4：評価者は、TOE をアクセスポイントから切断し、スニファを停止させなければならない (shall) ような 終了時刻をとして、タイマーを 1 分にセットしなければならない(shall)。 ステップ 5：評価者は、4 ウェイハンドシェイクのフレーム(Wireshark キャプチャで示される EAPOL-key)を識別し、IEEE 802.11-2012 で規定される 4 ウェイハンドシェイクのフレームと事前共有鍵から PTK と GTK を導出しなければならない(shall)。

	ステップ 6：評価者は、4 ウェイハンドシェイクが正常に完了した後、アクセスポイントと TOE の間で送信されキャプチャされたパケットから、フレーム制御値 0x4208 (先頭 2 バイトは 08 42 である) を持つ、先頭のデータフレームを選択しなければならない(shall)。評価者は、IEEE 802.11-2012 で規定されるとおり、選択されたパケットのデータ部分を復号するために GTK を利用しなければならない(shall)。また復号されたデータに ASCII 可読テキストが含まれていることを検証しなければならない(shall)。 ステップ 7：評価者は、フレーム制御値 0x4208 を持つ、次の 2 つのデータフレームについて、ステップ 6 を繰り返さなければならない(shall)。

FCS_TLSC_EXT 拡張認証プロトコル – トランスポート層セキュリティ(EAP-TLS)

FCS_TLSC_EXT.1/WLAN 拡張認証プロトコル-トランスポート層セキュリティ

FCS_TLSC_EXT.1.1/WLAN TSF は、以下の暗号スイートをサポートしている RFC 5216 で規定された EAP-TLS プロトコルをサポートする TLS 1.0 及び [選択：TLS 1.1 (RFC 4346)、TLS 1.2 (RFC 5246)、その他の TLS バージョンなし] を実装しなければならない(shall)：

- RFC 5246 に従った必須の暗号スイート：
  TLS_RSA_WITH_AES_128_CBC_SHA
- オプションの暗号スイート：
  [選択：
  なし
  RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA
  RFC 5246 で定義された TLS_RSA_WITH_AES_128_CBC_SHA256
  RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA256
  RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  RFC 5430 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  RFC 5430 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384]。

適用上の注釈：*ECDHE 暗号スイートのいずれかが ST 作成者によって選択される場合、TSF に FCS_TLSC_EXT.2/WLAN を含める必要がある(附属書 C を参照)。*

FCS_TLSC_EXT.1.2/WLAN TSF は、FCS_RBG_EXT.1 で規定される RBG を用いて、EAP-TLS 交換で利用される乱数値を生成しなければならない(shall)。

FCS_TLSC_EXT.1.3/WLAN TSF は、FIA_X509_EXT.1 で規定される X509 v3 証明書を利用しなければならない(shall)。

FCS_TLSC_EXT.1.4/WLAN TSF は、提示されたサーバ証明書の extendedKeyUsage フィールドに、Server Authentication purpose (OID 1.3.6.1.5.5.7.3.1 の id-kp 1) が含まれることを検証しなければならない(shall)。

FCS_TLSC_EXT.1.5/WLAN TSF は、TOE が受け入れる認証サーバ証明書に署名可能な CA (認証局) の一覧の設定を、許可された管理者に許可しなければならない(shall)。

FCS_TLSC_EXT.1.6/WLAN TSF は、EAP-TLS 交換中に提案され受け入れられてもよいアルゴリズムスイートの一覧の設定を、許可された管理者に許可しなければならない(shall)。

***適用上の注釈**：評価される構成でテストされる暗号スイートは、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るべきである(should)；必須のスイート以外にサポートされる暗号スイートがない場合、「なし」が選択されるべきである(should)。テスト環境のサーバ上で、管理上、評価される構成で利用可能な暗号スイートに制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために要求される。*

TLS 1.2 は、推奨プロトコルである。TLS 1.0 と TLS 1.1 は、TLS 1.2 がサポートされないときのため、現在は許容されている。TLS 1.0 及び TLS 1.1 は、112 ビット以上のセキュリティ強度でコネクションを保証するために必要な拡張を持っていない。これらの要件では、IETF によって標準化される新しい TLS のバージョンについて見直しされる予定である。

FCS_TLSC_EXT.1.4/WLAN は、認証サーバによって提示される証明書について、TOE が所定のチェックを実行することを要求する、クライアントによって提示される証明書について、認証サーバが実行しなければならないような、これに対応したチェックがある；つまり、クライアント証明書の extendedKeyUsage フィールドに、「Client Authentication(クライアント認証)」が含まれていること、及び digital signature bit (Diffie-Hellman 暗号スイートの場合) または key encipherment bit (RSA 暗号スイートの場合) がセットされていること。TOE が利用するために所与される証明書は、企業で利用されるために、これらの要件に適合しなければならない。

ベース PP の候補のそれぞれで定義される FIA_X509_EXT.1 要件は、下位のプラットフォームが実装すると想定されるような要件を定義する。

保証アクティビティ	
TSS	評価者は、サポートされる暗号スイートが規定されることを保証するため、TSS で本プロトコルの実装の記載をチェックしなければならない(shall)。評価者は、規定された暗号スイートに本コンポーネント用に列挙されたものが含まれることを保証するため、TSS をチェックしなければならない(shall)。評価者は、TLS が TSS の記述に適合するように TOE の設定についての指示が操作ガイダンスに含まれていることを保証するため、操作ガイダンスについてもチェックしなければならない(shall)。

AGD	評価者は、TLS が TSS の記述に適合するように TOE を設定するための指示が操作ガイダンスに含まれていることを保証するため、操作ガイダンスについてもチェックしなければならない(shall) (例えば、TOE によって公告される暗号スイートのセットは、その要件を満たすために制限されなければならないかもしれない)。 評価者は、EAP-TLS 交換で TOE が受け入れる認証サーバによって利用される証明書へ署名できる認証局のリストを管理者が設定するための指示、及び TOE によって EAP-TLS 交換中に提案され受け入れられるようなアルゴリズムのスイートを規定する方法についての指示が OPE ガイダンスに含まれることをチェックしなければならない(shall)。
テスト	TLS をテストするためのアプリケーションについて、評価者は作成しなければならない(shall)、または ST 作成者は提供しなければならない(shall)。 評価者は、また、以下のテストを実行しなければならない(shall) : • テスト 1 : 評価者は、本要件によって規定された暗号スイートのそれぞれを用いて TLS コネクションを確立しなければならない(shall)。このコネクションは、上位プロトコルの確立の一部として確立されてもよい、例、EAP セションの一部として。暗号スイートのネゴシエーションの成功を観測することは、このテストの意図を満たすには十分である；利用されている暗号スイートを判定する試行において、暗号化されたトラフィクの特性を検査する必要はない (例えば、暗号アルゴリズムが 128 ビット AES であって 256 ビット AES ではないこと)。 • テスト 2 : 評価者は、extendedKeyUsage フィールドに Server Authentication purpose を含むサーバ証明書を持つサーバを用いてコネクションの確立を試行し、コネクションが確立されることを検証しなければならない(shall)。次に評価者は extendedKeyUsage フィールドに Server Authentication purpose を持たないその他の有効なサーバ証明書をクライアントが拒否することを検証し、コネクションが確立されないことを検証すること。理想的には、2 つの証明書は、extendedKeyUsage フィールド以外は同一であるべきである(should)。 • テスト 3 : 評価者は、サーバが選択した暗号スイートと合致しないような、サーバ証明書を TLS コネクションで送信しなければならない(shall) (例えば、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートを利用すると同時に ECDSA 証明書を送信する、または ECDSA 暗号スイートの 1 つを利用すると同時に RSA 証明書を送信する)。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コネクションを切断することを検証しなければならない(shall)。 • テスト 4 : 評価者は、サーバが TLS_NULL_WITH_NULL_NULL 暗号スイートを選択するように設定し、クライアントがコネクションを拒否することを検証しなければならない(shall)。 • テスト 5 : 評価者は、トラフィクへの以下の改変を実施しなければならない(shall) :

	o Server Hello でサーバが選択した TLS バージョンを非サポートの TLS バージョン (例えば、2 バイト 03 04 で表現される 1.3) に変更し、クライアントがコネクションを拒否することを検証する。 o Server Hello ハンドシェイクメッセージにおけるサーバのノンスを少なくとも 1 バイト改変し、クライアントが Server Key Exchange ハンドシェイクメッセージを拒否すること (DHE または ECDHE 暗号スイートを利用する場合) またはサーバがクライアントの Finished ハンドシェイクメッセージを拒否することを検証する。 o Server Hello ハンドシェイクメッセージでサーバが選択した暗号スイートを Client Hello ハンドシェイクメッセージで提示されない暗号スイートに改変する。評価者は、クライアントが Server Hello を受信した後、接続を拒否することを検証しなければならない。(shall) o Server's Key Exchange ハンドシェイクメッセージの署名ブロックを改変し、Server Key Exchange メッセージを受信した後、クライアントが拒否することを検証する。 o Sever Finished ハンドシェイクメッセージの 1 バイトを改変し、クライアントが受信時に致命的アラートを送信し、あらゆるアプリケーションデータを送信しないことを検証する。 o サーバが ChangeCipherSpec メッセージを発行した後、サーバから、でたらめなメッセージを送信し、クライアントがコネクションを拒否することを検証する。

4.2.3 クラス：識別と認証(FIA)

TOE のベースライン要件は、I&A (訳注：識別と認証) に関してかなり限定される、それは、正式な管理者や一般利用者について定義されていないためである。TOE によって実行されるために要求される I&A の範囲は、無線アクセスシステムを介して保護されるネットワークへコネクションされることになるプロセスに関連している。さらに、通常は I&A プロセスの一部と見なされるようないくつかの要件、特に無線通信で利用される暗号プロトコル (WPA2) が、本 EP の他のセクションで規定されている。これは、保証アクティビティの作成と適用を容易にするとともに、理解しやすさのためにそれらのプロトコルの要件を一つにまとめるためになされた。したがって、本セクションの要件は、TOE がサポートしなければならない I&A 機能の残りの 2 つの側面をカバーする：

- **802.1X-2010 認証**. 802.1X-2010 標準 (及び関連する RFC) は、ネットワークアクセスの目的でのマシンの認証を規定する。この方法は、802.11-2012 標準を用いて無線運用の先駆けとして利用される。802.1X には、802.1X 交換に参加するいくつかの異なる当事者に対する要件が含まれるが、以下の要件は、802.1X での「サプリカント」としての TOE の役割に焦点が当てられている。

- **クレデンシャル**. 本セクションと本 EP の他のセクションで規定されるプロトコルとメカニズムは、802.1X 認証の実行において、EAP-TLS 交換で利用される証明書に依存する。

FIA_PAE_EXT ポートアクセスエンティティ認証

FIA_PAE_EXT.1 ポートアクセスエンティティ認証

FIA_PAE_EXT.1.1 TSF は、「サプリカント」の役割におけるポートアクセスエンティティ(PAE)について、IEEE 標準 802.1X に適合しなければならない(shall)。

***適用上の注釈**：本要件は、802.1X 認証交換でのサプリカントとしての TOE の役割をカバーする。その交換が正常に完了する場合、TOE は、EAP-TLS (またはその他の適切な EAP 交換) の結果として PMK を導出し、802.11 通信を開始するために無線アクセスシステム (オーセンティケータ) との 4 ウェイハンドシェイクを実行する。*

前述したように、交換中に少なくとも 2 つの通信パスが存在する；1 つは無線アクセスシステムとのパスで、1 つは中継として無線アクセスシステムを使用するような認証サーバとのパス。TOE は、802.1X-2010 で規定された、無線アクセスシステムとの EAP over LAN (EAPOL)コネクションを確立する。TOE と認証サーバは、EAP-TLS セション(RFC 5216)を確立する。

802.1X 認証実行のポイントは、ネットワークへのアクセスを得ることである(認証が成功し、すべての 802.11 ネゴシエーションが正常に実行されると仮定して)；802.1X の用語では、これは無線アクセスシステムによって維持される「管理されたポート」へのアクセスを TOE が得ることを意味する。

保証アクティビティ	
TSS	本 SFR の TSS 保証アクティビティはない。
AGD	本 SFR のガイダンスアクティビティはない。
テスト	評価者は、以下のテストを実行しなければならない(shall)：。 • テスト 1：評価者は、TOE がテストネットワークへアクセスしていないことを実証しなければならない(shall)。無線アクセスを介して認証サーバを用いて正常に認証した後、評価者は、TOE がテストネットワークへアクセスすることを実証しなければならない(shall)。 • テスト 2：評価者は、TOE がテストネットワークへアクセスしていないことを実証しなければならない(shall)。評価者は、EAP-TLS ネゴシエーションが失敗するように、無効なクライアント証明書を用いて認証を試行しなければならない(shall)。これにより、TOE がテストネットワークにアクセスすることがまだできないという結果になるべきである(should)。 • テスト 3：評価者は、TOE がテストネットワークへアクセスしていないことを実証しなければならない(shall)。評価者は、EAP-TLS ネゴシエーションが失敗するように、無効な認証サーバの証明書を用いて認証を試行しなければならない(shall)。これにより、TOE がテストネットワークにアクセスすることがまだできないという結果になるべきである(should)。

FIA_X509_EXT X.509 証明書検証

FIA_X509_EXT.2/WLAN X.509 証明書認証(EAP-TLS)

FIA_X509_EXT.2.1/WLAN TSF は、EAP-TLS 交換の認証をサポートするため、RFC 5280 によって定義される X.509 v3 証明書を利用しなければならない(shall)。

適用上の注釈：*RFC 5280 は、TSF によって実装されなければならない (must) 証明書の検証と認証パス検証の要件を定義する。ベース PP 候補のそれぞれで定義される FIA_X509_EXT.1 要件は、この RFC への適合性をサポートするために下位プラットフォームが実装することが期待される要件を定義する。*

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

保証アクティビティ	
TSS	評価者は、TOE がどの証明書を利用するか選択する方法、及び TOE がその証明書を利用できるように運用環境を構成するための管理者ガイダンスにおけるあらゆる必要な指示が TSS に記述されていることを保証するため、TSS をチェックしなければならない(shall)。 評価者は、高信頼チャネルの確立で利用される証明書の有効性チェック中にコネクションが確立できないときの TOE のふるまいについて TSS に記述されていることを確認するため、TSS を検査しなければならない(shall)。評価者は、高信頼チャネル間の区別について記述されていることを検証しなければならない(shall)。管理者がデフォルトのアクションを規定できるという要件の場合、評価者は、この設定アクションがどのように実行されるかについて指示が操作ガイダンスに含まれていることを保証しなければならない(shall)。
AGD	評価者は、TOE がどの証明書を利用するかを選択する方法、及び TOE がその証明書を利用できるように運用環境を設定するために必要なあらゆる指示について、管理者ガイダンスに記述されていることを保証するため、管理者ガイダンスをチェックしなければならない(shall)。
テスト	評価者は、各高信頼チャネルについて、以下のテストを実行しなければならない (shall)： テスト：評価者は、少なくとも何らかの部分で非 TOE IT エンティティとの通信によって証明書有効性チェックが実行されることを要求するような有効な証明書を利用して実証しなければならない(shall)。評価者は、そのときその証明書の有効性を TOE が検証できないように環境を操作し、FIA_X509_EXT.2.2 で選択されたアクションが実行されることを観測しなければならない(shall)。その選択されたアクションが管理者設定可能である場合、評価者は、すべてのサポートされる管理者設定可能なオプションが記述されたやり方でふるまうことを決定するため、操作ガイダンスに従わなければならない (shall)。

4.2.4　クラス：セキュリティ管理(FMT)

本 EP のセクション 1 で示すとおり、TOE は、個々の管理役割を維持することは要求されない。しかし、一般の利用者らが利用できるべきでない(should not) TOE 運用の特定の側面を設定する機能の提供が要求される。TOE がある程度のシステム管理的な管理策を提供する場合、附属書 C からの適切な要件が ST で利用されるべきである(should)。

FMT_SMF_EXT 管理機能の特定

FMT_SMF_EXT.1/WLAN 管理機能の特定(無線 LAN)

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

- *それぞれの無線ネットワークのセキュリティ方針を設定する：*
    - [選択：*TSF が WLAN 認証サーバの証明書を受け入れる CA を規定する、受け入れ可能な WLAN 認証サーバの証明書の FQDN を規定する]*
    - *セキュリティ種別*
    - *認証プロトコル*
    - *認証のために利用されるべきクライアントのクレデンシャル；*
- *(オプション)TSF が接続してもよい無線ネットワーク (SSID) を規定する；*
- *(オプション)証明書失効リストのチェックを有効化する／無効化する；*
- *(オプション)アドホックな無線クライアント間コネクション機能を無効化する；*
- *(オプション)無線ネットワークのブリッジ機能 (例えば、WLAN と携帯電話無線間のコネクションをスマートフォン上でブリッジし、ホットスポットとして機能できるようにする) を無効化する；*
- *(オプション)ローミング機能を無効化する；*
- *(オプション)IEEE 802.1X 事前認証を有効化する／無効化する；*
- *(オプション)PMK キャッシュを有効化する／無効化する及び設定する：*
    - *PMK エントリがキャッシュされる時間の量 (分) をセットする；*
    - *キャッシュ可能な PMK エントリの最大数をセットする。*

適用上の注釈：*インストールについて、WLAN クライアントは、TOE がインストールされるクライアントマシンに対して管理者を認証するために下位プラットフォームに依存している。*

確立されたセション鍵の暗号期間を設定する機能について、暗号期間を設定するための計測単位は 1 時間を超えてはならない(shall)*。例えば：秒、分及び時間の計測単位は許容可能であり、数日またはそれ以上の計測単位は許容されない。*

保証アクティビティ	
TSS	本 SFR の TSS 保証アクティビティはない。
AGD	評価者は、本 EP で義務付けられる管理機能がすべて操作ガイダンスに記述されること、及びその記述に管理機能に対応する管理義務を実行するために要求される情報が含まれることを確認するため、チェックしなければならない(shall)。
テスト	評価者は、TOE を設定し、上記要件で列挙された各オプションのテストによって、管理機能を提供するための TOE の能力をテストしなければならない(shall)。 ここでのテストが、FCS_TLSC_EXT 及び FTA_WSE_EXT のような、その他の要件のテストと併せて達成されてもよいことに留意すること。

4.2.5 クラス：TSF の保護(FPT)

FPT_TST_EXT.1/WLAN TSF 暗号機能テスト

FPT_TST_EXT.1/WLAN TSF 暗号機能テスト (無線 LAN)

FPT_TST_EXT.1.1/WLAN [選択：TOE、TOE プラットフォーム] は、TSF の正常な動作を実証するために、初期立ち上げ中 (電源投入時) 、自己テストのスイートを実行しなければならない(shall)。

FPT_TST_EXT.1.2/WLAN [選択：TOE、TOE プラットフォーム] は、格納された TSF 実行可能コードが実行のため TSF 提供の暗号サービスの利用を通してロードされるとき、TSF 実行可能コードの完全性を検証する機能を提供しなければならない(shall)。

適用上の注釈：*本 SFR は、下位プラットフォームによって実行される自己テスト機能と TSF によって提供されるものとを区別するため、繰り返されたものである。*

TOE は、ベース PP で定義されたプラットフォーム上で動作しているソフトウェアパッケージとして定義されているが、上記で要求される自己テストのアクティビティを実行することができる。しかし、暗号アルゴリズムの実装が下位プラットフォームによって提供される場合、TSF 自己テストは、TSF がその実装を利用しようとする前に、下位プラットフォームがそれ自体の自己テストを正常に完了したことを検証することのチェックであるようなケースであるかもしれない。下位プラットフォームの危殆化は自己テストが正しく機能しない可能性をもたらすため、これらの自己テストによって提供される保証を監査する上で、ホストプラットフォームに大きく依存することを理解するべきある(should)。

保証アクティビティ	
TSS	評価者は、立ち上げ時に TSF によって実行される自己テストについて TSS に詳述されることを保証するため、TSS を検査しなければならない(shall)；本記述は、そのテストで実際に何を行っているかの概要を含むべきである(should) (例、「メモリがテストされる」と言うよりも、「メモリは、それぞれのロケーションにある値を書き込み、その値が書き込まれたものと同一であることを保証するため読み出される」のような記述)。評価者は、それらのテストが TSF の正常な動作を実証するために十分であるという説明を TSS が行っていることを保証しなければならない(shall)。 評価者は、格納された TSF 実行可能コードが実行のためにロードされるとき、TSF 実行可能コードの完全性を検証する方法について TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。評価者は、このテストが、格納された TSF 実行可能コードの完全性が危始化しなかったことを実証するために十分であることを TSS が説明していることを保証しなければならない(shall)。評価者は、成功 (例、ハッシュが検証された) 及び不成功 (例、ハッシュが検証されない) のケースに取られるアクションを TSS (または操作ガイダンス) が記述していることについても保証すること。
AGD	評価者は、成功 (例、ハッシュが検証される) 及び不成功 (例、ハッシュが検証されない) のケースに取られるアクションを TSS (または操作ガイダンス) が記述していることについても保証しなければならない。
テスト	評価者は、以下のテストを実行しなければならない(shall)： • テスト 1：評価者は、既知の良好な TSF 実行可能コードの完全性チェックを実行し、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 実行可能コードを改変し、改変した TSF 実行可能コードの完全性チェックを実施し、そのチェックが失敗することを検証する。

4.2.6 クラス：TOE アクセス (FTA)

FTA_WSE_EXT 無線ネットワークアクセス

FTA_WSE_EXT.1 無線ネットワークアクセス

FTA_WSE_EXT.1.1 TSF は、FMT_SMF_EXT.1.1/WLAN で管理者によって設定されたとおり、受け入れ可能なネットワークとして指定された無線ネットワークのみへのコネクションを試行できなければならない(shall)。

***適用上の注釈**：本要件の意図は、TOE が接続を許可されるアクセスポイントを制限することを管理者に許可することである。割付は、許容可能なアクセスポイントを指定するため管理者によって利用可能な属性 (例、MAC アドレス、SSID、証明書等) を指定するために、 ST 作成者によって利用される。*

保証アクティビティ	
TSS	評価者は、許容可能なネットワーク (アクセスポイント) を指定するために利用可能なすべての属性が具体的に定義されることを決定するため、TSS を検査しなければならない(shall)。
AGD	評価者は、TSS で識別された属性のそれぞれを設定するためのガイダンスが操作ガイダンスに含まれていることを決定するため、操作ガイダンスを検査しなければならない(shall)。
テスト	評価者は、それぞれの属性について以下のテストも実行しなければならない(shall) : • テスト 1 : 評価者は、特定のアクセスポイントとのコネクションを許容するよう TOE を設定する。評価者は、許可されたアクセスポイントと許可されないアクセスポイントが TOE に対して両方とも「可視」であるようなテスト環境についても設定する。評価者は、それらが許可されたアクセスポイントと正常にセションを確立できることを実証しなければならない(shall)。次に、評価者は、許可されないアクセスポイントとのセション確立を試行し、そのアクセス試行が失敗するのを観測する。 • テスト 2 : 評価者は、EAP-TLS 認証 (有効な SSID が設定されるだけでなく、TOE が EAP-TLS 認証を完了するための証明書と共に提供されることも含めて) を用いて特定のアクセスポイントとのコネクションを許可するように TOE を設定する。評価者は、TOE が接続するよう設定された SSID をアクセスポイントがブロードキャストするが、認証サーバは有効なクレデンシャルを持っていないようなテスト環境についても設定する。次に、評価者は、有効な SSID／無効な認証サーバとのセションの確立を試行し、そのアクセス試行が失敗することを観測する。

4.2.7　クラス：高信頼パス/チャネル(FTP)

FTP_ITC_EXT 高信頼チャネル通信

FTP_ITC_EXT.1/WLAN 高信頼チャネル通信(無線 LAN)

FTP_ITC_EXT.1.1/WLAN　TSF は、それ自身と無線アクセスポイント間に、他の通信チャネルとは論理的に区別され、その端点の保証された識別を提供し、暴露からチャネルデータを保護し、及びチャネルデータ改変を検出する、高信頼通信チャネルを提供するために、802.11-2012、802.1X、及び EAP-TLS を利用しなければならない(shall)。

FTP_ITC_EXT.1.2/WLAN　TSF は、無線アクセスポイントコネクションのために、高信頼チャネルを介して通信を開始しなければならない(shall)。

***適用上の注釈**：上記要件の意図は、TOE とアクセスポイント間の通信を保護するために、本要件で識別された暗号プロトコルを利用することである。*

本要件は、最初に確立されたときに保護される通信だけでなく、電源供給停止後の再開にも保護されることを含んでいる。TOE セットアップの一部が、他の通信を保護するためのトンネルを手動で設定することを含むようなケースがあるかもしれない、また電源供給停止後に TOE が (必要な)手動での介入により再び通信の自動確立を試行する場合、重要な情報を入手またはコネクションを危殆化できるかもしれない場所に攻撃者が作った窓があるかもしれない。以下のテストは、

WLAN 通信チャネルのみをカバーすることを意図している(モバイルブロードバンド等の TOE 上で利用可能かもしれない他の通信チャネルを除く)。

保証アクティビティ	
TSS	評価者は、本要件で規定された暗号プロトコルという観点でアクセスポイントへ接続している TOE の詳細について、仕様には反映されないような TOE 特有のオプションや手順と共に、TSS に記述されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、TSS にリストされた全てのプロトコルが ST の要件で規定されて含まれていることについても確認しなければならない(shall)。
AGD	評価者は、アクセスポイントへのコネクション確立の手順が操作ガイダンスに含まれていること、及び意図せずにコネクションが切断されたときの復旧手順が含まれていることを確認しなければならない(shall)。
テスト	評価者は、以下のテストを実行しなければならない(shall) : • テスト 1 : 評価者は、本要件で規定されたプロトコルを利用し、操作ガイダンスに記述されるとおりコネクションをセットアップし、通信が成功することを保証し、TOE がアクセスポイントとの通信を開始できることを保証しなければならない(shall)。 • テスト 2 : 評価者は、許可された IT エンティティとの各通信チャネルについて、チャネルデータが平文で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、許可された IT エンティティとの各通信チャネルについて、チャネルデータの改変が 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)。 • テスト 4 : 評価者は、TOE からアクセスポイントまでの通信を物理的に遮断しなければならない(shall) (例えば、アクセスポイントの範囲外に TOE ホストを移動したり、アクセスポイントの電源をオフにしたりなど)。評価者は、少なくとも自動的にコネクションを再開するか、または新しいアクセスポイントへ接続するような試行において、その後の通信が適切に保護されることを保証しなければならない(shall)。 それ以上の保証アクティビティは、個々のプロトコルと関連する。

4.3 セキュリティ機能要件 - OS PP ベース

本 EP が OS PP を拡張する場合、WLAN クライアントは、ベース PP に適合する評価を受けた全体としてのオペレーティングシステムによって実装されたセキュリティ機能に依存すると想定される。本 EP への適合を主張する TOE が OS PP を主張されたベース PP として利用している場合、上記のセクション 4.2 で義務付けられているものに加えて、ベース PP で定義された SFR に対して ST 作成者が行わなければならない(must) あらゆる改変について、以下のセクションに記述される。

4.3.1　追加の要件の取り込み

定義されたセキュリティ対策方針を TOE が満たすためには、OS PP 主張は以下の追加の SFR と共に本 PP のベース要件のすべてを含まなければならない(must)：

4.3.2　クラス：暗号サポート(FCS)

FCS_CKM_EXT.3 暗号鍵破棄

適用上の注釈：*本 SFR は、OS PP に存在し、本 EP 用に改変される必要はない。しかし、その適用範囲は、本 EP によって記述された TSF により利用される鍵及び鍵材料を含むよう拡張されていることに留意されたい。鍵破棄機能は、少なくとも部分的に WLAN クライアント自体とは違って下位プラットフォームによって実装されると想定されるので、本 SFR は繰り返されなかった。 本要件の目的のため、TOE がゼロ化を実行するためにホストの正しい下位の機能を起動すれば十分である ― これは、TOE が、データのゼロ化を保証するためにカーネルモードのメモリドライバを含めなければならないことを意味するものではない。*

セキュリティ関連情報 (鍵、認証データ、及びパスワード等)は、セキュリティ上重要なデータの暴露または改変を防ぐため、使用されなくなったときにゼロ化されなければならない(must)。

上記のゼロ化は、鍵／暗号クリティカルセキュリティパラメタを他の場所に移動させる際に、平文の鍵/暗号クリティカルセキュリティパラメタを格納する中間的なストレージエリア (即ち、このようなデータのパスに含まれる、たとえばメモリバッファのような記憶域)にそれぞれ適用される。

さらに、IEEE 802.11-2012 では、無線 LAN クライアントの PMK の寿命を定めていない(IEEE の 11.6.1.3 節で説明されている)が、この寿命は制限されるべきであり、PMKSA は、同じ PMK が 24 時間を超えて連続使用されないようにクリアされるべきである。したがって、PMK について「もはや必要とされなくなったとき」とは 24 時間後である。

FCS_COP.1 暗号操作

適用上の注釈：*本 SFR のいくつかの繰り返しは、OS PP に存在しており、本 EP 用に改変される必要はない。しかし、それらの適用範囲は、そのセキュリティ機能を実行するために WLAN クライアントにより要求される暗号操作を含むよう拡張されることに留意されたい。*

FCS_RBG_EXT.1 乱数ビット生成

適用上の注釈：*本 SFR は OS PP に存在しており、本 EP 用に改変される必要はない。しかし、その適用範囲は、そのセキュリティ機能を実行するために WLAN クライアントにより要求される乱数ビット生成機能を含むよう拡張されることに留意されたい。*

4.4 セキュリティ機能要件 - MDF PP ベース

本 EP が MDF PP を拡張しようとする場合、WLAN クライアントは、全体としてモバイルデバイスによって実装され、かつベース PP に適合する評価を受けたセキュリティ機能に依存することが想定される。本 EP への適合を主張する TOE が主張されたベース PP として MDF PP を利用する場合、上記のセクション 4.2 によって義務付けられるものに加えて、ベース PP で定義される SFR に対して ST 作成者が行わなければならない(must) あらゆる改変について以下のセクションで記述される。

4.4.1 クラス：暗号サポート(FCS)

FCS_CKM_EXT.4 拡張：鍵破棄

***適用上の注釈**：本 SFR は、MDF PP に存在し、本 EP 用に改変する必要はない。しかし、その適用範囲は、本 EP によって記述される TSF により利用される鍵及び鍵材料を含むよう拡張されることに留意されたい。本 SFR は繰り返されていない、なぜなら鍵破棄機能は、少なくとも部分的に WLAN クライアント自身とは違って、下位プラットフォームによって実装されると想定されるからである。本要件の目的のため、TOE がゼロ化を実行するためにホストの正しい下位の機能を起動すれば十分である — これは、TOE が、データのゼロ化を保証するためにカーネルモードのメモリドライバを含めなければならないことを意味するものではない。*

セキュリティ関連情報 (鍵、認証データ、及びパスワード等)は、セキュリティ上重要なデータの暴露または改変を防ぐため、使用されなくなったときにゼロ化されなければならない(must)。

上記のゼロ化は、鍵／CSP を他の場所に移動させる際に、平文の鍵／CSP を格納する中間的なストレージエリア (即ち、このようなデータのパスに含まれる、たとえばメモリバッファのような記憶域)にそれぞれ適用される。

さらに、IEEE 802.11-2012 では、無線 LAN クライアントの PMK の寿命を定めていない(IEEE の 11.6.1.3 節で説明されている)が、この寿命は制限されるべきであり、PMKSA は、同じ PMK が 24 時間を超えて連続使用されないようにクリアされるべきである。したがって、PMK について「もはや必要とされなくなったとき」とは 24 時間後である。

FCS_COP.1 暗号操作

***適用上の注釈**：本 SFR のいくつかの繰り返しが MDF PP に存在し、本 EP 用に改変される必要はない。しかし、それらの適用範囲は、そのセキュリティ機能を実行するために WLAN クライアントにより要求される暗号操作を含めるよう拡張されることに留意されたい。*

FCS_RBG_EXT.1 乱数ビット生成

***適用上の注釈**：本 SFR は MDF PP に存在し、本 EP 用に改変される必要はない。しかし、その適用範囲は、そのセキュリティ機能を実行するために WLAN クライアントにより要求される乱数ビット生成機能を含めるよう拡張されることに留意されたい。*

5 セキュリティ保証要件

本 EP は、適合を主張できるベース PP 内で定義される SAR を超えるような SAR については定義していない。本 EP に適合する評価がなされる TOE が、本来 OS PP または MDF PP に適合する評価が同様になされることについて注釈することは重要である。これらの PP の両方は、セキュリティ機能要件 (SFR) 及び SAR に対応した数多くの保証アクティビティを含んでいる。さらに、本 EP には、ベース PP の SAR を同じように詳細化するような数多くの SFR ベースの保証アクティビティが含まれる。評価機関は、選択されたベース PP に適合する TOE を評価し、本 EP から取られた必要な SFR を用いてその評価を補完する。

附属書 A – 根拠

本 EP では、本書の最初のセクションの焦点は、WLAN クライアントによって対処される脅威；それらの脅威を軽減するために利用される方法；及び適合 TOE によって達成される軽減の範囲についての全体的な理解しやすさを増大させるためにナレーション風な表現を利用している。この表現スタイルは、形式化された評価アクティビティにすぐに役立つものではないため、本セクションには、本文書に関連する評価アクティビティ用に利用可能な表形式のものを含んでいる。

A.1 セキュリティ課題定義

A.1.1 前提条件

以下に列挙された具体的な条件が、TOE の運用環境に存在すると想定される。この前提条件はベース PP で定義されたものへの追加であり、TOE セキュリティ要件の策定における実践的現実及び TOE の利用上の基本的な環境条件の両方を含んでいる。

表 3：TOE 前提条件

前提条件	前提条件の説明
A.NO_TOE_BYPASS	情報は、無線クライアントと内部の有線ネットワーク間を TOE を介して通過することなしに流れることはできない。
A.TRUSTED_ADMIN	TOE 管理者は、信頼されるやり方ですべての管理者ガイダンスに従って適用すると信頼されている。

A.1.2 脅威

以下に列挙された脅威は、WLAN クライアントによって対処される。これらの脅威は、ベース PP で定義されたものへの追加であり、WLAN クライアントに適用されるすべてである。

表 4：**脅威**

脅威	脅威の説明
T.TSF_FAILURE	TOE のセキュリティメカニズムは、TSF の危始化をまねくような、障害を起こすかもしれない。
T.UNAUTHORIZED_ACCESS	利用者は、TOE データ及び TOE 実行可能コードへの許可されないアクセスを得るかもしれない。悪意のある利用者、プロセス、または外部 IT エンティティは、データまたは TOE 資源への許可されないアクセスを得るため、許可されたエンティティになりすましをするかもしれない。悪意のある利用者、プロセス、または外部 IT エンティティは、識別と認証データを得るため、自身を TOE として偽るかもしれない。

T.UNDETECTED_ACTIONS	悪意のあるリモート利用者または外部 IT エンティティは、TOE のセキュリティに悪影響を及ぼすようなアクションを取るかもしれない。これらのアクションは、検出されないままになるかもしれず、その結果それらの影響が有効に軽減することができない。

A.1.3 組織のセキュリティ方針

WLAN クライアントに特有の、組織のセキュリティ方針は識別されていない。しかし、ベース PP における組織のセキュリティ方針のすべてが、WLAN クライアントに適用される。

A.1.4 セキュリティ課題定義の対応関係

以下の表は、本 EP で定義された脅威と前提条件を、同様に本 EP で定義されまたは識別されたセキュリティ対策方針への対応付けを提供する。

表 5：**セキュリティ課題定義の対応関係**

脅威または前提条件	セキュリティ対策方針
A.NO_TOE_BYPASS	TOE.NO_TOE_BYPASS
A.TRUSTED_ADMIN	TOE.TRUSTED_ADMIN
T.TSF_FAILURE	O.TSF_SELF_TEST
T.UNAUTHORIZED_ACCESS	O.AUTH_COMM, O.CRYPTOGRAPHIC_FUNCTIONS, O.TOE_ADMINISTRATION、及び O.WIRELESS_ACCESS_POINT_ CONNECTION
T.UNDETECTED_ACTIONS	O.SYSTEM_MONITORING

A.2 セキュリティ対策方針

A.2.1 TOE のセキュリティ対策方針

以下の表には、WLAN クライアント特有のセキュリティ対策方針が含まれている。これらのセキュリティ対策方針は、ベース PP で定義されたものへの追加であり、すべてが WLAN クライアントに適用される。

表 6：TOE のセキュリティ対策方針

対策方針	対策方針の説明
O.AUTH_COMM	TOEは、許可されたアクセスポイントと通信を行っていること、及び許可されたアクセスポイントと偽るその他のエンティティではないことを保証する手段を提供し、アクセスポイントの本人性に対する保証を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS	TOE は、TOE 及びそのホスト環境の外部に送信されるデータの機密性を維持し、そのデータの改変の検出を可能にするため、暗号機能 (即ち、暗号化／復号及びデジタル署名操作) を提供または利用しなければならない。
O.SYSTEM_MONITORING	TOEは、監査データを生成する機能を提供する。
O.TOE_ADMINISTRATION	TOE は、管理者が TOE を設定できることを許可するためのメカニズムを提供する。
O.TSF_SELF_TEST	TOEは、セキュリティ機能が正常に動作することを保証するため、セキュリティ機能の何らかのサブセットをテストするための機能を提供する。
O.WIRELESS_ACCESS_POINT_CONNECTION	TOEは、コネクション先となる無線アクセスポイントを制限する機能を提供する。

A.2.2 運用環境のセキュリティ対策方針

以下の表には、WLAN クライアントの運用環境に特有のセキュリティ対策方針が含まれている。これらのセキュリティ対策方針は、ベース PP で定義された対策方針への追加であり、すべてが WLAN クライアントの運用環境に適用される。

表 7：OE のセキュリティ対策方針

対策方針	対策方針の説明
OE.NO_TOE_BYPASS	別々の場所にある外部と内部のネットワークの間で、TOE を介して通過することなしに、情報が流れることはできない。
OE.TRUSTED_ADMIN	TOE 管理者は、信頼されるやり方で、すべての管理者ガイダンスに従い、また適用すると信頼されている。

A.2.3 セキュリティ対策方針の対応関係

本 EP で識別または定義されたセキュリティ機能要件 (SFR) とセキュリティ対策方針の間の対応関係は、セクション 3 で提供される。

附属書 B - オプション要件

本 EP のドラフトについて、本附属書には、脅威、対策方針、根拠、または (ある場合には) 保証アクティビティ をサポートしない追加のコンポーネントが含まれている。1 回目のレビューと並行して、本サポート情報が策定され、本 EP の次回リリースへ組み込まれるだろう。本セクションに含まれる情報への意見 (含まれる要件が適合 TOE 候補に適用できるかどうか、及び WLAN クライアント製品へ幅広く適用可能な本附属書に含まれていない要件も同様に適用できるかどうか、の両方について)は、歓迎され募集中である。

本 EP の概説で示されるように、TOE が実装するかもしれないような、また本 EP に依然として適合するようないくつかの機能がある。これらの機能は、必須ではなく、IT 環境への依存を引き起す (例えば、TOE 管理者の識別と認証)。しかし、TOE がこのような機能を実装する場合、ST には、以下の情報を採用し、ST に含めることになる。

B.1 クラス：識別と認証(FIA)

TOE が管理機能を提供する場合、リモート管理、ローカル管理、及び管理者セションの保護を含め、その機能を規定するために適用可能な多くの要件がある。本 EP のこのバージョンでは、このようなクライアントの機能を規定するため、無線アクセスシステムプロテクションプロファイルからの管理者要件を利用することは受け入れ可能である。

交換中に利用される証明書を格納し管理する機能を TOE が提供するような場合、以下の SFR が ST に含まれることが可能である。本 SFR は、証明書格納機能が TOE により実際に提供される場合に用いられることを意図しており、TSF が下位プラットフォームにより提供される格納メカニズムに依存するような場合は意図していない。

FIA_X509_EXT 証明書の検証

FIA_X509_EXT.4 証明書の格納と管理

FIA_X509_EXT.4.1 TSF は、証明書を格納して不正な削除や改変から保護しなければならない (shall)。

FIA_X509_EXT.4.2 TSF は、許可された管理者に対し、本 EP で規定されるセキュリティ機能によって利用される X.509v3 証明書を TOE にロードするための機能を提供しなければならない (shall)。

保証アクティビティ	
TSS	評価者は、本 EP の要件を満たすために利用される証明書を含むような、実装されたすべての証明書ストアについて TSS に記述されることを決定するため、TSS を検査しなければならない(shall)。この記述は、証明書がストアへロードされる方法、及びストアが不正なアクセスから保護される方法に関する情報を含まなければならない (shall)。
AGD	本要件の AGD 保証アクティビティはない。
テスト	評価者は、証明書の利用を要求するようなシステムのそれぞれの機能について、以下のテストを実行しなければならない(shall) :

	テスト 1：評価者は、有効な証明書パスのない証明書の利用が機能の不成功をもたらすことを実証しなければならない(shall)。評価者は次に、その機能で利用されるべき証明書を検証するために必要な証明書または複数の証明書をロードし、機能の成功を実証しなければならない(shall)。 評価者は次に、証明書のうちの 1 つを削除し、機能の不成功を示さなければならない(shall)。

B.2 監査要件

ST 作成者によって、本附属書から選択された具体的な要件に依存して、ST 作成者は、選択された要件について ST における対応する表の適切な監査可能事象を含めるべきである(should)。

要件	監査対象事象	監査記録の追加的内容
FIA_X509_EXT.2/WLAN	証明書をロードするための試行。 証明書を失効させるための試行。	なし。

附属書 C - 選択ベースの要件

本 EP の概説で示されるように、ベースライン要件 (TOE またはその下位プラットフォームによって実行されなければならない(must)もの) は、本 EP の本文中に含まれる。本 EP の本文中の選択に基づく追加の要件がある；特定の選択がなされる場合、以下の追加の要件が含まれる必要がある。

C.1 クラス：暗号サポート(FCS)

FCS_TLSC_EXT.2/WLAN TLS クライアントプロトコル

FCS_TLSC_EXT.2.1/WLAN TSF は、以下の NIST 曲線：[選択: secp256r1, secp384r1, secp521r1] 及びその他の曲線はなし、を用いて、Client Hello における Supported Elliptic Curves Extension を提示しなければならない(shall)。

適用上の注釈：*「TLS_ECDHE」で始まる暗号スイートが FCS_TLSC_EXT.1/WLAN で選択される場合、ST 作成者は本 SFR を含めなければならない(shall)。*

本要件は、認証と鍵共有のために許容される楕円曲線を FCS_COP.1(3) (ベース PP で定義)及び FCS_CKM.1/WLAN 及び FCS_CKM.2/WLAN (本 EP で定義)からの NIST 曲線に限定する。

保証アクティビティ	
TSS	評価者は、Supported Elliptic Curves Extension 及び要求されるふるまいがデフォルトで実行されるか、または設定可能であるかについて、TSS に記述されることを検証しなければならない(shall)。
AGD	Supported Elliptic Curves Extension が本要件を満たすために設定されなければならない(must)と TSS で示される場合、評価者は Supported Elliptic Curves Extension の設定についての指示が操作ガイダンスに含まれることを検証しなければならない(shall)。
テスト	評価者は、以下のテストを実行しなければならない(shall)： • テスト 1：評価者は、非サポートの ECDHE 曲線 (例えば、P-192) を用いて TLS コネクションで ECDHE 鍵交換メッセージを実行するようサーバを構成し、サーバの鍵交換ハンドシェイクメッセージの受信後に、TSF がコネクションを切断することを検証しなければならない(shall)。

附属書 D - オブジェクティブ要件

本セクションは、本 EP により規定されていないが将来のバージョンで含まれることが想定される要件のために予約される。将来の製品に対して評価の実施を計画しているベンダは、これらのオブジェクティブ要件を満たすような計画が推奨される。

現在、本 EP のために定義されたオブジェクティブ要件はない。

附属書 E - 参考資料、用語、及び略語

[1] Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009

[2] Draft Consistency Instruction Manual, for Basic Robustness Environments, Release 4.0, CC version 3.1, 2008

[3] Federal Information Processing Standard Publication (FIPS-PUB) 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001 (CHANGE NOTICES (12-03-2002))

[4] Federal Information Processing Standard Publication (FIPS-PUB) 180-3, Secure Hash Standard, October 2008

[5] Federal Information Processing Standard Publication (FIPS-PUB) 186-3, Digital Signature Standard (DSS), June 2009

[6] Federal Information Processing Standard Publication (FIPS-PUB) 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001

[7] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[8] NIST Special Publication 800-57, Recommendation for Key Management, March 2007

[9] NIST Special Publication 800-63, Electronic Authentication Guideline, April 2006

[10] NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) , March 2007

[11] NSA Glossary of Terms Used in Security and Intrusion Detection, Greg Stocksdale, NSA Information Systems Security Organization, April 1998. Need to update to CNSS 4009

[12] RFC 2865 Remote Authentication Dial In User Service (RADIUS), June 2000

[13] RFC 2868 RADIUS Attributes for Tunnel Protocol Support, June 2000

[14] RFC 3575 IANA Considerations for RADIUS, July 2003

[15] RFC 3579 RADIUS (Remote Authentication Dial In User Service Support For Extensible Authentication Protocol (EAP), September 2003

[16] RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003

[17] RFC 5216 The EAP-TLS Authentication Protocol, March 2008

[18] WPA2 Standard

[19] U.S. Government Approved Protection Profile - Protection Profile for Mobile Device Fundamentals Version 2.0, September 17, 2014

[20] U.S. Government Approved Protection Profile - Protection Profile for General Purpose Operating Systems Version 4.0, August 14, 2015

アクセスポイント – 無線クライアントホストの有線ネットワークへのアクセスを可能にするようなネットワークインタフェースを提供する。一度、有線インフラ上の信頼されるノードとして認証されると、AP は無線クライアントと AP の RF インタフェース間の無線ネットワーク上で暗号サービスを提供する。

管理者 – TOE を設定する管理者特権を有する利用者。

認証サーバ – 認証のために、無線クライアントから認証クレデンシャルを受信する有線ネットワーク上の認証サーバ。

認証クレデンシャル – 利用者または管理者が TOE またはネットワークへのアクセスを許可されることを検証するためにシステムが利用する情報。クレデンシャルは、利用者名とパスワードまたはより強い証明書と同じように簡単なものとすることができる。

クリティカルセキュリティパラメタ (CSP) – セキュリティ関連情報、例えば、秘密暗号鍵及びプライベート暗号鍵、及びパスワードや PIN 等の認証データで、その暴露や改変は、暗号モジュールのセキュリティを侵害する可能性があるもの。

エントロピー源 – この暗号機能は、1 つ以上のノイズ源からの出力を累積することによって乱数生成器用のシード値を提供する。本機能には、所与の出力を推測するために必要とされる最小限の作業の尺度、及びノイズ源が正常に動作していることを保証するためのテストが含まれる。

拡張認証プロトコル(EAP) – 無線ネットワークで利用される認証フレームワーク。TOE は EAP-TLS をサポートする。EAP-TLS は PKI を用いて認証サーバ及び無線クライアントの両方を認証する。

FIPS 承認された暗号機能 –以下のいずれかであるような、セキュリティ機能 (例、暗号アルゴリズム、暗号鍵管理技法、または認証技法) ：1) 連邦情報処理規格(FIPS)で規定、または 2) FIPS で採用かつ FIPS の附属書または FIPS により参照される文書のいずれかで規定。

IEEE 802.1X ― 有線のネットワークへ接続するデバイス (無線クライアント) に対する認証メカニズムを定義するような、ポートベースのネットワークアクセス制御のための IEEE 標準。IEEE 802.1X のサポートに必要とされる主要コンポーネントは、サプリカント(無線クライアント(訳注：TOEのこと))、オーセンティケータ(TOE(訳注：正しくは無線アクセスシステム))、及び認証サーバである。

IT 環境 –TOE 機能性とセキュリティ方針をサポートする、TOE 境界外にある、ハードウェア及びソフトウェア。

運用環境 – TOE が運用される環境。

SAR(セキュリティ保証要件) – 開発者と評価機関がセキュリティ機能要件への適合性を実証するために、開発及び評価の方法を記述する。SAR は、開発者と評価者のための具体的なテストについて記述するべきである(should)。

SFR(セキュリティ機能要件) – TOE によって満たさなければならない(must) セキュリティ機能について記述する。SFR は、具体的な技術に合わせて作成される。

ST(セキュリティターゲット) – TOE のセキュリティ特性について記述し、特定する。

TOE(評価対象) - 本 EP の要件に適合する評価を受けるハードウェア、ソフトウェア、及びガイダンスを含む製品または製品のセットを指す。

TOE セキュリティ機能(**TSF**) – TSP の適正な実施のために信頼されなければならない(must) TOE のすべてのハードウェア、ソフトウェア、及びファームウェアからなるセット。

TOE セキュリティ方針(TSP) – TOE 内での資産が管理、保護及び配付される方法について統制する規則のセット。

TOE 要約仕様(**TSS**) – TOE がすべての SFR を満たす方法についての記述。

許可されない利用者 – TOE を利用することを管理者によって許可されていない利用者。

AES	Advanced Encryption Standard
AF	Authorization factor(許可要素)
AS	Authentication Server(認証サーバ)
CAVS	Cryptographic Algorithm Validation System(暗号アルゴリズム検証システム)
CC	Common Criteria(コモンクライテリア)
CCTL	Common Criteria Testing Laboratory(コモンクライテリア評価機関)
CM	Configuration Management(構成管理)
COTS	Commercial Off-The-Shelf(商用製品)
CMVP	Cryptographic Module Validation Program(暗号モジュール試験及び認証制度)
DRBG	Random Bit Generator(乱数ビット生成器)
DoD	Department of Defense(国防総省)
EAL	Evaluation Assurance Level(評価保証レベル)
ES	Encryption Subsystem(暗号サブシステム)
FIPS	Federal Information Processing Standards(連邦情報処理規格)
GCMP	Galois/Counter Mode Protocol (ガロア／カウンタ モード プロトコル)
ISSE	Information System Security Engineers(情報システムセキュリティエンジニア)
IT	Information Technology(情報技術)
KDF	Key Derivation Function(鍵導出関数)
OSP	Organizational Security Policy(組織のセキュリティ方針)
PMK	Pairwise Master Key(マスター鍵ペア)

PP	Protection Profile(プロテクションプロファイル)
PTK	Pairwise Temporal Key(一時的な鍵ペア)
PUB	Publication(パブリケーション)
RBG	Random Bit Generator(乱数ビット生成器)
SAR	Security Assurance Requirement(セキュリティ保証要件)
SF	Security Function(セキュリティ機能)
SFR	Security Functional Requirement(セキュリティ機能要件)
ST	Security Target(セキュリティターゲット)
TOE	Target Of Evaluation(評価対象)
TSF	TOE Security Function(TOE セキュリティ機能)
TSFI	TSF Interface(TSF インタフェース)
TSS	TOE Summary Specification(TOE 要約仕様)