ネットワークデバイスのコラボラティブプロテクション プロファイル (NDcPP) 拡張パッケージ 無線ローカルエリアネットワーク (WLAN) アクセスシステム

2015 年 5 月 29 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

表の一覧

1. 概説

本拡張パッケージ (EP) は、無線ローカルエリアネットワーク (WLAN) アクセスシステム (無線通信データを暴露と改変から保護するような、暗号化された IEEE802.11 リンクを確立するプライベートネットワークのエッジにあるデバイスやシステムであると定義される) に対するセキュリティ要件を記述し、十分に定義され記述された脅威の軽減を目的とする最小限のベースライン要件を提供することを意図している。しかし、本 EP は、それ自体で完結するわけはなく、むしろ*ネットワークデバイスのコラボラティブプロテクションプロファイル (ND cPP) のセキュリティ要件*を拡張するものである。 本概説では、適合する評価対象 (TOE) の機能について記述し、ND cPP と連携して本 EP がどのように利用されるかについても論じる。

1.1 適合主張

ネットワークデバイスのコラボラティブプロテクションプロファイル (ND cPP) のセキュリティ要件は、一般のネットワーク基盤のデバイスについてのベースラインセキュリティ機能要件 (SFR) 及びセキュリティ保証要件 (SAR) を定義している。本 EP は、WLAN アクセスシステムネットワーク基盤のデバイスに特有である追加の SFR と対応する「保証アクティビティ」により ND cPP ベースラインを拡張する役割を果たす。保証アクティビティとは、TOE の SFR への適合性を決定するために、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

ND cPP の EP として、本 EP 及び ND cPP の両方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において適切に組み合わされることが想定される。本 EP は、そうすることが困難でなくまた曖昧であるべき(should)でないように特に定義された。ST は、適合主張において ND cPP (現在のバージョンは http://www.niap-ccevs.org/pp/を参照) 及び本 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 EP は、具体的には WLAN (IEEE 802.11) アクセスシステムに対処する。 適合する WLAN アクセスシステムは、ネットワークに接続され、企業ネットワーク全体において基盤の役割を持つような、ハードウェアとソフトウェアから成るシステムである。特に、WLAN アクセスシステムは、企業ネットワークへの、認証され暗号化されたパスを提供するようなセキュアな無線 (IEEE 802.11) リンクを確立し、これにより、「無線」送信される情報の暴露リスクを軽減する。

本 EP は、ND cPP の上に構築されるため、適合 TOE は、ここで次に論じられる脅威の環境に対応して、本 EP で定義される追加機能とともに ND cPP で要求される機能を実装する義務がある。

2. セキュリティ課題記述

本拡張パッケージ (EP) は、ネットワークパケットが WLAN アクセスシステムを介して有線プライベートネットワークと無線クライアントの間の境界を横断するような状況に対処するため、作成される。WLAN アクセスシステムは、通信データの管理、認証、暗号化、及び保護と取り扱い等のセキュリティ機能をサポートすることにより、利用者 (無線クライアント) と有線 (高信頼) ネットワークの間にセキュアな通信を提供する。通信データを暴露や改ざんから保護するため、WLAN アクセスシステムは、セキュアな通信を確立するために利用される。WLAN アクセスシステムは、セキュアな暗号学的トンネルの一端を提供し、認証された無線クライアントとのネゴシエーションされた WLAN アクセスシステムのセキュリティ方針に従ってネットワークパケットの暗号化と復号を実行する。複数の同時無線接続をサポートし、これらの相手との複数の暗号学的なトンネルの確立と終了が可能である。

WLAN アクセスシステムの正しいインストール、設定、及び管理は、正常な運用に重要である。

本 EP は、ND cPP で識別された脅威について繰り返さないが、それらすべては、所与の適合性及びゆえに ND cPP 上の本 EP の依存性を適用することに留意されたい。ND cPP には、そのセキュリティ機能を提供する TOE の能力に対する脅威のみを含むが、本 EP は運用環境における資源に対する脅威のみに対処することに留意されたい。ND cPP の脅威と本 EP で定義される脅威はともに、WLAN アクセスシステム TOE によって対処されるセキュリティ脅威の包括的なセットを定義する。

2.1 脅威

2.1.1 許可されない情報の暴露

保護されたネットワーク上のデバイスは、保護されたネットワークの外部のデバイスによってもたらされる、許可されないアクティビティの実行を試行するかもしれないという脅威にさらされるかもしれない。悪意のある外部のデバイスが保護されたネットワーク上のデバイスと通信できる場合、または保護されたネットワーク上のデバイスが悪意のある外部のデバイスとの通信を確立できる場合 (例、WLAN 通信データを不心得者にさらすような WLAN データ暗号化の欠如／不十分である結果として) 、それらの内部デバイスは、情報の許可されない暴露の影響を受けやすいかもしれない。

(T.NETWORK_DISCLOSURE)

2.1.2 サービスへの不適切なアクセス

保護されたネットワークの外部にあるデバイスは、保護されたネットワークの内部からのみアクセスされること、または保護されたネットワークへの認証された経路を利用するエンティティによってのみアクセスされることを意図するような、保護されたネットワーク上にあるサービスを使おうと捜すかもしれない。

(T. NETWORK_ACCESS)

2.1.3 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殆化を招く可能性がある。

(T.TSF_FAILURE)

2.1.4 データ完全性の危殆化

保護されたネットワーク上のデバイスは、保護されたネットワークの外部にあるデバイスによって提示される、許可なしにデータの改変を試行するかもしれないような脅威にさらされるかもしれない。悪意ある既知の外部デバイスが保護されたネットワーク上のデバイスと通信できる場合、または保護されたネットワーク上のデバイスがそのような外部のデバイスとの通信を確立できる場合、その通信に含まれるデータは、完全性喪失の影響を受けやすいかもしれない。

(T.DATA_INTEGRITY)

2.1.5 リプレイ攻撃

許可されない個人がシステムへのアクセスをうまく得る場合、敵対者は「リプレイ」攻撃を実行する機会を得るかもしれない。この攻撃方法は、無線ネットワーク全体に渡って流れているパケットをキャプチャし、その後、意図された受信者に知られずにそのパケットを送信することを、その個人に許してしまう。

(T.REPLAY_ATTACK)

2.2 前提条件

WLAN アクセスシステムの前提条件は、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た方針を実施する。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、[ND cPP] で記述されたものに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 データ保護

情報の許可されない暴露、サービスへの不適切なアクセス、サービスの誤使用、サービス停止、及びネットワークベースの偵察に関連する課題に対処するため、適合 TOE は、暗号機能を実装する。これらの機能は、機密性を維持し、TOE の外部で送信されるデータの改変の検知を可能とすることを意図している。

侵入という観点から、WLAN アクセスシステムは、具体的な WLAN 利用者とシステムにのみへのアクセスに制限するだけではなく、ネットワークトラフィクが暗号化されるか、平文で送信されるのかを決定する役割も担う。これらの制限により、許可されないエンティティによるネットワークポートのスキャニング (レイヤ 3 以上) を防止でき、保護されたネットワーク上の情報へのアクセスを正しく認証された WLAN クライアントシステムから入手可能なものに限定できる。

(O.CRYPTOGRAPHIC_FUNCTIONS -> FCS_COP.1(1), FCS_IPSEC_EXT.1, FCS_CKM.1(1), FCS_CKM.2(2), FCS_CKM.2(3), FIA_PSK_EXT.1)

3.1.2 認証

情報の許可されない暴露に関連する課題にさらに深く対処するため、適合 TOE の認証能力は、WLAN ピアが WLAN アクセスシステムとの WLAN 接続を確立することを許容する。WLAN 端点は、許可された外部 IT エンティティと通信していることを保証するために相互に認証する。

入口と出口の両方の観点から、WLAN アクセスシステムは、保護されたネットワーク資源と許可された WLAN クライアントデバイスの間でのみ通信を許可するため、認証 (例、EAP-TLS) とデータ暗号化 (例、128 ビット AES) の組み合わせを用いて構成可能である。

(O.AUTHENTICATION -> FTP_ITC.1, FCS_IPSEC_EXT.1, FIA_AFL.1, FIA_UAU.6, FIA_8021X_EXT.1, FTA_TSE.1)

3.1.3 セキュアでない操作

TOE のハードウェアに障害が発生するか TOE のソフトウェアの完全性が危殆化するような事が起こるかもしれない、後者は悪意のある目的かまたは悪意がない目的かに起因するものがある。ハードウェアまたはソフトウェアの仕様の範囲外での TOE 運用の懸念に対処するため、TOE は、自己テストのメカニズムを介して報告される問題の発見に際して直ちにシャットダウンすること。

(O.FAIL_SECURE -> FPT_FLS.1, FPT_TST_EXT.1)

3.1.4 システム監視

WLAN アクセスシステムの動作を監視できる管理者の課題に対処するため、ND cPP からの本セキュリティ対策方針は、以下のように拡張される。

WLAN の機能とセキュリティに特有の監査対象事象が追加された。

(O.SYSTEM_MONITORING -> FAU_GEN.1)

3.1.5 TOE 管理

本セキュリティ対策方針は、WLAN アクセスシステムのリモート管理に含まれる問題に対処する。適合 TOE は、リモート管理者による認証試行失敗に対処するために必要な機能を提供すること。

(O.TOE_ADMINISTRATION -> FIA_AFL.1, FMT_SMR.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ために要求される対策方針は、セクション A.2.2 で定義される。

4 セキュリティ要件

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* のパート 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 TOE セキュリティ機能要件

本 EP は ND cPP を拡張するものなので、セキュリティ機能のいくつかは、ベース PP から継承されたものである (また、本書に含まれていない) ことが想定される。 本セキュリティ機能には、次のものが含まれる：FCS_CKM.1、FCS_CKM.2、FCS_CKM.4、FCS_COP.1(2)、FCS_COP.1(3)、FCS_COP.1(4)、FCS_RBG_EXT.1、FCS_IPSEC_EXT.1、FIA_X509_EXT.1、及び FTP_TRP.1。

本 EP には、何らかの形の改変を必要とするような、ND cPP に存在する 4 つの SFR コンポーネントがある。本 EP には、新たに導入された 10 個の SFR があり、同様に 13 の監査事象が追加され、規定された。

4.2.1 ND cPP セキュリティ機能要件に関する指示

本セクションは、WLAN アクセスシステム EP で関連する SFR をサポートするために ND cPP に含まれる特定の SFR に対してどのような選択がなされなければならない (must) かについて ST 作成者に指示している。 これは、必須の選択がなされたエレメントを表現することによって得られる。ST 作成者は、TOE に存在する具体的な機能やふるまいを保証するため、残っている選択項目について自分の望むとおりに完成することができる。要求される必要な選択の提供に加え

て、本 EP に適合するために ND cPP FPT_TST_EXT.1 コンポーネントに追加されなければならない(must)エレメント、FPT_TST_EXT.1.2 がある。

全部の保証アクティビティが本セクションの要件について繰り返される訳ではなく、すでに ND cPP に取り込まれているものを補足するために必要とされる追加テストのみが含まれる。ここで規定するとおり、これらの SFR に適合する ST 及び TOE を評価するときに評価者にとって重要なことは、正しい選択がなされていること、及び適切なテストが要件への適合性を実証するために実行されることである。

4.2.1.1 FCS_COP.1(1) 暗号操作(AES データ暗号化／復号)

FCS_COP.1.1(1) **詳細化**：TSF は、以下に合致する、特定された暗号アルゴリズム ***CBC、CCMP*** [選択: GCM、GCMP] モード**で利用される AES** と暗号鍵長 ***128 ビット*** [選択：192 ビット、256 ビット]に従って、**暗号化／復号**を実行しなければならない(shall)：***ISO 18033-3 で指定される AES、NIST SP 800-38C と IEEE 802.11-2012 で定義される CCMP、*** [選択: ISO 10116 で指定される CBC、ISO 19772 で指定される GCM、NIST SP800-38D と IEEE 802.11ac-2013 で指定される CCMP と GCMP] 。

適用上の注釈： 本要件は、128 ビットの鍵長を持つ AES に 2 つのモードが実装されることを義務付けている。これらのモードがすべての暗号化／復号の機能の両方について利用されるとは想定されていない。むしろ、義務化は特定の目的に役立つ：FCS_IPSEC 要件を適合するために CBC モードが必須であり、また IEEE 802.11-2012 を適合するために AES-CCMP (SP 800-38C で指定される CCM で AES を利用するもの) が実装されなければならない(must)。

FCS_COP.1.1(1) の最初の選択で、ST 作成者は AES が動作する追加の利用モードを選ぶべきである(should)。2 番目の選択で、ST 作成者は本機能によりサポートされる鍵長を選ぶべきである(should)。 128 ビット CCMP は、FCS_CKM.1.1(2) に適合するため必須となる。

オプションとして、256 ビットの鍵長を用いる AES-CCMP-256 または AES-GCMP-256 が IEEE 802.11ac 接続用に実装されるかもしれないことに留意されたい。 将来、これらのモードの 1 つが必須となるかもしれない。

保証アクティビティ：

テスト

ND cPP で規定されるテストに追加して、評価者は、以下のテストについても実行しなければならない(shall)。

AES-CCM テスト

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

128 ビット及び 256 ビットの鍵

2 つのペイロード長. 1 つのペイロード長は、0 バイト以上のサポートされる最も短いペイロード長としなければならない(shall)。その他のペイロード長は、32 バイト (256 ビット) 以下のサポートされる最も長いペイロード長としなければならない(shall)。

2 つまたは 3 つの関連データ長. 1 つの関連データ長は 0 としなければならない(shall)、サポートされる場合。1 つの関連データ長は、0 バイト以上でサポートされる最も短い関連データ長としなければならない(shall)。 1 つの関連データ長は、32 バイト (256 ビット) 以下でサポートされる最も長い関連データ長としなければならない(shall)。実装が 216 バイトの関連データ長をサポートする場合、216 バイトの関連データ長がテストされなければならない(shall)。

ノンス長. 7 と 13 バイトを含めて、その間のサポートされるすべてのノンス長が、テストされなければならない(shall)。

タグ長. 4、6、8、10、12、14 及び 16 バイトのサポートされるすべてのタグ長がテストされなければならない(shall)。

このモードについて IEEE 802.11 で規定された制限 (ノンス長の 13 とタグ長の 8) のため、その選択が上で規定された範囲に入っている限り、サポートされる長さのサブセットをテストすることは許容される。この場合、評価者は、これらはサポートされる長さのみであることを保証しなければならない(shall)。AES-CCM の生成- 暗号化機能をテストするため、評価者は以下の 4 つのテストを実行しなければならない(shall) :

テスト 1 : サポートされる鍵及び関連データ長のそれぞれについて、またサポートされるペイロード、ノンス及びタグ長のいずれかについて、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得しなければならない(shall)。

テスト **2**. サポートされる鍵及びペイロード長のそれぞれについて、またサポートされる関連データ、ノンス及びタグ長のいずれかについて、評価者は 1 つの鍵の値、1 つのノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得しなければならない(shall)。

テスト 3 : サポートされる鍵及びノンス長のそれぞれについて、またサポートされる関連データ、ペイロード及びタグ長のいずれかについて、評価者は 1 つの鍵の値及び 10 個の関連データ、ペイロード及びノンスの値の 3 組を供給し、得られた暗号文を取得しなければならない(shall)。

テスト **4** : サポートされる鍵及びタグ長のそれぞれについて、またサポートされる関連データ、ペイロード及びノンス長のいずれかについて、評価者は 1 つの鍵の値、1 つの

ノンスの値及び 10 ペアの関連データ及びペイロードの値を供給し、得られた暗号文を取得しなければならない(shall)。

上記テストのそれぞれで正しいことを決定するため、評価者は暗号文を、既知の良好な実装を用いた同じ入力の生成 – 暗号化の結果と比較しなければならない(shall)。

AES-CCM の復号–検証機能をテストするため、サポートされる関連データ長、ペイロード長、ノンス長、及びタグ長のそれぞれの組み合わせについて、評価者は 1 つの鍵の値と 15 個のノンス、関連データ及び暗号文の 3 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 のセット毎に、不合格となるべき(should) 10 個の組と合格となるべき(should) 5 個の組とを供給しなければならない(shall)。

さらに、評価者は、AES-CCMPのIEEE 802.11-2012実装をさらに検証するため、IEEE 802.11-02/362r6文書 “Proposed Test vectors for IEEE 802.11 TGi” (2002年9月10日付) のセクション2.1「AES-CCMP Encapsulation Example」及びセクション2.2「Additional AES CCMP Test Vectors」のテストを利用しなければならない(shall)。

4.2.1.2 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 は、ND cPP の附属書 B から継承されたものである。しかし、本 EP では必須 (選択ベースではなく) とみなされており、ST に含まれなければならない(must)。

4.2.1.3 FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 **詳細化：** TSF は、それ自身と**以下の機能をサポートする許可された IT エンティティ間に：WLAN クライアント、監査サーバ、802.1X 認証サーバ、及び [割付：*[その他の機能]*]** その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、及び暴露からのチャネルデータの保護及びチャネルデータの改変の検出を提供する**高信頼通信チャネルを提供するために IEEE 802.11-2012 (WPA2)、 IEEE 802.1X、 IPsec、及び** [選択: SSH、 TLS、HTTPS、その他のプロトコルなし] **を利用できる**なければならない(shall)。

適用上の注釈： 上記要件の意図は、TOE がその機能を実行するために対話する許可された IT エンティティとのすべての外部通信を保護するために暗号プロトコルを利用することにある。IEEE 802.1X を用いた IEEE 802.11-2012 (WPA2) が無線クライアントとの通信に要求される；IPsec が少なくとも認証サーバとの通信に要求される。

TOE がその他の必要な許可された IT エンティティ (NTP サーバ、監査サーバ) と通信する場合、IPsec またはその他の列挙されたプロトコルの 1 つ (SSH、TLS 及び TLS/HTTPS が許可される) を利用しなければならない(must)、また、ST 作成者は、適切な選択を行い、次にその選択に対応する(NDcPP の) 附属書 B に詳述された要件がまだ存在しなければ ST に含めることを保証する。通信を開始する側に関する要件は存在しないが、ST 作成者は TOE が許可された IT エンティティとの通信を開始できるサービスを FTP_ITC.1.3 の割付において列挙する。

本要件は、通信が最初に確立される際だけでなく、中断後に再開する際にも保護されることを意味している。

本 SFR の残りのエレメントは、一切の改変なしにベース ND cPP から直接継承されている。
リモート管理者との通信は、NDcPP から直接継承された FTP_TRP によりカバーされている。

保証アクティビティ：

評価者は、本 SFR についてベース ND cPP で規定された保証アクティビティに加えて、次のアクティビティを実行しなければならない(shall)。

TSS

評価者は、本要件で識別された許可された IT エンティティとのすべての通信について、各通信メカニズムがその IT エンティティについて許可されたプロトコルに関して識別されていることを決定するため TSS を検査しなければならない(shall)。評価者は、TSS に列挙されたすべてのプロトコルが ST の要件に規定され、含まれていることについても確認しなければならない(shall)。

ガイダンス

評価者は、許可された各 IT 各エンティティと許容されるプロトコルを確立するための指示がガイダンス証拠資料に含まれていること、及び接続が意図せずに破損した場合の復旧手順がその中に盛り込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、ガイダンス証拠資料に記述されるとおりにセットアップして、通信が成功することを保証して、許可された各 IT エンティティとの各プロトコルを用いた通信が評価の過程でテストされることを保証しなければならない(shall)。

テスト 2： 本要件で定義されるとおり TOE が開始できるような各プロトコルについて、評価者は、実際に通信チャネルが TOE から開始されることが可能であることを保証するため、ガイダンス証拠資料に従わなければならない(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、テスト 1 の間にテストされた許可された各 IT エンティティに対応する各プロトコルについて、確立された接続を物理的に中断しなければならない(shall)。評価者は、物理的な接続性が回復されるとき、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)。

テスト 5： 評価者は、まず WPA2 (TKIP へのフォールバック無しの、AES) のみをアクセスシステムが利用するよう設定し、次に WPA2 (AES) 接続がアクセスシステムとクライアントデバイス

の間でなされることを保証しなければならない(shall)。最後に、評価者は、AES をサポートしないクライアントデバイスをアクセスシステムに接続するよう試行して、アクセスシステムが接続を拒否すること (TKIP にフォールバックしないこと) を保証しなければならない(shall)。

さらなる保証アクティビティは、具体的なプロトコルに対応している。

4.2.1.4 FPT_TST_EXT.1 拡張: TSF テスト

FPT_TST_EXT.1.1 TSF は、TSF の正常な動作を実証するため、最初の起動時（電源投入時）及び[選択：通常の動作中に定期的に、許可された利用者のリクエストで、条件で [割付：*自己テストが起動するべき(should)条件*]] に、以下の自己テストのスイートを実行しなければならない(shall)：[割付：*TSF により実行される自己テストのリスト*]。

FPT_TST_EXT.1.2 TSF は、FCS_COP.1(2)で規定された TSF 提供の暗号サービスの利用を通して実行のためにロードされるとき、蓄積された TSF 実行可能コードの完全性を検証するための機能を提供しなければならない(shall)。

保証アクティビティ：

評価者は、本 SFR のベース ND cPP で規定された保証アクティビティに追加して、以下のアクティビティを実行しなければならない(shall)：

TSS

評価者は、起動時に TSF により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)；この記述には、そのテストが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」という記述よりも、「メモリは、ある値を各メモリのロケーションに書き込み、それを読み出すことによって、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テストされる」のような記述が利用されるべきである)。評価者は、TSF が正常に動作していることを実証するのにそれらのテストで十分であるという説明が TSS でなされていることを保証しなければならない(shall)。

評価者は、格納されている TSF 実行可能コードが実行のためにロードされるときに、その実行可能コードの完全性を検証する方法について TSS で説明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)、それには、検証ステップと共に、完全性を保証するために利用される「チェック値」の生成と保護も含まれる。この記述は、これらの機能の実行で利用されるデジタル署名サービスについてもカバーされなければならない(shall)。評価者は、この機能を初期化または操作するために管理者によって要求されるあらゆるアクションが存在していることを保証するために、操作ガイダンスについてもチェックすること。

ガイダンス

評価者は、成功 (例、ハッシュが検証される) の場合、及び不成功 (例、ハッシュが検証されない) の場合に実行するアクションについて、TSS（または、操作ガイダンス）に記述されていることも保証すること。

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 : 操作ガイダンスに従って、評価者は、完全性保護システムを初期化しなければならない(shall)。評価者は、TSF ソフトウェアのロードを起動するためのアクションを実行し、完全性メカニズムが完全性の誤りを含むような実行可能コードにフラグを立てないことを観測しなければならない(shall)。

テスト 2 : 評価者は、TSF 実行可能コードを改変し、その実行可能コードが TSF によってロードされるようにしなければならない(shall)。評価者は、完全性違反が引き起こされていることを観測しなければならない(shall) (モジュールが改変されて、フォーマットが破損してモジュールが実行不能になったという事実ではなく、完全性の違反がモジュールをロードするための障害の原因であると決定されるように注意が払われなければならない(must))。

4.2.2 TOE セキュリティ機能要件

本 EP の本文中のセキュリティ機能要件は、ND cPP から継承されるものと WLAN AS の TOE に特有のものに分けられる。本セクションには、TOE によって満たさなければならない(must) 要件で、ベース ND cPP ではカバーされないような要件が含まれている。

4.2.2.1 FCS_CKM.1(2) 暗号鍵生成 (WPA2 接続用の対称鍵)

FCS_CKM.1.1(2) **詳細化**：TSF は、以下 **[*IEEE 802.11-2012*]** 及び [選択: IEEE 802.11ac-2014、その他の規格なし]に合致する **FCS_RBG_EXT.1 で特定された乱数ビット生成器を用いて**、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***] 及び [選択 : 256 ビット、その他の鍵長なし] に従って、**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 ビット出力する PRF-384 である。GCMP の利用は、IEEE 802.11ac-2013 (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-SHA-384 (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。本 EP で規定される RBG によって生成された乱数値、本 EP で規定される HMAC 機能をその他の情報と共に利用して行われるような、 (本 EP で規定

されている RBG を通して) GTK の導出について、PMK からの PTK の導出と共に、言及する。これは、主に 802.11-2012 の 11 章で規定される。

保証アクティビティ：

TSS

暗号プリミティブは、本 EP のどこかで規定された保証アクティビティを通して検証される。 評価者は、無線クライアントへのセキュアな接続の確立と維持において、本 EP で定義され実装されるプリミティブが TOE によって利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)。この記述には、GTK 及び PTK が生成される方法または導出される方法が含まれなければならない(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方法についての記述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たテストだけでなく、実行された第三者テストの証明 (例、WPA2 認証) についても含まれる。評価者は、テスト手法の説明が、プロトコル特有の詳細がテストされる範囲を決定するために十分詳細であることを保証しなければならない(shall)。

テスト

評価者は、TOE と無線クライアントの間のフレームを収集するパケットスニフィングツールを用いて、以下のテストについても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／またはクライアントの 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接続をセットアップし、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 WLAN クライアントと通信するように 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 WLAN クライアントの間の接続を開始し、TOE がクライアントと認証し、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 からクライアントを切断しスニファを停止させなければならない(shall)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、クライアントと 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 0x4208 を持たない、TOE とクライアントの間で次の 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)。

4.2.2.2 FCS_CKM.2(2) 暗号鍵配付 (PMK)

FCS_CKM.2.1(2) **詳細化**： TSF は、以下 [***IEEE 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：[***802.1X 認証サーバから***] に従って、**802.11 マスタ鍵ペア (PMK) を受信**しなければならない(shall)。

適用上の注釈： 本要件は、TOE によって RADIUS サーバから受信されるマスタ鍵ペア(PMK)に適用する。本要件の意図は、適合 TOE がクライアントとのセキュアな通信を確立する前に 802.1X 認証を実行することを保証することである。この意図は、本 EP への適合評価されたあらゆる WLAN AS が WPA2-ENT と証明書ベースの認証メカニズムをサポートし、ゆえに事前共有鍵のみをサポートするような実装を許容しないことである。RADIUS サーバとの通信は、IPsec 保護の接続を介して実行されることが要求されるので、PMK の転送は保護される。

保証アクティビティ：

TSS

評価者は、PMK が TSF へ転送される方法 (即ち、どの EAP 属性を通して) について 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)。

テスト

評価者は、提供された設定ガイダンスに従って、TOE と RADIUS サーバの間のセションを確立しなければならない(shall)。次に、評価者は、PMK が暴露されないことを決定するため、TOE への無線クライアントの接続試行が成功する間に、RADIUS サーバと TOE の間を通過するトラフィクを検査しなければならない(shall)。

4.2.2.3 FCS_CKM.2(3) 暗号鍵配付 (GTK)

FCS_CKM.2.1(3) **詳細化**：TSF は、以下の**[NIST SP 800-38F、パケットフォーマット及びタイミングの検討についての IEEE 802.11-2012] 、および、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 (GTK)** を配付しなければならない(shall)。

適用上の注釈： 本要件は、接続されるクライアントへのブロードキャスト及びマルチキャストのメッセージで用いるために TOE によって生成されるグループ一時鍵 (GTK) に適用される。802.11-2012 は、NIST SP 800-38F で規定される 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)という事実と共に、転送フォーマットを規定する。

保証アクティビティ：

TSS

評価者は、本 EP で特定された AES の実装を用いて GTK が配付の前にラップされる方法、及び複数のクライアントが TOE へ接続する際に GTK が配付される方法についても 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)。

テスト

評価者は、無線クライアントと TOE の間でフレームを収集するためにパケットスニフィングツールを用いて次のテストについても実行しなければならない(shall) (FCS_CKM.1.1(2) の保証アクティビティと組み合わせて実行してもよい)。

ブロードキャスト／マルチキャストの機能を完全にテストするため、これらのステップは、評価者が複数のクライアントを TOE に接続して実行しなければならない(shall)。評価者は、TOE に接続されたクライアントサブセットの中から少なくとも 2 つのマルチキャストグループで、それぞれ少なくとも 2 つのクライアントから成るが TOE に接続されたすべてのクライアントよりも少ないようなマルチキャストグループを作成しなければならない(shall)。クライアントのいくつか (すべてではない) は、両方のグループに属していなければならない(shall)。評価者は、確立された GTK が適切な参加しているクライアントに送信されることを保証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／またはクライアントの 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接続をセットアップし、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クライア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、テスト用でのみ使用される

ステップ 3：評価者は、スニフィングツールを起動し、TOE とクライアントの間の接続を開始し、クライアントが TOE 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 からクライアントを切断しスニファを停止させなければならない(shall)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 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、TOE とクライアント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)。

4.2.2.4 FIA_AFL.1 認証失敗時の取り扱い

FIA_AFL.1.1 **詳細化**： TSF は、**管理者によるリモート認証の試行**に関して、**管理者設定可能な正の整数回の連続する**認証試行の失敗が生じたときを検出しなければならない(shall)。

FIA_AFL.1.2 定義された認証試行の失敗回数に**達した**とき、TSF は [選択、1 つを選択： 問題のあるリモート管理者が認証成功することをローカル管理者によって [割付：*アクション*] が講じられるまで防止；問題のあるリモート管理者が認証成功することを管理者が定義した時間が経過するまで防止] をしなければならない(shall)。

適用上の注釈： 本要件は、このようなやり方でローカルの管理者のアカウントをロックすることは意味がないため、ローカルコンソール上の管理者には適用されない。これは、（例えば）ローカルの管理者に別のアカウントを要求すること、またはローカルとリモートのログイン試行を区別する認証メカニズムを実装することによって、対処が可能である。ローカル管理者によって講じられる「アクション」は、実装に特有のものであり、管理者ガイダンスで定義される (例えば、ロックアウトのリセットやパスワードのリセット)。ST 作成者は、TOE がこの処理をどのように実装しているかに応じて、認証失敗の取り扱いについての選択肢の 1 つを選択する。

保証アクティビティ：

TSS

評価者は、リモート管理アクションのためにサポートされるそれぞれの方法について、連続する認証試行の失敗が検出され追跡される方法の記述が含まれていると決定するため、TSS を検査しなければならない(shall)。TSS は、リモート管理者の TOE へのログオン成功の防止方法と、この能力を回復するために必要なアクションについても記述しなければならない(shall)。

ガイダンス

評価者は、連続する認証試行の失敗回数 (1.1) と時間 (1.2、実装された場合) の設定のための指示が提供されること、及びリモート管理者が再度ログオン成功することを許可するプロセスが規定されるそれぞれの「アクション」について記述されること (そのオプションが選択されている場合) を保証するため、操作ガイダンスについても検査しなければならない(shall)。異なるアクションまたはメカニズムが、採用されるセキュアなプロトコルに応じて実装される場合 (例、TLS 対 SSH)、すべてについて記述されなければならない(must)。

テスト

評価者は、リモートの管理者が TOE にアクセスするそれぞれの方法について、次のテストを実行しなければならない(shall) (例、TLS、 SSH) :

テスト 1 : 評価者は、TOE によって許容される連続する認証試行の失敗回数を設定するために操作ガイダンスを利用しなければならない(shall)。評価者は、一度限界値に達したら、有効なクレデンシャルを用いた試行が成功しないことをテストしなければならない(shall)。本要件で規定されるそれぞれのアクションについて、評価者は、操作ガイダンスに従っていること、またリモート管理者のアクセスを許容するそれぞれのアクションの実行が成功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 によって許容される連続する不成功の認証試行回数と、有効なログインがリモート管理者に対して許容されるまでの時間を設定するため、操作ガイダンスを利用しなければならない(shall)。無効なログイン試行の規定された回数を超えて有効なログインが可能でないことを示した後、評価者は、別のアクセス試行までの時間によって定義されたインターバルの間、待機することが、リモート管理者に有効なクレデンシャルを用いたログインの成功をもたらすことを示さなければならない(shall)。

4.2.2.5 FIA_UAU.6 再認証

FIA_UAU.6.1 TSF は、条件 : 利用者が自分のパスワードを変更するときに、[選択 : TSF 起動によるロック(FTA_SSL) に従う、[割付 : *その他の条件*]、その他の条件なし]のもとで、管理利用者を再認証しなければならない(shall)。

保証アクティビティ :

テスト

評価者は、本要件で規定される条件のそれぞれについて次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、操作ガイダンスによる指示のとおり、パスワードの変更を試行しなければならない(shall)。本試行の間に、評価者は再認証が要求されることを検証しなければならない (shall)。

4.2.2.6 FIA_8021X_EXT.1 拡張：802.1X ポートアクセスエンティティ(認証装置)認証

FIA_8021X_EXT.1.1 TSF は、「認証装置(Authenticator)」の役割での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)。

FIA_8021X_EXT.1.2 TSF は、RFC 2865 と 3579 に適合する RADIUS 認証サーバとの通信をサポートしなければならない(shall)。

FIA_8021X_EXT.1.3 TSF は、この認証交換が正常に完了する前に、その 802.1X 制御ポートへのアクセスが無線クライアントに一切与えられないことを保証しなければならない(shall)。

適用上の注釈：本要件は、802.1X 認証交換における認証装置としての TOE の役割をカバーする。交換がうまく完了すると、TOE は RADIUS サーバから PMK を入手し、802.11 通信を始めるために無線クライアント(サプリカント) と 4 ウェイハンドシェイクを実行する。

既に示されたように、少なくとも 3 つ通信経路が交換中に存在する；2 つの経路では TOE が端点として存在し、1 つの経路では TOE が転送ポイントとしてのみ機能する。TOE は、802.1X-2007 で規定されるとおり無線クライアントとの EAP over LAN (EAPOL) 接続を確立する。TOE は、RADIUS サーバとの RADIUS プロトコル接続 (IPsec 接続の中でトンネルされる) についても確立する (または既に確立している)。無線クライアントと RADIUS サーバは EAP-TLS セションを確立する (RFC 5216)；このトランザクションにおいて、TOE は、その EAPOL/RADIUS 端点から単に EAP-TLS パケットを取り、それらをその他の端点へ転送するだけである。なぜなら、具体的な認証方法 (この場合は TLS) は TOE にははっきりしないため、本 EP の RFC 5126 に関する要件は一切ない。しかし、ベース RADIUS プロトコル (2865) は、実装と保証アクティビティで対処される必要のあるアップデート(3579) が含まれる。さらに、RFC 5080 では、開発者によって対処される必要がある実装の問題が含まれるが、新たな要件は一切課されない。

802.1X 認証を実行する意味は、(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前提で) ネットワークへのアクセスを提供することにある：802.1X の用語では、これは、無線クライアントが TOE によって維持される「制御されたポート」へのアクセスを有することを意味する。

保証アクティビティ：

TSS

TSF が 802.1X-2010 標準を正しく実装していることを示すため、評価者は、TSS に次の情報が含まれていることを保証しなければならない(shall)：

- TOE が実装する標準のセクション(段落)、
- 識別されたそれぞれのセクションについて、標準によって許容される実装におけるあらゆるオプションが規定される；及び

- 識別されたそれぞれのセクションについて、不適合の正当化を含め、あらゆる不適合が識別され、記述される。

RADIUS サーバへの接続は IPsec トンネル(FCS_IPSEC_EXT.1)に含まれるので、これらの通信に保護を提供するため、本要件で識別された RFC に詳述されたセキュリティメカニズムには依存しない。その結果、RFC の詳しい分析は一切要求されない。しかし、評価者は、TOE が本要件で列挙された RFC に適合することを保証するため、製品開発者によって取られるような対策(証拠資料、テスト) について TSS に記述されることを保証しなければならない(shall)。

テスト

テスト 1：評価者は、無線クライアントがテストネットワークへアクセスできないことを実証しなければならない(shall)。TOE を介して RADIUS サーバとうまく認証した後、評価者は、無線クライアントがテストネットワークへアクセスできることを実証しなければならない(shall)。

テスト 2： 評価者は、無線クライアントがテストネットワークにアクセスでき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、無線クライアントがテストネットワークへまだアクセスできていないという結果が得られるべきである(should)。

テスト 3： 評価者は、無線クライアントがテストネットワークにアクセスでき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、無効な RADIUS 証明書を用いて認証試行を行わなければならない(shall)。これにより、無線クライアントがテストネットワークへまだアクセスできていないという結果が得られるべきである(should)。

注釈： 上記のテスト 2 と 3 は、「EAP-TLS が機能する」というテストではないが、テストの副産物ではある。テストは、実際に、本コンポーネントの 3 番目のエレメントのように、(2 つの不成功のモードの下で) 不成功の認証がそのネットワークへのアクセスの拒否をもたらすことを示している。

4.2.2.7 FIA_PSK_EXT.1 拡張：事前共有鍵の作成

FIA_PSK_EXT.1.1 TSF は、 [選択: IEEE 802.11 WPA2-PSK、IPsec、その他のプロトコルなし、[割付: *その他のプロトコルで事前共有鍵を用いるもの*]] に対して、事前共有鍵を利用できなければならない(shall)。

FIA_PSK_EXT.1.2 TSF は、以下のようなテキストベースの事前共有鍵を受け入れることができなければならない(shall)：

- 22 文字及び[選択: [割付: *その他のサポートされる長さ*]、その他の長さなし] であること；
- 大文字と小文字、数字、及び特殊文字 (「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、及び「)」を含む) の任意の組み合わせで構成されること。

FIA_PSK_EXT.1.3 TSF は、ビットベースの事前共有鍵を[選択: 受け入れる、FCS_RBG_EXT.1 で規定された乱数ビット生成器を用いて生成する] ことができなければならない(shall)。

適用上の注釈： 最初の選択で、その他のプロトコルが事前共有鍵を利用できる場合、それらが同様に割付に列挙されるべきである；さもなければ、「その他のプロトコルなし」が選択されるべきである(should)。本要件の意図は、すべてのプロトコルがテキストベースとビットベースの事前共有鍵の両方をサポートしていることである。

テキストベースの事前共有鍵の長さについて、相互運用性の推進を支援するため、共通の長さ (22 文字) が要求される。その他の長さがサポートされる場合、それらが割付に列挙されるべきである(should)； この割付は、同様に、ある範囲の値 (例、「5 から 55 文字までの長さ」) についても規定できる。

FIA_PSK_EXT.1.3 については、ST 作成者は、TSF が単にビットベースの事前共有鍵を受け入れるだけなのか、事前共有鍵を生成できるのかについて規定する。それらを生成する場合、本要件は、事前共有鍵が TOE によって提供される RBG を用いて生成されなければならない(must)ことを規定する。

保証アクティビティ：

TSS

評価者は、テキストベースとビットベースの事前共有鍵の両方を許容するようなすべてのプロトコルを TSS が識別していること、及び 22 文字のテキストベースの事前共有鍵がサポートされていることを TSS に記述していることを保証するため、TSS を検査しなければならない(shall)。本要件によって識別されたそれぞれのプロトコルについて、評価者は、利用者によって入力されたキーシーケンスからのテキストベースの事前共有鍵 (例、ASCII 表現) を、プロトコルによって利用されるビット列への変換が行われるような調整について TSS に記述されていること、及びこの調整が FIA_PSK_EXT.1.3 要件の最後の選択と一貫していることを確認しなければならない(shall)。

評価者は、ビットベースの事前共有鍵が生成されるプロセスについて TSS で記述されていることを保証するため TSS についても検査しなければならない(shall) (TOE がこの機能をサポートする場合)、またこのプロセスが FCS_RBG_EXT.1 で規定される RBG を利用することを確認しなければならない(shall)。

ガイダンス

評価者は、操作ガイダンスが強いテキストベースの事前共有鍵の作成についての管理者へのガイダンスを提供していること、及び (選択にて入力可能な鍵としてさまざまな長さを示す場合) サポートされる長さの範囲についての情報を操作ガイダンスが提供し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)。ガイダンスは、事前共有鍵で許容可能な文字を規定しなければならない(must)、またそのリストは FIA_PSK_EXT.1.2 に含まれるリストの上位セットでなければならない(must)。

評価者は、本要件で識別されたそれぞれのプロトコルについてビットベースの事前共有鍵を入力するのか、ビットベースの事前共有鍵を生成するのか (またはその両方) についての指示が操作ガイダンスに含まれることを確認しなければならない(shall)。

テスト

評価者は、各プロトコルについて、次のテストも実行しなければならない(shall) (または、プロトコルのインスタンス化、TOE において異なる実装によって実行される場合)。これらのテストの 1 つまたはそれ以上が 1 つのテストケースで実行できることに留意されたい。

テスト 1： 評価者は、操作ガイダンスに従って、許容される文字の組み合わせを含む 22 文字の事前共有鍵を作成し、その鍵を用いてプロトコルのネゴシエーションが成功することを実証しなければならない(shall)。

テスト 2 [条件付き]： TOE が複数の長さの事前共有鍵に対応できる場合、評価者は、最小の長さ；最大の長さ；許容可能な範囲内の長さ；及びサポート可能な範囲を超える無効な長さ (上と下の両方) を用いて、テスト 1 を繰り返さなければならない(shall)。最小長、最大長、及び含まれる長さのテストは成功するべきであり(should)、無効な長さは TOE によって拒否されなければならない(must)。

テスト 3 [条件付き]： TOE がビットベースの事前共有鍵を生成しない場合、評価者は、適切な長さのビットベースの事前共有鍵を取得し、それを操作ガイダンスの指示に従って入力しなければならない(shall)。次に評価者は、その鍵でプロトコルのネゴシエーションが成功できることを実証しなければならない(shall)。

テスト 4 [条件付き]： TOE がビットベースの事前共有鍵を生成する場合、評価者は、適切な長さのビットベースの事前共有鍵を生成し、操作ガイダンスの指示に従ってそれを利用しなければならない(shall)。次に評価者は、その鍵を用いてプロトコルのネゴシエーションが成功できることを実証しなければならない(shall)。

4.2.2.8 FPT_FLS.1 セキュアな状態を保持する障害

FPT_FLS.1.1　TSF は、以下の種別の障害が生じたときはセキュアな状態を保持しなければならない(shall)：電源投入時の自己テストの障害。

適用上の注釈：本要件の意図は、TOEに備わるフェールセキュア機能を表現することである。これは、識別された障害のいずれかが発生する際に TOE がセキュアな／安全な状態 (シャットダウン) を達成できなければならない(must)という意味である。

保証アクティビティ：

TSS

評価者は、TOE のフェールセキュア機能の実装が文書化されていると決定するため、TSS のセクションをレビューなければならない(shall)。評価者はまず、ST で規定されるすべての障害モードが記述されることを保証するため、TSS セクションを検査しなければならない(shall)。評価者は、セキュアな状態の定義が定められ、且つ鍵材料と利用者データの保護を保証するために適していることを決定するため、TSS をレビューしなければならない(shall)。

テスト

ST で規定されるそれぞれの障害モードについて、評価者は、TOE が、それぞれの障害モード種別を開始した後、セキュアな状態 (シャットダウン) を達成することを保証しなければならない(shall)。

4.2.2.9 FMT_SMR.1 セキュリティ管理役割

FMT_SMR.1.3 TSF は、無線クライアントから TOE をリモートで管理する能力がデフォルトでは無効化されていなければならない(shall)ことを保証しなければならない(shall)。

保証アクティビティ：

ガイダンス

評価者は、ローカルとリモートの両方で TOE を管理するための指示が、リモート管理用クライアント上で実行される必要がある任意の設定を含めて、操作ガイダンスに含まれていることを保証するため、操作ガイダンスをレビューしなければならない(shall)。

テスト

評価者は、次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、初めて使用するために操作ガイダンスから TOE を設定した後、デバイスの「有線」部分で TOE との管理セションを確立することが可能であることを実証しなければならない(shall)。次に評価者は、TOE にうまく接続できるような同じように設定された無線クライアントが管理を行うために使用できないことを実証しなければならない(shall)。

4.2.2.10 FTA_TSE.1 TOE セション確立

FTA_TSE.1.1 **詳細化：** TSF は、**TOE インタフェース、時刻、曜日、**[割付：*その他の属性*] に基づき**無線クライアントセションの**確立を拒否できなければならない(shall)。

適用上の注釈：「TOE インタフェース」は、WLAN クライアントが接続される TOE におけるデバイスに関して規定されることが可能である (例、具体的な WLAN アクセスポイント)。「時刻」と「曜日」は、それぞれ「1 日のうちの時刻」及び「1 週のうちの曜日」を指す。

割付は、セション確立の拒否の原因となり得るような追加の属性を規定するために ST 作成者によって利用されるべきである。

保証アクティビティ：

TSS

評価者は、クライアントセションを拒否できるようなすべての属性が特別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)。

ガイダンス

評価者は、TSS で識別されるそれぞれの属性を設定するためのガイダンスが TSS に含まれ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、次のテストについても実行しなければならない(shall)：

テスト 1： 評価者は、無線クライアントとのクライアントセションをうまく確立する。次に評価者は、そのクライアントのアクセスが、属性の具体的な値に基づいて拒否されるように、システムを設定するため、操作ガイダンスに従う。評価者は次に、属性の設定に違反したセションの確立を試行しなければならない(shall) (例えば、クライアントが接続しようとしている TOE インタフェースに基づいて拒否される WLAN アクセス (例、WLAN アクセスポイント)であるか、クライアントが接続試行しようとする時刻または曜日に基づいて拒否されるアクセスである)。評価者は、そのアクセス試行が失敗することを観測しなければならない(shall)。

4.2.2.11 FAU_GEN.1 監査データ生成

ND cPP にある FAU_GEN.1 の SFR を拡張するために役立つような、追加の監査対象事象がある。以下の事象は、適合するセキュリティターゲットとの関連で NDcPP の事象と組み合わせられるべきである(should)。

以下の監査事象が、本 EP では要求される。

要件	監査対象事象	追加の監査記録の内容
FCS_CKM.1(2)	鍵生成アクティビティの失敗。	なし。
FCS_CKM.2(2)	鍵配付アクティビティの失敗。	なし。
FCS_CKM.2(3)	鍵配付アクティビティの失敗、GTK ラッピングに関連する失敗を含む。	ラップされた鍵の意図した受信者の識別子。
FCS_COP.1(1)	WPA2 暗号化または復号の失敗。	暗号利用モード、暗号化/復号されるオブジェクト名称／識別子、接続の非 TOE 端点(IP アドレス)。
FCS_IPSEC_EXT.1	プロトコルの失敗。IPsec SA の確立／終了。IKEv2 から IKEv1 への鍵交換ネゴシエーション「ダウン」。	失敗の理由。成功と失敗の両方の接続の非 TOE 端点(IP アドレス)。
FTP_ITC.1	高信頼チャネル確立試行の失敗(IEEE 802.11 を含む)。チャネルデータ改変の検出。	チャネルのイニシエータ及びターゲットの識別情報。
FIA_AFL.1	不成功の認証試行のしきい値への到達、及び取られたアクション(例、アカウントの無効化)、及びその後の、適切であれば、正常状態への回復(例、端末の再度有効化)。	なし。
FIA_UAU.6	再認証の試行。	試行の起点(例、IP アドレス)
FIA_8021X_EXT.1	認証の交換が成功して完了する前に 802.1X 制御ポートへのアクセス試行。	提供されたクライアントの本人性(MAC アドレス)。
FIA_PSK_EXT.1	なし。	なし。
FPT_FLS.1	TSF の障害。	TSF が失敗したことを表示、発生した障害の種別と共に。
FPT_TST.EXT.1	本セットの TSF 自己テストの実行。検出された完全性違反。	完全性違反について、完全性違反の原因となった TSF コードファイル。
FTA_TSE.1	セション確立のメカニズムに起因するセション確立の拒否。	拒否の理由、確立試行の起点

表 1：監査対象事象

附属書 A – 根拠

本 EP において、本文書の最初のセクションは、WLAN アクセスシステム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般的な理解を助ける意図で、説明文表現を用いている。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、本セクションでは、本書に関連する評価アクティビティで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

TOE の運用環境では、以下に記載した固有の条件が存在すると想定されている。この前提条件は NDcPP で定義されたものに追加されたものであり、TOE のセキュリティ要件策定時の事実上の現実と TOE 利用上の基本的な環境条件の両方が含まれる。

前提条件名称	前提条件定義
A.CONNECTION	接続されるネットワークを流れるすべての適用可能なネットワークトラフィック上で TOE セキュリティ方針が実施されることを保証するようなやり方で、TOE が個別のネットワークに接続されると想定される。

表 2：前提条件

A.1.2 脅威

以下に列挙した脅威は、WLAN アクセスシステムによって対処される。これらの脅威は、NDcPP で定義されるものに追加して WLAN アクセスシステムに適用されるすべての脅威である。

脅威名	脅威の定義
T.NETWORK_DISCLOSURE	保護ネットワーク上の機密情報は、侵入または退出ベースのアクションにより暴露されるかもしれない。
T. NETWORK_ACCESS	保護されているネットワーク上のサービスには、そのネットワークの外部から不正アクセスが成し遂げられるかもしれない。
T.TSF_FAILURE	TOE のセキュリティメカニズムに障害が生じ、TSF の危殆化につながるかもしれない。
T.DATA_INTEGRITY	悪意ある者が、送信中のデータの変更を試みる。その結果、完全性が失われる。
T.REPLAY_ATTACK	悪意ある IT エンティティまたは外部の IT エンティティが、ネットワークにアクセスできる場合、そのエンティティはネットワーク中を横断する情報を採取して、意図した受信者にその情報を転送できるかもしれない。

表 3：脅威

A.1.3 組織のセキュリティ方針

WLAN アクセスシステムに特有な組織ポリシーは識別されていない。 しかし、ND cPP におけるすべての組織のセキュリティ方針は、WLAN アクセスシステムに適用される。

A.1.4 セキュリティ課題定義の対応関係

次の表は、本 EP で定義された脅威と前提条件を、本 EP で定義されたまたは識別されたセキュリティ対策方針への対応付けについても提供する。

脅威または前提条件	セキュリティ対策方針
A.CONNECTION	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.AUTHENTICATION と O.CRYPTOGRAPHIC_FUNCTIONS
T. NETWORK_ACCESS	O. AUTHENTICATION、O.TOE_ADMINISTRATION
T.TSF_FAILURE	O.FAIL_SECURE、O.SYSTEM_MONITORING
T.DATA_INTEGRITY	O.CRYP TOGRAPHIC_FUNCTIONS
T.REPLAY_ATTACK	O.AUTHENTICATION と O.CRYPTOGRAPHIC_FUNCTIONS

表 4：セキュリティ課題定義の対応関係

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

次の表は、WLAN アクセスシステムに特有のセキュリティ対策方針が含まれる。これらのセキュリティ対策方針は、ND cPP で定義された、WLAN アクセスシステムに適用されるすべての対策方針に追加されたものである。
ND cPP セキュリティ対策方針の 2 つ(O.SYSTEM_MONITORING と O.TOE_ADMINISTRATION)が本 EP では拡張されたが、対応するセキュリティ対策方針定義には影響を与えないことに留意されたい。

セキュリティ対策方針名称	セキュリティ対策方針定義
O.CRYPTOGRAPHIC_FUNCTIONS	TOE は、機密性を維持する手段としてデータを暗号化し復号し、TOE の外部に送信される TSF データの検出と改変を可能にするための手段を提供する。
O.AUTHENTICATION	TOE は、許可された外部エンティティとの通信を保証するために利用者を認証する手段を提供する。
O.FAIL_SECURE	自己テストの失敗の際に、TOE は、管理者によって設定されたセキュリティ方針に適合しない間にデータが送信できないことを保証するためにシャットダウンする。
O.SYSTEM_MONITORING	TOE は、WLAN の機能とセキュリティに特有の事象を監査する手段を提供する。
O.TOE_ADMINISTRATION	TOE は、リモートの管理者による不成功の認証試行に対処するために必要な機能を提供する。

表 5：TOE のセキュリティ対策方針

A.2.2 運用環境のセキュリティ対策方針

次の表は、WLAN アクセスシステムの運用環境に特有のセキュリティ対策方針が含まれる。これらのセキュリティ対策方針は、ND cPP で定義されるものに追加して WLAN アクセスシステムの運用環境に適用されるすべての対策方針である。

セキュリティ対策方針の名称	セキュリティ対策方針の定義
OE.CONNECTIONS	TOE 管理者は、接続されたネットワークの中で流れるネットワークトラフィク上の方針を TOE が効果的に実行できるようなやり方で TOE がインストールされることを保証する。

表 6：TOE のセキュリティ対策方針

A.2.3 セキュリティ対策方針の対応関係

本 EP で識別され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 の概説で示したように、ベースライン要件は本 EP の本文に含まれる。ST に含めることのできる追加要件があるが、TOE が本 EP への適合を主張するために必ずしもそれらを盛り込む必要はない。附属書の要件は本 EP の本文には含まれていないので、すべての WLAN アクセスシステムが分散型システムとして実装されることは必須ではない。TOE が複数のコンポーネントの間で物理的に分散されている場合、それらのコンポーネント間の通信は保護されなければならず(must)、以下の要件は ST に含まれなければならない(must)。

ST 作成者は、附属書 B、附属書 C、及び／または附属書 D における要件に対応するかもしれないが列挙されないような要件(例、FMT 型の要件)についても ST に含まれることを保証する責任があることに留意されたい。

B.1 FPT_ITT.1 基本 TSF 内データ転送保護

FPT_ITT.1.1 **詳細化：** TSF は、TSF データが TOE の異なるパーツ間で送られる場合、TSF データを暴露と改変から保護するため、**すべてのその他の高信頼通信に見合うセキュリティ強度を備えた** [選択：少なくとも 1 つを選択： IPsec、SSH、TLS、TLS/HTTPS] **を利用**しなければならない(shall)。

適用上の注釈： 本要件は、分散型 TOE のコンポーネント間のすべての通信が暗号化された通信チャネルの利用を通して保護されることを保証する。本高信頼通信チャネルで送信されるデータは、その選択で選ばれたプロトコルで定義されるように暗号化される。ST 作成者は、TOE によってサポートされるメカニズムを選択し、次に、それらの選択に対応する ND cPP の適切な要件が、まだ存在していなければ、ST に複写されることを保証する。
本要件の目的のため、セキュリティ強度は NIST SP 800-57 で定義されており、「commensurate（見合う）」とは、その強度が、最小限、本 EP で列挙された暗号化プリミティブの要件を満たさなければならない(must)ことを意味し、「other trusted communications（その他の高信頼通信）」とは、FPT_ITC で規定されるメカニズムを指す。

保証アクティビティ：

TSS

評価者は、分散型 TOE コンポーネントを保護するために利用される方法とプロトコルが記述されていることを決定するため、TSS を検査しなければならない(shall)。評価者は、また TOE 管理

のサポートにおいて TSS で列挙されるすべてのプロトコルが本要件で規定されるものと一貫しており、それらが ST の要件に含まれることについても確認しなければならない(shall)。評価者は、すべての方法を検査し、その強度が FCS_CKM、FCS_COP、及び選択されたプロトコル要件で記述された要件を満たすことを保証しなければならない(shall)。評価者は、各プロトコルによって利用される鍵／アルゴリズムの様々な強度を TSS が明確に識別していること、及びそのチャネルの全体的な強度が利用される強度の最低であることを示すことを保証しなければならない(shall)。

ガイダンス

評価者は、サポートされる方法のそれぞれについて、通信パス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)。

テスト

評価者は、次のテストについても実行しなければならない(shall)：

テスト 1： 評価者は、操作ガイダンスに記述されるとおり接続を設定し、通信が成功することを保証しつつ、それぞれの (操作ガイダンスで) 規定された通信方法を用いた通信が評価の過程においてテストされることを保証しなければならない(shall)。

テスト 2： 評価者は、それぞれの通信方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。

さらなる保証アクティビティが、具体的なプロトコルに対応する。

B.2 FCS_CKM.2(4) 暗号鍵配付

FCS_CKM.2.1(4) **詳細化：** TSF は、以下の：[**FCS_COP セキュリティ強度**] **及び暗号鍵を暴露しない** に合致する、指定された暗号鍵配付方法：[**FPT_ITT**] に従って **IEEE 802.11 の鍵**を配付しなければならない(shall)。

適用上の注釈：本要件は、IEEE 802.11 接続の成功に必要なあらゆる鍵に適用する (FCS_CKM.2.1(3) によってカバーされない)。ある鍵がその他のアクセスポイントに配付されなければならない(must)場合、この通信はそれに見合った暗号強度のメカニズムを介して実行されなければならない(must)。分散型 TOE のあらゆるコンポーネントとの通信は高信頼通信を介して実行されることが要求されるので、これらの鍵の配送は保護される。

保証アクティビティ：

TSS

評価者は、どの鍵が TOE の外部に配付されるか、どこに送信されるか、及びこの転送の目的について、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)。

ガイダンス

これがシステムの構成に依存する場合、評価者は、その鍵が適切に保護される設定方法についての指示が操作ガイダンスに含まれることを確認しなければならない(shall)。

テスト

本要件は、暗号プリミティブ、セキュアなプロトコル、及び FPT_ITT についてのテストと組み合わせてテストされる。

附属書 C – 選択ベースの要件

本 EP の概説で示すように、本 EP の本文には、ベースライン要件 (TOE または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) が含まれている。本 EP の本文中の選択に基づいた追加の要件がある；特定の選択がなされる場合、以下の追加の要件が含まれる必要がある。

現時点では、ND cPP の選択ベース要件から直接継承されないような選択ベース要件は識別されていない (例、FCS_HTTPS_EXT)。

附属書 D - オブジェクティブ要件

本 EP の概説で示すように、本 EP の本文には、ベースライン要件 (TOE または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) が含まれている。望ましいセキュリティ機能を規定するような追加の要件があり、このような要件が本附属書に含まれる。本 EP の将来のバージョンにおいて、これらの要件がオブジェクティブ要件からベースライン要件へ移行することが想定される。

現時点では WLAN AS の TOE に特有のオブジェクティブ要件は識別されていない。