無線ローカルエリアネットワーク（ＷＬＡＮ）
クライアントのプロテクションプロファイル

原文タイトル：

Protection Profile for Wireless Local Area Network (WLAN) Clients

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。
http://www.niap-ccevs.org/pp/pp_wlan_cli_v1.0.pdf

Information Assurance Directorate

情報保証局

2011 年 12 月 19 日
バージョン 1.0

平成 24 年 9 月 18 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

目次

表一覧

図一覧

改定履歴

バージョン	日付	内容
1.0	2011 年 12 月	初版

1　PP 序論

1 本プロテクションプロファイル(PP)は、ワイヤレスネットワーク上のセンシティブ且つ無分類のデータ保護のための市販（COTS）のワイヤレスローカルエリアネットワーク（WLAN）クライアントの購買をサポートする。本PPでは、WLAN及びそのサポート環境における方針、前提条件、脅威、セキュリティ対象、セキュリティ機能要件、セキュリティ保証要件について詳細を述べる。

2 主な意図は、WLANクライアントにより示されている脅威に対抗する必要があるセキュリティ機能要件の我々の理解を開発者に明確に伝えることである。 STのTOE要約仕様（TSS）の記述は、製品（評価対象）のアーキテクチャと重要なセキュリティ業務が正しく実行されていることを保証するために使用されるメカニズムを記載することが期待されている。

1.1 TOE の PP 概要

3 本書はWLANクライアントのセキュリティ機能要件について説明する。本PPにより定義するTOEは、WLANクライアントで、クライアントマシン（通常「リモートアクセスクライアント」と呼称）にて実行するコンポーネントである。TOEはクライアントデバイスとWLANアクセスシステムとの間にセキュアワイヤレストンネルを構築し、これにより全データが送信される。WLANアクセスシステムは承認されたクライアントのみが認証サーバにより認証されアクセス可能となることを確実とする。本PPの目的として、有線ネットワークへの一般ワイヤレス設定について議論する。しかし、本PPの要件を満たすものとして存在し得るその他のワイヤレス設定を排除することを意図としていない。本PPはいかなる特定の設定を要求するものではない。その代わり、本PPはワイヤレスユーザ、有線ネットワーク、及びその資源間の通信を供給するクライアントのセキュリティ要件に対処する。後述のセクションにて議論するとおり、PPがWLANクライアント及びその管理機能のみの機能性を網羅することを強調することが重要である。ここでは識別及び認証、監査記録のようなIT環境で実装される要件を課さない。例えば、これらの機能は、一般的な目的用OSを特定した要件に適合しなければならない（should）。

4 WLANクライアントはIEEE 802.1Xポートベースネットワークアクセス制御に対応する。ポートベースのアクセス制御のフレームワーク構造は３つの役割を定義する：サプリカント（TOE）、オーセンティケータ（WLAN Access System)、認証サーバ(AS)である。WLAN アクセスシステムはネットワークアクセスを供給する前に、TOEの認証をASに依存し、TOEの認証を要求する。WLANアクセスシステムはTOEとAS間のデバイスパスの役割をする。WLANアクセスシステムは、WLANクライアントがASにより認証された場合のみプライベートネットワークにアクセスすることを許可する。TOE及びASは、X.509 v3 証明書及び拡張認証プロトコルトランスポートレイヤーセキュリティ(EAP-TLS) メッセージを使用して相互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停止する。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に成功した場合のみ構築される。

1.1.1 TOE の用途及び主なセキュリティ機能

5 WLANクライアントにより、遠隔利用者はクライアントマシンを利用してプライベートネッ

6

トワークとのワイヤレス通信を構築することができる。プライベートネットワークとリモートアクセスWLANクライアント間をパスするIPパケットは暗号化されている。WLANクライアントは、ワイヤレス接続でありながら、送信中データの機密性、完全性及び保護を供給することにより、プライベートネットワークとの間のデータを保護する。

本PPのセキュリティ機能要件の中心となるのは、下記に示すWLANクライアントの基本事項である:

- WLANクライアントの認証
- 認証サーバの認証
- 送信データの暗号化による保護
- サービスの実行

7 WLANクライアントは、認証用にEAP-TLSを使用したIEEE 802.1Xにより、クライアントデバイスとネットワークインフラストラクチャ間に 802.11 トンネルを構築する。これにより EAP-TLS 変換の一部としてプライベートネットワークのASに対し、相互認証を行う。EAP-TLS変換は相互認証用にマシン証明書を利用する。WLANクライアントは、ASより送信されたマシン証明書を検証し、妥当性の確認を行い、信用できる認証機関(CA)による署名が行われているかを確認する。ASはWLANクライアント証明書を同時に認証する。EAP-TLS変換に成功すると、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を構築完了することを許可する。WLANクライアントはIEEE 802.11 に定めるとおり、 4 ウェイハンドシェイクを使用して、WLANアクセスシステムへの暗号化、認証されたチャネルを設定する。チャネルが構築されると、IEEE 802.11 に定めるとおり、WLANクライアントとWLANアクセスシステム間のすべての通信はCCMPモードのAESにより暗号化される。

8 WLANクライアント (図 1)は本PPにて定義するとおり、リモートアクセスクライアントマシンに対して実行するコンポーネントである。クライアントがWLANクライアント "マシン"の小さな一部として描写されていることに注意。このように、TOEは実行ドメイン及び適切な使用について、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、OS)に大いに依存しなければならない(must)。 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。

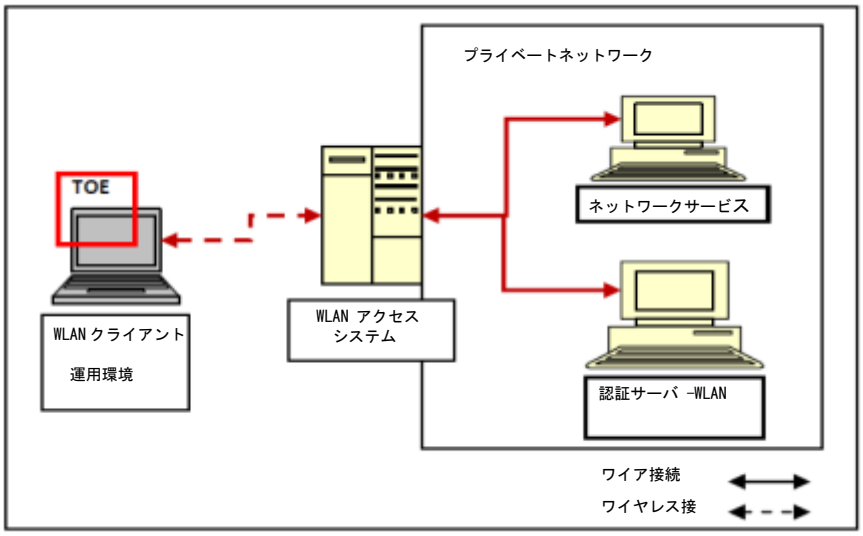

図 1： WLAN クライアント

9 WLANクライアントが適正に実行され重要な設計ミスのないことが前提とされる。TOEのセキュリティ機能には、管理、プロトコル適合、暗号化保護、監査生成が含まれる。WLANクライアントは適正な実行及び以下のクライアントマシン保護メカニズムにおいて、IT環境に依存する：監査レビュー、監査記録、認識及び認証、セキュリティ管理、セッション管理。ベンダはクライアントマシンをインストール及び管理するための設定ガイダンス(AGD_PRE, AGD_OPE)、及びすべての対象となる運用環境用のTOEを供給することが要求される。

1.1.2 暗号

10 WLANクライアントは、送信データの機密性、完全性、保護を供給するため、暗号化機能に依存する。WLANクライアントは、地理的に離れた 2 台のデバイス間におけるワイヤレストラフィックを暗号化することが前提とされている。WLANクライアントはWLANトンネルの終点となり、トンネルの構築及び維持に関係する暗号化機能を行う。標準プロトコル及びアルゴリズムを使用し、WLANクライアントは、ワイヤレスネットワークを移動する場合でも各メッセージが保護されていることを確実とする。CCMPモードにおけるAESアルゴリズムが送信中のデータ保護のために利用される。CCMP モードは２つのブロック暗号モードの組み合わせに基づく - カウンターモードは機密性を供給し、メッセージ認証子生成方式(CBC-MAC)によりデータの完全性を供給する。

11 認証、鍵生成、情報の暗号化に使用した暗号方式が十分に強固なものであり、実装において重大な設計ミスがない場合、攻撃者はワイヤレスデータを取得する暗号鍵空間を使用することができない。IEEE802.11 及びIEEE802.1X規格に定めるWPA2 の遵守、ランダムビット生成 (RBG)の適正な設定、及びセキュアな認証要因により、送信された情報が鍵空間を完全に使い切る以外の作業により取得することができないことを保証する。いかなる平文の

秘密鍵、プライベート鍵またはその他の暗号化されたセキュリティパラメタも、すでに使用されていない場合ゼロ化され、重要な機密データの暴露を防止する。

12

1.1.3 TOE 管理及び IT 環境

TOEの対応環境は重要である。ほとんどすべての場合において、TOEは一般目的のOSにおいて実行される純粋なソフトウェアソリューションである。したがって、TOEはその実行ドメイン及び適正な使用のため、TOEの運用環境 （システムハードウェア、ファームウェア、OS）に大いに依存しなければならない(must)。ベンダは必要機能を持つ運用環境を認識するための十分なインストール／設定要領及び正確な構成を供給することが前提となる。

13

TOEは特定の管理アクティビティ（要件で定められる）がTOEの許可された利用者のサブセットにより実行されることを要求する。 本PPはTOEが、これらの管理機能を管理の役割に制限する認証能力を識別、認証することを要求しない。つまりTOEベンダが遵守できる方法は多数存在する。例を以下に挙げる。

1. TOEは、許可された管理者の概念を含まないため、管理ユーティリティを呼び出すことができる場合、誰でもTOEを構成することができる。 この場合、PPを遵守するために、TOEの許可された利用者のサブセットだけが管理ユーティリティを実行することができるように、管理者が作業環境を構成するために使用する手順を詳述するAGD_OPE/PREガイダンスの一部として、TOEベンダは指示書を提供しなければならない(must)。例えば、管理者として許可された利用者だけが管理ユーティリティを実行することができるように、ガイダンスは運用環境でアクセス制御メカニズムを設定することを記述する。 このケースは本PPのベースライン要件を反映する。
2. TOEは、許可された管理者（または管理者グループ）の概念を含むが、識別、認証機能の実行は運用環境に依存し、許可された管理者の内部TOEに適合できるTOEに何等かの表示をパスする。このケースでは、STは要件を拡張し（附属書Ｃのテンプレートを使用）、TOEにより供給される能力を指定する必要がある。ベンダはTOEに情報をパスさせるための運用環境の構成または設定について説明する必要がある。
3. TOEは、ハードディスクを収納しているシステムのどの利用者がTOEにより提供される管理機能を使用する許可を与えられるかについて決定するために用いられる識別、認証能力を含む。 この場合、ST執筆者は、この機能を指定するためにSTの附属書Cで提供されるI&Aテンプレート情報を使う必要がある。

1.1.4 プロトコル適合

14

本PPに適合するTOEはWi-Fi Protected Access 2 (WPA2)に適合しなければならない(shall)。具体的には、WPA2 基準に定義されるとおりTOEはAES- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) を使用する。IEEE 802.1X がポートベースのアクセス制御アクセス制御に使用される。つまりクライアントは拡張認証プロトコルトランスポートレイヤーセキュリティ (EAP-TLS)によりワイヤレスクライアントと認証サーバ間の相互認証を行うことが前提とされる。EAP-TLSプロトコルはRFC 5216で定めるとおり、X.509 v3 証明書を使用するよう設定される。

2　セキュリティ課題記述

15 本PPは、エンティティがプライベートネットワークにワイヤレスでアクセスする場合の状況について記述する。プライベートネットワークへのアクセス許可をするには、エンティティ（マシン）が、セキュアな通信チャネルが構築される前に認証されなければならない(must)。TOEは、保護されたネットワークにアクセスすることを認証されることを意図するエンティティであり、IEEE 802.1Xフレームワークのサプリカントである。

16 WLANクライアントの適正なインストールと設定は正確な運用をするために重要である。これには管理者によるTOEの適正な取扱いを含む。

本章は以下の内容を認識する。

17

- WILANクライアントによる組織に対するIT関連の脅威
- 十分な保護を行うための管理が要求される環境脅威
- 適正なWLANクライアントのための組織のセキュリティ方針
- WLANクライアントの運用環境に対する重要な前提条件

2.1 脅威

18 本PPはインサイダーの脅威を保護できる要件を含まない。許可された利用者は敵対的、または悪意があると考慮されず、適切なガイダンスに従うことを一任される。許可された人員だけが、クライアント装置へアクセスできるべきである(should)。したがって、本PPの要件により示される主要な脅威エージェントは、保護されたネットワークにアクセスしようとする許可されていないエンティティである。このように彼ら自身をネットワークの合法的な利用者として確立しているネットワークに彼ら自身が認証することができるならば、エンティティは認可される。合法的なエンティティのネットワークアクセス要求と認証証明書の認証がワイヤレスネットワーク上で行われるため、それは攻撃の対象となり、暴露及び改ざんから保護されなければならない(must)。悪意のあるエンティティは合法的なWLANアクセスシステムに偽装することができ、たとえば結果としてクライアントデータや認証証明書の危殆化を引き起こす可能性がある。

ワイヤレス通信の使用は、新しい攻撃手口をネットワークにもたらす。攻撃者は保護された施設の範囲を破ったり、またはクライアント装置に接近することなくワイヤレス攻撃を開始したりすることができる。信号妨害とサービス不能攻撃は、一般的で、妨ぐのが困難である。これらの脅威は本PPにおける要件で網羅されていないため、ネットワークの有効性に対する前提条件がこれらに対処するために存在する。しかし、ワイヤレス通信を保護するのにその他のメカニズムを用いることができる。セキュリティ方針の不適切なネゴシエーションまたはワイヤレス接続を構築するために弱いプロトコルオプションを実施することは、利用者とTSFデータの暴露または改ざんという結果を招くと懸念される。攻撃者がワイヤレストラフィックを「盗聴する」のを防ぐことは不可能だが、プロトコル相互接続性と強い暗号化を要求する相互の同意を得るセキュリティ方針は、ワイヤレスLAN保護を構築するために不可避である。

20 その他の脅威エージェントは資源が再配分されるときに消去されないセキュリティ関連した情報を含む。 センシティブであることがもはや必要でない場合、このデータへのアクセスは妨げられなければならない(must)。TOEは残りのデータが適切に取り扱われ、使用後はセキュリティ関連の情報が他の利用者/プロセスによりアクセスできないことを確実にしなければならない。TSFの危殆化は認証データ、セッション鍵、役割／利用者情報、セキュリティメカニズム、TOEが保護するデータを含む。TOEまたはTSFデータは不正なアクセス及び更新から保護されなければならない(must)。

21 ネットワーク攻撃（例えば上記のTOEに対する攻撃）は、無許可のアクセス及びセキュリティの危殆化を発生させる唯一の原因ではない。製品を更新することは、脅威環境への変化が対処されることを確実とする一般的かつ必須の能力である。使われる一般の攻撃は、欠陥を持つソフトウェアのパッチを当てられていないバージョンの攻撃を含む。パッチをタイムリーに適用することにより、製品がセキュリティ方針を強化、維持できる可能性を高める。しかし、最新版は信用できる源からのものでなければならない。そうでない場合、攻撃者自身が、独自に選ぶ悪質なコードを含む「最新版」（例えばルートキット、ボットまたは他のマルウエア）を書くことが可能になるからである。

22 アクセスを得るメカニズム（ネットワーク攻撃、悪質なコード、設定エラーの利用、セッションハイジャックなど）にかかわらず、一旦攻撃者がアクセスを得ると、TOEとそのデータは危険にさらされる。TOE上でさらなる不正行為を隠すために監査記録生成を改ざんすることは、潜在的な問題を隠すだけでなく、悪意のあるアクションを引き起こした人物の特定を困難にする可能性がある。検知されないアクションは、TOEのセキュリティに悪影響を与え、引き起こされる問題を軽減することを困難にする可能性がある(may)。監査レビューとストレージはIT環境によって取り扱われるため、本PPの範囲外であることに注意すること。 しかし、これがTOE保護のために適切及びセキュアに実行されることが想定される。

23 以下の表は、WLAN クライアント及び運用環境により対処される脅威リストである。以下で認識されるすべての脅威において想定される攻撃者の専門技術レベルは、高度ではない。

表 1：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が失敗しTSFの危殆化を引き起こす可能性がある。(may)
T.UNAUTHORIZED_ACCESS	利用者はTOEデータ及びTOE実行可能コードへの実行可能ファイルコードを得る可能性がある(may)。データまたはTOE資源への実行可能ファイルコードを得るために、悪意のある利用者、プロセスまたは外部のITエンティティは認証されたエンティティに偽装する可能性がある(may)。悪意のある利用者、プロセスまたは外部のITエンティティは、識別と認証データを得るTOEとして偽る可能性がある。
T.UNAUTHORIZED_UPDATE	悪意のある利用者が最終利用者にTOEのセキュリティ機能を危殆化する可能性のある製品の更新供給を試みる。
T.UNDETECTED_ACTIONS	悪意のある遠隔利用者または外部のITエンティティは、TOEのセキュリティに悪影響を与える措置を取る可能性がある。これらのアクションは検知されずに維持する可能性がある。したがってこの影響を効果的に軽減することができない。
T.USER_DATA_REUSE	利用者データは、最初の送信者によって意図されない送信先に、不注意に送られる可能性がある(may)。

2.2 組織のセキュリティ対策方針

24

組織のセキュリティ対策方針は、プライベートネットワークとパブリックネットワーク間の境界線を越えるネットワークパケットを保護するため、適用性により選定される。手順に関する方針も、前提条件として記載されている。 正式な参照を持たない方針は、方針記述により作成及び正式化されることが期待される。

表 2：組織のセキュリティ対策方針

対策方針	対策方針の説明
P.COMPATIBILITY	TOEは、同じプロトコルを使用して他のネットワーク設備との相互接続性を実現するため、実装されたプロトコルに対するRequest for Comments (RFC)要件を満たさなければならない(must)。
P.CONFIGURABILITY	TOEは、運用のセキュリティ関連の設定を行う機能を提供しなければならない(must)。

2.3 前提条件

25 セキュリティ問題を定義する本節では、セキュリティ機能を提供するための運用環境に関する前提条件を示す。TOEがこれらの前提条件に満たない運用環境にある場合、TOEはそのセキュリティ機能の全てを提供することができない場合がある（may）。前提条件は、運用環境の物理的環境、人員、接続性に関するものである。

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TOEを通過せずにワイヤレスクライアントとインターナル有線ネットワーク間を行き来できない。
A.PHYSICAL	TOE及びそれが含むデータの価値に相当する物理的なセキュリティは、環境によって提供されると想定される。
A.TRUSTED_ADMIN	TOE管理者は信頼された方法ですべての管理者ガイダンスに従って、適用するものと信頼される。

3　セキュリティ対策方針

26 セキュリティ対策方針は、評価対象（TOE）及び脅威から派生する運用環境、組織のセキュリティ対策方針、及び第 2 節で述べた前提条件のための要求である。 第 4 節は、TOE、より正式にはSFRのためのセキュリティ対策方針について再述する。TOEはSFRに対して評価される。

3.1 TOE のセキュリティ対策方針

27 表 4 はTOEのセキュリティ対策方針を示す。これらのセキュリティ対策方針は識別された脅威に対処する及び／または識別されたその他の組織のセキュリティ対策方針を遵守するために記述された意図を反映する。TOEはこれらの対策方針に対し、セキュリティ機能要件を満たすことにより適合する。

表 4：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、認証されたアクセスポイントであると偽るエンティティとでなく、実際に認証されたアクセスポイントと通信していることを確実とする手段を提供し、そのアクセスポイントに対し保証を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS	TOEは、機密性を維持するために暗号化機能（暗号化/復号と電子署名操作）を提供し、TOEとそのホスト環境の外側に送られるデータ改ざんの検知を許可する。
O.PROTOCOLS	TOEは、相互接続性を保証するために、RFC及び/又は工業仕様書に従って、標準化されたプロトコルがTOEに実装されていることを保証する。
O.RESIDUAL_INFORMATION_CLEARING	TOEは、資源が再割当された場合、保護された資源に含まれるデータが使用できないことを保証する。
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を設定できるメカニズムを提供する。
O.TSF_SELF_TEST	TOEは、適正に動作していることを保証するために、セキュリティ機能のサブセットをテストする機能を提供する。
O.VERIFIABLE_UPDATES	TOEは、TOEに対する更新が管理者によって変更されていないこと、及び（任意で）信用できるソースから検証できることを保証することを手伝う機能を提供する。
O.WIRELESS_ACCESS_POINT_CONNECTION	TOEは接続するワイヤレスアクセスポイントを制限する能力を提供する。

3.2 運用環境に対するセキュリティ対策方針

28 TOEの運用環境は、そのセキュリティ機能（TOEのためのセキュリティ対策方針によって定

義される）を正しく提供することをTOEがサポートするための技術的かつ手続き的な処置を実行する。この部分的な解決は運用環境のためのセキュリティ対策方針と呼ばれており、運用環境が達成しなければならないゴールを示した一連の記述で構成される。

29 本節は、IT領域または、非技術的であるか手続き的な手段で対処されるセキュリティ対策方針を定める。第 2.3 節で識別される前提条件は、環境のためのセキュリティ対策方針として統合される。それは環境に更なる要件を賦課し、主に手続き的または管理的な処置により適合される。表 5 は、環境のためのセキュリティ対策方針を識別する。

表 5：運用環境のため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	TOEを経由せず異なる場所にある外部ネットワークと内部ネットワーク間で情報を送受信することはできない。
OE.PHYSICAL	TOEの値とそれが含むデータに相応した物理的なセキュリティは、運用環境によって提供されると想定される。
OE.TRUSTED_ADMIN	TOE管理者は信頼された方法によりすべての管理者ガイダンスに従い適用するものと信頼される。

3.3 セキュリティ対策方針根拠

30 本節では第 2 節に定義したセキュリティ対策方針の根拠を記載する。表 6 はセキュリティ対策方針から脅威、方針に至るまでのマッピングを示す。

表 6：脅威及び方針に対するセキュリティ対策方針マッピング

脅威／方針	脅威／方針に対応する対策方針	根拠
T.TSF_FAILURE TOE のセキュリティメカニズムに失敗し、TSF の危殆化を招くことがある(may)。	O.TSF_SELF_TEST TOE はセキュリティ機能のサブセットをテストする能力を提供し、適切な運用を確実とする。	O. TSF_SELF_TESTはTSF の正しい動作を正常に実証するために、TSFがセルフテストスイートを実行することを保証することで、この脅威に対抗する。
T.UNAUTHORIZED_ACCESS 利用者は TOE データ及び TOE 実行可能コードに対する非認証のアクセスを得ることができる(may)。悪意のある利用者、プロセス、ま	O.AUTH_COMM TOEは、認証アクセスポイントと偽装したエンティティではなく、実際に認証されたアクセスポイントと通信していることを確証する手段を提供し、そのア	O.AUTH_COMMは、 TOEはそのアクセスポイントと通信する前にすべてのアクセスポイントを確認し、認証することによりこの脅威を軽減する。TOEはまた、通信前に相互認証を確実に

脅威／方針	脅威／方針に対応する対策方針	根拠
たは外部のITエンティティは認証されたエンティティに偽装してデータやTOE資源に対する実行可能ファイルを得る可能性がある(may)。悪意のある利用者、プロセス、または外部のITエンティティはＩＤ及び認証データを獲得するため、偽装することがある(may)。	クセスポイントの保証を提供する。 O.CRYPTOGRAPHIC_FUNCTIONS TOEは暗号化機能(暗号化／復号及び電子署名操作)を持ち、機密性を維持し、物理的に離れた場所にある、またはTOEの外側にあるデータ間で送信されるTSFデータ改ざんの検知を許可しなければならない(shall)。 O.TOE_ADMINISTRATION TOEは管理者がTOEを設定できるメカニズムを提供する。 O.WIRELESS_ACCESS_POINT_CONNECTION TOE は接続するワイヤレスアクセスポイントを制限する能力を提供する。	するためにアクセスポイントに自身の証明書を送ることができなければならない(must)。 O.CRYPTOGRAPHIC_FUNCTIONSは、他の保護メカニズムで必要な基礎となる暗号化機能を提供することによりこの脅威を軽減することに貢献する。 O.TOE_ADMINISTRATIONは、TOEがセキュアな方法で設定されるメカニズムを提供することを要求する。 O.WIRELESS_ACCESS_POINT_CONNECTIONは、TOEが接続することのできるアクセスポイントを制限するメカニズムを提供することにより、脅威を軽減する。
T.UNAUTHORIZED_UPDATE 悪意のある利用者が、TOEのセキュリティ機能を危殆化するおそれのある更新を最終利用者に供給しようと試みる。	O.VERIFIABLE_UPDATES TOEは、すべての更新が改ざんされておらず（任意で）信用のおけるソースからのものであることを管理者が確認できる能力を提供する。	O.VERIFIABLE_UPDATESは管理者が更新を確認できることを確実とする。
T.UNDETECTED_ACTIONS 悪意のある遠隔利用者または外部のITエンティティがTOEのセキュリティに悪影響をもたらすアクションをとる可能性がある(may)。これらのアクションは検知されず、効果的に軽減することができない。	O.SYSTEM_MONITORING TOE は監査データの生成能力を提供する。	O.SYSTEM_MONITORINGは、管理者が監査メカニズムを設定し、多数の基準に基づいてアクションを記録する能力を提供することにより、この脅威を軽減する。
T.USER_DATA_REUSE 利用者データは、最初の送信者によって意図されない送信先に、不注意に送られ	O.RESIDUAL_INFORMATION_CLEARING TOEは、保護資源に含まれるすべてのデータは資源が再配置され	O.RESIDUAL_INFORMATION_CLEARINGは、資源がある利用者／プロセスによりリリースされ別の利用者／プロセスにより再

脅威／方針	脅威／方針に対応する対策方針	根拠
る可能性がある(may)。	ると入手不可能となることを確実とする。	配置された場合、TSFデータ及び利用者データが継続するものでないことを確実とすることにより、この脅威に対応する。
P.COMPATIBILITY TOE は実行されたプロトコルに対し、同じプロトコルを使用する他のネットワーク機器との相互操作を容易にするため、Request for Comments (RFC) の要件を満たさなければならない(must)。	O.PROTOCOLS TOE は、相互接続性、また集中監査サーバ及びRADIUS認証サーバとの通信をサポートすることを確実にするために、標準化されたプロトコルが TOE にて RFC や産業仕様に実行されることを確実とする。	O.PROTOCOLSは、標準化されたプロトコルがTOEに実行され、ITエンティティ間で同じプロトコルを使用して相互接続性を確実にすることを要求することにより、この方針を満たす。
P.CONFIGURABILITY TOEは､運用のセキュリティ関連の設定を行う機能を提供しなければならない(must)。	O.TOE_ADMINISTRATION TOEは管理者がTOEを設定できるメカニズムを提供する。	O.TOE_ADMINISTRATIONは、TOEがセキュリティ設定に必要とされるメカニズムを提供することにより方針を満たす。

31 表 7 はセキュリティ対策方針から前提条件までの対応関係を示す。

表 7：セキュリティ対策方針から前提条件までのマッピング

前提条件	前提条件に対応する対策方針	根拠
A.NO_TOE_BYPASS 情報は TOE を経由せずワイヤレスクライアントと内部の有線ネットワーク間を行き来できない。	OE.NO_TOE_BYPASS 情報は TOE を経由せずに異なる場所に位置する外部及び内部ネットワーク間を行き来できない。	OE.NO_TOE_BYPASSは、すべての外部／内部ネットワーク間を行き来する情報がTOEを経由することを確実とする。
A.PHYSICAL TOE の値とそれが含むデータに相応した物理的なセキュリティは、環境によって提供されると前提条件される。	OE.PHYSICAL TOE の値とそれが含むデータに相応した物理的なセキュリティは、運用環境によって提供されると前提条件される。	OE.PHYSICALは、TOE、TSFデータ、及び保護された利用者データが物理的な攻撃（窃盗、改ざん、破壊、盗聴など）から保護されることを確実とする。物理的攻撃にはTOE環境に対する非認証の侵入を含むが、TOE環境に認証された個人による破壊行為は含まれない。

前提条件	前提条件に対応する対策方針	根拠
A.TRUSTED_ADMIN TOE 管理者は信用のおける方法ですべての管理者ガイダンスに従いこれを適用することを一任される。	OE.TRUSTED_ADMIN TOE 管理者は信用のおける方法ですべての管理者ガイダンスに従いこれを適用することを一任される。	OE.TRUSTED_ADMINは、管理者が適切に訓練を受け、管理者ガイダンスが管理者に対し環境及びTOEを適切に設定する方法を指示し、間違いを防ぐことを確実とする。

4　セキュリティ要件及び根拠

32 セキュリティ要件は、機能的要件と保証要件に分けられる。 SFRはセキュリティ対策方針の正式な例示で、第 4.1 節に適用上の注意を示す。それらは通常抽象概念のより詳細なレベルにあるが、完全翻訳でなければならない（セキュリティ対策方針が完全に対応されなければならない）。CCは、いくつかの理由により、標準化された言語への翻訳を要求する：

●評価対象の正確な記述を提供するため、TOEのセキュリティ対策方針は通常、自然言語で述べられているため、標準化された言語へ翻訳することによりTOEの機能のより正確な記述を強化できる。

●２つのSTの比較を行うことができるため。異なるST執筆者はセキュリティ対策方針について異なる用語を使用する可能性があるため、標準化された言語を使用することにより同一の用語、概念の使用を強化することができる。これにより比較が容易になる。

33 セキュリティ保証要件（SAR）は一般的に、挿入されSFRとは別にリストされる常用文である。また、共通評価方法（CEM）は、選定されたSARに基づき評価される間に参照される。 本PPではよりカスタマイズされたアプローチが、標準プロテクションプロファイルのニューモデルに基づき行われる。SARは第 4.3 節で文脈と完全さのためにリストアップし、評価者が各々のSFRとSARに関してこのTOEのために行う必要があるアクティビティは「保証アクティビティ」の段落で詳述する。 保証アクティビティは、評価を完了させるためにおこなわなければならないアクティビティの規範的な説明である。 保証アクティビティは、本PPで２カ所に記載される。特定のSFRと関係するものは第 4.1 節に記載、SFRから独立しているものについては第 4.3 節で詳述する。

34 直接SFRと関連するアクティビティについては、各SFR後、１つ以上の保証アクティビティがリストされ、このテクノロジーに対して提供される保証を達成するために実行される必要があるアクティビティを詳述する。

35 SFRから独立しているアクティビティを必要とするSARについては、第 4.3 節でSARに関連した特定の保証アクティビティが書かれたSFRへのポインタと共に、達成されるべき追加の保証アクティビティについて示す。

36 将来のプロテクションプロファイルでは、実際の製品評価から学んだ教訓に基づいて、よ

り詳細な保証アクティビティが提供される。

37

4.1 セキュリティ機能要件

本節では、TOEにより提供されるセキュリティ機能に特有であるTOEに対するSFRを識別し、WLANクライアントと他のTOEを区別する。 SFRの重点分野は、監査、暗号、セキュリティ管理、セルフテスト、及び許可された外部ITエンティティ（WLANアクセスシステム、認証サーバなど）との通信に関連する。

表 8：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_GEN.1 監査データ生成
	FAU_SEL.1 選択的監査
暗号化サポートクラス（FCS）	FCS_CKM.1 暗号鍵生成（対称鍵）
	FCS_CKM.2 暗号鍵配送（GTK）
	FCS_CKM_EXT.4 暗号鍵破棄
	FCS_COP.1(1) 暗号操作（データ暗号化／復号）
	FCS_COP.1(2) 暗号操作（暗号署名）
	FCS_COP.1(3) 暗号操作（暗号ハッシュ）
	FCS_COP.1(4) 暗号操作（鍵付きハッシュメッセージ認証）
	FCS_COP.1(5) 暗号操作（WPA2 データ暗号化／復号）
	FCS_EAP-TLS_EXT.1 拡張：拡張認証プロトコルトランスポートレイヤーセキュリティ （EAP-TLS）
	FCS_RBG_EXT.1 拡張: 暗号操作（ランダムビット生成）
利用者データ保護クラス(FDP)	FDP_RIP.2 全残存情報保護
認識及び認証クラス(FIA)	FIA_8021X_EXT.1 拡張： 802.1X ポートアクセスエンティティ（サプリカント）認証
	FIA_X509_EXT.1 拡張: X.509 証明書
セキュリティ管理クラス(FMT)	FMT_SMF.1 管理機能仕様書
TSF 保護(FTP)	FPT_TST_EXT.1 拡張: TSFテスト
	FPT_TUD_EXT.1 拡張: 高信頼更新
TOE アクセス(FTA)	FTA_ WSE_EXT.1 拡張: ワイヤレスセッション構築
高信頼パス／チャネル(FTP)	FTP_ITC.1 TSF間高信頼チャネル

4.1.1 クラス: セキュリティ監査(FAU)

セキュリティ監査データ生成(FAU_GEN)

FAU_GEN.1　　監査データ生成

FAU_GEN.1.1　TSFは下記の監査事象の監査記録を生成しなければならない（shall）。

a) 監査機能の起動及び終了
b) 監査の指定なしのレベルに対するすべての監査対象事象
c) すべての管理アクション
d) [*表９にリストされる特別に定義される監査事象*].

適用上の注意：

38 *ST執筆者は、他の監査対象事象を表に含めることができる。なお、これらは提示されるリストに制限しない。*

39 *a)の場合、参照される監査機能は、TOEにより提供される。 たとえば、TOEが実行可能スタンドアロンであった場合には、TOE自体の起動及び終了を監査することはこの条項の要求を満たすのに十分である。*

40 *本書に含まれるSFRの監査可能な側面の多くが管理アクションに対応する。 上記の c）はすべての管理アクションが監査可能であることを要求するため、これらのアクションの監査能力に関する追加の仕様は表９に提示しない。TOE自体が管理者のためにI&Aを実行する能力を提供する必要はないが、本要件はTOEがPPによって「管理アクション」（主にTOEにより提供される機能の設定について）と評される事象を監査する能力を備えていることを意味する。TOEによって生成される監査データが根底にあるIT環境の監査能力を備えていることを確実とするために必要なステップを、OPEガイダンスが詳述することが前提となる。*

保証アクティビティ：

41 *評価者は操作ガイダンスを確認し、それが監査対象事象の全てをリストアップし、監査記録用のフォーマットを提供することを確実とする。各フィールドの簡潔な説明に加え、各監査記録フォーマットのタイプが網羅されていなければならない。(must) 評価者は、PPによって命令されるあらゆる監査事象タイプが記述され、フィールドの説明がFAU_GEN.1.2で要求される情報と表９で指定された追加情報を含むことを確認する。*

42 *評価者は特に、失敗した暗号化事象の内容に関して操作ガイダンスが明確になっていることを確実としなければならない。表９では、操作の暗号化モードを詳述している情報及び暗号化されている対象の名前及び識別子が要求される。 評価者は、名前または識別子が、監査ログをレビューする管理者が暗号化操作のコンテクスト（データ暗号化の際に行われる鍵ネゴシエーション・交換など）、及び他のＩＴシステムとの通信に関して暗号化失敗に対する非TOEのエンドポイントの接続を決定することができるのに十分であることを確実とする。*

43 *評価者は、本PPのコンテクストで関連する管理アクションの決定も行わなければならない。(shall) 機能性はSFRで指定されていないため、TOEは本PPのコンテクストで評価されない機能を含むことがある。この機能性は、操作ガイダンスで記述される管理的側面を持つことがある。そのような管理アクションがTOEの評価された設定で実行されないため、評価者は操作ガイダンスを検証し、PPで指定される要求を強化するために不可欠なサブコマンド、スクリプト及び設定ファイルを含むどの管理コマンドが、TOEに実装されるメカニズムの設定（実行の可否を含む）に関連するかを決定しなければならない(shall)。これにより「す*

べての管理アクション」が形成される。評価者はこのアクティビティを AGD_OPEガイダンスが要求を満たすことを確実とするためのアクティビティの一部として行うことができる。

44 *評価者は、本PPの機能要件に関連する保証アクティビティに従い、TOEに監査記録を生成させることによりTOEの正確な監査記録生成能力をテストする。また、評価者は本PPのコンテクストで適用できる各管理アクティビティが監査可能であることをテストする。テスト結果を確認するとき、評価者はテスト中に生成される監査記録が管理ガイドで指定されたフォーマットにマッチし各監査記録のフィールドには適当なエントリがあることを確実としなければならない(shall)。*

45 *直接セキュリティメカニズムをテストすることに関連してテストを達成することに注意する。 たとえば、提供される管理ガイダンスが正しいことを確認するためのテストは AGD_OPE.1 が満たされていることを確認し、監査記録が予想通りに発生することを確かめるために必要である管理アクションの実行に対応すべきである(should)。*

FAU_GEN.1.2	TSFは各監査記録に少なくとも以下の情報を記録しなければならない。(shall) a) 事象の日時、事象のタイプ、サブジェクトの識別、事象の結果（成功／失敗） b) 各監査タイプに対し、PP/STに含まれる機能コンポーネントの監査対象事象定義に基づく情報［*以下の表の３列目に示す情報*］

適用上の注意：

46 *前回のコンポーネントとして、ST執筆者は生成された追加情報を表９に更新しなければならない(should)。要件における「サブジェクトＩＤ」とは、たとえば管理者のＩＤまたは影響するネットワークインタフェースとなる。*

保証アクティビティ：

47 *本アクティビティはFAU_FEN.11 のテストに関連して達成すべきである(should)。*

表 9：監査対象事象

要件	監査対象事象	追加の監査記録内容
FAU_GEN.1	なし	
FAU_SEL.1	監査収集機能の作動中に起こる監査設定に対するすべての変更	なし
FCS_CKM.1	鍵生成アクティビティの失敗	なし
FCS_CKM.2	鍵配送アクティビティの失敗	なし
FCS_CKM_EXT.4	鍵廃棄プロセスの失敗	クリアされる対称またはエンティティの識別

要件	監査対象事象	追加の監査記録内容
FCS_COP.1(1)	暗号化または復号の失敗	暗号化操作モード、暗号化／復号される対象の名前／拡張子
FCS_COP.1(2)	暗号署名の失敗	暗号化操作モード、署名／確認される対象の名前／拡張子
FCS_COP.1(3)	ハッシュ機能の失敗	暗号化操作モード、ハッシュされる対象の名前／拡張子
FCS_COP.1(4)	非データ統合に対する暗号化ハッシュの失敗	暗号化操作モード、ハッシュされる対象の名前／拡張子
FCS_COP.1(5)	WPA2 暗号化または復号の失敗	暗号化操作モード、暗号化／復号される対象、接続の非TOE終点（IPアドレス）の名前／拡張子
FCS_EAP-TLS_EXT.1	プロトコルの失敗 認証の失敗	失敗の原因 成功／失敗両方の場合の接続の非TOE終点（IPアドレス）
FCS_RBG_EXT.1	ランダム化プロセスの失敗	なし
FDP_RIP.2	なし	
FIA_8021X_EXT.1	802.1Xコントロールポートへのアクセスの試み	提供されるクライアントＩＤ（IPアドレス）
FIA_X509_EXT.1	なし	
FMT_SMF.1	なし	
FPT_TST_EXT.1	TSFセルフテスト一式の実行 検知された統合違反	統合の違反については、違反の原因となったTSFコードファイル
FPT_TUD_EXT.1	更新の開始 更新統合の確認失敗	追加情報なし
FTA_WSE_EXT.1	アクセスポイントへのすべての接続の試み	接続あれるアクセスポイントの識別
FTP_ITC.1	高信頼チャネルを構築するすべての試み チャネルデータ変更の検知	チャネルの非TOE終点の識別

セキュリティ監査事象選択　(FAU_SEL)

FAU_SEL.1　　選択監査

FAU_SEL.1.1　TSFは、以下の属性に基づきすべての監査対象事象から監査を受ける事象を選択できなければならない。(shall)

a) 事象タイプ

b) 監査可能なセキュリティ事象の成功

c) 監査可能なセキュリティ事象の失敗

d) [割付:その他の属性]

適用上の注意:

48 *この要件の意図は監査事象を引き起こすために選択され得るすべての基準を識別することである。ST執筆者については、割付は追加基準をリストアップまたは「なし」と表示する。監査可能な事象タイプは表９にリストアップする。*

保証アクティビティ:

49 *ガイダンスがすべての事象タイプを項目別にあげ、選択可能なすべての属性を要件に従って記述することを確実とするために、評価者は管理ガイダンスをレビューし割当てリストにそれらの属性が含まれることを確実にしなければならない(shall)。管理ガイダンスは、予備選択の設定の仕方を含むとともに、マルチ価値予備選択のために構文（存在する場合）を説明しなければならない(shall)。管理ガイダンスは現在実施されている選択基準に関係なく、常に記録される監査記録も識別しなければならない(shall)。*

50 *評価者はまた以下のテストを実施しなければならない(shall)。*

● *テスト 1: 要件にリストされる各属性について、評価者は属性の選択がその属性（または管理ガイダンスで識別されるとおり、常に記録されるもの）による監査事象だけが記録されることを示すようにテストを考案しなければならない(shall)。*

● *テスト 2 [条件付き]: TSFがより複雑な監査予備基準（複数の属性、属性を用いた論理的表現）をサポートする場合、評価者はこの能力が正しく実装されていることを示すテストを考案しなければならない(shall)。　評価者はまたテスト計画において、そのテストが係る能力を実施するのに十分であり代表的であるよう正当化する短い解説を提供しなければならない(shall)。*

4.1.2 クラス：暗号サポート (FCS)

51 暗号化要件はまた、IEEE 802.11 規格に基づいた WPA2 エンタープライズの Wi-Fi 認証要件の使用を必要とするよう構成されている。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、デバイスのデータ通信の相互運用性をテストし、セキュリティで保護された接続のために Advanced Encryption Standard（AES）カウンタとメッセージ認証コード（MAC）アルゴリズム（AES-CCMP と呼ばれる）との併用を義務づける。

暗号鍵管理 (FCS_CKM)

FCS_CKM.1　暗号鍵生成（WPA2 接続のための共通鍵）

FCS_CKM.1.1 **詳細化**：TSF は、指定された暗号鍵**導出**アルゴリズム**[PRF-384]**に従って、指定された暗号化鍵サイズ**[128 ビット]**で、**FCS_RBG_EXT.1 で指定された生成器**を使用し、**[802.11-2007]**の条件を満たす、**1 時間を超えない単位の管理上設定された鍵有効期間**で、**対称**暗号鍵を**導出**しなければならない。

適用上の注意：

52 *この要件は、クライアントが認証された後に生成された/アクセスポイントとクライアント間の通信のために導出される鍵にのみ適用される。これは、本 PP で定められた本 PP で指定されている SHA-1 やその他の情報を用いた HMAC 機能である RBG によって生成されるランダムな値を使用して処理される PMK からの PTK 導出を指す。これは主に第 8 章の 802.11-2007 に定められている。*

保証アクティビティ：

53 *暗号プリミティブは､本 PP の後半で定められた保証アクティビティを通じて検証される。評価者は、TSS が本 PP で定義され実装されたプリミティブが、ワイヤレスクライアントへのセキュアな接続を確立及び維持に際しどのように TOE に使用されてかを説明していることを確認しなければならない。TSS はまた、開発者がその実装が暗号化規格に準拠していることを保証する方法を説明しなければならない。これには、開発組織によって実施されたテストだけでなく、実行されている付加的な第三者試験も含まれる。評価者は、テスト方法の説明が、プロトコルの仕様の詳細のテストの程度を決定するうえで十分な詳細なものであることを保証しなければならない。セッション鍵の鍵有効期間を設定する方法を記述していること、また仕様書の精度は一時間以上にならないことを確認するために、評価者は管理者ガイダンスを確認しなければならない。評価チームは、次のテストを実行しなければならない。*

- *テスト 1：管理者ガイダンスに続いて、評価者は、セッション鍵の鍵有効期間を設定しなければならない。評価者はアクセスポイントに TOE を接続し、鍵有効期間以上の時間の接続を維持しなければならない。評価者は設定された鍵有効期間*

の後、再ネゴシエーションを開始し、新しいセッション鍵を確立するためことを決定しなければならない。

FCS_CKM.2　暗号鍵配布（GTK）

FCS_CKM.2.1　**詳細化**：TSF は、指定された暗号鍵の配布方法に応じて、**グループ一時鍵**を配布しなければならない：以下の条件を満たしていること：[EAPOL-Key フレームの AES キーラップ]：[AES キーラップには RFC3394、パケットフォーマットとタイミングの考慮事項については 802.11-2007] 及び**暗号化鍵を公開しないこと**。

適用上の注意：

54 *この要件は、接続先の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のため TOE によって受信されたグループ一時鍵（GTK）に適用される。802.11-2007 は、転送の形式及び RFC3394 で定められた AES キーラップメソッドによってラップされる必要があることを指定する。TOE は、このような鍵を解除することができなければならない。*

保証アクティビティ：

55 *評価者は、TSS が本 PP で指定された AES 実装を使用して TOE での使用のためにインストールされる前に、GTK がどのように解除されるかを TSS が説明していることを確認しなければならない。また評価者は、以下のテストを実行しなければならない：*

・テスト 1：評価者は TOE を正常にアクセスポイントに接続しなければならない。TOE 接続の際、評価者は GTK が TOE とアクセスポイントの間の空隙で送信されていないことを確認しなければならない。

・テスト 2：評価者は、ブロードキャストメッセージが、TOE が接続されているアクセスポイントによって送信されるようにしなければならない。評価者は、メッセージが暗号化されており、転送中に読み取ることができないこと、また TOE が送信されたメッセージを復号・解読できることを確認しなければならない。

FCS_CKM_EXT.4　暗号鍵ゼロ化

FCS_CKM_EXT.4.1　**詳細化**：不要になったとき、TSF は、すべての平文の秘密と秘密暗号鍵と CSP をゼロ化しなければならない。

適用上の注意：

56 *セキュリティ上重要なデータの暴露または改ざんを防ぐため、使用されなくなったセキュリティ関連情報（鍵、認証データ、パスワード）は全てゼロ化しなければならない。*

57 *上記のゼロ化は、別の場所に鍵/ CSP の転送時の平文の鍵/CSP の各中間格納領域（すなわちこのようなデータのパスに含まれるメモリバッファなど何らかのストレージ）に適用される。*

58 *TOE は必ずしもホスト IT 環境を考慮していないので、この能力の程度には多少の制限がある。この要件の目的のため、ゼロ課の実行のためには TOE がホストの正しい基本的な関数を呼び出せば十分である。これは、TOE が、データがゼロ化されていることを確認するためにカーネルモードのメモリドライバを含める必要があるということを意味するものではな*

い。

保証アクティビティ：

59 *評価者は、TSS は、ゼロ化された時（例えば使用後すぐ、システムの終了時など）、実行されるゼロ化プロシージャのタイプ（ゼロで上書き、ランダムパタンで 3 回上書きなど）について、それぞれの秘密鍵（鍵は対称暗号化に使用される）、秘密鍵及び鍵の生成に使用される CSP を説明していることを確実にするために確認しなければならない。保護する材料のために複数の種類のメモリが使用されている場合、評価者は TSS はデータが格納されているメモリの面でのゼロ化プロシージャについて説明していることを確実にするために確認しなければならない（例えば、「フラッシュに格納された秘密鍵はゼロで一度上書きするとゼロ化されるが、内蔵ハードディスクドライブに保存された秘密鍵は各書き込み開始前に変更されたランダムなパタンで 3 回上書きするとゼロ化される」。ゼロ化を検証するためにリードバックが行われた場合、これも記載しなければならない。*

暗号操作（FCS_COP）

FCS_COP.1（1） 暗号操作（データの暗号化／復号）

FCS_COP.1.1（1） **詳細化**：TSF は、指定された暗号アルゴリズム［割付：**1 つ以上のモード**］で動作する AES］と暗号鍵サイズ 128 ビット、256 ビット及び以下に適合する［**選択**：192 ビット、**他の鍵サイズなし**］に従って、［暗号化と復号］を実行しなければならない：

- **FIPS PUB 197、「Advanced Encryption Standard (AES)」**
- **［選択：NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D, NIST SP 800-38E］**

適用上の注意：

60 割付のため、*ST 執筆者は、AES が動作する単数または複数のモードを選択しなければならない。最初の選択の際、ST 執筆者は、この機能でサポートされている鍵サイズを選択しなければならない。2 つ目の選択の際、ST 執筆者は、割付で指定されたモードを記述する標準規格を選択しなければならない。*

61 *この要件は、ワイヤレストラフィックの暗号化には適用されないことに注意する。要件 FCS_COP.1 (5) は、ワイヤレス WPA2 暗号化/復号に使用されるモード、鍵サイズ及び標準を定義する。*

保証アクティビティ：

62 *評価者は、"The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS) and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)"（これらの文書は http://csrc.nist.gov/groups/STM/cavp/index.html で入手可能）を上記要件のテスト時のガイドとし、上記要件で選択したモードに適切なテストを使用しなければならない。これには、評価者が、テスト中に検証されるテストベクタを生成できる、アルゴリズムの高信頼参照実装を持っていることを必要とする。*

FCS_COP.1（2） 暗号操作（暗号署名）

FCS_COP.1.1（2）　**詳細化**：TSF は、以下の［**選択**］に従い**暗号署名サービス**を実行しなければならない。［**選択**：

(1) 2048 ビット以上の鍵サイズ（法）電子署名アルゴリズム（DSA）

(2) 2048 ビット以上の鍵サイズ（法）RSA 電子署名アルゴリズム

(3) 鍵サイズ 256 ビット以上の楕円曲線電子署名アルゴリズム（ECDSA）

適用上の注意：暗号化された署名にとって好ましいアプローチとして、楕円曲線は本 PP の将来的な出版物に必要となる。

この選択は以下の条件を満たしていなければならない：

電子署名アルゴリズムの場合：

- **［選択：FIPS PUB186-3、“Digital Signature Standard”］**

RSA 電子署名アルゴリズムの場合：

- **［選択：FIPS PUB186-3、“Digital Signature Standard”］**

楕円曲線電子署名アルゴリズムの場合：

- **［選択：FIPS PUB186-3、“Digital Signature Standard”］**
- **TSF は、「NIST 曲線」P-256、P-384 を実装しなければならない。［選択：P-521、他の曲線なし］（FIPS PUB 186-3 “Digital Signature Standard”に定義された通り）**

適用上の注意：

63 *ST 執筆者は、電子署名を実行するために実装されたアルゴリズムを選択すべきである（should）。複数のアルゴリズムが使用可能な場合、この要件は、機能を指定するため繰り返されるべきである（should）。選択されたアルゴリズムについて、ST 執筆者は、そのアルゴリズムのために実装されているパラメタを指定するため適切な割付/選択を行うべきである（should）。*

64 *楕円曲線ベースのスキームについては、鍵のサイズは、ベースポイントの位数の log2 を参照する。電子署名のための好ましいアプローチとして、ECDSA は、本 PP の将来的な出版物に必要となる。*

保証アクティビティ：

65 *上記の要件をテストする際のガイドとして、評価者は、「The Digital Signature Algorithm Validation System」（DSA2VS）、「The Elliptic Curve Digital Signature Algorithm Validation System」（ECDSA2VS）, and 「The RSA Validation System」（RSA2VS）の署名生成及び署名検証の部分を使用しなければならない。使用する検証システムは、ST で識別された適合基準（すなわち、FIPS PUB 186-3）を遵守しなければならない。これには、評価者が、テスト中に検証されるテストベクタを生成できる、アルゴリズムの高信頼参照実装を持っていることを必要とする。*

FCS_COP.1（3）　暗号操作（暗号化ハッシュ）

FCS_COP.1.1(3)　**詳細化**：TSF は、指定暗号アルゴリズム［**選択：SHA-1、SHA-256、SHA-384**］と *FIPS PUB 180-3「Secure Hash Standard」*の条件を満たす**メッセージダイジェストサイズ[選択：160、256、384] ビット**、に従って、［*暗号化ハッシュサービス*］を実行しなければならない。

適用上の注意：

66 *ハッシュアルゴリズムの選択は、メッセージダイジェストサイズの選択に対応していなければならない。例えば SHA-1 が選択された場合、その唯一の有効なメッセージダイジェストサイズの選択は 160 ビットとなる。*

保証アクティビティ：

67 *評価者は、上記の要件をテストする際のガイドとして、「The Secure Hash Algorithm Validation System (SHAVS)」を使用しなければならない。これには、評価者が、テスト中に検証可能なテストベクタを生成できるアルゴリズムの高信頼参照実装を持っていることを必要とする。*

FCS_COP.1(4)　暗号操作（鍵付きハッシュメッセージ認証）

FCS_COP.1.1（4）　**詳細化**：TSF は、指定した暗号アルゴリズム HMAC-［選択：SHA-1、SHA-256、SHA-384］、鍵サイズ［**割付：HMAC で使用されるキーサイズ（ビット単位）**］及び以下の条件を満たす**メッセージダイジェスト**のサイズ［選択：160、256、384］**ビット**に従い鍵付きハッシュメッセージ認証を行わなければならない：**FIPS PUB198-1、「The Keyed-Hash Message Authentication Code」及び FIPS PUB180-3、「Secure Hash Standard」**。

適用上の注意：

68 *ハッシュアルゴリズムの選択は、メッセージダイジェストサイズの選択に対応していなければならない。例えば HMAC-SHA-256 が選択された場合、その唯一の有効なメッセージダイジェストサイズの選択は 256 ビットとなる。*

69 *メッセージダイジェストのサイズは、上記で使用した基本となるハッシュアルゴリズムに対応する。ハッシュ計算後に HMAC の出力を切り捨てることは、様々なアプリケーションの適切なステップであることに注意する。これは、この要件への準拠を無効にするものではない。しかし ST は、切り捨てが行われること、最終出力のサイズ及びこの切り捨てが準拠する規格を明記すべきである。*

保証アクティビティ：

70 *上記の要件をテストする際のガイドとして、評価者は、「The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)」を使用しなければならない。これには、評価者が、テスト中に検証されるテストベクタを生成できる、アルゴリズムの高信頼参照実装を持っていることを必要とする。*

FCS_COP.1（5）　暗号操作（WPA2 データ暗号化／復号）

FCS_COP.1.1（5）　**詳細化**：TSF は、以下の要件を満たす**指定された暗号アルゴリズム AES CCMP と 128 ビットの暗号化キーサイズに従い、暗号化と復号**を実行しなければならない：**FIPS PUB 197、NIST SP 800-38C 及び IEEE802.11-2007**。

適用上の注意：

71

EEE802.11-2007 に準拠するためには、128 ビットの暗号鍵サイズを持つ AES CCMP（800-38C SP が定める通り、CCM に AES を使用）を実装しなければならないことに注意する。将来的にはこの規格が更新され、新しい暗号モードが NIST によって審査・承認されていくにつれ、この要件には、追加のあるいは新たな暗号化モード及び鍵サイズ要件が加えられる可能性がある。

保証アクティビティ：

72 *評価者は、上記の要件をテストする際のガイドとして、「The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)」のテストを使用しなければならない。これには、評価者が、テスト中に検証されるテストベクタを生成できる、アルゴリズムの高信頼参照実装を持っていることを必要とする。*

73 *加えて評価者は、AES-CCMP の IEEE802.11-2007 の実装をさらに確認するために、2002 年 9 月 10 日付の IEEE802.11-02/362r6 文書「IEEE 802.11 TGI のための提案テストベクタ」第 2.1 項「AES-CCMP カプセル化の例」及び第 2.2 項「追加 AES CCMP テストベクタ」のテストを使用しなければならない。*

拡張：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_EAP-TLS_EXT）

FCS_EAP-TLS_EXT.1 拡張：拡張認証プロトコルトランスポート層セキュリティ

FCS_EAP-TLS_EXT.1.1 TSF は RFC5216 で指定される通り、以下の暗号化方式をサポートする EAP-TLS プロトコルを実装しなければならない。

- RFC 3268 に準拠する必須暗号化方式
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- 付加的な暗号化方式

  [選択：
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5430

]。

FCS_EAP-TLS_EXT.1.2 TOE は FCS_RBG_EXT.1 で指定された RBG を使用し、EAP-TLS 交換で使用されるランダム値を生成しなければならない。

FCS_EAP-TLS_EXT.1.3 TSF は、FIA_X509_EXT.1 で指定される通り X503 v3 証明書を使用しなければならない。

FCS_EAP-TLS_EXT.1.4 TSF は、サーバ証明書拡張の Key Usage フィールドにサーバ認証目的（OID 1.3.6.1.5.5.7.3.1 の id-kp1）が含まれていることを確認しなければならない。

FCS_EAP-TLS_EXT.1.5 TSF は、TOE によって受け入れられた認証サーバの証明書に署名することを許可された権限のある管理者が CA のリストを設定することを認めなければならない。

FCS_EAP-TLS_EXT.1.6 TSF は、許可管理者が、EAP-TLS 交換時に提案され受け入れられる可能性のあるアルゴリズム方式のリストを設定することを許可しなければならない。

適用上の注意：

74 *評価構成で使用する暗号スイートは、この要件によって制限される。ST 執筆者はサポートされている付加的な暗号スイートを選択しなければならない。必須のスイート以外にサポートされた暗号スイートが存在しない場合は、「なし」を選択しなければならない。管理評価構成で使用できる暗号スイートを制限することが認められる。*

75 *上記の方式 B アルゴリズム（RFC5430）は、実装に適したアルゴリズムである。*

FCS_EAP-TLS_EXT.1.4 では TOE は、認証サーバから提示された証明書に特定のチェックを実行する必要があるが、認証サーバがクライアントによって提示された証明書に実行しなければならない対応チェックがある。すなわち、クライアント証明書の extendedKeyUsage フィールドに「クライアント認証」が含まれていること及び鍵合意ビット（Diffie-Hellman の暗号化方式の場合）または鍵暗号化ビット（RSA 暗号スイートの場合）が設定されていることの確認である。TOE の使用を目的として取得した証明書を企業で使用するためには、これらの要件に準拠する必要がある。

保証アクティビティ：

76 *TSF が RFC を正しく実装していることを示すために、評価者は、TSS には以下の情報が含まれていることを確認しなければならない：*

・FCS_EAP_TLS_EXT.1 要素にリストされた該当 RFC の節ごと、「しなければならない」(must)としない全ての文（例えば「可能性がある」(may)、「すべきである」(should)、「すべきでない」(should)について、TOE は、そのようなオプションを実装している場合、TSS で説明しなければならない。もし記載された機能が規格で「すべきでない」(should not)「してはならない」(must not)とされている場合、TSS は、これは TOE が

実装されたセキュリティ方針に悪影響を与えないという理論的根拠を提供しなければならない。

・RFC の各節について、「すべきである」に関する機能の省略は記述されなければならない。

77 *TOE が実行しなければならない、規格に含まれない処理であるすべての TOE 固有の拡張機能、またはセキュリティ要件に影響を与える可能性があり規格で許可されている代替の実装を記載しなければならない。*

78 *評価者は、付加的な特性（例えば、拡張子がサポートされている、クライアント認証がサポートされている）が指定されていることを確認し、サポートされている暗号化方式も同様に指定されていることを確かめるため、TSS のこのプロトコルの実装の記述を確認しなければならない。*

78 *評価者は、指定された暗号スイートは、このコンポーネントに示されているものと同一であることを確かめるために TSS を確認しなければならない。また評価者は、TLS が TSS の説明に適合するように、運用ガイダンスに TOE 設定手順が含まれていることを確認しなければならない（例えば、TOE によって利用された暗号スイートのセットは、要件を満たすために制限を受けねばならないかもしれない）。*

79 *評価者は、管理者が EAP-TLS 交換時に、TOE 及び EAP-TLS 交換の際に TOE によって提案・受理されるアルゴリズム方式を指定する方法についての命令によって受け入れられる認証サーバによって使用される証明書に署名するために許可されている認証局のリストを設定するための指示が OPE 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。*

80 *また評価者は、以下のテストを実行しなければならない：*

- *テスト 1：評価者は、要件によって指定された暗号スイートのそれぞれを使用して TLS 接続を確立しなければならない。この接続は、より高いレベルのプロトコルの確立の一環として（例えば EAP セッションの一部として）確立される可能性がある。テストの目的を満たすためには、（ワイア上で）暗号化方式の正常なネゴシエーションを観察すれば十分である。使用されている暗号方式を識別しようとして （例えば、暗号化アルゴリズムが 128 ビット AES でなく、256 ビット AES であるなど）暗号化されたトラフィックの特性を調べる必要はない。*
- *テスト 2：各サポート済み証明書署名アルゴリズムについて、以下のテストが繰り返される。評価者は、extendedKeyUsage フィールドにサーバ認証目的を含む認証サーバの証明書を持つサーバを使用して、接続の確立を試み、接続が確立されていることを確認しなければならない。評価者はその後、クライアントが extendedKeyUsage フィールドに、サーバ認証目的を欠いた、その他の場合には有効なサーバ証明書を拒否し、接続が確立されていないことを確認する。理想的には、2 つの証明書が extendedKeyUsage フィールドを除いて同一となるべきである。*
- *テスト 3：PRE／OPE ガイダンスで提供されるガイダンスに従い、CA は認証サーバ証明書において「許容」として構成され、その後、評価者は、ワイヤレス接続を開始し、ワイヤレスクライアントが正常に接続できることを確認する。評価者は次に、その他の場合には有効な証明書が、TOE に許可されていない CA によって署名されるようにシステムを構成する。このような証明書を提示して認証サーバに認証させようとした場合、接続は拒否されるはずである。*
- *テスト 4：評価者は、このコンポーネントの最初の要素で指定されたものだけに制限された EAP-TLS ネゴシエーション中に提案されるプロトコルのリストを設定するにあた*

り、管理者用ガイダンスに従わなければならない。評価者はアクセスポイントとの接続を開始し、設定されたプロトコルだけが提案されていることを確認しなければならない。初期リストがクライアントによって提案されたプロトコルの全体集合のサブセットでない場合、評価者は最初のテストで使用されるプロトコルのサブセットを指定してテストを繰り返さなければならない。

拡張：暗号操作（ランダムビット生成）(FCS_RBG_EXT)

FCS_RBG_EXT.1　拡張：暗号操作（ランダムビット生成）

FCS_RBG_EXT.1.1　TSF は、[以下のひとつから選択：
1 つまたは複数の独立したハードウェアベースのノイズ源
1 つまたは複数の独立したソフトウェアベースのノイズ源
ハードウェアベースとソフトウェアベースのノイズ源の組み合わせ]のエントロピー蓄積源でシードされた[以下から 1 つを選択:[選択：Hash_DRBG （任意）、 HMAC_DRBG （任意）、CTR_DRBG（AES）、Dual_EC_DRBG（任意）] を使用した NIST SP800-90]、FIPS PUB 140-2 附属書 C、AES を使用した X9.31 付録 2.4] に従いすべてのランダムビット生成（RBG）サービスを実行しなければならない。

FCS_RBG_EXT.1.2　決定論的 RBG は、鍵の最大ビット長に少なくとも等しいエントロピー［以下から 1 つを選択：128 ビット、256 ビット］と、これが生成する承認要素を伴ってシードされなければならない。

適用上の注意：

81 *NIST SP800-90 付録 C は、おそらく FIPS-140 の将来のバージョンで必要となる最小エントロピーの測定について説明する。可能であれば、これはすぐに使用されるべきであり、本 PP の将来のバージョンで必要となる。*

82 *FCS_RBG_EXT.1.1 の最初の選択に際しては、ST 執筆者は RGB サービス（800-90 か 140-2 付録 C）が準拠する規格を選択する。2 番目の選択については、ST 執筆者は、クライアントが RBG のエントロピー収集する方法を示す。*

83 *SP 800-90 は、乱数を生成する 4 つの方法を含んでいる。これらはそれぞれ、順番に、基礎となる暗号プリミティブ（ハッシュ関数／暗号）に依存する。ST 執筆者は、(800-90 が選択されている場合）使用する関数を選択し、要件または TSS で使用される特定の基本的な暗号プリミティブを含む。Hash_DRBG または HMAC_DRBG には識別ハッシュ関数（SHA-1、SHA-224、SHA-256、SHA-384、SHA-512）のいずれかが許可されているが、CT_DRBG には AES ベースの実装のみが許可されている。Dual_EC_DRBG には 800-90 に定義された曲線のいずれかが許可されているが、ST 執筆者は、選択された曲線だけでなく、使用されるハッシュアルゴリズムを含めなければならない。*

84 *FIPS PUB 140-2 付録 C については、現在、3-key TripleDES と AESAlgorithms を使用した ANSI X9.31 付録 A.2.4 に基づく NIST-Recommended Random Number Generator 第 3 節に記載されている方法のみが有効であることに注意する。ここで使用される AES の実装の*

ための鍵の長さが利用者データを暗号化するために使用されるものと異なる場合、別のキーの長さを反映するために FCS_COP.1 を詳細化または反復する必要がある可能性がある。FCS_RBG_EXT.1.2 の選択については、ST 執筆者は RBG をシードするために使われるエントロピーのビット数の最小値を選択する。

85 *ST 執筆者は、基礎となる機能が TOE の基準要件に含まれていることを確認する。*

86 *将来的には、「エントロピー源テストの方法：要件とテスト方法の説明」で説明した要件のほとんどは、本 PP で必要となる。フォロー保証アクティビティは現在、必要とされるアクティビティのサブセットだけを反映している。*

保証アクティビティ：

87 *評価者は、TOE で使用される RBG を含む製品のバージョン番号を決定するため、TSS の項を参照しなければならない。また評価者は、TSS が、エントロピーが収集されるノイズ源を記述していることを確認しなければならない。評価者はさらに、RBG で使用される基本的な機能とパラメタがすべて TSS に記載されていることを確認する。*

88 *評価者は、TSS がエントロピー入力を取得するための方法を含む RBG モデルの説明を含んでいることを確認するとともに、使用エントロピーの同定、エントロピーが各ソースからどのように生産／収集されるかの同定、エントロピーは、それぞれのエントロピー源によって生成されるかの同定を行わなければならない。また評価者は、TSS は、エントロピー源状態テスト、この状態テストがエントロピー源の状態の判断に純分であると判断する根拠、既知のエントロピー源故障のモードを記述していることを確認しなければならない最後に評価者は、時間及び／または環境的条件による出力と変動の独立性の観点から、TSS が RBG の出力の説明を含んでいることを確認しなければならない。*

89 *RGB が適合しているとする規格の種類を問わず、評価者は以下のテストを実行する：*

- *テスト 1：評価者は<u>エントロピー源のテスト方式</u>を使用し、各エントロピー源のエントロピーの推定値を決定しなければならない。評価者は、TSS は、すべてのエントロピー源から得たすべての結果の最小値であるエントロピーの推定値が含まれていることを確認しなければならない。*

90 *評価者は、RBG が準拠する規格に応じて、次のテストを実行しなければならない。*

FIPS 140-2 Annex C に適合する実装、

91 *本節に含まれるテスト用の参照は、The Random Number Generator Validation System（RNGVS）[RNGVS]。評価者は次の 2 つのテストを実施しなければならない。「期待値」は、その正確性がわかっているアルゴリズムの参照実装によって生成されることに注意する。正確性の証明は各スキームに任されている。*

92 *評価者は、可変シードテストを実行しなければならない。各 128 ビットの 128 ペアー組（シード、DT）を TSF RBG 機能に提供しなければならない。また評価者は、128（シード、DT）のペアすべてが一定であるである鍵（AES アルゴリズムに適した長さのもの）を提供しなければならない。DT の値は、セットごとに 1 ずつインクリメントされる。シード値はセット内にリピートがあってはならない。評価者は、TSF によって返された値が期待値と一致していることを確認する。*

93 *評価者は、モンテカルロテストを実行しなければならない。このテストでは、TSF RBG 関数への最初のシードと DT の値を指定する。これらはそれぞれ 128 ビットである。評価者は、*

テスト全体を通して一定である鍵（AES アルゴリズムに適切な長さのもの）を提供しなければならない。評価者はその後、3-key TripleDES と AES Algorithms を使用した ANSI X9.31 付録 A.2.4 に基づく NIST-Recommended Random Number Generator 第 3 節に指定される通り、繰返しごとに 1 ずつインクリメントされている DT の値で TSF の RBG と後続の繰返しのために生成される新しいシードを 10,000 回呼び出す。評価者は、生成された 10,000 番目の値が期待値と一致していることを確認する。

NIST SP800-90 に適合する実装

94 *評価者は、RNG の実装のための 15 の試験を行わなければならない。評価者はまた、運用大ダンスに RNG の機能設定のための適切な指示が含まれていることを確認しなければならない。*

95 *RNG の予測耐性が有効になっている場合、各試験は以下から構成される。(1) drbg のインスタンス化 (2) ランダムビットの最初のブロックの生成 (3) ランダムビットの第二のブロックの作成 (4) インスタンス化の撤回。評価者は、ランダムなビットの第二のブロックは期待値であることを確認する。評価者は、それぞれの試験のための 8 つの入力値を生成しなければならない。第一はカウント (0～14) である。次の 3 つはインスタンス化操作のためのエントロピー入力、ナンス及びパーソナル化文字列である。次の 2 つは最初の呼び出しで生成する追加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。「ランダムビットの 1 つのブロックを生成」は、 出力ブロックの長さに等しいリターンビット数を持つランダムなビットを生成することを意味する (NIST SP 800-90 で定義された通り)。*

96 *RNG が予測耐性を持たない場合、各試験は以下から構成される。(1) drbg のインスタンス化 (2) ランダムビットの最初のブロックの生成 (3) 再シード (4) ランダムビットの第二のブロックの作成 (5) インスタンス化の撤回。評価者は、ランダムなビットの第二のブロックが期待値であることを確認する。評価者は、それぞれの試験のための 8 つの入力値を生成しなければならない。第一はカウント (0～14) である。次の 3 つはインスタンス化操作のためのエントロピー入力、ナンス及びパーソナル化文字列である。5 つ目の値は最初の呼び出しで生成する追加入力である。6 つ目と 7 つ目はこの呼び出しで再シードする追加入力とエントロピー入力である。最後の値は 2 番目の生成呼び出しの追加入力である。*

97 *次の段落には、評価者により入力値が生成／選択されるいくつかの詳細な情報が記載される。*

***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。*

***ナンス**：ナンスがサポートされている場合 (df のない CTR_DRBG するはナンスを使わない)、ナンスビットの長さはシードの長さの半分である。**個別化文字列**：文字列の長さ≦シードの長さでなければならない。実装が 1 種類の個別化文字列の長さをサポートしている場合、同じ長さを両方の値に用いてよい。複数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使用しなければならない。実装で個別化文*

字列を使用しない場合、値を供給する必要はない。

***追加入力**：* *追加入力文字列のビット長は、個別化文字列長と同じ既定値及び制約条件がある。*

4.1.3 クラス： 利用者データ保護(FDP)

残存情報保護（FDP_RIP）

FDP_RIP.2 全残存情報保護

FDP_RIP.2.1 TSF は、[選択：資源の割付、資源割付の解除] 時に、資源の以前の情報の内容をすべて使用不可にしなければならない。

適用上の注意：

98 *この要件は例えば、プロトコルデータユニット（PDU）は、暗号鍵マテリアルなど、残存情報が埋め込まれていないことを保証する。ST 執筆者は以前の情報をいつ使用不可にするかを指定するために選択を使用する。*

保証アクティビティ：

99 *この要件の文脈における「資源」とは、TOE を通じて（セキュリティ管理者が TOE に接続する際のようにこれに「対して」というのと対照的に）送られるネットワークパケットである。懸案事項は、ネットワークパケットが送信された後も、パケットで使用されるバッファまたはメモリ領域にはまだそのパケットのデータが含まれていること、そしてそのバッファが再使用される場合、それらのデータはそのまま残り、新しいパケットに入り込む可能性があるということである。評価者は、ネットワークパケットを処理する際にパケット処理はデータが再利用されないことを決定できる程度を TSS が説明していることを確実にするために確認しなければならない。評価者は、この説明が少なくとも以前のデータが上書き/ゼロ化される方法、またバッファ処理のどの時点でこれが起こるかを説明していることを確認しなければならない。*

4.1.4 クラス：識別と認証 (FIA)

100 I&A に関しては、正式な管理者または汎用の利用者が定義されていないため、TOE のベースライン要件はかなり制限されている。TOE によって実行されるために必要な I&A の範囲は、ワイヤレスアクセスシステムを介して保護されたネットワークに接続されるプロセスに関連している。さらに、通常の I&A プロセスの一部と見なされうる要件の一部は、本 PP の他の節、特にワイヤレス通信のための暗号化プロトコル（WPA2）に関する項目で指定される。これはグループ化されたこれらのプロトコルの要件をまとめ、わかりやすくするとともに作成と保証アクティビティの適用を容易にするために行われた。従って本節の要件は、TOE がサポートしなければならない I&A 機能の残りの 2 つの側面をカバーしたものである。

- **802.1X-2010 の認証**　02.1X-2010 規格（及び関連する RFC）は、ネットワークにアクセスする目的でマシンの認証を指定する。この方法は、802.11-2007 規格を使用したワイヤレス操作の前駆体として使用される。802.1X は、802.1X 交換に参加するいくつかの異なる当事者向けの要件が含まれているが、以下の要件は、802.1X ごとに 「サプリカント」としての役割を果たす TOE の役割をターゲットにしている。
- **クレデンシャル**　本項及び本 PP の他の項で指定されたプロトコルとメカニズムは、802.1X 認証を実行する際に EAP-TLS 交換で使用する証明書に依存する。

拡張：802.1X ポートアクセス制御認証（FIA_8021X_EXT）

FIA_8021X_EXT.1　拡張：802.1X ポートアクセスエンティティ（サプリカント）の認証

FIA_8021X_EXT.1.1　TSF は「サプリカント」の役割において、ポートアクセスエンティティ（PAE）のための IEEE 規格の 802.1X に準拠しなければならない。

適用上の注意：

101　*この要件は、802.1X 認証交換のサプリカントとしての TOE の役割をカバーしている。交換が正常に完了している場合、TOE は 802.11 の通信を開始するために EAP-TLS（または他の適切な EAP 変換）の結果として PMK を導出し、ワイヤレスアクセスシステム（認証システム）による 4 ウェイハンドシェイクを実行する。*

102　*前述したように、交換中に存在する通信パスは少なくとも 2 つある。ワイヤレスアクセスシステムを持つものと、リレーとしてワイヤレスアクセスシステムを使用する認証サーバを伴うものである。TOE は、802.1X-2010 で指定されたワイヤレスアクセスシステムで LAN（EAPOL）接続を経由し EAP を確立する。TOE と認証サーバは EAP-TLS セッション（RFC5216）を確立する。*

103　*802.1X 認証を実行する意義は、（正常に認証され、すべての 802.11 ネゴシエーションが正常に実行されたとして）ネットワークへのアクセスを得ることである。802.1X の用語で、これは、TOE がワイヤレスアクセスシステムによって維持される「制御ポート」へのアクセスを得ることを意味する。*

保証アクティビティ：

104　*TSF が正しく 802.1X-2010 規格を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確認しなければならない。*

- *TOE が実装されている規格の節*
- *識別された各節について、規格で許可される任意のオプションが指定される。*
- *識別された各節について、非準拠の理由を含めて、任意の非適合性が識別され、説明される。*

105　*評価者は、次のテストを実行しなければならない：*

- *テスト 1：評価者は、TOE 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。ワイヤレスアクセスシステムを介して認証サーバで正常に認証した後、評価者は、TOE がテストネットワークにアクセスできることを実証しなければならない。*
- *テスト 2：評価者は、TOE がテストネットワークへのアクセス権を持たないことを*

実証しなければならない。評価者は、EAP-TLS のネゴシエーションが失敗するよう、無効なクライアント証明書を使用して認証を試みなければならない。TOE はまだテストネットワークへの接続を持っていないはずである。

- *テスト 3：評価者は、TOE 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。評価者は、EAP-TLS のネゴシエーションが失敗するよう、無効なクライアント証明書を使用して認証を試みなければならない。TOE はまだテストネットワークへの接続を持っていないはずである。*

X509 証明書（FIA_X509_EXT）

FIA_X509_EXT.1　拡張：X.509 証明書

FIA_X509_EXT.1.1　TSF は、EAP-TLS 交換の認証をサポートするため、RFC 5280 で定義された X.509v3 証明書を使用しなければならない。

適用上の注意：

106 *これは、この要件に従って TOE により実装される必要がある RFC 5280 証明書の検証と証明書パスの検証要件を定義していることに留意する。*

保証アクティビティ：

107 *TSF は、RFC 5280 に従って、X.509v3 証明書の使用をサポートしていることを示すために、評価者は、TSS には、次の情報を記述していることを確実にしなければならない。TSF が RFC 5280 に従って X.509v3 証明書の使用をサポートしていることを示すために、評価者は、TSS に次の情報が記載されていることを確認しなければならない：*

- *RFC 5280 の各節では、「～しなければならない」でない文言（例えば「可能性がある」「すべきである（SHOULD）」「すべきでない（SHOULD NOT）」）は全て、読者は TOE が規格の特定の部分を実装しているかどうかを判断することができるように記載しなければならない(shall)。*
- *RFC 5280 の各節では、「すべきである（SHOULD）」に適合しない文言は全て説明されなければならない(shall)。*
- *TOE が実行する、セキュリティ要件に影響を与える可能性のある、規格に含まれていない TOE 固有の拡張機能や処理が記述されなければならない(shall)。*

108 *さらに評価者は、TOE が、TSS に記述されている実装に準拠し、規格及び TSS で指定された証明書パスを形成することができ、規格（CRL 処理を含む証明書パスの検証）で指定された証明書を検証することができる証明書を処理することを示すテストを講じなければならない。このテストは、チームのテスト計画書に記載しなければならない。*

109 *本 PP の将来のバージョンでは、TOE の証明書処理機能のためのより明示的なテストの要件を持つことに留意すべきである。さらに、プロトコル固有の証明書の処理のテストは、この保証アクティビティで必要とされるテストによって実行され、これと組み合わせる必要がある。*

110 *評価者は管理者用ガイダンスを確認し、TOE が使用する証明書を選択する方法及び TOE が*

証明書を使用できるようオペレーティング環境を構成するために必要な指示について説明していることを確認しなければならない。

111 *評価者は、証明書を使用する必要があるシステム内の各関数について次のテストを実行しなければならない：*

- *テスト1：評価者は、有効な証明書パスなしに証明書を使用すると機能に支障をきたすことを実証しなければならない。次に評価者は、管理者ガイドを使用して、証明書の検証のために必要な証明書を読み込み、機能が正常であることを実証しなければならない。評価者は、その後証明書のいずれかを削除し、機能が正常に動作しないことを実証しなければならない。*

4.1.5 クラス：セキュリティ管理 (FMT)

112 本 PP の 1 節に示すように､TOE は分離した管理役割を維持するためには必要とされない。しかしこれらは、一般の利用者に利用可能であるべきではない TOE 運用の特定の側面を設定する機能を提供するために必要である。TOE がある程度の管理制御を提供しない場合は、附属書 C の適切な要件を ST で使用するべきである。

管理機能の仕様 (FMT_SMF)

FMT_SMF.1 管理機能の特定

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

- **TOE が認証サーバ証明書を受け付ける CA の指定**
- **許容できる認証サーバの証明書の FQDN の指定**
- **証明書失効リストのチェックを有効化／無効化**
- **確立されたセッション鍵の鍵有効期間の設定。鍵有効期間を設定するための測定単位は 1 時間を超えない**
- **アドホックワイヤレスのクライアント間接続機能の無効化**
- **ワイヤレスネットワークブリッジ機能の無効化**
- **EAP-TLS 交換時の提案・受諾されるアルゴリズム方式の指定**
- **TOE の接続のために許容されるワイヤレスネットワークの指定**
- **認証前に IEEE 802.1X を有効化／無効化する能力**
- **PMK 有効化／無効化と PMK キャシュ構成を行う能力**
  〇PMK エントリがキャッシュされる時間（分単位）の設定
  〇キャッシュ可能な PMK エントリの最大数の設定
- **TOE を更新し、更新を検証する能力**
- **本 PP の他の節で識別されたすべてのセキュリティ管理機能を設定する能力**
- **［割付：追加の管理機能］。**

適用上の注意：

113 *インストールでは、WLAN クライアントはクライアントマシンに管理者を認証させるうえ*

114

で IT 環境に依存する。

この機能については確立したセッション鍵の鍵有効期間を設定し、鍵有効機関を設定するための測定単位は 1 時間を超えてはならない。例えば秒、分、時間の測定単位は許容できるが、日またはそれ以上の測定単位は許容されない。

115 ***保証アクティビティ：***

116 *評価者は、運用ガイダンスに PP で義務付けられたすべての管理機能が説明されていること、また、この説明に、管理機能に関連する管理業務を実行するために必要な情報が含まれていることを確認しなければならない。評価者は、TOE を設定し、上記の要件に記載されている各オプションをテストすることで、管理機能を提供する TOE の機能をテストしなければならない。*

117 *なお、ここでのテストは、FCS_EAP-TLS_EXT と FTA_WSE_EXT など他の要件のテストと同時に実行することができることに留意する。*

4.1.6 クラス：TSF の保護 (FPT)

拡張：TSF セルフテスト (FPT_TST_EXT)

FPT_TST_EXT.1.1 TSF は、初期起動（電源オン）時の TSF の正しい動作を実証するために、一連のセルフテストを実行しなければならない。

FPT_TST_EXT.1.2 TSF は、TSF が提供する暗号化サービスを使用して実行するために読み込む際に、格納されている TSF 実行コードの整合性を検証する能力を提供しなければならない。

適用上の注意：

118 *TOE は、一般的に IT 環境内で実行されているソフトウェアパッケージであるが、上記の必要なセルフテストを実行することもできる。しかし、上記の試験により提供される保証を評価する際、ホスト環境上に重要な依存関係があることを理解しなければならない（ホスト環境が侵害された場合、セルフテストは意味がないことを意味する）。*

保証アクティビティ：

119 *評価者は、起動時に TSF によって実行されるセルフテストを詳細に記述していることを確実にするために TSS を検査しなければならない。この記述は、テストが実際に行っていることのアウトラインを含めなければならない（例えば、「メモリがテストされている」という説明よりも、「メモリは、各メモリ位置に値を書き込み、これを読み戻してこれが書き込まれたものと同一であることを確認するテストが行われている」という説明が使われなければならない）。評価者は、TSF が正常に動作していることを実証するためのテストが十分であるという議論を TSS が行っていることを保証しなければならない。*

120 *評価者は、TSS が実行のために読み込まれたときに保存されている TSF 実行コードの整合性を検証する方法について説明していることを確実にするために TSS を検査しなければな*

らない。評価者は、テストが格納されている TSF 実行コードの整合性が損なわれていないことを実証するのに十分であるという主張を TSS が行っていることを保証しなければならない。評価者はまた、TSS（または運用ガイダンス）が正常な例（例えば、検証されたハッシュ）と異常な例（例えば、検証されないハッシュ）について行われるアクションを記述していることを実証しなければならない。評価者は、次のテストを実行しなければならない。

- *テスト 1：評価者は、既知の良好な TSF の実行可能ファイルの整合性チェックを実行し、チェックが正常であることを確認する。*
- *テスト 2：評価者は、TSF の実行可能ファイルを変更し、変更された TSF の実行可能ファイルの整合性チェックを実行し、チェックが失敗したことを確認する。*

拡張：高信頼更新（FPT_TUD_EXT.1）

FPT_TUD_EXT.1　拡張：高信頼更新

FPT_TUD_EXT.1.1　TSF は許可管理者に対し、TOE のファームウェア／ソフトウェアの現在のバージョンを照会する能力を提供しなければならない。

FPT_TUD_EXT.1.2　TSF は許可管理者に対し、TOE のファームウェア／ソフトウェアの更新を開始する能力を提供しなければならない。

FPT_TUD_EXT.1.3　TSF は、更新プログラムをインストールする前に、電子署名メカニズムと［選択：公開されたハッシュ、他の機能なし］を使用して、ファームウェア／ソフトウェアの TOE の更新を確認する手段を提供しなければならない。

適用上の注意：

121　*三番目の要素で参照されている電子署名メカニズムは FCS_COP.1（2）で指定されたものである。参照された公開ハッシュは、FCS_COP.1（3）で指定された関数のいずれかによって生成される。*

保証アクティビティ：

122　*TOE への更新は許可され、ソースによって署名されており、関連付けられているハッシュ値を持つ可能性があり、または正規のソースによって署名されている。電子署名が使用されている場合、承認されたソースの定義は、更新の検証メカニズムによって使用される証明書がデバイスに含まれる方法の説明とともに、TSS に含まれている。評価者は、この情報が TSS に含まれていることを実証する。評価者は、TSS（または運用ガイダンス）が候補である更新を取得する方法、電子署名の検証または更新のハッシュ計算に関連付けられている処理、正常な例（例えば、検証されたハッシュ）と異常な例（例えば、検証されないハッシュ）について行われるアクションを記述していることを実証する。評価者は、次のテストを実行しなければならない。*

- *テスト 1：評価者は、製品の現在のバージョンを決定するためにバージョン検証アクティビティを行う。評価者は、運用ガイダンスに記載されている手順を使用して正規の更新を取得し、これが正常に TOE にインストールされていることを確認する。その後評価者は、予想通り更新が機能することを実証するために他の保証アクティビティテストのサブセットを実行する。更新後評価者は、バージョンが更新プログラムのそれと正常に対応していることを確認するために再びバージョン検証アクティビティを行う。*
- *テスト 2：評価者は、製品の現在のバージョンを決定するためにバージョンの検証アクティビティを行う。評価者は、不正な更新を取得または生成し、これの TOE へのインストールを試みる。評価者は、TOE が更新を拒否することを確認する。*

4.1.7　クラス：TOE アクセス (FTA)

拡張：ワイヤレスセッションの確立（FTA_WSE_EXT）

FTA_WSE_EXT.1　拡張：ワイヤレスセッションの確立

FTA_WSE_EXT.1.1 承認された管理者によって設定された通り、TSF は［割付：許容可能なネットワークのリストを識別するために使用する属性］に基づいて、許容可能なネットワークとして指定されたワイヤレスネットワークへの接続を試みしなければならない。

適用上の注意：

123 *この要件の目的は、管理者は TOE が接続を許可されているアクセスポイントを制限することができるようにすることである。この割付は、許容可能なアクセスポイントを指定するために管理者が使用できる属性（例えば、IP アドレス、SSID など）を指定するために ST 執筆者によって使用される。*

保証アクティビティ：

124 *評価者は、許容可能なネットワーク（アクセスポイント）を指定するために使用することができるすべての属性が特に定義されていることを判断するために TSS を検査しなければならない。評価者は、TSS で識別される各属性を構成するためのガイダンスが含まれていることを判断するために運用ガイダンスを検査しなければならない。評価者は、各属性の次のテストを実行しなければならない：*

- *テスト 1：評価者は、特定のアクセスポイントとの接続を可能にするために TOE を構成する。評価者はまた、許可されたアクセスポイントと許可されていないアクセスポイントがいずれも TOE にとって「可視的」であるようにテスト環境を設定する。評価者は、自らが正常に許可されるアクセスポイントとのセッションを確立できる*

ことを実証しなければならない。評価者はその後、許可されたアクセスポイントとのセッションの確立を試み、アクセスの試行が失敗したことを確認する。

4.1.8 クラス: 高信頼パス通信チャネル (FTP)

高信頼チャネル (FTP_ITC)

FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 詳細化：TSF は、自身と**ワイヤレスアクセスポイント**との間に論理的に他の通信チャネルとは異なり、そのエンドポイントの保証 ID と**チャネルデータの公開の変更と検出**からのチャネルデータの保護を提供し、高**信頼**通信チャネルを提供するために 802.11-2007、802.1X、EAP-TLS を使用しなければならない。

FTP_ITC.1.2 TSF は、TSF が高信頼チャネル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。

FTP_ ITC.1.3 TSF は、接続されたネットワークを介した他の通信の前に、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。

適用上の注意：

125 *上記の要件の目的は、TOE とアクセスポイント間の通信を保護するための要件で特定された暗号プロトコルを使用することである。*

126 *要件は、通信が最初に確立されたときだけでなく、停止後再開した時にも保護されていることを示す。この場合他の通信を TOE のセットアップの一部に手動トンネルの設定が含まれている可能性があり、停止後に、TOE が（必要に応じて）手動による介入を伴って自動的に通信を再確立しようとした場合、攻撃者が重要な情報を得るや、接続を侵害する機会を与える。*

保証アクティビティ：

127 *評価者は、仕様書に反映されない場合がある TOE 固有のオプションや手順と共に、要件で指定された暗号プロトコルの面でアクセスポイントに接続された TOE の詳細を説明していることを判断するために TSS を検査しなければならない。評価者はまた、TSS に記載されているすべてのプロトコルが ST の要件で指定されており、含まれていることを確認しなければならない。評価者は、運用ガイダンスにアクセスポイントへの接続を確立するための手順が含まれていること及び接続が意図せずに中断された場合の回復手順が記載されていることを確認しなければならない。評価者は、次のテストを実行しなければならない：*

- *テスト 1：評価者は、運用ガイダンスで説明されるように接続を設定し、通信を確保して、TOE が要件で指定されたプロトコルを使用してアクセスポイントとの通信を開始できることを確実にしなければならない。*
- *テスト 3：認証 IT エンティティを備えた各通信チャネルについて、評価者は、チャネルのデータが平文で送信されていないことを確実にしなければならない。*
- *テスト 5：評価者は物理的にアクセスポイントへの TOE からの接続を中断しなければならない（例えば、TOE ホストをアクセスポイントの範囲外に動かす、アクセスポイントをオフにするなど）。自動的に接続を再開するか、または新しいアクセスポイントに接続する何らかの試行の場合、評価者は、その後の通信が適切に最低限に保護されていることを確認しなければならない。*

128 *さらなる保証アクティビティは、特定のプロトコルに関連付けられている。*

4.2 セキュリティ機能要件根拠

129 本節では、節 4.1 で定義されている TOE セキュリティ機能要件の根拠を説明する。表 10 は、目的が要件で対処されているという対応する論理的根拠を持つセキュリティ機能要件からセキュリティ目標へのマッピングを示す。

130 ベンダによって提供されるセキュリティターゲット（ST）には、2 つの節から構成されるセキュリティ要件根拠が含まれている：

- どの SFR が TOE のセキュリティ対策方針に対処しているかを示すトレーシング
- TOE のすべてのセキュリティ目標が事実上 SFR によって対処されている（CC パート 1 あたり、節 B7）ことの正当さの説明。

表 10：TOE セキュリティ機能要件根拠

対策方針	対策方針に対処する要件	根拠
O.AUTH_COMM TOE は、承認アクセスポイントであることを装った他のエンティティで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確認する手段及びその ID のアクセスポイントへの保証を提供する。	FCS_CKM.1 FCS_COP.1(2) FCS_EAP-TLS_EXT.1 FIA_8021X_EXT.1 FIA_X509_EXT.1 FTP_ITC.1	FTP_ITC.1（及びサポート要件 FCS_CKM.1、FCS_COP.1 （ 2 ）、 FCS_EAP-TLS_EXT.1 、FIA_8021X_EXT.1、と FIA_X509_EXT.1）では、TOE が TOE とリモート管理者及び情報暴露または改ざんからこのチャネルを通過するデータを保護する高信頼 IT エンティティの間に個別の通信チャネルを作成するメカニズムを提供する必要がある。これは要件で指定されたプロトコルを使用して暗号的に行われ、これらのプロトコルは、チャネルデータのエンドポイント及び保護の確実な相互認証を提供するものである。
O.CRYPTOGRAPHIC_	FCS_CKM.1 FCS_CKM.2	FCS_CKM.1 は、対称鍵を生成する。これらの鍵は、FCS_COP.1（5）で指定された AES 暗号化／

対策方針	対策方針に対処する要件	根拠
FUNCTIONS TOE は、機密性を維持し、TOE とそのホスト環境の外で送信されるデータの変更の検出を可能にするために暗号化機能（すなわち、暗号化／復号と電子署名の操作）を提供しなければならない。	FCS_CKM_EXT.4 FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) FCS_COP.1(5) FCS_RBG_EXT.1 FIA_X509_EXT.1	復号機能によって使用される。FCS_CKM.2 は、ワイヤレスクライアント通信のための暗号鍵の配布方法が標準に準拠しており露出しないことを保証する。 FCS_CKM_EXT.4 は、鍵を確実にするための機能を提供し、鍵マテリアルがゼロ化されている。TOE は、ほとんどの場合、ホスト上で実行されているソフトウェアの実体であるため、この要件の範囲は、ソフトウェアがデータを消去するため、適切な関数を呼び出していることを確認することである。ホストは最終的にデータがクリアであることを確認する責任がある。 FCS_COP.1（1）は、AES が PP で指定された様々なプロトコルの暗号化と復号の操作を実行するために使用されることを指定する。 FCS_COP.1（2）では、電子署名の機能は、高信頼更新のために TOE に実装されており、証明書の操作がトラフィックを保護するために使用されるプロトコルに関連付けられていることが必要である。 FCS_COP.1（3）FCS_COP.1（4）は、TSF は、データの整合性の検証と非データの整合性操作のための Secure Hash Algorithm のアルゴリズムの実装を使用してハッシュサービスを提供することを必要とする。 FIA_X509_EXT.1 は、前述の暗号化操作の多くをサポートするために使用される証明書が適切な規格に準拠していることを必要とする。 FCS_RBG_EXT.1 は、ロバストなランダムビット生成機能が存在することを必要とする。
O.PROTOCOLS TOE は、標準化されたプロトコルが TOE から RFC または業界の仕様書に実装されていることを確認する。	FCS_EAP-TLS_EXT.1 FIA_8021X_EXT.1 FTP_ITC.1	FCS_EAL-TLS_EXT.1 、 FIA_8021X_EXT.1 、 FTP_ITC.1（802.11-2007 用）は全て、実装を必要とするプロトコルに適用される基準を参照する（またそれらの規格上の制限を示す）。
O.RESIDUAL_INFOR	FCS_CKM_EXT.4 FDP_RIP.2	FCS_CKM_EXT.4 は、不要になった全ての暗号鍵の破壊を保証する。 FDP_RIP.2 は、資源の内容は明示的にデータへ

対策方針	対策方針に対処する要件	根拠
MATION_CLEARING TOE は、資源が再割付された際、保護された資源に含まれている全てのデータが利用不可能であることを保証する。		のアクセス権を付与された対象以外には使用できないことを確認するために使用される。パケットの内容が後続のパケットで暴露されることを防ぐため、本 TOE では、ネットワークパケットを構築するために使用されるメモリがクリアされること、またはいくつかのバッファ管理方式が採用されていることが不可欠である（例えばパディングがパケットの構築に使用されている場合、これに別の利用者データや TSF データを含めてはならない）。
O.SYSTEM_MONITORING TOE は、監査データを生成する機能を提供する。	FAU_GEN.1 FAU_SEL.1	FAU_GEN.1 は TOE が記録することができなければならない一連の事象を定義し、FAU_SEL.1 はどの監査対象事象が監査証跡に記録されるかを管理者が設定できるようにする。
O.TOE_ADMINISTRATION TOE は、管理者が TOE を構成することができるようにするメカニズムを提供する。	FAU_SEL.1 FMT_SMF.1	FAU_SEL.1 は、監査事象が記録されるよう設定する能力を必要とし、FMT_SMF.1 は、TOE の他の部分の構成要件を提供する。はじめにで述べたように、TOE は管理役割を提供する必要はないが、IT 環境と組み合わせられた TOE は、これらの機能をホストマシンの一般利用者のサブセットに制限することができなければならない。
O.TSF_SELF_TEST TOE は、セキュリティ機能の一部のサブセットをテストする機能を提供し、これが正常に動作していることを確認する。	FPT_TST_EXT.1	FPT_TST_EXT.1 は、TOE が TSF の正しい動作を保証し格納されている実行ファイルの成功性の問題を検出するために、セルフテストのスイートを提供することを必要とする。
O.VERIFIABLE_UPDATES TOE は、TOE への更新が変更されないこと及びこれが（オプショ	FCS_COP.1（2） FCS_COP.1（3） FPT_TUD_EXT.1	FCS_COP.1（2）と FCS_COP.1（3）は、電子署名アルゴリズムと更新の検証に使用されるハッシュ関数を指定する。 FPT_TUD_EXT.1 は実行中のファームウェアのバージョンを確認する更新を開始し、インストール前に TOE へのファームウェア／ソフトウェアの更新を確認する方法を提供する。

対策方針	対策方針に対処する要件	根拠
ンで)信頼できるソースからのものであることを管理者が検証できることを確保するための機能を提供する。		
O.WIRELESS_ACCES S_POINT_CONNECTI ON TOE は、接続先のワイヤレスアクセスポイントを制限する機能を提供する。	FTA_WSE_EXT.1	FTA_WSE_EXT.1 は、アクセスポイントの識別情報に基づいてワイヤレスアクセスポイントへのアクセスを制御する機能を提供する。

4.3 セキュリティ保証要件

131 3 節の TOE のセキュリティ対策方針は、2.1 節と 2.2 節の「組織のセキュリティ対策方針」で識別された脅威に対処するために構築された。4.1 節のセキュリティ機能要件（SFR）は、セキュリティ対策方針の正式なインスタンス化である。

132 4 節への導入部で示すように、本節には CC からの SAR の完全なセットが含まれているが、評価者によって実行される保証アクティビティは本節及び 4.1 節に記載されている。

133 ファミリごとに、開発者によって提供される必要がある追加の証拠資料／アクティビティ（存在する場合）を明確にするために、開発者アクションエレメントに「開発者向け注意事項」が提供される。内容／記述と評価アクティビティエレメントについては、追加の保証アクティビティ（既に 4.1 節に含まれている保証アクティビティ）が、エレメントごとではなく、ファミリ全体として記述されている。さらに、本節に記述されている保証アクティビティは、4.1 節に規定されているものに対する補足である。

134 表 11 にまとめた TOE セキュリティ保証要件は、本 PP の 2 節で識別される脅威と方針に対処するために要求される管理・評価アクティビティを特定する。4.4 節では、本 PP の一連の保証要件を選択するための根拠を簡潔に提供する。

表 11：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	保証コンポーネントの説明
開発	ADV_FSP.1	基本的な機能仕様
ガイダンス文書	AGD_OPE.1	利用者運用ガイダンス
	AGD_PRE.1	調製用利用者ガイダンス

テスト	ATE_IND.1	独立テスト - 適合
脆弱性評価	AVA_VAN.1	脆弱性分析
ライフサイクルサポート	ALC_CMC.1	TOE のラベリング
	ALC_CMS.1	TOE の CM 範囲

4.3.1 クラス ADV：開発

135 本 PP に適合する TOE については、TOE に関する情報は、最終利用者が利用できるガイダンスマニュアル及び ST の TOE 要約仕様（TSS）の部分に記載される。TOE の開発者が TSS を書くことは必要でないが、TOE の開発者は、機能要件に関連した TSS に含まれている製品の説明に同意する必要がある。4.1 節に含まれている保証アクティビティは、TSS の節の適切な内容を決定するのに十分な情報と ST の作者を提供する必要がある。

4.3.1.1 ADV_FSP.1 基本機能仕様

136 機能仕様は TOE セキュリティ機能インタフェース（TSFI）について説明する。これは、これらのインタフェースの形式的または完全な仕様を備えている必要はない。さらに、本 PP に適合する TOE は、必ず TOE 利用者（管理者利用者を含む）が直接起動可能な運用環境へのインタフェースを有するため、このようなインタフェースには間接的なテストのみ可能であるかもしれない。従って、このようなインタフェースを単体で説明することにはほとんど意味がない。本 PP のファミリ用のアクティビティは機能要件に応じて TSS で提示されるインタフェース及び AGD の文書に示されているインタフェースを理解することに焦点を当てるべきであり、追加の「機能仕様」文書が指定された保証アクティビティを満たす必要はない。

137 TOE へのインタフェースを理解する上で、対処すべき脅威は、攻撃者がワイヤレス接続を介して有線ネットワークへの不正アクセスを得ることであるということを考慮しなければならない。ワイヤレスクライアントと有線ネットワーク間の通信をサポートする TOE インタフェースは、認証された利用者のみがアクセスを許可され、暗号化トンネルが確立されている保護を必要とする重要なインタフェースである。ワイヤレスクライアントインタフェースに加え、管理インタフェース（TOE が設定されている方法）も記述する必要がある。

138 評価する必要があるインタフェースは、独立した、抽象的なリストとしてというよりは、記載されている保証アクティビティを行うために必要とされる情報を通じて特徴づけられる。

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。

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

開発者向け注意事項：本節の導入部に示すように、機能仕様は、ST の TSS で提供される情報と共に、AGD_OPR と AGD_PRE の文書に含まれる情報で構

成される。機能要件の保証アクティビティとは、マニュアル及び TSS 節に存在しなければならない証拠を指す。これらは直接 SFR に関連付けられているため、要素 ADV_FSP.1.2D でのトレースは既に暗黙的に行われ、追加の文書化は必要ない。

内容と記述エレメント：

ADV_FSP.1.1C　機能仕様は、SFR を実施し SFR をサポートする各 TSFI について、使用の目的と方法を記述しなければならない。

ADV_FSP.1.2C　機能仕様は、SFR を実施し SFR をサポートする各 TSFI に関連付けられたすべてのパラメタを識別しなければならない。

ADV_FSP.1.3C　機能仕様は、SFR 非干渉としてのインタフェースの暗黙的な分類の根拠を提供しなければならない。

ADV_FSP.1.4C　追跡は、機能仕様における TSFI に対する SFR の追跡を実証しなければならない。

評価者アクションエレメント：

ADV_ FSP.1.1E　評価者は、提供される情報が証拠の内容と記述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。

ADV_ FSP.1.2E　評価者は、機能仕様が SFR の正確かつ完全なインスタンス化であることを決定しなければならない。

保証アクティビティ：

139　*これらの SAR に関連する特定の保証アクティビティはない。機能仕様の文書は、4.1 節で説明する評価アクティビティ及び AGD、ATE、AVA SAR についての説明に含まれるその他のアクティビティを支援するために提供されている。機能仕様情報の内容に関する要件は、実行された他の保証アクティビティによって暗黙的に評価される。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行することができない場合、十分な機能仕様が提供されていない。*

4.3.2　クラス AGD：ガイダンス文書

140　ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、管理モデルの記述と、運用環境（WLAN クライアントをホストするシステム）がセキュリティ機能の役割を満たすことを管理者が確認する方法の記述を含める必要がある。文書は管理者に読みやすい砕けたスタイルでなければならない。

141　ガイダンスは、ST で述べられた通り、製品がサポートするすべての運用環境について提供されなければならない。ガイダンスには以下が含まれる：

- この環境における TOE の正常なインストールの指示
- 製品として及び大規模な運用環境のコンポーネントとしての TOE のセキュリティ管理の指示
- TOE の機能、環境機能、または両者の組み合わせのいずれかを使用して保護された管理機能を提供するための指示

142　特定のセキュリティ機能に関連するガイダンスも作成される。そのような指導上の要件は、4.1 節で指定された保証アクティビティに含まれる。

4.3.2.1 AGD_OPE.1　利用者運用ガイダンス

開発者アクションエレメント：

AGD_OPE.1.1D　開発者は利用者運用ガイダンスを提供しなければならない。

開発者向け注意事項：ここで情報を繰り返すよりも、評価者がチェックされることを指導の詳細を確認するため、開発者はこのコンポーネントの保証アクティビティを確認する必要がある。これにより十分なガイダンスの作成のために必要な情報が提供される。

内容と記述エレメント：

AGD_OPE.1.1C　各利用者の各役割について利用者運用ガイダンスは、セキュアな処理環境で制御されるべき、利用者がアクセスできる機能と権限（適切な警告など）を記述しなければならない。

AGD_OPE.1.2C　各利用者の各役割について利用者運用ガイダンスは、セキュアな方法で TOE が提供する利用可能なインタフェースを使用する方法について説明しなければならない。

AGD_OPE.1.3C　各利用者の各役割について利用者運用ガイダンスは、必要に応じてセキュアな値を示しつつ、利用可能な機能とインタフェース、特に利用者の制御下にあるすべてのセキュリティパラメタを記述しなければならない。

AGD_OPE.1.4C　各利用者の各役割について利用者運用ガイダンスは、実行する必要がある利用者がアクセス可能な機能への相対的なセキュリティ関連事象（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）の各タイプを明示しなければならない。

AGD_OPE.1.5C　利用者運用ガイダンスは、（故障や動作エラーに続く操作を含む）TOE

の操作のすべての可能なモード､その結果及びセキュアな動作を維持するための含意を識別しなければならない。

AGD_OPE.1.6C　ST で説明するように運用環境のセキュリティ目標を達成するために従うべきセキュリティ対策を記述しなければならない。

AGD_OPE.1.7C　利用者運用ガイダンスは、明確かつ合理的でなければならない。

評価者アクションエレメント：

AGD_OPE.1.1E　評価者は、提供される情報が証拠の内容と記述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。

保証アクティビティ：

143　操作中、ガイダンスに記載されるべきアクティビティは、（管理者以外の）利用者によって実行されているものと、管理者によって実行されているものの 2 つの広範なカテゴリに分類される。これは、管理者以外の利用者に必要なほとんどの手続きは 4.1 節の保証アクティビティで参照されていることに留意する。

144　管理機能に関して、いくつかは 4.1 節で説明済みであるが、以下の追加情報が必要である。

145　運用ガイダンスは、少なくとも、操作中に TOE で評価構成が実行されている（または実行できる)、ネットワークインタフェース上で受信されるデータを処理できるプロセスを一覧表示しなければならない（複数が存在する可能性があり、これはネットワークインタフェース上で「リスンする」プロセスに限られない)。ネットワークデータを処理するものだけを決定しようとするよりも､TOE で評価された構成で実行されている(または実行できる)すべてのプロセスを一覧表示した方がよい。記載されているプロセスごとに、管理ガイダンスは、プロセスの機能とサービスが実行されるために用いられる特権についての短い（1～2 行）説明を含む。「特権」には、ハードウェアの特権レベル（例えば、リング 0、リング 1)、特にプロセスに関連付けられている任意のソフトウェアの権限、プロセスが実行されている利用者の役割に関連付けられている権限が含まれる。

146　運用ガイダンスは､TOE の評価構成に関連付けられた暗号化エンジンを構成するための手順を含まなければならない。これは管理者に、他の暗号化エンジンのその使用は、TOE の CC 評価中に評価またはテストされていない旨の警告を提供しなければならない。

147　この文書では、ハッシュを確認するか電子署名を検証するかして､TOE への更新を確認するためのプロセスを記述する必要がある。評価者は、このプロセスは、次の手順が含まれていることを確認しなければならない：

- ハッシュについては、特定の更新のためのハッシュを得ることができる場所の説明が入手可能である。FCS_COP.1 (2) メカニズムによって使用される証明書を取得するための、電子署名、手順については、署名された更新は、証明書の所有者から受信されていることを確認する。これは、最初に製品に同梱されるか、または他の手段によって入手できる。

- 更新自体を取得するための指示。これは、TOE への更新をアクセシブルにするための指示（例えば、特定のディレクトリ内への配置）を含める必要がある。
- 更新プロセスの開始及び処理が成功または失敗したかどうかを識別するための指示。これにはハッシュ／電子署名の生成が含まれる。

4.3.2.2 AGD_PRE.1 詳細化手順

開発者アクションエレメント：

AGD_PRE.1.1D 開発者は、その詳細化方法と共に TOE を提供しなければならない（shall）。

開発者向け注意事項：運用ガイダンスと同様、開発者は詳細化手順に関して必要な内容を決定するために保証アクティビティに目を向ける必要がある（should）。

内容と記述エレメント：

AGD_ PRE.1.1C 詳細化手順は、開発者の配付手続きに従い、配付される TOE のセキュアな受入に必要なすべての手順を説明しなければならない(shall)。

AGD_ PRE.1.2C ST で説明したように、調製手順では TOE のセキュアなインストール及び運用環境のセキュリティ対策方針に基づき運用環境のセキュアな準備に必要なすべての手順を説明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、提供される情報が証拠の内容と記述のために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 がセキュアな操作のために準備され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：

148 上記の導入部に示すように、特に TOE 機能要件をサポートするための運用環境を設定するときのドキュメンテーションに関して重要な期待がある。評価者は、TOE のガイダンスが適切に ST 内で TOE に対して主張されているすべてのプラットフォーム及びコンポーネント（つまり、ハードウェア及びオペレーティングシステムの組み合わせである）に言及していることを確認しなければならない。

149 評価者は、以下のガイダンスが提供されていることを確認しなければならない。

- 序文に示されるように、TOE の管理は、TOE のすべての利用者のグループのサブセットである 1 名または複数名の管理者によって実行される。システム全体（TOE と運用環境）は、この機能を提供しなければならないが、機能性の実装のための責任は、完全な運用環境の責任から完全な TOE の責任まで、変化する場合がある。高レベルでは、運用環境がその担当機能の一部を提供するように構成されるよう、ガイダンスは適切な指示を含まなければならない。TOE が利用者の集団から管理者利用者の分離を可能にするメカニズムを提供していない場合、手順は例えば OS I&A メカニズムの OS の構成をカバーし利用者に固有の(OS ベース)のアイデンティティを提供し、TOE の管理者は、管理の実行可能ファイルへのアクセス権を持つよう、追加のガイダンスは TOE の管理者 ID（または ID）を使用して OS の DAC メカニズムの構成上のインストーラを指示する。TOE がこの機能の一部または全部を提供している場合、適切な要件は ST の付録 C に含まれ、これらの要件に関連付けられている保証アクティビティは、TOE 及び運用環境の両方に必要なガイダンスについて詳説する。

評価者は、次のテストを実行しなければならない：

- テスト 1［条件付］：すべての TOE 利用者からの管理者利用者の分離が運用環境の設定のみによって実行された場合、評価者は、ST に記載の構成ごとに、管理者ガイダンスに従ってシステムを構成した後、管理者以外の利用者が TOE の管理機能にアクセスすることができないことを確認する。

4.3.3 クラス ATE: テスト

150 テストは、システムの機能的側面と共に設計や実装上の弱点を利用した側面において指定されている。前者は、ATE_IND ファミリを介して行われ、後者は AVA_VAN ファミリを介している。本 PP で指定された保証レベルにおいて、テストは設計情報の可用性に依存したアドバタイズ機能とインタフェースに基づいている。評価プロセスの主要出力の一つは、次の要件に指定されたテスト報告書である。

4.3.3.1 ATE_IND.1 独立テスト - 適合

151 TSS に記述されている機能と同様に提供される管理（構成及び操作を含む）の資料を確認するためのテストが実行される。テストの焦点は、SAR のためのいくつかの追加のテストが 4.3 節で指定されているが、4.1 節で指定された要件が満たされていることを確認することである。アクティビティ活動は、これらのコンポーネントに関連付けられている最低限のテストアクティビティを識別する。評価者はテスト計画とテストの結果を文書化する報告書と同様、本 PP への適合を主張しているプラットフォーム／TOE の組み合わせに焦点を当てたカバレージ論証を作成する。

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に TOE を提供しなければならない。

内容と記述エレメント：

ATE_IND.1.1C　TOE は、テストに適したものとする。

評価者アクションエレメント：

ATE_IND.1.1E　評価者は、提供される情報が証拠の内容と記述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。

ATE_IND.1.2E　評価者は、TSF が指定どおりに動作することを確認するため、TSF のサブセットをテストしなければならない。

保証アクティビティ：

152　評価者は、システムのテストの側面を文書化するテスト計画及び報告書を作成しなければならない。テスト計画は、本 PP の保証アクティビティの本文に含まれるテストのアクションのすべてをカバーする。保証アクティビティに記載されているテストごとにテストケースを用意する必要はないが、評価者は ST の該当する各テストの要件がカバーされていることをテスト計画に記載する必要がある。

153　テスト計画はテストするプラットフォームを識別し、テスト計画に含まれているが ST には含まれていないプラットフォームについては、テスト計画でプラットフォームをテストしていない理由を説明する。この説明はテストされたプラットフォームとテストされていないプラットフォームの違いに言及し、差異が実行されるテストに影響を与えないという議論を行う必要がある。違いが全く影響を持たないと単純に断定するだけでは十分でなく、論理的根拠を提供する必要がある。ST に記載されているすべてのプラットフォームがテストされている場合根拠は全く必要ない。

154　テスト計画は、テストする各プラットフォームと AGD 文書に記載されていたもの以外に必要な任意のセットアップの構成を説明する。評価者はテストの一部として、または標準テスト前の条件として各プラットフォームのインストールとセットアップのために AGD 文書に従うことが期待されていることに留意する。これには特別なテストドライバやツールが含まれる場合がある。各ドライバやツールについて、ドライバやツールが TOE とそのプラットフォームによる機能のパフォーマンスには悪影響を与えないよう論証（単なる主張ではなく）が提供される。

155　テスト計画は、ハイレベルのテストの目的だけでなく、それらの目的を達成するために従うべきテスト手順を示す。これらの手順には、期待される結果が含まれる。テスト報告書には（単なるテスト計画の注釈付きのバージョンでありうる）の詳細なテスト手順が実行されたときに発生したアクティビティと、テストの実際の結果が含まれる。これは累積的なアカウントでなければならず、従ってテストが失敗に終わり、修正がインストールされ、テストが再度行われて成功した場合、報告書は「成功」だけでなく「失敗」と「成功」について示す。

4.3.4 クラス AVA:　脆弱性評定

156　このプロテクションプロファイルの最初の生成については、評価機関は、これらのタイプの製品にどのような脆弱性が発見されているかを発見するためにオープンソースを調査することが期待されている。ほとんどのケースでは、これらの脆弱性は、基本的な攻撃者を超えた洗練を必要とする。侵入ツールが作成され、一様に評価機関に配布されるまでは、評価者は、TOE のこれらの脆弱性をテストすることは期待されない。評価機関はこれらの脆弱性の可能性についてベンダから提供された文書に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や将来のプロテクションプロファイルの開発のために使用される。

4.3.4.1 AVA_VAN.1　脆弱性調査

開発者アクションエレメント：

AVA_VAN.1.1D　開発者はテスト用の TOE を提供しなければならない。

内容と記述エレメント：

AVA_VAN.1.1C　TOE はテストに適していなければならない。

評価者アクションエレメント

AVA_VAN.1.1E　評価者は、提供される情報が証拠の内容と記述のために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。

VA_VAN.1.2E　評価者は、TOE の潜在的な脆弱性を識別するためのパブリックドメインソースの検索を実行しなければならない。

AVA_VAN.1.3E　評価者は、TOE が基本的な攻撃能力を持つ攻撃者によって実行される攻撃に耐性があることを決定するために、識別された潜在的な脆弱性に基づいて、侵入テストを実施しなければならない。

保証アクティビティ：

157　ATE_IND と同様、評価者はこの要件に関して、その結果を文書化する報告書を生成しなければならない。この報告書は、物理的に ATE_IND に記載されている全体のテスト報告書、または別の文書の一部である可能性がある。評価者は、一般的にワイヤレス LAN クライアント製品で発見されている脆弱性及び特定の TOE に関係する脆弱性を決定するため、パブリック情報の検索を実行する。評価者は調べられるソースと報告書で発見された脆弱性を文書化する。発見された各脆弱性について、評価者はその非適用性に関しての理論的根拠

を提供するか、適切な場合はこの脆弱性を確認するためにテスト（ATE_IND で提供されるガイドラインを使用する）を策定する。適合性は、脆弱性を悪用するために必要な攻撃手口を評価することによって決定される。例えばブート時にキーの組み合わせを押すことで脆弱性を検出できる場合、本 PP の保証レベルのテストが適しているといえる。例えば脆弱性を悪用するために電子顕微鏡と液体窒素のタンクが必要な場合、テストは適切でなく、適切な正当化が策定される。

4.3.5 クラス ALC: ライフサイクルサポート

158 本 PP に適合する TOE のため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、最終利用者に対し可視的なライフサイクルのさまざまな側面ではなく、TOE のベンダの開発及び構成管理プロセスの検査に限定されている。これは開発者が製品の全体的な信頼に貢献するプラクティスの重要な役割を減少させるためのものではない。むしろ、それはこの保証レベルでの評価に利用できるようにするための情報の反映である。

4.3.5.1 ALC_CMC.1 TOE のラベル付け

159 このコンポーネントは、同じベンダの他製品またはバージョンと区別することができ、最終利用者によって調達される際に簡単に指定できるよう、TOE の識別を対象としている。

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 の参照を提供しなければならない。

内容と記述エレメント：

ALC_CMC.1.1C TOE は、その一意の参照でラベル付けしなければならない。

評価者アクションエレメント：

ALC_CMC.2.1E 評価者は、提供される情報が証拠の内容と記述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。

保証アクティビティ：

160 評価者は、ST が特に ST の要件を満たしているバージョンを識別する識別子（例えば製品名／バージョン番号）を含んでいることを確保するために ST を確認しなければならない。さらに評価者は、バージョン番号は ST のものと一致していることを確かめるためにテストのために受け取った AGD のガイダンスと TOE のサンプルを確認しなければならない。ベンダがウェブサイト上で TOE の広告を維持する場合、評価者は、ST の情報は、製品を区別するために十分であることを確認するためにウェブサイト上の情報を調べなければならない。

4.3.5.2 ALC_CMS.1　TOE CM カバレージ

161　TOE とそれに関連する評価証拠要件の適用範囲を考慮し、このコンポーネントの保証アクティビティは ALC_CMC.1 に挙げられる保証アクティビティでカバーされている。

開発者アクションエレメント：

ALC_CMS.2.1D　開発者は、TOE の構成リストを提供しなければならない。

内容と記述エレメント：

ALC_CMS.2.1C　構成リストには、以下を含まなければならない：TOE 自体、及び SAR で必要とされる評価証拠。

ALC_CMS.2.2C　構成リストは、構成項目を一意に識別しなければならない。

評価者アクションエレメント：

ALC_CMS.2.1E　評価者は、提供される情報が、証拠の内容と記述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。

保証アクティビティ：

162　本 PP の「SARS *が要求する*評価証拠」は、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共に ST 内の情報に限定される。TOE が明確に特定されていること及びこの識別が ST と AGD ガイダンス（ALC_CMC.1 の保証アクティビティで行われる通り）と一致していることを保証することにより、評価者は暗黙的に、このコンポーネントに必要な情報を確認する。

4.4　セキュリティ保証要件根拠

163　これらのセキュリティ保証要件の選択の根拠は、これがこの技術の最初の標準プロテクションプロファイルであるということである。最初のプロテクションプロファイルは開発のベストプラクティスを保証するために使用される。これらの製品タイプに脆弱性が発見された場合、実際のベンダプラクティスに基づいてより厳格なセキュリティ保証要件が義務付けられる。

附属書 A:サポート表、参考文献、頭字語

[1] Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009（情報技術セキュリティ評価（CC）バージョン 3.1、R3　2009 年 7 月）

[2] Draft Consistency Instruction Manual, for Basic Robustness Environments, Release 4.0, CC version 3.1, 2008（基本的なロバスト性環境のための整合性指示書ドラフト　リリース 4.0、CC バージョン 3.1　2008 年）

[3] Federal Information Processing Standard Publication （FIPS-PUB）140-2(連邦政府情報処理規格出版物 140-2)、Security Requirements for Cryptographic- Modules, National Institute of Standards and Technology May 25, 2001（暗号モジュールのセキュリティ要件、国立標準技術研究所、2001 年 5 月 25 日）（変更通知 2002 年 12 月 3 日）

[4] Federal Information Processing Standard Publication(連邦政府情報処理規格出版物）（FIPS-PUB）180-3、Secure Hash Standard, October 2008(セキュアハッシュ規格、2008 年 10 月）

[5] Federal Information Processing Standard Publication(連邦政府情報処理規格出版物）(FIPS-PUB) 186-3、Digital Signature Standard (DSS), June 2009(電子署名規格 (DSS)、2009 年 6 月）

[6] Federal Information Processing Standard Publication (FIPS-PUB) 197 連邦政府情報処理規格出版物 (197、Advanced Encryption Standard の仕様 (AES)、2001 年 11 月 26 日

[7] NIST　Special Publication SP800-38C、Recommendation for Block Cipher Modes of Operation:
The CCM Mode for Authentication and Confidentiality, NIST　SP May 2004 ブロック暗号モードのための推奨事項：認証と機密性のための CCM モード、2004 年 5 月

[8] NIST　Special Publication　SP800-57、Recommendation for Key Management, NIST SP　March 2007 鍵管理のための推奨事項、2007 年 3 月

[9] NIST　Special Publication 800-63、Electronic Authentication Guideline, NIST SP　April 2006 電子認証ガイドライン 2006 年 4 月

[10] NIST Special Publication　800-90、Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) ,NIST　SP　March 2007　決定論的ランダムビット生成器を使用した乱数生成のための推奨事項（改訂版)、2007 年 3 月

[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 NSA 版セキュリティと侵入検出用語集、Greg Stockdale、NSA 情報システムセキュリティ機構、1998 年 4 月。 4009 CNSS に更新する必要あり。

[12] RFC 2865 Remote Authentication Dial In User Service (RADIUS), June 2000 RFC 2865 利用者サービスにおけるリモート認証ダイヤル (RADIUS)、2000 年 6 月

[13] RFC 2868 RADIUS Attributes for Tunnel Protocol Support, June 2000 RFC 2868 トンネルプロトコルサポートのための RADIUS 属性、2000 年 6 月

[14] RFC 3575 IANA Considerations for RADIUS, July 2003 RFC3575 RADIUS のための IANA の考慮事項、2003 年 7 月

[15] RFC 3579 RADIUS (Remote Authentication Dial In User Service Support For Extensible
Authentication Protocol (EAP), September 2003 RFC3579 RADIUS (拡張認証プロトコル (EAP) のためのリモート認証ダイヤルイン利用者サービスサポート、2003 年 9 月

[16] RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, September 2003 RFC 3580 IEEE 802.1X 利用者サービスにおけるリモート認証ダイヤル (RADIUS) 使用上のガイドライン、2003 年 9 月

[17] RFC 5216 The EAP-TLS Authentication Protocol, March 2008 RFC5216 EAP-TLS 認証プロトコル、2008 年 3 月

[18] WPA2 Standard (WPA2 規格)

AES	Advanced Encryption Standard
AF	Authorization factor (認可ファクタ)
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-Shel (市販の)
CMVP	Cryptographic Module Validation Program(暗号化モジュール試験及び認証制度)
DRBG	Deterministic Random Bit Generator (決定論的ランダムビット

	生成器）
DoD	Department of Defense（米国国防総省）
EAL	Evaluation Assurance Level（評価保証レベル）
ES	Encryption Subsystem（暗号化サブシステム）
FIPS	Federal Information Processing Standards（連邦政府情報処理規格）
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）
OSP	Organization Security Policy（組織のセキュリティ方針）
PP	Protection Profile（プロテクションプロファイル）
PUB	Publication（出版）
RBG	Random Bit Generator（ランダムビット生成器）
SAR	Security Assurance Requirements（セキュリティ保証要件）
SF	Security Function（セキュリティ機能）
Security Functional Requirement	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 Functionality （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）

附属書 B: NIST SP 800-53/CNSS 1253 マッピング

NIST SP800-53/CNSS1253 管理策のいくつかは、適合 TOE によって完全にまたは部分的に対処されている。本節は、取り上げられた要件を概説しており、TOE が運用構成に組み込まれるときに要求される追加テスト（存在する場合）を認証担当者が決定するために利用できる。

適用上の注意：本バージョンでは、簡単なマッピングが提供される。将来のバージョンには、認証チームのための更なる情報を提供する追加の説明を含む予定である。この追加情報は、TOE が提供される適合の程度を議論し、マッピングを制御する SFR に関する詳細が含まれる。加えて、指定された保証アクティビティの包括的な見直し、SAR を満たすためのアクティビティの一部として発生する評価アクティビティのレビューが要約され、コンプライアンスを決定した方法（例えば、文書のレビュー、ベンダ主張、テスト／検証の程度）に関する認証チームの情報が提供される。この情報は認証チームに対し、指定された管理策への適合の度合いを判断するため実行する必要のある追加アクティビティを示す（あれば）。

選択については ST が行い、ST は割付を充填するため、ST が完全で評価されるまで最終文章は必ずしも作成されない。従ってこの情報は PP に加え ST にも含まれるべきである。さらに、特定の実装に基づいて評価者が行うアクティビティにはいくつかの解釈（例えば「修正」）が必要となるかもしれない。このスキームは、このタイプの情報を記入するための監督係（例えば認証要員）を設けるか、保証アクティビティの一環としてこれを評価者に行わせてよい。検証アクティビティは、認証チームが評価チームの作業に加え何をしなければならないか（あれば）を決定するために提供しなければならない重要な情報である。

識別子	名称	該当 SFR
AC-3	アクセス（制御の）施行	FMT_SMF.1
AU-2	監査対象事象	FAU_GEN.1
AU-2		FAU_GEN.1
AU-2 (4)	監査記録の内容	FAU_GEN.1
AU-3		FAU_GEN.1
AU-7	監査の低減及び報告書の生成	FAU_SEL.1
AU-10	否認防止	FCS_COP.1(2)
AU-12	監査の生成	FAU_GEN.1
CM-5	変更のためのアクセス制限	FPT_TUD_EXT.1
IA-3	デバイスの識別と認証	FCS_EAP-TLS_EXT.1, FIA_8021X_EXT.1, FTP_ITC
IA-5	認証子の管理	FIA_X509_EXT.1
SC-4	共有資源の情報	FDP_RIP.2
SC-8	伝送の整合性	FTP_ITC.1
SC-9	伝送の機密性	FTP_ITC.1
SC-12	暗号鍵の確立と管理	FCS_CKM.1, FCS_CKM.2,

識別子	名称	該当 SFR
		FCS_CKM_EXT.4
SC-13	暗号の使用	FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_RBG_EXT.1
SI-6	セキュリティ機能の検証	FPT_TST_EXT.1

附属書 C：追加要件

164 *PP の本草案について、この附属書は、サポートする脅威、対策方針、根拠、または（一部の場合）保証アクティビティはなく追加のコンポーネントを含む。このサポート情報は、最初のレビューサイクルと並行して発展し、PP の次のリリースに組み込まれる。本節に含まれる情報（記載された要件が潜在的な準拠 TOE に適用されうるかどうか、またこの付録に含まれていない要件が WLAN クライアント製品に広く適用できるかどうか）に関するコメントが強く望まれる。*

165 本 PP の導入部に示すように、本 PP に適合し、TOE が実装できる機能がいくつかある。これらの機能は IT 環境（例えば TOE 管理者の識別と認証）に依存することになるため、必要ではない。ただし TOE がそのような機能を実装する場合、ST 執筆者は以下の情報を取得し、ST に記載する。この附属書に含まれない要件を ST に含めてもよいが、本 PP への適合性を主張する前に、評価を監督する国内認証機関（スキーム）によるレビュー及び承認を得る必要がある。

C.1 クラス: セキュリティ監査(FAU)

166 監査レビュー、及び/またはストレージが TOE によってサポートされている場合、次の監査要件は必要に応じて ST に含めなければならない。

監査レビュー（FAU_SAR.1）

FAU_SAR.1 監査レビュー

FAU_SAR.1.1 TSF は、**許可された管理者に、**監査記録からすべての**監査データ**を読み取る機能を提供しなければならない（shall）。

FAU_SAR.1.2 **詳細化**：：TSF は、**許可された管理者**が情報を解釈するために~~利用者~~適した形式で監査記録を提供しなければならない（shall）。

制限付き監査レビュー（FAU_SAR.2）

FAU_SAR.2 制限付き監査レビュー

FAU_SAR.2.1 **詳細化**：TSF は**許可された管理者を除く**全ての利用者の**監査証跡における**監査記録への読み取りアクセスを禁止しなければならない。

FAU_STG_EXT.4 監査データ損失の防止

FAU_STG_EXT.4.1　TSF は管理者に対し、監査証跡が満杯の場合、以下のアクションのいずれかまたは複数を選択する機能を提供しなければならない：

a）権限のある管理者が起こしたものを除く監査対象事象の発生を防ぐ

b）最も古い格納監査記録を上書きする

適用上の注意：

167 *TOE は監査対象事象を防ぐことにより、許可された管理者に監査データ損失を防止するためのオプションを用意する。これらの状況下で許可された管理者のアクションが監査される必要はない。TOE はまた、許可された管理者に「古い」の監査記録を上書きする代わりに、サービス妨害攻撃から保護する監査対象事象を予防するためのオプションを提供する。*

C.2 クラス: 識別と認証(FIA)

168 TOE が管理機能を提供している場合には、リモート管理、ローカル管理、及び管理セッションの保護などの機能を規定するために適用できる多くの要件がある。PP の本バージョンについては、クライアントのための機能を規定するためワイヤレスアクセスシステムのプロテクションプロファイルの管理要件を使用してよい。

169 TOE が通信時に使用される証明書を格納及び管理する機能を提供している場合、次の要件が ST に含まれることがある。

X509 証明書（FIA_X509_EXT）

FIA_X509_EXT.2　拡張：X.509 証明書の保管と管理

FIA_X509_EXT.2.2　TSF は証明書を格納し、不正な削除や改変からこれを保護しなければならない。

FIA_X509_EXT.2.3 TSF は権限のある管理者に対し、本 PP で指定されたセキュリティ機能で使用するための X.509v3 証明書を TOE に読み込むための能力を提供しなければならない。

適用上の注意：

170 *FIA_X509_EXT.1.2 は TSF によって使用され処理される証明書に適用される。運用環境内（例えば RADIUS サーバ）の他のコンポーネントによって使用されプロセスされている証明書は、このエレメントでカバーすることを意図されていない。*

保証アクティビティ：

171 *TSS は、本 PP の要件を満たすために使用される証明書が含まれた全ての実装証明書ストアを記述しなければならない。この説明は、証明書がストアに読み込む方法に関する情報及びストアが不正アクセスから保護される方法を含まれなければならない。*

172 *評価者は、証明書を使用する必要があり、システム内の各関数の次のテストを実行しなければならない：*

・テスト 1：評価者は、有効な証明書パスなく証明書を使用すると機能障害が起こることを証明しなければならない。評価者は、証明書や関数で使用する証明書を検証するために必要な証明書を読み込み、正常に機能することを実証しなければならない。評価者はその後いずれかの証明書を削除し、機能が失敗することを示す。

C.3 監査要件

173 ST 執筆者によってこの附属書から選択された特定の要件に応じ、ST 執筆者は選択された要件を、ST の対応する表内に適切な監査対象事象を記載する必要がある。

要件	監査対象事象	追加の監査証跡の内容
FAU_SAR.1	なし。	
FAU_SAR.2	監査記録の読み取りを試行する。	なし。
FAU_STG_EXT.4	監査証跡が容量に達する。	なし。
FIA_X509_EXT.2	証明書の読み込みを試行。 証明書の失効化を試行。	なし。

附属書 D：文書の表記規則

174 英国綴りを米国綴りで置き換えたことを除き、本 PP に使用される表記、書式、及び表記規則は、コモンクライテリア（CC）のバージョン 3.1 と一貫している。PP 読者の訳に立つように一部を抜粋して示す。

175 本 PP で使用される表記、書式、及び表記法は、コモンクライテリア（CC）のバージョン 3.1 と概ね一貫している。ここでは、PP 読者の役に立つように一部を抜粋して示す。CC は、機能要件と保証要件に対していくつかの操作を実行することを許可する。*詳細化*、*選択*、*割付*及び*繰返し*は、CC 3.1 パート 1 の附属書 C4 で定義される。これらの各操作は本 PP で使用される。

176 **詳細化の表記法**

詳細化作業は、要件に詳細を追加するために使用され、要件にさらなる制限を加える。セキュリティ要件の詳細化は要素番号の後に**太字**の「詳細化」の語で示されるとともに要件の追加のテキストに太字で記載される。

選択の表記法

177 **選択**操作は、要件を記載する際に CC によって提供された一つ以上のオプションを選択するために使用される（附属書 C.4.3 第 1 部 CC3.1 を参照）。PP 執筆者によって作られた選択肢は、**太字**、括弧及び「選択」の語の削除によって選択を示す。執筆者が記入する選択は、選択されることになっていることを示すとともに、角カッコで[選択：]と示される。

割付の表記法

178 パスワードの長さ（附属書 C.4.2 第 1 部 CC3.1 を参照）など、指定されていないパラメタに特定の値を割り付けるため、**割付**操作が使用される。PP 執筆者によって作られた割り当ての**太字**の値を表示するので、括弧と「代入」の語が削除される。ST 執筆者が記入する選択は、選択されることになっていることを示すとともに、角カッコで[割付：]と示される。

繰返しの表記法

179 様々な操作（附属書 C.4.1 第 1 部 CC3.1 を参照）でコンポーネントが繰り返されたとき、**繰返し**操作が使用される。繰返し数（iteration_number）は、コンポーネント識別子の後に括弧で表示される。

180 反復操作は全てのコンポーネント上で実行される可能性がある。PP／ST 執筆者は、同じコンポーネントに基づいて複数の要件を含めることにより、反復操作を実行する。コンポーネントの各反復は、そのコンポーネントの他の全ての反復とは異なるものでなければならず、これは割り当てと異なるまたは別の方法で改良を適用することにより選択を完了することで実現される。

拡張要件表記法

181 CC が作者のニーズを満たすために適切な要件を提供していない場合、拡張要件が許可される。拡張された要件は要件の明確化に際し識別され、CC クラス／ファミリ／コンポーネントモデル使用に必要とされねばならない。

適用上の注意

182 適用上の注意には、開発者、評価者、及び ISSE ための一般的な情報とともに、適合 TOE のセキュリティターゲットの構築に関錬または有用であると考えられる追加のサポート情報が含まれる。適用上の注意には、コンポーネントの許可される操作に関するアドバイスが含まれる。

保証アクティビティ

183 脅威を軽減するため、保証アクティビティは TOE に課せられた機能要件の共通評価方法として機能する。アクティビティは、TSS に記載された TOE の特定の側面を分析するための評価者の指示が含まれ、ST 執筆者に TSS の節のこの情報を含める暗黙の要件を課す。将来のバージョンでは別の付属書または文書にこれらの要件を移動する可能性があるが、PP の本バージョンでは、これらのアクティビティは直接、機能及び保証コンポーネントに関連付けられている。

附属書 E：用語

アクセスポイント - ワイヤレスクライアントホストの有線ネットワークホストへのアクセスを可能にするネットワークインタフェースを提供する。一度有線インフラストラクチャの信頼されたノードとして認証されると、AP はワイヤレスクライアントと AP の RF インタフェースとの間のワイヤレスネットワークの暗号化サービスを提供する。

管理者 - TOE を設定する管理者権限を持つ利用者。

認証サーバ - 認証のためワイヤレスクライアントから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 - システムが、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ていることを確認するために使用する情報。クレデンシャル情報は利用者名とパスワードなどの単純なものや、より強力な証明書であることもある。

クリティカルセキュリティパラメタ（CSP） - その暴露または改ざんが暗号モジュールのセキュリティを危険にさらしうるセキュリティ関連の情報（例えば秘密鍵とプライベート鍵、及び、パスワードや PIN などの認証データ）

エントロピー源 - この暗号化機能は、1 つまたは複数のノイズ源からの出力を蓄積することにより、乱数生成器のシードを提供する。機能には、与えられた出力を推測するために必要な最小作業の指標及びノイズ源が正常に動作することを確認するためのテストが含まれる。

拡張認証プロトコル（EAP） - ワイヤレスネットワークで使用する認証フレームワーク。TOE は EAP-TLS をサポートしている。 EAP-TLS は認証サーバとワイヤレスクライアントの両方を認証するために PKI を使用する。

FIPS によって承認された暗号化機能 - 以下のいずれかであるセキュリティ機能（例えば、暗号アルゴリズム、暗号鍵管理技術、認証技術）：(1) 連邦政府情報処理規格（FIPS）に指定されている (2) FIPS に採択され、FIPS の付録または FIPS で参照される文書内で指定されている。

IEEE 802.1X - 有線ネットワークに接続するデバイス（ワイヤレスクライアント）に対する認証メカニズムを定義する、ポートベースのネットワークアクセス制御を行うための IEEE 規格。IEEE 802.1X をサポートするために必要な主なコンポーネントは、サプリカント（ワイヤレスクライアント)、認証システム（TOE）及び認証サーバである。

IT 環境 - TOE 境界の外側にあり TOE の機能とセキュリティ方針をサポートしているハード

ウェアとソフトウェア。

運用環境 - TOE が動作している環境。

SAR（セキュリティ保証要件） - 開発者とセキュリティ機能要件の遵守を実証する研究室の開発と評価の方法論を説明する。SAR は開発者や評価者のために特定のテストを記述する必要がある。

SFR（セキュリティ機能要件） - TOE が満たさなければならないセキュリティ機能を説明する。SFR は特定の技術に合わせて詳細化される。

ST（セキュリティターゲット） - TOE のセキュリティ特性を記述し、識別する。

TOE は、（評価ターゲット）-本 PP の要件に照らして評価されるハードウェア、ソフトウェア及びガイダンスを含む製品の製品やセットを指す。

TOE セキュリティ機能（TSF） - TSP の正しい実施のために依存しなければならない TOE の全てのハードウェア、ソフトウェア、ファームウェアから構成されるセット。

TOE セキュリティ方針（TSP） - アセットの管理・保護・配布方法を規制する一連のルール。

TOE 要約仕様（TSS） - TOE がすべての SFR を満たす方法の記述。

権限のない利用者 - TOE の使用を管理者に承認されていない利用者

附属書 F：PP の識別

タイル：	ワイヤレスローカルエリアネットワーク(WLAN)クライアントのためのプロテクションプロファイル
バージョン：	1.0
スポンサー：	National Information Assurance Partnership (NIAP)
CC バージョン：	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(CC)、バージョン 3.1、R3　2009 年 7 月
キーワード：	認証サーバ、WLAN クライアント、WLAN アクセスシステム、EAP、EAP-TLS、IEEE 802.11、IEEE 802.1X