無線ローカルエリアネットワーク（WLAN）アクセスシステム用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) Access Systems

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_as_v1.0.pdf

Information Assurance Directorate

NSA 情報保証局

2011年 12月 1 日
バージョン 1.0

平成 24 年 3 月 13 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

1　はじめに（イントロダクション） 1
1.1　TOE の PP 概要 1
1.1.1　TOE の用途及び主なセキュリティ機能 1
1.1.2　暗号化 2
1.1.3　管理 2
1.1.4　プロトコル適合 3
1.1.5　TOE 以外の利用可能なハードウェア/ソフトウェア/ファームウェア 3
2　セキュリティ課題記述 4
2.1　脅威 4
2.2　組織のセキュリティ方針 7
2.3　前提条件 7
3　セキュリティ対策方針 8
3.1　TOE に関するセキュリティ対策方針 8
3.2　運用環境に関するセキュリティ対策方針 9
3.3　セキュリティ対策方針の根拠 10
4　セキュリティ要件及び根拠 15
4.1　セキュリティ機能要件 15
4.1.1　セキュリティ監査クラス（FAU） 17
4.1.2　暗号サポートクラス（FCS） 23
4.1.3　利用者データ保護クラス（FDP） 37
4.1.4　識別及び認証クラス（FIA） 38
4.1.5　セキュリティ管理クラス（FMT） 48
4.1.6　TSF 保護クラス（FPT） 51
4.1.7　資源利用クラス 53
4.1.8　TOE アクセスクラス（FTA） 54
4.1.9　高信頼パス/チャネルクラス（FTP） 56
4.2　セキュリティ機能要件の根拠 59
4.3　セキュリティ保証要件 68
4.3.1　ADV クラス：開発 68
4.3.2　AGD クラス：ガイダンス文書 70
4.3.3　ATE クラス： テスト 73
4.3.4　AVA クラス：脆弱性評定 74
4.3.5　ALC クラス：ライフサイクルサポート 75
4.4　セキュリティ保証要件の根拠 76

附属書 A：サポート表と参考文献..... 77
附属書 B：NIST SP 800-53/CNSS 1253 マッピング 79
附属書 C：追加要件 81
附属書 D：本書の表記規則..... 89
附属書 E：用語 91
附属書 F：PP の識別..... 93

表一覧

表 1：脅威 6
表 2：組織のセキュリティ方針 7
表 3：TOE の前提条件..... 7
表 4：TOE に関するセキュリティ対策方針..... 8
表 5：運用環境に関するセキュリティ対策方針 9
表 6：セキュリティ対策方針と脅威及び方針の対応関係 10
表 7：セキュリティ対策方針と前提条件の対応関係 14
表 8：TOE セキュリティ機能要件..... 15
表 9：監査対象事象 18
表 10：TOE セキュリティ機能要件に関する根拠..... 59
表 11：TOE セキュリティ保証要件..... 68

改訂履歴

バージョン	日付	説明
1.0	2011年12月01日	初回リリース

1 はじめに（イントロダクション）

1 本プロテクションプロファイル（PP）は、無線ネットワーク上の機密ではあるが機密扱いになっていないデータを保護するための市販（COTS）の無線ローカルエリアネットワーク（WLAN）の購買をサポートする。本PPでは、WLANとそのサポート環境に関する方針、前提条件、脅威、セキュリティ対策方針、セキュリティ機能要件、及びセキュリティ保証要件を詳述する。

2 主な意図は、WLANアクセスシステムによって対処されている脅威に対抗するために必要なセキュリティ機能要件に関する我々の理解を開発者に明確に伝達することである。STのTOE要約仕様（TSS）での記述は、製品（評価対象）のアーキテクチャ及び重大なセキュリティトランザクションが正しく実装されていることを保証するためのメカニズムを記載することが期待される。

1.1 TOE の PP 概要

3 本書は、WLANアクセスシステムのセキュリティ機能要件を規定する。WLANアクセスシステムは、無線クライアントと有線ネットワーク間のリンクを制御することで、有線ネットワークへの安全な無線アクセスを提供する。TOEは、1つまたは複数の物理コンポーネントによって実装できる。

1.1.1 TOE の用途及び主なセキュリティ機能

4 WLANアクセスシステムは、管理、認証、暗号化、及び移動中のデータの保護と処理をサポートするために集中管理機能、方針、制御、及び暗号化サービスを提供することで、利用者（無線クライアント）と有線ネットワーク（例えば企業ネットワーク）間の安全な通信を提供するための安全な無線アクセスソリューションに寄与する。WLANアクセスシステムでは、ネットワークアクセスを提供する前に、無線クライアントが認証サーバを使用してクライアントを認証して、802.1X認証を実行する必要がある。WLANアクセスシステムは、無線クライアントと認証サーバ間のパススルーデバイスとして機能する。認証が成功する場合のみ、安全な通信トンネルが形成される。認証の成功に続いて、WLANアクセスシステムは、各無線クライアントとのセッション鍵を導出する。WLANアクセスシステムと無線クライアント間の以後のすべての通信が暗号化される。WLANアクセスシステムは、認証された無線クライアントから発信されるトラフィックを復号し、トラフィックをバックエンドネットワークに渡す。同様に、WLANアクセスシステムは、バックエンドネットワークから認証された無線クライアントに送信されるトラフィックを暗号化する。WLANアクセスシステムは、複数の同時無線接続をサポートし、それらのピアとの間の複数の暗号トンネルを確立し、終了することができる。

5 適合TOEは、802.1X認証を使用して、802.11規格の拡張サービスセット（ESS）要件を満たすだろう。独立基本サービスセット（IBSS）操作、または事前共有鍵を使用するESS操作に関連する要件はない。従って、検証される主張もない。

6 TOEは管理の役割を維持する。管理者は、TOEを管理する前に認証されなければならない。WLANアクセスシステムは、管理者ログインを実行するために、リモート認証メカニズム及びローカル認証メカニズムの両方をサポートする。リモート管理者は、例えばSSHまたはTLS/HTTPSによって実装された安全な接続を通じて、WLANアクセスシステムにリモートにアクセスできる。既定では、無線側からTOEを設定する機能は無効になっている。

7 WLANアクセスシステムが複数の物理コンポーネントによって実装されている場合は、コ

ンポーネント間で交換される制御/設定データを保護するために、TOEコンポーネント間の安全なチャネルが提供される。同様に、運用環境内のITエンティティ（RADIUSサーバ、監査サーバ）も、安全なチャネル経由でTOEと通信する。すべてのITエンティティ（TOEコンポーネント及びTOE外部のコンポーネント）は、共有秘密または認証用のX.509v3機械証明書の使用を通じて認証される。

8 WLANアクセスシステムのすべてのコンポーネントが正しく実装され、重大な設計上の誤りが含まれないことが想定される。ベンダは、サポートされるすべての運用環境のためにTOEを正しくインストールし、管理するためのガイダンス文書（AGD_PRE、AGD_OPR）を提供することが要求される。

1.1.2 暗号化

9 WLANアクセスシステムは、地理的に離れている2台のデバイス間を流れる無線トラフィックを暗号化することが期待される。WLANアクセスシステムは、WLANトンネルのエンドポイントとして機能し、トンネルの確立と維持に関連する多数の暗号機能を実行する。認証、鍵の生成、及び情報の暗号化に使用される暗号方式が十分に堅牢であり、実装に重大な設計上の誤りがないなら、攻撃者は無線データを取得するために暗号鍵空間を総当りできないだろう。 IEEE 80211及びIEEE 802.1X規格に規定されているWPA2への適合、正しいシードで生成したランダムビット生成器（RBG）、及び安全な認証要因により、鍵空間の総当り以下の作業では送信される情報にアクセスできないことが保証される。平文の秘密鍵及び私用鍵または他の暗号セキュリティパラメタは、セキュリティ上重要なデータの開示を防止するために、使用されなくなったときゼロ化される。

10 無線トラフィックの保護に加えて、WLANアクセスシステムは、リモート管理者セッション用の安全な通信機能を提供し、それ自体と外部認証サーバ間のRADIUSパケットを保護しなければならない。これらの対策により、ピア認証、データ機密性と完全性、及びプロトコル適合を使用した内部及び外部インタフェースからの無許可アクセスが防止される。

1.1.3 管理

11 WLANアクセスシステムは、TOEをインストール、設定、及び保守するために、管理者の役割を提供しなければならない。TOEは、管理責任を実行するために、リモートとローカルの両方で認証されたアクセスを提供する。本PPでは1つの管理役割が要求されるが、ST執筆者は、管理の役割（例えば暗号管理者、監査管理者）を区別するためにさらに管理機能を分割するために、追加の管理役割を含めることができる。この場合、ST執筆者は、適切な管理者役割に機能を制限するために、FMT_SMR要件を詳細化し、該当するセキュリティ管理要件を更新する必要があるだろう。

12 許可された管理者は、要求されるガイダンス文書に正しく従う。TOEは、以下の管理機能を提供できなければならない。

- リモート管理者によって許可されるであろう連続認証失敗試行の最大回数を指定する、
- 暗号機能の動作を変更する、
- 外部認証サーバ、NTPサーバ、及び監査サーバとの通信を設定する、及び
- 監査収集を有効にする、無効にする、及び設定する。

1.1.4 プロトコル適合

13 本PPに適合するTOEは、Wi-Fi保護されたアクセス2（WPA2）の要件に合致しなくてはならない。 具体的には、TOEは、WPA2規格に定義されているAdvanced Encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol （AES-CCMP）を使用する。 IEEE 802.1Xは、ポートベースのアクセス制御に使用される。クライアントは、無線クライアントと認証サーバ間の相互認証にExtensible Authentication Protocol-Transport Layer Security （EAP-TLS）を用いて認証することが期待される。 WLANアクセスシステムは、EAPパケット（2869）を転送する追加サポートと共に認証サーバとの通信用にRADIUSプロトコル（RFC2865）をも実装する。

14 また、本PPに適合するTOEは、さらに認証サーバとのRADIUS通信を保護するために、Internet Engineering Task Force （IETF） Internet Protocol Security （IPsec） Encapsulating Security Payload （ESP）プロトコルを実装し、これに適合する。 リモート管理者とのセキュアな通信を保証するために、IPsec、SSH、またはTLS/HTTPSも使用される。

1.1.5 TOE 以外の利用可能なハードウェア/ソフトウェア/ファームウェア

15 WLANアクセスシステムが802.1X WLANソリューションに寄与するため、TOEがサポートする環境は有意義である。802.1Xは、WLANネットワークへの認証されたアクセスを提供するための枠組を定義する。802.1X用語では、WLANアクセスシステムは認証者であり、無線クライアントと認証サーバ間で交換されるEAP-TLSメッセージの中継地点として機能する。無線クライアントとRADIUS認証サーバはTOEに含まれず、TOEの運用環境に含まれると見なされる。TOEは、そのすべてでTOEが構成される1つまたは複数のコンポーネントによって実装できる。

16 また、TOEは、監査記録の保存とレビューについて、TOE以外の監査サーバに依存する。TOEは監査記録を生成するが、これらの監査記録の保存及び管理者がこれらの監査記録をレビューすることを許可する機能は、運用環境によって提供される。

2 セキュリティ課題記述

17 本プロテクションプロファイル（PP）は、ネットワークパケットが有線私用ネットワークと無線クライアント間の境界を通過する状況に対処するために執筆される。開示と改ざんから移動中のデータを保護するため、安全な通信を確立するためにWLANアクセスシステムが作られる。WLANアクセスシステムは、安全な暗号トンネルの片側を提供し、その認証された無線クライアントとの間で交渉された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。

18 WLANアクセスシステムの適切な設置、設定、及び管理がその正しい動作にとって重大であり、そのため、管理者によるTOEの正しい取り扱いについても扱う。

19 この章は以下を識別する。

- WLANアクセスシステムによって対抗される組織に対するIT関連の脅威。
- 十分な保護を提供するために制御を要求する環境の脅威。
- 必要に応じてWLANアクセスシステムのための組織のセキュリティ方針。
- WLANアクセスシステム運用環境に関する有意義な前提条件。

2.1 脅威

20 無線ネットワークの使用により、ネットワークに新しい攻撃ベクターが導入される。攻撃者は保護された施設の境界を越えて侵入したり、アクセスシステムへのアクセスを取得することなく、無線攻撃を開始できる。信号混信やサービス妨害（DoS）攻撃はよく行われ、防止しがたい。WLANアクセスシステムは、複数の同時無線接続をサポートし、それらのピアとの間の複数の暗号トンネルを確立し、終了することができる。これらの対策は、プロトコル適合に関する要件及び資源利用に関する割当制限と合わせて、サービス妨害（DoS）攻撃を低減し、資源の枯渇を防止するために有効である。

21 また、本PPは、内部者の脅威に対して保護できる要件を含まない。これには、許可されたエンドポイント（例えば許可されたクライアントデバイスまたは許可されたITエンティティ/ピア）の不正使用が含まれる。許可された利用者は敵対するまたは悪意があるとは見なされず、適切なガイダンスに従うことが信用される。許可された人物のみが、機器、管理用コンソール、及びデバイスにアクセスできるべきである。従って、主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試みる許可されていないエンティティである。合法のエンティティ及びクレデンシャルによるネットワークアクセス要求は安全でない領域から来ることもあるので、ネットワーク攻撃の可能性があり、開示と改ざんから保護されなければならない。悪意のあるエンティティは、例えば、TOEと合法のWLANクライアント間で交換されるパケットを盗聴して、クレデンシャルを盗もうと試みたり、許可された利用者になりすます可能性がある。

22 ただし、無線通信を保護するために、他のメカニズムを使用できる。無線接続を確立するためのセキュリティ方針の不適切な交渉または弱いプロトコルオプションの施行は、利用者データやTSFデータの開示または改ざんが行われうる課題である。攻撃者が無線トラフィックを「盗聴」することを防止することは不可能であるが、プロトコルの相互接続性及び強力な暗号化を要求する相互に合意されたセキュリティ方針が、無線LAN保護を確立するために必須である。

23 同様に、（TOEによって保護されるネットワークに対し）TOE自体への管理者アクセス権を得ようと試みるリモート利用者は、他の脅威エージェントを定義する。汎用でないシステ

ムとして、TOEは、設置、設定、及び保守を行えるように、管理者のみにTOEへの直接アクセスを許可する。 TOEはリモート管理をサポートするため、TOEは有効な管理者によって入力されたデータを不正に操作する、またはリモート管理者ログインを取得して管理者権限を取得しようとするネットワーク攻撃にさらされる。

24 TOE及びTOEが保護するネットワークに対する上記のようなネットワーク攻撃は、無許可アクセスを取得し、セキュリティを無力化するための唯一の手段ではない。製品の更新は、脅威環境の変更が対処されることを保証するためによく使用される必要な機能である。よく使用される攻撃ベクターには、周知の不具合を含んでいるソフトウェアにパッチを当てていないバージョンに対する攻撃が含まれる。適時にパッチを適用することで、製品のセキュリティ方針の維持と施行の可能性が高まる。ただし、適用される更新は、信頼できる源から来るものでなければならない。そうでないと、攻撃者は、代わりに好みの悪意のあるコードを含む「更新」を自作することができる。

25 許可された管理者は敵対するものでなく、信用できるものと見なされるが、過ちを犯さないとは見なされないため、一部の管理者アクションがTOEのセキュリティに悪影響する場合がある。例えば、管理者はそうと知らずに悪意のあるコードを含むプログラムを実行したり、意図せずに間違ったセキュリティメカニズムを設定することがある。WLAN接続を確立するために使用されるプロトコルオプションを弱体化するセキュリティ方針の交渉は、利用者データやTSFデータの開示または改ざんが行われうる課題である。強力なアルゴリズム/オプションを使用するようにTOEを設定する機能と同様、プロトコルの相互接続性及び強力な暗号化を要求する相互に合意されたセキュリティ方針が、無線LAN保護を確立するために必須である。

26 TOEとの相互作用の保護は、ネットワークとデバイスのセキュリティに対して重大である。ただし、認証されたセッション自体へのアクセスが得られる場合、提供されるセキュリティは役に立たない。多くの運用環境で、ネットワークデバイスを管理するために使用される機械は、管理者以外の人物からアクセスできる。考慮する必要がある管理セッションには、管理者が（例えばコンソール経由で）デバイスにローカル接続される場合と管理者がリモート接続される場合の2つの種類がある。接続の種類にかかわらず、アクティブセッションが放置された場合には、物理的に機械にアクセスできる者は、許可にかかわらず、だれでもセッションにアクセスできるだろう。機械及び基礎となる保護ネットワークへの不正侵入が獲得される。

27 アクセスを得るメカニズム（ネットワーク攻撃、悪意のあるコード、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、攻撃者がアクセスを得ると、TOE及びそのデータが不正入手される。監査の不正使用により、TOEに対する有害アクションを隠蔽するために、監査証跡を削除し、監査記録を改ざんすることが可能になる。これにより、潜在的な問題が隠蔽され、信頼される管理者が問題を警戒できず、悪意のあるアクションを引き起こした人物を特定することが困難になる。TSFデータの不正使用には、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、及びTOEが保護するデータが含まれる。

28 ネットワーク攻撃に加えて、悪意のある更新、及び検出されないアクション、TOE自体のエラーが、利用者データ、TOE、及び保護対象ネットワークに対する低減しなければならない脅威になることがある。TOEは、資源がある利用者/プロセスから解放され、別の利用者/プロセスに割り当てられるとき、データが永続的に残留しないことを保証しなければならない。そうでない場合、TOEを通過するデータは意図せず再利用され、別の利用者に送信される場合があり、これは許容できない不正使用を引き起こす。また、TOEは、障害が検出されたとき、安全な状態を維持しなければならない。一般に、TOEのセキュリティメカニズムは、基本的なメカニズムの集合（メモリ管理、プロセス実行の優先モードなど）

からより複雑なメカニズムの集合へと構築される。基本的なメカニズムの障害により、より複雑なメカニズムが無力化され、その結果、TSFの無力化または障害になる場合がある。

29 次の表に、WLANアクセスシステムと運用環境によって対処される脅威の一覧を示す。下記のすべての脅威について、想定される攻撃者の専門知識レベルは高度ではない。

表 1：脅威

脅威	脅威の説明
T.ADMIN_ERROR	管理者は意図せずにTOEを間違って設置し、設定することがあり、セキュリティメカニズムの実効性が失われる。
T.RESOURCE_EXHAUSTION	プロセスまたは利用者は、TOEの重大な資源を消耗してTOEサービスへのアクセスを拒否できる。
T.TSF_FAILURE	TOEのセキュリティメカニズムが故障し、TSFが不正使用される場合がある。
T.UNAUTHORIZED_ACCESS	利用者は、TOEデータ及びTOE実行コードへの無許可アクセスを得ることができる。 悪意のある利用者、プロセス、または外部ITエンティティは、データまたはTOE資源への無許可アクセスを取得するために、許可されたエンティティになりすますことがある。 悪意のある利用者、プロセス、または外部ITエンティティは、識別情報と認証データを取得するために、TOEになりすますことがある。
T.UNAUTHORIZED_UPDATE	悪意のあるパーティは、TOEのセキュリティ機能を無効にすることができる製品の更新を最終利用者に提供しようとする。
T.UNDETECTED_ACTIONS	悪意のあるリモート利用者または外部ITエンティティは、TOEのセキュリティに悪影響するアクションを取ることがある。 これらのアクションが検出されないまま残り、その効果を実質的に低減できないことがある。
T.USER_DATA_REUSE	利用者データが、意図せずして元の送信者の意図しない宛先に送信されることがある。

2.2 組織のセキュリティ方針

30 組織のセキュリティ方針は、WLANアクセスシステムへの適用可能性に応じて選択された。手続きに関連する方針も、前提条件として記載されている。方針の説明に従って、形式的な参照のない方針が作成され、公式化されることが期待される。

表 2：組織のセキュリティ方針

方針	方針の説明
P.ACCESS_BANNER	TOEは、TOEにアクセスすることで利用者が承諾する使用の制限、法的同意、または該当するその他の情報を記述する最初の見出しを表示しなければならない。
P.ACCOUNTABILITY	TOEの許可された利用者は、TOE内の自分のアクションについて責任を持たなければならない。
P.ADMIN_ACCESS	管理者は、保護された通信チャネルを通じて、ローカルとリモートの両方でTOEを管理できなければならない。
P.COMPATIBILITY	TOEは、同じプロトコルを使用して他のネットワーク機器（認証局、NTPサーバなど）との相互接続を実現するために、実装されたプロトコルについてRFC（Request for Comments）要件を満たさなければならない。
P.EXTERNAL_SERVERS	TOEは、集中監査サーバ及びRADIUS認証サーバとの通信用の標準化された（RFC）プロトコルをサポートしなければならない。

2.3 前提条件

31 セキュリティ問題の定義の本節では、セキュリティ機能を提供するために運用環境に関する前提条件を示す。これらの前提条件を満たさない運用環境にTOEが配置される場合、TOEはそのすべてのセキュリティ機能を提供できなくなる場合がある。前提条件には、運用環境の物理的、人為的、及び接続的側面がある。

表 3：TOE の前提条件

前提条件	前提条件の説明
A.NO_GENERAL_PURPOSE	TOEの操作、管理及びサポートに必要なサービスを除き、TOEが使用できる汎用の計算機能（コンパイラや利用者アプリケーションなど）は存在しないと仮定する。
A.NO_TOE_BYPASS	情報は、TOEを通過せずに無線クライアントと内部有線ネットワーク間を流れることができない。
A.PHYSICAL	TOE及びそこに含まれるデータの価値に相当する物理的なセキュリティが、環境によって提供されると仮定する。
A.TRUSTED_ADMIN	TOE管理者は、信頼される方法で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 セキュリティ対策方針

32 セキュリティ対策方針は、第2章の脅威、組織のセキュリティ方針、及び前提条件から導出する評価対象（TOE）と運用環境に関する要件である。第4章では、TOEに関するセキュリティ対策方針を、より形式的にセキュリティ機能要件（SFR）と言い換えている。TOEは、SFRに対して評価される。

3.1 TOE に関するセキュリティ対策方針

33 表 4に、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抗し、識別された組織のセキュリティ方針に適合するために、記載されている意図を反映している。TOEは、セキュリティ機能要件を満たすことで、これらの対策方針に適合しなければならない。

表 4：TOE に関する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、利用者がTOEになりすます他のエンティティと通信していないこと、及びTOEが許可されたITエンティティになりすます他のエンティティでなく、許可されたITエンティティと通信していることを保証する手段を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS	TOEは、TOEの物理的に分離している部分間で送信される、またはTOEの外部に保存されるTSFデータの機密性を維持し、改ざんの検出を可能にするために、暗号機能（暗号化/復号及びデジタル署名操作）を提供する。
O.DISPLAY_BANNER	TOEは、TOEの使用に関する助言的警告を表示する。
O.FAIL_SECURE	TOEは、電源投入時自己テストの失敗の後では安全な方法で失敗しなければならない。
O.PROTECTED_COMMUNICATIONS	TOEは、管理者、分散されたTOEの他の部分、及び許可されたITエンティティに保護された通信チャネルを提供する。
O.PROTOCOLS	TOEは、相互接続性を保証するために、RFC及び/また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、及び集中監査サーバ及びRADIUS認証サーバとの通信をサポートしていることを保証する。
O.REPLAY_DETECTION	TOEは、認証データ、他のTSFデータ、及びセキュリティ属性のリプレイを検出し、拒否する手段を提供する。
O.RESIDUAL_INFORMATION_CLEARING	TOEは、資源が再割当されるとき、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.RESOURCE_AVAILABILITY	TOEは、TOE資源（永続記憶域など）を消耗する利用者の試みを低減するメカニズムを提供しなければならない。
O.ROBUST_TOE_ACCESS	TOEは、管理者のTOEへの論理的なアクセスを制御し、無線クライアントから管理アクセスを制御するメカニズムを提供する。
O.SESSION_LOCK	TOEは、ハイジャックされた無人セッションのリスクを低減するメカニズムを提供しなければならない。
O.SYSTEM_MONITORING	TOEは、監査データを生成し、それらのデータを外部ITエンティティに送信する機能を提供する。

O.TIME_STAMPS	TOEは、高信頼タイムスタンプ及び管理者がこれらのタイムスタンプに使用される時刻を設定する機能を提供しなければならない。
O.TOE_ADMINISTRATION	TOEは、管理者のみがログインし、TOEを設定できることを保証するためのメカニズムを提供し、ログインしている管理者の保護を提供する。
O.TSF_SELF_TEST	TOEは、それが正しく動作していることを保証するために、そのセキュリティ機能の部分集合をテストする機能を提供する。
O.VERIFIABLE_UPDATES	TOEは、TOEの更新が改ざんされないことを管理者によって（オプションで）信頼される源から検証できることを保証する機能を提供する。
O.WIRELESS_CLIENT_ACCESS	TOEは、TOEとの接続において無線クライアントを制限する機能を提供する。

3.2 運用環境に関するセキュリティ対策方針

34 TOEの運用環境は、TOEが（TOEに関するセキュリティ対策方針で定義される）そのセキュリティ機能を正しく提供するための技術的及び手続き的対策を実装する。部分から成るこのソリューションのことを運用環境に関するセキュリティ対策方針と呼び、運用環境が達成するべき対策方針を記述する1組の文から構成される。

35 本節では、ITドメインによって、または技術的または手続き的でない対策によって対処するべきセキュリティ対策方針を定義する。2.3節で規定されている前提条件は、環境に関するセキュリティ対策方針として組み込まれる。これらの前提条件から環境に関する追加要件が生じ、追加要件は手続き的または管理的対策を通じて満たされる。表 5に、環境に関するセキュリティ対策方針を示す。

表 5：運用環境に関するセキュリティ対策方針

対策方針	対策方針の説明
OE.NO_GENERAL_PURPOSE	TOEの操作、管理及びサポートに必要なサービスを除き、TOEが使用できる汎用の計算機能（コンパイラや利用者アプリケーションなど）は存在しない。
OE.NO_TOE_BYPASS	情報は、TOEを通過せずに、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を流れることができない。
OE.PHYSICAL	TOE及びそこに含まれるデータの価値に相当する物理的なセキュリティが、IT環境によって提供されると仮定する。
OE.TRUSTED_ADMIN	TOE管理者は、信頼される方法で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の根拠

36 本節では、第3章で定義したセキュリティ対策方針の根拠について説明する。表 6に、セキュリティ対策方針と脅威及び方針の対応関係を示す。

表 6：セキュリティ対策方針と脅威及び方針の対応関係

脅威/方針	脅威と方針に対応する対策方針	根拠
T.ADMIN_ERROR 管理者は意図せずにTOEを間違って設置し、設定することがあり、セキュリティメカニズムの実効性が失われる。	O.TOE_ADMINISTRATION TOEは、管理者のみがログインし、TOEを設定できることを保証するためのメカニズムを提供し、ログインしている管理者の保護を提供する。 OE.TRUSTED_ADMIN TOE管理者は、信頼される方法で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。	O.TOE_ADMINISTRATIONは、管理者が実行できる機能を制限してこの脅威を低減する役割を果たす。 必要でないときに管理者アクセス権を取り消すことも、過ちが起きる可能性を減らす。 OE.TRUSTED_ADMINは、管理者が適正に訓練され、管理者ガイダンスで間違いを避けるために環境とTOEを正しく設定する方法が管理者に指示されていることを保証することで、この脅威を低減する。
T.RESOURCE_EXHAUSTION プロセスまたは利用者は、TOEの重大な資源を消耗してTOEサービスへのアクセスを拒否できる。	O.RESOURCE_AVAILABILITY TOEは、TOE資源（永続記憶域など）を消耗する利用者の試みを低減するメカニズムを提供しなければならない。	O.RESOURCE_AVAILABILITYは、資源を消耗しようとする試みに対処するメカニズムと方針がTOEに実装されていることを保証することで、脅威を低減する。
T.TSF_FAILURE TOEのセキュリティメカニズムが故障し、TSFが不正使用される場合がある。	O.FAIL_SECURE TOEは、電源投入時自己テストの失敗の後では安全な方法で失敗しなければならない。 O.TSF_SELF_TEST TOEは、それが正しく動作していることを保証するために、そのセキュリティ機能の部分集合をテストする機能を提供する。	O.FAIL_SECUREは、失敗が検出されたときTOEが安全な状態を維持することを保証することで、この脅威の低減に寄与する。 O.TSF_SELF_TESTは、TSFの正しい動作を正常に実証するために、TSFが自己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実行コードへの無許可アクセスを得ることができる。悪意のある利用者、プロセス、または外部ITエンティティは、データまたはTOE資源への無許可アクセスを取得するために、許可されたエンティティになりすますことがある。 悪意のある利用者、プロセス、または外部ITエンティティは、識別情報と認証デ	O.AUTH_COMM TOEは、利用者がTOEになりすます他のエンティティと通信していないこと、及びTOEが許可されたITエンティティになりすます他のエンティティでなく、許可されたITエンティティと通信していることを保証する手段を提供する。	O.AUTH_COMMは、TOEアクセスを許可したり、その利用者に関連するセキュリティをセットアップしたりする前に、すべての利用者を識別し、認証することを保証することで、この脅威を低減する。 また、TOEは、通信の前に相互認証を保証するために、それ自身の証明書を利用者に送信できなければならない。

ータを取得するために、TOEになりすますことがある。		
	O.CRYPTOGRAPHIC_FUNCTIONS TOEは、TOEの物理的に分離している部分間で送信される、またはTOEの外部に保存されるTSFデータの機密性を維持し、改ざんの検出を可能にするために、暗号機能（暗号化/復号及びデジタル署名操作）を提供する。 O.PROTECTED_COMMUNICATIONS TOEは、管理者、分散されたTOEの他の部分、及び許可されたITエンティティに保護された通信チャネルを提供する。 O.ROBUST_TOE_ACCESS TOEは、管理者のTOEへの論理的なアクセスを制御し、無線クライアントから管理アクセスを制御するメカニズムを提供する。 O.SESSION_LOCK TOEは、ハイジャックされた無人セッションのリスクを低減するメカニズムを提供しなければならない。	O.CRYPTOGRAPHIC_FUNCTIONSは、他の保護メカニズムに必要な基礎となる暗号機能を提供することで、この脅威の低減に寄与する。 O.PROTECTED_COMMUNICATIONSは、データ送信中のTOEと許可された管理者間の通信の保護を保証することで、この脅威の低減に寄与する。 O.ROBUST_TOE_ACCESSは、TOEアクセスまたはすべての管理者のためにTOE仲介アクセスを許可する前に、TOEがすべての管理者を識別し、認証することを要求することで、この脅威を低減する。 O.SESSION_LOCKは、利用者がセッションをロックする方法またはTOEが一定時間後にロックして、許可されたセッションが端末でハイジャックできないことを保証する方法をTOEが提供することを要求することで、この脅威を低減する。
	O.TOE_ADMINISTRATION TOEは、管理者のみがログインし、TOEを設定できることを保証するためのメカニズムを提供し、ログインしている管理者の保護を提供する。 O.REPLAY_DETECTION TOEは、認証データ、他のTSFデータ、及びセキュリティ属性のリプレイを検出し、拒否する手段を提供する。 O.WIRELESS_CLIENT_ACCESS TOEは、TOEとの接続において無線クライアントを制限する機能を提供する。	O.TOE_ADMINISTRATIONは、TOEのリモート及びローカル管理を可能にするメカニズム（例えば、ローカル認証、リモート認証、TOEをリモートとローカルに設定及び管理する手段）をTOEが提供することを要求する。 O.REPLAY_DETECTIONは、悪意のあるアクターによって取得された合法の管理者またはエンティティからのセッション（またはセッションの一部）をリプレイすることで、無許可アクセスを防止する。 O.WIRELESS_CLIENT_ACCESSは、望ましいTOEのセキュリティ体勢に従って無線クライアントアクセスを制限するメカニズムを提供することで、脅威を低減する。

T.UNAUTHORIZED_UPDATE 悪意のあるパーティは、TOEのセキュリティ機能を無効にすることができる製品の更新を最終利用者に提供しようとする。	O.VERIFIABLE_UPDATES TOEは、TOEの更新が改ざんされないことを管理者によって（オプションで）信頼される源から検証できることを保証する機能を提供する。	O.VERIFIABLE_UPDATESは、管理者が更新を確認できることを保証する。
T.UNDETECTED_ACTIONS 悪意のあるリモート利用者または外部ITエンティティは、TOEのセキュリティに悪影響するアクションを取ることがある。 これらのアクションが検出されないまま残り、その効果を実質的に低減できないことがある。	O.SYSTEM_MONITORING TOEは、監査データを生成し、それらのデータを外部ITエンティティに送信する機能を提供する。	O.SYSTEM_MONITORINGは、特定の利用者のアクションを記録したり、利用者の識別情報に基づいて監査証跡をレビューしたりするために監査メカニズムを設定する機能を管理者に提供することで、この脅威を低減する。
T.USER_DATA_REUSE 利用者データが、意図せずして元の送信者の意図しない宛先に送信されることがある。	O.RESIDUAL_INFORMATION_CLEARING TOEは、資源が再割当されるとき、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.RESIDUAL_INFORMATION_CLEARINGは、資源がある利用者/プロセスから解放され、別の利用者/プロセスに割り当てられるとき、TSFデータと利用者データが永続的に残らないことを保証することで、この脅威に対抗する。
P.ACCESS_BANNER TOEは、TOEにアクセスすることで利用者が承諾する使用の制限、法的同意、または該当するその他の情報を記述する最初の見出しを表示しなければならない。	O.DISPLAY_BANNER TOEは、TOEの使用に関する助言的警告を表示する。	O.DISPLAY_BANNERは、許可されていないTOEの使用に関する警告をすべての利用者に提供する、許可された管理者が設定できる見出しをTOEが表示することを保証することで、この方針を満たす。
P.ACCOUNTABILITY TOEの許可された利用者は、TOE内の自分のアクションについて責任を持たなければならない。	O.ROBUST_TOE_ACCESS TOEは、管理者のTOEへの論理的なアクセスを制御し、無線クライアントから管理アクセスを制御するメカニズムを提供する。 O.SYSTEM_MONITORING TOEは、利用者に関連するセキュリティ関連事象を検出し、その記録を作成する機能を提供する。	O.ROBUST_TOE_ACCESSは、TOEアクセスまたはすべての管理者のためにTOE仲介アクセスを許可する前に、TOEがすべての管理者を識別し、認証することを要求することで、この方針をサポートする。 O.SYSTEM_MONITORINGは、特定の利用者のアクションを記録したり、利用者の識別情報に基づいて監査証跡をレビューしたりするために監査メカニズムを設定する機能を管理者に提供することで、この方針をサポートする。
	O.TIME_STAMPS TOEは、高信頼タイムスタンプ及び管理者がこれらのタイムスタンプに使用される時刻を設定する機能を提供しなければならない。	O.TIME_STAMPSは、TOEが高信頼タイムスタンプを提供することを要求することで、この方針をサポートする役割を果たす。 これは監査記録が生成されるときに使用され、管理

		者は監査可能なアクションとおそらくは孤立したシステムでそれらのアクションが行われた時刻を関連付けることができる。 この機能は、そのアクションによってそれらの監査記録が生成されることになった利用者に関する説明責任を提供する上で有効である。
P.ADMIN_ACCESS 管理者は、保護された通信チャネルを通じて、ローカルとリモートの両方でTOEを管理できなければならない。	O.CRYPTOGRAPHIC_FUNCTIONS TOEは、TOEの物理的に分離している部分間で送信される、またはTOEの外部に保存されるTSFデータの機密性を維持し、改ざんの検出を可能にするために、暗号機能（暗号化/復号及びデジタル署名操作）を提供する。 O.PROTECTED_COMMUNICATIONS TOEは、管理者、分散されたTOEの他の部分、及び許可されたITエンティティに保護された通信チャネルを提供する。 O.TOE_ADMINISTRATION TOEは、管理者のみがログインし、TOEを設定できることを保証するためのメカニズムを提供し、ログインしている管理者の保護を提供する。	O.CRYPTOGRAPHIC_FUNCTIONSは、他の保護メカニズムに必要な基礎となる暗号機能を提供することで、この脅威の低減に寄与する。 O.PROTECTED_COMMUNICATIONSは、データ送信中のTOEと許可された管理者間の通信の保護を保証することで、この脅威の低減に寄与する。 O.TOE_ADMINISTRATIONは、TOEのリモート及びローカル管理を可能にするメカニズム（例えば、ローカル認証、リモート認証、TOEをリモートとローカルに設定及び管理する手段）をTOEが提供することを要求することで、この方針をサポートする
P.COMPATIBILITY TOEは、同じプロトコルを使用して他のネットワーク機器との相互接続を実現するために、実装されたプロトコルについてRFC（Request for Comments）要件を満たさなければならない。	O.PROTOCOLS TOEは、相互接続性を保証するために、RFC及び/または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、及び集中監査サーバ及びRADIUS認証サーバとの通信をサポートしていることを保証する。	O.PROTOCOLSは、同じプロトコルを使用するITエンティティ間の相互接続性を保証するために、標準化されたプロトコルをTOEに実装することを要求することで、この方針を満たす。
P.EXTERNAL_SERVERS TOEは、集中監査サーバ及びRADIUS認証サーバとの通信用の標準化された（RFC）プロトコルをサポートしなければ	O.PROTOCOLS TOEは、相互接続性を保証するために、RFC及び/または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	O.PROTOCOLSは、監査と認証がローカルでも提供される場合であっても、TOEが外部監査サーバ及びRADIUS認証サーバと通信できることを保証することで、方針を満たす。

ならない。	れていること、及び集中監査サーバ及びRADIUS認証サーバとの通信をサポートしていることを保証する。	

37 表 7に、セキュリティ対策方針と前提条件の対応関係を示す。

表 7：セキュリティ対策方針と前提条件の対応関係

前提条件	前提条件に対応する対策方針	根拠
A.NO_GENERAL_PURPOSE TOEの操作、管理及びサポートに必要なサービスを除き、TOEが使用できる汎用の計算機能（コンパイラや利用者アプリケーションなど）は存在しないと仮定する。	OE.NO_GENERAL_PURPOSE TOEの操作、管理及びサポートに必要なサービスを除き、TOEが使用できる汎用の計算機能（コンパイラや利用者アプリケーションなど）は存在しない。	OE.NO_GENERAL_PURPOSEは、TOEに汎用の計算機能や保存機能が含まれないことを保証する。 これにより、悪意のあるプロセスからTSFデータが保護される。
A.NO_TOE_BYPASS 情報は、TOEを通過せずに無線クライアントと内部有線ネットワーク間を流れることができない。	OE.NO_TOE_BYPASS 情報は、TOEを通過せずに、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を流れることができない。	OE.NO_TOE_BYPASSは、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のすべての情報の流れがTOEを通過することを保証する。
A.PHYSICAL TOE及びそこに含まれるデータの価値に相当する物理的なセキュリティが、環境によって提供されると仮定する。	OE.PHYSICAL TOE及びそこに含まれるデータの価値に相当する物理的なセキュリティが、運用環境によって提供されると仮定する。	OE.PHYSICALは、TOE、TSFデータ、及び保護される利用者データが、物理的な攻撃（盗難、改ざん、破壊、または盗聴など）から保護されることを保証する。 物理的な攻撃にはTOE環境への許可されていない侵入者を含めることもできるが、TOE環境へのアクセスを許可されている個人によって行われる物理的な破壊行為は含まれない。
A.TRUSTED_ADMIN TOE管理者は、信頼される方法で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。	OE.TRUSTED_ADMIN TOE管理者は、信頼される方法で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。	OE.TRUSTED_ADMINは、管理者が適正に訓練され、管理者ガイダンスで間違いを避けるために環境とTOEを正しく設定する方法が管理者に指示されていることを保証する。

4 セキュリティ要件及び根拠

38 セキュリティ要件は、機能要件と保証要件に分割される。セキュリティ機能要件（SFR）はセキュリティ対策方針の形式的な具体化であり、4.1節の適用上の注意で提供される。通常は、より詳細なレベルの抽象化であるが、完全な翻訳でなければならない（セキュリティ対策方針を完全に取り扱わなければならない）。CCでは、いくつかの理由で標準化された言語に翻訳することが必要である。

- 評価対象の正確な記述を提供するため。通常、TOEに関するセキュリティ対策方針が自然言語で作成されるため、標準化された言語に翻訳することで、TOEの機能のより正確な記述が強制する。
- 2つのSTを比較できるようにするため。異なるST執筆者がセキュリティ対策方針を記述する際に異なる用語を使用する場合があるので、標準化された言語を使用することで同じ用語と概念の使用が強制される。そのため、比較が容易になる。

39 セキュリティ保証要件（SAR）は、通常、SFRとは別に挿入され、記載される定型文である。次に、選択したSARに基づいて、評価中に共通評価方法（CEM）が参照される。本PPでは、標準プロテクションプロファイルの新しいモデルに基づいて、より柔軟な方法を採る。4.3節では文脈と完全さのためにSARが記載されているが、このTOEで各SFRとSARに関して評価者が実行する必要があるアクティビティは、「保証アクティビティ」の段落に詳述されている。保証アクティビティは、評価を実施するために行わなければならないアクティビティの正式の説明である。本PPでは、保証アクティビティを2か所で取り扱っている。特定のSFRに関連する保証アクティビティは4.1節で取り扱い、SFRに依存しない保証アクティビティは4.3節で取り扱う。

40 SFRに直接関連するアクティビティについては、SFRごとに1つまたは複数の保証アクティビティが記載され、この技術用に提供される保証を達成するために実行する必要があるアクティビティが詳述されている。

41 SFRに依存しない活動が必要なSARについては、実施する必要がある追加の保証活動とSARに関連する具体的な保証活動が記載されたSFRへのポインタが4.3節に記載されている。

42 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習したレッスンに基づいて、より詳細な保証アクティビティが提供されるだろう。

4.1 セキュリティ機能要件

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
セキュリティ監査クラス（FAU）	FAU_GEN.1 監査データ生成
	FAU_GEN.2 利用者識別関連付け
	FAU_SEL.1 選択的監査
	FAU_STG.1 保護された監査証跡格納（ローカル格納）
	FAU_STG_EXT.1 外部監査証跡格納
	FAU_STG_EXT.3 監査サーバ接続性喪失時のアクション
暗号サポートクラス（FCS）	FCS_CKM.1(1) 暗号鍵生成（WPA2接続用の対称鍵）
	FCS_CKM.1(2) 暗号鍵生成（非対称鍵）
	FCS_CKM.2(1) 暗号鍵配付（PMK）
	FCS_CKM.2(2) 暗号鍵配付（GTK）
	FCS_CKM_EXT.4 暗号鍵ゼロ化

	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_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_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 残留情報完全保護
識別及び認証クラス（FIA）	FIA_AFL.1 認証失敗処理
	FIA_PMG_EXT.1 パスワード管理
	FIA_UIA_EXT.1 利用者識別及び認証
	FIA_UAU_EXT.5 拡張：パスワードベースの認証メカニズム
	FIA_UAU.6 再認証
	FIA_UAU.7保護された認証フィードバック
	FIA_8021X_EXT.1 拡張：802.1Xポートアクセスエンティティ（認証者）認証
	FIA_PSK_EXT.1 拡張：事前共有鍵作成
	FIA_X509_EXT.1 拡張：X509証明書
セキュリティ管理クラス（FMT）	FMT_MOF.1セキュリティ機能動作の管理
	FMT_MTD.1(1) TSFデータの管理（一般的TSFデータ）
	FMT_MTD.1(2) TSFデータの管理（認証データの読取）
	FMT_MTD.1(3) TSFデータの管理（すべての対称鍵の読取）
	FMT_SMF.1 管理機能の指定
	FMT_SMR.1 セキュリティ管理役割
TSFの保護（FPT）	FPT_FLS.1 故障時の安全確保
	FPT_RPL.1 リプレイ検出
	FPT_STM.1 高信頼タイムスタンプ
	FPT_TST_EXT.1 拡張：TSFテスト
	FPT_TUD_EXT.1 拡張：高信頼更新
資源利用（FRU）	FRU_RSA.1 最大割当制限
TOEアクセス（FTA）	FTA_SSL_EXT.1 TSF起動のセッションロック
	FTA_SSL.3 TSF起動の終了
	FTA_SSL.4 利用者起動の終了
	FTA_TAB.1 デフォルトのTOEアクセスバナー
	FTA_TSE.1 TOEセッション確立
高信頼パス/チャネル（FTP）	FTP_ITC.1 TSF間高信頼チャネル
	FTP_TRP.1 高信頼パス

4.1.1 セキュリティ監査クラス（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、以下の監査対象事象の監査記録を生成できなければならない。

a) 監査機能の起動及び終了、

b) 監査の未特定レベルに関するすべての監査対象事象、及び

c) *すべての*管理者アクション、

d) [*特に*表 9*に記載の定義済みの監査対象事象*]。

適用上の注意：

43 *ST執筆者は、他の監査対象事象を直接表に含めることができる。表の記載内容に制限されない。*

44 本書に記載されているSFRの多くの監査可能側面は、管理アクションを取り扱う。*上記の項目cは、すべての管理アクションが監査対象であることを要求する。従って、*表 9*には、これらのアクションの監査可能性の追加規定は存在しない。*

保証アクティビティ：

45 *評価者は、管理ガイドをチェックし、すべての監査対象事象が記載され、監査記録の書式が提供されていることを確認しなければならない。各項目の短い記述と共に、各監査記録の書式タイプを網羅しなければならない。評価者は、PPによって義務付けられているすべての監査事象タイプが記述され、FAU_GEN.1.2で要求される情報及び*表 9*に規定されている追加情報が項目の記述に含まれていることを確認しなければならない。*

46 *評価者は、特に失敗した暗号事象に関する内容が明記されていることを確認しなければならない。*表 9*では、操作の暗号モードを詳述する情報及び暗号化されるオブジェクトの名前または識別コードが要求される。評価者は、名前または識別コードが監査ログをレビューする管理者が（例えば、鍵交渉交換中に実行される、移動中のデータを暗号化するときに実行される)暗号操作の文脈及び他のITシステムとの通信に関連する暗号失敗に関する接続のTOE以外のエンドポイントを決定できるほど十分であることを確認しなければならない。*

47 *評価者は、本PPの文脈において関連のある管理アクションも決定しなければならない。TOEは、SFRに機能が規定されていないために本PPの文脈では評価されない機能を含んでいてもよい。この機能は、運用ガイダンスに記述される管理側面を持つことができる。このような管理アクションはTOEの評価される構成では実行されないため、評価者は、運用ガイダンスを検査し、サブコマンド、スクリプト、及び構成ファイルを含めてどの管理コマンドが、PPに規定されている要件を施行する、従って「すべての管理のアクション」を形成するために必要なTOEに実装されているメカニズムの設定（有効化や無効化を含む）に関連するかを決定しなければならない。評価者は、AGD_OPEガイダンスが要件を満たすことの確認に関連するアクティビティの一環としてこのアクティビティを実行してもよい。*

48 *評価者は、本PP内の機能要件に関連する保証アクティビティに従ってTOEに監査記録を生成させることで、TOEが監査記録を正しく生成する機能をテストしなければならない。さ*

らに、評価者は、本PPの文脈において適用可能な各管理アクションが監査可能であることをテストしなければならない。テスト結果を検証する際、評価者は、テスト中に生成される監査記録が管理ガイドに規定されている書式と一致し、各監査記録の項目に適切な項目があることを確認しなければならない。

49 *なお、ここでのテストは、セキュリティメカニズムのテストと直接組み合わせて実行することができる。例えば、TOEがリプレイ試行を検出できることを確認するテストは、FPT_RPL.1要件が満たされることを実証するために実行される可能性が高い。別の例としては、提供される管理者ガイダンスが正しいことを確認するために実行されるテストがAGD_OPE.1が満たされることを検証し、監査記録が期待通りに生成されることを確認するために必要な管理アクションの呼出しに対処するべきである。*

FAU_GEN.1.2 TSFは、少なくとも以下の情報を各監査記録に記録しなければならない。

a) 事象の日時、事象のタイプ、監査対象の識別情報、及び事象の結果（成功または失敗）、及び

b) 監査事象タイプごとに、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いて、[下記の表の第3列に規定されている情報]。

適用上の注意：

50 *前のコンポーネントの場合と同様、ST執筆者は、生成される追加情報で*表 9*を更新するべきである。この要件の文脈における「監査対象の識別情報」は、例えば管理者の利用者IDまたは影響を受けるネットワークインタフェースなどである。*

保証アクティビティ：

このアクティビティは、FAU_GEN.1.1.のテストと組み合わせて実行するべきである。

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_GEN.2	なし。	
FAU_SEL.1	監査収集機能の実行中に行われる監査設定に対するすべての変更。	なし。
FAU_STG.1	なし。	
FAU_STG_EXT.1	なし。	
FAU_STG_EXT.3	接続性の喪失。	なし。
FCS_CKM.1(1)	鍵生成アクティビティの失敗。	なし。
FCS_CKM.1(2)	鍵生成アクティビティの失敗。	なし。
FCS_CKM.2(1)	鍵配付アクティビティの失敗	なし。
FCS_CKM.2(2)	GTKの包込みに関連する失敗を含む鍵配付アクティビティの失敗。	包み込まれた鍵の意図した受領者の識別子。
FCS_CKM_EXT.4	鍵ゼロ化プロセスの失敗	ゼロ化を要求または引き起こす監査対象の識別情報、消去中のオブジェクトまたはエンティティの識別情報。
FCS_COP.1(1)	暗号化または復号の失敗。	操作の暗号モード、暗号化/復号されるオブジェクトの名前/識別子

FCS_COP.1(2)	暗号署名の失敗。	操作の暗号モード、署名/検証されるオブジェクトの名前/識別子。
FCS_COP.1(3)	ハッシュ関数の失敗。	操作の暗号モード、ハッシュされるオブジェクトの名前/識別子。
FCS_COP.1(4)	データ以外の完全性のための暗号ハッシュの失敗。	操作の暗号モード、ハッシュされるオブジェクトの名前/識別子。
FCS_COP.1(5)	WPA2暗号化または復号の失敗。	操作の暗号モード、暗号化/復号されるオブジェクトの名前/識別子、接続のTOE以外のエンドポイント（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への交換に関する交渉「ダウン」。	失敗の理由。 成功と失敗両方の接続のTOE以外のエンドポイント（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_AFL.1	認証失敗試行の閾値への到達、取られるアクション（アカウントの無効化など）、及び適切な場合、正常状態への復旧（端末の再有効化など）。	なし。
FIA_PMG_EXT.1	なし。	
FIA_UIA_EXT.1	識別と認証のメカニズムのすべての使用。	提供される利用者識別情報、試行元（IPアドレスなど）。
FIA_UAU.5	認証メカニズムのすべての使用。	試行元（IPアドレスなど）。
FIA_UAU.6	再認証の試行。	試行元（IPアドレスなど）。
FIA_UAU.7	なし。	
FIA_8021X_EXT.1	802.1X制御ポートへのアクセス試行。	提供されるクライアント識別情報（IPアドレス）。
FIA_PSK_EXT.1	なし。	
FIA_X509_EXT.1	証明書の読込試行。 証明書の取消試行。	なし。
FMT_MOF.1	なし。	
FMT_MTD.1(1)	なし。	
FMT_MTD.1(2)	なし。	
FMT_MTD.1(3)	なし。	
FMT_SMF.1	なし。	
FMT_SMR.1	なし。	
FPT_FLS.1	TSFの故障。	発生した障害のタイプでTSFが故障したという表示。
FPT_RPL.1	検出されたリプレイ攻撃。	リプレイ攻撃の対象となった利用者の識別情報。 リプレイ攻撃源の識別情報（源のIPアドレスなど）。
FPT_STM.1	なし。	
FPT_TST_EXT.1	このTSF自己テスト集合の実行。 検出された完全性違反。	完全性違反の場合、完全性違反を引き起こしたTSFコードファイル。
FPT_TUD_EXT.1	更新の開始。 更新の完全性検証の失敗。	追加情報なし。
FRU_RSA.1	超過された最大割当制限。	資源識別子。
FTA_SSL_EXT.1	セッションのロックメカニズムによる対話型セッションのロック。 対話型セッションのロック解除試行。	なし。

FTA_SSL.3	セッションのロックメカニズムによるリモートセッションの終了。	なし。
FTA_SSL.4	中止またはログオフによるセッションの終了。	なし。
FTA_TAB.1	なし。	
FTA_TSE.1	セッション確立メカニズムによるセッション確立の拒否。	拒否の理由、確立試行の根源。
FTP_ITC.1	高信頼チャネルを確立しようとするすべての試行。 チャネルデータの変更の検出。	チャネルのイニシエータとターゲットの識別。
FTP_TRP.1	リモート管理セッションを確立しようとするすべての試行。 セッションデータの変更の検出。	開始するITエンティティの識別（IPアドレスなど）。

FAU_GEN.2　　利用者監査関連付け

FAU_GEN.2.1　　識別された利用者のアクションの結果として生じる監査事象について、TSFは、各監査対象事象を事象を引き起こした利用者の識別情報に関連付けることができなければならない。

適用上の注意：

51 *識別/認証が成功するまで利用者はTSFの制御下にないため、利用者IDが既知の利用者のIDと一致しないログイン失敗試行については、利用者の関連付けは要求されない。*

保証アクティビティ：

52 *このアクティビティは、FAU_GEN.1.1.のテストと組み合わせて実行するべきである。*

セキュリティ監査事象選択（FAU_SEL）

FAU_SEL.1　　選択的監査

FAU_SEL.1.1　　TSFは、以下の属性に基づいて、すべての監査対象事象の集合から監査されるべき事象の集合を選択できなければならない。

- **a) 管理者識別情報、**
- **b) 事象タイプ、**
- **c) 監査可能セキュリティ事象の成功、**
- **d) 監査可能セキュリティ事象の失敗、及び**
- **e) [割付：その他の属性]。**

適用上の注意：

53 この要件の意図は、監査事象をトリガするために選択できるすべての基準を識別することである。*ST執筆者は、割付を使用して追加基準または「なし」を記載する。監査対象事象タイプは表 9に記載されている。*

保証アクティビティ：

54 *評価者は、割付に記載されている属性を含むように、要件に従ってすべての事象タイプが箇条書きにされ、選択可能なすべての属性が記述されていることを確認するために管理者ガイダンスをレビューする。また、管理者ガイダンスは、事前選択を設定する方法に関す*

る指示を含み、複数の値を持つ事前選択用の構文（存在する場合)を説明しなければならない。また、管理者ガイダンスは、現在施行されている選択条件にかかわらず、常に記録される監査記録を識別しなければならない。

55 *評価者は、以下のテストも実行しなければならない。*

- *テスト1：要件に記載されている属性ごとに、評価者は、属性を選択することにより、その属性を持つ監査事象のみ（または管理者ガイダンスに識別されている常に記録される監査事象）が記録されることを示すテストを考案しなければならない。*
- *テスト2[条件付き]：TSFがより複雑な監査事前選択基準（複数の属性、属性を使用した論理式など）の指定をサポートする場合、評価者は、この機能が正しく実装されていることを示すテストを考案しなければならない。また、評価者は、テストの集合が代表的であり、機能を試験するのに十分であることを正当化する短い説明をテスト計画に提供しなければならない。*

セキュリティ監査証跡格納（FAU_STG）

FAU_STG.1	**保護された監査証跡格納（ローカル記憶域）**
FAU_STG.1.1	**詳細化**：TSFは、監査証跡にローカルに格納された監査記録**[割付**：**記憶域の量]**を、不正な削除から保護しなければならない。
FAU_STG.1.2	TSFは、監査証跡に格納された監査記録への不正な改変を防止できなければならない。

適用上の注意：

56 *監査情報をエクスポートする機能に加えて、TOEは何らかの量のローカル記憶域を持つことが要求される。ST執筆者は、監査記録用に使用できるローカル記憶域の量で割付を完成する。これは、メガバイト（MB）、平均監査記録件数などが可能である。*

保証アクティビティ：

評価者は、ローカルに保存される監査データの量、ローカル監査データ記憶域が一杯になった場合の処置、及びこれらの記録を不正アクセスから保護する方法が記載されていることを確認するために、TSSを検査しなければならない。また、評価者は、ローカル監査データと監査ログサーバに送信される監査データ間の関係が記述されていることを決定するために、運用ガイダンスを検査しなければならない。例えば、監査事象が生成されるとき、外部サーバとローカル記憶域に同時に送信されるかどうか、またはバッファとして使用されるローカル記憶域がデータを監査サーバに送信することで定期的に「消去」されるかどうか。

FAU_STG_EXT.1	**外部監査証跡格納**
FAU_STG_EXT.1.1	TSFは、[選択：IPsec、SSH、TLS、TLS/HTTPS]プロトコルを実装する高信頼チャネルを使用して、生成される監査データを外部ITエンティティに送信できなければならない。

適用上の注意：

57 *また、TOEは、監査記録の保存とレビューについて、TOE以外の監査サーバに依存する。TOEは監査記録を生成するが、これらの監査記録の保存及び管理者がこれらの監査記録をレビューすることを許可する機能は、運用環境によって提供される。ST執筆者は、選択を*

使用してこの接続が保護される手段を選択する。また、ST執筆者は、選択と一致するサポートプロトコル要件がSTに含まれていることを確認する。

保証アクティビティ：

58 *評価者は、監査データを外部監査サーバに転送する手段及び高信頼チャネルを提供する方法が記述されていることを確認するために、TSSを検査しなければならない。高信頼チャネルメカニズムのテストは、特定の高信頼チャネルメカニズムのための関連する保証アクティビティに規定されている通りに実行される。また、評価者は、監査サーバへの高信頼チャネルを確立する方法が記述されていること、及び監査サーバに関する要件（特定の監査サーバプロトコル、要求されるプロトコルのバージョンなど）、及び監査サーバと通信するために必要なTOEの設定が記述されていることを確認するために、運用ガイダンスを検査しなければならない。評価者は、この要件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、提供されるガイダンス文書に従って、TOE と監査サーバ間のセッションを確立しなければならない。次に、評価者は、監査サーバに転送される監査データを生成するように設計された、評価者が選ぶいくつかのアクティビティの間に、監査サーバと TOE 間を通過するトラフィックを検査しなければならない。評価者は、これらのデータがこの転送中に明確に表示されえず、監査サーバによって正常に受信されることを観察しなければならない。評価者は、テスト中に監査サーバで使用される特定のソフトウェア（名前、バージョン）を記録しなければならない。*

FAU_STG_EXT.3	**監査サーバ接続性喪失時のアクション**
FAU_STG_EXT.3.1	TSFは、TOEによって生成される監査データを収集する外部ITエンティティとのリンクが使用できなくなった場合、[割付：アクション]を実行しなければならない。

適用上の注意：

59 *ST執筆者は、監査サーバとのリンクが喪失した場合にTOEが取るアクション（管理者を呼び出す、通過パケットを停止するなど）を記述する。*

保証アクティビティ：

60 *評価者は、監査サーバとの通信を確立する方法が管理者に指示されていることを確認するために、管理者ガイダンスを検査しなければならない。ガイダンスは、安全な方法でこのチャネルを確立する方法（IPsec、TLSなど）を指示しなければならない。評価者は、TOEと監査サーバ間のリンクが喪失した場合にどのようなアクションが取られるかを決定するために、管理者ガイダンスを確認する。これは、ネットワーク接続性の喪失、または安全なプロトコルリンクの停止による場合がある。*

61 *評価者は、接続性の喪失中に取得されたローカル監査事象が監査サーバ上の監査証跡と同期すること、送信できるデータに関する制限（例えば、故障時間が長い場合は、この間に生成されるすべての記録をローカル記憶域に格納されていないかもしれないなど）を管理者に知らせること、を確認するために、接続が復旧した後で行わなければならないアクティビティを決定するために、運用ガイダンスを検査しなければならない。*

62 *評価者は、この要件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、監査サーバとのリンクを確立することによって管理者ガイダンスをテストする。なお、これは、FAU_GEN.1 に規定されている保証アクティビティを実行するために行う必要がある。評価者は、管理ガイドに記載されているアクションが正しく行われることを決定するために、通信リンクを中断しなけ*

ればならない（例えば、ネットワークケーブルを抜く、プロトコルリンクを停止する、監査サーバをシャットダウンするなど）。

4.1.2 暗号サポートクラス（FCS）

暗号鍵管理（FCS_CKM）

FCS_CKM.1(1) **暗号鍵生成（WPA2接続用の対称鍵)**

FCS_CKM.1.1(1) **詳細化：**：TSFは、以下の**[802.11-2007]**に合致する、**FCS_RBG_EXT.1で指定されたランダムビット生成器を使用して**、指定された暗号鍵サイズ**[128ビット]**を持つ指定された暗号鍵**導出**アルゴリズム**[PRF-384]**に従って、**対称**暗号鍵を**導出**しなければならない。

適用上の注意：

63 *この要件は、クライアントが認証された後でアクセスポイントとクライアント間の通信用に生成/導出される鍵のみに適用される。この要件は、（本PPに規定されているRBGによる）GTKの生成、及び本PPに規定されているRBGによって生成されるランダム値を使用して行われるPMKからのPTKの導出、本PPに規定されているSHA-1を使用するHMAC関数、及びその他の情報を参照する。これは、802.11-2007の主にChapter 8に規定されている。*

保証アクティビティ：

64 暗号プリミティブは、本PPの後の方で規定されているアクティビティによって検証される。評価者は、TOEが本PPによって定義され、実装されたプリミティブを使用して無線クライアントとの安全な接続を確立し、維持する方法がTSSに記述されていることを検証しなければならない。また、TSSは、開発者の実装が暗号規格に適合することを保証する開発者の方法に関する記述を提供しなければならない。これには、開発組織によって行われるテストだけでなく、実行される第三者のテストも含まれる。評価者は、テスト方法の記述が、プロトコルがテストされる詳細の程度を決定するために十分な詳しさで行われていることを確認しなければならない。

FCS_CKM.1(2) **暗号鍵生成（非対称鍵）**

FCS_CKM.1.1(2) **詳細化：**TSFは、以下、及び112ビットの対称鍵強度と等価またはそれ以上の指定された暗号鍵サイズに従って、**鍵確立のために使用される非対称**暗号鍵を生成しなければならない。:

[選択：

- *NIST Special Publication 800-56A、有限体に基づく鍵確立スキームのための「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」、*
- *NIST Special Publication 800-56A、楕円曲線に基づく鍵確立スキームのための「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」及び「NIST曲線」P-256、P-384、及び[選択：P-521、他の曲線なし]（FIPS PUB 186-3、「Digital Signature Standard」で定義されている通り）の実装、*

- *NIST Special Publication 800-56B、RSAに基づく鍵確立スキームのための「Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography」]*

適用上の注意：

65 *このコンポーネントは、TOEによって使用される様々な暗号プロトコル（IPsecなど）用の鍵を確立するために使用される公開鍵/私用鍵ペアをTOEが生成できることを要求する。複数スキームがサポートされる場合、ST執筆者は、この機能を取得するためにこの要件を繰り返すべきである。使用されるスキームは、ST執筆者によって選択から選ばれる。*

66 *本PPでは、使用されるドメインパラメタがプロトコルの要件によって規定されているため、TOEがドメインパラメタを生成することは期待されない。従って、TOEが本PPに規定されているプロトコルに適合する際に必要な追加のドメインパラメタ検証はない。*

67 *生成される2048ビットDSA及びrDSA鍵の鍵強度は、112ビットの対称鍵強度と等価またはそれ以上である必要がある。等価な鍵強度の詳細は、NIST Special Publication 800-57、「Recommendation for Key Management」を参照。*

保証アクティビティ：

68 *評価者は、ST執筆者によって行われた選択に応じて、上記の要件をテストする際のガイドとして、「The FIPS 186-3 Digital Signature Algorithm Validation System（DSA2VS)」、「The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)」、及び「The RSA Validation System (RSA2VS)」の鍵ペア生成部分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ーを生成できるアルゴリズムの高信頼な参照実装を保有することが要求される。*

69 *行われた選択に応じてTSF実装が800-56A及び/または800-56Bに適合することを示すために、評価者は、TSSに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。*

- *TSSは、TOEが適合する該当する800-56規格のすべての節を記載しなければならない。*
- *TSSに記載される該当する節ごとに、「shall」（しなければならない）でない（すなわち「shall not」（してはならない)、「should」（するべきである)、及び「should not」（するべきでない)）すべての文について、TOEがこのようなオプションを実装する場合は、それをTSSに記述しなければならない。含まれる機能が規格に「shall not」（してはならない）または「should not」（するべきでない）と示されている場合、TSSは、TOEによって実装されたセキュリティ方針に悪影響しない根拠を提供しなければならない。*
- *（選択された）800-56A及び800-56Bの該当する節ごとに、「shall」（しなければならない）または「should」(するべきである）文に関連する機能の省略を記述しなければならない。*
- *TOEが実施すべきセキュリティ要件に影響を与える可能性のあるようなTOE 固有の拡張、文書に含まれない処理、または文書によって許可される代替実装について記述しなければならない。*

FCS_CKM.2(1)	**暗号鍵配付（PMK）**
FCS_CKM.2.1(1)	**詳細化**：TSFは、以下の[802.11-2007]に合致し、かつ**暗号鍵を開示しない**、指定された暗号鍵配付方法：[**802.1X認証サーバから**

受信]に従って、**802.11ペアマスター鍵PMK**を配付しなければならない。

適用上の注意：

70 *この要件は、TOEがRADIUSサーバから受信したペアマスター鍵PMKに適用される。この要件の意図は、事前共有鍵のみをサポートする実装を許さないことに加えて、クライアントとの安全な通信を確立する前に、適合TOEが802.1X認証を実装していることを保証することである。 RADIUSサーバとの通信はIPsecで保護された接続経由で実行されることが要求されるため、PMKの転送が保護される。*

保証アクティビティ：

71 *評価者は、PMKをTSFに転送する方法（すなわち、どのEAP属性を使用するか）が記述されていることを決定するために、TSSを検査しなければならない。*

72 *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、提供されるガイダンス文書に従って、TOE と RADIUS サーバ間のセッションを確立しなければならない。 次に、評価者は、PMK が開示されないことを決定するために、無線クライアントを TOE に接続する試行が成功するときに RADIUS サーバと TOE 間を通過するトラフィックを検査しなければならない。*

FCS_CKM.2(2) **暗号鍵配付（GTK）**

FCS_CKM.2.1(2) **詳細化：**TSFは、以下の：[AES鍵包込みについてはRFC 3394、パケットフォーマットとタイミングの留意事項については802.11-2007]に合致し、かつ**暗号鍵を開示しない**、指定された暗号鍵配付方法：[EAPOL鍵フレーム内のAES鍵包込み]に従って、**グループ一時鍵GTK**を配付しなければならない。

適用上の注意：

73 *この要件は、TOEが接続されてい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メッセージで使用するためにTOEによって生成されるグループ一時鍵（GTK）に適用される。802.11-2007は、転送フォーマット及びRFC 3394に規定されているAES鍵包込み方法によって転送フォーマットを包み込まなければならないことを規定する。*

保証アクティビティ：

74 *評価者は、本PPに規定されているAES実装を使用してGTKを配付する前にGTKを包み込む方法、及び複数クライアントがTOEに接続しているときにGTKを配付する方法が記述されていることを確認するために、TSSをチェックしなければならない。評価者は、次のテストも実行しなければならない。*

- *テスト1：評価者は、正常に複数のクライアントをTOEに接続しなければならない。評価者は、クライアントを接続するとき、GTKがクライアントとTOE間で平文で送信されないことを観察しなければならない。*
- *テスト2：評価者は、正常に複数のクライアントをTOEに接続しなければならない。評価者は、メッセージが暗号化され、判読できないことを確認しなければならない。*
- *テスト3：評価者は、TOEに接続されているクライアントの部分集合間に、それぞれがTOEに接続されているすべてのクライアントより少ない2台以上のクライアントから構成される2つ以上のマルチキャストグループを作成しなければならない。（すべてでなく）一部のクライアントは両方のグループに属さなければならない。*

評価者は、確立されたGTKが参加クライアントに送信され、クライアントとTOE間を流れるトラフィックから決定できないことを確認しなければならない。

- *テスト4：評価者は、TOEに接続されている各マルチキャストグループ内のクライアントにマルチキャストメッセージを送信しなければならない。評価者は、各メッセージが暗号化され、判読できない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 TSFは、もはや必要でなくなったとき、すべての平文の秘密と秘密暗号鍵及び暗号セキュリティパラメタをゼロ化しなければならない。

適用上の注意：

75 *セキュリティ上重要なデータの開示または改ざんを防止するために、セキュリティ関連情報（鍵、認証データ、パスワードなど）は、使用されなくなったとき、ゼロ化されなければならない。*

76 *上記のゼロ化は、鍵/重大なセキュリティパラメタが他の場所に転送されるとき、平文鍵及び/または重大なセキュリティパラメタ用の各中間記憶域（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）に適用される。*

保証アクティビティ：

77 *評価者は、各秘密鍵（対称暗号化に使用される鍵）、私用鍵、及び鍵を生成するために使用される重大なセキュリティパラメタ、それらがゼロ化されるとき（例えば、使用直後、システムシャットダウン時など）、及び実行されるゼロ化手順のタイプ（ゼロで上書きする、ランダムパターンで3回上書きするなど）がTSSに記述されていることを確認しなければならない。保護される情報を保存するために異なるタイプのメモリが使用される場合、評価者は、データが保存されるメモリまたは記憶域のタイプの観点から、ゼロ化手順がTSSに記述されていることを確認しなければならない（例えば、「フラッシュに保存される秘密鍵はゼロで1回上書きしてゼロ化される、内蔵ハードディスクドライブに保存される秘密鍵は、書込みの都度変更されるランダムパターンで3回上書きしてゼロ化される」）。*

暗号操作（FCS_COP）

FCS_COP.1(1) **暗号操作（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、指定された暗号アルゴリズム、[**[割付：1つまたは複数のモード]**で動作するAES]及び暗号鍵サイズ128ビット、256ビット、及び**[選択：192ビット、他の鍵サイズなし]**に従って、[暗号化及び復号]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：

78 *割付では、ST執筆者は、AESが動作するモードを選択するべきである。最初の選択では、ST執筆者は、この機能によってサポートされる鍵サイズを選択するべきである。2番目の選*

択では、ST執筆者は、割付に指定されたモードを記述する規格を選択するべきである。

79 *なお、この要件は、無線トラフィック暗号化には適合されない。要件FCS_COP.1(5)は、無線WPA2暗号化/復号に使用されるモード、鍵サイズ及び規格を定義する。*

保証アクティビティ：

80 *評価者は、上記の要件をテストするためのガイドとして、上記の要件で「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)」、及び「The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)」の中から選択されたモードに適したテストを使用しなければならない（これらの文書は、http：//csrc.nist.gov/groups/STM/cavp/index.htmlから入手できる）。これには、評価者がテスト中に検証可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

FCS_COP.1(2) **暗号操作（暗号署名）**

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

(1) 鍵サイズ（法）が2048ビット以上のデジタル署名アルゴリズム（DSA）、

(2) 鍵サイズ（法）が2048ビット以上のRSAデジタル署名アルゴリズム（rDSA）、または

(3) 鍵サイズ(法）が256ビット以上の楕円曲線デジタル署名アルゴリズム（ECDSA）]

適用上の注意：本PPの将来の刊行では、望ましい暗号署名方式として、楕円曲線が要求されるだろう。

であって、以下に準拠するもの：

デジタル署名アルゴリズムの場合：

- **[選択：FIPS PUB 186-3、「Digital Signature Standard」]**

RSAデジタル署名アルゴリズムの場合：

- **[選択：FIPS PUB 186-3、「Digital Signature Standard」]**

楕円曲線デジタル署名アルゴリズムの場合：

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

適用上の注意：

81 *ST執筆者は、デジタル署名を実施するよう実装されるアルゴリズムを選択するべきである。*

もし複数のアルゴリズムが利用可能であれば、この要件（及び関連するFCS_CKM.1要件）は、機能性を特定するために繰り返し記述されるべきである。選択されたアルゴリズムに関して、ST執筆者は適切な割付／選択を行い、そのアルゴリズムについて実装されたパラメタを特定するべきである。

82 *楕円曲線に基づくスキームに関して、鍵サイズはbase pointの位数のlog2をとった値を意味する。 本PPの将来の刊行では、望ましいデジタル署名として、ECDSAが要求されるだろう。*

保証アクティビティ：

83 *評価者は、上記の要件をテストする際のガイドとして、「The Digital Signature Algorithm Validation System (DSA2VS)」、「The Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)」、及び「The RSA Validation System (RSA2VS)」の署名生成及び署名検証部分を使用しなければならない。 使用される検証システムは、STに識別される適合規格（例えばFIPS PUB 186-3）に適合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ーを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

FCS_COP.1(3)	**暗号操作（暗号技術的ハッシュ）**
FCS_COP.1.1(3)	**詳細化：**TSFは、以下に合致する、規定された暗号アルゴリズム**［選択：SHA-1、SHA-256、SHA-384］**及び**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、**暗号技術的ハッシュサービス**を実施しなければならない。**FIPS Pub 180-3、「Secure Hash Standard」**

適用上の注意：

84 *ハッシュ生成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が選択される場合、有効なメッセージダイジェストサイズ選択は160ビットのみであろう。*

保証アクティビティ：

85 *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ーを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

FCS_COP.1(4)	**暗号操作（鍵付ハッシュメッセージ認証）**
FCS_COP.1.1(4)	**詳細化：**TSFは、以下に合致する、規定され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で使用される鍵サイズ（ビット数）]**、及び**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、**鍵付ハッシュメッセージ認証**を実施しなければならない。**FIPS PUB 198-1、「The Keyed-Hash Message Authentication Code」、及びFIPS PUB 180-3、「Secure Hash Standard」**

適用上の注意：

86 *ハッシュ生成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が選択される場合、有効なメッセージダイジェストサイズ選択は256ビットのみであろう。*

87 *上記のメッセージダイジェストサイズは、使用される基礎となるハッシュアルゴリズムに対応する。なお、ハッシュ計算に続くHMAC出力の切詰めは、様々なアプリケーションで*

適切なステップである。これによりこの要件との適合が無効になるわけではないが、切詰めが実行されること、最終出力のサイズ、及びこの切詰めが適合する規格をSTに記載するべきである。

保証アクティビティ：

88 *評価者は、上記の要件をテストする際のガイドとして、「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可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

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：**FIPS PUB 197、NIST SP 800-38C、及びIEEE 802.11-2007**に合致する、**指定された暗号アルゴリズムAES CCMP及び128ビットの暗号鍵サイズに従って、暗号化及び復号を**実行しなければならない。。

適用上の注意：

89 *なお、IEEE 802.11-2007に適合するために、128ビットの暗号鍵サイズを持つAES CCMP(SP 800-38Cに規定されているようにCCMでAESを使用する）が実装されなければならない。将来、この規格が更新され、新しい暗号モードがNISTによってレビューされ、承認されたとき、追加/新しい暗号モードと鍵サイズに関する要件がこの要件に含まれる場合がある。*

保証アクティビティ：

90 *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)」に記載されている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可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

91 *また、評価者は、AES-CCMPのIEEE 802.11-2007実装をさらに検証するために、2002年9月10日付けのIEEE 802.11-02/362r6文書「Proposed Test vectors for IEEE 802.11 TGi」のSection 2.1 AES-CCMP Encapsulation Example and Section 2.2 Additional AES CCMP Test Vectorsに記載されているテストを使用しなければならない。*

拡張：インターネットプロトコルセキュリティ（FCS_IPSEC_EXT）

92 TOEは、RADIUSプロトコルを実装する認証サーバと通信することが要求される。この接続の保護を強化するために、適合TOEは、RADIUSプロトコルが移動する認証サーバとのIPsec接続を実装する。他のITエンティティ(監査サーバなど）またはリモート管理者が特定のTOEのためにIPsecを使用する場合は、この要件も適合される。次の要件にはRADIUSまたは認証サーバ固有の側面はない。

FCS_IPSEC_EXT.1	**拡張：インターネットプロトコルセキュリティ（IPsec）通信**
FCS_IPSEC_EXT.1.1	TSFは、暗号アルゴリズムAES-CBC-128、AES-CBC-256（ともにRFC 3602に規定されている)、[選択：他のアルゴリズムなし、RFC 4106に規定されているAES-GCM-128、AES-GCM-256]を使用し、[選択、1つ以上を選択する：RFC 2407、2408、2409、RFC 4109に定義されているIKEv1、及び[選択：ハッシュ関数に関する他のRFCなし、ハッシュ関数に関するRFC 4868]、RFC 5996（Section 2.23に規定されている必須のNATトラバースのサポー

	ト付き）、4307に定義されているIKEv2、及び認証サーバとの接続に関する[選択：ハッシュ関数に関する他のRFCなし、ハッシュ関数に関するRFC 4868]]及び[選択：他のサーバなし、[割付：TOEが接続するサーバのリスト]]を使用して、RFC4303によって定義されるIPsecプロトコルESPを実装しなければならない。
FCS_IPSEC_EXT.1.2	TSFは、ESP機密性及び完全性セキュリティサービスのみが使用されることを保証しなければならない。
CS_IPSEC_EXT.1.3	TSFは、IKEv1 Phase 1交換がメインモードのみを使用することを保証しなければならない。
FCS_IPSEC_EXT.1.4	TSFは、[選択：IKEv1 SAの存続期間がパケット数と時間で制限できる：Phase 1 SAは24時間、Phase 2 SAは8時間、IKEv2 SAの存続期間がパケット数と時間に基づいて管理者によって設定できる]ことを保証しなければならない。
FCS_IPSEC_EXT.1.5	TSFは、FCS_RBG_EXT.1に規定されているランダムビット生成器を使用して、[割付：NIST SP 800-57、*Recommendation for Key Management - Part 1：General*のTable 2に記載されている、交渉されるDiffie-Hellmanグループに関連付けられた「セキュリティのビット数」の値の2倍以上である（1つまたは複数の）ビット数]ビット以上の長さを持つ、IKE Diffie-Hellman鍵交換で使用される秘密の値x（xは$g^x \bmod p$のx）を生成しなければならない。
FCS_IPSEC_EXT.1.6	TSFは、特定のIPsec SAの存続期間中に特定のナンス値が繰り返される確率が2^[割付：NIST SP 800-57、*Recommendation for Key Management - Part 1：General*のTable 2に記載されている、交渉されるDiffie-Hellmanグループに関連付けられた「セキュリティのビット数」]の中の1未満になるような方法でIKE交換に使用されるナンスを生成しなければならない。
FCS_IPSEC_EXT.1.7	TSFは、すべてのIKEプロトコルが、DH Group 14（2048ビットMODP）及び[選択：DH Group 24（256ビットPOSを備えた2048ビットMODP）、DH Group 19（256ビットランダムECP）、DH Group 20（384ビットランダムECP）、[割付：TOEによって実装された他のDHグループ]、他のDHグループなし]を実装することを保証しなければならない。
FCS_IPSEC_EXT.1.8	TSFは、すべてのIKEプロトコルが事前共有鍵及びRFC 4945に適合するX.509v3証明書を使用する[選択、1つ以上を選択する：DSA、rDSA、ECDSA]を使用して、ピア認証を実装することを保証しなければならない。
FCS_IPSEC_EXT.1.9	TSFは、既定で、[選択：*IKEv1 Phase 1*、*IKEv2 IKE_SA*]接続を保護するために交渉される対称アルゴリズムの（鍵のビット数としての）強度が、交渉される保護する[選択：*IKEv1 Phase 2*、*IKEv2 CHILD_SA*]接続を保護するために交渉される対称アルゴリズムの（鍵のビット数としての）強度以上であることを保証できなければならない。

適用上の注意：

93 *WLANアクセスシステムと認証サーバ間のRADIUS通信を保護するために、少なくともFCS_IPSEC_EXT.1がサポートされる。最初の選択は、サポートされる追加暗号アルゴリズムを識別するために使用される。適合TOEは両方を提供できるが、IKEv1またはIKEv2のいずれかのサポートを提供しなければならない。2番目の選択は、この選択を行うために使用される。IKEv1の場合、要件は、RFC 2409に適合するIKE実装にRFC 4109に記述されている追加/変更を加えることが要求されると解釈されるべきである。RFC 4868は、IKEv1とIKEv2の両方で使用するための追加のハッシュ関数を識別する。これらの関数が実装される場合は、3番目（IKEv1の場合）及び4番目（IKEv2の場合）の選択を使用できる。最後の選択/割付は、通信がIPsecによって保護され、TOEが通信する他のサーバ/サービス（監査サーバなど）を指定する。*

94 FCS_IPSEC_EXT.1.4：*ST執筆者は、最初の要件での選択に応じて、IKEv1要件またはIKEv2要件のいずれか（または両方）を選択する。IKEv1要件は、（AGD_OPEによって義務付けられた文書内の該当する指示により）許可された管理者が設定可能な存続期間を提供する、または実装に制限を「ハードコード」することで、達成できる。 IKEv2の場合、ハードコード化される制限はないが、この場合には管理者が値を設定できることが要求される。一般に、SAの存続期間を含めて実装のパラメタを設定するための指示は、AGD_OPE用に生成される管理者ガイダンスに含めるべきである。TOEが同じ鍵で保護されるトラフィックの量（その鍵で保護されるすべてのIPsecトラフィックの総量）に対する制限を設定できる限り、パケット数の代わりにMB/KB数を使用して要求を詳細化することが適切である。*

*95 実装ではSAの形成に使用するために異なるDiffie-Hellmanグループを交渉できるので、FCS_IPSEC_EXT.1.5とFCS_IPSEC_EXT.1.6の割付に複数の値を含めることができる。サポートされるDHグループごとに、ST執筆者は、800-57のTable 2を参照して、DHグループに関連付けられた「セキュリティのビット数」を決定する。 次に、一意の値を使用して、割付を記入する（1.5の場合は2倍にされる、1.6の場合は割付に直接挿入される）。例えば、実装がDH Group 14（2048ビットMODP）及びGroup 20（NIST曲線P-384を使用するECDH）をサポートすると仮定する。 Table 2から、セキュリティのビット数の値は、Group 14では112、Group 20では192である。次に、FCS_IPSEC_EXT.1.5では割付が「*224、384+」になり、FCS_IPSEC_EXT.1.6では「*112、192+」になる（ただし、この場合は、おそらく数学的に意味を持つように要件を詳細化するべきであろう）。*

96 FCS_IPSEC_EXT.1.7： *選択は、サポートされる追加のDHグループを指定するために使用される。 これは、IKEv1及びIKEv2交換に適用される。 本PPの将来のバージョンでは、DH Group 19（256ビットランダムECP）及びDH Group 20（384ビットランダムECP）が要求されるだろう。 追加のDHグループが指定される場合は、それらのDHグループが（確立された一時鍵の観点から）FCS_CKM.1(2)に記載されている要件に適合しなければならないことに注意するべきである。*

97 FCS_IPSEC_EXT.1.8： *事前共有鍵及び1つ以上の公開鍵に基づくピア認証方法が適合TOEに要求される。ST執筆者は、TOEの実装を反映するために1つまたは複数の公開鍵スキームを選択する。また、ST執筆者は、それらの方法をサポートするために、使用されるアルゴリズム（及び提供される場合は鍵生成機能も）を反映する適切なFCS要件が記載されていることを確認する。なお、TSSは、これらのアルゴリズムを使用する方法を詳述する(例えば、2409は、公開鍵を使用する3つの認証方法を規定し、サポートされる各方法がTSSに記述される)。*

98 FCS_IPSEC_EXT.1.9： *ST執筆者は、TOEの実装に基づいて、IKE選択のいずれかまたは両方を選択する。明らかに、選択されるIKEバージョンは、このコンポーネントだけでなく、このエレメント内の他のエレメントに関する他の選択とも一貫しているべきである。TOEはこ*

の機能を設定可能にしてもよいが、評価される構成の既定の設定（「出荷時」またはOPE文書内のガイダンス文書による）は、この機能を有効にしなければならない。

保証アクティビティ：

99 *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_IPSEC_EXT.1エレメントについて記載されている該当する各RFCの節ごとに、「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）、及び「SHOULD NOT」（するべきでない）など）すべての文について、TOEがこのようなオプションを実装する場合は、それをTSSに記述しなければならない。 含まれる機能が規格に「SHOULD NOT」（するべきでない）または「MUST NOT（してはならない）と示されている場合、TSSは、TOEによって実装されたセキュリティ方針に悪影響しない根拠を提供しなければならない。*
- 各RFCの節ごとに、「MUST」（しなければならない）または「SHOULD」（するべきである）文に関連する機能の省略を記述しなければならない。
- *TOEが施行する予定のセキュリティ要件に影響するかもしれないTOE固有の拡張、規格に含まれない処理、または規格によって許可される代替実装を記述しなければならない。*

100 *評価者は、IPsec接続を要求または許可するすべてのサーバ/サービスがTSSに記載されていることを確認しなければならない。また、評価者は、テスト及び分析アクティビティを実行するとき、アクティビティが識別されているすべてのサーバに適用されることを確認しなければならない。評価者は、テストアクティビティの間、識別された通信を行うことができるという保証を提供するために、1つ以上のテストでサーバのすべてのタイプについて1つ以上のインスタンスが使用されることを確認しなければならない。また、評価者は、これらの接続のTOE以外のエンドポイントに関する構成情報（製品及びバージョン番号を含む）がテスト報告書に記録されることを確認しなければならない。*

101 *評価者は、IKEv2を実装するTOEについて次のテストも実行しなければならない。*

- *テスト1[条件付き]：評価者は、TSS 及びRFC 4306、Section 2.23 に記載されている通りNAT トラバース処理を実行するように、TOE を設定しなければならない。 評価者は、IPsec 接続を開始し、NAT トラバースが正常に行われることを決定しなければならない。*

102 *FCS_IPSEC_EXT.1.2 - 評価者は、「機密性専用」ESPセキュリティサービスを無効にする方法が記述されていることを検証するために、TSSを検査しなければならない。 また、評価者は、ESP用の「機密性専用」セキュリティサービスの交渉を無効にするために必要な設定が記述されていること、及びパケット全体を保護するためにトンネルモードが優先ESPモードであることを示す助言が存在することを決定するために、運用ガイダンスを検査しなければならない。*

- *テスト1：評価者は、運用ガイダンスに記載されているようにTOE を設定し、「機密性専用」セキュリティサービスを使用するESP を使用して接続の確立を試みなければならない。 この試行は失敗するべきである。 次に、評価者は、機密性及び完全性セキュリティサービスを使用するESP を使用して、接続を確立しなければならない。*

103 *FCS_IPSEC_EXT.1.3 - 評価者は、TOEによってサポートされるIPsecプロトコルの記述に、IKEv1 Phase 1交換ではアグレッシブモードが使用されず、メインモードのみが使用されることが*

記載されていることを確認するために、TSSを検査しなければならない。これにより操作の前にTOEの設定が要求される場合、評価者は、この設定の指示が運用ガイダンスに含まれていることを確認するために、運用ガイダンスをチェックしなければならない。 評価者は、以下のテストも実行しなければならない。

- *テスト1：評価者は、運用ガイダンスに記載されているようにTOE を設定し、IKEv1 Phase 1 接続をアグレッシブモードで使用して接続の確立を試みなければならない。 この試行は失敗するべきである。次に、評価者は、メインモード交換がサポートされていることを示すべきである。*

104 *FCS_IPSEC_EXT.1.4 – IKEv1要件が選択される場合、評価者は、IKEv1 SAの存続期間（Phase 1とPhase 2の両方）を確立する方法がTSSに記述されていることを確認する。存続期間が設定可能の場合、評価者は、これらの値を設定するための適切な指示が運用ガイダンスに含まれていることを検証する。 IKEv2要件については、評価者は、値が設定可能であり、値を設定するための指示が運用ガイダンスに存在することを検証する。また、評価者は、IKEv1、IKEv2、またはその両方を設定するのいずれかに応じて、以下のテストを実行する。*

- *テスト1（IKEv1）：評価者は、Phase 1 SAを確立し、その再交渉の前に24時間以上Phase 1 SAを維持するテストを作成しなければならない。 評価者は、24時間以内にこのSAが閉じられるまたは再交渉されることを観察しなければならない。 このようなアクションがTOEを特定の方法で設定することを要求する場合、評価者は、運用ガイダンスに記載されているようにTOEの設定機能が動作することを実証するテストを実装しなければならない。*
- *テスト2（IKEv1）：評価者は、Phase 2 SAについてテスト1と同様のテストを実行しなければならない。ただし、存続期間は、24時間でなく8時間である。*
- *テスト3（IKEv1及びIKEv2）：評価者は、許可されるパケット数によって最大存続期間を設定しなければならない。これはIKEv1の場合はハードコード化される値であってもよい。そうでない場合、評価者は、運用ガイダンスに従う。評価者は、SAを確立し、このSAを通過するパケット数が許可されているパケット数を超える場合に接続が閉じられることを決定しなければならない。*
- *テスト4（IKEv2）：評価者は、SAの時間ベースの最大存続期間を設定し、それからSAを確立しなければならない。 評価者は、確立された時間内にこのSAが閉じられる、または再交渉されることを観察しなければならない。*

105 *FCS_IPSEC_EXT.1.5、FCS_IPSEC_EXT.1.6 - 評価者は、TSFによってサポートされるDHグループごとに、「x」（FCS_IPSEC_EXT.1.5に定義されている）及び各ナンスを生成するプロセスがTSSに記述されていることを確認しなければならない。評価者は、本PPの要件に適合する生成される乱数が使用され、「x」の長さ及びナンスが要件の規定に適合することがTSSに示されていることを確認しなければならない。*

106 *FCS_IPSEC_EXT.1.7 - 評価者は、要件に規定されているDHグループが、TSSでサポートされるDHグループとして記載されていることを確認しなければならない。複数のDHグループがサポートされている場合、評価者は、特定のDHグループを指定する方法/ピアと交渉する方法がTSSに記述されていることを確認する。評価者は、次のテストも実行しなければならない。*

- *テスト1：サポートされるDH グループごとに、評価者は、その特定のDH グループを使用してすべての IKE プロトコルを正常に完成できることを確認するために、テストを実行しなければならない。*

107 FCS_IPSEC_EXT.1.8 – 評価者は、事前共有鍵を確立し、IPsec接続の認証に使用する方法がTSSに記述されていることを確認しなければならない。評価者は、TOE用の事前共有鍵を生成し、確立する方法が運用ガイダンスに記述されていることをチェックしなければならない。TSS及び運用ガイダンスの記述は、事前共有鍵を生成するTOE及び事前共有鍵を使用するだけのTOEの両方のために事前共有鍵を確立できることも示さなければならない。評価者は、次のテストも実行しなければならない。

- *テスト1：評価者は、2 つのピア間の IPsec 接続を確立するために、運用ガイダンスに示されている通りに事前共有鍵を生成し、それを使用しなければならない。TOE が事前共有鍵の生成をサポートする場合、評価者は、鍵の確立が鍵を生成する TOE のインスタンスだけでなく、鍵を使用するだけの TOE のインスタンスのためにも実行されることを確認しなければならない。*

108 評価者は、TOEによって使用されるIKEピア認証プロセスの記述がTSSに含まれていること、及びこの記述が選択で指定されたアルゴリズムの使用を網羅していることをチェックしなければならない。FCS_IPSEC_EXT.1.1に関する保証アクティビティの一環として、RFC 4945の必須エレメントとオプションのエレメントが記載されなければならない。評価者は、以下のテストも実行しなければならない。

- *テスト1：サポートされるアルゴリズムごとに、評価者は、そのアルゴリズムを使用するピア認証を正常に実行できることをテストしなければならない。*
- *テスト2：（RFC 4945からの）サポートされる識別ペイロードごとに、評価者は、ピア認証を正常に実行できることをテストしなければならない。*
- *テスト3：評価者は、認証用の壊れたまたは無効の証明書パスがIKEピア認証中に検出され、その結果、接続が確立されないことを実証するテストを考案しなければならない。*
- *テスト4：評価者は、CRLを通じて取り消された証明書がIKEピア認証中に検出され、その結果、接続が確立されないことを実証するテストを考案しなければならない。*

109 FCS_IPSEC_EXT.1.10 – 評価者は、IKE及びESP交換に許可されるアルゴリズムの潜在的な強度（対称鍵のビット数として）がTSSに記述されていることをチェックしなければならない。TSSには、交渉されるアルゴリズムの強度（対称アルゴリズム内の鍵のビット数として）が交渉を保護しているIKE SAの強度以下であることを確認するために、IKEv1 Phase 2及び/またはIKEv2 CHILD_SAスイートを交渉するときに行われるチェックも記述されていなければならない。評価者は、以下のテストも実行しなければならない。

- *テスト1：このテストは、TOE によってサポートされる IKE のバージョンごとに実行されなければならない。評価者は、サポートされている各アルゴリズム及び要件に識別されているハッシュ関数を使用して、IPsec 接続を正常に交渉しなければならない。*
- *テスト2：このテストは、TOE によってサポートされる IKE のバージョンごとに実行されなければならない。評価者は、IKE SA にとって使用されている暗号化アルゴリズムより強度が高い暗号化アルゴリズム（すなわち、IKE SA 用に使用される鍵サイズより大きい鍵サイズを持つ対称アルゴリズム）を選択する ESP 用の SA の確立を試行しなければならない。*

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、[選択、1つを選択：[選択：Hash_DRBG（任意）、HMAC_DRBG（任意）、CTR_DRBG（AES）、Dual_EC_DRBG（任意）]を使用するNIST Special Publication 800-90、FIPS Pub 140-2 Annex C、AESを使用するX9.31 Appendix 2.4]に従って、1つ以上の独立したTSFハードウェアに基づくノイズ源からエントロピーを蓄積するエントロピー源によってシードされた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	決定性RBGは、少なくともそれが生成する鍵と許可要因の最も大きいビット長に等しい、最低でも[選択、1つを選択：128ビット、256ビット]のエントロピーによってシードされなければならない。

適用上の注意：

110 *NIST Special Pub 800-90、Appendix Cには、おそらくFIPS-140の将来の版で要求されるであろう最小エントロピー値が記載されている。可能であれば、これをただちに使用するべきであり、本PPの将来のバージョンで要求されるだろう。*

111 *FCS_RBG_EXT.1.1の最初の選択では、ST執筆者は、RBGサービスが適合する規格（800-90または140-2 Annex Cのいずれか）を選択するべきである。*

112 *SP800-90には、4つの異なる乱数生成方法が含まれている。各方法は、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、使用される関数を選択し（800-90が選択される場合）、使用される特定の基礎となる暗号プリミティブを要件またはTSSに記載する。Hash_DRBGまたはHMAC_DRBGについては指定されたハッシュ関数（SHA-1、SHA-224、SHA-256、SHA-384、SHA-512）が許されるが、CT_DRBGについてはAESに基づく実装のみが許される。Dual_EC_DRBGについては800-90に定義されている任意の曲線が許されるが、ST執筆者は選択した曲線を記載するだけでなく、使用されるハッシュアルゴリズムも記載しなければならない。*

113 *なお、現在FIPS Pub 140-2 Annex Cでは、NIST- Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms、Section 3に記載されている方法のみが有効である。 ここで使用されるAES実装用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鍵の長さと異なる場合は、異なる鍵の長さを反映するためにFCS_COP.1を調整するか、繰り返さなければならないことがある。FCS_RBG_EXT.1.2における選択では、ST執筆者は、RBGをシードするために使用されるエントロピーの最小ビット数を選択する。*

114 *また、ST執筆者は、TOEの基底要件に基礎となる関数が含まれていることを確認する。*

115 *将来は、「A Method for Entropy Source Testing：Requirements and Test Suite Description」に記載されているほとんどの要件が、本PPによって要求されるだろう。現在、以下の保証アクティビティは、要求されるアクティビティの部分集合のみを反映している。*

保証アクティビティ：

116 *評価者は、TOEで使用されるRBGを含んでいる製品のバージョン番号を決定するために、TSS節をレビューしなければならない。また評価者は、エントロピーが収集されるハードウェアベースのノイズ源がTSSに記載されていること、及びこのノイズ源がUSBフラッシュドライブに搭載されていることを確認しなければならない。さらに、評価者は、RBGに使用されるすべての基礎となる関数とパラメタがTSSに記載されていることを検証する。*

117 評価者は、エントロピー入力を取得する方法、使用されるエントロピー源を識別する方法、各エントロピー源からエントロピーを生成し、収集する方法、及び各エントロピー源によって生成されるエントロピーの量など、RBGモデルの記述がTSSに含まれていることを検証しなければならない。また、評価者は、エントロピー源ヘルステスト、エントロピー源のヘルスを決定するためにヘルステストが十分である根拠、及びエントロピー源の故障の既知のモードがTSSに記載され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/または環境条件による出力と分散の独立性の観点で、RBG出力の記述がTSSに含まれていることを検証しなければならない。

118 RBGが適合を主張する規格にかかわらず、評価者は次のテストを実行する。

- テスト1：評価者は、エントロピー源テストスイートを使用して各エントロピー源のエントロピー見積りを決定する。評価者は、すべてのエントロピー源から得られるすべての結果の最小値であるエントロピー見積りが、TSS に含まれていることを確認しなければならない。

119 また、評価者は、RBGが適合する規格に応じて、以下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

120 本節に含まれるテストについての参考文献は、The Random Number Generator Validation System (RNGVS) [RNGVS]である。 評価者は、以下の2つのテストを実行しなければならない。なお、「期待値」は、正しいと知られているアルゴリズムの標準実装により生成される。正しさの証明は各認証機関（スキーム）に任されている。

121 評価者は、可変シードテストを実行しなければならない。評価者は、TSF RBG機能に対する128ペア（シード、DT）のセットをそれぞれ128ビットで提供しなければならない。また、評価者は、すべての128ペア（シード、DT）に対して一定の値の（AESアルゴリズムについて適切な長さの）鍵を提供しなければならない。DTの値は、それぞれのセットについて1ずつ増加される。セットの中で、シードの値は重複してはならない。評価者はTSFから返される値が期待値と一致していることを確認する。

122 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、それぞれ128ビットの初期シードとDT値をTSF RBG関数に与える。また、評価者は、テストを通して一定の値の（AESアルゴリズムについて適切な長さの）鍵を提供しなければならない。評価者は、（毎回）DTの値を1ずつ増加させつつ、TSF RBGを10,000回呼び出して、次の繰り返しで使用される新しいシードは、NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms、Section 3で指定されるように生成される。評価者は、10,000回目に生成された値が期待値と一致することを確認する。

NIST Special Publication 800-90に適合する実装

123 評価者は、RBG実装について、15回試行を実施しなければならない。もし、RBGが設定変更可能であれば、評価者は設定ごとに15回試行しなければならない。また、評価者は、RBG機能性を設定変更するために適切な指示が操作ガイダンスに含まれていることも確認しなければならない。

124 RBGが予測耐性を備えている場合、それぞれの試行は(1)drbgの具体化、(2)ランダムビット列の1番目のブロックの生成、(3)ランダムビット列の2番目のブロックの生成、(4)終了処理(ゼロ化)、から成り立つ。評価者は、ランダムビット列の2番目のブロックが期待値であ

ることを検証する。評価者は、それぞれの試行について８つの入力値を生成しなければならない。１番目は、整数カウンタ（0-14）である。次の3つは、具体化操作のためのエントロピー入力、ナンス（Nonce）、及び個別化文字列である。次の2つは、（乱数）生成の初回の呼び出しについての追加入力とエントロピー入力である。最後の2つは、（乱数）生成の2回目の呼び出しのための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。「ランダムビット列の１ブロックを生成する」とは、（NIST SP 800-90で定義された）出力ブロック長に等しい返されたビット数のランダムビット列を生成するという意味である。

125 *RBGが予測耐性を備えていない場合、それぞれの試行は(1)drbgの具体化、(2)ランダムビット列の1番目のブロックの生成、(3)初期化、(4)ランダムビット列の2番目のブロックの生成、(5)終了処理（ゼロ化）、から成り立つ。評価者は、ランダムビット列の2番目のブロックが期待値であることを検証する。評価者は、それぞれの試行について８つの入力値を生成しなければならない。１番目は、整数カウンタ（0-14）である。次の3つは、具体化操作のためのエントロピー入力、ナンス（Nonce）、及び個別化文字列である。5番目の値は、初回生成呼び出しへの追加入力である。6番目と7番目は、再シード呼び出しへの追加入力及び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への追加入力である。*

126 *次の段落は、評価者によって生成／選択される入力値のいくつかについての詳細情報を含んでいる。*

127 ***エントロピー入力**：エントロピー入力の長さは、シード長と等しくなければならない。*

128 ***ナンス（Nonce）**：ナンスがサポートされている（dfなしのCTR_DRBGがナンスを使用しない）場合、ナンスビット長はシード長の半分となる。*

129 ***個別化文字列**：個別化文字列の長さは、シード長以下でなければならない。もし、実装がある個別化文字列の長さのみをサポートするなら、両方の値について同じ長さが利用可能である。もし、複数の長さの文字列がサポートされているなら、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。もし、実装が個別化文字列を使用しないなら、値を提供する必要はない。*

130 ***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を持つ。*

4.1.3 利用者データ保護クラス（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、すべてのオブジェクト[選択：への資源の割当て、からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを実施しなければならない。

適用上の注意：

131 *この要件は、例えば、プロトコルデータ単位（PDU）が暗号鍵関連情報のような残存情報で埋められないことを保証する。ST執筆者は、選択を使用して、以前の情報を利用できなくするときを指定する。*

保証アクティビティ：

132 *この要件の文脈における「資源」とは、（管理者がTOEに接続するときの「接続先」に対し）TOEを通じて送信されるネットワークパケットである。問題は、ネットワークパケットが送信された後、パケットによって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からのデータが含まれ、そのバッファが再利用されるとき、それらのデータが残存し、新しいパケットに入る場合があることである。評価者は、ネットワークパケットを処理するときにデータが再利用されないことを決定できる程度にパケット処理がTSSに記述されていることを確認しなければならない。評価者は、この記述に少なくとも以前のデータがどのようにゼロ化/上書きされ、バッファ処理のどの時点でこれが行われるかが記載されていることを確認しなければならない。*

4.1.4 識別及び認証クラス（FIA）

133 TOEは、その稼働中に異なる利用者とITエンティティに対する多様な識別及び認証（I&A）方式をサポートしなければならない。I&Aプロセスの一部と見なされるいくつかの要件、特に複数のサービス用に使用される暗号プロトコル（IPsec、WPA2など）に関連する要件は、本PPの他の節に規定されている。これは、理解と保証アクティビティの執筆と適用を容易にするために、それらのプロトコルに関する要件をまとめておくために行われた。

134 現在、SNMP（SNMPv3を含む）は、本PPの要件を満たすことができないため、TOEを管理するための唯一の手段として許容可能なオプションではないことに注意するべきである。ただし、SNMPがリモート管理用にFTP_TRP.1.1に記載されているいずれかのプロトコル内にトンネルされる場合は、（FMT要件によって）要求される機能がそのインタフェースを通じて使用できるなら、TOEを管理するために使用できる。

135 この節の要件は、適合TOEのI&A機能のいくつかの側面を取り扱う。

- **管理者用のI&A**．管理者は、TOEによって識別され、認証される唯一の利用者である。無線クライアントはそのクライアント経由でネットワークに接続する人間を代表しているが、これらの利用者はTOEによって識別も認証もされない。
- **802.1X-2010認証**．802.1X-2010規格（及び関連するRFCS）は、ネットワークにアクセスする目的のための機械の認証を規定する。この方法は、802.11-2007規格を使用する無線操作への先駆として使用される。802.1Xには802.1X交換に参加するいくつかの異なるパーティに関する要件が含まれるが、下記の要件は802.1Xによる「認証者」としてのTOEの役割を対象にしている。
- **クレデンシャル**．PPの本節及び他の節に規定されているプロトコルとメカニズムは、I&Aプロセスで使用されるいくつかの異なるクレデンシャルに依存する。パスワード（管理者用）、事前共有鍵（IPsec及び潜在的にITエンティティとの他の（TLS、SSH）接続用）、及び証明書（IPsec接続及び潜在的に管理者（IPsec、TLS、SSH）用）。

136 以下の要件は、わかりやすくするために可能な範囲で（アルファベット順でなく）これらのカテゴリ別に分類されている。

認証失敗時の取り扱い（FIA_AFL）

FIA_AFL.1	**認証失敗時の取り扱い**
FIA_AFL.1.1	**詳細化**：TSFは、**リモート認証を試みる管理者**に関して、**許可された管理者が**設定できる**正の整数値**回の**連続**不成功認証試行

が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数に**達した**とき、TSFは、[選択、1つを選択：許可されたローカル管理者によって[割付：アクション]が取られるまで問題のリモート管理者の認証成功を防止、許可された管理者が定義した時間が経過するまで問題のリモート管理者の認証成功を防止**]しなければならない**。

適用上の注意：

137 *この方法でローカル管理者のアカウントをロックすることには意味がないため、この要件はローカルコンソールにいる管理者には適用されない。これは、（例えば）ローカル管理者には別のアカウントを要求する、または認証メカニズム実装にローカルのログイン試行とリモートのログイン試行を区別させることで対処できよう。ローカル管理者によって取られる「アクション」は実装ごとに異なり、管理者ガイダンスに定義されるだろう（例えば、ロックアウトのリセットまたはパスワードのリセット）。ST執筆者は、TOEでの処理の実装に基づいて、いずれかの認証失敗処理を選択する。*

保証アクティビティ：

138 *評価者は、リモート管理のアクションについてサポートされる方法ごとに、連続認証失敗試行を検出し、追跡する方法の記述が含まれていることを決定するために、TSSを検査しなければならない。また、TSSは、リモート管理者によるTOEへのログオン成功を防止する方法及びこの機能を復元するために必要なアクションを記述しなければならない。また、評価者は、（そのオプションが選択される場合）指定される「アクション」ごとに、連続認証失敗試行回数（1.1）及び時間（1.2、実装されている場合）を設定するための指示が提供され、リモート管理者に再びログイン成功を許可するプロセスが記述されていることを確認するために、運用ガイダンスを検査しなければならない。認証方法（TSLまたはSSH）に基づいて異なるアクションまたはメカニズムが実装されている場合は、すべてを記述しなければならない。*

139 *評価者は、リモート管理者がTOEにアクセスする方法（TSLまたはSSH）ごとに、以下のテストを実行しなければならない。*

- *テスト1[最初の選択項目について条件付き]：評価者は、運用ガイダンスを使用して、TOEによって許可される連続認証失敗試行回数を設定しなければならない。評価者は、制限に到達したら、有効なクレデンシャルがあっても試行が成功しないことをテストしなければならない。要件に規定されているアクションごとに、評価者は、運用ガイダンスに従い、各アクションを実行することで、リモート管理者によるアクセスが成功することを示さなければならない。*
- *テスト2[2番目の選択項目について条件付き]：評価者は、運用ガイダンスを使用して、TOEによって許可される連続認証失敗試行回数及びリモート管理者の有効なログインが許可されるまでの時間を設定しなければならない。無効ログイン試行の指定回数を超え、有効なログインが不可能なことが示された後で、評価者は、他のアクセス試行が行われるまでの定義された時間が過ぎると、有効なクレデンシャルを使用したリモート管理者のログオンが成功することを示さなければならない。*

パスワード管理（FIA_PMG）

FIA_PMG_EXT.1 パスワード管理

FIA_PMG_EXT.1.1 TSFは、管理者パスワードに以下のパスワード管理機能を提供

しなければならない。

1. *パスワードは、大文字、小文字、数字、及び特殊文字（"!"、"@" "#"、"$"、"%"、"^"、"&"、"*"、"("、及び")"）の任意の組合せから構成できなければならない。*
2. *最小パスワード長は許可された管理者によって設定可能であり、8文字以上のパスワードをサポートしなければならない。*
3. *パスワードを構成する必要な文字の種類と個数を規定するパスワード作成ルールは、管理者によって設定可能でなければならない。*
4. *パスワードには、許可された管理者によって設定可能な最大存続期間がなければならない。*
5. *新しいパスワードは、前のパスワードから4文字以上変更されなければならない。*

適用上の注意：

140 *なお、FIA_UAU.6ではパスワードを変更するとき再認証が要求されるため、4文字以上が変更されていることを決定するためにパスワードの平文バージョンを保存する必要はない。*

141 *「管理パスワード」とは、ローカルコンソールで、またはSSHやHTTPSのようなパスワードをサポートするプロトコル経由で管理者によって使用されるパスワードを指す。*

142 *上記の項目3の意図は、例えば、パスワードに1文字以上の大文字、1文字以上の小文字、1文字以上の数字、及び1文字以上の特殊文字が含まれ、TOEがこの制限を実施することを許可された管理者が指定できることである。「種類」は、このエレメント内の項目1に記載されているすべての種類を指す。*

保証アクティビティ：

143 *評価者は、強力なパスワードの作成に関するガイダンスが管理者に提供され、最小パスワード長を設定するための指示、パスワード作成ルールの定式化と仕様及びTOE用にこれらを設定する方法、及びパスワードの最大存続期間を設定する方法が提供されていることを決定するために、運用ガイダンスを検査しなければならない。評価者は、以下のテストも実行しなければならない。なお、単一のテストケースでこれらのテストの1つまたは複数を実行することができる。*

- *テスト1：評価者は、要件に規定されているように、異なるパスワード作成ルールでTOEを設定しなければならない。次に、評価者は、ルールの集合ごとに、何らかの方法で要件を満たすパスワードと要件を満たさないパスワードの両方を作成しなければならない。パスワードごとに、評価者は、作成ルールが実施されていることを検証しなければならない。評価者にはすべての可能な作成ルールをテストすることは要求されない（実行不可能でもある）が、評価者は、要件に記載されているすべての文字、ルール特性、及び最小長がサポートされていることを確認し、テスト用に選択されたそれらの文字の部分集合を正当化しなければならない。*
- *テスト2：評価者は、運用ガイダンスに最大パスワード存続期間を設定するための指示が含まれていることを確認しなければならない。次に、評価者は、この存続期間をいくつかの値に設定し、それぞれの値について存続期間が実施されていることを確認しなければならない。*

- *テスト3：評価者は、前のパスワードからの4文字以上の変更が実施されていることをテストしなければならない。*

FIA_UIA_EXT.1	**利用者識別及び認証**
FIA_UIA_EXT.1.1	TSFは、TOE以外のエンティティが識別及び認証プロセスを開始することを要求する前に、以下のアクションに対する応答を許可しなければならない。 • FTA_TAB.1に従って警告見出しを表示する、 • [割付：サービスのリスト、TOE以外の要求に応えてTSFによって実行されるアクション]。
FIA_UIA_EXT.1.2	TSFは、管理利用者のために他のTSFによるアクションを許可する前に、各管理利用者が正常に識別され、認証されることを要求しなければならない。

適用上の注意：

144 *この要件は、TOEとの接続によって使用できるサービスではなく、TOEから直接使用できるサービスの利用者（管理者及び外部Tエンティティ）に適用される。外部エンティティは識別及び認証の前にサービスをほとんど使用できないか、まったく使用できないが、使用できるサービス（おそらくICMPエコー）がある場合は、これらを割付文に記載すべきである。それ以外の場合は、「サービスなし」が許容可能な割付である。*

145 *認証は、ローカルコンソール経由またはパスワードをサポートするプロトコル（SSHなど）経由のパスワードに基づく認証、または証明書に基づく認証（SSH、TLS）が可能である。*

146 *外部Tエンティティ（監査サーバまたはNTPサーバなど）との通信の場合、このような接続はそのプロトコルが識別及び認証を実行するFTP_ITC.1に従って実行されなければならない。すなわち、接続の確立が識別と認証プロセスの開始と「解釈」されるので、このような通信（例えば、認証サーバとのIPsec接続の確立）を割付に指定する必要はない。*

保証アクティビティ：

147 *評価者は、製品用にサポートされているログオン方法（ローカル、リモート（HTTPS、SSH）など）ごとにログオンプロセスが記述されていることを決定するために、TSSを検査しなければならない。この記述には、許可される/使用される証明書、実行されるプロトコルトランザクション、及び「ログオンの成功」を構成するものに関連する情報が含まれていなければならない。評価者は、必要なログイン準備ステップ（事前共有鍵、トンネル、証明書などのような証明書関連情報の確立）が記述されていることを決定するために、運用ガイダンスを検査しなければならない。サポートされるログイン方法ごとに、評価者は、ログオンが成功するための明確な指示が運用ガイダンスに提供されていることを確認しなければならない。ログイン前に提供されるサービスが制限されることを保証するための設定が必要な場合、評価者は、許可されるサービスの制限に関する十分な指示が運用ガイダンスに提供されていることを決定しなければならない。*

148 *評価者は、管理者がTOEにアクセスする（ローカル及びリモート）方法ごとに、またログイン方法によってサポートされるクレデンシャルのタイプごとに、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、運用ガイダンスを使用して、ログイン方法のためにサポートされている適切な証明書を設定しなければならない。その証明書/ログイン方法*

について、評価者は、正しいI&A情報の提供によりシステムにアクセスでき、間違った情報の提供によりアクセスが拒否されることを示さなければならない。

- *テスト2：評価者は、運用ガイダンスに従って許可されたサービスを設定し（存在する場合）、それから外部リモートエンティティが使用できるサービスを決定しなければならない。評価者は、使用できるサービスのリストが要件に規定されているサービスに制限されていることを決定しなければならない。*
- *テスト3：ローカルアクセスについて、評価者は、ログインの前にローカル管理者が使用できるサービスを決定し、このリストが要件と一貫していることを確認しなければならない。*

FIA_UAU_EXT.5　　パスワードベースの認証メカニズム

FIA_UAU_EXT.5.1　　TSFは、管理利用者認証を実行するために、ローカルパスワードに基づく認証メカニズム、[選択：[割付：*他の認証メカニズム*]、なし]を提供しなければならない。

FIA_UAU_EXT.5.2　　TSFは、期限が切れたパスワードを持つ管理利用者が[選択：期限が切れたパスワードを正しく入力した後で新しいパスワードを作成する必要がある、管理者によってパスワードがリセットされるまでロックアウトされる]ことを保証しなければならない。

適用上の注意：

145 *この要件はローカル管理者ログインのみに適用され、実質的にこの目的のためにTOEにパスワードベースのメカニズムが存在することを要求する。ST執筆者は、ローカルでない管理利用者のために、サポートされている他の認証メカニズム（認証サーバなど）を割付に記入することができる。管理利用者のために外部認証メカニズムがサポートされていない場合、ST執筆者は、選択に「なし」を選ぶべきである。*

保証アクティビティ：

146 *この要件に関する保証アクティビティは、FIA_UIA_EXT.1に関する保証アクティビティで網羅されている。他の認証メカニズムが指定される場合、評価者は、FIA_UIA_EXT.1に関するアクティビティにそれらの方法を含めなければならない。*

FIA_UAU.6　　再認証

FIA_UAU.6.1　　TSFは、以下の条件で管理利用者を再認証しなければならない。*利用者がパスワードを変更するとき、[選択：TSFが開始するロックの後（FTA_SSL）、[割付：他の条件]、他の条件なし]。*

保証アクティビティ：

147 *評価者は、要件に規定されている条件ごとに、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、運用ガイダンスの指示に従って、パスワードの変更を試みなければならない。この試行にあたり、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。*

FIA_UAU.7　　保護された認証フィードバック

FIA_UAU.7.1　　TSFは、ローカルコンソールで認証が実行されているとき、管理利用者に曖昧なフィードバックのみを提供しなければならない。

適用上の注意：

148 *「曖昧なフィードバック」とは、TSFが（パスワードのエコーのように）利用者によって入力された認証データをそのままでは表示しないことを指す。ただし、進行状況は提供してもよい（各文字をアスタリスクで置き換えるなど）。また、TSFが認証プロセス中に認証データが表示されるような情報を利用者に返さないことも指す。*

保証アクティビティ：

149 *評価者は、許可されるローカルログイン方法ごとに、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 にローカルに認証されなければならない。この試行にあたり、評価者は、クレデンシャルを入力する際に曖昧なフィードバックのみが提供されることを検証しなければならない。*

802.1Xポートアクセス制御認証（FIA_8021X_EXT）

FIA_8021X_EXT.1	**802.1Xポートアクセスエンティティ（認証者）認証**
FIA_8021X_EXT.1.1	TSFは、「認証者」の役割にあるポートアクセスエンティティ（PAE）について、IEEE規格802.1Xに適合しなければならない。
FIA_8021X_EXT.1.2	TSFは、RFC 2865及び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。
FIA_8021X_EXT.1.3	TSFは、この認証交換の正常終了の前に、802.1Xで制御されるTSFのポートへのアクセスが無線クライアントに提供されないことを保証しなければならない。

適用上の注意：

150 *この要件は、802.1X認証交換における認証者としてのTOEの役割を取り扱う。交換が正常終了する場合、TOEはRADIUSサーバからPMKを取得し、802.11通信を開始するために無線クライアント（サプリカント）との4ウェイハンドシェイクを実行する。*

151 *既に示したように、交換中には、エンドポイントとしてのTOEに2つ、転送ポイントとしてのみ機能するTOEに1つの少なくとも3つの通信パスが存在する。TOEは、802.1X-2007に規定されているように、無線クライアントとのEAP over LAN（EAPOL）接続を確立する。また、TOEは、（IPsec接続の中でトンネルされる）RADIUSサーバとのRADIUSプロトコル接続を確立する（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セッションを確立する（RFC 5216）。このトランザクションでは、TOEは単にそのEAPOL/RADIUSエンドポイントからEAP-TLSパケットを取得し、他のエンドポイントに転送する。TOEは具体的な認証方法（この場合TLS）を認識しないため、本PPにはRFC 5126に関する要件はない。ただし、基本RADIUSプロトコル（RFC 2865）には、実装と保証アクティビティで取り扱う必要がある更新（RFC 3579）がある。さらに、RFC 5080には開発者が解決する必要がある実装課題が含まれているが、それによって新しい要件は課されない。*

152 *802.1X認証を実行する意味は、（認証が成功し、すべての802.11交渉が正常に実行されると仮定して）ネットワークへのアクセスを提供することである。802.1Xの用語で表現すると、これは、無線クライアントがTOEによって維持される「制御ポート」にアクセスできることを意味する。*

保証アクティビティ：

153 *TSFが802.1X-2010規格を正しく実装していることを示すために、評価者は、TSSに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。*

- *TOEが実装する規格の節（段落）、*
- *識別される節ごとに規格によって許可されるオプションが指定される、及び*
- *識別される節ごとに、不適合の正当化を含めて、不適合が識別され、記述される。*

154 *RADIUSサーバとの接続はIPsecトンネル（FCS_IPSEC_EXT.1）に含まれるため、これらの通信の保護を提供するために、要件に識別されたRFCに詳述されているセキュリティメカニズムには依存しない。その結果、RFCの徹底的な分析は要求されない。ただし、評価者は、TOEがこの要件に記載されているRFCに適合することを保証するために製品開発者が行う対策がTSSに記述されていることを確認しなければならない（文書、テスト）。*

155 *評価者は、以下のテストも実行しなければならない。*

- *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にアクセスできないことを実証しなければならない。TOE経由でRADIUSサーバに正常に認証された後で、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ることを実証しなければならない。*
- *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。評価者は、EAP-TLS交渉が失敗するような無効の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。 その結果、無線クライアントはまだテストネットワークにアクセスできないはずである。*
- *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。評価者は、EAP-TLS交渉が失敗するような無効のRADIUS証明書を使用して認証を試みなければならない。 その結果、無線クライアントはまだテストネットワークにアクセスできないはずである。*

156 *上記のテスト2及び3は、EAP-TLSの動作がテストされるが、「EAP-TLSが動作する」ことのテストではないことに注意するべきである。テストは、実際に認証の失敗（2つの失敗モードで）の結果、ネットワークへのアクセスが拒否されることである。これは、このコンポーネントの3番目のエレメントである。*

事前共有鍵作成（FIA_PSK_EXT）

157 TOEは、最低でもIPsecプロトコルで使用するための事前共有鍵をサポートしなければならない。また、（WPA2を除き）他のプロトコルでも事前共有鍵を使用できる。下記の要件に規定されているように、TOEは、2種類の事前共有鍵をサポートしなければならない。最初のタイプを「テキストベースの事前共有鍵」と呼び、パスワードのように標準文字セットからの文字列として利用者が入力する事前共有鍵を指す。このような事前共有鍵は、文字列がビット列に変換されるように条件付けされなければならない。

158 2番目のタイプを（標準用語がないため）「ビットベースの事前共有鍵」と呼び、管理者からコマンドでTSFによって生成される鍵または管理者によって「直接形式」で入力される鍵を指す。「直接形式」とは、テキストベースの事前共有鍵のような「条件付け」なしで、入力が鍵として直接使用されることを意味する。例えば、鍵を構成するビットを表す16進数の文字列がそうである。

159 下記の要件は、TOEがテキストベース事前共有鍵とビットベースの事前共有鍵の両方をサ

ポートしなければならないことを義務付ける。ただし、ビットベースの事前共有鍵の生成は、TOEまたは運用環境のいずれで行ってもよい。

FIA_PSK_EXT.1	**拡張：事前共有鍵作成**
FIA_PSK_EXT.1.1	TSFは、IPsec及び**[選択：他のプロトコルなし、[割付：事前共有鍵を使用する他のプロトコル]]**用の事前共有鍵を使用できなければならない。
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付けることができなければならない。 • **22文字及び*[選択：[割付：他のサポートされる長さ]、他の長さなし]*、** • 大文字、小文字、数字、及び特殊文字（"!"、"@" "#"、"$"、"%"、"^"、"&"、"*"、"("、及び")"）の任意の組合せから構成される。
FIA_PSK_EXT.1.3	TSFは、[選択：SHA-1、SHA-256、SHA-512、[割付：*テキスト文字列の条件付け方法*]]を使用して、テキストベースの事前共有鍵を条件付けしなければならない。
FIA_PSK_EXT.1.4	TSFは、ビットベースの事前共有鍵を[選択：受け付ける、FCS_RBG_EXT.1で規定されているランダムビット生成器を使用して生成する]ことができなければならない。

適用上の注意：

160 *最初の選択では、他のプロトコルが事前共有鍵を使用できる場合、それを割付に記載するべきである。それ以外の場合は、他のプロトコルなし」を選択するべきである。この要件の意図は、すべてのプロトコルがテキストベースの事前共有鍵及びビットベースの事前共有鍵の両方をサポートすることである。*

161 *テキストベースの事前共有鍵の長さについては、相互接続性を促進するために共通の長さ（22文字）が要求される。他の長さがサポートされる場合は、割付に記載するべきである。この割付は、値の範囲（例えば「5～55文字の長さ」）も指定できる。*

162 *FIA_PSK_EXT.1.3の選択では、ST執筆者は、管理者によって入力されるテキスト文字列を鍵として使用されるビット列に「条件付ける」方法を選択する、または入力する。これは、規定されているハッシュ関数のいずれかを使用する、または割付文を通じて他の方法を使用することで行うことができる。*

163 *FIA_PSK_EXT.1.4では、ST執筆者は、TSFが単にビットベースの事前共有鍵を受け付けるのか、またはビットベースの事前共有鍵を生成できるのかを指定する。TSFがビットベースの事前共有鍵を生成する場合、要件にはTOEによって提供されるRBGを使用して生成されなければならないと規定されている。*

保証アクティビティ：

164 *評価者は、強力なテキストベースの事前共有鍵の作成に関するガイダンスが管理者に提供されていること、及び（様々な長さの鍵を入力できることが選択に示されている場合）より短いまたはより長い事前共有鍵の利点に関する情報が提供されていることを決定するために、運用ガイダンスを検査しなければならない。ガイダンスは、事前共有鍵に使用できる文字を指定しなければならない。また、リストは、FIA_PSK_EXT.1.2に含まれるリストのスーパーセットでなければならない。*

165 評価者は、テキストベースの事前共有鍵及びビットベースの事前共有鍵の両方を許可するすべてのプロトコルが識別されていること、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が記載されていることを確認するために、TSSを検査しなければならない。要求に識別されているプロトコルごとに、評価者は、利用者によって入力されるキーシーケンス（ASCII表現）からプロトコルによって使用されるビット列にテキストベースの事前共有鍵を変換するために行われる条件付けがTSSに記載されていること、及びこの条件付けがFIA_PSK_EXT.1.3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。

166 評価者は、要件に識別されているプロトコルごとに、ビットベースの事前共有鍵を入力する、またはビットベースの事前共有鍵を生成する（またはその両方の）ための指示が運用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。また、評価者は、ビットベースの事前共有鍵を生成するプロセスが記述されている（TOEがこの機能をサポートする場合）ことを確認するために、TSSを検査しなければならない。また、このプロセスがFCS_RBG_EXT.1で規定されているRBGを使用することを確認しなければならない。

167 また、評価者は、プロトコル（またはTOEの別の実装によって実行される場合はプロトコルの具体化）ごとに、以下のテストを実行しなければならない。なお、単一のテストケースでこれらのテストの1つまたは複数を実行することができる。

- *テスト1：評価者は、運用ガイダンスに従って許可される文字の組合せが含まれている22文字の事前共有鍵を作成し、鍵を使用してプロトコル交渉を正常に実行できることを実証しなければならない。*
- *テスト2[条件付き]：TOEが複数の長さの事前共有鍵をサポートする場合、評価者は、最小の長さ、最大の長さ、及び無効の長さを使用してテスト1を繰り返さなければならない。最小の長さと最大の長さのテストは成功しなければならない。無効の長さはTOEによって拒否されなければならない。*
- *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、運用ガイダンスの指示に従って、適切な長さのビットベースの事前共有鍵を入手し、入力しなければならない。次に、評価者は、鍵を使用してプロトコル交渉を正常に実行できることを実証しなければならない。*
- *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、運用ガイダンスの指示に従って、適切な長さのビットベースの事前共有鍵を生成し、使用しなければならない。次に、評価者は、鍵を使用してプロトコル交渉を正常に実行できることを実証しなければならない。*

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、RFC 5280によって定義されているX.509v3証明書を使用して、IPsec及び[選択：他のプロトコルなし、TLS、SSH]接続用の認証をサポートしなければならない。
FIA_X509_EXT.1.2	TSFは、証明書を保存し、許可されていない削除と変更から保護しなければならない。
FIA_X509_EXT.1.3	TSFは、本PPに規定されているセキュリティ機能が使用するために、許可された管理者がX.509v3証明書をTOEに読み込む機能を提供しなければならない。

適用上の注意：

168 *FIA_X509_EXT.1.1では、ST執筆者は、認証に証明書を使用する管理接続を実装するために使用されるプロトコルを選択するべきである。 RFC 5280には、この要件に従ってTOEによって実装されなければならない証明書検証及び認定パス検証要件が定義されていることに注意するべきである。*

169 *選択されるプロトコルによっては、規定されたプロトコル固有の追加証明書関連要件（及び関連する保証アクティビティ）が存在する場合がある（例えば、IPsecに関するRFC 4945）。これらの追加要件は、そのプロトコルに関連する要件に規定されている。*

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。運用環境内の他のコンポーネント（例えばRADIUSサーバ）によって使用され、処理される証明書は、このエレメントでは取り扱われない。*

保証アクティビティ：

171 *TSFがRFC 5280に従ってX.509v3証明書の使用をサポートすることを示すために、評価者は、TSSに以下の情報が記述されていることを確認しなければならない。*

- *TOEが規格のその特定の部分を実装することを読者が決定できるように、RFC 5280の節ごとに「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）、及び「SHOULD NOT」（するべきでない）など）すべての文を記述しければならない。*
- *RFC 5280の節ごとに、「MUST」（しなければならない）または「SHOULD」（するべきである）にへの不適合を記述しなければならない。*
- *TOEが施行する予定のセキュリティ要件に影響するかもしれないTOE固有の拡張または規格に含まれない処理を記述しなければならない。*

172 *さらに、評価者は、TOEがTSSに記述されている実装に従う証明書を処理し、規格及びTSSに規格に規定されている通りに認定パスを形成でき、規格に規定されている通りに証明書を検証できる（CRL処理を含む認定検証パス）ことを示すテストを考案しなければならない。このテストは、チームテスト計画に記述されなければならない。*

173 *本PPの将来の刊行ではTOEの証明書処理機能に関するより明示的なテスト要件が記載されることに注意するべきである。さらに、プロトコル固有の証明書処理テストを実行する必要があり、この保証アクティビティによって要求されるテストと組み合わせることができる。*

174 *TSSは、本PPの要件を満たすために使用される証明書を含む、実装されたすべての証明書記憶域を記述しなければならない。この記述は、証明書を記憶域に読み込み、記憶域を無許可アクセスから保護する方法に関する情報を含まなければならない。*

175 *評価者は、証明書の使用を要求するシステムの各機能について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、有効な認定パスなしに証明書を使用する場合、機能が失敗することを実証しなければならない。次に、評価者は、機能に使用される証明書を検証するために必要な証明書を読み込み、機能が成功することを実証しなければならない。次に、評価者は、いずれかの証明書を削除し、機能が失敗することを示さなければならない。*

4.1.5 セキュリティ管理クラス（FMT）

176 この節の主な意図は、怠慢な利用者がWLANアクセスシステムを安全でない状態に放置することを防止するために、管理者が実行しなければならない重大なアクティビティを規定することである。適合TOEの管理モデルは、本PPの1.1.3節に記述されている。TOEが追加機能を提供する場合は、附属書Cからの該当する管理及びI&A要件をSTに含めるべきである。

FMT_MOF.1 **セキュリティ機能のふるまいの管理**

FMT_MOF.1.1 **詳細化：TSFは、本PPで識別されているTOEのすべてのセキュリティ機能のふるまいを動作させる、を停止する、を停止する、を決定する、を改変する能力を、許可された管理者に制限しなければならない。**

適用上の注意：

177 *TOEの利用者のみが管理利用者である。従って、この要件は、管理利用者以外の利用者がPPのセキュリティ要件を実装するために使用されるTOEのメカニズムを操作できないことを示すために存在する。これらの機能は、管理または冗長の観点からTOEコンポーネントをネットワークに追加し、構造化するためにTOEに実装されている機能を明示的に網羅する。*

保証アクティビティ：

178 *評価者は、本PPの要件に応えて実装された各機能が識別され、その構成情報が管理者のみが機能にアクセスできることを保証するために提供されていることを決定するために、運用ガイダンスをレビューしなければならない。評価者は、検査されるこの機能のリストに、TOEの追加インスタンスを構成に追加するメカニズム、及び複数のTOEインスタンスを管理階層及び/または冗長アーキテクチャに組み込む構成を含めなければならない。評価者は、運用ガイダンスに識別された管理機能ごとに、管理者がログインする前にインタフェース経由でアクセスできる管理機能が識別されていることを決定するために、TSSを検査しなければならない。また、評価者は、これらの機能のそれぞれについて、このインタフェースを通じてシステムの構成を操作する機能が管理利用者以外の利用者には許可されないことvがTSSに詳述されていることを確認しなければならない。*

TSFデータの管理（FMT_MTD）

FMT_MTD.1(1) **TSFデータの管理（一般的TSFデータ）**

FMT_MTD.1.1(1) TSFは、TSFデータを*管理*する機能を、*許可された管理者*に制限しなければならない。

適用上の注意：

179 *「管理」には、作成、初期化、表示、既定の変更、変更、削除、消去、及び追加などが含まれる。この要件は、TSFデータの管理に関する「既定」要件を意図している。FMT_MTDの他の繰返しは、具体的に識別されたTSFデータに関する異なる制限または使用できる操作を課すべきである。TSFデータには、暗号情報も含まれる。これらのデータの管理には、暗号プロトコルとインタフェースの関連付けなどが含まれるだろう。*

保証アクティビティ：

180 *管理機能はTSFデータを操作するため、FMT_MOF.1に関する保証アクティビティで評価者によって実行される分析はこの要件が満たされることを実証する。*

FMT_MTD.1(2) **TSFデータの管理（認証データの読取）**

FMT_MTD.1.1(2) **詳細化**：TSFは、**パスワードベースの認証データの読取を防止**しなければならない。

適用上の注意：

181 *要件の意図は、（暗号化されていないパスワードのような）生の認証データを読み取ることで利用者になりすますことができる場合、いかなる利用者または管理者であっても、「通常」のインタフェースを通じてこのようなデータを読み取ることができないということである。もちろん、すべての権限を持つ管理者は、メモリを直接読み取ったり、ファイルシステムを生で読み取ってパスワードを取得できるが、そのようなことはしないと信頼されている。*

保証アクティビティ：

182 *評価者は、適用上の注意に記載されているように、この要件に支配されるすべての認証データ及びその目的のために設計されているインタフェースを通じて認証データを表示できないように認証データを保存する方法が詳述されていることを決定するために、TSSを検査しなければならない。パスワードまたは他の認証データが平文で保存されない場合、TSSはパスワードを保護する方法及びパスワードを使用できる方法（管理者が入力するパスフレーズなど）を記述しなければならない。*

FMT_MTD.1(3) **TSFデータの管理（すべての対称鍵の読取に関して）**

FMT_MTD.1.1(3) **詳細化**：TSFは、すべての事前共有鍵、対称鍵、及び私用鍵の*読取*を**防止**しなければならない。

適用上の注意：

183 *要件の意図は、いかなる利用者または管理者であっても、「通常」のインタフェースを通じて識別された鍵（保存された鍵または一時鍵）を読み取るまたは表示することができないということである。もちろん許可された管理者はこれらの鍵を表示するためにメモリを直接読み取ることができるが、そのようなことはしないと信頼されている。*

保証アクティビティ：

184 *評価者は、適用上の注意に記載されているように、事前共有鍵、対称鍵、及び私用鍵を保存する方法及びその目的のために設計されているインタフェースを通じて表示できないことが詳述されていることを決定するために、TSSを検査しなければならない。これらの値が平文で保存されない場合は、これらの値を保護する/曖昧にする方法をTSSに記述しなければならない。*

管理機能の特定（FMT_SMF）

FMT_SMF.1 **管理機能の特定**

FMT_SMF.1.1 TSFは、以下のセキュリティ管理機能を実行できなければならない。:

- *それぞれFIA_UIA.1に規定されているように、エンティティが識別され、認証される前に使用できるTOEサービスのリストを設定する機能。*
- *暗号機能を設定する機能。*
- *TOEを更新し、デジタル署名機能を使用して更新を検証する機能（FCS_COP.1（2））及び[選択：他の機能なし、[割付：更新機能をサポートするために使用される他の暗号機能（または他の機能）]]。*

- *TOEの無許可使用に関するTOE助言的注意及び承諾警告メッセージを設定する機能。*
- ***本PPの他の節に識別されているすべてのセキュリティ管理機能を設定する機能。***

適用上の注意：

185 *FMT_SMF.1に関するセキュリティ管理機能は、PP全体に分散され、FMT_MOF、FMT_MSA、FMT_MTD、FMT_REV、FPT_TST_EXT、及び参照規格に規定されている暗号管理機能の要件の一部として含まれている。*

保証アクティビティ：

186 *この要件は、単に他の要件で規定されているメカニズムが実際にTOEに具体化されていることを保証する。従って、これらのメカニズムが存在し、他の要件と一貫している方法で動作することの検証は、それらの他の要件に関連する保証アクティビティを通じて提供される。*

セキュリティ管理役割（FMT_SMR）

FMT_SMR.1	**セキュリティ管理役割**
FMT_SMR.1.1	TSFは以下の役割を維持しなければならない： • **許可された管理者、** • ***[他の役割なし]***
FMT_SMR.1.2	TSFは、利用者を役割に関連付けしなければならない。
FMT_SMR.1.3	TSFは、以下の条件が満たされることを保証しなければならない： • **許可された管理者役割は、**TOEをローカルに管理できなければならない。 • **許可された管理者役割は、**TOEをリモートに管理できなければならない。 • **無線クライアントからTOEをリモートに管理する機能はデフォルトでは無効になっていなければならない。**

適用上の注意：

187 *FMT_SMR.1.2は、利用者アカウントをただ1つの役割に関連付けることを要求する。ただし、複数の利用者が同じ役割を持つことができ、TOEが役割を1人の利用者に制限することは要求されない。*

188 *FMT_SMR.1.3は、許可された管理者がローカルコンソール及びリモートメカニズム（IPsec、SSH、TLS/HTTPS）を通じて、TOEを管理できることを要求する。複数コンポーネントTOEの場合、他のTOEの設定コンポーネントの管理制御と構成を提供するTOEコンポーネントのみがローカル管理インタフェースを要求する。*

保証アクティビティ：

189 *評価者は、リモート管理用にクライアント上で実行する必要がある設定を含めて、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含まれていることを確認するために、*

運用ガイダンスをレビューしなければならない。評価のためのテストアクティビティを実行する過程で、評価者は、サポートされるすべてのインタフェースを使用しなければならないが、各インタフェースでの管理アクションを含む各テストを繰り返す必要はない。ただし、評価者は、本PPの要件に適合するTOEを管理するサポートされる各方法がテストされることを保証しなければならない。
例えば、TOEがローカルハードウェアインタフェース（SSH及びTLS/HTTPS）経由で管理できる場合、評価チームのテストアクティビティの間に3つの管理方法すべてを実行しなければならない。

190 *評価者は、次のテストも実行しなければならない。*

- *テスト1：評価者は、運用ガイダンスに従って初めて使用するためにTOE を設定した後で、デバイスの「有線」部分にTOE との管理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。次に、TOE に正常に接続できる同じ設定の無線クライアントを使用しても、管理を実行できないことを実証しなければならない。*

4.1.6 TSF 保護クラス（FPT）

フェールセキュア（FPT_FLS）

FPT_FLS.1	**フェールセキュア**
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くてはならない：**電源投入時自己テストの失敗**。

適用上の注意：
191 *この要件の意図は、TOEが備えるフェールセキュア機能を表現することである。すなわち、TOEは、識別されているフェール発生時にセキュアな状態を保持できなければならない。TOEが重要な処理を実行している最中にフェールが発生した場合、TOEは鍵関連情報と利用者データを非保護のまま残した状態で処理を終了してはならない。*

保証アクティビティ：
192 *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ことを決定するために、TSS節をレビューしなければならない。評価者は、最初にTSS節を検査して、STにすべての故障モードが記述されていることを確認しなければならない。次に、評価者は、特定された各故障モードタイプを挿入した後で、TOEがセキュアな状態を保持することを確認しなければならない。評価者は、セキュアな状態が定義されていること、鍵関連情報と利用者データの保護を保証するために適切であることを決定するために、TSSをレビューしなければならない。*

リプレイ検出（FPT_RPL）

FPT_RPL.1	**リプレイ検出**
FPT_RPL.1.1	TSFは、以下のエンティティに対するリプレイを検出しなければならない：[*TOEで終了されたネットワークパケット*]。
FPT_RPL.1.2	TSFは、リプレイが検出された場合、[*データを拒否する*]をしなければならない。

適用上の注意：
193 *ネットワーク輻輳または消失パケット受信確認のために複数のネットワークパケットを受*

信することは、リプレイ攻撃と見なされない。 この要件の意図は、信頼できる性質の通信（管理者とTOE、ITエンティティとTOE、TOEとTOE）がエレメントによって網羅され、リプレイできないことを保証することである。

高信頼タイムスタンプ（FPT_STM）

FPT_STM.1	**高信頼タイムスタンプ**
FPT_STM.1.1	TSFは、それ自体で使用するための高信頼タイムスタンプを提供できなければならない。

TSF自己テスト（FPT_TST）

FPT_TST_EXT.1	**拡張：TSFテスト**
FPT_TST_EXT.1.1	TSFは、TSFが正しく動作することを実証するために、初回の起動時（電源投入時）に自己テストスイートを実行しなければならない。
FPT_TST_EXT.1.2	TSFは、FCS_COP.1(2)に規定されているTSFによって提供される暗号化サービスの使用を通じて、実行のために読み込まれる保存されたTSF実行コードの完全性を検証する機能を提供しなければならない。

保証アクティビティ：

194 *評価者は、起動時にTSFによって実行される自己テストが詳述されていることを確認するために、TSSを検査しなければならない。この記述には、テストが実際に行う内容の概要が含まれるべきである（例えば、「メモリがテストされる」と述べるのではなく、「各メモリ位置に値を書き込み、それを読み戻して書き込まれた値と同じであることを確認することでメモリがテストされる」のような記述を使用しなければならない）。評価者は、TSFが正しく動作することを実証するためにテストが十分であることがTSSに記載されていることを確認しなければならない。*

195 *評価者は、保存されたTSF実行コードが実行のために読み込まれるとき、そのコードの完全性を検証する方法が記述されていることを確認するために、TSSを検査しなければならない。これには、完全性を保証するために使用される「チェック値」の生成と保護及び検証ステップが含まれる。 また、この記述は、これらの機能を実行するときに使用されるデジタル署名サービスを網羅しなければならない。また、評価者は、管理者がこの機能を初期化または実行するために必要なアクションが存在することを確認するために、運用ガイダンスをチェックしなければならない。*

196 *また、評価者は、成功する場合（ハッシュは検証された）及び失敗する場合（ハッシュは検証されなかった）に行われるアクションがTSS（または運用ガイダンス）に記述されていることを確認する。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、運用ガイダンスに従って、完全性保護システムを初期化しなければならない。評価者は、TSFソフトウェアを読み込むアクションを実行し、実行ファイルに完全性エラーが含まれていることが完全性メカニズムから通知されないことを観察しなければならない。*
- *テスト2：評価者は、TSF実行ファイルを変更し、その実行ファイルがTSFによって読み込まれるようにする。 評価者は、完全性違反がトリガされることを観察する（フォーマットが壊れているために実行できないようにモジュールが変更された*

ことでなく、完全性違反がモジュール読み込み失敗の原因であることが決定されるように、注意しなければならない)。

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、許可された管理者に、TOEファームウェア/ソフトウェアの現在のバージョンを問い合わせる機能を提供しなければならない。
FPT_TUD_EXT.1.2	TSFは、許可された管理者に、TOEファームウェア/ソフトウェアの更新を開始する機能を提供しなければならない。
FPT_TUD_EXT.1.3	TSFは、TOEのファームウェア/ソフトウェア更新をインストールする前に、デジタル署名メカニズム及び[選択：公開されたハッシュ、他の機能なし]を使用してそれらの更新を検証するための手段を提供しなければならない。

適用上の注意：

197 *3番目のエレメントで参照されるデジタル署名メカニズムは、FCS_COP.1(2)で規定されるメカニズムである。参照される公開されたハッシュは、FCS_COP.1(3)に規定されている機能の1つによって生成される。*

保証アクティビティ：

198 *TOEの更新は、許可された源によって署名され、ハッシュが関連付けられていることがある。デジタル署名メカニズムについては、許可された源の定義は、更新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記述と共にTSSに含まれる。評価者は、この情報がTSSに含まれていることを確認する。また、評価者は、候補更新を取得する方法、更新のデジタル署名の検証に関連する処理、及び実装されている場合、更新のハッシュを計算する方法、及び成功（署名、及び含まれる場合ハッシュは検証された）及び失敗（署名、及び含まれる場合ハッシュは検証できなかった）の場合に行われるアクションがTSS（または運用ガイダンス）に記述されていることを確認する。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、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実行する。評価者は、運用ガイダンスに記述されている手順を使用して合法の更新を入手し、正常にTOEにインストールされることを検証する。次に、評価者は、他の保証アクティビティの部分集合を実行して、更新が期待通りに機能することを実証する。更新の後で、評価者は、バージョンが更新のバージョンに正確に一致す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実行する。*
- *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、バージョン検証アクティビティを実行する。評価者は、違法の更新を入手または生成し、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検証する。*

4.1.7 資源利用クラス

資源割当て（FRU_RSA）

FRU_RSA.1	**最大割当て**

FRU_RSA.1.1 TSFは[選択：*個人利用者、定義された利用者のグループ、サブジェクト*]が[選択：*同時に、特定した時間*]使用できる、以下の資源[割付：*管理インタフェースをサポートする資源*]、[選択：[割付：*制御される資源*]、*他の資源なし*]の最大割当てを実施しなければならない：

適用上の注意：

199 *少なくとも、適合TOEは、リモート管理インタフェースをサポートするために使用される消耗可能資源に割当制限を課さなければならない。これらは最初の割付にリストされる。制御できる他の資源（例えばTCP接続資源）は、2番目の割付に記載すべきである。他の資源がない場合は、選択の最後の項目を選ぶべきである。制御対象の資源の消費者を反映するために、2番目の選択を行うべきである。最後の選択は、制御対象資源の使用に関連する時間を制限するために使用される（例えば、30秒間に特定のIPアドレスからのTCP接続要求数に対する割当制限）。*

保証アクティビティ：

200 *評価者は、割当制限メカニズムを通じて制御されるすべての資源が識別され、管理インタフェースをサポートするために使用される資源がこのリストに含まれていることを確認するために、TSSを検査しなければならない。評価者は、各資源を「使用済み」としてカウントする方法及び最大割当制限または使用量を決定する方法、及び割当制限に到達したときに行われるアクションがTSSに記述されていることを確認しなければならない。また、TSSは、割当制限が利用者または制御対象（この場合TOEプロセス）に課されるかどうか、及び割当制限が同時使用またはある期間にわたる累積使用に課されるかどうかについても記述しなければならない。評価者は、割当制限を確立するための指示が含まれている（設定可能な場合）こと、及び割当制限に到達したときに管理者が行うことができる、または行うべきであるアクションが記述されていることを決定するために、運用ガイダンスを検査しなければならない。*

201 *評価者は、制御される資源ごとに以下のテストも実行しなければならない。*

- *テスト1：評価者は、運用ガイダンスに従って、資源の割当制限を設定する（このような機能が提供される場合）。次に、評価者は、資源制限への到達を引き起こし、TSS に規定されているアクションが行われることを観察する。*

4.1.8 TOE アクセスクラス（FTA）

TSF起動によるセッションロックと終了（FTA_SSL）

FTA_SSL_EXT.1 **TSF起動セッションロック**

FTA_SSL_EXT.1.1 **詳細化**：TSFは、**ローカル**対話型セッションについて以下を実行しなければならない。[選択：

- セッションをロックする - ディスプレイデバイスを消去または上書きして現在の内容を読めなくし、セッションのロック解除以外の利用者のデータアクセス/ディスプレイデバイスアクティビティを無効にし、セッションのロックを解除する前に管理者がTSFに再認証することを要求する、
- セッションを終了する]

これは、許可された管理者が指定した無活動時間後のアクションである。

保証アクティビティ：

202 *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、運用ガイダンスに従って、コンポーネントで参照されている無活動時間に様々な値を設定する。設定される時間ごとに、評価者は、TOEとのローカル対話型セッションを確立する。次に、評価者は、設定された時間後にセッションがロックまたは終了されることを観察する。コンポーネントからロックが選択された場合、評価者は、セッションのロックを解除するときに再認証が必要になることを確認する。*

FTA_SSL.3 **TSF起動による終了**

FTA_SSL.3.1 TSFは、**許可された管理者が設定可能なセッション無活動時間**の後で、**リモート**対話型セッションを終了しなければならない。

保証アクティビティ：

203 *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、運用ガイダンスに従って、コンポーネントで参照されている無活動時間に様々な値を設定する。これらは、少なくとも運用ガイダンスに指定されている許容最小値と最大値及び他の1 つの値から構成されなければならない。設定される時間ごとに、評価者は、TOE とのリモート対話型セッションを確0 立する。次に、評価者は、設定された時間後にセッションが終了されることを観察する。*

FTA_SSL.4 **利用者起動による終了**

FTA_SSL.4.1 TSFは、管理者が開始する終了により管理者自身の対話型セッションを終了できるようにしなければならない。

保証アクティビティ：

204 *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との対話型ローカルセッションを開始する。次に、評価者は、運用ガイダンスに従ってセッションを終了またはログオフして、セッションが終了されることを観察する。*
- *テスト2：評価者は、TOEとの対話型リモートセッションを開始する。次に、評価者は、運用ガイダンスに従ってセッションを終了またはログオフして、セッションが終了されることを観察する。*

TOEアクセス見出し（FTA_TAB）

FTA_TAB.1 **デフォルトTOEアクセスバナー**

FTA_TAB.1.1 **詳細化：管理利用者**セッションを確立する前に、TSFは、**許可された管理者が指定**したTOEの無許可使用に関するTOE助言的**注意及び承諾**警告メッセージを表示できなければならない。

適用上の注意：

205 *この要件は、利用者とTOE間の対話型セッションに適用されることを意図している。接続*

またはプログラムによる接続（例えばネットワーク経由のリモート手順呼出）を確立するITエンティティは、この要件で網羅される必要はない。

保証アクティビティ：

206 *評価者は、管理者が使用できる（ローカル及びリモートの）各アクセス方法（例えばシリアルポート、SSH、HTTPS）が詳述されていることを確認するために、TSSをチェックしなければならない。評価者は、次のテストも実行しなければならない。*

- *テスト1：評価者は、運用ガイダンスに従って、注意及び承諾警告メッセージを設定する。次に、評価者は、TSSに指定されているアクセス方法ごとに、TOEとのセッションを確立しなければならない。評価者は、それぞれの場合に注意及び承諾警告メッセージが表示されることを検証しなければならない。*

TOEセッション確立（FTA_TSE）

FTA_TSE.1	**TOEセッション確立**
FTA_TSE.1.1	**詳細化**：TSFは、位置、時刻、日、[割付：その他の属性]に基づいて、**無線クライアントセッション**の確立を拒否できなければならない。

適用上の注意：

207 *「位置」は、ポート番号、IPアドレス、サブネット、VLAN、TOEインタフェースなどによって指定できる。*

208 *ST執筆者は、割付を使用して、セッション確立の拒否がそれに基づくことができる追加属性を指定する。*

保証アクティビティ：

209 *評価者は、クライアントセッションを拒否できるすべての属性が具体的に定義されていることを決定するために、TSSを検査しなければならない。評価者は、TSSに識別されている各属性を設定するためのガイダンスが含まれていることを決定するために、運用ガイダンスを検査しなければならない。評価者は、属性ごとに以下のテストも実行しなければならない。*

- *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ッションを正常に確立する。次に、評価者は、運用ガイダンスに従って、属性の特定の値に基づいてそのクライアントのアクセスが拒否されるようにシステムを設定する。次に、評価者は、属性の設定に違反するセッションの確立を試みなければならない（例えば、クライアントのIPアドレスに基づいて位置が拒否される）。評価者は、アクセスが失敗することを観察しなければならない。*

4.1.9 高信頼パス/チャネルクラス（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、**802.11-2007、IPsec、及び[選択：SSH、TLS、TLS/HTTPS、他のプロトコルなし]を使用**して、それ自体と**許可されたすべてのITエンティティ**間に、他の通信チャネルから論理的に分離され、そのエンドポイントの保証された識別、チャネルデータの**開示**からの保護、及び**チャネルデータの変更の検出**を提供する**高信頼**通信チャネルを提供しなければならない。

FTP_ITC.1.2	TSFは、TSFまたは許可されたITエンティティが高信頼チャネル経由の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、[割付：TSFが通信を開始できるサービスのリスト]のために高信頼チャネル経由の通信を開始しなければならない。

適用上の注意：

210 *上記の要件の意図は、暗号プロトコルを使用して、TOEがその機能を実行するために対話する許可されたエンティティとのすべての外部通信を保護することである。802.11-2007は、無線クライアントとの通信に要求される。IPsecは少なくとも認証サーバとの通信に要求される。許可された他のITエンティティ（NTPサーバ、監査サーバ）との通信が必要な場合、これらのITエンティティはIPsecまたはリストに記載されている他のプロトコル（SSH、TLS及びTLS/HTTPSが許可される）の1つを使用しなければならず、ST執筆者は適切な選択を行う。ST執筆者は、選択を行った後で、STに入れるために選択したものに対応する附属書Cの詳細な要件を選択する。*

211 *通信を開始するパーティに関する要件はないが、ST執筆者は、FTP_ITC.1.3に関する割付に、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リストする。*

212 *要件は、初めて確立されるとき通信が保護されるだけでなく、故障後の再開でも保護されることを意味する。一部のTOE設定には、他の通信を保護するために手動でトンネルを設定することが含まれる場合がある。故障後にTOEが（必要な）手動介入と共に自動的に通信を再確立しようと試みる場合、攻撃者が重大な情報を取得する、または接続を不正使用する隙が生じることがある。*

保証アクティビティ：

213 *評価者は、許可されたITエンティティとのすべての通信について、そのITエンティティに許可されるプロトコルによって各通信メカニズムが識別されることを決定するために、TSSを検査しなければならない。また、評価者は、TSSに記載されるすべてのプロトコルが、STの要件に規定され、含まれていることを確認しなければならない。評価者は、許可された各ITエンティティとの許可されたプロトコルを確立するための指示が運用ガイダンスに含まれていること、及び接続が意図せず壊れた場合の復旧手順が運用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。評価者は、以下のテストも実行しなければならない。*

- *テスト1：評価者は、運用ガイダンスに記述されている通りに接続を設定し、通信が成功することを確認して、各プロトコルを使用する許可された各ITエンティティとの通信が評価の進行中にテストされることを確認しなければならない。*
- *テスト2：要件に定義されているようにTOEが開始できるプロトコルごとに、評価者は、運用ガイダンスに従って、実際にTOEから通信チャネルを開始できることを確認しなければならない。*
- *テスト3：評価者は、許可されたITエンティティとの通信チャネルごとに、チャネルデータが平文で送信されないことを確認しなければならない。*
- *テスト4：評価者は、許可されたITエンティティとの通信チャネルごとに、チャネルデータの変更がTOEによって検出されることを確認しなければならない。*
- *テスト5：評価者は、テスト1でテストされる許可された各ITエンティティに関連付けられたプロトコルごとに、接続が物理的に中断されることを確認しなければならない。評価者は、物理的な接続が復元されるとき、通信が適切に保護されることを確認しなければならない。*

214 さらに特定のプロトコルに保証アクティビティが関連付けられている。

高信頼パス（FTP_TRP）

FTP_TRP.1	**高信頼パス**
FTP_TRP.1.1	**詳細化**：TSFは、**[選択、1つ以上を選択する**：**IPsec、SSH、TLS、TLS/HTTPS]を使用**して、それ自体と**リモート管理者**間に、他の通信チャネルから論理的に分離され、そのエンドポイントの保証された識別、通信されるデータの*開示*からの保護、*及び通信されるの変更の検出*を提供する**高信頼**通信パスを提供しなければならない。
FTP_TRP.1.2	詳細化：TSFは、リモート管理者が高信頼パス経由の通信を開始できるようにしなければならない。
FTP_TRP.1.3	TSFは、最初の管理者認証及びすべてのリモート管理アクションのために、高信頼パスの使用を要求しなければならない。

適用上の注意：

215 この要件は、許可されたリモート管理者（及びST執筆者が指定する他の役割）が高信頼パス経由でTOEとのすべての通信を開始すること、及びリモート管理者によるTOEとのすべての通信がこのパス経由で実行されることを保証する。この高信頼通信チャネルで渡されるデータは、最初の選択で選ばれたプロトコルに定義されているように暗号化される。ST執筆者は、TOEによってサポートされるメカニズムを選択し、それからその選択に対応する附属書Cの詳細な要件がSTにコピーされることを保証する（まだ存在しない場合）。

保証アクティビティ：

216 評価者は、それらの通信を保護する方法と共にリモートTOE管理方法が示されていることを決定するために、TSSを検査しなければならない。また、評価者は、TOE管理をサポートするためにTSSに記載されているすべてのプロトコルが要件に規定されているプロトコルと一貫しており、STの要件に含まれていることを確認しなければならない。評価者は、サポートされる方法ごとに、リモート管理セッションを確立するための指示が運用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。評価者は、以下のテストも実行しなければならない。

- *テスト1：評価者は、運用ガイダンスに記述されている通りに接続を設定し、通信が成功することを確認して、（運用ガイダンスに）指定されている各リモート管理方法を使用する通信が評価の進行中にテストされることを確認しなければならない。*
- *テスト2：サポートされるリモート管理方法ごとに、評価者は、運用ガイダンスに従って、リモート利用者が高信頼パスを呼び出さずにリモート管理セッションを確立するために使用できるインタフェースがないことを確認しなければならない。*
- *テスト3：評価者は、リモート管理方法ごとに、チャネルデータが平文で送信されないことを確認しなければならない。*
- *テスト4：評価者は、リモート管理方法ごとに、チャネルデータの変更がTOEによって検出されることを確認しなければならない。*

217 さらに特定のプロトコルに保証アクティビティが関連付けられている。

4.2 セキュリティ機能要件の根拠

218 本節では、4.1節で定義されているTOEセキュリティ機能要件の根拠について説明する。表10に、要件によって対策方針が達成される対応する根拠と共にセキュリティ機能要件とセキュリティ対策方針の対応関係を示す。

219 ベンダから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の根拠も含まれている。

- どのSFRがTOEのどのセキュリティ対策方針に対応するかを示す追跡、
- TOEのすべてのセキュリティ対策方針がSFRによって効果的に対処されることを示す1組の正当化（CCパート1、B7節）。

表 10：TOE セキュリティ機能要件に関する根拠

対策方針	対策方針を達成する要件	根拠
O.AUTH_COMM TOEは、利用者がTOEになりすます他のエンティティと通信していないこと、及びTOEが許可されたITエンティティになりすます他のエンティティでなく、許可されたITエンティティと通信していることを保証する手段を提供する。	FCS_IPSEC_EXT.1 [FCS_TLS_EXT.1 FCS_SSH_EXT.1 FCS_HTTPS_EXT.1] FTP_ITC.1 FTP_TRP.1	FTP_ITC.1及びFTP_TRP.1（及びサポートするプロトコル802.11-2007、FCS_IPSEC_EXT.1、FCS_TLS_EXT.1、FCS_SSH_EXT.1、及びFCS_HTTPS_EXT.1）は、TOEがTOEとリモートの管理者及び高信頼ITエンティティの両方との間にこのチャネルを通過するデータを開示または変更から保護する分離された通信チャネルを作成するメカニズムを提供することを要求する。
	FIA_8021X_EXT.1 FIA_UIA_EXT.1 FIA_PSK_EXT.1	FIA_X8021X_EXT.X1は、有線ネットワークへの無線クライアントアクセスを許可するために必要な2ウェイ認証を提供し、無線クライアントとの通信チャネルを確立するために802.11-2007 WPA2プロトコルの一部として機能する。 FIA_UIA_EXT.1は、通信パスの管理者側に保証を提供するために、管理者（リモート管理者を含む）がTOEによって識別され、認証されることを要求する。 FIA_PSK_EXT.1は、TOEが（テキストベースの事前共有鍵用の大きい文字セット、またはTOEの（または市販

		の）RBG機能による生成を通じて）TOEとその通信相手を相互に認証するために使用できる強力な事前共有鍵の形成をサポートすることを要求する。 *適用上の注意：ST執筆者は、TOEによって実装されるプロトコルを反映するために、根拠を変更しなければならない。*
O.CRYPTOGRAPHIC_FUNCTIONS TOEは、TOEの物理的に分離している部分間で送信される、またはTOEの外部に保存されるTSFデータの機密性を維持し、改ざんの検出を可能にするために、暗号機能（暗号化/復号及びデジタル署名操作）を提供する。	FCS_CKM.1(1) FCS_CKM.1(2) FCS_CKM.2(1) FCS_CKM.2(2) FCS_CKM_EXT.4	FCS_CKM.1(1)及びFCS_CKM.1(2)は、それぞれ対称鍵と非対称鍵を生成する。 これらの鍵は、FCS_COP.1(5)に規定されているAES暗号化/復号機能によって使用され、FCS_COP.1(2)に規定されている暗号署名に使用される。 FCS_CKM.2(1)及びFCS_CKM.2(2)は、無線クライアント通信用の暗号鍵配付方法が規格に従って実行され、開示されないことを保証する。 FCS_CKM_EXT.4は、鍵及び鍵関連情報がゼロ化されることを保証する機能を提供する。 これはTOEに常駐する鍵だけでなく、鍵関連情報が現われることがある中間領域（物理的メモリ、ページファイル、メモリダンプなど）にも適用される。
	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	FCS_COP.1(1)は、PPに規定されている様々なプロトコル用の暗号化及び復号操作を実行するためにAESが使用されることを規定する。 FCS_COP.1(2)は、許可されたITエンティティとリモート管理者の識別と認証に関連する高信頼更新及び証明書操作用のデジタル署名機能をTOEに実装することを要求する。 FCS_COP.1(3)及びFCS_COP.1(4)は、TSFがデータ完全性実証と操作データ完全性以外の操作のため

		に、Secure Hash Algorithm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要求する。 FCS_RBG_EXT.1は、鍵関連情報が堅牢に生成されることを保証する。 FIA_X509_EXT.1は、上記の多くの暗号操作をサポートするために使用される証明書が、該当する規格に適合することを要求する。
O.DISPLAY_BANNER TOEは、TOEの使用に関する助言的警告を表示する。	FTA_TAB.1	FTA_TAB.1は、利用者が認証されたセッションを確立できる前に、管理者が定義した見出しをTOEが表示することを要求する。 この見出しは、許可された管理者の完全な制御の下にあり、管理者はTOEの無許可使用に関する警告を指定する。
O.FAIL_SECURE TOEは、電源投入時自己テストの失敗の後では安全な方法で失敗しなければならない。	FPT_FLS.1	FPT_FLS.1は、失敗が検出されたとき、TOEが安全な状態を維持することを要求する。
O.PROTECTED_COMMUNICATIONS TSFは、TSFと他の高信頼ITエンティティ間を移動中のTSFデータを保護しなければならない。	FAU_STG_EXT.1 FCS_IPSEC_EXT.1 [FCS_TLS_EXT.1 FCS_SSH_EXT.1 FCS_HTTPS_EXT.1] FTP_ITC.1 FTP_TRP.1	FAU_STG_EXT.1は、外部監査記憶域間を転送中の監査記録を保護する。 FTP_ITC.1及びFTP_TRP.1（及びサポートするプロトコル802.11-2007、FCS_IPSEC_EXT.1、FCS_TLS_EXT.1、FCS_SSH_EXT.1、及びFCS_HTTPS_EXT.1)は、TOEがTOEとリモートの管理者及び高信頼ITエンティティの両方との間にこのチャネルを通過するデータを開示または変更から保護する分離された通信チャネルを作成するメカニズムを提供することを要求する。
	FIA_8021X_EXT.1 FPT_RPL.1	FIA_X8021X_EXT.X1は、有線ネットワークへの無線クライアントアクセスを許可するために必要な2ウェイ認証を提供し、無線クライアントとの通信チャネルを確立するために802.11-2007 WPA2プロトコルの一部として機能する。

		FPT_RPL.1は、許可されたITエンティティとの間で通信される管理者セッションまたはデータがリプレイできないことを保証する。 *適用上の注意：ST執筆者は、TOEによって実装されるプロトコルを反映するために、根拠を変更しなければならない。*
O.PROTOCOLS TOEは、相互接続性を保証するために、RFC及び/また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。	FCS_IPSEC_EXT.1 [FCS_TLS_EXT.1 FCS_SSH_EXT.1 FCS_HTTPS_EXT.1] FTP_ITC.1 FIA_8021X_EXT.1	FCS_IPSEC_EXT.1、 FCS_TLS_EXT.1、 FCS_SSH_EXT.1、 FCS_HTTPS_EXT.1、 FTP_ITC.1 （802.11-2007に関して）、 及びFIA_8021X_EXT.1 （802.11- 2007のサポートで）は、すべて実装することが要求されるプロトコルに適用可能な規格を参照する（及びそれらの規格に関する制限を示す）。 *適用上の注意：ST執筆者は、TOEによって実装されるプロトコルを反映するために、根拠を変更しなければならない。*
O.REPLAY_DETECTION TOEは、認証データ、他のTSFデータ、及びセキュリティ属性のリプレイを検出し、拒否する手段を提供する。	FPT_RPL.1	FPT_RPL.1は、TOEがリモート利用者からの認証データのリプレイを検出し、拒否することを要求する。
O.RESIDUAL_INFORMATION_CLEARING TOEは、資源が再割当されるとき、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。	FCS_CKM_EXT.4 FDP_RIP.2	FCS_CKM_EXT.4は、不要になったときの暗号鍵の破壊を保証する。 FDP_RIP.2は、データへのアクセスを明示的に許可された制御対象以外の制御対象には資源の内容が使用できないことを保証するために使用される。 このTOEの場合、パケットの内容が以後のパケットで開示されることを防止するために、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を消去する、または何らかのバッファ管理スキームを使用することが重要である

		（例えば、パケットの作成に埋込みが使用される場合、他の利用者のデータまたはTSFデータが含まれてはならない）。
O.RESOURCE_AVAILABILITY TOEは、TOE資源（永続記憶域など）を消耗する利用者の試みを低減するメカニズムを提供しなければならない。	FRU_RSA.1	FRU_RSA.1は、資源を制御し、DoS攻撃を軽減できるように、消耗資源の割当制限を課す。
O.ROBUST_TOE_ACCESS TOEは、管理者のTOEへの論理的なアクセスを制御し、無線クライアントから管理アクセスを制御するメカニズムを提供する。	FIA_AFL.1 FIA_PMG_EXT.1 FIA_UAU_EXT.5 FIA_UAU.6 FIA_UAU.7	FIA_AFL.1は、リモートから操作する無許可ユーザが、許可された管理者が何らかのアクションを取る（例えば、アカウントを再び有効にする）まで、または許可された管理者が定義した時間にわたって、当該アカウントをロックして認証データを推測することで、許可された管理者のアカウントにアクセスすることを防止する設定可能な認証失敗試行閾値を提供する。 FIA_PMG_EXT.1は、強力なパスワード及びパスフレーズを選択し、維持できることを保証するために管理利用者によって使用されるパスワードの属性を定義する。 FIA_UAU_EXT.5は、許可されていない利用者がTOEへの論理的なアクセスを取得できないことを保証するために、TSFがローカル認証方法（その1つはローカルパスワードに基づくメカニズムであることが要求され、他のオプション（潜在的に市販の）メカニズムが許可される）を提供することを要求する。 FIA_UAU.6は、パスワードが変更されたとき、またはセッションがロックされたとき、利用者が再認証されることを要求し、FIA_UAU.7は、認証フィードバックがローカルコンソールで曖昧にされることを保証する。

	FIA_UIA_EXT.1 FMT_SMR.1 FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	FIA_UIA_EXT.1は、TOEが仲介機能を実行する前にすべての利用者が識別され、認証されることを保証して、この対策方針を満たす役割を果たす。 FMT_SMR.1は、無線クライアントから管理アクションを実行する管理者の機能を制御する。この機能は、既定で無効になっていなければならない。 FTA_SSL_EXT.1は、認証された管理者に、放置されたローカル管理セッションがロックされ、TOE資源にアクセスするためにセッションを使用できる前にそのセッションに責任がある管理者が再認証されることを要求する無活動時間を指定する機能を提供する。 FTA_SSL.3は、管理者が定義した無活動リモートセッション時間が終了した後のリモートセッションを考慮する。これには利用者代理セッション及びリモート管理セッションが含まれる。 通常、リモートセッションはローカルセッションに提供されるものと同じ物理的な保護が得られないため、このコンポーネントは特に必要である。 FTA_SSL.4は、セッションが終了するのを待つのでなく、管理セッションを終了またはログオフする機能を管理者に提供する。
O.SESSION_LOCK TOEは、ハイジャックされた無人セッションのリスクを低減するメカニズムを提供しなければならない。	FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	FTA_SSL_EXT.1は、認証された管理者に、放置されたローカル管理セッションがロックされ、TOE資源にアクセスするためにセッションを使用できる前にそのセッションに責任がある管理者が再認証されることを要求する無活動時間を指定する機能を提供する。 FTA_SSL.3は、管理者が定義した無活動リモートセッシ

		ョン時間が終了した後のリモートセッションを考慮する。これには利用者代理セッション及びリモート管理セッションが含まれる。 通常、リモートセッションはローカルセッションに提供されるものと同じ物理的な保護が得られないため、このコンポーネントは特に必要である。 FTA_SSL.4は、セッションが終了するのを待つのでなく、管理セッションを終了またはログオフする機能を管理者に提供する。
O.SYSTEM_MONITORING TOEは、監査データを生成し、それらのデータを外部ITエンティティに送信する機能を提供する。	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1 FAU_STG.1 FAU_STG_EXT.1 FAU_STG_EXT.3 FPT_STM.1	FAU_GEN.1は、TOEが記録できなければならない事象の集合を定義する。 FAU_GEN.2は、監査記録が利用者識別情報を監査対象事象に関連付けることを保証する。 FAU_SEL.1は、管理者が監査証跡に記録する監査対象事象を設定できるようにする。 FAU_STG.1は、一部のローカル監査記憶域を無許可アクセスから保護しなければならないことを要求する。 FAU_STG_EXT.1は、外部監査記憶域間を転送中の監査記録を保護する。 FAU_STG_EXT.3は、外部監査記憶域へのリンクが使用できないときに発生しなければならない事象の集合を定義する。 FPT_STM.1は、TOEが監査記録に使用するための高信頼タイムスタンプを提供できることを要求する。
O.TIME_STAMPS TOEは、高信頼タイムスタンプ及び管理者がこれらのタイムスタンプに使用される時刻を設定する機能を提供しなければならない。	FPT_STM.1	FPT_STM.1は、TOEがそれ自体で使用するための、従って部分的にこの対策方針を満たす高信頼タイムスタンプを提供できることを要求する。 タイムスタンプには日時が含まれ、TOEが常に

		使用できるという意味で高信頼であり、クロックは単調増加でなければならない。
O.TOE_ADMINISTRATION TOEは、管理者のみがログインし、TOEを設定できることを保証するためのメカニズムを提供し、ログインしている管理者の保護を提供する。	FIA_PMG_EXT.1 FIA_UAU.5 FMT_MTD.1(1)-(3) FMT_MOF.1 FMT_SMF.1 FMT_SMR.1 FTP_TRP.1	FIA_PMG_EXT.1は、管理機能及び管理者がパスワード/秘密強度を指定する要件を定義する。 FIA_UAU_EXT.5は、許可されていない利用者がTOEへの論理的なアクセスを取得できないことを保証するために、TSFがローカル認証方法（その1つはローカルパスワードに基づくメカニズムであることが要求され、他のオプション（潜在的に市販の）メカニズムが許可される）を提供することを要求する。 FMT_MTD.1及びFMT_MOF.1は、特定の機能を管理する機能を制限し、許可された管理者のセキュリティ属性を識別する。 FMT_SMF.1は、管理者のみが実行しなければならない管理機能を規定する。 FMT_SMR.1は、管理アクションを実行するために、1つ以上の管理者役割（許可された管理者）を定義する。TSFは、利用者をこの役割に関連付けることができる。 FTP_TRP.1は、TSFがリモート管理用の高信頼パスを提供することを要求する。
O.TSF_SELF_TEST	FPT_FLS.1 FPT_TST_EXT.1	FPT_FLS.1は、失敗が検出されたとき、TOEが安全な状態を維持することを要求する。
TOEは、それが正しく動作していることを保証するために、そのセキュリティ機能の部分集合をテストする機能を提供する。		FPT_TST_EXT.1は、TSFの正しい操作を保証するためにTOEが自己テストスイートを提供することを要求する。

O.VERIFIABLE_UPDATES TOEは、TOEの更新が改ざんされないことを管理者によって（オプションで）信頼される源から検証できることを保証する機能を提供する。	FCS_COP.1(2) FCS_COP.1.(3) FPT_TUD_EXT.1	FCS_COP.1(2)及び FCS_COP.1(3)は、更新の検証に使用されるデジタル署名アルゴリズムとハッシュ関数を規定する。 FPT_TUD_EXT.1は、実行中のファームウェアのバージョンを決定し、更新を開始し、ファームウェア/ソフトウェアがインストール前にTOEに更新されることを検証する方法を提供する。
O.WIRELESS_CLIENT_ACCESS TOEは、TOEとの接続において無線クライアントを制限する機能を提供する。	FTA_TSE.1	FTA_TSE.1は、時刻、位置(例えばIPアドレス)、及びTOEが実装できる他の属性に基づいて無線クライアントによる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

220 3.1 節のTOEに関するセキュリティ対策方針は、2.1節及び2.2節に引用されている組織のセキュリティ方針に識別されている脅威に対応するために作成された。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形式的な具体化である。

221 第4章の序説に示されているように、本節にはCCからの完全なSAR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については4.1節と本節で詳述されている。

222 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文書/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」が提供されている。内容/プレゼンテーション及び評価者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保証アクティビティに対する補足である。

223 表 11に示すTOEセキュリティ保証要件は、本PPの第2章に識別されている脅威と方針に対応するために要求される管理アクティビティと評価アクティビティを識別する。 4.4節は、本PPに関するこのセキュリティ保証要件の集合を選択するための簡潔な正当化を提供する。

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	基本機能仕様
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
テスト	ATE_IND.1	独立テスト - 適合
脆弱性評定	AVA_VAN.1	脆弱性調査
ライフサイクルサポート	ALC_CMC.1	TOEのラベル付け
	ALC_CMS.1	TOE CM範囲

4.3.1 ADV クラス：開発

224 このPPに適合するTOEについては、TOEに関する情報は、最終利用者が使用できるガイダンス文書及びSTのTOE要約仕様（TSS）部分に含まれる。TOE開発者がTSSを執筆することは要求されないが、TOE開発者は、機能要件に関連しているため、TSSに含まれる製品の記述に同意しなければならない。4.1節に含まれる保証アクティビティは、TSS節に適した内容を決定するために十分な情報をST執筆者に提供するはずである。

4.3.1.1 ADV_FSP.1 基本機能仕様

225 機能仕様は、TOEセキュリティ機能インタフェース（TSFI）を記述する。これらのインタフェースの形式的または完全な仕様書を持つことは必要でない。さらに、本PPに適合するTOEは、TOE利用者（管理利用者を含む）によって直接起動されない運用環境とのインタフェースを必ず備えているはずであるから、このようなインタフェースでは間接的なテストしか可能でないため、このようなインタフェースを記述することを規定する意味はほとんどない。本PPでは、このファミリに関するアクティビティは、機能要件に対応してTSSで規定されるインタフェース及びAGD文書に規定されるインタフェースの理解に集中するべきである。規定されている保証アクティビティを満たすために、追加の「機能仕様」書は必要でないはずである。

226 TOEとのインタフェースを理解する上で、対抗すべき脅威が無線接続を通じて有線ネットワークに無許可アクセスしようとする攻撃者であることを考慮することが重要である。認証された利用者のみにアクセスが許可され、暗号化されたトンネルが確立されるような保護を要求する無線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、重要なインタフェースである。無線クライアントインタフェースに加えて、管理インタフェース（TOEを設定する方法）についても記述する必要がある。TOEはリモートとローカル両方のTOEの管理をサポートするため、ローカル及びリモート認証及び設定/保守機能への管理者アクセスを提供するインタフェースを記述しなければならない。

227 TOEが複数コンポーネントTOEである場合には、仮想管理ネットワークを作成するために使用されるインタフェースが記述される。

228 評価する必要があるインタフェースの特徴は、独立した抽象的なリストでなく、リストに記載されている保証アクティビティを実行するために必要な情報を通じて表現される。

開発者アクションエレメント：

ADV_FSP.1.1D 開発者は、機能仕様を提供しなければならない。

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

開発者向け注意事項： 本節の序説で示したように、機能仕様は、STのTSSに提供されている情報と共に、AGD_OPR及びAGD_PRE文書に含まれている情報から構成される。 機能要件内の保証アクティビティは、文書及びTSS節に存在するべきである証拠を指し示す。これらはSFRに直接関連付けられるため、エレメントADV_FSP.1.2Dでの追跡は既に明示的に行われており、追加文書は必要でない。

内容とプレゼンテーションエレメント：

ADV_FSP.1.1C 機能仕様は、SFRが実施し、SFRが支援する各TSFIを使用する目的と方法を記述しなければならない。

ADV_FSP.1.2C 機能仕様書は、SFRが実施し、SFRがサポートする各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 機能仕様書は、SFR非干渉としてのインタフェースの暗黙的な分類に関する根拠を提供しなければならない。

ADV_FSP.1.4C 追跡は、機能仕様書におけるSFRのTSFIへ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、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

ADV_ FSP.1.2E 評価者は、機能仕様が正確で完全なSFRの具体化であることを確認しなければならない。

保証アクティビティ：

229 *このSARに関連する保証アクティビティは特にない。機能仕様書は、4.1節に述べられた評価アクティビティやAGD、ATE、AVA SARに述べられた他のアクティビティをサポートするために提供されている。 機能要件に関する情報の内容についての要件は、実行された他の保証アクティビティを通じて暗黙的に評価されている。インタフェース情報が不十分なために評価者がアクティビティを実行できなければ、適切な機能仕様が提供されていないのである。*

4.3.2 AGD クラス：ガイダンス文書

230 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。ガイダンスは、運用環境（WLANアクセスシステムが常駐するネットワーク）がセキュリティ機能に関する役割を満たすことができることを管理者が検証する方法の記述を含まなければならない。文書は、形式的にならず、管理者にとって読みやすいものであるべきである。

231 ガイダンスは、STで主張されている通り、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。 このガイダンスは、以下を含む。

- その環境においてTOEを正常にインストールするための指示、及び
- 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、TOEのセキュリティを管理するための指示、及び
- ローカル及びリモートにTOEにログインするための指示。

232 特定のセキュリティ機能に関するガイダンスも提供される。このようなガイダンスに関する要件は、4.1節に指定されている保証アクティビティに含まれている。

4.3.2.1 AGD_OPE.1 利用者操作ガイダンス

開発者アクションエレメント：

AGD_OPE.1.1D 開発者は、利用者操作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、評価者がチェックするガイダンスの詳細を確定するために、開発者はこのコンポーネントの保証アクティビティをレビューするべきである。それによって、許容可能なガイダンスの準備に関する必要な情報が提供されるだろう。

内容とプレゼンテーションエレメント：

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

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

AGD_OPE.1.3C 利用者操作ガイダンスは、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、

必要に応じて安全な値を示し、利用者の役割ごとに記述しなければならない。

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

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

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

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

評価者アクションエレメント：

AGD_OPE.1.1E　評価者は、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

保証アクティビティ：

233 *操作中、ガイダンスに記述す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るアクティビティと管理者によって実行されるアクティビティという広範な2つのカテゴリに分類される。管理者以外の利用者に必要な手順は、4.1節の保証アクティビティで参照されていることに注意するべきである。*

234 *管理機能に関しては、そのいくつかが4.1節に記述されているが、次のように追加情報が要求される。*

235 *運用ガイダンスは、少なくともTOEの操作中に評価される構成のTOEで実行され（または実行できるであろう）、ネットワークインタフェース上で受信されたデータを処理できるプロセスを記載しなければならない（おそらく複数のプロセスが存在し、ネットワークインタフェースを「リスン」するプロセスに制限されない）。ネットワークデータを処理するプロセスのみを決定しようとする試みの代わりに、評価される構成のTOEで実行される（または実行できるであろう）すべてのプロセスを記載することは許容される。記載されるプロセスごとに、プロセスの機能、及びサービスを実行する権限の短い記述（1～2行）が管理者ガイダンスに含まれるだろう。「権限」には、ハードウェア権限レベル（例えば、リング0、リング1）、特にプロセスに関連付けられたソフトウェア権限、及びプロセスが実行される利用者役割に関連付けられた権限が含まれる。*

236 *運用ガイダンスには、評価される構成のTOEに付属する暗号エンジンを設定するための指示を含めなければならない。運用ガイダンスは、TOEのCC評価中に他の暗号エンジンの使用は評価されず、テストされなかったことを警告として管理者に提供しなければならない。*

237 *文書は、ハッシュをチェックする、またはデジタル署名を検証するのいずれかによってTOEの更新を検証するためのプロセスを記述しなければならない。評価者は、このプロセスに以下の手順が含まれていることを検証しなければならない。*

1. *ハッシュの場合は、更新のハッシュを入手できる場所の記述。デジタル署名の場合は、証明書所有者から署名付き更新を受け取ったことを確認するために 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指示。これは製品に同梱することも、他の手段で入手することもできる。*
2. *更新を取得するための指示自体。これには、TOEから更新にアクセスできるようにするための指示（特定のディレクトリに配置するなど）も含めるべきである。*
3. *更新プロセスを開始するための指示、及びプロセスの成功または失敗を区別するための指示。これには、ハッシュ/デジタル署名の生成が含まれる。*

4.3.2.2 AGD_PRE.1　準備手続き

開発者アクションエレメント：

AGD_PRE.1.1D　開発者は、準備手続きを含め、TOEを提供しなければならない。

開発者向け注意事項：　操作ガイダンスと同様に、開発者は準備手続きに関して必要となる内容を決定するために、保証アクティビティに関心を向けるべきである。

内容とプレゼンテーションエレメント：

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

AGD_ PRE.1.2C　準備手続きには、TOEの安全な設置、及びSTに記述された運用環境のセキュリティ対策方針に従った運用環境の安全な準備に必要なすべてのステップを記述しなければならない。

評価者アクションエレメント：

AGD_ PRE.1.1E　評価者は、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

AGD_ PRE.1.2E　評価者は、TOEが操作のためにセキュア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。

保証アクティビティ：

238 *上記の序説で説明した通り、特に、TOE機能要件をサポートするために運用環境を設定するとき、文書に関して大きな期待がある。評価者は、TOE用に提供されたガイダンスが適切にST でTOEについて主張されたすべてのプラットフォームとコンポーネント（すなわちハードウェアとオペレーティングシステムの組合せ）に対処していることを確認しなければならない。*

239 *評価者は、次のガイダンスが提供されることを確認しなければならない。*

- *TOEコンポーネント間の制御/設定ネットワークトラフィックが暗号化され、これが適合TOEに許可される唯一の設定であるように、仮想管理ネットワークを設定する方法を詳述する指示及び情報が管理者に提供される。TOEが複数コンポーネントTOE である場合は、附属書Cからの該当する要件をSTに記載し、それらの要件に関連する保証アクティビティがTOEと運用環境の両方に必要なガイダンスの詳細を提供する。*

- *序説に示されているように、TOEの管理は管理者役割によって実行される。ハイレベルでは、ガイダンスは、ローカル及びリモート認証される管理者アクセスを許可するための適切な指示を含んでいなければならない。*

4.3.3 ATE クラス：テスト

240 テストは、機能の観点と共に、設計や実装の弱さを利用する観点について指定される。 前者は、ATE_INDファミリを通して行われ、後者は、AVA_VANファミリを通して行われる。本PPで指定される保証レベルでは、テストは設計情報が利用可能かに依存して、公開されている機能性及びインタフェースに基づく。 評価プロセスの主な出力の1つは、以下の要件に規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

241 テストは、TSS（TOE要約仕様）に記載されている機能性や提供される管理文書（設定や運用も含む）を確認するために実行される。テストの焦点は、一部の追加テストは4.3節でSARとして特定されているが、4.1節に特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。保証アクティビティは、これらのコンポーネントに関する最小テストアクティビティを識別する。評価者は、テスト計画や結果を記載するテスト報告書と、本PPに適合を主張するプラットフォーム/TOEコンビネーションに焦点を当てる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。

内容とプレゼンテーションエレメント：

ATE_IND.1.1C TOEはテストに適していなければならない。

評価者アクションエレメント：

ATE_IND.1.1E 評価者は、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

ATE_IND.1.2E 評価者は、指定された通りにTSF操作を確認するためにTSFのサブセットをテストしなければならない。

保証アクティビティ：

242 評価者は、システムのテスト面を記載したテスト計画と報告書を準備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体に含まれるテストアクションすべてをカバーする。保証アクティビティに載っているテストごとにテストケースが必要ではないが、評価者は該当する各テスト要件がSTでカバーされていることをテスト計画に記載しなければならない。

243 テスト計画はテストされるプラットフォームを特定し、テスト計画にはなくSTに含まれるプラットフォームについては、テスト計画はプラットフォームのテストのためではない正当化の理由を提供する。この正当性は、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を述べなければならず、その違いが実行されるテストに影響しないことを議論しなければならない。その違いによる影響がないと単に断言するのは不十分であり、根拠が提供されなければならない。もしSTに主張されたすべてのプラットフォームがテストされるのであれば、根拠は必要ない。

244 *テスト計画は、テストされる各プラットフォームの構成を記述し、AGD文書に含まれるもの以外にも必要となるセットアップについても記述する。注意すべきことは、評価者は各プラットフォームの実装とセットアップについて、テストの一部か標準プレテスト条件として、AGD文書に従うことが期待されている。これは、特別なテストドライバやツールを含むかもしれない。各ドライバやツールに関して、ドライバやツールがTOEやプラットフォームの機能のパフォーマンスに悪影響を与えないよう論証（単なる主張ではなく）が提供されるべきである。*

245 テスト計画は、ハイレベルのテスト目標とこの目標を達成するために従うテスト手順を特定する。*これらの手順は、期待される結果を含む。テスト報告書（単なるテスト計画の注釈付きのバージョンかもしれないが）は、テスト手順が実行された際のアクティビティを詳述し、テストの実際の結果を含む。これは累積的計算であるべきであり、テストの実行が不合格に終わった場合は、修正をインストールし、テストを正しく再実行し、報告書には、単なる「合格」の結果だけでなく、「不合格」と「合格」の結果（論点を補強する例証）を示さなければならない。*

4.3.4 AVA クラス：脆弱性評定

246 本PPの第一世代（初版）のために、評価機関は、これらの製品のタイプに見つかった脆弱性を見つけるため、オープンソースを調査することが求められる。ほとんどの場合、これらの脆弱性は、基本的な攻撃以上の複雑さを必要とする。侵入ツールが作られ評価機関に一様に配付されるまで、評価者はTOEのそれらの脆弱性をテストすることは求められない。評価機関は、ベンダから提供された文書に載っているこれらの脆弱性の可能性についてコメントすることが求められている。この情報は、侵入テストツールの開発や将来のPPの開発のために使われるだろう。

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、テストのためにTOEを提供しなければならない。

内容とプレゼンテーションエレメント：

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、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

AVA_VAN.1.2E 評価者は、TOEの潜在的な脆弱性を特定するために公開情報の探索を実施しなければならない。

AVA_VAN.1.3E 評価者は、特定された潜在的な脆弱性に基づいて、TOEが基本的な攻撃能力を持つ攻撃者による攻撃に抵抗することを決定するために、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：

247 *ATE_INDと同様に、評価者はこの要件に関して、所見を記載するために報告書を作らなければならない。この報告書は、物理的に、ATE_INDに述べている全体的なテスト報告書の一部*

でも別文書でもよい。評価者は、WLANアクセスシステム製品全般で見つかった脆弱性や特定のTOEに関連する脆弱性を決定するために公開情報を検索しなければならない。評価者は、参考にした情報源と見つかった脆弱性を報告書に記載する。見つかった各脆弱性について、評価者は脆弱性を確認するために、適切であれば、不適用性に関連する根拠を提供するか、(ATE_INDで提供されるガイドラインを使って）テストを策定する。適合性は、脆弱性を利用するために必要とされる攻撃のベクトルを査定することにより決まる。例えば、もし脆弱性がブートアップ時に鍵の組合せを押すことによって検知されたら、本PPの保証レベルのテストが適しているであろう。脆弱性の悪用に、例えば、電子顕微鏡とタンク一杯の液体ニトロジェンが必要となるならば、テストは適しておらず、適切な正当化が策定されるべきである。

4.3.5 ALC クラス：ライフサイクルサポート

248 本PPに適合するTOEに提供される保証レベルに関して、ライフサイクルサポートは、TOEベンダの開発、構成管理プロセスの調査よりも、最終利用者に見えるライフサイクルの側面に限定される。これは、製品の全体的な信頼に貢献するために開発者が実践する重要な役割を軽減するということではなく、むしろ、この保証レベルでの評価に利用される情報の反映である。

4.3.5.1 ALC_CMC.1 TOE のラベル付け

249 このコンポーネントは、TOEを特定することを対象としており、これを使うことによって、最終利用者が購入した際に同じベンダの他の製品やバージョンと区別することができ、容易に特定できる。

開発者アクションエレメント：

ALC_CMC.1.1D 開発者は、TOEとTOEの参照を提供しなければならない。

内容とプレゼンテーションエレメント：

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

評価者アクションエレメント：

ALC_CMC.2.1E 評価者は、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

保証アクティビティ：

250 評価者は、STの要件を満たすバージョンを明確に特定する識別子（製品の名前、バージョン番号等）をSTが含んでいることを確認するために、STをチェックしなければならない。さらに、評価者は、STに載っているバージョン番号と一致していることを確認するために、AGDガイダンスとテスト用に受け取ったTOEサンプルをチェックしなければならない。ベンダがTOEを宣伝するWebサイトを維持している場合は、STの情報が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、評価者はWebサイトの情報を調査しなければならない。

4.3.5.2 ALC_CMS.1 TOE CM カバレージ

251 TOEの範囲と関連する評価証拠要件をもってすると、このコンポーネントの保証アクティビティは、ALC_CMC.1 に載っている保証アクティビティでカバーされる。

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。

内容とプレゼンテーションエレメント：

ALC_CMS.2.1C　構成リストは、TOE自体、及びSARが要求する評価証拠を含まなければならない。

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

評価者アクションエレメント：

ALC_CMS.2.1E　評価者は、提供された情報が証拠の内容とプレゼンテーションに対するすべての要件を満たすことを確認しなければならない。

保証アクティビティ：

252 *本PPの「SARが要求する評価証拠」とは、AGD要件のもとで管理者や利用者に提供されるガイダンスに加え、STの情報に限定される。TOEが明確に識別され、この識別がSTやAGDガイダンス（ALC_CMC.1 の保証アクティビティになされているように）と一致していることを確認することによって、評価者は暗黙的にこのコンポーネントが必要とする情報を確認する。*

4.4 セキュリティ保証要件の根拠

253 これらのセキュリティ保証要件を選択するための根拠は、これがこの技術に関する米国政府の最初のプロテクションプロファイルであることである。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で脆弱性が見つかった場合は、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だろう。

附属書 A：サポート表と参考文献

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[18] WPA2 Standard

略語

AES	Advanced Encryption Standard（高度暗号規格）
AF	Authorization factor（認証要素）
AS	Authorization subsystem（許可サブシステム）
CAVS	Cryptographic Algorithm Validation System（暗号アルゴリズム検証システム）
CC	Common Criteria（コモンクライテリア）
CCTL	Common Criteria Testing Laboratory（コモンクライテリア評価機関）
CM	Configuration management（構成管理）
COTS	Commercial Off-The-Shelf（民生品）
CMVP	Cryptomodule Validation Program（暗号モジュール検証プログラム）
DRBG	Deterministic Random Bit Generator（決定性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）
SFR	Security Functional Requirement（セキュリティ機能要件）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security 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 SP 800-53/CNSS 1253の管理策のいくつかは、適合TOEによって完全または部分的に対処される。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）を認定担当者が決定するために利用できる。

適用上の注意：このバージョンは、簡単なマッピングのみを提供する。この追加情報は、TOEによって提供される適合の程度（例えば、完全に管理策を満たす、部分的に管理策を満たす）について議論している管理策マッピングに対するSFRについての詳細を含むだろう。さらに、適合が決定された方法に関する情報（文書レビュー、ベンダ主張、テスト/検証の程度）を認定チームに提供するために、規定された保証アクティビティ及びSARを満たす一環として行われる評価アクティビティの総合的なレビューが要約されるだろう。この情報は、規定された管理策の適合の程度を決定するために、実行する必要がある追加アクティビティ（存在する場合）を認定チームに示すだろう。

STは選択の範囲までは選択できるので、割付を記入して、STが完成し評価されるまでは必ずしも最終的なストーリーは出来上がらない。したがって、この情報はPPに対する追加としてSTに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によって実行されるアクティビティに対するいくつかの必要な解釈（例えば、「修正」等）があるかもしれない。スキームは監督担当（例えば検証者）がこの種の情報を与えることができるか、または保証アクティビティの一部として評価者によって実施されるかもしれない。検証アクティビティは提供されなければならない重要な部分の情報であり、評価チームの作業に追加して行う必要があることがある場合、認定チームがそれを決定できるように提供されなければならない。

識別子	名称	適用可能なSFR
AC-3	アクセス制御の実施	FMT_MOF.1、 FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1
AC-6	特権の最小化	FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3)
AC-7	ログイン試行の失敗	FIA_AFL.1
AC-8	システムの利用に関する通知	FTA_TAB.1
AC-11	セッションのロック	FIA_UAU.6, FTA_SSL_EXT.1
AC-14	識別または認証なしで許可される活動	FIA_UIA_EXT.1
AC-17(7)	リモートアクセス	FCS_SSH_EXT.1
AU-2	監査対象事象	FAU_GEN.1
AU-2(4)		FAU_GEN.1
AU-3	監査記録の内容	FAU_GEN.1, FAU_GEN.2
AU-3(1)		FAU_GEN.1
AU-5	監査処理の不具合に対する対応	FAU_STG_EXT.3
AU-7	監査両の低減と報告書の作成	FAU_SEL.1
AU-8	タイムスタンプ	FPT_STM.1
AU-9	監査情報の保護	FAU_STG.1, FAU_STG_EXT.1
AU-10	否認防止	FCS_COP.1(2)

AU-12	監査生成	FAU_GEN.1
CM-5	変更のためのアクセス制限	FPT_TUD_EXT.1
IA-2	ユーザ識別及び認証	FIA_UIA_EXT.1, FIA_UAU_EXT.5, FPT_RPL.1
IA-3	デバイスの識別及び認証	FIA_8021X_EXT.1, FTP_ITC
IA-5	認証コードの管理	FIA_PMG_EXT.1, FIA_PSK_EXT.1, FIA_X509_EXT.1
IA-6	認証コードのフィードバック	FIA_UAU.7
SC-4	残存情報	FDP_RIP.2
SC-6	リソースの優先度	FRU_RSA.1
SC-8	伝送する情報の完全性	FCS_IPSEC_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FTP_ITC.1
SC-9	伝送する情報の機密性	FCS_IPSEC_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FCS_SSH_EXT.1, FTP_ITC.1
SC-10	ネットワークの切断	FTA_SSL.3
SC-11	高信頼パス	FTP_TRP.1
SC-12	暗号鍵の確立と管理	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM_EXT.4
SC-13	暗号化の利用	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_FLS.1, FPT_TST_EXT.1

附属書 C：追加要件

254 *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、追加コンポーネントを含んでいる。このサポート情報は、最初のレビューサイクルに沿って開発され、次回のPPの公開に組み込まれる予定である。本節に含まれる情報（含まれる要件が潜在的な適合TOEに適用可能かどうか、またこの附属書に含まれていないがWLANアクセスシステム製品に広く適用可能な要件）に関するコメントを歓迎すると共に、ぜひお願いしたい。*

255 本PPの序説に示したように、本PPに適合し、TOEが実装できるいくつかの機能がある。これらの機能は、IT環境に依存することになるため必須ではない（例えばTOEの管理者の識別及び認証）。ただし、TOEがこのような機能を実装する場合、ST執筆者は次の情報を取得してSTに記載する。この附属書に含まれない要件をSTに含めることはできるが、本PPへの適合を主張する前に、評価を監督する国の認証機関（スキーム）によるレビューと容認に支配される。

C.1 セキュリティ監査クラス（FAU）

256 監査レビュー及び/または保存がTOEによってサポートされる場合は、必要に応じてSTに以下の監査要件を記載しなければならない。

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

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き、**監査証跡内の**監査記録へのすべての利用者読取りアクセスを禁止しなければならない。
FAU_STG_EXT.4	**監査データ消失の防止**
FAU_STG_EXT.4.1	TSFは、許可された管理者に、以下の1つまたは複数のアクションを選択する機能を提供しなければならない。 a) 許可された管理者が行う事象を除き、監査対象事象を防止する、及び b) 監査証跡が一杯の場合、保存されている最も古い監査記録を上書きする。

適用上の注意：

257 *TOEは、許可された管理者に、監査対象事象の発生を防止して監査データの消失を防止するオプションを提供する。このような状況で許可された管理者のアクションを監査することは要求されない。また、TOEは、許可された管理者に、「古い」監査記録を上書きするオ*

プションを提供する。これにより、サービス妨害（DoS）攻撃から保護できる。

C.2 暗号サポートクラス（FCS）

拡張：HTTPS（FCS_HTTPS_EXT）

サポートされるプロトコルとしてHTTPSが選択される場合は、この要件をSTに含めなければならない。

FCS_HTTPS_EXT.1	**拡張：HTTPセキュリティ（HTTPS）**
FCS_HTTPS_EXT.1.1	TSFは、RFC 2818に適合するHTTPSプロトコルを実装しなければならない。
FCS_HTTPS_EXT.1.2	TSFは、FCS_TLS_EXT.1に規定されているようにTLSを使用してHTTPSを実装しなければならない。

適用上の注意：

258 *ST執筆者は、実装が識別された規格に適合していることを決定するために十分な詳細を提供しなければならない。これは、このコンポーネントにエレメントを追加する、またはTSSの追加の詳細を通じて行うことができる。*

保証アクティビティ：

259 *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_HTTPS_EXT.1エレメントについて記載されている該当する各RFCの節ごとに、「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）、及び「SHOULD NOT」（するべきでない）など）すべての文について、TOEがこのようなオプションを実装する場合は、それをTSSに記述しなければならない。含まれる機能が規格に「SHOULD NOT」（するべきでない）または「MUST NOT」（してはならない）と示されている場合、TSSは、TOEによって実装されたセキュリティ方針に悪影響しない根拠を提供しなければならない。*
- *各RFCの節ごとに、「MUST」（しなければならない）または「SHOULD」（するべきである）文に関連する機能の省略を記述しなければならない。*
- *TOEが施行する予定のセキュリティ要件に影響するかもしれないTOE固有の拡張、規格に含まれない処理、または規格によって許可される代替実装を記述しなければならない。*

260 *FCS_HTTPS_EXT.1.2 - 評価者は、TLSプロトコルによって要求されるクライアント認証と処理スタックの別のレベルで実行できる管理者認証の比較に焦点を当てて、HTTPSがTLSを使用して管理セッションを確立する方法が明記されていることを確認するために、TSSをチェックしなければならない。このアクティビティに関するテストは、TLSテストの一環として実施される。そのため、TLSテストがTLSプロトコルレベルで実行される場合、追加テストが必要になる場合がある。*

拡張：Secure Shell（FCS_SSH_EXT）

サポートされるプロトコルとしてSSHが選択される場合は、この要件をSTに含めなければならない。

FCS_SSH_EXT.1	**拡張：Secure Shell （SSH）**
FCS_SSH_EXT.1.1	TSFは、RFC 4251、4252、4253、及び4254に適合するSSHプロトコルを実装しなければならない。
FCS_SSH_EXT.1.2	TSFは、その鍵を使用して2^{28}以下のパケットが送信された後で、SSH接続に鍵が再入力されることを保証しなければならない。
FCS_SSH_EXT.1.3	TSFは、SSHプロトコルが[割付：タイムアウト時間]のRFC 4252に定義されているように認証のタイムアウト時間を実装し、クライアントが単一のセッションで実行できる認証失敗試行回数を[割付：最大試行回数]に制限していることを保証しなければならない。
FCS_SSH_EXT.1.4	TSFは、SSHプロトコル実装がRFC 4252に記述されているように以下の認証方法をサポートしていることを保証しなければならない：公開鍵ベース、パスワードベース。
FCS_SSH_EXT.1.5	TSFは、RFC 4253に記述されているように、SSHトランスポート接続内の[割付：バイト数]バイトより大きいパケットが削除されることを保証しなければならない。
FCS_SSH_EXT.1.6	TSFは、SSHトランスポート実装が以下の暗号化アルゴリズムを使用することを保証しなければならない：AES-CBC-128、AES-CBC-256-CBC、[割付：AEAD_AES_128_GCM、AEAD_AES_256_GCM、他の暗号化アルゴリズムなし]。
FCS_SSH_EXT.1.7	TSFは、SSHトランスポート実装が、その公開鍵アルゴリズムとしてSSH_RSA及び[選択：PGP-SIGN-RSA、PGP-SIGN-DSS、他の公開鍵アルゴリズムなし]を使用することを保証しなければならない。
FCS_SSH_EXT.1.8	TSFは、SSHトランスポート接続に使用されるデータ完全性アルゴリズムはhmac-sha1及び[選択：他のアルゴリズムなし、hmac-sha1-96、hmac-md5、hmac-md5-96]であることを保証しなければならない。
FCS_SSH_EXT.1.9	TSFは、diffie-hellman-group14-sha1がSSHプロトコル用に使用される唯一許可された鍵交換方法であることを保証しなければならない。

適用上の注意：

261 *FCS_SSH_EXT.1.1 - ST執筆者は、実装が識別された規格に適合していることを決定するために十分な詳細を提供しなければならない。これは、このコンポーネントにエレメントを追加する、またはTSSの追加の詳細を通じて行うことができる。*

262 *FCS_SSH_EXT.1.3 – 最初の割付では、ST執筆者は、認証セッションの開始から認証が失敗してセッションがタイムアウトするまでのタイムアウト時間（例えば「10分」）を挿入するべきである。 2番目の割付では、最大認証失敗試行回数を指定する。RFCには、サーバはこの失敗試行回数の後でセッションを落とすべきであると記載されている。*

263 *FCS_SSH_EXT.1.5 - RFC 4253は、パケットは「妥当な長さ」であるべきであり、そうでなけ*

れば削除されるという但書付きで「大きいパケット」の受入れを規定している。ST執筆者は、受け入れられる最大パケットサイズを割付に入れ、TOEでの「妥当な長さ」を定義するべきである。

264 *FCS_SSH_EXT.1.6 - 本PPの以後の刊行では、AES-GCMが必須になり、CBCがオプションになる可能性がある。 割付で、ST執筆者は、AES-GCMアルゴリズムを選択できる。AES-GCMがサポートされない場合は、「他のアルゴリズムなし」を選択できる。AES-GCMが選択される場合は、対応するFCS_COP項目がSTに存在するべきである。*

265 *FCS_SSH_EXT.1.7 - RFC 4253は、許可された必須の公開鍵アルゴリズムを規定する。この要件は、SSH-RSAを「必須」とし、他の2つの公開鍵アルゴリズムをSTに主張できるようにする。ST執筆者は、適切な選択を行い、SSH_RSAのみが実装される場合は「他の公開鍵アルゴリズムなし」を選択するべきである。*

266 *FCS_SSH_EXT.1.8 - RFCに従ってHMAC-SHA1が要求されるが、追加の完全性アルゴリズムも許可される。ST執筆者は、TOEに実装されるアルゴリズムを選択する。追加のアルゴリズムがない場合は、そのように選択するべきである。*

保証アクティビティ：

267 *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_SSH_EXT.1エレメントについて記載されている該当する各RFCの節ごとに、「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）、及び「SHOULD NOT」（するべきでない）など）すべての文について、TOEがこのようなオプションを実装する場合は、それをTSSに記述しなければならない。 含まれる機能が規格に「SHOULD NOT」（するべきでない）または「MUST NOT」（してはならない）と示されている場合、TSSは、TOEによって実装されたセキュリティ方針に悪影響しない根拠を提供しなければならない。*
- *各RFCの節ごとに、「MUST」（しなければならない）または「SHOULD」（するべきである）文に関連する機能の省略を記述しなければならない。*
- *TOEが施行する予定のセキュリティ要件に影響するかもしれないTOE固有の拡張、規格に含まれない処理、または規格によって許可される代替実装を記述しなければならない。*

268 *FCS_SSH_EXT.1.2 - 評価者は、ある鍵を使用して2^{28}を超えるパケットが送信される前にTOEがSSH接続に鍵を再入力することを確認するために、TSSを検査しなければならない。この効果がTOEの設定によって達成される場合、評価者は、適切な値を設定するための指示が含まれていることを確認するために、運用ガイダンスを検査しなければならない。*

269 *FCS_SSH_EXT.1.3 - 評価者は、タイムアウト時間及び要件に規定されている認証失敗試行回数の後でセッション接続を切断する方法がTSSに指定されていることを確認しなければならない。これらの値が設定可能であり、管理者が指定できる場合、評価者は、これらの値を設定するための指示が含まれていることを確認するために、運用ガイダンスをチェックしなければならない。評価者は、以下のテストも実行しなければならない。*

- *テスト1：評価者は、TOEへの認証がタイムアウト時間を超えた場合、現在のセッションが切断され、接続するために新しいセッションを開始する必要があることを実証しなければならない。タイムアウト時間が設定可能である場合、評価者は、メカニズムが規定通りに動作することを確認するために、運用ガイダンスに従っ*

て2つ以上の異なるタイムアウト時間を実装できることを確認しなければならない。

- *テスト2：評価者は、要件に規定されている回数のSSH認証失敗により現在のセッションが切断され、接続するために新しいセッションを開始する必要があることを実証しなければならない。回数が設定可能である場合、評価者は、メカニズムが規定通りに動作することを確認するために、運用ガイダンスに従って2つ以上の異なる試行回数（例えば3回、5回）を実装できることを確認しなければならない。*

270 *FCS_SSH_EXT.1.4 - 評価者は、認証に使用することが許可されている公開鍵アルゴリズムの記述がTSSに含まれていることを確認し、このリストがFCS_SSH_EXT.1.7に適合し、パスワードベースの認証方法も許可されていることを確認しなければならない。評価者は、以下のテストも実行しなければならない。*

- *テスト1：評価者は、サポートされる公開鍵アルゴリズムごとに、TOEが利用者接続を認証するために公開鍵アルゴリズムの使用をサポートしていることを示さなければならない。このテストを実行するために必要な設定アクティビティは、運用ガイダンスの指示に従って実行しなければならない。*
- *テスト2：評価者は、運用ガイダンスを使用して、TOEがパスワードベースの認証を受け付けるように設定し、認証者としてパスワードを使用してSSH経由で利用者を正常にTOEに認証できることを実証しなければならない。*

271 *FCS_SSH_EXT.1.5 - 評価者は、RFC 4253に規定されている「大きいパケット」を検出し、処理する方法が TSSに記述されていることをチェックしなければならない。評価者は、次のテストも実行しなければならない。*

- *テスト1：評価者は、TOE がこのコンポーネントに規定されているサイズより大きいパケットを受信した場合、パケットが削除されることを実証しなければならない。*

272 *FCS_SSH_EXT.1.6 - 評価者は、TSSのこのプロトコルの実装の記述をチェックして、オプションの特性が指定され、サポートされている暗号化アルゴリズムも指定されていることを確認しなければならない。評価者は、TSSをチェックして、指定された暗号化アルゴリズムがこのコンポーネント用に記載されている暗号化アルゴリズムと同じであることを確認しなければならない。また、評価者は、運用ガイダンスをチェックして、SSHがTSSの記述に適合する（例えば、要件に適合するためにTOEによって宣伝されるアルゴリズムの集合を制限する）ようにTOEを設定するための指示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、次のテストも実行しなければならない。*

- *テスト1：評価者は、要件によって規定されている各暗号化アルゴリズムを使用して、SSH 接続を確立しなければならない。プロトコルの正常な交渉によりテストの意図が満たされることを（有線側で）観察すれば十分である。*

273 *FCS_SSH_EXT.1.7 - FCS_SSH_EXT.1.4に関連付けられた保証アクティビティがこの要件を検証する。*

274 *FCS_SSH_EXT.1.8 - 評価者は、TSSをチェックして、サポートされるデータ完全性アルゴリズムが記載され、そのリストがこのコンポーネントのリストと一致することを確認しなければならない。また、評価者は、運用ガイダンスをチェックして、管理者がTOEとのSSH接続に許可されたデータ完全性アルゴリズムのみが使用されていること（特にMAC「以外の」アルゴリズムが許可されていないこと）を確認する方法に関する指示が含まれていること*

を確認しなければならない。

275 *FCS_SSH_EXT.1.9 - 評価者は、許可された管理者がDH Group 14を使用してSSH用のすべての鍵交換が実行されるようにTOEを設定できる構成情報が運用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。*この機能がTOEに「ハードコード」される場合、評価者は、TSSをチェックして、これがSSHプロトコルの議論に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、次のテストも実行しなければならない。*

- *テスト1：評価者は、diffie-hellman-group1-sha1 鍵交換を実行し、試行が失敗することを観察しなければならない。次に、評価者は、diffie- hellman-group14-sha1 鍵交換を実行し、試行が成功することを観察しなければならない。*

拡張：Transport Layer Security（FCS_TLS_EXT）

サポートされるプロトコルとしてTLSが選択される場合は、この要件をSTに含めなければならない。

FCS_TLS_EXT.1	**拡張：Transport Layer Security（TLS）**
FCS_TLS_EXT.1.1	TSFは、以下のサイファスイートをサポートする次のプロトコルの中から、1つまたは複数のプロトコルを実装しなければならない：[選択：TLS 1.0 （RFC 2346）、TLS 1.1 （RFC 4346）、TLS 1.2 （RFC 5246）]。 **必須のサイファスイート：** 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 **オプションのサイファスイート：** 選択：なし TLS_RSA_WITH_AES_128_CBC_SHA256 *TLS_RSA_WITH_AES_256_CBC_ SHA256* *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256* *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256* *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256* *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384* *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256* *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*].

適用上の注意：

276 *ST執筆者は、TLS実装を反映するように、適切な選択と割付を行わなければならない。ST執筆者は、実装が識別された規格に適合していることを決定するために十分な詳細を提供しなければならない。これは、このコンポーネントにエレメントを追加する、またはTSSの追加の詳細を通じて行うことができる。*

277 *評価される設定に使用されるサイファスイートは、この要件によって制限される。ST執筆者は、サポートされるオプションのサイファスイートを選択するべきである。必須スイート以外のサイファスイートがサポートされない場合は、「なし」を選択するべきである。実装によって交渉されるスイートをこの要件のスイートに制限するために管理手順を実行する必要がある場合は、AGD_OPEによって規定されている適切な指示をガイダンスに含め*

る必要がある。

278 *上記のSuite Bアルゴリズム（RFC 5430）が実装に望ましいアルゴリズムである。本PPの将来の刊行では、TLS 1.2 （RFC 5246）のサポートが要求される予定である。さらに、本PPの将来の刊行では、規定されている旧バージョンのSSL/TLSプロトコルを使用するすべての接続試行を拒否する手段をTOEが提供することが要求される。*

保証アクティビティ：

279 *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_TLS_EXT.1エレメントについて記載されている該当する各RFCの節ごとに、「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）、及び「SHOULD NOT」（するべきでない）など）すべての文について、TOEがこのようなオプションを実装する場合は、それをTSSに記述しなければならない。 含まれる機能が規格に「SHOULD NOT」（するべきでない）または「MUST NOT」（してはならない）と示されている場合、TSSは、TOEによって実装されたセキュリティ方針に悪影響しない根拠を提供しなければならない。*
- *各RFCの節ごとに、「MUST」（しなければならない）または「SHOULD」（するべきである）文に関連する機能の省略を記述しなければならない。*
- *TOEが施行する予定のセキュリティ要件に影響するかもしれないTOE固有の拡張、規格に含まれない処理、または規格によって許可される代替実装を記述しなければならない。*

280 *評価者は、TSSをチェックして、指定されたサイファスイートがこのコンポーネント用に記載されている暗号化アルゴリズムと同じであることを確認しなければならない。また、評価者は、運用ガイダンスをチェックして、TLSがTSSの記述に適合する（例えば、要件に適合するためにTOEによって宣伝されるサイファスイートの集合を制限する）ようにTOEを設定するための指示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、次のテストも実行しなければならない。*

- *テスト1：評価者は、要件によって規定されている各サイファスイートを使用して、TLS 接続を確立しなければならない。 この接続は、上位プロトコルの確立の一環として、例えばHTTPS セッションの一環として確立できる。 サイファスイートの正常な交渉によりテストの意図が満たされることを（有線側で）観察すれば十分である。 使用されているサイファスイートを区別する（例えば、暗号アルゴリズムは128 ビットAES であり、256 ビットAES でない）ために、暗号化されたトラフィックの特性を検査する必要はない。*

C.3 TSF保護クラス（FPT）

281 TOEが物理的に複数のコンポーネントに分散されている場合は、それらのコンポーネント間の通信を保護しなければならない。これは、許可されたITエンティティとの通信と同じ方法で実行するべきである。

FPT_ITT.1	**基本的内部TSFデータ転送保護**
FPT_ITT.1.1(1)	**詳細化：**TSFは、TSFデータがTOEの個別の部分間で送信されるとき、**[選択、1つ以上を選択：IPsec、SSH、TLS、TLS/HTTPS]の使用を通じて**、TSFデータを開示と***変更から保護***しなければならな

い。

適用上の注意：

282 *この要件は、分散された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使用を通じて保護されることを保証する。この高信頼通信チャネルで渡されるデータは、最初の選択で選択されたプロトコルに定義されているようには暗号化される。ST執筆者は、TOEによってサポートされるメカニズムを選択し、それからその選択に対応する附属書Cの詳細な要件がSTにコピーされることを保証する（まだ存在しない場合）。*

保証アクティビティ：

283 *評価者は、分散されたTOEコンポーネントを保護するための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に、TSSを検査しなければならない。また、評価者は、TOE管理をサポートするためにTSSに記載されているすべてのプロトコルが要件に規定されているプロトコルと一貫しており、STの要件に含まれていることを確認しなければならない。評価者は、サポートされる方法ごとに、通信パスを確立するための指示が運用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。評価者は、以下のテストも実行しなければならない。*

- *テスト1：評価者は、運用ガイダンスに記述されている通りに接続を設定し、通信が成功することを確認して、（運用ガイダンスに）指定されている各通信方法を使用する通信が評価の進行中にテストされることを確認しなければならない。*
- *テスト2：評価者は、通信方法ごとに、チャネルデータが平文で送信されないことを確認しなければならない。*
- *テスト3：評価者は、通信方法ごとに、チャネルデータの変更がTOEによって検出されることを確認しなければならない。*

284 *さらに特定のプロトコルに保証アクティビティが関連付けられている。*

C.4 監査要件

ST執筆者がこの附属書から選択する具体的な要件に基づいて、ST執筆者は、選択した要件に対応する適切な監査対象事象をSTの表に含めるべきである。

要件	監査対象事象	追加の監査記録内容
FCS_TLS_EXT.1	プロトコルの失敗。 TLSセッションの確立/終了。	失敗の理由。 成功と失敗両方の接続のTOE以外のエンドポイント（IPアドレス）。
FCS_SSH_EXT.1	プロトコルの失敗。 SSHセッションの確立/終了。	失敗の理由。 成功と失敗両方の接続のTOE以外のエンドポイント（IPアドレス）。
FCS_HTTPS_EXT.1	プロトコルの失敗。 HTTPSセッションの確立/終了。	失敗の理由。 成功と失敗両方の接続のTOE以外のエンドポイント（IPアドレス）。
FPT_ITT.1	なし。	

附属書 D：本書の表記規則

285 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。ここでは、PP読者の役に立つように一部を抜粋して示す。

286 本PPで使用される表記、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C.4に定義されている。 これらの各操作は本PPで使用される。

詳細化表記規則

287 **詳細化**操作は、要件に詳細を追加し、さらに要件を制限するために使用される。セキュリティ要件の詳細化は、太字の要件内のエレメント番号と追加テキストの後の**太字**の「 詳細化」という語句によって示される。

選択表記規則

288 **選択**操作は、要件の記載中のCCによって提供される1つまたは複数のオプションを選択するために使用される（CC 3.1パート1の附属書C.4.3を参照）。 PP執筆者によって行われた選択は、**太字**で選択を示し、括弧及び「選択」という語句は削除される。 ST執筆者によって埋められるべき選択は、[選択：]として角括弧内に示され、選択が行われるべきことを示す。

割付表記規則

289 **割付**操作は、パスワードの長さのように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に使用される（CC 3.1パート1の附属書 C.4.2を参照）。**太字**で示される値はPP執筆者によって行われた割付を示し、括弧及び「割付」という語句は削除される。ST執筆者によって埋められるべき割付は、[割付：]として角括弧内に示され、割付が行われるべきことを示す。

繰返し表記規則

290 **繰返し**操作は、コンポーネントが様々な操作で置換されるときに使用される（CC 3.1パート1の附属書 C.4.1を参照）。繰返し回数（iteration_number）は、コンポーネント識別子の後に括弧内に示される。

291 繰返し操作は、すべてのコンポーネントに対して実行できる。PP/ST執筆者は、同じコンポーネントに基づいて複数を要件を含めることで繰返し操作を実行する。コンポーネントの繰返しは、それぞれそのコンポーネントの他のすべての繰返しと異なっていなければならない。それには、別の方法で割付と選択を行うか、別の方法で詳細化を適用する。

拡張要件表記規則

292 執筆者のニーズを満たすのに適した要件がCCにない場合、拡張要件を使用できる。 **拡張要件**は識別されなければならず、要件を明確にする上でCCクラス/ファミリ/コンポーネントモデルを使用することが要求される。拡張要件は、コンポーネント内の「EXT」の挿入で示される。

適用上の注意

293 適用上の注意には、適合するTOE用のセキュリティターゲットの構築に関連するまたは役に立つと見なされる追加の補足情報及び開発者、評価者、及びISSEに対する一般的な情報が含まれる。また、適用上の注意には、コンポーネントの許可された操作に関する助言も含まれる。

保証アクティビティ：

294 保証アクティビティは、脅威を低減するためにTOEに課される機能要件に関する共通評価方法として機能する。アクティビティには、評価者がTSSの記載に従ってTOEの特定の側面を分析するための指示が含まれる。したがってST執筆者には、この情報をTSS節に記載する暗黙的要件が課される。これらのアクティビティは、本バージョンのPPでは機能コンポーネントと保証コンポーネントに直接関連しているが、将来のバージョンではこれらの要件が別の附属書または文書に移動される可能性がある。

附属書 E：用語

アクセスポイント（access point） - 無線クライアントが有線ネットワークにアクセスできるようにするネットワークインタフェースを提供する。 APは、有線インフラストラクチャ上の高信頼ノードとして認証されると、無線クライアントとAPのRFインタフェース間の無線ネットワーク上の暗号化サービスを提供する。

管理者（administrator） - TOEを設定する管理者権限を持つ利用者。

認証サーバ（authentication server） - 認証のために無線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（authentication credential） - 利用者または管理者がTOEまたはネットワークにアクセスすることを許可されていることを確認するためにシステムが使用する情報。 クレデンシャルは、利用者名とパスワードのように単純なものから、より強力なものまである。

重大なセキュリティパラメタ（CSP：Critical Security Parameter） - 開示や改ざんにより暗号化モジュールのセキュリティが無効になるセキュリティ関連情報。例えば、秘密暗号鍵と私用暗号鍵、パスワードやPINのような認証データ。

エントロピー源（entropy source） - この暗号機能は、1つまたは複数のノイズ源からの出力を蓄積して、乱数生成器用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。

Extensible Authentication Protocol （EAP） - 無線ネットワークで使用される認証の枠組。TOEは、EAP-TLSをサポートする。EAP-TLSは、PKIを使用して、認証サーバ及び無線クライアントの両方を認証する。

FIPS承認済み暗号機能（FIPS-approved cryptographic function） - 次のいずれかのセキュリティ機能（例えば、暗号アルゴリズム、暗号鍵管理手法、または認証手法）：1）連邦情報処理規格（FIPS）に規定されている、または2）FIPSに採用され、FIPSの附属書またはFIPSが参照する文献に規定されている。

IEEE 802.1X - 有線ネットワークに接続するためにデバイス（無線クライアント）への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に関する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（無線クライアント）、認証者（TOE）、及び認証サーバである。

IT環境（IT environment） - TOE境界の外部にあってTOE機能及びセキュリティ方針をサポートするハードウェア及びソフトウェア。

運用環境（operational environment） - TOEが運用される環境。

SAR（security assurance requirements：セキュリティ保証要件） - 開発者と評価機関がセキュリティ機能要件適合を実証するための開発方法と評価方法を記述する。SARは、開発者と評価者のために具体的なテストを記述するべきである。

SFR（security functional requirement：セキュリティ機能要件） - TOEによって満たされなければならないセキュリティ機能を記述する。SFRは、特定の技術に合わせて変更される。

ST（security target：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（target of evaluation：評価対象） - 本PPの要件に対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または製品の集合を指す。

TOEセキュリティ機能（TSF：TOE security functionality） - TSPの正しい実施に依存しなければならないすべてのハードウェア、ソフトウェア、及びTOEの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：TOE security policy） - TOE内の資産を管理、保護、配付する方法を規定する1組のルール。

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

許可されていない利用者（unauthorized user） - 管理者によってTOEの使用を許可されていない利用者。

附属書 F：PP の識別

タイトル：	無線ローカルエリアネットワーク（WLAN）アクセスシステム用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 改訂3、2009年7月
キーワード：	WLAN、アクセスポイント、WLANアクセスシステム、EAP、IEEE 802.11