ネットワーク・デバイスのセキュリティ要件

原文タイトル：

Security Requirements for Network Devices

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_nd_v1.0.pdf

Information Assurance Directorate

NSA 情報保証局

2010 年 12 月 10 日
バージョン 1.0

平成 24 年 1 月 24 日　翻訳 暫定第 0.3 版
独立行政法人情報処理推進機構
技術本部セキュリティセンター
情報セキュリティ認証室

目　次

表一覧

１　はじめに（イントロダクション）

このプロテクション・プロファイル（PP）は、ネットワーク・デバイス（ネットワークへ接続されるインフラ用デバイスと定義される）のためのセキュリティ要件を記述しており、明確に定義され、記述された脅威を低減することを目的とした最低限で、ベースライン（必須）の要件を提供することを意図している。それは、「伝統的な」プロテクション・プロファイルと文書に含まれる要件の一連の評価についての進化を意味している。このイントロダクションは、適合 TOE の特徴を記述し、本書の読者に対するガイダンスとして PP の進化的な観点についても議論する。

1.1　適合する評価対象（TOE）

本書は、ネットワーク・デバイスのためのプロテクション・プロファイルである。本 PP の文中におけるネットワーク・デバイスは、ネットワークに接続され、企業全体の基盤的な役割を持っているハードウェア及びソフトウェアから構成されたデバイスである。本 PP への適合を主張するべき「ネットワーク・デバイス」の例としては、ルータ、ファイアウォール、IDS、監査サーバ、及びスイッチ等のレイヤー３の機能性を持つデバイスを含む。ネットワークへ接続されるが、本 PP に対しての評価に適していないデバイスの例としては、モバイル・デバイス（「スマートフォン」）、エンドユーザ用ワークステーション、SQL サーバ、Web サーバ、アプリケーション・サーバ、及びデータベース・サーバ等が含まれる。レイヤー１及び／またはレイヤー２で動作するデバイス、例えばハブ、ブリッジ、及びアクセス・スイッチ等は、もしそれらがリモート管理用のネットワーク・インタフェースを備えていれば、本 PP に対する評価に適している。

TOE が（記述された脅威環境への対応として）実装を義務付けられている機能性が以下の節で議論されているが、ここで簡単に記述すると役立つ。適合 TOE は、脅威に対抗するセキュリティ機能を TOE に対して提供し、法規制により課せられているポリシーを実施する。適合 TOE は、分散 TOE のエレメント間の通信（例えば、ネットワーク IDS センサーと集中化された IDS マネージャの間等）、または単一企業における TOE の具体化（例えば、ルータ間等）を保護しなくてはならない。TOE は、識別と認証サービスを提供し、適度な複雑さのパスワードやパスフレーズをサポートし、これらのサービスをリモート（リモート・ログイン）と同様にローカルに（すなわち、ローカル・ログオン）提供しなければならない。TOE は、TOE におけるセキュリティ関連アクティビティに関連した一連のイベントについての監査機能も提供しなければならないが、これらのイベントは TOE から距離のあるデバイスへ保存される。TOE は共通ネットワーク DOS 攻撃に対する保護機能を提供しなければならない、また TOE に対する更新プログラムの検証機能も提供しなければならない。

本 PP が要求するプロトコルは証明書を活用するが、本 PP のバージョンでは証明書基盤における要件を課さない（例えば、証明書の有効性を検証するために OCSP を利用する等）。このような要件は本書の今後のバージョンで追加される。

本 PP の一連の要件が、エンドユーザにある程度の価値を提供できるようなより速く、低コストで評価されるための範囲に限定されることを意図している。たくさんの追加の機能性（及び要件）が含まれるような STs は、推奨されない。将来的なモジュールとして、一連の追加の機能性（例えば、ファイアウォール、VPNs 等）が利用され、追加の機能性を指定したい ST 作成者がその時には利用可能となる。

２　セキュリティ課題記述

前節に詳述したように、適合 TOE が対処するセキュリティ課題は、特定のタイプのネットワーク・デバイスの特定の機能性をターゲットにしたものとは対照的に、ネットワーク・デバイスに共通する脅威とポリシーによって記述される。附属書 A : サポート表は、より「伝統的（トラディショナル）」な形式でセキュリティ課題記述（SPD）を表現している。次の節で適合 TOE が対処する課題を詳細化する；附属書 A の「伝統的（トラディショナル）」な記述への言及も含まれる。

2.1　TOE との通信

ネットワーク・デバイスは、管理者と同じように、他のネットワーク・デバイスとネットワーク越しに通信を行う。通信の両端は、TOE から地理的にも論理的にも離れており、さまざまな他の機器を通過する。これらの中間にあるシステムは、敵対者の管理下にあるかもしれないし、TOE との通信を危険にさらす可能性があるかもしれない。これらの通信は 3 つのカテゴリー（リモート管理者と通信中の TOE ; 分散処理環境における別のインスタンスまたは自身のインスタンスとの通信中の TOE ; その TOE の別のインスタンスではない別の IT エンティティと通信中の TOE（例えば、NTP サーバやピアルータ等））にある間は、両端の間の通信に対する脅威は同様となる。

TOE による平文通信が重要なデータ（例えば、パスワード、設定、経路更新など）を中間のシステムによって読み取られたり、かつ／または直接操作されたりして、TOE を危険にさらすかもしれない。いくつかのプロトコルは保護を提供するために使われるが、それらの各プロトコルは多種多様なオプションが実装されうる上、さらに RFC に記載されたプロトコル仕様に適合した全体的なプロトコルの実装がされているのである。例えば、弱い暗号アルゴリズム（DES のように RFC になってはいるが）を使った場合、敵対者に暗号化チャネル上のデータを読み取られたり、直接操作されたりする可能性があり、そのような攻撃を防止することのできる対策をくぐり抜けられてしまう。さらに、もしプロトコルがあまり使われていないオプションや非標準のオプションが実装されていれば、プロトコル仕様に適合しているかもしれないが、大企業で使われている典型的な、他の装置と連携を取ることができないだろう。

たとえ通信経路が保護されていても、外部利用者（リモート管理者、分散した TOE の別なインスタンス、またはピアルータのような信頼された IT エンティティなど）がだまされてしまい、悪意のある第三者利用者またはシステムが TOE であると思ってしまう可能性がある。例えば、中間者が TOE からの接続要求を横取りして、外部利用者があたかも TOE であるように応答することがありうる。すると、同様に、TOE は相手が非合法なリモート・エンティティであるとき、だまされて合法なリモート・エンティティと通信を確立したと思ってしまうこともありうる。ある攻撃者は悪意のある仲介者攻撃（マン・イン・ミドル型の攻撃）を埋め込み、中間のシステムが改ざんされたり、このシステムによってトラフィックが中継されたり、検査されたり、変更されたりしてしまう。適切な対策が適用されていなければ、暗号化通信チャネルを経由してこの攻撃が埋め込まれることもありうる。これらの攻撃は、ある意味、悪意のある攻撃者によってネットワーク・トラフィック（例えば、認証セッション）をキャプチャーしたり、そのトラフィックを「プレイバック」してエンドポイントが合法なリモート・エンティティと通信していると思ってしまうようにだますことを可能にしてしまう。

[T.UNAUTHORIZED_ACCESS]

2.2 悪意のある「更新（アップデート）」

利用される共有な攻撃の手口（vector）の多くは、よく知られた瑕疵（バグ）を含むソフトウェアのパッチ未適用のバージョンに対する攻撃を含むので、脅威環境に対する変更を確認するために、ネットワーク・デバイスのファームウェアの更新が必要である。タイムリーなパッチの適用はシステムが「手ごわい標的（hard target）」であると確証を与える、したがって、製品がメンテナンスされ、セキュリティポリシーが実施されうるだろうと言う可能性を増加させている。しかし、製品に適用されるべき更新は、ある程度信頼できるものでなければならない。さもないと、攻撃者は自分自身で「更新」を作成して、例えばルートキット、ボット、またはその他の悪意のあるソフトのように彼らの選んだ悪意のあるコードを含んだものに置き換えられることが起きうる。一度この「更新」がインストールされると、攻撃者はシステムの制御やデータのすべてを手に入れてしまう。

この脅威へ対抗するための典型的な方法は、更新に対するハッシュ値を追加したり、さらにこれらのハッシュ値に暗号操作（例えば、デジタル署名）を追加したりする方法が考えられる。しかし、これらの方法の有効性は更なる脅威を発生させる。例えば、弱いハッシュ関数は攻撃者が合法なアップデートを変更してもハッシュ値が変更されないままになってしまうような結果を招いてしまう可能性がある。暗号署名スキームに関しては、以下のような依存性がある。

1) 署名を提供するために利用される暗号アルゴリズムの強度、及び
2) 署名を検証するエンドユーザの能力（信頼のルート（認証局）へ遡るデジタル署名の階層に対する典型的なチェックを含む）。

もし暗号署名スキームが弱いならば、攻撃者に改ざんされてしまい、エンドユーザは悪意のある更新をインストールしてしまい、合法であると考えてしまう。同様に、もし信頼のルートが改ざん可能であれば、強いデジタル署名アルゴリズムであっても悪意のある更新がインストールされるのを防ぐことはできない（攻撃者は改ざんされた信頼のルートを使って更新に対して自身の署名を用意に作成してしまい、悪意のある更新が検知されることなくインストールされてしまうからである）。

[T.UNAUTHORIZED_UPDATE]

2.3 検知されないシステム活動

いくつかの脅威は TOE の特定の能力で検知されるが、検知することができないような切迫した、または発生しているセキュリティ改ざんを示す脅威もある。管理者は、TOE が提供するセキュリティを危険にさらすような行動、例えばセキュリティパラメタの設定ミス、を無意識のうちに TOE に対して行っている可能性がある。利用者データへの応答として行われる処理（例えば、安全な通信セッションの確立や保護されたセッションに関連した暗号化処理） は、TOE のセキュリティ・メカニズムの障害や侵害の兆候（例えば、セッションが確立されるべきでないときの IT エンティティとのセッションの確立）を示す可能性がある。TOE のセキュリティに影響を及ぼしうる活動の兆候が検知または観測されない場合、責任者は気が付かず、問題を修正できないまま、TOE に対して有害な活動が実行される可能性がある。さらに、もしデータが保存されず、記録が生成されないなら、TOE の再構築や侵害の程度を理解する能力に悪影響を与えることになるであろう。

TOE が監査データを生成することをこの PP が必要としながらも、これらのデータは TOE 上に蓄積される必要はなく、むしろ信頼された外部の IT エンティティ（例えば、システムログサーバ）に送信する方が良い。これらのデータは中間のシステムに読み出されたり改ざんされたりして、潜在的に疑わしい活動の兆候をマスキングするかもしれない。また、TOE

が外部の IT エンティティとの接続性を喪失し、監査情報が信頼できる相手に送られないという場合もあるかもしれない。

[T.ADMIN_ERROR, T.UNDETECTED_ACTIONS, T.UNAUTHORIZED_ACCESS]

2.4 TOE へのアクセス

2.1 節で述べたような、TOE が多種の外部者との通信そのものに焦点を当てた通信を処理するという脅威に加えて、TOE へのアクセスを試みることから生じる脅威、或いは、それらのアクセスを試みる手段が成功した時に生じる脅威もある。

例えば、もし TOE へのアクセスを対話型で認められている利用者（局所的にコンソールとつながっていたり、SSH のようなセッション・オリエンティッドなプロトコルでつながっていたりする）と、このように TOE を使う権限がない利用者を TOE が区別できなければ、TOE の設定は信用できないと思われる。この区別ができると想定しても、TOE へのアクセス権のない攻撃者によって許可されたアカウントが危険におかされたり、使われたりするという脅威がまだ存在する。

そのような攻撃の１つの手口（vector）としては、TOE の権限を持った管理者による粗末なパスワードの使用が挙げられる。短すぎるパスワードや辞書に載っている語を使ったような簡単に推測できるパスワード、または、頻繁に変えていないパスワードについては、総当たり攻撃の影響を受けやすい。さらに、もしパスワードが一定の期間はっきりと見えたりしていれば（例えば、正当な利用者がログオン時にタイプしている時）、傍観者がパスワード情報を取得して、システムに不正にアクセスすることもあり得る。

正当な利用者がログオンした際でも、考えられる脅威は多数ある。パスワードを変更している途中で､もし TOE がパスワードを変更されるアカウントと利用者を確定できなければ、誰でも正当なアカウントのパスワードを変更して、そのアカウントを引き継ぐことができる。もし利用者がログインセッションの途中で放っておいた際に、そのデバイスにアクセス権のない別の人が座って不当に TOE にアクセスを始めるかもしれない。

[T.UNAUTHORIZED_ACCESS]

2.5 資源の枯渇

ネットワーク・インタフェースのデバイスに対して昨今ますます増加している攻撃が DoS 攻撃である。すべてのデバイスに関して共通するリソースがいくつかあり、検討する必要がある。つまり、それは、管理用インタフェースをサポートするリソースである。例えば、もし攻撃者が接続表に書き込むことができたら、管理者は管理機能を行うネットワーク・デバイス・インタフェースに間接的に接続できなくなってしまう。

その他のリソースも攻撃され得るかもしれないが、それは、いささかデバイスの性質によるところがある。例えば、ネットワークの一時的記憶装置上でレベル２までしか作動しないスイッチに関していえば、ネットワークの一時的記憶装置上のさらに高いレベルまで作動するアプリケーション・フィルタリング・ファイアーウォールと同じ DoS 攻撃の懸念はないであろう。他に考慮すべき点としては、デバイスにどのくらいのメモリ（記憶容量）があるか、処理能力はどれくらいか、デバイスにバッファー割り振り等がどれだけあるか、そして、攻撃者が不当にリソースを消費しようとしてもその機能を実行ことができずデバイスを放棄する可能性がどれくらいあるか等がある。

[T.RESOURCE_EXHAUSTION]

2.6　利用者データ漏洩

本 PP に含まれる脅威のほとんどは TSF や管理データに関してのものであるが、その他にもすべてのネットワーク・デバイスが緩和すべきである、利用者データに対する脅威がある。TOE 内を行き来するデータは、何らかの事情で他の利用者に送られるかもしれない。これらのデータはセンシティブかもしれないので、受け入れないセキュリティ侵害を引き起こすかもしれない。対処すべき具体的な脅威としては、初めのネットワーク・トラフィックの発信者によって、意図されない利用者にネットワーク・トラフィックが送られ、何らかの事情で再利用され得るという、ネットワーク・トラフィックを処理する際に TOE によって保持される利用者データに関係するものがある。

[T.USER_DATA_REUSE]

2.7　TSF 機能停止

TOE のセキュリティメカニズムは、一般的に、初期的な一連のメカニズム（例えば、メモリ管理、プロセス実行の特権モード）から、さらに複雑な一連のメカニズムまで積み上げられる。初期的なメカニズムの障害は、さらに複雑なメカニズムのセキュリティ侵害につながり、最終的に TSF のセキュリティ侵害をもたらす。

[T.TSF_FAILURE]

3　セキュリティ対策方針

適合 TOE は、脅威に対抗するセキュリティ機能を TOE に対して提供し、法規制により課せられているポリシーを実施する。次の節では、前に説明した、適合 TOE への参入の動機となった脅威を踏まえて、この機能に関する説明を述べる。提供されるセキュリティ機能は、TOE のエレメント間やエレメントへの保護された通信、TOE への管理されたアクセスとその設定能力、セキュリティ関連のイベントを検知するシステム・モニタリング、リソースの在庫管理、TOE の更新のソースを検証する能力を含む。

3.1　保護された通信

2.1 節「TOE との通信」に述べた TOE とのセンシティブなデータの送受信に関する問題に対処するために、適合 TOE は暗号化をそれらや両端の間の通信パスに提供する。それらの経路は、IPsec、TLS/HTTPS、SSH の 3 つの基本プロトコルのうち 1 つ（以上）を使って実装される。これらのプロトコルは様々な実装の選択を提示する RFC によって特定されている。要件は、相互運用性や暗号攻撃に対する抵抗を提供するために、これらの選択のいくつか（特に暗号プリミティブ）に課せられている。適合 TOE は、それらの特定された選択すべてをサポートしながら、さらに他のアルゴリズムやプロトコルをサポートするかもしれない。それらの付加的なメカニズムが評価されるかどうかは、認証機関によりけりである。もしそれらの付加的なメカニズムが評価されなければ、TOE 操作時に無効化されるよう（または、ある特定のセキュリティ機能に影響を与えないよう）、管理者に指導が行われなければならない。

通信のための漏洩保護（改ざんの検知）の提供に加えて、本書に述べた各プロトコル（IPsec、SSH 、TLS/HTTPS）は、暗号を使った安全な方法で、両端の相互認証を提供する。つまり、たとえ両端間で悪意のある攻撃者がいたとして、通信パスのどちらかの端を取って代わろうとしても、反対側の通信相手が見破ることができる。各プロトコルの要件は、プロトコルそのもののメカニズムに加えて、2.1 節に述べられたようなリプレイ攻撃に対する保護を提供し、通常は、通信のリプレイが検知されるよう各通信の固有値（unique value）を含んでいる。

（FAU_STG_EXT.3, FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FCS_COMM_PROT_EXT.1 (FCS_IPSEC_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1), FPT_PTD.1(2), FPT_ITT.1(1), FPT_ITT.1(2), FPT_RPL.1, FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1(1),FTP_TRP.1(2)）

3.2　検証できる更新

2.2 節「悪意のある「更新（アップデート）」」で概要を説明したように、セキュリティ管理者がシステムの更新が信頼されうると確証するのに失敗すると、システム全体が危険に冒されることにつながる。更新の信頼を確立する第一段階としては、更新をインストールする前にシステムアドミニストレータによって確認できる、更新に対するハッシュ値を公開することである。そうすれば、セキュリティ管理者が更新をダウンロードでき、ハッシュ値を算出でき、公開されたハッシュ値と比較することができる。これによって、ダウンロードした更新が公開されたハッシュ値と関連付けられる一方で、もし更新/ハッシュ値の組み合わせのソースが侵害されたり、信頼できないものであれば、それを示すことができない。そのため、システムには脅威が残ったままである。更新のソースの信頼を確立するため、システムは暗号メカニズムを提供でき、更新を調達する手段、更新を暗号化して TOE が持つデジタル署名メカニズムを使って更新をチェックする手段、システムの更新をインストールする手段を提供することができる。このプロセスが完全に自動化されることに要件はない一方で、管理指導要綱（administrative guidance documentation）に手動で行わなけ

ればならない手段についてや管理者が更新した署名を確証する方法については詳述するだろう（will）。

（FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3)）

3.3 システム・モニタリング

2.3 節「検知されないシステム活動」で議論されたように、セキュリティ管理者が、設定または/或いはシステム操作に関連する意図的や意図的でない問題を発見することができるという情報が存在するのを確信させるために、適合 TOE はそのような活動の検知を目的とした監査データを生成する能力を持っている。管理上の活動（administrative activities）の監査（報告書）で、システムの設定が誤っている際の修正措置（corrective action）の情報を急いで提供するべきである。選択システムイベントの監査により、TOE の重要部分（例えば、稼動していない暗号プロバイダープロセス）の障害の兆候や疑わしい性質を持った異常な/変則な活動（例えば、不審な時間の管理セッションの確立、セッション立ち上げやシステム認証の度重なる失敗）を提供することができる。

場合によっては、多くの監査情報がありすぎて、TOE や監査情報をレビューする担当の管理者が圧倒されるかもしれない。生成された監査データが TOE の DoS 状態を引き起こすような可能性を軽減するために、TOE は外部の信頼されたエンティティに監査情報を送ることができなければならない。この情報は、外部のデバイスに送信されたときの情報を整理するのに役立てるため、信頼性のあるタイムスタンプを実行しなければならない。

監査サーバとの通信の喪失は問題である。この脅威に対しては潜在的な軽減/緩和策があるが、本 PP は特別なアクションの実行を規定していない。このアクションによって監査情報を保存し、それでいて TOE に機能性責任を満たすよう許可する段階で、ある特定の環境においての TOE の適合性に関する決定を押し進めるべきである。

（FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FAU_STG_EXT.3, FPT_STM.1）

3.4 TOE 管理

管理者が TOE と交信するのに信用がある手段を提供するため、TOE はパスワードを使ってログオンするメカニズムを提供する。管理者は、破られにくいパスワードを組み立てる能力を持たなければならず、パスワードを定期的に変えることができるように、環境が整ったメカニズムでなければならない。管理者がパスワードをタイプしているのを攻撃者に見られるような環境を避けるため、ログオン時にパスワードは隠されなければならない。アカウントの不正な使用のリスクを軽減するために、セッションのロックや終了も実装されなければならない。

（FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU_EXT.5, FIA_UAU.6, FIA_UAU.7, FMT_MTD.1, FMT_SMF.1, FMT_SFR.1, FPT_PTD.1(1), FTA_SSL_EXT.1, FTA_SSL.3）

3.5 資源利用

2.5 節「資源の枯渇」で議論されたように、DoS 攻撃は、運転機能またはセキュリティ機能を行う TOE の能力に影響を与え得る。そのような攻撃の影響を緩和するために、配分可能な枯渇性資源の量の割り当てがなされている。これらの割り当てによって、TOE はデバイスを使用可能に保つためにリソースの一部を蓄えることができ、そのような攻撃の影響は管理者によって対処される。

（FRU_RSA）

3.6 残存情報消去

利用者データが何らかの事情でオリジナルの送信者の意図しないネットワーク・トラフィックに含まれるという脅威に対抗するため、TSF は TOE から送られたネットワークパケットが前のネットワーク処理情報の「残り物」のデータを含まないよう確証する。

（FDP_RIP.2）

3.7 TSF 自己テスト

TSF に利用されているセキュリティ・メカニズムに内在する障害を検知するため、TSF は自己テストを実行する。この自己テストの範囲は、製品開発者に委ねられているが、さらに複雑な一連の自己テストを行うことによって、エンタープライズ・アーキテクチャを発展させた、さらに信頼できるプラットフォームを作るべきである。

（FPT_TST_EXT.1）

4 セキュリティ要件

この章にあるセキュリティ機能要件は、IT セキュリティ評価のためのコモンクライテリア、バージョン 3.1 リビジョン 3 のパート 2、及び追加の拡張機能コンポーネントから導き出されている。

4.1 表記法

CC は、セキュリティ機能要件についての次に示す操作を定義している：割付、選択、選択及び詳細化に含まれる割付。この文書は、CC で定められた操作を識別するために次のようなフォント表記法を用いる。

- 割付：*イタリック*書体で表記する；
- PP 作者による詳細化：**ボールド**書体、及び必要ならば取消し線で表記する；
- 選択：アンダーライン書体にて表記する；
- 選択における割付：イタリック及びアンダーラインされた書体で表記する；
- 繰り返し：例えば、(1)、(2)、(3) 括弧における繰り返し回数を追加することにより表記する

TOE SFR の要件名の後に、「EXT」ラベルを付けて表記している。

4.2 TOE セキュリティ機能要件

この節は、TOE のセキュリティ機能要件を識別している。以下の表 1 にある TOE セキュリティ機能要件は、次の下位の節に詳細に記述されている。

表 1：TOE セキュリティ機能要件と監査対象事象

機能要件	監査対象事象	追加の監査記録内容
FAU_GEN.1	なし。	
FAU_GEN.1	なし。	
FAU_STG_EXT.1	なし。	
FAU_STG_EXT.3	接続性の喪失。	追加情報なし。
FCS_CKM.1	機能性の起動の失敗。	追加情報なし。
FCS_CKM_EXT.4	機能性の起動の失敗。	追加情報なし。
FCS_COP.1(1)	機能性の起動の失敗。	追加情報なし。
FCS_COP.1(2)	機能性の起動の失敗。	追加情報なし。
FCS_COP.1(3)	機能性の起動の失敗。	追加情報なし。
FCS_COP.1(4)	機能性の起動の失敗。	追加情報なし。
FCS_RBG_EXT.1	プロセスのランダム化失敗。	追加情報なし。
FCS_COMM_PROT_EXT.1	なし。	
FDP_RIP.2	なし。	
FIA_PMG_EXT.1	なし。	
FIA_UIA_EXT.1	識別・認証メカニズムの利用すべて。	提供された利用者識別。試行元（例：IP アドレス）。
FIA_UAU_EXT.5	認証メカニズムの利用すべて。	試行元（例：IP アドレス）。
FIA_UAU.6	再認証の試行。	試行元（例：IP アドレス）。
FIA_UAU.7	なし。	
FMT_MTD.1	なし。	
FMT_SMF.1	なし。	

FMT_SMR.1	なし。	
FPT_ITT.1(1)	なし。	
FPT_ITT.1(2)	なし。	
FPT_PTD.1(1)	なし。	
FPT_PTD.1(2)	なし。	
FPT_RPL.1	検知されたリプレイ攻撃。	試行元（例：IP アドレス）。
FPT_STM.1	時刻に対する変更。	時刻に関する新旧の値。試行元（例：IP アドレス）。
FPT_TUD_EXT.1	更新の開始。	追加情報なし。
FPT_TST_EXT.1	TSF 自己テストが完了したことの表示。	テストで生成された「成功」または「失敗」以外の追加情報。
FRU_RSA.1	最大割当ての超過。	資源の識別情報
FTA_SSL_EXT.1	対話セッションのロック解除に関する試行。	追加情報なし。
FTA_SSL.3	ｾｯｼｮﾝﾛｯｸﾒｶﾆｽﾞﾑによるﾘﾓｰﾄｾｯｼｮﾝの終了。	追加情報なし。
FTA_TAB.1	なし。	
FTP_ITC.1(1)	高信頼チャネルの開始。高信頼チャネルの終了。高信頼チャネル機能の失敗。	開始元の識別情報、及び失敗した高信頼ﾁｬﾈﾙ確立の試行対象。
FTP_ITC.1(2)	高信頼チャネルの開始。高信頼チャネルの終了。高信頼チャネル機能の失敗。	開始元の識別情報、及び失敗した高信頼チャネル確立の試行対象。
FTP_TRP.1(1)	高信頼チャネルの開始。高信頼チャネルの終了。高信頼チャネル機能の失敗。	主張された利用者の識別情報
FTP_TRP.1(2)	高信頼チャネルの開始。高信頼チャネルの終了。高信頼チャネル機能の失敗。	主張された利用者の識別情報

4.2.1 セキュリティ監査（FAU）

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) 監査機能の起動と終了；

b) 監査の基本レベルの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) [*表 1 に掲載された特別に定義されている監査対象事象*]。

適用上の注意：ST 作成者は、他の監査対象事象を直接表に含めることができる；それらは提供されている表に限定されるものではない。

本書に含まれる SFR の多くの監査対象の観点は、管理者アクションを取り扱うものである。上記の項目 c は、監査可能なすべての管理者アクションを要求しており、これらのアクションの監査可能性についての追加の仕様は表 1 において記載されていない。

保証アクティビティ：
評価者は、管理者ガイダンスをチェックし、すべての監査対象事象がリスト化され、監査記録のフォーマットが提供されていることを確実にしなければならない（shall）。それぞれの監査記録フォーマットタイプが網羅され、各フィールドの簡潔な説明とともに記述されていなければならない（shall）。評価者は、PP で強制された監査対象事象タイプ全部が記述されており、フィールドの記述が FAU_GEN.1.2 で要求されている情報、表 1 に記述された追加の情報を含んでいることを確実にするためにチェックしなければならない（shall）。

評価者は、管理者アクションが本 PP の文脈に関連しているかを決定しなければならない（shall）。評価者は、管理者ガイダンスを検査して、サブコマンド、スクリプト、及び設定ファイルを含めて、PP で指定された要件の実施に必須で、TOE に実装されているメカニズムの設定（有効または無効等を含む）に関連している管理者コマンドにはどのようなものがあるかを調べなければならない（shall）。評価者は、本 PP に関連したセキュリティ関連の管理者ガイダンスにおいてどのようなアクションがあるかを決定している間に取った方法またはアプローチについて文書化しなければならない（shall）。評価者は、本アクティビティを AGD_OPE ガイダンスが要件を満足していることを確実にする際に付随したアクティビティの一部として実施してもよい（may）。

評価者は、TOE に対して次の事象についての監査記録を生成させることによって、正しく監査記録を生成するための TOE の能力をテストしなければならない（shall）：チャネルの確立と終了、リプレイ攻撃の検知、管理者アクション。評価者は、あるチャネルの確立と終了が PP に含まれる暗号化プロトコル（すなわち、IPsec、SSH、TLS、HTTPS）のそれぞれについて実施されていることをテストしなければならない（shall）。TLS セッションの確立と終了を実証するテストは、HTTPS セッションに関するテストと組み合わせて実施することができる。リプレイ攻撃に関して、評価者は PP に含まれる暗号化プロトコルのそれぞれについて検出された場合にリプレイ攻撃監査対象事象が生成されることをテストしなければならない（shall）。管理者アクションに関して、評価者は、上記において評価者によって決定されたそれぞれのアクションが本 PP の文脈でセキュリティ関連であることをテストしなければならない（shall）。テスト結果を検査する際、評価者はテスト中に生成される監査記録が管理者ガイダンスで指定されたフォーマットと一致していること、及び各監査記録のフィールドが適切に入力されていることを確実にしなければならない（shall）。

ここで留意すべき点は、このテストはセキュリティ・メカニズムのテストとまったく同時に実施することができることである。例えば、本 TOE がリプレイ攻撃の試行を検知できることを確実にするテストは、おそらく要件 FPT_RPL.1 が満たされることを論証するために行われるだろう。別の例では、提供された管理者ガイダンスが正しいことを確実にするために実施されるテストは、AGD_OPE.1 が満たされてことを検証し、監査記録が想定されたとおり生成されていることを検証するために必要とされている管理者アクションの呼び出しを取り扱うべきであることを検証することである。

FAU_GEN.1.2　TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

a) 事象の日付及び時刻、事象の種別、サブジェクト識別情報、事象の結果（成功または失敗)；及び

b) 各監査対象事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付：表 1 のカラム 3 指定する情報]。

適用上の注意：以前のコンポーネントでは、ST 作成者は他の追加情報を生成して上記表 1 を更新するべきである。本要件の文脈における「サブジェクト識別情報」は、例えば、管理者ユーザ ID または影響を受けたネットワーク・インタフェースのいずれであってもよい。

FAU_GEN.2　利用者識別情報の関連付け

FAU_GEN.2.1　識別された利用者のアクションがもたらした監査対象事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

FAU_STG_EXT.1　外部監査証跡格納

FAU_STG._EXT.1.1　TSF は、［選択：FTP_ITC.1 で定義された高信頼チャネル経由で外部 IT エンティティに対して生成した監査データを送信、FTP_ITC.1 で定義された高信頼チャネル経由で外部 IT エンティティから監査データを受信し格納］できなければならない（shall）。

適用上の注意：もし、「受信と格納」オプションが上記の選択より選ばれた場合、ST 作成者は、TSF 監査データ格納の能力の詳細を記載するべきである（should）。

FAU_STG_EXT.3　監査サーバ接続性の喪失時のアクション

FAU_STG_EXT.3　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 エンティティへのリンクが利用不能であるならば、[割付: *アクション*] を取らなければならない（shall）。

適用上の注意：ST 作成者は、監査サーバへのリンクが利用不能であるならば、TOE が取るべきアクション（管理者へ連絡する、パケットの送出を停止する）を記述すること。

保証アクティビティ：
評価者は、管理者ガイダンスが管理者に対してどのように監査サーバとの通信を確立するかを指示していることを確実にするため、管理者ガイダンスを検査しなければならない（shall）。ガイダンスは、このチャネルがどのようにセキュアな方法（例えば、IPsec、TLS）で確立されるかを指示しなければならない（must）。評価者は、TOE と監査サーバ間のリンクが切れたときに必要なアクション（または処置）を管理者ガイダンスが決定していることを検査する。これはネットワーク接続性の喪失、またはセキュアなプロトコルのリンクが終了することにより発生することがある。

評価者は、監査サーバへのリンクを確立することにより管理者ガイダンスをテストしなければならない（shall）。 FAU_GEN.1 の元で記述された保証アクティビティを実施するために必要とされることに留意すること。評価者は、管理者ガイダンスに記述されたアクションが適切に実施さ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･リンクを終了する、監査サーバをシャットダウンする）（shall）。

4.2.2 暗号サポート（FCS）

FCS_CKM.1 暗号鍵生成（非対称鍵用）

FCS_CKM.1.1 **詳細化 :** TSF は、以下に合致するドメイン・パラメタ生成器及び **[選択 : (1) 乱数生成器、及び/または (2) 素数生成器] に従って、非対称暗号鍵**を生成しなければならない（shall）：

a) すべての場合：（すなわち、上記のいずれも)

- **ANSI X9.80(3 January 2000)「Prime Number Generation, Primality Testing, and Primality Certificates」 の決定論的方法を使用した乱数または構成的生成方法を用いる**
- **生成された鍵強度は、控えめな見積もりによる、112 ビットの対称鍵強度以上でなければならない（shall）。**

適用上の注意 : 生成された 2048 ビットの DSA 鍵及び rDSA 鍵の鍵強度は、112 ビットの対称鍵強度と同等またはそれ以上である必要がある。同等な鍵強度についての情報として、NIST Special Publication 800-57「Recommendation for Key Management」を参照すること。

b) 有限体に基づく鍵確立スキームで用いられるドメイン・パラメタの場合：

- **NIST Special Publication 800-56A, 「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」（離散対数暗号を用いた鍵確立スキームに関する勧告）**

c) RSA に基づく鍵確立スキームで用いられるドメイン・パラメタの場合：

- **NIST Special Publication 800-56B「Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography」（素因数分解暗号を用いた鍵確立スキームに関する勧告）**

d) 楕円曲線に基づく鍵確立スキームで用いられるドメイン・パラメタの場合：

- **NIST Special Publication 800-56A, 「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」（離散対数暗号を用いた鍵確立スキームに関する勧告）**
- **TSF は「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 」（デジタル署名標準））。**

適用上の注意 : このコンポーネントは TOE が FCS_COP.1(2)においてデジタル署名操作で利用する公開／秘密鍵ペアを生成できることを要求している。もし、複数のスキームがサポートされている場合、ST 作成者はこの能力を示すために、この要件と FCS_COP.1(2) を繰り返し記述するべきである（should）。

保証アクティビティ：
評価者は、上記要件のテストにおけるガイダンスとして、「The FIPS 186-3 Digital Signature Algorithm Validation System (DSAVS または DSA2VS)」、「The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)」、及び「The RSA Validation System (RSAVS)」のドメイン・パラメタ生成及び鍵ペア生成部分を利用しなければならない（shall）。これは、評価者がテストにおいて検証されるテストベクターの生成が可能であり、良いものであると知られているアルゴリズムの標準実装を持っていることを要求している。

FCS_CKM_EXT.4　暗号鍵のゼロ化

FCS_CKM_EXT.4.1　TSF はすべての平文の秘密鍵及びプライベート鍵と CSPs について、必要がなくなったときにゼロ化しなければならない（shall）。

適用上の注意：「暗号クリティカル・セキュリティ・パラメタ」は、FIPS 140-2 において、「セキュリティに関するじょうほうであって、その開示または変更が、暗号モジュールのセキュリティを危殆化し得るもの（例えば、秘密鍵及びプライベート鍵、及びパスワードや PINs のような認証データ）として定義される。

上記のゼロ化は、鍵／暗号クリティカル・セキュリティ・パラメタをほかの記憶場所に移動させる際に、平文のカギ／暗号クリティカル・セキュリティ・パラメタのための、それぞれの中間格納領域（すなわち、このようなデータが流れる経路に含まれる（例えば、メモリバッファのような）いかなるストレージ）に適用される。

保証アクティビティ：
評価者は、TSS が、それぞれの秘密鍵（鍵は対称暗号化のために利用される）、プライベート鍵、及び鍵生成のために利用される CSPs；いつそれらがゼロ化されるか（例えば、使用後直ちに、システムのシャットダウン時、等）；及び実施されるゼロ化処理のタイプ（ゼロで上書き、ランダムなパタンで 3 回上書き、等）を記述していることを確実にしていることを検査しなければならない（shall）。もし、保護すべきものを格納するためにさまざまな種類のメモリが利用されている場合、評価者は TSS において、データが格納されているメモリを単位としてゼロ化処理（例えば、flash に格納されている秘密鍵はゼロで 1 回上書きされ、一方、内部ハードドライブに格納された秘密鍵は、各書き込み動作前に変更されるランダムパターンを使って 3 回上書きされる）が記述されていることを確実にするために検査しなければならない（shall）。

FCS_COP.1(1)　暗号操作（データ暗号化／復号に関して）

FCS_COP.1.1(1) **詳細化：**TSF は、以下に合致する 128 ビット、256 ビット、及び **［選択：192 ビット、他の鍵サイズなし］**の暗号鍵サイズ、及び指定された暗号アルゴリズム［［**割付：ひとつ以上の利用モード**］での AES 操作］に従って、［暗号化及び復号］を実施しなければならない（shall）：

- **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：割付に関して、ST 作成者は AES の 1 つまたは複数の利用モードを選択するべきである（should）。第一番目の選択に関して、ST 作成者はこの機能性によりサポートされる鍵サイズを選択するべきである（should）。2 番目の選択に関して、ST 作成者は割付において指定された利用モードを記述する規格を選択するべきである（should）。

保証アクティビティ：
評価者は、上記要件をテストする際のガイダンスとして以下の文書から上記の要件で選択した利用モードに適切なテストを使用しなければならない（shall）。
「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)」
（これらの文書は http://csrc.nist.gov/groups/STM/cavp/index.html から利用可能）
これは、評価者がテストにおいて検証されるテストベクターの生成が可能であり、良いものであると知られているアルゴリズムの標準実装を持っていることを要求している。

FCS_COP.1(2)　暗号操作（暗号署名に関して）

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

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

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

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

適用上の注意：暗号署名のための望ましいアプローチとして、楕円曲線がこの PP の将来の版で要求されるだろう。

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」、FIPS PUB 186-2、「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」、FIPS PUB 186-2、「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」、FIPS PUB 186-2、「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（curves）」 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（shall）。**

適用上の注意：ST 作成者は、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 作成者は適切な割付／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。

FIPS PUB 186-2 が FIPS PUB 186-3 に改訂される間、製品が新しい規格に対応するまでの間は古い規格に適合主張することが許されている。将来的に製品は FIPS PUB 186-2 への適合主張が許されなくなる。ST 作成者は、TOE に関して適切な適合規格を選択する。

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 $\log_2$ をとった値を意味する。デジタル署名の望ましいアプローチとして、ECDSA はこの PP の将来の版で要求されるだろう。

保証アクティビティ：
評価者は、上記要件をテストする際のガイダンスとして、「The Digital Signature Algorithm Validation System」(DSAVS または DSA2VS)、「The Elliptic Curve Digital Signature Algorithm Validation System」(ECDSAVS または ECDSA2VS)、及び「The RSA Validation System」(RSAVS)の署名生成と署名検証部分を利用しなければならない(shall)。　利用される検証システムは、ST で識別された適合規格（すなわち、FIPS PUB 186-2 または FIPS PUB 186-3）に従わなければならない（shall）。これは、評価者がテストにおいて検証されるテストベクターの生成が可能であり、良いものであると知られているアルゴリズムの標準実装を持っていることを要求している。

FCS_COP.1(3)　暗号操作（暗号ハッシュに関して）

FCS_COP.1.1(3)　**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**[選択：SHA-1、SHA-256、SHA-384、SHA-512］及びメッセージダイジェストサイズ［選択：160、256、384、512］ビット**に従って、［暗号ハッシュサービス］を実施しなければならない（shall）：*FIPS Pub 180-3、「Secure Hash Standard」*

適用上の注意：ハッシュアルゴリズムの選択は、メッセージ・ダイジェストのサイズと合致しなければならない；例えば、SHA-1 が選択された場合、有効なメッセージ・ダイジェストは 160 ビットのみとなる。

本 PP の後続版では、SHA-1 は、もはや暗号ハッシュとしての承認されたアルゴリズムではなくなっているだろう。

保証アクティビティ：
評価者は、上記要件をテストする際のガイダンスとして「The Secure Hash Algorithm Validation System (SHAVS)」を使用しなければならない（shall）。*これは、評価者がテストにおいて検証されるテストベクターの生成が可能であり、良いものであると知られているアルゴリズムの標準実装を持っていることを要求している。*

FCS_COP.1(4)　暗号操作（鍵付ハッシュメッセージ認証に関して）

FCS_COP.1.1(4)　**詳細化：**TSF は、以下に合致する**メッセージ・ダイジェストのサイズ［選択：160、256、384、512］ビット、［割付：HMAC で利用されるビットサイズ（ビット）］の鍵サイズ、**及び指定された暗号アルゴリズム HMAC-**［選択：　SHA-1、SHA-256、SHA-384、SHA-512］**に従って、［鍵付ハッシュメッセージ認証（keyed-hash message authentication)］を実施しなければならない（shall）：*FIPS Pub 198-1「The Keyed-Hash Message Authentication Code」、及び FIPS Pub 180-3　「Secure Hash Standard」*

保証アクティビティ：
評価者は、上記要件をテストする際のガイダンスとして「The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)」を使用しなければならない(shall)。*これは、評価者がテストにおいて検証可能なテストベクターの生成が可能であり、良いものであると知られているアルゴリズムの標準実装を持っていることを要求している。*

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、少なくともひとつ以上の独立した TSF ベースのノイズ源からエントロピーを蓄積する何らかのエントロピー源によって初期化されたシード（seed）として与えられた［選択：以下から選択する［選択：Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)］を用いた NIST Special Publication 800-90 ；FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES］に従ってすべてのランダムビット生成（RBG）サービスを実施しなければならない（shall）。

FCS_RBG_(EXT).1.2　決定論的 RBG は、少なくとも（その RBG が）生成する鍵及び認証要素のの最大長以上、かつ、最低限［選択、次から１つを選択：128 ビット、256 ビット］のエントロピーによって初期化されなければならない（shall）。

適用上の注意：NIST Special Pub 800-90, Appendix C は、おそらく FIPS-140 の将来のバージョンで要求されるミニマム・エントロピー測定について記述している。可能であれば、直ちにこれを使用するべきであり、本 PP の将来のバージョンでは要求されるだろう。

FCS_RBG_(EXT).1.1 の最初の節について、ST 作成者は RBG サービスが適合する規格（NIST SP 800-90 または FIPS Pub 140-2 Annex C のいずれか）を選択するべきである（should）。

SP 800-90 は、４つの異なる乱数生成手法を含んでいる；これらはそれぞれの内在する暗号プリミティブ（ハッシュ関数／暗号）に依存している。ST 作成者は、（もし SP 800-90 が選択された場合）使用される関数を選択肢、要件または TSS の中で使用される特定の暗号プリミティブを含めるだろう。識別されたハッシュ関数のいずれか（SHA-1、SHA-224、SHA-256、SHA-384、SHA-512）が Hash_DRBG または HMAC_DRBG に関して許容され、CTR_DRBG に対して AES に基づく実装が許可される。
800-90 で定義された曲線（curves）のみが、Dual_EC_DRBG に対して許可されるが、ST 作成者は選択した曲線（Curve）を含めなければならない（must）*だけでなく、使用されるハッシュアルゴリズムも含めなければならない*（must）。

FIPS Pub 140-2 Annex C に関して以下の通り注意すること。現在、3-Key Triple DES 及び AES アルゴリズムを用いた ANSI X9.31 Appendix A.2.4 に基づく NIST 推奨乱数生成器、第３章に記述された手法のみが有効である。ここで使用される AES 実装の鍵長が利用者データを暗号化に使用するものと異なる場合、FCS_COP.1 は異なる鍵長を反映するために合致させるか、または繰り返し記述しなければならないかもしれない。 FCS_RBG_(EXT).1.2 における選択について、ST 作成者は RBG を初期化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。

ST 作成者は、TOE のベースライン要件にすべての内在する関数が含まれることも確実にすること。

保証アクティビティ：
評価者は、TSS 節をレビューして、TOE で使用される RBG(s) を含んでいる製品のバージョンを決定しなければならない（shall）*。評価者は、TSS で、エントロピーを収集するハードウェアに基づくノイズ源が記述されていることを確認した上で、このノイズ源の場所も確認しなければならない*（shall）*。評価者は、さらに RBG で使用されるすべての内在する関数及びパラメタが TSS にリスト化されていることを検証するだろう。*

評価者は、エントロピー入力を取得する方法に加えて、使用されるエントロピー源の識別及び各エントロピー源からどれだけエントロピーが生成されるのかを含めた、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（shall）。*評価者は、エントロピー源故障（failure）の既知のモードを記述していることも確認しなければならない*（shall）。*最後に、評価者は、TSS 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 出力が記述されていることを確実にしなければならない*（shall）。

評価者は、RBG が適合する規格に従って、以下のテストも実施しなければならない（shall）。

FIPS 140-2, Annex C に適合した実装

この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、次の２つのテストを実施しなければならない。「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ことに注意すること。正しさの証明は各認証機関（スキーム）に任されている。

評価者は、可変シードテスト（Variable Seed Test）を実施しなければならない（shall）。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（shall）。評価者は、また、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（shall not）。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。

評価者は、モンテカルロテストを実施しなければならない（shall）。このテストでは、それぞれ 128 ビットの初期シードと DT を TSF RBG 関数に与える。評価者は、また、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 10000 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、10000 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 へ適合する実装

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（shall）。もし、RBG が設定変更可能であれば、評価者はそれぞれの設定条件について 15 回試行を行わなければならない（shall）。評価者は、また、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（shall）。

もし、RBG が予測耐性（prediction resistance）を備えている場合、それぞれの試行は(1)drbg のインスタンス化、(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二番目のブロック 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（shall）。１番目は、整数カウンタ（0-14）である。次の３つは、インスタンス化操作のためのエントロピー入力、ナンス（Nonce）、およ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（文字列）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（文字列）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、（drbg から）得られるビ

ット列のビット長が（NIST SP800-90 で定義された）出力ブロック長に等しいようなランダムビット列を生成するという意味である。

もし、RBG が予測耐性（prediction resistance）を備えていない場合、それぞれの試行は(1)drbg のインスタンス化、(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（shall）。1 番目は、カウンタ（0-14）である。次の３つは、インスタンス化操作のためのエントロピー入力、ナンス（Nonce）、およ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（文字列）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（文字列）とエントロピー入力である。

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より多くの情報を含んでいる。

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。

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（one-half）となる。

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（shall）。もし、実装が個別化文字列を使用しないなら、値を供給する必要はない。

追加の情報：追加入力文字列のビット長は、個別化文字列長と同じデフォルト値及び制約条件を持つ。

FCS_COMM_PROT_EXT.1　通信保護

FCS_COMM_PROT_EXT.1.1　TSF は、［選択：IPsec、SSH］及び［選択：TLS/HTTPS、他のプロトコルなし］を用いて通信を保護しなければならない。

適用上の注意：上記の要件の意図は、暗号プロトコルを使用して通信を保護するということである。IPsec または SSH のいずれかが必須である；しかし、適合 TOE に実装されている場合、両方が選択されてもよい（may）。さらに、TLS/HTTPS は、それが実装されている場合選択されてもよい。ST 作成者が適切な選択を行った後、ST に記載されるそれらの選択に関連した付属書 C に記述された詳細な要件が選択されることになる。保証アクティビティは特定のプロトコルについて関連付けられているので、このコンポーネントには関連する保証アクティビティはない。

4.2.3 利用者データ保護（FDP）

FDP_RIP.2 全残存情報保護

FDP_RIP.2.1 TSF は、ある資源の以前の情報内容のすべてがすべてのオブジェクト［選択：への資源の割り当て、からの資源の解放］において利用不可能であることを確認しなければならない（shall）。

保証アクティビティ：
この要件の文脈における「資源」は、TOE を通して（セキュリティ管理者が TOE へ接続している場合とのように、「to」の反対の意味で） 送信されるネットワークパケットである。ネットワークパケットが一度送信されたならば、パケットが使用しているバッファまたはメモリエリアはそのパケットからのデータをまだ含んでおり、かつバッファが再利用された場合、それらのデータは残っているかもしれないし、新しいパケットへ道をあけるかもしれないという懸念がある。評価者は、TSS がネットワークパケットを処理する際にデータが再利用されないことを決定できるよう拡張についてのパケット処理を記述していることを確認するためチェックしなければならない（shall）。評価者は、以前のデータがどのようにゼロ化／上書きされるか、バッファ処理のどのポイントでこれが発生するかについて最低限の記述があることを確認しなければならない（shall）。

4.2.4 識別と認証（FIA）

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として、次のようなパスワード管理能力を提供しなければならない：

1. *パスワードは、アルファベットの大文字、小文字、数字、及び記号 （ “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, 及び “)” を含む ）の組み合わせから作られなければならない；*
2. *ミニマムなパスワード長は、セキュリティ管理者によって設定可能でなければならない、かつ 8 文字以上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文字列として要求される文字種と数について指定しているパスワード作成規則が、セキュリティ管理者によって設定可能でなければならない。*

   適用上の注意：この警告の意図は、セキュリティ管理者して可能であること、たとえば、パスワードは少なくとも 1 つの大文字、 1 つの小文字、 1 つの数字、及び 1 つの記号を含む；そして TOE は、この制約条件を実施する。「文字種」は、このエレメントの項目 1 にリスト化されたすべての文字種を参照する。

4. *パスワードは、セキュリティ管理者によって、最大の利用可能期間を定めなければならない。*
5. *新しいパスワードは、以前のパスワードから最低 4 文字以上変更されたものでなければならない。*

適用上の注意：最低 4 文字以上の変更を確実にするため、平文のパスワードを保存する必要はないことに注意すること、なぜなら、FIA_UAU.6 はパスワード変更の再に再認証を要求しているからである。「管理者パスワード」は、管理者によってローカルコンソールで使

用されるパスワードを参照する、またはパスワードをサポートする SSH や HTTPS 等のプロトコルを通して参照する。

保証アクティビティ：
評価者は、操作ガイダンスがセキュリティ管理者に対して強いパスワードの作成についてのガイダンスを提供していること、及び最小パスワード長の設定；パスワード作成規則の公式化や仕様、及び TOE におけるこれらの設定方法；及びパスワードの最大の利用可能期間の設定方法、に関する指示を操作ガイダンスが提供していることを決定するため、操作ガイダンスを検査しなければならない（shall）。評価者は、次のテストについても実施しなければならない。これらの 1 つ以上のテストが 1 つのテストケースで実施できることに注意すること。

- テスト 1： 評価者は、要件で指定されたとおり、TOE を異なるパスワード作成ルールで設定しなければならない（shall）。評価者は、その際規則のそれぞれのセットについて要件を満たすか、または満たせないかのいずれかのパスワードを何らかの方法で作成しなければならない（shall）。それぞれのパスワードについて評価者は、作成規則が実施されたことを検証しなければならない（shall）。評価者は、すべての可能な作成規則をテストすることは要求されていない（またはできそうにない）、評価者は、要件にリスト化され、サポートされている、すべての文字、規則の特性、及びミニマムな長さについて、テストのために選択した文字のサブセットとして相応しいものにしたうえで、テストしなければならない（shall）。
- テスト 2： 評価者は、操作ガイダンスに、パスワードの最大の利用可能期間の設定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。評価者は、この利用可能期間にいくつかの値を設定し、それらの値がそれぞれ実施されることを確認しなければならない（shall）。
- テスト 3： 評価者は、以前のパスワードから最低限 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（shall）。これは、複数のパスワードで実施しなければならない（shall）。

FIA_UIA_EXT.1　利用者識別及び認証

FIA_UIA_EXT.1.1　TSF は、利用者が識別及び認証される前に、利用者の代わりに実施するべき［選択：［割付：*TOE が提供するサービスのリスト*］、*サービスなし*］を許可しなければならない（shall）。

FIA_UIA_EXT.1.2　TSF は、利用者の代わりにその他すべての TSF 仲介アクションを許可する前にそれぞれの利用者に対して識別及び認証の成功を要求しなければならない（shall）。

適用上の注意： この要件は、TOE を通した接続によるサービスではなく、直接 TOE からのサービスを受ける利用者（管理者）に対して適用される。認証は、ローカルコンソール、またはパスワードをサポートするプロトコル（SSH 等）を通したパスワードベースであるか、または証明書ベース（SSH,TLS）で行われる。

FIA_UAU_EXT.5　拡張：パスワードベース認証メカニズム

FIA_UAU_EXT.5.1　TSF は、利用者認証を実施するため、［選択：［割付：*他の認証メカニズム*］、なし］によるローカルなパスワードベースの認証を提供しなければならない（shall）。

FIA_UAU_EXT.5.2　TSF は、パスワードの有効期限が切れた利用者が［選択：有効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ことを要求、管理者がパスワードをリセットするまでロックアウト］されることを確認しなければならない（shall）。

適用上の注意： ST 作成者は、RADIUS サーバのようにローカルではない認証メカニズムをサポートするような他の割付を行うことも可能である。もし外部の認証メカニズムがサポートされない場合、ST 作成者は選択において「なし」を選択するべきである（should）。

FIA_UAU.6　再認証

FIA_UAU.6.1　TSF は、以下の条件において利用者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：次の TSF 起動ロック（FTA_SSL）、［割付：その他の条件］］。*

保証アクティビティ：
評価者は、次のテストを実施しなければならない：

- テスト 1： 評価者は、操作ガイダンスによって指示されたようにパスワードの変更を試行しなければならない。試行の際に、評価者は最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にて認証の最中に利用者に対して*見えないフィードバック（Obscured feedback）*のみが提供されなければならない。

適用上の注意： 見えないフィードバック（Obscured feedback）は、（それぞれの文字をアスタリスク（＊）として）入力状況の表示が提供されるかもしれないが、TSF が（パスワードのエコーとして）利用者によって入力された認証データが目に見える表示を生成しないことを意味している。これは、認証データの表示を提供するかもしれない利用者に対して認証プロセスの間にいかなる情報も返さないことも意味している。

4.2.5　セキュリティ管理（FMT）

FMT_MTD.1　TSF データの管理（一般的な TSF データに関して）

FMT_MTD.1.1　TSF は、*セキュリティ管理者*に対して *TSF データを管理する*ための能力を制限しなければならない（shall）。

適用上の注意： 「管理する」という言葉は、作成、初期化、閲覧、デフォルトの変更、修正、削除、消去及び追加に限定しないことを含んでいる。（The word “manage” includes but is not limited to create, initialize, view, change default, modify, delete, clear, and append.） この要件は、TSF データの管理において可変な操作についての「デフォルト」要件となることを意図している；ここで、TSF データとは、FMT_MTD の他の繰り返しは異なる制約条件、または特別に識別された TSF データ等をさす。TSF データには暗号化の情報も同様に含むとともに、これらの管理は、例として、インタフェースを伴う暗号化プロトコルの連携動作を含む。

FMT_SMF.1　管理機能の特定

FMT_SMF.1.1　TSF は、次の管理機能を実施する能力を持っていなければならない：

- FIA_UIA.1 で指定されるようにあるエンティティが識別及び認証される前に、TOE サービスのリストをそれぞれ設定する能力。
- *暗号機能性を設定する能力。*

- *TOE を更新、及びデジタル署名能力（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化機能（または他の機能）］］を用いて更新を検証する能力。*

適用上の注意： 最低限、TOE は、管理者に対して信頼される発信元からの更新であることを検証する機能性を提供しなければならない；これはデジタル署名を用いて行われる。もし他のメカニズムが使用される場合、それらは割付において指定されるべきである；それ以外の場合、「他の機能なし」が選択されるべきである。使用される他のメカニズムが暗号化であれば、ST 作成者は FCS コンポーネントを用いてそれらが指定されていることを確認するべきであり、それらのコンポーネントが割り付けにおいて参照されていることを確認するべきである。

FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1 TSF は、役割を維持しなければならない：

- *［セキュリティ管理者、*
- *選択：［割付：他の管理者としての役割］、他の役割なし］］。*

適用上の注意：PP 作成者は、与えられた技術または能力（例えば、監査能力の包含は「監査者」役割の作成を要求するかもしれない）について適切な役割が追加されるべきである。FMT_MOF、FMT_MTF、及び FMT_MSA 要件はこのような場合における役割の能力を反映するために追加されなければならない。

FMT_SMR.1.2 TSF は、利用者を役割と関連付けることができるようにしなければならない。

4.2.6 TSF の保護（FPT）

FPT_ITT.1(1) 基本 TSF 内データ転送保護（漏洩）

FPT_ITT.1.1(1) **詳細化：**TSF は、**TSF 提供の暗号化サービス：［割付：*TSF データを漏洩から保護するために使用される FCS 指定のサービス*］**を通して TOE の別々の部分の間で送信される TSF データを漏洩から保護しなければならない。

適用上の注意： ST 作成者は、利用可能な暗号かサービスへの参照を割付の宣言に含める（例えば、IPsec が使用される場合、FCS_IPSEC_EXT への参照が求められる）。

FPT_ITT.1(2) 基本 TSF 内データ転送保護 （改ざん）

FPT_ITT.1.1(2) **詳細化：**TSF は、**TSF 提供の暗号化サービス：［割付：*TSF データの改ざんを検出するために使用される FCS 指定のサービス*］**を通して TOE の別々の部分の間で送信される TSF データの改ざんを検出しなければならない。

FPT_PTD.1(1) TSF データの管理 （認証データの読み出しに関して）

FPT_PTD.1.1(1) **詳細化：**TSF は、平文のパスワードの読み出しを防止しなければならない。

適用上の注意：この要件は、誰かが利用者に成りすましをしようとこのようなデータを読み出ししようとした場合、「通常の」インタフェースを通して TSF （非暗号化パスワード等） に対して利用者を直接識別するための認証データをどの利用者または管理者も読み出しできないことを意図している。もちろん、すべての強力な管理者は直接パスワードをキ

ャプチャーしたメモリを読み出すことができるかもしれないが、そのようなことはやらないと信じられている。同様に、システムは、認証プロセスの一部として利用者の公開鍵に信頼を置いている、鍵は認証データと考えられるが、鍵を読み出しできることはその利用者を危険にさらさないので、この要件を範囲以下には落とさないだろう。

保証アクティビティ：
評価者は、平文のパスワードが、適用上の注意に概説されているように、その目的のために特別に設計されたインタフェースを通して閲覧されることができないような方法で保存されていることを詳細に記述していることかどうかについてTSS を検査しなければならない。もし、パスワードが平文で保存されていない場合、TSS はパスワードがどのように保護されているかを記述しなければならない。

FPT_PTD.1(2)　TSF データの管理　（すべての対称鍵の読み出し　（Reading）　に関して）

FPT_PTD.1.1(2)　**詳細化**：TSF は、すべてのプリシェアード鍵、対称鍵、及びプライベート鍵の読み出しを防止しなければならない。

適用上の注意：この要件は、「通常の」インタフェースを通して　（保存された、または一時的に）　識別された鍵をどの利用者または管理者も読み出しできないことを意図している。もちろん、すべての強力な管理者は直接パスワードをキャプチャーしたメモリを読み出すことができるかもしれないが、そのようなことはやらないと信じられている。

保証アクティビティ：
評価者は、プリシェアード鍵、対称鍵、及びプライベート鍵が、適用上の注意に概説されているように、その目的のために特別に設計されたインタフェースを通して閲覧されることができないような方法で保存されていることを詳細に記述していることかどうかについてTSS を検査しなければならない。もし、これらの値が平文で保存されていない場合、TSS はどのようにそれらが保護／不可視化されているかを記述しなければならない（shall）。

FPT_RPL.1　リプレイ検出

FPT_RPL.1.1　TSF は、次のエンティティについてリプレイを検出しなければならない：［TOE において終端する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とき、［データの破棄］を実施しなければならない。

適用上の注意：　1 番目のエレメントは、高信頼であるという特性　（管理者から TOE へ、IT エンティティから TOE へ、TOE から TOE へ）　がエレメントによってカバーされており、リプレイ攻撃の対象でないような通信を意図している。

FPT_STM.1　高信頼タイムスタンプ

FPT_STM.1.1　TSF は、自身の利用のために信頼できるタイムスタンプを提供できなければならない。

拡張：高信頼アップデート（更新）（FPT_TUD_(EXT).1）

FPT_TUD_(EXT).1　拡張：高信頼アップデート　（更新）

FPT_TUD_(EXT).1.1　TSF は、セキュリティ管理者に TOE のファームウェア／ソフトウェアの現在のバージョンを問い合わせる能力を提供しなければならない。

FPT_TUD_(EXT).1.2　TSF は、セキュリティ管理者に TOE のファームウェア／ソフトウェアに対する更新を開始する能力を提供しなければならない。

FPT_TUD_(EXT).1.3　TSF は、それらの更新をインストールする前に［選択：デジタル署名メカニズム、公開されたハッシュ値］を用いて TOE のファームウェア／ソフトウェアを検証する手段を提供しなければならない。

適用上の注意：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(3) で指定されたうちの 1 つにより生成される。公開されたハッシュ値は、FCS_COP.1(2) で指定されたうちの 1 つにより生成される。本 PP の次の版において、デジタル署名が要求されるだろう。

保証アクティビティ：
TOE の更新は、それらとともに提供されるか、認証局により署名されて提供される。もし、デジタル署名が使用される場合、そのデバイスに含まれる更新検証メカニズムによってどのように証明書が利用されるかの記述を伴って、認証局の定義が TSS に含まれる。評価者は、TSS に含まれるこの情報を確認する。評価者は、また、TSS （または操作ガイダンス） にどのように更新の候補が入手できるか；更新についてのデジタル署名の検証またはハッシュ値の計算についての処理；成功 （ハッシュ値または署名が検証された） 及び失敗 （ハッシュ値または署名が検証されなかった） 場合にとるべきアクションについて記述されていることを確認する。評価者は、以下のテストを実施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施する。評価者は、操作ガイダンスに記述された手続きを用いて合法な更新を入手し、TOE がうまくインストールされたことを検証する。そして評価者は、想定どおり更新が動作することを論証するため、他の保証アクティビティのテストのサブセットを実施する。更新の後、評価者は再度バージョンの検証アクティビティを実施し、更新されたバージョンを検証する。
- 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バージョン検証アクティビティを実施する。評価者は、合法な更新を入手または購入し、TOE にそれをインストールしようと試みる。評価者は、TOE が更新を拒否することを検証する。

FPT_TST_EXT.1　TSF テスト

FPT_TST_EXT.1.1　TSF は、TSF の正しい動作を証明するため、初期スタートアップ（電源 ON）時にセルフテストを実行しなければならない。

保証アクティビティ：：
評価者は、スタートアップ時に TSF によって実行されるセルフテストを詳述していうことを確認するため、TSS を検査しなければならない。この記述は実際にどのようなテスト実行されるかを含めなければならない （例えば、「メモリがテストされた」というよりも、「メモリが各メモリのロケーションにある値を実際に書き込み、それを読み出して何が書き込まれたかを確認するテストを実施した」という表現を使用しなければならない）。評価者は、TSS においてテストが TSF の動作が正しいことを証明するに十分な論証がされていることを確認しなければならない。

4.2.7 資源利用（FRU）

FRU_RSA.1 最大割当て （Quotas）

FRU_RSA.1.1 TSF は、［選択：個人利用者、定義された利用者、サブジェクト］が［選択：同時に、指定された時間を越えて］利用できる次の資源：［割付：管理者インタフェースをサポートする資源］、［選択：［割付：制御された資源］、他の資源なし］の最大の割当てを実施しなければならない。

適用上の注意：最低限、適合 TOE は、リモート管理者インタフェースをサポートするために利用される枯渇しうる資源についての割当てを課さなければならない；これらは２番目の割付にリスト化されている。制御されうる他の資源 （例えば、TCP 接続資源） は、１番目の割付にリスト化される；もし選択されるべき最後の項目であり、他の資源がない場合。１番目の選択は制御されるべき資源の消費者を反映して選択されるべきである。2 番目の選択は、制御される資源の利用に関してのタイムフレームを制限するために使用される（例えば､30 秒間にある与えられた IP アドレスからの TCP 接続要求の数についての割当て等）。

4.2.8 TOE アクセス（FTA）

FTA_SSL_EXT.1 TSF 起動セッションロック

FTA_SSL_EXT.1.1 TSF は、ローカルな対話セッションについて、セキュリティ管理者指定の非アクティブである時間間隔後に、以下を実施しなければならない［選択：

- セッションをロックする – 利用者のデータへのアクセス／デバイスの表示等、セッションのアンロック以外のアクティビティを無効にして、セッションをアンロックする前に管理者が TSF への再認証を行うことを要求する；
- セッションを終了する］ 。

保証アクティビティ：
評価者は、次のテストを実施しなければならない：

- テスト 1： 評価者は、操作ガイダンスに従い、コンポーネントで参照される非アクティブである時間間隔にいくつかの異なる値を設定する。それぞれの設定された時間間隔について、評価者は TOE とのローカルな対話セッションを確立する。評価者は、設定された期間間隔後に、セッションがロックまたは終了されることを観察する。もし、ロックがコンポーネントから選択された場合、評価者はセッションをアンロックしようとするときに再認証が求められることを確認する。

FTA_SSL.3 TSF 起動による終了

FTA_SSL.3.1 **詳細化：**TSF は、 [セキュリティ管理者が設定可能なセッション非アクティブである時間間隔］後に、**リモート**な対話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：
評価者は、以下のテストを実施しなければならない：

- テスト 1： 評価者は、操作ガイダンスに従い、コンポーネントで参照されている非アクティブである時間のいくつかの異なる値を設定する。それぞれの設定された時間間隔について、評価者は TOE とのリモートな対話セッションを確立する。評価者は、設定された時間間隔の後、セッションが終了されることを観察する。

FTA_TAB.1　デフォルト TOE アクセス・バナー

FTA_TAB.1.1　**詳細化：利用者／管理者**セッションが確立する前に、TSF は、**セキュリティ管理者指定の** TOE の認可されない利用に関するアドバイザリー**通知及び合意**の警告メッセージを表示しなければならない。

適用上の注意：この要件は、人間の利用者と TOE の間の対話セッションに適用することをいとしている。通信を確立している IT エンティティまたはプログラム的な接続　（例えば、ネットワーク越しのリモートプロシージャコール）　は、この要件によってカバーされることを要求されない。

保証アクティビティ：
評価者は、TSS をチェックして、管理者が利用可能なアクセス方式　（ローカル及びリモート）　のそれぞれについて詳細　（例えば、シリアルポート、SSH、HTTPS 等）　が記述されているか確認しなければならない。評価者は、次のテストを実施しなければならない：

- テスト 1：　評価者は、操作ガイダンスに従い、通知や受諾警告メッセージを設定する。評価者は、TSS に指定されたアクセス方式ごとに TOE とのセッションを確立しなければならない。評価者は、それぞれのインスタンスで表示される通知や受諾警告メッセージを検証しなければならない。

4.2.9　高信頼パス／チャネル（FTP）

FTP_ITC.1(1)　TSF 間高信頼チャネル

FTP_ITC.1.1(1)　**詳細化：**TSF は、**認可された IT エンティティ**と TSF 自身との間の、他の通信チャネルと論理的に異なる**高信頼**通信チャネルを提供し、エンドポイントの確かな識別とチャネルデータの漏洩からの保護を提供するため、［割付：***FCS 指定サービス***］を使用しなければならない。

FTP_ITC.1.2(1)　**詳細化：**TSF は、TSF、***または認可された IT エンティティ*** が高信頼チャネルを経由して通信を開始することを許可しなければならない。

FTP_ITC.1.3(1)　TSF は、［*すべての認証機能*、［割付：*ピア間の保護された通信／プロトコル*］のための高信頼チャネルを経由した通信を開始しなければならない。

適用上の注意：ST 作成者は、高信頼チャネルを確立するために使うプロトコルの名称を割付に記載するべきである。この要件は、TOE が IT ピア　（VPN、ルータ更新、他）との通信を確立する場合について述べている。

FTP_ITC.1(2)　TSF 間高信頼チャネル

FTP_ITC.1.1(2)　**詳細化：**　TSF は、**認可された IT エンティティ**と TSF 自身との間の、他の通信チャネルと論理的に異なる**高信頼**通信チャネルを**提供**し、エンドポイントの確かな識別と**データの改ざんの検出**を提供するため、［割付：***FCS 指定サービス***］を使用しなければならない。

FTP_ITC.1.2(2)　**詳細化：**TSF は、TSF、***または認可された IT エンティティ*** が高信頼チャネルを経由して通信を開始することを許可しなければならない。

FTP_ITC.1.3(2)　TSF は、［*すべての認証機能*、［割付：*ピア間の保護された通信／プロトコル*］］のための高信頼チャネルを経由した通信を開始しなければならない。

適用上の注意：ST 作成者は、高信頼チャネルを確立するために使うプロトコルの名称を割付に記載するべきである。この要件は、TOE が IT ピア（VPN、ルータ更新、他）との通信を確立する場合について述べている。

FTP_TRP.1(1)　高信頼パス

FTP_TRP.1.1(1)　**詳細化：**TSF は、リモート管理者と TSF 自身との間の、他の通信経路と論理的に異なる通信経路を提供し、エンドポイントの確かな識別と通信データの漏洩からの保護を提供するため、［割付：***FCS 指定サービス***］を使用しなければならない。

FTP_TRP.1.2(1)　TSF は、リモート管理者に高信頼パスを経由した通信の開始を許可しなければならない。

FTP_TRP.1.3(1)　**詳細化：**TSF は、*すべてのリモート管理者アクション*について高信頼パスの使用を要求しなければならない。

FTP_TRP.1(2)　高信頼パス

FTP_TRP.1.1(2)　**詳細化：**TSF は、リモート管理者と TSF 自身との間の、他の通信経路と論理的に異なる通信経路を提供し、エンドポイントの確かな識別と**通信データの改ざんの検出**を提供するため、［割付：***FCS 指定サービス***］を使用しなければならない。

適用上の注意：詳細化は必要である、なぜなら TSF はデータが改ざんされることを防止するよう要求されていないから　（多くの場合、現実的でないため）；改ざんの検出で十分であるため。

FTP_TRP.1.2(2)　TSF は、*リモート管理者*に高信頼パスを経由した通信の開始を許可しなければならない。

FTP_TRP.1.3(2)　**詳細化：**TSF は、*すべてのリモート管理者アクション*について高信頼パスの使用を要求しなければならない。

4.3 セキュリティ保証要件

第 3 章の TOE のセキュリティ対策方針は、第 2 章で特定された脅威に対処するために構成された。4.2 節の SFR （セキュリティ機能要件） は、セキュリティ対策方針の正式な具体化である。PP は、評価者が評価を適用された文書を査定して独立テストを行う範囲を構成するために EAL1 セキュリティ保証要件（SAR）から集められた。

この節は、CC からの SAR の一式を含む一方、評価者によって行われた保証アクティビティについて、4.2 節とこの節の両方に詳述する。本 PP に適合すると書かれた ST に対する TOE を評価するための一般的なモデルは、次の通りである：
ST が評価で承認された後、CCTL（ Common Criteria Testing Laboratory：評価機関） が TOE を入手し、IT 環境や TOE に対する管理ガイダンスをサポートする。保証アクティビティは ST に載っており （CCTL によって、ST 内または別文書のいずれかとして TOE 特有のものとして詳細化されるであろう）、CCTL によって実行されるであろう。CCTL も EAL 1 の CEM によって義務付けられたすべての活動を期待されている。これらの活動の結果は報告され、（使われた管理ガイダンスと一緒に）評価用に提示される。

各保証ファミリに対して、開発者にとってどんな追加書類／活動が必要かを明確にするため、開発者アクション・エレメントに「開発者向け注意事項」が提供される。その内容／プレゼンテーション・エレメントや評価者アクティビティ・エレメントに対して、追加の保証アクティビティ （4.2 節と EAL1 の CEM に既に含まれる） は、各エレメントとしてではなく、ファミリとしてまとめて説明されている。さらに、この節に説明されている保証アクティビティは、4.2 節に詳述されているものを補完する。

TOE セキュリティ保証要件は表 2 に要約されているが、本 PP の第 2 章で特定された脅威を対処するのに必要な管理・評価アクティビティを特定する。

表 2：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記述
Development （開発）	ADV_FSP.1	基本機能仕様
Guidance Documents （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
Tests （テスト）	ATE_IND.1	独立テスト－適合
Vulnerability Assessment （脆弱性アセスメント）	AVA_VAN.1	脆弱性調査
Life Cycle Support （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 の CM 範囲

4.3.1 ADV クラス：開発

EAL1 では、TOE の情報は、エンドユーザが入手可能なガイダンス文書や ST の TSS 部分に含まれている。TOE 開発者が TSS を書く必要はない一方で、TOE 開発者は機能要件に関して TSS に含まれる製品の詳述に同意しなければならない。保証アクティビティは CEM と連動して 4.2 節に説明されているが、ST 執筆者が TSS 部分の適切な内容を決定し、十分な情報のもと提供しなければならない。

4.3.1.1 ADV_FSP.1 基本機能仕様

機能仕様は TSFI を記述している。EAL1 では、これらのインタフェースの正式で完全な仕様である必要はない。さらに、本 PP に適合する TOE は、TOE ユーザによって直接引き起こされるものではない運用環境のインタフェースが必要となり、EAL1 ではそのようなインタフェースの間接的テストのみが可能であるので、インタフェースを特定するにはあまり意味がない。本 PP は、このファミリのアクティビティが、機能要件に対する TSS に示されたインタフェースと AGD 文書に示されたインタフェースの理解にフォーカスすべきである。保証アクティビティを満たすための、追加の「機能仕様」書は必要ない。

評価される必要のあるインタフェースは、独立した抽象的なリストよりも、記載された保証アクティビティを行う必要のある情報を通して述べられる。

開発者アクション・エレメント：

ADV_FSP.1.1D　開発者は機能仕様を提供しなければならない。

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

開発者向け注意事項：　この章の序論で示した通り、機能仕様は、ST の TSS で提供される情報に加えて、AGD_OPE と AGD_PRE 文書で提供される情報から成り立っている。機能要件における保証アクティビティは関連文書と TSS 節に存在するべき証拠を指している ; なぜなら、それらが SFR と直接関連しているので、エレメント ADV_FSP.1.2D のトレース （追跡） は、既に暗黙的になされており、追加の文書化は必要ない。

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 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない。

ADV_FSP.1.2C　機能仕様は、SFR 実施及び SFR 支援に関連するすべてのパラメタを識別しなければならない。

ADV_FSP.1.3C　機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を示さなければならない。

ADV_FSP.1.4C　追跡は、機能仕様での TSFI に対する SFR の追跡を実証するものでなければならない。

評価アクション・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*（shall）。

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：
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、4.2 節に述べられた評価アクティビティや AGD、ATE、AVA セキュリティ保証要件に述べられた他のアクティビティを支援するために提供されている。機能要件に関する情報の内容についての要件は、遂行された他の保証アクティビティのおかげで暗黙的に評価されている。もし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遂行できなければ、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

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、運用環境がセキュリティ機能性における役割を果たすことができることを、権限のあるユーザが確認する方法についての記述を含まなければならない（must）。 文書は非公式であっても権限のあるユーザが読みやすいものであるべきである（should）。

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 をうまく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。

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の特定の要件は、4.2 節で指定されるような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（shall）。

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（should）。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を提供されだろう。**

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、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない（shall）。

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

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

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

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

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

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

評価アクション・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*（shall）。

保証アクティビティ：
操作ガイダンスの内容の中には、4.2 節の保証アクティビティと CEM に従った TOE の評価によって確証される。以下の追加情報も必要とする。

操作ガイダンスは最低限、ネットワーク・インタフェース上で受け取ったデータ（これらのうち 1 つ以上ありそうだが、ネットワーク・インタフェース上で“listens （リッスン）”するプロセスに限定されない）を処理できる操作の際に、評価された構成において TOE 上で動作している （または動作できた）プロセスをリストアップしなければならない。ネットワークデータを処理するプロセスだけを決定しようとする代わりに、評価された構成において TOE 上で作動作している （または動作できた）プロセスすべてをリストアップすれば許容できる。リストアップされたそれぞれのプロセスについて、管理者ガイダンスが処理機能や、サービスが動作する際の「特権」についての簡短な （例えば、1、2 行の） 記述を含んでいるだろう。「特権」というのは、ハードウェアの特権レベル （例えば、ring 0, ring 1） と、プロセスに特に関連したソフトウェア特権、及びプロセスが動作する際の利用者の役割に関連するあらゆる特権を含む。

操作ガイダンスは、TOE の評価された構成に関連した暗号エンジンの設定に関する指示を含まなければならない（shall）。それは、TOE の CC 評価において、他の暗号エンジンの使用については評価もテストも実施されていないということについて、管理者に対する警告を提供しなければならない（shall）。

1. *文書類には、ハッシュ値をチェックするか、またはデジタル署名を検証するかのいずれかによって、TOE への更新を検証するプロセスを記述しなければならない。評価者は、このプロセスが、後述するステップを含むか検証しなければならない*（must）*。ハッシュ値については、既知の更新用のハッシュ値がどこで入手可能かについての記述。デジタル署名については、証明書の所有者から受け取った署名済みの更新を確認するための、FCS_COP.1(2)メカニズムによって使用される証明書の入手の指示。これは、初めから製品と一緒に提供されるかもしれないし、他の方法で入手可能かもしれない*（may）。
2. *更新自体を入手するための指示。これは、TOE へアクセス可能な更新の指示を含むべきである（例えば、特定のディレクトリーの配置など）*（should）。
3. *更新のプロセスを開始するためとそのプロセスが成功したかどうかを見定めるための指示。これは、ハッシュ値／デジタル署名の生成を含む。*

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（shall）。

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（should）。

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 のセキュアな受入れに必要なすべてのステップを記述しなければならない（shall）。

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

評価アクション・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*（shall）。

AGD_PRE.1.2E 評価者は、TOE がセキュアな操作のために準備されることを確認するために準備手続きを*適用しなければならない*（shall）。

保証アクティビティ：
上記の序論で説明した通り、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時、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的確に ST の TOE を要求するすべてのプラットフォームに対処するか確認しなければならない（shall）。

4.3.3 ATE クラス：テスト

テストは、機能の観点とともに、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アウトプットの 1 つは、以下の要件の中に特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

テストは、TSS（TOE 要約仕様）に述べられた機能性や提出された管理文書（コンフィギュレーションや運用上も含む）を確認するために行われた。テストの焦点は、追加のテストが 4.3 節の SAR として特定されているが、4.2 節に特定された要件が満たされているかを確かめることである。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追加のテストアクティビティを識別する。評価者は、テスト計画や結果を実証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あ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（shall）。

内容とプレゼンテーション・エレメント：

ATE_IND.1.1C TOE はテストに適してなければならない（shall）。

評価アクション・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*（shall）。

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*（shall）。

保証アクティビティ：
評価者は、システムのテスト面を実証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、CEM に含まれるテストアクションすべてと本 PP の保証アクティビティの本体をカバーする。保証アクティビティに載っているテスト毎にテストケースが必要ではないが、評価者は ST の適切なテストの要件がカバーされていることがテスト計画に実証されていなければならない（must）。

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か議論されなければならない。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、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。

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状態として、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ーやツールを含むかもしれない（may）*。各ドライバーやツールに関して、ドライバーやツールが TOE の機能性やプラットフォーム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*（should）*。これは、使用される暗号エンジンの設定も含む。このエンジンに実装される暗号アルゴリズムは本 PP に特定されており、評価された暗号プロトコル（IPsec, TLS/HTTPS, SSH）で使われる。*

テスト計画は、ハイレベルのテストとこの目的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、テスト方法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、もしテストが不合格に終わったら、調整され、テストをうまく再試行し、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（shall）*。*

4.3.4 AVA クラス：脆弱性評定

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べ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配付されるまで、評価者は TOE のそれらの脆弱性をテストしないことが求められる。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類い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的な 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（shall）。

内容とプレゼンテーション・エレメント：

AVA_VAN.1.1C TOE はテストに適してなければならない（shall）。

評価アクション・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*（shall）。

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*（shall）。

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 が基本的な攻撃の可能性を持つ攻撃者による攻撃に抵抗するために、侵入テストを*実施しなければならない*（shall）。

保証アクティビティ：
ATE_IND と同様に、評価者はこの要件に関して、到達した結論を実証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ありうる。評価者は、一般的なネットワーク・インフラストラクチャー・デバイス中に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知の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報告書で見つかった脆弱性を実証する。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のキーコンビネーション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。もし、脆弱性の搾取することに、例えば、専門家のスキルと電子顕微鏡が必要となるならば、テストは適しておらず、適切な正当化の理由が説明されるべきである。

4.3.5 ALC クラス：ライフサイクル・サポート

本 PP に適合する TOE に適応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、エンドユーザ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、この保証レベルの評価に利用される情報の現れである。

4.3.5.1 ALC_CMC.1 TOE のラベル付け

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、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、エンドユーザが購入した際に容易に特定できる。

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（shall）。

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（shall）。

評価アクション・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*（shall）。

保証アクティビティ：
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 が含んでいるか確実にするために、ST を検査しなければならない（shall）。*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かを確認するために、AGD ガイダンスとテスト用に受け取った TOE サンプルを検査しなければならない*（shall）。*もしベンダが、TOE を宣伝するウェブサイトを維持していたら、ST の情報が製品を識別するのに十分かどうかを確実にするために、評価者はウェブサイトの情報を検証しなければならない*（shall）。

4.3.5.2 ALC_CMS.1 TOE CM カバレージ

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（shall）。

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（shall）。

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（shall）。

評価アクション・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（shall）。

保証アクティビティ：
本 PP の「セキュリティ保証要件が要求する評価証拠」とは、AGD 要件のもとで管理者やユーザ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 が明確に特定され、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。

根拠

脅威から対策方針へ、並びに対策方針から要件へトレースする根拠は、第 2 章及び第 3 章の文章に含まれている。未解決のマッピングのみが前提条件、組織のセキュリティ方針に関するもので、これらは以下の附属書 A に含まれている。

附属書 A：サポート表

本プロテクションプロファイルでは、ネットワークデバイスに対する脅威；それらの脅威を軽減するために用いられる手法；適合する TOE によって達成される脅威に対する軽減の度合いについての全般的な理解しやすさを向上させるため、本書の冒頭における議論の中心が物語風の説明で書かれている。この説明のスタイルは形式的な評価アクティビティにすぐに役立つものではないため、本附属書は本書に関連する評価アクティビティにおいて使用可能な表形式のものとして提供する。

前提条件

次の小節でリストアップされた特定の条件がTOEの運用環境において存在することが前提とされている。これらの前提条件はTOEセキュリティ要件の開発における現実的に実現するもの及びTOE使用時の必須の環境条件として含まれている。

PP 作成者は、特定の技術に関する前提条件が残っていること、表が適切なものとなるように修正されるべきであることを確実なものとしなければならない。

表 3：TOE 前提条件

前提条件の名称	前提条件の記述
A.NO_GENERAL_PURPOSE	TOEの操作、管理、サポートに必要なサービス以外に、TOEで利用可能な汎用コンピューティング能力（例えば、コンパイラーまたはユーザアプリケーション）がないことを前提とする。
A.PHYSICAL	TOE及び取り扱うデータの価値に見合った、物理的セキュリティが環境によって提供されていることを前提とする。
A.TRUSTED_ADMIN	TOE管理者は信頼された方法によって管理者ガイダンスすべてに従い適用すると信頼されている。

脅威

次の脅威は、本書に記述された要件を含むとき、PP による技術特有の脅威へ組み込まれるべきである。本書に記述された要件への修正、省略、及び追加はこのリストに影響を与えるかもしれない（may）ため、PP 作成者は適切となるようにこれらの脅威を修正または削除するべきである。

表 4：脅威

脅威の名称	脅威の定義
T.ADMIN_ERROR	管理者が、意図せずに、セキュリティメカニズムが有効に働かないような、インストールまたはTOEの誤った設定を行ってしまうかもしれない（may）。
T.RESOURCE_EXHAUSTION	プロセスまたは利用者がTOEの重要な資源の枯渇によってTOEのサービスへのアクセスを拒絶されるかもしれない（may）。
T.TSF_FAILURE	TOEのセキュリティメカニズムが、TSFのセキュリティ侵害を招き、うまく動作しないかもしれない。
T.UNDETECTED_ACTIONS	悪意のあるリモート利用者または外部のITエンティティが、TOEのセキュリティに悪影響するようなアクションを起こすかもしれない（may）。これらのアクションは、検出されずに留まるかもしれず（may）、その影響が有効に軽減することできない。
T.UNAUTHORIZED_ACCESS	利用者がTOEデータ及びTOE実行コードへ不正にアクセスできてしまうかもしれない（may）。悪意の利用者、または外部ITエンティティが、データまたはTOE資源に不正にアクセスするために、認可されたエンティティであると成りすますかもしれない（may）。悪意の利用者、プロセス、または外部ITエンティティが識別及び認証データを取得するため、TOE自身であると詐称するかもしれない（may）。
T.UNAUTHORIZED_UPDATE	悪意の人が末端利用者に対してTOEのセキュリティ機能を危険にさらすような製品の更新情報を提供しようとする。
T.USER_DATA_REUSE	利用者データが、不注意によって送信元の意図しない宛先に送信されるかもしれない（may）。

組織のセキュリティ方針

組織のセキュリティ方針は、セキュリティ上必要なものとして取り組むべき、組織に導入されている規則、慣習、及び手続の集まりである。PP 作成者は、特定の技術に適用するあらゆる方針が次の表に記述されていること、及び以下にリストアップされている方針が適用可能であることを確実にしなければならない（shall）。

表 5：組織のセキュリティ方針

方針の名称	方針の定義
P.ACCESS_BANNER	TOEは、TOEのアクセスによって利用者が同意する使用上の制限、法的合意、またはその他あらゆる適切な情報を記述している初期バナーを表示しなければならない（shall）。

TOE のためのセキュリティ対策方針

表 6：TOE のセキュリティ対策方針

TOE セキュリティ対策方針	TOE セキュリティ対策方針の定義
O.PROTECTED_COMMUNICATIONS	TOEは、管理者、分散型TOEの他の一部、認可されたITエンティティとの保護された通信チャネルを提供する。
O.VERIFIABLE_UPDATES	TOE は、TOE に対する更新が改変されていないこと、（オプションで）信頼される発信元からのものであること、を管理者がすべて検証できることの確認に役立つ能力（機能）を提供する。
O.SYSTEM_MONITORING	TOE は、監査データを生成し、そのデータを外部 IT エンティティへ送信する能力（機能）を提供する。
O.DISPLAY_BANNER	TOE は、TOE の使用に関するアドバイザリー警告を表示する。
O.TOE_ADMINISTRATION	TOE は、管理者だけがログインでき、TOE を設定できることを確認するメカニズムを提供し、ログインした管理者に対する保護を提供する。
O.RESIDUAL_INFORMATION_CLEARING	TOE は、資源が再割当てされるとき、保護された資源に含まれるいかなるデータも利用できないことを確実にする。
O.RESOURCE_AVAILABILITY	TOE は、TOE 資源が枯渇させるような利用者の攻撃を軽減するようなメカニズムを提供しなければならない。（たとえば、永続的なストレージ等）
O.SESSION_LOCK	TOE は、無視されたセッションがハイジャックされるようなリスクを軽減するメカニズムを提供しなければならない。
O.TSF_SELF_TEST	TOE は、セキュリティ機能性のサブセットについて正しく動作することを確認するためにテストする能力（機能）を提供する。

次の表は、運用環境の対策方針について記述する。前提条件が本 PP には追加されているので、これらの対策方針はこれらの追加を反映して論証されるべきである。

表 7：運用環境のセキュリティ対策方針

TOE セキュリティ対策方針	TOE セキュリティ対策方針の定義
OE.NO_GENERAL_PURPOSE	TOE で利用可能な一般的な目的の処理能力（例えば、コンパイラまたは利用者アプリケーション）はなく、もっぱら TOE をサポートするための運用や管理のために必要なサービスがある。
OE.PHYSICAL	TOE 及び TOE に含まれるデータの価値にふさわしい物理的セキュリティが環境によって提供されている。
OE.TRUSTED_ADMIN	TOE 管理者は信頼された方法ですべての管理者ガイダンスに従って適用するよう信頼されている。

附属書 B：NIST SP 800-53／CNSS 1253 マッピング

NIST SP 800-53/CNSS の 1253 管理策のいくつかは、適合 TOE によって十分にまたは一部分は対処される。本節は、取り上げられた要件を概説しており、TOE が運用構成に含まれるときに要求される追加のテストとしてどのようなものが要求されるか、もし必要なら認証に関係する人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。将来のベージョンでは、認証チームのための情報を提供できるように追加して述べる。この追加の情報は、TOE によって提供される適合の度合い（例えば、十分に管理策を満たす、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。この情報は、認証チームに対して、特定の管理策への適合の度合いを決定するために実施する必要がある追加のアクティビティ、もしあれば、どのようなものがあるかを示すだろう。

ST は選択の範囲までは選択できるので、割付を埋めて、ST が完成し評価されるまでは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、特定の実装に基づく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（認証要員）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、認証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	適用可能なセキュリティ機能要件
AC-3	アクセス制御の実施	FMT_MTD.1
AC-6	特権の最小化	FMT_MTD.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	監査対象のイベント	FAU_GEN.1
AU-2(4)	(4) 監査対象イベントリスト中の特権関数の実行	FAU_GEN.1
AU-3	監査記録の内容	FAU_GEN.1, FAU_GEN.2
AU-3(1)	(1) 種別、場所、サブジェクト毎に詳細な追加情報を含める機能を有する	FAU_GEN.1
AU-5	監査処理の不具合に対する対応	FAU_STG_EXT.3
AU-8	タイムスタンプ	FPT_STM.1
AU-10	否認防止	FCS_COP.1(2)
AU-12	監査生成	FAU_GEN.1
IA-2	ユーザ識別及び認証	FIA_UIA_EXT.1, FIA_UAU_EXT.5
IA-5	認証コードの管理	FIA_PMG_EXT.1
IA-6	認証コードのフィードバック	FIA_UAU.7
SC-4	共有リソースにおける情報	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, FPT_ITT.1(2), FTP_ITC_1(2)
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, FPT_ITT.1(1), FTP_ITC_1(1)
SC-10	ネットワークの切断	FTA_SSL.3
SC-11	高信頼経路	FTP_TRP.1(1), FTP_TRP.1(2)
SC-12	暗号鍵の確立と管理	FCS_CKM.1, FCS_CKM_EXT.4
SI-6	セキュリティ機能の検証	FPT_TST_EXT.1

附属書 C：追加の要件

この PP の本文に示される通り、管理者、（配付される）TOE の他の部分、または外部 IT エンティティの間の通信チャネルの情報漏えいに対して脅威を低減することができる。IPsec または SSH が TOE によって実装されなければならないが、両方とも実装してもよいし、IPsec と SSH のいずれかに追加して、TLS/HTTPS を実装してもかまわない。それぞれのプロトコル・スーツに関連した要件があるので、本 PP における追加要件の仕様は、紛らわしいし、問題がある。なぜなら追加要件の仕様は CC によってサポートの準備ができていないからである。できるだけ明確にこの状況を述べるために、次のような要件が FCS_COMM_PROT_EXT.1 コンポーネントの選択に依存する ST に含めるべきである。
行われる選択に依存して ST のはじめで語られる情報へのマイナーな調整が要求されることに注意すること。さらに、選択された要件に依存時、C1.2 節の監査対象事象からの適切な情報は、ST における監査対象事象の表に追加される必要があるだろう。

C1.1 要件

FCS_IPSEC_EXT.1　Explicit: IPSEC

FCS_IPSEC_EXT.1.1　TSF は、暗号アルゴリズム AES-CBC-128、AES-CBC-256（両方とも RFC3602 で指定される）、[選択：他のアルゴリズムなし、RFC4106 で定義される AES-GCM-128、RFC4106 で指定される AES-GCM-256］を用いた RFC4303 で定義されるような ESP プロトコル、及びセキュリティ・アソシエーションを確立するために RFC2407、RFC2408、RFC2409 及び RFC4109 で指定される IKEv1；［選択：他の手法なし、RFC4306、RFC4307 で定義される IKEv2］を用いた IPsec を実装しなければならない（shall）。

適用上の注意：この PP の次の公開において、AES-GCM が必須となり、CBC はオプションとなるだろう。同様に IKEv2 のサポートは必須となり、IKEv1 サポートはオプションとなるだろう。

AES-CBC-128 及び AES-CBC-256 のサポートが上記では要求されている; AES-GCM-128 または AES-GCM-256 がサポートされる場合、適切な選択が行われるが、それ以外の場合の選択は「他のアルゴリズムなし」となる。

IKEv1 及び／または IKEv2 のついてのこの要件を詳細化するために RFC4868 をオプションとして主張するハッシュアルゴリズムとして含むことは許容される。もしそうなら、ST 作成者は FCS_COP.1(3) をそれに応じて修正するべきである。

IKEv1 のサポートが上記で要求されおり、もし IKEv2 がサポートされる場合、それが選択さるべきであり、それ以外は「他の手法なし」が選択される。

ST 作成者は、適切な選択及び割付を行い、IPsec 実装に反映しなければならない。ST 作成者は、識別された規格にどのように適合するか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対してエレメントを追加するか、TSS に詳細を追加するかによって行うことができる。

HMAC-SHA-1 は、RFC によって CBC モードの IKE 実装によるハッシュアルゴリズムとして要求されている。他のハッシュアルゴリズムが主張される場合、要件または TSS 節はそれらのアルゴリズムを識別しなければならず、かつ適切な選択が FCS_COP.1(4) で行われる必要がある。
IKEv1 について、上記要件は RFC4109 で記述されるように追加／修正された RFC2409 に適合している IKE 実装を要求しているものとして解釈されるものである。

アルゴリズム・スーツB（RFC 4869）は、実装上望ましいアルゴリズムである。

FCS_IPSEC_EXT.1.2　TSF は、IKEv1 Phase 1 交換がメインモードのみを使用することを確実にしなければならない（shall）。

保証アクティビティ：
評価者は、TSS を検査し、「秘匿性のみ」の ESP モードがどのように無効になっているかが記述されているかを検証しなければならない。評価者は、操作ガイダンスを検査し、「秘匿性のみ」モードが無効であること、及びトンネルモードがパケット全体を保護できるので望ましいESP モードであるということを示すアドバイザリーが存在することを確実にするために必要な、いずれの設定が記述されているかを決定しなければならない（shall）。

評価者TOE でサポートされるIPsec プロトコルの記述において、以下を確実にするためにTSS を検査しなければならない（shall）。アグレッシブモードがIKEv1 フェーズ１交換で使用されないこと、及びメインモードのみが使用されることが記述されていること。もし、操作の前にTOE の設定が要求される場合、評価者は、この設定のための指示が操作ガイダンスに含まれていることを確実にするために操作ガイダンスをチェックしなければならない（shall）。評価者以下のテストも実施しなければならない：

- テスト 1：評価者は、操作ガイダンスで指示されているとおり TOE を設定し、アグレッシブモードで IKEv1 フェーズ 1 接続を用いて接続を確立しようと試みなければならない（shall）。この試みは失敗するだろう。そのとき、評価者はメインモード交換がサポートされることを示すべきである。
- テスト 2：評価者は、操作ガイダンスで指示されているとおり TOE を設定し、「秘匿性のみ」モードで ESP を用いて接続を確立しようと試みなければならない（shall）。この試みは失敗するだろう。そのとき、評価者は、秘匿性及びインテグリティモードで ESP を用いて接続を確立しなければならない（shall）。

FCS_IPSEC_EXT.1.3　TSF は、IKEv1 SA ライフタイムが、フェーズ１ SA については 24 時間以内、フェーズ２ SA については 8 時間以内に制限可能であることを確実にしなければならない（shall）。

適用上の注意：上記要件は、セキュリティ管理者が設定可能なライフタイム（必須の項目として、AGD_OPE によって要求される文書における妥当なFMT 要件を伴って）提供されるか、または実装における「ハードコーディング」された制限のいずれかによって達成される。

保証アクティビティ：
評価者は、IKEv1 SA（フェーズ１及びフェーズ２の両方）についてのライフタイムの確立方法についてTSS に記述されていることを確実にするためチェックしなければならない（shall）。それらが設定可能な場合、評価者はこれらの値を設定するための適切な指示が操作ガイダンスに含まれることを検証する。評価者は次のテストについても実施する：

- テスト 1：評価者は、フェーズ 1 SA が確立され、再ネゴシエートされる前に 24 時間以上維持されるようなテストを構築しなければならない（shall）。評価者は、この SA が終了されるか、24 時間以内に再ネゴシエートされることを観察しなければならない（shall）。このようなアクションが TOE が特別な方法で設定されることを要求する場合、評価者は、TOE の設定能力が操作ガイダンスに文書化されているとおり動作することを実証するテストを実施しなければならない（shall）。

- テスト 2：評価者は、ライフタイムが 24 時間の代わりに 8 時間になるようなものを除いて、フェーズ２ SA についてテスト 1 と同様のテストを実施しなければならない（shall）。

FCS_IPSEC_EXT.1.4　TSF は、IKEv1 SA ライフタイムがフェーズ２ SA についてのトラフィック[割付：100-200 の間の数]MB に制限可能であることを確実にしなければならない（shall）。

適用上の注意：上記の要件は、上記要件は、セキュリティ管理者が設定可能なライフタイム(AGD_OPE によって必須なものとして要求される文書における妥当な FMT 要件を伴って）提供されるか、または実装における「ハードコーディング」された制限のいずれかによって達成される。ST 作成者は、要件によって指定された範囲のデータ量を選択する。

一般的に、SA のライフタイムを含めて、実装上のパラメタの設定についての指示は、FMT 要件を通して指定されるべきであり、AGD_OPE について生成された管理者ガイダンスに含まれるべきである（should）。

保証アクティビティ：
評価者は、IKEv1 フェーズ２ SA のライフタイムが、与えられた SA を用いて許されるフローのトラフィック量ごとに、どのように確立されるかが TSS に記述されていることを確実にするためにチェックする。その値が設定可能な場合、評価者は操作ガイダンスに含まれるこれらの値の設定に関する指示が妥当であることを検証する。評価者は次のテストも実施する：

- テスト 1：評価者はフェーズ 2 SA が確立され、上記割付で指定されたデータよりも多くのデータが接続（コネクション）越しに流れているのを維持しようと試みるようなテストを構築しなければならない（shall）。評価者はこの SA が終了するか、指定されたデータ量を超える前に再ネゴシエーションが行われることを観察しなければならない（shall）。このようなアクションが、特定の方法で TOE が設定されることを要求する場合、評価者は TOE の設定能力が操作ガイダンスに文書化されているように動作することを実証するテストを実施しなければならない（shall）。

FCS_IPSEC_EXT.1.5　TSF は、すべての IKE プロトコルが DH Groups 14 (2048-bit MODP)、及び [選択：24 (2048-bit MODP with 256-bit POS)、19 (256-bit Random ECP)、20 (384-bit Random ECP)、[割付：TOE によって実施されるその他の DH groups]、その他の DH groups なし] を実行することを確実にしなければならない（shall）。

適用上の注意：　上記は、TOE が DH Group 14 をサポートすることを要求している。その他の Groups がサポートされている場合、それらは、（groups 24、19 及び 20 から）選択されるか、または上記割付で指定されるかしなければならない; それ以外は、「その他の DH groups なし」が選択されるべきである。これは IKEv1 に対して適用され、（もし実装されていれば）IKEv2 交換にも適用される。

本 PP の将来の発行において、DH Groups 19 (256-bit Random ECP) 及び 20 (384-bit RandomECP) が要求されるだろう。

保証アクティビティ：
評価者は、TSS においてサポートされているとおり、要件において指定された DH Groups がリストアップされていることを確実にするためにチェックしなければならない（shall）。それらが、ひとつ以上の DH group をサポートしている場合、評価者は、特定の DH group が通信相手との間で指定／ネゴシエートされる方法について TSS に記述されていることを確実にするためにチェックする。評価者は次のテストについても実施しなければならない：

- テスト 1：それぞれのサポートされている DH group について、評価者は、すべての IKE プロトコルが特定の DH group を用いて成功裏に完了できることを確実にするためにテストしなければならない（shall）。

FCS_IPSEC_EXT.1.6　TSF は、すべての IKE プロトコルが［選択：DSA、rDSA、ECDSA］アルゴリズムを用いて Peer Authentication を実行することを確実にしなければならない（shall）。

適用上の注意：選択されたアルゴリズムは FCS_COP.1(2)についての適切な選択に対応するべきである（should）。

保証アクティビティ：
評価者は、TSS が、TOE で用いられる IKE peer authentication プロセスの記述を含んでいること、及びこの記述が要件で指定されているアルゴリズムまたは署名アルゴリズムの仕様を含んでいることをチェックしなければならない（shall）。評価者は、次のテストについても実施しなければならない（shall）。

- テスト 1：それぞれのサポートされている署名アルゴリズムについて、評価者は、そのアルゴリズムを用いた peer authentication が成功裏に達成できることをテストしなければならない（shall）。

FCS_IPSEC_EXT.1.7　TSF は、IPsec 接続の認証おいて使用するプリシェアード鍵（RFCs において参照されているとおり）の仕様をサポートしなければならない（shall）。

保証アクティビティ：
評価者は、TSS が、どのようにプリシェアード鍵が確立され、IPsec 接続の認証で使用されるかを記述していることを確実にするために検査しなければならない（shall）。評価者は、TOE においてプリシェアード鍵がどのように生成及び確立されるべきであるかについて操作ガイダンスに記述されていることをチェックしなければならない（shall）。TSS 及び操作ガイダンスにおける記述は、単にプリシェアード鍵を使用する TOE と同様に、両方の TOE において、どのようにプリシェアード鍵の確立が達成されるかについても示していなければならない。評価者は、次のテストも実施しなければならない：

- テスト 1：評価者は、操作ガイダンスに示されるとおり、プリシェアード鍵を生成し、ピア間における IPsec 接続を確立し、使用しなければならない（shall）。もし、TOE がプリシェアード鍵の生成をサポートしている場合、評価者は、鍵を単に取り込んで使用する TOE のインスタンスと同様に、鍵生成する TOE のインスタンスについても、鍵の確立が実行されることを確実にしなければならない（shall）。

FCS_IPSEC_EXT.1.8　TSF は以下をサポートしなければならない（shall）：

1. *プリシェアード鍵は、大文字、小文字、数字、及び記号の組み合わせにより構成されることが可能でなければならない（shall）（以下の記号を含む：“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, 及び “)”）；*
2. *22 文字、及び［選択：［割付：その他のサポートされた長さ］、その他の長さ無し］のプリシェアード鍵。*

適用上の注意：　プリシェアード鍵については、通常 22 文字の長さが相互接続性を推進するために要求される。もし、ほかの長さがサポートされる場合、それらは、割付にリストアップされるべきであり、この割付は値の範囲についても指定することが可能である（例えば、「５から５５文字の長さ」）のように。

保証アクティビティ：
評価者は、操作ガイダンスにおいて、強い鍵の生成や許可された文字セットに関するガイダンスを含み、プリシェアード鍵の生成について記述されていることを確実にするためチェックしなければならない（shall）。評価者は、要件を満たさないようなプリシェアード鍵の制限をこのガイダンスが行っていないかチェックしなければならない（shall）。管理者が（操作ガイダンスに違反して）要件に適合しないような鍵を選択できたり、このコンポーネントに指定されたルールを満たすことを確実にするためにTOE が鍵をチェックするというような要件がなかったりすることについて注意されるべきである（should）。しかし、管理者は上記のルール（及び操作ガイダンス）に従ったパスワードを生成するよう選択するべきである：TOE はこの選択を禁止しないようにするべきである。評価者は次のテストについても実施しなければならない（shall）；これは、FCS_IPSEC_EXT.1.7 の Test 1 との組み合わせになるかもしれない：

- テスト 1： 評価者は、上記生成要件に適合する 22 文字長のプリシェアード鍵を生成しなければならない（shall）。評価者は、この鍵を使って IPsec 接続を成功裏に確立しなければならない（shall）。評価者がサポートされた要件にリストアップされた記号または長さのすべてについてテストすることは要求されていないが、もしサブセットが実際に使用される場合は、テストで選択される文字のサブセットに調整することが要求されている。

FCS_TLS_EXT.1　Explicit: TLS

FCS_TLS_EXT.1.1　TSF は、次のサイファー・スーツ （cyphersuites） をサポートしている次のプロトコルの一つ以上を実装しなければならない（shall） ［選択：TLS 1.0 （RFC2346）、TLS 1.1 （RFC4346）、TLS 1.2 （RFC5246） ］。

Mandatory Ciphersuites:
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

Optional Ciphersuites:
[selection:
None
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： ST 作成者は、TLS 実装を反映した適切な選択及び割付を行わなければならない（must）。ST 作成者は、実装がどのように識別された規格に適合しているかを決定するために十分な詳細情報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か、TSS に詳細情報を追加する方法によって行うことができる。

評価された構成で使用されるべきサイファースーツ （ciphersuites） は、この要件によって制限される。ST 作成者は、サポートされるオプションのサイファースーツを選択するべき

である（should）；もし必須のスーツ以外のサイファースーツがない場合は、「なし」が選択される。もし実装によってネゴシエートされるスーツがこの要件において制限されように管理ステップが取られる必要がある場合、適切な指示がAGD_OPE によって求められるガイダンスに含まれる必要がある。

上記にリストアップされているスーツB アルゴリズム（RFC5430）は、実装が推奨されうアルゴリズムである。本PP の将来の版は、TLS 1.2（RFC5246）のサポートを要求するだろう。さらに、本PP の将来の版では、特定の古いバージョンのSSL／TLS プロトコルを用いたすべての接続の試行を拒否する手段をTOE が提供することを要求するだろう。

保証アクティビティ：
評価者は、オプションのcharacteristics （例えば、拡張サポート、クライアント認証サポート）が指定されていること、及びサイファースーツ・サポートが同様に指定されていることを確実にするためにＴＳＳにこのプロトコルの実装の記述をチェックしなければならない（shall）。評価者は、指定されたサイファースーツがこのコンポーネントに地ストアップされたものと識別可能であることを確実にするためTSS をチェックしなければならない（shall）。評価者は、TLS がTSS における記述（例えば、TOE によって広告されるサイファースーツのセットが要件に適合するよう制限されなければならないかもしれないような記述）に適合するように、TOE を設定する際の指示が操作ガイダンスに含まれていることを確実にするため操作ガイダンスをチェックしなければならない（shall）。評価者は、次のテストについても実施しなければならない（shall）：

- テスト 1： 評価者は、要件で指定されたサイファースーツのそれぞれを用いてTLS 接続を確立しなければならない。この接続は、より高いレベルのプロトコル、例えば、HTTPS セッションの一部として、確立されなければならないかもしれない。テストの意図を満足するようなサイファースーツのネゴシエーションに成功したことを（有線で）観測すれば十分である；使用されているサイファースーツ（例えば、暗号アルゴリズムが 128 ビットの AES で 256 ビットの AES でない場合）を見定めようとする試みにおいて暗号化されたトラフィックを検査することは必要ではない。

FCS_SSH_EXT.1　Explicit: 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（shall）。

適用上の注意： ST 作成者は、実装が識別された規格にどのように適合しているかを決定するために十分に詳細な情報を提供しなければならない（must）；これは、このコンポーネントへエレメントを追加すること、またはTSS に詳細な追加を行うことのいずれかによって得られる。

FCS_SSH_EXT.1.2　TSF は、SSH 接続がその鍵を使った 228 パケット以上の送信において鍵の更新が行われることを確実にしなければならない（shall）。

保証アクティビティ：
評価者は、TOE が与えられた鍵で228 パケット以上送信される前にSSH 接続で鍵を更新することをTSS が指定していることを確実にするため、TSS を検査しなければならない（shall）。もし、この効果がTOE の設定によって達成される場合、評価者は適切な値の設定についての指示が操作ガイダンスに含まれていることを確実にするために操作ガイダンスを検査しなければならない（shall）。

FCS_SSH_EXT.1.3　TSF は、SSH プロトコルが RFC 4252 の［割付：タイムアウト間隔］に定義されているように認証のタイムアウト間隔を実装していること、及び 1 回のセッションにおける［割付：最大試行回数］の試行においてクライアントが行う可能性のある認証失敗試行回数に対する制限を提供していることを確実にしなければならない（shall）。

適用上の注意： 最初の割付では、ST 作成者は、認証が不成功の場合にセッションがタイムアウトするべき時間の後、認証セッションの開始からのタイムアウト間隔（例えば、「10 分」）を入れるべきである（should）。2 番目の割付では、最大認証失敗試行回数が指定される。RFC はこの失敗した試行回数の後、サーバーはセッションを落とすべきであると指示している。

保証アクティビティ：
評価者は、要件にて指定された認証失敗試行回数の後、セッション接続を落とすためのタイムアウト間隔及び手法を TSS が指定していることを確実にしなければならない（shall）。これらの値が設定可能で、かつセキュリティ管理者によって指定されうる場合、評価者は、これらの値の設定についての指示が操作ガイダンスに含まれていることを確実にするために操作ガイダンスをチェックしなければならない（shall）。評価者は次のテストについても実施しなければならない（shall）：

- テスト 1：評価者は、現在のセッションの切断における TOE の結果に対する認証のためのタイムアウト間隔よりも長い時間をかけて、評価者が接続試行のための新しいセッションを開始する必要がある状態で検証しなければならない（shall）。タイムアウト間隔が設定可能である場合、評価者は指定されたメカニズムが動作することを確実にするため、少なくと２つの異なる間隔で、操作ガイダンスにしたがって実装されていることを確実にしなければならない（shall）。
- テスト 2：評価者は、現在のセッションを切断するための要件に指定された値と等しい SSH 認証失敗試行回数実施して、評価者が接続のための新しいセッションの試行を求められることを実証しなければならない（shall）。この回数が設定可能な場合、評価者は、指定されたとおりメカニズムが動作することを確実にするために、少なくとも２つのことなる制限（例えば、3 回の試行と 5 回の試行）にて操作ガイダンスにしたがって実装されていることを確実にしなければならない（shall）。

FCS_SSH_EXT.1.4　TSF は、 SSH プロトコル実装が RFC 4252 において、記述されている次の認証手法をサポートしていることを確実にしなければならない（shall）：公開鍵ベース、パスワードベース。

保証アクティビティ：
評価者は、TSS が FCS_SSH_EXT.1.7 に適合するリストとして認証のために使用可能な公開鍵アルゴリズムの記述を含んでいること、及びパスワードベース認証手法も許可されていることを確実にするためにチェックしなければならない（shall）。評価者は、次のテストについても実施しなければならない：

- テスト 1：評価者は、サポートされている公開鍵アルゴリズムのそれぞれについて、TOE がユーザ接続を認証するための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（shall）。このテストをサポートするために必要なあらゆる設定アクティビティは、操作ガイダンスにある指示にしたがって実施されなければならない（shall）。
- テスト 2：操作ガイダンスを使用して、評価者はパスワードベース認証を許可するため TOE を設定しなければならない（shall）、またユーザが認証コードとしてパスワードを用いて SSH 越しに TOE と認証を成功することができることを実証しなければならない（shall）。

FCS_SSH_EXT.1.5　TSF は、RFC 4253 に記述されているとおり、SSH トランスポート接続における[割付:バイト数]以上のパケットが廃棄されることを確実にしなければならない(shall)。

適用上の注意： RFC 4253 は、「大きなパケット」の許可について「妥当な長さ」のパケットであるかまたは廃棄するべきパケットかについての注意を提供している。割付は、TOE における「妥当な長さ」を定義することによって、ST 作成者によって最大許容パケットサイズが記入されるべきである（should）。

保証アクティビティ：
評価者は、RFC 4253 における「大きなパケット」がどのように検出され、取り扱われるかを TSS が記述していることをチェックしなければならない（shall）。評価者は次のテストについても実施しなければならない（shall）：

- テスト 1： 評価者は、TOE がこのコンポーネントで指定されたよりも長いパケットを受信した場合、パケットが廃棄されることを実証しなければならない(shall)。

FCS_SSH_EXT.1.6　TSF は、SSH トランスポート実装が、次の暗号アルゴリズムを用いていることを確実にしなければならない（shall）： AES-CBC-128、AES-CBC-256、［割付：AEAD_AES_128_GCM、 AEAD_AES_256_GCM、他のアルゴリズムなし］。

適用上の注意： 本 PP の次の公開において、AES-GCM が必須となり、CBC がオプションとなるだろう。割付において、ST 作成者は AES-GCM アルゴリズム、またはもし AES-GCM がサポータされていない場合は「他のアルゴリズムなし」を選択することができる。AES-GCM が選択された場合、ST において関連する FCS_COP の項目が存在するべきである（should）。

保証アクティビティ：
評価者は、オプション機能が指定されていること、及びサポートされている暗号アルゴリズムが指定されていることについても同様に確実にするため、TSS におけるこのプロトコルの実装に関する記述をチェックしなければならない（shall）。評価者は指定された暗号アルゴリズムがこのコンポーネントでリストアップされているものと同一であることを確実にしなければならない。評価者は、SSH が TSS における記述に適合できるように（すなわち、TOE によって広告される一連のアルゴリズムは要件を満たすよう制限されなければならないかもしれない）、操作ガイダンスが TOE の設定に関する指示を含んでいることを確実にするためチェックしなければならない（shall）。評価者は、次のテストについても実施しなければならない（shall）：

- テスト 1 : 評価者は、要件によって指定される暗号アルゴリズムそれぞれを用いて SSH 接続を確立しなければならない（shall）。テストの意図を満たすためには、プロトコルのネゴシエーションに成功することを(LAN 上で)観測すれば十分である。

FCS_SSH_EXT.1.7　TSF は、SSH トランスポート実装が、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］を使用することを確実にしなければならない（shall）。

適用上の注意： RFC 4253 は、必須及び許容される公開鍵アルゴリズムを指定している。この要件は SSH-RSA「必須」かつ ST で主張されるべき２つの他のアルゴリズムを許可している。ST 作成者は、もし SSH-RSA のみが実装されている場合「他の公開鍵アルゴリズムなし」が選択されるように、適切な選択を行うべきである。

保証アクティビティ：
FCS_SSH_EXT.1.4 に関連する保証アクティビティは、この要件を検証する。

FCS_SSH_EXT.1.8　TSF は、SSH トランスポート接続において使用するデータインテグリティアルゴリズムが［選択：hmac-sha1、hmac-sha1-96、hmac-md5、hmac-md5-96］であることを確実にしなければならない（shall）。

保証アクティビティ：
評価者は、サポートされているデータインテグリティアルゴリズムをリストアップしていること、及びそのリストがこのコンポーネントのリストに対応していることをチェックしなければならない（shall）。評価者は、許可されているデータインテグリティアルゴリズムのみが TOE との SSH 接続で使用されること（特に「非」MAC アルゴリズムは許可されていないこと）をどのように確実にするかについての管理者向けの指示を操作ガイダンスに含んでいることを確実にするため、操作ガイダンスをチェックしなければならない（shall）。

FCS_SSH_EXT.1.9　TSF は、diffie-hellman-group14-sha1 が SSH プロトコルで使用される唯一許可された鍵交換手法であることを確実にしなければならない（shall）。

保証アクティビティ：
評価者は、操作ガイダンスが DH group 14 を用いて SSH のためのすべての鍵交換が実施されるように TOE をセキュリティ管理者が設定することを許可するような設定情報を含んでいることを確実にしなければならない（shall）。もしこの能力が TOE に「ハードコードされて」いる場合、評価者は、SSH プロトコルの議論において記述されていることを確実にするために TSS をチェックしなければならない（shall）。評価者は次のテストについても実施しなければならない（shall）：

- テスト 1：評価者は、diffie-hellman-group1-sha1 鍵交換を実施しようと試行しなければならない（shall）、そしてその試行が失敗することを観察しなければならない（shall）。評価者は、diffie-hellman-group14-sha1 鍵交換の実施を試行して、その試行が成功することを観察しなければならない（shall）。

FCS_HTTPS_EXT.1　Explicit: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（shall）。

適用上の注意： ST 作成者は、実装が識別された規格にどのように適合するかを決定するために十分な詳細情報を提供しなければならない（must）；これは、このコンポーネントにエレメントを追加したり、TSS に詳細を追加したりすることによって実施することができる。

FCS_HTTPS_EXT.1.2　TSF は、FCS_TLS_EXT.1 で指定されているように TLS を用いた HTTPS を実装しなければならない（shall）。

保証アクティビティ：
評価者は、TLS プロトコルによって要求されるクライアント認証、対、処理スタックの異なるレベルで実施されるかもしれないセキュリティ管理者認証に焦点を当てて、TSS が管理者セッションを確立するために HTTPS がどのように TLS を使用するかを明確にしていることを確実にするため、TSS をチェックしなければならない（shall）。このアクティビティに関するテストは TLS テストの一部として実施される；これは、TLS プロトコルレベルで TLS テストが実施される場合、テストが追加されることになる。

C1.2 監査対象事象

C1.1 節より ST 作成者によって選択された特定の要件に依存して、ST 作成者は、ST の関連する表に、選択された要件について適切な監査対象事象を含めるべきである（should）。

機能要件	監査対象事象	追加の監査記録内容
FCS_IPSEC_EXT.1	IPsec 確立の失敗。 IPsec SA の確立／終了。	失敗の理由。 成功及び失敗に関する非 TOE の接続先（IP アドレス）。
FCS_TLS_EXT.1	TLS セッション確立の失敗。 TLS セッションの確立／終了。	失敗の理由。 成功及び失敗に関する非 TOE の接続先（IP アドレス）。
FCS_SSH_EXT.1	SSH セッション確立の失敗。 SSH セッションの確立／終了。	失敗の理由。 成功及び失敗に関する非 TOE の接続先（IP アドレス）。
FCS_HTTPS_EXT.1	HTTPS セッション確立の失敗。 HTTPS セッションの確立／終了。	失敗の理由。 成功及び失敗に関する非 TOE の接続先（IP アドレス）。