Security Requirements for Network Devices

ネットワーク・デバイスのセキュリティ要件

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を検討するため、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_v1.1.pdf

Information Assurance Directorate

NSA 情報保証局

08 June 2012
2012 年 6 月 8 日
Version 1.1
バージョン 1.1

平成 24 年 12 月 5 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

目次

表一覧

改訂履歴

バージョン	日付	摘要
1.0	2010 年 12 月 10 日	初版リリース
1.1	2012年　6月　8日	コミュニティレビュー及び製品評価の適用からのコメントによるアップデート

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。

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セクション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 : 補足表は、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、更に 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中間者攻撃(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ータの設定ミス、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。

更に、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

セクション 2.1 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。更に、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]

2.6 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、更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、更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

セクション 2.1「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、ST において指定された選択のすべてをサポートしなければならないが、追加のアルゴリズムやプロトコルをサポートしてもよい。もしそれらの付加的なメカニズムが評価されない場合、ガイダンスにより、それらが評価されていないという事実を管理者に対して明確にする説明を提供しなければならない。

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、セクション 2.1 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。
(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,
FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1, (FCS_IPSEC_EXT.1, FCS_SSH_EXT.1,
FCS_TLS_EXT.1, FCS_HTTPS_EXT.1), (FPT_ITT.1(1),
FPT_ITT.1(2)))[1]

[1] ST 作成者は、附属書 C よりどちらが選択されたかにより FTP_ITC.1 及び FTP_TRP.1 をサポートするコンポーネントのリストを適用するべきである(should)。同様に、FPT_ITT の繰り返しは、TOE が提供する場合に限り適用可能である。もし、これらのコンポーネントが本 PP の附属書 C から ST に引用しない場合、ST 作成者上記リストから削除するべきである。

3.2　検証できる更新

セクション 2.2「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

セクション 2.3「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すすめるべきである。

(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。パスワードは目に見えない形で保存しなければならず、かつパスワードが平文で表示されるようなパスワード又はパスワードファイルを明確に読み出すためのインタフェースが全く提供されていない状態でなければならない。

(FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU.7, FMT_MTD.1, FMT_SMF.1, FMT_SFR.1, FPT_APW_EXT.1, FTA_SSL_EXT.1, FTA_SSL.3)

3.5 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)

3.6 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、更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、更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

このセクション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：<u>アンダーライン</u>書体にて表記する；
- 選択における割付：<u>*イタリック及びアンダーラインされた*</u>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

このセクションは、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、次の下位のセクション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	
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

機能要件	監査対象事象	追加の監査記録内容
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 ｱﾄﾞﾚｽ)。
FIA_UAU_EXT.2	認証ﾒｶﾆｽﾞﾑの利用すべて。	試行元(例：IP ｱﾄﾞﾚｽ)。
FIA_UAU.7	なし。	
FMT_MTD.1	なし。	
FMT_SMF.1	なし。	
FMT_SMR.2	なし。	
FPT_SKP_EXT.1	なし。	
FPT_APW_EXT.1	なし。	
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 ｱﾄﾞﾚｽ)。
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。
FTA_SSL_EXT.1	対話セションのロック解除に関する試行。	追加情報なし。
FTA_SSL.3	ｾｼｮﾝﾛｯｸﾒｶﾆｽﾞﾑによるﾘﾓｰﾄｾｼｮﾝの終了。	追加情報なし。
FTA_SSL.4	対話セションの終了。	追加情報なし。
FTA_TAB.1	なし。	
FTP_ITC.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_TRP.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

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) 監査の未指定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 に対して表 1 に記載された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)。これはある事象のすべてのインスタンスを含むべきである -- 例えば、あるシステムにおいていくつかの異なる識別及び認証メカニズムが存在する場合、FIA_UIA_EXT.1 の複数の事象が各メカニズムについて生成されなければならない。評価者は、ST に含まれる暗号化プロトコルのそれぞれについてのチャネルの確立と終了に関して監査記録が生成されていることをテストしなければならない (shall)。もし、HTTPS が実装されている場合、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。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、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。

保証アクティビティ：
このアクティビティは、FAU_GEN.1.1 のテストと同時に実施されるべきである(should)。

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。

保証アクティビティ：
このアクティビティは、FAU_GEN.1.1 のテストと同時に実施されるべきである(should)。

FAU_STG_EXT.1　外部監査証跡格納

FAU_STG._EXT.1.1　TSF は、［選択：外部 IT エンティティに対して生成した監査データの送信、外部 IT エンティティから監査データの受信と格納］を［選択：IPsec、SSH、TLS、TLS/HTTPS］プロトコルを実装している高信頼チャネルを用いて、実施できなければならない(shall)。

適用上の注意：

監査サーバとして動作しないTOE に対する本PP の適用に際して、監査記録を格納しレビューを行うための非TOE である監査サーバにTOE は依存する。　TOE は、監査記録を生成するが、これらの監査記録の格納及びこれらの監査記録のレビューを管理者に許可する機能は運用環境によって提供されている。ST 作成者はこれらの場合に最初の選択の最初の節を選択する。　本PP は、監査サーバとしての要件を指定するために使用することもできる；この場合、最初の選択の2 番目の節が使用される。
2 番目の選択では、ST 作成者は、この接続が保護される手段を選択する。ST 作成者は、サポートしているプロトコル要件がST に含まれている選択と一致することも確実にする。
保証アクティビティ：
2 つのタイプのTOE（監査サーバとして動作するものと外部監査サーバへデータを送信するもの）に関して、ある程度のローカルストレージが存在している。評価者は、TSS を検査し、そこにローカルに格納される監査データの量が記載されていることを確認しなければならない(shall)；ローカル監査データの

保存が満杯になった時に何が起きるか；また、どのようにして不正なアクセスからこれらの記録を保護しているか。 評価者は、操作ガイダンスを検査し、（TOE が監査サーバとして動作していない場合について）そこにローカル監査データと監査ログサーバへ送信される監査データの関係について記載されていることも確認しなければならない(shall)。 例えば、ある監査事象が生成されたとき、それが外部サーバとローカル保存に対して同時に送信されるのか、それともローカル保存はバッファとして使用され、監査サーバにデータを送信することによって定期的に「消去」されるのか。

TOE が監査サーバとして動作する

評価者は、TSS を検査し、そこにTOE に対して監査データを送信するために非TOE エンティティからサポートされる接続、及びどのように高信頼チャネルが提供されるのかについて記載されていることを確認に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に関する一連の保証アクティビティに指定されたとおり実施されるものである。 評価者は、操作ガイダンスを検査し、そこにTOE との高信頼チャネルがどのように確立されるかについて、TOE に接続して監査データを送信するその他のIT エンティティのあらゆる要件（特に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）、その他のIT エンティティと通信を行うために必要なTOE の構成・設定についても記載されていることも確認しなければならない(shall)。 評価者は、本要件に関して次のようなテストを実施しなければならない(shall)。

- *テスト 1：評価者は、提供された設定ガイダンスに従って外部IT エンティティとTOE の間にセションを確立しなければならない(shall)。 評価者は、その時、TOE へ送信される監査データを生成するために設計された評価者の選択によるいくつかのアクティビティの間におけるIT エンティティとTOE の間を通過するトラフィックを検査しなければならない(shall)。 評価者は、これらのデータがこの転送の間に平文で見ることができないこと、及びそれらがTOE に正常に受信されていることを観測しなければならない(shall)。 評価者は、このテストを2 番目の選択で選択したプロトコルそれぞれについて実施しなければならない(shall)。*

TOE が監査サーバとして動作しない

評価者は、TSS を検査し、そこに監査データが外部監査サーバに転送される手段について、及びどのように高信頼チャネルが提供されるかについて記載されていることを確認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に関する一連の保証アクティビティに指定されたとおり実施されるものである。 評価者は、操作ガイダンスを検査し、そこに監査サーバとの高信頼チャネルがどのように確立されるかについて、監査サーバに関するあらゆる要件（特に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）、監査サーバと通信を行うために必要なTOE の構成・設定についても記載されていることも確認しなければならない(shall)。 評価者は、本要件に関して次のようなテストを実施しなければならない(shall)。

- *テスト 1：評価者は、提供された設定ガイダンスに従ってTOE と監査サーバの間にセションを確立しなければならない(shall)。 評価者は、その時、監査サーバへ送信される監査データを生成するために設計された評価者の選択によるいくつかのアクティビティの間における監査サーバとTOE の間を通過するトラフィックを検査しなければならない(shall)。 評価者は、これらのデー*

タがこの転送の間に平文で見ることができないこと、及びそれらが監査サーバに正常に受信されていることを観測しなければならない(shall)。 評価者は、テストに際して監査サーバ上で使用した特定のソフトウェア(名称、バージョン)を記録しなければんらない(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**鍵生成**で使用される**非対称**暗号鍵を生成しなければならない(shall) :

［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」 (離散対数暗号を用いた鍵確立スキームに関する勧告)*
- *NIST Special Publication 800-56A, 楕円曲線に基づく鍵確立スキーム、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」 (デジタル署名標準) において定義されるとおり）実装のための「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)*
- *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」 (素因数分解暗号を用いた鍵確立スキームに関する勧告)* ］

及び共通鍵強度 112 ビット相当、又はそれ以上の指定された暗号鍵サイズ。

適用上の注意 :

このコンポーネントは、TOE により用いられるさまざまな暗号プロトコル（例えば、IPsec）の鍵確立目的で用いられる公開鍵／秘密鍵ペアをTOE が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 作成者はこの機能を明らかにするためにこの要件を繰り返しするべきである(should)。使用されるスキームはこのセクションから ST 作成者によって選択される。

使用されるドメイン・パラメタは、本PP のプロトコル要件によって指定されるので、TOE がドメイン・パラメタを生成することは想定されていない、したがって本PP で指定されたプロトコルにTOE が適合しているならば、追加のドメイン・パラメタ検証は一切必要ではない。

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。

保証アクティビティ :

評価者は、ST 作成者が実施した選択に応じて、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 (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。

選択に応じて、TSF が800-56A 及び／又は800-56B に適合していることを示すため、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 が適合しようとしている 適切な800-56 規格のすべての選択をリストアップしなければならない(shall)。*
- *TSS にリストアップされたそれぞれの適切なセクションにおいて、「shall（しなければならない）」以外（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）」）のすべての記述において、もしTOE がこのようなオプションを実装している場合、TSS に記述されていなければならない(shall)。*
- *800-56A 及び 800-56B のそれぞれの適切なセクションにおいて、「shall（しなければならない）」又は「should（するべきである）」という記述に関連する機能についてのあらゆる省略は、記述されていなければならない(shall)。*

いかなるTOE 特有の拡張、文書に含まれていない処理、又はTOE が実施すべきセキュリティ要件に影響を与えうるような文書によって許可された別の実装は、記述されていなければならない(shall)。

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 :

- **FIPS PUB 186-3、「Digital Signature Standard」**

RSA デジタル署名アルゴリズムの場合 :

- **FIPS PUB 186-2 又は 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 :

- **FIPS PUB 186-3、「Digital Signature Standard」、FIPS PUB 186-2、「Digital Signature Standard」]**
- **TSF は、「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) (FIPS PUB 186-3、「Digital Signature Standard」に定義されている通り)。**

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。

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-224、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、224、**

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・ダイジェストサイズは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、224、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-224、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」*

本PP の将来のバージョンでは、SHA-1 は、有効なハッシュアルゴリズムとしては削除されているかもしれない。開発者は他のリストアップされたハッシュアルゴリズムへの移行が求められている。

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。*

Extended: Cryptographic Operation (Random Bit Generation) (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: 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［次のうち１つ又は両方を選択：ソフトウェアベースのノイズ源、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)として与えられて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の最初のセクションについて、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)。

FCS_RBG_EXT.1.1における２番目の選択に関して、ST作成者はエントロピー源がソフトウェアベースか、ハードウェアベースか、又はその両方かを明示する。もし、複数のエントロピー源がある場合、STはそれぞれのエントロピー源について、またそれがハードウェアベースであるかソフトウェアベースであるかについても詳述すること。ハードウェアベースのノイズ源が推奨される。

FIPS Pub 140-2 Annex Cに関する注意事項として、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推奨の乱数生成器、セクション３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ふくまれることも確実にすること。

保証アクティビティ：
文書が生成されなければならない(shall)*－かつ、評価者は、附属書D、エントロピーに関する文書化及び評価（assessment）に基づいた－アクティビティを実施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

このセクション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 テスト)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*, セクション 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。

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、及び以下の特殊文字：［選択：“!”, “@”,*

“#”, “$”, “%”, “^”, “&”, “”, “(“, “)”、［割付：その他の文字］］の組み合わせから作られなければならない(shall)；*

2. *最小パスワード長は、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１５文字以上パスワードをサポートしなければならない(shall)；*

適用上の注意：ST作成者はTOEがサポートする特殊文字を選択する；それらは割付を用いて追加されたサポート特殊文字としてオプションとしてリストアップしてもよい。「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、要件を満たすパスワード、又は要件を満たさないパスワードのいずれか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、TOEがそのパスワードサポートしていることを検証しなければならない(shall)。評価者は、すべての作成可能なパスワードをテストすることは要求されていない(又はできそうにない)、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)。

利用者識別及び認証（FIA_UIA）

FIA_UIA_EXT.1　利用者識別及び認証

FIA_UIA_EXT.1.1　TSF は、非 TOE エンティティに対して識別及び認証プロセスを起動する用に要求する前に、次のアクションを許可しなければならない(shall)：

- FTA_TAB.1 に従い、警告バナーを表示する；
- ［選択：その他のアクションなし、［割付：サービスのリスト、非 TOE の要求への応答として TSF によって実施されるアクション。］］

FIA_UIA_EXT.1.2　TSF は、管理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管理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(管理者及び外部 IT エンティティ)に対して適用される。識別及び認証の前に外部エンティティが利用可能な

サービスはほとんどないか、又は全くない状態であるべき(should)なので、もし利用可能なもの（おそらくICMP echo）がある場合は、割付のところにリストアップされるべき(should)であり；さもなければ、「その他のアクションなし」が選択されるべき(should)である。

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。

外部IT エンティティ（例、監査サーバ、又はNTP サーバ等）との通信に関して、このような接続はFTP_ITC.1 に記載された識別及び認証を実行するプロトコルに従って実行されなければならない(must)。このような通信（例、認証サーバとのIPsec 接続の確立）は必ずしも割付に記述しなくてもよいだろうことを意味している、なぜなら接続の確立は、識別及び認証プロセスの起動として「カウント」するからである。

保証アクティビティ：

評価者は、TSS を検査して、製品がサポートしているそれぞれのログオン方式（ローカル、リモート（HTTPS、SSH、等）についてのログオンプロセスが記述されていることを決定しなければならない(shall)。 この記述は、許可され／使用されるクレデンシャルに関連する情報、実行されるいかなるプロトコルトランザクション、及び何によって「ログイン成功」としているかについての情報を含んでいなければならない(shall)。 評価者は、操作ガイダンスを検査し、ログインのために必要な準備的なステップ（例、プリシェアードキー、トンネル、証明書等のクレデンシャル材料の構築）が記述されていることを決定しなければならない(shall)。 それぞれのサポートされているログイン方式に関して、評価者は操作ガイダンスによりログイン成功のための明確な説明が提供されていることを確認しなければならない(shall)。 もし、ログインが制限される前に提供されるサービスを確認するために設定が必要な場合には、評価者は操作ガイダンスが許可されたサービスの制限に関する十分な説明が提供されていることを決定しなければならない(shall)。

評価者は、ログイン方式がサポートするクレデンシャルのタイプのそれぞれと同様に、管理者がTOE へアクセスする方式のそれぞれ（ローカル及びリモート）について、以下のテストを実施しなければならない(shall)：

- *テスト１：評価者は、ログイン方式がサポートする適切なクレデンシャルを設定するために操作ガイダンスを用いなければならない(shall)。そのクレデンシャル／ログイン方式について、評価者は、提供されている正しいI&A 情報によってシステムへのアクセス可能となることと同時に、正しくない情報によってアクセスの拒否となることを示さなければならない(shall)。*
- *テスト２：評価者は、操作ガイダンスに従って許可されたサービス（もし、あれば）を設定しなければならない、またその時に外部リモートエンティティに対して利用可能なサービスであるかどうかを決定しなければならない(shall)。評価者は、利用可能なサービスのリストが要件で定められたものに限定されていることを決定しなければならない(shall)。*
- *テスト３：ローカルアクセスについて、評価者はローカルの管理者がログインの前にどのようなサービスを利用可能であるかを決定し、かつ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(shall)。*

FIA_UAU_EXT.2　拡張 : パスワードベース認証メカニズム

FIA_UAU_EXT.2.1　TSF は、管理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)。

保証アクティビティ :

この要件の保証アクティビティは、FIA_UIA_EXT.1 の保証アクティビティがカバーしている。もし、その他の認証メカニズムが指定されている場合、評価者はそれらの方式を FIA_UIA_EXT.1 のアクティビティに追加しなければならない(shall)。

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管理者に対して*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。

保証アクティビティ :

評価者は、許可されたローカルなログインの方式のそれぞれについて、以下のテストを実施しなければならない(shall) :

- *テスト 1 : 評価者は、TOE に対してローカルに認証しなければならない(shall)。この試行と同時に、評価者は、認証情報の入力時にほとんど見えないフィード場あくが抵抗されていることを検証しなければならない(shall)。*

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。

保証アクティビティ：

評価者は、本PP の要件に応じて実装されたTSF データを操作する機能のそれぞれが識別されていること、及び管理者のみがその機能にアクセスできることを決定するために、ガイダンスをレビューしなければならない(shall)。 評価者は、操作ガイダンスで識別された管理者機能のそれぞれについて；管理者ログインの前にインタフェースを通してアクセス可能な管理者機能それぞれを決定するために、TSS を検証しなければならない(shall)。 これらの機能のそれぞれについて、評価者は、これらのインタフェースを通してTSF データを操作できる能力をどのようにして管理者以外に許可していないことをTSS が詳述していることも確認しなければならない(shall)。

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：

- *ローカル及びリモートにTOE を管理するための能力*
- *TOE を更新する能力、及び［選択：デジタル署名、公開されたハッシュ、その他のメカニズムなし］を用いて、更新をインストールする前に、その更新を検証する能力。*
- *［選択：*
    - *FIA_UIA_EXT.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提供のサービスのリストを設定する能力。*
    - *暗号機能を設定する能力。*
    - *その他の機能なし。］*

適用上の注意：TOE は、ローカル及びリモート両方の管理者に対する機能を、信頼される発信元からの更新であることを管理者が検証する能力と同様に提供しなければならない。それらはデジタル署名、及びオプションとして公開されたハッシュを用いてアクションを実施できなければならない(must)。 ST 作成者は最初の選択を用いて、公開ハッシュ検証オプションが利用可能かどうかを選択する、これはFPT_TUD_EXT.1.3 における関連する選択と一致しなくてはならない(must)。 もしTOE が管理者に対して識別又は認証の前に利用可能なサービスを設定するための能力を提供する場合、又はもしTOE の暗号機能のいずれかが設定可能である場合、ST 作成者は適切な選択又は2 番目の選択におけるいくつかの選択を行う、それ以外の場合「その他の能力なし」を選択する。

保証アクティビティ：

FMT_SMF.1 に関するセキュリティ管理機能は、本PP の至る所で提供され、FMT_MTD、FPT_TST_EXT、及び関連規格において指定されているいずれの暗号管理機能における要件の一部として含まれている。これらの要件への適合はFMT_SMF.1 への適合を満足する。

FMT_SMR.2　セキュリティ役割における制約事項

FMT_SMR.1.1　TSFは、役割を維持しなければならない(shall)：

- **許可された管理者。**

FMT_SMR.2.2　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(shall)。

FMT_SMR.2.3　TSF は、条件

- 許可された管理者役割は、ローカルに TOE を管理できなければならない(shall)；
- 許可された管理者役割は、リモートに TOE を管理できなければならない(shall)；

が満足されていることを保証しなくてはならない(shall)。

適用上の注意：

FMT_SMR.2.2 は、利用者アカウントがただ1 つの役割に関連付けされることを要求している。しかし、複数の利用者が同じ役割を持っていてもよく、TOE は役割をただ一人の人に制限するようには要求されていない。

FMT_SMR.2.3 は、許可された管理者がローカルコンソールを通して、またリモートメカニズム（IPsec、SSH、TLS、TLS/HTTPS）を通して、TOE を管理できることを要求している。 複数コンポーネントの TOE については、管理統制やその他の TOE コンポーネントの設定を提供する 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：

評価者は、リモート管理用クライアント上で実行される必要があるあらゆる設定を含み、TOE をローカル及びリモートに管理するための説明を含んでいることを確認するために、操作ガイダンスをレビューしなければならない(shall)。評価のためのテストアクティビティ全体において、それぞれのインタフェースを用いた管理者アクションを含むそれぞれのテストを繰り返す必要はないが、評価者はすべてのサポートされているインタフェースを使用しなければならない(shall)。 しかし、評価者は、本PP の要件に適合するTOE を管理するためにサポートされている方式のそれぞれがテストされることを保証しなければならない(shall)；例えば、TOE がローカルなハードウェアインタフェースを通して管理することができる場合；SSH；及び TLS/HTTPS；その際に、すべての３つの管理方式が評価チームのテストアクティビティの間に検査されなければならない。

4.2.6　TSF の保護(FPT)

FPT_SKP_EXT.1　　拡張：TSF データの保護（すべての対象鍵の読み出しについて）

FPT_SKP_EXT.1.1　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(shall)。

適用上の注意：
この要件の意図は、「通常」のインタフェースを通して、管理者が（保存されている又は一時的な）識別された鍵を読み出したり、又は閲覧したりすることができないことである。 管理者はこれらの鍵を閲覧するためにメモリーを直接読み出すことができると理解されているが、実際には些細な仕事ではなく

管理者としての作業のうちのかなりの仕事となるかもしれない。 管理者は信頼できる職員と考えられるので、彼らがこのようなアクティビティを行おうとはしないと想定される。

保証アクティビティ：

評価者は、適用上の注意において概説した通り、あらゆるプリシェアード鍵、対称鍵及びプライベート鍵がどのように保存されるか、またそれらがその目的に特化して設計されたインタフェースを通して閲覧されることが不可能であることを決定するためにTSS を検査しなければならない(shall)。 もし、それらの値が平文で保存されていない場合、TSS はそれらがどのように保護され見えなくなっているかを記述していなければならない(shall)。

FPT_APW_EXT.1　　拡張： 管理者パスワードの保護

FPT_APW_EXT.1.1　TSF は、パスワードを非平文の形式で保存しなければならない(shall)。

FPT_APW_EXT.1.2　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(shall)。

適用上の注意：

この要件の意図は、生のパスワード認証データが平文で保存されていないこと、及び「通常」のインタフェースを通して、利用者も管理者も平文のパスワードが読み出すことができないことである。 もちろん、全能の管理者は直接メモリーを読み出してパスワードを取得できるだろうが、そのようなことはやらないと信頼されている。

本PP のこのバージョンにおいて非平文形式でパスワードを保存する方式に関する要件は存在しないが、FCS_COP の要件に基づく暗号方式が推奨されている。 本PP の将来バージョンでは、NIST SP 800-63 よりレベル2 クレデンシャル保存要件に適合するFCS_COP ベースの暗号方式が要求されるだろう。

保証アクティビティ：

評価者は、本要件に関わる全ての認証データ、及び保存の際に平文のパスワードデータを見えなくするために使用する方式についてTSS に記述し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(shall)。TSS は、適用上の注意において概説した通り、その目的に特化して設計されたインタフェースを通してパスワードが閲覧されることが不可能であるような方法で、パスワードが保存されていることについても詳細に記述していなければならない(shall)。

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。

保証アクティビティ：

評価者は、TSS が時間を活用するセキュリティ機能をそれぞれリストアップしていることを保証するために、TSS を検証しなければならない(shall)。TSS は、どのように時間がメンテナンスされ、時間に関

連する機能についてのそれぞれのコンテクストにおいてどの程度信頼できると考えられるかについての記述を提供する。

評価者は、時間のセット方法について管理者に説明していることを保証するため、操作ガイダンスを検査する。もし、TOE がNTP サーバの使用をサポートする場合、操作ガイダンスは、どのようにTOE とNTP サーバの間に通信路が確立されるか、及びこの通信をサポートするためにTOE 上のNTP クライアントの設定にはどのようなものがあるか、について説明する。

- *テスト１：評価者は、操作ガイドを用いて時刻をセットする。評価者は、そのとき時刻が正しくセットされたことを観察するために利用可能なインタフェースを使用しなければならない(shall)。*
- *テスト２：［条件付き］もし、TOE がNTP サーバの使用をサポートしている場合、評価者は、TOE 上のNTP クライアントを設定するために操作ガイダンスを使用しなければならない(shall)。 評価者は、NTP サーバが予測通りに時刻をセットすることを観測する。 もし、TOE がNTP サーバとの接続を確立するために、複数の暗号プロトコルをサポートしている場合、評価者はサポートされているプロトコルそれぞれを用いてこのテストを実施しなければならない(shall)。*

拡張：高信頼アップデート(FPT_TUD_(EXT).1)

FPT_TUD_EXT.1　拡張：高信頼アップデート

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る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。

評価者は、このようなテストで起こり得るエラー、及び管理者が対応するべきアクションについて操作ガイダンスに記述されているこも確認しなければならない；　このような起こり得るエラーはTSS に記述された内容と一致していなければならない(shall)。

4.2.7　TOE アクセス(FTA)

FTA_SSL_EXT.1　TSF 起動セションロック

FTA_SSL_EXT.1.1　TSFは、ローカルな対話セションについて、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

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ションを確立する。評価者は、設定された時間間隔の後、セ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、管理者起動による管理者自身の対話型セションの終了を許可しなければならない(shall)。

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(shall)：

- テスト１：評価者は、TOE との対話型ローカルセションを起動する。そして、評価者は、操作ガイダンスに従い、セションを終了するか、又はセションをログオフして、セションが終了されることを観測する。
- テスト２：評価者は、TOE との対話型リモートセションを起動する。そして、評価者は、操作ガイダンスに従い、セションを終了するか、又はセションをログオフして、セションが終了されることを観測する。

FTA_TAB.1　デフォルト TOE アクセス・バナー

FTA_TAB.1.1　**詳細化：管理者**セションを確立する前に、TSFは、**セキュリティ管理者指定の**TOEの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の間の対話セションに適用することを意図している。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TSSに指定されたアクセス方式ごとにTOEとのセ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)

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、［選択：IPsec、SSH、TLS、TLS／HTTPS］を用いて、TSF自身と以下の機能をサポートする許可されたITエンティティとの間の高信頼通信チャネルを提供しなければならない(shall)：監査サーバ、「選択：認証サーバ、割付：［その他の機能］」、この機能は、他の通信チャネルと論理的に区別され、その終端の保証された識別と、チャネルデータの暴露、削除、改変からの保護を提供する。

FTP_ITC.1.2　TSFは、TSF、又は***許可された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(shall)。

FTP_ITC.1.3　TSFは、［割付：*ピTSFが通信を開始できるサービスのリスト*］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(shall)。

適用上の注意：

上記要件の意図は、その機能を実行するためにTOE が交信する許可されたIT エンティティとの外部通信を保護するため、暗号プロトコルを使用することである。しかしながら、VPN ゲートウェイ機能を指定するためのものではない；このような例においては別のVPN プロテクションプロファイルが使用されるべきである。 保護（リストアップされたプロトコルのひとつによる）は、少なくとも監査情報を集めるためのサーバとの通信のために要求されている。 もし、認証サーバ（例、RADIUS）と通信する場合、ST 作成者は、FTP_ITC.1.1 における「認証サーバ」を選択し、この接続はリストアップされたプロトコルのひとつによって保護されなければならない(must)。 もし、他の許可されたIT エンティティ（例、NTP サーバ）が保護される場合、ST 作成者は、適切な割付（それらのエンティティについて）と選択（それらの通信を保護するために使用されるプロトコルについて）。 ST 作成者が選択を行った後、ST に記載のそれらのプロトコルに関連した附属書C における詳細な要件を選択するものとする。 要するに、外部の監査収集サーバとの接続は、リストアップされたプロトコルのひとつによって保護されることが要求されている。 もし、外部認証サーバがサポートされている場合、リストアップされたプロトコルの一つを用いて通信を保護することが要求されている。 その他の外部サーバのいずれについても、外部通信は保護されなければならないが、もし保護が主張されていれば、識別されたプロトコルで保護されなければならない。

どちらが通信を開始するかについての要件はないので、ST 作成者は、FTP_ITC.1.3 の割付において、TOE が 許可された IT エンティティとの間で、通信を開始できるサービスについて、リストアップする。

この要件は、通信が初めて確立されたときに通信が保護されることを意味するだけでなく、停止状態の後の再開においても通信が保護されることを意味する。TOE セットアップのいくつかの部分はその他の通信を保護するためのトンネルを手動でセットアップすることも含むような場合もあり得るし、もし停止の後にTOE が（必要な）手動介入とともに自動的に通信を再確立しようする場合、攻撃者が重要な情報を入手する、又は接続を侵害することができるかもしれないような窓が作られてしまうかもしれない。

保証アクティビティ：

評価者は、TSS を検査して、この要件で識別されている許可された IT エンティティとのすべての通信について、それぞれの通信メカニズムがその IT エンティティについて許可されたプロトコルの観点で識別されていることを決定しなければならない(shall)。評価者はTSS にリストアップされているプロトコルがST の要件に指定され、含まれていることも確認しなければならない。 評価者は、操作ガイダンスにそれぞれの許可されている IT エンティティとの間で許可されたプロトコルをを確立するための説明が含まれていることと、意図しない通信の切断に対する復旧のための説明が含まれていることを確認しなければならない(shall)。 評価者は以下のテストについても実施しなくてはならない：

a. *テスト１：評価者は、操作ガイダンスに記述されているとおりに通信をセットアップし、通信が成功していることを確認したうえで、それぞれの許可されている IT エンティティとの間のそれぞれのプロトコルを用いる通信が評価の過程においてテストされることを保証しなければならい(shall)。*
b. *テスト２：この要件に定義されたとおり TOE が開始できるプロトコルそれぞれについて、評価者は操作ガイダンスに従い通信チャネルが TOE から開始できるという事実を保証しなければならない(shall)。*
c. *テスト３：評価者は、許可されている IT エンティティとの間の各通信チャネルについて、チャネルデータが平文で送信されないことを保証しなければならない(shall)。*
d. *テスト４：評価者は、許可されている IT エンティティとの間の各通信チャネルについて、チャネルデータの改変が TOE によって検知されていることを保証しなければならない(shall)。*
e. *テスト５：評価者は、テスト 1 においてテストされた許可されている IT エンティティのそれぞれと関連したプロトコルのそれぞれについて、通信が物理的に中断されることを保証する。評価者は、物理的な接続が復旧されうとき、通信が適切に保護されていることを保証しなければならない(shall)。*

さらなる保証アクティビティが特定のプロトコルに関連している。

高信頼パス（FTP_TRP）

FTP_TRP.1　　高信頼パス

FTP_TRP.1.1 **詳細化**: TSFは、**[以下より少なくともひとつを選択: IPsec、SSH、TLS、TLS/HTTPS]を使用し、**TSF自身と**リモート管理者**との間の**高信頼**通信パスを提供しなければならない(shall)、その際その他の通信パスと論理的に区別され、エンドポイントの確かな識別と通信データの*漏洩*からの保護と*通信データの改変の検知*を提供する。

FTP_TRP.1.2 **詳細化**: 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(shall)。

FTP_TRP.1.3 TSF は、*最初の管理者認証とすべてのリモート管理アクション*について、高信頼パスの使用を要求しなければならない(shall)。

適用上の注意:

この要件は許可されたリモートの管理者が高信頼パスを経由してTOEとの間のすべての通信を開始すること、リモート管理者によるTOEとの間のすべての通信がこのパス上で実行されることを保証する。 この高信頼通信チャネルを通過するデータは、最初の選択で選ばれたプロトコルを定義のとおりに暗号化される。 ST作成者はTOEによってサポートされるメカニズム又は複数のメカニズムを選択して、もし選択がまだであればSTへコピーされるそれらの選択に関連している附属書Cにおける詳細な要件を保証する。

保証アクティビティ:

評価者は、TSSを検査して、リモートのTOE管理の方法が、どのようにそれらの通信が保護されるかとともに示されていることを決定しなければならない(shall)。 評価者は、すべてのプロトコルがTSSの本要件で指定されているものと一貫しているTOE管理をサポートにおいてリストアップされており、STにおける要件に含まれていることも確認しなければならない(shall)。 評価者は、操作ガイダンスがそれぞれのサポートされている方法についてのリモート監理セションを各地るスルタンの説明を含んでいつ頃を確認しなければならない(shall)。 評価者は、以下のテストも実施しなければならない(shall):

a. *テスト1:評価者は、(操作ガイダンスで)指定されたリモート管理方法のそれぞれを用いた通信が、操作ガイダンスに記述されている通りに接続のセットアップがなされ、その通信が成功していることを確認した上で、評価の過程においてテストされていることを保証しなければならない(shall)。*

b. *テスト2:サポートされているリモート管理のそれぞれの方法について、評価者は、操作ガイダンスに従い、リモート利用者が高信頼パスを起動せずにリモート管理セションを確立するために使用できるようなインタフェースがないことを保証しなければならない(shall)。*

c. *テスト3:評価者は、リモート管理のそれぞれの方法について、チャネルデータが平文で送信されないことを保証しなければならない(shall)。*

d. *テスト4:評価者は、リモート管理のそれぞれの方法について、チャネルデータの改変がTOEによって検知されることを保証しなければならない(shall)。*

4.3　セキュリティ保証要件

セクション 3 の TOE のセキュリティ対策方針は、セクション 2 で特定された脅威に対処するために構成された。セクション 4.2 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。

このセクションは、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、セクション 4.2 とこのセクション両方に詳述する。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 テスト ing 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。これらのアクティビティの結果は報告され、(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／アクティビティ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。更に、このセクションに説明されている保証アクティビティは、セクション 4.2 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 のセクション 2 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
テスト s (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セクション 4.2 に説明されているが、ST 作成者が 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。更に、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、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：	このセクション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セクション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、セクション4.2 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、セクション 4.2 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、セクション4.2 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)。

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)。

1. *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。*

TOE は、本PP の下で行われる評価範囲から漏れてしまうようなセキュリティ機能を含んでいるかもしれない。層がガイダンスは、管理者に対して、どのセキュリティ機能が評価アクティビティによってカバーされているかを明確にしなければならない。

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、システムの機能的な観点についても、設計や実装の弱さを利用する観点と同様に仕様書に記載される。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及びインタフェースに基づいている。 評価プロセスの主なアウトプットの１つが、以下の要件に定めら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、追加のテストがセクション 4.3 の SAR として特定されているが、セクション 4.2 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、テストの一部が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、公開情報の検索を行い、一般的なネットワーク基盤装置及び実装された通信プロトコルで見つかった脆弱性について、特定の TOE に関連する脆弱性と同様に決定する。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記述する。見つかったそれぞれ脆弱性について、評価者は脆弱性を利用可能でないことを示す根拠を提供するか、脆弱性を確認するために (ATE_IND で提供されるガイドラインを用いて) テストが適切であれば、計画する。適切かどうかは、脆弱性を利用するために必要な攻撃ベクターを検査することにより判定する。例えば、もし脆弱性が起動時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、脆弱性の悪用に、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求められる。

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 に提供される保証レベルにおいて、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)*。更に、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、セクション 2.0 及び 3.0 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、これらは以下の付属書 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、本書の冒頭セクション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

次のサブセクション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.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T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T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、及びいか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。

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.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.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_テスト	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。本セクションは、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、を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、には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	セションのロック	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)		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-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
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-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
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
SC-10	ネットワークの切断	FTA_SSL.3
SC-11	高信頼経路	FTP_TRP.1
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、(分散型)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。セキュアな通信プロトコル(IPsec、SSH、TLS、TLS/HTTPS)のうち一つは実装されなければならず、これにより（最低限）監査サーバやリモート管理者に保護された接続性を提供する。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に対処するために、FTP_ITC.1及びFTP_TRP.1コンポーネントの選択に依存して、以下の要件がSTに含まれるべきである。

さらに、分散型TOEは本PPへの適合を主張することが許されている。このような場合、TOEの異なる部分同士の通信が保護される必要があり、かつそのためにST作成者はSTの本文において、FPT_ITTを２つ繰り返して記述することになる。

注意事項として、STの冒頭で説明する情報への小さな修正が選択の実施によって要求される。さらに、選択された要件によって、セクションC1.2 *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、RFC4303で定義されたIPsecプロトコルを実装しなければならない(shall) 。その際、以下の暗号アルゴリズム 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、AES-GCM-128、AES-GCM-256 これらはRFC4106で指定される］、及び［以下のうち少なくとも選択：以下で定義されたIKEv1（RFC2407、2408、2409、RFC4109）、及び［選択：ハッシュ関数のためのその他のRFCなし、ハッシュ関数のためのRFC4868］；以下で定義されたIKEv2（RFC5996（セクション2.23で指定されているNATトラバーサルのサポートを必須とする）、RFC4307）及び［選択：ハッシュ関数のためのその他のRFCなし、ハッシュ関数のためのRFC4868］］。

適用上の注意：1番目の選択は、追加の暗号アルゴリズムとしてサポートされるものを識別するために使用される。IKEv1又はIKEv2のいずれかのサポートが提供されなければならない(must)が、適合するTOEは両方をサポートできる；2番目の選択がこれについての選択である。 IKEv1については、要件としてRFC2409とRFC4109の追加／修正に適合したIKE実装が要求されているものとして解釈されるものとする。 RFC4868は、追加のハッシュ関数としてIKEv1及びIKEv2の双方で用いられるものとして識別される；もしこれらの関数が実装される場合、三番目（IKEv1用）と4番目（IKEv2用）の選択が使用される。　IKEv2は2014年1月1日以降は必須となる。

FCS_IPSEC_EXT.1.2　TSF は、IKEv1 Phase 1 鍵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 g ろうp 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)：［選択：“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, ［割付：その他の文字］］；*
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：ST 作成者は、TOE がサポートする記号を選択する；それらは、オプションとして割付を用いて、サポートされる追加の記号をリストアップしてもよい。プリシェアード鍵の長さについては、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 のテスト 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鵜場合は、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、次の暗号スイート (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暗号スイート (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暗号スイートを選択するべきである(should)；もし必須のスーツ以外の暗号スイートがない場合は、「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。2010 年12 月のNDPP v1.0 公開より、商用ネットワークデバイスでTLS 1.2 サポートの普及拡大を考慮しつつ、発展を制限してきた。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；しかし、2012 年後半にTLS 1.2 のサポートが要件として含まれないNDPP v2.0 が公開されそうであるが、SSL 2.0 又は SSL 3.0 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NDPP v2.0 は要求するだろう。

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、及び暗号スイート・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、指定された暗号スイート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暗号スイート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、要件で指定された暗号スイート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暗号スイート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；使用されている暗号スイート(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。

本PP の次のバージョンにおいて、rekeying に関する要件が追加となる予定である。要件は、「TSF は、ある鍵を用いて 2^{28} パケットを超えて送信されないように、SSH 接続はrekey されることを確実にしなければならない(shall)。」となる予定である。

FCS_SSH_EXT.1.2　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方式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.1.3　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.1.4　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 : 割付において、ST 作成者は、AES-GCM アルゴリズム、又はAES-GCM がサポートされていない場合は「その他のアルゴリズムなし」を選択することができる。 もしAES-GCM が選択された場合、ST のFCS_COP のエントリーと一致するべきである(should)。2010 年12 月のNDPP v1.0 の公開より、商用ネットワークデバイスにおけるAES-GCM のサポート の普及拡大を考慮してきた。2012 年後半に公開されるNDPP v2.0 ではAES-GCM とAES-CBC がオプションとして要求される予定である。

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.1.5　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.1.6　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.1.7　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　明示的な：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。

FPT_ITT.1　基本内部 TSF データ転送保護

FPT_ITT.1.1　**詳細化**：TSF は TSF データを暴露から保護し、**かつその改変を検知**しなければならない(shall)。ただし、TOE の分離された部分の間で［**以下のうち 1 つ以上を選択：IPsec、SSH、TLS、TLS/HTTPS**］**を用いて** TSF データが送信されるときとする。

適用上の注意：

この要件は分散型の 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によって保護されることを保証する。 この高信頼通信でやり取りされるデータは、最初の選択で選んだプロトコルとして定義したとおり暗号化される。ST 作成者は、TOE によってサポートされる 1 つ又は複数のメカニズムを選択し、そのとき附属書 C における詳細要件がすでに ST に存在しなければ、ST にコピーされていることを確実にする。

保証アクティビティ：

評価者は、分散 TOE のコンポーネントを保護するために使用する方式やプロトコルが記述されていることを判定するために TSS を検査しなければならない(shall)。 評価者は、TOE 管理者に対してサポートされる TSS にリストアップされたすべてのプロトコルが ST の要件に記述され、特定されたものと一貫していることも確認しなければならない(shall)。 評価者は、それぞれのサポートされている方式について通信チャネルを確立するための説明が操作ガイダンスに含まれていることを確認しなければならない(shall)。 評価者、次のテストも実施しなければならない(shall)：

- *テスト 1：評価者は、評価の過程で、操作ガイダンスに記述された接続のセットアップを行い、通信が成功していることを確認した上で、それぞれの（操作ガイダンスにおいて）指定された通信方式がテストされ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、通信方式のそれぞれについて、チャネルデータが平文で送信されていないことを確実にしなければならない(shall)。*
- *テスト 3：評価者は、通信方式のそれぞれについて、チャネルデータの改変が TOE によって検知されることを確実にしなければならない(shall)。*

さらなる保証アクティビティが特定のプロトコルについて関連している。

C1.2 監査対象事象

セクションC.1.1 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)。
FPT_ITT.1(1)	なし	なし
FPT_ITT.1(2)	なし	なし

適用上の注意：

セション確立失敗の監査は、実装に大きく依存しており、現在産業界で標準化されてはいない。 PP の本バージョンでは、監査可能として、特定のリストが義務付けられていないか、又はこのような失敗の種別が義務付けられている。 もし評価された製品において「標準」として、評価対象事象の明確なセットとして現れた場合、本PP の将来のバージョンにおいて監査される必要がある、厳格なプロトコル失敗について、より明確になるだろう。

保証アクティビティ：

評価者は、TSS が監査可能なプロトコル失敗の（ユーザレベル接続の認証失敗を除いておそらく空（カラ）の）リストを TSS が含んでいることを確実するため、チェックしなければならない(shall)。

附属書 D：エントロピーに関する文書と評定

エントロピー源の文書は十分詳細に記述されるべきであり、読んだ後、評価者はそのエントロピー源、及びなぜそれがエントロピーを提供するために依存され得るのかを完全に理解するであろう。この文書は、複数の章か記述されたセクションを含むべきである(should)：設計記述、エントロピー正当化、操作条件、及び健全性テスト。 この文書は、TSS の一部として要求されるものではない。

設計記述

文書は、すべてのエントロピー源コンポーネントの繰り返しを含み、完全なものとして、エントロピー源の設計を含まなければならない(shall)。それは、エントロピー源の操作についてそれがどのように働き、どのようにエントロピーが生成され、かつどのように処理されていない(生の) データがテスト目的のためにエントロピー源の中から取得され得るのかを記述するものである。文書はどこからランダム性

が来るのか、次にどこを通り、生出力（ハッシュ、XOR、他）のあらゆる後処理、場合によっては、それがどこに保存されるか、そして最後にそれがどのようにエントロピー源から出力されるのかについて示すように、エントロピー源設計をたどっていくべき(should)である。 処理（例、ブロッキング）におけるあらゆる条件についてもエントロピー源設計に記述されるべき(should)である。ダイアグラムや例が推奨される。

この設計は、エントロピー源のセキュリティ境界の内容記述、及び境界の外の敵がエントロピーレートに影響を与えることができないことをどのようにセキュリティ境界が保証しているかについての記述についても含んでいなければならない(must)。

エントロピー正当化

エントロピー源の予測不可能性がどこから来て、確率論的ふるまい（確率分布の説明と特定のエントロピー源の分布に関する正当化がこれを説明するための一つの方法である）を見せるエントロピー源においてなぜ確信が得られるのかについての技術的な議論がなされるべき(should)である。 この議論は想定されるエントロピーレートの記述を含みと、TOE 乱数シード処理に十分なエントロピーが入力されることあなたがどのように確信したかを説明するだろう。この考察は、エントロピー源がなぜエントロピーをもつビットを生成することに依存できるかについての正当化の一部をなすだろう。

操作条件

文書には、エントロピー源がランダムデータを生成すると予測される操作条件の範囲を含んでいるだろう。そこには、それらの条件の下でエントロピー源が操作を続けられることを保証するため、システム設計において取られる対策について明確に記述する。同様に文書は、エントロピー源が機能不全又は矛盾したものとなる条件についても記述しなければならない(shall)。 失敗を検知するために用いられる方式又はエントロピー源の質も低下についても含まれるべき(should)である。

健全性テスト

さらに明確に言うと、すべてのエントロピー源健全性テストは及びその根拠が文書化されるだろう。これは健全性テスト、実施されるそれぞれの健全性テスト（例、起動時、連続的に、又はオンデマンド）におけるレート及び条件、それぞれの健全性テストの予測される結果、及びエントロピー源における意図つ以上の失敗を検出するために適切であるとそれぞれのテストが信じられる理由を示す根拠について含んでいるだろう。