IPsec 仮想プライベートネットワーク（VPN）クライアント用のプロテクションファイル

原文タイトル：

Protection Profile for IPsec Virtual Private Network (VPN) Clients

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。
正式な文書は、以下の URL よりダウンロード可能です。
http://www.niap-ccevs.org/pp/pp_vpn_ipsec_client_v1.0.pdf

Information Assurance Directorate

情報保証局

2011 年 12 月 29 日
バージョン 1.0

平成 24 年 9 月 18 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

目　次

1　PP のイントロダクション 1
1.1　TOE の PP 概要 1
1.1.1　TOE の用途及び主なセキュリティ機能 1
1.1.2　暗号 2
1.1.3　TOE 管理と IT 環境 2
1.1.4　プロトコル適合 3

2　セキュリティ課題記述 4
2.1　脅威 4
2.2　組織のセキュリティ方針 5
2.3　前提条件 6

3　セキュリティ対策方針 7
3.1　TOE のセキュリティ対策方針 7
3.2　運用環境のセキュリティ対策方針 7
3.3　セキュリティ対策方針の根拠 8

4　セキュリティ要件及び根拠 12
4.1　セキュリティ機能要件 12
4.1.1　クラス：セキュリティ監査（FAU） 13
4.1.2　クラス：暗号サポート（FCS） 17
4.1.3　クラス：利用者データ保護（FDP） 32
4.1.4　クラス：識別及び認証（FIA） 33
4.1.5　クラス：セキュリティ管理（FMT） 36
4.1.7　クラス：高信頼パス/チャネル（FTP） 39
4.2　セキュリティ機能要件の根拠 40
4.3　セキュリティ保証要件 43
4.3.1　ADV クラス：開発 44
4.3.2　AGD クラス：ガイダンス文書 46
4.3.3　ATE クラス：テスト 49
4.3.4　AVA クラス：脆弱性評定 50
4.3.5　ALC クラス：ライフサイクル・サポート 51
4.4　セキュリティ保証要件根拠 53

附属書 A：サポート表、参考文献及び略語 54

附属書 B：NIST SP 800-53／CNSS 1253 マッピング 56

附属書 C：追加要件 57

附属書 D：本書の表記規則 60

附属書 E：用語 62

附属書 F：PP の識別 64

表一覧

表 1：脅威 5
表 2：組織のセキュリティ方針 5
表 3：TOE の前提条件 6
表 4：TOE のセキュリティ対策方針 7
表 5：運用環境のセキュリティ対策方針 8
表 6：セキュリティ対策方針と脅威及び方針の対応関係 9
表 7：セキュリティ対策方針と前提条件の対応関係 10
表 8：TOE セキュリティ機能要件 13
表 9：監査対象事象 15
表 10：TOE セキュリティ機能要件に関する根拠 41
表 11：セキュリティ保証要件 44

図一覧

図 1：VPN クライアント 1

改訂履歴

バージョン	日付	説明
1.0	2011 年 12 月	初回リリース

1 PP 序論

1 本プロテクションプロファイル（PP）は、認証されたリモートエンドポイントまたはゲートウェイにセキュアなトンネルを提供するための市販（COTS）の IPsec 仮想プライベートネットワーク（VPN）クライアントの購買をサポートする。本 PP では、VPN とそのサポート環境に関する方針、前提条件、脅威、セキュリティ対策方針、セキュリティ機能要件及びセキュリティ保証要件を詳述する。

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

1.1 TOE の PP 概要

3 本書は、VPN クライアントのセキュリティ機能要件を規定する。VPN は、VPN クライアントと VPN ゲートウェイの 2 つの VPN ピア間で、プライベートデータの保護された伝送を提供する。本 PP で定義された TOE は、リモートアクセスクライアント上で実行するコンポーネントである VPN クライアントである。VPN クライアントはプライベートネットワークの外部または内部に配置することを目的としており、また、VPN ピアへのセキュアなトンネルを提供する。このトンネルは、パブリックネットワークを移動する情報の、機密性、完全性及びデータ認証を提供する。本書に準拠するすべての VPN クライアントは IPsec をサポートする。

1.1.1 TOE の用途及び主なセキュリティ機能

4 VPN クライアントは、リモートユーザが保護されていないパブリックネットワークからプライベートネットワークへの、暗号化された IPsec トンネルを確立するために、クライアントコンピュータを使用できるようにする（図 1 を参照）。TOE は、パブリックネットワークと、基盤となる OS の VPN クライアント上に常駐するエンティティ（ソフトウェア、ユーザなど）の間に位置する。プライベートネットワークからパブリックネットワークへ通過する IP パケットは、その宛先が送信元と同じ VPN ポリシーをサポートするリモートアクセス VPN クライアントの場合は暗号化される。VPN クライアントは、たとえデータがパブリックネットワークを通過しても、送信中データの機密性、完全性及び保護を提供しながら、自身とそのピアの間のデータを保護する。

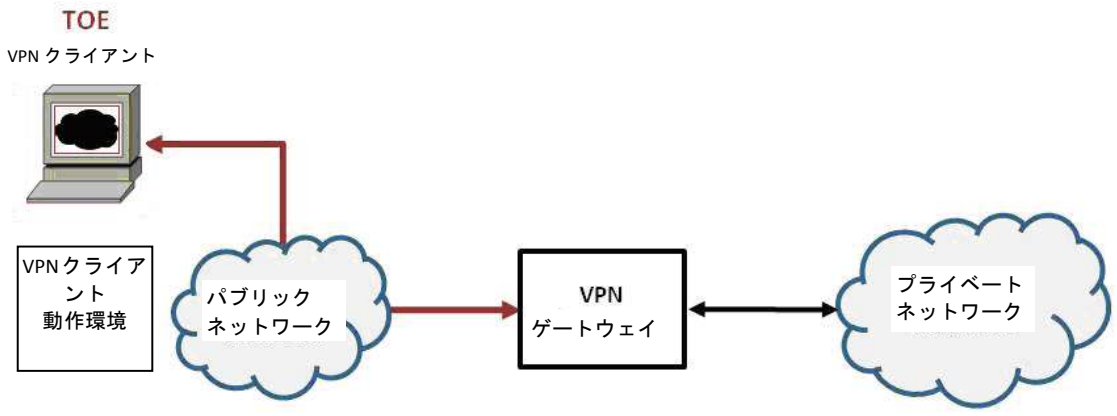


図 1：VPN クライアント

5 本 PP のセキュリティ機能要件の焦点は、以下の VPN クライアントの基本的な観点である。

- VPN ピアの認証
- 通過中のデータの暗号化保護及び
- サービスの実施

6 VPN クライアントは、別の VPN エンドポイントクライアントまたは VPN ゲートウェイ（VPN 通信では「リモート」エンドポイントである）で、VPN 接続を確立できる。VPN エンドポイントは、許可された外部 IT エンティティと通信していることを保証するためにお互いを認証する。VPN ピアの認証はインターネット鍵交換（IKE）ネゴシエーションの一部として実行される。IKE ネゴシエーションは、認証のためにお互いの事前共有鍵または既存の公開鍵基盤を使用する。IKE が完了すると、カプセル化されたセキュリティペイロード（ESP）でセキュアな IPsec トンネルが確立される。

7 VPN クライアントが正しく実装され、重大な設計上の誤りが含まないことが想定される。VPN クライアントは、それを正しく実行するための IT 環境に加え、監査レビュー、監査記録、ユーザ識別及び認証、セキュリティ管理、セッション管理といった、クライアントマシンの保護メカニズムに依存する。ベンダは、サポートされるすべての運用環境のためにクライアントマシンと TOE を正しくインストールし、管理するためのガイダンス構成文書（AGD_PRE、AGD_OPE）を提供することが要求される。

1.1.2 暗号

8 IPsec VPN クライアントは、自身と VPN ピア間を流れるすべての情報を暗号化することが期待される。VPN クライアントは、IPsec VPN トンネルのエンドポイントとして機能し、トンネルの確立と維持に関連する多数の暗号機能を実行する。認証、鍵の生成及び情報の暗号化に使用される暗号方式が十分に堅牢であり、実装に重大な設計上の誤りがない場合は、攻撃者はデータを取得するために暗号鍵空間を総当りできない。IPsec 規格への適合、正しいシードで生成したランダムビット生成器（RBG）及びセキュアな認証要因により、鍵空間の総当り以外の攻撃では送信される情報にアクセスできないことが保証される。平文の秘密鍵及び秘密鍵または他の暗号セキュリティパラメタは、セキュリティ上重要なデータの暴露を防止するために、使用されなくなったときにゼロ化される。

1.1.3 TOE 管理と IT 環境

9 TOE のサポート環境は重要である。ほとんどすべての場合において、TOE は、純粋に汎用オペレーティングシステム上で実行するソフトウェアソリューションである。そのため、TOE は、その実行ドメインと適切な使用のために、TOE 運用環境（システムハードウェア、ファームウェア及びオペレーティングシステム）に大きく依存しなければならない（must）。ベンダは、必要な機能を備えた運用環境を特定し、運用環境を正しく設定する方法について指示を提供するために、インストールと設定に関して十分な指示を提供することが求められる。

TOE では、特定の管理アクティビティ（要件に定義された）を TOE の許可された利用者のサブセットによって実行されることが必要となる。本 PP では、識別機能と認証機能を提供することによりこれらの管理機能を管理者の役割に制限する場合は、TOE に要件は発生しない。このことは、TOE ベンダが適合となる際に、さまざまな方法があることを示す。例えば、次のような方法がある。

- TOE に、権限を持つ管理者の概念を含めない。管理ユーティリティを起動できれば誰で

も TOE を設定できる。この場合、PP に適合するためには、TOE ベンダは、TOE の許可された利用者のサブセットだけが管理ユーティリティを実行できる運用環境を設定するため、管理者が使用する指示を詳述した AGD_OPE/PRE ガイダンスの一部として指示を提供しなければならない（must）。例えば、ガイダンスに、管理者が許可した利用者だけが管理ユーティリティを実行できるよう運用環境にアクセス制御メカニズムを設定していることを記述する。これにより、本 PP のベースライン要件を反映する。

- TOE に、権限を持つ管理者（1 人または一連の管理者）の概念を含めるが、運用環境を使用して識別機能と認証機能を実行し、権限を持つ管理者の TOE 内表現と一致するある程度の表示を TOE に渡すための運用環境に依存する。この場合、ST 執筆者は、TOE で提供される機能を指定するため、要件を追加する必要がある（附属書 C で提供されるテンプレートを使用）。ベンダは、TOE に情報を渡すのを支援するために必要な、運用環境の構成または設定を記述する必要がある。
- TOE に、ハードディスクを収容しているシステムのどの利用者が TOE で提供される管理機能を使用することが許可されるのかを決定する、独自の識別機能と認証機能を含める。この場合、ST 執筆者は、附属書 C で提供される I&A テンプレート情報を ST の本文に使用して、この機能を特定する必要がある。

1.1.4 プロトコル適合

10 本 PP に適合する TOE は、Internet Engineering Task Force（IETF）Internet Protocol Security（IPsec）Security Architecture for the Internet Protocol、RFC 4301 及びカプセル化されたセキュリティペイロード（ESP）プロトコルを実装し、これに適合する。IPsec ESP は、現在 RFC 2406 と RFC 4303 に規定されている。IPsec VPN クライアントは、トンネルモードとトランスポートモードで ESP をサポートし、ESP 機密性及び完全性セキュリティサービスのみを使用する。AH プロトコルをサポートするのに、IPsec VPN クライアントは必要ではない。

11 IPsec VPN クライアントは、VPN エンティティとのセッション鍵を認証し、確立するために、RFC 2407、2408、2409、4109 に定義されている Internet Key Exchange（IKE)v1 プロトコル、または RFC 5996 （2.23 節に規定されている必須の NAT トラバースのサポート付き）と 4307 に規定されている IKEv2 プロトコルのいずれかを使用する。

12 実装されている IKE のバージョンに関連する RFC 4301 への適合に例外がある。RFC には、「注意：本書は、IKEv2 では利用可能だが IKEv1 では利用可能ではない、いくつかの機能、例えば、ローカル及びリモートの範囲をあらわす SA のネゴシエーション、または同じセレクターを持つ複数の SA のネゴシエーションなどのサポートを義務付けている。」という内容が記載されている。そのため、本文書は、IKEv2 または同等の機能を持つ鍵及びセキュリティアソシエーション管理システムの使用を前提としている。PP の本バージョンに対し、ST 執筆者は、IKE のどちらかのバージョンを実装する選択肢を有する。IKEv2 なしで IKEv1 を選んだ場合、TOE は技術的に RFC 4301 に適合しないが、VPN クライアント PP の本バージョンに適合すると考えられる。PP の以降のバージョンは、IKEv2 を必要とする可能性が高い。

2 セキュリティ課題記述

13 本 PP は、リモートユーザが、プライベートネットワーク（例えばユーザのオフィスネットワーク）へアクセスするために、パブリックネットワークを利用するという状況に対処するために書かれている。ネットワークパケットの保護は、パブリックネットワークとプライベートネットワークの間の境界を通過するときに求められている。暴露と改ざんから移動中のデータを保護することを目的として、セキュアな通信を確立するために VPN が作成される。VPN クライアントは、セキュアな VPN トンネルの一端を提供し、VPN クライアントとネゴシエーションされた VPN セキュリティポリシーに従って、ネットワークパケットの暗号化と復号を実行する。

14 VPN クライアントの適切なインストール及び設定が、正確な運用をするために重要で、それゆえに管理者による TOE の適切な取り扱いについても対処する。

15 本章は、以下を識別する。

- VPN クライアントによって対抗される組織に対する IT 関連の脅威。
- 十分な保護を提供するために制御を要求する環境の脅威。
- 必要に応じて VPN クライアントのための組織のセキュリティ方針。
- VPN クライアント運用環境に関する重要な前提条件。

2.1 脅威

16 本 PP は、内部者の脅威に対して保護できる要件を含まない。許可された利用者は敵対するまたは悪意があるとは見なされず、適切なガイダンスに従うことが信用される。許可された人物のみがクライアント装置にアクセスできるべきである（should）。従って、主な脅威エージェントは、保護されたネットワークにアクセスしようと試みる許可されていないエンティティである。プライベートネットワークに対し自身が本物であることを証明することができる場合、エンティティは許可される。このように、ネットワークの正当な利用者として自身を確立する。この状況では、TOE は本物であることを要求しなければならない（must）、要求エンティティである。確立された接続は、ネットワーク攻撃の可能性があり、暴露と改ざんから保護されなければならない（must）。同様に、TOE が正当な VPN ピア（例えば、VPN ゲートウェイ）との通信トンネルを確立すること及び VPN ピアが信用されたエンティティになりすましていないことも、TOE は保証しなければならない（must）。相互認証は、許可されていないエンティティとの接続を禁止する。TOE は、エラーや悪意のあるアクションによって引き起こされるセキュリティ侵害から自身を保護する。

17 VPN 接続を確立するためのセキュリティ方針の不適切なネゴシエーション、または弱いプロトコルオプションの施行は、利用者データ及び TSF データの暴露または改ざんが行われる課題でもある。プロトコル相互接続性及び強力な暗号化を要求する相互に合意されたセキュリティ方針が、VPN 保護を確立するために必須である。

18 その他の脅威エージェントは、資源が再割当されるときにクリアされないセキュリティ関連の情報を含み、センシティブな値が不要になった場合は、これらのデータへのアクセスは保護されなければならない（must）。TOE は、残存データが適切に取り扱われることを保証しなければならず（must）、それにより、セキュリティ関連の情報は、それが使用された後で他のユーザ/プロセスによってアクセスできない。TSF データの漏洩には、認証データ、セッション鍵、セキュリティメカニズム及び TOE が保護するデータが含まれる。TOE または TSF データは、不適切なアクセスと更新から保護されなければならない（must）。

19 TOE に対する上記のようなネットワーク攻撃は、無許可アクセスを取得し、セキュリティを無力化するための唯一の手段ではない。製品の更新は、脅威環境の変更が対処されることを保証するために、一般的で必要な機能である。一般的に使用される攻撃手口には、不具合を含んでいるソフトウェアにパッチを当てていないバージョンに対する攻撃が含まれる。適時にパッチを適用することで、製品のセキュリティ方針の維持と施行の可能性を高める。ただし、更新は、信頼できるソースからのものでなければならない（must）。さもないと、

攻撃者は自分自身で「更新」を作成して、例えばルールキット、ボット、またはその他のマルウェアェア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る。

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

21 次の表に、VPN クライアント及び運用環境によって対処される脅威の一覧を示す。下記のすべての脅威について、想定される攻撃者の専門知識レベルは高度ではない。

表 1：脅威

脅威の名称	脅威の定義
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（may）。
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な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	悪意の人がエンドユーザに対して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（may）。
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を及ぼす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.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）。

2.2 組織のセキュリティ方針

22 組織のセキュリティ方針は、プライベートネットワークとパブリックネットワークの間の境界を越えるネットワークパケットを保護するため、適用性により選択された。手続きに関連する方針も、前提条件として記載されている。方針記述に従って、正式な参照のない方針が作成され、公式化されることが期待される。

表 2：組織のセキュリティ方針

方針の名称	方針の定義
P.COMPATIBILITY	TOEは、同じプロトコルを使用して他のネットワーク機器との相互接続性を実現するために、実装されたプロトコルについてRFC

方針の名称	方針の定義
	（Request for Comments）要件を満たさなければならない（must）。
P.CONFIGURABILITY	TOEは、運用のセキュリティ関連観点を設定する機能を提供しなければならない(must)。

2.3 前提条件

23 セキュリティ課題の定義のこの節では、セキュリティ機能を提供できるようにするために運用環境に課す前提条件を示す。これらの前提条件を満たさない運用環境に TOE が配置される場合、TOE はそのすべてのセキュリティ機能を提供できなくなるかもしれない（may）。前提条件は、運用環境の物理的な環境、人員及び接続性に対して課すことができる。

表 3：TOE の前提条件

セキュリティ対策方針	セキュリティ対策方針の定義
A.NO_TOE_BYPASS	情報は、TOEを通過しないでVPNクライアントのホストが接続されているネットワーク上を流れることができない（cannot）。
A.PHYSICAL	TOE 及びそこに含まれるデータの価値に相当する物理的なセキュリティが、環境によって提供されると想定される。
A.TRUSTED_ADMIN	TOE 管理者は、信頼される方法ですべての管理者ガイダンスに従い、適用するものと信頼される。

3 セキュリティ対策方針

24 セキュリティ対策方針は、第 2 章の脅威、組織のセキュリティ方針及び前提条件から導出する評価対象（TOE）と運用環境に関する要件である。第 3 章では、TOE に関するセキュリティ対策方針を、より正式にセキュリティ機能要件（SFR）と言い換えている。TOE は、SFR に対して評価される。

3.1 TOE のセキュリティ対策方針

25 表 4 に、TOE のセキュリティ対策方針を示す。これらのセキュリティ対策方針は、識別された脅威に対抗し、識別された組織のセキュリティ方針に適合するために、記載されている意図を反映している。TOE は、セキュリティ機能要件を満たすことで、これらの対策方針に適合する。

表 4：TOE のセキュリティ対策方針

セキュリティ対策方針	セキュリティ対策方針の定義
O.AUTH_COMM	TOE は、利用者が TOE になりすます他のエンティティと通信していないこと及び TOE が許可された IT エンティティになりすます他のエンティティでなく、許可された IT エンティティと通信していることを保証する手段を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS	TOE は、機密性を維持するための暗号化機能（例えば、暗号化/復号及び電子署名操作）を提供し（shall）、TOE 及びそのホスト環境の外部で送信されるデータの改ざんを検出することを可能にする。
O.PEER_AUTHENTICATION	TOE は、TOE とのセキュリティアソシエーションを確立しようとする、お互いのピア TOE が本物であることを証明する。
O.PROTOCOLS	TOE は、相互接続性を保証するために、RFC 及び/または工業仕様書に従って、標準化されたプロトコルが TOE に実装されていることを保証する。
O.RESIDUAL_INFORMATION_CLEARING	TOE は、資源が再割当されるとき、保護された資源に含まれるデータが使用できないことを保証する。
O.SYSTEM_MONITORING	TOE は、監査データを生成する機能を提供する。
O.TOE_ADMINISTRATION	TOE は、管理者が TOE を設定できるメカニズムを提供する。
O.TSF_SELF_TEST	TOE は、正しく動作していることを保証するために、セキュリティ機能のサブセットをテストする機能を提供する。
O.VERIFIABLE_UPDATES	TOE は、TOE への更新が管理者によって変更されていないこと、及び（任意で）信頼できるソースから検証できることを保証することを手助けする機能を提供する。

3.2 運用環境に関するセキュリティ対策方針

26 TOE の運用環境は、セキュリティ機能（TOE のセキュリティ対策方針で定義された）を正しく提供するために TOE を支援する、技術的及び手続き的な手段を実装する。この部分的なソリューションは運用環境のセキュリティ対策方針と呼ばれ、運用環境で達成するべき目

標を示した一連の記述から成る。

27 本節では、IT ドメインによって、または技術的または手続き的な手段以外によって対処するセキュリティ対策方針を定義する。2.3 節で特定されている前提条件は、環境のセキュリティ対策方針として組み込まれている。これらの前提条件は、主に手続き的または管理上の手段によって満たされる、追加の要件を課す。表 5 に、環境のセキュリティ対策方針を示す。

表 5：運用環境のセキュリティ対策方針

対策方針	対策方針の説明
OE.NO_TOE_BYPASS	情報は、TOEを通過しないでVPNクライアントのホストが接続されているネットワーク上を流れることができない。
OE.PHYSICAL	TOE 及びそこに含まれるデータの価値に相当する物理的なセキュリティが、運用環境によって提供されると仮定する。
OE.TRUSTED_ADMIN	TOE 管理者は､信頼される方法ですべての管理者ガイダンスに従い、適用するものと信頼される。

3.3 セキュリティ対策方針根拠

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

表 6：セキュリティ対策方針と脅威及び方針の対応関係

脅威/方針	脅威と方針に対応する対策方針	根拠
T.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（may）。	O.TSF_SELF_TEST TOEは、それが正しく動作していることを保証するために、そのセキュリティ機能のサブセットをテストする機能を提供する。	O.TSF_SELF_TESTは、TSFの正しい動作を正常に実証するために、TSFがセルフテストスイートを実行することを保証することで、この脅威に対抗する。
T.UNAUTHORIZED_ACCESS 利用者が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な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)。	O.AUTH_COMM TOEは、利用者がTOEになりすます他のエンティティと通信していないこと及びTOEが許可されたITエンティティになりすます他のエンティティでなく、許可されたITエンティティと通信していることを保証する手段を提供する。 O.CRYPTOGRAPHIC_FUNCTIONS TOEは、機密性を維持するための暗号化機能(例えば、暗号化/復号及び電子署名操作）を提供し（shall）、TOEの物理的に分離された部分間で送信される、またはTOEの外部に保存されるTSFデータの改ざんを検出することを可能にする。 O.PEER_AUTHENTICATION TOEは、TOEとのセキュリティ・アソシエーションを確立しようとする、お互いのピアTOEが本物であることを証明する。 O.TOE_ADMINISTRATION TOEは、管理者がTOEを設定できるメカニズムを提供する。	O.AUTH_COMM及び O.PEER_AUTHENTICATIONは、そのピアと通信する前に、TOEがすべてのピアを識別し、認証することを保証することで、この本脅威を軽減する。また、TOEは、通信の前に相互認証を保証するために、それ自身の証明書をピアに送信できなければならない（must）。 O.CRYPTOGRAPHIC_FUNCTIONSは、他の保護メカニズムに必要な基礎となる暗号化機能を提供することで、この脅威の軽減に寄与する。 O.TOE_ADMINISTRATIONは、セキュアな方法でTOEが設定されることができるメカニズムを、TOEが提供することを要求する。
T.UNAUTHORIZED_UPDATE 悪意の人がエンドユーザ	O.VERIFIABLE_UPDATES TOEは、TOEへの更新が管理者に	O.VERIFIABLE_UPDATESは、管理者が更新を確認できることを保証する。

脅威/方針	脅威と方針に対応する 対策方針	根拠
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(may)。	よって変更されていないこと及び（オプションで）信頼できるソースから検証できることを保証する機能を提供する。	
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。	O.SYSTEM_MONITORING OE は、監査データを生成する機能を提供する。	O.SYSTEM_MONITORING は、基準の数に基づいて、アクションを記録する監査メカニズムを設定する機能を管理者に提供することで、この脅威を軽減する。
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）。	O.RESIDUAL_INFORMATION_CLEARING TOE は、資源が再割当されるとき、保護された資源に含まれるデータが使用できないことを保証する。	O.RESIDUAL_INFORMATION_CLEARING は、資源がある利用者/プロセスから解放され、別の利用者/プロセスに割り当てられるとき、TSF データと利用者データが永続的に残らないことを保証することで、この脅威に対抗する。
P.COMPATIBILITY TOE は、同じプロトコルを使用して他のネットワーク機器との相互接続を実現するために、実装されたプロトコルについて RFC（Request for Comments）要件を満たさなければならない（must）。	O.PROTOCOLS TOE は、相互接続性を保証するために、RFC 及び/または工業仕様書に従って標準化されたプロトコルが TOE に実装されていること及び集中監査サーバ及び RADIUS 認証サーバとの通信をサポートしていることを保証する。	O.PROTOCOLS は、同じプロトコルを使用する IT エンティティ間の相互接続性を保証するために、標準化されたプロトコルを TOE に実装することを要求することで、この方針を満たす。
P.CONFIGURABILITY TOE は、運用のセキュリティ関連観点を設定する機能を提供しなければならない（must）。	O.TOE_ADMINISTRATION TOE は、管理者が TOE を設定できるメカニズムを提供する。	O.TOE_ADMINISTRATION は、TOE をセキュアに設定するのに必要なメカニズムを、TOE が提供することを保証することで、この方針を満たす。

29 表 7 に、セキュリティ対策方針と前提条件の対応関係を示す。

表 7：セキュリティ対策方針と前提条件の対応関係

前提条件	前提条件に対応する 対策方針	根拠
A.NO_TOE_BYPASS 情報は、TOEを通過しないでVPNクライアントのホストが接続されているネッ	OE.NO_TOE_BYPASS 情報は、TOEを通過しないでVPNクライアントのホストが接続されているネットワーク上を流れ	OE.NO_TOE_BYPASS は、ネットワーク上を流れるすべての情報が、TOE を通過することを保証する。

前提条件	前提条件に対応する 対策方針	根拠
トワーク上を流れることができない。	ることができない。	
A.PHYSICAL TOE 及びそこに含まれるデータの価値に相当する物理的なセキュリティが、環境によって提供されると仮定する。	OE.PHYSICAL TOE及びそこに含まれるデータの価値に相当する物理的なセキュリティが、運用環境によって提供されると仮定する。	OE.PHYSICAL は、TOE、TSF データ及び保護される利用者データが、物理的な攻撃（盗難、改ざん、破壊、または盗聴など）から保護されることを保証する。物理的な攻撃には TOE 環境への許可されていない侵入者を含めることもできるが、TOE 環境へのアクセスを許可されている個人によって行われる物理的な破壊行為は含まれない。
A.TRUSTED_ADMIN TOE 管理者は、信頼される方法ですべての管理者ガイダンスに従い、適用するものと信頼される。	OE.TRUSTED_ADMIN TOE 管理者は、信頼される方法ですべての管理者ガイダンスに従い、適用するものと信頼される。	OE.TRUSTED_ADMIN は、管理者が適正に訓練され、管理者ガイダンスで間違いを避けるために環境と TOE を正しく設定する方法が管理者に指示されていることを保証する。

4　セキュリティ要件及び根拠

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

- 評価対象の正確な記述を提供するため。通常、TOE に関するセキュリティ対策方針が自然言語で作成されるため、標準化された言語への翻訳が、TOE の機能のより正確な記述を強化する。
- 2 つの ST を比較できるようにするため。異なる ST 執筆者がセキュリティ対策方針を記述する際に異なる用語を使用する場合があるので、標準言語が同じ用語と概念の使用を強化する。これが容易な比較を可能にする。

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

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

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

34 将来のプロテクションプロファイルでは、実際の製品評価から学んだ教訓に基づいて、より詳細な保証アクティビティが提供される。

4.1　セキュリティ機能要件

35 本節は、TOE によって提供されるセキュリティ機能に特有の TOE のセキュリティ要件を識別し、また、他の TOE からの VPN クライアントを区別する。SFR の重点分野は、監査、暗号、セキュリティ管理、セルフテスト及び許可された外部 IT エンティティ（VPN ゲートウェイなど）との通信に関連する。

表 8：TOE セキュリティ機能要件

機能クラス	機能コンポーネント
セキュリティ監査（FAU）	FAU_GEN.1 監査データ生成
	FAU_SEL.1 選択的監査
暗号サポートクラス（FCS）	FCS_CKM.1 暗号鍵生成（非対称鍵）
	FCS_CKM_EXT.4 暗号鍵ゼロ化
	FCS_COP.1(1) 暗号操作（データ暗号化/復号）
	FCS_COP.1(2) 暗号操作（暗号署名）
	FCS_COP.1(3) 暗号操作（暗号ハッシュ）
	FCS_COP.1(4) 暗号操作（鍵付ハッシュメッセージ認証）
	FCS_IPSEC_EXT 拡張:インターネットプロトコルセキュリティ（IPsec）通信
	FCS_RBG_EXT.1 拡張: 暗号操作（ランダムビット生成）
利用者データ保護クラス（FDP）	FDP_RIP.2 残留情報完全保護
識別及び認証クラス（FIA）	FIA_PSK_EXT.1 拡張：事前共有鍵作成
	FIA_X509_EXT.1 拡張：X.509 証明書
セキュリティ管理クラス（FMT）	FMT_SMF.1 管理機能の指定
TSF の保護（FPT）	FPT_TST_EXT.1 拡張：TSF テスト
	FPT_TUD_EXT.1 拡張：高信頼更新
高信頼パス/チャネル（FTP）	FTP_ITC.1 TSF 間高信頼チャネル

4.1.1 クラス：セキュリティ監査（FAU）

セキュリティ監査データ生成（FAU_GEN）

FAU_GEN.1　　監査データ生成

FAU_GEN.1.1　TSF は、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（shall）。

a) 監査機能の起動及び終了、

b) 監査の指定なしのレベルに関するすべての監査対象事象及び

c) *すべての*管理者アクション、

d) [*特に表 9 に記載の定義済みの監査対象事象*]。

適用上の注意：

36 *ST 執筆者は、他の監査対象事象を直接表に含めることができる。それらは提供されている表に限定されるものではない。*

37 *「a」の場合、参照された監査機能は TOE によって提供されるものである。例えば、TOE がスタンドアロン実行可能であって、TOE 自身の起動と終了を監視していた場合、本条項の要件を満たすのに十分である。*

38 *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 9 には記載されていない。TOE 自身が、管理者用の I&A を実行する機能を提供する必要はないが、本要件は、PP によって記述される事象を TOE が「管理者アクション」として（主として TOE によって提供される機能の設定を対応する）監査する能力があることを暗示する。OPE ガイダンスは TOE によって作成される監査データを保証するために必要な手順を詳しく説明し、基盤となる IT 環境の監査能力と統合されると予想される。*

保証アクティビティ：

39 *評価者は、運用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（must）。評価者は、PP で強制された監査対象事象の種別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 9 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確認しなければならない（shall）。*

40 *評価者は、特に失敗した暗号事象に関する内容が明記されていることを確認しなければならない（shall）。表 9 では、操作の暗号モードを詳述する情報及び暗号化されるオブジェをレビューする管理者が（例えば、鍵ネゴシエーション交換中に実行される、通過中のデータを暗号化するときに実行される）暗号操作の文脈及び他の IT システムとの通信に関連する暗号失敗に関する接続の TOE 以外のエンドポイントを決定できるほど十分であることを確認しなければならない（shall）。*

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

42 *評価者は、本 PP 内の機能要件に関連する保証アクティビティに従って TOE に監査記録を生成させることで、TOE が監査記録を正しく生成する機能をテストしなければならない（shall）。さらに、評価者は、本 PP の文脈において適用可能な各管理アクションが監査可能であることをテストしなければならない（shall）。テスト結果を検証する際、評価者は、テスト中に生成される監査記録が管理ガイドに規定されている書式と一致し、各監査記録の項目に適切な項目があることを確認にしなければならない（shall）。*

43 *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（should）。
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（shall）。

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、[*下記の表の第 3 列に規定されている情報*]。

適用上の注意：

44 *以前のコンポーネントでは、ST 執筆者は他の追加情報を生成して表 9 を更新するべきである（should）。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。*

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

表 9：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_SEL.1	監査収集機能の実行中に行われる監査設定に対するすべての変更。	なし。
FCS_CKM.1	鍵生成アクティビティの失敗。	なし。
FCS_CKM_EXT.4	鍵ゼロ化プロセスの失敗。	消去中のオブジェクトまたはエンティティの識別情報。
FCS_COP.1(1)	暗号化または復号の失敗。	操作の暗号モード、暗号化/復号されるオブジェクトの名前/識別子。
FCS_COP.1(2)	暗号署名の失敗。	操作の暗号モード、署名/検証されるオブジェクトの名前/識別子。
FCS_COP.1(3)	ハッシュ関数の失敗。	操作の暗号モード、ハッシュされるオブジェクトの名前/識別子。
FCS_COP.1(4)	データ以外の完全性のための暗号ハッシュの失敗。	操作の暗号モード、ハッシュされるオブジェクトの名前/識別子。
FCS_IPSEC_EXT.1	TOE によって所有されるネットワークパケットを、DISCARD、BYPASS、PROTECT するという決定。 IPsec SA の確立の失敗。 IPsec SA の確立/終了。	ソースサブジェクトの推定される識別。 送信先サブジェクトの識別。 該当する場合は、トランスポート層プロトコル。 該当する場合は、ソースサブジェクトサービスの識別子。 決定に適用される SPD 内のエントリ。

		失敗の理由。 成功と失敗両方の接続の TOE 以外のエンドポイント（IP アドレス）。
FCS_RBG_EXT.1	プロセスのランダム化失敗。	なし。
FDP_RIP.2	なし。	
FIA_PSK_EXT.1	なし。	
FIA_X509_EXT.1	なし。	
FMT_SMF.1	なし。	
FPT_TST_EXT.1	この TSF セルフテスト集合の実行。 検出された完全性違反。	完全性違反の場合、完全性違反を引き起こした TSF コードファイル。
FPT_TUD_EXT.1	更新の開始。 更新の完全性検証の失敗。	追加情報なし。
FTP_ITC.1	高信頼チャネルを確立しようとするすべての試行。 チャネルデータの変更の検出。	チャネルの TOE 以外のエンドポイントの識別。

セキュリティ監査事象選択（FAU_SEL）

FAU_SEL.1　　選択的監査

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

a) 事象種別、

b) 監査可能セキュリティ事象の成功、

c) 監査可能セキュリティ事象の失敗及び

d) [割付：その他の属性]。

適用上の注意：

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

保証アクティビティ：

47 *評価者は、割付に記載されている属性を含むように、要件に従ってすべての事象種別が箇条書きにされ、選択可能なすべての属性が記述されていることを確認するために管理者ガイダンスをレビューしなければならない（shall）。また、管理者ガイダンスは、事前選択を設定する方法に関する指示を含み、複数の値を持つ事前選択用の構文（存在する場合）を説明しなければならない（shall）。*

また、管理者ガイダンスは、現在施行されている選択条件にかかわらず、常に記録される監査記録を識別しなければならない（shall）。

48 *評価者は、以下のテストも実行しなければならない（shall）。*

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

4.1.2 クラス：暗号サポート（FCS）

FCS_CKM.1　　暗号鍵生成（非対称鍵）

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

[選択：

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

適用上の注意：

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

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

51 *生成される2048ビットDSA及びrDSA鍵の鍵強度は、112ビットの対称鍵強度と等価または*

それ以上である必要がある。等価な鍵強度の詳細は、NIST Special Publication 800-57、「Recommendation for Key Management」を参照。

保証アクティビティ：

52 評価者は、ST 執筆者によって行われた選択に応じて、上記の要件をテストする際のガイドとして、「The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)」、「The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)」及び「The RSA Validation System (RSA2VS)」の鍵ペア生成部分を使用しなければならない（shall）。これには、評価者がテスト中に検証可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。

53 行われた選択に応じて TSF が 800-56A 及び/または 800-56B に適合することを示すために、評価者は、TSS に以下の情報が含まれていることを確認しなければならない（shall）。

- TSS は、TOE が適合する該当する 800-56 規格のすべての節を記載しなければならない（shall）。
- TSS に記載される該当する節ごとに、「shall」（しなければならない）でない（すなわち「shall not」（してはならない）、「should」（するべきである）及び「should not」（するべきでない））すべての文について、TOE がこのようなオプションを実装する場合は、それを TSS に記述しなければならない。含まれる機能が規格に「shall not」（してはならない）または「should not」（するべきでない）と示されている場合、TSS は、TOE によって実装されたセキュリティ方針に悪影響しない（will not）根拠を提供しなければならない（shall）。
- （選択された）800-56A 及び 800-56B の該当する節ごとに、「shall」（しなければならない）または「should」（するべきである）文に関連する機能の省略を記述しなければならない（shall）。

TOE が実施すべきセキュリティ要件に影響を与える可能性のあるような TOE 固有の拡張（may）、文書に含まれない処理、または文書によって許可される代替実装について記述しなければならない。

FCS_CKM_EXT.4　暗号鍵のゼロ化

FCS_CKM_EXT.4.1 **詳細化**：TSF はすべての平文の秘密鍵及び秘密鍵と CSP 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：

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

55 上記のゼロ化は、鍵／CSP をほかの記憶場所に移動させる際に、平文のカギ／CSP のための、それぞれの中間格納領域（つまり、メモリバッファのような、データが流れる経路に含まれるストレージ）に適用される。

56 TOE は、必ずしもホスト IT 環境を含むとは限らないため、本機能の範囲は、ある程度は必ず制限される。本要件の目的は、TOE がゼロ化を実行するためにホストの正しい基本的な機能を呼び出すのに十分である。これは、データが確実にゼロ化されるために TOE がカーネルモードのメモリドライバを含んでいなければならないことを意味しているのではない。

保証アクティビティ：

57 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）、秘密鍵及び

58

鍵生成のために利用される CSP、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種別（ゼロで上書き、ランダムパタンで 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確認しなければならない（shall）。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 回上書きされるが、内部ハードドライブに格納された秘密鍵は、それぞれの書き込み動作前に変更されるランダムパタンを使って 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確認しなければならない（shall）。ゼロ化を検証するためにリードバックがされている場合、これも同様に記載されていなければならない（shall）。

暗号操作（FCS_COP）

FCS_COP.1(1)　　暗号操作（データ暗号化／復号）

FCS_COP.1.1(1)　**詳細化**：TSF は、以下に合致する 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：

59 *割付に関して、ST 執筆者は 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 執筆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 執筆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：

60 *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）
これには、評価者がテスト中に検証可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。

FCS_COP.1(2)　　暗号操作（暗号署名）

FCS_COP.1.1(2)　**詳細化**：TSF は、以下に従って**暗号署名サービス**を実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）の電子署名アルゴリズム（DSA）

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

(3) 256 ビット以上の鍵サイズの楕円曲線電子署名アルゴリズム（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 の将来のバージョンで要求される。

であり、以下に準拠するもの：

電子署名アルゴリズムの場合：

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

RSA 電子署名アルゴリズムの場合：

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

楕円曲線電子署名アルゴリズムの場合：

- **[選択：FIPS PUB 186-3、「Digital Signature Standard」]**
- **TSF は、（FIPS PUB 186-3、「Digital Signature Standard」に定義されている通り）「NIST 曲線（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：

61 *ST 執筆者は、電子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り（should）、複数のアルゴリズムが利用可能な場合は、本要件（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（should）。選択されたアルゴリズムに関して、ST 執筆者は適切な割付／選択を行い、そのアルゴリズムについて実装されたパラメタを特定するべきである（should）。*

62 *楕円曲線に基づくスキームに関して、鍵サイズはベースポイントの位数の log_2 をとった値を意味する。電子署名の望ましいアプローチとして、ECDSA は本 PP の将来のバージョンで要求される。*

保証アクティビティ：

63 *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）、「The Elliptic Curve Digital Signature Algorithm Validation System」（ECDSAVS）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 186-3）に従わなければならない（shall）。これには、評価者がテスト中に検証可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

FCS_COP.1(3)　　暗号操作（暗号ハッシュ）

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］及びメッセージダイジェストサイズ［選択：160、256、384］ビット**に従って、［暗号ハッシュサービス］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：

64 *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（must）。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（would）。*

保証アクティビティ：

65 *評価者は、上記の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）。これには、評価者がテスト中に検証可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

FCS_COP.1(4)　　暗号操作（鍵付ハッシュメッセージ認証）

FCS_COP.1.1(4)　**詳細化**：TSF は、以下に合致する**メッセージダイジェストのサイズ[選択：160、256、384] 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]** に従って、**鍵付ハッシュメッセージ認証**を実施しなければならない（shall）。
FIPS PUB 198-1、「The Keyed-Hash Message Authentication Code」及び FIPS PUB 180-3、「Secure Hash Standard」。

適用上の注意：

66 *ハッシュ生成アルゴリズムの選択は、メッセージダイジェストサイズの選択に対応していなければならない（must）。例えば、HMAC-SHA-256 が選択される場合、有効なメッセージダイジェストサイズ選択は 256 ビットのみである。*

67 *上記のメッセージダイジェストサイズは、使用される基礎となるハッシュアルゴリズムに対応する。なお、ハッシュ計算に続く HMAC 出力の切詰めは、様々なアプリケーションで適切なステップである。これによりこの要件との適合が無効になるわけではないが、切詰めが実行されること、最終出力のサイズ及びこの切詰めが適合する規格を ST に記載するべきである（should）。*

保証アクティビティ：

68 *評価者は、上記の要件をテストする際のガイドとして、「The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)」を使用しなければならない（shall）。 これには、評価者がテスト中に検証可能なテストベクターを生成できるアルゴリズムの高信頼参照実装を保有することが要求される。*

拡張：インターネットプロトコルセキュリティ（FCS_IPSEC_EXT）

69 本構成要素は、実装される予定の IPsec アーキテクチャ及び適合する TOE のプロトコルを規定する。IPsec アーキテクチャは、RFC 4301 に定義される。本 PP に含まれる要件は、VPN クライアントがトランスポートとトンネルモードの両方を実装することを義務付けている。実装されている IKE のバージョンに関連する RFC 4301 への適合に例外がある。RFC には、「注意：本書は、IKEv2 では利用可能だが IKEv1 では利用可能ではない、いくつかの機能、例えば、ローカル及びリモートの範囲をあらわす SA のネゴシエーション、または同じセレクターを持つ複数の SA のネゴシエーションなどのサポートを義務付けている。」という内容が記載されている。そのため、本文書は、IKEv2 または同等の機能を持つ鍵及びセキュリティアソシエーション管理システムの使用を前提としている。PP の本バージョンに対し、ST 執筆者は、IKE のどちらかのバージョンを実装する選択肢を有する。IKEv2 なしで IKEv1 を選んだ場合、TOE は技術的に RFC 4301 に適合しないが、VPN クライアント PP の本バージョンに適合すると考えられる。PP の以降のバージョンは、IKEv2 を必要とする可能性が高い。

70 TOE は、VPN ピア（その他の VPN クライアントエンドポイント及び VPN ゲートウェイ）と通信するために使用される接続を確立するために使われる IPsec プロトコルを使用するため

に必要とされる。他の IT エンティティ（監査サーバなど）やリモート管理者が、特定の TOE のために IPsec を使用する場合は、この要件も適合される。

FCS_IPSEC_EXT.1　拡張:インターネットプロトコルセキュリティ（IPsec）通信

FCS_IPSEC_EXT.1.1　TSF は、RFC4301 に規定されている通り、IPsec アーキテクチャを実装しなければならない(shall)。

FCS_IPSEC_EXT.1.2　TSF は、トランスポートモードとトンネルモードの両方を実装しなければならない（shall）。

FCS_IPSEC_EXT.1.3　TSF は、他に一致しないものすべてと合致し、破棄する名目上の最終エントリを持つべきである（should）。

FCS_IPSEC_EXT.1.4　TSF は、AES-CBC-128、AES-CBC-256（ともに RFC 3602 に規定されている）、[選択：他のアルゴリズムなし、RFC 4106 に規定されている暗号アルゴリズム AES-GCM-128、AES-GCM-256]を使用して、RFC4303 によって定義される IPsec プロトコル ESP を実装しなければならない（shall）。

FCS_IPSEC_EXT.1.5　TSF は、次のプロトコルを実装しなければならない（shall）。[選択、1 つ以上を選択する：RFC 2407、2408、2409、RFC4109 に定義されている IKEv1]及び[選択：ハッシュ関数に関する他の RFC なし、ハッシュ関数に関する RFC 4868]、RFC 5996（2.23 節に規定されている必須の NAT トラバースのサポート付き）と 4307 に定義されている IKEv2 及び[選択：ハッシュ関数に関する他の RFC なし、ハッシュ関数に関する RFC 4868]。

FCS_IPSEC_EXT.1.6　TSF は、ESP 機密性及び完全性セキュリティサービスのみが使用されることを保証しなければならない（shall）。

FCS_IPSEC_EXT.1.7　TSF は、IKEv1 Phase 1 交換がメインモードのみを使用することを保証しなければならない（shall）。

FCS_IPSEC_EXT.1.8　TSF は、[選択：IKEv1 SA のライフタイムライフタイムがパケット数と時間で制限できる：Phase 1 SA は 24 時間、Phase 2 SA は 8 時間、IKEv2 SA のライフタイムがパケット数と時間に基づいて管理者によって設定できる]ことを保証しなければならない（shall）。

FCS_IPSEC_EXT.1.9　TSF は、FCS_RBG_EXT.1 に規定されているランダムビット生成器を使用して、[割付：NIST SP 800-57、*Recommendation for Key Management – Part 1：General* の Table 2 に記載されている、ネゴシエーションされる Diffie-Hellman グループに関連付けられた「セキュリティのビット数」の値の 2 倍以上である（1 つまたは複数の）ビット数]ビット以上の長さを持つ、IKE Diffie-Hellman 鍵交換で使用される秘密の値 x（「x」は gx mod p の x）を生成しなければならない（shall）。

FCS_IPSEC_EXT.1.10 TSF は、特定の IPsec SA のライフタイム中に特定のナンス値が繰り返される確率が 2^[割付：NIST SP 800-57、R*ecommendation for Key Management – Part 1：General* の Table 2 に記載されている、ネゴシエーションされる Diffie-Hellman グループに関連付けられた「セキ

ュリティのビット数」]の中の 1 未満になるような方法で IKE 交換に使用されるナンスを生成しなければならない（shall）。

FCS_IPSEC_EXT.1.11 TSF は、すべての IKE プロトコルが、DH Group 14（2048 ビット MODP）及び[選択：DH Group 24（*256 ビット POS を備えた 2048 ビット MODP*）、DH Group 19（*256 ビットランダム ECP*）、DH Group 20（*384 ビットランダム ECP*）、[割付：TOE によって実装された他の DH グループ]、*他の DH グループなし*]を実装することを保証しなければならない（shall）。

FCS_IPSEC_EXT.1.12 TSF は、すべての IKE プロトコルが事前共有鍵及び RFC 4945 に適合する X.509v3 証明書を使用する[選択、1 つ以上を選択する：*DSA*、*rDSA*、*ECDSA*]を使用して、ピア認証を実装することを保証しなければならない（shall）。

FCS_IPSEC_EXT.1.13 TSF は、既定で、[選択：*IKEv1 Phase 1*、*IKEv2 IKE_SA*]接続を保護するためにネゴシエーションされる対称アルゴリズムの（鍵のビット数としての）強度が、ネゴシエーションされる保護する[選択：*IKEv1 Phase 2*、*IKEv2 CHILD_SA*]接続を保護するためにネゴシエーションされる対称アルゴリズムの（鍵のビット数としての）強度以上であることを保証できなければならない（shall）。

適用上の注意：

71 *FCS_IPSEC_EXT.1.1 は、IPsec の実装が、IPsec 装置（ゲートウェイまたはホスト）の構造上及び機能上の観点に適合しなければならないことを規定している。ここで規定されている「MAY」（トランスポートモードをサポートする。）及び「SHOULD」（他の「ルール」に一致しないパケットを捨てる SPD の最後のエントリ）として、RFC がこれらの機能を識別するので、ここで規定される要素 FCS_IPSEC_EXT.1.2 及び FCS_IPSEC_EXT.1.3 は文章でなければならない（shall）。*

72 *FCS_IPSEC_EXT.1.4 は、ESP の実装において使用されなければならないアルゴリズムを義務付け（must）、TOE 評価の一部として考慮される 2 つのほかのアルゴリズムを選択することを可能にする。*

73 *FCS_IPSEC_EXT.1.5 は、IKE に関する TOE の実装を規定するために ST 執筆者によって使用される。適合 TOE は両方を提供できるが、IKEv1 または IKEv2 のいずれかのサポートを提供しなければならない（must）。最初の選択は選ぶために使用される。IKEv1 の場合、要件は、RFC 2409（満たされなければならない RFC2407 及び 2408 の観点を規定している（must））に適合する IKE 実装に、RFC 4109 に記述されている追加/変更を加えることが要求されると解釈されるべきである。RFC 4868 は、IKEv1 と IKEv2 の両方で使用するための追加のハッシュ関数を識別する。これらの関数が実装される場合は、3 番目（IKEv1 の場合）及び 4 番目（IKEv2 の場合）の選択を使用できる。*

74 *FCS_IPSEC_EXT.1.8：ST 執筆者は、FCS_IPSEC_EXT.1.5. の選択に応じて、IKEv1 要件または IKEv2 要件のいずれか（または両方）を選択する。IKEv1 要件は、（AGD_OPE によって義務付けられた文書内の該当する指示により）許可された管理者が設定可能なライフタイムを提供する、または実装に制限を「ハードコード」することで、達成できる。IKEv2 の場合、ハードコード化される制限はないが、この場合には管理者が値を設定できることが要求される。一般に、SA のライフタイムを含めて実装のパラメタを設定するための指示は、AGD_OPE 用に生成される管理者ガイダンスに含めるべきである（should）。TOE が同じ鍵で保護されるトラフィックの量（その鍵で保護されるすべての IPsec トラフィックの総量）に対する制限を設定できる限り、パケット数の代わりに MB/KB 数を使用して要件を詳細化すること*

が適切である。

75 *実装では SA の形成に使用するために異なる Diffie-Hellman グループをネゴシエーションできるので（may）、FCS_IPSEC_EXT.1.9 と FCS_IPSEC_EXT.1.10 の割付に複数の値を含めることができる（may）。サポートされる DH グループごとに、ST 執筆者は、800-57 の表 2 を参照して、DH グループに関連付けられた「セキュリティのビット数」を決定する。次に、一意の値を使用して、割付を記入する（1.9 の場合は 2 倍にされ、1.10 の場合は割付に直接挿入される）。例えば、実装が DH グループ 14（2048 ビット MODP）及びグループ 20（NIST 曲線 P-384 を使用する ECDH）をサポートすると仮定する。表 2 から、セキュリティのビット数の値は、グループ 14 では 112、グループ 20 では 192 である。次に、FCS_IPSEC_EXT.1.9 では割付が「224、384」になり（would）、FCS_IPSEC_EXT.1.10 では「112、192」になる（would）（ただし、この場合は、おそらく数学的に意味を持つように要件を詳細化するべきであろう（should））。*

76 *FCS_IPSEC_EXT.1.11：選択は、サポートされる追加の DH グループを指定するために使用される。これは、IKEv1 及び IKEv2 交換に適用される。本 PP の将来のバージョンでは、DH グループ 19（256 ビットランダム ECP）及び DH グループ 20（384 ビットランダム ECP）が要求される。追加の DH グループが指定される場合は、それらの DH グループが（確立された一時鍵の観点から）FCS_CKM.1 に記載されている要件に適合しなければならない（must）ことに注意するべきである。*

77 *FCS_IPSEC_EXT.1.12：事前共有鍵及び 1 つ以上の公開鍵に基づくピア認証方法が適合 TOE に要求される。ST 執筆者は、TOE の実装を反映するために 1 つまたは複数の公開鍵スキームを選択する。また、ST 執筆者は、それらの方法をサポートするために、使用されるアルゴリズム（及び提供される場合は鍵生成機能も）を反映する適切な FCS 要件が記載されていることを確認する。なお、TSS は、これらのアルゴリズムを使用する方法を詳述する（例えば、2409 は、公開鍵を使用する 3 つの認証方法を規定し、サポートされる各方法が TSS に記述される）。*

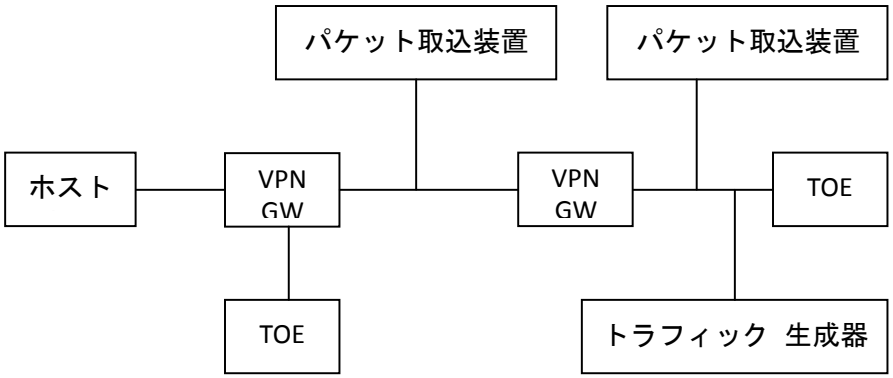
78 *FCS_IPSEC_EXT.1.13：ST 執筆者は、TOE の実装に基づいて、IKE 選択のいずれかまたは両方を選択する。明らかに、選択される IKE バージョンは、このコンポーネントだけでなく、このエレメント内の他のエレメントに関する他の選択とも一貫しているべきである（should）。TOE はこの機能を設定可能にしてもよいが、評価される構成の既定の設定（「出荷時」または OPE 構成文書内のガイダンス文書による）は、この機能を有効にしなければならない（must）。*

保証アクティビティ：

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

- *いずれかの FCS_IPSEC_EXT.1 エレメントについて記載されている該当する各 RFC の節ごとに、「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）及び「SHOULD NOT」（するべきでない）など）すべての文について、TOE がこのようなオプションを実装する場合は、それを TSS に記述しなければならない（shall）。含まれる機能が規格に「SHOULD NOT」（するべきでない）または「MUST NOT（してはならない）と示されている場合、TSS は、TOE によって実装されたセキュリティ方針に悪影響しない根拠を提供しなければならない（shall）。*
- *各 RFC の節ごとに、「SHOULD」（するべきである）文に関連する機能の省略を記述しなければならない（shall）。*

TOE が施行する予定のセキュリティ要件に影響するかもしれない TOE 固有の拡張、規格に含まれない処理、または規格によって許可される代替実装を記述しなければならない（shall）。



80 *評価者は、上記で示したテスト環境と同等のテスト環境を最低限作らなければならない（shall）。TOE の 2 通りの具体化が、TOE がピア TOE で動作可能なことを検証するために必要であることが期待される。また、TOE が操作のトランスポートモードを正しく実装できることを実証するために、VPN ゲートウェイ（図中の VPN GW）が使用されることも期待される。トラフィック生成器トラフィック生成器が、ネットワークパケットを構築するために使用されること、さらに評価者に、ICMP、IPv4、IPv6、UDP 及び TCP パケットヘッダーにあるフィールドを操作できる能力を与えることが期待される。評価者は、テスト環境に差分の正当化を提供しなければならない（must）。その正当化の 1 つは、ホストがトラフィック生成器を実装できるものかもしれない（may）。評価者が、有線上に実際にあるパケットにアクセスすることが期待されるため、パケット取込装置用に同じ引数を作るのははるかに困難だろう。*

81 *FCS_IPSEC_EXT.1.1 - 評価者は、運用ガイダンスが DISCARD、BYPASS 及び PROTECT のためのルールを規定する SPD にエントリを構築する方法を評価者に示していることを検証するために、運用ガイダンスを検査しなければならない（shall）。*

- *テスト 1：評価者は、DISCARD、BYPASS 及び PROTECT のためのルールがある TOE の SPD を設定しなければならない（shall）。ルールの構築に使用されるセレクターは、各パケットが 3 つのルールのうちの 1 つに合致するパケットヘッダーにある適切なフィールドと一緒に 3 つのネットワークパケットで評価者が送信できるものと異なっていなければならない（shall）。評価者は、適切なパケットが破棄され、修正なしで通り抜けることを許可され、IPsec 実装で暗号化されるといった、期待された動作を TOE が示したとことを、監査証跡及びパケットキャプチャで確認する。*
- *テスト 2：評価者は、代替操作（BYPASS と PROTECT）と一緒に２つの同等な SPD エントリを考案しなければならない（shall）。エントリは、2 つの異なる順番で配置されなければならない（should）、いずれの場合も評価者は、適切なパケットを作成すること及びパケットキャプチャと確認用のログを使って、最初のエントリが両方の場合で強制されていることを確認しなければならない（shall）。*
- *テスト 3：評価者は、1 つがもう一方のサブセットである 2 つのエントリが展開されるべき場合(例えば、特定のアドレス対ネットワークセグメント)を除き(should)、上記の手順を繰り返さなければならない（shall）。再度、ルールの特異性に関わらず、評価者は、最初のエントリが強制されていることを確認するために両方の順番をテストすべきである（should）。*

82 *FCS_IPSEC_EXT.1.2 - 評価者は、運用ガイダンスが各モードで TOE が設定される方法を管理者に示していることを確認しなければならない（shall）。*

- *テスト 1：評価者は、トンネルモードの TOE とトンネルモードの VPN GW を設定するために運用ガイダンスを使用する。評価者は、許容される暗号アルゴリズム、認*

証手法などのいずれかを使用するため、さらに許容される SA がネゴシエーション ネゴシエーションされることが可能であることを保証にするために 2 つの装置を設定する。次に、評価者は、ピア間でセションを開始しなければならない(shall)。評価者は、監査証跡及びキャプチャーされたパケットで、トンネルモードを使って正常な接続が確立されたことを確認する。

- *テスト 2：評価者は、対象としての VPN GW（例えば、IPsec 接続上のテルネットを使った管理を目的として）で VPN GW に接続するトランスポートモードで動作する TOE を設定するために運用ガイダンスを使用する。評価者は、許容された暗号アルゴリズム、認証手法などのいずれかを使用するため、許容される SA がネゴシエーションされることが可能であることを保証にするために TOE と VPN GW を設定する。それから、評価者は、VPN クライアントを使って TOE との接続を開始する。評価者は、監査証跡及びキャプチャーされたパケットで、トランスポートモードを使って正常な接続が確立されたことを確認する。*

83 *FCS_IPSEC_EXT.1.3 - 評価者は、SPD に対してパケットが処理される方法、一致しない「ルール」があるかどうか、最後のルールが存在すること、暗黙的または明示的にネットワークパケットが破棄される原因となるものについて、TSS が説明していることを検証するために TSS を検査しなければならない（shall）。*

- *テスト 1：評価者は、ネットワークパケットを DISCARD、BYPASS 及び PROTECT する操作を含むエントリを持つ TOE の SPD を設定しなければならない(shall)。また、評価者は、FCS_IPSEC_EXT.1 に関するすべての監査対象事象を有効にするために TOE を設定する。評価者は、FCS_IPSEC_EXT.1.1 を憲章するために作られた SPD を使用することができる（may）。評価者は、BYPASS エントリに合致するネットワークパケットを構築し、そのパケットを TOE に送らなければならい（shall）。評価者は、ネットワークパケットが修正なしで TOE によって通されることを確認するべきである（should）。次に、評価者は、評価者が作成したエントリに一致しないパケットヘッダーにあるフィールドを修正しなければならない（shall）（以前のエントリのいずれにも合致しないパケットを破棄する最後のエントリである「TOE 作成」がある可能性がある（may））。評価者は TOE にパケットを送信し、パケットがどの TOE のインタフェースへも流れることを許可されなかったことを確認する。評価者は、予想通りにパケットが破棄されたことを明記する監査記録が作成されたことを確認しなければならない（shall）。*

84 *FCS_IPSEC_EXT.1.4 - 評価者は、すべての指定されたアルゴリズム（最低限、AES-CBC-128 と AES-CBC-256）が実装されていることを検証するために、TSS を検査しなければならない（shall）。*

85 *FCS_IPSEC_EXT.1.5- 評価者は、TOE によって少なくとも IKE の 1 つのバージョンが実装されていることを検証するために TSS を検査しなければならない（shall）。IKEv2 が実装されている場合、評価者は、TOE が RFC4301（IKEv1 でサポートされていない義務付けられた機能を IKEv2 のみがサポートする）に完全に適合する方法について、TSS が説明していることを保証する。*

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

- *テスト 1[条件付き]：評価者は、TSS 及び RFC 5996、2.23 節に記載されている通り NAT トラバース処理を実行するように、TOE を設定しなければならない（shall）。評価者は、IPsec 接続を開始し、NAT が正常に通過されることを確定しなければならない（shall）。*

87 *FCS_IPSEC_EXT.1.6 - 評価者は、「機密性専用」ESP セキュリティサービスを無効にする方法が記述されていることを検証するために、TSS を検査しなければならない（shall）。また、評価者は、ESP 用の「機密性専用」セキュリティサービスのネゴシエーションネゴシエーションを無効にするために必要な設定が記述されていること及びパケット全体を保護するためにトンネルモードが優先 ESP モードであることを示す報告が存在することを判定するために、運用ガイダンスを検査しなければならない（shall）。*

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

88 *FCS_IPSEC_EXT.1.7 - 評価者は、TOE によってサポートされる IPsec プロトコルの記述に、IKEv1 Phase 1 交換ではアグレッシブモードが使用されず、メインモードのみが使用されることが記載されていることを確認するために、TSS を検査しなければならない（shall）。これにより操作の前に TOE の設定が要求される場合、評価者は、この設定の指示が運用ガイダンスに含まれていることを確認するために、運用ガイダンスを調べなければならない（shall）。評価者は、以下のテストも実行しなければならない。（shall）。*

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

89 *FCS_IPSEC_EXT.1.8 - IKEv1 要件が選択される場合、評価者は、IKEv1 SA のライフタイム（Phase 1 と Phase 2 の両方）を確立する方法が TSS に記述されていることを確認する。ライフタイムが設定可能の場合、評価者は、これらの値を設定するための適切な指示が運用ガイダンスに含まれていることを検証する。IKEv2 要件について、評価者は、値が設定可能であり、値を設定するための指示が運用ガイダンスに存在することを検証する。また、評価者は、IKEv1、IKEv2、またはその両方を設定するかのいずれかに応じて、以下のテストを実行する*

- *テスト 1（IKEv1）：評価者は、Phase 1 SA が確立され、それが再ネゴシエーションされる前に 24 時間以上維持されるテストを作成しなければならない（shall）。評価者は、24 時間以内にこの SA が閉じられるか再ネゴシエーションされることを確認しなければならない（shall）。このようなアクションが、TOE が特定の方法で設定されることを要求する場合、評価者は、運用ガイダンスに記載されているように TOE の設定機能が動作することを実証するテストを実行しなければならない（shall）。*
- *テスト 2（IKEv1）：評価者は、Phase 2 SA についてテスト 1 と同様のテストを実行しなければならない（shall）。ただし、ライフタイムは 24 時間でなく 8 時間である。*
- *テスト 3（IKEv1 及び IKEv2）：評価者は、許可されるパケット数によって最大ライフタイムを設定しなければならない（shall）。これは IKEv1 の場合はハードコード化される値であってもよい（may）。そうでない場合、評価者は、運用ガイダンスに従う。評価者は、SA を確立し、この SA を通過するパケット数が許可されたパケット数を超えた場合、接続が閉じられることを確認しなければならない（shall）。*

- *テスト 4（IKEv2）：評価者は、SA の時間ベースの最大ライフタイムを設定し、次に SA を確立しなければならない（shall）。 評価者は、確立された時間内にこの SA が閉じられるか再ネゴシエーションされることを確認しなければならない（shall）。*

90 *FCS_IPSEC_EXT.1.9, FCS_IPSEC_EXT.1.10 - 評価者は、TSF によってサポートされる DH グループごとに、「x」（FCS_IPSEC_EXT.1.9 に定義されている通り）及び各ナンスを生成するプロセスを TSS が記述していることを確認しなければならない（shall）。評価者は、本 PP の要件に適合する生成される乱数が使用され、「x」の長さ及びナンスが要件の規定に適合することを TSS が示していることを確認しなければならない（shall）。*

91 *FCS_IPSEC_EXT.1.11 -評価者は、要件に規定されている DH グループが、TSS でサポートされるものとして記載されていることを確認しなければならない（shall）。複数の DH グループがサポートされている場合、評価者は、特定の DH グループがピアと一緒に指定/ネゴシエーションされる方法を TSS が記述していることを確認する。評価者は、次のテストも実行しなければならない（shall）。*

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

92 *FCS_IPSEC_EXT.1.12 - 評価者は、事前共有鍵が確立され、IPsec 接続の認証に使用される方法を TSS が記述していることを確認しなければならない（shall）。評価者は、TOE 用の事前共有鍵が生成及び確立される方法が運用ガイダンスに記述されていることを確認しなければならない（shall）。また、TSS 及び運用ガイダンスの記述には、単に事前共有鍵を使用するだけでなく、事前共有鍵を生成できる両方の TOE に対して、事前共有鍵の確立が施行される方法がしめされていなければならない（shall）。評価者は、次のテストも実行しなければならない（shall）。*

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

93 *評価者は、TOE によって使用される IKE ピア認証プロセスの記述が TSS に含まれていること及びこの記述が選択で指定されたアルゴリズムの使用を網羅していることを確認しなければならない(shall)。本コンポーネントに関する保証アクティビティの一環として、RFC 4945 の必須エレメントとオプションのエレメントが上記で詳述されたように記載されなければならない（shall）。評価者は、以下のテストも実行しなければならない（shall）。*

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

- *テスト 4：評価者は、CRL を通じて取り消された証明書が IKE ピア認証中に検出され、その結果、接続が確立されないことを実証するテストを考案しなければならない（shall）。*

94 *FCS_IPSEC_EXT.1.13 - 評価者は、IKE 及び ESP 交換に許可されるアルゴリズムの潜在的な強度（対称鍵のビット数として）が TSS に記述されていることを確認しなければならない（shall）。TSS には、ネゴシエーションされるアルゴリズムの強度（対称アルゴリズム内の鍵のビット数として）がネゴシエーションを保護している IKE SA の強度以下であることを確認するために、IKEv1 Phase 2 及び/または IKEv2 CHILD_SA スイートをネゴシエーションするときに行われるチェックも記述されていなければならない（shall）。評価者は、以下のテストも実行しなければならない（shall）。*

- *テスト 1：このテストは、TOE によってサポートされる IKE のバージョンごとに実行されなければならない（shall）。評価者は、サポートされている各アルゴリズム及び要件に識別されているハッシュ関数を使用して、IPsec 接続を正常にネゴシエーションしなければならない（shall）。*
- *テスト 2：このテストは、TOE によってサポートされる IKE のバージョンごとに実行されなければならない（shall）。評価者は、IKE SA に対して使用されている暗号化アルゴリズムより強度が高い暗号化アルゴリズム（すなわち、IKE SA 用に使用される鍵サイズより大きい鍵サイズを持つ対称アルゴリズム）を選択する ESP 用の SA の確立を試行しなければならない（shall）。こういった試行は失敗するべきである（should）。*
- *テスト 3：このテストは、TOE によってサポートされる IKE のバージョンごとに実行されなければならない（shall）。評価者は、サポートされたアルゴリズムのひとつではないアルゴリズム及び要件で識別されるハッシュ関数を使って、IKE SA の確立を施行しなければならない（shall）。そのような試行は失敗するべきである（should）。*
- *テスト 4：このテストは、TOE によってサポートされる IKE のバージョンごとに実行されなければならない（shall）。評価者は、FCS_IPSEC_EXT.1.4 で識別されていない暗号化アルゴリズムの選択をする ESP 用の SA（IKE SA を確立するために使用される適切なパラメタが想定される）の確立を施行しなければならない(shall)。そのような試行は失敗するべきである（should）。*

拡張：暗号操作（ランダムビット生成）（FCS_RBG_EXT）

FCS_RBG_EXT.1　　拡張：暗号操作（ランダムビット生成）

FCS_RBG_EXT.1.1　TSF は、[選択、1 つを選択：[選択：Hash_DRBG（任意）、HMAC_DRBG（任意）、CTR_DRBG（AES）、Dual_EC_DRBG（任意）]を使用する NIST Special Publication 800-90、FIPS Pub 140-2 Annex C、AES を使用する X9.31 Appendix 2.4]に従って、選択したエントロピーを蓄積するエントロピー源によってシードされたすべてのランダムビット生成（RBG）サービスを実行しなければならない（shall）。
[選択：ひとつを選択：
1 つ以上の独立したハードウェアベースのノイズ源、
1 つ以上の独立したソフトウェアベースのノイズ源、
ハードウェアベースとソフトウェアベースのノイズ源の組み合わせ]。

FCS_RBG_EXT.1.2　決定性 RBG は、少なくともそれが生成する鍵と認可ファクタの最も大

きいビット長に等しい、最低でも[選択、1つを選択：128ビット、256ビット]のエントロピーによってシードされなければならない（shall）。

適用上の注意：

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

96 *FCS_RBG_EXT.1.1の最初の選択では、ST執筆者は、RBGサービスが適合する規格（800-90または140-2 Annex Cのいずれか）を選択するべきである（should）。2番目の選択として、ST執筆者は、クライアントがRBG用のエントロピーを集める方法を示す。*

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

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

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

100 *将来は、A Method for Entropy Source Testing：Requirements and Test Suite Descriptionに記載されているほとんどの要件が、本PPによって要求される。現在、以下の保証アクティビティは、要求されるアクティビティのサブセットのみを反映している。*

保証アクティビティ：

101 *評価者は､TOEで使用されるRBGを含んでいる製品のバージョン番号を決定するために､TSS節をレビューしなければならない（shall）。また評価者は、エントロピーが収集されるノイズ源がTSSに記載されていることも確認しなければならない（shall）。さらに、評価者は､RBGに使用されるすべての基礎となる関数とパラメタがTSSに記載されていることを検証する。*

102 *評価者は､エントロピー入力を取得する方法､使用されるエントロピー源を識別する方法、各エントロピー源からエントロピーを生成/収集する方法、各エントロピー源によって生成されるエントロピーの量など､RBGモデルの記述がTSSに含まれていることを検証しなければならない（shall）。また、評価者は、エントロピー源ヘルステスト、エントロピー源のヘルスを決定するためにヘルステストが十分である根拠及びエントロピー源の故障の既知のモードがTSSに記載されていることを確認しなければならない（shall）。最後に、評価*

者は、時間及び/または環境条件による出力と分散の独立性の観点で、RBG 出力の記述が TSS に含まれていることを検証しなければならない（shall）。

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

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

104 *また、評価者は、RBG が適合する規格に応じて、以下のテストを実行しなければならない（shall）。*

FIPS 140-2、Annex C に適合する実装

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

106 *評価者は、可変シードテストを実行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）。また、評価者は、すべての 128 ペア（シード、DT）に対して一定の値の（AES アルゴリズムについて適切な長さの）鍵を提供しなければならない（shall）。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）。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。*

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

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

108 *評価者は、RNG 実装に対して 15 回試行を実施しなければならない（shall）。RNG が設定変更可能な場合、評価者は設定ごとに 15 回試行を実施しなければならない（shall）。また、評価者は、RNG 機能性を設定するために適切な指示が運用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）。*

109 *RNG が予測耐性を備えている場合、それぞれの試行は(1)drbg の具体化、(2)ランダムビット列の 1 番目のブロックの生成、(3)ランダムビット列の 2 番目のブロックの生成、(4)終了処理(ゼロ化）、から成り立つ。評価者は、ランダムビット列の 2 番目のブロックが期待値であることを検証する。評価者は、それぞれの試行について 8 つの入力値を生成しなければならない（shall）。 1 番目は、整数カウンタ（0-14）である。次の 3 つは、具体化操作のためのエントロピー入力、ナンス（Nonce）及び個別化文字列である。次の 2 つは、（乱数）生成の初回の呼び出しについての追加入力とエントロピー入力である。最後の 2 つは、（乱数）生成の 2 回目の呼び出しのための追加入力とエントロピー入力である。これらの*

値はランダムに生成される。「ランダムビット列の 1 ブロックを生成する」とは、(NIST SP 800-90 で定義された) 出力ブロック長に等しい返されたビット数のランダムビット列を生成するという意味である。

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

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

> ***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**：ナンスがサポートされている（df なしの CTR_DRBG がナンスを使用しない）場合、ナンスビット長はシード長の半分となる。*
> ***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。実装がある個別化文字列の長さのみをサポートする場合は、両方の値について同じ長さが利用可能である。複数の長さの文字列がサポートされている場合は、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）。実装が個別化文字列を使用しない場合は、値を提供する必要はない。*
> ***追加入力**：追加入力文字列のビット長は、個別化文字列長と同じ既定値及び制約条件を持つ。*

4.1.3 クラス：利用者データ保護 (FDP)

残存情報保護 (FDP_RIP)

FDP_RIP.2　　全残存情報保護

FDP_RIP.2.1　TSF は、すべてのオブジェクト[選択：*への資源の割当て、からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できないように強制しなければならない（shall）。

適用上の注意：

112 *この要件は、例えば、プロトコルデータ単位（PDU）が暗号鍵関連情報のような残存情報で埋められないことを保証する。ST 執筆者は、以前の情報がいつ利用できなくなるかを指定するために選択を使用する。*

113 ***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。懸念されるのは、一度ネットワークパケットが送信されると、パケットによって使用されるバッファやメモリエリアが、そのパケットからのデータをまだ含んでおり、そのバッファが再利用される場合に、それらのデータが残って新しいパケットに入り込むかもしれないと

いう点である。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確実にするため確認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）。

4.1.4 クラス：識別及び認証（FIA）

114 形式的な管理ユーザや一般的な目的のユーザが定義されていないため、TOE に関するベースライン要件は I&A に関してかなり制限されている。TOE によって実行されるのに必要な I&A の範囲は、IPsec 接続を確立するときにマシンレベルで行われた認証に関連している。これらの I&A 要件は、理解しやすさと保証アクティビティの執筆と適用を容易にするためにまとめられた IPsec プロトコルに関する要件を維持するために、FCS_IPSEC_EXT.1 コンポーネントに規定されている。そのため本節の要件は、本 PP で規定されているプロトコルによって使用されるクレデンシャルのみについて詳述する。

事前共有鍵作成（FIA_PSK_EXT）

115 TOE は、最低でも IPsec プロトコルで使用するための事前共有鍵をサポートしなければならず（must）、また、他のプロトコルでも事前共有鍵を使用できる（may）。下記の要件に規定されているように、TOE によってサポートされなければならない 2 種類の事前共有鍵がある（must）。1 つ目のタイプを「テキストベースの事前共有鍵」と呼び、パスワードのように標準文字セットからの文字列として利用者が入力する事前共有鍵を指す。このような事前共有鍵は、文字列がビット列に変換され、鍵として使用されるように条件付けられなければならない（must）。

116 2 番目のタイプを「ビットベースの事前共有鍵」（標準用語がないため）と呼び、管理者からコマンドで TSF によって生成される鍵または管理者によって「直接形式」で入力される鍵を指す。「直接形式」とは、テキストベースの事前共有鍵のような「条件付け」なしで、入力が鍵として直接使用されることを意味する。例えば、鍵を構成するビットを表す 16 進数の文字列がそうである。

117 下記の要件は、TOE がテキストベース事前共有鍵とビットベースの事前共有鍵の両方をサポートしなければならないことを義務付けるが（must）、ビットベースの事前共有鍵の生成は、TOE または運用環境のいずれで行ってもよい（may）。

FIA_PSK_EXT.1　拡張：事前共有鍵作成

FIA_PSK_EXT.1.1 TSF は、IPsec 及び[選択：*他のプロトコルなし*、[割付：事前共有鍵を使用する他のプロトコル]]用の事前共有鍵を使用できなければならない（shall）。

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

- 22 文字及び*[選択：[割付：他のサポートされる長さ]、他の長さなし]*、
- 大文字、小文字、数字及び特殊文字（「!」、「@」、「#」、「$」、「 %」、「^」、「&」、「*」、「(「及び」) 」を含む）の任意の組合せから構成される。

FIA_PSK_EXT.1.3 TSF は、[選択：SHA-1、SHA-256、SHA-512、[割付：*テキスト文字列の条件付け方法*]]を使用して、テキストベースの事前共有鍵を条件付けしなければならない（shall）。

FIA_PSK_EXT.1.4 TSF は、ビットベースの事前共有鍵を[選択：受け付ける、FCS_RBG_EXT.1 で規定されているランダムビット生成器を使用して生成する]ことができなければならない（shall）。

適用上の注意：

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

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

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

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

保証アクティビティ：

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

123 *評価者は、テキストベースの事前共有鍵及びビットベースの事前共有鍵の両方を許可するすべてのプロトコルが識別されていること、さらに 22 文字のテキストベースの事前共有鍵がサポートされていることが記載されていることを確認するために、TSS を検査しなければならない（shall）。要件に識別されているプロトコルごとに、評価者は、利用者によって入力されるキーシーケンス（ASCII 表現など）からプロトコルによって使用されるビット列にテキストベースの事前共有鍵を変換するために行われる条件付けが TSS に記載されていること及びこの条件付けが FIA_PSK_EXT.1.3 要件の最後の選択と一致していることを確認しなければならない（shall）。*

124 *評価者は、要件に識別されているプロトコルごとに、ビットベースの事前共有鍵を入力する、またはビットベースの事前共有鍵を生成する（またはその両方の）ための指示が運用ガイダンスに含まれていることを確認しなければならない（shall）。また、評価者は、ビ*

ットベースの事前共有鍵を生成するプロセスが記述されている（TOE がこの機能をサポートする場合）ことを確認するために、TSS を検査しなければならない（shall）。また、このプロセスが FCS_RBG_EXT.1 で規定されている RBG を使用することを確認しなければならない（shall）。

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

- *テスト 1：評価者は、運用ガイダンスに従って許可される文字の組合せが含まれている 22 文字の事前共有鍵を作成し（shall）、鍵を使用してプロトコルネゴシエーションを正常に実行できることを実証しなければならない。*
- *テスト 2[条件付き]：TOE が複数の長さの事前共有鍵をサポートする場合、評価者は、最小の長さ、最大の長さ及び無効の長さを使用してテスト 1 を繰り返さなければならない（shall）。最小の長さと最大の長さのテストは成功しなければならない（should）、無効の長さは TOE によって拒否されなければならない（must）。*
- *テスト 3[条件付き]：TOE がビットベースの事前共有鍵を生成しない場合、評価者は、運用ガイダンスの指示に従って、適切な長さのビットベースの事前共有鍵を入手し、入力しなければならない（shall）。次に、評価者は、鍵を使用してプロトコルネゴシエーションを正常に実行できることを実証しなければならない(shall)。*
- *テスト 4[条件付き]:TOE がビットベースの事前共有鍵を生成する場合､評価者は、運用ガイダンスの指示に従って､適切な長さのビットベースの事前共有鍵を生成し、使用しなければならない（shall）。次に、評価者は、鍵を使用してプロトコルネゴシエーションを正常に実行できることを実証しなければならない（shall）。*

X509 証明書（FIA_X509_EXT）

FIA_X509_EXT.1　拡張：X.509 証明書

FIA_X509_EXT.1.1　TSF は、RFC 5280 によって定義されている X.509v3 証明書を使用して、IPsec 接続用の認証をサポートしなければならない（shall）。

適用上の注意：

126 *RFC 5280 には、この要件の通り TOE によって実装されなければならない（must）証明書検証及び認定パス検証要件が定義されていることに注意するべきである（should）。*

保証アクティビティ：

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

- *TOE が規格のその特定の部分を実装することを読者が決定できるように、RFC5280 の節ごとに「MUST」（しなければならない）でない（例えば、「MAY」（してもよい）、「SHOULD」（するべきである）及び「SHOULD NOT」（するべきでない）など）すべての文を記述しなければならない（shall）。*
- *For each section of RFC 5280, any non-conformance to "SHOULD" statements shall be described;*

RFC 5280 の節ごとに、「SHOULD」（するべきである）文への不適合を記述しなければならない（shall）。

- *Any TOE-specific extensions or processing that is not included in the standard that may impact the security requirements the TOE is to enforce shall be described.*
  TOE が施行する予定のセキュリティ要件に影響するかもしれない（may）TOE 固有の拡張または規格に含まれない処理を記述しなければならない（shall）。

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

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

130 *評価者は、TOE がどの証明書を使用するかを選択する方法と、TOE が証明書を使用できるように運用環境を設定するために必要なすべての指示が管理ガイダンスに記述されていることを保証するために、管理者ガイダンスを確認しなければならない（shall）。*

131 *評価者は、証明書の使用を要求するシステムの各機能について以下のテストを実行しなければならない（shall）。*

- *テスト 1：評価者は、有効な認定パスなしに証明書を使用する場合、機能が失敗することを実証しなければならない（shall）。次に、評価者は、管理ガイダンスを使って、機能に使用される証明書を検証するために必要な証明書を読み込み、機能が成功することを実証しなければならない（shall）。次に、評価者は、いずれかの証明書を削除し、機能が失敗することを示さなければならない（shall）。*

4.1.5 クラス：セキュリティ管理（FMT）

132 本 PP の第 1 章で示されたように、TOE は分離した管理役割を維持するためには必要とされない。しかしながら、それらは、一般の利用者が利用できるべきではない（should）、TOE 運用のある側面を設定するための機能を提供するために必要とされる。TOE がある程度の管理コントロールを提供する場合、附属書 C からの適切な要件が ST で使用されるべきである（should）。

管理機能の特定（FMT_SMF）

FMT_SMF.1　　管理機能の特定

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

- **IKE ネゴシエーション中に提案され受け付けられなければならないセキュリティアソシエーションを規定しなければならない（shall）。**
- **使用される IKE プロトコルバージョンの設定。**

- **使用される IKE 認証手法を設定する。**
- **確立されたセッション鍵の暗号期間を設定する。暗号期間を設定する測定単位は 1 時間以下でなければならない（shall）。**
- **証明書失効を設定する。**
- **IPsec 交換中に提案され受け付けられるかもしれないアルゴリズムスイートを規定する（may）。**
- **可能であればピアツーピア接続の認証方法を規定する。**
- **TOE を更新する及び更新を検証する機能。**
- **本 PP の他の節に識別されているすべてのセキュリティ管理機能を設定する機能。**
- **[割付：追加の管理機能]**

適用上の注意：

133 *インストールする場合、VPN クライアントは IT 環境を信頼して、管理者が本物であることをクライアントマシンに証明する。*

134 *確立されたセッション鍵の暗号期間の設定機能の場合、暗号期間を設定する測定単位は 1 時間以下でなければならない（shall）例えば、秒、分及び時間の測定単位が設定可能で、1 日以上の測定単位は設定できない。*

135 ***保証アクティビティ：***

136 *評価者は、PP で義務付けられているすべての管理機能が運用ガイダンスに記載されていること及びその記述が、管理機能に関連する管理義務を実行するために必要な情報を含んでいることを確認しなければならない（shall）。評価者は、TOE を設定すること及び上記要件に記載されている各オプションをテストすることで、管理機能を提供する TOE の機能をテストしなければならない（shall）。*

137 *なお、ここでテストすることは、FCS_IPSEC_EXT.1 などの他の要件のテストと同時に実施することができる。*

4.1.6 TSF 保護クラス（FPT）

拡張:TSF セルフテスト（FPT_TST_EXT）

FPT_TST_EXT.1 拡張：TSF セルフテスト

FPT_TST_EXT.1.1 TSF は、TSF が正しく動作することを実証するために、初回の起動時（電源投入時）にセルフテストスイートを実行しなければならない（shall）。

FPT_TST_EXT.1.2 TSF は、TSF によって提供される暗号化サービスの使用を通じて、実行のために読み込まれる保存された TSF 実行コードの完全性を検証する機能を提供しなければならない（shall）。

適用上の注意：
TOE は、一般的に IT 環境で実行するソフトウェアパッケージと同時に、上記で必要なセルフテストアクティビティを実行することもできる。しかしながら、上記で述べられたテスト（ホスト環境に障害が起きた場合、セルフテストが重要ではなくなることを意味する）によって提供される保証を評価するのに、ホスト環境に大きく依存することが理解されるべきである（should）。

保証アクティビティ：

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

139 *評価者は、保存された TSF 実行コードが実行のために読み込まれるとき、そのコードの完全性を検証する方法が TSS に記述されていることを確認するために、TSS を検査しなければならない（shall）。評価者は、実行のために読み込まれる保存された TSF 実行コードの完全性が侵害されていないことを実証するためにテストが十分であることが、TSS に記載されていることを確認しなければならない（shall）。また、評価者は、成功する場合（例えば、ハッシュは検証された）及び失敗する場合（例えば、ハッシュは検証されなかった）に行われるアクションが TSS（または運用ガイダンス）に記述されていることを確認する。評価者は、以下のテストを実行しなければならない（shall）。*

- *テスト 1：評価者は、既知の良い TSF 実行コードの完全性チェックを実行し、確認が成功することを検証する。*
- *テスト 2：評価者は、TSF 実行コードを修正し、修正された TSF 実行コードの完全性チェックを実行し、さらにチェックが失敗することを検証する。*

拡張：高信頼更新（FPT_TUD_EXT.1）

FPT_TUD_EXT.1　拡張：高信頼更新

FPT_TUD_EXT.1.1 TSF は、許可された管理者に、TOE ファームウェア/ソフトウェアの現在のバージョンを問い合わせる機能を提供しなければならない（shall）。

FPT_TUD_EXT.1.2 TSF は、許可された管理者に、TOE ファームウェア/ソフトウェアの更新を開始する機能を提供しなければならない。

FPT_TUD_EXT.1.3 TSF は、TOE のファームウェア/ソフトウェア更新をインストールする前に、電子署名メカニズム及び[選択：公開されたハッシュ、他の機能なし]を使用してそれらの更新を検証するための手段を提供しなければならない（shall）。

適用上の注意：

140 *3 番目のエレメントで参照される電子署名メカニズムは、FCS_COP.1(2)で規定されるメカニズムである。参照される公開されたハッシュは、FCS_COP.1(3)に規定されている機能の 1 つによって生成される。*

保証アクティビティ：

141 *TOE の更新は、許可されたソースによって署名され、ハッシュが関連付けられていること、または、許可されたソースによって署名されることがある（may）。電子署名が使用される場合、許可されたソースの定義は、更新検証メカニズムによって使用される証明書がデバイスに含まれる方法の記述と共に TSS に含まれる。評価者は、この情報が TSS に含まれて*

いることを確認する。また、評価者は、更新候補を取得する方法、更新の電子署名の検証に関連する処理または更新のハッシュを計算する方法、さらに成功（ハッシュまたは署名は検証された）及び失敗（ハッシュまたは署名は検証できなかった）の場合に行われるアクションが TSS（または運用ガイダンス）に記述されていることを確認する。評価者は、以下のテストを実行しなければならない（shall）。

- *テスト 1：評価者は、製品の現在のバージョンを決定するために、バージョン検証アクティビティを実行する。評価者は、運用ガイダンスに記述されている手順を使用して合法の更新を入手し、正常に TOE にインストールされることを検証する。次に、評価者は、他の保証アクティビティのサブセットを実行して、更新が期待通りに機能することを実証する。更新の後で、評価者は、バージョンが更新のバージョンに正確に一致することを確認するために、再びバージョン検証アクティビティを実行する。*
- *テスト 2：評価者は、製品の現在のバージョンを決定するために、バージョン検証アクティビティを実行する。評価者は、違法の更新を入手または生成し、TOE へのインストールを試みる。評価者は、TOE が更新を拒否することを検証する。*

4.1.7 高信頼パス/チャネルクラス（FTP）

高信頼チャネル（FTP_ITC）

FTP_ITC.1　TSF 間高信頼チャネル

FTP_ITC.1.1　**詳細化**：TSF は、**IPsec を使用して**、それ自体と **VPN ピア**間に、他の通信チャネルから論理的に分離され、そのエンドポイントの保証された識別、**チャネルデータの暴露から**の保護及び**チャネルデータの変更の検出**を提供する**高信頼**通信チャネルを提供しなければならない（shall）。

FTP_ITC.1.2　TSF は、信頼されたチャネル経由の通信を開始するために、*リモート IT エンティティである TSF* を許可しなければならない（shall）。

FTP_ ITC.1.3　TSF は、*接続を移動するすべてのトラフィックのために*高信頼チャネル経由の通信を通過しなければならない（shall）。

適用上の注意：

142　*上記の要件の意図は、TOE と別の VPN クライアント、または VPN ゲートウェイ（どちらもプロトコルの意味でピアとしての役割を果たす）間の通信を保護するために、要件で識別された暗号プロトコルを使用することである。*

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

保証アクティビティ：

144　*評価者は、要件で規定されている暗号プロトコルの観点から、TOE 固有のオプションまたは*

仕様には反映されない手順と一緒に、TSS にアクセスポイントに接続する TOE の詳細が記述されていることを確認するために TSS を検査しなければならない（shall）。また、評価者は、TSS に記載されるすべてのプロトコルが、ST の 要件に規定され、含まれていることを確認しなければならない（shall）。評価者は、アクセスポイントとの接続を確立するための指示が運用ガイダンスに含まれていること、及び接続が意図せず壊れた場合の復旧手順が運用ガイダンスに含まれていることを確認しなければならない（shall）。評価者は、以下のテストも実行しなければならない（shall）。

- *テスト 1：評価者は、要件に規定されたプロトコルを使い、運用ガイダンスに記述されている通りに接続を設定し、通信が成功することを確認して、TOE が VPN ピアとの通信を開始できることを確認しなければならない（shall）。*
- *テスト 3：評価者は、許可された IT エンティティとの通信チャネルごとに、チャネルデータが平文で送信されないことを確認しなければならない（shall）。*
- *テスト 4：評価者は、許可された IT エンティティとの通信チャネルごとに、チャネルデータの変更が TOE によって検出されることを確認しなければならない（shall）。*
- *テスト 5：評価者は、TOE からピアへの接続物理的に中断しなければならない（shall）。評価者は、少なくとも、自動的に接続を再開するか新しいアクセスポイントへ接続することを試す場合は、以降の接続が適切に保護されることを確認しなければならない（shall）。*

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

4.2 セキュリティ機能要件根拠

146 本節では、4.1 節で定義されている TOE セキュリティ機能要件の根拠について説明する。表 10 に、要件によって対策方針が対処される対応する根拠と共に、セキュリティ機能要件からセキュリティ対策方針への対応関係を示す。

147 ベンダから提供されるセキュリティターゲット（ST）には、2 つの節から構成されるセキュリティ要件の根拠も含まれている。

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

表 10：TOE セキュリティ機能要件に関する根拠

対策方針	対策方針に取り組む要件	根拠
O.AUTH_COMM TOE は、利用者が TOE になりすます他のエンティティと通信していないこと及び TOE が許可された IT エンティティになりすます他のエンティティでなく、許可された IT エンティティと通信していることを保証する手	FCS_CKM.1 FCS_COP.1(1) FCS_COP.1(2) FCS_IPSEC_EXT.1 FIA_PSK_EXT.1 FIA_X509_EXT.1 FTP_ITC.1	FTP_ITC.1（及びサポートする要件、FCS_CKM.1、FCS_COP.1(1)、FCS_COP.1(2)、FCS_IPSEC_EXT.1、FIA_PSK_EXT.1 及び FIA_X509_EXT.1）は、TOE が TOE とリモートの管理者及び高信頼 IT エンティティの両方との間にこのチャネルを通過するデータを漏洩

対策方針	対策方針に取り組む要件	根拠
段を提供する。		または変更から保護する、異なる通信チャネルを作成するメカニズムを提供することを要求する。これは、要件で規定されたプロトコルを暗号化して使用することで行われる。これらのプロトコルは、エンドポイントの保証された相互認証及びチャネルデータの保護を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS TOE は、機密性を維持するための暗号化機能（例えば、暗号化/復号及び電子署名操作）を提供しなければならず（shall）、さらに TOE 及びそのホスト環境の外部で送信されるデータの改ざんを検出することを可能にする。	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 FIA_X509_EXT.1	FCS_CKM.1 は非対称鍵を生成する。これらの鍵は、IPSEC 用の一時鍵及び潜在的な他の公開鍵に基づく鍵共有スキーム方式によって使用される。 FCS_CKM_EXT.4 は、鍵及び鍵関連情報がゼロ化されることを保証する機能を提供する。ほとんどの場合、TOE は、ホスト上で実行するソフトウェアエンティティであり、本要件の範囲は、ソフトウェアがデータをクリアするために適切な機能を起動することを確実にすることである。ホストは最終的にデータを確実にクリアする責任を負う。 FCS_COP.1(1)は、PP に規定されている様々なプロトコル用の暗号化及び復号操作を実行するために AES が使用されることを規定する。 FCS_COP.1(2)は、トラフィックを保護するために使用されるプロトコルに関連する高信頼更新及び証明書操作用の電子署名機能を TOE に実装することを要求する。 FCS_COP.1(3)及び FCS_COP.1(4)は、TSF がデータ完全性実証と操作データ完全性以外の操作のために、Secure Hash Algorithm アルゴリズムの実装を使用して、ハッシュサービスを提供することを要求する。 FIA_X509_EXT.1 は、上記の多くの暗号操作をサポートするために使用される証明書が、該当する規格に適合することを要求する。

対策方針	対策方針に取り組む要件	根拠
		FCS_RBG_EXT.1 は堅牢なランダムビット生成機能が存在することを要求する。
O.PEER_AUTHENTICATION TOE は、TOE とのセキュリティアソシエーションを確立しようとする、お互いのピア TOE が本物であることを証明する。	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1 は、TOE が IKE プロトコルを使って IPsec を実装しなければならないことを規定する（must）。本プロトコルを実装することで、すべての通信で使用される暗号鍵及びアルゴリズムとモードを含む、セキュリティアソシエーションを確立するために、それぞれのピア TOE でセキュアで認証されたプロトコルを確立する。それぞれの自身の暗号鍵で、2 つのピア TOE 間に複数のセキュリティアソシエーションを確立することができる。認証は、電子署名または事前共有鍵を経由することができる（may）。
O.PROTOCOLS TOE は、相互接続性を保証するために、RFC 及び/または工業仕様書に従って標準化されたプロトコルが TOE に実装されていることを保証する。	FCS_IPSEC_EXT.1 FTP_ITC.1	FCS_IPSEC_EXT.1 及び FTP_ITC.1 は、実装することが要求されるプロトコルに適用可能な規格を参照する（及びそれらの規格に関するすべての制限を示す）。
O.RESIDUAL_INFORMATION_CLEARING TOE は、資源が再割当されるとき、保護された資源に含まれるデータが使用できないことを保証する。	FCS_CKM_EXT.4 FDP_RIP.2	FCS_CKM_EXT.4 は、不要になった場合に暗号鍵の破壊を保証する。 FDP_RIP.2 は、データへのアクセスを明示的に許可された制御対象以外の制御対象には資源の内容が使用できないことを保証するために使用される。この TOE の場合、パケットの内容が以後のパケットで暴露されることを防止するために、ネットワークパケットを構築するために使用されるメモリを消去する、または何らかのバッファ管理スキームを使用することが重要である（例えば、パケットの作成に埋込みが使用される場合、他の利用者のデータまたは TSF データが含まれてはならない(must)）。
O.SYSTEM_MONITORING TOE は、監査データを生成する機能を提供する。	FAU_GEN.1 FAU_SEL.1	FAU_GEN.1 は、TOE が記録できなければならない事象の集合を定義するが（must）、FAU_SEL.1 は、管理者が監査証跡にどの監査対象事象が記録されるかを設定できるようにする。
O.TOE_ADMINISTRATION	FAU_SEL.1 FMT_SMF.1	FAU_SEL.1 は、監査対称事象が記録されるように設定できる機能を

対策方針	対策方針に取り組む要件	根拠
TOE は、管理者が TOE を設定できるメカニズムを提供する。		必要とするが、FMT_SMF.1 は、TOE のほかの部分に対する設定要件を提供する。序説で述べたように、TOE は管理者の役割を提供する必要はないが、IT 環境との組み合わせで、TOE はホストマシンの一般ユーザのサブセットに対するこれらの機能を制限できなければならない（must）。
O.TSF_SELF_TEST TOE は、それが正しく動作していることを保証するために、そのセキュリティ機能のサブセットをテストする機能を提供する。	FPT_TST_EXT.1	FPT_TST_EXT.1 は、TSF の正しい操作を保証するために TOE がセルフテストスイートを提供すること及び自身が保存された実行可能ファイルの完全性の問題を検出することを要求する。
O.VERIFIABLE_UPDATES TOE は、TOE への更新が管理者によって変更されていないこと及び（オプションで）信頼できるソースから検証できることを保証することを手助けする機能を提供する。	FCS_COP.1(2) FCS_COP.1.(3) FPT_TUD_EXT.1	FCS_COP.1(2)及び FCS_COP.1(3)は、更新の検証に使用される電子署名アルゴリズムとハッシュ関数を規定する。 FPT_TUD_EXT.1 は、実行中のファームウェアのバージョンを決定し、更新を開始し、ファームウェア/ソフトウェアがインストール前に TOE に更新されることを検証する方法を提供する。

4.3 セキュリティ保証要件

148 3.1 節の TOE に関するセキュリティ対策方針は、2.1 節及び 2.2 節に引用されている組織のセキュリティ方針に識別されている脅威に対応するために作成された。4.1 節のセキュリティ機能要件（SFR）は、セキュリティ対策方針の形式的なインスタンス化である。

149 第 4 章の序説に示されているように、本節には CC からの完全な SAR セットが含まれているが、評価者によって実行される保証アクティビティについては 4.1 節と本節で詳述されている。

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

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

表 11：セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネントの説明
開発	ADV_FSP.1	基本機能仕様
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
テスト	ATE_IND.1	独立テスト - 適合
脆弱性評定	AVA_VAN.1	脆弱性調査
ライフサイクルサポート	ALC_CMC.1	TOE のラベル付け
	ALC_CMS.1	TOE の CM 範囲

4.3.1 ADV クラス：開発

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

4.3.1.1 ADV_FSP.1 基本機能仕様

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

154 TOE とのインタフェースを理解する上で、対抗すべき脅威が、ネットワーク（TOE のピアツーピア接続経由か TOE と VPN ゲートウェイ接続のいずれか）を通って送信されたユーザーデータの機密性及び完全性であること、また、接続を通過することができる認証データであること考慮することが重要である。さらに、その構成次第では、TOE は TOE 背後のネットワークへの認証されていないアクセスの保護を提供することができる（may）。ネットワークインタフェースに加え、管理インタフェース（TOE を設定する方法）についても記述する必要がある。

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

開発者アクションエレメント：

ADV_FSP.1.1D 開発者は機能仕様を提供しなければならない（shall）。

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（shall）。

開発者向け注意事項： 本節の序説で示したように、機能仕様は、ST の TSS に提供されている情報と共に、AGD_OPR 及び AGD_PRE 証拠文書に含まれている情報から構成される。機能要件内の保証アクティビティは、

証拠文書及び TSS 節に存在するべきである証拠を指し示す。これらは SFR に直接関連付けられるため、エレメント ADV_FSP.1.2D での追跡は既に明示的に行われており、証拠文書は必要でない。

内容と記述エレメント：

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（shall）。
ADV_FSP.1.2C	機能仕様は、SFR 実施及び SFR 支援の各 TSFI 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（shall）。
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（shall）。
ADV_FSP.1.4C	追跡は、機能仕様での TSFI に対する SFR の追跡を実証しなければならない（shall）。

評価者アクションエレメント：

ADV_ FSP.1.1E	評価者は、提供された情報が証拠の内容と記述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 のインスタンス化であることを決定しなければならない（shall）。

保証アクティビティ：

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

4.3.2 AGD クラス：ガイダンス文書

157 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、管理モデルの記述と、運用環境（VPN クライアントになるシステム）がセキュリティ機能に関する役割を満たすことができることを管理者が検証する方法の記述を含まなければならない（must）。証拠文書は、形式的ではないスタイルで、管理者が読みやすいものであるべきである（should）。

158 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（must）。このガイダンスは、以下を含む。

- その環境において TOE を正常にインストールするための指示
- 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

- TOE 機能、環境機能、またはこの 2 つの機能の組み合わせのいずれかを使用して、保護された管理機能を提供するための指示

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

4.3.2.1 AGD_OPE.1 利用者操作ガイダンス

開発者アクションエレメント：

AGD_OPE.1.1D 開発者は、利用者操作ガイダンスを提供しなければならない（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る。

内容と記述エレメント：

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）。

評価者アクションエレメント：

AGD_OPE.1.1E　評価者は、提供された情報が証拠の内容と記述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）。

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

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

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

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

164 *証拠文書は、ハッシュをチェックする、または電子署名を検証するいずれかによって TOE の更新を検証するためのプロセスを記述しなければならない（must）。評価者は、このプロセスに以下の手順が含まれていることを検証しなければならない（shall）。*

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

4.3.2.2　AGD_PRE.1　準備手続き

開発者アクションエレメント：

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

開発者向け注意事項： 運用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）。

内容と記述エレメント：

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）。

評価者アクションエレメント：

AGD_PRE.1.1E 評価者は、提供された情報が証拠の内容と記述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：

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

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

- *序論の部分で示したように、TOE の管理は、TOE のすべての利用者のグループのサブセットである 1 人以上の管理者によって行われる。システム全体（TOE 及び運用環境）でこの機能を提供しなければならないが（must）、機能の実装責任は、完全に運用環境の責任である場合から完全に TOE の責任である場合までさまざまである。責任を負う機能を提供するように運用環境を構成するよう、高レベルでガイダンスに適切な指示が含まれなければならない（must）。管理利用者を一般の利用者から分離できるようにするメカニズムを TOE が提供しない場合は、指示によって、例えば、OS の I&A メカニズムの OS 設定をカバーし、利用者の一意（OS ベース）の識別情報を提供する。また、更なるガイダンスで、TOE 管理者だけが管理用の実行可能ファイルにアクセスできるよう、TOE 管理識別情報（1 つまたは複数）を使用した OS の DAC メカニズムの設定についてインストーラに指示する。TOE がこの機能性の一部またはすべてを提供する場合は、附属書 C の該当する要件を ST に含め、それらの要件に関連する保証アクティビティにより、TOE と運用環境の両方に必要なガイダンスについて詳細を提供する。*

評価者は、以下のテストも実施しなければならない（shall）。

- *テスト 1［条件付］：すべての TOE 利用者からの管理者である利用者の分離を運用*

環の設定のみで実施する場合、評価者は、ST で主張される設定ごとに、管理者ガイダンスに従ってシステムを設定した後で管理者でない利用者が TOE 管理機能にアクセスできないことを確認する。

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

168 テストは、TSS に述べられた機能性や提出された証拠文書（設定や運用を含む）を確認するために行われる。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、4.1 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最小限のテストアクティビティを識別する。評価者は、テスト計画や結果を実証するテスト報告書と、本 PP への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)。

内容と記述エレメント：

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

評価者アクションエレメント：

ATE_IND.1.1E 評価者は、提供された情報が証拠の内容と記述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 が動作することを確認するために 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：

169 *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（shall）。テスト計画は、本 PP の保証アクティビティの本体に含まれるすべてのテストアクションをカバーする。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）。

170 *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（must）、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（must）。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場合は、根拠は必要ない。*

171 *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 証拠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（should）、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やツールを含むかもしれない（may）。各ドライバやツールに関して、ドライバやツールが 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。*

172 *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

173 本プロテクションプロファイルの第一世代（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。侵入ペネトレーション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証拠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プロテクションプロファイルの開発のために使われる。

4.3.4.1 AVA_VAN.1 脆弱性調査

開発者アクションエレメント：

AVA_VAN.1.1D 開発者は、テストのために TOE を提供しなければならない（shall）。

内容と記述エレメント：

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

評価者アクションエレメント：

AVA_VAN.1.1E 評価者は、提供された情報が証拠の内容と記述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：

174 *ATE_IND と同様に、評価者はこの要件に関して、報告書を作成して到達した結論を文書化しなければならない（shall）。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に含めても別文書でもよい。評価者は、公知の情報を検索して、一般的な VPN クライアント製品で見つかった脆弱性及び特定の TOE に関連する脆弱性を判断しなければならない。評価者は、参照した情報源及び見つかった脆弱性を報告書に文書化する。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、不適合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用して）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手口を評価することにより決まる。例えば、もし脆弱性がブートアップ時に鍵の組み合わせを押すことによって検知できれば、テストは本 PP の保証レベルに適しているだろう。もし、脆弱性の悪用に、例えば、電子顕微鏡や液体窒素のタンクが必要となるならば、テストは適しておらず、適切な正当化を策定することになる。*

4.3.5 ALC クラス：ライフサイクルサポート

175 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

176 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)。

内容と記述エレメント：

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

評価者アクションエレメント：

ALC_CMC.2.1E 評価者は、提供された情報が証拠の内容と記述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：

177 *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

178 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）。

内容と記述エレメント：

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）。

評価者アクションエレメント：

ALC_CMS.2.1E 評価者は、提供された情報が証拠の内容と記述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：

179 *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。*

4.4 セキュリティ保証要件根拠

180 これらのセキュリティ保証要件を選択するための根拠は、これがこの技術に関する最初の標準プロテクションプロファイルであることである。最初のプロテクションプロファイルは、開発のベストプラクティスを保証するために使用される。これらの製品タイプで脆弱性が見つかった場合は、実際のベンダプラクティスに基づいて、より厳格なセキュリティ保証要件が義務付けられる。

附属書 A：サポート表、参考文献及び略語

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

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

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

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

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

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

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

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

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

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

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

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

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

[14] RFC 3579 RADIUS (Remote Authentication Dial in User Service Support For Extensible Authentication Protocol (EAP), September 2003

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

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

[17] WPA2 Standard

AES	Advanced Encryption Standard
AF	Authorization factor（認可ファクタ）
AS	Authorization subsystem（認可サブシステム）
CAVS	Cryptographic Algorithm Validation System（暗号アルゴリズム検証システム）
CC	Common Criteria（コモンクライテリア）
CCTL	Common Criteria Testing Laboratory（コモンクライテリア評価機関）
CM	Configuration management（構成管理）
COTS	Commercial Off-The-Shelf（市販の）
CMVP	Cryptographic Module Validation Program（暗号モジュール試験及び認証制度）
DRBG	Deterministic Random Bit Generator（決定論的ランダムビット生成器）
DoD	Department of Defense（米国国防総省）
EAL	Evaluation Assurance Level（評価保証レベル）
ES	Encryption Subsystem（暗号化サブシステム）
FIPS	Federal Information Processing Standards（連邦政府情報処理規格）
ISSE	Information System Security Engineers（情報システムセキュリティエンジニア）
IT	Information Technology（情報技術）
OSP	Organization Security Policy（組織セキュリティ方針）
PP	Protection Profile（プロテクションプロファイル）
PUB	Publication（出版）
RBG	Random Bit Generator（ランダムビット生成器）
SAR	Security Assurance Requirements（セキュリティ保証要件）
SF	Security Function（セキュリティ機能）
SFR	Security Functional Requirement（セキュリティ機能要件）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）
TSFI	TSF Interface（TSFインタフェース）
TSS	TOE Summary Specification（TOE要約仕様）

附属書 B：NIST SP 800-53／CNSS 1253 マッピング

NIST SP 800-53/CNSS の 1253 管理策のいくつかは、適合 TOE によって完全にまたは部分的に対処される。本節は、取り上げられた要件を概説しており、TOE が運用構成に組み込まれるときに要求される追加のテスト（存在する場合）を認証担当者が決定するために利用できる。

適用上の注意：本バージョンでは、簡単なマッピングのみを提供する。将来のベージョンでは、認証チームのための更なる情報を提供する追加の説明を含む予定である。この追加情報は、TOE によって提供される適合の程度（例えば、完全に管理策を満たす、部分的に管理策を満たす）について議論している管理策マッピングに対する SFR についての詳細を含むだろう。さらに、適合が決定された方法に関する情報（文書レビュー、ベンダ主張、テスト/検証の程度）を認定チームに提供するために、規定された保証アクティビティ及び SAR を満たす一環として行われる評価アクティビティの総合的なレビューが要約されるだろう。この情報は、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。

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（should）。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（may）。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（must）、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_SMF.1
AU-2	監査対象事象	FAU_GEN.1
AU-2(4)		FAU_GEN.1
AU-3	監査記録の内容	FAU_GEN.1
AU-3(1)		FAU_GEN.1
AU-7	監査の低減と報告書の作成	FAU_SEL.1
AU-10	否認防止	FCS_COP.1(2)
AU-12	監査生成	FAU_GEN.1
CM-5	変更のためのアクセス制限	FPT_TUD_EXT.1
IA-3	デバイスの識別と認証	FCS_IPSEC_EXT.1, FTP_ITC.1
IA-5	認証子の管理	FIA_PSK_EXT.1, FIA_X509_EXT.1
SC-4	共有資源における情報	FDP_RIP.2
SC-8	伝送（する情報）の完全性	FCS_IPSEC_EXT.1, FTP_ITC.1
SC-9	伝送（する情報）の機密性	FCS_IPSEC_EXT.1, FTP_ITC.1
SC-12	暗号鍵の確立と管理	FCS_CKM.1, FCS_CKM_EXT.4
SC-13	暗号の利用	FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1
SI-6	セキュリティ機能の検証	FPT_TST_EXT.1

附属書 C：追加要件

181 *PP の本草案について、この附属書は、サポートする脅威、対策方針、根拠、または（一部の場合）保証アクティビティはなく、追加コンポーネントを含んでいる。このサポート情報は、最初のレビューサイクルに沿って開発され、次回の PP の公開に組み込まれる予定である。本節に含まれる情報（含まれる要件が潜在的な適合 TOE に適用可能かどうか、またこの附属書に含まれていない要件が VPN クライアント製品に広く適用可能かどうか）に関するコメントを歓迎すると共に、ぜひお願いしたい。*

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

C.1　クラス：セキュリティ監査（FAU）

183 監査レビュー及び/またはストレージが TOE によってサポートされる場合は、必要に応じて ST に以下の監査要件を記載しなければならない（must）。

監査レビュー（FAU_SAR.1）

FAU_SAR.1　　監査レビュー

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

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

制限付き監査レビュー（FAU_SAR.2）

FAU_SAR.2　　制限付き監査レビュー

FAU_SAR.2.1　**詳細化**：TSF は、**許可された管理者を除き、監査証跡内の**監査記録へのすべての利用者読取りアクセスを禁止しなければならない（shall）。

FAU_STG_EXT.4　　監査データ消失防止

FAU_STG_EXT.4.1　TSF は、許可された管理者に対し、監査証跡が一杯の場合、以下の 1 つまたは複数のアクションを選択する機能を提供しなければならない（shall）。

a) 許可された管理者が行う事象を除き、監査対象事象を防止する、及び、

b)保存されている最も古い監査記録を上書きする。

184 *適用上の注意：*
TOE は、許可された管理者に、監査対象事象の発生を防止して監査データの消失を防止するオプションを提供する。このような状況で許可された管理者のアクションを監査することは要求されない。また、TOE は、許可された管理者に、「古い」監査記録を上書きするオプションを提供する。これにより、サービス妨害攻撃から保護できる（may）。

C.2 クラス：識別及び認証（FIA）

185 TOE が管理機能を提供する場合、リモート管理、ローカル管理及び管理セッションの保護を含む機能を規定するために適用することができる多くの要件がある。PP の本バージョンに対し、クライアントに対してそういった機能を規定するために、VPN ゲートウェイプロテクションプロファイルから管理要件を使用することが受け入れられる。

186 TOE が、交換中に使用される証明書を保存及び管理することができる機能を提供する場合は、以下の要件を ST に含めることができる。

X509 証明書（FIA_X509_EXT）

FIA_X509_EXT.2 拡張：X.509 証明書保管及び管理

FIA_X509_EXT.1.2 TSF は、証明書を保存し、許可されていない削除と変更から保護しなければならない。（shall）。

FIA_X509_EXT.1.3 TSF は、本 PP に規定されているセキュリティ機能が使用するために、許可された管理者が X.509v3 証明書を TOE に読み込む機能を提供しなければならない（shall）。

適用上の注意：
187 *FIA_X509_EXT.1.2 は、TSF によって使用され、処理される証明書に適用される。運用環境内の他のコンポーネント（例えば RADIUS サーバ）によって使用され、処理される証明書は、このエレメントでは取り扱われない。*

保証アクティビティ：
188 *TSS は、本 PP の要件を満たすために使用される証明書を含む、実装されたすべての証明書記憶域を記述しなければならない（shall）。この記述は、証明書をストレージに読み込み、ストレージを無許可アクセスから保護する方法に関する情報を含まなければならない（shall）。*

189 *評価者は、証明書の使用を要求するシステムの各機能について以下のテストを実行しなければならない（shall）。*

- *テスト 1：評価者は、有効な認定パスなしに証明書を使用する場合、機能が失敗することを実証しなければならない（shall）。次に、評価者は、機能に使用される証明書を検証するために必要な証明書を読み込み、機能が成功することを実証しなければならない（shall）。次に、評価者は、いずれかの証明書を削除し、機能が失敗することを示さなければならない（shall）。*

C.3 監査要件

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

機能要件	監査対象事象	追加の監査記録内容
FCS_TLS_EXT.1	プロトコルの失敗。 TLS セッションの確立/終了。	失敗の理由。 成功及び失敗に関する非 TOE エンドポイントの接続先（IP アドレス）。
FCS_SSH_EXT.1	プロトコルの失敗。 SSH セッションの確立/終了。	失敗の理由。 成功及び失敗に関する非 TOE エンドポイントの接続先（IP アドレス）。
FCS_HTTPS_EXT.1	プロトコルの失敗。 HTTPS セッションの確立/終了。	失敗の理由。 成功及び失敗に関する非 TOE エンドポイントの接続先（IP アドレス）。
FPT_ITT.1	なし。	

附属書 D：本書の表記規則

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

191 本 PP で使用される表記、書式、及び表記法は、コモンクライテリア（CC）のバージョン 3.1 と概ね一貫している。ここでは、PP 読者の役に立つように一部を抜粋して示す。CC は、機能要件と保証要件に対していくつかの操作を実行することを許可する。*詳細化*、*選択*、*割付*、及び*繰返し*は、CC 3.1 パート 1 の附属書 C.4 に定義されている。これらの各操作は本 PP で使用される。

詳細化表記法

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

選択表記法

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

割付表記法

194 **割付**操作は、パスワードの長さのように指定されていないパラメタに特定の値を割り付けるために使用される（CC 3.1 パート 1 の附属書 C.4.2 を参照）。**太字**で示される値は PP 執筆者によって行われた割付を示し、括弧及び「割付」という語句は削除される。ST 執筆者によって埋められるべき割付は、[割付：]として角括弧内に示され、割付が行われるべきことを示す。

繰返し表記法

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

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

拡張要件表記法

197 執筆者のニーズを満たすのに適した要件が CC にない場合、拡張要件を使用できる。**拡張要件**は識別されなければならず（must）、要件を明確にする上で CC クラス/ファミリ/コンポ

ーネントモデルを使用することが要求される。拡張要件は、コンポーネント内の「EXT」の挿入で示される。

適用上の注意

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

保証アクティビティ：

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

附属書 E：用語

管理者 – TOE を設定する管理者権限を持つ利用者。

認証サーバ (AS) – 保護されたネットワークにアクセスしようとするエンティティ（ユーザまたはクライアント）の認証を容易にするために設計されたエンティティ。

許可された – オブジェクト、システムまたはシステムエンティティへのアクセス権限を許可されたエンティティ

クリティカルセキュリティパラメタ(CPS) – 漏洩や改ざんにより暗号化モジュールのセキュリティが無効になるセキュリティ関連情報。例えば、秘密暗号鍵とプライベート暗号鍵、パスワードや PIN のような認証データ。

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

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

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

運用環境– TOE が運用される環境。

プライベートネットワーク– 許可されていないユーザやエンティティによるアクセスから保護されるネットワーク

特権モード– IT 環境の管理者権限を必要とする機能を、ユーザが実行できるようにする TOE の操作モード。

パブリックネットワーク– すべてのユーザ及びエンティティに表示され、許可されていないアクセスに対して保護されていないネットワーク（インターネット等）。

セキュリティ保証要件（SAR）– TOE が SFR を満たす保証を取得する方法の記述。

セキュリティ機能要件（SFR）– TOE に関するセキュリティ対策方針の標準言語への翻訳。

セキュリティターゲット（ST）– 特定の識別された TOE に対するセキュリティに必要な処理系実装依存の記述。

評価対象（TOE）– ガイダンスに添付される可能性のある、ソフトウェア、及び/またはハードウェアのセット。本 PP では、TOE は VPN クライアントである。

脅威エージェント – データの破壊、漏洩、改ざん及び/またはサービス妨害を通して、情報システムに悪影響を与えようとするエンティティ。

TOE セキュリティ機能（TSF）– SFR の正しい実施に依存しなければならない TOE のすべて

のハードウェア、ソフトウェア及びファームウェアを組み合わせた機能（must）。

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

許可されていない利用者- 許可された管理者によって TOE またはプライベートネットワークへのアクセスを許可されていないエンティティ（装置またはユーザ）。

権限のないモード - VPN クライアントユーザに対して VPN クライアント機能を提供するだけの、TOE の運用モード。

VPN クライアント-保護されていないパブリックネットワークからプライベートネットワークを通る暗号化された IPsec トンネルを確立するために、リモートユーザがクライアントコンピュータを使用できるようにする TOE。

VPN クライアントユーザ- 権限のないモードで TOE を操作するユーザ。

VPN ゲートウェイ- IP パケットがプライベートネットワークとパブリックネットワークの間の境界を通過するときに、IP パケットの暗号化及び複合化を実行するコンポーネント。

VPN ピア- VPN 接続で TOE と通信する VPN クライアントまたはゲートウェイ。

附属書 F：PP の識別

タイトル：	IPsec 仮想プライベートネットワーク（VPN）クライアント用のプロテクションファイル
バージョン：	1.0
スポンサー：	National Information Assurance Partnership (NIAP)
CC バージョン：	情報技術セキュリティ評価のためのコモンクライテリア（CC）バージョン 3.1 R3、2009 年 7 月
キーワード：	認証サーバ、IKE、IPsec、PKI、VPN、VPN Client、VPN