IPsec 仮想プライベートネットワーク (VPN)

クライアントのプロテクションプロファイル

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。

https://www.niap-ccevs.org/pp/pp_vpn_ipsec_client_v1.3.pdf

Information Assurance Directorate

2013 年 4 月 12 日
バージョン 1.3

平成 25 年 11 月 12 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

表の目次

図の目次

改版履歴

バージョン	日付	内容
1.0	2011 年 12 月	初版発行
1.1	2012 年 12 月	軽微な更新。暗号要件を VPN ゲートウェイ拡張パッケージと一貫させた。
1.2	2013 年 1 月	**FCS_COP.1.1(2)** を更新し、VPN ゲートウェイ拡張パッケージと一貫させた。
1.3	2013 年 4 月	証明書が CA 証明書とみなされるために満たされなければならない条件として、basicConstraints フィールドが存在し cA フラグが TRUE に設定されることが認証パス検証アルゴリズムによって確証されるよう、X.509 要件を更新。

1 PP 概論

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のエンドポイントまたはゲートウェイへのセキュアなトンネルを提供する、市販 (COTS) の IPsec 仮想プライベート (VPN) クライアントの調達をサポートするものである。本 PP では、VPN とその支援環境の方針、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について詳述する。

2 ここでの主な意図は、VPN クライアントによって対処されることになる脅威に対抗するために必要とされるセキュリティ機能要件の我々の理解を、明確に開発者へ伝えることである。セキュリティターゲット (ST) の TOE 要約仕様 (TSS) 中の記述には、製品 (評価対象) のアーキテクチャ及び重要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確実にするために用いられるメカニズムが文書化されていることが期待される。

1.1 TOE の PP 概要

3 この文書は、VPN クライアントのセキュリティ機能要件 (SFR) を規定する。VPN によって、VPN クライアントと VPN ゲートウェイとの間でプライベートなデータの伝送が保護される。本 PP によって定義される TOE は VPN クライアントであり、これはリモートアクセスクライアント上で実行されるコンポーネントである。VPN クライアントは専用ネットワークの外部または内部に位置することが想定されており、VPN ゲートウェイへのセキュアなトンネルを提供する。このトンネルは、公共ネットワークを通過する情報に機密性、完全性、及びデータ認証を提供する。本 PP に適合するすべての VPN クライアントは、IPsec をサポートする。

1.1.1 TOE の利用方法と主要なセキュリティ機能

4 VPN クライアントによって、リモートユーザはクライアントコンピュータを使って専用ネットワークへの暗号化された IPsec トンネルを、保護されていない公共ネットワークを通して確立することが可能となる (図 1 を参照)。TOE は公共ネットワークと、VPN クライアントの基盤となる OS 上に常駐するエンティティ (ソフトウェア、利用者など) との間に位置する。専用ネットワークから公共ネットワークへ通過する IP パケットは、その宛先が発信元ネットワークと同一の VPN 方針をサポートするリモートアクセス VPN クライアントである場合、暗号化されることになる。VPN クライアントは自分自身と VPN ゲートウェイとの間のデータを保護することによって、たとえ公共ネットワークを通過する際であっても、通過中のデータの機密性、完全性、及び保護を提供する。

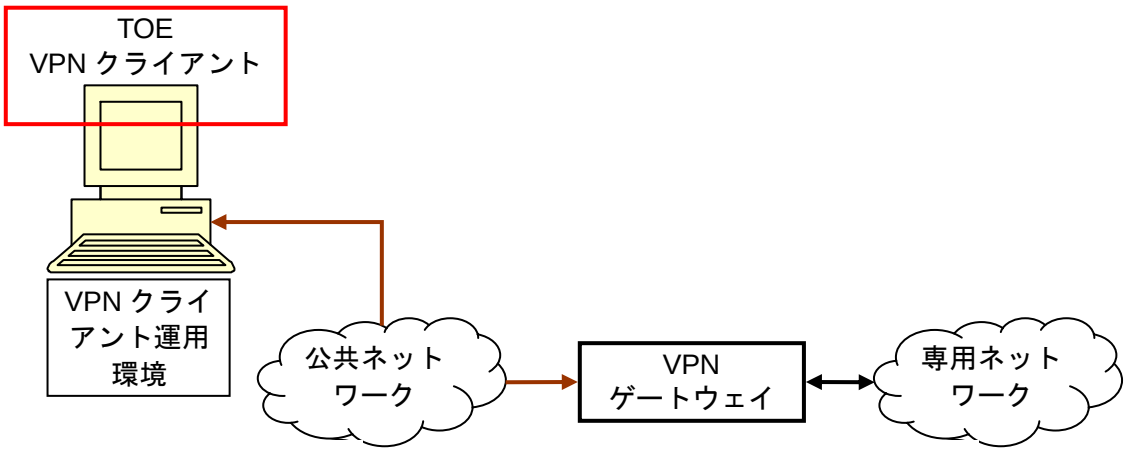


図 1 ：VPN クライアント

5 本 PP のセキュリティ機能要件は、以下の VPN クライアントの基本的な側面に焦点を絞っている。

- VPN ゲートウェイの認証、
- 通過中のデータの暗号保護、及び
- サービスの実装。

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 (これが VPN 通信の「リモート」エンドポイントである) との VPN 接続を確立することができる。VPN エンドポイントは互いに認証を行って、認可された外部 IT エンティティと通信を行っていることを確証する。VPN ゲートウェイの認証は、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行われる。IKE ネゴシエーションは、既存の公開鍵基盤を利用して認証を行うが、オプションとして事前共有鍵を用いることもできる。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) によって保護された IPsec トンネルが確立される。

7 VPN クライアントは適切に実装され、重大な設計ミスが含まれないことが前提となる。VPN クライアントは IT 環境に加えて、監査レビュー、監査ストレージ、識別と認証、セキュリティ管理、及びセッションマネジメントというクライアントマシン保護メカニズムにもその適切な実行を依存している。ベンダは、サポートされているすべての運用環境においてクライアントマシン及び TOE を正しくインストールし管理するための構成ガイダンス (AGD_PRE, AGD_OPE) を提供することが求められる。

1.1.2 暗号

8 IPsec VPN クライアントは、自分自身とその VPN ゲートウェイとの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働き、トンネルの確立と維持に関連する数多くの暗号機能を行う。認証、鍵の生成、及び情報の暗号化に用いられる暗号が十分に堅牢であり、実装に重要な設計ミスがない場合、敵対者は暗号鍵空間を総当りしてデータを取得することができないことになる。IPsec 標準への準拠、適切にシードが供給されたランダムビット生成器 (RBG)、そしてセキュアな認証ファクタによって、鍵空間の総当りよりも少ない労力で送信された情報へアクセスすることが不可能であることが確実となる。任意の平文の共通鍵及び秘密鍵、あるいはその他の暗号セキュリティパラメタは、セキュリティ的に重要なデータの開示を防止するため、もはや使われなくなった時点でゼロ化される。

1.1.3 TOE 管理と IT 環境

9 TOE の支援環境は重要である。ほとんどすべての場合、TOE は汎用オペレーティングシステム上で実行される純粋なソフトウェアソリューションである。それゆえ TOE は、その実行ドメイン及びその適切な使用を 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) に全面的に依存しなくてはならない (must)。ベンダには、運用環境に必要な機能を特定するために十分なインストール及び構成の指示を提供すること、そしてそれを正しく構成する方法に関する指示を提供することが期待される。

TOE は、TOE の正当な利用者のサブセットによって特定の管理アクティビティ (要件中に定義される) が行われることを必要とする。本 PP では、これらの管理機能を管理的役割に制約するために識別と認証の機能を提供するという要件を TOE には課さないが、これは TOE ベンダが適合できる方法が多数存在することを意味する。以下にその例を挙げる。

- TOE には、正当な管理者の概念が含まれない。管理ユーティリティを呼び出すことができるものは誰でも、TOE を構成できる。この場合、PP へ適合するためには、

TOE ベンダは AGD_OPE/PRE ガイダンスの一部として、TOE の正当な利用者のサブセットのみが管理ユーティリティを実行できるように運用環境を構成するために管理者が用いる手順を詳述する指示を提供しなくてはならない (must) 。そのガイダンスには例えば、管理者の許可した利用者のみが管理ユーティリティを実行できるような、運用環境中のアクセス制御メカニズムの構成が記述されることになるだろう。この例は、本 PP の基本要件を反映している。

- TOE には正当な管理者 (または管理者のセット) の概念が含まれるが､運用環境に依存して識別と認証の機能を実行し、その後正当な管理者の TOE 内部表現とマッチ可能な何らかの情報が TOE へ渡される。この場合、ST 作成者は (附属書 C に提供されるテンプレートを用いて) 要件を追加して、TOE によって提供される機能を規定する必要があるだろう。ベンダは、情報を TOE へ渡すことをサポートするために必要な運用環境の構成または設定があれば、それを記述する必要があるだろう。
- TOE には、ハードディスクを収容するシステムのどの利用者に、TOE によって提供される管理機能の利用が認可されているかを判定するために用いられる、それ独自の識別と認証の機能が含まれる。この場合、ST 作成者は附属書 C に提供される I&A を ST 本体に用いて、この機能を規定する必要があるだろう。

1.1.4 プロトコルへの準拠

10 本 PP を満たす TOE は、インターネットエンジニアリングタスクフォース (IETF) のインターネットプロトコルセキュリティ (IPsec) 『インターネットプロトコルのためのセキュリティアーキテクチャ』RFC 4301 と共に、IPsec のカプセル化されたセキュリティペイロード (ESP) プロトコルを実装する。IPsec ESP は、RFC 2406 及び 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またはトランスポートモードのいずれかで、あるいはその両方のモードで ESP をサポートする。

11 IPsec VPN クライアントは、RFC 2407、RFC 2408、RFC 2409、RFC 4109 に定義されるインターネット鍵交換 (IKE)v1 プロトコル、または RFC 5996 (セクション 2.23 に規定される NAT トラバーサルのサポートが強制される) 及び RFC 4307 に規定される IKEv2 プロトコルを用いて、VPN エンティティを認証しセッション鍵を確立する。

12 TSF が正しく RFC を実装していることを示すために、評価者は本 PP に文書化される保証アクティビティを実施しなくてはならない (shall)。本 PP の将来のバージョンでは、保証アクティビティが増補されるか、あるいはこの版に現在記述されているものよりも多くの面で RFC への準拠を確認する新たな保証アクティビティが導入されるかもしれない。

2 セキュリティ課題定義

13 本 PP は、リモートユーザが公共ネットワークを利用して専用ネットワーク (例えば、利用者のオフィスネットワーク) へアクセスする状況に対処するために作成された。ネットワークパケットは公共ネットワークと専用ネットワーク間の境界を通過することになるため、その保護が望まれる。通過中のデータを開示や改変から保護するため、VPN が作成されてセキュアな通信が確立される。このセキュアな VPN トンネルの一端を VPN クライアントが提供し、VPN クライアントと VPN ゲートウェイとの間でネゴシエーションされた VPN セキュリティ方針にしたがってネットワークパケットの暗号化及び復号を行う。

14 VPN クライアントが適切に設置及び構成されることは、その正しい運用に不可欠であり、管理者による TOE の適切な取扱いもまた対処される。

15 この章では、以下を特定する。

- VPN クライアントによって対抗される組織への IT 関連の脅威、
- 十分な保護を提供するためにコントロールが必要とされる環境への脅威、
- 必要に応じて、VPN クライアントの組織のセキュリティ方針、及び
- VPN クライアントの運用環境に関する重要な前提条件。

2.1 脅威

16 本 PP には、内部者の脅威に対して保護を提供できる要件は含まれていない。正当な利用者は敵対的または悪意があるとはみなされず、また適切なガイダンスを遵守すると信頼されている。正当な要員のみが、クライアントデバイスへアクセスできるべきである (should)。したがって、最も重要な脅威エージェントは、保護ネットワークへのアクセスを行おうと試みる権限のないエンティティである。エンティティは、自分自身を専用ネットワークへ認証することによって自分自身がネットワークの本物の利用者であることを立証できれば、権限があるとされる。この状況において、TOE は認証を行わなくてはならない要求側の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対象となるため、開示及び改変から保護されなくてはならない (must)。同様に TOE は本物の VPN ゲートウェイとの通信トンネルを確立し、また VPN ゲートウェイが高信頼エンティティに成りすましていないことを確証しなくてはならない (must)。相互認証によって、権限のないエンティティとの接続は禁止されることになる。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危殆化から自分自身を保護することになる。

17 不適切なセキュリティ方針のネゴシエーションや弱いプロトコルオプションを強制して VPN 接続を確立してしまうことも、利用者データ及び TSF データの開示または改変に結びつく可能性のある懸念点である。プロトコルの相互運用性や、強い暗号化を要求する相互に合意されたセキュリティ方針は、VPN 保護を確立するための責務である。

18 その他の脅威エージェントには、リソースが再割り当てされる際にクリアされないセキュリティ関連情報が含まれる。機密性のある値がもはや必要なくなった際、これらのデータへのアクセスは禁止されなくてはならない (must)。TOE は、セキュリティ関連情報が使用された後その他の利用者／プロセスによってアクセスされないよう、残存データが適切に取り扱われることを確実にしなくてはならない (must)。TSF データの危殆化には、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、不適切なアクセスや更新から保護されなくてはならない (must)。

19 TOE に対して上述したネットワーク攻撃は、不正なアクセスを行い、セキュリティを危殆化させる唯一の経路ではない。製品を更新することは、脅威環境への変更へ確実に対処す

るために必要な、通常の機能である。利用される攻撃ベクトルには、欠陥が内在するソフトウェアのパッチされていないバージョンへの攻撃が伴うことが多い。パッチをタイムリーに適用することによって、製品がそのセキュリティ方針を維持し強制できる可能性が増大する。しかし、更新は信頼されたソースからのものでなくてはならない (must)。そうでなくては、攻撃者がルートキットやボット、あるいはその他のマルウェアなど、自分たちの選択した悪意のあるコードを含んだ独自の「更新」を作成することができてしまう。

20 アクセスを得るために用いられたメカニズムにかかわらず (ネットワーク攻撃、悪意のあるコード、構成中のエラーの利用、セッションのハイジャックなど)、敵対者がアクセスできるようになったら最後、TOE とそのデータは危殆化してしまう。監査記録の生成を改変して、それ以降 TOE に行われた任意の悪質なアクションを隠すことによって、潜在的な問題がマスクされる可能性があるとともに、その悪意のあるアクションを引き起こした人物の特定が困難になる。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及ぼす可能性があり、また引き起こされた問題を低減することが困難となる可能性がある。監査レビューと監査ストレージは IT 環境によって処理されるため、これらは本 PP の範囲外であることに注意されたい。しかし、これが適切に行われセキュアに TOE を保護することは前提とされる。

21 以下の表に、VPN クライアントと運用環境によって対処される脅威を列挙した。以下に特定されるすべての脅威について、前提とされる攻撃者の専門的知識のレベルは、未習熟である。

表 1 : 脅威

脅威	脅威の説明
T.TSF_FAILURE	TOE のセキュリティメカニズムが故障し、TSF の危殆化をもたらすおそれがある。
T.UNAUTHORIZED_ACCESS	利用者が、TOE データ及び TOE 実行可能形式コードへの権限のないアクセスを行うおそれがある。悪意のある利用者、プロセス、または外部 IT エンティティが、データまたは TOE リソースへアクセスするために正当なエンティティに成りすますおそれがある。悪意のある利用者、プロセス、または外部 IT エンティティが、自分自身を TOE と偽って提示し、識別と認証のデータを取得するおそれがある。
T.UNAUTHORIZED_UPDATE	悪意のある人物が、TOE のセキュリティ機能を危殆化させるおそれのある製品への更新をエンドユーザへ供給することを試みるおそれがある。
T.USER_DATA_REUSE	利用者データが、本来の送信者が意図しない宛先へ不用意に送信されるおそれがある。

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、専用ネットワークと公共ネットワークとの間の境界を通過するネットワークパケットを保護するために適用できることを理由として選択された。手続きと関連する方針も、前提条件として言明されている。形式的な参照情報を持たない方針は、方針の説明にしたがって作成され形式化されることが期待される。

表 2：組織のセキュリティ方針

方針	方針の説明
P.COMPATIBILITY	TOE は、同一のプロトコルを用いる他のネットワーク機器との相互運用性を高めるため、実装されたプロトコルの Request for Comments (RFC) 要件を満たさなくてはならない (must)。
P.CONFIGURABILITY	TOE は、その運用のセキュリティ関連の側面を構成できる機能を提供しなくてはならない (must)。

2.3 前提条件

23 セキュリティ課題を定義するこのセクションでは、セキュリティ機能を提供可能とするために運用環境に対して課される前提条件を示す。TOE がこれらの前提条件を満たさない運用環境に配置された場合、もはや TOE はそのセキュリティ機能のすべてを提供することはできないかもしれない。前提条件は、物理的環境、人的、及び運用環境の接続性に対して課される可能性がある。

表 3：TOE の前提条件

前提条件	前提条件の説明
A.NO_TOE_BYPASS	情報は、TOE を経由せずに 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へ流出することはできない。
A.PHYSICAL	TOE 及びそれに含まれるデータの価値に対応した物理的セキュリティが、環境によって提供されることが前提とされる。
A.TRUSTED_ADMIN	TOE 管理者は、すべての管理ガイダンスを信頼された方法で遵守し適用すると信頼されている。

3 セキュリティ対策方針

24 セキュリティ対策方針は、評価対象 (TOE) 及び運用環境に関する要件であって、セクション 2 の脅威、組織のセキュリティ方針、そして前提条件から導出されたものである。セクション 3 では、TOE に関するセキュリティ対策方針を SFR として、より形式的に再び述べる。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特定する。これらのセキュリティ対策方針は、特定された脅威に対抗する、または特定された任意の組織のセキュリティ方針に準拠する、あるいはその両方の言明された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によって、これらの対策方針を満たす。

表 4 : TOE のセキュリティ対策方針

対策方針	対策方針の説明
O.AUTH_COMM	TOE は、TOE であるふりをした別のエンティティと利用者が通信していないことを確実にするとともに、TOE が正当な IT エンティティのふりをしている別のエンティティではなく正当な IT エンティティと通信を行っていることを確実にする手段を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS	TOE は、暗号機能 (すなわち、暗号化／復号及びデジタル署名操作) を提供することによって機密性を維持し、また TOE 及びそのホスト環境の外部へ送信されるデータの改変を検出することを可能としなくてはならない (shall)。
O.GW_AUTHENTICATION	TOE は、セキュリティアソシエーションを確立しようと試みる VPN ゲートウェイを認証する。
O.PROTOCOLS	TOE は、相互運用性を確実にするために、RFC または業界規格あるいはその両方に準拠した標準化されたプロトコルが TOE に実装されていることを確実にする。
O.RESIDUAL_INFORMATION_CLEARING	TOE は、保護されたリソースに含まれるいかなるデータも、そのリソースが再割り当てされた際に利用できないことを確実にする。
O.TOE_ADMINISTRATION	TOE は、管理者が TOE を構成できるメカニズムを提供する。
O.TSF_SELF_TEST	TOE は、TOE が適切に動作していることを確実にするため、TOE のセキュリティ機能の何らか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 へのいかなる更新も改変されておらず、また (オプションとして) 信頼されたソースからのものであることが管理者によって検証できることを確実にするための機能を提供する。

3.2 運用環境のセキュリティ対策方針

26 TOE の運用環境は、TOE がそのセキュリティ機能 (これは、TOE のセキュリティ対策方針によって定義される) を正しく提供できるように支援する、技術的及び手続的手段を実装する。このパートごとのソリューションは、運用環境のセキュリティ対策方針と呼ばれ、また運用環境が達成すべき目標を記述する一連の言明によって構成される。

27 このセクションでは、IT ドメインによって、もしくは非技術的または手続き的手段によって対処されるべきセキュリティ対策方針を定義する。セクション 2.3 中に特定された前提条件は、運用環境のセキュリティ対策方針として組み込まれている。これによって環境に対する追加的な要件が課されるが、これらは主に手続き的または管理的手段によって満たされる。表 5 に、環境のセキュリティ対策方針を特定する。

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 を経由せずに 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へ流出することはできない。
OE.PHYSICAL	TOE 及びそれに含まれるデータの価値に対応した物理的セキュリティが、運用環境によって提供されることが前提とされる。
OE.TRUSTED_ADMIN	TOE 管理者は、すべての管理ガイダンスを信頼された方法で遵守し適用すると信頼されている。

3.3 セキュリティ対策方針の根拠

28 このセクションでは、セクション 3 で定義されるセキュリティ対策方針の根拠を記述する。表 6 に、セキュリティ対策方針から脅威及び方針への対応付けを示す。

表 6：セキュリティ対策方針から脅威及び方針への対応付け

脅威／方針	脅威及び方針に対処する対策方針	根拠
T.TSF_FAILURE TOE のセキュリティメカニズムが故障し、TSF の危殆化をもたらすおそれがある。	O.TSF_SELF_TEST TOE は、TOE が適切に動作していることを確実にするため、TOE のセキュリティ機能の何らか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 がセルフテストスイートを実行して TSF の正しい運用の例証に成功することを確実にすることによって、この脅威へ対抗する。
T.UNAUTHORIZED_ACCESS 利用者が、TOE データ及び TOE 実行可能形式コードへの権限のないアクセスを行うおそれがある。悪意のある利用者、プロセス、または外部 IT エンティティが、データまたは TOE リソースへアクセスするために正当なエンティティに成りすますおそれがある。悪意のある利用者、プロセス、または外部 IT エンティティが、自分自身を TOE と偽って提示し、識別と認証のデータを取得するおそれがある。	O.AUTH_COMM TOE は、TOE であるふりをした別のエンティティと利用者が通信していないことを確実にするとともに、TOE が正当な IT エンティティのふりをしている別のエンティティではなく正当な IT エンティティと通信を行っていることを確実にする手段を提供する。 O.CRYPTOGRAPHIC_FUNCTIONS TOE は、暗号機能 (すなわち、暗号化／復号及びデジタル署名操作) を提供することによって機密性を維持し、また TOE の物理的に分離した部分間で送信される、または TOE 外部に保存される、データの改変を検出することを可能としなくてはならない (shall)。 O.GW_AUTHENTICATION TOE は、セキュリティアソシエーションを確立しようと試みる VPN ゲートウェイを認証する。 O.TOE_ADMINISTRATION TOE は、管理者が TOE を構成できるメカニズムを提供する。	O.AUTH_COMM 及び O.GW_AUTHENTICATION は、TOE がそのエンティティとの通信に先立って VPN ゲートウェイの識別と認証を行うことを確実にすることによって、この脅威を低減するために役立つ。また TOE は、通信に先立って相互認証を確実にするために、自分自身の資格情報を VPN ゲートウェイへ送信できなくてはならない (must)。 O.CRYPTOGRAPHIC_FUNCTIONS は、他の保護メカニズムに必要とされる基盤となる暗号機能を提供することによって、この脅威の低減に貢献する。 O.TOE_ADMINISTRATION は、TOE がセキュアな方法で構成されることを可能とするメカニズムの提供を TOE に要求する。

脅威／方針	脅威及び方針に対処する対策方針	根拠
T.UNAUTHORIZED_UPDATE 悪意のある人物が、TOE のセキュリティ機能を危殆化させるおそれのある製品への更新をエンドユーザへ供給することを試みるおそれがある。	O.VERIFIABLE_UPDATES TOE は、TOE へのいかなる更新も改変されておらず、また (オプションとして) 信頼されたソースからのものであることが管理者によって検証できることを確実にするための機能を提供する。	O.VERIFIABLE_UPDATES は、管理者が更新を確認できることを確実にする。
T.USER_DATA_REUSE 利用者データが、本来の送信者が意図しない宛先へ不用意に送信されるおそれがある。	O.RESIDUAL_INFORMATION_CLEARING TOE は、保護されたリソースに含まれるいかなるデータも、そのリソースが再割り当てされた際に利用できないことを確実にする。	O.RESIDUAL_INFORMATION_CLEARING は、ある利用者／プロセスによって解放されたリソースが別の利用者／プロセスへ割付けられた際に TSF データ及び利用者データが永続的でないことを確実にすることによって、この脅威へ対抗する。
P.COMPATIBILITY TOE は、同一のプロトコルを用いる他のネットワーク機器との相互運用を促進するため、実装されたプロトコルの Request for Comments (RFC) 要件を満たさなくてはならない (must)。	O.PROTOCOLS TOE は、相互運用性を確実にするために、RFC または業界規格あるいはその両方に準拠した標準化されたプロトコルが TOE に実装されていることを確実にするとともに、集中型の監査サーバ及び RADIUS 認証サーバとの通信をサポートすることをも確実にする。	O.PROTOCOLS は、標準化されたプロトコルが TOE に実装されていることを要求し、同一のプロトコルを利用する IT エンティティ間での相互運用性を確実にすることによって、この方針を満たす。
P.CONFIGURABILITY TOE は、その運用のセキュリティ関連の側面を構成できる機能を提供しなくてはならない (must)。	O.TOE_ADMINISTRATION TOE は、管理者が TOE を構成できるメカニズムを提供する。	O.TOE_ADMINISTRATION は、TOE をセキュアに構成するために必要とされるメカニズムを TOE が提供することを確実にすることによって、この方針を満たす。

29 表 7 に、セキュリティ対策方針から前提条件への対応付けを示す。

表 7：セキュリティ対策方針から前提への対応付け

前提条件	前提条件に対処する対策方針	根拠
A.NO_TOE_BYPASS 情報は、TOE を経由せずに 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	OE.NO_TOE_BYPASS 情報は、TOE を経由せずに 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へ流出することはできない。	OE.NO_TOE_BYPASS は、ネットワーク上へ流れるすべての情報が TOE を経由することを確実にする。

前提条件	前提条件に対処する対策方針	根拠
へ流出することはできない。		
A.PHYSICAL TOE 及びそれに含まれるデータの価値に対応した物理的セキュリティが、環境によって提供されることが前提とされる。	OE.PHYSICAL TOE 及びそれに含まれるデータの価値に対応した物理的セキュリティが、運用環境によって提供されることが前提とされる。	OE.PHYSICAL は、TOE、TSF データ、及び保護された利用者データが物理的攻撃 (例えば、窃盗、破壊、あるいは傍受など) から保護されることを確実にする。物理的攻撃には、TOE 環境への権限のない侵入者が含まれるかもしれないが、TOE 環境へのアクセス権限を与えられている個人によって行われるかもしれない物理的な破壊アクションは含まれない。
A.TRUSTED_ADMIN TOE 管理者は、すべての管理ガイダンスを信頼された方法で遵守し適用すると信頼されている。	OE.TRUSTED_ADMIN TOE 管理者は、すべての管理ガイダンスを信頼された方法で遵守し適用すると信頼されている。	OE.TRUSTED_ADMIN は、管理者が適切に教育されていること、そして管理ガイダンスでミスなしに適切に環境を構成する方法が管理者に指示されていることが確実にする。

4 セキュリティ要件と根拠

30 セキュリティ要件は、機能要件と保証要件に大別される。SFR は、セキュリティ対策方針の形式的な具体化であり、適用上の注意と共にセクション 4.1 で提供される。これらは通常、抽象概念よりも詳細なレベルで行われるが、完全な変換である必要がある (セキュリティ対策方針は完全に対処されなくてはならない (must))。CC ではいくつかの理由から、この標準化された言語への変換が要求されている。

- 何が評価されるべきかについて、正確な記述を提供するため。TOE のセキュリティ対策方針は通常自然言語で形式化されるが、標準化された言語への変換によってより正確な TOE の機能の記述が強制される。
- 2 件の ST 間の比較を可能とするため。異なる ST 作成者は自分のセキュリティ対策方針の記述に異なる専門用語を使っているかもしれないが、標準化された言語によって同一の専門用語と概念の使用が強制される。これによって容易な比較が可能となる。

31 セキュリティ保証要件 (SAR) は、典型的には SFR とは独立して挿入され列挙される定型文である。そして選択された SAR に基づいた評価中に、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た、よりカスタム化されたアプローチが取られている。本 PP でも SAR は文脈と完全性に応じてセクション 4.3 に列挙されているが、SFR と SAR のそれぞれについて評価者がこの TOE に行う必要のあるアクティビティは「保証アクティビティ」のパラグラフに詳述されている。保証アクティビティは、評価を完全なものとするために行われなくてはならないアクティビティの規範的な記述である。保証アクティビティは本 PP の 2 か所に配置されている。具体的な SFR と関連付けられたものはセクション 4.1 に配置され、SFR と独立したものはセクション 4.3 に詳述されている。

32 SFR と直接関連付けられるアクティビティについては、各 SFR の後に 1 つ以上の保証アクティビティが列挙され、この技術に提供される保証を実現するために行われる必要のあるアクティビティが詳述される。

33 SFR とは独立したアクティビティを必要とする SAR については、実現される必要のある追加的保証アクティビティが、その SAR と関連付けられた特定の保証アクティビティが書かれる対象となった SFR への参照とともに、セクション 4.3 に示されている。

34 このプロテクションプロファイルの将来の世代では、実際の製品評価から得られた教訓に基づいた、より詳細な保証アクティビティを提供することになるかもしれない。

4.1 セキュリティ機能要件

35 このセクションでは、TOE によって提供されるセキュリティ機能に特有であり、また VPN クライアントを他の TOE から差異化する TOE の SFR を特定する。SFR の焦点となる分野は、監査、暗号、セキュリティ管理、セルフテスト、及び正当な外部 IT エンティティ (例えば、VPN ゲートウェイ) との通信に関連したものである。

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
暗号サポートクラス (FCS)	FCS_CKM.1(1) 暗号鍵生成 (非対称鍵)
	FCS_CKM.1(2) 暗号鍵生成 (非対称鍵—IKE)
	FCS_CKM_EXT.4 暗号鍵のゼロ化
	FCS_COP.1(1) 暗号操作 (データの暗号化／復号)
	FCS_COP.1(2) 暗号操作 (暗号署名)
	FCS_COP.1(3) 暗号操作 (暗号ハッシュ)
	FCS_COP.1(4) 暗号操作 (鍵付きハッシュによるメッセージ認証)
	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 十分な残存情報の保護
識別と認証クラス (FIA)	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 管理機能の仕様
TSF の保護 (FPT)	FPT_TST_EXT.1 拡張：TSF のテスト
	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：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、以下にしたがって**鍵確立に用いられる非対称**鍵を生成しなくてはならない (shall)。

- *有限体ベースの鍵確立スキームについては、NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"*
- *楕円曲線ベースの鍵確立スキーム及び「NIST 曲線」P-256、P-384 及び [selection: P-521、その他の曲線なし] (FIPS PUB 186-3, "Digital Signature Standard" の定義による) の実装については、NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"*
- *選択:RSA ベースの鍵確立スキームについては、NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes、その他なし]*

また、規定された暗号鍵サイズは *112 ビットの強度を持つ対称鍵と同等、またはそれよりも大きくなくてはならない。*

適用上の注意：

36 *このコンポーネントは、TOE によって利用されるさまざまな暗号プロトコルの鍵確立の目的に用いられる公開鍵／秘密鍵ペアを TOE が生成できることを要求している。*

37 *用いられるべきドメインパラメタは本 PP のプロトコル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ておらず、したがって本 PP に規定されたプロトコルに TOE が準拠する際には追加的なドメインパラメタの検証は必要とされない。*

保証アクティビティ：

38 *評価者は、ST 作成者によって行われた選択に応じて、上記の要件を試験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用いなくてはならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。*

39 *行われた選択に応じて TSF が 800-56A または 800-56B あるいはその両方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ることを確証しなくてはならない (shall)。*

- *TSS には、TOE が適合する適切な 800-56 標準のすべての選択が列挙されていなくてはならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなくてはならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションを TOE が実装している場合には、それが TSS に記述されなくてはならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠を TSS は提供しなくてはならない (shall)。*
- *800-56A 及び 800-56B (選択に応じて) の該当するセクションのそれぞれにおいて、「しなくてはならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それを記述しなくてはならない (shall)。*

TOE が強制すべきセキュリティ要件に影響する可能性のある TOE に特有の拡張、文書に含まれていない処理、または文書によって許可された代案の実装が存在する場合には、それを記述しなくてはならない (shall)。

FCS_CKM.1(2) 暗号鍵生成 (非対称鍵—IKE)

FCS_CKM.1.1(2) **詳細化**：TSF は、以下にしたがって **IKE ピア認証に用いられる非対称**鍵を生成しなくてはならない (shall)。

[選択、少なくとも 1 つを選択：

- RSA 方式については、FIPS PUB 186-3, “Digital Signature Standard (DSS)”の附属書 B.3、
- ECDSA スキームについては、FIPS PUB 186-3, “Digital Signature Standard (DSS)”の附属書 B.4 ならびに「NIST 曲線」P-256、P-384 及び [選択：P-521、その他の曲線なし] の実装、
- AES を使用した RSA スキームについて ANSI X9.31-1998 の附属書 A.2.4]

また、規定された暗号鍵サイズは *112 ビットの強度を持つ対称鍵と同等、またはそれよりも大きく*なくてはならない。

適用上の注意：ANSI X9.31-1998 のオプションは、この文書の将来の版では選択から削除されることになる。現時点では、業界がモダンな FIPS PUB 186-3 標準への移行を完了するまでに多少の時間を許可するため、この選択は FIPS PUB 186-3 のみに限定されてはいない。

この要件が TOE に生成を求める鍵は、IKE (v1 または v2 のいずれか) 鍵交換中に VPN エンティティの認証に用いられることが意図されている。公開鍵は X509v3 証明書中の識別情報との関連付けが求められる一方で、この関連付けは TOE によって実施されることは求められておらず、運用環境中の認証局による実施が期待されている。

FCS_IPSEC_EXT.1 に示した通り、TOE には認証をサポートする RSA または ECDSA (あるいはその両方) の実装が求められる。

生成された 2048 ビット RSA 鍵の強度は、112 ビットの対称鍵強度と同等、またはそれよりも大きい必要がある。鍵強度の同等性については、NIST Special Publication 800-57, "Recommendation for Key Management" を参照されたい。

保証アクティビティ：

評価者は、ST 作成者によって実施された選択に応じて、"The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)" 及び "The RSA Validation System (RSA2VS)" の鍵ペア生成の部分を、上記の要件をテストする際のガイドとして利用しなくてはならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。

評価者は、TSS に鍵ペアの生成される方法が記述されていることをチェックし確証しなくてはならない (shall)。TSF の実装が FIPS PUB 186-3 に準拠していることを示すために、評価者は TSS に下記の情報が含まれることを確証しなくてはならない (shall)。

- *TSS には、TOE が準拠する附属書 B のすべてのセクションが列挙されていなくてはならない (shall)。*
- *TSS に列挙された該当するセクションのそれぞれについて、「しなくてはならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションを TOE が実装している場合には、それが TSS に記述されなくてはならない (shall)。含まれる機能が標準においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合には、TOE によって実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠を TSS は提供しなくてはならない (shall)。*
- *附属書 B の該当するセクションのそれぞれにおいて、「しなくてはならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合には、それを記述しなくてはならない (shall)。*

TOE に特有の拡張、附属書に含まれていない処理、または附属書によって許可された代案の実装であって TOE が強制すべきセキュリティ要件に影響するかもしれないものが存在する場合には、それを記述しなくてはならない (shall)。

FCS_CKM_EXT.4　　暗号鍵のゼロ化

FCS_CKM_EXT.4.1　　**詳細化**：TSF は、すべての平文の共通暗号鍵及び秘密暗号鍵ならびに CSP を、もはや必要とされなくなった際にゼロ化しなくてはならない (shall)。

適用上の注意：

40 *あらゆるセキュリティ関連情報 (鍵や認証データ、そしてパスワードなど) は、セキュリテ*

ィ上重要なデータの開示または改変を防止するため、もはや使われなくなった際にはゼロ化されなくてはならない (must)。

41 *上記のゼロ化は、平文鍵／CSP のすべての中間ストレージ領域 (例えば、メモリバッファなどの任意のストレージであって、そのようなデータのパス中に含まれるもの) へ、そこから別の場所へ鍵／CSP が転送された直後に適用される。*

42 *TOE には必ずしもホスト IT 環境が含まれるとは限らないので、この機能の範囲は必然的にある程度制約される。この要件の目的においては、TOE がホストの基盤となる正しい機能を呼び出してゼロ化を行うことで十分である (これは、データがゼロ化されることを確実にするため TOE にカーネルモードメモリドライバが含まれる必要があることは意味しない)。*

保証アクティビティ：

43 *評価者は、共通鍵 (共通鍵暗号化に用いられる鍵)、秘密鍵、及び鍵の生成に用いられる CSP のそれぞれについて、それらがゼロ化される時点 (例えば、使用直後、システムのシャットダウン時、など)、及び行われるゼロ化手続きの種類 (ゼロで上書き、ランダムパターンで 3 度上書き、など) が TSS に記述されていることをチェックして確証しなくてはならない (shall)。保護されるべきマテリアルの保存に異なる種類のメモリが用いられている場合、評価者はデータが保存されるメモリに関するゼロ化手続き (例えば、「フラッシュメモリ上に保存される共通鍵はゼロで 1 度上書きすることによってゼロ化されるが、内部ハードドライブ上に保存される共通鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってゼロ化される」) が TSS に記述されていることをチェックして確証しなくてはならない (shall)。ゼロ化を検証するためにリードバックが行われる場合、このことも記述されなくてはならない (shall)。*

44

暗号操作 (FCS_COP)

FCS_COP.1(1) **暗号操作 (データの暗号化／復号)**

FCS_COP.1.1(1) **詳細化:** TSF は、規定された暗号アルゴリズムとして **GCM、CBC、**[**割付：*1 つ以上のモード、他のモードなし***] *で動作する AES* 及び暗号鍵サイズとして 128 ビット、256 ビット、及び [**選択: 192 ビット、その他の鍵サイズなし**] であって下記を満たすものにしたがって、[*暗号化及び復号*] を行わなくてはならない (shall)。

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **NIST SP 800-38D, NIST SP 800-38A [選択：NIST SP 800-38B、NIST SP 800-38C、NIST SP 800-38E、その他の標準なし]**

適用上の注意：

45 *本 PP は、IPsec 及び IKE プロトコルにおいて GCM 及び CBC の使用を要求する (FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6)。したがって、IPsec 要件との一貫性のため ST 作成者にこれら 2 つのモードを確実に取り込ませるよう、NDPP 中の FCS_COP.1.1(1) エレメントがここで規定されている。*

保証アクティビティ：

46 *評価者は、上記の要件をテストする際のガイドとして"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 から入手できる) から、上記の要件において選択されたモードに適切なテストを用いなくてはならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。

FCS_COP.1(2) 暗号操作 (暗号署名)

FCS_COP.1.1(2) **詳細化**：TSF は、下記にしたがって**暗号署名サービス**を実施しなくてはならない (shall)。

- **[選択、次から少なくとも 1 つを選択 :** ***2048 ビット以上の鍵サイズ (modulus) の RSA デジタル署名アルゴリズム (RSA) であって*** **FIPS PUB 186-2 または FIPS PUB 186-3, “Digital Signature Standard” *を満たすもの*、**
- ***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) であって*** **FIPS PUB 186-3, “Digital Signature Standard” 及び 「NIST 曲線」P-256、P-384 及び [選択：P-521、その他の曲線なし] (FIPS PUB 186-3, “Digital Signature Standard” の定義による) *を満たすもの*]。**

保証アクティビティ：

47 *評価者は、"The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)" 及び "The RSA Validation System (RSA2VS)" の署名生成及び署名検証の部分を上記の要件をテストする際のガイドとして利用しなくてはならない (shall)。用いられる検証システムは、ST 中に特定される準拠標準 (すなわち FIPS PUB 186-3) に適合しなくてはならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。*

FCS_COP.1(3) 暗号操作 (暗号ハッシュ)

FCS_COP.1.1(3) **詳細化**：TSF は、**[選択：SHA-1、SHA 256、SHA 384]** にしたがい、**メッセージダイジェストのサイズが [選択：160、256、384] ビットの**、以下 *FIPS Pub 180-3, “Secure Hash Standard”* を満たす暗号ハッシュサービスを行わなくてはならない (shall)。

適用上の注意：

48 ハッシュアルゴリズムの選択は、メッセージサイズの選択と対応していなくてはならない (must)。例えば SHA-1 が選択された場合に唯一の有効なメッセージダイジェストサイズの選択は 160 ビットとなる。

保証アクティビティ：

49 *評価者は、上記の要件をテストする際のガイドとして"The Secure Hash Algorithm Validation System (SHAVS)" を用いなくてはならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。*

FCS_COP.1(4) 暗号操作 (鍵付きハッシュによるメッセージ認証)

FCS_COP.1.1(4) **詳細化**：TSF は、規定された暗号アルゴリズム **HMAC-** [選択：

SHA-1、SHA-256、SHA-384]、鍵サイズ **[割付：HMAC に用いられる（ビット単位の）鍵サイズ]、及びメッセージダイジェストサイズ** [選択：160、256、384] **ビット**であって、以下：**FIPS PUB 198-1, “The Keyed-Hash Message Authentication Code”、及び FIPS PUB 180-3, “Secure Hash Standard”**を満たすものにしたがって、**鍵付きハッシュメッセージ検証**を行わなくてはならない (shall)。

適用上の注意：

50 *ハッシュアルゴリズムの選択は、メッセージサイズの選択と対応していなくてはならない (must)。例えばHMAC-SHA-256 が選択された場合に唯一の有効なメッセージダイジェストサイズの選択は256 ビットとなる。*

51 *上記のメッセージダイジェストサイズは、基盤となって用いられるハッシュアルゴリズムに対応する。ハッシュ計算の後に HMAC の出力を切り捨てることは、さまざまなアプリケーションにおいて適切なステップであることに注意されたい。このことは、この要件への適合性を無効とするものではないが、切り捨てが行われること、最終出力のサイズ、そしてこの切り捨てが準拠する標準がST に言明されるべきである (should)。*

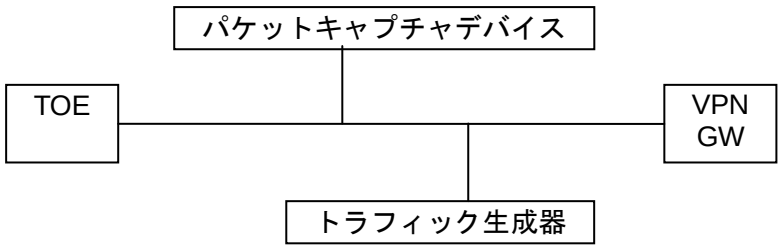
保証アクティビティ：

52 *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)" を用いなくてはならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。*

拡張：インターネットプロトコルセキュリティ (FCS_IPSEC_EXT)

53 TSF が正しく RFC を実装していることを示すために、評価者は下記の保証アクティビティを実施しなくてはならない (shall)。本 PP の将来のバージョンでは、保証アクティビティが増補されるか、あるいはこの版に現在記述されているものよりも多くの面で RFC への準拠を確認する新たな保証アクティビティが導入されるかもしれない。

54 TOE は、VPN ゲートウェイとの通信に用いられる接続を確立するために IPsec プロトコルを利用することが求められる。



評価者は最低限、上に示したテスト環境と同等のテスト環境を作成しなくてはならない (shall)。ネットワークパケットの作成と、評価者が ICMP、IPv4、IPv6、UDP、及び TCP パケットヘッダ中のフィールドを操作できるようにするため、トラフィック生成器を利用することが期待される。評価者は、テスト環境に差異があれば、その正当化を提供しなくてはならない (must)。

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、RFC 4301 の規定により IPsec アーキテクチャを実装しなくてはならない (shall)。

保証アクティビティ：

TSS

TOE の実装が上記のように RFC 4301 に準拠していることを判定する以外には、何も行うことはない。

ガイダンス

評価者は操作ガイダンスを調査して、破棄 (DISCARD)、バイパス (BYPASS)、及び保護 (PROTECT) のルールを規定するエントリを SPD に構築する方法が管理者へ指示されていることを検証しなくてはならない (shall)。

テスト

評価者は、操作ガイダンスを用いて TOE を構成し、下記のテストを行う。

テスト 1：評価者は TOE の SPD を、DISCARD、BYPASS、PROTECT のルールが存在するよう構成しなくてはならない (shall)。各パケットが 3 つのルールのどれか 1 つにマッチするように、パケットヘッダに適切なフィールドを持つ 3 つのネットワークパケットを評価者が送り込むことができるよう、ルールの構築に用いられる選択肢は異なっていなくてはならない (shall)。評価者は、TOE が期待されたふるまいを示していることを、監査証跡を通して、またパケットキャプチャによって確認する。適切なふるまいとは、適切なパケットが破棄され、変更なしに通過し、IPsec の実装によって暗号化されることである。

テスト 2：評価者は、BYPASS と PROTECT という別の操作を行う、2 つの同一の SPD エントリを作り上げなくてはならない (shall)。これらのエントリは次に 2 通りの異なる順序でデプロイされるべきであり、どちらの場合についても評価者は、該当するパケットを生成してパケットキャプチャ及びログによって確認を行うことにより、両方の場合で最初のエントリが適用されることを確証しなくてはならない (shall)。

テスト 3：評価者は、一方が他方の部分集合（例えば、特定のアドレスとネットワークセグメント）となるように 2 つのエントリを作り上げるべきことを違いとして、上記の手順を繰り返さなくてはならない (shall)。ここでも管理者は両方の順序をテストして、ルールの限定性にかかわらず、最初のエントリが適用されることを確証すべきである (should)。

FCS_IPSEC_EXT.1.2 TSF は、[選択、少なくとも 1 つを選択：トンネルモード、トランスポートモード] を実装しなくてはならない (shall)。

保証アクティビティ：

TSS

評価者は TSS をチェックし、TOE がトンネルモードまたはトランスポートモード、あるいはその両方 (選択による) で動作できると言明されていることを確証する。

ガイダンス

評価者は、運用ガイドが管理者へ選択された各モードの TOE の構成方法を指示していることを確認しなくてはならない (shall)。

テスト

テスト 1 (条件付き)：トンネルモードが選択されている場合、評価者は操作ガイダンスを用いて TOE をトンネルモードで動作するように構成し、また VPN GW をトンネルモードで

動作するように構成する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いてTOE 及びVPN GW を構成し、許容されるSA がネゴシエーションできることを確証する。評価者は次に、TOE からの接続を開始し、VPN GW ピアへ接続しなくてはならない (shall)。評価者は、トンネルモードを用いた接続の確立が成功していることを、監査証跡及びキャプチャされたパケットで確認する。

テスト2 (条件付き)：トランスポートモードが選択されている場合、評価者は操作ガイダンスを用いてTOE をトランスポートモードで動作するように構成し、またVPN GW もトランスポートモードで動作するように構成する。評価者は、任意の許容される暗号アルゴリズム、認証手法などを用いてTOE 及びVPN GW を構成し、許容されるSA がネゴシエーションできることを確証する。評価者は次に、TOE からの接続を開始し、VPN GW へ接続する。評価者は、トランスポートモードを用いた接続の確立が成功していることを、監査証跡及びキャプチャされたパケットで確認する。

FCS_IPSEC_EXT.1.3 TSF は、その他のエントリにマッチしなかったものすべてにマッチして破棄する名目的なエントリを SPD の最後に持たなくてはならない (shall)。

保証アクティビティ：

TSS

評価者はTSS を調査して、SPD に対してパケットが処理される方法と、マッチする「ルール」が存在しない場合には暗黙的または明示的にネットワークパケットを破棄させる最後のルールの存在が、TSS に記述されていることを検証しなくてはならない (shall)。

ガイダンス

評価者は、操作ガイダンスがSPD の構築方法に関する指示を提供していることをチェックし、そのガイダンスを用いてTOE を構成し、以下のテストを行う。

テスト

テスト1：評価者はTOE のSPD に、ネットワークパケットを破棄 (DISCARD)、バイパス (BYPASS)、及び保護 (PROTECT) する操作が含まれるエントリが存在するよう構成しなくてはならない (shall)。また評価者はTOE を、FCS_IPSEC_EXT.1 に関するすべての監査対象事象が有効となるよう構成する。評価者は、FCS_IPSEC_EXT.1.1 を検証するために作成されたSPD を使ってもよい。評価者はBYPASS エントリとマッチするネットワークパケットを構築し、そのパケットをTOE へ送信しなくてはならない (shall)。評価者は、ネットワークパケットがTOE によって適切な宛先インタフェースへ変更なしに通過されることを確認すべきである (should)。評価者は次に、パケットヘッダのフィールドを変更し、評価者が作成したエントリへはもはやマッチしないようにしなくてはならない (shall) (最後のエントリとして、それまでのエントリのどれにもマッチしなかったパケットを破棄する「TOE によって作成された」エントリが存在するかもしれない)。評価者はそのパケットをTOE へ送信し、パケットがどのTOE のインタフェースへも流れて行くことが許可されないことを確認する。評価者は、期待されたようにパケットが破棄されたことを示す監査証跡が生成されることを検証しなくてはならない (shall)。

FCS_IPSEC_EXT.1.4 TSF は、RFC 4303 の定義による IPsec プロトコル ESP を、RFC 4106 の規定による暗号アルゴリズム AES-GCM-128、AES-GCM-256、[選択：AES-CBC-128、AES-CBC-256 (両者とも RFC 3602 によって規定される) と Secure Hash Algorithm (SHA) ベースの HMAC との組み合わせ、その他のアルゴリズムなし] を用いて実装しなくてはならない (shall)。

保証アクティビティ：

TSS

評価者は TSS を調査して、アルゴリズム AES-GCM-128 及び AES-GCM-256 が実装されていることを検証しなくてはならない (shall)。ST 作成者が AES-CBC-128 または AES-CBC-256 のいずれかを要件に選択している場合には、評価者はそれらもまた TSS に記述されていることを検証する。さらに、評価者は SHA ベースの HMAC アルゴリズムが FCS_COP.1(4) 暗号操作 (鍵付きハッシュメッセージ認証) に規定されるアルゴリズムに準拠していることを確証する。

ガイダンス

評価者は操作ガイダンスをチェックして、AES-GCM-128 及び AES-GCM-256 アルゴリズムを使用するように TOE を構成する方法について指示が与えられていること、また AES-CBC-128 または AES-CBC-256 のいずれかが選択されている場合にはこれらについても使用方法がガイダンスに指示されていることを確証する。

テスト

テスト 1 : 評価者は操作ガイダンスの指示により TOE を構成し、TOE が AES-GCM-128 及び AES-GCM-256 アルゴリズムのそれぞれを使用するように構成するとともに、ESP を使用した接続の確立を試行しなくてはならない (shall)。ST 作成者が AES-CBC-128 または AES-CBC-256 のいずれかを選択している場合には、TOE はこれらのアルゴリズムを使用するよう構成され、評価者は選択されたこれらのアルゴリズムについて ESP を使用した接続の確立を試行する。

FCS_IPSEC_EXT.1.5 TSF は、以下のプロトコルを実装しなくてはならない (shall)。 [選択、少なくとも 1 つを選択：RFC 2407、RFC 2408、RFC 2409、RFC 4109、[選択：拡張シーケンス番号についてその他の RFC なし、拡張シーケンス番号について RFC 4304] 及び [選択 : ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] の定義による IKEv1 ; RFC 5996 (セクション 2.23 の規定による NAT トラバーサルのサポートが強制される)、RFC 4307、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] の定義による IKEv2]。

保証アクティビティ：

TSS

評価者は TSS を調査して、IKEv1 または IKEv2、あるいはその両方が実装されていることを検証しなくてはならない (shall)。

ガイダンス

評価者は操作ガイダンスをチェックして、IKEv1 または IKEv2 あるいはその両方 (選択による) を使用するように TOE を構成する方法が管理者に指示されていることを確証し、またガイダンスを利用して NAT トラバーサルを実施するよう TOE を構成し、下記のテストを行う。

テスト

テスト 1 : 評価者は、TSS 及び RFC 5996 のセクション 2.23 の記述により NAT トラバーサル処理を実施するよう TOE を構成しなくてはならない (shall)。評価者は IPsec 接続を開始し、NAT トラバーサルが成功することを判定しなくてはならない (shall)。

FCS_IPSEC_EXT.1.6 TSF は、[選択、少なくとも 1 つを選択：IKEv1、IKEv2] プロトコルにおける暗号化されたペイロードに暗号アルゴリズムとして RFC 6379 の規定による AES-CBC-128、AES-CBC-256 及び [選択：RFC 5282 の規定による AES-GCM-128、AES-GCM-256、その他のアルゴリズムなし] を確実に用いなくてはならない（shall）。

保証アクティビティ：

TSS

評価者は、IKEv1 または IKEv2 あるいはその両方のペイロードの暗号化に用いられるアルゴリズムがTSS に特定されていること、及びアルゴリズム AES-CBC-128、AES-CBC-256 が指定されていること、さらに要件の選択においてその他が選択されている場合には、それらがTSS の論拠に含まれていることを確証しなくてはならない (shall)。

ガイダンス

評価者は、必須のアルゴリズム (要件において選択された追加アルゴリズムがあればそれについても) を使用するよう TOE を構成できる方法が操作ガイダンスに記述されていることを確証する。次にガイダンスを用いてTOE を構成し、下記のテストを実施する。

テスト

テスト 1：評価者は、IKEv1 または IKEv2 あるいはその両方のペイロードの暗号化に AES-CBC-128 を使用するようTOE を構成し、AES-CBC-128 を用いて暗号化されたペイロードのみを受け付けるように構成されたピアデバイスとの接続を確立しなくてはならない (shall)。評価者は、監査証跡を参照してこのアルゴリズムがネゴシエーションにおいて使用されたものであることを確認すること。

FCS_IPSEC_EXT.1.7 TSF は、IKEv1 フェーズ 1 交換ではメインモードのみを確実に用いなくてはならない (shall)。

保証アクティビティ：

TSS

評価者はTSS を調査して、TOE でサポートされている IPsec プロトコルの記述において、IKEv1 フェーズ 1 交換に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言明されていることを確証しなくてはならない (shall)。これは構成可能なオプションであってもよい。

ガイダンス

動作前にTOE のモードを構成する必要がある場合には、評価者は操作ガイダンスをチェックしてこの構成の指示がそのガイダンスに含まれていることを確証しなくてはならない (shall)。

テスト

テスト1 (条件付き)：評価者は操作ガイダンスの指示によりTOE を構成して、アグレッシブモードでIKEv1 フェーズ1 接続を使用して接続の確立を試行しなくてはならない (shall)。この試行は失敗するはずである (should)。評価者は次に、メインモードの交換がサポートされていることを示すべきである (should)。このテストは、IKEv1 が上記 FCS_IPSEC_EXT.1.5 プロトコル選択において選択されていない場合には適用されない。

FCS_IPSEC_EXT.1.8 TSF は、確実に [選択：IKEv2 SA ライフタイムを [選択：管理者、VPN ゲートウェイ] がパケット数／バイト数または経過時間に基づいて構成できるとともにフェーズ 1 SA については 24 時間かつフェーズ 2 SA については 8 時間にその値が制限でき、IKEv1 SA ライフタイムを [選択：管理者、VPN ゲートウェイ] がパケット数／バイト数または経過時間に基づいて構成できるとともにフェーズ 1 SA については 24 時間かつフェーズ 2 SA については 8 時間にその値が制限でき] なくてはならない (shall)。

適用上の注意：

ST 作成者は、自分の実装における IKE のバージョンに基づいて選択が与えられる。この選択の中にはさらに、どのエンティティがSA の寿命の「構成」を担当するかをST 作成者が規定できる選択が存在する。管理者がクライアントを構成できる実装や、VPN ゲートウェ

イがSA ライフタイムをクライアントにプッシュする実装は、両方とも受容可能である。

SA ライフタイムに関する限り、TOE は送信されたバイト数、または送信されたパケット数に基づいてライフタイムを制限できる。パケットベース、あるいはボリュームベースの SA ライフタイムはいずれも受容可能である。

保証アクティビティ：

TSS

ライフタイムの確立及び適用方法については RFC に記載されており、評価者はこのセクションの冒頭に述べたように TSS を調査する。

ガイダンス

評価者は、SA ライフタイムの値が構成可能であり、その指示が操作ガイダンス中に存在することを検証する。評価者は、管理者または VPN ゲートウェイのどちらかがフェーズ 1 SA の値を 24 時間、フェーズ 2 SA の値を 8 時間に設定できることを確証する。現時点ではパケット数またはバイト数に関して義務付けられている値は存在しないため、評価者はこれが構成できることのみを確証する。

テスト

このテストにあたって、評価者は双方が適切に構成されていることを確証する必要がある。RFC には以下のように記載されている。「IKEv1 と IKEv2 との違いは、IKEv1 SA のライフタイムがネゴシエーションされることである。IKEv2 においては、SA の両端が独自のライフタイム方針を SA に適用し、必要に応じて SA の鍵更新を行う責任がある。両端で異なるライフタイム方針が採用されている場合、その結果として、より短いライフタイムの側が常に鍵更新を要求することになるだろう。両端で同一のライフタイム方針が採用されている場合、同時に双方が鍵更新を開始することもあり得る (その結果、冗長な SA が生じる)。このようなことが起きる確率を減らすため、鍵更新要求のタイミングにはジッタを持たせるべきである (SHOULD)。」

下記のテストはそれぞれ、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のバージョンごとに実施されなくてはならない (shall)。

テスト 1：評価者は、操作ガイダンスにしたがって許容される最大のパケット数（またはバイト数）についてのライフタイムを構成しなくてはならない (shall)。評価者は SA を確立し、この SA の通過が許可されるパケット数 (またはバイト数) を超えた際に接続がクローズされることを判定しなくてはならない (shall)。

テスト 2：評価者は、フェーズ 1 SA が確立され、再ネゴシエーション前に 24 時間を超えて維持が試みられるようにテストを構築しなくてはならない (shall)。評価者は、24 時間以内にこの SA がクローズされるか、再ネゴシエーションされることを確認しなくてはならない (shall)。そのようなアクションのために TOE が特定の構成を必要とする場合には、評価者は TOE の構成機能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例証するテストを実施しなくてはならない (shall)。

テスト 3：評価者は、ライフタイムが 24 時間ではなく 8 時間であることを違いとして、テスト 1 と同様のテストをフェーズ 2 SA に対して実施しなくてはならない (shall)。

FCS_IPSEC_EXT.1.9 TSF は、IKE Diffie-Hellman 鍵交換に用いられる秘密の値 x (g^x mod p における「x」) を、FCS_RBG_EXT.1 に規定されるランダムビット生成器を用い、また少なくとも [割付：NIST SP 800-57, *Recommendation for Key Management – Part 1: General* の表 2 に掲げるネゴシエーション済み Diffie-Hellman グループに関連付けられた「等価安全性 (bits of security)」の値の少なくとも 2 倍のビット数 (1 つまたは複数)] のビット長を有するように生成しなくてはならない (shall)。

保証アクティビティ：

評価者は、TSF のサポートする DH グループのそれぞれについて、「x」(FCS_IPSEC_EXT.1.9 の定義による) 及び各ノンスを生成するプロセスが TSS に記載されていることをチェックし確証しなくてはならない (shall)。評価者は、本 PP 中の要件を満たす生成された乱数が使われること、及び「x」とノンスの長さが要件中の規定を満たすことが、TSS に示されていることを検証しなくてはならない (shall)。

FCS_IPSEC_EXT.1.10 TSF は、IKE 交換に用いられるノンスを、特定の IPsec SA の寿命内に特定のノンス値が繰り返される確率が 2^[割付：NIST SP 800-57, *Recommendation for Key Management – Part 1: General* の表 2 に掲げるネゴシエーション済み Diffie-Hellman グループに関連付けられた「等価安全性 (bits of security)」の値 (1 つまたは複数)] 分の 1 未満になるように生成しなくてはならない (shall)。

保証アクティビティ：

評価者は、TSF のサポートする DH グループのそれぞれについて、「x」(FCS_IPSEC_EXT.1.9 の定義による) 及び各ノンスを生成するプロセスが TSS に記載されていることをチェックし確証しなくてはならない (shall)。評価者は、本 PP 中の要件を満たす生成された乱数が使われること、及び「x」とノンスの長さが要件中の規定を満たすことが、TSS に示されていることを検証しなくてはならない (shall)。

FCS_IPSEC_EXT.1.11 TSF は、すべての IKE プロトコルに DH グループ 14 (2048 ビット MODP)、19 (256 ビットランダム ECP)、及び [選択：5 (1536 ビット MODP)、24 (2048 ビット MODP と 256 ビット POS)、20 (384 ビットランダム ECP)、[割付：TOE の実装するその他の DH グループ]、その他の DH グループなし] が実装されていることを確実にしなくてはならない (shall)。

保証アクティビティ：

評価者は、要件に規定される DH グループがサポートされているものとして TSS に列挙されていることをチェックし確証しなくてはならない (shall)。1 つよりも多くの DH グループがサポートされている場合、評価者は特定の DH グループをピアとの間で指定／ネゴシエーションする方法が TSS に記載されていることをチェックし確証する。評価者はまた、下記のテストを実施しなくてはならない (shall)。

テスト 1：サポートされている DH グループのそれぞれについて、評価者はその特定の DH グループを用いてすべての IKE プロトコルの完了が成功することをテストし確証しなくてはならない (shall)。

FCS_IPSEC_EXT.1.12 TSF は、すべての IKE プロトコルで RFC 4945 及び [選択：事前共有鍵、その他の手法なし] に準拠する X.509v3 証明書を用いる [選択、少なくとも 1 つを選択：*RSA*、*ECDSA*] を用いたピア認証が行われることを確実にしなくてはならない (shall)。

保証アクティビティ：

TOE が附属書 C に規定される X.509 証明書関連の機能 (例えば、保護された証明書ストア、または認証パス検証) を行う場合、これらの機能と関連付けられた要件は PP 本体中の FIA_X509_EXT.1 コンポーネントに配置され、また関連付けられた保証アクティビティは ST 作成者によってここに配置されることになる。

TSS

評価者は、RSA または ECDSA あるいはその両方がピア認証を行うために使われるものとして TSS に特定されていることを確証する。この記述は、FCS_COP.1(2) 暗号操作 (暗号署名) に規定されているアルゴリズムと一貫していなくてはならない (must)。

このセクションで事前共有鍵が選択されている場合、事前共有鍵が確立され IPsec 接続の

認証に用いられる方法がTSS に記述されていることを評価者はチェックして確証しなくてはならない (shall)。評価者は、事前共有鍵が生成されTOE に対して確立される方法が操作ガイダンスに記述されていることをチェックしなくてはならない (shall)。またTSS と操作ガイダンス中の記述には、事前共有鍵を生成できるTOE と、単純に事前共有鍵を利用するだけのTOE との両方について、事前共有鍵の確立が達成される方法が示されていなくてはならない (shall)。

ガイダンス

評価者は、暗号アルゴリズムとしてRSA またはECDSA あるいはその両方を使用するようにTOE を設定する方法が操作ガイダンスに記述されていることを確証する。

以下のテストのための環境を構築しTOE を構成するため、評価者は信頼できるCA へ接続するようにTOE を構成する方法も操作ガイダンスに記載されていることを確証し、またそのCA の有効な証明書がTOE にロードされ「信頼できる (trusted)」とマークされることを確証すること。

テスト

効率性の観点から、ここで実施するテストはFIA_X509_EXT.1 拡張 : X.509 証明書、具体的にはFIA_X509_EXT.1.4 及びFIA_X509_EXT.1.5 のテストの部分と組み合わせて行われる。下記のテストは、上記FCS_IPSEC_EXT.1.12 の選択において選択されたピア認証プロトコルのそれぞれについて繰返し行われなくてはならない (shall)。

テスト1 : 評価者はTOE に公開鍵―秘密鍵ペアを生成させ、署名してもらうためにCSR (証明書署名要求) をCA (TOE と、接続確立のために用いられるピアVPN の双方から信頼されている) へ送付させなくてはならない (shall)。DN（共通名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country) の値もまた、この要求の中で渡されることになる。

テスト2 : 評価者は、RSA またはECDSA アルゴリズムを用いて署名された証明書を用いて、IKE 交換中にリモートピアを認証しなくてはならない (shall)。このテストによってリモートピアが、TOE の証明書に署名した信頼できるCA の証明書を持っていることと、DN に関してビット単位の比較を行うことが確証される。このDN のビット単位の比較によって、ピアが信頼できるCA によって署名された証明書を持つことだけでなく、その証明書が期待されるDN からのものであることもまた確証される。評価者は、TOE を構成して証明書をVPN 接続と関連付ける (例えば、一部の実装では証明書マップ) ことになる。これが、DN のチェック対象となる。

テスト3 : 評価者は、CRL またはOCSP のどちらが選択されているかに応じて、TOE が失効した証明書を適切に処理できることをテストしなくてはならない (shall)。両方とも選択されている場合には、それぞれの手法についてテストが実施される。このEP のドラフトにおいては、評価者は信頼の連鎖の1 つ上位のみをテストする必要がある (将来のドラフトでは、上位の連鎖全体について検証を行って確証することが要求されるかもしれない)。評価者は、有効な証明書が用いられていること、そしてSA が確立されることを確証しなくてはならない (shall)。評価者は次に、失効することになる証明書 (選択において選択された手法のそれぞれについて) を用いてテストを試み、もはや証明書が有効ではない場合にはTOE がSA を確立しないことを確証する。

テスト4 : 評価者は、信用できるCA から署名された証明書について、DN がマッチしない場合 (4 つのフィールドのどれかを期待値とマッチしないように変更すればよい) には SA が確立されないことをテストしなくてはならない (shall)。

テスト5 : 評価者は、証明書有効性確認エンティティへの接続が到達不可能である場合にSA を確立するか、または確立しないかTOE を構成可能であることを確証しなくてはなら

ない (shall)。証明書有効性確認のために選択された手法のそれぞれについて、評価者は証明書の有効性確認を試行する。このテストにおいては、証明書が失効するかどうかは問題ではない。SA が確立を許可される「モード」では、接続が行われる。SA が確立されるべきでない場合には、接続は拒否される。

テスト 6 [条件付き]：評価者は、操作ガイダンスに示されるように事前共有鍵を生成して TOE と VPN GW ピアとの間の IPsec 接続を確立させなくてはならない (shall)。TOE が事前共有鍵の生成をサポートしている場合、鍵を生成する TOE のインスタンスだけではなく、単に鍵を受け取り利用するだけの TOE のインスタンスについても、鍵の確立が行われることを評価者は確証しなくてはならない (shall)。

FCS_IPSEC_EXT.1.13 TSF は、デフォルトで [選択 : *IKEv1 フェーズ 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強度 (鍵のビット数の意味で) が [選択 : *IKEv1 フェーズ 2*、*IIKEv2 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強度 (鍵のビット数の意味で) よりも大きいか、等しいことを確実にしなくてはならない (shall)。

保証アクティビティ：

TSS

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 (対称鍵のビット数の意味で) が TSS に記述されていることをチェックしなくてはならない (shall)。また TSS には、IKEv1 フェーズ 2 または IKEv2 CHILD_SA スイートあるいはその両方のネゴシエーション時に行われる、ネゴシエーションされたアルゴリズムの強度 (対称アルゴリズムにおける鍵のビット数の意味で) がネゴシエーションを保護する IKE SA の強度以下であることを確証するために行われるチェックについて記述されていなくてはならない (shall)。

ガイダンス

評価者は、単純にガイダンスにしたがって TOE を構成し、下記のテストを実施する。

テスト

テスト 1：このテストは、TOE のサポートする IKE の各バージョンについて実施されなくてはならない (shall)。評価者は、サポートされているアルゴリズムと要件中に特定されたハッシュ関数のそれぞれを用いて IPsec 接続のネゴシエーションを成功させなくてはならない (shall)。

テスト 2：このテストは、TOE のサポートする IKE の各バージョンについて実施されなくてはならない (shall)。評価者は、IKE SA に用いられているものよりも強度の大きい暗号化アルゴリズム (すなわち、IKE SA に用いられているものよりも大きい鍵サイズの対称アルゴリズム) を選択する ESP について SA の確立を試行しなくてはならない (shall)。そのような試行は失敗するはずである (should)。

テスト 3：このテストは、TOE のサポートする IKE の各バージョンについて実施されなくてはならない (shall)。評価者は、サポートされているアルゴリズム以外のアルゴリズムと要件中に特定されたハッシュ関数を用いて IKE SA の確立を試行しなくてはならない (shall)。そのような試行は失敗するはずである (should)。

テスト 4：このテストは、TOE のサポートする IKE の各バージョンについて実施されなくてはならない (shall)。評価者は、FCS_IPSEC_EXT.1.4 に特定されていない暗号化アルゴリズムを選択する ESP (適切なパラメタが IKE SA の確立に用いられると想定して) について SA の確立を試行しなくてはならない (shall)。そのような試行は失敗するはずである (should)。

適用上の注意：

55 *FCS_IPSEC_EXT.1.7* は、IKEv1 が選択されている場合にのみ適用される。

56 *FCS_IPSEC_EXT.1.8 : ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 中の選択によっては両方を) 選択する。IKEv1 要件は、正当な管理者に構成可能なライフタイムを提供すること (AGD_OPE によって強制される文書中の適切な指示と共に)、または制限を実装に「ハードコーディング」することの、いずれかの手段によって達成することができる。IKEv2 については、ハードコーディングされた制限は存在しないが、この場合には管理者が値を構成できることが必要とされる。一般的には、SA のライフタイムを含む実装のパラメタを設定するための指示が、AGD_OPE に関して作成された管理ガイダンス中に含まれるべきである (should)。TOE が同一の鍵によって保護されるトラフィック量 (その鍵によって保護されるすべての IPsec トラフィックの全体量) の制限を設定できるよう、パケット数の代わりに MB/KB 数によって要件を詳細化することは妥当である。また、SA のライフタイム管理及び強制が TOE 外部 (すなわち、VPN ゲートウェイ上で) 行われるように要件を詳細化することも妥当ではあるが、このように要件が詳細化された場合であっても、評価者は上記の関連付けられた保証アクティビティを実施しなくてはならない (shall)。*

57 *実装によっては、異なる Diffie-Hellman グループを SA の形成中に用いるようネゴシエーションすることが許可されているかもしれないため、FCS_IPSEC_EXT.1.9 と FCS_IPSEC_EXT.1.10 中の割付は複数の値を含むかもしれない。サポートされている DH グループのそれぞれについて、ST 作成者は 800-57 の表 2 を参照して、その DH グループに関連付けられる「等価安全性」を判定する。次に、それぞれ一意の値を用いて割付への記入が行われる (1.9 については倍の値を、1.10 については直接その値を割付へ記入する)。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートしている実装を想定してみよう。表 2 から、グループ 14 の等価安全性は 112 であり、グループ 20 については 192 である。したがって FCS_IPSEC_EXT.1.9 の割付は「[224, 384]」となり、FCS_IPSEC_EXT.1.10 の割付は「[112,192]」となるであろう (しかしこの場合には、数学的に意味のある値とするために、おそらく要件を詳細化すべきだろう (should))。*

58 *FCS_IPSEC_EXT.1.11 : この選択は、追加的にサポートされる DH グループを規定するために用いられる。これは、IKEv1 及び IKEv2 鍵交換に適用される。本 PP の将来のバージョンでは、DH グループ 20 (384 ビットランダム ECP) が必要とされることになる。何らかの追加的な DH グループが規定される場合、それは FCS_CKM.1 に掲げる要件に (確立される短期鍵の意味で) 適合しなくてはならないことに注意すべきである (should)。*

59 *FCS_IPSEC_EXT.1.12 : 適合 TOE には少なくとも 1 つの公開鍵ベースのピア認証手法が必要とされる。TOE による実装を反映して、1 つ以上の公開鍵方式が ST 作成者によって選択される。また ST 作成者は、用いられるアルゴリズム (及び、提供されている場合には鍵生成機能) を反映した適切な FCS 要件が列挙され、これらの手法がサポートされることも確証する。TSS には、これらのアルゴリズムが用いられる方法も詳述されることになる (例えば、2409 では公開鍵を用いる 3 つの認証手法が規定されており、TSS ではこれらのうちサポートされているものが記述されることになる) ことに注意されたい。*

60 *FCS_IPSEC_EXT.1.13 : ST 作成者は、TOE による実装に基づいて IKE に関する選択のいずれか、あるいは両方を選択する。もちろん、選択された IKE バージョンはこのエレメントだけでなく、このコンポーネント中の他のエレメントの他の選択とも一貫しているべきである (should)。TOE がこの機能を構成可能とすることは受容可能であるが、評価される構成中のデフォルト構成 (「箱から出した状態」または OPE 文書中の構成ガイダンスによる) では、この機能が有効になっていなくてはならない (must)。*

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、すべてのランダムビット生成 (RBG) サービスを [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)] を用いる NIST Special Publication 800-90； FIPS Pub 140-2 附属書 C； AES を用いる X9.31 附属書 2.4] にしたがい、[選択：1 つを選択：1 つ以上の独立したハードウェアベースの雑音源、1 つ以上の独立したソフトウェアベースの雑音源、ハードウェアベースとソフトウェベースの雑音源の組み合わせ] からエントロピーを蓄積するエントロピー源によってシードを供給して実施しなくてはならない (shall) 。

FCS_RBG_EXT.1.2 決定論的 RBG は、鍵とそれが生成する認可ファクタとの中で最も長いビット長と少なくとも等しい、最小で [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が供給されなくてはならない (shall)。

適用上の注意：

61 *NIST Special Pub 800-90 の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり、また本 PP の将来のバージョンでは必要とされることになる。*

62 *FCS_RBG_EXT.1.1 の最初の選択に関しては、ST 作成者は RBG サービスが適合する標準 (800-90 または 140-2 附属書 C のいずれか) を選択すべきである (should)。2 番目の選択については、ST 作成者はクライアントが RBG にエントロピーを収集する方法を示す。*

63 *SP 800-90 には、4 つの異なる乱数生成手法が含まれる。これらはそれぞれ、基盤とな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 作成者は利用される関数を選択し (800-90 が選択されている場合)、要件または TSS に用いられる具体的な基盤となる暗号プリミティブを取り込む。特定されたハッシュ関数 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) はいずれも Hash_DRBG または HMAC_DRBG に許可されるが、CT_DRBG には AES ベースの実装のみが許可される。800-90 に定義された任意の曲線が Dual_EC_DRBG に許可される一方で、ST 作成者は選択された曲線だけではなく、利用されるハッシュアルゴリズムも含めなくてはならない (must)。*

64 *FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に記述されている手法のみが有効であることに注意されたい。ここで用いられる AES 実装の鍵の長さが利用者データの暗号化に用いられるものと異なる場合には、異なる鍵の長さを反映するために FCS_COP.1 が調整されるか、繰り返される必要があるかもしれない。FCS_RBG_EXT.1.2 の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。*

65 *また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に含まれていることを確証する。*

66 *将来には、A Method for Entropy Source Testing: Requirements and Test Suite Description に記述される要件の大部分が本 PP によって要求されることになる。以下の保証アクティビティは、現在のところ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：

67 *評価者は TSS セクションをレビューして、TOE に用いられる RBG を含む製品のバージョン番号を判定しなくてはならない (shall)。また評価者は、エントロピーが収集される 1 つまたは複数の雑音源が TSS に記述されていることを確認しなくてはならない (shall)。さらに評価者は、RBG に用いられるすべての基盤となる機能とパラメタが、TSS に列挙されていることを検証する。*

68 *評価者は、RBG モデルの記述が TSS に含まれることを検証しなくてはならない (shall)。これには、エントロピー入力を取得する手法の他にも、利用されるエントロピー源の特定、各エントロピー源からエントロピーが生成／収集される方法、そして各エントロピー源によって作成されるエントロピーの量が含まれる。また評価者は、エントロピー源のヘルステスト、そのヘルステストによってエントロピーソースの健全性が判定できる理由の根拠、そしてエントロピー源の既知の故障モードが TSS に記述されていることも確証しなくてはならない (shall)。最後に評価者は、時間または環境条件あるいはその両方の変化と出力との独立性の観点から、RBG 出力の記述が TSS に含まれていることを確証しなくてはならない (shall)。*

69 *RBG がどの標準への適合を主張しているかに関わらず、評価者は以下のテストを行う。*

- *テスト 1：評価者は、エントロピー源テストスイート (Entropy Source Test Suite) を用いることによって、各エントロピー源のエントロピーの推定値を判定しなくてはならない (shall)。評価者は、全エントロピー源から得られたすべての結果の最小値であるエントロピーの推定値が TSS に含まれていることを確証しなくてはならない (shall)。*

70 *評価者は、RBG が準拠する標準にしたがって、以下のテストを行わなくてはならない (shall)。*

FIPS 140-2 の附属書 C に準拠する実装

71 *このセクションに含まれるテストの参照情報は、乱数生成検証システム (RNGVS) [RNGVS] である。評価者は、以下の 2 つのテストを実施しなくてはならない (shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装によって作成されたものであることに注意されたい。正しさの証明は、各スキームに任される。*

72 *評価者は、可変シードテストを行わなくてはならない (shall)。評価者は 128 セットの (Seed, DT) ペア (それぞれ 128 ビット) を TSF の RBG 機能に提供しなくてはならない (shall)。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなくてはならない (shall)。DT の値は、各セットについて 1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない (shall not)。評価者は、TSF によって返される値が期待値と一致することを確証する。*

73 *評価者は、モンテカルロテストを行わなくてはならない (shall)。このテストについては、評価者がシードの初期値及び DT の値 (それぞれ 128 ビット) を TSF の RBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなくてはならない (shall)。次に評価者は TSF の RBG を、繰返しのたびに DT の値を 1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms のセクション 3 に規定されるように次回の繰返しの際の新たなシードを作成して、10,000 回呼び出す。評価者は、作成された 10,000 番目の値が期待値と一致することを確証する。*

NIST Special Publication 800-90 に準拠する実装

74 *評価者は、RNG 実装の 15 回のトライアルを行わなくてはならない (shall)。RNG が構成可能な場合、評価者は各構成について 15 回のトライアルを行わなくてはならない (shall)。また評価者は、RNG 機能を構成するための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くてはならない (shall)。*

75 *RNG が有効な予測困難性を持つ場合、1 回のトライアルは (1) drbg をインスタンス化し、(2) ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順になる。評価者は、ランダムなビ*

ットの 2 番目のブロックが期待された値であることを検証する。評価者は、各トライアルに 8 つの入力値を生成しなくてはならない (shall)。最初はカウント (0～14) である。次の 3 つはエントロピー入力とノンス、そしてインスタンス化操作の個別化文字列である。次の 2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の 2 つは、2 番目の生成呼出しへの追加的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。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90 に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

76 *RNG が予測困難性を持たない場合、1 回のトライアルは (1) drbg をインスタンス化し、(2) ランダムなビットの最初のブロックを生成し、 (3) シードを再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各トライアルに 8 つの入力値を生成しなくてはならない (shall)。最初はカウント (0～14) である。次の 3 つはエントロピー入力とノンス、そしてインスタンス化操作の個別化文字列である。5 番目の値は、最初の生成呼出しへの追加的入力である。6 番目と 7 番目は、シードを再供給する呼出しへの追加的入力とエントロピー入力である。最後の値は、2 回目の生成呼出しへの追加的入力である。*

77 *以下のパラグラフには、評価者によって生成／選択されるべき入力値のいくつかについて、より多くの情報が含まれている。*

> ***エントロピー入力**：エントロピー入力値の長さは、シードの長さと等しくなくてはならない (must)。*
>
> ***ノンス**:ノンスがサポートされている場合 (df のない CTR_DRBG はノンスを利用しない)、ノンスのビット長はシードの長さの半分となる。*
>
> ***個別化文字列**:個別化文字列の長さは、シードの長さ以下でなくてはならない (must)。実装が 1 通りの個別化文字列の長さしかサポートしていない場合には、両方の値に同一の長さが使用できる。2 通り以上の文字列の長さがサポートされている場合、評価者は 2 つの異なる長さの個別化文字列を用いなくてはならない (shall)。実装が個別化文字列を用いない場合、値を供給する必要はない。*
>
> ***追加的入力**：追加的入力のビット長は、個別化文字列の長さと同一のデフォルトと制約を持つ。*

4.1.2 クラス：利用者データ保護 (FDP)

残存情報の保護 (FDP_RIP)

FDP_RIP.2	**十分な残存情報の保護**
FDP_RIP.2.1	TSF は、すべてのオブジェクト [選択: *へのリソースの割り当て、からのリソースの割り当て解除*] の際に、そのリソースのあらゆる以前の情報コンテンツが利用できなくなることを確実にしなくてはならない (shall)。

適用上の注意：

78 *この要件は、例えばプロトコルデータユニット (PDU) が、暗号鍵マテリアルのような残存情報によってパディングされないことを確実にするためのものである。ST 作成者は、選択を用いて以前の情報が利用できなくなる時点を規定する。*

保証アクティビティ：

79 *この要件の文脈における「リソース」とは、TOE を通して (TOE へセキュリティ管理者が接続する場合のように TOE「へ」ではなく) 送信されるネットワークパケットである。懸念点は、ネットワークパケットが送信された後でも、そのパケットによって利用されたバッファまたはメモリ領域にはいまだにそのパケットからのデータが含まれており、そしてそのバッファが再利用された場合にそれらのデータが残存していて新たなパケットに紛れ込むおそれがあるということである。評価者は、ネットワークパケットを処理する際にデータが再利用されることがないと判定できる程度にパケット処理が TSS に記述されていることをチェックして確証しなくてはならない (shall)。評価者は、この記述に少なくとも以前のデータがゼロ化／上書きされる方法と、バッファ処理のどの時点でこれが行われるかについて、記述されていることを確証しなくてはならない (shall)。*

4.1.3 クラス：識別と認証 (FIA)

80 TOE のベースライン要件は、形式的な管理者または汎用の利用者が定義されていないため、I&A に関してはかなり制約されたものになっている。TOE によって行われることが必要とされる I&A の範囲は、IPsec 接続を確立する際にマシンレベルで行われる認証に関係するものである。これらの I&A 要件は FCS_IPSEC_EXT.1 コンポーネントに規定されている。これは、IPsec プロトコルをグループにまとめるという要件を守ることによって、わかりやすさと共に保証アクティビティの作成と適用を容易にするためである。したがって、このセクションにおける要件は本 PP に規定されるプロトコルによって用いられる資格情報のみをカバーするものである。

81 附属書 C.1 に存在する **FIA_X509_EXT.1** コンポーネントに、2 つのエレメントが存在することは重要なので注意されたい。これらの 2 つのエレメントは、基盤となるオペレーティングシステムを利用して何らかのレベルの保護が提供されると想定される証明書の保護に関するもの、及び所与の証明書の有効性チェックに関するものである。VPN クライアントが有効性チェックを行うことは可能であり、その場合には要件 (FIA_X509_EXT.1.5) が PP 本体のこのセクションに移されることになるだろう。TOE がオペレーティングシステムに依存してこのチェックを行うこともあるかもしれず、この場合には要件は C.1 に残されて、環境によってチェックが行われ、結果が TOE へ提供されるという明確な指摘がなされることになる。

X509 証明書 (FIA_X509_EXT)

FIA_X509_EXT.1 拡張：X.509 証明書

FIA_X509_EXT.1.1 TSF は、RFC 5280 の定義による X.509v3 証明書を用いて、IPsec 接続の認証をサポートしなくてはならない (shall)。

適用上の注意：

82 *証明書有効性確認と認証パス検証の要件であって、この要件にしたがって TOE が実装しなくてはならないものが RFC 5280 に定義されていることに注意すべきである (should)。*

FIA_X509_EXT.1.3 TSF は、本 PP に規定されるセキュリティ機能によって使用される X.509v3 証明書を管理者が TOE へロードする機能を提供しなくてはならない (shall)。

FIA_X509_EXT.1.4 TSF は、RFC 2986 の規定による証明書要求メッセージを生成し、またその要求には以下の情報を提供できなくてはならない (shall)：公開鍵、共通名 (Common Name)、組織 (Organization)、組織単位 (Organizational Unit)、及び国 (Country)。

適用上の注意：

FIA_X509_EXT.1.4 に言及される公開鍵は、FCS_CKM.1(2) の規定により TOE が生成する

公開鍵—秘密鍵ペアの、公開鍵の部分である。

FIA_X509_EXT.1.8 TSF は、証明書または認証パスが無効と判断された場合、SA を確立してはならない (shall not)。

FIA_X509_EXT.1.9 TSF は、証明書に含まれる識別名 (DN) が接続の確立を試行しているエンティティに期待される DN にマッチしない場合、SA を確立してはならない (shall not)。

FIA_X509_EXT.1.10 TSF が証明書の有効性を判定する接続を確立できないとき、TSF は、管理者の選択により、SA を確立するか、または SA の確立を禁止しなくてはならない (shall)。

適用上の注意：

FIA_X509_EXT.1.8 の意図は、証明書有効性確認情報を提供する役割のエンティティに TOE が接続できない場合に、TOE にセッションの確立を許可するか禁止するか構成できるようにしておくことである。例えば、マシンがダウンしていたりネットワークパスが切断されていたりするために CRL が取得できない場合には、CA へ到達できないという理由で TOE が新たな SA を確立できなくしてしまうのではなく、引き続きセッションを確立できるように TOE を構成することを管理者は選択するかもしれない。

保証アクティビティ：

83 *評価者は管理ガイダンスをチェックして、TOE が X.509 証明書を使うように構成する方法が記述されていることを確証しなくてはならない (shall)。この記述には、TOE へ証明書をロードする方法、鍵を生成しその後 TOE そのものの証明書を取得するために CRM 要求を行う方法が含まれる。またこの記述では、ゲートウェイを認証するために用いられる証明書の有効性に関わる決定が行えない場合、TOE に SA の確立を許可するか、または許可しないかを構成する方法も、管理者に指示される。構成によっては、TOE が証明書の有効性情報を取得するために VPN ゲートウェイを介した接続を確立する必要があるかもしれない。*

評価者は TSS を調査して、要件を満たすように TOE が証明書を実装している方法が記述されていることを判定しなくてはならない (shall)。この記述には、どの側面が TOE によって行われ、またどれが運用環境に割り当てられるかが含まれる。

要件が満たされていることを確証するためのテストは、IPsec 要件 FCS_IPSEC_EXT.1.12 と組み合わせて行われる。

4.1.4 クラス：セキュリティ管理 (FMT)

84 本 PP のセクション 1 で示したように、TOE が別個の管理役割を維持管理することは求められていない。しかし、一般利用者の間では利用できるべきではない TOE 操作の特定の側面を構成する機能を提供することは求められている。TOE が何らかの程度の管理コントロールを提供する場合には、附属書 C からの適切な要件が ST に用いられるべきである (should)。

管理機能の仕様 (FMT_SMF)

FMT_SMF.1	**管理機能の仕様**
FMT_SMF.1.1	TSF は、下記の管理機能を行えなくてはならない (shall)。 • **IKE ネゴシエーション中に提案され受け入れられなくてはならないセキュリティアソシエーションの規定、** • **利用される IKE プロトコルバージョンの構成、** • **利用される IKE 認証テクニックの構成、**

- **確立されたセッション鍵の暗号有効期間の構成。暗号有効期間の構成に用いられる測定単位は、1 時間よりも大きくてはならない (shall not)、**
- **証明書失効チェックの構成、**
- **IPsec 交換中に提案され受け入れることのできるアルゴリズムスイートの規定、**
- **許可されている場合、ピアツーピア接続に用いられる認証手法の規定、**
- **TOE を更新する能力、及び更新を検証する能力、**
- **本 PP の他のセクションにおいて特定されるすべてのセキュリティ管理機能を構成する能力、**
- **[割付：任意の追加的な管理機能]。**

適用上の注意：

85 *設置については、VPN クライアントは IT 環境に依存して管理者をクライアントマシンへ認証する。*

86 *確立されたセッション鍵の暗号有効期間を構成する機能については、暗号有効期間の構成に用いられる測定単位は、時間よりも大きくてはならない (shall not)。例えば、秒、分、及び時間の測定単位は受容可能であり、日やそれよりも大きな測定単位は受容不可である。*

87 *VPN ゲートウェイが構成情報を VPN クライアントへ「プッシュ」するような例もあるかもしれない。これは管理の形態として受容可能であり、ST 作成者は ST 中に、どの管理機能が VPN クライアントに常駐するプラットフォーム上で行われるのか、そしてどれが VPN ゲートウェイによって行われるのかを単純に明示しなくてはならない (must)。機能が重複する (すなわち、プラットフォーム上のエンドユーザによって、あるいはゲートウェイによって行われることが可能な) 場合もあり得るが、ST が明確であってこの機能を行う方法がガイダンス文書に記述されている限り、これは問題ない。*

88 ***保証アクティビティ：***

89 *評価者は、PP によって必須とされるすべての管理機能が操作ガイダンスに記述されており、その記述にはその管理機能と関連付けられた管理職務を行うために必要とされる情報が含まれていることをチェックし確認しなくてはならない (shall)。評価者は、TOE を構成し上記の要件中に列挙されたすべてのオプションをテストすることによって、管理機能を提供する TOE の能力をテストしなくてはならない (shall)。*

90 *適用上の注意に言明されているように、TOE はプラットフォーム上でローカルに構成されてもよいし、あるいは VPN ゲートウェイからリモートに構成されてもよい。ST には、ローカル及びリモートに行える機能が明確に言明されること。ガイダンス文書には、これを行う方法も記述されること。評価者には、構成が管理できると ST 及びガイダンス文書に言明されているすべての方法で、この機能をテストすることが期待される。*

91 *ここでのテストは、FCS_IPSEC_EXT.1 などの他の要件のテストと組み合わせて実施されてもよいことに注意されたい。*

4.1.5 クラス：TSF の保護 (FPT)

拡張：TSF のセルフテスト (FPT_TST_EXT)

FPT_TST_EXT.1　　拡張：TSF のセルフテスト

FPT_TST_EXT.1.1　　TSF は、最初の起動中 (電源投入時) に一連のセルフテストを実行し、TSF の正しい動作を例証しなくてはならない (shall)。

FPT_TST_EXT.1.2　　TSF は、TSF の提供する暗号サービスを使用して、保存された TSF 実行可能形式コードが実行のためにロードされた際にその完全性を検証する機能を提供しなくてはならない (shall)。

適用上の注意：

TOE は典型的には IT 環境中で動作するソフトウェアパッケージであるが、それでも上記で求められるセルフテストアクティビティを行うことは可能である。しかし、上述のテストによって提供される保証の評定において、ホスト環境への多大な依存が存在する (ホスト環境が危殆化した場合にはセルフテストは意味をなさなくなることを意味する) ことは理解されるべきである (should)。

保証アクティビティ：

92　*評価者は TSS を調査して、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証しなくてはならない (shall)。この記述には、実際に行われるテストの概要 (例えば、「メモリがテストされる」と言うだけではなく、「各メモリロケーションに値を書き込み、それを読み出して書き込んだ値と同一であることを確証することによってメモリがテストされる」のような記述が用いられなくてはならない (shall)) が含まれるべきである (should)。評価者は、TSF が正しく動作していることをテストが十分に例証しているという論拠が TSS に示されていることを確証しなくてはならない (shall)。*

93　*評価者は TSS を調査して、保存された TSF 実行可能形式コードが実行のためにロードされた際にその完全性が検証される方法が記述されていることを確証しなくてはならない (shall)。評価者は、TSF 実行可能形式コードの完全性が危殆化されていないことをテストが十分に例証しているという論拠が TSS に示されていることを確証しなくてはならない (shall)。また評価者は、TSS (または操作ガイダンス) に成功した (例えば、ハッシュが検証された) 場合と不成功だった (例えば、ハッシュが検証されなかった) 場合に行われるアクションが記述されていることも検証する。評価者は、下記のテストを実施しなくてはならない (shall)。*

- *テスト 1：評価者は、既知の正当な TSF 実行可能形式に関する完全性チェックを行い、そのチェックが成功することを検証する。*
- *テスト 2：評価者は、TSF 実行可能形式を改変し、その改変された TSF 実行可能形式に関する完全性チェックを行い、その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、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能力を正当な管理者へ提供しなくてはならない (shall)。

FPT_TUD_EXT.1.2　　TSF は、TOE ソフトウェアの更新を開始する能力を正当な管理者へ提供しなくてはならない (shall)。

FPT_TUD_EXT.1.3　　TSF は、デジタル署名メカニズム及び [選択：公開ハッシュ、その他の機能なし] を用いて、TOE のファームウェア／ソフトウェア更新を、そのインストール前に検証する手段を提供しなく

てはならない (shall)。

適用上の注意：

94 *3 番目のエレメントにおいて参照されているデジタル署名メカニズムは、FCS_COP.1(2) に規定されているものである。参照されている公開ハッシュは、FCS_COP.1(3) に規定された関数のいずれかによって生成される。*

保証アクティビティ：

95 *TOE への更新は、正当なソースによって署名されると共にそれと関連付けられたハッシュを持つか、あるいは正当なソースによって署名される。デジタル署名が用いられる場合、更新検証メカニズムによって用いられる証明書がどのようにしてデバイスに含まれるかという記述とともに、正当なソースの定義が TSS 中に含まれる。評価者は、この情報が TSS に含まれることを確証する。また評価者は、更新候補が取得される方法、更新のデジタル署名の検証または更新のハッシュの計算に関連した処理、そして成功の (ハッシュまたは署名が検証された) 場合と不成功の (ハッシュまたは署名が検証できなかった) 場合に行われるアクションが、TSS (または操作ガイダンス) に記述されていることを確証する。評価者は、下記のテストを実施しなくてはならない (shall)。*

- *テスト 1：評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを判定する。評価者は、操作ガイダンスに記述されている手順を用いて本物の更新を取得し、その TOE へのインストールが成功することを検証する。その後、評価者はその他の保証アクティビティテストのサブセットを行い、更新が期待されたとおり機能していることを例証する。更新の後、評価者はバージョン検証アクティビティを再び行って、バージョンが更新のバージョンと正しく対応していることを検証する。*
- *テスト 2：評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを判定する。評価者は、偽物の更新を取得または作成し、TOE へそれをインストールしようと試みる。評価者は、TOE がその更新を拒否することを検証する。*

4.1.6 クラス：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、**IPsec を用いて**、それ自身と **VPN ゲートウェイ**との間の**高信頼**通信チャネルであって、他の通信チャネルとは論理的に別個であり、そのエンドポイントの保証された識別とチャネルデータの**開示からの**保護**ならびにチャネルデータの改変の検出**を提供するものを提供しなくてはならない (shall)。
FTP_ITC.1.2	TSF は、*その* TSF の高信頼チャネルを介した通信の開始を許可しなくてはならない (shall)。
FTP_ ITC.1.3	TSF は、*その接続を通過するすべてのトラフィックについて*、高信頼チャネルを介した通信を開始しなくてはならない (shall)。

適用上の注意：

96 *上記の要件の意図は、要件中に特定された暗号プロトコルを利用して TOE と VPN ゲートウェイとの間の通信が保護されることである。TOE と VPN ゲートウェイの両方が、プロトコルの意味でのピアとして動作する。*

97 *この要件は、通信が当初確立された際だけではなく、中断後の再開に関しても保護されることを意味している。TOE 設定の一部として他の通信を保護するためにトンネルを手作業で設定することが必要とされる場合があったとして、そして中断後に TOE が (必要とされる) 人手での介入と共に自動的に通信を再確立しようと試みる場合、攻撃者が重要な情報を得たり接続を危殆化できたりするウィンドウが形成されるかもしれない。*

保証アクティビティ：

98 *評価者は TSS を調査して、仕様に反映されていないかもしれない TOE 特有のオプションまたは手続きと共に、要件に規定された暗号プロトコルの観点から TOE のアクセスポイントへの接続の詳細が記述されていることを判定しなくてはならない (shall)。また評価者は、TSS に列挙されたすべてのプロトコルが規定され ST 中の要件に含まれていることを確認しなくてはならない (shall)。評価者は、アクセスポイントへの接続を確立するための指示が操作ガイダンスに含まれていることと、万一接続が意図せず切断されてしまった際の回復の指示が含まれていることを確認しなくてはならない (shall)。評価者はまた、下記のテストを実施しなくてはならない (shall)。*

- *テスト 1：評価者は、操作ガイダンス中の記述により接続を設定し通信が成功することを確証することによって、TOE が要件中に規定されたプロトコルを用いて VPN ゲートウェイとの通信を開始できることを確証しなくてはならない (shall)。*
- *テスト 2：評価者は、VPN ゲートウェイとの通信チャネル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証しなくてはならない (shall)。*
- *テスト 3：評価者は、VPN ゲートウェイとの通信チャネルのそれぞれについて、チャネルデータの改変が TOE によって検出されることを確証しなくてはならない (shall)。*
- *テスト 4：評価者は、TOE から VPN ゲートウェイへの接続を物理的に中断しなくてはならない (shall)。評価者は少なくとも、接続を自動的に再開しようとする、または新たなアクセスポイントへ接続しようとするあらゆる試行の場合において、それ以降の通信が適切に保護されることを確証しなくてはならない (shall)。*

99 *これ以外の保証アクティビティは、特定のプロトコルと関連付けられる。*

4.2 セキュリティ機能要件の根拠

100 このセクションでは、セクション 4.1 で定義される TOE セキュリティ機能要件の根拠を記述する。表 10 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付けを、その対策方針が要件によって対処されるという根拠と共に示す。

101 ベンダによって提供されるセキュリティターゲット (ST) にも、以下の 2 つおセクションからなるセキュリティ要件の根拠が含まれている。

- どの SFR がどの TOE のセキュリティ対策方針に対処するかを示す追跡と、
- TOE のすべてのセキュリティ対策方針が効果的に SFR によって対処されていることを示す一連の正当化。 (CC パート 1、セクション B7 による)。

表 9：TOE セキュリティ機能要件の根拠

対策方針	対策方針へ対処する要件	根拠
O.AUTH_COMM	FCS_CKM.1	FTP_ITC.1 (及びそれをサポートする要件 FCS_CKM.1、FCS_COP.1(1)、

TOE は、TOE であるふりをした別のエンティティと利用者が通信していないことを確実にするとともに、TOE が正当な IT エンティティのふりをしている別のエンティティではなく正当な IT エンティティと通信を行っていることを確実にする手段を提供する。	FCS_COP.1(1) FCS_COP.1(2) FCS_IPSEC_EXT.1 FIA_PSK_EXT.1 FIA_X509_EXT.1 FTP_ITC.1	FCS_COP.1(2)、FCS_IPSEC_EXT.1、FIA_PSK_EXT.1、及び FIA_X509_EXT.1) は、TOE とリモート管理者及び高信頼 IT エンティティの両方との間に別個の通信チャネルを作成するメカニズムであって、このチャネルを通過するデータは開示または改変から保護されるものを TOE が提供することを要求する。これは、要件によって規定されるプロトコルを用いて暗号学的に行われる。これらのプロトコルは確実なエンドポイントの相互識別とチャネルデータの保護を提供する。
O.CRYPTOGRAPHIC_FUNCTIONS TOE は、暗号機能（すなわち、暗号化／復号及びデジタル署名操作）を提供することによって機密性を維持し、また TOE 及びそのホスト環境の外部へ送信されるデータの改変を検出することを可能としなくてはならない (shall)。	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。この鍵は、IPSEC の短期鍵生成に用いられ、またその他の公開鍵ベースの鍵合意方式に用いられる可能性もある。 FCS_CKM_EXT.4 は、鍵及び鍵マテリアルを確実にゼロ化する機能を提供する。多くの場合 TOE はホスト上で動作するソフトウェアエンティティとなるため、この要件の範囲はそのソフトウェアがデータをクリアする適切な機能を呼び出すことを確実にすることである。データがクリアされたことを確実にする責任は、最終的にホストが負うことになる。 FCS_COP.1(1) は、本 PP に規定されるさまざまなプロトコルの暗号化及び復号操作を行うために、AES が用いられることを規定している。 FCS_COP.1(2) は、高信頼更新及びトラフィックを保護するために用いられるプロトコルと関連した証明書の操作を行うために、TOE にデジタル署名機能が実装されることを要求している。 FCS_COP.1(3) 及び FCS_COP.1(4) は、データ完全性の検証及び非データ完全性操作を行うために、Secure Hash Algorithm アルゴリズムの実装を用いたハッシュサービスを TSF が提供することを要求している。 FIA_X509_EXT.1 は、先に述べた暗号操作の多くをサポートするために用いられる証明書が、適切な標準に準拠することを要求している。

		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している。
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試みるすべてのピア TOE を認証する。	FCS_IPSEC_EXT.1	FCS_IPSEC_EXT.1 は、IKE プロトコルを用いた IPsec を TOE が実装しなくてはならない (must) と規定している。このプロトコルを実装することによって、TOE はセキュリティアソシエーションの確立を目的として、セキュアで認証されたチャネルを各ピア TOE との間で確立することになる。これには、すべての通信に用いられる暗号鍵とアルゴリズム、そしてモードの確立が含まれる。2 つのピア TOE 間で、それぞれ独自の暗号鍵を用いる、複数のセキュリティアソシエーションを確立することも可能である。認証は、デジタル署名によって、またオプションとして事前共有鍵によって行うこともできる。
O.PROTOCOLS TOE は、相互運用性を確実にするために、RFC または業界規格あるいはその両方に準拠した標準化されたプロトコルが TOE に実装されていることを確実にする。	FCS_IPSEC_EXT.1 FTP_ITC.1	FCS_IPSEC_EXT.1 と FTP_ITC.1 は、実装を要求するプロトコルに適用される標準を参照して (そしてこれらの標準に何らかの制限があればそれを示して) いる。
O.RESIDUAL_INFORMATION_CLEARING TOE は、保護されたリソースに含まれるいかなるデータも、そのリソースが再割り当てされた際に利用できないことを確実にする。	FCS_CKM_EXT.4 FDP_RIP.2	FCS_CKM_EXT.4 は、任意の暗号鍵がもはや必要なくなった際に破壊されることを確実にしている。 FDP_RIP.2 は、リソースの内容がそのデータへのアクセスを明示的に許可されたもの以外のサブジェクトへ利用できないことを確実にするために用いられている。この TOE に関しては、ネットワークパケットを構築するために用いられるメモリがクリアされるか、またはパケットの内容がその後のパケット中で開示されてしまうことを防止するような (例えば、パケットの構築にパディングが用いられる場合、それには別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何らかのバッファ管理方式が採用されることが必須である。
O.SYSTEM_MONITORING TOE は、監査データを生成する機能を提供すること。	FAU_GEN.1 FAU_SEL.1	FAU_GEN.1 は TOE が記録できなくてはならない事象のセットを定義する一方で、FAU_SEL.1 は管理証跡にどの管理対象事象が記録されることになるのかを管理者が構成できるようにしている。

O.TOE_ADMINISTRATION TOE は、管理者が TOE を構成できるメカニズムを提供する。	FAU_SEL.1 FMT_SMF.1	FAU_SEL.1 は記録されるべき監査対象事象を構成する能力を要求している一方で、FMT_SMF.1 は TOE の別の部分についての構成要件を提供している。概論で述べたように、TOE が管理的役割を提供することは要求されていないが、TOE と IT 環境との組み合わせにおいては、ホストマシンの一般利用者のサブセットへこれらの機能を制約できなくてはならない (must)。
O.TSF_SELF_TEST TOE は、TOE が適切に動作していることを確実にするため、TOE のセキュリティ機能の何らか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 の正しい動作を確約するための一連のセルフテストを提供すること、そして保存された実行可能形式の完全性の問題を検出することを TOE に要求している。
O.VERIFIABLE_UPDATES TOE は、TOE へのいかなる更新も改変されておらず、また (オプションとして) 信頼されたソースからのものであることが管理者によって検証できることを確実に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) と FCS_COP.1(3) は、更新の検証に用いられるデジタル署名アルゴリズムとハッシュ関数を規定している。 FPT_TUD_EXT.1 は、実行されているファームウェアのバージョンを判定し、更新を開始し、そしてインストール前に TOE へのファームウェア／ソフトウェア更新を検証する方法を提供している。

4.3 セキュリティ保証要件

102 セクション 3.1 中の TOE に関するセキュリティ対策方針は、セクション 2.1 中に特定された脅威とセクション 2.2 中に引用された組織のセキュリティ方針へ対処するために構築された。セクション 4.1 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実体化である。

103 セクション 4 の概論に示したように、このセクションには CC からの SAR の完全なセットが含まれている一方で、評価者によって行われるべき保証アクティビティはこのセクションと共にセクション 4.1 にも記述されている。

104 それぞれのファミリについて、「開発者への注意」が開発者アクションエレメントについて提供され、（もしあれば）開発者によって提供される必要のある追加的文書／アクティビティを説明している。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加的アクティビティ (セクション 4.1 にすでに含まれているものに加えて) が記述されている。さらに、このセクションに記述された保証アクティビティは、セクション 4.1 に規定されたものとは相補的な関係にある。

105 表 11 に要約される TOE セキュリティ保証要件は、本 PP のセクション 2 に特定される脅威と方針へ対処するために必要とされる管理及び保証アクティビティを特定している。セクション 4.4 には、本 PP についてこの保証要件のセットを選択したことについての簡潔な正当化が提供される。

表 10：TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネントの記述
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	利用者準備ガイダンス
試験	ATE_IND.1	独立テスト—適合
脆弱性の評定	AVA_VAN.1	脆弱性分析
ライフサイクルサポート	ALC_CMC.1	TOE のラベリング
	ALC_CMS.1	TOE CM カバレージ

4.3.1 ADV クラス：開発

106 本 PP に適合する TOE については、TOE に関する情報は ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれている。TOE 開発者が TSS を作成することは要求されてはいないが、TOE 開発者は TSS に含まれている製品の記述を、機能仕様に関して一致させなくてはならない (must)。セクション 4.1 に含まれる保証アクティビティは、TSS セクションにふさわしい内容を判定する上で ST 作成者に十分な情報を提供すべきである (should)。

4.3.1.1 ADV_FSP.1 基本機能仕様

107 機能仕様は、TOE のセキュリティ機能インタフェース (TSFI) を記述するものである。これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者 (管理ユーザを含む) によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、そのようなインタフェースそれ自体を規定することにはあまり意味がない。そのようなインタフェースは間接的なテストしかできないためである。本 PP のこのファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示されるインタフェースと、AGD 文書に提示されるインタフェースのの理解に焦点を絞るべきである (should)。規定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とされるべきではない (should not)。

108 TOE へのインタフェースを理解するにあたって、対抗されるべき脅威がネットワークを介して (TOE のピアツーピア接続、または TOE から VPN ゲートウェイへの接続のいずれかによって) 送信される利用者データの機密性及び完全性であるとともに、この接続を通過する可能性のあるデータの認証でもあることを考慮することは重要である。さらに、TOE はその構成にもよるが、TOE 背後のネットワークへの不正なアクセスへの保護を提供してもよい。これらのネットワークインタフェースに加えて、管理インタフェース (TOE を構成する方法) も記述される必要がある。

109 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としてではなく、列挙された保証アクティビティを行うために必要な情報を通して特徴づけされる。

開発者の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くてはならない (shall)。

ADV_FSP.1.2D　開発者は、機能仕様から SFR への追跡を提供しなくてはならない (shall)。

開発者への注意：　このセクションの概論で述べたように、機能仕様は AGD_OPR 及び AGD_PRE 文書に含まれる情報と、ST の TSS に提供される情報との組み合わせで構成されている。機能仕様中の保証アクティビティは、文書及び TSS セクションに存在すべき証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容及び提示エレメント：

ADV_FSP.1.1C　機能仕様には、SFR を強制する、及び SFR をサポートする TSFI のそれぞれについて、使用の目的と手法が記述されなくてはならない (shall)。

ADV_FSP.1.2C　機能仕様には、SFR を強制する、及び SFR をサポートする TSFI のそれぞれについて、関連するすべてのパラメタが特定されなくてはならない (shall)。

ADV_FSP.1.3C　機能仕様には、SFR 非干渉と暗黙に分類されているインタフェースについて、その根拠が提供されなくてはならない (shall)。

ADV_FSP.1.4C　追跡は、機能仕様における SFR から TSFI への追跡を例証するものでなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)。*

ADV_ FSP.1.2E　評価者は、機能仕様が SFR の正確かつ完全な実体化であることを判定しなくてはならない (shall)。

保証アクティビティ：

110　*これらの SAR に関連付けられた具体的な保証アクティビティは存在しない。機能仕様文書はセクション 4.1 に記述された評価アクティビティと、AGD、ATE、及び AVA SAR に関して記述されたその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。機能仕様情報の内容についての要件は、行われるその他の保証アクティビティの特質により暗黙に評定される。不十分なインタフェース情報しか存在しなかったために評価者がアクティビティを行うことができなかった場合には、十分な機能仕様が提供されていなかったことになる。*

4.3.2 AGD クラス：ガイダンス文書

111　ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、管理モデルの記述と、運用環境 (VPN クライアントを収容するシステム) がそれ自身のセキュリティ機能の役割を満たすことを管理者が検証する方法の記述が含まれなくてはならない (must)。この文書は、管理者によって読解可能な非形式的なスタイルであるべきである (should)。

112　製品がサポートすると ST で主張されているすべての運用環境についてガイダンスが提供

されなくてはならない (must)。このガイダンスには、以下が含まれる。

- その環境への TOE のインストールを成功させるための指示、及び
- 製品として、またより大規模な運用環境のコンポーネントとして、TOE のセキュリティを管理するための指示、及び
- TOE の機能、環境の機能、あるいはこれら 2 つの組み合わせのいずれかを用いることによって保護された管理機能を提供するための指示。

113 また、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。そのようなガイダンスに関する要件は、セクション 4.1 に規定された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

開発者の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くてはならない (shall)。

開発者への注意： ここで繰返し情報を提示するのではなく、開発者はこのコンポーネントに関する保証アクティビティをレビューして、評価者がチェックすることになるガイダンスの詳細を確認すべきである (should)。これによって、受容可能なガイドラインの作成に必要な情報が提供されることになる。

内容及び提示エレメント：

AGD_OPE.1.1C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用者にアクセス可能な機能及び特権であってセキュアな処理環境において制御されるべきものが、適切な警告を含めて記述されなくてはならない (shall)。

AGD_OPE.1.2C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、TOE によって提供される利用可能なインタフェースをセキュアな方法で利用する方法が記述されなくてはならない (shall)。

AGD_OPE.1.3C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用可能な機能及びインタフェース、特に利用者の制御下にあるすべてのセキュリティパラメタが、該当する場合にはセキュアな値を示しつつ、記述されなくてはならない (shall)。

AGD_OPE.1.4C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用者にアクセス可能な機能であって、TSF の制御下でエンティティのセキュリティ的な特徴の変更を含めて、実行される必要のあるものに関連するセキュリティ関連事象のすべての種類が明示されなくてはならない (shall)。

AGD_OPE.1.5C 利用者操作ガイダンスには、TOE のすべてのあり得る運用モード (故障または操作エラー後の運用を含めて) と、その結果及びセキュアな運用を維持することへの影響が特定されなくてはならない (shall)。

AGD_OPE.1.6C 利用者操作ガイダンスには、利用者の役割のそれぞれについて、ST に記述される運用環境に関するセキュリティ対策方針を達成するために遵守されるべきセキュリティ対策が記述されなくてはならない (shall)。

AGD_OPE.1.7C　利用者操作ガイダンスは、明確かつ妥当なものでなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)*。

保証アクティビティ：

114 *運用中、ガイダンスに記述されるべきアクティビティは大きく 2 つに分類される。一方は (管理者ではない) 利用者によって行われるもの、他方は管理者によって行われるものである。非管理ユーザに必要とされる大部分の手続きは、セクション 4.1 の保証アクティビティ中で参照されていることに注意すべきである (should)。*

115 *管理機能に関しては、いくつかはすでにセクション 4.1 に述べたが、追加的情報が以下のように必要とされる。*

116 *操作ガイダンスには、少なくとも TOE の評価される構成上で実行されている (または実行可能な) プロセスであって、ネットワークインタフェース上で受信したデータの処理が可能であるもの (このようなものは 2 つ以上存在する可能性があり、またそのネットワークインタフェース上で「リッスン」するプロセスには限定されない) が列挙されなくてはならない (shall)。ネットワークデータを処理するものだけを判定しようと試みるのではなく、TOE の評価される構成上で実行されている (または実行可能な) すべてのプロセスを列挙することは受容可能である。列挙されたプロセスのそれぞれについて、管理ガイダンスにはそのプロセスの機能とそのサービスが実行される特権の短い (例えば、1 行か 2 行の) 記述が含まれることになる。「特権」には、ハードウェアの特権レベル (例えば、リング 0 やリング 1)、そのプロセスと特に関連付けられた任意のソフトウェア特権、及びそのプロセスがその代理として、またはその支配下で動作する利用者の役割と関連付けられた特権が含まれる。*

117 *操作ガイダンスには、TOE の評価される構成と関連付けられた暗号エンジンを構成するための指示が含まれなくてはならない (shall)。TOE の CC 評価の中で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、管理者へ与えられなくてはならない (shall)。*

118 *文書には、ハッシュのチェックまたはデジタル署名の検証のいずれかによって、TOE への更新を検証するためのプロセスが記述されなくてはならない (must)。評価者は、このプロセスに以下の手順が含まれることを検証しなくてはならない (shall)。*

- *ハッシュについては、所与の更新についてのハッシュがどこで取得できるかという記述。デジタル署名については、署名された更新が証明書の所有者から受信されていることを確証するために、FCS_COP.1(2) メカニズムによって用いられる証明書を取得するための指示。これは、製品と共に最初から供給されていてもよいし、何らかの別の手段によって取得されてもよい。*
- *更新そのものを取得するための指示。これには、更新をアクセス可能とするための指示 (例えば、特定のディレクトリへの格納) が含まれるべきである (should)。*
- *更新プロセスを開始するための、そしてそのプロセスが成功したか失敗したかを判別するための指示。これには、ハッシュ／デジタル署名の生成が含まれる。*

4.3.2.2 GD_PRE.1 準備手続き

開発者のアクションエレメント：

AGD_PRE.1.1D　開発者は、TOE の準備手続きを含めて TOE を提供しなくてはならない (shall)。

開発者への注意：　操作ガイダンスと同様に、開発者は保証アクティビティを見た上で準備手続きに関して必要とされる内容を判定すべきである (should)。

内容及び提示エレメント：

AGD_ PRE.1.1C　準備手続きには、開発者の配付手続きにしたがって配付された TOE をセキュアに受領するために必要なすべての手順が記述されなくてはならない (shall)。

AGD_ PRE.1.2C　準備手続きには、TOE のセキュアな設置に必要なすべての手順と、ST に記述された運用環境のセキュリティ対策方針にしたがった運用環境のセキュアな準備に必要なすべての手順が記述されなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)。*

AGD_ PRE.1.2E　評価者は、TOE が運用のためにセキュアに準備できることを確認するために、準備手続きを*適用しなくてはならない (shall)。*

保証アクティビティ：

119　*保証アクティビティ：上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の構成にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST 中に TOE について主張されているすべてのプラットフォーム及びコンポーネント (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み合わせ) へ十分に対応していることをチェックして確証しなくてはならない (shall)。*

120　*評価者は、以下のガイダンスが提供されていることをチェックして確証しなくてはならない (shall)。*

- *概論マテリアルに示したように、TOE の管理は TOE の全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 プラス運用環境) がこの機能を提供することが事実でなくてはならないが、その機能を実装する責任は、完全に運用環境の責任から、完全に TOE の責任まで変動する可能性がある。高レベルにおいては、ガイダンスには運用環境が責任を持つ機能の部分を提供できるように運用環境を構成するための適切な指示が含まれていなくてはならない (must)。利用者全体から管理ユーザを分離するためのメカニズムを TOE が提供しない場合には、例えば、OS の I&A メカニズムが一意の (OS ベースの) 利用者の識別を提供するような OS の構成をカバーするような指示と、1 つまたは複数の TOE 管理識別情報を用いた OS の DAC メカニズムの構成を設置者に指示するようなさらなるガイダンスとが与えられ、TOE 管理者のみが管理用実行可能形式へアクセスできるようにする。TOE がこの機能の一部または全部を提供する場合には、適切な要件が附属書 C から ST へ取り込まれ、これらの要件と関連付けられた保証アクティビティが TOE と運用環境の両方に必要とされるガイダンスの詳細を提供する。*

また評価者は、下記のテストを実施しなくてはならない (shall)。

- *テスト 1 [条件付き]：すべての TOE 利用者からの管理ユーザの分離が運用環境の構成を通してのみ行われる場合、評価者は、ST 中に主張されるすべての構成について、管理ガイダンスにしたがってシステムを構成した後には管理者でないユーザが TOE の管理機能へアクセスできないことを確証する。*

4.3.3 ATE クラス：テスト

121 テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について規定される。前者は ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 PP に規定された保証レベルにおいては、テストは設計情報の利用可能性に依存した、通知された機能及びインタフェースに基づいて行われる。評価プロセスの主要なアウトプットのひとつは、以下の要件に規定されるテスト報告である。

4.3.3.1 ATE_IND.1 独立テスト—適合

122 テストは、TSS に記述された機能と、提供された管理 (構成及び操作を含む) 文書を確認するために行われる。テストで重視されるのは、セクション 4.1 に規定された要件が満たされていることの確認であるが、いくつかの追加的テストがセクション 4.3 中の SAR について規定されている。保証アクティビティは、これらのコンポーネントと関連付けられた最小テストアクティビティを特定する。評価者は、テストの計画及び結果、ならびに本 PP への適合を主張するプラットフォーム／TOE に絞られたカバレージの論拠を文書化した、テスト報告を作成する。

開発者のアクションエレメント：

ATE_IND.1.1D 開発者は、テストに用いられる TOE を提供しなくてはならない (shall)。

内容及び提示エレメント：

ATE_IND.1.1C TOE は、テストに適当なものでなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)。*

ATE_IND.1.2E 評価者は、TSF が規定されたように動作していることを確認するために TSF のサブセットを*テストしなくてはならない (shall)。*

保証アクティビティ：

123 *評価者は、システムのテストの側面を文書化したテスト計画とテスト報告を作成しなくてはならない (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中に列挙されたテストのそれぞれについて 1 つのテストケースを用意する必要はないが、ST 中の該当するテスト要件のそれぞれがカバーされていることを評価者はテスト計画中に文書化しなくてはならない (must)。*

124 *テスト計画にはテストされるプラットフォームが特定され、そしてテスト計画には含まれていないが ST に含まれているプラットフォームについては、そのプラットフォームをテストしないことについての正当化をテスト計画が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われようとしているテストにその違いが影響しないという論拠が示されなくてはならない (must)。単にその違いが影響しないと主張するだけでは十分ではない。根拠が提供されなくてはなら*

ない (must)。ST 中のすべてのプラットフォームがテストされる場合には、根拠は必要とされない。

125 *テスト計画にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。テストの一部としての、または標準的なテスト前の条件としての、各プラットフォームの設置及び設定について、評価者が AGD 文書にしたがうことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の性能に悪影響を与えないという、(単なる主張ではなく) 論拠が提供される。*

126 *テスト計画には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も特定される。これらの手順には、期待される結果も含まれる。テスト報告 (テスト計画へ単に注釈を加えたものであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなくてはならず、したがって失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。*

4.3.4 AVA クラス：脆弱性評定

127 本プロテクションプロファイルの第一世代については、オープンソースの調査を行って、これらの種類の製品にどのような脆弱性が発見されているのかを見出すことが評価ラボに期待される。多くの場合、これらの脆弱性には基本的な攻撃者を超える巧妙さが必要とされる。ペネトレーションツールが作成されて評価ラボへあまねく配付されるまでは、評価者はこれらの脆弱性のテストを TOE で行うことが期待できないことになる。ラボには、ベンダによって提供された文書を考慮して、これらの脆弱性の存在する可能性についてコメントすることが期待される。この情報はペネトレーションテストツールの開発と、将来のプロテクションプロファイルの開発に用いられることになる。

4.3.4.1 AVA_VAN.1 脆弱性調査

開発者のアクションエレメント：

AVA_VAN.1.1D 開発者は、テストに用いられる TOE を提供しなくてはならない (shall)。

内容及び提示エレメント：

AVA_VAN.1.1C TOE は、テストに適当なものでなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)。*

AVA_VAN.1.2E 評価者は、TOE 中に潜在する脆弱性を特定するために、パブリックドメインソースの検索を*行わなくてはならない (shall)。*

AVA_VAN.1.3E 評価者は、基本的な攻撃能力を有する攻撃者によって行われる攻撃に TOE が耐えられることを判定するために、特定された潜在する脆弱性に基づいて、ペネトレーションテストを*実施しなくてはならない (shall)。*

保証アクティビティ：

128 *ATE_IND と同様に、評価者は報告を作成し、この要件に関連する自分たちの結論を文書化しなくてはならない (shall)。この報告は、物理的には ATE_IND に言及される全体的なテスト報告の一部であってもよいし、あるいは別個の文書であってもよい。評価者は、公開された情報の検索を行って、一般的な VPN クライアント製品に発見された脆弱性と、特定の TOE に関する脆弱性を特定する。評価者は、参考としたソースと発見された脆弱性を報告中に文書化する。発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、あるいはそのほうが適切であれば脆弱性を確認するためのテストを策定するか (ATE_IND に提供されるガイドラインを用いて) のどちらかを行う。適切かどうかは、その脆弱性を利用するために必要とされる攻撃ベクトルの評定によって判定される。例えば、ブート時にあるキーの組み合わせを押すことによって脆弱性が検出できる場合、本 PP の保証レベルにおいてはテストが適当と思われる。例えば、脆弱性の悪用に電子顕微鏡と液体窒素のタンクが必要とされる場合には、テストは適当ではなく、適切な根拠が策定される。*

4.3.5 ALC クラス：ライフサイクルサポート

129 本 PP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの調査ではなく、ライフサイクルのエンドユーザに可視の側面に限定される。これは、製品の全体的な信頼度の向上において開発者の手腕が果たす重要な役割を減じようとするものではない。そうではなく、この保証レベルにおける評価に関して利用可能とされるべき情報を反映したものなのである。

4.3.5.1 ALC_CMC.1 TOE のラベル付け

130 このコンポーネントは、TOE を同一ベンダの他の製品またはバージョンから区別でき、またエンドユーザによって調達される際に容易に指定できるように、TOE を識別することを目標としている。

開発者のアクションエレメント：

ALC_CMC.1.1D 開発者は、TOE 及び TOE への参照情報を提供しなくてはならない (shall)。

内容及び提示エレメント：

ALC_CMC.1.1C TOE は、その一意の参照情報によってラベル付けされなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)*。

保証アクティビティ：

131 *評価者は ST をチェックして、ST の要件を満たすバージョンを具体的に特定する識別情報 (製品名／バージョン番号など) が含まれていることを確証しなくてはならない (shall)。さらに、評価者は AGD ガイダンス及びテスト用に受け取った TOE サンプルをチェックして、バージョン番号が ST 中のものと一貫していることを確証しなくてはならない (shall)。ベンダが TOE を宣伝するウェブサイトを維持管理している場合、評価者はそのウェブサイト上の情報を調査して、ST 中の情報がその製品を識別するために十分であることを確証しな*

くてはならない (shall)。

4.3.5.2 ALC_CMS.1 TOE の CM カバレージ

132 TOE の適用範囲とそれに関連した評価証拠の要件を考慮して、このコンポーネントの保証アクティビティは ALC_CMC.1 に関して列挙された保証アクティビティによってカバーされる。

開発者の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くてはならない (shall)。

内容及び提示エレメント：

ALC_CMS.2.1C 構成リストには、以下が含まれなくてはならない (shall)：TOE そのもの、及び SAR によって要求される評価証拠。

ALC_CMS.2.2C 構成リストには、構成要素が一意に識別されなくてはならない (shall)。

評価者の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資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない (shall)。*

保証アクティビティ：

133 *本 PP において「SAR によって要求される評価証拠」は、ST 中の情報と、AGD 要件の下で管理者及び利用者に提供されたガイダンスとの組み合わせに限られる。TOE が具体的に識別され、その識別が ST 及び AGD ガイダンスの内容と一貫していることを確証する (ALC_CMC.1 に関する評価アクティビティ中で行われるように) ことによって、評価者は暗黙にこのコンポーネントによって要求される情報を確認する。*

4.4 セキュリティ保証要件の根拠

134 これらのセキュリティ保証要件を選択した根拠は、本 PP 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だからである。この最初のプロテクションプロファイルが、開発ベストプラクティスを確認するために用いられる。これらの種類の製品に脆弱性が発見された場合には、より厳格なセキュリティ保証要件が、現実のベンダのプラクティスに基づいて義務付けられることになる。

附属書A： 参考表と参照資料及び略語

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[18] WPA2 Standard

AES	Advanced Encryption Standard
AF	認可ファクタ
AS	認可サブシステム
CAVS	暗号アルゴリズム検証システム
CC	コモンクライテリア
CCTL	コモンクライテリア評価機関
CM	構成管理
COTS	市販 (COTS) の
CMVP	暗号モジュール試験及び評価制度
DRBG	決定論的ランダムビット生成器
DoD	(米国) 国防省
EAL	評価保証レベル
ES	暗号化サブシステム
FIPS	連邦情報処理規格
ISSE	情報システムセキュリティエンジニア
IT	情報技術
OSP	組織のセキュリティ方針
PP	プロテクションプロファイル
PUB	公開
RBG	ランダムビット生成器
SAR	セキュリティ保証要件
SF	セキュリティ機能
SFR	セキュリティ機能要件
ST	セキュリティターゲット
TOE	評価対象
TSF	TOE セキュリティ機能
TSFI	TSF インタフェース
TSS	TOE 要約仕様

附属書B： NIST SP 800-53/CNSS 1253 との対応付け

NIST SP 800-53/CNSS 1253 管理策のいくつかは、適合 TOE によって完全または部分的に対処されている。このセクションは対処されている要件を概説し、また TOE がその運用構成に組み込まれた際に (もしあれば) どんな追加的テストが必要かを検定員が判定するために利用することができる。

適用上の注意：このバージョンでは、単純な対応付けのみが提供されている。将来のバージョンでは、検定チームへさらに情報を提供する追加的な説明文が含まれることになる。追加的情報には、SFR から管理策への対応付けに関する詳細が含まれ、TOE によって提供される適合の程度が論じられることになる (例えば、完全に管理策を満たす、部分的に管理策を満たす)。さらに、規定された保証アクティビティの包括的なレビューと、SAR を満たす過程で行われる評価アクティビティがまとめられ、適合が判定される方法 (例えば、文書レビュー、ベンダの主張、テスト／検証の程度) に関する情報を検定チームへ提供することになる。この情報は、規定された管理策への適合の程度を判定するために (もしあれば) どんな追加的アクティビティを行う必要があるかを検定チームへ示すことになる。

ST は選択に関して選択を行い、また割付に記入することになるため、ST が完成し評価されるまで最終的なストーリーは必ずしもでき上がらないかもしれない。したがって、この情報は PP に加えて ST にも含まれるべきである (should)。また、特定の実装に基づいて評価者によって行われるアクティビティには何らかの必要な解釈 (例えば、「変更」) が存在するかもしれない。スキームは、監督者 (例えば、検証者) にこの種の情報を記入させるかもしれないし、あるいは評価者に評価アクティビティの一環として行わせるかもしれない。評価チームの作業に加えて検定チームが (もしあれば) 何をする必要があるかを判定できるように、評価アクティビティは提供されなくてはならない (must) 必須の情報である。

識別子	名称	該当する SFRs
AC-3	アクセス制御の実施	FMT_SMF.1
AU-2	監査対象の事象	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	監査量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	監査の生成	FAU_GEN.1
CM-5	変更のためのアクセス制限	FPT_TUD_EXT.1
IA-3	デバイスの識別と認証	FCS_IPSEC_EXT.1, FTP_ITC.1
IA-5	認証子の管理	FIA_PSK_EXT.1, FIA_X509_EXT.1
SC-4	共有リソース中の情報	FDP_RIP.2
SC-8	伝送される情報の完全性	FCS_IPSEC_EXT.1, FTP_ITC.1
SC-9	伝送される情報の機密性	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	暗号の使用	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： 追加的要件

135 *このPP のドラフトでは、この附属書には追加的コンポーネントが含まれるが、それをサポートする脅威、対策方針、根拠、または (場合によって) 保証アクティビティは含まれない。最初のレビューサイクルと並行して、このサポート情報は開発され、PP の次回リリースに取り込まれることになる。このセクションに含まれる情報へのコメント (ここに含まれる要件が適合 TOE 候補へ適用されかどうかについても、この附属書には含まれないが VPN クライアント製品には広く適用できる要件についても、どちらでも) は、歓迎され募集される。*

本 PP の概論で示したように、ベースライン要件 (TOE によって行われなくてはならないもの) は本 PP の本体に含まれている。TOE が依然として本 PP に適合するような形で ST に含めることのできる追加的要件が存在する。これらの要件が、この附属書に含まれる。この附属書には、2 つの別個の種類の要件がある。セクション C.1 に含まれるものは TOE または運用環境のいずれかによる実装が要求されるものであり、X.509 証明書の利用に関するものである。TOE がこの機能を運用環境に依存するのではなく、実装することを選択した場合には、これらの要件は ST 作成者によって ST の本体へ移動されることになる。

136 それに対してセクション C.2 中及びそれ以降の要件は、要求はされ**ない**が、TOE によって実装され得るものである。その場合、ST 作成者はこの附属書から適切な情報を取り出し、それを自分の ST へ取り込むことになる。ST 作成者は、附属書 C と関連付けられるかもしれないが列挙されていない要件 (例えば、FMT タイプの要件) も、ST に確実に取り込む責任があることに注意されたい。この附属書に含まれない要件は、評価を監督する国家スキームによるレビュー及び承認を受けてから、本 PP への適合主張が行えるようになる。

C.1 クラス：識別と認証 (FIA)

PP 本体では、IPsec エンドポイントの認証に X.509 証明書の使用を必須とする要件を TOE に課している (FIA_X509_EXT.1.1, FCS_IPSEC_EXT.1.12)。相手方の VPN ゲートウェイに関しても、EP はそれらの要件を課している。これはソフトウェアのみの製品であるため、TOE が基盤となるオペレーティングシステムに依存して X.509 証明書の取り扱い／管理の側面の一部を行うことはあり得る。これらのうち最初のものは FIA_X509_EXT.1.2 であり、TOE が証明書の何らかのレベルの保護を提供できるというものであるが、おそらく基盤となる OS が不正な改変または削除からの最終的な保護を証明書に提供することになるであろう。もうひとつの側面は、証明書が有効であるかどうかの判定であり、FIA_X509_EXT.1.5、または認証パスに有効な CA 証明書が含まれていれば FIA_X509_EXT.1.6 及び FIA_X509_EXT.1.7 である。この機能が TOE によって行われるのであれば、この要件は PP 本体へ移される。有効性のチェックが環境によって行われ、有効または無効の回答が TOE に提供される場合には、この要件はここ、附属書 C.1 に残される。

X509 証明書 (FIA_X509_EXT)

FIA_X509_EXT.2 拡張：X.509 証明書の保管及び管理

FIA_X509_EXT.1.2 TSF は、証明書を保存し不正な削除及び改変から保護しなくてはならない (shall)。

適用上の注意：

137 *FIA_X509_EXT.1.2 は、TSF によって利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) によって利用され処理される証明書を、このエレメントの対象とすることは意図されていない。*

保証アクティビティ：

138 *評価者は、TSS に本 PP の要件を満たすために使われる証明書を含む、実装されたすべての証明書ストアが記述されることを確証しなくてはならない (shall)。この記述には、証明*

書がストアへロードされる方法、及びストアを不正なアクセスから保護する方法に関する情報が含まれなくてはならない (shall)。この記述は、TOE が証明書の保護に何らかの役割を果たすか、または保護の提供に関して TOE が環境に完全に依存しているかを示す。

評価者はガイダンス文書を調査して、証明書の不正な改変または削除を防止するために TOE または環境のいずれかを構成する方法が記述されていることを確証しなくてはならない (shall)。

139 *評価者は、証明書の使用を要求するシステム内の機能のそれぞれについて、以下のテストを行わなくてはならない (shall)。*

テスト 1 : 評価者は、有効な認証パスのない証明書を使用すると、その機能が失敗することを例証しなくてはならない (shall)。次に評価者は、その機能で使われるべき証明書の検証に必要とされる 1 または複数の証明書をロードし、その機能が成功することを例証しなくてはならない (shall)。次に評価者は、これらの証明書の 1 つを削除して、その機能が失敗することを示さなくてはならない (shall)。

FIA_X509_EXT.1.5 TSF は、[選択 : RFC 2560 の規定によるオンライン証明書状態プロトコル (OCSP)、RFC 5759 の規定による証明書失効リスト (CRL)] を用いて証明書を検証しなくてはならない (shall)。

FIA_X509_EXT.1.6 TSF は、すべての CA 証明書に関して basicConstraints 拡張が存在し cA フラグが TRUE に設定されていることを確証することによって認証パスを検証しなくてはならない (shall)。

FIA_X509_EXT.1.7 TSF は、basicConstraints 拡張が存在しないか cA フラグが TRUE に設定されていない場合、その証明書を CA 証明書として取り扱ってはならない (shall not)。

適用上の注意 :

採用される証明書失効手法の選択は ST 作成者に任されているが、本 PP の将来の版では TOE の管理者が両方の手法を利用できることが必須とされることになる。

保証アクティビティ :

評価者は、証明書の有効性チェックが行われる場所 (TOE、または環境) が TSS に記述されていることを確証しなくてはならない (shall)。TOE が環境にチェックと結果の提供を要求することもあり得るし、あるいは TOE がチェックを自分で行うこともあり得る。評価者は、認証パス検証アルゴリズムの記述が TSS に提供されていることも確証する。

評価者はガイダンス文書に、有効性チェックが TOE と環境のどちらによって行われるかに関わらず、有効性チェックを設定するために必要な情報が利用者へ提供されていることを確証する。ガイダンス文書には、チェックに用いられる手法を選択する方法と、証明書の有効性に関わる情報を提供するエンティティとの保護された通信パスを設定する方法が指示される。

テスト 1 : 評価者は、CRL または OCSP のどちらが選択されているかに応じて、TOE が失効した証明書を適切に処理できることをテストしなくてはならない (shall)。両方とも選択されている場合には、それぞれの手法についてテストが実施される。この EP のドラフトにおいては、評価者は信頼の連鎖の 1 つ上位のみをテストする必要がある (将来のドラフトでは、上位の連鎖全体について検証を行って確証することが要求されるかもしれない)。評価者は、有効な証明書が用いられていること、そして SA が確立されることを確証しなくてはならない (shall)。評価者は次に、失効することになる証明書 (選択において選択された手法のそれぞれについて) を用いてテストを試み、もはや証明書が有効ではない場合には TOE が SA を確立しないことを確証する。

テスト 2 : 評価者は、TOE の証明書を発行した CA の証明書に basicConstraints 拡張が含まれないように認証パスを構築しなくてはならない (shall)。この認証パスの検証は失敗する。

テスト 3 : 評価者は、TOE の証明書を発行した CA の証明書の basicConstraints 拡張中の

cA フラグがセットされていないように認証パスを構築しなくてはならない (shall)。この認証パスの検証は失敗する。

テスト 4：評価者は、TOE の証明書を発行した CA の証明書の basicConstraints 拡張中の cA フラグが TRUE にセットされているように認証パスを構築しなくてはならない (shall)。この認証パスの検証は成功する。

C.2 クラス：セキュリティ監査 (FAU)

監査の生成を TOE が提供している場合、ST 作成者によって適切な選択や割付が行われた上で、以下の監査要件が ST に取り込まれなくてはならない (must)。脅威、対策方針、及び根拠もここに含まれているが、セクション 2 に提示したセキュリティ課題定義に移動されることになるだろう。

T.UNDETECTED_ACTIONS	悪意のあるリモートユーザまたは外部 IT エンティティが、TOE のセキュリティに悪影響を及ぼすアクションを取るおそれがある。これらのアクションが検出されないままの状態となり、したがってその影響が効果的に低減されないおそれがある。

O.SYSTEM_MONITORING	TOE は、監査データを生成する機能を提供すること。

T.UNDETECTED_ACTIONS 悪意のあるリモートユーザまたは外部 IT エンティティが、TOE のセキュリティに悪影響を及ぼすアクションを取るおそれがある。これらのアクションが検出されないままの状態となり、したがってその影響が効果的に低減されないおそれがある。	O.SYSTEM_MONITORING TOE は、監査データを生成する機能を提供すること。	O.SYSTEM_MONITORING は、多くの基準に基づいてアクションを記録する監査メカニズムを構成する機能を管理者へ提供することによって、この脅威を低減する。

セキュリティ監査データの生成 (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することができなくてはならない (shall)。

a) 監査機能の開始と終了、

b) 監査のレベルが規定されていないすべての監査対象事象、及び

c) すべての管理アクション、

d) [*表 9 (訳注：表 11 の間違い) に列挙された、具体的に定義された監査対象事象*]。

適用上の注意：

140 *ST 作成者は、その他の監査対象事象を直接テーブルへ取り込むことができる。監査対象事象は、提示されたリストに制限されてはいない。*

141 *「a」の場合、言及された監査機能は TOE によって提供されるものである。例えば、TOE*

がスタンドアロンの実行可能形式であった場合、TOE 自身の起動及びシャットダウンの監査は、この条項の要件を満たすのに十分であろう。

142 *この文書に含まれる SFR の監査対象の側面の多くが、管理アクションに関するものである。上記の項目 c はすべての管理アクションが監査対象であることを要求しているため、これらのアクションの監査対象性の追加の仕様は表 9 (訳注：表 11 の間違い) には示されていない。TOE それ自身は管理者へ I&A を行う能力の提供を必要としないため、この要件は「管理アクション」として PP に記述される事象(主に、TOE によって提供される機能の構成に関するもの) を監査する機能を TOE が有することを意味している。OPE ガイダンスには、TOE によって生成される監査データが基盤となる IT 環境の監査機能と統合されることを確実にする手順を詳述することが期待される。*

保証アクティビティ：

143 *評価者は操作ガイダンスをチェックして、すべての監査対象事象が列挙されており、また監査記録のフォーマットが提供されていることを確証しなくてはならない (shall)。監査記録のフォーマットの種類はすべて、各フィールドの簡潔な記述とともに、カバーされなくてはならない (must)。評価者は、PP によって必須とされるすべての監査事象種別が記述され、またフィールドの記述には FAU_GEN.1.2 に要求される情報と、表 9 (訳注：表 11 の間違い) に規定される追加的情報が含まれていることをチェックして確証しなくてはならない (shall)。*

144 *評価者は特に、失敗した暗号事象の内容に関して操作ガイダンスが明確であることを確証しなくてはならない (shall)。表 9 (訳注：表 11 の間違い) において、操作の暗号モード及び暗号化されようとしているオブジェクトの名称または識別子を詳述することが要求されている。評価者は、管理者が監査ログをレビューして暗号オペレーションの文脈 (例えば、鍵ネゴシエーションの交換中に行われた、通過中のデータの暗号化中に行われた) と、他の IT システムとの通信に関連した暗号の失敗に関する TOE とは反対側のエンドポイントを判定するのにその名前または識別子が十分であることを確証しなくてはならない (shall)。*

145 *また評価者は、本 PP の文脈において重要な管理アクションの判定を行わなくてはならない (shall)。TOE には、その機能が SFR に規定されていないという理由で、本 PP の文脈においては評価されない機能が含まれているかもしれない。この機能は、操作ガイダンスに記述される管理的側面を持っているかもしれない。そのような管理アクションは TOE の評価される構成では行われることがないため、評価者は操作ガイダンスを調査して、サブコマンドやスクリプト、そして構成ファイルを含めたどの管理コマンドが、PP に規定された要件の強制に必要な TOE に実装されたメカニズムの構成 (有効化または無効化を含む) に関連しているのかを判定し、それによって「すべての管理アクション」のセットを形成しなくてはならない (shall)。評価者はこのアクティビティを、AGD_OPE ガイダンスが要件を満たすことを確証することに関連したアクティビティの一部として行ってもよい。*

146 *評価者は、本 PP 中の機能要件と関連付けられた保証アクティビティにしたがって TOE に監査記録を生成させることによって、TOE が正しく監査記録を生成できる能力をテストしなくてはならない (shall)。また評価者は、本 PP の文脈において該当する管理アクションのそれぞれが監査対象であることをテストしなくてはならない (shall)。テスト結果を検証する際に、評価者はテスト中に生成された監査記録が管理ガイドに規定されたフォーマットと一致することと、各監査記録のフィールドが適切なエントリを有することを確証しなくてはならない (shall)。*

147 *ここでのテストは、セキュリティメカニズムを直接テストすることと組み合わせて達成できることに注意されたい。例えば、提供された管理ガイダンスが正しいことを確証するために行われるテストは、AGD_OPE.1 が満たされることを検証し、したがって監査記録が期待通り生成されたことの検証に必要な管理アクションの呼び出しに対処しているはずである (should)。*

FAU_GEN.1.2 TSF は、少なくとも下記の情報を各監査記録内に記録しなくてはならない (shall)。

a) 事象の日付及び時刻、事象の種類、サブジェクトの識別情報、及び事象の結果 (成功または失敗)、ならびに

b) 監査事象種別のそれぞれについて、PP/ST に含まれる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 3 列目に規定された情報*]。

適用上の注意：

148 *先ほどのコンポーネントと同様に、ST 作成者は生成された追加的情報によって表 9 (訳注：表 11 の間違い) を更新すべきである (should)。この要件の文脈において「サブジェクトの識別情報」とは、例えば、管理者の利用者 ID または影響されるネットワークインタフェースのどちらかとなる。*

保証アクティビティ：

149 *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達成されるべきである (should)。*

表 11：監査対象事象

要件	監査対象事象	監査記録の追加的内容
FAU_GEN.1	なし。	
FAU_SEL.1	監査収集機能が動作している間に生じたすべての監査構成への変更。	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。	クリアされようとしていた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／復号されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(2)	暗号署名の失敗。	操作の暗号モード、署名／検証されようとしていたオブジェクトの名称／識別子。
FCS_COP.1(3)	ハッシュ関数の失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_COP.1(4)	非データ完全性の暗号ハッシュの失敗。	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子。
FCS_IPSEC_EXT.1	TOE によって処理されたネットワークパケットの破棄 (DISCARD)、バイパス (BYPASS)、保護 (PROTECT) の決定。 IPsec SA の確立失敗。 IPsec SA の確立／終了。	想定される送信元サブジェクトの識別情報。 宛先サブジェクトの識別情報。 該当する場合、トランスポート層プロトコル。 該当する場合、送信元サブジェクトのサービス識別子。 決定に適用された SPD 中のエントリ。 失敗の理由。 成功と失敗の両方の場合に

要件	監査対象事象	監査記録の追加的内容
		ついて、接続の TOE とは反対側のエンドポイント (IP アドレス)。
FCS_RBG_EXT.1	ランダム化プロセスの失敗。	なし。
FDP_RIP.2	なし。	
FIA_PSK_EXT.1	なし。	
FIA_X509_EXT.1	なし。	
FMT_SMF.1	なし。	
FPT_TST_EXT.1	TSF セルフテストのこのセットの実行。 検出された完全性違反。	完全性違反については、その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。 更新の完全性の検証のあらゆる失敗。	追加的情報なし。
FTP_ITC.1	高信頼チャネルを確立しようとするすべての試み。 チャネルデータの改変の検出。	そのチャネルの TOE とは反対側のエンドポイントの識別情報。

セキュリティ監査事象の選択 (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、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することができなくてはならない (shall)。

a) 事象の種別、

b) 監査対象セキュリティ事象の成功、

c) 監査対象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：

150 *この要件の意図は、監査事象を引き起こすために選択可能なすべての基準を特定することである。これは、クライアント上のインタフェースを利用者／管理者が呼び出すことによって構成されるか、あるいは事象が監査されるクライアントへ指示するために VPN ゲートウェイが利用するインタフェースかもしれない。ST 作成者は、割付を利用して任意の追加的基準を列挙するか、あるいは「なし」とする。監査対象事象種別は、表 9 (訳注：表 11 の間違い) に列挙されている。*

保証アクティビティ：

151 *評価者は管理ガイダンスをレビューして、ガイダンスにすべての事象種別が列挙されていること、そして割付に列挙されている属性を含めて、要件にしたがって選択可能なすべての属性が記述されていることを確証しなくてはならない (shall)。また管理ガイダンスには、事前選択を設定する方法、または VPN ゲートウェイがクライアントを構成する方法の指示が含まれるとともに、(もしあれば) 複数値の事前選択の構文が説明されなくてはならない (shall)。また管理ガイダンスには、現在強制されている選択基準に関わらず、常に記録される監査記録が特定されていなくてはならない (shall)。*

152 *また評価者は、以下のテストを行わなくてはならない (shall)。*

- *テスト 1：要件に列挙される属性のそれぞれについて、評価者はその属性の選択に*

よってその属性を持つ監査事象 (または、管理ガイダンスに特定される、常に記録される監査事象) のみが記録されることを示すテストを考案しなくてはならない (shall)。

テスト 2 [条件付き]：TSF がさらに複雑な監査事前選択基準の仕様 (例えば、複数の属性、属性を用いた論理式) をサポートしている場合には、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くてはならない (shall)。また評価者は、テスト計画中に、そのテストのセットが典型的なものであり、その機能を行使するのに十分であることを正当化する短い説明文を提供しなくてはならない (shall)。

153 監査レビューまたは監査ストレージあるいはその両方が TOE によってサポートされている場合、必要に応じて以下の監査要件が ST に取り込まれなくてはならない (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**正当な管理者**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くてはならない (shall)。
FAU_SAR.1.2	**詳細化**：TSF は、~~利用者~~**正当な管理者**が情報を解釈するのに適した形式で監査記録を提供しなくてはならない (shall)。

制約された監査レビュー (FAU_SAR.2)

FAU_SAR.2	**制約された監査レビュー**
FAU_SAR.2.1	**詳細化**：TSF は、**正当な管理者を除いて、**すべての利用者に**監査記録への**読み取りアクセスを禁止しなくてはならない (shall)。

FAU_STG_EXT.4	**監査データの損失の防止**
FAU_STG_EXT.4.1	TSF は、監査証跡に空きがない場合、取られるアクションとして以下の 1 つ以上を選択する機能を正当な管理者へ提供しなくてはならない (shall)： a) 正当な管理者によるものを除き、監査対象事象の抑制、及び b) 最も古く保存された監査記録の上書き。

適用上の注意：

154 *TOE は、監査事象の発生を防止することによって監査データの損失を防止するオプションを正当な管理者へ提供する。これらの状況下での正当な管理者のアクションが、監査されることは要求されていない。また TOE は、監査対象事象を抑止するのではなく、「古い」監査記録を上書きするオプションを正当な管理者へ提供する。これによって、サービス拒否攻撃への保護が提供できるかもしれない。*

C.3 クラス：識別と認証 (FIA)

155 TOE が管理機能を提供する場合、その機能を規定するために適用可能な要件は、リモート管理やローカル管理、そして管理セッションの保護など、数多く存在する。このバージョンの PP では、VPN ゲートウェイのプロテクションプロファイルからの管理要件を用いて、クライアントのそのような機能を規定することは受容可能である。

156 TOE が交換中に用いられる証明書を保存し管理する能力を提供する場合、以下の要件を ST

に取り込むことができる。

事前共有鍵の作成 (FIA_PSK_EXT)

157 TOE は IPsec プロトコルに使用する事前共有鍵をサポートしてもよく、またその他のプロトコルにも事前共有鍵を使用してもよい。TOE がサポートしなくてはならない事前共有鍵には、以下の要件中に規定される 2 種類がある。1 種類目は「テキストベースの事前共有鍵」と呼ばれ、パスワードと同様に標準的なキャラクタセットからなる文字列としてユーザによって入力される事前共有鍵を指す。そのような事前共有鍵は、文字列がビット列に変換された後に鍵として用いられるよう、調整されなくてはならない (must)。

158 2 種類目は (標準的な用語が存在しないため) 「ビットベースの事前共有鍵」と呼ぶことにする。これは、管理者からのコマンドにより TSF が生成するか、または管理者によって「直接形式 (direct form)」で入力される鍵である。「直接形式」とは、テキストベースの事前共有鍵のように「調整」されるのではなく、入力が直接鍵として用いられることを意味する。例としては、鍵を構成するビットを表現する 16 進数の文字列が挙げられるであろう。

159 以下の要件は、TOE がテキストベース及びビットベースの両方の事前共有鍵をサポートしなくてはならないことを義務付けているが、ビットベースの事前共有鍵の生成は TOE によって、または運用環境内のどちらで行われてもよい。

FIA_PSK_EXT.1	**拡張：事前共有鍵の作成**
FIA_PSK_EXT.1.1	TSF は、IPsec 及び [選択：*その他のプロトコルなし*、[割付：事前共有鍵を用いる他のプロトコル]] に事前共有鍵を用いることができなくてはならない (shall)。
FIA_PSK_EXT.1.2	TSF は、以下の条件を満たすテキストベースの事前共有鍵を受け入れることができなくてはならない (shall)。 • 22 文字及び *[選択：[割付：その他のサポートされている長さ]、その他の長さなし]* であること。 • 大文字及び小文字、数字、ならびに特殊文字 (“!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、及び “)”) の任意の組み合わせから構成されること。
FIA_PSK_EXT.1.3	TSF は、[選択、少なくとも 1 つを選択：[選択：SHA-1、SHA-256、SHA-512、[割付：*テキスト文字列の調整手法*]] を用いてテキストベースの事前共有鍵を調整し、ビットベースの事前共有鍵の [選択：受け入れ、FCS_RBG_EXT.1 に規定されたランダムビット生成器を用いた生成] ができ] なくてはならない (shall)。

適用上の注意：

160 *最初の選択においては、別のプロトコルが事前共有鍵を利用できるのであれば、そのプロトコルが割付中に列挙されるべきである (should)。そうでなければ、「その他のプロトコルなし」が選択されるべきである (should)。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とビットベースの両方の事前共有鍵をサポートすることである。*

161 *テキストベースの事前共有鍵の長さについては、相互運用性の向上を意図して、よく使われる長さ (22 文字) が必要とされている。その他の長さがサポートされる場合、それは割付中に列挙されるべきである (should)。また、この割付で値の範囲 (例えば、「5 文字から 55 文字までの長さ」) を規定することもできる。*

162 *FIA_PSK_EXT.1.3 の選択においては、ST 作成者はサポートされる事前共有鍵の種類を規定する。「テキストベースの事前共有鍵」が選択された場合、ST 作成者は、管理者によって入力されたテキスト文字列が鍵として用いられるビット列に「調整」される手法を記入する。これは、規定されたハッシュ関数のいずれかによって、または割付文による何らかの*

その他の手法によって行うことができる。「ビットベースの事前共有鍵」が選択された場合、ST 作成者は、TSF がビットベースの事前共有鍵を単に受け入れるのか、それともそれを生成することができるのかを規定する。生成できる場合、それは TOE によって提供される RBG を用いて生成されなくてはならない、と要件には規定されている。

保証アクティビティ：

163 *評価者は操作ガイダンスを調査して、強いテキストベースの事前共有鍵の作成に関して管理者へガイダンスが提供されていることを判定し、そして (さまざまな長さの鍵が入力できることが選択によって示されている場合には) 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判定しなくてはならない (shall)。ガイダンスには事前共有鍵に使用できる文字が指定されていなくてはならず、またそのリストは FIA_PSK_EXT.1.2 に含まれるリストのスーパーセットでなくてはならない (must)。*

164 *評価者は TSS を調査して、テキストベース及びビットベースの両方の事前共有鍵が許可されるすべてのプロトコルが特定されていること、そして 22 文字のテキストベースの事前共有鍵のサポートが言明されていることを確証しなくてはならない (shall)。「テキストベースの事前共有鍵」が選択されている場合、要件によって特定されるプロトコルのそれぞれについて、調整が行われてテキストベースの事前共有鍵がユーザの入力した鍵のシーケンス (例えば ASCII 表現) からそのプロトコルの用いるビット列へ変換されることが TSS に言明されていること、そしてこの調整が FIA_PSK_EXT.1.3 要件における最後の選択と一貫していることを、評価者は確認しなくてはならない (shall)。*

165 *「ビットベースの事前共有鍵」が選択されている場合、評価者は、要件中に特定されるプロトコルのそれぞれについてビットベースの事前共有鍵を入力するか、ビットベースの事前共有鍵を生成するか (あるいはその両方) の指示が操作ガイダンスに含まれていることを確認しなくてはならない (shall)。また評価者は TSS を調査して、ビットベースの事前共有鍵が生成されるプロセスが記述されていること (TOE がこの機能をサポートしている場合) を確証し、またこのプロセスが FCS_RBG_EXT.1 に規定される RBG を用いることを確認しなくてはならない (shall)。*

166 *評価者はまた、各プロトコル (TOE 上の異なる実装によって実施される場合には、プロトコルの具体化) について以下のテストを実施しなくてはならない (shall)。単一のテストケースによって、これらのテストの 1 つ以上が実施できることに注意されたい。*

- *テスト 1 : 評価者は、操作ガイダンスにしたがって許可される文字の組み合わせを含む 22 文字の事前共有鍵を作成し、この鍵を用いたプロトコルネゴシエーションが成功することを例証しなくてはならない (shall)。*
- *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している場合、管理者は最小限の長さ、最大限の長さ、及び無効な長さを用いてテスト 1 を繰り返さなくてはならない (shall)。最小限及び最大限の長さのテストは成功するはずであり、無効な長さは TOE によって拒否されなくてはならない (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、評価者は適切な長さのビットベースの事前共有鍵を取得して、操作ガイダンス中の指示にしたがってそれを入力しなくてはならない (shall)。評価者は次に、その鍵を用いたプロトコルネゴシエーションが成功することを例証しなくてはならない (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、評価者は適切な長さのビットベースの事前共有鍵を生成して、操作ガイダンス中の指示にしたがってそれを使用しなくてはならない (shall)。評価者は次に、その鍵を用いたプロトコルネゴシエーションが成功することを例証しなくてはならない (shall)。*

附属書D： 文書の表記

167 英国式つづりを米国式つづりに置き換えた以外には、本 PP に用いられる記法、様式、及び表記はコモンクライテリア (CC) のバージョン 3.1 と一貫している。PP の読者を助けるため、選択された表記法についての議論をここで行う。

168 本 PP に用いられる記法、様式、及び表記はコモンクライテリア (CC) のバージョン 3.1 に用いられたものと一貫している。PP の読者を助けるため、選択された表記法についての議論をここで行う。CC では、機能及び保証要件に対していくつかの操作を行うことを許可している。*詳細化*、*選択*、*割付*、及び*繰返し*がCC 3.1 のパート 1 の附属書 C4 に定義されている。これらの操作のすべてが、本 PP で用いられている。

詳細化の表記

169 **詳細化**の操作は、要件に詳細を付け加え、これによってさらに要件を制約するために用いられる。セキュリティ要件の詳細化は、エレメント番号の後に**太字**で表記された「詳細化」という単語と、太字で表記された要件中の追加的な本文によって示される。

選択の表記

170 **選択**の操作は、CC によって要件の言明中に提供された 1 つ以上の選択肢を選択するために用いられる (CC 3.1 のパート 1、附属書 C.4.3 を参照)。PP 作成者によってなされた選択は**太字**で表記されたその選択と、大括弧及び「選択」の文字を削除して示される。ST 作成者によって記入されるべき選択は、大括弧中に選択が行わるべきことを示す指示によって示される： [選択：]。

割付の表記

171 **割付**の操作は、例えばパスワードの長さのように、まだ規定されていないパラメタへ特定の値を割り付けるために用いられる (CC 3.1 のパート 1、附属書 C.4.2 を参照)。**太字**で示された値は、その割付が PP 作成者によってなされたことを示し、大括弧と「割付」の文字は削除される。ST 作成者によって記入されるべき割付は、大括弧中に割付が行わるべきことを示す指示によって示される： [割付：]。

繰返しの表記

172 **繰返し**の操作は、変化する操作と共にコンポーネントが繰り返される場合に用いられる (CC 3.1 のパート 1、附属書 C.4.1 を参照)。繰返し回数 (iteration number) は、コンポーネントの識別子に引き続く括弧の中で示される。

173 繰返しの操作は、すべてのコンポーネント上で実行できる。PP/ST 作成者は、同一のコンポーネントに基づく複数の要件を取り込むことによって、繰り返し操作を行う。コンポーネントの各繰返しは、そのコンポーネントの他のすべての繰り返しとは異なっていなくてはならず (shall)、これは割付及び選択を異なる方法で完成させることによって、または異なる方法で詳細化を適用することによって、実現される。

拡張要件の表記

174 拡張要件は、作成者のニーズを満たす適切な要件を CC が提供していない場合に許可される。**拡張要件**は特定されなくてはならず (must)、またその要件を関連付けるにあたって CC のクラス／ファミリ／コンポーネントモデルを利用することが要求される。拡張要件は、コンポーネント中に「EXT」を挿入することによって示される。

適用上の注意

175 適用上の注意には、適合 TOE のセキュリティターゲットの構築に関連する、または役立つと考えられる追加的なサポート情報に加えて、開発者や評価者、そして ISSE に関する一般的な情報が含まれる。適用上の注意には、コンポーネントの許可された操作に関するアドバイスも含まれる。

保証アクティビティ

176 保証アクティビティは、TOE に課された機能要件が脅威を低減するための共通評価方法として役立つ。このアクティビティには、TSS に文書化された TOE の特定の側面を評価者が分析するための指示が含まれているため、ST 作成者にはこの情報を TSS セクションへ取り込むという暗黙の要件が課される。このバージョンの PP においては、これらのアクティビティは機能及び保証コンポーネントと直接関連付けられているが、将来のバージョンではこれらの要件が別個の附属書または文書へ移動されるかもしれない。

附属書E： 用語集

管理者 – 特権モードで TOE を構成する管理者権限を有する利用者。

認証サーバ (AS) – 保護ネットワークへのアクセスを試みるエンティティ（利用者またはクライアント）の認証に役立つよう設計されたエンティティ。

正当な (権限のある) – オブジェクトやシステム、またはシステムエンティティへのアクセス権限を付与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 (CSP) – セキュリティ関連情報、例えば共通暗号鍵や秘密暗号鍵、そしてパスワードや PIN などの認証データであって、その開示または変更が暗号モジュールのセキュリティの危殆化をもたらす可能性のあるもの。

エントロピー源 – この暗号機能は、1 つ以上の雑音源からの出力を蓄積することによって乱数生成器にシードを供給する。この機能には、所与の出力を推測するために必要とされる最低限の労力の計量と、雑音源が適切に動作していることを確実にするためのテストが含まれる。

FIPS 承認済み暗号機能 – セキュリティ機能（例えば、暗号アルゴリズム、暗号鍵管理テクニック、あるいは認証テクニック）であって、 1) 連邦情報処理規格 (FIPS) に規定されているか、 2) FIPS に採用され、FIPS の附属書または FIPS によって参照される文書のどちらかに規定されているもの。

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

運用環境 – その中で TOE が運用される環境。

専用ネットワーク – 権限のない利用者またはエンティティによるアクセスから保護されたネットワーク。

特権モード – TOE の動作モードであって、IT 環境の管理者権限が要求される機能の実行を、利用者へ許可するもの。

公共ネットワーク – すべての利用者及びエンティティに可視であり、不正なアクセスからの保護が行われないネットワーク (例えばインターネット)。

セキュリティ保証要件 (SAR) – TOE が SFR を満たしているという保証がどのようにして得られるかという記述。

セキュリティ機能要件 (SFR) – TOE のセキュリティ対策方針を、標準化された言語に変換したもの。

セキュリティターゲット (ST) – 具体的な特定された TOE に関する、実装に依存したセキュリティの必要性の言明。

評価対象 (TOE) – ソフトウェア、ファームウェア、またはハードウェア、あるいはこれらの任意の組み合わせであって、ガイダンスが伴う可能性がある。本 PP に関しては、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、開示、改変、またはサービス拒否、あるいはこれらの任意の組み合わせによって情報システムに危害を加えようと試みるエンティティ。

TOE セキュリティ機能 (TSF) – TOE のすべてのハードウェアとソフトウェア、そしてファームウェアの結合した機能であって、SFR の正しい強制のために信頼されなくてはならない (must) もの。

TOE 要約仕様 (TSS) – TOE が SFR のすべてをどのように満たしているかという記述。

権限のない利用者 – 正当な管理者によって TOE または専用ネットワークへのアクセスを認可されていないエンティティ（デバイスまたは利用者)。

非特権モード – TOE の動作モードであって、VPN クライアントユーザへ VPN クライアント機能のみを提供するもの。

VPN クライアント – リモートユーザがクライアントコンピュータを使って専用ネットワークへの暗号化された IPsec トンネルを、保護されていない公共ネットワークを通して確立することを可能とする TOE。

VPN クライアントユーザ – 非特権モードで TOE を操作する利用者。

VPN ゲートウェイ – IP パケットが専用ネットワークと公共ネットワークの境界を通過する際に、その暗号化及び復号を行うコンポーネント。

附属書F： PP 識別情報

タイトル :	Protection Profile for IPsec Virtual Private Network (VPN) Clients (仮想プライベートネットワーク (VPN) クライアントのプロテクションプロファイル)
バージョン :	1.1
スポンサー :	(米国) 国立情報保証パートナーシップ (NIAP)
CC のバージョン :	Common Criteria for Information Technology Security Evaluation (CC) Version 3.1, R3 July 2009 (情報技術セキュリティ評価のためのコモンクライテリア (CC) バージョン 3.1 改訂第 3 版､2009 年 7 月)
キーワード :	認証サーバ、IKE、IPsec、PKI、VPN、VPN クライアント、VPN

附属書G： エントロピーの文書化と評価

エントロピー源の文書は、それを読んだ後の評価者が完全にエントロピー源を理解し、それがエントロピーを供給すると信頼できる理由を理解できるように、十分に詳細であるべきである (should)。この文書には、設計の記述、エントロピーの正当化、運用条件、及びヘルステストという、複数の詳細なセクションが含まれるべきである (should)。この文書は、TSS の一部である必要はない。

設計の記述

文書には、すべてのエントロピー源コンポーネントの相互作用を含めた、エントロピー源の全体的な設計が含まれなくてはならない (shall)。これにはエントロピー源の動作が記述され、どのように動作するのか、どのようにエントロピーが作り出されるのか、そしてどのように未処理 (生の) データをエントロピー源の内部からテスト目的で取り出すことができるのか、などが含まれることになる。この文書では、エントロピー源の設計の概略が説明され、ランダム性がどこから由来し、次にどこへ渡されるのか、任意の生の出力の後処理 (ハッシュ、XOR など)、保存されるのか (保存されるとすればどこに)、そして最後に、どのようにしてエントロピー源から出力されるのかを示すべきである (should)。処理に課される条件があれば (例えば、ブロッキング)、それもエントロピー源の設計の中で記述されるべきである (should)。図や例を利用することが望ましい。

また、この設計にはエントロピー源のセキュリティ境界の内容の説明と、境界外部の敵対者がエントロピー量に影響を与えられないことがどのようにしてセキュリティ境界によって確実とされるのかという説明が含まれなくてはならない (must)。

エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、エントロピー源が確率的な挙動を示すことがなぜ確信できるのか (確率分布の説明と、その分布が特定のエントロピー源によって得られるという正当化を行うことは、これを記述する方法のひとつである) という、技術的な議論が存在すべきである (should)。この議論には、期待されるエントロピー量の記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられると確信できる理由の説明が含まれることになる。この議論は、エントロピー源がエントロピーを含むビットを作り出すと信頼できる理由の正当化の一部となる。

運用条件

また文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。これには、これらの条件の下でエントロピー源が動作し続けることを確実にするために、システムの設計に取り入れられた対策が明確に記述されることになる。同様に、文書にはエントロピー源が不調または一貫しない動作となることがわかっている条件も記述されなくてはならない (shall)。エントロピー源の故障または機能低下を検出するための手法が、含まれなくてはならない (shall)。

ヘルステスト

さらに具体的に、すべてのエントロピー源ヘルステストとその根拠が文書化されることになる。これには、ヘルステストの記述、各ヘルステストが行われる頻度及び条件 (例えば、起動時、連続、またはオンデマンド)、各ヘルステストに期待される結果、そしてそれぞれのテストがエントロピー源の 1 つ以上の故障を検出するために適当であると信じられる理由を示す根拠が含まれることになる。