ネットワークデバイスプロテクションプロファイル（NDPP）拡張パッケージ VPN ゲートウェイ

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_nd_vpn_gw_ep_v1.1.pdf

Information Assurance Directorate

2013 年 4 月 12 日
バージョン 1.1

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

1　概論 6

1.1　適合主張 6
1.2　本拡張パッケージの使用方法 6
1.3　適合評価対象 6

2　セキュリティ課題記述 8

2.1　情報の不正開示 8
2.2　サービスへの不適切なアクセス 9
2.3　サービスの悪用 9
2.4　データ完全性の危殆化 10
2.5　リプレイ攻撃 10

3　セキュリティ対策方針 11

3.1　データの暗号化及び復号 11
3.2　認証 11
3.3　アドレスベースのフィルタリング 11
3.4　セキュアでない操作 11
3.5　ポートベースのフィルタリング 12
3.6　システム監視 12
3.7　TOE の管理 12

4　セキュリティ要件 13

4.1　表記 13
4.2　TOE セキュリティ機能要件 13
4.2.1　NDPP セキュリティ機能要件の方向性 13
4.2.2　FCS_CKM.1 (2) 暗号鍵生成（非対称鍵） 16
4.2.3　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 17
4.2.4　FPF_RUL_EXT.1 パケットフィルタリング 18
4.2.5　FIA_AFL.1 認証失敗の取り扱い 20
4.2.6　FIA_X509_EXT.1 拡張：X.509 証明書 21
4.2.7　FMT_MOF.1 セキュリティ機能のふるまいの管理 22
4.2.8　FPT_FLS.1 フェイルセキュア 22
4.2.9　セキュリティ監査 22

5　保証アクティビティ 23

5.1.1　FCS_CKM.1 暗号鍵生成（非対称鍵） 23

5.1.2 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 25
5.1.3 FPF_RUL_EXT.1 拡張：パケットフィルタリング 31
5.1.4 FIA_AFL.1 認証失敗の取り扱い 37
5.1.5 FIA_X509_EXT.1 拡張：X.509 証明書 37
5.1.6 FMT_SMF.1 管理機能の仕様 38
5.1.7 FPT_FLS.1 フェイルセキュア 38
5.1.8 FAU_GEN.1 監査事象及び詳細 38
5.2 セキュリティ保証要件 39
5.2.1 AVA_VAN.1 脆弱性調査 39

6 根拠 41

6.1 セキュリティ課題定義 41
6.1.1 前提条件 41
6.1.2 脅威 41
6.1.3 組織のセキュリティ方針 42
6.1.4 セキュリティ課題と定義の対応 42
6.2 セキュリティ対策方針 42
6.2.1 TOE のセキュリティ対策方針 42
6.2.2 運用環境のセキュリティ対策方針 43
6.2.3 セキュリティ対策方針の対応 43

7 附属書 C：追加要件 44

7.1.1 事前共有鍵の作成（FIA_PSK_EXT） 44
7.1.2 FIA_PSK_EXT.1 拡張：事前共有鍵の作成 44

8 附属書 D：モビリティの要件 46

8.1 セキュリティ課題の記述 46
8.2 脅威 46
8.2.1 不正なクライアントの接続 46
8.2.2 セッションのハイジャック 46
8.2.3 保護されないクライアントのトラフィック 46
8.3 対策方針 46
8.3.1 クライアント接続確立の制約 46
8.3.2 リモートセッションの終了 47
8.3.3 割り当てられたプライベートアドレス 47
8.4 FTA：TOE アクセス 47
8.4.1 FTA_SSL.3 TSF 主導による終了 47
8.4.2 FTA_TSE.1 TOE セッションの確立 47
8.4.3 FTA_VCM_EXT.1 VPN クライアント管理 47

9　附属書 E 48

改版履歴

バージョン	日付	説明
1.0	2011 年 12 月	初版リリース
1.1	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　概論

本拡張パッケージ（EP）は、VPN ゲートウェイ（専用ネットワークの端点で IPsec トンネルを終端する装置と定義され、デバイス認証、機密性、そして公共または信頼できないネットワークを通過する情報の完全性を提供する）のセキュリティ要件を記述し、また明確に定義かつ記述された脅威の低減を目的とした要件の最小限のベースライン･セットの提供を意図している。 しかし、本 EP は本 EP 自体で完結するものではなく、*ネットワークデバイスのセキュリティ要件*プロテクションプロファイル（NDPP）を拡張するものである。この概論では、適合する評価対象（TOE）の特徴を記述し、また本 EP が NDPP との関連においてどのように使われるべきかも論じることとする。

1.1　適合主張

*ネットワークデバイスのセキュリティ要件*プロテクションプロファイル（NDPP）は、一般的なネットワークインフラストラクチャデバイスのベースラインセキュリティ機能要件（SFR）及びセキュリティ保証要件（SAR）を定義する。本 EP は、VPN ゲートウェイネットワークインフラストラクチャデバイスに特有の SFR 及びそれに関連した「保証アクティビティ」によって、NDPP ベースラインを拡張するものである。保証アクティビティは、TOE の SFR への適合性を判定するために評価者が実施するアクションである。

本 EP は、*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*，バージョン 3.1，リリース 4 に適合している。CC パート 2 拡張及び CC パート 3 適合である。

1.2　本拡張パッケージの使用方法

NDPP の EP として、本 EP と NDPP 双方の内容が各製品固有のセキュリティターゲットの文脈で適切に組み合わされることが期待される。本 EP は、そのような使用方法において困難さやあいまいさが存在しないよう、具体的に定義されている。ST は、適用される NDPP（現行バージョンについては http://www.niap-ccevs.org/pp/を参照）及び本 EP のバージョンをその適合主張の中で特定しなくてはならない（must）。

1.3　適合評価対象

本 EP では、もっぱら IPsec VPN トンネルを終端するネットワークゲートウェイデバイスを取り扱う。適合 VPN ゲートウェイは、複数の別個のネットワークに接続されるハードウェア及びソフトウェアからなるデバイスであり、またエンタープライズネットワーク全体においてインフラストラクチャとしての役割を担うものである。具体的には、VPN ゲートウェイは他拠点への認証かつ暗号化されたパスを提供するセキュアなトンネルを確立し、それによって信頼できないネットワークを通過する情報の漏えいリスクを低減させる。

本 EP のベースライン要件は、複数拠点間 VPN ゲートウェイデバイスに必要と判断されたものである。しかし適合 TOE には、リモートクライアントのヘッドエンドとして動作する能力が含まれてもよい。この機能はオプションであるため、リモートクライアントベースの要件は附属書 D に含まれている。

本 EP は NDPP 上に構築されるため、適合 TOE は NDPP に要求される機能と共に、本書で以下に論ずる脅威環境に対応して、本 EP に定義される追加機能をも実装することが義務付けられる。

本 EP における一連の要件は、より迅速かつ低コストの評価を推奨してエンドユーザへ付加価値を提供するため、意図的に範囲が限定されている。

2　セキュリティ課題記述

VPN ゲートウェイは、保護ネットワークへの侵入や保護ネットワークからの漏えいなど、信頼できないネットワークを通過するデータの機密性及び完全性に関するさまざまなセキュリティの脅威に対応する。ここで用いられる*保護ネットワーク*という用語は、アクセスを制御するための規則が定義されている、接続されたネットワークを意味する。それゆえ、所与の VPN にはその具体的な構成により、さまざまな保護及び非保護ネットワークが同時に接続されている可能性がある。また、すべての接続されたネットワークが管理者の裁量によって*保護可能*であることが前提となることも、明らかであろう。以下に用いられる*内向き（ingress）のトラフィック*という用語は保護ネットワークの外部に存在する脅威エージェントからのトラフィックを表し、また以下に用いられる*外向き（egress）のトラフィック*という用語は保護ネットワークの内部に存在する脅威エージェントからのトラフィックを表す。該当する脅威には、情報の不正開示、サービスへの不適切なアクセス、及びネットワークベースの偵察が含まれる。しかしデータと比較して、脅威エージェントの位置は問題ではない。例として、データの漏えいとは、そのデータを持ち出すための適切な権限なしにデータが持ち出されたことを意味する。これは、外部から（pull）も内部から（push）も起こり得る。外部からの侵入の結果かもしれないし、内部者の行為によるものかもしれない。サイトは、そのセキュリティ方針を策定し、そのニーズを満たすために VPN によって適用されるルールセットを構成する責任を負う。

本 EP では NDPP で特定された脅威を繰り返すことはしないが、本 EP の NDPP への適合性、したがって依存性のためにはそれらの脅威がすべて適用されることに注意されたい。また、NDPP には TOE がそのセキュリティ機能を提供するための能力への脅威のみが含まれるが、本 EP は運用環境におけるリソースへの実際上の（business）脅威のみを取り扱うことにも注意されたい。NDPP の脅威と本 EP に定義される脅威とを合わせて、VPN TOE によって対処されるセキュリティの脅威の包括的な集合が定義されるのである。

2.1　情報の不正開示

保護ネットワーク上のデバイスは、不正なアクティビティを行おうとする、保護ネットワーク外部に位置するデバイスによる脅威にさらされる可能性がある。既知の悪意のある外部デバイスが保護ネットワーク上のデバイスと通信できる場合、または保護ネットワーク上のデバイスがこれらの外部デバイスとの通信を確立できる場合（例えば、*フィッシング*エピソードの結果または電子メールメッセージへの不用意な応答によって）、これらの内部デバイスは情報の不正開示を許可してしまうかもしれない。

侵入という観点から見ると VPN ゲートウェイは、保護ネットワーク内部の特定の*送信先*ネットワークアドレス及びポートのみにアクセスを制限するだけではなく、ネットワークトラフィックが暗号化されるか、それとも平文で送信されるかに関しても関与する。これらの制限により、一般的なネットワークポートスキャンが保護ネットワークまたはマシンへ到達することを防止でき、さらに保護ネットワーク上の情報へのアクセスを、特定されたネットワークノード上の専用に構成されたポートから取得可能なものだけに制限することもできる（例えば、指定された企業 Web サーバ上の Web ページ）。加えて、アクセスを特定の*送信元*アドレス及びポートのみに制限することにより、特定のネットワークまたはネットワークノードが保護ネットワークへアクセスすることを阻止し、これによってさらに情報開示の可能性を限定することもできる。

漏えいという観点から見ると VPN ゲートウェイは、保護ネットワーク上で動作するネットワークノードが他のネットワークと接続及び通信する方法を制限することにより、これらのノードが情報を発出する方法及び相手先を制限することができる。特定の外部ネットワークを完全にブロックすることもできるし、あるいは外向きのトラフィックを特定のアドレスまたはポート、あるいはその両方に制限することもできるであろう。対案として、保護ネットワーク上のネットワークノードが利用可能な外向きトラフィックのオプションを慎重に管理することもできる（例えば外部への接続を確実に暗号化して、パケットスニッフィングによる不適切なデータの開示の可能性をさらに低減するため）。

(T.NETWORK_DISCLOSURE)

2.2 サービスへの不適切なアクセス

保護ネットワーク内部から、または保護ネットワーク内への認証されたパスを用いるエンティティからのアクセスのみが意図されている、保護ネットワーク上に位置するサービスを、保護ネットワーク外部に位置するデバイスが実行しようとするかもしれない。同様に、保護ネットワーク外部に位置するデバイスが、保護ネットワーク内部からのアクセスが不適切なサービスを提供するかもしれない。

内向きの観点から見ると VPN ゲートウェイは、信頼されたネットワーク上で動作するエンティティ（例えば、ピア VPN ゲートウェイが接続をサポートしているネットワーク上で動作するマシン）による外部利用を意図したネットワークサービスのみが、しかも意図したポートを介してのみ、アクセス可能となるように構成することができる。これは、保護されたネットワーク内部での利用またはアクセスのみを意図したネットワークサーバまたはサービスへ、保護ネットワーク外部のネットワークエンティティがアクセスする可能性を低減するために役立つ。

外向きの観点から見ると VPN ゲートウェイは、保護ネットワーク内部から特定の外部サービスのみが（例えば、送信先ポートに基づいて）アクセスできるように、あるいはさらに暗号化されたチャネルを介してアクセスされるように構成することができる。例えば、外部メールサービスへのアクセスをブロックすることによって、管理下にない電子メールサーバへのアクセスを禁止する企業方針、またはメールサーバへのアクセスは暗号化されたリンク上で行わなくてはならないという企業方針を強制することができる。

(T. NETWORK_ACCESS)

2.3 サービスの悪用

保護ネットワーク外部に位置するデバイスが、保護ネットワーク内部で提供されている特定の公共サービスへのアクセスを許可されている一方で、これらの許可された公共サービスと通信しながら不適切なアクティビティを行おうとするかもしれない。また保護ネットワーク内部から提供される特定のサービスが、保護ネットワーク外部からアクセスされた場合にリスクとなるかもしれない。

内向きの観点から見ると、外部ネットワーク上で動作するエンティティは特定の保護ネットワーク向けの利用方針には束縛されないことが一般的には前提となる。その場合であっても VPN ゲートウェイは、方針違反をログに記録して、公共利用可能サービスについて公開された利用規約への違反をを指摘できるかもしれない。

外向きの観点から見ると VPN ゲートウェイは、保護ネットワークの利用方針の強制や監視に役立つよう構成することができる。他の脅威の項で説明したように、ステートフルトラフィックフィルタファイアウォールはデータの発出や外部サーバへのアクセス、さらにはサービスの中断を限定するために役立つ。これらはすべて保護ネットワークの利用方針に関連する可能性があり、それゆえ方針の強制対象ともなり得る。さらに VPN ゲートウェイは、保護ネットワークと外部ネットワークとの境界をまたぐネットワークの利用をログに記録するように構成でき、それによって利用方針違反の可能性を特定するために役立てることができる。

(T.NETWORK_MISUSE)

2.4 データ完全性の危殆化

保護ネットワーク上のデバイスは、権限なくデータの改変を行おうとする、保護ネットワーク外部に位置するデバイスによる脅威にさらされるかもしれない。既知の悪意のある外部デバイスが保護ネットワーク上のデバイスと通信できる場合、または保護ネットワーク上のデバイスがこれらの外部デバイスとの通信を確立できる場合、通信に含まれるデータが完全性を失ってしまうかもしれない。

(T.DATA_INTEGRITY)

2.5 リプレイ攻撃

権限のない人物がシステムへのアクセスを得ることに成功した場合、その敵対者は「リプレイ」攻撃を行う機会を得るかもしれない。この攻撃手法では、その人物がネットワーク全体を通過するパケットをキャプチャして、おそらくは意図した受信者に気付かれることなく、後にそのパケットを送信することが可能となる。

(T.REPLAY_ATTACK)

3　セキュリティ対策方針

セクション 2 で記述したセキュリティ課題は、暗号化機能とパケットフィルタリングとの組み合わせによって対処されることになる。適合 TOE はセキュリティ機能を提供し、そのセキュリティ機能が TOE への脅威へ対処し、法令または規則によって課される方針を強制することになる。以下のサブセクションでは、これまでに論じた脅威／方針へ対策するために必要なセキュリティ対策方針の記述が提供される。そのセキュリティ対策方針の記述は、[NDPP] に記述されたものへの追加である。

注：以下の各サブセクションでは、具体的なセキュリティ対策方針が特定され（*O.*によって明示される）、その対策方針を満たすためのメカニズムを提供するセキュリティ機能要件（SFR）と関連付けられる。

3.1　データの暗号化及び復号

情報の不正開示、サービスへの不適切なアクセス、サービスの悪用、サービスの中断、及びネットワークベースの偵察に関連する課題に対処するため、適合 TOE は暗号化機能を実装すること。この機能の目的は、機密性を保つとともに TOE 外部から送信されるデータの検出と改変を可能とすることである。

（ O.CRYPTOGRAPHIC_FUNCTIONS → FCS_COP.1, FCS_RBG_EXT.1, FCS_IPSEC_EXT.1)

3.2　認証

情報の不正開示に関連する課題へのさらなる対処として、適合 TOE の認証能力（IPsec）が VPN ピアと別の VPN ピアとの VPN 接続の確立を可能とする。VPN エンドポイントは互いに認証を行って、正当な外部 IT エンティティと通信を行っていることを確実にする。

(O.AUTHENTICATION → FTP_ITC.1, FCS_IPSEC_EXT.1)

3.3　アドレスベースのフィルタリング

情報の不正開示、サービスへの不適切なアクセス、サービスの悪用、サービスの中断または拒否、及びネットワークベースの偵察に関連する課題に対処するため、適合 TOE はパケットフィルタリング能力を実装すること。この機能は、該当するネットワークトラフィックの発出元（送信元）または受信側（送信先）あるいはその両方のネットワークアドレスに加え、確立された接続情報に基づいて、保護ネットワークと他の接続されたネットワーク間のネットワークトラフィックのフローを制限することになる。

(O.ADDRESS_FILTERING → FPF_RUL_EXT.1)

3.4　セキュアでない操作

TOE のハードウェアが故障していたり、TOE のソフトウェアが危殆化したりする場合があるかもしれない。後者は、悪意によって行われる場合も、そうでない場合もある。TOE のハードウェアまたはソフトウェア仕様から逸脱した動作という懸念に対処するため、TOE はセルフテストメカニズムによって問題の発見が報告された際にはシャットダウンすること。

(O.FAIL_SECURE → FPT_FLS.1)

3.5 ポートベースのフィルタリング

情報の不正開示などに関連する課題へのさらなる対処として、ネットワークトラフィックにおいて識別された発出元（送信元）または受信側（送信先）あるいはその両方のネットワークポート（またはサービス）に加え、確立された接続情報に基づいて、保護ネットワークと他の接続されたネットワーク間のネットワークトラフィックのフローを適合 TOE のポートフィルタリング機能によって制限すること。

(O.PORT_FILTERING → FPF_RUL_EXT.1)

3.6 システム監視

管理者が VPN ゲートウェイの動作を監視できるようにするという課題に対処するため、NDPP に由来するこのセキュリティ対策方針は、以下のように拡張される。

適合 TOE は、ネットワークトラフィックのフローをログに記録する能力を実装すること。具体的には、ネットワークトラフィックが構成されたルールにマッチすることが判明した場合に「ログ」できるよう、管理者がパケットフィルタリングルールを構成する方法を TOE は提供すること。結果として、「ログ」するように構成されたルールへのマッチにより、マッチが生じた場合にはいつでも有益な事象ログが記録されるようにすること。さらに、セキュリティアソシエーション（SA）の確立は、ピア VPN ゲートウェイ間だけでなく、認証局（CA）との場合にも監査可能であること。

(O.SYSTEM_MONITORING → FAU_GEN.1, FPF_RUL_EXT.1)

3.7 TOE の管理

VPN ゲートウェイの管理に伴う課題に対処するため、NDPP に由来するこのセキュリティ対策方針は、以下のように拡張される。*下記の機能の利用は、NDPP 中の要件にしたがって保護されることが前提となっていることに注意されたい。*

管理者がパケットフィルタリングルールと共に、TOE によって強制される IPsec プロトコルの暗号化部分をも構成するために必要な機能を、適合 TOE は提供すること。

(O.TOE_ADMINISTRATION → FMT_SMF.1, FIA_AFL.1)

4　セキュリティ要件

このセクションでは TOE のセキュリティ機能要件を規定するとともに、評価者が実施する保証アクティビティも規定する。

4.1　表記

本 EP 中の SFR が拡張される際には、本 EP 及び他の EP、または PP でも使用できるよう柔軟に、またそのような操作が本 EP の文脈で実施されるよう定義される。

CC では、割付、選択、選択中の割付及び詳細化という、セキュリティ機能要件に関する操作を定義している。本文書では、以下のフォント規則を用いて、CC によって定義される操作を特定する。

- 割付：イタリック体のテキストで示す。
- EP 作成者によって行われた詳細化：太字テキスト、及び必要に応じて取り消し線で示す。
- 選択：下線付きテキストで示す。
- 選択中の割付：イタリック体の下線付きテキストで示す。
- 繰返し：例えば (1), (2), (3) など、繰返し回数をカッコ内に付記して示す。

4.2　TOE セキュリティ機能要件

NDPP 中に存在する SFR コンポーネントであって、本 EP で何らかの形の変更が必要とされるものは 8 つ存在する。新たに導入される SFR であって本 EP に含まれるものは 7 つ存在し、また 3 つの監査事象も規定されている。

4.2.1 NDPP セキュリティ機能要件の方向性

このセクションでは、VPN ゲートウェイ PP 中の関連する SFR をサポートするために、NDPP に含まれる特定の SFR にどの選択を行わなくてはならないかを ST 作成者に指示する。これは、強制的な選択が行われるエレメントを表明することによって行われる。ST 作成者は、残った選択項目を自分の望む通りに選んでよい。特定の機能またはふるまいが TOE に存在することを確実にするため、SFR エレメント中の選択も行われている。要求される必要な選択の提供以外にも、NDPP FPT_TST_EXT.1 コンポーネントが本 EP に適合するために追加しなくてはならないエレメント、FPT_TST_EXT.1.2 が存在する。

このセクションでは要件に関して保証アクティビティを繰り返すことはしない。これらはすでに NDPP に取り込まれているからである。ここで規定したように SFR に対して ST 及び TOE を評価する際に評価者にとって重要なことは、適切な選択が行われていること、及び適切なテストが実施され要件への適合性が例証されることである。

4.2.1.1.　FCS_CKM.1(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）。

- *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 [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）の実装については、NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”*
- *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”*
- [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 ビットの対称鍵強度と同等、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：本 EP は鍵確立に特定のアルゴリズムが用いられることを要求しており、また NDPP からの要件をこのように具体化することによって確実に正しい選択が行われる。

4.2.1.2. 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：本 EP 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。

4.2.1.3. 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*]**。

4.2.1.4. 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 Appendix C； AES を用いる X9.31 Appendix 2.4] にしたがい、TSF ハードウェアベースの雑音源及び [選択：ソフトウェアベースの雑音源、その他の独立した TSF ハードウェアベースの雑音源、その他の雑音源なし] 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）。

適用上の注意：NDPP は、雑音源がソフトウェアベースかハードウェアベースかの選択を ST 作成者に許可している。本 EP へ適合するためには、少なくとも 1 つのハードウェアベース雑音源が存在しなくてはならない（must）。

ハードウェア雑音源は、その物理的性質によって決定論的な規則で説明できないデータを作成するコンポーネントである。換言すれば、ハードウェアベースの雑音源は、予測できない物理的プロセスから乱数列を生成する。例えば、ループ状に接続された奇数のインバータゲートからなるリングオシレータをサンプリングすることが考えられる。ここで電気的パルスはインバータからインバータへ、ループを周回しながら伝播する。インバータにはクロックが与えられていないので、ループを周回するために必要な正確な時間は、さまざまな物理的効果によって各インバータから次に接続されたインバータへの遅延時間が変わるため、わずかに変動することになる。この変動が、概略固有振動数のまわりで時間とともにドリフトとジッタを引き起こす結果となる。この、バイナリ値を振動するリングオシレータの出力が、ひとつのインバータから一定周期（オシレータの固有周波数よりもはるかに遅い周期）でサンプリングされる。

同様に、正確かつ予測可能な規則では説明できない変動的なふるまいをするハードウェアコンポーネントであれば、ハードウェアベースの雑音源として用いることができる。また、少なくともひとつの雑音源がハードウェアベースである限り、複数の独立した雑音源を用いて発生するエントロピーを増大させ、攻撃の可能性を減少させる（攻撃者が複数のランダムビットストリームを攻略しなければならないため）ことも可能である。機械的な入出力デバイスやシステムカウンタによって引き起こされる割り込みのタイミングは、この要件においてはハードウェアベースの雑音源とはみなされないことに注意すべきである（should）。

エントロピーに関するさらに詳しい説明については、NDPP の附属書 D を参照されたい。

4.2.1.5. FMT_SMF.1 管理機能の仕様

FMT_SMF.1.1 TSF は、下記のセキュリティ管理機能を実施できなくてはならない（shall）。

- *暗号化機能を構成する能力、*
- *IPsec 機能を構成する能力、*
- 管理者が、本 EP において特定される TOE のすべてのセキュリティ機能のふるまいを有効化、無効化、決定、及び変更する能力、
- *本 EP 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。*

4.2.1.6. FPT_TUD_EXT.1 拡張：高信頼更新

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：NDPP は、ST 作成者が規定を望む検証手法のオプションを提供している。本 EP への適合のためには、デジタル署名メカニズム（FCS_COP.1(2) に規定されたものの 1 つ）が採用されなくてはならない（must）。

4.2.1.7. FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 詳細化：TSF は、IPsec 及び [選択：SSH、TLS、TLS/HTTPS、その他のプロトコルなし] を用いて、それ自身とすべての認可された IT エンティティ間に、他の通信チャネルとは論理的に別個の、確実な両エンドポイントの識別及び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、高信頼通信チャネルを提供しなくてはならない（shall）。

適用上の注意：NDPP は、IPsec 以外の高信頼チャネルを外部 IT エンティティとの通信に利用することを許可している。本 EP へ適合するため、管理者が構成可能なオプションとして TOE に IPsec が必ず提供されるように選択が行われている。

4.2.1.8. FPT_TST_EXT.1 拡張：TSF のテスト

FPT_TST_EXT.1.2 TSF は、FCS_COP.1(2) に指定された 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：NDPP には、このコンポーネントが 1 つ含まれている。それは、TSF の正しい動作を例証するセルフテストスイートを単純に要求する。EP へ適合するために、このエレメントがそのコンポーネントへ付け加えられている。

4.2.2 FCS_CKM.1 (2) 暗号鍵生成（非対称鍵）

FCS_CKM.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 スキームについては FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix B.3；
• ECDSA スキームについては FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix 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 スキームについはて ANSI X9.31-1998, Appendix A.2.4
]

また、規定された暗号鍵サイズは 112 ビットの対称鍵強度と同等、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すため、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 ピ

ア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 にはピア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。

4.2.3 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

ここに規定する一連の IPsec 要件は、NDPP に規定される IPsec 要件に優先する。

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）。

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）。

適用上の注意：本 EP の将来の版では、TSF にトンネルモードとトランスポートモードの両方の実装が求められることになる。

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）。

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）。

適用上の注意：AES-CBC の選択が行われた場合、SHA ベースの HMAC は NDPP FCS_COP.1(4) 暗号操作（鍵付きハッシュメッセージ認証）の要件に規定されるものと一貫していなくてはならない（must）。

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）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]。

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）。

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）。

適用上の注意：エレメント 1.7 は、IKEv1 が選択されている場合にのみ適用される。

FCS_IPSEC_EXT.1.8 TSF は、確実に [選択：IKEv2 SA ライフタイムを管理者がパケット数または経過時間に基づいて構成できフェーズ 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 ライフタイムを管理者がパケット数または経過時間に基づいて構成できフェーズ 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：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が望ましい。

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 Table 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）。

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 Table 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）。

FCS_IPSEC_EXT.1.11 TSF は、すべての IKE プロトコルが 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] を実装することを確実にしなくてはならない（shall）。

FCS_IPSEC_EXT.1.12 TSF は、すべての IKE プロトコルが 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*] を用いてピア認証を実施することを確実に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）。

4.2.4 FPF_RUL_EXT.1 パケットフィルタリング

FPF_RUL_EXT.1.1 TSF は、TOE によって処理されるネットワークパケットに対してパケットフィルタリングを実施できなくてはならない（shall）。

FPF_RUL_EXT.1.2 TSF は、下記のネットワークトラフィックプロトコルを処理できなくてはならない（shall）。

- インターネットプロトコル（IPv4）
- インターネットプロトコルバージョン 6（IPv6）
- 伝送制御プロトコル（TCP）
- ユーザデータグラムプロトコル（UDP）

また、本 SFR の他のエレメントに要求される範囲で、下記の RFC によって定義されるネットワークパケットヘッダフィールドを検査できなくてはならない。

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP)

適用上の注意：このエレメントは、TOE によって解釈可能なインポート（受信側ネットワークトラフィックまたは内向き）及びエクスポート（送信側（または送信のために形成される）ネットワークトラフィックもしくは外向き）ネットワークトラフィックの範囲を定義するために必要なプロトコル及びプロトコル定義への参照を特定している。

これらの RFC に規定されるプロトコルフォーマットはいまだに使用されている一方で、もはや安全ではないとみなされているふるまいが多くの RFC に定義されている。例えば、RFC792 には「リダイレクト」ICMP タイプが定義されているが、これは敵対者から送られてくるかもしれないので受け入れは安全とはみなされない。「ソースクエンチ」メッセージは、その送信元の検証が不可能であるため安全ではない。

FPF_RUL_EXT.1.3 TSF は、下記のネットワークプロトコルフィールドを用いたパケットフィルタリングルールの定義ができなくてはならない（shall）。

- IPv4
  - 送信元アドレス
  - 送信先アドレス
  - プロトコル
- IPv6
  - 送信元アドレス
  - 送信先アドレス
  - ネクストヘッダ（プロトコル）
- TCP
  - 送信元ポート
  - 送信先ポート
- UDP
  - 送信元ポート
  - 送信先ポート

及び、個別インタフェース。

適用上の注意：このエレメントには、本要件によって強制されるルールを構築する際に適用できるさまざまな属性が特定されている。適用インタフェースは TOE のプロパティであり、他の特定された属性は関連する RFC に定義されている。プロトコルは、TCP、UDP、ICMP などの適用プロトコルを特定する IPv4 のフィールドであることに注意（IPv6 ではこのフィールドは「ネクストヘッダ」と呼ばれる）。また上述の「インタフェース」は、当該ネットワークトラフィックが受信された、あるいは送信される予定の、外部ポートである。

FPF_RUL_EXT.1.4 TSF は、下記の操作をパケットトラフィックフィルタリングルールに関連付けることができなくてはならない（shall）：許可、拒否、及びログ。

適用上の注意：このエレメントは、ネットワークトラフィックとマッチするために使われるルールに関連付けられる操作を定義している。ログに記録されるデータはセキュリティ監査要件に特定されていることに注意されたい。セクション 4.2.9 を参照。

FPF_RUL_EXT.1.5 TSF は、個別ネットワークインタフェースのそれぞれに、パケットトラフィックフィルタリングルールを割り当てることができなくてはならない（shall）。

適用上の注意：このエレメントは、どこにルールを割り当てることができるかを特定している。具体的には、適合 TOE はその利用可能かつ特定可能な個別ネットワークインタフェースであって、レイヤ 3 及び 4 のネットワークトラフィックを処理するもののそれぞれに、固有のフィルタリングルールを割り当てることができなくてはならない（must）。特定可能とは、そのインタフェースが TOE 内で一意かつ特定可能であることを意味し、必ずしもインタフェースがネットワークの観点から可視であることは必要とされない（例えば、そのインタフェースに IP アドレスが割り当てられている必要はない）。個別ネットワークインタフェースとは、TOE への共通論理パスを共有する 1 つ以上の物理接続である。例えば、TOE には複数の物理ネットワークポートを公開する SFP モジュールをサポートした SFP ポートが存在するかもしれないが、すべての外部ポートに共通のドライバが利用されるため、これらは単一の個別ネットワークインタフェースとして取り扱うことができる。

各インタフェースには個別のルールセットが存在するかもしれないし、あるいは特定の複数インタフェースへ何らかの方法でルールを関連付ける共通ルールセットが存在するかもしれないことに注意されたい。

FPF_RUL_EXT.1.6 TSF は、該当する（FPF_RUL_EXT.1.5 にしたがって判定される）パケットフィルタリングルールを、以下の順序で処理しなくてはならない（shall）：管理者によって定義される順序。

適用上の注意：このエレメントは、構成されたフィルタリングルールのマッチが処理される順序を、管理者が定義可能であることを要求している。

FPF_RUL_EXT.1.7 TSF は、マッチングルールが特定されないパケットフローを拒否しなくてはならない（shall）。

適用上の注意：このエレメントは、どのルールも適用されなかった際のふるまいは常にネットワークトラフィックの拒否であることを要求している。

認証失敗の取り扱い（FIA_AFL）

4.2.5　FIA_AFL.1 認証失敗の取り扱い

FIA_AFL.1.1 **詳細化**：TSF は、**管理者のリモート認証の試み**に関連して発生した認証試行の不成功の**連続**回数が、**管理者によって構成可能な正の整数**に達したことを検出できなくてはならない（shall）。

FIA_AFL.1.2 認証試行の不成功の回数が定義された数に**達した**場合、TSF は [選択、1 つを選択：ローカル管理者によって [割付：アクション] が取られるまで問題のリモート管理者の認証成功を防止；管理者によって定義される時間が経過するまで問題のリモート管理者の認証成功を防止] しなくてはならない（shall）。

適用上の注意：この要件は、ローカルコンソール上の管理者には適用されない。このような形でローカル管理者のアカウントをロックすることは意味をなさないからである。これは、（例えば）ローカル管理者には別のアカウントを必要とすることによって、またはローカルとリモートのログイン試行を区別する認証メカニズムを実装することによって対処可能であろう。ローカル管理者によって取られる「アクション」は実装固有であり、管理者ガイダンスに定義されるであろう（例えば、ロックアウトリセットまたはパスワードリセ

ット）。ST 作成者は、TOE がこのハンドラをどう実装しているかによって、認証失敗の取り扱いに関する選択の 1 つを選択する。

4.2.6　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 及び [選択：その他のプロトコルなし、TLS、SSH] 接続の認証をサポートしなくてはならない（shall）。

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）。

FIA_X509_EXT.1.3 TSF は、本 PP に規定されるセキュリティ機能が使用するため、認証済み管理者が X.509v3 証明書を 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 で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.1.5 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）。

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 EP 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要とされることになる。

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）。

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るかネットワークパスが切断されているために 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。

4.2.7 FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1.1 **詳細化**：TSF は、本 EP に特定されるすべてのセキュリティ機能のふるまいを有効化、無効化、決定、及び変更できる能力を、認証された管理者に制約することができなくてはならない（shall）。

4.2.8 FPT_FLS.1 フェイルセキュア

FPT_FLS.1.1 **詳細化**：TSF は、以下の種類の失敗が発生した際に**シャットダウン**しなくてはならない（shall）：電源投入時セルフテストの失敗、TSF 実行可能形式イメージの完全性チェックの失敗、雑音源ヘルステストの失敗。

適用上の注意：この要件に関連する失敗は、NDPP 中の FPT_TST_EXT.1.1 要件、及び本 EP 中に規定される FPT_TST_EXT.1.2 要件である。

4.2.9 セキュリティ監査

これ以外のセキュリティ監査に関する SFR は存在しないが、NDPP に見出される FAU_GEN.1 SFR を拡張するための追加監査対象事象は存在する。それゆえ、適合セキュリティターゲットの文脈において下記の事象は NDPP の事象と結合されるべきである（should）。

下記の監査事象が、本 EP に必要とされる。

4-1 FAU_GEN.1 監査事象及び詳細

要件	監査対象事象	追加監査記録の内容
FCS_IPSEC_EXT.1	ピアによるセッション確立	送信元及び送信先アドレス 送信元及び送信先ポート TOE インタフェース
FIA_X509_EXT.1	CA によるセッション確立	送信元及び送信先アドレス 送信元及び送信先ポート TOE インタフェース
FPF_RUL_EXT.1	「ログ」操作と共に構成されたルールの適用	送信元及び送信先アドレス 送信元及び送信先ポート トランスポート層プロトコル TOE インタフェース
	過大なネットワークトラフィックのためパケットが損失した通知	パケットを処理できなかった TOE インタフェース

適用上の注意：セッション確立に関しては、TOE がセッションの確立に関連したすべてのパケットを監査できることが期待される。これには IKE フェーズ 1 及びフェーズ 2 のネゴシエーションが含まれるであろう。TOE は、成功したセッションの確立中のすべてのパケットをログに記録でき、また損失または破棄されたあらゆるパケットをログに記録できなくてはならない（must）。

5　保証アクティビティ

このセクションは、本 EP 中に含まれる SFR に関連した保証アクティビティで構成されている。保証アクティビティは、関連する CC コンポーネントに応じてグループ分けされている。

保証アクティビティの意図は、ST の TOE 要約仕様（TSS）に必要とされる内容、TOE の操作ガイダンスに必要とされる内容、及び評価者によって独立して実施されることが必要とされるテストアクティビティへ対応することである。

評価者には、セッションの確立、セッションパケットの変更または作成、及びパケットが TOE を通過しているかどうかと、それらのパケットの内容の調査を行うために適切なツールを有することが想定されている。一般的には、必要に応じて TOE のパケットフィルタリングルールの構成及びロギング機能を用いて適切な判定に至ることが期待される。

以下に示すテストは、個別ネットワークインタフェース種別のそれぞれについて、繰り返される必要がある。インタフェース種別の定義（すべてのパケットが TOE 内の同一の論理パスを通して処理される）を考慮して、パケットが TOE を通過する可能性のあるすべての論理パスが本 EP に規定されたセキュリティ方針を遵守していることをテストによって確証することが必要である。

評価者は最低限、以下に示す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）。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）。

5.1.1　FCS_CKM.1 暗号鍵生成（非対称鍵）

FCS_CKM.1.1

TSS

1　行われた選択に応じて TSF が 800-56A 及び 800-56B（選択による）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 に記述されていなくてはならない（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 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）。

ガイダンス

評価者は、操作ガイダンスに鍵生成機能が呼び出される方法が記述されているか、またサポートされている署名スキームのそれぞれについてそのプロセスに関連する入力及び出力が記述されているかをチェックしなくてはならない（shall）。また評価者は、鍵生成処理の出力のフォーマット及び場所に関して、ガイダンスが提供されていることをチェックしなくてはならない（shall）。

テスト

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 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。

FCS_CKM.1.2

TSS

評価者は、TSS が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 に記述されていなくてはならない（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）。

ガイダンス

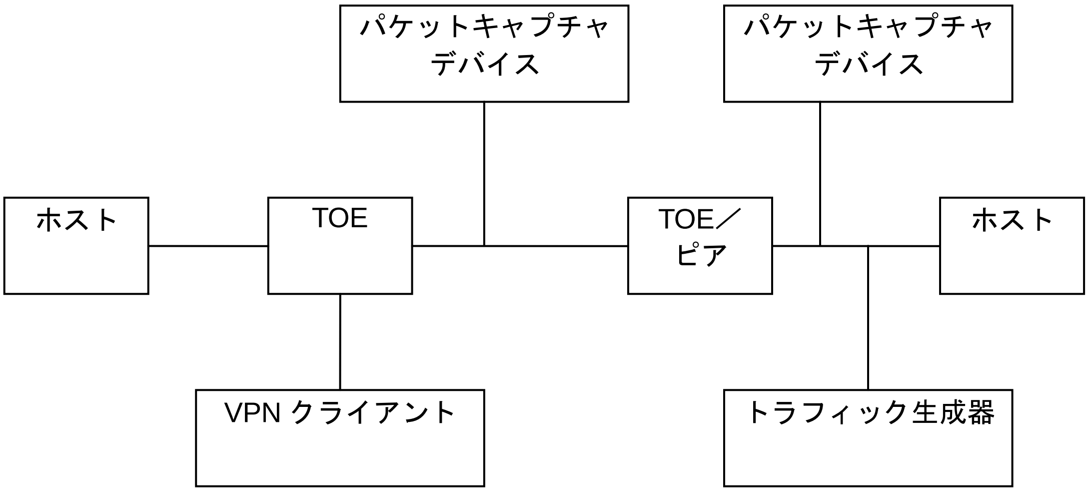
評価者は、操作ガイダンスに鍵生成機能が呼び出される方法が記述されているか、またサポートされている署名スキームのそれぞれについてそのプロセスに関連する入力及び出力が記述されているかをチェックしなくてはならない（shall）。また評価者は、鍵生成処理の出力のフォーマット及び場所に関して、ガイダンスが提供されていることをチェックしなくてはならない（shall）。

テスト

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。

5.1.2　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

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 EP 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。



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）。TOE の 2 つの実体を用いれば、おそらくテストの実施が容易となるし、テストが失敗した場合に TOE への追跡が容易となるはずである。しかし、TOE の 1 つの実体と、テストアクティビティを満たすために TOE と交信するための必要な機能を提供する 1 台のデバイスとが存在するテストベッドを構築するのも評価者の自由である。ST 作成者が VPN ヘッドエンドの要件を追加した場合には、TOE がリモートアクセス VPN ヘッドエンドとしてふるまえることを例証するとともに、VPN クライアント管理に関して規定された要件を例証するために VPN クライアントを用いることが期待される。ネットワークパケットの作成と、評価者が 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）。そのような正当化のひとつの例として、トラフィック生成器をホスト上に実装することが考えられる。評価者が実際に伝送路上のパケットへアクセスできることが期待されるため、パケットキャプチャデバイスに関して同様の議論を行うことは困難であろう。

FCS_IPSEC_EXT.1.1

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、以下のテストを行う。

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

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 をトンネルモードに構成し、また TOE ピアをトンネルモードに構成する。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 2 つのピア TOE 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、ピア間のセッションを開始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、VPN クライアントからパケットを受け取った際に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 クライアントを構成し、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、VPN クライアントを用いて TOE とのコネクションを開始する。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

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

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、TOE で AES-GCM-128 及び AES-GCM-256 アルゴリズムを使用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 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 を機密性及び完全性モードで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 を機密性及び完全性モードで使用した接続の確立を試行する。

FCS_IPSEC_EXT.1.5

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

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

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

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。TOE は、送信されたバイト数に基づいてライフタイムを制限してもよく、これは受容可能であろう。

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, FCS_IPSEC_EXT.1.10

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

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：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

TSS

評価者は、RSA または ECDSA あるいはその両方がピア認証を実施する際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）。

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 5 つのテストは、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 及び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、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 5：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 6：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。

テスト 7：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 8：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。

FCS_IPSEC_EXT.1.13

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各アルゴリズム、及び要件中に特定されたハッシュ関数を用いて 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）。

5.1.3 FPF_RUL_EXT.1 拡張：パケットフィルタリング

FPF_RUL_EXT.1.1

TSS

評価者は、TOE の初期化／スタートアッププロセスの記述が TSS に提供されており、そこにはネットワークパケットの処理がどこで開始されるかが明示されており、またこのプロセス中にはパケットが流れないという主張をサポートする論拠が提供されていることを検証しなくてはならない（shall）。

評価者は、ネットワークパケットの処理に関与するコンポーネント（例えば、プロセスやタスクなどのアクティブなエンティティ）を特定するとともに、コンポーネントが故障の場合にもパケットがルールセットを適用されずに TOE を通過して流れることのないような保護手段を記述する説明文が TSS に含まれていることも検証しなくてはならない（shall）。これには、例えばプロセスの終了などのコンポーネント自体の障害、またはメモリバッファがフルのためパケットを処理できないなどのコンポーネント内部の障害が含まれるかもしれない。

ガイダンス

この要件に関連した操作ガイダンスは、以下のテスト保証アクティビティで評価される。

テスト

テスト 1：評価者は、TOE が初期化している最中に TOE を通過してネットワークトラフィックを流すことを試さなくてはならない（shall）。初期化中でなければルールセットによって拒否されるはずのネットワークパケットを定常的に TOE のインタフェースへ向けて流しながら、パケットスニファを接続してリッスンさせ、ネットワークトラフィックが通過できているかどうかを判断すべきである（should）。

注：ルールセットの適用に関連する残りのテストは、以下のテスト保証アクティビティにおいて行われる。

FPF_RUL_EXT.1.2

TSS

評価者は、下記のプロトコルがサポートされているとの記載が TSS にあることを検証しなくてはならない（shall）。

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP)

評価者は、特定された RFC への適合性が TOE の開発者によって判定される方法（例えば、第三者による相互運用性テスト、プロトコル適合性テスト）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、下記のプロトコルがサポートされているとの記載が操作ガイダンスにあることを検証しなくてはならない（shall）。

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP)

TOE によって処理される、ST 中に含まれるその他のプロトコル（例えば IPsec、IKE、可能性としては HTTPS、SSH、及び TLS）がガイダンスに記述されていること。評価者は、どのプロトコルが TOE 評価の一部とはみなされないか明確になっていることを確証する。

テスト

この要件に関連したテストは、以下のテスト保証アクティビティによって行われる。

FPF_RUL_EXT.1.3/FPF_RUL_EXT.1.4/FPF_RUL_EXT.1.5

TSS

評価者は、パケットフィルタリング方針及び下記の属性が TSS に記述されていることを検証しなくてはならない（shall）。

- IPv4
  - 送信元アドレス
  - 送信先アドレス
  - プロトコル
- IPv6
  - 送信元アドレス
  - 送信先アドレス
  - ネクストヘッダ（プロトコル）
- TCP
  - 送信元ポート

- 送信先ポート

- UDP
  - 送信元ポート
  - 送信先ポート

評価者は、各ルールが以下のアクションを特定できることを検証しなくてはならない（shall）: 許可、拒否、及びログ。

評価者は、パケットフィルタリング方針の対象となるすべてのインタフェース種別が TSS に特定され、また個別ネットワークインタフェースにルールが関連付けられる方法が説明されていることを検証しなくてはならない（shall)。インタフェースが共通のインタフェース種別（例えば、同一の内部論理パスが用いられる場合、あるいは共通のデバイスドライバが用いられる場合）にグループ分けできる場合には、それらを一括して 1 つの個別ネットワークインタフェースとして取り扱うことができる。

ガイダンス

評価者は、関連するプロトコルのパケットフィルタリングルール内で下記の属性が構成可能であると操作ガイダンスに特定されていることを検証しなくてはならない（shall)。

- IPv4
  - 送信元アドレス
  - 送信先アドレス
  - プロトコル
- IPv6
  - 送信元アドレス
  - 送信先アドレス
  - ネクストヘッダ（プロトコル）
- TCP
  - 送信元ポート
  - 送信先ポート
- UDP
  - 送信元ポート
  - 送信先ポート

評価者は、各ルールに以下のアクションを特定できることが操作ガイダンスに示されていることを検証しなくてはならない（shall）: 許可、拒否、及びログ。

評価者は、個別ネットワークインタフェースにルールが関連付けられる方法が操作ガイダンスに説明されていることを検証しなくてはならない（shall)。

評価者は、個別ネットワークインタフェースのインタフェース種別を判定する方法（例えば、個別ネットワークインタフェースのデバイスドライバを判定する方法）が操作ガイダンスに説明されていることを検証しなくてはならない（shall)。

テスト

テスト 1 : 評価者は操作ガイダンスの指示を用いて、下記の属性のそれぞれについてパケットを許可、拒否、及びログするパケットフィルタルールが作成できることをテストしなくてはならない（shall)。

- IPv4
  - 送信元アドレス
  - 送信先アドレス
  - プロトコル
- IPv6
  - 送信元アドレス

    - 送信先アドレス
    - ネクストヘッダ（プロトコル）
- TCP
    - 送信元ポート
    - 送信先ポート
- UDP
    - 送信元ポート
    - 送信先ポート

テスト 2：上記のテスト保証アクティビティを繰り返して、TOE のサポートする個別ネットワークインタフェース種別のそれぞれについてパケットフィルタリングルールが定義できることを確証する。

これらのテストアクティビティは、ルールの実効性がテストされる FPF_RUL_EXT.1.7 のテストと組み合わせて実施されるべきである（should）ことに注意されたい。ここで評価者が確証することは、十分なガイダンスが提供されており、TOE が管理者による上記の属性に基づいたルールセットの作成をサポートしていることだけである。FPF_RUL_EXT.1.7 のテストアクティビティは、テストされる必要のあるプロトコル／属性の組み合わせを定義している。これらの組み合わせを手作業で構成してもこれらのテストアクティビティの目的は達成されることになるが、これらの組み合わせを別の方法で構成する（例えば自動化することによって）場合には、ガイダンスが正しいことと TOE 管理者によって全範囲の構成が達成できることを確証するためにこれらのテストアクティビティが必要となるかもしれない。

FPF_RUL_EXT.1.6

TSS

評価者は、デフォルトルール、確立されたセッションにパケットが属するかどうかの判定、及び管理者によって定義され順序づけられたルールセットの適用などを含めた、着信するパケットに適用されるアルゴリズムが 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、パケットフィルタリングルールの順序がどのように決まるかが操作ガイダンスに記述され、管理者がルール処理の順序を構成できるように必要な指示が提供されていることを検証しなくてはならない（shall）。

テスト

テスト 1：評価者は、許可と拒否という別の操作を行う、2 つの同一のパケットフィルタリングルールを作り上げなくてはならない（shall）。これらのルールは次に 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ルールが適用されることを確証しなくてはならない（shall）。

テスト 2：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 つのルール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）。

FPF_RUL_EXT.1.7

TSS

評価者は、パケットフィルタリングルールの適用プロセスと、別の必要条件によってネットワークトラフィックが許可されない限りにおいてどのルールもマッチしない場合のふるまい（デフォルトまたは管理者によって構成されたもののいずれか）がパケットの拒否（すなわち、FPF_RUL_EXT.1.6 または FPF_RUL_EXT.1.7）であることが、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、ネットワークトラフィックにルールや特別な条件が適用されない場合のふるまいが、操作ガイダンスに記述されていることを検証しなくてはならない（shall）。そのふるまいが構成可能な場合には、マッチするルールがない場合のふるまいをパケットの拒否に構成するための適切な指示が操作ガイダンスに提供されていることを、評価者は検証しなくてはならない（shall）。

テスト

テスト 1 : 評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの組み合わせと共に、定義済みの IPv4 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを許可しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが許可され（すなわち、パケットが TOE を通過した後キャプチャされ）ログに記録されるように、定義済みの IPv4 トランスポート層プロトコルのそれぞれにマッチする、設定された送信元及び送信先アドレスの範囲内のパケットを生成しなくてはならない（shall）。

テスト 2 : 評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの組み合わせと共に、定義済みの IPv4 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを拒否しログに記録するように、またそれ以外のすべてのトラフィックを許可するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが拒否され（すなわち、該当するどのパケットも TOE を通過してキャプチャされず）ログに記録されるように、定義済みの IPv4 トランスポート層プロトコルのそれぞれにマッチする、設定された送信元及び送信先アドレスの範囲内のパケットを生成しなくてはならない（shall）。

テスト 3 : 評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの組み合わせと共に、定義済みの IPv4 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを許可しログに記録するように、TOE を構成しなくてはならない（shall）。さらに評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの（上記で許可されたものとは）異なる組み合わせと共に、定義済みの IPv4 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを拒否しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが拒否され（すなわち、該当するどのパケットも TOE を通過してキャプチャされず）ログに記録されるように、定義済みの IPv4 トランスポート層プロトコルのそれぞれにマッチする、上記で設定されたすべての送信元及び送信先アドレスの範囲外のパケットを生成しなくてはならない（shall）。

テスト 4 : 評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アド

レス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの組み合わせと共に、定義済みの IPv6 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを許可しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが許可され（すなわち、パケットが TOE を通過した後キャプチャされ）ログに記録されるように、定義済みの IPv6 トランスポート層プロトコルのそれぞれにマッチする、設定された送信元及び送信先アドレスの範囲内のパケットを生成しなくてはならない（shall）。

テスト 5 : 評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの組み合わせと共に、定義済みの IPv6 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを拒否しログに記録するように、またそれ以外のすべてのトラフィックを許可するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが拒否され（すなわち、該当するどのパケットも TOE を通過してキャプチャされず）ログに記録されるように、定義済みの IPv6 トランスポート層プロトコルのそれぞれにマッチする、設定された送信元及び送信先アドレスの範囲内のパケットを生成しなくてはならない（shall）。

テスト 6 : 評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの組み合わせと共に、定義済みの IPv6 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを許可しログに記録するように、TOE を構成しなくてはならない（shall）。さらに評価者は、特定の送信元アドレス及び特定の送信先アドレス、特定の送信元アドレス及びワイルドカード送信先アドレス、ワイルドカードソースアドレス及び特定の送信先アドレス、及びワイルドカード送信元アドレス及びワイルドカード送信先アドレスの（上記で許可されたものとは）異なる組み合わせと共に、定義済みの IPv6 トランスポート層プロトコル（表 9-1 定義済みのプロトコル固有値を参照）のそれぞれを拒否しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが拒否される（すなわち、該当するどのパケットも TOE を通過してキャプチャされない）ように、定義済みの IPv6 トランスポート層プロトコルのそれぞれにマッチする、設定された送信元及び送信先アドレスの範囲外のパケットを生成しなくてはならない（shall）。

テスト 7 : 評価者は、選択した送信元ポート、選択した送信先ポート、及び選択した送信元及び送信先ポートの組み合わせを用いて、プロトコル 6（TCP）を許可しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが許可され（すなわち、パケットが TOE を通過した後キャプチャされ）ログに記録されるように、設定された TCP ポートにマッチするパケットを生成しなくてはならない（shall）。

テスト 8 : 評価者は、選択した送信元ポート、選択した送信先ポート、及び選択した送信元及び送信先ポートの組み合わせを用いて、プロトコル 6（TCP）を拒否しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが拒否され（すなわち、該当するどのパケットも TOE を通過してキャプチャされず）ログに記録されるように、設定された TCP ポートにマッチするパケットを生成しなくてはならない（shall）。

テスト 9 : 評価者は、選択した送信元ポート、選択した送信先ポート、及び選択した送信元及び送信先ポートの組み合わせを用いて、プロトコル 17（UDP）を許可しログに記録するように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが許可され（すなわち、パケットが TOE を通過した後キャプチャされ）ログに記録されるように、設定された UDP ポートにマッチするパケットを生成しなくてはならない（shall）。ここで評価者は、UDP ポート 500（IKE）が一連のテストに確実に含まれるようにする。

テスト 10 : 評価者は、選択した送信元ポート、選択した送信先ポート、及び選択した送信元及び送信先ポートの組み合わせを用いて、プロトコル 17（UDP）を拒否しログに記録す

るように、TOE を構成しなくてはならない（shall）。評価者は、確実にパケットが拒否され（すなわち、該当するどのパケットも TOE を通過してキャプチャされず）ログに記録されるように、設定された UDP ポートにマッチするパケットを生成しなくてはならない（shall）。ここでもまた評価者は、UDP ポート 500 が一連のテストに確実に含まれるようにする。

5.1.4 FIA_AFL.1 認証失敗の取り扱い

TSS

管理者は TSS を調査して、サポートされているリモート管理アクション手法のそれぞれについて、連続する不成功の認証試行を検出し追跡する方法が含まれていることを判定しなくてはならない（shall）。また TSS には、リモート管理者に TOE へのログオンを成功させないための手法について、またこの機能を回復するために必要なアクションについて、記述されていなくてはならない（shall）。

ガイダンス

また評価者は操作ガイダンスを調査して、連続する不成功の認証試行の回数（1.1）及び時間間隔 (1.2、実装されている場合）を構成するための指示が提供されていること、及びリモート管理者に再びログオンの成功を許可するプロセスが、規定される「アクション」ごとに記述されていること（そのオプションが選択されている場合）を確証しなくてはならない（shall）。採用されているセキュアなプロトコル（例えば、TLS や SSH）に応じて異なるアクションまたはメカニズムが実装されている場合には、すべてが記述されなくてはならない（must）。

テスト

評価者は IPsec について、及び TOE へリモート管理者がアクセスするための他の手法（例えば TLS、SSH）のそれぞれについて、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を用いて、TOE が許可する連続する不成功の認証試行の回数を構成しなくてはならない（shall）。評価者は、その制限に達すると有効な資格情報を用いた試行が成功しないことをテストしなくてはならない（shall）。要件に規定されたアクションのそれぞれについて、操作ガイダンスにしたがってリモート管理者のアクセスを許可するためのそれぞれのアクションの実施が成功することを、評価者は示さなくてはならない（shall）。

テスト 2：評価者は操作ガイダンスを用いて、TOE の許可する連続する不成功の認証試行の回数及びリモート管理者の有効なログインが許可されるまでの時間間隔を構成しなくてはならない（shall）。指定された回数の不正なログイン試行を越えて有効なログインが不可能となったことを示した後に、評価者は時間間隔によって定義される期間だけ待機してからもう一度アクセス試行を行えば、リモート管理者の有効な資格情報を用いたログインを成功させる結果となることを示さなくてはならない（shall）。

5.1.5 FIA_X509_EXT.1 拡張：X.509 証明書

TSS

TSS には、本 EP 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）。また TSS の記述には、TOE が標準での規定により認証パスを形成する方法、及び証明書が検証される方法についての論拠（CRL または OCSP あるいはその両方が、認証パス検証アルゴリズムと共に論拠に含まれる）が含まれること。

ガイダンス

評価者は、管理者が証明書を証明書ストアへロードする方法が操作ガイダンスに記述されていることを検証しなくてはならない（shall）。保護のレベルが管理者によって管理できる場合、ガイダンスには保護メカニズムを管理する方法が記述される。ガイダンスは管理者

に、鍵ペアの生成方法と CA への証明書要求メッセージの生成方法を指示する。

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。

TOE が SA の確立を許可するか、または許可しないかを管理者が構成する方法も、操作ガイダンスに記述される。

テスト

このコンポーネントに関連するテストは、FCS_IPSEC_EXT.1.12 要件にまとめられている。

5.1.6 FMT_SMF.1 管理機能の仕様

TSS

評価者は、パケットフィルタファイアウォールルールの構成方法が TSS に記述されていることを検証しなくてはならない（shall）。このアクティビティは、FPF_RUL_EXT.1 の TSS 保証アクティビティで対処されているべきことに注意されたい。

ガイダンス

評価者は、パケットフィルタファイアウォールルールの構成方法が操作ガイダンスに記述されていることを検証しなくてはならない（shall）。これには、構成可能なデフォルトがあればその設定方法、及び該当するルールの属性、アクション、及び関連するインタフェースのそれぞれを構成する方法が含まれる。評価者は、構成されたルールが適切に順序付けられていることを管理者が確証できるような指示が、操作ガイダンスに提供されていることも確証しなくてはならない（must）。このアクティビティは、FPF_RUL_EXT.1 のガイダンス保証アクティビティで対処されているべきことに注意されたい。

テスト

テスト 1 : 評価者は、パケットフィルタファイアウォールルールを構成するために用いられる機能によって期待される変化がルールに生じ、それが正しく適用されることを例証するテストを考え出さなくてはならない（shall）。多数のルールの組み合わせ及び順序付けのシナリオが構成され、有効なネットワークトラフィック及び無効なネットワークトラフィックの両方を TOE に通過させようと試みることによってテストされる必要がある。このアクティビティは、FPF_RUL_EXT.1 のテスト保証アクティビティの組み合わせで対処されているべきことに注意されたい。

5.1.7 FPT_FLS.1 フェイルセキュア

TSS

評価者は、セルフテストの失敗、TSF 実行可能形式イメージの完全性チェックの失敗、または雑音源のヘルステストの失敗が生じた際に TOE が確実にシャットダウンする方法が TSS に記述されていることを確証しなくてはならない（shall）。例えばセキュリティに影響しないとみなされる故障など、シャットダウンが発生しない場合が存在するならば、それらの場合を特定し、その場合分けと TOE のセキュリティ方針を強制する能力が影響されない理由の正当化とを支持する根拠（が提供されなくてはならない）。

5.1.8 FAU_GEN.1 監査事象及び詳細

以下に、FAU_GEN.1 への適合性を確証するために評価者によって実施されるべき保証アクティビティが定義されている。

TSS

評価者は、該当するルールと関連付けられたネットワークトラフィックをログに記録するようにパケットフィルタファイアウォールルールを構成する方法が TSS に記述されていることを検証しなくてはならない（shall）。このアクティビティは、FPF_RUL_EXT.1 の TSS 保証アクティビティの組み合わせで対処されているべきことに注意されたい。

評価者は、TOE のネットワークインタフェースの 1 つがネットワークトラフィックによって飽和させられた際に TOE がどのような挙動を示すかが TSS に記述されていることを検証しなくてはならない（shall）。TOE が処理できないパケットを損失することは許容可能であるが、いかなる状況下であっても TOE が、許可操作が適用されるルールを満たさず、許可された確立済みのセッションにも属さないパケットを通過させることは許可されない。実装の制限により、TOE が損失したパケットを監査することは常に可能とは限らない。損失したパケットが監査されないような、これらの制限及び状況は、TSS に記述されなくてはならない（shall）。

ガイダンス

評価者は、該当するネットワークトラフィックのロギングを行わせるためのパケットフィルタファイアウォールルールの構成方法が操作ガイダンスに記述されていることを検証しなくてはならない（shall）。このアクティビティは、FPF_RUL_EXT.1 のガイダンス保証アクティビティの組み合わせで対処されているべきことに注意されたい。

テスト

下記のテストは､他の要件の文脈とは切り離して実行することが求められる｡SFR への TOE の適合性を試験する際には､この SFR の文脈で特定のテストが開発され実行される以外は､通常通り監査機能をオンにして TOE のふるまいが本 EP の他の SFR に準拠していることをテストすることになる。

テスト 1：評価者は、TOE がすべてのパケットを処理できなくなるようにネットワークパケットで TOE を飽和させようと試みなくてはならない（shall）。これには、TOE が処理できる帯域幅を制限するよう、評価者が TOE を構成することが必要となるかもしれない（例えば、10 MB のインタフェースの使用）。

5.2 セキュリティ保証要件

本 EP に対して評価される TOE は、本質的に NDPP に対しても評価されることに注意しなくてはならない。NDPP には、セキュリティ機能要件（SFR）及び SAR の双方に関連する数多くの保証アクティビティが含まれている。それに加えて、本 EP には NDPP に特定された EAL に関連付けられた SAR を同様に詳細化する、SFR ベースの保証アクティビティが多数含まれている。NDPP が規定する SAR に関連付けられた保証アクティビティは TOE 全体に対して実施され、ここに記述された特定の脆弱性テストが追加される。

5.2.1 AVA_VAN.1 脆弱性調査

保証アクティビティ：

評価者は、ICMPv4、ICMPv6、IPv4、及び IPv6 プロトコルのそれぞれについて、RFC に未定義となっている属性、タイプ（Type）、コード（Code）、及びトランスポート層プロトコルのすべての値を順番に取るネットワークパケットを生成しなくてはならない（shall）。例えば、ICMPv4 には 8 ビットのタイプフィールドと 8 ビットのコードフィールドがある。RFC には 21 種類のタイプしか定義されていない（表 4-2 を参照）が、取り得る値は 256 種類存在する。各タイプにはコードが関連付けられており、RFC で定義されるコードの数はタイプによって異なる。評価者には、タイプ及びコード（可能な組み合わせをすべて含む）の取り得る RFC で未定義の値をすべて取るようにパケット（定義済みの値はすでに FPF_RUL_EXT.1.10 においてテストされている）を構築して、個別インタフェース種別のそれぞれへ向けて送信し、TOE がこれらのパケットを適切に処理するかどうかを判定することが要求される。これらのパケットはどれもルールにはマッチせず、許可されたセッシ

ョンにも属さないので、パケットは損失されるはずである（should）。これらの状況下で損失されるパケットのファイアウォールによる監査に関しては要件が存在しないため、評価者はファイアウォールがこれらのパケットに TOE の通過を許可しないことを確証しなくてはならない（shall）。

上記で必要とされる未定義属性のテストに加えて、評価者は必要とされるプロトコルヘッダ中の残りのフィールド（FTP を除く）のインテリジェントファズテストを実施しなくてはならない（shall）。インテリジェントファズの意図は、ルールセットが適用された際に拒否されるように、パケットの各プロトコルヘッダフィールドにランダムな値を持たせることである（それ以外の点ではパケットは正しく構築される）。評価者は統計的に有意なサンプルサイズ（これはプロトコルフィールドの長さによって異なる）が用いられ、それがレポートの中で正当化されていることを確証する。

評価者は、TOE が提供する診断情報（例えばロギング、プロセスの状態、インタフェースのエラー）をすべて参照して、そのようなパケットの処理によって TOE が悪影響を受けているかどうかを判定すべきである（should）。

6　根拠

本 EP において、この文書の最初のセクションでは主に説明文による提示により、IPsec VPN ゲートウェイによって対処される脅威、これらの脅威を低減するために用いられる手法、及び適合 TOE によって達成される低減の程度について、全体的にわかりやすく説明しようと試みた。この提示のスタイルはそのまま形式化された評価アクティビティには適用できないため、このセクションでは表形式のアーティファクトを用いて、この文書に関連付けられる評価アクティビティを説明する。

6.1　セキュリティ課題定義

6.1.1　前提条件

以下に列挙する特定の条件が、TOE の運用環境に存在することが前提となる。これらの前提条件は NDPP に定義されたものに付け加えられるものであり、TOE セキュリティ要件の開発における実質的な事実と、TOE の使用にあたって必須となる環境条件の両方が含まれる。

6-1 TOE の前提条件

前提条件名	前提条件の定義
A.CONNECTIONS	TOE は、接続されたネットワーク間に流れるすべての該当するネットワークトラフィックへ TOE セキュリティ方針が確実に強制されるように、別個のネットワークへ接続されていることが前提とされる。

6.1.2　脅威

以下に列挙する脅威が、VPN ゲートウェイによって対処される。これらの脅威は、NDPP に定義されたものに付け加えられるものであり、そのすべてが VPN ゲートウェイに適用されることに注意されたい。

6-2 脅威

脅威名	脅威の定義
T.NETWORK_DISCLOSURE	保護ネットワーク上の機密性のある情報が、内向きまたは外向きのアクションによって開示されるおそれがある。
T. NETWORK_ACCESS	保護ネットワーク上のサービスへそのネットワーク外部から、または逆に保護ネットワーク外部のサービスへ保護ネットワーク内部から、不正アクセスが行われるおそれがある。
T.NETWORK_MISUSE	保護ネットワークによって利用可能とされているサービスへのアクセスが、運用環境方針に反して利用されるおそれがある。
T.TSF_FAILURE	TOE のセキュリティメカニズムが不具合を起こし、TSF の危殆化をもたらす恐れがある。
T.REPLAY_ATTACK	悪意のある、または外部の IT エンティティがネットワークへのアクセスを得た場合、ネットワーク全体を通過する情報をキャプチャし、意図された受信者へ送信する能力をそのエンティティが有しているおそれがある。
T.DATA_INTEGRITY	送信されようとしているデータを悪意のある人物が改変しようとし、完全性が失われる結果となる。

6.1.3　組織のセキュリティ方針

VPN ゲートウェイに特有な組織のセキュリティ方針は特定されていない。しかし、NDPP 中の組織のセキュリティ方針はすべて、VPN ゲートウェイに適用される。

6.1.4　セキュリティ課題と定義の対応

以下の表は、本 EP に定義される脅威及び前提条件を、やはり本 EP に定義または特定されるセキュリティ対策方針へ対応付けるためのものである。

6-3 セキュリティ課題と定義の対応

脅威または前提条件	セキュリティ対策方針
A.CONNECTIONS	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.ADDRESS_FILTERING 及び O.PORT_FILTERING
T. NETWORK_ACCESS	O.ADDRESS_FILTERING、O.RELATED_CONNECTION_FILTERING 及び O.PORT_FILTERING
T.NETWORK_MISUSE	O.ADDRESS_FILTERING、O.PORT_FILTERING 及び O.SYSTEM_MONITORING
T.TSF_FAILURE	O.FAIL_SECURE
T.REPLAY_ATTACK	O.CRYPTOGRAPHIC_FUNCTIONS
T.DATA_INTEGRITY	O.CRYPTOGRAPHIC_FUNCTIONS

6.2　セキュリティ対策方針

6.2.1　TOE のセキュリティ対策方針

以下の表には、VPN ゲートウェイに特有のセキュリティ対策方針が含まれている。これらのセキュリティ対策方針は NDPP に定義されたものに付け加えられるものであり、そのすべてが VPN ゲートウェイに適用される。NDPP セキュリティ対策方針のうち 2 つ（O.SYSTEM_MONITORING 及び O.TOE_ADMINISTRATION）が本 EP において拡張されている一方で、これが対応するセキュリティ対策方針の定義には影響していないことに注意されたい。

6-4 TOE のセキュリティ対策方針

セキュリティ対策方針名	セキュリティ対策方針の定義
O.ADDRESS_FILTERING	TOE は、送信元及び送信先アドレスに基づいてネットワークパケットをフィルタしログに記録する手段を提供すること。
O.AUTHENTICATION	TOE は、ユーザを認証して正当な外部 IT エンティティと通信していることを確証する手段を提供すること。
O.CRYPTOGRAPHIC_FUNCTIONS	TOE は、機密性を維持し TOE 外部へ送信される TSF データの検出及び修正を可能とする手段として、データの暗号化及び復号機能を提供すること。
O.FAIL_SECURE	セルフテストの失敗に際して、TOE はシャットダウンし、管理者によって構成されたセキュリティ方針を遵守していない状態であってもデータが通過できないことを確証すること。
O.PORT_FILTERING	TOE は、送信元及び送信先トランスポート層ポートに基づいてネットワークパケットをフィルタしログに記録する手段を提供すること。

6.2.2　運用環境のセキュリティ対策方針

以下の表には、VPN ゲートウェイの運用環境に特有のセキュリティ対策方針が含まれている。これらのセキュリティ対策方針は NDPP に定義されたものに付け加えられるものであり、そのすべてが VPN ゲートウェイの運用環境に適用される。

6-5 運用環境のセキュリティ対策方針

セキュリティ対策方針名	セキュリティ対策方針の定義
OE.CONNECTIONS	TOE 管理者は、接続されたネットワーク間を流れるネットワークトラフィックに TOE がその方針を実効的に適用できるように、TOE がインストールされていることを確実にすること。

6.2.3　セキュリティ対策方針の対応

本 EP において特定または定義されているセキュリティ機能要件（SFR）とセキュリティ対策方針との対応は、セクション 3 に記載されている。

7　附属書 C：追加要件

7.1.1　事前共有鍵の作成（FIA_PSK_EXT）

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 がサポートしてもよい事前共有鍵には、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）。

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。

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。

下記の要件によって、ST 作成者が本 EP の本文中の FCS_IPSEC_EXT.1.12 において事前共有鍵を選択した場合、これらの要件を ST に取り込むことが可能となる。

7.1.2　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：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なくてはならない（shall)）。

FIA_PSK_EXT.1.4 TSF は、ビットベースの事前共有鍵を [選択：受け入れ、FCS_RBG_EXT.1 に規定されるランダムビット生成器を用いて生成] できなくてはならない（shall）。

保証アクティビティ

TSS

評価者は TSS を調査して、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、及び 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）。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、及びこの調整が 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）。

ガイダンス

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するガイダンスが管理者へ提供されていること、及び（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）。

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）。

テスト

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）。

8　附属書 D：モビリティの要件

この附属書には、「ヘッドエンド」VPN ゲートウェイデバイス用に ST 作成者がオプションとして選択してもよい要件が含まれている。本 EP の本文中の要件は、複数拠点間 VPN ゲートウェイ装置に必要と判定されたものである。VPN 装置のもうひとつの用途として、モバイルユーザ向けのアーキテクチャにおいて、リモートクライアントが信頼できるネットワークへアクセスするためのセキュアな手段を提供することがある。これらのデバイスは、リモート VPN クライアントの管理機能（例えば、IP アドレスの割り当て、クライアントセッションの管理）を提供するが、信頼できるネットワーク間にセキュアな通信パスを提供することに限定された VPN ゲートウェイにはこれらの機能は必ずしも見られない。したがってすべての VPN ゲートウェイにこの TOE のモビリティ面の提供を義務付けるのではなく、以下の要件をオプションとして規定する。この意味は、複数拠点間 VPN ゲートウェイはこれらの機能を提供しなくてもよいが、モビリティコミュニティへの提供を意図したデバイスは、本 EP の本文中の（そしてもちろん NDPP 中の）要件に加えて、本附属書に規定される要件をも実装するということである。

8.1　セキュリティ課題の記述

ピアツーピア複数拠点環境における VPN ゲートウェイ向けに特定された脅威に加えて、VPN ヘッドエンド構成において憂慮される一意な懸念点がいくつか存在する。

8.2　脅威

8.2.1　不正なクライアントの接続

VPN クライアントは VPN ゲートウェイへ接続するために必要な資格情報（例えば、証明書、事前共有鍵）を持っている可能性があり、リモートクライアントまたはクライアントが動作しているマシンが危殆化されて不正な接続を行おうとする場合が考えられる。

(T.UNAUTHORIZED_CONNECTION)

8.2.2　セッションのハイジャック

セッションのアクティビティのためにリモートクライアントのセッションがハイジャックされる場合が考えられる。これは、セッションを確立するために利用されたマシンからユーザが立ち去ってしまったことにより、発生する可能性がある。

(T.HIJACKED_SESSION)

8.2.3　保護されないクライアントのトラフィック

リモートマシンのネットワークトラフィックが、敵対的なネットワークに公開されるおそれがある。ユーザは、敵対的な（または不明な）ネットワークを使わざるを得ず、トラフィックを適切にルーティングできずにネットワークトラフィックを送信するかもしれない。

8.3　対策方針

8.3.1　クライアント接続確立の制約

リモートクライアントが危殆化し「通常」の運用外のヘッドエンド VPN ゲートウェイとの接続の確立を試行する懸念に対処するため、この対策方針ではリモートクライアントが接続を確立できる条件を規定する。管理者は、管理者が適切と考える属性に基づいてクライアントの接続要求を受け入れるように、ヘッドエンド VPN ゲートウェイを構成することができる。

(O.CLIENT_ESTABLISHMENT_CONSTRAINTS → FTA_TSE.1)

8.3.2 リモートセッションの終了

アクティビティがない場合、リモートクライアントのセッションは脆弱となる可能性がある。これは主に、リモート接続が確立されたデバイスからユーザが立ち去ることが原因である。一部のデバイスは「画面のロック」やログアウト機能を有しているが、これらの機能は必ずしも構成可能または利用可能とは想定されない。この懸念に対処するため、管理者によって指定される時間間隔内のセッション終了機能が必要とされる。

(O.REMOTE_SESSION_TERMINATION → FTA_SSL.3)

8.3.3 割り当てられたプライベートアドレス

リモートクライアントが、信頼できるゲートウェイとのセキュアな通信を要請する場合がある。ユーザが信頼できないネットワークを介して接続している場合であっても、クライアントのネットワークパケットのルーティングを管理する既知のエンティティとユーザが確実に通信できるようにすることは可能なはずである（should）。これは、VPN ヘッドエンドがゲートウェイの管理する IP アドレスを割り当てるとともに、クライアントのネットワークトラフィックのルーティングポイントを提供することによって達成できる。

(O.ASSIGNED_PRIVATE_ADDRESS → FTA_VCM_EXT.1)

8.4 FTA：TOE アクセス

以下の要件は、VPN クライアントからのセッションの確立をどのように TOE がサポートするかを規定する。

8.4.1 FTA_SSL.3 TSF 主導による終了

FTA_SSL.3.1 **詳細化**：TSF は**リモート VPN クライアント**セッションを [*管理者によって構成可能なセッションのインアクティブな時間間隔*] 後に終了しなくてはならない（shall）。

適用上の注意：この要件は NDPP に存在するが、リモート管理者のインアクティブなセッションを意図したものである。ここでは、この要件は SA を確立している VPN クライアントに適用される。一定の構成可能な時間間隔がアクティビティなしに経過した後で、VPN ヘッドエンドとクライアントとの間の接続は終了する。ST 作成者がこの VPN ヘッドエンド向けの要件を ST に含めている場合、この要件は NDPP 中の要件と共に繰り返されるべきである（should）。

8.4.2 FTA_TSE.1 TOE セッションの確立

FTA_TSE.1.1 **詳細化**：TSF は、場所、時刻、日付、[割付：その他の属性] に基づいて、**リモート VPN クライアント**セッションの確立を拒否できなくてはならない（shall）。

適用上の注意：本 EP に関しては、場所はクライアントの IP アドレスとして定義される。

8.4.3 FTA_VCM_EXT.1 VPN クライアント管理

FTA_VCM_EXT.1.1 TSF は、セキュリティセッションの確立成功にあたって VPN クライアントへプライベート IP アドレスを割り当てなくてはならない（shall）。

適用上の注意：この要件に関するプライベート IP アドレスは、TOE がヘッドエンドとなっている信頼できるネットワーク内部のものである。

9 附属書 E

以下の表は、パケットフィルタリングルールの定義及び適用の構成、またはテストに用いられる、IPv4 及び IPv6 のプロトコルフィールドの RFC 定義済みの値を特定するものである。

9-1 定義済みのプロトコル固有値

プロトコル	定義済み属性
IPv4	トランスポート層プロトコル 1 - Internet Control Message トランスポート層プロトコル 2 - Internet Group Management トランスポート層プロトコル 3 - Gateway-to-Gateway トランスポート層プロトコル 4 - IP in IP (encapsulation) トランスポート層プロトコル 5 - Stream トランスポート層プロトコル 6 - Transmission Control トランスポート層プロトコル 7 - UCL トランスポート層プロトコル 8 - Exterior Gateway Protocol トランスポート層プロトコル 9 - any private interior gateway トランスポート層プロトコル 10 - BBN RCC Monitoring トランスポート層プロトコル 11 - Network Voice Protocol トランスポート層プロトコル 12 - PUP トランスポート層プロトコル 13 - ARGUS トランスポート層プロトコル 14 - EMCON トランスポート層プロトコル 15 - Cross Net Debugger トランスポート層プロトコル 16 - Chaos トランスポート層プロトコル 17 - User Datagram トランスポート層プロトコル 18 - Multiplexing トランスポート層プロトコル 19 - DCN Measurement Subsystems トランスポート層プロトコル 20 - Host Monitoring トランスポート層プロトコル 21 - Packet Radio Measurement トランスポート層プロトコル 22 - XEROX NS IDP トランスポート層プロトコル 23 - Trunk-1 トランスポート層プロトコル 24 - Trunk-2 トランスポート層プロトコル 25 - Leaf-1 トランスポート層プロトコル 26 - Leaf-2 トランスポート層プロトコル 27 - Reliable Data Protocol トランスポート層プロトコル 28 - Internet Reliable Transaction トランスポート層プロトコル 29 - ISO Transport Protocol Class 4 トランスポート層プロトコル 30 - Bulk Data Transfer Protocol トランスポート層プロトコル 31 - MFE Network Services Protocol トランスポート層プロトコル 32 - MERIT Intermodal Protocol トランスポート層プロトコル 33 - Sequential Exchange Protocol トランスポート層プロトコル 34 - Third Party Connect Protocol トランスポート層プロトコル 35 - Inter-Domain Policy Routing Protocol トランスポート層プロトコル 36 - XTP トランスポート層プロトコル 37 - Datagram Delivery Protocol トランスポート層プロトコル 38 - IDPR Control Message Transport Protocol トランスポート層プロトコル 39 - TP++ Transport Protocol トランスポート層プロトコル 40 - IL Transport Protocol トランスポート層プロトコル 41 - Simple Internet Protocol トランスポート層プロトコル 42 - Source Demand Routing Protocol トランスポート層プロトコル 43 - SIP Source Route トランスポート層プロトコル 48 - Mobile Host Routing Protocol トランスポート層プロトコル 49 - BNA トランスポート層プロトコル 50 - SIPP Encap Security Payload トランスポート層プロトコル 51 - SIPP Authentication Header トランスポート層プロトコル 52 - Integrated Net Layer Security TUBA トランスポート層プロトコル 53 - IP with Encryption

プロトコル	定義済み属性
IPv4	トランスポート層プロトコル 54 - NBMA Next Hop Resolution Protocol トランスポート層プロトコル 61 - any host internal protocol トランスポート層プロトコル 62 - CFTP トランスポート層プロトコル 63 - any local network トランスポート層プロトコル 64 - SATNET and Backroom EXPAK トランスポート層プロトコル 65 - Kryptolan トランスポート層プロトコル 66 - MIT Remote Virtual Disk Protocol トランスポート層プロトコル 67 - Internet Pluribus Packet Core トランスポート層プロトコル 68 - any distributed file system トランスポート層プロトコル 69 - SATNET Monitoring トランスポート層プロトコル 70 - VISA Protocol トランスポート層プロトコル 71 - Internet Packet Core Utility トランスポート層プロトコル 72 - Computer Protocol Network Executive トランスポート層プロトコル 73 - Computer Protocol Heart Beat トランスポート層プロトコル 74 - Wang Span Network トランスポート層プロトコル 75 - Packet Video Protocol トランスポート層プロトコル 76 - Backroom SATNET Monitoring トランスポート層プロトコル 77 - SUN ND PROTOCOL-Temporary トランスポート層プロトコル 78 - WIDEBAND Monitoring トランスポート層プロトコル 79 - WIDEBAND EXPAK トランスポート層プロトコル 80 - ISO Internet Protocol トランスポート層プロトコル 81 - VMTP トランスポート層プロトコル 82 - SECURE-VMTP トランスポート層プロトコル 83 - VINES トランスポート層プロトコル 84 - TTP トランスポート層プロトコル 85 - NSFNET-IGP トランスポート層プロトコル 86 - Dissimilar Gateway Protocol トランスポート層プロトコル 87 - TCF トランスポート層プロトコル 88 - IGRP トランスポート層プロトコル 89 - OSPFIGP トランスポート層プロトコル 90 - Sprite RPC Protocol トランスポート層プロトコル 91 - Locus Address Resolution Protocol トランスポート層プロトコル 92 - Multicast Transport Protocol トランスポート層プロトコル 93 - AX.25 Frames トランスポート層プロトコル 94 - IP-within-IP Encapsulation Protocol トランスポート層プロトコル 95 - Mobile Internetworking Control Protocol トランスポート層プロトコル 96 - Semaphore Communications Security Protocol トランスポート層プロトコル 97 - Ethernet-within-IP Encapsulation トランスポート層プロトコル 98 - Encapsulation Header トランスポート層プロトコル 99 - any private encryption scheme トランスポート層プロトコル 100 – GMTP
IPv6	トランスポート層プロトコル 0 - IPv6 Hop-by-Hop Option トランスポート層プロトコル 1 - Internet Control Message トランスポート層プロトコル 2 - Internet Group Management トランスポート層プロトコル 3 - Gateway-to-Gateway トランスポート層プロトコル 4 - IPv4 encapsulation トランスポート層プロトコル 5 - Stream トランスポート層プロトコル 6 - Transmission Control トランスポート層プロトコル 7 - CBT トランスポート層プロトコル 8 - Exterior Gateway Protocol トランスポート層プロトコル 9 - any private interior gateway トランスポート層プロトコル 10 - BBN RCC Monitoring トランスポート層プロトコル 11 - Network Voice Protocol トランスポート層プロトコル 12 - PUP トランスポート層プロトコル 13 - ARGUS トランスポート層プロトコル 14 - EMCON トランスポート層プロトコル 15 - Cross Net Debugger トランスポート層プロトコル 16 - Chaos トランスポート層プロトコル 17 - User Datagram トランスポート層プロトコル 18 – Multiplexing トランスポート層プロトコル 19 - DCN Measurement Subsystems トランスポート層プロトコル 20 - Host Monitoring トランスポート層プロトコル 21 - Packet Radio Measurement トランスポート層プロトコル 22 - XEROX NS IDP

プロトコル	定義済み属性
IPv6	トランスポート層プロトコル 23 - Trunk-1 トランスポート層プロトコル 24 - Trunk-2 トランスポート層プロトコル 25 - Leaf-1 トランスポート層プロトコル 26 - Leaf-2 トランスポート層プロトコル 27 - Reliable Data Protocol トランスポート層プロトコル 28 - Internet Reliable Transaction トランスポート層プロトコル 29 - Transport Protocol Class 4 トランスポート層プロトコル 30 - Bulk Data Transfer Protocol トランスポート層プロトコル 31 - MFE Network Services Protocol トランスポート層プロトコル 32 - MERIT Intermodal Protocol トランスポート層プロトコル 33 - Datagram Congestion Control Protocol トランスポート層プロトコル 34 - Third Party Connect Protocol トランスポート層プロトコル 35 - Inter-Domain Policy Routing Protocol トランスポート層プロトコル 36 - XTP トランスポート層プロトコル 37 - Datagram Delivery Protocol トランスポート層プロトコル 38 - IDPR Control Message Transport Proto トランスポート層プロトコル 39 - TP++ Transport Protocol トランスポート層プロトコル 40 - IL Transport Protocol トランスポート層プロトコル 41 - IPv6 encapsulation トランスポート層プロトコル 42 - Source Demand Routing Protocol トランスポート層プロトコル 43 – Routing Header for IPv6 トランスポート層プロトコル 44 – Fragment Header for IPv6 トランスポート層プロトコル 45 - Inter-Domain Routing Protocol トランスポート層プロトコル 46 - Reservation Protocol トランスポート層プロトコル 47 - General Routing Encapsulation トランスポート層プロトコル 48 - Dynamic Source Routing Protocol トランスポート層プロトコル 49 - BNA トランスポート層プロトコル 50 - Encap Security Payload トランスポート層プロトコル 51 - Authentication Header トランスポート層プロトコル 52 - Integrated Net Layer Security トランスポート層プロトコル 53 - IP with Encryption トランスポート層プロトコル 54 - NBMA Address Resolution Protocol トランスポート層プロトコル 55 - Mobility トランスポート層プロトコル 56 - Transport Layer Security Protocol using Kryptonet key management トランスポート層プロトコル 57 - SKIP トランスポート層プロトコル 58 – ICMP for IPv6 トランスポート層プロトコル 59 – No Next Header for IPv6 トランスポート層プロトコル 60 – Destination Options for IPv6 トランスポート層プロトコル 61 - any host internal protocol トランスポート層プロトコル 62 - CFTP トランスポート層プロトコル 63 - any local network トランスポート層プロトコル 64 - SATNET and Backroom EXPAK トランスポート層プロトコル 65 - Kryptolan トランスポート層プロトコル 66 - MIT Remote Virtual Disk Protocol トランスポート層プロトコル 67 - Internet Pluribus Packet Core トランスポート層プロトコル 68 - any distributed file system トランスポート層プロトコル 69 - SATNET Monitoring トランスポート層プロトコル 70 - VISA Protocol トランスポート層プロトコル 71 - Internet Packet Core Utility トランスポート層プロトコル 72 - Computer Protocol Network Executive トランスポート層プロトコル 73 - Computer Protocol Heart Beat トランスポート層プロトコル 74 - Wang Span Network トランスポート層プロトコル 75 - Packet Video Protocol トランスポート層プロトコル 76 - Backroom SATNET Monitoring トランスポート層プロトコル 77 - SUN ND PROTOCOL-Temporary トランスポート層プロトコル 78 - WIDEBAND Monitoring トランスポート層プロトコル 79 - WIDEBAND EXPAK トランスポート層プロトコル 80 - ISO Internet Protocol トランスポート層プロトコル 81 - VMTP トランスポート層プロトコル 82 - SECURE-VMTP トランスポート層プロトコル 83 - VINES トランスポート層プロトコル 84 - TTP トランスポート層プロトコル 84 - Internet Protocol Traffic Manager

プロトコル	定義済み属性
IPv6	トランスポート層プロトコル 85 - NSFNET-IGP トランスポート層プロトコル 86 - Dissimilar Gateway Protocol トランスポート層プロトコル 87 - TCF トランスポート層プロトコル 88 - EIGRP トランスポート層プロトコル 89 - OSPFIGP トランスポート層プロトコル 90 - Sprite RPC Protocol トランスポート層プロトコル 91 - Locus Address Resolution Protocol トランスポート層プロトコル 92 - Multicast Transport Protocol トランスポート層プロトコル 93 - AX.25 Frames トランスポート層プロトコル 94 - IP-within-IP Encapsulation Protocol トランスポート層プロトコル 95 - Mobile Internetworking Control Pro. トランスポート層プロトコル 96 - Semaphore Communications Sec. Pro. トランスポート層プロトコル 97 - Ethernet-within-IP Encapsulation トランスポート層プロトコル 98 - Encapsulation Header トランスポート層プロトコル 100 - GMTP トランスポート層プロトコル 101 - Ipsilon Flow Management Protocol トランスポート層プロトコル 102 - PNNI over IP トランスポート層プロトコル 103 - Protocol Independent Multicast トランスポート層プロトコル 104 - ARIS トランスポート層プロトコル 105 - SCPS トランスポート層プロトコル 106 - QNX トランスポート層プロトコル 107 - Active Networks トランスポート層プロトコル 108 - Payload Compression Protocol トランスポート層プロトコル 109 - Sitara Networks Protocol トランスポート層プロトコル 110 - Compaq Peer Protocol トランスポート層プロトコル 111 - IPX in IP トランスポート層プロトコル 112 - Virtual Router Redundancy Protocol トランスポート層プロトコル 113 - PGM Reliable Transport Protocol トランスポート層プロトコル 114 - any 0-hop protocol トランスポート層プロトコル 115 - Layer Two Tunneling Protocol トランスポート層プロトコル 116 - D-II Data Exchange (DDX) トランスポート層プロトコル 117 - Interactive Agent Transfer Protocol トランスポート層プロトコル 118 - Schedule Transfer Protocol トランスポート層プロトコル 119 - SpectraLink Radio Protocol トランスポート層プロトコル 120 - UTI トランスポート層プロトコル 121 - Simple Message Protocol トランスポート層プロトコル 122 - SM トランスポート層プロトコル 123 - Performance Transparency Protocol トランスポート層プロトコル 124 - ISIS over IPv4 トランスポート層プロトコル 125 - FIRE トランスポート層プロトコル 126 - Combat Radio Transport Protocol トランスポート層プロトコル 127 - Combat Radio User Datagram トランスポート層プロトコル 128 - SSCOPMCE トランスポート層プロトコル 129 - IPLT トランスポート層プロトコル 130 - Secure Packet Shield トランスポート層プロトコル 131 - Private IP Encapsulation within IP トランスポート層プロトコル 132 - Stream Control Transmission Protocol トランスポート層プロトコル 133 - Fiber Channel トランスポート層プロトコル 134 - RSVP-E2E-IGNORE トランスポート層プロトコル 135 - Mobility Header トランスポート層プロトコル 136 - UDPLite トランスポート層プロトコル 137 - MPLS-in-IP トランスポート層プロトコル 138 - MANET Protocols トランスポート層プロトコル 139 - Host Identity Protocol トランスポート層プロトコル 140 - Shim6 Protocol トランスポート層プロトコル 141 - Wrapped Encapsulating Security Payload トランスポート層プロトコル 142 - Robust Header Compression