ネットワークデバイス cPP (NDcPP)／ステートフル トラフィックフィルターファイアウォール cPP (FWcPP) 拡張パッケージ VPN ゲートウェイ

バージョン：2.1

2017-03-08

National Information Assurance Partnership

平成 29 年 10 月 25 日　翻訳 第 1.0 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

バージョン	日付	説明
1.0	2011 年 12 月	初期リリース
1.1	2013 年 4 月	証明書パス検証アルゴリズムが、CA 証明書と見なされる証明書に対して満たさ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 にセットされることを保証しなければならないことを規定するよう X.509 要件を更新した。
2.0	2015 年 10 月	NDPP から NDcPP への移行によりもたらされたベース PP への変更を反映するために更新された。
2.1	2017 年 3 月	フォーマット変更、追加のベース PP として FWcPP を追加するための更新、NIAP 技術的決定の結果を反映したその他の技術的な更新。

目次

1 序説

1.1 概要

本拡張パッケージ（EP）は、VPN ゲートウェイのセキュリティ要件を記述する。これは、デバイスの認証、公共の、または信頼されないネットワークを通過する情報の機密性と完全性を提供するような、IPsec トンネルを終端するプライベートネットワークの端点にあるデバイスであると定義される。本 EP は、VPN ゲートウェイ技術に対してよく定義され記述された脅威の低減を目標とした、最小限のベースライン要件の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コラボラティブプロテクションプロファイル*（NDcPP）及び*ステートフルフィルターファイアウォールのコラボラティブプロテクションプロファイル*(FWcPP)を拡張するものである。この序説では、適合する評価対象（TOE）の特徴を記述し、また本 EP が NDcPP 及び／または FWcPP と併せてどのように使われるべきかについても説明する。

1.2 用語

以下のセクションは、本 EP で利用されるコモンクライテリアと技術用語の両方を提供する。

1.2.1 コモンクライテリア用語

コモンクライテリア(CC)	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(国際標準 ISO/IEC 15408)
コモンクライテリア評価機関	National Voluntary Laboratory Accreditation Program (NVLAP) によって認定され、かつ、コモンクライテリアに基づく評価の実施を NIAP 認証機関によって承認された、コモンクライテリア評価及び認証スキーム(CCEVS)における、IT セキュリティ評価機関
共通評価方法(CEM)	情報技術セキュリティ評価のための共通評価方法
拡張パッケージ(EP)	ある PP によって記述された製品の具体的なサブセットに対するセキュリティ要件の実装に依存しないセット
プロテクションプロファイル(PP)	ある種別の製品に対するセキュリティ要件の実装に依存しないセット
セキュリティ保証要件(SAR)	TOE の適切な SFR の実装が評価者によってどのように検証されるかについての要件
セキュリティ機能要件(SFR)	TOE によるセキュリティ実施についての要件
セキュリティターゲット(ST)	具体的な製品に対する実装に依存するセキュリティ要件のセット
評価対象(TOE)	評価される製品
TOE セキュリティ機能(TSF)	評価される製品のセキュリティ機能
TOE 要約仕様(TSS)	ST における SFR を TOE がどのように満たすかの記述

1.2.2 技術用語

用語	意味
ヘッドエンド	他の基盤デバイス (例、サイト間) とは対照的に、エンドポイント VPN クライアントを用いて VPN ゲートウェイが VPN 接続性を確立しようとする VPN ユースケース
パケットフィルタリング	外部ネットワーク宛または外部ネットワークからのトラフィクがその宛先へ通過するか、破棄されるかをエッジネットワークデバイスが決定するような処理
VPN ゲートウェイ	プライベートネットワークのエッジに常駐し、外部ネットワークに常駐するコンピュータからの VPN 接続性の確立を許可する、ある種別のネットワークデバイス
仮想プライベートネットワーク(VPN)	分散型ワイドエリアネットワークを越える、暗号学的にセキュアなネットワークメカニズムを—バーレイするためのメカニズム

1.3 適合評価対象

本 EP は、IPsecVPN トンネルを終端するような、ネットワークゲートウェイデバイスに特別に対応する。適合 VPN ゲートウェイは、2 つ以上の区別されるネットワークに接続され、企業ネットワーク全体における基盤的役割を持ったハードウェアとソフトウェアからなるデバイスである。特に、VPN ゲートウェイは、認証され暗号化された別のサイトへの経路を提供するするようなセキュアなトンネルを確立し、それにより、信頼されないネットワークを遷移している情報の暴露のリスクを低減する。

本 EP のベースライン要件は、複数サイトの VPN ゲートウェイデバイスのために必要であると決定されるようなものである。しかし、適合 TOE は、リモートクライアントのためのヘッドエンドとして動作する能力を含んでもよい。なぜならこの機能はオプションであり、リモートクライアントベースの要件は、附属書 A に含まれているからである。

本 EP は、NDcPP と FWcPP 上に構築される。本 EP への適合を主張する TOE は、これらの PP の少なくとも 1 つに対しても適合主張しなければならない。これらの PP は、一般的に「ベース PP」として本 EP の至る所で参照される。適合 TOE は、本 EP により定義される脅威を低減するため、本 EP で定義された追加の機能に沿ってベース PP で要求された機能を実装する義務がある。

本 EP の要件のセットはエンドユーザに何らかの価値を提供するより早い、低コストの評価を促進するための適用範囲に限定されることを意図している。

1.3.1 TOE 境界

本 EP に適合する TOE の物理的境界は、ハードウェアアプライアンス(一般的なネットワークデバイスまたはトラフィクフィルタファイアウォールのいずれか)である。TOE の論理的境界には、本 EP で定義される VPN 機能と関連する機能と同様に主張されるベース PP によって要求されるすべての機能が含まれる。本 EP と主張されたベース PP により定義されるセキュリティ機能に関連しないようなネットワークデバイスにより提供される任意の機能は、本 TOE の適用範囲外であると見なされる。

1.4 ユースケース

本 EP は、以下に定義される、VPN ゲートウェイ TOE について、3 つの可能性のあるユースケースを定義する。最初の 2 つのユースケースの 1 つは、適合 TOE に対して常に適用可能である。3 番目のユースケースは、オプションのユースケースであり、最初の 2 つのいずれかを伴う。

[ユースケース 1] ネットワークデバイス

VPN ゲートウェイは、ルータまたはスイッチ、または複数サイトの VPN ゲートウェイ機能を提供することに専用のデバイスのような、一般的なネットワークデバイスアプライナンスにより提供される機能の一部である。

[ユースケース 2] ファイアウォール

VPN ゲートウェイは、ファイアウォール機能に加えて、複数サイトの VPN ゲートウェイ機能を提供するステートフルトラフィクフィルタファイアウォールデバイスに含まれる。

[ユースケース 3] リモートクライアントヘッドエンド

VPN ゲートウェイは、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を提供する。

2 適合主張

適合ステートメント

本 EP に適合するため、ST は、[CC] パート 1 (ASE_CCL)で定義される正確適合 (StrictConformance) のサブセットである、完全適合(訳注 : Exact Conformance)を論証しなければならない。ST は、い K の本 PP におけるすべてのコンポーネントを含まなければならない :

- 無条件 (常に要求されるようなもの)
- 選択ベース (特定の選択が無条件の要件で選ばれたときに要求されるもの)

また、以下のコンポーネントについても含んでもよい :

- オプション
- オブジェクティブ (訳注 : 将来、この機能が普及した際に、無条件の要件になるもの)

無条件の要件は、本文書の本文 (セクション 5) にあるが、附属書には選択ベース、オプション、及びオブジェクティブ要件がふくまれる。ST には、これらのコンポーネントの任意のものを繰り返ししてもよいが、本 EP で定義されない追加のコンポーネント (例、CC パート 2 または 3 から) を導入してはならない。

CC 適合主張

本 EP は、コモンクライテリアバージョン 3.1 リビジョン 4 [CC] のパート 2 (拡張) 及び 3 (適合) に適合する。

PP 主張

本 EP は、いずれのプロテクションプロファイルへの適合も主張しない。

パッケージ主張

本 EP は、いずれのパッケージへの適合も主張しない。

3　セキュリティ課題記述

3.1　脅威

本 EP で定義される以下の脅威は、主張されたベース PP で定義された脅威を拡張する。

T.UNAUTHORIZED_CONNECTION、T.HUACKED_SESSION、T.UNPROTECTED_TRAFICの脅威は、TOE が VPN ヘッドエンドデバイスとして機能しているようなユースケースでのみ適用可能である。附属書 A.1 のオプション SFR が主張されない場合、ST は、これらの脅威を省略可能である。

T.DATA_INTEGRITY

保護された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、保護された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されたネットワーク上のデバイスと通信できる場合、または保護された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.NETWORK_ACCESS

保護されたネットワーク内部から、または保護された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、保護されたネットワーク上に位置するサービスを、保護された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、保護されたネットワーク外部に位置するデバイスが、保護された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、保護された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、保護された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ければならないという企業方針を強制することができる。

T.HUACKED_SESSION

リモートクライアントのセションがセションアクティビティのためにハイジャックされるような場合があるかもしれない。これは、利用者がセションを確立するために利用された機械から離れたために、達成される可能性がある。

T.NETWORK_DISCLOSURE

保護された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されたネットワーク上のデバイスと通信できる場合、または保護された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、保護された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、さらに保護された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、保護された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_MISUSE

保護されたネットワーク外部に位置するデバイスが、保護された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。また保護されたネットワーク内部から提供される特定のサービスが、保護された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、保護された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された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、保護された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.REPLAY_ATTACK

権限のない個人がシステムへのアクセスを得ることに成功する場合、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、その個人がネットワークの至る所を通過してい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。以下の条件をトラフィクが満たす場合に、トラフィクはリプレイの対象となる：

- 平文：暗号化されないトラフィクを閲覧する能力を持つ攻撃者は、望まれる結果を引き起こすためにリプレイする通信の適切なセグメントを識別することができる。

- 完全性なし：平文のトラフィクであると同時に、攻撃者は、キャプチャされたトラフィクに対して任意の改変を行うことができ、受信者がこれらの改変を検知する手段を持たない場合に望まれる結果を引き起こすためにそれをリプレイする。

T.UNAUTHORIZED_CONNECTION

VPN クライアントは､VPN ゲートウェイと接続するために必要なクレデンシャル (例、証明書、事前共有鍵) を持っているかもしれないが、リモートクライアント、またはたクライアントが動作しているマシンが危殆化して、許可されない接続を試行するような場合があるかもしれない。

T.UNPROTECTED_TRAFFIC

リモートマシンのネットワークトラフィクは、敵意のあるネットワークに曝されるかもしれない。利用者は、トラフィクを適切に送信できない状況でネットワークトラフィクを送信するため、敵意のある (または未知の) ネットワークを利用するように要求されるかもしれない。

3.2 前提条件

本 EP で定義された以下の前提条件は、主張されたベース PP によって定義された脅威を拡張する。

A.CONNECTIONS

TOE セキュリティ方針が、接続されたネットワークの間で流れている、すべての適用可能なネットワークトラフィク上で、実施されることを保証するようなやり方で、区別されたネットワークへ接続されていることを前提としてする。

3.3 組織のセキュリティ方針

本 EP は、主張されたベース PP で定義されたものを越えて、追加の組織のセキュリティ方針を定義しない。

4　セキュリティ対策方針

4.1　TOE の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。これは、本 EP により対処され、本 EP が主張されるとき TSF 内に含まれることが必須であることなしに NDcPP からのあらゆる機能を含まないような対策方針として参照される。

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。

O.ADDRESS_FILTERING

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クのフローを制限することになる。

以下に対処：FPF_RUL_EXT.1

O.ASSIGNED_PRIVATE_ADDRESS

リモートクライアントが信頼されるゲートウェイを用いてセキュアな通信を除くような場合がある。利用者は、信頼されないネットワーク経由で接続するかもしれないが、クライアントのネットワークパケットの送信を制御する既知のエンティティと通信できることを保証することはまだ可能であるべきである。これは、クライアントネットワークトラフィク用にルーティングポイントを提供することを同様に、ゲートウェイが管理する IP アドレスを割り当てている VPN ヘッドエンドによって達成可能である。

以下に対処：FTA_VCM_EXT.1 (オプション)

O.AUTHENTICATION

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。

以下に対処：FTP_ITC.1、FCS_IPSEC_EXT.1

O.CLIENT_ESTABLISHMENT_CONSTRAINTS

リモートクライアントが危殆化され、「正常の」操作以外のヘッドエンド VPN ゲートウェイを用いてコネクションの確立を試行するという懸念に対処するため、本対策方針は、リモートクライアントがコネクションを確立するかもしれないという条件を規定する。管理者は、ヘッドエンド VPN ゲートウェイを管理者が適切であると感じるような属性に基づいてコネクションのためのクライアントの要求を受け入れるように設定するかもしれない。

以下に対処：FTA_TSE.1 (オプション)

O.CRYPTOGRAPHIC_FUNCTIONS

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。

以下に対処： FCS_CKM.1/IKE、FCS_COP.1(1)、FCS_COP.1(2)、FCS_COP.1(3)、FCS_COP.1(4)、FCS_IPSEC_EXT.1、FCS_RBG_EXT.1、FIA_PSK_EXT.1 (選択ベース)

O.FAIL_SECURE

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。

以下に対処：FPT_FLS.1/SelfTest、FPT_TST_EXT.1、FPT_TST_EXT.2、FPT_TUD_EXT.1

O.PORT_FILTERING

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。

以下に対処：FPF_RUL_EXT.1

O.REMOTE_SESSION_TERMINATION

リモートクライアントのセションは、アクティビティがない時に脆弱になる可能性がある。これは、リモートコネクションを確立したデバイスから利用者が離れたことが主たる原因である。何らかのデバイスでは、「ロックスクリーン」またはログアウト機能があるが、それらは、設定されていること、または利用可能であると常に仮定することはできない。この懸念に対処するため、セション終了機能が管理者が規定する時間の間隔に必要となる。

以下に対処：FTA_SSL.3 (オプション)

O.SYSTEM_MONITORING

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。

以下に対処：FAU_GEN.1、FPF_RUL_EXT.1

O.TOE_ADMINISTRATION

適合 TOE は、TOE によって実施される IPsec プロトコルの暗号化の側面と同様に、管理者がパケットフィルタリング規則を設定するために必要な機能を提供する。

以下に対処：FIA_AFL.1、FMT_MOF.1/AdminAct、FMT_MTD.1/AdminAct、FMT_SMF.1

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針は、VPN ゲートウェイに特有であるものは一切識別されなかった。しかし、NDcPP 及び／または FWcPP (ベース PP として主張されたものによって) のすべての環境のセキュリティ対策方針が VPN ゲートウェイに適用される。

5　セキュリティ要件

本セクションに含まれるセキュリティ機能要件は、追加の拡張機能コンポーネントと共に、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 改訂第 4 版から導き出されている。

CC は、セキュリティ機能要件についての操作を定義する：割付、選択、選択の中の割付及び詳細化。本文書は、CC によって定義された操作を識別するために以下のフォント表記を利用する：

- **詳細化**操作（**太字体**で示す）は、ある要件の詳細情報を追加するために利用される、ゆえに、要件をさらに制限する。
- **選択**（*イタリック体*で示す）*:* は、要件の記述において、[CC]によって提供された 1 つまたは複数の選択肢を選択するために利用される。
- **割付**操作（*イタリック体*で示す）は、パスワード長のような、規定されないパラメタに具体的な値を割り付けるために利用される。角括弧内の値は割付を示す。
- **繰返**操作：括弧内の数字を用いて識別される（例、「(1)」）。
- **拡張 SFR :** は、SFR 名称の後にラベル「EXT」を付けることによって識別される。

5.1　NDcPP セキュリティ機能要件の方向性

本セクションでは、VPN ゲートウェイ EP の関連する SFR をサポートするために、NDcPP に含まれる特定の SFR に対してなどの選択が行わなければならない（must）かを ST 作成者に指示する。これは、必須の選択が行われたエレメントを表わすことによりキャプチャされる。ST 作成者は、残りの選択項目を自分の望む通りに完成することができる。特定の機能またはふるまいが TOE にあることを保証するため、SFR エレメントの選択も同様に行われる。

NDcPP から取られた各 SFR の保証アクティビティは、本 EP で特に示されることなしに、その PP のサポート文書で定義されるように、完成されるべきである(should)。

いくつかの要件について、SFR 内の特定の個別のエレメントのみが本 EP について変更されたことに留意されたい。以下の選択から省略された SFR エレメントは、NDcPP のそれらの定義から改変されていない適合 ST に含まれるべきものである(should)。

5.1.1　監査データ生成

本 EP によって定義されたセキュリティ監査のための追加の SFR は一切ない。しかし、NDcPP にある FAU_GEN.1 の拡張に寄与する追加の監査対象事象がある。このように、以下の事象が適合セキュリティターゲットにおいて、NDcPP の要件と統合されるべきである(should)。

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

表 5-1 FAU_GEN.1 監査事象と詳細情報

適用上の注釈： *セッション確立について、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だろう。TOE は、セション確立の成功でのすべてのパケットをログ出力し、ドロップまたは破棄したあらゆるパケットをログ出力できなければならない（must）。*

保証アクティビティ

TSS

評価者は、適用可能な規則に関連するネットワークトラフィクをログ出力するように TSF が設定できる方法について、TSS に記述されていることを検証しなければならない(shall)。本アクティビティが FPF_RUL_EXT.1 の TSS 保証アクティビティと組み合わせて対処されるべきである(should)ことに留意されたい。

評価者は、そのインタフェースの 1 つがネットワークトラフィクによって一杯になったときの TOE のふるまい方について、TSS に記述されていることを検証しなければならない(shall)。処理できないパケットを TOE がドロップすることは受け入れ可能であるが、いかなる状況においても、許可操作を許すための、または許可され確立されたセションに属する、規則を満たさないようなパケットを通すことは、TOE には許されない。TOE が実装の制限のためにドロップされたパケットを監査することを常に可能ではないかもしれない。ドロップされたパケットが監査されない事象におけるこれらの制限と状況は、TSS に記述されなければならない(shall)。

ガイダンス (訳注：以下は、TSS と同じ内容なので、TSS をガイダンス証拠資料に置き換えて読む必要がある)

評価者は、適用可能な規則に関連するネットワークトラフィクをログ出力するように TSF が設定できる方法について、TSS に記述されていることを検証しなければならない(shall)。本アクティビティが FPF_RUL_EXT.1 の TSS 保証アクティビティと組み合わせて対処されるべきである(should)ことに留意されたい。

評価者は、そのインタフェースの 1 つがネットワークトラフィクによって一杯になったときの TOE のふるまい方について、TSS に記述されていることを検証しなければならない(shall)。処理できないパケットを TOE がドロップすることは受け入れ可能であるが、いかなる状況においても、許可操作を許すための、または許可され確立されたセションに属する、規則を満たさないようなパケットを通すことは、TOE には許されない。TOE が実装の制限のためにドロップされたパケットを監査することを常に可能ではないかもしれない。ドロップされたパケットが監査されない事象におけるこれらの制限と状況は、TSS に記述されなければならない(shall)。

テスト

以下のテストは、その他の要件の範囲外で実行されることが期待される。本 SFR への TOE の適合性のテスト中に、具体的なテストが策定されて、本 SFR について実行されるか、または現状のまま通常通り実行されるか

のいずれかである、本 EP の他の SFR へ適合における TOE のふるまいをテスト中に監査機能は、起動されている。

テスト 1：評価者は、TOE がすべてのパケットを処理できないように、ネットワークパケットで TOE を満たすよう試行しなければならない(shall)。これは、TOE が取り扱うことのできる帯域を制限するように評価者が TOE を設定するよう要求するかもしれない(例、10MB インタフェースの利用(訳注：10Mbps インタフェースの間違いか))。評価者は、次に、受信パケットのすべてを処理できないことを TOE が正しく記録することを検証し、また TOE ログ出力のふるまいが TSS と一貫していることを検証するために、監査ログを閲覧しなければならない(shall)。

5.1.2 暗号サポート (FCS)

FCS_COP.1(1) 暗号操作（データ暗号化／復号）

FCS_COP.1.1(1) TSF は、以下：*ISO 18033-3 で規定される AES、ISO 10116 で規定される CBC、ISO 19772 で規定される GCM* に合致する、特定された暗号アルゴリズム*利用モード GCM,CBC で動作する AES* 及び暗号鍵長 *128 ビット、256 ビット、*及び [***選択：192 ビット、他の鍵長なし***]にしたがって、*暗号化／復号* を行わなければならない(shall)。

適用上の注釈： *本 SFR は、最小限 128 及び 256 ビットの両方の鍵長と同様に、GCM と CBC の両方を義務付けることによって、NDcPP でのその定義から改変された。*

FCS_IPSEC_EXT.1 拡張：IPsec

FCS_IPSEC_EXT.1.3 TSF は、[選択：*トランスポートモード、トンネルモード*] を実装しなければならない。

適用上の注釈： *サポートされる利用モードの選択は、RFC4301 に従って実行されなければならない(shall)。TSS では、サポートされる利用モードについての詳細情報を提供しなければならない(shall)。*

本 SFR は、NDcPP から変更されていない。しかし、本 EP の将来のバージョンがトンネンるモードとトランスポートモードの両方を TSF が実装することを要求するだろうことに留意するためにここに含まれた。

FCS_IPSEC_EXT.1.4 TSF は、セキュアハッシュアルゴリズム(SHA)べいーす HMAC と共に、暗号アルゴリズム AES-CBC-128、AES-CBC-256 (RFC3602 により両方とも規定される) 及び **AES-GCM-128 (RFC4106 で規定される)、AES-GCM-256 (RFC 4106 で規定される)**を用いて、RFC 4303 によって定義されるとおり IPsec プロトコル ESP を実装しなければならない(shall)。

適用上の注釈： *本 SFR エレメントは、両方とも元々のエレメントの定義の選択可能である、AES-GCM-128 及び AES-GCM-256 を義務付けることによって NDcPP での定義から改変された。*

FCS_IPSEC_EXT.1.11 TSF は、IKE プロトコルが、DH グループ 14(2048bit MODP)、19(256 ビットのランダム ECP)、及び[*選択：5 (1536 ビット MODP)、24 (2048 ビット MODP と 256 ビット POS)、他の DH グループなし*]を実装していることを保証しなければならない(shall)。

適用上の注釈：　*本 SFR エレメントは、両方とも元々のエレメントの定義の選択可能である、DH グループ19 と 20 を義務付けることによってNDcPP での定義から改変された。*

5.1.3　セキュリティ管理 (FMT)

FMT_MOF.1/AdminAct セキュリティ機能のふるまいの管理

本 SFR は、NDcPP でオプションとして定義されているが、本 EP では必須のもとして含まれている。SFR の文章は、NDcPP の定義から変更されていないが、本 EP に適合する ST への包含は、「TOE セキュリティ機能」がベース PP によって定義された関連する機能と同様に、本 EP で規定される機能を含むために、理解されるべきである(should)ことを意味する。

FMT_MTD.1/AdminAct TSF データの管理

FMT_MTD.1.1　TSF は、暗号鍵**と VPN** 操作**のために利用される証明書を改変、削除、生成／インポートする能力を**セキュリティ管理者に制限しなければならない(shall)。

適用上の注釈：　*本 SFR は、NDcPP でオプションとして定義されているが本 EP では必須のもとして含まれている。VPN 操作のために利用される鍵と証明書を特別に参照するよう詳細化されることにも留意されたい。*

FMT_SMF.1/AdminAct TSF データの管理

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

- *TOE をローカル及びリモートで管理する能力；*
- *アクセスバナーを設定する能力；*
- *セション終了またはロックの前のセションの非アクティブ時間を設定する能力；*
- *TOE アップデートをインストールンする前にディジタル署名を用いてアップデートを検証し、TOE を更新する能力；*
- ***暗号機能を設定する能力；***
- ***IPsec 機能を設定する能力；***
- ***X.509v3 証明書をインポートする能力；***
- ***本EP で識別された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、決定及び改変する能力；***
- ***本 EP の他の選択で識別されたすべてのセキュリティ管理機能を設定する能力；***

  [選択：
- *監査のふるまいを設定する能力；*
- *FIA_UIA_EXT.1 で規定されるとおり、あるエンティティが識別及び認証される前に利用可能なTOE 提供のサービスのリストを設定する能力；*
- *他の機能なし]。*

適用上の注釈： *冗長性を防ぐため、本 EP への適合を主張する ST は、本 EP によってすでに必須であるので、FMT_SMF.1 を完成するときに、ND cPP で定義されるとおり、「暗号機能を設定する能力」を選択するべきである(should)。*

以下の保証アクティビティは、本 SFR について NDcPP サポート文書によって規定された保証アクティビティへの追加として実行されるべきである。

保証アクティビティ

TSS

評価者は、VPN トラフィクにためのトラフィクフィルタ規則が設定可能な方法について、TSS に記述されていることを検証しなければならない(shall)。このアクティビティが FPF_RUL_EXT.1 の TSS 保証アクティビティと変更して対処可能であることに留意されたい。

ガイダンス

評価者は、設定可能なデフォルトの設定方法と適合可能な規則属性、アクション、及び関連するインタフェースのそれぞれの設定方法を含めて、露トラフィクフィルタ規則の設定方法について、操作ガイダンスに記述されていることを検証しなければならない(shall)。評価者は、設定された規則が正しく配列されることを管理者が保証できるような指示についても操作ガイダンスが提供していることを保証しなければならない(must)。本アクティビティが FPF_RUL_EXT.1 のガイダンス保証アクティビティと統合して対処されるべきであることに留意されたい。

テスト

評価者は、TSF を設定するために利用される機能が規則の期待される変更を作り出すこと、及びそれらが正しく実施されることを実証するテストを考案しなければならない(shall)。多くの規則の組み合わせと配列シナリオが設定される必要がある、有効及び無効の両方のネットワークトラフィクの TOE 通過を試行することによりテストされる必要がある。本アクティビティが FPF_RUL_EXT.1 のテスト保証アクティビティと統合して対処されるべきであることに留意されたい。

5.1.4 TSF の保護 (FPT)

FPT_TUD__EXT.1 拡張：TSF テスト

FPT_TUD_EXT.1.3 TSF は、TOE へのファームウェア／ソフトウェアアップデートのインストール前に、*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、それらのアップデートを認証する手段を提供しなければならない(shall)。

適用上の注釈： *NDcPP は、ST 作成者が特定したい検証手法の選択肢を提供する。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) で規定されたものの 1 つ)が採用されなければならない(must)。ST 作成者が ST に NDcPP FPT_TUD_EXT.1 の他の 2 つのエレメントを改変なしに含めるべきである(should)ことに留意されたい。これは、「システムソフトウェアアップデートのコード署名」が NDcPP の FIA_X509_EXT.2 で選択される場合 NDcPP で規定されるとおり、NDcPP の選択ベース SFR である FPT_TUD_EXT.2 を含むトリガーともなるかもしれない。*

5.1.5 高信頼パス／チャネル (FTP)

FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC_EXT.1.1 **詳細化**：TSF は、それ自身と**以下の機能をサポートする許可された IT エンティティ**：**監査サーバ、VPN 通信、[*選択：認証サーバ、[割付：その他の機能]、その他の機能なし*]** 間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及びチャネルデータの暴露からの保護及びチャネルデータの改変の検知を提供する、高信頼通信チャネルを提供するため、**IPsec、及び [*選択：SSH、TLS、TLS/HTTPS、他のプロトコルなし*]** を利用しなければならない(shall)。

適用上の注釈： *NDcPP は、IPsec 以外の高信頼チャネルが外部 IT エンティティとの通信に利用可能であることを許容するが、VPN ゲートウェイ機能を規定する本 EP とは異なる。本 EP に適合するためには、TOE が VPN ゲートウェイ機能のために IPsec を提供しなければならない(must)ように、選択がなされる。(列挙されたプロトコルに少なくとも 1 つによる)保護は、監査情報(NDcPP で)を収集するサーバとの通信に少なくとも要求される。他の許可された IT エンティティとの通信について、ST 作成者は、適切な選択／割付を成し、これらのセタクに従って附属書 C から関連する要件を含める。*

5.2 FWcPP セキュリティ機能要件の方向性

FWcPP は、NDcPP で定義されたものと同一の数多くの SFR を定義している。TOE の一部として本 EP の包含によって影響を受ける NDcPP の SFR のすべては、同じ言い回しと保証アクティビティを持つ FWcPP 内にも存在する。したがって、FWcPP に適合する VPN ゲートウェイ TOE は、本 EP のセクション 5.1 で定義された同じ SFR 改変を実行するべきである。セクション 5.1 のすべてのステートメントは、FWcPP が主張されたベース PP である場合に同様に適用可能である。

評価者は、本 EP によって明示的に記述された場合を除き、FWcPP のサポート文書で規定されるとおりの保証アクティビティを実行することによって、これらの SFR を評価しなければならない(shall)。

5.3 TOE セキュリティ機能要件

5.3.1 暗号サポート (FCS)

FCS_CKM.1/IKE 暗号鍵生成 (IKE ピア認証用)

FCS_CKM.1.1/IKE TSF は、以下にしたがって **IKE ピア認証のために利用される非対称**暗号鍵を生成しなければならない(shall)：

[*選択、以下の少なくとも 1 つを選ぶ：*

- *FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 for RSA Scheme;*
- *FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4 for ECDSA shemes and Implementing “NIST curves” P-256, P-384 and [選択：P-521, 他の曲線なし]*]

及び対称鍵強度 112 ビット以上の規定された暗号鍵長。

適用上の注釈： *本要件を通して、TOE によって生成されることを要求される鍵は、IKE(V1 または V2 のいずれか) 鍵交換の間の VPN ピアの認証のために利用されることを意図している。公開鍵が X.509v3 証明書のアイデンティティと関連付けられることが要求されるが、この関連付けは、TOE によって実行されることは要求されない、またその代わりに、運用環境にある認証局によって実行されることが期待される。*

FCS_IPSEC_EXT.1 で示されるとおり、TOE は、ぴあにんしょうについて、RSA またはECDSA (または両方) をサポートする実装が要求される。

2048 ビット RSA 鍵ペアの生成された鍵強度は、112 ビットの対称鍵強度と同等またはそれ以上である必要がある。同等な鍵強度の情報については、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

TSS

評価者は、鍵ペアが生成される方法について、TSS に記述されていることを保証するためチェックしなければならない(shall)。TSF 実装が FIPS PUB 186-4 に適合することを示すため、評価者は、以下の情報が TSS に含まれていることを保証しなければならない(shall) :

- TSS には、TOE が適合する附属書 B のすべての選択が列挙されなければならない(shall) ;
- TSS に列挙されたそれぞれの適用可能な選択について、「shall」ではないすべてのステートメントについて(即ち、「shall not」、「should」、「should not」)、TOE がこのような選択肢を実装する場合、TSS に記述されなければならない(shall)。含まれる機能が「shall not」または「should not」として標準(FIPS PUB 186-4)に示される場合、TSS は、TOE によって実装されたセキュリティ方針にこれが敵対的に影響しない根拠を提供しなければならない(shall) ;
- 適用可能な Fuzokusho B のそれぞれの選択について、「shall」または「should」ステートメントに関連する機能の省略があれば、記述されなければならない(shall) ;

附属書に含まれないような TOE 独自の拡張や処理、または TOE が実施するべきセキュリティ方針に影響を与えるかもしれないような附属書によって許可された代替の実装は、記述されなければならない(shall)。

ガイダンス

評価者は、鍵生成機能が起動される方法について操作ガイダンスに記述され、サポートされるそれぞれの署名方法の処理に関連する入力と出力について記述されていることをチェックしなければならない(must)。評価者は鍵生成プロセスの出力のフォーマットとロケーションに関して、ガイダンスが提供していることについてもチェックしなければならない(shall)。

テスト

評価者は、ST 作成者によって実行された選択によって、上記要件のテストでのガイドとして、”FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System （ECDSA2VS）”及び“RSA Validation System (RSA2VS)”の鍵ペア生成の部分を利用しなければならない(shall)。これは、評価者がテスト中に検証可能なテスト勉クタを生成できるような、それらのアルゴリズムの信頼された参照実装を有することを要求する。

5.3.2 識別と認証 (FIA)

FIA_AFL.1 認証失敗時の取り扱い

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ければならない（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] しなければならない（shall）。

適用上の注釈：*本要件は、このやり方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がないので、ローカルコンソールでの管理者には適用されない。これは、(例えば)ローカル管理者に別のアカウントを要求すること、または認証メカニズムの実装にローカルとリモートのログインを区別させることで対処可能である。ローカル管理者による「アクション」は、実装依存であり、管理者ガイダンスに定義されるだろう(例えば、ロックアウトのリセットやパスワードのリセット)。ST 作成者は、TOE がこのハンドラをどのように実装したかにより、認証失敗時の取り扱いの選択肢の 1 つを選ぶ。*

保証アクティビティ

TSS

評価者は、連続する認証試行失敗が検知され追跡される方法の記述がリモート管理者アクションのためのサポートされるそれぞれの方法について、TSS に含まれていることを決定するため、TSS を検査しなければならない(shall)。TSS には、リモート管理者が TOE へのとグオン成功を防止されるによる方法、及びこの能力をレストアするために必要なアクションについても記述されなければならない(shall)。

ガイダンス

評価者は、連続する認証試行失敗回数 (FIA_AFL/1/1)と時間間隔(実装される場合、FIA_AFL.1.1) の設定についての指示が提供されること、及びリモート管理者再度ログオン成功することを許可するプロセスが特定されたそれぞれの「アクション」(その選択肢が選ばれた場合)について記述されていることを保証するため、操作ガイダンスについても検査しなければならない(shall)。採用されたセキュアプロトコル(例、TLSとSSH)によって異なるアクションやメカニズムが実装される場合、すべてが記述されなければならない(must)。

テスト

評価者は、リモート管理者が TOE をアクセスするそれぞれの方法(例、TLS、SSH)について、以下のテストについても実行しなければならない(shall)：

テスト 1：評価者は、TOE によって許可される連続する認証試行失敗回数を設定するため、操作ガイダンスを利用しなければならない(shall)。評価者は、一度限界に達したなら、有効なクレデンシャルを用いた試行が成功しないことをテストしなければならない(shall)。本要件によって特定されるそれぞれのアクションについて、評価者は、操作ガイダンスへの準拠とリモート管理者アクセスを許可するそれぞれのアクションの実行か成功することを示さなければならない(shall)。

テスト 2：評価者は、TOE によって許可される連続する認証試行失敗回数と有効なログインがリモート管理者に許可された後の時間間隔を設定するために操作ガイダンスを利用しなければならない(shall)。規定された無効ログイン試行回数の超過と有効なログインが不可能だることを示した後、評価者は、別のアクセス試行の前に時間間隔により定義されたインターバルのために松ことで、有効なクレデンシャルを用いてリモート管理者にログオン成功の能力をもたらすことを示されなければならない(shall)。

FIA_X509__EXT.4 証明書のアイデンティティ

FIA_X509_EXT.4.1 TSF は、コネクションの確立を試行しているエンティティについての証明書に含まれる識別名(DN)が期待される DN と合致しない場合に SA を確立してはならない(shall not)。

保証アクティビティ

TSS

TSS は、本 EP の要件を満たすために利用される証明書を含むような実装されたすべての証明書ストアについて、記述しなければならない(shall)。この記述は、証明書がそのストアにロードされる方法、及びそのストアが許可されないアクセスから保護される方法に関する情報を含まなければならない(shall)。TSS 記述には、標準にて規定された証明パスを TOE が形成する方法と証明書が検証される方法(CRL 及び／または OCSP が、証明書パス検証アルゴリズムと同様に、説明に含まれる)についての説明も含まれる。

ガイダンス

評価者は、SA の確立を許可または不許可するための TOE の設定方法について操作ガイダンスに記述されていることを検証しなければならない(shall)。

テスト

本 SFR は、NDcPP によって定義されるとおり、FCS_IPSEC_EXT.1 の一部としてテストされる。

5.3.3 パケットフィルタリング (FPF)

FPF_RUL_EXT.1 パケットフィルタリングの規則

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上でパケットフィルタリングを実行しなければならない(shall)。

保証アクティビティ

TSS

評価者は、ネットワークパケットの処理が実行開始する場合について明確に示すような、TOE の初期化／起動処理の記述を TSS が提供していること、及びこの処理中にパケットが流れることができないというアサーション(宣言)をサポートする説明を提供していることを検証しなければならない(shall)。

評価者は、ネットワークパケットの処理に含まれるコンポーネント(例、処理やタスクのようなアクティブなエンティティ)を識別する説明が TSS に含まれていること、及びコンポーネント故障の事象でルールセ

ットの適用なしに TOE を通してパケットが流れることを防止する防護策について TSS に記述されていることを検証しなければならない(shall)。これは、終了された処理のようなコンポーネントの故障、またはメモリバッファの満杯及びパケットを処理できないようなコンポーネントないでの故障を含む可能性がある。

ガイダンス

本要件に関連する操作ガイダンスは、後述のテスト保証アクティビティで評価される。

テスト

評価者は、TOE が初期化されている間、TOE を通してネットワークトラフィクを流すように試行しなければならない(shall)。ルールセットにより拒否されるか、そうでなければ流れるようなネットワークパケットの安定したフローは、任意のネットワークトラフィクが許可されるかを監視するためのパケットスニファを用いて、TOE のインタフェースで制御されるべきである(should)。

注釈：ルールセットの適用に関連する残りのテストは、後のテスト保証アクティビティで対処される。

FPF_RUL_EXT.1.2 TSF は、以下のネットワークトラフィクプロトコルを処理しなければならない(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)
- トランスポートコントロールプロトコル(TCP)
- ユーザデータグラムプロトコル(UDP)

及び本 SFR の他のエレメントで義務付けられた拡張に対して、以下の RFC によって定義されたネットワークパケットヘッダフィールドを検査できなければならない(shall)

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

適用上の注釈： *本エレメントは、プロトコルを特定し、インポート(ネットワークトラフィクを受信または進入)及びエクスポート(ネットワークトラフィクを送信—または送信されるよう形成、または発出)するとき、どの程度ネットワークトラフィクが TOE によって解釈可能かの範囲への定義を提供するプロトコル定義を参照する。*

RFC で規定されたプロトコルフォーマットは、依然利用されるが、多くの RFC は、もはや従うのは安全ではないようなふるまいを定義している。例えば、RFC792 は、「リダイレクト」ICMP タイプを定義した、これは、敵対者から来たときに安全とは見なされない；発信元は検証できないので、安全ではないような、「発信元消去」メッセージ。

保証アクティビティ

TSS

評価者は、以下のプロトコルがサポートされることを TSS が示していることを検証しなければならない(shall)：

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

評価者は、特定された RFC への適合が TOE 開発者によって決定された方法について TSS に記述されていることを検証しなければならない(shall) (例、サードパーティの相互運用性テスト、プロトコル適合テスト)。

ガイダンス

評価者は、以下のプロトコルがサポートされていることを操作ガイダンスが示していることを検証しなければならない(shall) :

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

ガイダンスには、TOE によって処理される ST 内に含まれる他のプロトコル(例、IPsec、IKE、もしかすると HTTPS、SSH、及び TLS)について記述されるだろう。評価者はどのプロトコルが TOE 評価の一部として見なされなかったかを明確にしていることを保証する。

テスト

本要件に関係するテストは、後のテスト保証アクティビティで対処される。

FPF_RUL_EXT.1.3 TSF は、以下のネットラークプロトコルフィールドを用いてパケットフィルタリング規則の定義を許可しなければならない(shall) :

- IPv4
  - 発信元アドレス
  - 宛先アドレス
  - プロトコル
- IPv6
  - 発信元アドレス
  - 宛先アドレス
  - Next ヘッダ(プロトコル)
- TCP
  - 発信元ポート
  - 宛先ポート
- UDP
  - 発信元ポート
  - 宛先ポート

適用上の注釈： *本エレメントは、本要件によって実施されるべき規則を作成するときに適用可能な、さまざまな属性を識別する一適用可能なインタフェー*

スは、TOE の特性であり、特定された属性の残りは、関連する RFC で定義される。プロトコルが、TCP、UDP、ICMP 等の適用可能なプロトコルを識別する IPv4 フィールド(IPv6 では、このフィールドは「next ヘッダ」と呼ばれる)。また、上記で識別された「インタフェース」は、適用可能なネットラークトラフィクが受信されたか、あるいは送信されるであろう、外部ポートである。

FPF_RUL_EXT.1.4 TSF は、パケットフィルタリング規則に関連する以下の操作を許可しなければならない(shall) ：許可、拒否、破棄、及びログ出力。

適用上の注釈： *本エレメントは、ネットワークトラフィクの照合に利用される規則への関連付けができる操作を定義する。*

FPF_RUL_EXT.1.5 TSF は、それぞれの区別されたネットワークトラフィクに割り付けられるべきパケットフィルタリング規則を許可しなければならない(shall)。

適用上の注釈： *本エレメントは、規則が割付可能な場合を識別する。特に、適合する TOE は、レイヤ3 及び 4 ネットワークトラフィクを取り扱うような、利用可能で識別可能な区別されたネットワークインタフェースのそれぞれに特有のフィルタリング規則を割り当てられなければならない(must)。識別可能なとは、インタフェースが一意で TOE 内で識別可能であることを意味する、またネットワークの観点から可視であるようなインタフェースを必ずしも要求しない(例、それに割り当てられた IP アドレスを持つ必要はない)。区別されたネットワークインタフェースは、TOE への共通の論理的経路を共有するような、1 つ以上の物理的なコネクションである。例えば、TOE は、多くの物理的ネットワークポートを曝すような、SFP モジュールをサポートするスモールフォームファクタプラガブル(SFP)ポートを有しているかもしれないが、共通のドライバは、すべての外部ポートのために利用されるので、それらは 1 つの区別されたネットワークインタフェースとして取り扱うことできる。*

それぞれのインタフェースについての別のルールセット、または代わりにどうにかしてルールを特定のインタフェースと関連付けるような、共有されたルールセットであるに可能性があることに留意されたい。

保証アクティビティ

TSS

評価者は、パケットフィルタリング方針と以下の属性について、TSS に記述されていることを検証しなければならない(shall)：

- IPv4
    - 発信元アドレス
    - 宛先アドレス
    - プロトコル
- IPv6
    - 発信元アドレス
    - 宛先アドレス
    - プロトコル
- TCP

    - 発信元ポート
    - 宛先ポート
- UDP
    - 発信元ポート
    - 宛先ポート

評価者は、それぞれの規則が以下の各ションを識別できることを検証しなければならない(shall)：許可、拒否、及びログ出力。

評価者は、TSS が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を識別していること、及びルールが区別されるネットワークインタフェースと関係づけする方法を説明することを検証しなければならない(shall)。インタフェースが共通のインタフェース種別へ(例、同じ内部の論理的な経路が利用される場合、おそらく共通のデバイスドライバが利用される場合)、グループ化可能である場合、それらが区別されたネットワークインタフェースとして累積的に取り扱い可能である。

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規則ないで設定可能なものとして以下の属性を操作ガイダンスが識別することを検証しなければならない(shall)：

- IPv4
    - 発信元アドレス
    - 宛先アドレス
    - プロトコル
- IPv6
    - 発信元アドレス
    - 宛先アドレス
    - プロトコル
- TCP
    - 発信元ポート
    - 宛先ポート
- UDP
    - 発信元ポート
    - 宛先ポート

評価者は、それぞれの規則が以下のアクションを識別できることを操作ガイダンスが示していることを検証しなければならない(shall)：許可、拒否、及びログ出力。

評価者は、規則が区別されたネットワークインタフェースと関連付けされる方法について、操作ガイダンスが説明していることを検証しなければならない(shall)。

テスト

評価者は、以下のテストを実行しなければならない(shall)：

テスト 1 : 評価者は、パケットフィルタ規則が以下の属性のそれぞれについてパケットを許可、拒否、及びログ出力するよう作成可能であることをテストするため、操作ガイダンスの指示を利用しなければならない(shall) :

- IPv4
  - 発信元アドレス
  - 宛先アドレス
  - プロトコル
- IPv6
  - 発信元アドレス
  - 宛先アドレス
  - プロトコル
- TCP
  - 発信元ポート
  - 宛先ポート
- UDP
  - 発信元ポート
  - 宛先ポート

テスト 2 : TOE によってサポートされた、それぞれの区別されたネットワークインタフェース種別について、パケットフィルタリング規則が定義可能であることを保証するため、上記テスト保証アクティビティを繰り返す。

規則の有効性がテストされるような FPF_RUL_EXT.1.7 のものと併せて、これらのテストアクティビティが実行されるべきであることに留意されたい ; ここでは評価者が単にガイダンスが十分であることを保証している、また TOE が管理者の上記属性に基づくルールセットの作成を支援する。FPF_RUL_EXT.1.7 のテストアクティビティは、テストが要求されるプロトコル／属性の組み合わせを定義する。それらの組み合わせが手動で設定される場合、それは、これらのテストアクティビティを満たすが、それらの組み合わせがそれ以外で設定される場合(例、自動化を用いて)、これらのテストアクティビティは、ガイダンスが正しいこと、かつ設定の全範囲が TOE 管理者によって達成可能であることを保証するために必要であるかもしれない。

FPF_RUL_EXT.1.6 TSF は、以下の順序 : 管理者定義された、で、適用可能なパケットフィルタリング規則を(FPF_RUL_EXT.1.5 に従って決定されるとおり)処理しなければならない(shall)。

適用上の注釈 : *本エレメントは、管理者が設定されたフィルタリング規則が照合のために処理される順序を定義可能であることを要求する。*

保証アクティビティ

TSS

評価者は、入ってくるパケットに適用されるアルゴリズムについて、デフォルト規則の処理、パケットが確立されたセションの一部であるかど

うかの決定、管理が定義し順序付けしたルールセットの適用を含めて、TSS に記述されていることを検証しなければならない(shall)。

ガイダンス

評価者は、パケットフィルタリング規則の順序が決定される方法について操作ガイダンスに記述され、管理者が規則処理の順序を設定できるように必要な指示を操作ガイダンスが提供していることを検証しなければならない(shall)。

テスト

評価者は、以下のテストを実行しなければならない(shall) :

テスト 1 : 評価者は、別の操作 － 許可と拒否 を用いて 2 つの同じパケットフィルタリング規則を考案しなければならない(shall)。その規則は、次に 2 つの区別された順序で配置されるべきであり(should)、それぞれのケースで、評価者は、確認のためにパケットキャプチャとログを用いて、最初の規則が両方のケースで適用可能なパケットの生成によって、実施されることを保証しなければならない(shall)

テスト 2: 評価者は、2 つの規則が 1 つが他のサブセットであるように(例、具体的なアドレス vs.ネットワークセグメント) 考案されるべきであることを除いて、上記手順を繰り返さなければならない(shall)。また、評価者は、最初の者が規則の特異性に関わらず実施されることを保証するため、両方の順序をテストするべきである(should)。

FPF_RUL_EXT.1.7 TSF は、照合規則が特定されない場合に、トラフィクをドロップしなければならない(shall)。

保証アクティビティ

TSS

評価者は、パケットフィルタリング規則を適用する処理について、TSS に記述されていること、及び別の要求された条件がネットワークトラフィクを許可せず(即ち、FPF_RUL_EXT.1.6 または FPF_RUL_EXT.1.7)、規則との照合ができないとき、そのふるまい(デフォルトで、または管理者によって設定されたとおりに) がそれらのパケットを拒否することを検証しなければならない(shall)。

ガイダンス

評価者は、ネットワークトラフィクに適用される規則や特別な条件がない場合のふるまいについて、操作ガイダンスに記述されていることを検証しなければならない(shall)。そのふるまいが設定可能である場合、評価者は、操作ガイダンスが規則に合致しないパケットを拒否するようにそのふるまいを設定するための適切な指示を提供することを検証しなければならない(shall)。

テスト

評価者は、以下のテストを実行しなければならない(shall) :

テスト 1: 評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと共に、それぞれの定義された IPv4 トランスポート層プロトコル(表 5-2 を参照) を許可し、ログ出力するように、TOE を設定しなければならない(shall)。評価者は、それぞ

れの定義された IPv4 トランスポート層プロトコルに合致する、設定された発信元及び宛先アドレス内にあるパケットを、それらが許可(即ち、TOE を通過した後そのパケットをキャプチャすることによって)され、ログ出力されることを保証するため、生成しなければならない(shall)。

テスト 2: 評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと共に、それぞれの定義された IPv4 トランスポート層プロトコル(表 5-2 を参照)を拒否し、ログ出力することを除き、すべてのトラフィクを許可するように、TOE を設定しなければならない(shall)。評価者は、それぞれの定義された IPv4 トランスポート層プロトコルに合致し、設定された発信元及び宛先アドレス内のパケットを、それらが拒否(即ち、適用可能なパケットが TOE を通過しないことをキャプチャすることによって)され、ログ出力されることを保証するため、生成しなければならない(shall)。

テスト 3: 評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと共に、それぞれの定義された IPv4 トランスポート層プロトコル(表 5-2 を参照) を許可し、ログ出力するように、TOE を設定しなければならない(shall)。さらに、評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと異なる(上記の許可されるものと異なる)組み合わせと共に、それぞれの定義された IPv4 トランスポート層プロトコル(表 5-2 を参照)を拒否し、ログ出力するように、TOE を設定しなければならない(shall)。評価者は、それぞれの IPv4 トランスポート層プロトコルと合致し、かつ上記で設定されたすべての発信元及び宛先アドレスの範囲外のパケットを生成し、それらが拒否(即ち、適用可能なパケットが TOE を通過しないことをキャプチャすることによって)されることを保証しなければならない(shall)。

テスト 4: 評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと共に、それぞれの定義された IPv6 トランスポート層プロトコル(表 5-2 を参照)を許可し、ログ出力するように、TOE を設定しなければならない(shall)。評価者は、それぞれの定義された IPv6 トランスポート層プロトコルと合致し、設定された発信元と宛先アドレス内のパケットを生成し、それらが許可(即ち、TOE を通過した後そのパケットをキャプチャすることによって)され、ログ出力されることを保証しなければならない(shall)。

テスト 5: 評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと共に、それぞれの定義された IPv6 トランスポート層プロトコルを拒否し、ログ出力することを除き、トラフィクを許可するように TOE を設定しなければならない(shall)。評価者は、それぞれの定義された IPv6 トランスポート層プロトコルと合致する、設定された発信元及び宛先アドレス内にあるパケットを、そ

れらが拒否(即ち、適用可能なパケットが TOE を通過しないことをキャプチャすることによって)され、ログ出力されることを保証するため、生成しなければならない(shall)。

テスト 6: 評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと共に、それぞれの定義された IPv6 トランスポート層プロトコル(表 5-2 を参照)を許可し、ログ出力することを除き、すべてのトラフィクを許可するように、TOE を設定しなければならない(shall)。さらに、評価者は、具体的な発信元アドレスと具体的な宛先アドレス、具体的な発信元アドレスとワイルドカード宛先アドレス、ワイルドカード発信元アドレスと具体的な宛先アドレス、及びワイルドカード発信元アドレスとワイルドカード宛先アドレスと異なる(上記の許可されるものと異なる)組み合わせと共に、それぞれの定義された IPv6 トランスポート層プロトコル(表 5-2 を参照)を拒否し、ログ出力するように、TOE を設定しなければならない(shall)。評価者は、それぞれの IPv6 トランスポート層プロトコルと合致し、かつ上記で設定されたすべての発信元及び宛先アドレスの範囲外のパケットを生成し、それらがドロップ(即ち、適用可能なパケットが TOE を通過しないことをキャプチャすることによって)され、ログ出力されることを保証しなければならない(shall)。

テスト 7: 評価者は、選択された発信元ポート、選択された宛先ポート、及び選択された発信元と宛先ポートの組み合わせを用いて、プロトコル 6 (TCP) を許可しログ出力するように、TOE を設定しなければならない(shall)。評価者は、設定された発信元及び宛先 TCP ポートと合致するパケットを生成し、それらが許可(即ち、TOE を通過した後そのパケットをキャプチャすることによって)され、ログ出力されることを保証しなければならない(shall)。

テスト 8: 評価者は、選択された発信元ポート、選択された宛先ポート、及び選択された発信元と宛先ポートの組み合わせを用いて、プロトコル 6 (TCP) を拒否しログ出力するように、TOE を設定しなければならない(shall)。評価者は、設定された発信元及び宛先 TCP ポートと合致するパケットを生成し、それらが拒否(即ち、適用可能なパケットが TOE を通過しないことをキャプチャすることによって)され、ログ出力されることを保証しなければならない(shall)。

テスト 9: 評価者は、選択された発信元ポート、選択された宛先ポート、及び選択された発信元と宛先ポートの組み合わせを用いて、プロトコル 17 (UDP) を許可しログ出力するように、TOE を設定しなければならない(shall)。評価者は、設定された発信元及び宛先 UDP ポートと合致するパケットを生成し、それらが許可(即ち、TOE を通過した後そのパケットをキャプチャすることによって)され、ログ出力されることを保証しなければならない(shall)。ここで、評価者は、UDP ポート 500 (IKE) がテストのセットに含まれることを保証する。

テスト 10: 評価者は、選択された発信元ポート、選択された宛先ポート、及び選択された発信元と宛先ポートの組み合わせを用いて、プロトコル 17 (UDP) を拒否しログ出力するように、TOE を設定しなければならない(shall)。評価者は、設定された発信元及び宛先 UDP ポートと合致するパケットを生成し、それらが拒否 (即ち、適用可能なパケットが TOE を通過しないことをキャプチャすることによって)され、ログ出力

されることを保証しなければならない(shall)。ここで、評価者は、UDP ポート 500 (IKE)がテストのセットに含まれることを保証する。

以下の表は、設定及びその他 p ケットフィルタリング規則定義と実施のテストで利用されるべき、IPv4 と IPv6 のプロトコルフィールドについて RFC で定義された値を特定する。

プロトコル	定義された属性
IPv4	Transport Layer Protocol 1 - Internet Control Message
	Transport Layer Protocol 2 - Internet Group Management
	Transport Layer Protocol 3 - Gateway-to-Gateway
	Transport Layer Protocol 4 - IP in IP (encapsulation)
	Transport Layer Protocol 5 - Stream
	Transport Layer Protocol 6 - Transmission Control
	Transport Layer Protocol 7 - UCL
	Transport Layer Protocol 8 - Exterior Gateway Protocol
	Transport Layer Protocol 9 - any private interior gateway
	Transport Layer Protocol 10 - BBN RCC Monitoring
	Transport Layer Protocol 11 - Network Voice Protocol
	Transport Layer Protocol 12 - PUP
	Transport Layer Protocol 13 - ARGUS
	Transport Layer Protocol 14 - EMCON
	Transport Layer Protocol 15 - Cross Net Debugger
	Transport Layer Protocol 16 - Chaos
	Transport Layer Protocol 17 - User Datagram
	Transport Layer Protocol 18 - Multiplexing
	Transport Layer Protocol 19 - DCN Measurement Subsystems
	Transport Layer Protocol 20 - Host Monitoring
	Transport Layer Protocol 21 - Packet Radio Measurement
	Transport Layer Protocol 22 - XEROX NS IDP
	Transport Layer Protocol 23 - Trunk-1
	Transport Layer Protocol 24 - Trunk-2
	Transport Layer Protocol 25 - Leaf-1
	Transport Layer Protocol 26 - Leaf-2
	Transport Layer Protocol 27 - Reliable Data Protocol
	Transport Layer Protocol 28 - Internet Reliable Transaction
	Transport Layer Protocol 29 - ISO Transport Protocol Class 4
	Transport Layer Protocol 30 - Bulk Data Transfer Protocol
	Transport Layer Protocol 31 - MFE Network Services Protocol
	Transport Layer Protocol 32 - MERIT Internodal Protocol

プロトコル	定義された属性
	Transport Layer Protocol 33 - Sequential Exchange Protocol
	Transport Layer Protocol 34 - Third Party Connect Protocol
	Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol
	Transport Layer Protocol 36 - XTP
	Transport Layer Protocol 37 - Datagram Delivery Protocol
	Transport Layer Protocol 38 - IDPR Control Message Transport Protocol
	Transport Layer Protocol 39 - TP++ Transport Protocol
	Transport Layer Protocol 40 - IL Transport Protocol
	Transport Layer Protocol 41 - Simple Internet Protocol
	Transport Layer Protocol 42 - Source Demand Routing Protocol
	Transport Layer Protocol 43 - SIP Source Route
	Transport Layer Protocol 44 - SIP Fragment
	Transport Layer Protocol 45 - Inter-Domain Routing Protocol
	Transport Layer Protocol 46 - Reservation Protocol
	Transport Layer Protocol 47 - General Routing Encapsulation
	Transport Layer Protocol 48 - Mobile Host Routing Protocol
	Transport Layer Protocol 49 - BNA
	Transport Layer Protocol 50 - SIPP Encap Security Payload
	Transport Layer Protocol 51 - SIPP Authentication Header
	Transport Layer Protocol 52 - Integrated Net Layer Security TUBA
	Transport Layer Protocol 53 - IP with Encryption
	Transport Layer Protocol 54 - NBMA Next Hop Resolution Protocol
	Transport Layer Protocol 61 - any host internal protocol
	Transport Layer Protocol 62 - CFTP
	Transport Layer Protocol 63 - any local network
	Transport Layer Protocol 64 - SATNET and Backroom EXPAK
	Transport Layer Protocol 65 - Kryptolan
	Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol
	Transport Layer Protocol 67 - Internet Pluribus Packet Core
	Transport Layer Protocol 68 - any distributed file system
	Transport Layer Protocol 69 - SATNET Monitoring
	Transport Layer Protocol 70 - VISA Protocol
	Transport Layer Protocol 71 - Internet Packet Core Utility
	Transport Layer Protocol 72 - Computer Protocol Network Executive
	Transport Layer Protocol 73 - Computer Protocol Heart Beat

プロトコル	定義された属性
	Transport Layer Protocol 74 - Wang Span Network
	Transport Layer Protocol 75 - Packet Video Protocol
	Transport Layer Protocol 76 - Backroom SATNET Monitoring
	Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary
	Transport Layer Protocol 78 - WIDEBAND Monitoring
	Transport Layer Protocol 79 - WIDEBAND EXPAK
	Transport Layer Protocol 80 - ISO Internet Protocol
	Transport Layer Protocol 81 - VMTP
	Transport Layer Protocol 82 - SECURE-VMTP
	Transport Layer Protocol 83 - VINES
	Transport Layer Protocol 84 - TTP
	Transport Layer Protocol 85 - NSFNET-IGP
	Transport Layer Protocol 86 - Dissimilar Gateway Protocol
	Transport Layer Protocol 87 - TCF
	Transport Layer Protocol 88 - IGRP
	Transport Layer Protocol 89 - OSPFIGP
	Transport Layer Protocol 90 - Sprite RPC Protocol
	Transport Layer Protocol 91 - Locus Address Resolution Protocol
	Transport Layer Protocol 92 - Multicast Transport Protocol
	Transport Layer Protocol 93 - AX.25 Frames
	Transport Layer Protocol 94 - IP-within-IP Encapsulation Protocol
	Transport Layer Protocol 95 - Mobile Internetworking Control Protocol
	Transport Layer Protocol 96 - Semaphore Communications Security Protocol
	Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation
	Transport Layer Protocol 98 - Encapsulation Header
	Transport Layer Protocol 99 - any private encryption scheme
	Transport Layer Protocol 100 - GMTP
IPv6	Transport Layer Protocol 1 - Internet Control Message
	Transport Layer Protocol 2 - Internet Group Management
	Transport Layer Protocol 3 - Gateway-to-Gateway
	Transport Layer Protocol 4 - IPv4 encapsulation
	Transport Layer Protocol 5 - Stream
	Transport Layer Protocol 6 - Transmission Control
	Transport Layer Protocol 7 - CBT
	Transport Layer Protocol 8 - Exterior Gateway Protocol

プロトコル	定義された属性
	Transport Layer Protocol 9 - any private interior gateway
	Transport Layer Protocol 10 - BBN RCC Monitoring
	Transport Layer Protocol 11 - Network Voice Protocol
	Transport Layer Protocol 12 - PUP
	Transport Layer Protocol 13 - ARGUS
	Transport Layer Protocol 14 - EMCON
	Transport Layer Protocol 15 - Cross Net Debugger
	Transport Layer Protocol 16 - Chaos
	Transport Layer Protocol 17 - User Datagram
	Transport Layer Protocol 18 - Multiplexing
	Transport Layer Protocol 19 - DCN Measurement Subsystems
	Transport Layer Protocol 20 - Host Monitoring
	Transport Layer Protocol 21 - Packet Radio Measurement
	Transport Layer Protocol 22 - XEROX NS IDP
	Transport Layer Protocol 23 - Trunk-1
	Transport Layer Protocol 24 - Trunk-2
	Transport Layer Protocol 25 - Leaf-1
	Transport Layer Protocol 26 - Leaf-2
	Transport Layer Protocol 27 - Reliable Data Protocol
	Transport Layer Protocol 28 - Internet Reliable Transaction
	Transport Layer Protocol 29 - Transport Protocol Class 4
	Transport Layer Protocol 30 - Bulk Data Transfer Protocol
	Transport Layer Protocol 31 - MFE Network Services Protocol
	Transport Layer Protocol 32 - MERIT Internodal Protocol
	Transport Layer Protocol 33 - Datagram Congestion Control Protocol
	Transport Layer Protocol 34 - Third Party Connect Protocol
	Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol
	Transport Layer Protocol 36 - XTP
	Transport Layer Protocol 37 - Datagram Delivery Protocol
	Transport Layer Protocol 38 - IDPR Control Message Transport Proto
	Transport Layer Protocol 39 - TP++ Transport Protocol
	Transport Layer Protocol 40 - IL Transport Protocol
	Transport Layer Protocol 41 - IPv6 encapsulation
	Transport Layer Protocol 42 - Source Demand Routing Protocol
	Transport Layer Protocol 45 - Inter-Domain Routing Protocol

プロトコル	定義された属性
	Transport Layer Protocol 46 - Reservation Protocol
	Transport Layer Protocol 47 - General Routing Encapsulation
	Transport Layer Protocol 48 - Dynamic Source Routing Protocol
	Transport Layer Protocol 49 - BNA
	Transport Layer Protocol 52 - Integrated Net Layer Security
	Transport Layer Protocol 53 - IP with Encryption
	Transport Layer Protocol 54 - NBMA Address Resolution Protocol
	Transport Layer Protocol 55 - Mobility
	Transport Layer Protocol 56 - Transport Layer Security Protocol using Kryptonet key management
	Transport Layer Protocol 57 - SKIP
	Transport Layer Protocol 58 – ICMP for IPv6
	Transport Layer Protocol 59 – No Next Header for IPv6
	Transport Layer Protocol 61 - any host internal protocol
	Transport Layer Protocol 62 - CFTP
	Transport Layer Protocol 63 - any local network
	Transport Layer Protocol 64 - SATNET and Backroom EXPAK
	Transport Layer Protocol 65 - Kryptolan
	Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol
	Transport Layer Protocol 67 - Internet Pluribus Packet Core
	Transport Layer Protocol 68 - any distributed file system
	Transport Layer Protocol 69 - SATNET Monitoring
	Transport Layer Protocol 70 - VISA Protocol
	Transport Layer Protocol 71 - Internet Packet Core Utility
	Transport Layer Protocol 72 - Computer Protocol Network Executive
	Transport Layer Protocol 73 - Computer Protocol Heart Beat
	Transport Layer Protocol 74 - Wang Span Network
	Transport Layer Protocol 75 - Packet Video Protocol
	Transport Layer Protocol 76 - Backroom SATNET Monitoring
	Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary
	Transport Layer Protocol 78 - WIDEBAND Monitoring
	Transport Layer Protocol 79 - WIDEBAND EXPAK
	Transport Layer Protocol 80 - ISO Internet Protocol
	Transport Layer Protocol 81 - VMTP
	Transport Layer Protocol 82 - SECURE-VMTP
	Transport Layer Protocol 83 - VINES

プロトコル	定義された属性
	Transport Layer Protocol 84 - TTP
	Transport Layer Protocol 84 - Internet Protocol Traffic Manager
	Transport Layer Protocol 85 - NSFNET-IGP
	Transport Layer Protocol 86 - Dissimilar Gateway Protocol
	Transport Layer Protocol 87 - TCF
	Transport Layer Protocol 88 - EIGRP
	Transport Layer Protocol 89 - OSPFIGP
	Transport Layer Protocol 90 - Sprite RPC Protocol
	Transport Layer Protocol 91 - Locus Address Resolution Protocol
	Transport Layer Protocol 92 - Multicast Transport Protocol
	Transport Layer Protocol 93 - AX.25 Frames
	Transport Layer Protocol 94 - IP-within-IP Encapsulation Protocol
	Transport Layer Protocol 95 - Mobile Internetworking Control Pro.
	Transport Layer Protocol 96 - Semaphore Communications Sec. Pro.
	Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation
	Transport Layer Protocol 98 - Encapsulation Header
	Transport Layer Protocol 100 - GMTP
	Transport Layer Protocol 101 - Ipsilon Flow Management Protocol
	Transport Layer Protocol 102 - PNNI over IP
	Transport Layer Protocol 103 - Protocol Independent Multicast
	Transport Layer Protocol 104 - ARIS
	Transport Layer Protocol 105 - SCPS
	Transport Layer Protocol 106 - QNX
	Transport Layer Protocol 107 - Active Networks
	Transport Layer Protocol 108 - Payload Compression Protocol
	Transport Layer Protocol 109 - Sitara Networks Protocol
	Transport Layer Protocol 110 - Compaq Peer Protocol
	Transport Layer Protocol 111 - IPX in IP
	Transport Layer Protocol 112 - Virtual Router Redundancy Protocol
	Transport Layer Protocol 113 - PGM Reliable Transport Protocol
	Transport Layer Protocol 114 - any 0-hop protocol
	Transport Layer Protocol 115 - Layer Two Tunneling Protocol
	Transport Layer Protocol 116 -D-II Data Exchange (DDX)
	Transport Layer Protocol 117 - Interactive Agent Transfer Protocol
	Transport Layer Protocol 118 - Schedule Transfer Protocol

プロトコル	定義された属性
	Transport Layer Protocol 119 - SpectraLink Radio Protocol
	Transport Layer Protocol 120 - UTI
	Transport Layer Protocol 121 - Simple Message Protocol
	Transport Layer Protocol 122 - SM
	Transport Layer Protocol 123 - Performance Transparency Protocol
	Transport Layer Protocol 124 - ISIS over IPv4
	Transport Layer Protocol 125 - FIRE
	Transport Layer Protocol 126 - Combat Radio Transport Protocol
	Transport Layer Protocol 127 - Combat Radio User Datagram
	Transport Layer Protocol 128 - SSCOPMCE
	Transport Layer Protocol 129 - IPLT
	Transport Layer Protocol 130 - Secure Packet Shield
	Transport Layer Protocol 131 - Private IP Encapsulation within IP
	Transport Layer Protocol 132 - Stream Control Transmission Protocol
	Transport Layer Protocol 133 - Fibre Channel
	Transport Layer Protocol 134 - RSVP-E2E-IGNORE
	Transport Layer Protocol 135 - Mobility Header
	Transport Layer Protocol 136 - UDPLite
	Transport Layer Protocol 137 - MPLS-in-IP
	Transport Layer Protocol 138 - MANET Protocols
	Transport Layer Protocol 139 - Host Identity Protocol
	Transport Layer Protocol 140 - Shim6 Protocol
	Transport Layer Protocol 141 - Wrapped Encapsulating Security Payload
	Transport Layer Protocol 142 - Robust Header Compression

表 5-2 トランスポート層プロトコル 値テーブル

5.3.4 TSF の保護 (FPT)

FPT_FLS.1/SelfTest フェールセキュア (自己テスト障害)

FPT_FLS.1.1/SelfTest TSF は、以下の種別の障害 : [*電源投入時の自己テストの障害、TSF 実行可能イメージの完全性チェックの障害、ノイズ源ヘルステストの障害*] が発生する場合、**シャットダウン**しなければならない (shall)。

適用上の注釈 : *本要件に関連する障害は、NDcPP/FWcPP の FPT_TST_EXT.1.1 要件及び本 EP で規定された FPT_TST_EXT.2.1 要件である。*

保証アクティビティ

TSS

評価者は、自己テスト障害、TSF 実行イメージの完全性チェック失敗、またはノイズ源のヘルステスト失敗時のシャットダウンをどのように TOE が保証するかについて、TSS に記述されていることを保

証しなければならない(shall)。例えば、障害がセキュリティ関連でないと思われる等、シャットダウンが発生しないような場合に、それらのケースが特定され、TOE のセキュリティ方針を実施する能力が影響を受けない理由の分類と正当化を支援する根拠があること。

FPT_TST_EXT.2 拡張：TSF テスト

FPT_TST_EXT.2.1 TSF は、FCS_COP.1(2) で規定された TSF 提供の暗号サービスの利用を通して、実行のためにロードされるときに、格納された TSF 実行可能コードの完全性を検証する機能を提供しなければならない(shall)。

適用上の注釈： *本要件は、実行されるべきである自己テストの 1 つによる方法を規定することによって、NDcPP/FWcPP で定義された自己テスト要件において拡張する。「格納された TSF 実行コード」とは、デバイスのソフトウェアイメージ全体を指し、本 EP によって定義された VPN ゲートウェイ機能に関連するコードそのものではない。*

5.4 TOE セキュリティ保証要件

本 EP は、ベース PP で定義されるものを越えて、いずれの追加セキュリティ保証要件も定義しない。本 EP に対する適合評価された TOE は、本質的にベース PP に対して同様に適合評価される。ベース PP によって規定される SAR に関連する保証アクティビティは、TOE 全体に対して実行される。

本 EP は、新しい SAR を規定しないが、VPN ゲートウェイ機能の存在とパケットフィルタリングを実行する TOE の能力は、潜在的な敵対者に対する追加の攻撃ベクターを導入する。したがって、評価者は、主張されたベース PP の AVA_VAN.1 のために定義されたアクティビティへの追加として、脆弱性分析の一部として、以下のセクション 5.4.1 で定義されたアクティビティを実行しなければならない(shall)。

5.4.1 クラス AVA: 脆弱性分析

評価者は、IPv4 と IPv6 の RFC によって定義されていないようなトランスポート層プロトコル属性のためのすべての値を繰り返すようなネットワークパケットを生成しなければならない(shall)。例えば、IPv4 は、トランスポート層プロトコルのための 8 ビットフィールドを持つ。100 個のみのトランスポート層プロトコルの値が IPv4 の RFC で定義されている (FPF_RUL_EXT.1 の表 5-2 を参照) が、256 個の可能性のある値が存在する。評価者は、トランスポート層プロトコル(すべての組み合わせを含めて) の RFC(定義された値は FPF_RUL_EXT.1.7 ですでにテストされている)で定義されていないそれぞれの可能性のある値を使うパケットを作るよう、また TOE がこれらのパケットを適切に取扱うことを決定するためにそれぞれの区別されたインタフェース種別をターゲットにするよう要求される。これらのパケットが規則に合致しない、または許可されたセションに属していないので、パケットはドロップされるべきである(should)。このような状況かでドロップされているパケットを VPN ゲートウェイが監査するような要件は一切ないので、評価者は、VPN ゲートウェイがこのようなパケットが TOE を通過することを許可しないことを保証しなければならない(shall)。IPv6 について、プロトコル番号 0 (ホップバイホップオプション)、60 (宛先オプション)、44 (フラグメント)、51 (AH)、及び 50 (ESP) は、トランスポート番号ではなく、むしろ拡張ヘッダー番号であり、テストから除外されるべきである(should)。

上記で要求される未定義属性テストに追加して、評価者は、要求されるプロトコルヘッダ(FTP を除く)の残りのフィールドのインテリジェントなファジングテストを実行しなければならない(shall)。インテリジェントファジングの意図は、規則が適用されるときにそれが拒否されるようにプロトコルヘッダのそれぞれのフィールドへランダムな

値を挿入させたパケット、さもなければパケットが正しく作られることである。評価者は、プロトコルフィールドによって様々な、報告書で利用され、正当化されるような、統計的に意味のあるサンプル数を保証する。

評価者は、TOE がこのようなパケットの処理によって敵対的な影響を受けたかどうかを決定するために、TOE が提供する何らかの診断(例、ログ出力、処理状態、インタフェースエラー)を参考にするべきである。

A. オプション要件

ベースライン要件は、本 EP の本文に含まれる。追加の要件を ST に含めることは可能であるが、TOE が本 EP への適合主張するために必須ではない。本附属書は、要件によって記述された機能を製品が提供する場合、ST 作成者の裁量で TOE 境界内に含まれるかもしれないオプションの要件を定義する。

これらの要件が含まれる場合、関連する管理機能やそれらに関連する監査対象事象を定義することは、ST 作成者の責任である。

A.1 VPN ヘッドエンド機能のオプション要件

本セクションには、「ヘッドエンド」VPN ゲートウェイデバイスのために、ST 作成者によってオプションで選択されてもよい要件を含む。本 EP の本文の要件は、複数サイトの VPN ゲートウェイアプライアンスのために必要と決定され者である。VPN アプライアンスの別のアプリケーションは、アーキテクチャにおいて、リモートクライアントが信頼されるネットワークをアクセスするかもしれないようなセキュアな手段を提供することによって、モバイルユーザに提供することを意図している。これらのデバイスは、信頼されたネットワーク間のセキュアな通信経路の提供に限定される VPN ゲートウェイでは必ずしも見つからないような、リモート VPN クライアントを管理(例、IP アドレスを割り当てて、クライアントセションを管理して)するための機能を提供する。TOE でのこのモビリティの側面をすべての VPN ゲートウェイが義務付けるよりもむしろ、次の要件がオプションとして規定される。これが意味するものは、複数サイトの VPN ゲートウェイがこれらの機能を提供する必要はないが、それらのモビリティコミュニティを供給仕様とするデバイスは、本附属書で規定されるものと同様に、本 EP の本文でその要件(及びもちろん NDcPP 及び／または FWcPP)を実装する。

A.1.1 FTA_SSL.3/VPN TSF 起動による終了 (FTA_SSL.3)

FTA_SSL.3.1/VPN 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*] 後に終了しなければならない（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 NDcPP 中の要件と共に繰り返されるべきである（should）。*

保証アクティビティ

TSS

評価者は、非アクティブな VPN クライアントセションを終了するための TSF の能力について記述されていることを検証するため、TSS を検査しなければならない(shall)。

ガイダンス

評価者は、有効な VPN クライアントセションの終了についてのタイムリミットの設定方法について、管理者に指示を与えていることを検証するため、操作ガイダンスを検査しなければならない(shall)。

テスト

評価者は、次のテストを実行しなければならない(shall)：

テスト 1：評価者は、5 分間の非アクティブタイマーをセットするために、操作ガイダンスで提供されるステップに従わなければならない(shall)。評価者は、次に VPN クライアントを TOE に接続し、4 分 50 秒間アイドル状態にし、このとき VPN にアクセスを要求するようなアクションを行うことによって、VPN クライアントがまだ接続されていること観測しなければならない(shall)。評価者は、次にクライアントをディスコネクトし、再コネクトし、5 分 10 秒間待って、同じアクションを試行し、それが成功しないことを観測しなければならない(shall)。評価者は、次に VPN クライアントセションがちょうど 5 分間存続していることを監査ログデータを用いて検証しなければならない(shall)。

テスト 2：評価者は、待ち時間と期待される監査ログデータをそれぞれ調整して、非アクティブタイマーを 10 分に設定して、テスト 1 を繰り返さなければならない(shall)。

A.1.2 FTA_TSE.1 TOE セション確立

FTA_TSE.1.1 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ければならない（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。*

保証アクティビティ

TSS

評価者は、TSF が、最小限日時と IP アドレスを含めて、他の有効なリモート VPN クライアントセションの確立(例、クライアントクレデンシャルが有効で、期限切れでなく、失効していない等)を拒否できる方法について記述されていることを検証するために TSS を検査しなければならない(shall)。

ガイダンス

評価者は、TSS に記述されたそれぞれの属性について、VPN クライアントセション確立を拒否するようなアクセス制限を有効化する方法についての指示を操作ガイダンスが提供していることを決定するため、操作ガイダンスをレビューしなければならない(shall)。

テスト

評価者は、次のテストを実行しなければならない(shall)：

テスト 1：評価者は、TOE へリモート VPN クライアントへ接続成功し、接続されたクライアントからの IP アドレスを記録して、次にそれをディスコネクトしなければならない(shall)。評価者は、接続からのその IP アドレスを禁止し、同じ VPN クライアントを用いて再接続の試行するために操作ガイダンスに記述されたステップに従い、それが成功しないことを観測しなければならない(shall)。

テスト 2：評価者は、TOE へリモート VPN クライアントを接続成功し、次にそれをディスコネクトしなければならない(shall)。評価者は、特定の日付(これが曜日または具体的な日にちかどうか)から VPN クライアントを禁止するため、操作ガイダンスに記述されたステップに従い、同じ VPN クライアントを用いて再接続を試行し、それが成功しないことを観測しなければならない(shall)。

テスト 3: 評価者は、TOE へリモート VPN クライアントを接続成功し、次にそれをディスコネクトする。評価者は、その VPN クライアントをテストが行われる時間間隔を含む、ある時間帯の間だけ禁止するために操作ガイダンスに記述されたステップに従い、同じ VPN クライアントをもちいて再接続を試行し、それが成功しないことを観測しなければならない(shall)。

テスト 4 : [条件付き] 他の属性が FTA_TSE.1 で識別される場合、評価者は、これらのぞくせいのそれぞれの実施を実証するためにテスト 1 から 3 に類似したテストを実行し、その属性に基づくその接続を拒否するよう TSF を設定し、連続背う接続試行が成功しないことを実証しなければならない(shall)。

A.1.3 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ければならない（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*

保証アクティビティ

TSS

評価者は、プライベート IP アドレスを接続された VPN クライアントへ割り当てるための TSF の能力を TSS にて主張していることを検証するため、TSS をチェックしなければならない(shall)。

ガイダンス

本要件の操作ガイダンスアクティビティはない。

テスト

評価者は、リモート VPN クライアントを TOE へ接続し、TOE の内部 IP アドレスと同様にその IP アドレスを記録しなければならない(shall)。評価者は、2 つの IP アドレスが同じネットワークに属していることを検証しなければならない(shall)。評価者は、リモート VPN クライアントをディスコネクトし、その下位プラットフォームの IP アドレスが、もはや以前のステップで識別されたプライベートネットワークの一部ではないことを検証しなければならない(shall)。

B. 選択ベース要件

本 EP への序説で示す通り、ベースライン要件(TOE または下位プラットフォームによって提供されなければならないもの) は、本 EP の本文に含まれる。本 EP の本文での選択に基づく追加の要件がある；特定の選択がなされると、以下の追加の要件が含まれる必要がある。

B.1 事前共有鍵の選択ベース要件

「事前共有鍵」が NDcPP/FWcPP の FCS_IPSEC_EXT.1.13 で選択される場合に、以下の SFR が主張されなければならない(must)。

B.1.1 事前共有鍵の作成 (FIA_PSK_EXT)

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ければならない（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ければならない（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ければならない（shall））。

FIA_PSK_EXT.1.4 TSF は、ビットベースの事前共有鍵を [選択：受け入れ、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] できなければならない（shall）。

適用上の注釈： *乱数ビット生成器機能は、ベース PP によって提供される。*

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ければならない（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、評価者は確認しなければならない（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ければならない（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ければならない（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ければならない（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ければならない（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ければならない（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ければならない（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 を繰り返さなければならない（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ければならない（must）。

テスト 3 [条件付き] : TOE がビットベースの事前共有鍵を生成しない場合、評価者は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ければならない（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ければならない（shall）。

テスト 4 [条件付き]: TOE がビットベースの事前共有鍵を生成する場合、評価者は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ければならない（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ければならない（shall）。

C. オブジェクティブ要件

本 EP への序説で示す通り、ベースライン要件(TOE または下位プラットフォームによって提供されなければならないもの) は、本 EP の本文に含まれる。望ましいセキュリティ機能を規定する追加の要件があり、これらの要件は、本附属書に含まれる。これらの要件は本 EP の将来のバージョンでオブジェクティブ要件からベースライン要件へ移行するだろう。

現時点では、本製品に特有のオブジェクティブ要件は識別されていない。

D. エントロピー証拠資料とアセスメント

本 TOE は、NDcPP 及び／FWcPP の「エントロピー証拠資料とアセスメント」セクションで概説された要件を越えた、エントロピー源を記述するような、追加の補足情報を要求しない。他のベース PP と同様に、唯一の追加の要件は、ベース PP によって要求される機能に追加して、エントロピー証拠資料についても、TOE の具体的な VPN ゲートウェイ機能に適用することである。

E. 参考文献

識別子	表題
[CC]	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 • パート 1：概説と一般モデル、CCMB-2012-09-001,バージョン 3.1 改訂第 4 版、2012 年 9 月 • パート 2：セキュリティ機能コンポーネント、CCMB-2012-09-002, バージョン 3.1 改訂第 4 版、2012 年 9 月 • パート 3：セキュリティ保証コンポーネント、CCMB-2012-09-003, バージョン 3.1 改訂第 4 版、2012 年 9 月
[CEM]	情報技術セキュリティ評価のための共通方法、 評価方法、CCMB-2012-09-004, バージョン 3.1 改訂第 4 版、2012 年 9 月
[NDcPP]	ネットワークデバイスのコラボラティブプロテクションプロファイル、バージョン 1.0、2015 年 2 月

F. 頭字語

NDcPP 及び FWcPP の頭字語定義は、ここで定義されるものについてして参考にされるべきである。

頭字語	定義
IKE	Internet Key Exchange
TCP	Transmission Control protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network