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
パッケージステートフルトラフィックフィルタファイアウォール

原文タイトル：

Network Device Protection Profile (NDPP) Extended Package
Stateful Traffic Filter Firewall

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。
正式な文書は、以下の URL よりダウンロード可能です。
http://www.niap-ccevs.org/pp/pp_nd_tffw_ep_v1.0.pdf

Information Assurance Directorate

情報保証局

2011 年 12 月 19 日
バージョン 1.0

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

目次

1 序論

この拡張パッケージ（EP）は、ステートフルトラフィックフィルタファイアウォール（ステートフルパケットインスペクションを使用することにより最適化されたレイヤ 3 およびレイヤ 4（IP および TCP/UDP）ネットワークトラフィックをフィルタにかけるデバイスと定義される）のセキュリティ要件を記述しており、明確に定義され、記述された脅威を十分に低減することを目的とした最低限で、ベースライン（必須）の要件を提供することを意図している。この EP は、これ自体で完結しておらず、*ネットワークデバイス*プロテクションプロファイル（NDPP）の*セキュリティ要件*を拡張したものである。このイントロダクションでは、適合 TOE の特徴を記述し、また、本 EP が NDPP と関連してどのように使用されるかについても議論する。

1.1 適合主張

ネットワークデバイス・プロテクションプロファイル（NDPP）の*セキュリティ要件*では、一般に、ネットワークインフラストラクチャーデバイスのベースライン（必須）のセキュリティ機能要件（SFR）およびセキュリティ保証要件（SAR）について定義する。本 EP は、ステートフルトラフィックフィルタファイアウォールネットワークインフラストラクチャーデバイス特有のさらなる SFR および関連のある「保証アクティビティ」により、NDPP ベースラインを拡張するために有用である。保証アクティビティとは、評価者が TOE の SFR への適合性を判断するために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、リビジョン 3 に準拠している。これは CC パート 2 を拡張したものであり、CC パート 3 に適合している。

1.2 本拡張パッケージ使用方法

NDPP の EP として、本 EP および NDPP の内容はいずれも、製品特有のセキュリティターゲットの文中に適切に混在していると予想される。本 EP では、その際、難しいまたはあいまいなものとならないように（should）、具体的に定義されている。ST では、適合の主張において、適用可能な NDPP のバージョン（現バージョンについては、http://www.niap-ccevs.org/pp/を参照）および本 EP を確認しなければならない（must）。

1.3 適合する評価対象

本 EP は、ファイアウォール関連のセキュリティ機能を導入しているネットワークデバイスの評価に関する要件を定義する一連の関連 EP のひとつである。こうした製品は、一般に、バウンダリープロテクションデバイスまたは専用ファイアウォール、ルーター、おそらく付属ネットワーク間での情報の流れを管理するためにデザインされたスイッチなどの一連のデバイスである。ファイアウォール関連セキュリティ機能を導入しているネットワークデバイスは、数多くある用途のなかで唯一となる２つの異なるネットワーク（信頼されたまたは保護されたエンクレーブとインターネットなど、信頼できない外部ネットワーク）を分離する際に有用である場合もある。一般的に、ファイアウォールには、幅広い範囲の設定およびネットワーク情報の流れに関するポリシーを有効にする複数の物理的および論理的ネットワークが接続されている。

本 EP では、特に、ネットワークレイヤ 3 および 4 のステートフルトラフィックフィルタリングを実施するネットワークデバイスについて検討する。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、２つ以上の異なるネットワークに接続するハードウェアおよびソフトウェアから構成されるデバイスであり、企業全体のネットワークにおいて基盤的な役割がある。

本 EP は、NDPP 上に作成されているため、適合 TOE は、引き続き本書で検討する脅威環境に対して、本 EP においてさらに定義した機能性のほかに、NDPP に必要な機能性を導入することが義務付けられている。簡潔にいうと、適合 TOE では、ネットワークレイヤ 3 および 4 のトラフィック属性（すなわちアドレスおよびポート）に応じて設定された規則に基づく付属ネットワーク間の情報の流れ（すなわちパケット）と潜在的にはネットワークレイヤ 7 までの導出セッション状況情報を管理する。

本 EP の一連の要件は、最終利用者にある程度の価値を提供できるようなより速く、低コストで評価されるため

の範囲に限定されることを意図している。本 EP の草案をさらに考慮し、附属書にはオプションの機能性について記載する（トランスペアレントモードなど）。今後のファイアウォール EP は、一連の追加機能（例えば、アプリケーションフィルタリング）を特定するために使用し、その後、ST 執筆者が追加機能を特定するために使用できる。本 EP の本文中では、このような追加機能は、評価を行うことを目的としている場合には、単に無視されている。ただし、本書で定義したセキュリティ要件による何らかの影響がある場合を除く。このほかの例としては、ネットワークアドレス変換（NAT）またはポートアドレス変換（PAT）が挙げられる。本 EP に対して評価を行うデバイスの多くは、NAT または PAT を行う可能性がある一方で、この可能性を特定する要件は存在しない。NAT および PAT は、主にセキュリティメカニズムではないとの前提条件に基づいてこうした判断が行われたが、このような設置を行うことによって、ネットワークトポロジーが隠れることを意味していると考えられている場合もあるが、これはむしろネットワークを指定する便宜上作成されたものである。

２セキュリティ課題記述

ステートフルトラフィックフィルタファイアウォールにより、保護ネットワークへの潜入および保護ネットワークからの流出に関与するセキュリティ脅威の範囲を指定する。「*保護ネットワーク*」という用語は、本書ではアクセスを管理するために規則が定義されている付属ネットワークを示すために用いる。このため、ある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、保護されているか否かにかかわらず、それぞれ特定の設定に応じてさまざまな付属ネットワークを同時に有する可能性がある。また、付属ネットワークはいずれも、認可された管理者の判断により*保護できる*と推定されることを明確にするべきである（should)。

以下に示す用語「イングレストラフィック」は、保護ネットワーク外に存在する脅威エージェントからのトラフィックを示し、以下に示す用語「エグレストラフィック」は、保護ネットワーク内に存在する脅威エージェントからのトラフィックを示す。適用可能な脅威には、情報の不正公開、不適切なサービスへのアクセス、サービスの誤用、サービス運用妨害（DOS）およびネットワークベースの偵察などが挙げられる。しかし、こうしたデータに関連して、脅威エージェントが存在する場所は重要ではない。例えば、データの流出は、データを削除するための適切な認可なくデータが削除されたことを意味する。こうしたデータは、出し入れ可能である。これは、外部からの潜入またはインサイダーの行為の結果と考えられる。サイトには、ファイアウォールをニーズに適合させるためのセキュリティ方針の作成および規則集の作成を行う責任がある。

本 EP では、こうした方針および規則にすべて適合することに注力しており、このため、本 EP は NDPP に依存してはいるが、NDPP に記載されている脅威について、繰り返し記載していない点に留意のこと。また、NDPP では、TOE がセキュリティ機能を提供する性能に対する脅威についてのみ記載され、本 EP では、運用環境での資源に対するビジネス上の脅威についてのみ検討している点に留意のこと。NDPP の脅威および本 EP で定義されている脅威ではいずれも、ステートフルトラフィックフィルタファイアウォール TOE によって指定される一連のセキュリティ上の脅威について、包括的に定義する。

2.1 情報の不正公開

保護ネットワーク上のデバイスは、保護ネットワーク外に設置されたデバイスによる脅威を受ける可能性があり、これは、不正行為が行われようとしていると考えられる可能性がある。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状態にある場合または保護ネットワーク上のデバイスがこうした他のデバイスとの通信を構築できる場合（*フィッシング*エピソードの結果として、または電子メールメッセージへの不注意な対応によるなど)、こうした内部デバイスは情報の不正公開の影響を受けやすい可能性がある。

また、ステートフルトラフィックフィルタファイアウォールでは、潜入が見込まれることから、特定の*送信先*ネットワークアドレスおよび保護ネットワーク内のポートのみにアクセスを制限するために有用である。こうした制限を設定することにより、一般的なネットワークポートのスキャニングが保護されているネットワークまたは設備で行われないようにすること、または保護されたネットワーク上の情報へのアクセスを認定されたネットワークノード上に特に設定されたポートから得られるアクセスに制限することなどができる（指定された企業のウェブサーバのウェブページなど)。また、今後、情報の公開を制限することによって、特定のネットワークまたはネットワークノードを保護ネットワークへのアクセスからブロックできるようにアクセスを特定の *ソース*アドレスおよびポートのみに制限できる。

また、ステートフルトラフィックフィルタファイアウォールでは、流出が見込まれることから、情報を広められる方法および場所が制限されている他のネットワークに保護ネットワーク上で作動するネットワークノードを接続し、通信できる手段を制限するために有用である。
特定の外部ネットワークを一斉にブロックできるか、またはエグレスを特定のアドレスまたはポートのいずれか一方またはその両方に制限できる。その代わりに、保護ネットワーク上のネットワークノードを使用できるエグレスのオプションは、たとえば、追放することによりデータの不正公開をさらに低減するために認可ずみ

プロキシまたはフィルタにより外部への接続ルートを確実に決定することを目的として、注意深く管理することができる。

(T.NETWORK_DISCLOSURE)

2.2 不適切なサービスへのアクセス

保護ネットワーク外にあるデバイスでは、デバイス保護ネットワーク内からのみアクセスすることを意図した保護ネットワーク上のサービスの実施に努めることができる。同様に、保護ネットワーク外に設置されているデバイスでは、保護ネットワーク内からの不適切なアクセスとなるサービスを提供する可能性がある。

ステートフルトラフィックフィルタファイアウォールでは、イングレスが見込まれることから、こうした外部消費用ネットワークサーバのみおよび目的とするポートのみ経由してアクセスできるように設定できる。これは、保護ネットワーク外のネットワークエンティティにとっては、保護ネットワーク内の消費またはアクセスのみに向けたネットワークサーバまたはサービスにアクセスする可能性を低減するために有用である。

また、ステートフルトラフィックフィルタファイアウォールでは、エグレスが見込まれることから、保護ネットワーク内からは特定の外部サービスのみアクセスできるように(送信先ポートを利用するなど)設定できる。例えば、外部メールサービスへのアクセスをブロックして、管理されていない電子メールサーバへのアクセスに対して企業方針を施行することができる。この関連で、外部サーバが代わりとなるポート（例えばこれは、アプリケーションフィルタファイアウォールがさらに信頼できる保護を提供している場所である）でサービスを提供できるため、ステートフルトラフィックフィルタファイアウォールの有効性がかなり制限されている点に留意のこと。

(T. NETWORK_ACCESS)

2.3 サービスの誤用

特に保護ネットワーク内で提供される*公共の*サービスへのアクセスが許可されている一方で、保護ネットワーク外に設置されているデバイスは、公共サービスが許可されているネットワークとの通信を行う上で不正行為を行う可能性がある。保護ネットワーク内から提供される特定のサービスでも、保護ネットワーク外からアクセスした場合、リスクを示す可能性がある。

一般に、外部ネットワーク上で動作するエンティティでは、イングレスが見込まれることから、ある保護ネットワークの使用方針による制限がないと仮定される。それにもかかわらず、ステートフルトラフィックフィルタファイアウォールでは、公的に利用できるサービスについて公表されている使用法の違反を示す可能性のある方針違反行為を記録できる。

ステートフルトラフィックフィルタファイアウォールでは、エグレスが見込まれることから、保護ネットワークの使用方針の施行および監視を補助するために設定することができる。他の脅威にて説明したとおり、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、データの配布、外部サーバへのアクセスのほか、サービス運用妨害（DOS）を制限するためにも有用である。これらはすべて保護ネットワークの使用方針に関与している可能性がある。また、ある面では、これらの施行を条件としている。また、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、保護ネットワークと外部ネットワーク間でのネットワークの使用を記録するように設定でき、その結果は使用方針の違反を認定するために有用である。

(T.NETWORK_MISUSE)

2.4 サービス運用妨害（DOS）

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、保護ネットワーク外から大量の協定サービスリクエストを受けた場合に、資源の枯渇に関連するサービス運用妨害（DOS）攻撃に対して脆弱である可能性がある。

ステートフルトラフィックフィルタファイアウォールでは、イングレスが見込まれることから、こうした外部消費用ネットワークサーバのみおよび目的とするポートのみ経由してアクセスできるように設定できる。その結果、攻撃は、そのために設定した（「強化した」など）サーバおよびサービスの選択に制限することができる。これは有効な攻撃面を少なくし、内部サーバへの外部ネットワークによる攻撃の可能性を軽減するために有用である。こうした外部からアクセス可能なサーバに対する攻撃は、攻撃手口を低減する可能性のある設定ポートに制限される。

ステートフルトラフィックフィルタファイアウォールでは、エグレスが見込まれることから、保護ネットワーク内からは特定の外部サービスのみアクセスできるように（送信先ポートを利用するなど）設定できる。例えば、外部メールサーバへのアクセスをブロックし、ウイルス、悪意のあるソフトなどの取り込みに繋がる可能性があり、最終的に保護ネットワーク上でのサービス運用妨害（DOS）となる電子メールベースの攻撃機会を低減することができる。外部サーバが代わりとなるポート（例えばこれは、アプリケーションフィルタファイアウォールがさらに信頼できる保護を提供している場所である）でサービスを提供できるため、ステートフルトラフィックフィルタファイアウォールの有効性が、かなり制限されている点に留意のこと。しかし、ロギングは、阻止できなかったサービス運用妨害（DOS）（ウイルスの拡散または「ボットネット」行為パターンの検出など）を確認する際に有用となり得る。

(T.NETWORK_サービス運用妨害（DOS）)

3 セキュリティ対策方針

第二節に記載されているセキュリティ課題は、主にステートフルトラフィックフィルタリング性能により対処する。適合 TOE により、TOE に対する脅威に対処し、法律または規制により課せられている方針を施行するセキュリティ機能性が得られる。以下の節では、前述の脅威または方針に適合する必要のあるセキュリティ対策方針について説明する。セキュリティ対策方針に関する説明は、[NDPP]に記載した説明に追加するものである。

注意：以下の各節では特定のセキュリティ対策方針を確認し（O により強調表示）、対策方針を満たすためのメカニズムとなる関連のあるセキュリティ機能要件（SFR）に適合させる。

3.1 アドレスベースフィルタリング

情報の不正公開、サービスへの不適切なアクセス、サービスの誤用・途絶・妨害及びネットワークベースの偵察に関連する問題に対処するには、適合 TOE、ステートフルトラフィックフィルタリング性能を実装する。この機能では、確立された接続情報とともに、適用可能なネットワークトラフィックを発信（送信元）するかまたは受信（送信先）するかのいずれか一方またはその両方のネットワークノードのネットワークアドレスに基づいて、保護ネットワークとその他の付属ネットワークとの間でのネットワークトラフィックの流れを制限する。

(O.ADDRESS_FILTERING → FFW_RUL_EXT.1)

3.2 ポートベースフィルタリング

さらに情報の不正公開などに関連する問題に対処するためには、確立されている接続情報と同様に、適合 TOE のポートフィルタリング機能により、保護ネットワーク及びネットワークトラフィックで確認される発信（送信元）ポート（またはサービス）または受信（送信先）ポート（またはサービス）に基づくその他の付属ネットワーク間でのネットワークトラフィックの流れを制限する。

(O.PORT_FILTERING → FFW_RUL_EXT.1)

3.3 ステートフルインスペクション

ステートフルパケットインスペクションは、TOE を介したパケットフローの実行を補助するために使用される。TOE では、TOE インタフェースで処理するそれぞれのパケットに対する規則集を適用するというよりも、パケットが「承認済み」の確立されている接続に属するか判断する。パケットが確立されたセッションの一部であるか否かを判断するために使用される最低限の属性セットは、TCP 用及び UDP 用に指定され、ST 執筆者は、TCP セッションが考えられる属性を拡張し、希望に応じて、ICMP プロトコルを追加できる。

(O.STATEFUL_INSPECTION → FFW_RUL_EXT.1)

3.4 関連接続フィルタリング

ここでは、「動的規則」の作成に関する概念を検討する。これにより、予想されるアプリケーション層のプロトコルのふるまいにより、規則集で許可されている接続を作成することにより、新しい接続またはパスが作成される。ファイル転送プロトコルは、こうしたプロトコルの一例であり、許可されているコマンド接続に対応してデータ接続が作成される。

(O.RELATED_CONNECTION_FILTERING → FFW_RUL_EXT.1)

3.5 システムモニタリング

ステートフルトラフィックフィルタリング機能の動作をモニターできるシステム管理者の問題に対処するには、本セキュリティ対策方針は、NDPP で開始されたものであり、以下のとおり拡張される。

適合 TOE では、ネットワークトラフィックの流れをログする性能を実装する。具体的には、ネットワークトラフィックが設定された規則に適合していることが明らかである場合、TOE には、管理者が「ログ」するためのファイアウォール特定のファイアウォール規則を設定する手段が提示される。その結果、「ログ」するために設定されたファイアウォール規則に適合することにより、適合が発生すると必ず、情報提供イベントログとなる。

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

3.6 TOE 管理

信頼できるステートフルトラフィックフィルタリング性能の管理手段で、関連のある課題に対処するには、NDPP で開始された本セキュリティ対策方針は、以下のとおり拡張される。*NDPP に記載されている要件に従って、以下に示す機能の使用が保護されていると仮定している点に留意のこと。*

適合 TOE では、TOE よって施行されるファイアウォール規則を設定するにあたって管理者に必要な機能を提示

する。

(O.TOE_ADMINISTRATION → FMT_SMF.1)

4 セキュリティ要件

本節には、TOE セキュリティ機能要件及び評価者が行う保証アクティビティについて記載する。

4.1 表記法

本 EP での SFR は拡張されているが、本 EP、その他の EP または PP では、SFR は柔軟性のある使用方法において定義され、このため、本 EP の文中でこうした操作が行われる。

CC は、セキュリティ機能要件についての次に示す操作を定義している：割付、選択、選択及び詳細化に含まれる割付。この文書は、CC で定められた操作を識別するために次のようなフォント表記法を用いる。

- 割付：イタリック書体で表記する；
- EP 作者による詳細化：太字、及び必要ならば取消し線で表記する；
- 選択：アンダーラインで表記する；
- 選択における割付：イタリック及びアンダーラインで表記する；
- 繰返し：(1)、(2)、(3)など、括弧内に 繰返し回数を追加することにより表記する

4.2 TOE セキュリティ機能要件

本 EP には、10 の要素から成る 1 つの SFR コンポーネントがある。ステートフルトラフィックフィルタ SFR のほかに、NDPP に規定されている SFR にさらに 2 つ（FAU_Gen.1（2 つの監査事象が追加）及び FMT_SMF.1（ファイアウォール規則を設定するための管理機能））が追加されている。

4.2.1 FFW_RUL_EXT.1　　ステートフルトラフィックフィルタリング

FFW_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でステートフルトラフィックフィルタリングを実行しなければならない(should)。

適用上の注意：この要素は、TOE インタフェースで処理されるネットワークパケットに適用される方針（ステートフルトラフィックフィルタリング）として特定される。いずれのパケットも、適用する本方針が記載されている規則集があるか、またはそのパケットが確立された接続に属しているかを判断するかによって、TOE のインタフェースで受領される。本コンポーネント内のその他の要素は、方針の詳細事項について記載している。

TOE にも根本的なプラットフォームが含まれており、規則集にフローを許可する規則が含まれない限り、または、パケットのフローが許可され、確立された接続に属していると考えられない限り、ネットワークパケットをフローさせることができない点に留意することが重要である。このため、TOE 開始時及び TOE が遭遇する可能性のある不具合発生時には、原則として「true」を保持しなければならない（must)。

FFW_RUL_EXT.1.2　　TSF は、以下のネットワークトラフィックプロトコルを処理しなければならない：
- インターネットコントロールメッセージプロトコルバージョン 4（(ICMPv4)
- インターネットコントロールメッセージプロトコルバージョン 6（ICMPv6)
- 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)
- 転送コントロールプロトコル（TCP)
- 利用者データグラムプロトコル（UDP)

本 SFR の他の要素において指定された範囲で、以下の RFC によって定義されたネットワークパケット・ヘッダーフィールドを調査できる。
- RFC 792（ICMPv4)
- RFC 4443（ICMPv6)

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

適用上の注意：この要素ではプロトコルを特定し、インポート時（ネットワークトラフィックの受信またはイングレス（ingress)）及びエクスポート時（ネットワークトラフィックの送信時もしくは送信用のフォーマット時、またはエグレス（egress)）に、ネットワークトラフィックがTOEによって説明できる範囲を定義する際に有用なプロトコルの定義について記載する。

RFCに記載されているプロトコルのフォーマッティングを依然として使用する一方で、多くのRFCでは、準拠するには安全であるとは考えられないふるまいを定義している。例えば、RFC792では、相手方から発信された場合に安全だと考えられない「リダイレクト」ICMPタイプ、そのソース（送信元）を検証できないため安全ではない「ソースクエンチ」メッセージを定義していた。

FFW_RUL_EXT.1.3 TSF は、以下のネットワークプロトコルフィールドを使用するフィールドステートフルトラフィックフィルタリング規則の定義しなければならない：

-ICMPv4
- o タイプ
- o コード

-ICMPv6
- o タイプ
- o コード

-IPv4
- o 送信元アドレス
- o 送信先アドレス
- o トランスポート層プロトコル

-IPv6
- o送信元アドレス
- o 送信先アドレス
- o トランスポート層プロトコル

-TCP
- o 送信元ポート
- o 送信先ポート

-UDP
- o 送信元ポート
- o 送信先ポート

及び別のインタフェース

適用上の注意：この要素では、本要件によって施行される規則を構築するにあたって適用可能なさまざまな属性を特定する。適用可能なインタフェースは、TOE の属性であり、残りの確認済みの属性は、関連 RFC 中に定義されている。「トランスポート層プロトコル」は、適用可能なプロトコル（TCP、UDP、ICMP または GRE など）を特定する IPv4/IPv6 フィールドである点に留意のこと。また、上述の「インタフェース」とは、適用可能なネットワークトラフィックを受信するか、または交互に送信する外部ポートである。

FFW_RUL_EXT.1.4　TSF では、ステートフルトラフィックフィルタリング規則に関連する操作（許可、拒否、ログ）を許可しなければならない（shall）

適用上の注意：本要素では、ネットワークトラフィックを適合させるために使用する規則に関連する可能性のある操作を定義する。ログされるデータは、セキュリティ監査要件第 4.2.2.節に記載されている点に留意のこと。

FFW_RUL_EXT.1.5　TSF では、ステートフルトラフィックフィルタリング規則をそれぞれ異なるネットワークインタフェースに割付けできるようにしなければならない（shall）：

適用上の注意：この要素では、規則を割付けられる場所を特定する。具体的には、適合 TOE では、レイヤ 3 及び 4 ネットワークトラフィックを扱うそれぞれが適用可能であり、識別可能な各ネットワークインタフェース特有のフィルタリング規則を割付けることができなければならない（must）。具体的には、「識別可能」とは、TOE 内ではそのインタフェースが固有のものであり、識別可能であり、ネットワークの観点から必ずしも目に見える必要はない（例えば、割付けられた IP アドレスを所有する必要はない）ことを意味する。それぞれのネットワークインタフェースとは、TOE において共通の論理パスを共有する 1 箇所以上の物理的接続である。例えば、TOE には多数の物理的ネットワークポートに曝露される SFP モジュールをサポートする SFP ポートがある可能性があるが（might）、しかし、これはすべての外部ポートに対して共通のドライバーを使用するため、１つのネットワークインタフェースとして扱うことができる。

それぞれのインタフェースによって異なる規則集または特定のインタフェースと何らかの関連のある共有規則集である可能性がある点に留意のこと。

FFW_RUL_EXT.1.6　TSF は、以下でなければならない（shall）：
a)以下のプロトコルのために許可され、確立されたセッションに適合する場合、さらにステートフルトラフィックフィルタリング規則を処理することなくネットワークパケットを承認する：以下のネットワークパケット属性に基づく TCP、UDP、[選択：ICMP、他のプロトコルなし]：

1. TCP：送信元及び送信先アドレス、送信元及び送信先ポート、シーケンス番号、フラグ

2. UDP：送信元及び送信先アドレス、送信元及び送信先ポート

3. [選択：‘ICMP:送信元及び送信先アドレス[選択:タイプ、コード[*割付：適合属性リスト*]]’他のプロトコルなし]

b)以下に基づいて既存のトラフィックフローを確立されている一連のトラフィックフローから除去する：[選択：セッション静止タイムアウト、予測された情報の流れの完了]。

適用上の注意：この要素では、完全に処理した設定規則とは対照的に、セッションが確立され、トラフィックフローを判断するために使用されるといった状況を TOE が判断及び管理できるプロトコルが特定されることを必要とする。また、本要素では、ネットワークパケットが適合しているか及び確立したセッションが特定されているかを判断するために、適用可能な属性が使用されることを必要とする。

プロトコルとして ICMP を選択する際に、パケットが確立された「接続」に属しているか否かを判断する場合、送信元アドレス及び送信先アドレスを考慮する必要がある。ICMP パケットが確立された接続フローにおいて考えられるものであるか否かを判断する場合に、さらに頑健な性能とするためにこのタイプ及びコードの属性を使用する可能性がある。例えば、エコーリクエストを受領していない場合、エコーによる返答がフローの一部となることは期待していない。IPv6 属性を使用する可能性のある（may 実装については、ICMP 属性を選択するにあたって、オープン割付が残存する。

本要素の項目 b)では、TCP パケットにおいて FIN フラグを用いたいずれか一方のエンドポイントにより開始された TCP セッションを終結させるなどの事象を監視することによって、ファイアウォールが一連の確立された情報の流れから確立された情報の流れを取り除くべきであるか否かを判断できる方法を特定することを必要としている。プロトコルを異なる方法で扱う場合、ST によりこうした違いが特定されることが想定される。

FFW_RUL_EXT.1.7　TSF は以下のネットワークプロトコルを処理できなければならない（shall）:
1.FTP、
2.[選択:H.323:*[割付：他のサポートプロトコル]*、他のプロトコルなし]、

規則を同時に定義するか、または以下のタイプのネットワークトラフィックが可能なセッションを確立する:

-FTP: RFC 959 に記載されているとおり、FTP プロトコルに準拠している TCP データセッション
- [選択：*[割付：さらにサポートしたプロトコル及びこうしたプロトコルに基づいて許可されるネットワークトラフィックのタイプのリスト]*、なし]。

適用上の注意：本要素では、既存の規則には明確にフローを許可していない場合でも、ネットワークトラフィックが可能なファイアウォールとするためにさらに複雑なプロトコルを特定することを必要とする。例えば、FTP プロトコルでは、利用者がファイルを転送する場合、コントロール接続及びデータ接続をいずれも必要とする。ポート 21（FTP サーバ上のコントロールポート）及びポート 20（アクティブモードのサーバ上のデータポート）など、よく知られたポートが含まれる場合、顧客側で使用される 1023 個を超えるランダムポートがある。受動モードでは、FTP サーバは、ポート 20 の代わりに 1023 個を超えるランダムポートを使用できる。データ接続は、受動モードの顧客によって開始され、能動モードの FTP サーバによって模倣される。

こうしたタイプのプロトコルでは、規則集が拒否する可能性があっても（規則では、顧客またはおそらくサーバによって使用されるランダムポートが予測できないため、拒否するための初期設定の規則を適用する可能性があるなど)、「新しい」接続を確立できる。TSF では、トラフィックフローを管理する動的規則を作成できる可能性がある。または、TSF は、RFC に指定されているとおり、プロトコルを実装するにあたっての期待値に基づいて、暗示的に新しい接続を確立できる可能性がある。

いかなるネットワークパケットもレイヤ 4（TCP/UDP）を超えて調査されることは期待されていない点に留意することが重要である。本要件では、単に予測不可能な UDP/TCP ポートに期待された接続が正確に確立されるために、ST 執筆者がファイアウォールに「穴をあける」条件を規定することを必要としている。

ST 執筆者がさらにプロトコルを含む場合、上記第 2 項の FTP で行ったとおり、プロトコルのふるまいを規定した RFC を特定しなければならない（must)。

FFW_RUL_EXT.1.8　TSF では、以下の初期設定のステートフルトラフィックフィルタリング規則をすべてのネットワークトラフィック上で施行しなければならない（shall）。

1. *TSF では、無効なフラグメントのパケットを拒否し、ロギングできなければならない（shall）。*
2. *TSF では、完全に再度組み立てることのできないフラグメント化された IP パケットを拒否し、ロギングできなければならない（shall）。*
3. *ネットワークパケットの送信元アドレスがネットワークパケットを受領したネットワークインタフェースのアドレスと同じ場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
4. *ネットワークパケットの送信元アドレスがネットワークパケットを受領したネットワークインタフェースと関連のあるネットワークに従属していない場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
5. *ネットワークパケットの送信元アドレスがブロードキャストネットワーク上にあると定義されている場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
6. *ネットワークパケットの送信元アドレスがマルチキャストネットワーク上にあると定義されている場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
7. *ネットワークパケットの送信元アドレスがループバックアドレスであると定義されている場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
8. *ネットワークパケットの送信元アドレスがマルチキャストである場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
9. *ネットワークパケットの送信元または送信先アドレスがリンクローカルアドレスである場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
10. *IPv4 の RFC 5735 に記載されているとおり、ネットワークパケットの送信元アドレスまたは送信先アドレスが「今後使用するための保存」アドレスと定義されている場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
11. *IPv6 の RFC 3513 に記載されているとおり、ネットワークパケットの送信元アドレスまたは送信先アドレスが「不特定アドレス」または「今後定義及び使用するための保存」アドレスと定義されている場合、TSF は、ネットワークパケットを拒否し、ロギングできなければならない（shall）。*
12. *TSF は、IP オプション（ルーズソースルーティング、ストリクトソースルーティング、規定されたレコードルートなど）付きのネットワークパケットを拒否し、ロギングできなければならない（shall）：*

13. [選択：*[割付：TOE によって施行される他の初期設定規則]*その他の規則なし]。

適用上の注意：本要素では、必ず適用する最低限の初期設定規則について定義する。パケットが上記に記載された規則に基づいて拒否される可能性がある場合、関連のある攻撃を検出できるように TOE もロギングできる必要がある点に留意のこと。ログされるデータは、セキュリティ監視要件で特定されている点に留意のこと。

上記項目 1 及び 2 では、TOE によるフラグメント化したパケットの処理方法について記載する。項目 1 では、無効なフラグメントの概念について記載し、これにより ST 執筆者は、無効なフラグメントの構成を定義できる。実装が容認される場合には、フラグメント化したパケットはいずれも無効であると考えられる。他に実装が容認される場合には、以前受領したフラグメントと一部重なるフラグメント化したパケットを無効と考えることができる。項目 2 では、規則集は、フラグメント化したパケット攻撃の脅威に対処するために、パケットを再度組み立てる場合のみ適用とすることを確認している。項目 1 では、無効フラグメントのロギングには、無効フラグメント内でフラグメントがなくなっているため、パケットヘッダーにおいて予想されるすべてのフィールドを含むことはできない可能性がある点に留意のこと。

項目 4 では、ネットワークインタフェースと「関連のあるネットワーク」がそのインタフェースと関連のある即時サブネットを超えることを目的としている。例えば、ネットワークトポロジーには、ルーター及びファイアウォールインタフェースの「後部」にあるサブネットを含む。ルーズ RPF を適用できない場合、この事例であるか否かを判断するために、ストリクト RPF（Strict Reverse Path Forwarding）の実装は容認できる。このほかに容認できる実装例には、この初期設定を無効にできるアクセス管理リストの使用が挙げられる。

項目 13 では、（規則集を定義した管理者が特定されているか否かにかかわらず）施行される規則をさらに規定できるようにしている。ここに規定された規則のタイプには、クリスマスツリーパケットのフィルタリング、既存の接続に関連のない非 SYN パケットのフィルタリング及びスプリットハンドシェイク（split handshake）接続のフィルタリングなどが含まれる可能性がある。本要素でも、到達できないホストであるために ICMP レスポンスなどパケットのフローを*許可する*ふるまいを示すために使用できる可能性がある。

FFW_RUL_EXT.1.9　FFW_RUL_EXT.1.6 または FFW_RUL_EXT.1.7 を適用しない場合、TSF は、管理者の定義した以下の順で適用可能なステートフルトラフィックフィルタリング規則（FFW_RUL_EXT.1.5 に従って決定したとおり）を処理しなければならない（shall）。

適用上の注意：本要素では、管理者は、設定されたフィルタリング規則に適合するために処理する順番を定義できるものとする。

FFW_RUL_EXT.1.10　FFW_RUL_EXT.1.6 または FFW_RUL_EXT.1.7 を適用しない場合、適合規則を確認していない場合には、TSF は、パケットフローを拒否しなければならない（shall）。

適用上の注意：本要素では、いずれの規則も適用されず、他の操作も必要とされない場合、パケットが確立されたセッションに含まれる場合を除き、必ずしも禁止する必要はないが、必ずネットワークトラフィックを拒否するふるまいとすることを必要とする。

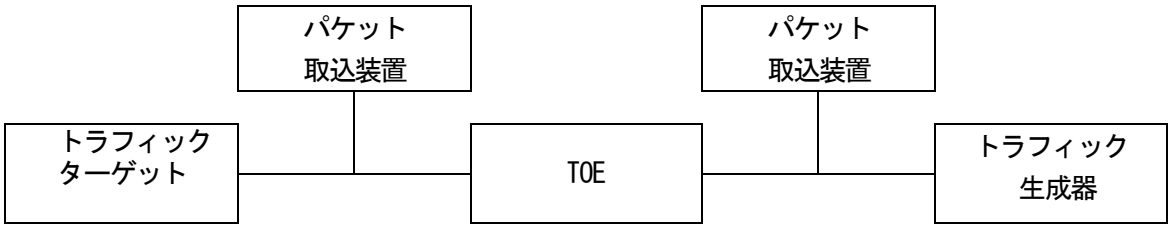
4.2.1.1 保証アクティビティ

以下の表には、FFW_RUL_EXT.1 に準拠していることを確認するために評価者が実施する保証アクティビティについて示す。保証アクティビティは、ST の TSS に必要な内容、TOE 操作ガイダンスに必要な内容、評価者が単独で行う必要のある必要なテスト活動に対処することを目的としている。

評価者は、セッションの確立、セッションパケットの修正または作成にあたって適切なツールがあり、また、これらのパケットの内容を検討する場合と同様に、評価者は、TOE を介してパケットを得るか否かを認知していると仮定する。一般に、TOE のトラフィックフィルタファイアウォール規則の設定機能及びロギング機能は、必要に応じて、適切な決定に到達するために使用できることが期待される。

以下に示すテストは、各ネットワークインタフェースのタイプに対して、繰返し行う必要がある。インタフェースのタイプを定義するにあたって（すべてのパケットが TOE 内の同じ論理パスを介して処理される)、本 EP に記載されているセキュリティ方針に適合する TOE を介してパケットを取得できるすべての論理パスを確認するためにテストを行う必要がある。

評価者は、最低限でも以下に示す環境と同様のテスト環境を構築しなければならない（shall)。 また、評価者は、テスト環境が異なる場合は、必ず正当な理由を示すべきである（must)。



4-1 FFW_RUL_EXT.1 保証アクティビティ

SFR	アクティビティ	保証アクティビティ
FFW_RUL_EXT.1.1	TSS	評価者は、TSS には、TOE の初期化/開始プロセスに関する説明が記載されていることを検証しなければならない（shall)。これには、ネットワークパケットの処理が開始される場所が明確に表示され、この処理中にパケットがフローできないとするアサーションを裏付ける詳解が提示される。 評価者は、TSS にはネットワークパケットの処理に関するコンポーネント(例えば、プロセスまたはタスクなどのアクティブエンティティなど）を特定する注釈が記載され、コンポーネントの不具合発生時には、規則集を適用せずに TOE を介してパケットがフローしないように保護手段が記載されていることを検証しなければならない（shall)。 これにより、完了したプロセスまたはコンポーネント内の不具合（メモリバッファが一杯になる、パケットを処理できないなど）などのコンポーネントの不具合を対象とすることができる。
	ガイダンス	本要件に関連する操作ガイダンスは、次のテスト保証アクティビティにおいて評価する。
	テスト	テスト１：評価者は、TOE を初期化する間、TOE を介してネットワークトラフィックをフローさせるよう試みなければならない（shall)。規則集によって別に定義されているネットワークパケットの安定したフローは、あらゆるネットワークトラフィックが許可されているかどうかリッスンするパケットスニファにより、TOE のインタフェースで指示されるべきである。 注意：規則集の適用に関するその他のテストについては、次のテスト保証アクティビティに記載する。

SFR	アクティビティ	保証アクティビティ
FFW_RUL_EXT.1.2	TSS	評価者は、TSS には以下のプロトコルがサポートされていることが記載されていることを検証しなければならない（shall）。 - RFC 792（ICMPv4） - RFC 4443（ICMPv6） - RFC 791（IPv4） - RFC 2460（IPv6） - RFC 793（TCP） - RFC 768（UDP） 評価者は、TSS に TOE 開発者によって、確認された RFC との適合性がどのように判断されているか（例えば、第三者相互運用性テスト、プロトコル適合テスト）について記載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、操作ガイダンスには以下のプロトコルがサポートされていることが記載されていることを検証しなければならない（shall）。 - RFC 792（ICMPv4） - RFC 4443（ICMPv6） - RFC 791（IPv4） - RFC 2460（IPv6） - RFC 793（TCP） - RFC 768（UDP） ガイダンスに、TOE によって処理される他のプロトコルが記載されている場合、これらのプロトコルが TOE 評価の一部として考えられていない点について明らかにするべきである。
	テスト	本要件に関連するテストは、次のテスト保証アクティビティにおいて取り上げる。
FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4/FFW_RUL_EXT.1.5	TSS	評価者は、TSS には、ステートフルパケットフィルタリング方針が記載されていることを検証しなければならない（shall）。また、以下の属性が関連プロトコルのステートフルトラフィックフィルタリング規則内で設定可能であることを確認する。 -ICMPv4 o タイプ o コード -ICMPv6 o タイプ o コード -IPv4 o 送信元アドレス o 送信先アドレス o トランスポート層プロトコル -IPv6 o送信元アドレス o 送信先アドレス o トランスポート層プロトコル -TCP o 送信元ポート o 送信先ポート -UDP o 送信元ポート o 送信先ポート

SFR	アクティビティ	保証アクティビティ
		評価者は、それぞれの規則がアクション（許可、拒否及びログ）を特定できることを検証しなければならない（shall）。 評価者は、TSSにより、ステートフルパケットフィリタリング方針に従ってすべてのインタフェースが特定され、規則がどのようにそれぞれのネットワークインタフェースに関連しているかを説明していることを検証しなければならない（shall）。インタフェースを一般的なインタフェースタイプ（例えば、同じ内部論理パスを使用している場合、おそらく一般的なデバイスドライバーを使用している場合など）に分類できる一方で、それぞれのネットワークインタフェースとして集合的に扱うことができる。
	ガイダンス	評価者は、操作ガイダンスでは、以下の属性が関連のあるプロトコルのステートフルトラフィックフィルタリング規則内で設定可能であるとして、特定されていることを検証しなければならない（shall）。
		-ICMPv4 o タイプ o コード -ICMPv6 o タイプ o コード -IPv4 o 送信元アドレス o 送信先アドレス o トランスポート層プロトコル -IPv6 o送信元アドレス o 送信先アドレス o トランスポート層プロトコル -TCP o 送信元ポート o 送信先ポート -UDP o 送信元ポート o 送信先ポート
		評価者は、操作ガイダンスでは、各規則によりアクション（許可、拒否及びログ）を特定できることが記載されていることを検証しなければならない（shall）。 評価者は、操作ガイダンスにて、規則がどのようにそれぞれのネットワークインタフェースに関与しているか説明していることを検証しなければならない（shall）。 評価者は、操作ガイダンスにおいて、それぞれのネットワークインタフェースのタイプを決定する方法について説明していることを検証しなければならない（shall）。 評価者は、操作ガイダンスにおいて、それぞれのネットワークインタフェースのタイプを決定する方法（それぞれのネットワークインタフェースのデバイスドライバー決定方法など）について説明していることを検証しなければならない（shall）。
	テスト	テスト1：評価者は、以下のそれぞれの属性のパケットを許可、拒否、ログするステートフルパケットフィルタファイアウォール規則を作成できるかテストするために、操作ガイダンスに記載されている指示を適用しなければならない（shall）。
		-ICMPv4 o タイプ o コード -ICMPv6 o タイプ o コード -IPv4 o 送信元アドレス o 送信先アドレス

SFR	アクティビティ	保証アクティビティ
		o トランスポート層プロトコル -IPv6 o送信元アドレス o 送信先アドレス o トランスポート層プロトコル -TCP o 送信元ポート o 送信先ポート -UDP o 送信元ポート o 送信先ポート
		テスト2:TOEによって支持されているそれぞれ異なるネットワークインタフェースタイプのステートフルトラフィック・フィルタリング規則を定義できることを確認するために上記の保証アクティビティを繰り返し行う。 こうしたテストアクティビティは、規則の有効性をテストするFFW_RUL_EXT.1.10のテストアクティビティと同時に施行するべきである（should）点に留意のこと。FFW_RUL_EXT.1.10のテストアクティビティでは、 テスト対象となるプロトコル/属性の組合せを定義する。こうした組合せを手動にて設定する場合、テストアクティビティの目的を満たすかもしれないが、その他の組合せで設定する場合（自動化を用いるなど)、ガイダンスが正しく、TOE管理者によって全設定範囲を獲得できるためにこうしたテストアクティビティが必要となる可能性がある。
FFW_RUL_EXT.1.6	TSS	評価者は、TSSがステートフルセッションの取扱いをサポートするプロトコルを特定することを検証しなければならない。ST 執筆者によって選択された場合、TSSによりTCP、UDP及びICMPを特定しなければならない（shall)。 評価者は、TSSにステートフルセッションがどのように確立され（ハンドシェイク処理を含む)、維持されているかが記載されていることを検証しなければならない（shall)。 評価者は、TCPについてはセッションを決定するにあたって、TSSが以下の属性の使用を特定し、記載していることを検証しなければならない（shall)：送信元アドレス及び送信先アドレス、送信元ポート及び送信先ポート、シーケンス番号及び各フラグ。 評価者は、UDPについてはセッションを決定するにあたって、TSSが以下の属性を特定し、記載していることを検証しなければならない：送信元アドレス及び送信先アドレス、送信元ポート及び送信先ポート。 評価者は、ICMP（選択した場合）については、セッションを決定するにあたってTSS が以下の属性を特定し、記載していることを検証しなければならない（shall)：送信元アドレス及び送信先アドレス、FFW_RUL_EXT.1.6で選択されたその他の属性。 評価者は、確立されたステートフルセッションをどのように取り除くかについてTSSに記載されていることを検証しなければならない（shall)。TSSは、通常の完了時またはタイムアウト条件に基づいて、いずれのプロトコルもどのように接続を取り除くかを記載しなければならない（shall)。また、TSSは、セッションの取り除きが有効となる時（セッションに適合する可能性のある次のパケットを処理する前など）を記載しなければならない（shall)。
	ガイダンス	評価者は、操作ガイダンスには、ステートフルセッションのふるまいが記載されていることを検証しなければならない。例えば、TOEは、既存セッションの一部として許可されているパケットをログできないかもしれない（might)。

SFR	アクティビティ	保証アクティビティ
	テスト	テスト1: 評価者は、TOE が TCP トラフィックを許可し、ログを行うために設定しなければならない（shall）。評価者は、TCP セッションを初期化しなければならない（shall）。TCP セッションが確立されるのと同時に、評価者は、変更トラフィックはセッションの一部として承認されないことを決定するために（ログイベントが発生し、規則集が適用されたことが明らかになるなど）、不正確なフラグのついたセッション確立パケットを導入しなければならない（shall）。TCP セッションがうまく確立された後、評価者は、変更パケットが確立されたセッションの一部として承認されていないことを検証するために、属性（送信元アドレス及び送信先アドレス、送信元ポート及び送信先ポート、シーケンス番号、フラグ）を決定するそれぞれのセッションを１つずつ変更しなければならない（shall）。 テスト2：評価者は、TSS に記載したテスト１に従って確立した TCP セッションを完了させなければならない（shall）。その後、評価者は、規則集に準拠せずに、TOE を介して転送されていないことを確認するために、前のセッションの定義に適合するパケットをすぐに送信しなければならない（shall）。 テスト3：評価者は、TSS に記載したテスト１に従って確立した TCP セッションを失効（タイムアウトに到達など）させなければならない（shall）。評価者は、規則集に準拠せずに、TOE を介して転送していないことを確認するために以前のセッションに適合するパケットを送信しなければならない（shall）。 テスト4：評価者は、UDP トラフィックを許可し、ログを行うために TOE を設定しなければならない（shall）。評価者は、UDP セッションを確立しなければならない（shall）。一度 UDP セッションが確立されると、評価者は、変更パケットが確立されたセッションの一部として承認されていないことを検証するために、それぞれのセッションを決定する属性（送信元及び送信先アドレス、送信元及び送信先ポート）を１つずつ変更しなければならない（shall）。

SFR	アクティビティ	保証アクティビティ
		テスト5：評価者は、TSSに記載されているとおりテスト4に従って確立したUDPセッションを失効させなければならない（shall）（すなわちタイムアウトに到達する）。評価者は、規則集に準拠せずに、TOE を介して転送していないことを確認するために以前のセッションに適合するパケットを送信しなければならない（shall）。 テスト6：ICMP を選択した場合、評価者は、ICMP トラフィックを許可し、ログを行うためにTOEを設定しなければならない（shall）。評価者は、TSSに記載されているとおり、ICMP 用のセッションを確立しなければならない（shall）。一度ICMPが確立されると、変更パケットが確立されたセッションの一部として承認されていないことを検証するために、評価者は、属性（送信元及び送信先アドレス及び FFW_RUL_EXT.1.6 で選択されたその他の属性）を決定するそれぞれのセッションを１つずつ変更しなければならない（shall）。 テスト7：該当する場合、評価者は、TSSに記載したテスト6に従って確立したICMPセッションを完了させなければならない。その後、評価者は、規則集に準拠せずに、TOEを介して転送されていないことを確認するために、前のセッションの定義に適合するパケットをすぐに送信しなければならない（shall）。 テスト8：評価者は、TSSに記載されているとおりテスト6に従って確立したICMP セッションを失効させなければならない（すなわち、タイムアウトに到達する）。評価者は、規則集に準拠せずに、TOE を介して転送していないことを確認するために以前のセッションに適合するパケットを送信しなければならない。
FFW_RUL_EXT.1.7	TSS	評価者は、TSSが動的パケットフィルタリング規則の自動作成を行うことのできるプロトコルを特定していることを検証しなければならない。動的規則が作成されるよりも、TOEがいくつかの特定されたプロトコルのふるまいをサポートするためにステートフルセッションを確立する（might）場合もある。TSSは、FTP及び任意で他のプロトコルを特定しなければならない（shall）。 評価者は、TSSがセッションの確立及び除去の動的性質を説明していることを検証しなければならない（shall）。TSSでは、ロギングの問題も説明しなければならない（shall）。 評価者は、FTPについては、FTPデータセッションがFTPコントロールセッションに対して TOE を介してどのように許可されるか TSS が説明していることを検証しなければならない（shall）。 評価者は、その他のそれぞれ選択したプロトコルについては、TSSがプロトコルごとのセッションの確立及び除去の動的性質を説明し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、操作ガイダンスには、動的セッションの確立機能について記載されていることを検証しなければならない（shall）。 評価者は、操作ガイダンスには、TSSに従って動的セッションのロギングについて記載されていることを検証しなければならない（shall）。

SFR	アクティビティ	保証アクティビティ
	テスト	テスト１：評価者は、FTP セッションを許可し、ログするため及び 1024 を超える TCP ポートを拒否し、ログするためのステートフルトラフィック・フィルタリング規則を定義しなければならない（shall）。引き続き、評価者は、これを確実に継承するために FTP セッションを確立しなければならない（shall）。評価者は、操作ガイダンスに準拠していることを検証するために発生したログを検討しなければならない（shall）。 テスト２：テスト１より引き続き、評価者は、FTP データセッションによって 1024 を超えるポートを使用し、FTP セッションを完了させることを決定しなければならない（shall）（パケットスニファを使用するなど）。また、TCP パケットは TOE を介して同じ送信元アドレス及びポート、送信先アドレス及びポートにより送信できないことを検証しなければならない（shall）。 テスト３：評価者は、それぞれサポートしているプロトコルについて、そのプロトコル用の上述の手順を繰り返し行なわなければならない（shall）。いずれの場合も、動的規則を作成し、有効であるものにするためにポートをブロックする範囲を決定するため、評価者が適用可能な RFC または標準を使用しなければならない（must）。
FFW_RUL_EXT.1.8	TSS	評価者は、TSS には以下が自動的に拒否され、ログ可能の状態となるパケットとして特定されていることを検証しなければならない（shall）： 1. 無効なフラグメントであるパケット。無効なフラグメントの構成物の説明を含む。 2. 完全に再度組み立てることのできないフラグメント 3. 送信元アドレスがネットワークパケットを受領したネットワークインタフェースのアドレスと同じであるパケット 4. 送信元アドレスがネットワークパケットを受領したネットワークインタフェースに関連のあるネットワークに属していない場合のパケット。TOE により送信元アドレスがあるネットワークインタフェースに関連のあるネットワークに属しているか否かを判断する方法の説明を含む。 5. 送信元アドレスがブロードキャストネットワーク上のものであると定義されているパケット 6. 送信元アドレスがマルチキャストネットワーク上のものであると定義されているパケット 7. 送信元アドレスがループバックアドレスであると定義されているパケット 8. IPv4 用 RFC 1918 及び IPv6 用 RFC 3513 に記載されているとおり、送信元アドレスが保存アドレスであると定義されているパケット 9. ネットワークパケットの送信元アドレスまたは送信先アドレスがリンクローカルアドレスであるパケット 10. IPv4 用 RFC 5735 に記載されているとおり、ネットワークパケットの送信元アドレスまたは送信先アドレスが「今後使用するための保存」アドレスとして定義されているパケット 11. IPv6 用 RFC 3513 に記載されているとおり、ネットワークパケットの送信元アドレスまたは送信先アドレスが「不特定アドレス」または「今後定義及び使用するための保存」アドレスとして定義されているパケット 12. IP オプション付きパケット：ルーズソースルーティング、ストリクトソースルーティングまたは規定のレコードルート 13. FFW_RUL_EXT.1.8.で定義されているその他のパケット
	ガイダンス	評価者は、操作ガイダンスに、廃棄されたが、初期設定によりログされた可能性のあるパケットについて記載されていることを検証しなければならない（shall）。適用可能なプロトコルを特定する場合、その説明が TSS と一致している必要がある。ロギングを設定できる場合は、評価者は、自動的に拒否されるパケットの監査を設定するために適用可能な指示が提示されていることを検証しなければならない（shall）。

SFR	アクティビティ	保証アクティビティ
	テスト	テスト１：評価者は、パケットの自動拒否に関する各条件を順にテストを行わなければならない（shall）。いずれの場合も、TOE は、すべてのネットワークトラフィックを許可するように設定するべきである（should）。また、評価者は、拒否されるパケットまたはパケットフラグメントを発生させなければならない（shall）。必ず許可できないパケットまたはパケットフラグメントが TOE から通過しないように、評価者は、パケットキャプチャを使用しなければならない（shall）。 テスト 2：上述の場合はいずれも、評価者は、拒否されたパケットのロギングが可能になるように、あらゆる適用可能なガイダンスを使用しなければならない（shall）。上述の場合はいずれも、評価者は、拒否されたパケットまたはパケットフラグメントが適切にログされていることを検証しなければならない（shall）。
FFW_RUL_EXT.1.9zz	TSS	評価者は、TSS には着信するパケットに適用されるアルゴリズムが記載されていることを検証しなければならない（shall）。初期設定規則の処理、パケットを確立されたセッションの一部とするか否かの決定、規則集を定義し、整理する管理者の適用を含む。
	ガイダンス	評価者は、操作ガイダンスに、管理者が規則処理順序を設定できるようにステートフルトラフィックフィルタリング規則の順序決定方法が記載され、必要な指示が提示されていることを検証しなければならない（shall）。
	テスト	テスト 1：評価者は、代替操作（許可及び拒否）のある 2 つ同じステートフルトラフィックフィルタリング規則を立案しなければならない（shall）。その後、規則を 2 つの異なる順序に展開するべきである（should）。いずれの場合も、評価者は、最初の規則がいずれの場合にも適用可能なパケットを発生させ、パケットキャプチャを用いることによって施行され、確認のためにログすることを検証しなければならない（shall）。 テスト 2：評価者は、上述の手順を繰り返し行おうとする。ただし、2 つの規則を立案し、1 つは他方のサブセットとすべく場合を除く（特定のアドレス対ネットワークセグメントなど）。評価者は、規則の特殊性に関係なく最初の順序を施行することを確認するために、いずれの順序でもテストを行わなければならない（shall）。
FFW_RUL_EXT.1.10	TSS	評価者は、TSS にはステートフルトラフィックフィルタリング規則を適用するプロセスが記載されていること及び規則に適合していない場合は、ふるまい（初期設定によるものまたは管理者による設定のいずれか一方）により、パケットを拒否できることを検証しなければならない（shall）。ただし、他の必要な条件によりネットワックトラフィックが許可されている場合は除く（すなわち、FFW_RUL_EXT.1.6 または FFW_RUL_EXT.1.7）。

SFR	アクティビティ	保証アクティビティ
	ガイダンス	評価者は、規則または特別な条件をネットワークトラフィックに適用しない場合、操作ガイダンスにはふるまいが記載されていることを検証しなければならない（shall）。ふるまいが設定可能であれば、評価者は、操作ガイドラインには、規則に適合していないパケットを拒否するふるまいを設定するための適切な指示が記載されていることを検証しなければならない（shall）。
	テスト	テスト 1：評価者は、定義された ICMPv4 タイプおよびコードを許可し、ログするために TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、許可され（TOE を介して通過した後、パケットを獲得することによってなど）、ログされていることを確認するためにそれぞれ定義した ICMPv4 タイプおよびコードに適合するパケットを発生させる。 テスト 2：評価者は、定義された ICMPv4 タイプおよびコードを拒否し、ログするために TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、拒否され（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）、ログされていることを確認するためにそれぞれ定義した ICMPv4 タイプおよびコードに適合するパケットを発生させる。 テスト 3：評価者は、ICMPv4 規則のない状態で TOE を設定しなければならない（shall）。評価者は、拒否されていること（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）を確認するためにそれぞれ定義した ICMPv4 タイプおよびコードに適合するパケットを発生させる。 テスト 4：評価者は、定義された ICMPv6 タイプおよびコードを許可し、ログするために TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、許可され（TOE を介して通過した後、パケットを獲得することによってなど）、ログされていることを確認するためにそれぞれ定義した ICMPv6 タイプおよびコードに適合するパケットを発生させる。 テスト 5：評価者は、定義された ICMPv6 タイプおよびコードを拒否し、ログするために TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、拒否され（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）、ログされていることを確認するためにそれぞれ定義した ICMPv6 タイプおよびコードに適合するパケットを発生させる。 テスト 6：評価者は、ICMPv6 規則のない状態で TOE を設定しなければならない（shall）。評価者は、拒否されていること（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）を確認するためにそれぞれ定義した ICMPv6 タイプおよびコードに適合するパケットを発生させる。 テスト 7：評価者は、特定の送信元アドレスと特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスとに関連して、定義された IPv4 トランスポート層プロトコルを許可し、ログするために TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、許可し（TOE を介して通過した後、パケットを獲得することによってなど）、ログされていることを確認するためにそれぞれ定義した IPv4 トランスポート層プロトコルに適合し、設定された送信元アドレスおよび送信先アドレス内でパケットを発生させなければならない（shall）。 テスト 8：評価者は、特定の送信元アドレスおよび特定の送信先アドレス、

SFR	アクティビティ	保証アクティビティ
		特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスに関連してすべてのトラフィックを許可するために TOE を設定しなければならない（shall）。ただし、それぞれ定義された IPv4 トランスポート層プロトコルを拒否し、ログする場合は除く（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、拒否され（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）、ログされていることを確認するためにそれぞれ定義した IPv4 トランスポート層プロトコルに適合するパケットを発生させなければならない（shall）。 テスト 9：評価者は、特定の送信元アドレスおよび特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスに関連してそれぞれ定義された IPv4 トランスポート層プロトコルを許可し、ログするための TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。 また、評価者は、特定の送信元アドレスと特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスなど、（上記で許可されているもとのとは）異なる組合せに関連してそれぞれ定義された IPv4 トランスポート層プロトコルを拒否し、ログするための TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、拒否されていること（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）を確認するために、それぞれ定義した IPv4 トランスポート層プロトコルおよび上述のとおり設定されているすべての送信元アドレスおよび送信先アドレスの範囲外に適合するパケットを発生させなければならない（shall）。 テスト 10：評価者は、特定の送信元アドレスおよび特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスに関連して、それぞれ定義された IPv6 トランスポート層プロトコルを許可し、ログするための TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、許可され（TOE を介して通過した後、パケットを獲得することによってなど）、ログされていることを確認するためにそれぞれ定義した IPv6 トランスポート層プロトコルおよび設定した送信元アドレスおよび送信先アドレス内に適合するパケットを発生させなければならない（shall）。 テスト 11：評価者は、特定の送信元アドレスおよび特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスに関連してすべてのトラフィックを許可するために TOE を設定しなければならない（shall）。ただし、それぞれ定義された IPv6 トランスポート層プロトコルを拒否し、ログする場合は除く（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、拒否され（TOE を介して通過した後、パケットを獲得しないことによってなど）、ログされていることを確認するために、それぞれ定義した IPv6 トランスポート層プロトコルおよび設定した送信元アドレスおよび送信先アドレス内に適合するパケットを発生させなければならない（shall）。 テスト 12：評価者は、特定の送信元アドレスおよび特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスに関連して、それぞれ定義された IPv6 トランスポート層プロトコルを許可し、ログするために TOE を設定しなければならな

SFR	アクティビティ	保証アクティビティ
		い（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。また、評価者は、特定の送信元アドレスと特定の送信先アドレス、特定の送信元アドレスとワイルドカード送信先アドレス、ワイルドカード送信元アドレスと特定の送信先アドレス、ワイルドカード送信元アドレスとワイルドカード送信先アドレスなど、（上記で許可されているもとのとは）異なる組合せに関連して、それぞれ定義された IPv6 トランスポート層プロトコルを拒否し、ログするために TOE を設定しなければならない（shall）（表 4-2 定義されたプロトコル特定の属性を参照）。評価者は、拒否されている（TOE を介して通過した後、適用可能なパケットを獲得しないことによってなど）ことを確認するために、それぞれ定義した IPv6 トランスポート層プロトコルおよび上述のとおり設定したすべての送信元アドレスおよび送信先アドレスの範囲外に適合するパケットを発生させなければならない（shall）。 テスト 13：評価者は、選択された送信元ポート、選択された送信先ポートおよび選択された送信元ポートと送信先ポートとの組み合わせを用いて、TCP を許可し、ログを行うために TOE を設定しなければならない（shall）。評価者は、許可され（TOE を介して通過した後、パケットを獲得することによってなど）、ログされていることを確認するために、設定した送信元 TCP ポートおよび送信先 TCP ポートに適合するパケットを発生させなければならない（shall）。 テスト 14：評価者は、選択された送信元ポート、選択された送信先ポートおよび選択された送信元ポートと送信先ポートとの組み合わせを用いて、TCP を拒否し、ログを行うために TOE を設定しなければならない（shall）。評価者は、拒否され（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）、ログされていることを確認するために、設定した送信元 TCP ポートおよび送信先 TCP ポートに適合するパケットを発生させなければならない（shall）。 テスト 15：評価者は、選択された送信元ポート、選択された送信先ポートおよび選択された送信元ポートと送信先ポートとの組み合わせを用いて、UDP を許可し、ログを行うために TOE を設定しなければならない（shall）。評価者は、許可され（TOE を介して通過した後、パケットを獲得することによってなど）、ログされていることを確認するために、設定した送信元 UDP ポートおよび送信先 UDP ポートに適合するパケットを発生させなければならない（shall）。 テスト 16：評価者は、選択された送信元ポート、選択された送信先ポートおよび選択された送信元ポートと送信先ポートとの組み合わせを用いて UDP を拒否し、ログを行うために TOE を設定しなければならない（shall）。評価者は、拒否され（TOE を介して通過した適用可能なパケットが獲得されないことによってなど）、ログされていることを確認するために、設定した送信元 UDP ポートおよび送信先 UDP ポートに適合するパケットを発生させなければならない（shall）。

以下の表には、設定する際に使用される適用可能なプロトコルについて、RFC により定義されているタイプ、コードおよびトランスポート層の属性、さもなければ、試験を行うステートフルトラフィックフィルタファイアウォール規則の定義および施行を特定する。こうしたプロトコルに定義するためのみに必要な属性が、すべて特定の TOE 操作環境内で使用できると考えられるネットワークアドレスおよびポートであることから、TCP および UDP は表に記載されていない点に留意のこと。

4-2 定義されたプロトコル特定の属性

プロトコル	定義された属性
ICMPv4	タイプ 0(Echo Reply)（エコーリプライ） タイプ 3(Destination Unreachable)（送信先到達不能） タイプ 3 コード 0(Net Unreachable)（ネット到達不能数） タイプ 3 コード 1(Host Unreachable)（ホスト到達不能） タイプ 3 コード 2(Protocol Unreachable)（プロトコル到達不能） タイプ 3 コード 3(Port Unreachable)（ポート到達不能） タイプ 3 コード 4(Fragmentation Needed and Don't Fragment was set)（必要なフラグメント化およびフラグメント化禁止が設定されていない場合） タイプ 3 コード 5(Source Route Failure)（送信元ルートの不具合） タイプ 3 コード 6(Destination Network Unknown)（送信先ネットワークが不明） タイプ 3 コード 7(Destination Host Unknown)（送信先ホストが不明） タイプ 3 コード 8（Source Host Isolated)（送信元ホストが通信できない） タイプ 3 コード 9(Communication with Destination Network is Administratively Prohibited)（管理上、送信先ネットワークとの通信が禁止されている） タイプ 3 コード 10(Communication with Destination Host is Administratively Prohibited)（管理上、送信先ホストとの通信が禁止されている） タイプ 3 コード 11(Destination Network Unreachable for Type of Service)（指定されたサービスタイプでは、送信先ネットワークに到達不能） タイプ 3 コード 12(Destination Host Unreachable for Type of Service)（指定されたサービスタイプでは、送信先ホストに到達不能） タイプ 3 コード 13(Communication Administratively Prohibited)（管理上通信が禁止されている） タイプ 4(Source Quench)（ソースクエンチ） タイプ 5（Redirect）（リダイレクト） タイプ 5 コード 0(Redirect Datagram for the Network (or subnet))（指定されたネットワーク(またはサブネット）へのルート変更） タイプ 5 コード 1(Redirect Datagram for the Host)（指定されたホストへのルート変更） タイプ 5 コード 2(Redirect Datagram for the Type of Service and Network)（指定されたサービスおよびネットワークのタイプへのルート変更） タイプ 5 コード 3(Redirect Datagram for the Type of Service and Host)（指定されたサービスおよびホストのタイプのタイプへのルート変更） タイプ 6(Alternative Address for Host)（ホスト用代替アドレス） タイプ 6 コード 0(Alternate Address for Host)（ホスト用代替アドレス） タイプ 8(Echo)（エコー） タイプ 9(Router Advertisement)（ルーター通知） タイプ 10(Router Selection)（ルーター選択） タイプ 11（Time Exceeded)（時間超過） タイプ 11 コード 0（Time to Live exceeded in Transit)（生存時間 TTL がゼロになった） タイプ 11 コード 1（Fragment Reassembly Time Exceeded)（受信側でフラグメントの再構成に失敗または時間切れ） タイプ 12（Parameter Problem)（パラメタ異常）

プロトコル	定義された属性
	タイプ 12 コード 0 (Pointer indicates the error) (ポインタの値によりエラーを示す) タイプ 12 コード 1 (Missing a Required Option) (ポインタの値は使用しない) タイプ 12 コード 2 (Bad Length) (パラメタ長の不正) タイプ 13 (Timestamp) (タイムスタンプ) タイプ 14 (Timestamp Reply) (タイムスタンプリプライ) タイプ 15 (Information Request) (情報要求) タイプ 16 (Information Reply) (情報応答) タイプ 17 (Address Mask Request) (アドレスマスク要求) タイプ 18 (Address Mask Reply) (アドレスマスク応答) タイプ 30(Traceroute) (トレースルート) タイプ 31(Datagram Conversion Error)(データグラム変換エラー) タイプ 32 (Mobile Host Redirect) (移動体ホストのリダイレクト) タイプ 35 (Mobile Registration Request) (移動体登録要求) タイプ 36 (Mobile Registration Reply) ICMPv6 (移動体登録応答)
ICMPv6	タイプ 1 (Destination Unreachable) (送信先到達不能) タイプ 1 コード 0 (no route to destination) (着信へのルートなし) タイプ 1 コード 1 (communication with destination administratively prohibited) (管理上、送信先との通信が禁止されている) タイプ 1 コード 2 (beyond scope of source address) (送信元アドレスの範囲外) タイプ 1 コード 3(address unreachable) (アドレス到達不可) タイプ 1 コード 4(port unreachable) (ポート到達不可) タイプ 1 コード 5 (source address failed ingress/egress policy) (イングレス/エグレスポリシーでの送信元アドレスの誤り) タイプ 1 コード 6 (no route to destination) (送信先ルートの拒絶) タイプ 1 コード 7 (Error in Source Routing Header) (送信元ルーティングヘッダーエラー) タイプ 2 (Packet Too Big) (パケット過大) タイプ 3 (Time Exceeded) (時間超過) タイプ 3 コード 0 (hop limit exceeded in transit) (転送中にホップ限界を越えた) タイプ 3 コード 1(fragment reassembly time exceeded) (フラグメント組み立て時間超過) タイプ 4 (Parameter Problem) (パラメタ異常) タイプ 4 コード 0 (erroneous header field encountered) (ヘッダーフィールドに誤りがある) タイプ 4 コード 1 (unrecognized Next Header type encountered)(ヘッダータイプが認識されていない) タイプ 4 コード 2(unrecognized IPv6 option encountered) (IPv6 オプションが認識されていない) タイプ 100 (Private Experimentation)(プライベート実験) タイプ 101 (Private Experimentation)(プライベート実験) タイプ 128(Echo Request) (エコー要求) タイプ 129(Echo Reply) (エコー応答)

プロトコル	定義された属性
	タイプ 130 (Multicast Listener Query)（マルチキャストリスナー問い合わせ） タイプ 131 (Multicast Listener Report)（マルチキャストリスナーレポート） タイプ 132 (Multicast Listener Done)（マルチキャストリスナー終了） タイプ 133 (Router Solicitation)（ルーター要請） タイプ 134(Router Advertisement)（ルーター通知） タイプ 135 (Router Solicitation)（近隣要請） タイプ 136(Neighbor Advertisement)（近隣通知） タイプ 137(Redirect Message)（リダイレクトメッセージ） タイプ 138 (Router Solicitation)（ルーターリナンバリング） タイプ 138 コード 0(Router Renumbering Command)（ルーターリナンバリングコマンド） タイプ 138 コード 1 (Router Renumbering Result)（ルーターリナンバリング結果） タイプ 138 コード 225 (Sequence Number Reset)（シーケンス番号リセット） タイプ 139 (ICMP Node Information Query)（ICMP ノード情報問い合わせ） タイプ 139 コード 0 (The data field contains an IPv6 address which is the subject of this query)（データ情報フィールドには、本問い合わせの標題である IPv6 アドレスを含む） タイプ 139 コード 1 (The data field contains a name which is the subject of this query or is empty, as in the case of a NOOP)(データフィールドには、本問い合わせの標題である名前を含むまたは NOOP の場合空である。） タイプ 139 コード 2 (The Data field contains an IPv4 address which is the Subject of this Query.)（データフィールドには、本問い合わせの標題である IPv4 アドレスを含む） タイプ 140 (ICMP Node Information Response)（ICMP ノード情報応答） タイプ 140 コード 0 (A successful reply The Reply Data field may or may not be empty)(成功の応答。応答データフィールドが空であるか、または空でない可能性がある） タイプ 140 コード 1 (The Responder refuses to supply the answer. The Reply Data field will be empty)（応答者が回答の提供を拒否する。回答データフィールドは空となる） タイプ 140 コード 2 (Qtype of the Query is unknown to the Responder. The Reply Data field will be empty)（応答者には Q タイプの問い合わせは不明である。回答データフィールドは空である。） タイプ 141 (Inverse Neighbor Discovery Solicitation Message)(逆近隣探索要請メッセージ) タイプ 142 (Inverse Neighbor Discovery Advertisement Message)(逆近隣探索通知メッセージ) タイプ 143 (Version 2 Multicast Listener Report)(バージョン 2 マルチキャストリスナーレポート) タイプ 144 (Home Agent Address Discovery Request Message)（ホームエージェントアドレス探索要求メッセージ） タイプ 145 (Home Agent Address Discovery Request Message)（ホームエージェントアドレス探索要求メッセージ） タイプ 146 (Mobile Prefix Solicitation)（移動体プレフィックス要請） タイプ 147 (Mobile Prefix Solicitation)（移動体プレフィックス通知）

プロトコル	定義された属性
	タイプ 148 (Certification Path Solicitation Message) (証明書パス要請メッセージ) タイプ 149(Certification Path Advertisement Message) (証明書パス通知メッセージ) タイプ 150 (ICMP messages utilized by experimental mobility protocols such as Seamoby) (Seamoby などの実験移動性プロトコルによって利用された ICMP メッセージ) タイプ 151 (Multicast Router Advertisement) (マルチキャストルーター通知) タイプ 152 (Multicast Router Solicitation) (マルチキャストルーター要請) タイプ 153 (Multicast Router Termination) (マルチキャストルーターの終了) タイプ 154 (FMIPv6 Messages) (FMIPv6 メッセージ) タイプ 155 (RPL Control Message) IPv4 (RPL コントロールメッセージ)
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 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 Internodal 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

プロトコル	定義された属性
	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 44 - SIP Fragment
	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 - 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
	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

プロトコル	定義された属性
	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
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
	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

プロトコル	定義された属性
	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 Internodal 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

プロトコル	定義された属性
	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
	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

プロトコル	定義された属性
	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 - Fibre 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

4.2.2 セキュリティ監査

セキュリティ監査には、さらなる SFR はない。しかし、さらに NDPP で検索された FAU_GEN.1 SFR を拡張するために有用な監査可能な事象はある。このため、以下の事象は、適合するセキュリティターゲットの文中で NDPP の事象と組み合わせるべきである。

以下の監査事象は、ファイアウォール SFR が表示されている場合に適用可能である。

4-3 FAU_GEN.1 監査事象および詳細

SFR	監査事象	詳細
FFW_RUL_EXT.1	「ログ」操作により設定された規則を適用	送信元および送信先アドレス、送信元および送信先ポート、トランスポート層プロトコル、TOE インタフェース
	ネットワークトラフィック過大によりドロップしたパケットの表示	パケットを処理できない TOE インタフェース

4.2.2.1 保証アクティビティ

次の表には、FAU_GEN.1 に準拠していることを確認するために評価者が実施する保証アクティビティについて示す。

4-4 FAU_GEN.1 保証アクティビティ

SFR	アクティビティ	保証アクティビティ
FAU_GEN.1.1/FAU_GEN.1.2	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ックをログするために、ステートフルトラフィックフィルタファイアウォール規則をどのように設定できるかが記載されていることを検証するべきである（shall）。このアクティビティは、FFW_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点に留意のこと。 評価者は、TSS には、インタフェースのいずれかひとつがネットワークトラフィックによる負担を受けた場合の TOE のふるまいが記載されていることを検証するべきである（shall）。 TOE が処理できないパケットをドロップすることができるが、いかなる状態であっても、操作を許可できるか、または許可され、確立されているセッションに属している規則を満たしていないパケットを TOE により通過させることはできない。実装制限により、必ず TOE がドロップしたパケットを監査できるとは限らない（may）。ドロップしたパケットの事象が監査されない制限および環境は、TSS に記載されているべきである（shall）。
	ガイダンス	評価者は、操作ガイダンスに、ネットワークトラフィックのロギングが適用可能となるステートフルトラフィックフィルタファイアウォールの設定方法が記載されていることを検証するべきである（shall）。このアクティビティは、FFW_RUL_EXT.1 のガイダンス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点に留意のこと。

	テスト	テスト 1：評価者は、ロギング用のステートフルトラフィックフィルタファイアウォール規則を設定するために使用されるインタフェースにより、適用可能な規則と関連して、予想されるネットワークトラフィックログが発生することをテストしなければならない（shall）。 多くの規則の組合せおよび順序付けのシナリオは、適合しているネットワークトラフィックの許可、拒否およびログするためにデザインされた規則に適合する有効および無効なネットワークトラフィックをいずれも通過させる試みにより、設定およびテストを行う必要がある。このアクティビティは、FFW_RUL_EXT.1 のテスト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点に留意のこと。 テスト 2：評価者は、TOE がすべてのパケットを通過させることができなくなるように、TOE をネットワークパケットで満たすように試みるべきである（shall）。これにより評価者に、TOE が扱うことのできる帯域幅を制限するために、TOE を設定するように要求することが可能である（may）（10 MB インタフェースを使用するなど）。

4.2.3 セキュリティ管理

セキュリティ管理には、さらなる SFR はない。NDPP に記載されているとおり、ファイアウォールのふるまいを決定する際に有用な規則、初期設定などの閲覧は、セキュリティ管理者に制限される。さらに、こうしたセキュリティ管理機能に具体的に追加する必要のある規則はない。

NDPP には、特定のセキュリティ管理機能が存在するにあたって必要な FMT_SMF.1 が記載されている。以下のセキュリティ管理機能は、ファイアウォール SFR が表示されている場合には、適用可能である。このため、以下のセキュリティ管理機能は、適合するセキュリティターゲットの文中で NDPP のセキュリティ管理機能と組み合わせるべきである。

4-5 FMT_SMF.1 セキュリティ管理機能

SFR	セキュリティ管理機能
FFW_RUL_EXT.1	ファイアウォール規則を設定する

4.2.3.1 保証アクティビティ

以下の表には、FMT_SMF.1 に準拠していることを確認するために評価者が実施する保証アクティビティについて示す。

4-6 FMT_SMF.1 保証アクティビティ

SFR	アクティビティ	保証アクティビティ
FMT_SMF.1.1	TSS	評価者は、TSS 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規則をどのように設定できるかについて記載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は、FFW_RUL_EXT.1 の TSS 保証アクティビティとともに対処されるべきである点に留意のこと。
	ガイダンス	評価者は、操作ガイダンスには、設定可能な初期設定およびそれぞれ適用可能な規則の属性、アクションおよび関連のあるインタフェースといった設定方法など、ステートフルトラフィックフィルタファイアウォール規則の設定方法について記載されていることを検証しなければならない（shall）。評価者は、設定済み規則が適切に整理されていることを管理者が確認できる指示が操作ガイダンスにも記載されていることを確認しなければならない（must）。このアクティビティは、FFW_RUL_EXT.1 のガイダンス保証アクティビティとともに対処されるべきである点に留意のこと。

	テスト	テスト 1: 評価者は、ステートフルトラフィックフィルタファイアウォール規則の設定に使用される機能により、正しく実施される規則において予想される変更が発生することを示すテストを開発しなければならない（shall）。多くの規則の組合せおよび順序付けのシナリオは、有効および無効なネットワークトラフィックをいずれも TOE を介して通過させる試みにより設定し、テストを行う必要がある。このアクティビティは、FFW_RUL_EXT.1 のテスト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点に留意のこと。

4.3 セキュリティ保証要件

本 EP に対して評価された TOE が、NDPP に対しても同様に、本質的に評価される点に留意することは重要である。NDPP には、セキュリティ機能要件（SFR）および SAR のいずれにも関連のある多くの保証アクティビティが記載されている。また、本 EP には、同様に NDPP に記載されている EAL に関連のある SAR に絞り込んだ多くの SFR に基づく保証アクティビティが記載されている。NDPP によって規定されている SAR に関連のある保証アクティビティは、本書に記載されている特定の脆弱性テストのほかに、TOE 全体に対して行う。

4.3.1 AVA_VAN.1 脆弱性評定

保証アクティビティ：

評価者は、属性、タイプ、コード、トランスポート層プロトコルのすべての値を介して循環するネットワークパケットを発生させなければならない（shall）。これは、各プロトコル（ICMPv4、ICMPv6、IPv4 および IPv6）の RFC には定義されていない。例えば、ICMPv4 では、タイプについては 8 バイトフィールドがあり、コードについては 8 バイトフィールドがある。RFC では、21 タイプのみが定義されている（表 4-2 参照）が、256 の値まで可能である。いずれのタイプも関連するコードがあり、コードで定義されている RFC 数は、タイプに基づいて変化する。評価者は、タイプおよびコード（考え得るすべての組合せ）の RFC に定義されていないがそれぞれ可能な数値(定義されている数値はすでに FFW_RUL_EXT.1.10 においてテスト済みである）を使用するパケットを構築し、TOE がこうしたパケットを適切に扱っているか否かを判断するためにそれぞれのインタフェースタイプを対象とする必要がある。こうしたパケットがいずれも規則に適合しない場合、または許可されたセッションに属していない場合、パケットはドロップさせるべきである。ファイアウォールがこうした状況下でドロップするパケットを監査する要件がないため、評価者は、ファイアウォールが TOE を介してこうしたパケットをフローさせることができないことを確認しなければならない（shall）。

上記に必要とされている定義されていない属性をテストする場合に加えて、評価者は、必要なプロトコルヘッダー内の残りのフィールドにインテリジェントファズテスト(FTP を除く)を実施しなければならない(shall)。インテリジェントファジングの目的は、規則集が適用される場合に拒否されるように、他に正しく構築されているパケットに、それぞれのプロトコルヘッダーフィールドに挿入するランダム値を持たせることである。評価者は、統計上有意な標本サイズがレポート内で使用され、正当化されていることを確認する。この標本サイズは、プロトコルフィールド長によって異なる。

評価者は、こうしたパケットを処理することによって、TOE が悪影響を及ぼしたか否かを判断するために、TOE により提供されたいかなる診断（ロギング、プロセス状態、インタフェースエラーなど）も参考にするべきである。

5. 根拠

本 EP では、ステートフルトラフィックフィルタファイアウォールによって対処する脅威；それらの脅威を軽減するために用いられる手法；適合する TOE によって達成される脅威に対する軽減の度合いについての全般的な理解しやすさを向上させるため、本書の冒頭における議論の中心が物語風の説明で書かれている。この説明のスタイルは形式的な評価アクティビティにすぐに役立つものではないため、本節は本書に関連する評価アクティビティにおいて使用可能な表形式のものとして提供する。

5.1 セキュリティ課題定義

5.1.1 前提条件

以下にリストアップされた特定の条件が TOE の運用環境において存在することが前提とされている。これらの前提条件は、NDPP に定義されている条件に加えて、TOE セキュリティ要件の開発における現実的に実現するもの及び TOE 使用時の必須の環境条件として含まれている。

5-1 TOE 前提条件

前提条件の名称	前提条件の記述
A.CONNECTIONS	TOE は、付属ネットワークにフローする適用可能なすべてのネットワークトラフィックにおいて、TOE セキュリティポリシーが確実に施行される方法でそれぞれのネットワークに接続されていることを前提とする。

5.1.2 脅威

以下に示す脅威は、ステートフルトラフィックフィルタファイアウォールによって対処される。すべてがステートフルトラフィックフィルタファイアウォールに適用される場合、こうした脅威が NDPP に定義されている脅威に加わる点に留意のこと。

5-2 脅威

脅威の名称	脅威の定義
T.NETWORK_DISCLOSURE	保護ネットワークに関して細心の注意を払うべき情報については、イングレスまたはエグレスに基づくアクションの結果によって、公開される可能性がある。
T. NETWORK_ACCESS	ネットワーク外から保護ネットワーク上のサービスまたは保護ネットワーク内からの保護ネットワーク外の他のサービスに対して、不適切なアクセスが行われる可能性がある。
T.NETWORK_MISUSE	保護ネットワークによって利用可能なサービスへのアクセスは、運用環境ポリシーに反して使用できる。
T.NETWORK_サービス運用妨害（DOS）	保護ネットワーク内でのサービスに対する攻撃、または保護ネットワーク内からの悪意のあるエージェントへのアクセスによる間接的な攻撃により、その他保護ネットワーク内で利用できるサービスのサービス運用妨害（DOS）となる可能性がある。

5.1.3 組織のセキュリティ方針

ステートフルトラフィックフィルタファイアウォール特有の組織的方針は決定していない。しかし、NDPP の組織のセキュリティ方針はいずれもステートフルトラフィックフィルタファイアウォールに適用される。

5.1.4 セキュリティ課題記述への対応

以下の表は、本 EP で定義されているまたは特定されているセキュリティ対策方針に対して本 EP に記載されている脅威および前提条件の位置付けを示す。

5-3 セキュリティ課題記述の一致

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 および O.PORT_FILTERING
T. NETWORK_ACCESS	O.ADDRESS_FILTERING, O.RELATED_CONNECTION_FILTERING および O.PORT_FILTERING
T.NETWORK_MISUSE	O.ADDRESS_FILTERING, O.PORT_FILTERING および O.SYSTEM_MONITORING
T.NETWORK_サービス運用妨害（DOS）	O.ADDRESS_FILTERING, O.STATEFUL_INSPECTION および O.PORT_FILTERING

5.2 セキュリティ対策方針

5.2.1TOE のためのセキュリティ対策方針

以下の表には、ステートフルトラフィックフィルタファイアウォール特有のセキュリティ対策方針を示す。こうしたセキュリティ対策方針は、NDPP で定義されているセキュリティ対策方針に加えたものであり、すべてがステートフルトラフィックフィルタファイアウォールに適用される。本 EP では、二つの NDPP セキュリティ対策方針（O.SYSTEM_MONITORING および O.TOE_ADMINISTRATION）が拡張されているが、対応するセキュリティ対策方針の定義には、影響が及ぶことのない点に留意のこと。

5-4 TOE のため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、送信元アドレスおよび送信先アドレスに基づくネットワークパケットのフィルタを通過させ、ログする手段を提供する。
O.PORT_FILTERING	TOE は、送信元および送信先のトランスポート層ポートに基づくネットワークパケットのフィルタを通過させ、ログする手段を提供する。
O.STATEFUL_INSPECTION	TOE は、ネットワークパケットが、規則集を適用する前に許可され、確立された接続に属するか否かを判断する。
O.RELATED_CONNECTION_FILTERING	特定のプロトコルでは、TOE は、規則集によって許可された接続に対して、動的にネットワークパケットフローを許可する。

5.2.2 運用環境のセキュリティ対策方針

以下の表には、ステートフルトラフィックフィルタファイアウォールの運用環境特有のセキュリティ対策方針を示す。こうしたセキュリティ対策方針は、NDPP で定義されたセキュリティ対策方針に加えたものであり、すべて、ステートフルトラフィックフィルタファイアウォールの運用環境に適用する。

5-5 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、TOE が付属ネットワークのネットワークトラフィックのフロー上で効果的にその方針を実施できる方法で TOE がインストールされていることを確認する。

5.2.3 セキュリティ対策方針の一致

本 EP で規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関係は、第 3 節に記載されている。