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／
ステートフルトラフィクフィルタ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
侵入防止システム (IPS) の拡張パッケージ (EP)

2017 年 6 月 15 日
バージョン 2.11

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
情報セキュリティ認証室

目次

1 序説 4
1.1 適合主張 4
1.2 本拡張パッケージの使用方法 4
1.3 適合評価対象 4
2 セキュリティ課題定義 8
2.1 許可されない情報の暴露 8
2.2 許可されないアクセス 9
2.3 サービスへの不適切なアクセス 9
2.4 サービスの中断または拒否 9
3 セキュリティ対策方針 10
3.1 システム監視 10
3.2 ネットワークトラフィクポリシー違反の分析 10
3.3 ネットワークトラフィクポリシー違反への対抗措置 10
3.4 TOE の管理 10
3.5 高信頼通信 11
4 セキュリティ要件 12
4.1 表記法 12
4.2 TOE セキュリティ機能要件 12
4.2.1 FAU：セキュリティ監査 13
4.2.2 FMT：セキュリティ管理 15
4.2.3 IPS：侵入防止 16
5 テスト環境 28
6 セキュリティ保証要件 30
附属書 A： 根拠 31
A.1 セキュリティ課題定義 31
A.1.1 前提条件 31
A.1.2 脅威 31
A.1.3 組織のセキュリティ方針 32
A.1.4 セキュリティ課題定義の対応付け 32
A.2 セキュリティ対策方針 32
A.2.1 TOE のセキュリティ対策方針 32
A.2.2 運用環境のセキュリティ対策方針 33
A.2.3 セキュリティ対策方針の対応付け 33
A.3 セキュリティ機能要件の根拠 33
附属書 B： オプションの要件 35
B.1 要件 35
B.1.1 FAU：セキュリティ監査 35
B.1.2 FMT：セキュリティ管理要件 36
B.1.3 FPT：TSF の保護 37
B.1.4 FRU：資源の利用 39
B.1.5 IPS：侵入防止 40
附属書 C： 選択に基づいた要件 42
C.1 要件 42

C.1.1 FCS：暗号サポート.....42
附属書 D： オブジェクティブな要件.....43
D.1 要件.....43
D.1.1 FAU：セキュリティ監査.....43
附属書 E： 定義.....46
E.1 攻撃の定義.....46
E.2 用語と略語の定義.....47

表

表 4-1：セキュリティ機能要件.....12
表 4-2：監査対象事象と追加の監査記録の内容.....14
表 A-1：TOE の前提条件.....31
表 A-2：脅威.....31
表 A-3：方針.....32
表 A-4：セキュリティ課題定義の対応付け.....32
表 A-5：TOE のセキュリティ対策方針.....32
表 A-6：運用環境のセキュリティ対策方針.....33
表 A-7：明示的に言明された要件の根拠.....33
表 A-8：SFR 依存性の根拠.....33
表 D-1：事象表 (いくつかの例が挿入されている).....44

図

図 1：TOE 展開シナリオ図.....7
図 2：インラインモード試験トポロジーの例.....28
図 3：プロミスキャスモード試験トポロジーの例.....28

1 序説

本拡張パッケージ (EP) は、ネットワークベースの侵入防止システム (IPS) (プライベートネットワーク内、またはそのエッジに設置される侵入防止製品であって、リアルタイムにネットワークトラフィクの収集、検査、分析、そして対抗措置が可能なものと定義される) のセキュリティ要件を記述するものであって、明確に定義され記述された脅威の低減を目標とする要件の最小ベースラインセットの提供を意図している。本 EP はそれ自体で完結したものではなく、*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* (ND cPP) または*ステートフルトラフィクフィルタ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* (FW cPP) のいずれかを拡張するものである。この概論では適合評価対象 (TOE) の機能を記述するとともに、本 EP が ND cPP または FW cPP あるいはその両方との関連においてどのように使われるべきかについても論ずる。

1.1 適合主張

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 (ND cPP) は、ネットワークインフラストラクチャデバイス一般のベースラインセキュリティ機能要件 (SFR) 及びセキュリティ保証要件 (SAR) を定義する。*ステートフルトラフィクフィルタ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* (FW cPP) は、ND cPP と同様の SFR 及び SAR を定義するが、トラフィクフィルタファイアウォールに特有の要件が追加される。本 EP は、IPS デバイスに特有の追加の SFR 及び関連する「保証アクティビティ」によって、ND cPP または FW cPP のいずれかによるベースラインを拡張するものである。保証アクティビティは、TOE の SFR への適合性を判断するために評価者が行うアクションである。

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 改定第 4 版に適合している。CC パート 2 拡張及び CC パート 3 に適合する。

1.2 本拡張パッケージの使用方法

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

本 EP が ND cPP 上の構築に用いられる場合、適合 TOE は ND cPP に要求される機能と共に、本書でこれ以降論ずる脅威環境に対応して、本 EP に定義される追加機能をも実装することが義務付けられる。同様に、本 EP が FW cPP 上の構築に用いられる場合、適合 TOE はその PP のすべての要件と共に、本 EP によって定義される要件をも満たすことが期待される。本 EP によって拡張される PP は、「ベース PP」と呼ばれる。

ST 作成者は、IPS TOE が ND cPP の代わりに FW cPP への適合をも主張することが適切かどうかを考慮すべきである (should)。ある意味では、IPS EP は FW cPP を満たすように設定された TOE とは適合性がないかもしれない。これは、すべてのインタフェースが常に一定の種類のトラフィクをブロックすることを FW cPP が要求する一方で、このことはすべての IPS TOE 展開には適切でないかもしれないためである。しかし、ST 作成者がすべての認証済み IPS TOE 設定を本 IPS EP 及び FW cPP のすべての SFR に適合させようとする場合、本 IPS EP の作成者は 2 つの EP に適合性がないことは意図していない。

本 EP における要件のセットが適用範囲を限定されているのは、より迅速かつ安価な評価を推奨してエンドユーザへ価値を提供するために意図されたものである。

1.3 適合評価対象

本 EP は、特にネットワークベースの侵入防止システム (IPS) を対象とする。適合 IPS は、1 つ以上の個別のネットワークに接続される製品であり、全体的なエンタープライズセキュリティソリューションの一部として管理されるものである。特に、適合 IPS はネットワーク

セキュリティ管理者へ、潜在的に悪意のあるネットワークトラフィクのリアルタイムな監視、収集、ロギング、そして対抗措置を行う能力を提供する。本 EP は、IP トラフィク (TCP、UDP、ICMP、等) の検査に焦点を絞っている。この適用範囲の限定は、以下を含む数々の理由から意図されたものである：EP 内で定義されるテストの適用範囲 (保証手段) に合理的な境界を定義し、将来の EP がスキャナ、アナライザ、センサなどを含む他の IPS や機能へ対処できるようにすること。EP の適用範囲は他の IP プロトコル (例えば GRE、ESP、AH) のサポートを除外するものではないが、本 EP の適用範囲にはレイヤ 2 プロトコルや Ethernet を含む非 IP プロトコルの評価は含まれない。

本 EP のベースライン要件は侵入防止製品に必要なものとして定められたものであるが、適合 TOE は他のネットワークコンポーネントから全く独立した IPS 機能を提供してもよいし、より大規模なエンタープライズセキュリティソリューションの他のコンポーネントと連携して動作するよう展開されてもよい。例えば、すべての適合 IPS TOE はネットワークトラフィクの監視、収集、分析、及び対抗措置を行う何らかの能力を持たなければならない (must) が、適合 TOE は以下の実行もできるであろう：

- その 1 つ以上のインタフェースによって受動的に検出されたすべてのネットワークトラフィクを監視したり、及び／または検査のため IPS によって通過させられた、または IPS を通過した特定のトラフィクフローのみを監視したりすること。
- IPS データを外部監査ストレージホストへ送信すること、及びオプションとして IPS データを内部的に保存すること。IPS 監査データはプッシュ (TOE によって開始) されてもよいし、プル (リモートホストによって開始) されてもよい。IPS データがプッシュされるかプルされるかに関わらず、その送信は ND cPP 及び FW cPP の FAU_STG_EXT.1 に要求される保護された通信と一貫性のある形で保護されなければならない (must)。
- 管理者が TOE 上で直接設定可能なルールに基づいてネットワークトラフィクを分析すること、及びオプションとして他のシステムからインポート／適用されたルールに基づいてネットワークトラフィクを分析すること。
- 潜在的に悪意のあるトラフィクへ独立して対抗措置 (トラフィクフローをブロックすることによって、あるいはエンドポイントへセションのリセットを送信することによって) を取ること、及びオプションとして非 TOE コンポーネントへのコネクションを開始してその非 TOE コンポーネントにトラフィクフローを妨害させる／妨害するように設定することによってエンタープライズセキュリティソリューション全体の非 TOE コンポーネントと連携して対抗措置を取ること。

適合 IPS TOE と侵入検知システム (IDS) との間には多くの類似点が存在するが、いくつかの重要な相違点がある。適合 IPS TOE が IDS と異なるのは、適合 TOE はアクティブな潜在的脅威を終了させる／中断させるためのプロアクティブな対応を開始することが可能でなければならず (must)、また疑わしいトラフィクフローの中断を引き起こすであろう対応をリアルタイムに開始するという点である。潜在的に悪意のあるトラフィクが検出された際、TOE が監査事象やその他の警告を発生することができるだけでは十分ではない。しかし、IPS 管理者はそのようなプロアクティブな対応が有効とならないように TOE を設定することを選択してもよいし、そのような設定は TOE の有効な設定となるであろう。適合 TOE はその IDS 機能のみを有効として展開されてもよいが、適合 TOE は評価中にその能力を論証しなければならない (must)。

適合 TOE は、さまざまなアプローチを用いて潜在的に悪意のあるネットワークトラフィクを検出する。おおざっぱに言って、トラフィク分析は「既知」の脅威、または「未知」の脅威の識別に基づいて行うことが可能である。「既知」の脅威の識別はパターンマッチングによって、例えば IP パケット中の文字列のマッチング、あるいは偵察またはサービス拒否 (DoS) 攻撃に共通するトラフィクパターンのマッチングによって、行える。「未知」の脅威の識別は、さまざまな形態の「異常」検出を利用して行える。これは IPS が「異常」な (予期しない／典型的でない) トラフィクパターンを検出し対抗措置を取れるように、「予期される／典型的な」トラフィクパターンの定義が提供される (または「学習」／作成する) も

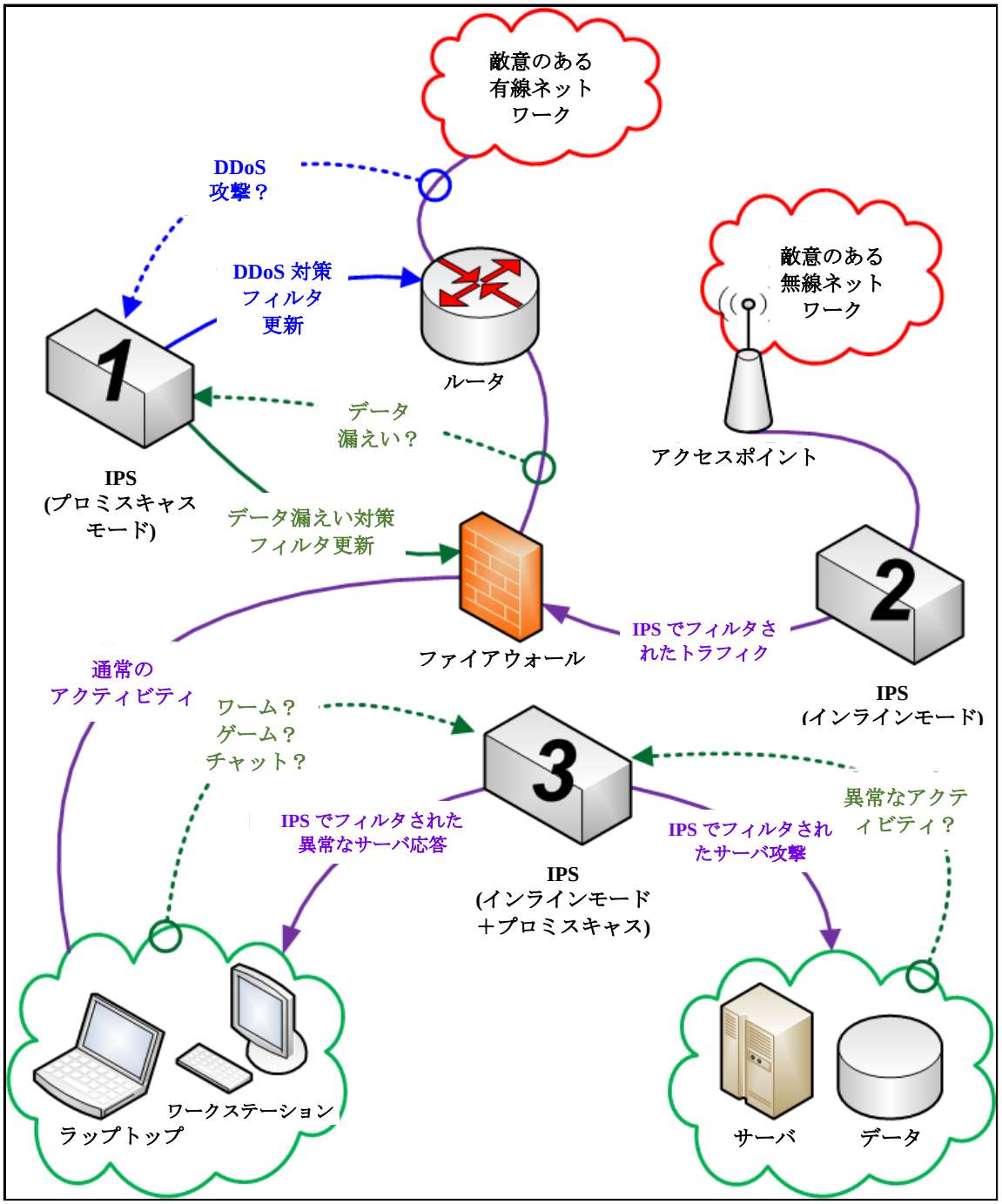
のである。

TOE は、IP ネットワーク上に分散された別個の TOE コンポーネントによって一部の SFR または SFR のエレメントが強制されるような分散 TOE であるかもしれない。そのような場合には、その製品のすべてのコンポーネントの総和が本 EP に定義される要件を満たせると共に個別コンポーネントのそれぞれが基本 ND cPP または FW cPP それ自身を満たせるように、TOE 境界が引かれなければならない (must)。さらに、これらの分散コンポーネント間のすべての通信は、ND cPP または FW cPP に定義される 1 つ以上の高信頼通信プロトコルを利用して保護されなければならない (must)。

TOE によってサポートされる展開シナリオには図 1 に示すものが含まれるであろう。これには、単一ネットワーク内で可能な IPS 機能の展開がいくつか含まれている。

- **IPS 1** はプロミスキャスモードで動作しており、境界ファイアウォール外部の 2 つの別個のネットワークからデータをキャプチャし、必要に応じてトラフィックフィルタ更新を境界ルータ及び境界ファイアウォールへ送信して、不要なトラフィックをリアルタイムでブロックする。
- **IPS 2** はインラインモードで動作しており、ワイヤレスネットワークへ送受信されるトラフィクを分析し、管理者定義 IPS ポリシーに違反する任意のトラフィクをリアルタイムでブロックする。
- **IPS 3** はプロミスキャスモードとインラインモードの組み合わせで動作している。この IPS には TOE を介したブリッジの作成またはルーティングを行う少なくとも 1 対のインタフェースがあり、トラフィクが TOE を通過する際にリアルタイムでトラフィクを分析しフィルタリングしている。同一の IPS には 1 個以上のプロミスキャスインタフェースがあり、それぞれ別個のネットワーク内を通過するトラフィクを収集し分析し、そして異常なアクティビティ、ワーム、あるいはその他の許可されないアクティビティへの対抗措置を取る。

図 1：TOE 展開シナリオ図



2 セキュリティ課題定義

IPS デバイスは、監視対象ネットワーク上の潜在的に悪意のあるトラフィクの検出とそれへの対抗措置に関連した一連のセキュリティ脅威に対処する。それらの脅威に対抗して、対象となるネットワークトラフィクへセキュリティポリシーが強制される。悪意のあるトラフィクは、監視対象ネットワーク上の 1 個以上のエンドポイントへ、またはネットワークインフラストラクチャへ、あるいは TOE そのものへの脅威を発生させるかもしれない。「監視対象ネットワーク」という用語は、ここでは TOE が直接接続される任意のネットワークと共に、ネットワークセグメント／サブネットであってそのトラフィクが分析のため IPS へ転送 (リダイレクトまたはコピー) されているものを意味する。

「IPS データ」という用語は本 EP を通して使われ、以下のいずれかまたはすべてが含まれる：ネットワークトラフィクから抽出され TOE 上に保存されるデータ；TOE によって行われた分析の結果；そしてその分析への TOE の対抗措置を示すメッセージ。本 EP で記述されるこの「IPS データ」は、IPS によって収集されるネットワークトラフィク及びそのネットワークトラフィクの分析に関連して生じる監査記録を意味し、その全てはベース PP の FAU_GEN に定義される「監査データ」、例えば管理者の認証や高信頼チャネルの確立／終了に関連した監査記録とは別個のものである。

サイトは、それ自身のリスク分析とその知覚される脅威とに関連して、サイトのセキュリティポリシーを開発し、そのニーズを満たす適切な対応がもたらされるように IPS が強制するルールセットを設定する責任を負う。適合 TOE によって低減される脅威には、以下の試行が含まれる可能性がある：

- さまざまなスキャンやマッピングテクニックの利用などによる、ネットワークベースの偵察 (監視対象ネットワークまたはそのエンドポイントに関する情報の探索)。
- サービス拒否攻撃などによる、監視対象ネットワーク、エンドポイント、またはサービスの通常機能の妨害。
- 力ずくのパスワード推定攻撃などによる、あるいは悪意のある実行可能コード、スクリプト、またはコマンドの送信による、1 個以上のネットワーク、エンドポイント、またはサービスへの不適切なアクセスの取得。
- クレジットカード番号の送信など、ポリシーに違反する情報の暴露／送信。データとの関連において、脅威エージェントの位置は関係ないことに留意されたい。例：データ漏えいは、それを移転する適切な認可なくデータが移転されたことを意味する。これはプルかもしれないし、プッシュかもしれない。外部からの侵入の結果として、あるいは内部者のアクションによって引き起こされる可能性がある。

本 EP では ND cPP または FW cPP あるいはその両方で特定された脅威を繰り返すことはしないが、本 EP の ND cPP または FW cPP への適合性、したがって依存性を考慮すればそれらの脅威がすべて適用されることに留意されたい。さらに、本 EP には ND cPP 及び FW cPP に定義されるものと同一の脅威の対象となる TOE 機能 (セキュリティ管理機能など) が記述される。脅威と対策方針との間の完全な対応付けは、本 EP の附属書 A に提供される。

ND cPP には、TOE がそれ自体の機能を提供する能力への脅威のみが含まれる。FW cPP には ND cPP と同一の脅威がすべて含まれるが、TOE の運用環境中の資源への脅威が追加される。本 EP はまた、運用環境中の資源への脅威に注目し、その一部は FW cPP に定義されるものと同様であるがトラフィクフィルタではなく IPS の視点から対処されることになる。主張されるベース PP の脅威と本 EP に定義される脅威とを合わせて、IPS TOE によって対処されるセキュリティの脅威の包括的なセットが定義される。

2.1 許可されない情報の暴露

保護ネットワーク上の機密性のある情報が、暗号化されていないクレジットカード番号の送信など、ポリシーに違反する情報の暴露／送信の結果として暴露されるおそれがある。

IPS TOE は、パケットペイロードのデータ文字列や文字のパターンを検査できること。

(T.NETWORK_DISCLOSURE)

2.2 許可されないアクセス

攻撃者が、力ずくのパスワード推定攻撃などによる、あるいは悪意のある実行可能コード、スクリプト、またはコマンドの送信による、1 個以上のネットワーク、エンドポイント、またはサービスへの不適切なアクセスの取得を試行するかもしれない。悪意のある外部デバイスが保護ネットワーク上のデバイスと通信できる場合には、これらのデバイスが情報の許可されない暴露を可能としてしまうかもしれない。

(T.NETWORK _ACCESS)

2.3 サービスへの不適切なアクセス

保護ネットワークによって提供されるサービスへのアクセスが、運用環境ポリシーに反して用いられるおそれがある。保護ネットワーク外部に位置するデバイスが、許可された公共サービスと通信する一方で不適切なアクティビティを行おうと試みるかもしれない (例えば、常駐ツールの操作、SQL インジェクション、フィッシング、強制リセット、悪意のある zip ファイル、偽装された実行可能形式、特権昇格ツール及びボットネット)。

(T.NETWORK_MISUSE)

2.4 サービスの中断または拒否

保護ネットワーク内部のサービスに対する攻撃によって、または保護ネットワーク内部から悪意のあるエージェントへのアクセスによって間接的に、保護ネットワーク内部で利用できるはずのサービスの拒否がもたらされるおそれがある。少数の発信源からの連携したサービス要求フラッディングの場合、資源の枯渇が発生する可能性がある。大部分の IPS は DDoS (分散サービス拒否) 攻撃に対する何らかの保護を提供するが、DDoS 攻撃に対する保護の提供は適合 TOE への要件ではない。これはファイアウォールやクラウドコンピューティング及び設計によって最もよく対処されるためである。しかし、DOS 保護は要求されることに留意されたい。

(T.NETWORK_DOS)

3 セキュリティ対策方針

セクション 2 に記述されたセキュリティ課題は、IPS 機能の組み合わせと、監視対象ネットワークのネットワークトラフィクへ効果的にポリシーが強制されるように TOE が設置されるという了解によって対処される。適合 TOE は、TOE への脅威に対処し、収集されたネットワークトラフィクデータへ分析プロセスを適用し、IPS 管理者によって IPS へ適用されるエンタープライズポリシーを実施する、セキュリティ機能を提供する。以下のサブセクションでは、これまでに論じた脅威／ポリシーに対処するために必要とされるセキュリティ対策方針の記述を提供する。

注記 : 以下のサブセクションのそれぞれには、具体的なセキュリティ対策方針が特定 (O.によって明示) されていて、これらはその対策方針を満たすメカニズムを提供する関連セキュリティ機能要件 (SFR) と対応付けられている。

3.1 システム監視

潜在的なネットワークポリシー違反を分析し対抗措置を取ることを可能とするため、IPS は監視対象ネットワーク上のネットワークトラフィクの本質的なデータエレメントを収集し保存することができなければならない (must)。

(O.SYSTEM_MONITORING -> FAU_ARP.1 (オブジェクティブ), FAU_GEN.1/IPS, FAU_SAR.1 (オブジェクティブ), FAU_SAR.2 (オブジェクティブ), FAU_SAR.3 (オブジェクティブ), FAU_STG.1 (オプション), FAU_STG.4 (オプション), FRU_RSA (オプション))

3.2 ネットワークトラフィクポリシー違反の分析

監視対象ネットワーク上に存在、または監視対象ネットワークを介して通信するエンティティは、承認済みネットワーク利用方法の潜在的違反についてネットワークアクティビティを効果的に分析されなければならない (must)。TOE は、情報の許可されない暴露、サービスへの不適切なアクセス、そしてネットワーク資源の乱用のリスクを低減させるために、監視対象ネットワークから収集されたデータを効果的に分析できなければならない (must)。

(O.IPS_ANALYZE -> IPS_ABD_EXT.1, IPS_IPB_EXT.1, IPS_NTA_EXT.1, IPS_SBD_EXT.1, IPS_SBD_EXT.2 (オプション))

3.3 ネットワークトラフィクポリシー違反への対抗措置

TOE は、IPS 管理者によって設定されたようにリアルタイムで対抗措置を取り、管理者定義 IPS ポリシーに違反すると判断されたトラフィクフローの終了またはブロックあるいはその両方を行えなければならない (must)。

(O.IPS_REACT -> FAU_ARP.1 (オブジェクティブ), IPS_ABD_EXT.1)

3.4 TOE の管理

ベース PP に定義される許可されない管理者アクセスの脅威に対応するために、適合 TOE は TOE の IPS 機能を管理者が設定するために必要な機能を提供すること。

(O.TOE_ADMINISTRATION -> FMT_MOF.1/IPS (オプション), FMT_MTD.1/IPS (オプション), FMT_SMF.1/IPS, FMT_SMR.2/IPS (オプション))

3.5 高信頼通信

ベース PP に定義される信頼できない通信チャネルの脅威により一層対応するために、適合 TOE は分散コンポーネントが存在する場合にはそれらの間の高信頼通信を提供すること。

(O.TRUSTED_COMMUNICATIONS (オプション) -> FPT_ITT.1 (オプション))

4 セキュリティ要件

本セクションでは TOE のセキュリティ機能要件を規定するとともに、評価者の行う保証アクティビティも規定する。

4.1 表記法

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

- 割付：*イタリック体*のテキストで示す。
- PP 作成者によってなされた詳細化：エレメント番号の後に**太字**で表記された「詳細化」という単語と、**太字**の追加されたテキスト及び必要に応じて取り消し線で表記された削除によって示される。
- 選択：下線付きテキストで示す。
- 選択中の割付：*イタリック体の下線付き*テキストで示す。
- 繰返し：SFR またはエレメント名に、スラッシュ及びその SFR またはエレメントのサポートする機能の一意の指示、例えば「/IPS」を付記して示す。

CC パート 2 が割付または選択の操作を指定しており、PP がすでにその操作を完了しているため ST 作成者がこの操作の実行ができない場合、その操作は上記の表記法を用いて示されるが ST 作成者に「選択：」または「割付：」というプロンプトが示されることはない。

明示的に言明された SFR は、TOE SFR の要件名の後にラベル「EXT」を持つことによって特定される。

4.2 TOE セキュリティ機能要件

ND cPP または FW cPP のいずれかの拡張パッケージとして、本 EP には IPS 機能に関連するいくつかの SFR と、関連する監査及び管理機能が定義される。本 EP に適合する TOE は、ND cPP または FW cPP あるいはその両方に適合することも期待される。本 EP は、これらの PP のいずれかに含まれるいかなるオプションの SFR の取り込みまたは除外も義務付けるものではなく、またこれらの PP 中で定義される SFR のいかなる選択、割付、または詳細化操作も完了させるものではない。本 EP によって定義される TOE の IPS 機能は、下表に示されると共に以下のセクションで定義される。

表 4-1：セキュリティ機能要件

クラス名	コンポーネント識別情報	コンポーネント名
FAU：監査生成	FAU_GEN.1/IPS	監査データの生成 (IPS)
FMT：セキュリティ管理	FMT_SMF.1/IPS	管理機能の特定 (IPS)
IPS：侵入防止システム	IPS_ABD_EXT.1	異常ベースの IPS 機能
	IPS_IPB_EXT.1	IP ブロッキング
	IPS_NTA_EXT.1	ネットワークトラフィク分析
	IPS_SBD_EXT.1	シグネチャベースの IPS 機能

4.2.1 FAU：セキュリティ監査

IPS EP には、IPS のふるまいに関する監査対象事象であって、ベース PP に定義される TSF のふるまいの監査対象事象と同様であるが、FAU_GEN.1 の別個の繰返しとしての存在が正当化されるほど十分に異なるものが定義される。

4.2.1.1 FAU_GEN.1/IPS：監査データの生成 (IPS)

FAU_GEN.1.1/IPS 詳細化：TSF は、以下の監査対象 **IPS** 事象の **IPS** 監査記録を生成できなければならない(shall)：

a) **IPS** 機能の及び終了；

b) 監査のレベルが [指定されない] すべての **IPS** 監査対象事象；及び

~~c) すべての管理アクション；~~

d) [*すべての異種の IPS 事象；*

e) すべての異種の IPS 対抗措置；

f) 規定された時間間隔内に発生した同種の事象の総数；及び

g) *規定された時間間隔内に発生した同種の対抗措置の総数。*]

適用上の注釈：*ST 作成者は提示されたリストに制約されず、生成される追加の情報があればそれによって以下の「事象の表」を更新すべきである(should)。EP 作成者は、標準的な (非 IPS データ) 監査機能についてはベース PP 中に定義される FAU_GEN.1 を用いるべきである(should)。*

「同種」及び「異種」の事象に関しては、異種の事象は単なるタイムスタンプ以外の何かが他の事象と異なる特性を有する事象である一方で、「同種」の事象はある時間内の同一事象の複数回の発生であってこれらの事象間の唯一の有意な違いがタイムスタンプであるものである。例えば、合理的な時間間隔内に発生した同一の種類の事象のすべてについて個別の監査メッセージを TOE が生成することは期待されない (例えば、TSF は Y 秒間に X 回繰り返された事象について 1 個の監査メッセージのみを生成する必要がある)。

FAU_GEN.1.2/IPS 詳細化：TSF は、各 **IPS 監査対象事象**内に少なくとも以下の情報を記録しなければならない(shall)：

a) 事象の日付及び時刻、事象**または対抗措置あるいはその両方**の種別、~~サブジェクトの識別情報、及び事象の結果 (成功または失敗)；~~及び；

b) **IPS** 監査**対象**事象種別のそれぞれについて、PP~~/ST~~ に含まれる機能コンポーネントの監査対象事象の定義に基づいた、表 4-2 *に列挙される具体的に定義された監査対象事象*]。

適用上の注釈：*前述の適用上の注釈と同様に、送信元及び宛先アドレス、IP、事象を引き起こしたシグネチャ、ポートなど、生成される追加の情報があれば、ST 作成者はそれによって以下の事象の表を更新すべきである(should)。*

IPS_SBD_EXT.1 及び IPS_ABD_EXT.1 に関しては、監査メッセージ中にアクションを明示的に特定することが必要ないであろう状況もいくつか存在するかもしれない、例えば：ポリシー定義の中で TOE のアクションが暗黙的に指定された場合、またはデフォルトのアクションがトラフィクを許可する場合、「ブロックされる」の欠如は、トラフィクが許可されることを暗黙的に示すだろう。

IPS_SBD_EXT.1 について、特定のヘ枝フィールドが審査され、デフォルトでドロップまたは改変される場合 (例、チェックサム不良のパケット、ゼロにセットされたリザーブビット)、このロギング要件は、適用されない。

表 4-2：監査対象事象と追加の監査記録の内容

要件	監査対象事象	追加監査記録の内容
FMT_SMF.1/IPS	IPS ポリシーエレメントの変更。	変更された IPS ポリシーエレメントの識別子または名称 (例、シグネチャ、ベースライン、または既知の良好な／既知の有害なリストが改変されたような)。
IPS_ABD_EXT.1	異常ベースの IPS ポリシーに、検査対象トラフィクが合致した。	送信元及び宛先 IP アドレス。
		ポリシーに合致すると判断されたヘッダフィールドの内容。
		パケットを受信した TOE インタフェース。
		事象を引き起こした異常ベースの IPS ポリシールールの側面 (例、スループット、曜日、頻度、等)。
		TOE によるネットワークベースのアクション (例、許可、ブロック、送信元 IP へのリセット送信、ファイアウォールへのブロック通知送信)。[1]
IPS_IPB_EXT.1	IPS ポリシーへ適用されている既知お良好なまたは既知の有害なアドレスのリストに、検査対象トラフィクが合致した。	送信元及び宛先 IP アドレス (及び、該当する場合、送信元アドレスまたは宛先アドレスあるいはその両方のどれがリストに合致したかの表示)。
		パケットを受信した TOE インタフェース。
		TOE によるネットワークベースのアクション (例、許可、ブロック、リセット送信)。[2]
IPS_NTA_EXT.1	TOE インタフェース上で有効な IPS ポリシーの改変。 適用された IPS ポリシーを持つ TOE インタフェースの有効化／無効化。 TOE インタフェース上で有効なモードの改変。	TOE インタフェースの識別情報。
		IPS ポリシー及びインタフェースモード (該当する場合)。
IPS_SBD_EXT.1	シグネチャベースの IPS ポリシーに、検査対象トラフィクが合致した。	合致したシグネチャの名称または識別子。
		送信元及び宛先 IP アドレス。
		シグネチャに合致すると決定されたヘッダフィールドの内容。
		パケットを受信した TOE インタフェース。
		TOE によるネットワークベースのアクション (例、許可、ブロック、リセット送信)。[3]
IPS_SBD_EXT.2.1 (オプション)	カプセル化パケットの検査。	カプセル化手法の表示。
IPS_SBD_EXT.2.2 (オプション)	フラグメント化パケットの再構成の失敗。	送信元及び宛先 IP アドレス。
		フラグメントを受信した TOE インタフェース。

[1] 適用上の注釈を参照。
[2] 適用上の注釈を参照。
[3] 適用上の注釈を参照。

要件	監査対象事象	追加監査記録の内容
IPS_SBD_EXT.2.3 (オプション)	TOE によるトラフィックの正規化。	破棄されたパケットの送信元及び宛先 IP アドレス。
		パケットを受信した TOE インタフェース。

アクティビティ	保証アクティビティ
TSS	評価者は、該当するポリシーと関連付けられた IPS データをロギングするよう TOE を設定する方法が、TSS 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、どの (同種の) IPS 事象種別を TOE が単一の監査記録へ結合するか、またそれが行われる条件 (例えば、閾値及び時間間隔) が、TSS に記述されていることを検証しなければならない(shall)。TSS には、(もしあれば) 設定可能な範囲についても記述されなければならない(shall)。 IPS_SBD_EXT.1 について、それぞれのフィールドに対して、評価者は、そのフィールドが検査される方法、及びロギングが該当しない場合は配備された集計のようなその他のメカニズムについて、TSS に記述されていることを検証しなければならない(shall)。
AGD	評価者は、該当する IPS データロギングを行うように TOE を設定する方法が、操作ガイダンスに記述されていることを検証しなければならない(shall)。 評価者は、同様の事象のログ出力に関して行うことのできる設定 (例、閾値の設定、時間帯の定義など) があれば、その指示が操作ガイダンスに提供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、IPS ポリシーを設定するために用いられるインタフェースから、その IPS ポリシーと関連した期待される IPS データが得られることをテストしなければならない(shall)。すべての要求される IPS 事象を引き起こすために、多くの IPS ポリシーの組み合わせと順序のシナリオが設定され、設定された IPS ポリシーと一致する許可されたネットワークトラフィクと異常なネットワークトラフィクの両方の通過を試行することによって、テストされる必要がある。本アクティビティは、その他の IPS 要件のテスト保証アクティビティの組み合わせを用いて対処されるべきである (should) ことに留意されたい。

4.2.2 FMT：セキュリティ管理

4.2.2.1 FMT_SMF.1/IPS 管理機能の特定 (IPS)

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

- *センサインタフェースに適用されるシグネチャの有効化、無効化、及び IPS 機能のふるまいの決定*
- *収集及び分析されるべきネットワークトラフィクを定義するようなこれらのパラメタの改変：*
  - *送信元 IP アドレス (ホストアドレス及びネットワークアドレス)*
  - *宛先 IP アドレス (ホストアドレス及びネットワークアドレス)*
  - *送信元ポート (TCP 及び UDP)*
  - *宛先ポート (TCP 及び UDP)*
  - *プロトコル (IPv4 及び IPv6)*
  - *ICMP のタイプ及びコード*
- *シグネチャの更新 (インポート)*
- *カスタムシグネチャの作成*
- *異常検出の設定*

- *シグネチャ、または異常の合致が検出されたときに、取られるべきアクションの有効化及び無効化*
- *IPS 対抗措置(リアクション)をトリガーする閾値の改変*
- *トラフィックをブロックするアクションの持続時間の改変*
- *既知良好及び既知有害リストの (IP アドレスまたはアドレス範囲の) 経変*
- *シグネチャベースの IPS ポリシーを上書きするような、既知の良好な及び既知の有害なリストの設定*]

***適用上の注釈:** 以下の保証アクティビティは、本 SFR のベース PP のサポート文書により規定される保証アクティビティに加えて、実行されるべきである。*

アクティビティ	保証アクティビティ
TSS	評価者は、IPS データ分析と対抗措置が設定できる方法が 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は、IPS_ABD_EXT.1、IPS_IPB_EXT.1 及び IPS_ABD_EXT.1 の TSS 保証アクティビティと共に対応されるべきである(should)ことに留意されたい
AGD	評価者は、SFR に定義される機能のそれぞれについて指示が操作ガイダンスに記述され、任意の設定可能なデフォルトの設定方法や該当する分析パターンマッチング手法及び対抗措置モードのそれぞれを設定する方法を含め、IPS データ分析と対抗措置を設定する方法が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	評価者は、以下のテストを行わなければならない(shall)： テスト 1：評価者は、シグネチャを作成し、インタフェース上でそれを有効化するために、操作ガイダンスを利用しなければならない(shall)。次に評価者は、シグネチャによってうまく引き起こされるようなトラフィクを生成しなければならない(shall)。評価者は、シグネチャ中の対応する対抗措置を TOE が適用することを確認すべきである(should)。 テスト 2：次に評価者はシグネチャを無効化し、同一のトラフィクの再生成を試行して TOE が対抗措置なしにトラフィクの通過を許可することを保証しなければならない(shall)。 テスト 3：評価者は、シグネチャをインポートし、テスト 1 で実施されたテストを繰り返すために、操作ガイダンスを利用しなければならない(shall)。 その他すべての機能は、IPS_ABD_EXT.1、IPS_SBD_EXT.1 のテスト保証アクティビティの組み合わせと共に対応されているべきである(should)ことに留意されたい。

4.2.3 IPS：侵入防止

4.2.3.1 IPS_ABD_EXT.1 異常ベースの IPS 機能

IPS_ABD_EXT.1.1 TSF は、[選択 (1 つ以上を選択):ベースライン (『予期され許可される』)、異常 (『予期されない』) トラフィクパターン] の定義を、以下の規定 [選択：

- *スループット ([割付： 時間間隔 (例、分、時間、日) あたりのデータエレメント (例、バイト、パケット等)])；*
- 時刻；
- 頻度；
- 閾値；
- [*割付：その他の手法*]]

及び以下のネットワークプロトコルのフィールド：

- [選択：IPS_SBD_EXT.1 に定義されるすべてのパケットヘッダ及びデータエレメント； [*割付：IPS_SBD_EXT.1 からのパケットヘッダ及びデータエレメントのサブセットリスト*]]

を含めてサポートしなければならない(shall)。

適用上の注釈：*ベースラインは既知良好トラフィクの定義である (IPS_ABD_EXT.1.3 によって許可される) 一方で、異常トラフィクは (『問題となる』) トラフィクの定義であって IPS_ABD_EXT.1.3 に定義されるその他のアクションによって取り扱われることになる。頻度は、例えば 1 時間のうちに確立された新規 FTP セション数など、定義された時間間隔における事象の発生回数 (シグネチャに合致するパケットの検出など) と定義することができる。『頻度』が選択された場合、TOE 上で頻度が定義される方法の説明が TSS に含まれなければならない(shall)。閾値は、例えば 1 時間当たり FTP によって転送されたデータのメガバイト数など、期待されるレベルまたは制約からの逸脱量またはパーセンテージとして定義することができる。『閾値』が選択された場合、TOE 上で閾値が定義される方法の説明が TSS に含まれなければならない(shall)。*

IPS_ABD_EXT.1.2 TSF は、 [選択：管理者による手作業の設定、自動化された設定] によって異常アクティビティの定義をサポートしなければならない(shall)。

適用上の注釈：*「ベースライン」及び「異常」は、TOE 管理者によって手作業で定義／設定される (または定義をインポートする) ものであってもよいし、あるいはある時間間隔内でネットワークトラフィクを検査することによって TOE が自動的に定義／作成できるもの (別名「プロファイリング」) であってもよい。IPS TOE がネットワークを「プロファイリング」してベースラインまたはルールを動的に定義する機能を持つことは本質的ではなく、また IPS TOE がその機能を持つ場合、そのような機能が IPS EP の一部として評価されることはない。*

IPS_ABD_EXT.1.3 TSF は、以下の操作を異常ベースの IPS ポリシーと関連付けられるようにしなければならない(shall)。

- 任意のモードにおいて、任意のセンサインタフェースについて： [選択：
  - トラフィクフローを許可する
  - 問題となるトラフィクの送信元アドレスへ TCP リセットを送信する；
  - 問題となるトラフィクの宛先アドレスへ TCP リセットを送信する；
  - ICMP [選択：ホスト、宛先、ポート] 到達不能通知を送信する；
  - 問題となるトラフィクパターンのブロックを非 TOE ネットワークデバイスに発動させる]
- インラインモードにおいて：
  - トラフィクフローを許可する
  - トラフィクフローをブロック／破棄する
  - 及び [選択：TOE を通過する以前にパケットを変更して転送する、その他のアクションなし]

アクティビティ	保証アクティビティ
TSS	評価者は、IPS_ABD_EXT.1.1 に規定されるベースラインまたは異常ベースの属性の作製、構築、及び適用が TSS 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、ベースラインが TOE によって定義され実装される方法の記述、または異常ベースのルールが管理者によって定義され設定される方法の記述が TSS に提供されていることを検証しなければならない(shall)。 評価者は、ベースラインまたは異常ベースのルールのそれぞれが IPS_ABD_EXT.1.3 で規定される対抗措置に関連付け可能であることを検証しなければならない(shall)。 評価者は、ベースラインまたは異常ベースのルールを適用可能なすべてのインタフェース種別が TSS に特定され、個別のネットワークインタフェースへそれらを関連付ける方法が説明されていることを検証しなければならない(shall)。インタフェースが共通のインタフェース種別にグループ分け可能な場合 (例えば、同一の内部論理パスが利用される場合、あるいは共通の

	デバイスドライバが利用される場合) それらはまとめて個別のネットワークインタフェースとして取り扱うことができる。
AGD	評価者は、IPS_ABD_EXT.1.1 でなされた選択に応じて手作業でベースラインまたは異常ベースのルールを作成するための指示が操作ガイダンスに提供されていることを検証しなければならない(shall)。ネットワークの動的な「プロファイリング」によってベースラインを確立することは、本 PP の適用範囲外であることに留意されたい。 評価者は、IPS_ABD_EXT.1.3 に規定される対抗措置をベースラインまたは異常ベースのルールと関連付けるための指示が操作ガイダンスに提供されていることを検証しなければならない(shall)。評価者は、異なるポリシーを個別のネットワークインタフェースと関連付けるための指示が操作ガイダンスに提供され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、以下のテストを行わなければならない(shall) : テスト 1 : 評価者は、操作ガイダンス中の指示を用いて、IPS_ABD_EXT.1.1 に規定される属性のそれぞれについて、ベースラインまたは異常ベースのルールを設定しなければならない(shall)。評価者は、ベースラインに合致しない、または異常ベースのルールに合致するトラフィクを送信し、設定された対抗措置を TOE が適用することを確認しなければならない(shall)。これは、IPS_ABD_EXT.1.1 中の各属性について行われなければならない(shall)。 テスト 2 : 上記のテスト保証アクティビティを繰り返して、TOE によってサポートされる個別のネットワークインタフェース種別のそれぞれについてベースラインまたは異常ベースのルールが定義可能であることを保証する。

4.2.3.2 IPS_IPB_EXT.1 IP のブロック

IPS_IPB_EXT.1.1 : TSF は、 [選択 : 送信元、宛先] IP アドレスの既知の良好な及び既知の有害なリストの設定及び実装をサポートしなければならない(shall)。

適用上の注釈 : *本 IPS EP が IP トラフィクの検査に限定されているため、本 SFR で定義されたアドレス種別は、IP アドレスに限定される (例、単一の IP または IP の範囲)。IPS TOE が、例えば MAC アドレスなど、他のアドレス種別に基づいてトラフィクフローの許可／禁止を行う機能を有効化することは禁止されていないが、その機能が存在する場合、どの設定で非 IP の既知の良好な及び既知の有害なアドレスのリストが IP ベースのアドレスリストよりも優先されることになるかは TSS 及びガイダンス文書で説明されなければならない (must)。*

IPS_IPB_EXT.1.2 : TSF は、IPS 管理者及び [選択 : その他の役割なし、 [*割付 : その他の役割*]] が以下の IPS ポリシーエレメント : [選択 : 既知の良好なリストのルール、既知の有害なリストのルール、IP アドレス、 [*割付 : その他の IPS ポリシーエレメント*]、その他の IPS エレメントなし] を設定できるようにしなければならない(shall)。

アクティビティ	保証アクティビティ
TSS	評価者は、パケット処理に関して良好／有害リストがトラフィクの分析方法へどう影響するかを検証しなければならない(shall)。また、送信元または宛先 IP アドレスの定義方法 (例えば単一 IP または IP アドレスの範囲) を含め、既知良好リスト、既知有害リスト、それらと関連付けられたルールを作成する属性についての詳細が TSS に提供されるべきである(should)。 また評価者は、すべての役割と、それらの役割のそれぞれについて要件に規定されているアクセスのレベルが TSS に特定されていることも検証しなければならない(shall)。
AGD	評価者は、要件で規定される役割のそれぞれが既知の良好な及び既知の有害なリストの属性を作成、変更及び削除できる方法に関する指示が管理ガ

	イダンスに提供され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、以下のテストを行わなければならない(shall)： テスト 1：評価者は、操作ガイダンス中の指示を用いて既知有害アドレスリストを作成しなければならない(shall)。そのリストから単一の IP アドレス、アドレスのリストまたはアドレスの範囲を用いて、評価者はそのリストが存在しなければ TOE に許可されたであろうトラフィクの TOE を介した送信を試行し、TOE が自動的にそのトラフィクを破棄することを確認しなければならない(shall)。 テスト 2：評価者は、操作ガイダンス中の指示を用いて既知良好アドレスリストを作成しなければならない(shall)。そのリストから単一の IP アドレス、アドレスのリストまたはアドレスの範囲を用いて、評価者はそのリストが存在しなければ TOE に拒否されたであろうトラフィクの TOE を介した送信を試行し、TOE が自動的にそのトラフィクを許可することを確認しなければならない(shall)。 テスト 3：評価者はリストのそれぞれに相反する IP アドレスを追加して、TOE が相反するトラフィクを IPS_NTA_EXT.1.1 の優先度と一貫性のある形で処理することを保証しなければならない(shall)。

4.2.3.3 IPS_NTA_EXT.1 ネットワークトラフィク分析

IPS_NTA_EXT.1.1 TSF は、TOE のセンサインタフェースへ転送される IP ベースのネットワークトラフィクの分析を行って、管理者定義 IPS ポリシーの違反を検出しなければならない(shall)。

適用上の注釈：*一部の TOE においては任意の TOE インタフェースがセンサインタフェースとなり得るのは事実かもしれないが、その機能は要件とはなっていない。この SFR では、「センサインタフェース」という用語は 1 つ以上の IPS ポリシーが適用されている任意の TOE インタフェースを指して使われる。管理者定義 IPS ポリシーは、1 つ以上の TOE インタフェースへ適用されるトラフィク分析、トラフィクのブロック、シグネチャ検出、または異常検出、あるいはこれらの組み合わせのルールの任意のセットである。TOE には、管理者が IPS ポリシーエレメント (既知良好リスト、既知有害リスト、シグネチャベースのルール、及び異常ベースのルール) の優先度を設定できるようにする能力があってもよいが、そのような設定可能性は一切本 EP では要求されない。*

アクティビティ	保証アクティビティ
TSS	評価者は、TOE のポリシー階層構造 (優先度) の観点から、IP トラフィクを分析する TOE の能力が TSS に説明されていることを検証しなければならない(shall)。IPS ポリシーエレメント (既知良好リスト、既知有害リスト、シグネチャベースのルール、及び異常ベースのルール) について TOE のポリシー階層構造順序付けが管理者によって設定可能かどうかは、TSS に特定されるべきである(should)。優先度が設定可能かどうかにかかわらず、評価者はデフォルトの優先度に加えて TOE のサポートする IP 分析機能が TSS に記述されていることを検証しなければならない(shall)。 この要件に関連付けられた TSS は、後続の保証アクティビティにおいて評定される。
AGD	評価者は、ガイダンスにデフォルトの優先度が記述されていることを検証しなければならない(shall)。 優先度が設定可能である場合。評価者は、優先度の設定方法がガイダンスに説明されていることを検証しなければならない(shall)。
テスト	この要件に関連付けられたテストは、後続の保証アクティビティにおいて評定される。

IPS_NTA_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 (検査する能力を有し) なければならない(shall) :

- インターネットプロトコル (IPv4)、RFC 791
- インターネットプロトコル バージョン 6 (IPv6)、RFC 2460
- インターネット制御通知プロトコル バージョン 4 (ICMPv4)、RFC 792
- インターネット制御通知プロトコル バージョン 6 (ICMPv6)、RFC 2463
- 伝送制御プロトコル (TCP)、RFC 793
- ユーザデータプロトコル (UDP)、RFC 768

適用上の注釈 : *プロトコル RFC の識別情報は、常に識別されたプロトコル RFC へすべてのパケットが適合することを TOE が保証しなければならない(must)ことを意味せず、また常に任意のトラフィクフローについて RFC への完全な適合性を TOE が実施できることを意味するものでもない。RFC の識別情報は、他の SFR 及び本 SFR で、別途、識別されるパケットの内容 (ヘッダ、フィールド、状態、コマンド等) を理解するための参照のフレームワークを提供するものである。ここでの意味は、SFR を通して識別される RFC パラメタの範囲で TOE が RFC 実装を理解する能力がなければならない(must)ということである。*

アクティビティ	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ていることが TSS に示されていることを検証しなければならない(shall) : ● IPv4 ● IPv6 ● ICMPv4 ● ICMPv6 ● TCP ● UDP 評価者は、識別されたプロトコルへの適合性が TOE 開発者によって決定される方法について、TSS に記述されていることを検証しなければならない(shall)。(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)
AGD	本要件に関連付けられたガイダンスは、後続の保証アクティビティにおいて評定される。
テスト	本要件に関連付けられたテストは、後続の保証アクティビティにおいて対応される。

IPS_NTA_EXT.1.3 TSF は、プロミスキャスモードに設定されたセンサインタフェースへ、及びインラインモードに設定されたインタフェースへ、シグネチャを割り当てることができるようにしなければならず(shall)、また、同時にセンサインタフェースとはせず TOE と外部エンティティとの間の通信のための「管理」として 1 つ以上のインタフェース割り当てをサポートしなければならない(shall)。

- プロミスキャス (待ち受けのみ) モード : [*割付 : インタフェース種別のリスト*] ;
- インライン (データパススルー) モード : [*割付 : インタフェース種別のリスト*] ;
- 管理モード : [*割付 : インタフェース種別のリスト*] ;
- [選択 :
  - セションリセット可能インタフェース : [*割付 : セションリセット可能なインタフェースのリスト*] ;
  - [*割付 : その他のインタフェース種別*] ;
  - その他のインタフェース種別なし]。

適用上の注釈 : インタフェース種別は、イーサネット、ギガビットイーサネット等である。プロミスキャスインタフェースは、トラフィクを検査する目的のみのためにネットワークトラフィクを待ち受けるものであるが、OSI レイヤ 2、レイヤ 3、またはより高いレイヤのいずれの機能も持たないため、ネットワークサービスがそのインタフェース上で待ち受け

ることはなく、そのインタフェース上で有効化される IP プロトコルスタックは存在しないため、そのインタフェースへは IP アドレスは割り当てられない。インラインインタフェースは 1 対のインタフェースであって、トラフィクフローが TOE によってリアルタイムにブロックまたは変更できるようにネットワークトラフィクが TOE を通過するパスを提供するものである。プロミスキャスインタフェースと同様に、インラインインタフェースは OSI レイヤ 3 及びより高位の機能をサポートしないのが典型的であるが、(インタフェースへ MAC アドレスを割り当てて) OSI レイヤ 2 機能を提供し、隣接するネットワークデバイスが TOE へ／を介してトラフィクを転送できるようにしてもよい。

TOE は、FTP_ITC、及び FTP_TRP に定義されるすべてのエンティティを含めたリモートエンティティと TOE との間の通信用に OSI レイヤ 3 インタフェースとして設定可能な管理 (administration/management) 目的で用いられる別個のインタフェースをサポートしてもよい。TOE はオプションとして追加のなインタフェース種別をサポートしてもよい。セションリセットインタフェースは、プロミスキャス、インライン、管理、またはその他のインタフェースのいずれかと同一であってもよいし、別個のインタフェースであってもよい。セションリセット機能は TOE の必須機能ではないが、SFR 内で選択可能なオプションである。

IPS_NTA_EXT.1.1 の適用上の注釈で触れたように、TOE が複数の単一目的インタフェース (例えば「センサ」インタフェース、「管理」インタフェースなど) を持つ必要はないが、1 つ以上の特定のインタフェース機能を果たすよう特定のポートを TOE が有効化できることは期待される。

アクティビティ	保証アクティビティ
TSS	評価者は、プロミスキャスのモードまたはインラインモードあるいはその両方で展開可能なすべてのインタフェース種別と、各展開モードを利用するために必要なインタフェースが TSS に特定されていることを検証しなければならない(shall) (最小限、インタフェースはインラインモードをサポートする必要がある)。また TSS には、管理インタフェースがセンサインタフェースとどう異なるかという記述が提供されるべきである(should)。
AGD	評価者は、TSS に概説される展開手法のそれぞれを展開する方法に関する指示が、操作ガイダンスに提供されていることを検証しなければならない(shall)。また評価者は、展開モードのそれぞれについてインタフェースへ IPS ポリシーを適用する指示が操作ガイダンスに提供されていることも検証しなければならない(shall)。管理インタフェースが設定可能である場合、評価者はインタフェースを管理インタフェースとして設定する方法が操作ガイダンスに説明されていることを検証しなければならない(shall)。 評価者は、TOE がリモートトラフィクフィルタリングデバイスへコマンドを送信する方法が操作ガイダンスに説明されていることを検証しなければならない (shall)。 注記 : TOE とリモートデバイスとの間のセキュアなチャネルの設定は、ベース PP の FTP_ITC.1 (ST 作成者がその他のインタフェース種別を選択した場合) または FTP_TRP.1 (管理モードにあるインタフェースについて) あるいはその両方に従って論じられることになるであろう。
テスト	この要件に関連付けられたテストは、プロミスキャス及びインラインインタフェースがテストされる後続の保証アクティビティ(例、IPS_SBD_EXT.1.7 のテスト) ならびにベース PP の FTP_ITC.1 (ST 作成者がその他のインタフェース種別を選択した場合) または FTP_TRP.1 (管理モードにあるインタフェースについて) あるいはその両方の要件中で完了される。

4.2.3.4 IPS_SBD_EXT.1 シグネチャベースの IPS 機能

IPS_SBD_EXT.1.1 TSF は、パケットヘッダの内容の検査をサポートし、また少なくとも以下のヘッダフィールドを検査できなければならない(shall) :

- IPv4：バージョン； ヘッダ長； パケット長； ID； IP フラグ； フラグメントオフセット； Time to Live (TTL)； プロトコル； ヘッダチェックサム； 送信元アドレス； 宛先アドレス； IP オプション； 及び [選択：サービスタイプ(ToS：Type of Service)、その他のフィールドなし]。
- IPv6：バージョン；ペイロード長； ネクストヘッダ； ホップリミット； 送信元アドレス； 宛先アドレス； ルーティングヘッダ； 及び [選択：トラフィッククラス、フローラベル、その他のフィールドなし]。
- ICMP：タイプ； コード； ヘッダチェックサム； 及び[選択：ID、 シーケンス番号、[割付： ICMP ヘッダのその他のフィールド]]。
- ICMPv6：タイプ； コード； 及びヘッダチェックサム。
- TCP：送信元ポート； 宛先ポート； シーケンス番号； アクノリッジ番号； オフセット； 予約； TCP フラグ； ウィンドウ； チェックサム； 緊急ポインタ； 及び TCP オプション。
- UDP：送信元ポート； 宛先ポート； 長さ； 及び UDP チェックサム。

アクティビティ	保証アクティビティ
TSS	評価者は、シグネチャルール内に何が含まれるか TSS 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、シグネチャのそれぞれが IPS_SBD_EXT.1.5 に規定される対抗措置に関連付け可能であることを検証しなければならない(shall)。 評価者は、シグネチャを適用可能なすべてのインタフェース種別が TSS に特定され、個別のネットワークインタフェースへルールを関連付ける方法が説明されていることを検証しなければならない(shall)。インタフェースが共通のインタフェース種別にグループ分け可能な場合 (例えば、同一の内部論理パスが利用される場合、あるいは共通のデバイスドライバが利用される場合) それらはまとめて個別のネットワークインタフェースとして取り扱うことができる。
AGD	評価者は、以下のプロトコル及びヘッダ検査フィールドを用いてルールを作成または設定あるいはその両方を行う方法に関する指示が操作ガイダンスに提供されていることを検証しなければならない(shall)。 ● IPv4：バージョン、ヘッダ長、パケット長、ID、IP フラグ、フラグメントオフセット、Time to Live (TTL)、プロトコル、ヘッダチェックサム、送信元アドレス、宛先アドレス、及び IP オプション。 ● IPv6：バージョン、トラフィッククラス、フローラベル、ペイロード長、ネクストヘッダ、ホップリミット、送信元アドレス、宛先アドレス、ルーティングヘッダ、ホームアドレスオプション。 ● ICMP：タイプ、コード、ヘッダチェックサム、及び残りのヘッダ (ICMP タイプとコードによって異なる)。 ● ICMPv6：タイプ、コード、及びヘッダチェックサム。 ● TCP：送信元ポート、宛先ポート、シーケンス番号、アクノリッジ番号、オフセット、予約、TCP フラグ、ウィンドウ、チェックサム、緊急ポインタ、及び TCP オプション。 ● UDP：送信元ポート、宛先ポート、長さ、及び UDP チェックサム。 評価者は、IPS_SBD_EXT.1.5 に規定される対抗措置をシグネチャルール中に選択または設定あるいはその両方を行う方法に関する指示が操作ガイダンスに提供され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、以下のテストを行わなければならない(shall)： テスト 1：評価者は、操作ガイダンス中の指示を用いて、以下に列挙された属性のそれぞれについて、IPS_SBD_EXT.1.5 に規定される対抗措置が選択または設定あるいはその両方が行われたパケットヘッダシグネチャが作成または設定あるいはその両方が行えることをテストしなければならない (shall)。属性のそれぞれには、その一意のシグネチャが独立して割り当てられなければならない(shall)：

	● IPv4：バージョン、ヘッダ長、パケット長、ID、IP フラグ、フラグメントオフセット、Time to Live (TTL)、プロトコル、ヘッダチェックサム、送信元アドレス、宛先アドレス、及び IP オプション。 ● IPv6：バージョン、トラフィッククラス、フローラベル、ペイロード長、ネクストヘッダ、ホップリミット、送信元アドレス、宛先アドレス、ルーティングヘッダ、ホームアドレスオプション。 ● ICMP：タイプ、コード、ヘッダチェックサム、及び残りのヘッダ (ICMP タイプとコードによって異なる)。 ● ICMPv6：タイプ、コード、及びヘッダチェックサム。 ● TCP：送信元ポート、宛先ポート、シーケンス番号、アクノリッジ番号、オフセット、予約、TCP フラグ、ウィンドウ、チェックサム、緊急ポインタ、及び TCP オプション。 ● UDP：送信元ポート、宛先ポート、長さ、及び UDP チェックサム。 パケットスニファを用いて、評価者はシグネチャを発動するトラフィクを生成し、パケットキャプチャを用いて各ルールの対抗措置が予期されるとおり行われたことを保証すること。 テスト 2：上記のテスト保証アクティビティを繰り返して、TOE によってサポートされるとおりシグネチャが適用可能な個別のネットワークインタフェース種別のそれぞれについてシグネチャベースの IPS ポリシーが定義可能であることを保証する。

IPS_SBD_EXT.1.2 TSF は、パケットペイロードデータの検査をサポートし、また少なくとも以下のデータエレメントを文字列ベースのパターンマッチングを行って検査できなければならない(shall)：

- ICMPv4 データ：ICMP ヘッダの最初の 4 バイト以降の文字。
- ICMPv6 データ：ICMP ヘッダの最初の 4 バイト以降の文字。
- TCP データ (20 バイトの TCP ヘッダ以降の文字)、以下の検出のサポートを含む：
  i) FTP (ファイル転送) コマンド：help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, 及び type。
  ii) HTTP (ウェブ) コマンド及び内容：GET 及び POST を含むコマンド、及び URL/URI に合致する管理者定義の文字列、及びウェブページの内容。
  iii) SMTP (電子メール) 状態：開始状態、SMTP コマンド状態、メールヘッダ状態、メールボディ状態、中断状態。
  iv) [選択： [*割付：その他の種類の TCP ペイロード検査*]、その他の種類の TCP ペイロード検査なし] ;
- UDP データ：8 バイトの UDP ヘッダ以降の文字；
- [*割付：その他の種類のパケットペイロード検査*]

さらに、TSF は複数のフラグメント化されていないパケットにわたって分割されている場合であっても悪意のあるペイロードを検出するために、ストリームの再構成または同等の機能をサポートしなければならない(shall)。

アクティビティ	保証アクティビティ
TSS	評価者は、文字列ベースの検出シグネチャ内に何が含まれるか TSS 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、パケットペイロード文字列ベースの検出シグネチャのそれぞれが IPS_SBD_EXT.1.5 に規定される対抗措置に関連付け可能であることを検証しなければならない(shall)。
AGD	評価者は、IPS_SBD_EXT.1.2 に定義されるパケットペイロード文字列ベースの検出フィールドを用いてルールを設定する方法に関する指示が操作ガイダンス

	に提供されていることを検証しなければならない (shall)。操作ガイダンスには、必要な場合、複数パケットにまたがるペイロードを検出するための方法が提供されなければならない(shall)。 評価者は、文字列ベースの検出シグネチャのそれぞれについて、IPS_SBD_EXT.1.5 に規定される対抗措置を設定する方法に関する指示が操作ガイダンスに提供されていることを検証しなければならない(shall)。 評価者は、シグネチャと関連付け可能な個別のネットワークインタフェースにルールを関連付ける方法に関する指示が操作ガイダンスに提供され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、以下のテストを行わなければならない(shall)： テスト 1 : 評価者は、操作ガイダンス中の指示を用いて、IPS_SBD_EXT.1.2 に規定される属性を用いて IPS_SBD_EXT.1.5 に規定される対抗措置へパケットペイロード文字列ベースの検出ルールが割り当て可能であることをテストしなければならない(shall)。プロトコルデータのすべてのあり得る文字列をテストすることは要求されない (それは不可能でもある) が、評価者は要件中の文字列の選択がテストされるものとして選択されていることを保証しなければならない (shall)。最小限、IPS_SBD_EXT.1.2 から以下の属性のそれぞれを用いた少なくとも 1 つの文字列が、各プロトコルについてテストされるべきである(should)。評価者は、ルール中の文字列に合致するパケットを生成し、設定されたように対応する対抗措置が取られることを確認しなければならない(shall)。 ● ICMPv4 データについては、少なくとも 1 つの文字列をテストする：ICMP ヘッダの最初の 4 バイト以降。 ● ICMPv6 データについては、少なくとも 1 つの文字列をテストする：ICMP ヘッダの最初の 4 バイト以降。 ● TCP (20 バイトの TCP ヘッダ以降の文字)： i) 少なくとも 1 つの FTP (ファイル転送) コマンドをテストする : help, noop, stat, syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, 及び type。 ii) HTTP (ウェブ) コマンドと内容： (1) GET コマンドと POST コマンドの両方をテストする (2) 少なくとも 1 つの URL/URI に合致する管理者定義の文字列、及びウェブページの内容をテストする。 iii) 少なくとも 1 つの SMTP (電子メール) 状態をテストする：開始状態、SMTP コマンド状態、メールヘッダ状態、メールボディ状態、中断状態。 iv) [選択： [割付：その他の種類の TCP ペイロード検査] 内で定義される任意の追加の属性種別の中で、少なくとも 1 つの文字列をテストする； ● 少なくとも 1 つの UDP データの文字列をテストする : 8 バイトの UDP ヘッダ以降の文字； ● [*割付：その他の種類のパケットペイロード検査*] に定義される追加属性種別のそれぞれについて、少なくとも 1 つの文字列をテストする] テスト 2 : 評価者はテスト 1 中のテストの 1 つを繰り返すが、定義されたルール中の文字列を含むフラグメント化されていない複数のパケットを生成しなければならない(shall)。 テスト 3 : 上記のテスト保証アクティビティを繰り返して、TOE によってサポートされるとおりシグネチャが適用可能な個別のネットワークインタフェース種別のそれぞれについてシグネチャベースの IPS ポリシーが定義可能であることを保証する。

IPS_SBD_EXT.1.3 : TSF は、IP センサインタフェースにおいて以下のヘッダベースのシグネチャを (IPS_SBD_EXT.1.1 に特定されるフィールドを用いて) 検出できなければならない(shall) :

a) IP 攻撃
   i) IP フラグメントの重複 (Teardrop 攻撃、Bonk 攻撃、または Boink 攻撃)
   ii) IP 宛先アドレスと等しい IP 送信元アドレス (Land 攻撃)
b) ICMP 攻撃
   i) フラグメント化された ICMP トラフィク (例えば Nuke 攻撃)
   ii) 巨大な ICMP トラフィク (Ping of Death 攻撃)
c) TCP 攻撃
   i) TCP NULL フラグ
   ii) TCP SYN+FIN フラグ
   iii) TCP FIN のみのフラグ
   iv) TCP SYN+RST フラグ
d) UDP 攻撃
   i) UDP Bomb 攻撃
   ii) UDP Chargen DoS 攻撃

アクティビティ	保証アクティビティ
TSS	評価者は、IPS_SBD_EXT.1.3 に定義される攻撃が TOE によって処理される方法とこれらの攻撃が特定された際にどの対抗措置が発動されるか TSS に記述されていることを検証しなければならない(shall)。
AGD	評価者は、IPS_SBD_EXT.1.3 に定義される攻撃を特定するルールと、IPS_SBD_EXT.1.5 に規定されるこれらの攻撃への対抗措置を設定するための指示が操作ガイダンスに提供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、IPS_SBD_EXT.1.3 中の攻撃シグネチャのそれぞれについて、ルールの作成または設定あるいはその両方を行わなければならない(shall)。攻撃のそれぞれについて、TOE はそれに対応するシグネチャを適用し、シグネチャの適用が可能な個別のネットワークインタフェース種別のそれぞれに対してそれを有効化すべきである(should)。評価者はパケットキャプチャを利用して、攻撃トラフィクが TOE によって検出されること、そして IPS_SBD_EXT.1.5 に規定される対抗措置が発動され攻撃をストップすることを保証しなければならない (shall)。それぞれの攻撃は、それに対応するシグネチャの特定が成功して特定の攻撃へ適切な対抗措置が取られたことを保証するため、順次行われるべきである(should)。

IPS_SBD_EXT.1.4 : TSF は、以下のトラフィクパターン検出シグネチャのすべてを検出すること、及びこれらのシグネチャを IPS センサインタフェースへ適用させることができなければならない(shall) :

a) ホストのフラッディング (DoS 攻撃)
   i) ICMP フラッディング (Smurf 攻撃、及び ping フラッド)
   ii) TCP フラッディング (例えば SYN フラッド)
b) ネットワークのフラッディング (DoS 攻撃)
c) プロトコル及びポートのスキャン
   i) IP プロトコルスキャン
   ii) TCP ポートスキャン
   iii) UDP ポートスキャン
   iv) ICMP スキャン

適用上の注釈：*この SFR では、TOE が検出できなければならない(must) パケットヘッダフィールド、パケットペイロード文字列、シグネチャの種類、及び潜在的に悪意のあるトラフィクパターン (例えばフラッディング及びスキャン) の最小限のセットを定義している。有*

効なシグネチャはこの SFR に列挙される 1 つ、数個、またはすべての属性から構成可能であり、また IPS TOE はこの SFR に列挙されない追加の属性の検査をサポートしてもよいが、SFR に列挙されるもののみが評価者によって試験される。この SFR に特定されるシグネチャの種類、トラフィクパターンなどのセットは、悪意のあるアクティビティを網羅的にあるいは完全に代表するリストであることを意図したものではなく、また DDoS 攻撃への対応を意味するものでもない。この SFR の意図は、単一の送信元 IP からの攻撃へ対応することである。

プロトコル及びポートのスキャンとは、目標プロトコル／ポート番号の明白な (シーケンシャルに番号付けされた) パターンを用いて、またはプロトコル／ポート番号のランダム化または送信間遅延時間のランダム化あるいはその両方により、1 つ以上の目標 IP アドレス上の複数のプロトコル／ポートを目標とすることによって、目標 IP アドレスでオープン／待ち受け／応答サービスをスキャンする偵察攻撃を意味する。

IPS 製品ベンダが定義済みシグネチャをサポートすることは理解され期待されるが、定義済みシグネチャそれ自体の有効性の検査は本 EP の目的ではない。そうではなく、本 EP はネットワークトラフィクの詳細な分析を行う TOE の能力に焦点を絞っており、またこれらの定義済みシグネチャは評価中に利用されてもよいが、評価チームはカスタム作成されたシグネチャも使用することが期待される。シグネチャの種類、トラフィクパターンなどのセットとしてこのセットが選択された理由は以下のとおりである： 1) テストの適用範囲に合理的な境界を設定すること、及び 2) パケット内容を検査し、一定の時間間隔にわたってトラフィクパターンを収集し、そして収集されたデータを対応付ける TOE の能力を論証するトラフィクパターンと、パケット内容の十分なサンプリングを提供すること。

IPS センサインタフェースは、IPS ポリシーがその時点で適用されている任意の TOE インタフェースを指す。

アクティビティ	保証アクティビティ
TSS	評価者は、IPS_SBD_EXT.1.4 に定義される攻撃が TOE によって処理される方法とこれらの攻撃が特定された際にどの対抗措置が発動されるか TSS に記述されていることを検証しなければならない(shall)。
AGD	評価者は、IPS_SBD_EXT.1.4 に定義される攻撃を特定するルールと、IPS_SBD_EXT.1.5 に規定されるこれらの攻撃への対抗措置を設定するための指示が操作ガイダンスに提供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、IPS_SBD_EXT.1.4 中の攻撃のそれぞれについて、独立したシグネチャを設定しなければならない(shall)。攻撃のそれぞれについて、TOE はそれに対応するシグネチャを適用し、シグネチャの適用が可能な個別のネットワークインタフェース種別のそれぞれに対してそれを有効化すべきである(should)。評価者はパケットキャプチャを利用して、攻撃トラフィクが TOE によって検出されること、そして IPS_SBD_EXT.1.5 に規定される対抗措置が発動され攻撃をストップすることを保証しなければならない(shall)。それぞれの攻撃は、それに対応するシグネチャの特定が成功して特定の攻撃へ適切な対抗措置が取られたことを保証するため、順次行われるべきである(should)。

IPS_SBD_EXT.1.5 TSF は、以下の操作をシグネチャベースの IPS ポリシーと関連付けられるようにしなければならない(shall)。

- 任意のモードにおいて、任意のセンサインタフェースについて：[選択：
  - トラフィクフローを許可する；
  - 問題となるトラフィクの送信元アドレスへ TCP リセットを送信する；
  - 問題となるトラフィクの宛先アドレスへ TCP リセットを送信する；
  - ICMP [選択：ホスト、宛先、ポート] 到達不能通知を送信する；
  - 問題となるトラフィクパターンのブロックを非 TOE ネットワークデバイスに発動させる]

- インラインモードにおいて：
  - トラフィクフローを許可する；
  - トラフィクフローをブロック／破棄する；
  - 及び [選択 : TOE を通過する以前にパケットを変更して転送する、その他のアクションなし]

適用上の注釈：*「発動させる」という用語は、以下を含む複数の種類の相互作用を可能とするため使われている：TOE が IP ネットワーク上でリモートデバイスへの認証済み接続を開始してリモートデバイスのリモート管理インタフェースを利用してそのデバイスのアクティブな設定を変更する場合;または TOE と非 TOE ネットワークデバイスとの間の接続が IP ネットワークを通過しない場合。ST 作成者が「……非 TOE ネットワークデバイスを発動させる」を選択し、TOE と非 TOE ネットワークデバイスとの間の接続が IP ネットワークを通過する場合、ST 作成者は非 TOE デバイスが (ベース PP の) FTP_ITC.1.3 で特定されていることを保証しなければならず(must)、また TOE とリモートデバイスとの間の接続は FTP_ITC.1 に従ってセキュアにされなければならない(must)。SFR の最後の丸印で、「TOE を通過する以前にパケットを変更して転送する」には、個人を特定できる可能性のある情報やその他のプライベートなデータ (電話番号、クレジットカード番号、等) の送信のような、ポリシーに違反する正規表現 (regex) に合致する文字列をパケットデータから削除するようなアクションが含まれるかもしれない。*

5 テスト環境

本セクションには、保証アクティビティに特定されるテストを行うために用いられる評価者テスト環境への期待が含まれる。

セションを確立し、セションパケットを改変または作成し、そしてパケットが TOE を通過するかどうかを認識すると共にこれらのパケットの内容を検査するために適切なツールを評価者が有することが前提となる。一般的には、IPS ルール設定及び TOE のログ出力機能が、必要に応じて適切な決定に至るために利用できることが期待される。

上記のテストは、TOE のすべての「センサ」インタフェース上のネットワークトラフィクを監視可能な個別のネットワークインタフェース種別のそれぞれについて繰り返される必要があり、これには、(IP アドレスや IP スタックを伴うまたは伴わないような、またそのインタフェースには TCP リセットのようなパケットの送信によって認められていないトラフィクフローの終了を試行できるような、またはできないような)「プロミスキャス」インタフェース、及び IP アドレスや IP スタックを伴うまたは伴わないインライン(パススルー)インタフェースが含まれることがあるが、TOE へリモートにアクセスするために用いられる、または syslog サーバ、AAA サーバ、リモートトラフィクフィルタリングデバイス、等への外向きの接続を開始するために TOE によって利用される管理インタフェースを含まない。

評価者は、最小限、以下に図示するテスト環境と機能的に同等のテスト環境を作成しなければならない(shall)。評価者は、テスト環境における相違があれば、その正当化を提供しなければならない(must)。TOE は、一部の SFR や SFR のエレメントがネットワーク上に分散された別個の TOE コンポーネントによって実施されるような、分散型 TOE であってもよい。分散型 TOE に関しては：

- 「インラインモード試験トポロジー」における「TOE」は、トラフィクのフローを制御する TOE コンポーネントでなければならない(must) が、その TOE コンポーネントはトラフィクを収集または分析するものと同一のコンポーネントである必要はない；
- 「プロミスキャスモード試験トポロジー」における「TOE」は、非 TOE トラフィクフィルタリングデバイスと通信する TOE コンポーネントでなければならない(must) が、その TOE コンポーネントはトラフィクを収集または分析するものと同一のコンポーネントである必要はない。

図 2：インラインモード試験トポロジーの例

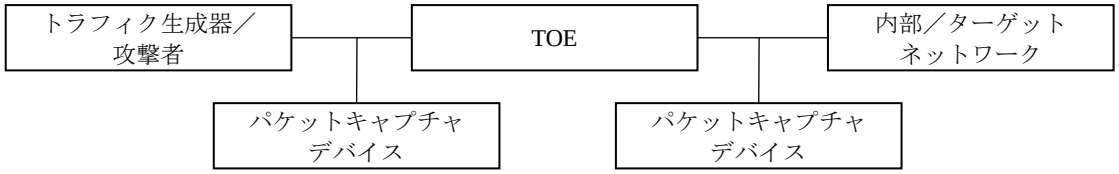
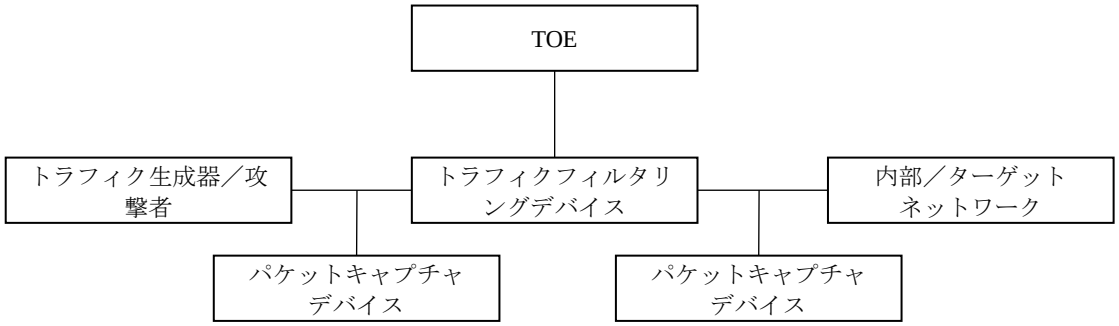


図 3：プロミスキャスモード試験トポロジーの例



2 つ以上のモードで展開可能な IPS デバイスでは、TOE の 2 つの実体化によってテストの実施が容易となることが多いが、TOE の 1 つのインスタンスが存在するとともに TOE と相互作用してテストアクティビティを満たすために必要な機能を提供するデバイスが存在するようなテストベッドを構築するのは評価者の自由である。

ネットワークパケットの構築にトラフィク生成器が用いられ、またネットワーク攻撃をシミュレートする能力を評価者へ提供することが期待される。トラフィク生成器は COTS (市販)、シェアウェア、またはフリーウェア製品であってもよい。特別な機器は必要とされない。

6 セキュリティ保証要件

本 EP には、ND cPP または FW cPP 中に定義されるもの以外には、いかなる SAR も定義されない。本 EP に対して評価される TOE は、本質的に選択されたベース PP に対しても評価されることは重要なので留意されたい。TOE を評価する際には、ベース PP に定義される SAR を、ベース PP に記述される部分だけでなく TOE 全体に適用することが必要とされる。

附属書A： 根拠

本 EP において、本文書の最初のセクションでは、IPS デバイスによって対処される脅威；これらの脅威を低減するために用いられる手法；及び適合 TOE によって達成される低減の程度についての、全体的な理解しやすさの向上を重視して、ナレーティブな表現を用いた。この表現のスタイルは、形式化された評価アクティビティにはそのまま適用できないため、本文書に関連付けられた評価アクティビティについて、利用可能な表形式のアーティファクトが、本セクションに含まれている。

A.1 セキュリティ課題定義

A.1.1 前提条件

以下に列挙する具体的な条件が、TOE の運用環境に存在することが前提となる。これらの前提条件には、ベース PP に定義されるものに加えて、TOE セキュリティ要件の開発における実践的な現実と TOE の利用上の不可欠な環境条件の両方が含まれる。

表 A-1：TOE の前提条件

前提条件の名称	前提条件の定義
A.CONNECTIONS	接続されたネットワーク間を流れるすべての該当するネットワークトラフィックに TOE セキュリティポリシーが強制されることが保証されるように、TOE が個別のネットワークへ接続されることが前提となる。

A.1.2 脅威

以下に列挙する脅威が IPS デバイスによって対処される。FW cPP がベース PP として主張される場合、これらの脅威のいくつかもまたそこで定義されることに留意されたい。これらの場合には、同一の一般的な脅威がファイアウォールと IPS 機能の組み合わせによって低減されることになる。

表 A-2：脅威

脅威の名称	脅威の定義
T.NETWORK_DISCLOSURE	保護ネットワーク上の機密性のある情報が、内向きまたは外向きベースのアクションの結果として暴露されるおそれがある。
T.NETWORK_ACCESS	保護ネットワーク上のサービスへそのネットワークの外部から、あるいは保護ネットワーク外のサービスへ保護ネットワーク内部から、許可されないアクセスが実行されるかもしれない。悪意のある外部デバイスがバックドアを介して保護ネットワーク上のデバイスと通信できる場合には、これらのデバイスが情報の許可されない暴露を可能としてしまうかもしれない。
T.NETWORK_MISUSE	保護ネットワークによって提供されるサービスへのアクセスが、運用環境ポリシーに反して用いられるおそれがある。保護ネットワーク外部に位置するデバイスが、許可された公共サービスと通信する一方で不適切なアクティビティを行おうと試みるかもしれない。例えば、常駐ツールの操作、SQL インジェクション、フィッシング、強制リセット、悪意のある zip ファイル、偽装された実行可能形式、特権昇格ツール及びボットネット。
T.NETWORK_DOS	保護ネットワーク内部のサービスに対する攻撃によって、または保護ネットワーク内部から悪意のあるエージェントへのアクセスによって間接的に、保護ネットワーク内部で利用できるはずのサービスの拒否がもたらされ

脅威の名称	脅威の定義
	るおそれがある。少数の発信源からの連携したサービス要求フラッディングの場合、資源の枯渇が発生する可能性がある。

A.1.3 組織のセキュリティ方針

TOE を展開する組織は、主張されるベース PP に定義されるすべての組織のセキュリティ方針に加えて、以下の組織のセキュリティ方針を満たすことが期待される。

表 A-3：方針

方針の名称	方針の定義
P.ANALYZE	潜在的侵入に関する結論を導出するための分析プロセス及び情報が IPS データに適用され、適切な対応アクションが取られなければならない (must)。

A.1.4 セキュリティ課題定義の対応付け

以下の表は、本 EP に定義される脅威、前提条件及び組織のセキュリティ方針 (OSP) を、やはり本 EP に定義または特定されるセキュリティ対策方針と対応付ける役割をしている。

表 A-4：セキュリティ課題定義の対応付け

脅威、前提条件、または OSP	セキュリティ対策方針
A.CONNECTIONS	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.SYSTEM_MONITORING O.IPS_ANALYSE, O.IPS_REACT
T.NETWORK_ACCESS	O.SYSTEM_MONITORING, O.IPS_ANALYSE, O.IPS_REACT
T.NETWORK_MISUSE	O.SYSTEM_MONITORING, O.IPS_ANALYSE, O.IPS_REACT
T.NETWORK_DOS	O.SYSTEM_MONITORING, O.IPS_ANALYSE, O.IPS_REACT
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS (ベース PP から)	O.TOE_ADMINISTRATION
T.UNSTRUSTED_COMMUNICATION_CHANNELS (ベース PP から)	O.TRUSTED_COMMUNICATIONS (オプション)
P.ANALYZE	O.IPS_ANALYZE, O.TOE_ADMINISTRATION

A.2 セキュリティ対策方針

A.2.1 TOE のセキュリティ対策方針

以下の表には、TOE のセキュリティ対策方針が含まれる。本 EP に適合する TOE は、これらのセキュリティ対策方針を満たすことができなければならない (shall)。

表 A-5：TOE のセキュリティ対策方針

セキュリティ対策方針の名称	セキュリティ対策方針の定義
O.SYSTEM_MONITORING	IPS は、監視対象ネットワーク上の乱用、不適切なアクセス、あるいは悪意のあるアクティビティと関連した IPS ポリシー違反を示す可能性のあるすべての事象に関する情報を収集し保存しなければならない (must)。
O.IPS_ANALYZE	IPS は、監視対象ネットワークから収集されたネットワークトラフィクデータへ分析プロセスを適用し、潜在的な侵入やネットワークトラフィクポリシーへ

セキュリティ対策方針の名称	セキュリティ対策方針の定義
	の違反に関する結論を導出しなければならない (must)。
O.IPS_REACT	IPS は、IPS ポリシー違反に関するその分析的結論に適切に対応しなければならない (must)。
O.TOE_ADMINISTRATION	IPS は、正当な管理者が TSF を設定する手法を提供する。
O.TRUSTED_COMMUNICATIONS	IPS は、TOE の分散コンポーネント間の通信が許可されない改変または暴露をこうむらないことを保証する。

A.2.2 運用環境のセキュリティ対策方針

以下の表には、IPS デバイスの運用環境に特有のセキュリティ対策方針が含まれている。これらのセキュリティ対策方針はベース PP に定義されるものに追加される。

表 A-6：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の名称	セキュリティ対策方針の定義
OE.CONNECTIONS	TOE 管理者は、監視対象ネットワークのネットワークトラフィクへ TOE がそのポリシーを効果的に強制することができるように TOE が設置されることを保証すること。

A.2.3 セキュリティ対策方針の対応付け

本 EP に特定または定義された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付けは、セクション 3 で提供される。

A.3 セキュリティ機能要件の根拠

表 A-7：明示的に言明された要件の根拠

SFR	根拠
IPS_ABD_EXT.1	この SFR は、運用環境から収集されたトラフィクから異常を分析し対抗措置を取る TOE の能力を正しく規定するために作成された。
IPS_IPB_EXT.1	この SFR は、既知の送信元 IP アドレスのホワイトリスト及びブラックリストを作成してシグネチャベースのトラフィク分析を上書きすることにより TOE のブロックを行う能力を最適化する TOE の能力を正しく規定するために作成された。
IPS_NTA_EXT.1	この SFR は、シグネチャベースと異常ベースの両方の検出についてトラフィクとネットワークプロトコルを分析する TOE の能力を正しく規定するために作成された。
IPS_SBD_EXT.1	この SFR は、運用環境から収集されたトラフィクからシグネチャを分析しシグネチャの合致に対抗措置を取る TOE の能力を正しく規定するために作成された。
IPS_SBD_EXT.2	この SFR は、トラフィク正規化を行い分析の目的でカプセル化及びフラグメント化されたパケットを再構成する適合 TOE の能力を定義するために作成された。

表 A-8：SFR 依存性の根拠

SFR	依存性	根拠
FAU_ARP.1	FAU_SAA.1	あるいは、(「潜在的なセキ

SFR	依存性	根拠
		ュリティ侵害」として、FAU_ARP.1.1 でフラグされるようなふるまいを決定するような) IPS クラスの拡張要件によって満たされる
FAU_GEN.1/IPS	FPT_STM.1	ベース PP から継承される
FAU_SAR.1	FAU_GEN.1/IPS	(FAU_GEN.1/IPS 繰り返しとして) EP に含まれる
FAU_SAR.2	FAU_SAR.1	EP に含まれる
FAU_SAR.3	FAU_SAR.1	EP に含まれる
FAU_STG.1	FAU_GEN.1	(FAU_GEN.1/IPS 繰り返しとして) EP に含まれる
FAU_STG.4	FAU_STG.1	EP に含まれる
FMT_MOF.1/IPS	FMT_SMF.1	(FMT_SMF.1/IPS 繰り返しとして) EP に含まれる
	FMT_SMR.1	(FMT_SMR.2/IPS 繰り返しとして)EP に含まれる階層的な SFR
FMT_MTD.1/IPS	FMT_SMF.1	(FMT_SMF.1/IPS 繰り返しとして) EP に含まれる
	FMT_SMR.1	(FMT_SMR.2/IPS 繰り返しとして)EP に含まれる階層的な SFR
FMT_SMF.1/IPS	依存性なし	該当せず
FMT_SMR.2/IPS	FIA_UID.1	あるいは、(1 つの SFR に識別と認証の両方を定義するような)ベース PP から検証された FIA_UIA_EXT.1 によって満たされる
FPT_FLS.1/Inline	依存性なし	該当せず
FPT_ITT.1	依存性なし	該当せず
FRU_RSA.1	依存性なし	該当せず
IPS_ABD_EXT.1	依存性なし	該当せず
IPS_IPB_EXT.1	依存性なし	該当せず
IPS_NTA_EXT.1	依存性なし	該当せず
IPS_SBD_EXT.1	依存性なし	該当せず
IPS_SBD_EXT.2	IPS_SBD_EXT.1	EP に含まれる

附属書B： オプション要件

ベースライン要件は、本 EP の本体に含まれる。これに追加して、これ以外の 3 種類の要件が附属書 B、C、及び D に特定されている。

(この附属書の) 第 1 の種類は、ST に含まれ得る要件であるが、TOE が本 EP への適合を主張するためには必要とされないものである。(附属書 C の) 第 2 の種類は、EP の本体中の選択に基づく要件である。特定の選択がなされた場合には、その附属書中の追加の要件が含まれることが必要となる。(附属書 D の) 第 3 の種類は、本 EP へ適合するためには要求されないが、本 EP の将来のバージョンのベースライン要件に含まれることになっているコンポーネントであり、IPS ベンダによる採用が推奨される。ST 作成者には、附属書 B、附属書 C、または附属書 D に含まれる要件と関連し得るが列挙されていない要件 (例えば、FMT タイプの要件) もまた、ST へ含まれることを保証する責任があることに留意されたい。

B.1 要件

オプションのセキュリティ機能要件は、以下のセクションに言明されている。

B.1.1 FAU：セキュリティ監査

「IPS データ」という用語には、ネットワークトラフィクから抽出され TOE 上に保存されるデータ；TOE によって行われた分析の結果；そしてその分析への TOE の対抗措置を示すメッセージのすべてが含まれる。この「IPS データ」の定義からはベース PP に関連する「監査データ」が除外される。除外されるデータには、管理者の認証、そして高信頼チャネルの確立／終了など、ベース PP の FAU_GEN に定義されるデータが含まれる。IPS データのレビューまたはストレージあるいはその両方やセキュリティ警報が TOE によってサポートされる場合には、以下の監査要件を適宜 ST に含めることができる。

B.1.1.5 FAU_STG.1 保護された監査証跡格納 (IPS データ)

FAU_STG.1.1 詳細化：TSF は、格納された~~監査記録~~**IPS データ**を許可されない削除から保護しなければならない (shall)。

FAU_STG.1.2 詳細化：TSF は、~~監査証跡中の~~格納された~~監査記録~~**IPS データ**への許可されない改変を [*防止*] できなければならない (shall)。

適用上の注釈：*FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

アクティビティ	保証アクティビティ
TSS	評価者は、IPS データが許可されない改変及び削除から保護される方法が TSS に特定されていることを保証しなければならない (shall)。
AGD	評価者は、IPS データを許可されない改変及び削除から保護する方法がガイダンス文書に記述されていることを確認しなければならない (shall)。
テスト	テスト 1：評価者は、IPS データが許可されない改変及び削除から保護できることを論証するテストを考案しなければならない (shall)。

B.1.1.6 FAU_STG.4 データ損失の防止 (IPS データ)

FAU_STG.4.1 詳細化：TSF は、~~監査~~**IPS データ**証跡が満杯になった場合、 [選択：「**それがなければ生成されたであろう監査 IPS** 事象**の生成**を無視」、「~~特別な権利を有する正当な利用者によるものを除いて~~、監査 **IPS** 事象を抑止」、「最も古く格納された~~監査記録~~ IPS データを上書き」]、及び [その他のアクションなし] **することができ**なければならない (shall)。

監査対象事象	追加監査記録の内容
ローカルな監査ストアがストレージの制限に達した。[4]	監査ストアに空きがなく、また (設定可能な場合) TOE がどのように対応したか (例えば新規監査対象事象の監査失敗、または監査対象事象の発生を抑止) の表示。

アクティビティ	保証アクティビティ
TSS	評価者は、IPS データ証跡に空きがなくなった際に IPS データのロギングがどのように取り扱われるか、TSS に特定されていることを保証しなければならない (shall)。また TSS には、IPS データのロギングが回復される方法も特定されなければならない (shall)。
AGD	評価者は、IPS データ証跡に空きがなくなった際に IPS データのロギングを管理するために必要なステップがガイダンス文書に記述されていることを確認しなければならない (shall)。
テスト	この要件にはテスト保証アクティビティは存在しない。

B.1.2 FMT：セキュリティ管理要件

TOE が複数の管理役割を許可する場合には、これらの要件を ST に含めることができる。

B.1.2.1 FMT_MOF.1/IPS セキュリティ機能のふるまいの管理

FMT_MOF.1.1/IPS TSF は、機能 [*IPS データの収集、分析、及び対抗措置*] のふるまいを改変する能力を[*正当な IPS 管理者*]に制限しなければならない (shall)。

アクティビティ	保証アクティビティ
TSS	評価者は、操作ガイダンスに特定される管理機能のそれぞれについて、管理者のログインに先立ってインタフェースを介してアクセス可能なものが特定されていることを決定するために、TSS を検査しなければならない(shall)。またこれらの機能のそれぞれについて、評価者はこのインタフェースを介してシステムの設定を操作する能力が非管理ユーザに許可されていないことが TSS に詳述されていることを確認しなければならない (shall)。
AGD	評価者は、本 EP の要件に対応して実装された機能のそれぞれが特定されていること、また管理者のみがその機能へアクセスできることを保証するための設定情報が提供されていることを決定するために、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	この SFR のテストは、本 EP に定義されるその他の FMT 要件のテストの一部として完了される。

B.1.2.2 FMT_MTD.1/IPS IPS データの管理

FMT_MTD.1.1/IPS 詳細化：TSF は、[*割付：~~TSF~~ IPS データのリスト*]を[選択：デフォルトの変更、問い合わせ、改変、削除、消去、 [*割付：その他の操作*]] する能力を、[*割付：IPS 管理者、IPS 分析者及び FMT_SMR.2/IPS で識別されたその他の IPS 特有の役割*] に制限しなければならない(shall)。

適用上の注釈：*ST には、どの役割 (IPS 管理者、IPS 分析者、及び FMT_SMR.2/IPS に特定されるその他の IPS 特有の役割) に IPS データへのアクセスが許可されるか定義されるべきである(should)。ST には、この要件を満たすために任意の数の役割が定義されてもよい。FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

[4] FAU_STG.4 の監査事象は、空きがない際に最も古い記録を上書きする監査ストアには適用されない。

アクティビティ	保証アクティビティ
TSS	評価者は、特定された役割のそれぞれについて、TOE 上でその役割に関連付けられた役割の責任とアクセス許可に関する記述が TSS に含まれていることを保証しなければならない(shall)。
AGD	評価者は操作ガイダンスをレビューして、正当な管理者が正当な役割及び要件中に特定された正当な役割の能力を制限するように設定するための指示が含まれていることを保証しなければならない(shall)。
テスト	この SFR に記述されたすべての操作が、すべての TOE インタフェースを介してアクセス可能であることは必要とされない。評価のためテストアクティビティを行うにあたって、評価者はこの SFR に記述される管理機能のそれぞれに該当するすべてのインタフェースを利用しなければならない(shall) が、各インタフェースについて管理アクションを伴う各テストを繰り返す必要はない。 テスト 1：評価者は、操作ガイダンスにより TOE を最初の使用のために設定した後、要件に定義される正当な役割のそれぞれを用いて IPS データを問い合わせ及び変更する能力が制限できることを論証しなければならない(shall)。

B.1.2.3 FMT_SMR.2/IPS セキュリティ役割 (IPS)

FMT_SMR.2.1/IPS 詳細化 : TSF は、役割： [***IPS 管理者、IPS 分析者、及び [選択： [割付：その他の正当な IPS 役割]、その他の役割なし]***] を維持しなければならない(shall)。

FMT_SMR.2.2/IPS TSF は、利用者を役割に関連付けなければならない(shall)。

FMT_SMR.2.3/IPS TSF は、[*割付：異なる役割の条件*] が満たされ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 に定義される役割は、IPS 機能の管理に特有のものを意図している。FMT_SMR.2 中でベース PP に定義される「正当な管理者」役割は本 EP に定義される「IPS 管理者」と同一の役割であってもよいし、異なる役割であって正当な管理者が TOE 全体を管理する完全な権利を持ち、IPS 管理者は IPS 特有の機能にのみ完全な権利を持っていてもよい。IPS 分析者の役割は、完全ではない権利を持つ役割を表現することが意図されている、または制限された読み出しのみの権利を持つかもしれない。その他の役割は、ST 作成者によって定義できる。FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

アクティビティ	保証アクティビティ
TSS	評価者は、IPS 管理者、IPS 分析者、及びこの SFR の割付において特定される任意のその他の役割の権利の間の違いが記述されていることを保証するため、TSS をレビューしなければならない(shall)。また TSS には、本 SFR で特定される IPS 管理者の権利と、ベース PP の FMT_SMR.2 に特定される正当な管理者との間で違いがある場合、それが記述されるべきである(should)。
AGD	この SFR には、操作ガイダンス保証アクティビティは存在しない。
テスト	TSF データの閲覧には管理役割が必要とされるため、FMT_MTD.1 の保証アクティビティにおいて評価者が行う分析によって、この要件が満たされていることが論証されることになる。

B.1.3 FPT：TSF の保護

B.1.3.1 FPT_FLS.1/Inline セキュアな状態を保持する故障

FPT_FLS.1.1/Inline 詳細化 : TSF は、以下の種別の故障が生じたときは、**インラインインタフェースについて**セキュアな状態を保持**することができ**なければならない(shall)： [*割付：*

TSF における故障の種類のリスト]。

適用上の注釈：*IPS EP におけるこの SFR の意図は、インラインインタフェースを通過するトラフィクについて事実上 IPS ポリシー違反を検出し対抗措置を取ることができなくなったり、トラフィクにこれらのインタフェースを通過させることができなくなったりするおそれのある、TOE に起こり得る故障の種類を ST 作成者が定義できるようにすることである。最初の詳細化「することができ (to be able)」は、TOE が部分的または完全に故障状態にある際でもトラフィクにインラインインタフェースを通過させられるように TOE 管理者が TOE を設定できるように、しかし TOE がそのように設定されていた場合にはトラフィクのブロックが可能であるという保証を提供するために、追加されている。この SFR の目的は、CC パート 2 に言明されているように、「特定されたカテゴリの故障が TSF に生じた際、TOE が常にその SFR を強制することを保証する」ためである。一部の SFR ではデータの検査が要求され、また検査はネットワークインタフェースが故障した際には行うことができないため、特定のコンポーネントの故障の際には「すべて」の SFR が引き続き強制されることが成り立つとは限らない。*

監査対象事象	追加監査記録の内容
TSF の故障。	発生した故障の種類。

アクティビティ	保証アクティビティ
TSS	評価者は、フェイルセキュアな機能の TOE の実装が文書化されていることを決定するために、TSS セクションをレビューしなければならない(shall)。まず評価者は、ST に規定されたすべての故障モードが記述されていることを保証するために、TSS セクションを検査しなければならない(shall)。次に評価者は、規定される故障モードの種類のそれぞれに入った後で TOE がセキュアな状態に達することを保証しなければならない(shall)。評価者は、これらの故障によってトラフィク転送がどのような影響を受けるかを TOE 管理者が設定できるかどうかを決定するために、TSS をレビューしなければならない(shall)。
AGD	本 SFR には、操作ガイダンス保証アクティビティは存在しない。
テスト	割付で列挙された故障の種類のそれぞれについて、TOE ベンダはその故障を引き起こすための手段を評価者へ提供しなければならず(must)、また評価者は故障の種類のそれぞれを再現して適用される IPS ポリシーが故障中に実施されたままであることを保証しなければならない(must)。例えば、電源の瞬断を含むさまざまな要因によって TOE のリブートが引き起こされる可能性がある。故障 (例、リブート) 時点でアクティブな IPS ポリシーが ICMP echo パケットが TOE によって破棄されることを保証している場合、評価者はシャットダウン中または TOE の再起動中のいかなる時点でも任意の ICMP echo パケットが TOE の通過を許可されないことを確認しなければならない(shall) (しかしこの例では、監査メカニズムが再開待ちの間 IPS 事象が監査されない期間が存在することは理解されるべきである(should))。

B.1.3.2 FPT_ITT.1 基本 TSF 内データ転送保護

FPT_ITT.1.1 詳細化：TSF は、TSF データが ~~TOE の分割された部分~~ **[*割付：分散 TOE コンポーネントのリスト*]** 間で送られる場合、**[選択：1 つ以上を選択：IPsec, SSH, TLS, HTTPS]** **を用いて** [暴露、改変] から保護しなければならない(shall)。

適用上の注釈：*ここでなされた選択に基づき、適合 ST はベース PP に定義された選択に基づいた SFR、FCS_IPSEC_EXT.1、FCS_HTTPS_EXT.1、FCS_SSHC_EXT.1、FCS_SSHS_EXT.1、FCS_TLSC_EXT.1、FCS_TLSC_EXT.2、FCS_TLSS_EXT.1、及び FCS_TLSS_EXT.2 の 1 つ以上を含むことになる。適合 ST はまた、オプションの O.TRUSTED_COMMUNICATIONS 対策方*

針を含むことになる。

アクティビティ	保証アクティビティ
TSS	評価者は TSS を検査して、要件中に特定される分散 TOE コンポーネント間のすべての通信について、そのコンポーネントに許可されるプロトコルの観点から、各通信メカニズムが特定されていることを判断しなければならない(shall)。また評価者は、TSS に列挙されたすべてのプロトコルが特定され、ST 中の要件に含まれていることを確認しなければならない(shall)。
AGD	評価者は、各 TOE コンポーネントに許可されるプロトコルを確立するための指示がガイダンス文書に含まれていること、及び万一接続が意図せず切断されてしまった際の回復指示が含まれていることを確認しなければならない(shall)。
テスト	評価者は、以下のテストを行わなければならない(shall)： テスト 1：評価者は、ガイダンス文書に記述されるように接続を設定し、通信が成功することを保証することによって、各 TOE コンポーネントとの各プロトコルを用いた通信が評価中にテスト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、分散 TOE コンポーネント間の通信チャネルのそれぞれについて、チャネルデータが平文で送信されないことを確証しなければならない(shall)。 テスト 3：評価者は、テスト 1 でテストされた各 TOE コンポーネントと関連付けられたプロトコルのそれぞれについて、接続が物理的に中断されるようにしなければならない(shall)。評価者は、物理的な接続性が回復された際、通信が適切に保護されていることを保証しなければならない(shall)。

B.1.4 FRU：資源の利用

B.1.4.1 FRU_RSA.1 最大割当て

FRU_RSA.1.1 TSF は、以下の資源の最大割当てを実施しなければならない(shall)： [*ネットワークトラフィックの検査をサポートする資源*] であって、 [サブジェクト] が [同時に] 利用可能であるもの。

適用上の注釈：*適合 TOE は、ネットワークトラフィックの検査をサポートするために用いられる枯渇性資源であって、『サブジェクト』(検査されるネットワークトラフィックフロー) が同時に利用可能であるものに対して割当てを課すこと。この要件の意図は、TOE のセンサインタフェース間のデータのフローが TOE の検査可能なトラフィック量を超える可能性があるように TOE が展開されないことを保証することである。検査されるべきデータのフロー(容量／スピード) が定義された割当てを超えた場合、TOE は超過した割当ての影響を示す警報を引き起こすべきである (should)。例えば、TOE がインラインに展開されている場合、割当ての超過は TSF にネットワークトラフィックの破棄 (転送ではなく) とネットワークトラフィック検査の失敗を引き起こすかもしれない。あるいは TOE がインラインに展開されていない場合、割当ての超過は検査なしにトラフィックが転送されることを引き起こすかもしれない。いずれの場合であっても、TSF が一部のネットワークトラフィックを検査できないかもしれないという意味で、最大割当ての超過は FAU_ARP に関連した「潜在的なセキュリティ違反」を引き起こす。*

監査対象事象	追加監査記録の内容
トラフィックフロー容量が最大割当てを超過した。	割当てを超過した TOE インタフェースの識別情報。

アクティビティ	保証アクティビティ
TSS	評価者は TSS を検査して、割当てメカニズムを介してコントロールされるすべての資源が特定されていることと、このリストにトラフィック検査をサポートするために利用される資源が含まれていることを保証しなければならない (shall)。評価者は、資源のそれぞれが「利用された」と計測される方法と、割当てまたは利用量の最大値が判断される方法、そして割当てに到達した際に取られるアクションが、TSS に記述されていることを保証しなければならない (shall)。
AGD	評価者は操作ガイダンスを検査して、割当てを規定するための指示 (割当てが設定可能な場合) が含まれ、また割当てへの到達に対応して管理者が取ることのできる、または取るべき (should) 任意のアクションが記述されていることを判断しなければならない (shall)。
テスト	テスト 1 : 評価者は操作ガイダンスに従って、資源の割当てを設定する (そのような機能が提供されている場合)。次に評価者は資源を割当てへ到達させ、TSS に規定されたアクションが発生することを確認する。

B.1.5 IPS：侵入防止

TOE がネットワークパケットの正規化の実装をサポートする場合には、以下の要件を ST へ含めることができる。

B.1.5.1 IPS_SBD_EXT.2 トラフィックの正規化

IPS_SBD_EXT.2.1 : TSF は、以下の手段によってカプセル化されたパケットの検査ができなければならない (shall) :

- [選択 : GRE、IP-in-IP、IPv4-in-IPv6、MPLS、PPTP、 [*割付 : その他のカプセル化手法*]、その他の手法なし]

アクティビティ	保証アクティビティ
TSS	評価者は、要件に定義されるトンネル内部のトラフィクを TOE が検査できる方法が、TSS に記述されていることを検証しなければならない (shall)。
AGD	評価者は操作ガイダンスを検査して、要件に特定されるカプセル化手法によってトンネリングされたパケットを検査するための指示が含まれることを判断しなければならない (shall)。
テスト	テスト 1 : 評価者は、要件に定義されるトンネル内で、以前のシグネチャベースのテストを再実行しなければならない (shall)。

IPS_SBD_EXT.2.2 : TSF は、IP 正規化を行ってフラグメント化されたパケットを検査のために再構成できるとともに、以下を行えなければならない (shall) : [選択 :

- プロミスキャスインタフェースにおいて収集されたデータについて : パケットが再構成できない場合に警告を生成する ;
- インラインインタフェースにおいて収集されたデータについて : いかなるパケットフラグメントも転送せず、また TSF がパケット全体を再構成できない場合には警告を生成する]。

アクティビティ	保証アクティビティ
TSS	評価者は、パケットがフラグメント化の後に再構成できない際に監査記録が生成される方法が TSS に記述されていることを検証しなければならない (shall)。また、インラインモードについては、評価者は TSS を検査してパケットが破棄されることを保証しなければならない (shall)。

アクティビティ	保証アクティビティ
AGD	この SFR には、操作ガイダンス保証アクティビティは存在しない。
テスト	評価者は、以下のテストを行わなければならない (shall) : テスト 1 : 評価者は、フラグメント化の後に再構成不可能なパケットを生成しなければならない (shall) ; 評価者は、IP 正規化のすべてのインスタンスについて監査事象が生成されることを保証しなければならない(shall)。 テスト 2 : インラインモードについて : 評価者は、パケットがフラグメント化の後に再構成できない際の自動的パケット拒否についてテストしなければならない(shall)。評価者はパケットキャプチャを利用して、IP トラフィクが TOE によって検出され、パケットが破棄されることを保証しなければならない(shall)。 テスト 3 : 評価者は、フラグメント化の後に再構成可能なパケットを生成しなければならない (shall) ; 評価者は、IP 正規化のすべてのインスタンスについて監査事象が生成されることを保証しなければならない(shall)。

IPS_SBD_EXT.2.3 : TSF は、TOE がインラインモードで展開されている場合に TOE を通過するトラフィクフローに対して TCP 正規化を行えるとともに、以下の転送を禁止できなければならない(shall) : [選択 :

- 重複するパケット ;
- 変更されたパケット ;
- シーケンス番号が連続していないパケット ;
- [選択 : [*割付 : 転送されるべきでない (should not) その他のパケット種別*]、その他のパケットなし]]

アクティビティ	保証アクティビティ
TSS	評価者は、以下の正規化に対してパケットが自動的に破棄されることが TSS に記述されていることを検証しなければならない(shall) : ● 重複するパケット ● 変更されたパケット ● シーケンス番号が連続していないパケット ● 要件中に定義される任意のその他の手法。
AGD	この SFR には、操作ガイダンス保証アクティビティは存在しない。
テスト	テスト 1 : 評価者は、以下の種類のパケットを生成し、そのパケットが破棄されることを確認しなければならない(shall) : ● 重複するパケット ● 変更されたパケット ● シーケンス番号が連続していないパケット ● 要件で定義された任意のその他の手法。

附属書C： 選択ベースの要件

本 EP の序説で示したように、ベースライン要件 (TOE またはその下位プラットフォームによって行われなければならない(must)もの) は、本 EP の本体に含まれる。これ以外にも EP の本体中の選択に基づく追加の要件が存在し、特定の選択がなされた場合には、以下の追加の要件が含まれる必要がある。

C.1 要件

選択ベースのセキュリティ機能要件は、以下のセクションに述べる。

C.1.1 FCS：暗号サポート

本 EP には、ND cPP または FW cPP によってすでに定義されたもの以外に、いかなる新規の選択ベースの要件も定義されない。しかし、FPT_ITT.1 で選択されたセキュアな通信プロトコルのそれぞれについて、適合 ST には ND cPP または FW cPP で定義された 1 つ以上の選択されたプロトコルに対応する選択ベースの要件が含まれなければならない(shall)ことに留意されたい。ST 作成者は、これらの要件のどれが、ベース PP に定義される高信頼チャネル／パスの機能ではなく、TSF 間高信頼通信に適用されるのかについて、明確に識別しなければならない(shall)。

附属書D： オブジェクティブ要件

本 EP の序説で示したように、ベースライン要件 (TOE またはその下位プラットフォームによって行われなければならない(must)もの) は本 EP の本体に含まれる。これ以外にも望ましいセキュリティ機能を規定する追加の要件が存在し、これらの要件はこの附属書に含まれる。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ことが期待される。

D.1 要件

オブジェクティブなセキュリティ機能要件は、以下のセクションで述べる。

D.1.1 FAU：セキュリティ監査

「IPS データ」という用語には、ネットワークトラフィクから抽出され TOE 上に保存されるデータ；TOE によって行われた分析の結果；及びその分析への TOE の対抗措置を示すメッセージのすべてが含まれる。この「IPS データ」の定義からはベース PP に関連する「監査データ」が除外される。除外されるデータには、管理者の認証、そして高信頼チャネルの確立／終了など、ベース PP の FAU_GEN に定義されるデータが含まれる。IPS データのレビューまたはストレージあるいはその両方やセキュリティ警報が TOE によってサポートされる場合には、以下の監査要件を適宜 ST に含めることができる。

D.1.1.1 FAU_ARP.1 セキュリティ警報

FAU_ARP.1.1 TSF は、セキュリティ侵害の可能性が検出された場合、[割付: アクションのリスト]を実行しなければならない (shall)。

適用上の注釈：*CC パート 2 において、FAU_ARP は FAU_SAA に依存して SFR の潜在的な違反を定義することが意図されている。FAU_SAA は、本 IPS EP には含まれず、その代わりに FRU_RSA が FAU_ARP に関連した「潜在的なセキュリティ違反」を定義するために用いられる。これは TOE がすべてのネットワークトラフィクを検査する能力を超えるネットワークトラフィクのスパイクを経験することであり、その事象によってネットワークトラフィクが破棄されたり検査されずに通過したりすることである。この SFR は、IPS TOE が取り得るアクションを定義するために用いられるべきであり(should)、これにはリモート監査サーバへセキュアに送信されなければならない(must) 監査証跡の一部ではない、1 つ以上のメッセージの生成が含まれてもよい。この SFR によって定義されるメッセージ送信アクションであって特に FAU_GEN.1/IPS と関係しないものは、通過中に暗号化される必要はない。この機能の主要な意図は通知のスピードであり、通過中のデータの完全性や機密性ではない。大部分の場合、FAU_STG_EXT.1 に該当する監査証跡は syslog データとなり、リモートに保存される監査データの完全性を保証するため通過中に保護されている。この SFR は、SNMP (トラップ) や SMTP (電子メール) などのプロトコルを介した単一の事象に関連したメッセージの送信をカバーすることを意図している。高信頼チャネル内での SNMP トラップ、SMTP 電子メール、あるいはその他の種類のメッセージ送信のセキュア化を (FTP_ITC.1 に定義されるように) サポートする TOE においては、ST 作成者はこれらのメッセージ送信手法を FTP_ITC.1 内またはこの SFR 内あるいはその両方で列挙することを選択できる。FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

アクティビティ	保証アクティビティ
TSS	評価者は、要件に規定される警報の記述が TSS に含まれることを検証しなければならない(shall)。また評価者は、監査データがセキュリティ警報インタフェースを介して送信できないことが TSS に言明されていることも検証しなければならない(shall)。
AGD	評価者は、FRU_RSA.1 に該当する場合に要件に規定される警報を有効化する方法がガイダンスに説明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、定義されたアクションを介して単一の事象に関係

アクティビティ	保証アクティビティ
	するメッセージの送信を論証するテストを考案しなければならない(shall)。このアクティビティは、IPS_ABD_EXT.1、IPS_SBD_EXT.1、及び FRU_RSA.1 のテスト保証アクティビティの組み合わせと共に対応できることに留意されたい。

D.1.1.2 FAU_SAR.1 監査レビュー (IPS データ)

FAU_SAR.1.1 詳細化：TSF は、[正当な管理者] が、~~監査記録~~**IPS 事象**から [*IPS データ*] を読み出せるようにしなければならない(shall)。

FAU_SAR.1.2 詳細化：TSF は、~~利用者~~**管理者に対し、**その情報を解釈するのに適した形式で~~監査記録~~**IPS データ**を提供しなければならない(shall)。

適用上の注釈：*検索やソーティングを可能とするグラフィカルな利用者インタフェースを TOE が提供することは予期されるが、要求はされない。また、そのような出力が同種の事象をグループ化して IPS データの管理レビューが容易に行えるようにすることは受容可能であろう。例えば、表示は事象種別や送信元 IP アドレスによるグループ化が可能で、以下の表サンプルに示すように、ある時間間隔内に発生した複数の事象が同一線上に表示されるかもしれない。そのようなビューが提供されるかどうかにかかわらず、個別事象発生の詳細を管理者が閲覧できることが期待される。FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

表 D-1：事象表 (いくつかの例が挿入されている)

時刻／日付	事象種別	対抗措置	事象の総数
2013-01-1 10:45:00	10.1.2.3 からのポートスキャン	10.1.2.3 からのトラフィックをすべてブロック	34

アクティビティ	保証アクティビティ
TSS	評価者は TSS を検査して、IPS 事象から IPS データを閲覧する管理者の能力、この IPS データが表示されるフォーマット、及び管理者にこのデータの閲覧が認可される方法が、記述されていることを検証しなければならない(shall)。
AGD	評価者は操作ガイダンスを検査して、TOE の管理インタフェースを用いて IPS 事象をアクセスし解釈する方法に関する指示が提供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、IPS データ (FAU_GEN に定義されるように生成された) が TOE の管理インタフェースから正当な管理者によって解釈可能であることを論証するテストを考案しなければならない(shall)。

D.1.1.3 FAU_SAR.2 限定監査レビュー (IPS データ)

FAU_SAR.2.1 詳細化：TSF は、明示的な読み出しアクセスを承認された**管理者**を除き、すべての~~利用者~~**管理者**に~~監査記録~~ **IPS データ**への読み出しアクセスを禁止しなければならない(shall)。

適用上の注釈：*FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

保証アクティビティ
IPS データの閲覧には管理役割が必要とされるため、FMT_MTD.1/IPS の保証アクティビティにおいて評価者が行う分析によって、この要件が満たされていることが論証されることになる。

D.1.1.4　FAU_SAR.3 選択可能監査レビュー (IPS データ)

FAU_SAR.3.1 詳細化：TSF は、[*フィルタリングパラメタ：リスクの格付け、時間間隔、送信元 IP アドレス、宛先 IP アドレス及び* [選択： [割付：*その他のフィルタリングパラメタ*]；*その他のフィルタリングパラメタなし*]；*及びソーティングパラメタ：事象 ID、事象種別、時間、シグネチャ ID、行われた IPS アクション、及び* [*選択：[割付：その他のソーティングパラメタ；その他のソーティングパラメタなし*]] に基づいて~~監査~~ **IPS データ**の[*フィルタリング及びソーティング*] を適用する能力を提供しなければならない(shall)。

適用上の注釈：*FAU_GEN.1/IPS に含まれる必要のある追加の監査対象 IPS 事象は存在しない。*

アクティビティ	保証アクティビティ
TSS	評価者は、要件に列挙されるパラメタを用いて IPS データのフィルタリング及びソーティングを適用する能力を TOE が有している方法の記述が TSS に含まれることを検証しなければならない(shall)。
AGD	評価者は管理ガイダンスをレビューして、ガイダンスにすべての事象種別が列挙されていることと、要件に従って選択可能であるべきすべての属性が、割付中に列挙された属性を含めて、記述されていることを保証しなければならない(shall)。また管理ガイダンスには、事前選択を設定する方法に関する指示が含まれると共に、(存在するならば) 複数値の事前選択のための構文が説明されなければならない(shall)。また管理ガイダンスには、その時点で強制されている選択基準に関わらず、常に記録される監査記録も特定されなければならない(shall)。
テスト	評価者は、以下のテストを行わなければならない(shall)： テスト 1：要件に列挙される属性のそれぞれについて、管理者はその属性の選択によってその属性を持つ監査事象 (または、管理ガイダンスに特定される、常に記録される監査事象) のみが記録されることを示すテストを考案しなければならない(shall)。 テスト 2 [条件付き]：TSF がさらに複雑な監査の事前選択基準 (例、複数の属性、属性を用いた論理式) をサポートする場合、評価者はこの機能が正しく実装されていることを示すテストを考案しなければならない(shall)。また評価者は、テスト計画書中に、そのテストのセットが典型的なものであり、その機能を行使するのに十分であることを正当化する短い説明文を提供しなければならない(shall)。

附属書E： 定義

E.1 攻撃の定義

タイトル	説明
DoS	サービス拒否
フラッディング Flooding	IP サブネット上に、または特定の IP アドレスを目標として、過大な量のトラフィクを発生させること。
IP Impossible パケット (Land)	送信元と宛先が同じアドレスであることが検知された IP パケット (Land 攻撃)。
IP オプション 有害オプションリスト IP Options Bad Option List	IP データグラムヘッダ中の IP オプションのリストが不完全または許可されない IP データグラム。
IP オプション パケットルート記録 Record Packet Route	データグラムの IP オプションリストにオプション 7 (Record Packet Route) を含む IP データグラム。
IP オプション タイムスタンプ Timestamp	データグラムの IP オプションリストにオプション 4 (Timestamp) を含む IP データグラム。
IP オプション セキュリティ Security	データグラムの IP オプションリストにオプション 2 (Security options) を含む IP データグラム。
IP オプション ルーズソースルート Loose Source Route	データグラムの IP オプションリストにオプション 3 (Loose Source Route) を含む IP データグラム。
IP オプション ストリクトソースルート Strict Source Route	データグラムの IP オプションリストにオプション 2 (Strict Source Routing) を含む IP データグラム。
IP フラグメント重複 (Teardrop, Bonk)	同一の IP データグラムに含まれる 2 つのフラグメントが、データグラムの一部を共有するようなオフセットを持っている。これは、フラグメント A がフラグメント B によって完全に上書きされたり、あるいはフラグメント A がフラグメント B によって部分的に上書きされたりすることを意味する可能性がある。
ICMP フラグメント (Ping of Death, Nuke)	IP ヘッダのプロトコルフィールドが 1 (ICMP) に設定され、Last Fragment ビットがセットされ、そして (IP offset * 8) + (IP data length) > 65535 であるような IP データグラム。IP offset (元のパケット内のこのフラグメントの開始位置を、8 バイトを単位として表現する) とパケットの残りを合わせると、IP パケットの最大サイズよりも大きくなる。
ICMP フラッディング (Smurf, ping flood)	パケット中の宛先 IP アドレスが宛先サブネットのブロードキャストアドレスであるため、そのサブネット上のすべてのマシンがブロードキャストに応答する。
スキャン (IP プロトコル、TCP ポート、UDP ポート)	期待される応答を発生させるようなトラフィクを送信することによって、特定の IP プロトコル番号、TCP ポート、あるいは UDP ポート上で待ち受けているサービスが存在するかどうかを判断しようとすること。
TCP FIN のみのフラグ	孤立した TCP FIN パケットが、特権ポート (1024 未満のポート番号) へ送信される。
TCP フラッド (SYN Flood)	標的ホストの中途半端にオープンした TCP セション数の制約を使い果たさせるため、SYN フラグがセットされた過大な数の TCP パケットを送信すること。
TCP NULL フラグ	SYN、FIN、ACK、あるいは RST フラグのいずれもセットされていない TCP パケットが、特定のホストへ送信される。
TCP SYN+FIN フラグ	SYN フラグと FIN フラグがセットされた TCP パケット。
UDP Bomb 攻撃	指定された UDP 長が指定された IP 長よりも短い。このような許可されない種類のパケットは、サービス拒否の試みと関連付けられる。
UDP Chargen DoS 攻撃	送信元ポートが 7 で宛先ポートが 19 の UDP パケットが検出されること。

E.2 用語と略語の定義

タイトル	説明
異常 (ネットワークトラフィク) Anomaly / Anomalous (network traffic)	定義されたベースラインに合致しないトラフィク、したがって予期されない、または非典型的なトラフィク。異常なトラフィクは必ずしも危険ではなく、また必ずしも監視対象ネットワークへの何らかの脅威を示すものではない。
ベースライン (ネットワークトラフィク) Baseline / Base-lining (network traffic)	監視対象ネットワーク上の予期される、または典型的なネットワークトラフィクとみなされるべきものを定義する。トラフィクベースラインは、ベースラインに合致するすべてのトラフィクが安全であることや、そのトラフィクが監視対象ネットワークへの潜在的な脅威とならないことを示すものではない。例えば：ベースラインに合致するトラフィクであっても、既知有害 IP アドレスに合致することがある；あるいは既知の脅威のシグネチャに合致することがある。
インラインモード Inline mode	TOE (または TOE コンポーネント) の展開であって、監視対象ネットワークのトラフィクが TOE を通して流れなければならない (must) ため、TOE にトラフィクをブロックする機会を提供するもの。
IPS	侵入防止システム (Intrusion Prevention System)
IPS ポリシー IPS policy	トラフィク分析、トラフィクのブロック、シグネチャ検出、または異常検出あるいはこれらの組み合わせ。多くの IPS ポリシーが TOE 上で定義され保存され得るが、IPS ポリシーは 1 つ以上の IPS インタフェースへ適用 (そのインタフェース上でアクティブに) されなければ何の効果も持たない。
(ネットワークトラフィクの) 正規化 Normalization (of network traffic)	有用なパケット／フラグメントのみが宛先への通過を許可されるような、ネットワークトラフィクのフィルタリング。正規化は、TOE がインラインモードで展開されている場合にのみ、TOE によって実施可能である。正規化には、重複パケット、再構成不可能なフラグメント、無効なチェックサムなど無効と判断されたパケット、シーケンス番号が連続していないパケットなどの、フィルタリングが含まれる可能性がある。
プロファイリング (ネットワークトラフィク) Profiling (network traffic)	ベースライン参照。
プロミスキャスモード Promiscuous mode	ネットワークインタフェースを待ち受けている (収集し検査している) IPS インタフェースの状態。プロミスキャスインタフェースは、トラフィクの待ち受けのみを行い送信を全く行わないものであってもよいし、あるいはインラインモードの展開と同様にそれを介して内向きと外向きの両方にトラフィクが流れるインタフェースであってもよい。
センサインタフェース Sensor interface	TOE の任意のインタフェースであって、IPS ポリシーがそれへ適用されているもの。