ISO/IEC 15408
Information Technology Security Evaluation

ヤマハポリシーフィルタリングモジュール
セキュリティターゲット

作成者： ヤマハ株式会社
日付： 2007/09/14
バージョン： 1.14

修正履歴

以下の表は、このドキュメントの修正履歴を示している。

ﾊﾞｰｼﾞｮﾝ	日付	作成者	コメント
1.0	2007/04/12	ヤマハ株式会社	・ 第 1.0 版作成
1.1	2007/04/16	ヤマハ株式会社	・ 非常用パスワードのデフォルト設定について修正した ・ ポリシーセット切り替えに関連する記述を削除した ・ 内部ネットワークリソースの記述を修正した ・ 識別･認証機能の説明を修正した
1.2	2007/04/23	ヤマハ株式会社	・ A.INTERNAL、OE.INTERNAL を追記した ・ FDP_IFF にてステートフルインスペクションの振る舞いを表現した ・ FIA_SOS を修正した
1.3	2007/04/26	ヤマハ株式会社	・ A.ENVIRONMENT、OE.ENVIRONMENT を修正した ・ LAN ポートのパケット処理の順番の説明を修正した ・ 役割の定義を修正した ・ 想定する攻撃者のレベルを修正した ・ A.CONFIG、OE.CONFIG を修正した ・ A.INTERNAL、OE.INTERNAL を削除した ・ FDP_IFF.1.3 の記述を修正した
1.4	2007/05/09	ヤマハ株式会社	・ ポリシーフィルターのログの例を修正した ・ 管理ユーザーの説明を修正した ・ 表 8-2 の誤植を修正した ・ ST 概要を修正した ・ OE.POLICY を追加した ・ A.ENVIRONMENT、OE.ENVIRONMENT を修正した ・ セキュリティ対策方針根拠を修正した ・ 不要な前提条件を削除した ・ 不要な機能要件を削除した ・ 情報資産の定義を修正した ・ 相互補完性の説明を修正した
1.5	2007/05/14	ヤマハ株式会社	・ 前提条件を追加した ・ FDP_IFF.1 の記述を修正した ・ FIA_UID.2 の記述を修正した ・ 機能要件の依存関係を修正した ・ 監査ログに関連する部分を修正した ・ FMT_MTD.1:4 を修正した ・ TOE セキュリティ機能根拠を修正した
1.6	2007/05/17	ヤマハ株式会社	・ 物理、論理構成図を修正した ・ OE.TIME を追加し、関連する部分を修正した ・ OE.ADMIN_USER の文言を修正した ・ FMT_MTD1:2 を修正し、関連する部分を修正した ・ 監査機能の起動と終了ログの文言を修正した ・ セキュリティ対策方針根拠を修正した ・ TOE セキュリティ機能要件根拠を修正した ・ FMT_MOF.1 を追加した ・ OE.ADMIN_USER の文言を修正した ・ O.I&A の説明を修正した ・ TOE 保証要件の妥当性を修正した
1.7	2007/05/18	ヤマハ株式会社	・ TOE セキュリティ機能要件根拠を修正した ・ TOE 要約仕様を修正した ・ TOE セキュリティ機能根拠を修正した

ﾊﾞｰｼﾞｮﾝ	日付	作成者	コメント
1.8	2007/06/14	ヤマハ株式会社	・ 保証手段ドキュメント名の変更
1.9	2007/07/05	ヤマハ株式会社	・ ST 概要の修正 ・ 非常用パスワードに関する記述の修正 ・ TOE のリビジョンの修正 ・ ログ例の誤植の修正 ・ TOE 要約仕様の修正
1.10	2007/07/11	ヤマハ株式会社	・ TOE 要約仕様の修正 ・ 前提条件、環境での対策、対応根拠の修正
1.11	2007/07/18	ヤマハ株式会社	・ 監査機能の起動と終了条件について修正
1.12	2007/07/19	ヤマハ株式会社	・ 監査機能の起動と終了条件について修正
1.13	2007/07/20	ヤマハ株式会社	・ 監査機能の起動と終了条件について修正
1.14	2007/09/14	ヤマハ株式会社	・ FIA_SOS に関する記述を削除した

目次

1. ST 概説

本章では、ST概説として、ST識別、ST概要、CC適合について記述する。

1.1. ST 識別

ST識別について、以下に記述する。

タイトル：	ヤマハポリシーフィルタリングモジュール セキュリティターゲット
バージョン：	1.14
TOE：	ヤマハポリシーフィルタリングモジュール
TOEのリビジョン：	1.02(2)
作成者：	ヤマハ株式会社
評価保証レベル：	EAL1
発行日：	2007/09/14
CCのバージョン：	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 （August 2005 CCIMB-2005-08-001） Part 2: Security functional requirements Version 2.3 （August 2005 CCIMB-2005-08-002） Part 3: Security assurance requirements Version 2.3 （August 2005 CCIMB-2005-08-003） Interpretations-0512
キーワード：	ファイアウォール、ルーター、フィルタリング

1.2. ST 概要

ST概要について、以下に示す。

本STは、TOEであるヤマハポリシーフィルタリングモジュール（以降、フィルタリングモジュールと呼ぶ）のセキュリティ仕様を記述した文書である。

TOEは、ステートフルインスペクション方式で通信パケットをフィルタリングする機能（ポリシーフィルターと呼ぶ）を持つファイアウォール製品である。TOEは、ヤマハのルーターに搭載されるファームウェアの一部として提供される。TOEの機能を実現するルーターには、少なくとも二つの（通信パケットを入出力することができる）LANポートと、一つの制御用のCONSOLEポートを備えている必要がある。このTOEはSRT100に搭載される。

SRTシリーズは、VPNやファイアウォール、QoSなどの機能を有したファイアウォールルーターである。

1.3. CC 適合の主張

本TOEは、下記のCCに適合している。

- CCパート2に適合する。
- CCパート3に適合する。
- パッケージ名として、EAL1に適合する。

1.4. 用語の定義

以降では、ISO15408関連の用語、及び本ST特有の用語について記述する。

1.4.1. ISO15408 関連の用語

表 1-1 ISO15408 関連の用語

項番	用語	説明
1.	CC	コモンクライテリア（Common Criteria）
2.	EAL	評価保証レベル（Evaluation Assurance Level）
3.	IT	情報技術（Information Technology）
4.	PP	プロテクションプロファイル（Protection Profile）
5.	SF	セキュリティ機能（Security Function）
6.	SFP	セキュリティ機能方針（Security Function Policy）
7.	SOF	機能強度（Strength of Function）
8.	ST	セキュリティターゲット（Security Target）
9.	TOE	評価対象（Target of Evaluation）
10.	TSC	TSF 制御範囲（TSF Scope of Control）
11.	TSF	TOE セキュリティ機能（TOE Security Functions）
12.	TSFI	TSF インターフェース（TSF Interface）
13.	TSP	TOE セキュリティ方針（TOE Security Policy）

1.4.2. 本 ST 特有の用語

表 1-2　本 ST 特有の用語

項番	用語	説明
1.	ルーター	ネットワーク上に流れるデータを他のネットワークにルーティング（経路選択）する機器、及びそのようなソフトウェアのことである。OSI 参照モデルでいうところの第 3 層（ネットワーク層）と第 4 層（トランスポート層）のプロトコルを解析し、転送処理を行う。ルーターが処理できないパケットや、管理ユーザーが遮断するよう設定したパケットがルーターに到着した場合、そのパケットを廃棄するなど、フィルタリング機能を持つものがほとんどである。
2.	フィルタリング	ルーターを通過するパケットやコネクションを解析し、IP アドレス、プロトコルやポート番号などの情報から、通過を許可したり、拒否したりするためのふるいにかける機能のことである。どのパケットを許可・拒否するかは、管理ユーザーが事前に設定をする。
3.	ファームウェア	ルーターのハードウェアに組み込まれたソフトウェアのことである。書き換え可能な不揮発性メモリにインストールされており、アップデートにより継続して機能拡張やバグフィックスの修正を行うことができる。本 TOE はルーターのファームウェア内の 1 機能として提供される。
4.	モジュール	１つの機能を実現するためのソフトウェアの集合のことである。
5.	GUI	Graphical User Interface の略称であり、マウスやポインティングデバイスなどを利用して視覚的に操作が行える直感型のインターフェースのことである。対称的に、CUI（Character-based User Interface）は、すべての操作をキーボードから文字を入力して行う記憶型のインターフェースである。
6.	ターミナルソフトウェア	端末として動作するアプリケーションのことであり、遠隔地に設置されたサーバやネットワーク機器を操作するために利用するものである。ターミナルソフトウェアは、端末エミュレータとも呼ばれ、Windows ではハイパーターミナル、Unix 系では GNOME 端末、kterm などがある。

項番	用語	説明
7.	入力遮断フィルター	ルーターに入力された不要なパケット（管理ユーザーが定義した通過を許可しないように設定したパケット）をいち早く破棄するために利用される機能のことである。つまり、ルーターの負担軽減のために利用されることを主に想定した機能である。 入力遮断フィルターは、ポリシーフィルターと機能は似ているが、ステートフルインスペクション方式のフィルタリングができないなど高度なフィルタリングを行うことはできない。入力遮断フィルターを利用せずにポリシーフィルターのみでフィルタリングを設定することも可能である。
8.	IDS	Intrusion Detection System の略称であり、ネットワーク上に流れるパケットを解析し、シグネチャマッチング（不正なパターンとのマッチングを行う）や異常検出（正常時のパケット以外のパケットを異常とみなす）などにより侵入検知を行う機能や機器のことである。SRT シリーズでの IDS は、シグネチャマッチングによる解析を行う。
9.	ステートフルインスペクション	TCP や UDP での通信のやり取り（状態）を保持しておき、正常なやり取りではない場合などに通信を遮断する機能のことである。 パケットのヘッダを解析してフィルタリングするダイナミックパケットフィルタリングに対して、パケットの情報の内容まで解析し、フィルタリングを行う。セキュリティ的にはパケットの偽装対策に効果がある。
10.	NAT	Network Address Translation の略称であり、内部ネットワークなどで利用するローカル IP アドレスをグローバル IP アドレスに変換する技術のことである。
11.	ポリシー	通信パケットの状態によって、通過・遮断を定義したもののことである。「LAN2 から LAN1 へ抜ける TELNET を破棄する 」、「LAN1 から LAN2 へ抜ける ping を許可する 」などのように、フィルター条件と動作を組み合わせて定義する。

項番	用語	説明
12.	ポリシーセット	ポリシーフィルターでの、ポリシーを適用される順に並べたもののことである。ポリシーは適用される順番に評価されていき、一致するポリシーの動作内容によって通過・遮断がされる。また、順番に評価され一つも一致するポリシーが無かった場合、その通信パケットは遮断される。ただし、フィルター条件が一つも設定されていない場合は、通信パケットは全て通過する。
13.	イーサネットフィルター	データリンク層でのフィルタリング機能のことである。データリンク層でのフィルタリングには、MAC アドレスを利用する。例えば、一致する MAC アドレス以外のホストからのアクセスを拒否するなどのように設定する。
14.	DCC	Dynamic Class Control の略称であり、クラスごとに優先度や帯域を割り当てて、クラス単位の使用帯域制御を行う（QoS）だけでなく、パソコンをはじめとするクライアント単位で使用帯域を監視する機能のことである。P2P ソフトウェアを使用している場合など、必要以上の帯域を使用しているクライアントのみの帯域を制限したり、通信を遮断したりするために利用する。
15.	コンソールコマンド	ルーターに直接コマンド（コンソールコマンド）を送って設定を行うコマンドのことである。コンソールコマンドは、TELNET、SSH、CONSOLE ポートに接続した PC からターミナルソフトウェアを利用してルーターへアクセスし、入力することができる。
16.	内部ネットワークと外部ネットワーク	ルーターを境界に、情報資産が存在する側を内部ネットワーク、そうではない側を外部ネットワークと呼ぶ。
17.	非常用パスワード	管理ユーザーがパスワードを忘れて TOE にアクセスできなくなった際に、非常用パスワードを利用して TOE にログインすることができる。CONSOLE ポートを経由したターミナルソフトウェアによるアクセスでのみ、非常用パスワードでのログインが可能である。非常用パスワード機能は管理ユーザーによって有効/無効が設定できる。デフォルト設定では、有効（利用できる）に設定されている。

2. TOE 記述

本章では、TOE記述として、TOEの製品種別、TOEのハードウェア要件及びTOEの物理的な範囲、TOEの論理的な範囲、TOEに関連する情報資産、役割の定義、TOEの機能、について記述する。

2.1. TOE の製品種別

ファイアウォール製品

2.2. TOE のハードウェア要件及び TOE の物理的な範囲

このTOEは、SRT100に搭載される。TOEの機能が適切に働くために必要なヤマハのルーターのハードウェア要件を説明する。

図 2-1 ～ 図 2-2 にSRT100の正面図及び背面図を示す。TOEのハードウェア要件として必須なものを“（必須）”として表す。つまり、LANポートとCONSOLEポートのみがTOEの要件としては必須であり、その他は（ルーターとしては必要ではあるが、TOEとしては）必須ではない。

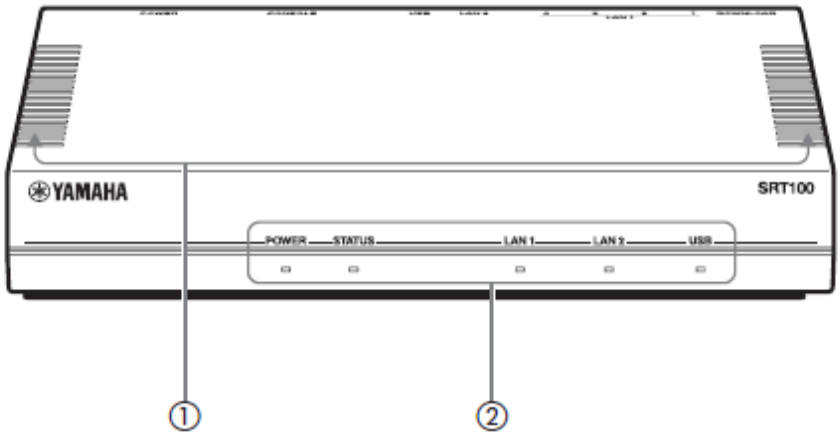


図 2-1 TOE のハードウェア要件（例、SRT100 の正面）

① 通風口

② ランプ

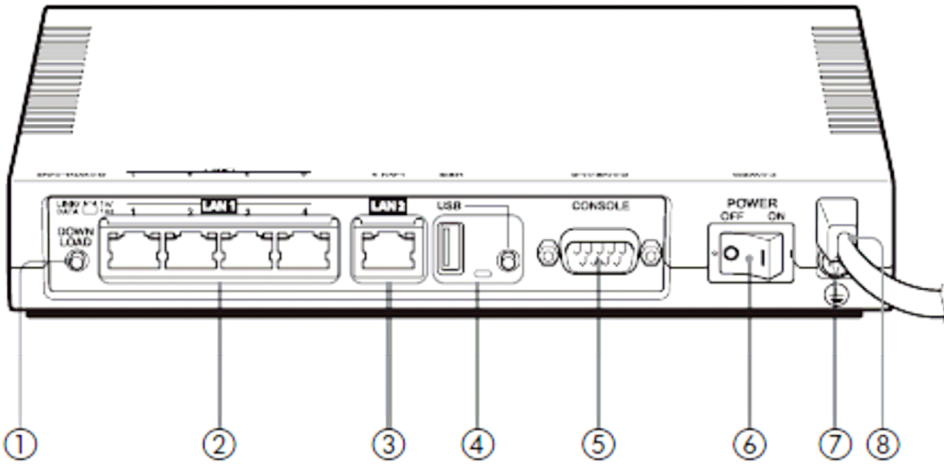


図 2-2　TOE のハードウェア要件（例、SRT100 の背面）

① DOWNLOADボタン
② LAN1ポート（必須）
③ LAN2ポート（必須）
④ USBポートとボタン
⑤ CONSOLEポート（必須）
⑥ POWERスイッチ
⑦ アース端子
⑧ 電源コード

図 2-3にTOEの物理的な範囲を示す。図中の実線はデータの流れを、破線は設定の適用の流れを表している。

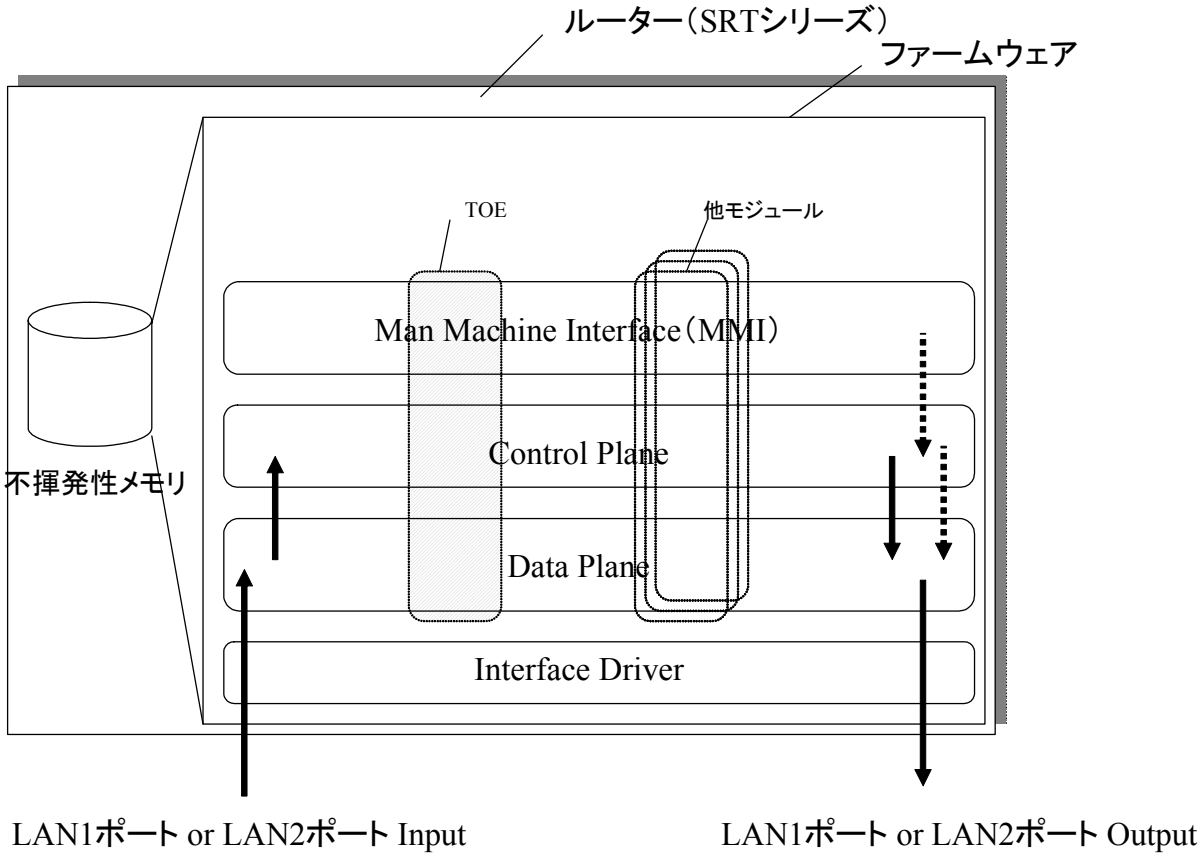


図 2-3 TOE の物理的な範囲

TOEの実装された機器は、内部に書き換え可能な記憶領域（不揮発性メモリ）を装備している。ファームウェアはこの不揮発性メモリに保存される。

ファームウェアは、（MMI、Control Plane、Data Plane、Interface Driver）4つの部分から構成されており、それぞれに役割がある。

Interface Driverは、LAN1ポートやLAN2ポート（通常は外部ネットワーク側のポートとなる）から入力された通信パケットを TOEや他のモジュールが解釈できるフォーマットに変換する役割である。また、TOEや他のモジュールによって処理された後はLAN1ポートやLAN2ポートへ出力される。

Data Planeは、Interface Driverから引き渡されたパケットの中身をチェックし、個々のパケットのフィルタリングやルーティングを行う役割である。この役割はTOEの実装された機器の中核の機能であり、高速に処理を行う必要がある。そのため、処理により時間を要する上位層の機能についてはここでは処理しない。例えば、TOEではステートフルインスペクション方式でフィルタリングの処理のみを行う（設定やステートフルインスペクションの状態保持はData Planeでは行わず、Control Planeにて行う）。

Control Planeは、Data Planeで処理する機能以外の動的経路制御プロトコルやVPN、バックアップ管理、その他の上位層の機能を持つ役割である。例えば、TOEはControl Planeでは、ステートフルインスペクションのコネクション状態を保持しており、通信パケットの状態との突合せを行う。ここではData Planeから引き渡されたデータに対してそれぞれの上位層の機能が処理を行う。

MMIは、TOEの実装された機器の設定を行う役割である。MMIで行われた設定は、Control PlaneとData Planeの設定にそれぞれ反映される。例えば、TOEでは、ポリシーフィルターの設定を行ったり、TOE管理のための識別・認証を行ったりする。

ファームウェア内の各モジュールは、（MMI、Control Plane、Data Plane）の3つの部分に縦断的に配置される。図 2-3での網掛けの部分が、TOE（ヤマハポリシーフィルタリングモジュール）である。

TOEの実装された機器の基本的な利用方法を以下に説明する。

1) 管理ユーザーは、CONSOLEポートを利用してTOEの実装された機器にアクセスする。
2) 管理ユーザーは、LAN1ポート、LAN2ポートの設定、フィルタリングの設定など、TOEの実装された機器の必要な設定を行う。
3) 管理ユーザーは、TOEの実装された機器を適切なネットワーク上に物理的に接続する。
4) TOEの実装された機器は、管理ユーザーの設定内容に基づいてTOEの実装された機器が設置されたネットワーク経路に流れるパケットの内容を判断し、フィルタリングなどの処理を行う。

2.3. TOE の論理的な範囲

図 2-4は、図 2-3を更に詳細化した図であり、TOEの論理的な範囲を示している。TOEの範囲は、図 2-4の中で網掛けがされた「ポリシーフィルター」とそれに関連する部分である。具体的には、「識別・認証機能」、「識別・認証管理機能」、「ポリシーフィルター」、「ポリシーフィルター設定」である。これらは総称して、ヤマハポリシーフィルタリングモジュールと呼ばれる。

「識別・認証機能」は、TOEの実装された機器の設定や設定の参照を行うために必ず通過しなければならない識別・認証機能である。識別・認証機能により認証されたユーザーは、ユーザーの属性値（administrator）によって、管理ユーザーへ昇格ができる。また、無操作状態で放置した場合、ユーザーの属性値（login-timer）の設定によって、自動的にTOEからログアウトされる。識別・認証されるユーザーは、「識別・認証管理機能」によりユーザーの追加、削除、属性値の変更がされる。

「ポリシーフィルター」は、通信パケットに付属するセキュリティ属性の値（表 2-2 参照）を判断に利用し、ステートフルインスペクション方式で通信パケットのフィルタリングを実現する機能である。この機能は、管理ユーザーにより「ポリシーフィルター設定」からフィルター条件が設定され、フィルター条件とマッチした通信パケットを通過、または遮断する。また、意図的にステートフルインスペクション方式でのフィルタリン

グをしたくない場合、“static-pass”という動作を設定することでステートフルインスペクション方式ではない通常のフィルタリングを行うことも可能である。ただし、フィルター条件が一つも設定されていない場合は、通信パケットは全て通過し、フィルター条件が一つでも設定されており、どの条件にもマッチしない場合は、遮断される。

TOEの機能の詳細については、2.6章を参照。

図 2-4について以下に説明する。図 2-4の実線矢印は、処理の流れを表しており、破線は設定の流れを表している。

- TOEの実装された機器は、サーバルームや施錠可能なスペースなどのシステム管理者以外触れない場所に設置される。
- TOEの実装された機器は、複数の接続ポート（SRT100の場合は、LAN1ポート、LAN2ポート、USBポート、CONSOLEポート、の4つのポート）を備えている。
  - LAN1ポート及びLAN2ポートは、図 2-4での「LAN1ポート or LAN2ポート Input」又は「LAN1ポート or LAN2ポート Output」のことであり、ネットワーク上のパケットをTOEの実装された機器に入力及び出力するポートである。ここで入力されたパケットは、フィルタリングやVPNなどの処理が行われる。また、LAN1ポート、LAN2ポートは、パケットの進行方向によってそれぞれがInput、Outputになりえる。例えば、LAN1ポートからパケットが入力される場合はLAN1ポートがInputになり、LAN2ポートがOutputになる。
  - CONSOLEポートは、図 2-4での「CONSOLEポート」のことであり、PCのRS-232C端子と接続することで、以下の操作が行える。
    - TOEの実装された機器の設定をする
    - TOEの実装された機器の設定ファイルを切り替える
    - TOEの実装された機器の設定を初期化する
- LAN1ポート又はLAN2ポートから入力されたパケットは、以下の順番にて処理される。
  - 管理機能に関するパケットの場合

    １）Interface Driverにて、TOEの実装された機器に入力されたパケットをTOEの実装された機器が解釈できるフォーマットに変換した後、「イーサネットフィルター」に引き渡す。

    ２）「イーサネットフィルター」にて、データリンク層でのフィルタリングを実施し、通過が許可された場合は、「入力遮断フィルター」に引き渡す。

    ３）「入力遮断フィルター」にて、不要なパケットであれば破棄され、そうでなければ「IDS」に引き渡す。

    ４）「IDS」にて異常なパケットであれば破棄され、そうでなければ「NAT（In）」に引き渡す。

    ５）「NAT（In）」にて受信側のアドレス変換処理がされ、「Routing（FIB）」に引き渡す。

６）「Routing（FIB）」にて適切な宛先にルーティングされ、「ポリシーフィルター」に引き渡す。

７）「ポリシーフィルター」にて、ステートフルインスペクション方式でのフィルタリングを行った後、TOEの実装された機器宛のパケットであった場合、「識別・認証機能」に引き渡す。

８）「識別・認証機能」にて利用者（サブジェクト）に対して、識別及び認証を行う。「識別・認証機能」にて認証された利用者であった場合、TOE及びTOEの実装された機器の設定を行うことができる。

- パケット通信処理の場合

１）Interface Driverにて、TOEの実装された機器に入力されたパケットをTOEの実装された機器が解釈できるフォーマットに変換した後、「イーサネットフィルター」に引き渡す。

２）「イーサネットフィルター」にて、データリンク層でのフィルタリングを実施し、通過が許可された場合は、「入力遮断フィルター」に引き渡す。

３）「入力遮断フィルター」にて、不要なパケットであれば破棄され、そうでなければ「IDS」に引き渡す。

４）「IDS」にて異常なパケットであれば破棄され、そうでなければ「NAT（In）」に引き渡す。

５）「NAT（In）」にて受信側のアドレス変換処理がされ、「Routing（FIB）」に引き渡す。

６）「Routing（FIB）」にて適切な宛先にルーティングされ、「ポリシーフィルター」に引き渡す。

７）「ポリシーフィルター」にて、ステートフルインスペクション方式でのフィルタリングを行った後、TOEの実装された機器以外を宛先とするパケットであった場合、「NAT（Out）」に引き渡す。

８）「NAT（Out）」にて送信側のアドレス変換処理がされ、「DCC」に引き渡す。

９）「DCC」にてクラスごとに優先度や帯域割り当てが行われ、LAN1ポート又はLAN2ポートへ出力する。

- TOEの実装された機器で取得できるログはログ管理機能にて管理される。TOEの実装された機器の各機能は、ログ管理機能に対してログの出力を指示し、ログ管理機能によってTOEの実装された機器内の不揮発性メモリや、syslogに出力される。本TOEでは、以下のログが取得される（詳細は、2.6章参照）。
  - 「ポリシーフィルター」での、フィルタリング結果のログ。syslog noticeコマンドでonと設定している場合に取得される。
  - 「識別・認証機能」での、管理ユーザー及び一般ユーザーのログイン、ログアウト時のログ。syslog infoコマンドでonと設定している場合に取得される。

- 「ポリシーフィルター」、「識別･認証機能」の管理ログ。ポリシーを設定する際や、ユーザーを追加・変更・削除する際などのTOE上で入力した全てのコマンドがログとして取得される。syslog execute commandコマンドでonと設定している場合に取得される。

※ 本TOEでは、ログ管理機能を環境での対策としている

- TOEの実装された機器及びTOEの設定を行う場合、管理ユーザーは、LAN1ポート及びLAN2ポート、CONSOLEポート、からTOEの実装された機器にアクセスする。TOEの実装された機器にアクセスすると、識別・認証が行われ、管理ユーザーは、設定を参照・変更することができ、一般ユーザーは設定の参照のみ行うことができる。以下、それぞれの設定方法について説明する。
  - LAN1ポート及びLAN2ポートから設定する場合は、ターミナルソフトウェアを利用してCUI（SSH）から設定をする。
  - CONSOLEポートから設定する場合は、CONSOLEポートとPCのRS-232C端子とを接続した状態でターミナルソフトウェアを利用して設定する。
- 「ポリシーフィルター設定」にて設定された情報は、「ポリシーフィルター」の動作に反映される。

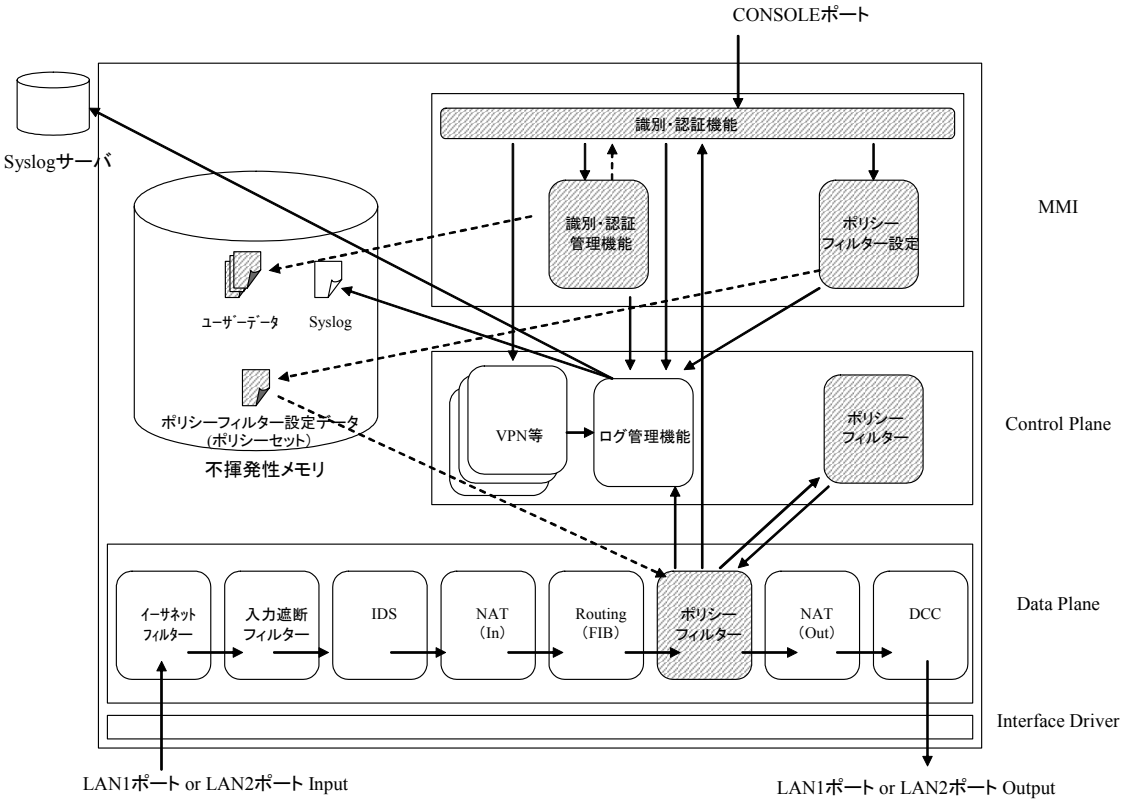


図 2-4 TOE の論理的な範囲

2.4. TOE に関連する情報資産

TOEに関連する情報資産（TSF data、User data）は、以下である。

（TSF data）

- ポリシーフィルター設定データ

  「ポリシーフィルター」のフィルター条件を定義した設定データ。

- ユーザーデータ

  TOE内のユーザーに関するデータ。主に以下がある。

表 2-1 ユーザーデータの説明

属性	説明	値
user	ユーザー識別名	ユーザー名
password	ユーザーのログインパスワード	32文字以内のASCII文字（大文字小文字は区別される）
administrator	administratorコマンドにより管理ユーザーに昇格することができる（on）かできない（off）かを決定するフラグ	On : administrator コマンドにより管理ユーザーに昇格することができる。またGUI の管理者ページへ接続することができる。 Off : administrator コマンドにより管理ユーザーに昇格することができない。またGUI の管理者ページへ接続することができない。
login-timer	無操作状態でログアウトするまでの時間 30～21474836（秒）の範囲、又はclear（ログアウトしない）で設定する	30..21474836、又はclear（ログアウトしない）

- 通信パケットのセキュリティ属性

  通信パケット毎に保持されるセキュリティ属性であり、以下がある。

表 2-2 通信パケットのセキュリティ属性

属性名	説明	値
source_interface	始点インターフェース	LAN インターフェース、PP インターフェース、TUNNEL インターフェース、ルーター自身[1]

[1] SSHクライアントからの応答を返す場合は、始点インターフェースがルーター自身となる

属性名	説明	値
dest_interface	終点インターフェース	LAN インターフェース、PP インターフェース、TUNNEL インターフェース、ルーター自身[2]
source_address	始点IPアドレス	IPアドレス
dest_address	終点IPアドレス	IPアドレス
service	サービス	アプリケーション名または、プロトコルとポート番号

（User data）

- 内部ネットワークリソース

  内部ネットワーク上に存在する組織の内部情報のうち、組織のポリシーで外部ネットワークから保護されるべきと特定された情報。組織のポリシーは、組織の責任者によって定められる。

2.5. 役割の定義

TOEに関連する役割を、以下に説明する。

（TOE内での役割）

- 管理ユーザー

  TOEの実装された機器の全ての設定の参照・変更やユーザーの管理を行うことができる役割である。TOE内で1アカウントのみ存在し、後述の一般ユーザーにてTOEの実装された機器にログインした後、管理ユーザーパスワードを入力することで管理ユーザー権限にて操作することができるようになる。ただし、非常用パスワードにてTOEへログインする際は、一般ユーザーを経由せずに、直接管理ユーザーとしてログインされる。

- 一般ユーザー

  TOEを管理するためにログインする全てのユーザーは、一般ユーザーとしてTOEに登録される。一般ユーザーは、設定内容や通信ログを参照することのみが行える、メンテナンス用の役割である。設定の変更はできない。

（組織としての役割）

- システム管理者

  組織のシステムやネットワークを管理する者である。管理ユーザーもシステム管理者に含まれる。

[2] ルーター自身に対するリクエストについては、終点インターフェースがルーター自身となる

2.6. TOE の機能

TOEの機能について以下に説明する。

2.6.1. 識別・認証機能

「識別・認証機能」は、TOEの実装された機器の設定や設定の参照を行うために必ず通過しなければならない識別・認証機能である。識別・認証機能により認証されたユーザーは、ユーザーの属性値（administrator）によって、管理ユーザーへ昇格ができる。また、無操作状態で放置した場合、ユーザーの属性値（login-timer）の設定によって、自動的にTOEからログアウトされる。識別・認証されるユーザーは、「識別・認証管理機能」によりユーザーの追加、削除、属性値の変更がされる。

TOEへのログイン手段は、SSH又はCONSOLEポートを利用した場合のみであり、TELNET及びHTTPなど、セキュアな通信が行えないログイン手段は、前提条件から利用しないようにしている。

管理ユーザーがパスワードを忘れてTOEにアクセスできなくなった際に、非常用パスワードを利用してTOEにログインすることができる。CONSOLEポートを経由したターミナルソフトウェアによるアクセスでのみ、非常用パスワードでのログインが可能である。非常用パスワード機能は管理ユーザーによって有効/無効が設定できる。デフォルト設定では、有効（利用できる）に設定されている。

「識別･認証機能」は、以下のログを取得する（ログ管理機能に出力する）ことができる。

- 識別・認証のログ

  管理ユーザー及び一般ユーザーのログイン、ログアウト時に取得されるログ。
  syslog infoコマンドでonと設定している際に取得される。（デフォルトon）

  ログの出力例を以下に示す。

一般ユーザーがログイン成功した場合：

2007/03/15 20:23:31: Login succeeded for *Serial*:[*IP アドレス*] *ユーザー名*

※ [IP アドレス]は、SSH 経由でアクセスした場合のみ取得される

一般ユーザーがログイン失敗した場合：

2007/03/15 20:27:21: Login failed for *Serial*

管理ユーザーがログイン成功した場合（administrator コマンド）：

2007/03/15 20:23:36: 'administrator' succeeded for *Serial* user: *ユーザー名*

管理ユーザーがログイン失敗した場合（administrator コマンド）：

2007/03/15 20:28:00: 'administrator' failed for *Serial* user: *ユーザー名*

一般ユーザーがログアウトした場合(exit コマンド、quit コマンド、あるいはタイマ満了時)：

2007/03/15 20:23:44: Logout from *Serial*: *ユーザー名*

※*斜体*は、状況により変化することを表している。

- 管理のログ

  ポリシーを設定する際や、ユーザーを追加・変更・削除する際などのTOE上で入力した全てのコマンドが記録として取得されるログ。
  syslog execute commandコマンドでonと設定している際に取得される。（デフォルトoff）

  ログの出力例を以下に示す。

YAMAHA（ユーザー名）が SSH 経由でユーザーを追加した場合：

2007/03/15 20:23:31: [MMI] Executed by SSH(YAMAHA): login user *user*

※*斜体*は、状況により変化することを表している。

2.6.2. ポリシーフィルター

「ポリシーフィルター」は、通信パケットに付属するセキュリティ属性の値（表 2-2 参照）を判断に利用し、ステートフルインスペクション方式で通信パケットのフィルタリングを実現する機能である。この機能は、管理ユーザーにより「ポリシーフィルター設定」からフィルター条件が設定され、フィルター条件とマッチした通信パケットを通過、または遮断する。通過の場合、パケットの宛先によって「識別・認証機能」や「NAT（Out）」に引き渡す。また、意図的にステートフルインスペクション方式を利用しない場合は、“static-pass”という動作を設定することで、ステートフルインスペクション方式ではない通常のフィルタリングを行うことも可能である。ただし、フィルター条件が一つも設定されていない場合は、通信パケットは全て通過し、フィルター条件が一つでも設定されており、どの条件にもマッチしない場合は、遮断される。

フィルター条件のことを、本STではポリシーと呼ぶ。ポリシーは、以下の項目を組み合わせ、作成される。

- source_interface
- dest_interface
- source_address
- dest_address
- service

ポリシーを複数組み合わせてフィルタリングのルールとして作成されたものは、ポリシーセットと呼ばれる。

ポリシーセットの作成例を以下に示す。

```
# ip policy filter 1 reject-log lan2 lan1 * * telnet
# ip policy filter 2 pass-log lan1 lan2 * * ping
# ip policy filter set 1 1,2
# ip policy filter set enable 1
```

通信パケットがポリシーとマッチした際のTOEの動作として、表 2-3の4通りが設定できる。TOE設定時のコマンドでは、表 2-3の4通りの動作ごとにログの取得の有無（ログ取得有：“-log”、ログ取得無：“-nolog”）を設定できる。例えば、通信パケットを通過させ、そのときのログを取得する場合は、“pass-log”と設定する。

表 2-3　通信パケットがポリシーとマッチした際の TOE の動作

項番	動作	説明
1.	pass	通信パケットを通過させる。TCP と UDP と ping については、 ステートフルインスペクション方式で通過させ、それ以外の通信パケットについては、そのまま通過させる
2.	static-pass	ステートフルインスペクション方式を使わずに通信パケットを通過させる
3.	reject	通信パケットを遮断する
4.	restrict	通信パケットを送信しようとするインターフェースが up しており、通信パケットを送信できる状態になっているならば通過させ、 そうでなければ通信パケットを遮断する。通信パケットを通過させる時には、TCP と UDP と ping については、 ステートフルインスペクション方式で通過させ、 それ以外の通信パケットについては、そのまま通過させる

「ポリシーフィルター」は、以下のログを取得する（ログ管理機能に出力する）ことができる。

- フィルタリング結果のログ

  ポリシーフィルターで通信パケットがフィルタリングされ、通過又は拒否された結果が記録として取得されるログ。
  syslog noticeコマンドでonと設定している際に取得される。（デフォルトoff）

  ログの出力例を以下に示す。

ポリシーに合致するコネクションやパケットが発生した場合：
2007/03/15 20:23:31: *Passed/Rejected/Restricted* at Policy Filter(*ポリシー番号*): *プロトコル パケットの情報*

※*斜体*は、状況により変化することを表している。

- 管理のログ

  ポリシーを設定する際や、ユーザーを追加・変更・削除する際などのTOE上で入力した全てのコマンドが記録として取得されるログ。
  syslog execute commandコマンドでonと設定している際に取得される。（デフォルトoff）

  ログの出力例を以下に示す。

YAMAHA（ユーザー名）が CONSOLE 経由でポリシーを設定した場合：

2007/03/15 20:23:31: [MMI] Executed by Serial(YAMAHA): ip policy filter 1 reject-log lan2 lan1 * * telnet

2007/03/15 20:23:31: [MMI] Executed by Serial(YAMAHA): ip policy filter 2 pass-log lan1 lan2 * * ping

2007/03/15 20:23:31: [MMI] Executed by Serial(YAMAHA): ip policy filter set 1 1 2

2007/03/15 20:23:31: [MMI] Executed by Serial(YAMAHA): ip policy filter set enable 1

※*斜体*は、状況により変化することを表している。

3. TOE セキュリティ環境

本章では、TOE を利用する上での前提条件、脅威、組織のセキュリティ方針について記述する。

まず、前提条件、脅威を検討する上で、TOE へ攻撃を行う者を「低レベルな攻撃者」と想定する。

3.1. 前提条件

以下に前提条件を示す。

A.ENVIRONMENT　システム管理者は、TOE の実装された機器、TOE に CONSOLE ポートで接続する管理端末、syslog サーバ、及びそれらを接続する管理用のネットワークを、システム管理者以外触れられない場所に設置する。

A.ADMIN_USER　システム管理者は、信頼でき、悪意を持った行動はしないものとする。

A.MANAGE　管理ユーザーは、以下の運用を行う。

- 必要最小限のユーザーを作成すること
- 一般ユーザー及び管理ユーザーのパスワードは 15 文字以上で設定すること
- login user コマンドは、パラメータにパスワードを指定しない形式で利用すること
- 設定した一般ユーザー及び管理ユーザーのパスワードが参照できないこと

A.CONFIG　管理ユーザーは、以下の設定を行う。

- ポリシーを最低 1 つ以上設定すること
- TOE を管理する際の一般ユーザー及び管理ユーザーの TOE への通信手段として、CONSOLE ポート又は SSH のみ利用できるように設定する（他の通信手段を利用できないようにする）こと
- TOE が動作する上で必要なポート（LAN ポート、CONSOLE ポート）以外は利用できないようにすること
- syslog execute command コマンドを on に設定すること
- syslog info コマンドを on に設定すること
- syslog notice コマンドを on に設定すること

A.BOUNDARY　　システム管理者は、内部ネットワークと外部ネットワークを接続する口は１つとし、その境界に TOE を設置する。

3.2. 脅威

以下に脅威を示す。

T.NET_FLOW　悪意ある者は、外部ネットワークからアクセスが許可されていない内部ネットワークリソースに対して不正にアクセスするかもしれない。

T.NOAUTH　　悪意ある者は、TOE の設定を不正に変更し、内部ネットワークリソースへの不正アクセスを試みるかもしれない。

3.3. 組織のセキュリティ方針

本 TOE において、組織のセキュリティ方針はない。

4. セキュリティ対策方針

本章では、TOE のセキュリティを確保する上で必要な、TOE のセキュリティ対策方針、環境のセキュリティ対策方針について記述する。

4.1. TOE のセキュリティ対策方針

以下に TOE のセキュリティ対策方針を示す。

O.NET_FLOW	TOE は、組織のポリシーに従って、通信パケットのヘッダ情報を利用した情報フロー制御を行わなければならない。
O.I&A	TOE は、(TOE の設定を変更する際など) TOE を管理する前に必ずユーザーを識別・認証しなければならない。
O.AUDIT	TOE は、TOE の機能の利用を記録する手段を、提供しなければならない。

4.2. 環境のセキュリティ対策方針

以下に環境のセキュリティ対策を示す。

OE.ENVIRONMENT	システム管理者は、TOE の実装された機器、TOE に CONSOLE ポートで接続する管理端末、syslog サーバ、及びそれらを接続する管理用のネットワークを、システム管理者以外触れられない場所に設置しなければならない。
OE.ADMIN_USER	組織の責任者は、セキュリティ意識が高く責任を持って管理ができる者をシステム管理者、管理ユーザーとして任命し、それらのセキュリティ意識のレベルを高く維持し続けるよう監督しなければならない。
OE.LOG_SIZING	管理ユーザーは、ログの出力先をログの保存のために必要十分なディスク容量が見積もられた syslog サーバに設定し、ディスク容量が満杯になる前に管理ユーザーにアラートを出したり、ディスクを自動的にローテーションするなどして、必要なログが消えてしまうことがないように運用しなければならない。

OE.MANAGE	管理ユーザーは、以下の運用を行わなければならない。 ・ 必要最小限のユーザーを作成する ・ 一般ユーザー及び管理ユーザーのパスワードは 15 文字以上で設定する ・ login user コマンドは、パラメータにパスワードを指定しない形式で利用する ・ 一般ユーザー及び管理ユーザーのパスワード設定時には参照できない形式で保存する設定にする
OE.CONFIG	管理ユーザーは、以下の設定を行わなければならない。 ・ ポリシーを最低 1 つ以上設定する ・ TOE を管理する際の一般ユーザー及び管理ユーザーの TOE への通信手段として、CONSOLE ポート又は SSH のみ利用できるように設定する（他の通信手段を利用できないようにする） ・ TOE が動作する上で必要なポート（LAN ポート、CONSOLE ポート）以外は利用できないようにする ・ syslog execute command コマンドを on に設定する ・ syslog info コマンドを on に設定する ・ syslog notice コマンドを on に設定する
OE.BOUNDARY	システム管理者は、内部ネットワークと外部ネットワークを接続する口は 1 つとし、その境界に TOE を設置しなければならない。
OE.POLICY	組織の責任者は、TOE により保護されるべき内部ネットワークリソースを特定し、組織のポリシーを定めなければならない。
OE.TIME	ログ管理機能は、TOE から出力されるログに付与される、信頼できる日付･時刻を提供しなければならない。

5. IT セキュリティ要件

本章では、TOE 又はその環境が満たしていなければならない TOE セキュリティ要件、IT 環境のセキュリティ要件について記述する。

5.1. TOE セキュリティ要件

以下では、TOEセキュリティ機能要件、TOEセキュリティ保証要件、最小機能強度（SOF）宣言について記述する。

5.1.1. TOE セキュリティ機能要件

TOEに必要な機能要件を、CC パート2より抜粋した結果を以下に記述する。

5.1.1.1. FAU_GEN.1 監査データ生成

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[**選択: 指定なし**]レベルのすべての監査対象事象; 及び

c) [**割付: 表 5-1の監査項目参照**]。

FAU_GEN.1.2 TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[**割付: 表 5-1の監査項目の追加の情報参照**]

依存性： FPT_STM.1

表 5-1 TOE における監査事象及び監査記録

機能要件	監査要件（CC の規定）	監査項目（TSF の実装）
FAU_GEN.1	なし	なし
FDP_IFC.1	なし	なし

機能要件	監査要件（CC の規定）	監査項目（TSF の実装）
FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセット(例えば、対象物のレベル低下の監査)。	ポリシーに合致するコネクションやパケットの発生の際に監査する （追加の情報）ポリシー番号、プロトコル、パケットの情報
FIA_UAU.2	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべての使用。	・ 一般ユーザー、管理ユーザーのログイン成功、失敗の際に監査する ・ 一般ユーザーがログアウトした時(exit コマンド、quit コマンド、あるいはタイマ満了時) （追加の情報）TOE へのアクセス手段
FIA_UAU.7	なし	なし
FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	・ 一般ユーザー、管理ユーザーのログイン成功、失敗の際に監査する ・ 一般ユーザーがログアウトした時(exit コマンド、quit コマンド、あるいはタイマ満了時) （追加の情報）TOE へのアクセス手段
FMT_MOF.1	a) 基本: TSF の機能のふるまいにおけるすべての改変。	監査機能の起動と終了の際に監査する （追加の情報）なし
FMT_MTD.1:1	a) 基本: TSF データの値のすべての改変。	ポリシーフィルター変更の際に監査する （追加の情報）なし
FMT_MTD.1:2	a) 基本: TSF データの値のすべての改変。	ユーザーの追加、変更、削除の際に監査する （追加の情報）なし
FMT_MTD.1:3	a) 基本: TSF データの値のすべての改変。	ポリシーフィルター設定情報の参照の際に監査する （追加の情報）なし

機能要件	監査要件（CC の規定）	監査項目（TSF の実装）
FMT_MTD.1:4	a) 基本: TSF データの値のすべての改変。	ユーザー情報の参照の際に監査する（追加の情報）なし
FMT_SMF.1	a) 最小：管理機能の使用	なし（監査が必要な事象無し）
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	なし（TOE には役割のグループが無いため）
FPT_RVM.1	なし	なし

5.1.1.2. FDP_IFC.1 サブセット情報フロー制御

FDP_IFC.1.1 TSFは、[割付: 以下のリスト]に対して[割付: ヤマハポリシーフィルタリングモジュール**SFP**]を実施しなければならない。

（サブジェクト）
ポリシーフィルターインターフェース

（情報）
外部ネットワークもしくは内部ネットワークから**TOE**に入力された通信パケット

（操作）
通過する、遮断される

依存性： FDP_IFF.1

5.1.1.3. FDP_IFF.1 単純セキュリティ属性

FDP_IFF.1.1 TSFは、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: ヤマハポリシーフィルタリングモジュール**SFP**]を実施しなければならない: [割付:以下のリスト]。

（サブジェクトのセキュリティ属性）
・なし

（情報のセキュリティ属性）
・source_interface
・dest_interface
・source_address
・dest_address
・service

FDP_IFF.1.2 TSFは、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: 通信パケットから得られた情報のセキュリティ属性と、ポリシー（フィルタリング条件）とのマッチングに

より評価し、ポリシーで通過が設定されている通信パケットの場合通過を許可する（それ以外の場合は遮断する）]。

FDP_IFF.1.3 TSFは、**[割付: FMT_MTD.1:1の管理ユーザーによって設定されたポリシーフィルター設定のうち、ステートフルインスペクションを利用したポリシーとして設定された通信の応答パケットのみ通過を許可する]**を実施しなければならない。

FDP_IFF.1.4 TSFは、以下の[**割付: 追加のSFP能力のリストは無い**]を提供しなければならない。

FDP_IFF.1.5 TSFは、以下の規則に基づいて、情報フローを明示的に承認しなければならない: [**割付: セキュリティ属性に基づいて、明示的に情報フローを承認する規則は無い**]

FDP_IFF.1.6 TSFは、次の規則に基づいて、情報フローを明示的に拒否しなければならない: [**割付: セキュリティ属性に基づいて、明示的に情報フローを拒否する規則は無い**]

依存性：FDP_IFC.1、FMT_MSA.3

5.1.1.4. FIA_UAU.2 アクション前の利用者認証

FIA_UAU.2.1 TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性：FIA_UID.1

5.1.1.5. FIA_UAU.7 保護された認証フィードバック

FIA_UAU.7.1 TSFは、認証を行っている間、[**割付: 画面には何も表示しない**]だけを利用者に提供しなければならない

依存性：FIA_UAU.1

5.1.1.6. FIA_UID.2 アクション前の利用者識別

FIA_UID.2.1 TSFは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性：なし

5.1.1.7. FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1.1 TSFは、機能[**割付: 監査機能**][**選択: を停止する、を動作させる**]能力を[**割付: 管理ユーザー**]に制限しなければならない。

依存性：FMT_SMF.1、FMT_SMR.1

5.1.1.8. FMT_MTD.1:1 TSF データの管理

FMT_MTD.1.1 TSFは、[**割付: ポリシーフィルター設定データ**]を[**選択: 改変**]する能力を[**割付:管理ユーザー**]に制限しなければならない。

依存性：FMT_SMF.1、FMT_SMR.1

5.1.1.9. FMT_MTD.1:2 TSF データの管理

FMT_MTD.1.1 TSFは、[割付: ユーザーデータ]を[選択: 改変、削除、その他の操作（追加）]する能力を[割付:管理ユーザー]に制限しなければならない。

補足：管理ユーザーは全てのユーザーのユーザーデータを変更することができるため、自身のパスワード及び全てのユーザーのパスワードを変更することができる。一般ユーザーは自身のユーザーデータ（パスワードを含む）を変更することができないため、変更する際は管理ユーザーに依頼する必要がある。

依存性：FMT_SMF.1、FMT_SMR.1

5.1.1.10. FMT_MTD.1:3 TSF データの管理

FMT_MTD.1.1 TSFは、[割付: ポリシーフィルター設定データ]を[選択: その他の操作（参照）]する能力を[割付:管理ユーザー、一般ユーザー]に制限しなければならない。

依存性：FMT_SMF.1、FMT_SMR.1

5.1.1.11. FMT_MTD.1:4 TSF データの管理

FMT_MTD.1.1 TSFは、[割付: ユーザーデータ]を[選択: その他の操作（参照）]する能力を[割付:管理ユーザー、一般ユーザー]に制限しなければならない。

補足：ただし、login userコマンドのパラメータにパスワードを指定した形式の場合、パスワードつきのコマンドの履歴がログとして残り一般ユーザーからも参照されるので、前提条件によりlogin userコマンドのパラメータにパスワードを指定した形式で利用しないよう制限する。

依存性：FMT_SMF.1、FMT_SMR.1

5.1.1.12. FMT_SMF.1 管理機能の特定

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：表 5-2のTSFによって提供されるセキュリティ管理機能参照]。

表 5-2 TSF によって提供されるセキュリティ管理機能

機能要件	管理要件（CC の規定）	管理項目（TSF の実装）
FAU_GEN.1	なし	なし
FDP_IFC.1	なし	なし
FDP_IFF.1	明示的なアクセスに基づく決定に	なし(TOE に入力される通信パケッ

機能要件	管理要件（CC の規定）	管理項目（TSF の実装）
	使われる属性の管理。	トの属性は管理しないため）
FIA_UAU.2	a）管理者による認証データの管理; b）このデータに関係する利用者による認証データの管理。	a）全てのユーザーのユーザーデータ（パスワード）の変更 b）なし（一般ユーザーは自身のパスワードを変更できないため）
FIA_UAU.7	なし	なし
FIA_UID.2	利用者識別情報の管理。	管理ユーザー及び一般ユーザーの追加、変更、削除
FMT_MOF.1	TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること;	なし（TOE には役割のグループが無いため）
FMT_MTD.1:1	TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること	なし（TOE には役割のグループが無いため）
FMT_MTD.1:2	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし（TOE には役割のグループが無いため）
FMT_MTD.1:3	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし（TOE には役割のグループが無いため）
FMT_MTD.1:4	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし（TOE には役割のグループが無いため）
FMT_SMF.1	なし	なし
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	ユーザーの管理（ユーザーデータを管理することと同義）
FPT_RVM.1	なし	なし

依存性：なし

5.1.1.13. FMT_SMR.1 セキュリティ役割

FMT_SMR.1.1 TSFは、役割[**割付：一般ユーザー、管理ユーザー**]を維持しなければならない。

FMT_SMR.1.2 TSFは、利用者を役割に関連づけなければならない。

依存性：FIA_UID.1

5.1.1.14. FPT_RVM.1 TSP の非バイパス性

FPT_RVM.1.1 TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性：なし

5.1.2. TOE セキュリティ保証要件

本TOEの保証レベルは、EAL1である。

5.1.3. 最小機能強度（SOF）宣言

本TOEの保証レベルは、EAL1であるため、AVA_SOF.1は含まれない。そのため、SOFを宣言する必要は無い。

5.2. IT 環境のセキュリティ要件

IT環境のセキュリティ要件は以下の通りである。

5.2.1.1. FPT_STM.1 高信頼タイムスタンプ（ログ管理機能）

FPT_STM.1.1 ログ管理機能は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性：なし

6. TOE 要約仕様

本章では、TOE セキュリティ機能、TOE セキュリティ機能と TOE セキュリティ機能要件との対応根拠、保証手段について記述する。

6.1. TOE セキュリティ機能

以下では、5.1.1章で記述したTOEセキュリティ機能要件を満たす、TOEセキュリティ機能について説明する。

6.1.1. SF.I&A（識別・認証機能）

本セキュリティ機能は、識別・認証に関するセキュリティ機能である。識別・認証に関する機能は、(1)ユーザーを識別・認証を実施する機能、(2)ユーザーを管理する機能、(3)識別・認証に関するログを取得する機能、に分類できる。

(1) ユーザーを識別・認証を実施する機能

TOEは、役割として管理ユーザーと一般ユーザーを区別して識別・認証する。全てのユーザーは、一般ユーザーとしてTOEに登録される必要があり、管理ユーザーとしてログインするためには、一旦一般ユーザーとしてTOEへログインし、更に管理ユーザーとしてログイン（昇格）する必要がある。ただし、非常用パスワードにてTOEへログインする際には、一般ユーザーを経由せず、直接管理ユーザーとしてログインされる。

一般ユーザー及び、管理ユーザーを識別・認証する認証メカニズムは、パスワード認証である。

パスワードを入力する際は、パスワードは画面には表示されず、盗み見られることは無い。

TOEを操作する前には、いかなるコンソールコマンドの実行も許されず、必ず識別・認証機能が働く。

(2) ユーザーを管理する機能

TOEのユーザーを管理する役割として、管理ユーザーと一般ユーザーが存在する。管理ユーザーは、ユーザーの追加、削除、属性値の改変、参照（パスワードは除く）を行うことができ、一般ユーザーは、ユーザーデータの参照のみ（パスワードは除く）行うことができる。よって、一般ユーザーは自身のパスワードを変更する際は、管理ユーザーに依頼する必要がある。

(3) 識別・認証に関するログを取得する機能

識別・認証機能は、ログ管理機能に対して以下の条件にて監査情報（ログ）を出力する。

- 一般ユーザー、管理ユーザーのログイン成功、失敗の際に監査する
  （追加の監査情報）TOEへのアクセス手段
- 一般ユーザーがログアウトした際に監査する(exitコマンド、quitコマンド、あるいはタイマ満了時)
  （追加の監査情報）TOEへのアクセス手段
- ユーザーの追加、変更、削除の際に監査する
  （追加の監査情報）なし
- ユーザー情報の参照の際に監査する
  （追加の監査情報）なし

取得されるログの監査情報は、「事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)、上記の追加の監査情報」である。日付・時刻は、ログ管理機能によりログ出力時に付与されるため、TOEは付与しない。

設定変更、参照他コマンド実行のログの出力は、syslog execute commandで設定できる。またinfoレベルのログは主にログインログアウトやコマンド実行などの情報である。この出力を行うか否かをsyslog infoコマンドで設定できる。

なお、識別・認証機能とポリシーフィルターのログ出力の起動と終了（監査の起動と終了）は、それぞれが独立して起動あるいは終了できるものではなく、同一の操作により行われる。監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。

ログの出力のON（監査の起動）：

- syslog execute command onかつ
- syslog info onかつ
- syslog notice on

ログ出力例：

2007/05/30 17:32:13: [MMI] Executed by Serial(user): syslog execute command on

2007/05/30 17:32:16: [MMI] Executed by Serial(user): syslog info on

2007/05/30 17:32:20: [MMI] Executed by Serial(user): syslog notice on

ログの出力のOFF（監査の終了）：

- syslog execute command offあるいは
- syslog info offあるいは
- syslog notice off

ログ出力例：

2007/05/30 17:30:55: [MMI] Executed by Serial(user): syslog info off

6.1.2. SF.POLICYFILTER（ポリシーフィルター）

本セキュリティ機能は、ポリシーフィルターに関するセキュリティ機能である。ポリシーフィルターに関する機能は、(1)ポリシーフィルターを設定する機能、(2)フィルタリングを実施する機能、(3)ポリシーフィルターに関するログを取得する機能、に分類できる。

(1) ポリシーフィルターを設定する機能

TOEのユーザーを管理する役割として、管理ユーザーと一般ユーザーが存在する。管理ユーザーは、フィルター条件（ポリシー及びポリシーセット）を参照・変更を行うことができ、一般ユーザーは、フィルター条件を参照のみ行うことができる。

ポリシーは、通信パケットの以下のセキュリティ属性値の条件を設定し、その条件にマッチした通信パケットの振る舞い（通過又は遮断）を設定する。

- source_interface
- dest_interface
- source_address
- dest_address
- service

IPアドレスにはIPv4とIPv6アドレスを指定できる。それぞれもセキュリティ属性は、それらの管理を容易にするためにグループ化して名前を付与することができる。

ポリシーを複数組み合わせてフィルタリングのルールとして作成する。ルールは階層構造をとることができ、最大4階層までの設定ができる。ポリシーを複数組み合わせたものは、ポリシーセットと呼ばれる。

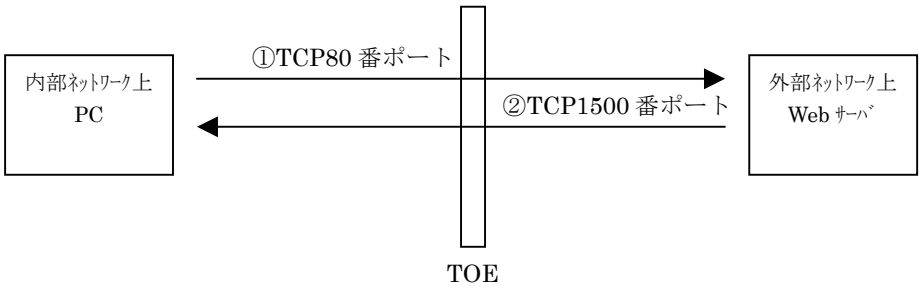
通信パケットがポリシーとマッチした際のTOEの動作として、表 6-1の4通りが設定できる。

表 6-1 通信パケットがポリシーとマッチした際の TOE の動作

項番	動作	説明
1.	pass	通信パケットを通過させる。TCP と UDP と ping については、 ステートフルインスペクション方式で通過させ、それ以外の通信パケットについては、そのまま通過させる
2.	static-pass	ステートフルインスペクション方式を使わずに通信パケットを通過させる
3.	reject	通信パケットを遮断する
4.	restrict	通信パケットを送信しようとするインターフェースが up しており、通信パケットを送信できる状態になっているならば通過させ、 そうでなければ通信パケットを遮断する。通信パケットを通過させる時には、TCP と UDP と ping については、 ステートフルインスペクション方式で通過させ、 それ以外の通信パケットについては、そのまま通過させる

(2) フィルタリングを実施する機能

TOEは、TOEに入力された全ての通信パケットのセキュリティ属性を確認し、ポリシーとのマッチングを行うことでステートフルインスペクション方式にてフィルタリングを行う（図 6-1参照）。また、ステートフルインスペクション方式での通過が許可される条件は表 6-2の通りである。



ポリシーフィルター設定を以下のように設定したと仮定する。
- 内部ネットワークから外部ネットワークへは全端末から HTTP（TCP80 番ポート）のみステートフルインスペクション方式で通過を許可する。
- 外部ネットワークから内部ネットワークへは全ての通信を遮断する。

内部ネットワーク上 PC から外部ネットワーク上 Web サーバへアクセスした際のフローは以下のようになる。
① 内部ネットワーク上 PC から外部ネットワーク上 Web サーバへ TCP80 番ポートでリクエストを送信する。
② TOE は、ステートフルインスペクション方式にて、①の応答であることを確認し、通過を許可する。
③ ・・・

つまり、通常は遮断されるはずである外部ネットワークからの通信が、内部ネットワークからのリクエストに対する適切な応答であった場合のみ通過が許可されるように、必要に応じて動的にポートが開閉する方式がステートフルインスペクション方式である。

図 6-1　ステートフルインスペクション方式の通信イメージ

表 6-2　ステートフルインスペクション方式で通過が許可される条件

項番	TCP*1 又は UDP*2	アプリケーション*3	アプリケーション固有の許可条件*4 （ポートを開く条件、ポートを閉じる条件）
1.	TCP	FTP（制御用のコネクション）	（ポートを開く条件）21 番ポート宛ての TCP コネクションが発生し、それに対する応答パケットを検知した場合
			（ポートを閉じる条件）そのコネクションに属するパケットが一定時間*5発生しないか、RST/FINを受信して一定時間*5経った場合
2.	TCP	FTP（データ転送用のコネクション）	（ポートを開く条件）あらかじめ制御用のコネクションにおける PORT/PASV/EPRT/EPSV コマンドでポート番号の交渉ができている場合
			（ポートを閉じる条件）制御用のコネクションと同様

項番	TCP*1 又は UDP*2	アプリケーション*3	アプリケーション固有の許可条件*4 （ポートを開く条件、ポートを閉じる条件）
3.	UDP	TFTP	（ポートを開く条件）TFTP コマンドの最初のパケットに対する応答 ACK パケットが来た場合
			（ポートを閉じる条件）データ部が短い(512 バイト未満)DATAパケットに対するACKパケットを受信した場合（一定時間*5を短縮させそのタイムアウトによって閉じる）
4.	UDP	DNS	（ポートを開く条件）問い合わせパケットに対する応答パケットが来た場合
			（ポートを閉じる条件）応答パケットが通過するかあるいは一定時間*5経過した場合
5.		PING	（ポートを開く条件）要求パケットに対して応答パケットが来た場合
			（ポートを閉じる条件）要求パケットが発生してから応答パケットが一定時間*5全くないか、あるいは応答パケットが一つでも通過してから一定時間経過した場合

*1 TCPでは、内部ネットワークから最初のパケットが発生して確立されたTCPコネクションのパケットについて、一定時間*5内に通信がある限り外部ネットワークから来たものの通過を許可（ポートを開く）する。またそのTCPコネクションでFINやRSTパケットが観測されると一定時間*5を短縮し、そのタイムアウトによってポートを閉じる。

*2 UDPでは、内部ネットワークから外部ネットワークへ通信が発生した場合に、外部ネットワークから内部ネットワークへの応答パケットの通過を許可（ポートを開く）する。該当ポートでパケットのやりとりが一定時間*5なければタイムアウトし、ポートを閉じる。

*3 ここで挙げた以外のアプリケーションは、そのアプリケーション固有の許可条件はなく、利用する TCP 及び UDP の処理のみ適用される。

*4 TCP、UDP とは別にアプリケーション固有の通過が許可される条件が適用される。

*5 一定時間は、ip policy filter timer コマンドでそれぞれ以下のように変更することができる。

オプション名	意味
tcp-syn-timeout	SYN を受けてから設定された時間内にデータが流れなければセッションを切断する
tcp-fin-timeout	FIN を受けてから設定された時間が経てばセッションを強制的に解放する
tcp-idle-time	設定された時間内に TCP セッションのデータが流れなければセッションを切断する

オプション名	意味
udp-idle-time	設定された時間内に UDP セッションのデータが 流れなければセッションを切断する
dns-timeout	DNS の query を受けてから設定された時間内に データが流れなければセッションを切断する
icmp-timeout	設定された時間内に ICMP セッションのデータが流れなければセッションを切断する（ping に適用される）

(3) ポリシーフィルターに関するログを取得する機能

ポリシーフィルターは、ログ管理機能に対して以下の条件にて監査情報（ログ）を出力する。

- ポリシーに合致するコネクションやパケットの発生の際に監査する
  （追加の監査情報）ポリシー番号、プロトコル、パケットの情報
- ポリシーフィルター変更の際に監査する
  （追加の監査情報）なし
- ポリシーフィルター設定情報の参照の際に監査する
  （追加の監査情報）なし

取得されるログの監査情報は、「事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)、上記の追加の監査情報」である。日付・時刻は、ログ管理機能によりログ出力時に付与されるため、TOEは付与しない。

設定変更、参照他コマンド実行のログ出力はsyslog execute commandで設定できる。またnoticeレベルのログは主にフィルタリングで処理されるパケットに関わる情報のログである。この出力を行うか否かをsyslog noticeコマンドで設定できる。

なお、識別・認証機能とポリシーフィルターのログ出力の起動と終了（監査の起動と終了）は、それぞれが独立して起動あるいは終了できるものではなく、同一の操作により行われる。監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。

ログの出力のON（監査の起動）：

- syslog execute command onかつ
- syslog info onかつ
- syslog notice on

ログ出力例：

2007/05/30 17:32:13: [MMI] Executed by Serial(user): syslog execute command on

2007/05/30 17:32:16: [MMI] Executed by Serial(user): syslog info on

2007/05/30 17:32:20: [MMI] Executed by Serial(user): syslog notice on

ログの出力のOFF（監査の終了）：

- syslog execute command offあるいは
- syslog info offあるいは
- syslog notice off

ログ出力例：

2007/05/30 17:32:46: [MMI] Executed by Serial(user): syslog notice off

2007/05/30 17:32:50: [MMI] Executed by Serial(user): syslog execute command off

6.2. TOE セキュリティ機能と機能要件との対応根拠

以下に、TOEセキュリティ機能と機能要件との対応根拠を示す。

表 6-3 IT セキュリティ機能 と機能要件との対応根拠

	SF.I&A	SF.POLICYFILTER
FAU_GEN.1	X	X
FDP_IFC.1		X
FDP_IFF.1		X
FIA_UAU.2	X	
FIA_UAU.7	X	
FIA_UID.2	X	
FMT_MOF.1	X	X
FMT_MTD.1:1		X
FMT_MTD.1:2	X	
FMT_MTD.1:3		X
FMT_MTD.1:4	X	
FMT_SMF.1	X	
FMT_SMR.1	X	
FPT_RVM.1	X	X

6.3. 保証手段

以下に5.1.2章で示したTOEセキュリティ保証要件を満たす保証手段を説明する。保証手段として提供される文書やTOEを示す。

表 6-4　保証要件と対応する保証手段

コンポーネント	保証手段
ACM_CAP.1	ヤマハポリシーフィルタリングモジュール構成管理計画書 ヤマハポリシーフィルタリングモジュール構成リスト
ADV_FSP.1	ヤマハポリシーフィルタリングモジュール機能仕様書
ADV_RCR.1	
ADO_IGS.1	お知らせ
AGD_ADM.1	コマンド設定運用説明書
AGD_USR.1	コマンドリファレンス
ATE.IND.1	-

7. PP 主張

本STが適合しているPPは無い。

8. 根拠

本章では、セキュリティ対策方針根拠、ITセキュリティ要件根拠、TOE要約仕様根拠、PP主張根拠について記述する。

8.1. セキュリティ対策方針根拠

以下では、前提条件・脅威・組織のセキュリティ方針とTOEのセキュリティ対策方針、環境のセキュリティ対策方針との対応根拠について記述する。表 8-1に対応関係を示す。表中の“X”が、対応を、“灰色のセル”は絶対対応しない箇所を意味する。

表 8-1 セキュリティ対策方針根拠

	O.NET_FLOW	O.I&A	O.AUDIT	OE.ENVIRONMENT	OE.ADMIN_USER	OE.MANAGE	OE.CONFIG	OE.LOG_SIZING	OE.BOUNDARY	OE.POLICY	OE.TIME
T.NET_FLOW	X		X					X		X	X
T.NOAUTH		X	X					X			X
A.ENVIRONMENT				X							
A.ADMIN_USER					X						
A.MANAGE						X					
A.CONFIG							X				
A.BOUNDARY									X		

T.NET_FLOWは、O.NET_FLOW、O.AUDIT、OE.LOG_SIZING、OE.POLICY、OE.TIMEによって対抗される。理由は以下の通りである。

a) 組織のポリシーに従ってフィルタリングされる（OE.POLICY、O.NET_FLOW）

組織の責任者がTOEにより保護されるべき内部ネットワークリソースを特定し、組織のポリシーを定め（OE.POLICY）、管理ユーザーにより組織のポリシーに従って通信パケットのヘッダ情報を利用したTOEによる情報フロー制御が行われるように設定し、TOEによりフィルタリングされるからである（O.NET_FLOW）。

b) ログが取得される（O.AUDIT、OE.LOG_SIZING、OE.TIME）

TOEのポリシーフィルターのフィルタリング結果のログ及びポリシーフィルターの管理ログが取得され（O.AUDIT）、ログに付与される信頼できる日付･時刻が、ログ管理機能により提供され（OE.TIME）、取得されたログはログがあふれて取得できない状態にならないよう管理ユーザーによりログの出力先をログの保存のために必要十分なディスク容量が見積もられたsyslogサーバに設定し、ディスク容量が満杯になる前に管理ユーザーにアラートを出したり、ディスクを自動的にローテーシ

ョンするなどして、必要なログが消えてしまうことがないように運用されるからである（OE.LOG_SIZING）。

T.NOAUTHは、O.I&A、O.AUDIT、OE.LOG_SIZING、OE.TIMEによって対抗される。理由は以下の通りである。

a) 確実に識別・認証される（O.I&A）

TOEの実装された機器、及びTOEの設定を参照・変更するためには、必ずTOEによりID・パスワードを利用して識別・認証されるからである。

b) ログが取得される（O.AUDIT、OE.LOG_SIZING、OE.TIME）

TOEの識別・認証の結果のログ及びユーザーの管理ログが取得され（O.AUDIT）、ログに付与される信頼できる日付･時刻が、ログ管理機能により提供され（OE.TIME）、取得されたログはログがあふれて取得できない状態にならないよう管理ユーザーによりログの出力先をログの保存のために必要十分なディスク容量が見積もられたsyslogサーバに設定し、ディスク容量が満杯になる前に管理ユーザーにアラートを出したり、ディスクを自動的にローテーションするなどして、必要なログが消えてしまうことがないように運用されるからである（OE.LOG_SIZING）。

A.ENVIRONMENTは、OE.ENVIRONMENTによって対抗される。理由は以下の通りである。

a) 物理的にセキュアな環境に設置される（OE.ENVIRONMENT）

システム管理者が、TOEの実装された機器、TOEにCONSOLEポートで接続する管理端末、Syslogサーバ、及びそれらを接続するネットワークを、システム管理者以外触れられない場所に設置するからである。

A.ADMIN_USERは、OE.ADMIN_USERによって対抗される。理由は以下の通りである。

a) システム管理者は信頼できる（OE.ADMIN_USER）

組織の責任者が、セキュリティ意識が高く責任を持って管理ができる者をシステム管理者、管理ユーザーとして任命し、それらのセキュリティ意識のレベルを高く維持し続けるよう監督するからである。

A.MANAGEは、OE.MANAGEによって対抗される。理由は以下の通りである。

a) TOEがセキュアに運用される（OE.MANAGE）

「必要最小限のユーザーを作成する」ことにより、脆弱なユーザーアカウントを残さないことにより、なりすましの利用を防ぐ。

「一般ユーザー及び管理ユーザーのパスワードは15文字以上で設定する」ことにより、脆弱なパスワードのユーザーアカウントが存在しないようにする。

「login userコマンドは、パラメータにパスワードを指定しない形式で利用する」ことにより、ログにパスワードの付いたコマンドの履歴が残らないようにする。

「一般ユーザー及び管理ユーザーのパスワード設定時には参照できない形式で保存する設定にする」ことにより、TOEの設定を表示するコマンドを実行した際に、一般ユーザー及び管理ユーザーのパスワードが平文で表示されることを防ぐ。

A.CONFIGは、OE.CONFIGによって対抗される。理由は以下の通りである。

a) TOEがセキュアに設定される（OE.CONFIG）

「ポリシーを最低1つ以上設定する」ことにより、ポリシーにマッチしない全ての通信パケットが遮断される。

「TOEを管理する際の一般ユーザー及び管理ユーザーのTOEへの通信手段として、CONSOLEポート又はSSHのみ利用できるように設定する（他の通信手段を利用できないようにする）」ことにより、管理ユーザー及び一般ユーザーとTOEとの通信を悪意ある者が盗聴することが困難になる。

「TOEが動作する上で必要なポート（LANポート、CONSOLEポート）以外は利用できないようにする」ことにより、管理ユーザーの意図しないTOEの使われ方をしてしまうことを防ぐ。

A.BOUNDARYは、OE.BOUNDARYによって対抗される。理由は以下の通りである。

a) 接続形態を制限する（OE.BOUNDARY）

システム管理者が、内部ネットワークと外部ネットワークを接続する口は1つとし、その境界にTOEを設置するからである。

8.2. IT セキュリティ要件根拠

以下では、TOEセキュリティ機能要件根拠、TOE保証要件の妥当性、IT環境に対するセキュリティ要件の根拠、ITセキュリティ機能要件依存性根拠、TOEセキュリティ機能要件相互補完性と内部一貫性、について記述する。

8.2.1. 最小機能強度レベルの適合性

本TOEの保証レベルは、EAL1であるため、AVA_SOF.1は含まれない。そのため、最小機能強度レベルの適合性を説明する必要は無い。

8.2.2. TOE セキュリティ機能要件根拠

以下では、TOEセキュリティ機能要件とセキュリティ対策方針との対応根拠について記述する。

表 8-2に対応関係を示す。表中の“X”が、対応を意味する。

表 8-2 TOE セキュリティ機能要件根拠

	FAU.GEN.1	FDP_IFC.1	FDP_IFF.1	FIA_UAU.2	FIA_UAU.7	FIA_UID.2	FMT_MOF.1	FMT_MTD.1:1	FMT_MTD.1:2	FMT_MTD.1:3	FMT_MTD.1:4	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1
O.NET_FLOW		X	X					X		X				X
O.I&A				X	X	X			X		X	X	X	X
O.AUDIT	X						X							X

O.NET_FLOW を実現するためには、以下の機能が必要である。

a) 管理ユーザーのみがポリシーフィルターの設定の変更・参照が行え、一般ユーザーがポリシーフィルターの設定の参照のみ行えるよう制限されること

b) 通信パケットから得られた情報のセキュリティ属性と、ポリシー（フィルタリング条件）とのマッチングにより評価し、ポリシーで通過が設定されている通信パケットの場合通過を許可し、それ以外の場合は遮断することが実施されること

a)は、FMT_MTD.1:1、FMT_MTD.1:3によって実現され、b)は、FDP_IFC.1、FDP_IFF.1、FPT_RVM.1によって実現される。

よって、通信パケットのヘッダ情報を利用した情報フロー制御を行うために上記の機能要件で必要十分である。

O.I&A を実現するためには、以下の機能が必要である。

a） TOE の管理を行う前に必ずパスワード認証メカニズムにて、認証時に入力するパスワードは表示されずに管理ユーザーと一般ユーザーが識別・認証されること

b） TOE に識別・認証された一般ユーザー又は管理ユーザーのみ TOE を管理することができること

c） TOE に識別・認証された、管理ユーザーのみがユーザーの管理（追加、改変、削除）が行え、一般ユーザーは参照のみ行えるよう制限されること

a)は、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FPT_RVM.1によって実現され、b)は、FMT_SMF.1、FMT_SMR.1によって実現され、c)はFMT_MTD.1:2、FMT_MTD.1:4によって実現される。

よって、TOEを管理する前に必ずユーザーを識別・認証されるため、上記の機能要件で必要十分である。

O.AUDIT を実現するためには、以下の機能が必要である。

a） ポリシーフィルターでのフィルタリング結果のログが取得されること

b） 管理ユーザー及び一般ユーザーのログイン、ログアウトのログが取得されること

c） ポリシーフィルター、識別･認証機能での管理ログが取得されること

d） (a)～(c)のログがバイパス無く確実に取得されること

e） 監査機能の起動と終了を管理者のみ行えるように制限すること

a)、b)、c)はFAU.GEN.1によって実現され、d)はFPT_RVM.1によって実現され、e)はFMT_MOF.1によって実現される。

よって、TOEの機能の利用を記録する手段を提供するため、上記の機能要件で必要十分である。

8.2.3. TOE 保証要件の妥当性

内閣官房情報セキュリティセンターから提示された「政府機関の情報セキュリティ対策のための統一基準（2005年12月版[全体版初版]）」において、「情報システムセキュリティ責任者は、構築する情報システムに重要なセキュリティ要件があると認めた場合には、当該情報システムのセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）のST 評価・ST 確認を受けること。」「IT製品・システムを調達する場合にはISO15408に基づき評価･認証されたかどうかを評価項目として活用する」とされている。これに対応するため、EAL1の品質保証レベルを保証する。

8.2.4. IT 環境に対するセキュリティ要件の根拠

以下では、IT環境に対するセキュリティ要件とセキュリティ対策方針との対応根拠について記述する。

表 8-3表 8-2に対応関係を示す。表中の“X”が、対応を意味する。

表 8-3 IT 環境に対するセキュリティ要件の根拠

	FPT_STM.1
OE.ENVIRONMENT	
OE.ADMIN_USER	
OE.MANAGE	
OE.CONFIG	
OE.LOG_SIZING	
OE.BOUNDARY	
OE.TIME	X

OE.TIME は、FPT_STM.1 によって実現される。なぜなら、FPT_STM.1 によって、ログ管理機能により TOE のログに付与される信頼できる日付･時刻が提供されるからである。

8.2.5. IT セキュリティ機能要件依存性根拠

以下に、ITセキュリティ機能要件の依存性について分析した結果を示す。

表 8-4 依存性根拠

選択した機能要件	依存する機能要件	依存性を満たさない機能要件
FAU_GEN.1	FPT_STM.1	なし
FDP_IFC.1	FDP_IFF.1	なし
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FMT_MSA.3 (①参照)
FIA_UAU.2	FIA_UID.1(*1)	なし
FIA_UAU.7	FIA_UAU.1(*2)	なし
FIA_UID.2	なし	なし
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	なし

選択した機能要件	依存する機能要件	依存性を満たさない機能要件
FMT_MTD.1:1	FMT_SMF.1 FMT_SMR.1	なし
FMT_MTD.1:2	FMT_SMF.1 FMT_SMR.1	なし
FMT_MTD.1:3	FMT_SMF.1 FMT_SMR.1	なし
FMT_MTD.1:4	FMT_SMF.1 FMT_SMR.1	なし
FMT_SMF.1	なし	なし
FMT_SMR.1	FIA_UID.1(*1)	なし
FPT_RVM.1	なし	なし
FPT_STM.1	なし	なし

*1　FIA_UID.2 を選択することで依存性は満たしている。

*2　FIA_UAU.2 を選択することで依存性は満たしている。

① FDP_IFF.1が依存するFMT_MSA.3は満たされていない。なぜなら、FDP_IFF.1で情報フロー制御されるサブジェクトのセキュリティ属性がないため、TOEによってセキュリティ属性が初期化されることは無い。よって依存関係は満たす必要は無い。

8.2.6. TOE セキュリティ機能要件相互補完性と内部一貫性

8.2.5章にて、TOEセキュリティ機能要件は、一部の例外を除き、それぞれと依存関係のあるTOEセキュリティ機能要件と相互補完している。これらのTOEセキュリティ機能要件以外で、明示的な依存関係は無いが、以下の追加の観点から各TOEセキュリティ機能要件の相互補完について記述する。

- バイパス防止
- 干渉防止
- 非活性化防止
- 無効化攻撃の検出

表 8-5にTOEセキュリティ機能要件の追加の観点の相互補完について示す。表中の“X”が、対応を意味する。

表 8-5　追加の観点の相互補完

	①バイパス防止	②干渉防止	③非活性化防止	④無効化攻撃の検出
FAU_GEN.1	X		X	
FDP_IFC.1	X			
FDP_IFF.1	X			X
FIA_UAU.2	X			X
FIA_UAU.7	X			
FIA_UID.2	X			X
FMT_MOF.1	X			
FMT_MTD.1:1	X			
FMT_MTD.1:2	X			
FMT_MTD.1:3	X			
FMT_MTD.1:4	X			
FMT_SMF.1	X			
FMT_SMR.1	X			

① バイパス防止

本TOEに選択された全てのTOEセキュリティ機能要件は、自身がバイパスされることにより、セキュリティ機能が正常に動作しないため、自身がバイパスされることを防止しなければならない。これに関し、FPT_RVM.1により全てのTOEセキュリティ機能が呼び出され成功することが保証される。

② 干渉防止

TOEへ物理的にアクセスできるのはシステム管理者（管理ユーザーも含まれる）だけである。また、システム管理者、及び管理ユーザーは、セキュリティ意識が高く責任を持って管理ができる者であり、TOEの機能を干渉（改ざん）することは無く、一般ユーザーは自身の権限を越えてTOEの設定を変更する操作はできないため干渉することはできない。また、TOEを経由して外部ネットワークから内部ネットワークへ通信を行う者（もしくはIT機器）は、TOEに対してパケットを送付することしかできず、TOEを操作できるサブジェクトではないため干渉することはできない。よって、セキュリティドメインを維持する必要は無い。

③ 非活性化防止

本STには、TOEの振る舞いに関する機能要件FMT_MOF.1が採用されており、FMT_MOF.1によって信頼でき悪意を持たない管理ユーザーのみTOEの監査機能の起動と終了を行うことが許可され、それ以外のユーザーは操作できない。そのため、セキュリティ機能が不正に非活性化されることは無い。

④ 無効化攻撃の検出

無効化攻撃の検出（ログ）は、FAU_GEN.1により必要なログが取得され、図 2-4のログ管理機能により適切に管理（ログの保管、ログの参照など）されており、無効化攻撃の検出ができなくなることは無い。

以上より、選択されたTOEセキュリティ機能要件は、相互に補完しあっているといえる。

8.3. TOE 要約仕様根拠

以下では、TOE セキュリティ機能根拠、TOEセキュリティ機能強度根拠、保証手段の根拠、PP主張根拠、について記述する。

8.3.1. TOE セキュリティ機能根拠

6.1章で示したように、各TOEセキュリティ機能が1つ以上のTOEセキュリティ機能要件に対応している。次に、各TOEセキュリティ機能要件と、TOEセキュリティ機能の対応箇所を示すことにより、対応できていることを表 8-6に示す。

表 8-6　TOE セキュリティ機能要件と TOE セキュリティ機能との対応関係の根拠

TOE セキュリティ機能要件	該当する TOE セキュリティ機能の記述
FAU_GEN.1	SF.I&A の(3) 識別・認証に関するログを取得する機能 「識別・認証機能は、ログ管理機能に対して以下の条件にて監査情報（ログ）を出力する。 ● 一般ユーザー、管理ユーザーのログイン成功、失敗の際に監査する （追加の監査情報）TOEへのアクセス手段 ● 一般ユーザーがログアウトした際に監査する(exitコマンド、quitコマンド、あるいはタイマ満了時) （追加の監査情報）TOEへのアクセス手段 ● ユーザーの追加、変更、削除の際に監査する （追加の監査情報）なし ● ユーザー情報の参照の際に監査する （追加の監査情報）なし 取得されるログの監査情報は、「事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)、上記の追加の監査情報」である。日付・時刻は、ログ管理機能によりログ出力時に付与されるため、TOEは付与しない。 設定変更、参照他コマンド実行のログの出力は、syslog execute commandで設定できる。またinfoレベルのログは主にログインログアウトやコマンド実行などの情報である。この出力を行うか否かをsyslog infoコマンドで設定できる。 なお、識別・認証機能とポリシーフィルターのログ出力の起動と終了（監査の起動と終了）は、それぞれが独立して起動あるいは終了できるものではなく、同一の操作により行われる。監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。 ログの出力のON（監査の起動）： ・ syslog execute command onかつ ・ syslog info onかつ ・ syslog notice on ログ出力例： 2007/05/30 17:32:13: [MMI] Executed by Serial(user): syslog execute command on 2007/05/30 17:32:16: [MMI] Executed by Serial(user): syslog info on 2007/05/30 17:32:20: [MMI] Executed by Serial(user): syslog notice on ログの出力のOFF（監査の終了）： ・ syslog execute command offあるいは ・ syslog info offあるいは ・ syslog notice off ログ出力例： 2007/05/30 17:30:55: [MMI] Executed by Serial(user): syslog info off」

TOE セキュリティ機能要件	該当する TOE セキュリティ機能の記述
	SF.POLICYFILTER の(3) ポリシーフィルターに関するログを取得する機能 「ポリシーフィルターは、ログ管理機能に対して以下の条件にて監査情報（ログ）を出力する。 ● ポリシーに合致するコネクションやパケットの発生の際に監査する （追加の監査情報）ポリシー番号、プロトコル、パケットの情報 ● ポリシーフィルター変更の際に監査する （追加の監査情報）なし ● ポリシーフィルター設定情報の参照の際に監査する （追加の監査情報）なし 取得されるログの監査情報は、「事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)、上記の追加の監査情報」である。日付・時刻は、ログ管理機能によりログ出力時に付与されるため、TOEは付与しない。 設定変更、参照他コマンド実行のログ出力はsyslog execute commandで設定できる。またnoticeレベルのログは主にフィルタリングで処理されるパケットに関わる情報のログである。この出力を行うか否かをsyslog noticeコマンドで設定できる。 なお、識別・認証機能とポリシーフィルターのログ出力の起動と終了（監査の起動と終了）は、それぞれが独立して起動あるいは終了できるものではなく、同一の操作により行われる。監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。 ログの出力のON（監査の起動）： ・ syslog execute command onかつ ・ syslog info onかつ ・ syslog notice on ログ出力例： 2007/05/30 17:32:13: [MMI] Executed by Serial(user): syslog execute command on 2007/05/30 17:32:16: [MMI] Executed by Serial(user): syslog info on 2007/05/30 17:32:20: [MMI] Executed by Serial(user): syslog notice on ログの出力のOFF（監査の終了）： ・ syslog execute command offあるいは ・ syslog info offあるいは ・ syslog notice off ログ出力例： 2007/05/30 17:32:46: [MMI] Executed by Serial(user): syslog notice off 2007/05/30 17:32:50: [MMI] Executed by Serial(user): syslog execute command off
FDP_IFC.1 FDP_IFF.1	SF.POLICYFILTER の(2) フィルタリングを実施する機能 「TOE は、TOE に入力された全ての通信パケットのセキュリティ属性を確認し、ポリシーとのマッチングを行うことでステートフルインスペクション方式にてフィルタリングを行う（図 6-1 参照）。また、ステートフルインスペクション方式での通過が許可される条件は表 6-2 の通りである。」

TOE セキュリティ機能要件	該当する TOE セキュリティ機能の記述
FIA_UAU.2 FIA_UID.2	SF.I&A の(1) ユーザーを識別・認証を実施する機能 「TOE は、役割として管理ユーザーと一般ユーザーを区別して識別・認証する。・・・TOE を操作する前には、いかなるコンソールコマンドの実行も許されず、必ず識別・認証機能が働く。」
FIA_UAU.7	SF.I&A の(1) ユーザーを識別・認証を実施する機能 「・・・パスワードを入力する際は、パスワードは画面には表示されず、盗み見られることは無い。・・・」
FMT_MOF.1	SF.I&A の(3) 識別・認証に関するログを取得する機能 「監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。」 SF.POLICYFILTER の(3) ポリシーフィルターに関するログを取得する機能 「監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。」
FMT_MTD.1:1	SF.POLICYFILTER の(1) ポリシーフィルターを設定する機能 「TOEは、管理ユーザーがフィルター条件（ポリシー及びポリシーセット）を参照・変更のみ行えるよう制限する。また、一般ユーザーが参照のみ行えるよう制限する。 ポリシーは、通信パケットの以下のセキュリティ属性値の条件を設定し、その条件にマッチした通信パケットの振る舞い（通過又は遮断）を設定する。 ● source_interface ● dest_interface ● source_address ● dest_address ● service ポリシーを複数組み合わせてフィルタリングのルールとして作成されたものは、ポリシーセットと呼ばれる。 通信パケットがポリシーとマッチした際の TOE の動作として、表 6-1 の 4 通りが設定できる。」

TOE セキュリティ機能要件	該当する TOE セキュリティ機能の記述
FMT_MTD.1:2	SF.I&A の(2) ユーザーを管理する機能 「TOEのユーザーを管理する役割として、管理ユーザーと一般ユーザーが存在する。管理ユーザーは、ユーザーの追加、削除、属性値の改変、参照（パスワードは除く）を行うことができ、一般ユーザーは、ユーザーデータの参照のみ（パスワードは除く）行うことができる。よって、一般ユーザーは自身のパスワードを変更する際は、管理ユーザーに依頼する必要がある。・・・」
FMT_MTD.1:3	SF.POLICYFILTER の(1) ポリシーフィルターを設定する機能 「TOEのユーザーを管理する役割として、管理ユーザーと一般ユーザーが存在する。管理ユーザーは、フィルター条件（ポリシー及びポリシーセット）を参照・変更を行うことができ、一般ユーザーは、フィルター条件を参照のみ行うことができる。 ポリシーは、通信パケットの以下のセキュリティ属性値の条件を設定し、その条件にマッチした通信パケットの振る舞い（通過又は遮断）を設定する。 ● source_interface ● dest_interface ● source_address ● dest_address ● service ポリシーを複数組み合わせてフィルタリングのルールとして作成されたものは、ポリシーセットと呼ばれる。 通信パケットがポリシーとマッチした際の TOE の動作として、表 6-1 の 4 通りが設定できる。」
FMT_MTD.1:4	SF.I&A の(2) ユーザーを管理する機能 「TOEのユーザーを管理する役割として、管理ユーザーと一般ユーザーが存在する。管理ユーザーは、ユーザーの追加、削除、属性値の改変、参照（パスワードは除く）を行うことができ、一般ユーザーは、ユーザーデータの参照のみ（パスワードは除く）行うことができる。よって、一般ユーザーは自身のパスワードを変更する際は、管理ユーザーに依頼する必要がある。・・・」

TOE セキュリティ機能要件	該当する TOE セキュリティ機能の記述
FMT_SMF.1	SF.I&A の(2) ユーザーを管理する機能 「管理ユーザーは、全てのユーザーの管理（参照・変更）を行うことができる。ユーザーの管理とは、ユーザーの追加、削除、属性値の改変を行うことである。 一般ユーザーは、ユーザーの管理（変更）は行うことはできないが、(参照)は行える。よって、一般ユーザーは自身のパスワードを変更する際は、管理ユーザーに依頼する必要がある。 パスワードは、32 文字以内で ASCII 文字（大文字小文字は区別される）を組み合わせて設定する。」 以上の管理機能により、TOE の管理要件を実現できる。
FMT_SMR.1	SF.I&A の(1) ユーザーを識別・認証を実施する機能 「TOE は、役割として管理ユーザーと一般ユーザーを区別して識別・認証する。・・・」
FPT_RVM.1	SF.I&A の(1) ユーザーを識別・認証を実施する機能 「・・・TOEを操作する前には、いかなるコンソールコマンドの実行も許されず、必ず識別・認証機能が働く。」 SF.POLICYFILTERの(2) フィルタリングを実施する機能 「TOE は、TOE に入力された全ての通信パケットのセキュリティ属性を確認し、ポリシーとのマッチングを行うことでステートフルインスペクション方式にてフィルタリングを行う（図 6-1 参照)。また、ステートフルインスペクション方式での通過が許可される条件は表 6-2 の通りである。」

8.3.2. TOE セキュリティ機能強度根拠

本TOEの保証レベルは、EAL1であるため、AVA_SOF.1は含まれない。そのため、TOE セキュリティ機能強度根拠を説明する必要は無い。

8.3.3. 保証手段の根拠

表 6-4で示したように、EAL1で必要とされる全てのTOE保証要件に対して、保証手段を対応付けている。また、保証手段によって、本STで規定したTOEセキュリティ保証要件が要求する証拠を網羅している。よって、EAL1におけるTOEセキュリティ保証要件が要求している証拠に合致していることは明白である。

8.3.4. PP 主張根拠

本STで参照されるPPはない。