IPCOM EXシリーズ
ファームウェア
セキュリティ ターゲット

2007年03月12日

第2.5版

富士通株式会社

更新履歴

版数	変更日	変更内容	変更箇所
1.0	2006.08.30	初版作成	全般（初回申請用として新規作成） － 1～2章：TOEの説明 － 3～4章：脅威と対策方針→ 8.1章：設定根拠説明 － 5章：TOEの実装要件→ 8.2章：対策方針と実装要件の根拠説明 － 6章：TOEの実装仕様→ 8.3章：実装要件と実装仕様の根拠説明
1.1	2006.09.19	問題点修正	記載内容の不備指摘の反映（2006.09.13 打合せ結果の反映）
1.2	2006.09.22	問題点修正	上記の続き（5章～8を修正）
1.3	2006.10.02	問題点修正	O.ACXのセキュリティ対策方針が不要と判断した（関連記事を削除）
			2.2に、TOE監査者の説明（想定される用途）を追記した。
			物理的アクセスに関与する記事を「TOEを動作させる装置」という表現に変更した。（4章まで修正済み）
	2006.10.06	問題点修正	内部レビュー：TOE要約の記事を修正（TOEの範囲が不明瞭だった）
1.4	2006.10.31	問題点修正	問題点修正（ASM.8、OE.12を追加、ASM.7、OE.8、OE.9、OE.10を削除、他）
1.5	2006.11.09	問題点修正	修正誤りの再修正（表現ミスなど） FAU_STG.1.bを削除 TOE要約の表現を修正（要求仕様的な表現→実装仕様的な表現）
	2006.11.10	問題点修正	内部レビュー：TOE要約の日本語表現不良を修正
1.6	2006.11.14	問題点修正	問題点修正 保護資産データに関する不明確部分を補足説明（図表現追加）
1.7	2006.11.17	問題点修正	問題点修正(6章と8章)
1.8	2006.11.22	問題点修正	問題点修正 － FAU_SEL.1、FAU_STG.1、FAU_STG.4bを削除 － ASM.SYSLOG、OE.SYSLOGを追加、および、誤記修正
1.9	2006.11.27	問題点修正	問題点修正 － ASM.SYSLOG、OE.SYSLOGを修正、OE.AUDVIEWを追加 － FAU_SAR.1を削除 － フィルタリング条件でICMPのメッセージタイプを削除
2.0	2006.11.28	問題点修正	ASM.SYSLOGの根拠説明を修正
	2006.11.29	問題点修正	SF_AUD.1.2に記事追加、SF_AUD.1.5に一覧表追加
2.1	2006.11.30	問題点修正	SF_ENV.2.4に記事追加、6.2保証手段の誤記修正
2.2	2006.12.04	問題点修正	ADV_FSP.1の記載変更 SF_ENV.1.2、SF_ENV.2.2の記事修正
2.3	2007.01.16	問題点修正	問題点修正 － 1.5のTOE管理者に、運用管理専用ネットワークの管理を追記 － 2.3.4の説明に、Syslogサーバの機能概要を追記
2.4	2007.01.31	問題点修正	問題点修正 － 2.3.2の説明に、装置オプションの補足事項を追加
2.5	2007.03.12	問題点修正	問題点修正 － 2.5のタイトル、2.5.1の説明文、3.2 文頭及びT1の説明文、8.1.1のT1の説明文において、資産に関する語句/説明修正

目次

第1章　ST概説

1.1 ST識別

本章では、STの識別情報を記述する。

STタイトル	IPCOM EXシリーズ ファームウェア セキュリティ ターゲット
STバージョン	2.5
ST発行日	2007年03月12日
ST発行者	富士通株式会社
TOEタイトル	IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント
TOEバージョン	V1.0.00
CCのバージョン	Common Criteria for Information Technology Security Evaluation Version 2.3 Interpretations-0512

本TOEの版数は、後述の保守端末を利用し、版数情報表示コマンドを実行することで確認できる。

1.2 ST概要

本STは、富士通株式会社が提供するファイアウォール製品であるIPCOM EXシリーズ ファームウェアのセキュリティ コンポーネントについて記述している。対象となるTOEは、IPCOM EXシリーズ ファームウェアとして提供される以下のセキュリティ コンポーネントである。

- IPパケットフィルタリング
- 運用支援
- 環境設定

IPCOM EXシリーズ ファームウェアとして以下のコンポーネントも同時配布されるが、これらのコンポーネントは、TOE対象外である。

- システムの二重化制御（装置の二重化機能、LAN二重化機能）
- 経路制御（RIP、OSPF、FNAルーティング、他）
- 暗号通信（IPSec-VPN機能、SSL-VPN機能、SSLアクセラレータ機能、認証機能）
- アドレス変換
- サーバ負荷分散
- リンク負荷分散
- QoS制御（帯域制御機能）
- 簡易サーバ（DNSサーバ機能、DHCPサーバ機能）

1.3 CC適合

本製品は、「外部ネットワークからの攻撃」や「他部門の内部ネットワーク(サブネットワーク)からの不正アクセス」から、自部門の内部ネットワークを保護することが可能である。このネットワーク・セキュリティ保護機能として、以下のセキュリティ要件に適合する。

- 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 参照資料

[CCパート1]

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model August 2005 Version 2.3 , CCMB-2005-08-001

[CCパート2]

Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements August 2005 Version 2.3 , CCMB-2005-08-002

[CCパート3]

Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements August 2005 Version 2.3 , CCMB-2005-08-003

1.5 用語

ここでは、本書で使用する用語について説明する。

内部ネットワーク

本TOEにより、外部ネットワークからのセキュリティの脅威に対して保護されるネットワーク・セグメント。それぞれの組織内部のイントラネット・セグメント、サーバ管理通信専用の運用管理専用ネットワーク・セグメント及び、インターネットに情報を公開するために設置された公開セグメント(DMZ:De-Militarized Zone 非武装セグメント)が「内部ネットワーク」に該当する。

運用管理専用ネットワーク

サーバ管理通信専用として独立させたネットワーク・セグメント。

外部ネットワーク

組織のセキュリティ ポリシーが及ばないインターネットや、自部門と異なる方針で運営管理されているイントラネットのネットワーク・セグメントで、保護対象となる内部ネットワーク以外のネットワーク・セグメント。

保守端末

TOEの運用～監査～保守において、TOE管理者またはTOE監査者が利用する専用端末。

コマンド操作端末

TOEとの通信にSSHプロトコルやTelnetプロトコルを利用し、コマンド形式(CLI)で操作する保守端末。

Webブラウザ端末

TOEとの通信にHTTPSプロトコルを利用し、Webブラウザ形式(GUI)で操作する保守端末。

システム運用管理部門

組織に属する内部ネットワークの運用管理責任を担う部署。

TOE管理者

TOEの設置～運用～監査～保守に渡って、本TOE及び運用管理専用ネットワークの運用全般の管理責任を担う管理者。主に、システム運用管理部門で策定されたセキュリティポリシーに基づき、本TOEの構成定義情報を設定し、セキュリティポリシーを具体化する。本TOEのユーザ認証機能では、管理者権限クラスがTOE管理者に該当する。

TOE監査者

TOEの運用～監査を担い、TOE管理者を補佐する副管理者。TOE管理者より権限が低く、本TOEの運用状況監視権限が許可され、本TOEの構成定義情報を変更する権限を持たない。本TOEのユーザ認証機能では、オペレーター権限クラスがTOE監査者に該当する。

編集モード

TOE管理者の権限に対する現在のステータスを意味する。このステータスには、通常モードと編集モードが存在し、編集モードは通常モードの権限を包含し、TOEを設定変更できる状態を意味する。

利用者

内部ネットワークに接続され、外部ネットワークにアクセスするユーザ、及び外部ネットワークに接続され、内部ネットワークにアクセスするユーザ。

IPパケットデータ

内部ネットワークと外部ネットワーク間で、送受信されるデータ。

内部セキュリティポリシー

システム運用管理部門が設定する内部ネットワークのセキュリティ方針であり、フィルタリングルールで実現される。

フィルタリングルール

内部セキュリティポリシーを具体化したルール。フィルタリングルールは、フィルタリング条件の組み合わせから構成される。

フィルタリング条件

IPパケットデータを内部ネットワークと外部ネットワーク間で通過／遮断するための条件。

構成定義情報ファイル

フィルタリング条件などの動作条件が列挙された構成定義情報を退避したファイル。

ロギング情報

TOEの監査記録において、任意の実行結果を意味する。 また、関連装置にロギング情報を転送する場合、イベント転送と表現する。

ロギング情報ファイル

TOEの監査記録において、格納または保存されたロギング情報の集まりを意味する。

第2章　TOE記述

2.1 TOEの概要

評価対象の種別

ファイアウォール製品

評価対象の機能概要

本TOEは、複数のネットワークの境界点に位置し、あるネットワークから受信した通信パケットを、事前に定められた規則（フィルタリングルール）に従って、別ネットワークへ配送、又は破棄するIPパケットフィルタリング機能を提供するファームウェアである。本機能により、外部ネットワーク上の通信リソースを利用できる利点を活かしながら、不正アクセスなどの脅威から、内部ネットワーク上の通信リソースを保護することができるようになる。

2.2 TOEの利用

本節では、TOEの利用環境、運用方法について説明する。

利用目的

外部ネットワークからの不正アクセスに対する脅威から、内部ネットワーク上の通信リソースを保護するために利用する。

利用環境

複数のネットワークの境界上に配置し、それぞれのネットワークを接続および中継する装置として利用する。
また、本TOEでは、グローバルIPアドレス体系（インターネット）とプライベートIPアドレス体系（イントラネット）を、IPアドレス体系を隠蔽しながら中継すること（IPアドレス変換機構）を想定していない。

構築方法

本TOEは、許可されたTOE管理者だけが運用可能である。また、接続するすべての内部ネットワークを統合的に管理することを目的とするシステム運用管理部門で策定された内部セキュリティポリシーが存在し、この識別されたセキュリティポリシーに従って、TOE管理者は、正しくTOEおよびTOEを動作させるハードウェア装置を構成、維持、運用する。また、運用管理補佐が必要な場合、TOE監査者を任命し、本TOEの運用監査（TOEへの不正アクセス監査や、内部ネットワークへの不正侵入の兆候監査）を依頼する。

運用方法

TOE監査者は、監査記録からTOEの構成変更や設定変更が必要となる不正アクセスの兆候を検出した場合、TOEの構成変更や設定変更が可能なTOE管理者に報告し、TOE管理者は適切な対処を実施する。

2.3 TOEの構成(物理構成)

本節では、TOEの物理構成について説明する。

2.3.1 TOEの範囲

TOEは、ファイアウォール装置であるIPCOM EXシリーズのファームウェアであり、以下のコンポーネントで構成される。このコンポーネントは、セキュリティ コンポーネントとして版数管理される。

- IPパケットフィルタリング
- 運用支援
- 環境設定

IPCOM EXシリーズ ファームウェアとして以下のコンポーネントも提供されるが、本TOEの対象外である。

- システムの二重化制御(装置の二重化機能、LAN二重化機能)
- 経路制御(RIP、OSPF、FNAルーティング、他)
- 暗号通信(IPSec-VPN機能、SSL-VPN機能、SSLアクセラレータ機能、認証機能)
- アドレス変換
- サーバ負荷分散
- リンク負荷分散
- QoS制御(帯域制御機能)
- 簡易サーバ(DNSサーバ機能、DHCPサーバ機能)

本ファームウェアは、専用ハードウェア装置の不揮発性メモリ領域に格納される。

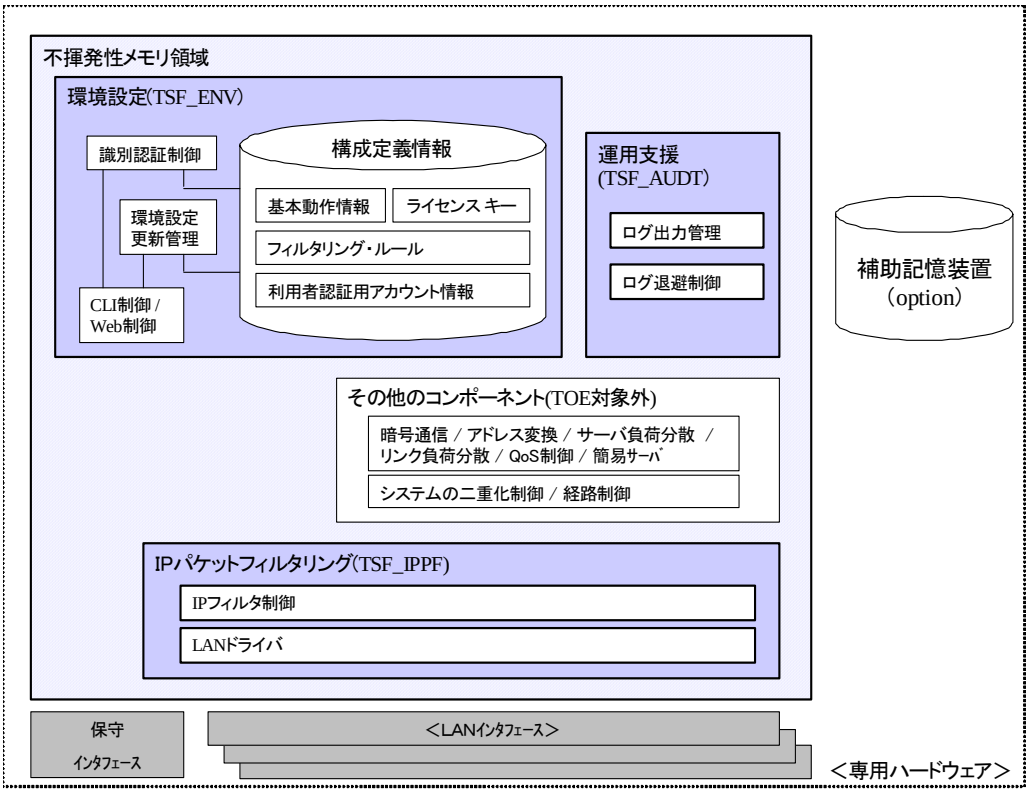


図2-1 TOEの物理構成

2.3.2 ハードウェア構成(本体装置)

TOEは、以下の専用ハードウェア装置上で動作させる。 また、各モデルには、TOE対象外の制御部(使用ライセンス)が標準添付されており、攻撃防御機能が標準実装されるSCモデルや、サーバ負荷分散機能が標準実装されるSLBモデルが提供される。

- 富士通 IPCOM-EX1000 SCモデル
- 富士通 IPCOM-EX1200 SCモデル
- 富士通 IPCOM-EX2000 SCモデル
- 富士通 IPCOM-EX1000 SLBモデル
- 富士通 IPCOM-EX1200 SLBモデル
- 富士通 IPCOM-EX2000 SLBモデル

TOEの初期構成システムとして提供されるSCモデルとSLBモデルは、各モデルで標準実装していない制御部のライセンスを追加購入することで、IPCOM EXシリーズ ファームウェアで提供している各種機能を利用可能になる。

TOE運用における上記本体装置上のハードウェア環境の概要を以下に記載する。

表2-1 本体装置/周辺装置の装置概要(基本実装)

装置概要	IPCOM EX1000	IPCOM EX1200	IPCOM EX2000	主要用途
LANインタフェース(標準)	100Mbps x 4	100Mbps x 4	1Gbps x 4	通信用
LANインタフェース(最大)	6	16	16	
通過性能(性能指標)	100Mbps	180Mbps	600Mbps	(目標値)
最大セッション数	100,000	200,000	500,000	
保守インタフェース (保守端末専用)	LAN x 1	LAN x 1	LAN x 1	環境設定用
	RS232C x 1	RS232C x 1	RS232C x 1	
導入用記憶装置(基本)	CD-ROM	CD-ROM	CD-ROM	導入用
不揮発性メモリ	1.0 GB	1.0 GB	2.0 GB	

表2-2 本体装置/周辺装置の装置概要(選択オプション)

装置オプション概要	IPCOM EX1000	IPCOM EX1200	IPCOM EX2000	備考
補助記憶装置(Option) (*2)	実装せず(*1)	実装せず(*1)	実装せず(*1)	ログ格納用
	HDD x 1	HDD x 1	HDD x 1	
LANインタフェース(Option)	増設なし	増設なし	増設なし	通信用
	100Mbps x 2	-	-	
	-	1Gbps x 4	1Gbs x 4	
	-	1Gbps x 8	1Gbs x 8	
	-	(その他)	(その他)	

*1:補助記憶装置(Option)を実装しない場合、監査記録を保存するためのSyslogサーバなど(後述)を設置しなければならない。
*2:SLBモデルでは自動的に選択され、HDDが搭載される。

表2-3 本体装置/周辺装置の装置概要(モデル依存仕様)

装置仕様概要	SCモデル	SLBモデル	備考
IPフィルタ制御の例外動作 (構成定義のデフォルト値)	パケット遮断	パケット通過	フィルタリング条件に合致しない場合の処理概要(*1)

*1:例外動作は、構成定義でパケット遮断またはパケット通過に初期値を設定変更することができる。

2.3.3 ネットワーク構成

本TOEを動作させるハードウェア装置は、複数のネットワークの境界点に位置し、以下のようなネットワーク構成になる。

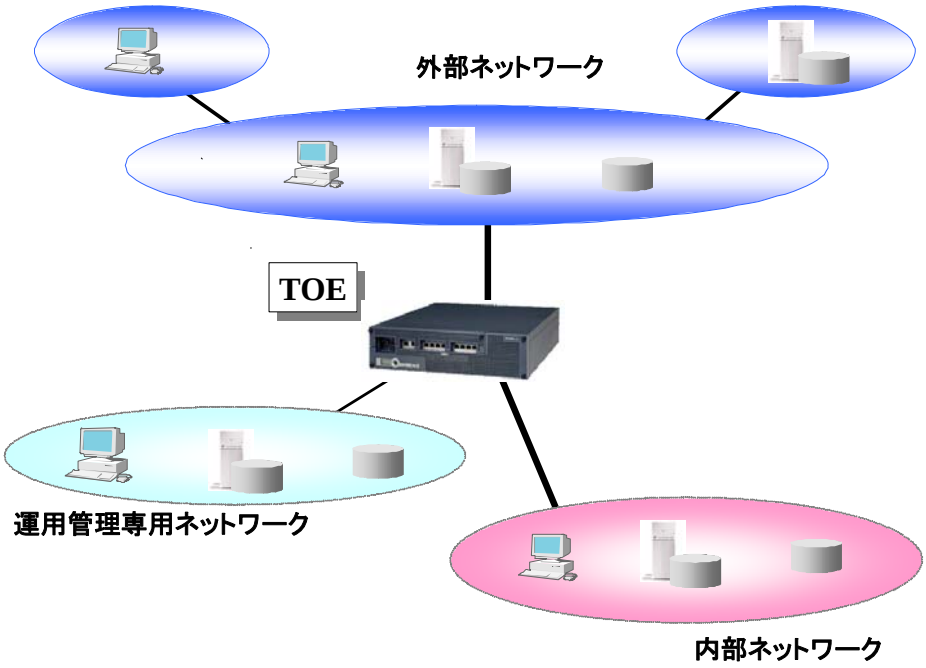


図2-2　TOEのネットワーク構成

上記のネットワーク構成では、外部ネットワークと内部ネットワークにおいて、相互のIPアドレス体系を隠蔽しない運用を想定している。

例えば、外部ネットワークがグローバルIPアドレス体系（インターネット）であれば、内部ネットワークもグローバルIPアドレス体系（インターネット）で運用する。（SCモデルで想定されるネットワーク環境である）　また、外部ネットワークがプライベートIPアドレス体系（イントラネット）であれば、内部ネットワークもプライベートIPアドレス体系（イントラネット）で運用する。（SLBモデルで想定されるネットワーク環境である）

運用管理専用ネットワークは、TOEの管理通信セグメントに利用し、外部ネットワークおよび内部ネットワークと通信できない独立したネットワークとして構築する。

2.3.4 ハードウェア構成(関連装置)

以下に、TOEが動作するハードウェア装置、保守端末及び、関連装置の構成を示す。

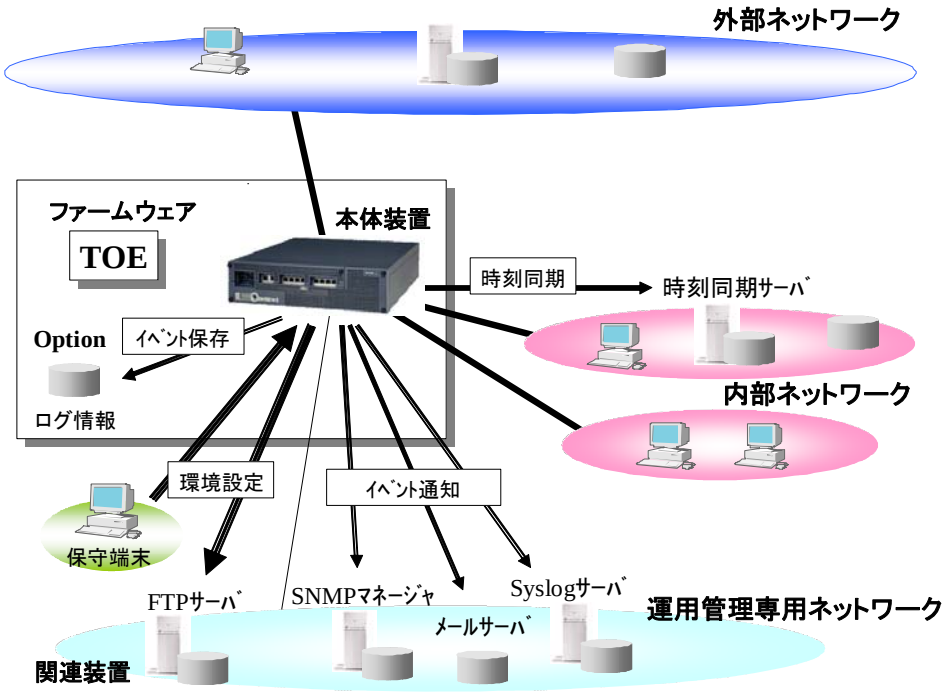


図2-3　TOEと関連装置の構成

本TOEを環境設定するための端末として、以下の保守端末を設置する。

- 保守端末(環境設定機能):本TOEの動作環境を設定または動作状況を監視するLAN接続したTelnetマシンまたは、LAN接続したWebブラウザまたは、RS232C接続したVT100互換端末で、運用管理専用ネットワークまたは、保守インタフェースに接続する。

本TOEの時刻を正確に保つため、以下の関連装置を設置する。

- 時刻同期サーバ(運用支援機能):本TOEの監査機能で重要イベントの記録(発生時刻)保証のため、時刻参照するサーバで、運用管理専用ネットワークまたは、内部ネットワークに接続する。

ロギング情報を継続保持可能な補助記憶装置(Option)を実装していない場合、ロギング情報を代理保持可能な以下の関連装置を設置する。

- Syslogサーバ(運用支援機能):本TOEの監査機能で重要イベントを検出した場合にイベントを通知するSyslogサーバで、運用管理専用ネットワークに接続する。本サーバは、ロギング情報を格納し、格納したロギング情報を維持監視するため、容量管理機能及び表示機能を有する。

本TOEの環境設定情報を退避する場合、または、重要イベントを遠隔装置で監視したい場合、以下の関連装置を設置する。

- 定義情報格納サーバ(環境設定機能):本TOEから定義情報を退避する独立したFTPサーバまたは、保守端末と同居するFTPサーバで、運用管理専用ネットワークに接続する。
- メールサーバ(運用支援機能):本TOEの監査機能で重要イベントを検出した場合に、イベントを通知するメールサーバで、運用管理専用ネットワークに接続する。
- SNMPマネージャ(運用支援機能):本TOEの監査機能で重要イベントを検出した場合に、イベントを通知するSNMPマネージャで、運用管理専用ネットワークに接続する。

2.4 TOEの機能(論理構成)

本TOEは、以下のような論理構成で動作する。

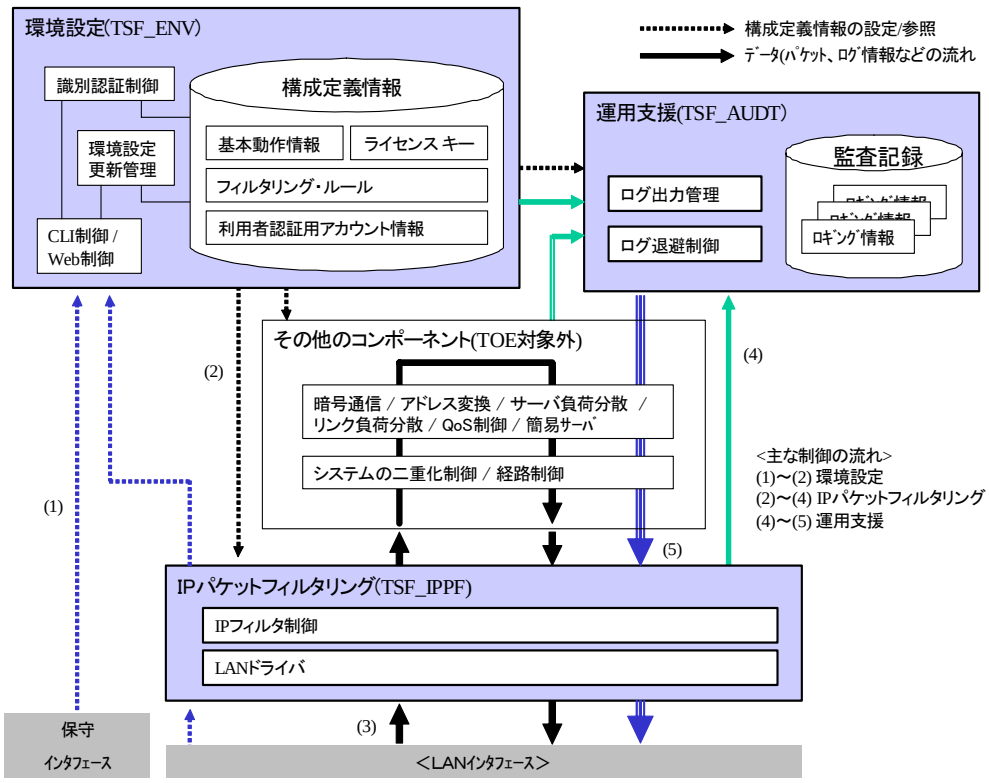


図2-4　TOEのソフトウェア構成

2.4.1 環境設定(TSF_ENV)

TSF_ENVは、TOEの動作環境を設定する機能を提供する。保守インタフェースか、IPパケットフィルタリング(TSF_IPPF)でパケット通過を設定したLANインタフェースに保守端末を接続することで、本TOEに通信することができる。本TOEに通信開始後、利用者識別認証が実行され、許可されたTOE管理者であれば、TOEの構成定義情報を設定または変更することができる。設定された構成定義情報は、構成定義情報の有効化操作により、IPパケットフィルタリング(TSF_IPPF)や運用支援(TSF_AUDT)に配布される。

- CLI制御及びWeb制御
  TOEを動作させるハードウェア装置の保守インタフェース(LAN接続またはRS232C接続)を制御し、保守端末との通信を常時確立可能とする。また、LANインタフェースに接続された保守端末から接続要求された場合、IPパケットフィルタリング(TSF_IPPF)で通過を許可されている通信に限り確立可能とする(CLI制御およびWeb制御では、接続元の正当性を検証しない)。保守端末からの接続要求後、識別認証制御を利用し、TOE管理者またはTOE監査者であるかを識別検証する。なお、本制御部では、TOE管理者として識別認証された場合、構成定義情報の更新や設定された構成定義情報を退避することも可能である。

- 識別認証制御
  CLI制御およびWeb制御のサブコンポーネントとして、識別認証制御を提供する。この識別認証制御では、アカウントおよびパスワードによる識別認証機能やパスワード変更機能を提供し、TOE管理者やTOE監査者を識別する。

● 環境設定更新管理
CLI制御およびWeb制御のサブコンポーネントとして、TOEの動作を決定する以下のような構成定義情報を参照および設定(変更)する機能を提供する。
- 基本動作情報(ルータまたはブリッジとして動作させるためのネットワーク情報など)
- フィルタリング・ルール(セキュリティポリシーとなるフィルタリング条件と動作)
- 利用者認証用アカウント情報(TOE管理者やTOE監査者のアカウント名やパスワード情報)

2.4.2 IPパケットフィルタリング(TSF_IPPF)

TSF_IPPFは、複数のLANインタフェース間で送受信されるIPパケットデータを評価し、通過または破棄の処理を行う。LANインタフェースから取得したIPパケットデータは、配布された構成定義情報に基づき、通過と判断したIPパケットデータだけ受信(内部転送)が許可される。通過と判断され受信が許可されたIPパケットデータは、その他のコンポーネント(TOE対象外)に内部転送され、経路制御により中継先のLANインタフェースが特定され、IPパケットフィルタリング(TSF_IPPF)に戻される。IPパケットフィルタリング(TSF_IPPF)は、経路制御で特定されたLANインタフェースを利用してIPパケットデータを送信する。

● IPフィルタ制御
LANドライバから通知されたIPパケットデータを、環境設定(TSF_ENV)によって通過可能(受信可能)と定義されたパケットに限り通過させ、その他のコンポーネント(TOE対象外)に通知する。また、通過および破棄と判断された時点で構成定義情報に基づき、監査記録を運用支援(TSF_AUDT)に通知する。その他のコンポーネント(TOE対象外)から返却されたIPパケットデータも、環境設定(TSF_ENV)によって通過可能(送信可能)と定義されたパケットに限り、LANドライバに送信を指示する。

● LANドライバ
LANインタフェースからIPパケットデータを受信し、IPフィルタ制御に通知する。また、IPフィルタ制御から通知されたIPパケットデータをLANインタフェースから送信する。なお、LANドライバは、保守インタフェース(LAN接続またはRS232C接続)を制御しない。

2.4.3 運用支援(TSF_AUDT)

TSF_AUDTは、通過または破棄のパケット処理記録や、TOEの動作結果となる監査記録を保管および退避する機能を提供する。 環境設定(TSF_ENV)やIPパケットフィルタリング(TSF_IPPF)から受け取ったロギング情報を、環境設定(TSF_ENV)で定義された方法でTOEの補助記憶装置(Option)に格納、または、指定された手段で監査記録を遠隔装置に転送する。 TOEに格納された監査記録は、保守端末を利用して退避または、全削除が許可される。なお、監査記録を遠隔装置に転送する場合も、IPパケットフィルタリング(TSF_IPPF)による評価が実施されるため、IPパケットフィルタリング指定で明示的に送信を許可(指定遠隔装置宛ての通信を許可)していなければならない。

● ログ出力管理
TOEを動作させるハードウェア装置に補助記憶装置(Option)が実装されている場合、この補助記憶装置にロギング情報を格納する。 また、遠隔関連装置へのイベント通知が指定されていれば、その装置にロギング情報をイベントとして転送する。 両方の定義が有効であれば、補助記憶装置(Option)に格納後、遠隔関連装置にもイベント転送する。

● ログ退避制御
TOEを動作させるハードウェア装置に補助記憶装置(Option)が実装されている場合、この補助記憶装置に格納されているロギング情報を退避する機能を提供する。 なお、ロギング情報の参照機能(モニタ機能)は、本TOEでは提供しない。

2.5 資産

本TOEに関係する資産には、以下のものがある。

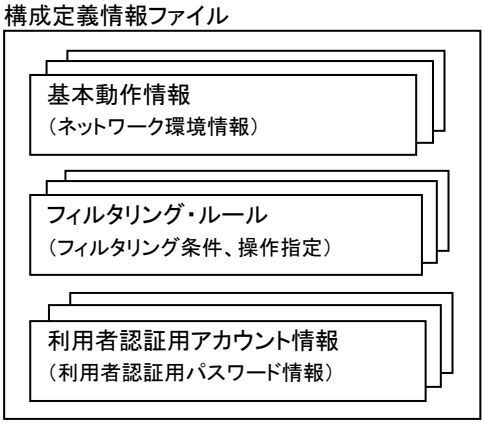
2.5.1 内部ネットワーク資産

内部ネットワーク資産とは、外部ネットワークからアクセスされる可能性がある内部ネットワーク上の内部セキュリティポリシーによって特定される資産である。内部セキュリティポリシーは、内部ネットワークを統合的に管理するシステム運用管理部門によって定められる。

2.5.2 TOE関連資産

TOE関連資産には以下のものがある。

● 構成定義情報
本TOEの動作を決定する重要な定義情報であり、内部ネットワーク上の資産を保護するセキュリティポリシーを保証するための関連資産になる。この構成定義情報は、本TOEの不揮発性メモリに格納される。この構成定義情報を関連装置に退避した場合、以下のようなファイル構成になり、退避時点の利用者認証用アカウント情報も含まれる。



- 基本動作情報（ネットワーク環境情報）：ネットワーク装置として動作するための基本情報が列挙されている。
- フィルタリング・ルール：IPパケットデータの通過または遮断条件が列挙されている。
- 利用者認証用アカウント情報（利用者認証用パスワード情報）：本TOEの利用者認証に利用するアカウント名とパスワード情報が列挙されている。

この構成定義情報が漏れた場合、不正アクセスの自動検出経路が迂回され、セキュリティ設定が甘いと判断された箇所を重点攻撃される可能性がある。また、利用者認証用アカウント情報が漏れた場合、TOE管理者やTOE監査者として不正アクセスされる可能性があるため、構成定義情報の改竄防止だけではなく、漏洩防止にも考慮が必要である。

● ロギング情報（監査記録）
本TOEの動作状況や処理結果を記録する情報であり、内部ネットワーク上の資産に対する侵害発生有無を監査するための関連資産になる。このロギング情報は、本TOEの補助記憶装置（Option）に格納される。
不正アクセスの監査状況や追跡状況を不正アクセス者に気づかれないようにするため、関連装置にイベント情報を転送または、ロギング情報ファイルとして退避する場合も、ロギング情報の漏洩防止を考慮する必要がある。

なお、本TOEではIPパケットデータの保護は行わない。

第3章　TOEセキュリティ環境

本章では、TOEのセキュリティ環境における想定、脅威及び組織のセキュリティ方針について記述する。

3.1 前提条件

本TOEは、次のセキュアな使用環境を想定している。

ASM.1（物理的アクセス）
TOEを動作させるハードウェア装置および保守端末は、物理的に不正アクセスできない。

ASM.2（接続形態）
TOEを動作させるハードウェア装置は、内部ネットワークと外部ネットワークまたは、内部ネットワークと内部ネットワークを唯一の接点で接続する形態でネットワークを構築する。

ASM.3（信頼できるTOE管理者）
TOE管理者およびTOE監査者は、TOEおよびTOEを動作させるハードウェア装置に関して不正をしない。

ASM.4（TOEの構成の管理）
TOE管理者は、TOEが正しく動作するよう、TOEおよびTOEを動作させるハードウェア装置を運用管理しなければならない。

ASM.6（データ漏洩不可）
関連装置および運用管理専用ネットワークから、TOE関連資産となるデータは漏洩しない。

ASM.8（時刻同期サーバ）
時刻同期サーバは、信用できる。

ASM.SYSLOG（ロギング情報）
ロギング情報を格納する補助記憶装置(Option)をTOEが動作するハードウェアに実装するか、ログの維持監視機能を持つSyslogサーバを設置する。

ASM.SLB（SLBモデル）
IPフィルタ制御の例外動作は、制限的（遮断）で運用する。

3.2 脅威

ここでは、TOE自身、及びTOEが設置されるITセキュリティ環境によって保護が必要となる、資産への想定される脅威について説明する。

低レベルの攻撃者によって想定される一般的な脅威は下記である。

T1（外部ネットワークから内部ネットワークへの不正アクセス）
外部ネットワークの攻撃者は、内部ネットワークに侵入し、内部ネットワーク資産の不正使用、改ざん、破壊、又は漏洩を図る恐れがある。

T2（TOEへの不正アクセスによるTOE関連資産の改ざん）
外部ネットワークまたは内部ネットワーク上の攻撃者は、本TOEに侵入し、構成定義情報を改ざんして不正なIPパケットデータやIP通信サービスを通過可能にする恐れがある。また、ロギング情報を改ざん、または、破壊し、不正行為の証拠を隠滅する恐れもある。

3.3 組織のセキュリティ方針

組織のセキュリティ方針は無い。

第4章　セキュリティ対策方針

本章では、TOEのセキュリティ対策方針における施策について記述する。

4.1 TOEのセキュリティ対策方針

本TOEに対するセキュリティ対策方針は、以下の通りである。

O.AC（外部ネットワーク利用者の制限）
TOEは、TOEにアクセスまたは、TOEを経由して内部ネットワークにアクセスしようとする外部ネットワークからの接続要求を制限する。

O.ADMIN（TOE管理者制御）
TOEは、TOE管理者およびTOE監査者だけがその動作環境の制御を行うことができるよう、TOE管理者およびTOE監査者のTOEへのアクセス認証機能を提供しなければならない。

O.AUDREC（監査記録）
TOEは、TOEを経由して送受信された通信状況を正確な日付／時間を伴って記録する機能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

TOE環境に対するセキュリティ対策方針は、以下の通りである。

OE.1（TOEの構成の管理）
TOE管理者は、内部セキュリティポリシーに従って、TOEおよびTOEを動作させるハードウェア装置を管理、運用しなければならない。

OE.2（運用管理専用ネットワークを含む物理的保護）
TOEを動作させるハードウェア装置、保守端末、構成定義情報やロギング情報を転送する関連装置（Syslogサーバ、メールサーバ、SNMPマネージャ、FTPサーバ）、および、それらを接続する運用管理専用ネットワークを、施錠可能な収納ラックやサーバ専用室に設置することで、物理的に保護しなければならない。

OE.3（TOE管理者の教育）
システム運用管理部門の責任者は、不正のないTOEおよびTOEを動作させるハードウェア装置の管理、運用ができるよう、TOE管理者およびTOE監査者を教育しなければならない。

OE.6（接続形態）
TOEを動作させるハードウェア装置は、外部ネットワークと内部ネットワークまたは、内部ネットワークと内部ネットワークを接続する唯一の接続点としてネットワークを構成しなければならない。

OE.11（運用管理専用ネットワークの管理）
TOE管理者は、運用管理専用ネットワークを、外部ネットワークおよび内部ネットワークと通信できない独立したネットワークとして設定しなければならない。

OE.12（時刻同期設定）
TOE管理者は、信頼できる時刻同期サーバ（NTPサーバ）を設定しなければならない。

OE.SYSLOG（ロギング情報の保持）
TOE管理者は、TOEが動作するハードウェアに補助記憶装置(Option)を実装するか、ロギング情報の維持監視機能を持つSyslogサーバを設置する。

OE.AUDVIEW（ロギング情報の監査）
TOE管理者は、TOEが動作するハードウェア上の補助記憶装置(Option)に格納されたロギング情報をFTPサーバ、または、保守端末に取り出し、テキストビューアで監査（参照）する。

OE.SLB（SLBモデル）
TOE管理者は、IPフィルタ制御の例外動作を制限的（遮断）に設定しなければならない。

第5章　ITセキュリティ要件

本章では、TOEのセキュリティ対策方針を果たすために、TOEと評価に使う証拠物件（文書など）が満たす必要のある機能、及び保証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

ここでは、TOE及び、その環境が満たすべきITセキュリティ要件の詳細について記述する。

5.1.1 TOEセキュリティ機能要件

5.1.1.1 運用支援に対するセキュリティ機能要件

■ **セキュリティ監査データ生成（FAU_GEN）** Security audit data generation

FAU_GEN.1 監査データ生成 (Audit data generation)

監査データ生成は、監査対象事象のレベルを定義し、記録ごとに記録されねばならないデータのリストを規定する。

下位階層

なし

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: 最小、基本、詳細、指定なし: から一つのみ選択]レベルのすべての監査対象事象; 及び
c) [割付:上記以外の個別に定義した監査対象事象]。

[選択:最小、基本、詳細、指定なし]

- 基本

各機能要件を選択した場合に監査対象とすべき基本レベル以下のアクション(規約)と、それに関連するTOEの監査対象事象（実行ログとして記録を残す事象）を示す。

表5-1　TOEの監査対象事象と個別に定義した監査対象事象

機能要件	監査対象とすべきアクション（規約）	TOEの監査対象事象
FAU_GEN.1	なし	ー
FAU_STG.4	a)　基本：監査格納失敗によってとられるアクション。	＜基本＞ メッセージログ：監査記録領域に関する記録ブロック満杯警告の発生状況を監査する。
FDP_IFC.1	なし	ー

機能要件	監査対象とすべきアクション(規約)	TOEの監査対象事象
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)。	＜基本＞ メッセージログ:TOEの起動を監査する。 セッションログ:IPパケットデータの通過/遮断を監査する。
FIA_UAU.2	a) 最小: 認証メカニズムの不成功になった使用; b) 基本: 認証メカニズムのすべての使用。	＜基本＞ アカウントログ:TOE管理者またはTOE監査者の認証成功／認証失敗を監査する。
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。	＜基本＞ アカウントログ:TOE管理者またはTOE監査者の認証成功／認証失敗を監査する。
FMT_MSA.1	a) 基本:セキュリティ属性の値の改変すべて。	＜基本＞ アカウントログ:TOE管理者の接続認証を監査する。 コマンドログ:構成定義設定変更の実行状況を監査する。 メッセージログ:構成定義情報の有効化操作を監査する。
FMT_MSA.3	a) 基本:許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本:セキュリティ属性の初期値の改変すべて。	＜基本＞ アカウントログ:TOE管理者の接続認証を監査する。 コマンドログ:構成定義設定変更の実行状況を監査する。 メッセージログ:構成定義情報の有効化操作を監査する。
FMT_MTD.1.a	a) 基本:TSF データの値のすべての改変。	＜基本＞ アカウントログ:TOE管理者の接続認証を監査する。 コマンドログ:利用者認証用アカウント情報の変更操作状況を監査する。 メッセージログ:構成定義情報の有効化操作を監査する。
FMT_MTD.1.b	a) 基本:TSF データの値のすべての改変。	なし(監査記録の初期化操作により、監査に必要な事象が消去される)
FMT_MTD.1.c	a) 基本:TSF データの値のすべての改変。	なし(監査が必要な改変操作なし)
FMT_SMF.1	a) 最小:管理機能の使用。	なし(監査が必要な事象なし)
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。	＜最小＞ コマンドログ:利用者認証用アカウント情報の変更操作状況を監査する。
FPT_STM.1	a) 最小:時間の変更; b) 詳細:タイムスタンプの提供。	＜最小＞ メッセージログ:時刻同期の成功/失敗を監査する。

[割付:上記以外の個別に定義した監査対象事象]

FDP_IFF.1の場合は、以下に定義した監査対象事象について「詳細」レベルを記録する。
- IPパケットデータの情報フロー制御実施時のセキュリティ属性

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: その他の監査関連情報]

[割付: その他の監査関連情報]

なし

依存性

FPT_STM.1 高信頼タイムスタンプ

■ セキュリティ監査事象格納(FAU_STG) Security audit event storage

FAU_STG.4 監査データ損失の防止 (Prevention of audit data loss) -（対象：補助記憶装置の実装あり）

監査データ損失の防止は、監査証跡が満杯になったときのアクションを規定する。

下位階層

FAU_STG.3

FAU_STG.4.1

TSFは、監査証跡が満杯になった場合、[選択: 監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択]及び[割付:監査格納失敗時にとられるその他のアクション]を行わねばならない。

[選択: 監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択]

- 最も古くに格納された監査記録への上書き

[割付:監査格納失敗時にとられるその他のアクション]

- 監査記録格納装置が故障した場合は、システム停止する。
- 監査記録の記録ブロックが満杯の場合、警告の監査記録を残し、関連装置に通知する。

依存性

FAU_STG.1 保護された監査証跡格納

5.1.1.2 IPパケットフィルタリングに対するセキュリティ機能要件

■ 情報フロー制御方針(FDP_IFC) (Information flow control policy)

FDP_IFC.1 サブセット情報フロー制御 (Subset information flow control)

サブセット情報フロー制御は、TOE における情報フローのサブセットについて適用可能な操作のサブセットに対し、識別された各情報フロー制御SFP が適切なものであることを要求する。

下位階層

なし

FDP_IFC.1.1

TSFは、[割付:サブジェクト、情報、及び、SFPによって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]に対して[割付:情報フロー制御SFP]を実施しなければならない。

[割付:情報フロー制御SFP]

- 情報フロー制御SFP:[IPパケットフィルタリング方針]

[割付:サブジェクト、情報、及び、SFPによって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト]

＜サブジェクトのリスト＞
・TOEのLANインタフェース

＜情報のリスト＞
・TOEを介して送受信されるIPパケットデータ

＜情報の流れを引き起こす操作のリスト＞
・IPパケットデータの通過(許可)
・IPパケットデータの遮断(拒否)

依存性

FDP_IFF.1 単純セキュリティ属性

■ 情報フロー制御機能（FDP_IFF） (Information flow control functions)

FDP_IFF.1 単純セキュリティ属性 (Simple security attributes)

単純セキュリティ属性は、情報とその情報を流したり受け取ったりするサブジェクトにおけるセキュリティ属性を要求する。単純セキュリティ属性は、この機能によって実施されなければならない規則を特定し、この機能によってセキュリティ属性がどのように引き出されるかを記述する。

下位階層

なし

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: 情報フロー制御SFP]を実施しなければならない: [割付:示されたSFP下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性]。

[割付：情報フロー制御SFP]

- 情報フロー制御SFP：[IPパケットフィルタリング方針]

[割付:示されたSFP下において制御されるサブジェクトと情報のリスト、及びセキュリティ属性]

＜サブジェクトのリスト＞
・TOEのLANインタフェース

＜情報のリスト＞
・TOEを介して送受信されるIPパケットデータ

＜情報の流れを引き起こす操作のリスト＞
・IPパケットデータの通過（許可）
・IPパケットデータの遮断（拒否）

＜サブジェクトのセキュリティ属性＞
・TOE上のIPパケットデータの受信LANインタフェース
・TOE上のIPパケットデータの送信LANインタフェース

＜情報のセキュリティ属性＞
・送信元IPアドレス（ホスト、又はネットワーク）
・送信先IPアドレス（ホスト、又はネットワーク）
・トランスポート層プロトコル（TCP、UDP、ICMP）
・送信元ポート番号（トランスポート層プロトコルがTCP、UDPの場合）
・送信先ポート番号（トランスポート層プロトコルがTCP、UDPの場合）

上記のリストおよびセキュリティ属性は、フィルタリング条件のデータに該当する。

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:各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]。

[割付:各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係]

- TOEは、実際に送受信されるIPパケットデータから得られたサブジェクト及び情報のセキュリティ属性と、フィルタリング条件から得られるサブジェクト及び情報のセキュリティ属性の関係を評価し、フィルタリング条件で通過設定されているIPパケットデータを通過させ、それ以外のIPパケットデータは遮断する。

FDP_IFF.1.3

TSFは、[割付:追加の情報フロー制御SFP規則]を実施しなければならない。

[割付:追加の情報フロー制御SFP規則]

なし。

FDP_IFF.1.4

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

[割付:追加のSFP能力のリスト]

なし。

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]

[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]

なし。

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]

[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]

なし。

依存性

FDP_IFC.1　サブセット情報フロー制御
FMT_MSA.3　静的属性初期化

5.1.1.3 環境設定に対するセキュリティ機能要件

■ 利用者認証(FIA_UAU) User authentication

FIA_UAU.2 アクション前の利用者認証 (User authentication before any action)

アクション前の利用者認証は、TSFがアクションを許可する前に、利用者が認証されることを要求する。

下位階層

FIA_UAU.1

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

■ 利用者識別(FIA_UID) User identification

FIA_UID.2 アクション前の利用者識別 (User identification before any action)

アクション前の利用者識別は、TSFがなんらかのアクションを認める前に、利用者が自分自身を識別することを要求する。

下位階層

FIA_UID.1

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

■ セキュリティ属性の管理（FMT_MSA） Management of security attributes

FMT_MSA.1 セキュリティ属性の管理 (Management of security attributes)

セキュリティ属性の管理は、許可利用者(役割)が、特定されたセキュリティ属性を管理することを認める。

下位階層

なし

FMT_MSA.1.1

TSFは、セキュリティ属性[割付:セキュリティ属性のリスト]に対し[選択:デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付:許可された識別された役割]に制限するために[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[割付:セキュリティ属性のリスト]

- TOE上のIPパケットデータの受信LANインタフェース
- TOE上のIPパケットデータの送信LANインタフェース
- 送信元IPアドレス（ホスト、又はネットワーク）
- 送信先IPアドレス（ホスト、又はネットワーク）
- トランスポート層プロトコル（TCP、UDP、ICMP）
- 送信元ポート番号（トランスポート層プロトコルがTCP、UDPの場合）
- 送信先ポート番号（トランスポート層プロトコルがTCP、UDPの場合）

[選択:デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]

- 問い合わせ
- 改変

[割付:許可された識別された役割]

識別された役割と選択の対応を示す。

許可された識別された役割	問い合わせ	改変
TOE管理者	○	○
TOE監査者	○	×

[割付: アクセス制御SFP、情報フロー制御SFP]

- 情報フロー制御SFP：[IPパケットフィルタリング方針]

依存性

[FDP_ACC.1 サブセットアクセス制御 または FDP_IFC.1 サブセット情報フロー制御]
FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.3 静的属性初期化 (Static Attribute Initialisation)

静的属性初期化は、セキュリティ属性のデフォルト値が、本来の性質として適切に許可的(permissive)あるいは制限的(restrictive)のどちらかになっていることを保証する。

下位階層

なし

FMT_MSA.3.1

TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]デフォルト値を与える[割付: アクセス制御SFP、情報フロー制御SFP]を実施しなければならない。

[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]

- 制限的

[割付: アクセス制御SFP、情報フロー制御SFP]

- 情報フロー制御SFP:[IPパケットフィルタリング方針]

FMT_MSA.3.2

TSFは、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[割付: 許可された識別された役割]

- TOE管理者

依存性

FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティ役割

■ TSFデータの管理（FMT_MTD） Management of TSF data

FMT_MTD.1.a TSFデータの管理 (Management of TSF data) -（構成定義情報の更新）

TSF データの管理は、許可利用者がTSF データを管理することを許可する。

下位階層

なし

FMT_MTD.1.1.a （構成定義情報）

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、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:許可された識別された役割]に制限しなければならない。

[割付:TSFデータのリスト]

- 利用者認証用アカウント情報

[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]

- 改変

[割付:許可された識別された役割]

- TOE管理者

依存性

FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MTD.1.b TSFデータの管理 (Management of TSF data) -（ロギング情報）

TSF データの管理は、許可利用者がTSF データを管理することを許可する。

下位階層

なし

FMT_MTD.1.1.b （ロギング情報）

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、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:許可された識別された役割]に制限しなければならない。

[割付:TSFデータのリスト]

- ロギング情報

[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]

- 消去
- その他の操作:[退避]

[割付:許可された識別された役割]

- TOE管理者

依存性

FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MTD.1.c　TSFデータの管理 (Management of TSF data) -（TOE関連資産の退避）

TSF データの管理は、許可利用者がTSF データを管理することを許可する。

下位階層

なし

FMT_MTD.1.1.c（TOE関連資産の退避）

TSFは、[割付:TSFデータのリスト]を[選択:デフォルト値変更、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:許可された識別された役割]に制限しなければならない。

[割付:TSFデータのリスト]

- 基本動作情報
- フィルタリング・ルール
- 利用者認証用アカウント情報

[選択:デフォルト値変更、問い合わせ、改変、削除、消去、[割付:その他の操作]]

- その他の操作:[バックアップ]

[割付:許可された識別された役割]

- TOE管理者

依存性

FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

■ 管理機能の特定(FMT_SMF) Specification of Management Functions

FMT_SMF.1 管理機能の特定 (Specification of Management Function)

管理機能の特定は、TSFが特定の管理機能を提供することを要求する。

下位階層

なし

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:TSFによって提供されるセキュリティ管理機能のリスト]

[割付: TSFによって提供されるセキュリティ管理機能のリスト]

表5-2 TOEの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	ー
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	なし(監査記録の制御パラメタは固定であり、管理対象にならない)
FDP_IFC.1	なし	ー
FDP_IFF.1	a) 明示的なアクセスに基づく決定に使われる属性の管理。	なし(IPフィルタリングのセキュリティ属性は固定であり、管理対象にならない)
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) TOE管理者アカウントの作成、参照、削除および、パスワード変更 b) TOE監査者アカウントのパスワード変更
FIA_UID.2	a) 利用者識別情報の管理。	a) TOE管理者およびTOE監査者のアカウントの作成、参照、削除
FMT_MSA.1	a) セキュリティ属性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(役割グループは固定であり、管理対象にならない)
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御SFPに対するデフォルト値の許可的あるいは制限的設定を管理すること。	a) なし(役割グループはTOE管理者だけであり、管理対象にならない) b) デフォルト通過禁止
FMT_MTD.1.a	a) 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(役割グループはTOE管理者だけであり、管理対象にならない)
FMT_MTD.1.b	a) 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(役割グループはTOE管理者だけであり、管理対象にならない)
FMT_MTD.1.c	a) 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(役割グループはTOE管理者だけであり、管理対象にならない)
FMT_SMF.1	なし	ー
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	なし(役割グループは固定であり、管理対象にならない)
FPT_STM.1	a) 時間の管理。	システム内時刻の管理(時刻同期サーバとの時刻補正)

依存性

なし

■ セキュリティ管理役割（FMT_SMR） Security management roles

FMT_SMR.1 セキュリティ役割 (Security roles)

セキュリティ役割は、TSF が認識するセキュリティに関する役割を特定する。

下位階層

なし

FMT_SMR.1.1

TSFは、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付:許可された識別された役割]

- TOE管理者
- TOE監査者

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 識別のタイミング

■ タイムスタンプ（FPT_STM） Time stamps

FPT_STM.1 高信頼タイムスタンプ (Reliable time stamps)

TSFがTSF機能のために高信頼タイムスタンプを提供することを要求する。

下位階層

なし

FPT_STM.1.1

TSFは、それ自身の利用のために、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

5.1.2 TOEセキュリティ保証要件

本章では、TOEセキュリティ保証要件を記述する。本TOEの評価保証レベルはEAL1である。全てのセキュリティ保証要件は、CCパート3で規定されているEAL1のコンポーネントを直接使用する。

表5-3　TOEのセキュリティ保証要件

クラス	コンポーネント名（ファミリ含む）	
ACM（構成管理）	ACM_CAP.1	バージョン番号
ADO（配布と運用）	ADO_IGS.1	設置、生成、及び立上げ手順
ADV（開発）	ADV_FSP.1	非形式的機能仕様
	ADV_RCR.1	非形式的対応の実証
AGD（ガイダンス文書）	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ATE（テスト）	ATE_IND.1	独立テスト

5.2 IT環境に対するセキュリティ要件

IT環境が提供するセキュリティ機能の機能要件は無い。

第6章　TOE要約仕様

TOEのセキュリティ要件に応じるTOEのセキュリティ機能及び保証方法について記述している。

6.1 TOEセキュリティ機能

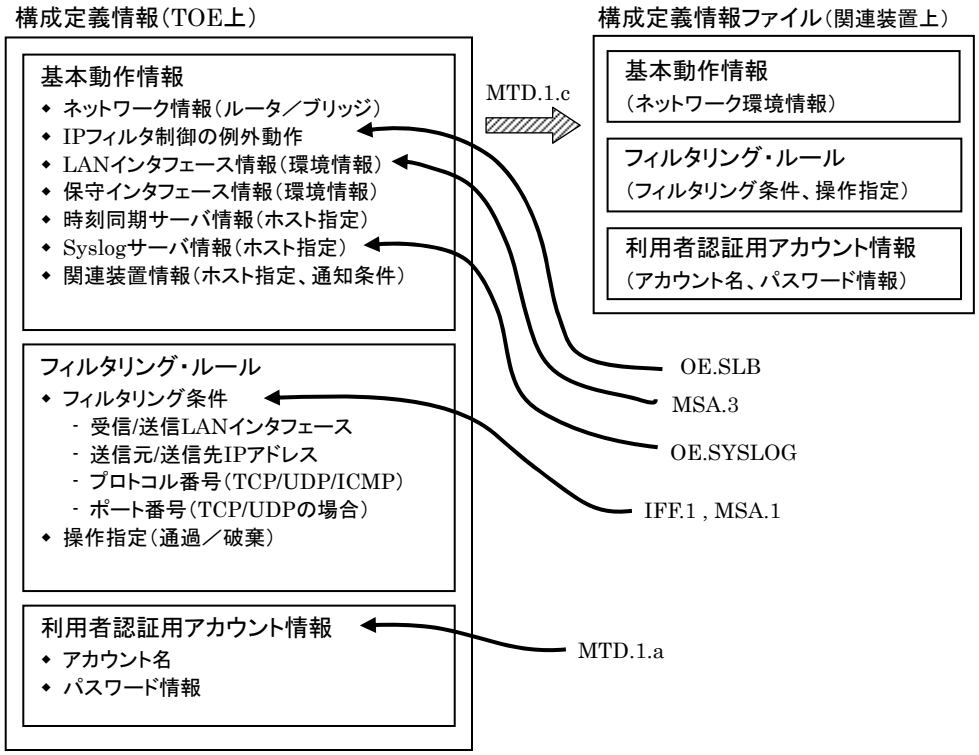
ここでは、本TOEが提供すべきセキュリティ機能を定義する。
表6-1は、各TOE要約仕様（実装する機能）とセキュリティ機能要件（必要とされる機能）の関係を示す。

表6-1 TOEセキュリティ機能とセキュリティ機能要件の対応関係

実装する仕様概要 / 機能要件	SF_ENV.1	SF_ENV.2	SF_ENV.3	SF_IPPF.1	SF_IPPF.2	SF_AUD.1	SF_AUD.2	SF_AUD.3
FAU_GEN.1	○	○		○	○	○		
FAU_STG.4						○		○
FDP_IFC.1				○	○			
FDP_IFF.1				○	○			
FIA_UAU.2	○							
FIA_UID.2	○							
FMT_MSA.1		○						
FMT_MSA.3		○						
FMT_MTD.1.a	○	○						
FMT_MTD.1.b	○					○	○	
FMT_MTD.1.c		○						
FMT_SMF.1	○	○	○					
FMT_SMR.1	○							
FPT_STM.1			○					

6.1.1 環境設定機能（SFP_ENV）

本TOEの動作環境を設定する機能を提供する。 TOE管理者だけが構成定義情報を改変（編集または設定復元）およびバックアップ可能とする。また、TOE監査者は構成定義情報の参照のみ可能とする。



6.1.1.1 利用者アカウント管理機能（SF_ENV.1）

SF_ENV.1.1：利用者アカウントの管理機能

本TOEでは、以下の利用者識別認証機能（アカウント管理）を提供する。利用者識別認証機能では、アカウント名とパスワード情報の両方を利用し、利用者識別と利用者認証を同時処理するPAP(Password Authentication Protocol)方式を実装する。また、TOE管理者に限り、通常モードと編集モードの2つの状態を定義し、編集モードのセキュリティ強化として、上記と同様の利用者認証機能を実装する。

表6-1-1　権限昇格状態と利用可能な管理者インタフェース

利用識別	状態管理	管理者インタフェース
TOE管理者	編集モード	構成定義情報（基本動作情報、フィルタリング・ルール、利用者認証用アカウント情報）の改変操作（リストアを含む）、削除操作および、バックアップ操作を許可する。 また、ロギング情報の初期化操作および退避操作を許可する。
	通常モード（接続直後）	構成定義情報（基本動作情報、フィルタリング・ルール）の参照操作を許可する。（改変操作は制限する）
TOE監査者	ー	

利用者アカウント管理機能では、TOE管理者として識別され、編集モードの状態になっている場合に限り、以下に列挙された利用者認証用アカウント情報の操作を許可する。

- TOE管理者のアカウント追加要求の場合、アカウント情報(パスワードを含む)を格納する。
- TOE監査者のアカウント追加要求の場合、アカウント情報(パスワードを含む)を格納する。
- TOE管理者のアカウント削除要求の場合、最後のTOE管理者であれば削除しない。
- TOE管理者のアカウント削除要求の場合、アカウント情報(パスワードを含む)を削除する。
- TOE監査者のアカウント削除要求の場合、アカウント情報(パスワードを含む)を削除する。
- TOE管理者のパスワード変更要求の場合、該当するアカウントのパスワード情報を更新する。
- TOE監査者のパスワード変更要求の場合、該当するアカウントのパスワード情報を更新する。

利用者アカウント管理機能では、TOE管理者として識別されていない場合、または、編集モードになっていない場合、利用者認証用アカウント情報の更新操作を拒否する。

SF_ENV.1.2:接続認証手順

本TOEに接続要求した場合、利用者識別機能および利用者認証機能により有効な利用者アカウントとパスワード情報の組み合わせであることを最初に確認する。接続認証完了後、認証されたアカウントの役割(TOE管理者やTOE監査者)を識別することで、接続認証失敗時の挙動が、アカウントの役割に依存しない構造にする。

SF_ENV.1.3:利用者認証時の監査記録

利用者認証時には、接続方法(telnet/http)または編集モードへの遷移コマンドの操作状況を含む監査事象を生成し、ロギング情報としてSF_AUD.1に記録を依頼する。

表6-1-2　利用者アカウント認証の監査記録(アカウントログ)

監査対象事象	監査記録のセキュリティ属性
ログイン成功(認証成功)	日時情報:発生日時 事象種類:情報(informational) 事象結果:ログイン受諾 サービス:telnet/http/編集モード(admin) 補助情報:利用者識別情報、保守端末のIPアドレス
ログイン拒否(認証失敗)	日時情報:発生日時 事象種類:警告(warning) 事象結果:ログイン拒否 サービス:telnet/http/編集モード(admin) 補助情報:利用者識別情報、保守端末のIPアドレス
ログアウト	日時情報:発生日時 事象種類:情報(informational) 事象結果:ログアウト サービス:telnet/http/編集モード(admin) 補助情報:利用者識別情報、保守端末のIPアドレス

6.1.1.2 環境設定機能 (SF_ENV.2)

SF_ENV.2.1:保守端末の設定

保守端末を物理的に接続する環境として、LANケーブル接続およびRS232C接続の保守インタフェースを提供する。この保守インタフェースでは、コマンド形式の操作コマンド処理と、コンソール形式の操作画面処理(RS232C接続を除く)を提供する。

表6-1-3　保守端末の管理者インタフェース

保守端末	設定体系	管理者インタフェース概要
VT100互換端末 (telnet通信または、 RS232C接続)	コマンド	設定コマンドと構成定義引数を指定することで、構成定義情報を更新することができるコマンドライン形式の設定インタフェースを提供する。
		保守インタフェースのIPアドレスを設定変更できる。
Webブラウザ端末 (http/https通信)	コンソール	設定項目を選択後、構成定義引数だけを指定することで、構成定義情報を更新することができるGUI形式の設定インタフェースを提供する。
		保守インタフェースのIPアドレス設定インタフェースを提供しない。(設定変更方法を提供しない)

TOEの導入開始時から運用中まで、保守インタフェースは常時利用可能として管理し、通信可能な状態を保持する。また、接続要求があった保守端末のIPアドレスが、保守インタフェースのIPセグメントに一致しない場合(運用管理専用ネットワークに保守端末が接続されている場合)、保守インタフェースではなく、IPフィルタ制御(SF_IPPF.1)に保守端末との通信処理を依頼する。

SF_ENV.2.2:環境設定手順(導入直後の初期設定)

本TOEの構成定義情報が存在しない場合(出荷初期状態の場合)、TOE管理者の利用者認証用アカウント情報を1つだけ自動作成する。 また、本TOEへの初回接続認証時に、自動作成したTOE管理者の利用者認証用アカウント情報に対する認証情報(パスワード情報)の設定を指導する。

SF_ENV.2.3:環境設定手順(通常設定)

SF_ENV.2.3.1:基本要素の設定

基本動作情報の設定操作を、TOE管理者に限り許可する。

IPフィルタ制御の 例外動作	IPフィルタ制御の例外動作の設定変更操作があった場合、構成定義情報の例外動作指定情報を更新する。(*1)
LANインタフェース	LANインタフェースに対して、有効化指定やIPアドレス割当て指定の設定変更操作があった場合、構成定義情報の該当情報を更新する。
保守インタフェース	保守インタフェースに対するIPアドレスの設定変更操作があった場合、構成定義情報の該当情報を更新する。
時刻同期サービス	信頼できる時刻同期サーバのホスト情報が設定された場合、構成定義情報の該当情報を更新する。
Syslogサービス	ロギング情報を転送するSyslogサーバのホスト情報が設定された場合、構成定義情報の該当情報を更新する。
イベント通知条件	ロギング情報を通知する関連装置のホスト情報と通知条件が設定された場合、構成定義情報の該当情報を更新する。

*1:IPフィルタ制御の例外動作のデフォルト値は「遮断」とする。但し、SLBモデルに関しては、「遮断」で運用することをガイダンスに明記する。

SF_ENV.2.3.2:フィルタリング条件の設定

フィルタリング・ルールの設定操作を、TOE管理者に限り許可する。 また、フィルタリング・ルールの参照操作をTOE管理者およびTOE監査者に限り許可する。

インタフェース	IPパケットデータを送受信するLANインタフェースを選択させ、フィルタリング・ルールの送信/受信インタフェース情報を更新する。なお、保守インタフェースは、この選択候補にしない。
フィルタリング条件	選択されたLANインタフェース(親)に対して、IPアドレスやポート番号などのフィルタリング条件(子)を1つまたは複数指定させ、フィルタリング・ルールのフィルタリング条件を追加または更新する。
操作指定	指定されたフィルタリング条件に対して、許可(通過)や禁止(破棄)の処理動作を指定させ、フィルタリング・ルールの操作指定を更新する。

SF_ENV.2.3.3:構成定義情報のバックアップとリストア

TOE管理者として識別されている場合、以下のバックアップ操作とリストア操作を許可する。

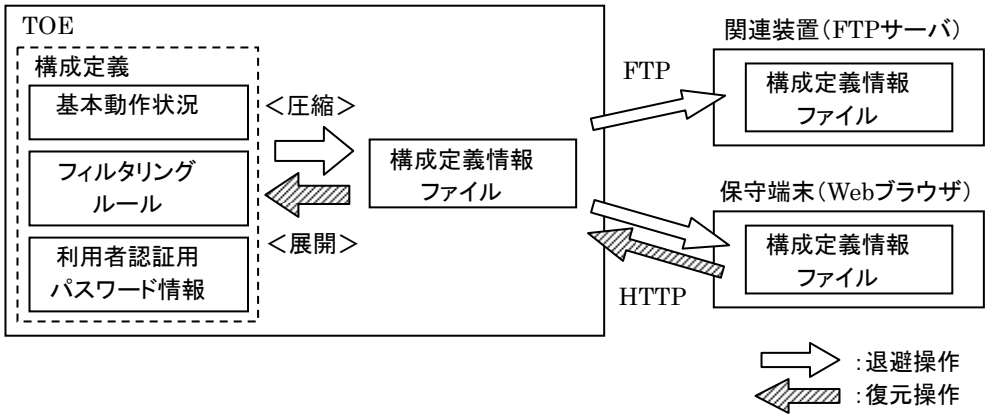
＜構成定義情報のバックアップ＞

- TOE上の基本動作情報、フィルタリング・ルールおよび、利用者認証用アカウント情報から、構成定義情報ファイルを生成し、関連装置(FTPサーバ)や保守端末(Webブラウザ)に移出(エクスポート)する。

＜構成定義情報のリストア＞

- 保守端末(Webブラウザ)に格納されている構成定義情報ファイルを、TOEに移入(アップロード)し、TOE上の構成定義情報(基本動作情報、フィルタリング・ルールおよび、利用者認証用アカウント情報)を削除後、アップロードした構成定義情報ファイルの内容に置き換える。

構成定義情報のバックアップおよびリストアは、以下のようなイメージで格納領域を管理する。



SF_ENV.2.4:環境設定更新の監査記録

TOEの環境設定更新操作時の処理結果として、以下のような監査事象を生成し、ロギング情報として SF_AUD.1に記録を依頼する。

表6-1-4-a　構成定義更新操作の監査記録(メッセージログ)

監査対象事象	監査記録のセキュリティ属性
ターミナルの初期化失敗	日時情報:発生日時 事象種類:警告(warning) 事象結果:ターミナルの初期化異常 補助情報:なし
Webコンソールサービスの開始失敗	日時情報:発生日時 事象種類:警告(warning) 事象結果:Webコンソールサービス開始異常 補助情報:なし
構成定義の更新成功(定義有効)	日時情報:発生日時 事象種類:情報(informational) 事象結果:配信正常完了 補助情報:なし
構成定義の更新拒否(更新失敗)	日時情報:発生日時 事象種類:重要(critical) 事象結果:配信失敗(従来定義での装置再起動) 補助情報:なし

表6-1-4-b　構成定義更新操作の監査記録(コマンドログ)

監査対象事象	監査記録のセキュリティ属性
フィルタリングルールのセキュリティ属性の改変	日時情報:発生日時 事象種類:情報(informational) 事象結果:設定変更 補助情報:フィルタリングルールのセキュリティ属性
IPフィルタ制御の例外動作の改変	日時情報:発生日時 事象種類:情報(informational) 事象結果:設定変更 補助情報:IPフィルタ制御の例外動作
利用者認証用アカウント情報の改変	日時情報:発生日時 事象種類:情報(informational) 事象結果:設定変更 補助情報:利用者認証用アカウント情報

6.1.1.3 時刻同期機能 (SF_ENV.3)

SF_ENV.3.1:日時の自動設定

NTP Version3 または NTP Version4 をサポートした時刻同期サーバ(NTPサーバ)に接続可能な時刻同期クライアント(NTPクライアント)機能を実装する。このNTPクライアント機能は、SF_ENV.2で設定され、構成定義情報に格納されているNTPサーバ情報を参照し、該当する時刻同期サーバ(NTPサーバ)に自動接続し、本TOEの時刻を定期的に自動補正するように実装する。

SF_ENV.3.2:時刻同期の監査記録

時刻同期機能の処理結果として、以下のような監査事象を生成し、ロギング情報としてSF_AUD.1に記録を依頼する。

表6-1-5　日時管理の監査記録(メッセージログ)

監査対象事象	監査記録のセキュリティ属性
時刻の手動設定	日時情報:発生日時 事象種類:情報(informational) 事象結果:時刻変更の通知 補助情報:変更前の時刻、変更後の時刻、利用者識別情報
時刻同期の開始	日時情報:発生日時 事象種類:情報(informational) 事象結果:時刻同期開始 補助情報:時刻同期サーバのホスト情報
時刻同期の成功	日時情報:発生日時 事象種類:情報(informational) 事象結果:時刻同期機能による時刻変更 補助情報:変更前の時刻、変更後の時刻
時刻同期の失敗	日時情報:発生日時 事象種類:エラー(error) 事象結果:時刻同期サーバとの通信エラー 補助情報:時刻同期サーバのホスト情報

6.1.2 IPパケットフィルタリング機能（SFP_IPPF）

6.1.2.1 IPフィルタ制御（SF_IPPF.1）

SF_IPPF.1.2：IPフィルタ制御のフィルタリング条件

IPフィルタ制御は、フィルタリング・ルールに格納されたフィルタリング条件に従って、IPパケットデータを通過または遮断する。通過または遮断は、以下のような処理で実装する。

- 受信LANインタフェースと、フィルタリング条件の受信LANインタフェースが一致するか評価する。
- 送信LANインタフェースと、フィルタリング条件の送信LANインタフェースが一致するか評価する。
- 送信元IPアドレス(ホスト、又はネットワーク)と、フィルタリング条件の送信元IPアドレス指定と一致するか評価する。
- 送信先IPアドレス(ホスト、又はネットワーク)と、フィルタリング条件の送信先IPアドレス指定と一致するか評価する。
- トランスポート層プロトコル(TCP、UDP、ICMP)番号が、フィルタリング条件のプロトコル(TCP、UDP、ICMP)指定と一致するか評価する。
- 送信元ポート番号(トランスポート層プロトコルがTCP、UDPの場合)が、フィルタリング条件のサービス(ポート番号)指定と一致するか評価する。
- 送信先ポート番号(トランスポート層プロトコルがTCP、UDPの場合)が、フィルタリング条件のサービス(ポート番号)指定と一致するか評価する。

上記の評価結果が「合致」と判定された場合、そのフィルタリング条件に合致する操作指定を確認し、以下の処理を実施する。

- 通過指定の場合、パケットデータおよび管理データを、その他のコンポーネント（TOE対象外）に中継する。また、パケット通過を意味するロギング情報を生成し、SF_AUD.1に記録依頼する。
- 遮断指定の場合、パケットデータおよび管理データを破棄する。また、パケット破棄を意味するロギング情報を生成し、SF_AUD.1に記録依頼する。

なお、TCPおよびUDPプロトコルの場合、ステートフル・インスペクション対応とし、通過指定と判定された通信コネクションを自動追従する。

SF_IPPF.1.3：IPフィルタ制御の例外動作

基本動作情報のIPフィルタ制御の例外動作が「パケット遮断」に設定されている場合、フィルタリング条件に合致しないIPパケットデータは、そのIPパケットデータを遮断(破棄)する。
基本動作情報のIPフィルタ制御の例外動作が「パケット通過」に設定されている場合、フィルタリング条件に合致しないIPパケットデータは、そのIPパケットデータの通過を許可する。
フィルタリング・ルールにフィルタリング条件が1つも存在しない場合、全てのIPパケットデータに対して、上記の例外動作を実行する。

SF_IPPF.1.4：IPフィルタ制御の通信デフォルト処理

基本動作情報にLANインタフェース情報が存在しない場合（初期化状態の場合）、SF_IPPF.2にパケット送受信のためのLANインタフェースを指定できないため、パケット受信をSF_IPPF.2に依頼しない。その結果、保守端末からの接続要求を含め、LANインタフェースを利用した一切の通信またはパケット中継が無条件に遮断される。

基本動作情報にLANインタフェース情報が登録され、SF_ENV.2から構成定義情報の更新適用が通知された時点で、パケット送受信のための管理インタフェースを指定し、SF_IPPF.2にパケット受信およびパケット送信を依頼する。

SF_IPPF.1.5:IPフィルタ制御の監査記録

IPパケット制御の処理結果として、TOE管理者がフィルタリング・ルールで記録すると設定したフィルタリング条件に限り、以下のような監査事象を生成し、ロギング情報としてSF_AUD.1に記録を依頼する。

表6-1-7　IPフィルタ制御の監査記録(セッションログ)

監査対象事象	監査記録のセキュリティ属性
TCP/IPパケット通過(許可)	日時情報:発生日時 事象種類:情報(informational) 事象結果:TCPコネクションの開始 補助情報:別表のコネクション情報
TCP/IPパケット破棄(禁止)	日時情報:発生日時 事象種類:警告(warning) 事象結果:TCPコネクションの拒否 補助情報:別表のコネクション情報
UDP/IPパケット通過(許可)	日時情報:発生日時 事象種類:情報(informational) 事象結果:UDPセッションの開始 補助情報:別表のコネクション情報
UDP/IPパケット破棄(禁止)	日時情報:発生日時 事象種類:警告(warning) 事象結果:UDPセッションの拒否 補助情報:別表のコネクション情報
IPパケット通過(許可)	日時情報:発生日時 事象種類:情報(informational) 事象結果:その他(ICMPを含む)のIPパケットの通過 補助情報:別表のコネクション情報
IPパケット破棄(禁止)	日時情報:発生日時 事象種類:警告(warning) 事象結果:その他(ICMPを含む)のIPパケットの拒否 補助情報:別表のコネクション情報

各監査事象には、以下のようなセキュリティ属性を付与する。

表6-1-8　コネクション情報ログのセキュリティ属性

監査事象区分	セキュリティ属性の拡張情報
TCPまたはUDPの場合	IPパケットデータを受信したLANインタフェース　または、 IPパケットデータを送信したLANインタフェース
	IPパケットデータの送信元IPアドレス
	IPパケットデータの送信先IPアドレス
	IPパケットデータのIPプロトコル情報(TCPまたはUDP)
	IPパケットデータの送信先ポート番号
	IPパケットデータの送信元ポート番号
ICMPの場合	IPパケットデータを受信したLANインタフェース　または、 IPパケットデータを送信したLANインタフェース
	IPパケットデータの送信元IPアドレス
	IPパケットデータの送信先IPアドレス
	IPパケットデータのIPプロトコル情報(ICMP)

6.1.2.2 LANドライバ機能 (SF_IPPF.2)

SF_IPPF.2.1:LANドライバ機能

LANドライバ機能は、以下のようなLANインタフェースを利用した通信制御処理インタフェースを提供する。

- LANインタフェース単位でのパケット受信
- LANインタフェース単位でのパケット送信
- LANインタフェース単位での故障検出及び動作モード制御

LANインタフェースの動作モードの初期値は、“使用せず(LinkDown)”とする。
また、LANインタフェースに対してパケット受信要求が来なければ、IPパケットデータは受信しない。

SF_IPPF.2.2:LANドライバの監査記録

LANインタフェースを管理するときの処理結果として、以下のような監査事象を生成し、ロギング情報として SF_AUD.1に記録を依頼する。

表6-1-9 LANインタフェースの監査記録(メッセージログ)

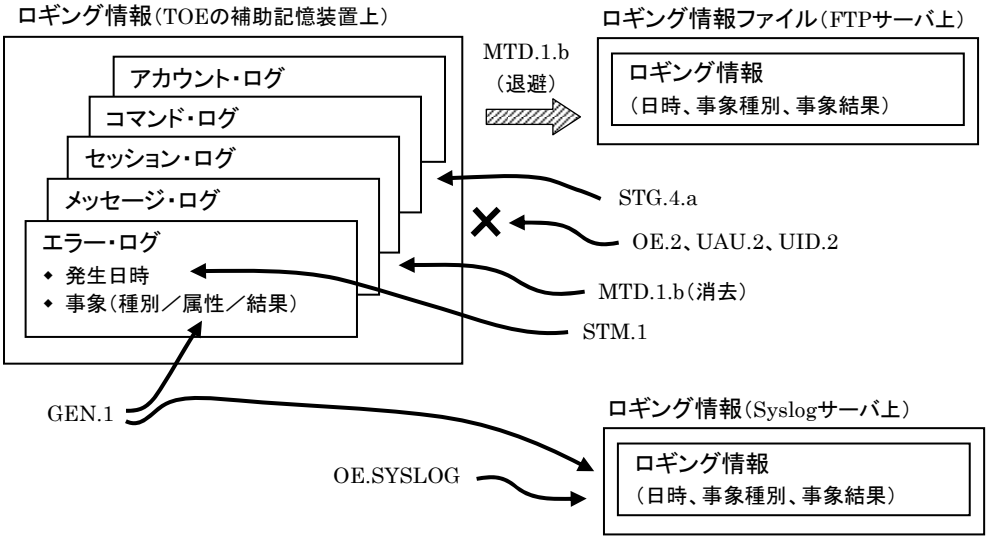
監査対象事象	監査記録のセキュリティ属性
LANインタフェースの正常検出	日時情報:発生日時 事象種類:情報(informational) 事象結果:LANインタフェース監視/正常状態への復帰 補助情報:LANインタフェース名
LANインタフェースの異常検出	日時情報:発生日時 事象種類:エラー(error) 事象結果:LANインタフェース監視/異常の検出 補助情報:LANインタフェース名

SF_IPPF.2.3:保守インタフェースとの排他管理

LANドライバ機能では、LANインタフェースだけを管理および制御し、保守インタフェースは管理および制御しない。

6.1.3 運用支援機能 (SFP_AUD)

本TOEのログイング情報(監査記録)を管理する機能を提供する。 この管理機能では、初期化操作と退避操作を提供し、TOE管理者だけに操作を許可する。



6.1.3.1 ログイング情報の管理機能 (SF_AUD.1)

SF_AUD.1.1:ログイング情報の種類

TOE上のコンポーネントから記録依頼されたログイング情報は、以下に列挙されたログイング情報に分類する。

- アカウントログ (最大10,000件程度保持)
  TOE管理者またはTOE監査者によるTOEへのログイン/ログアウト時刻を記録する。
- コマンドログ (最大1,000件程度保持)
  TOE管理者またはTOE監査者によるコマンド実行履歴を記録する。
- セッションログ (最大1,000,000件程度保持)
  IPパケットフィルタリング機能(TSF_IPPF)によるIPパケット処理結果(通過または遮断)を記録する。
- メッセージログ (最大10,000件程度保持)
  各TSFの起動時刻やその他の運用記録、各TSFが検出した異常イベントなどを記録する。
- エラーログ (最大100件程度保持)
  TOEのハードウェア装置に関連する異常イベントや故障イベントを記録する。

補助記憶装置(Option)が実装されている場合、記録依頼されたログイング情報を補助記憶装置(Option)に格納する。また、補助記憶装置(Option)が実装されていない場合、ログイング情報をTOE内に格納せずに、基本動作情報に設定されているSyslogサーバにログイング情報を転送する。

SF_AUD.1.2:ログイング機能の開始

ログイング機能は、TOE起動時に必須機能として自動起動するため、ログイング機能だけを再起動または停止することはできない。従って、ログイング機能の起動完了/停止確認は、TOE全体の起動/停止のイベントで代行する。また、後述のログイング情報の初期化時も、ログイング機能が一時停止することは無い。

ログイング情報を格納する補助記憶装置(Option)が実装されている環境で、ログイング機能の開始時に補助記憶装置の故障を検出した場合、本TOEを強制停止する。また、TOEの運用中に補助記憶装置の故障を検出した場合も、本TOEの運用を強制停止する。

SF_AUD.1.3:ロギング情報の初期化

TOE管理者(編集モード)の利用者認証が完了している場合、記録されたロギング情報の全消去操作を許可し、指定されたロギング情報が格納された領域を開放する。

SF_AUD.1.4:ロギング情報を記録するログファイルの管理

格納依頼されたロギング情報は、以下のような手順で格納制御する。

① 補助記憶装置(Option)が実装されている場合、補助記憶装置にロギング情報を格納する。
② 基本動作情報に関連装置(Syslogサーバ)への転送指定が存在すれば、該当装置に転送する。
③ 基本動作情報に関連装置(上記以外)へのイベント通知指定が存在すれば、SF_AUD.3を呼び出すことで、該当装置への転送を実現する。

なお、補助記憶装置(Option)の格納領域が満杯になった場合、以下のような上書き処理で格納管理する。

① 補助記憶装置のロギング情報格納領域は、数個の格納ブロックに分割管理しておく。
② 格納依頼時のロギング情報は、最新の格納ブロックに順次追加格納する。
③ 最新の格納ブロックが満杯になった場合、格納ブロック飽和のロギング情報を生成する。
④ 格納ブロック飽和事象は、SF_AUD.3(イベント通知機能)を利用して、TOE管理者に通知する。
⑤ 次の格納ブロックを獲得し、そのブロックを最新格納領域として、ロギング情報を格納する。
⑥ 全てのブロックが満杯になった場合、最古のブロックを破棄し、次のブロックとして再利用する。

SF_AUD.1.5:ロギング情報の監査記録

TOEの装置起動時およびロギング情報格納領域への管理操作時の処理結果として、以下のような監査事象を生成し、ロギング情報としてSF_AUD.1に記録を依頼する。

表6-1-10　ロギング情報の監査記録(メッセージログ)

監査対象事象	監査記録のセキュリティ属性
システムの正常起動(基本機能起動) *1	日時情報:発生日時 事象種類:情報(informational) 事象結果:システム起動(構成定義情報の配信) 補助情報:なし
システムの停止(通常停止操作)	日時情報:発生日時 事象種類:情報(informational) 事象結果:システム停止(装置停止指示完了) 補助情報:なし
ロギング情報格納領域の飽和通知	日時情報:発生日時 事象種類:情報(informational) 事象結果:ログファイルのローテーション通知 補助情報:なし

*1:正常起動時は、オプション機能を除き、機能単位(サービス単位)の起動監査事象を記録しない。

6.1.3.2 ロギング情報の退避機能 (SF_AUD.2)

TOE管理者(編集モード)として利用者認証が完了している場合、ロギング情報の退避を許可する。

SF_AUD.2.1:ロギング情報の退避

補助記憶装置(option)が実装されている場合、補助記憶装置(option)に記録された以下のロギング情報をブロック単位のロギング情報ファイルとして、関連装置に退避(エクスポート)することができる。

- アカウントログ(TOEへのログイン/ログアウト要求履歴)
- コマンドログ(TOE管理者またはTOE監査者によるコマンド実行履歴)
- セッションログ(通過または遮断のIPパケット処理結果)
- メッセージログ(TSF起動時刻、TSF運用記録、TSF異常検出記録、その他の異常発生記録)
- エラーログ(TOEのハードウェア装置に関連する異常発生記録や故障発生記録)

6.1.3.3 イベント通知機能 (SF_AUD.3)

SF_AUD.3.1:イベント通知

基本動作情報に関連装置へのイベント通知条件が設定されている場合、、記録依頼されたロギング情報がイベント通知条件に合致するか判定し、基準値に合致する場合、イベント通知条件の補助情報として設定されているMailサーバやSNMPマネージャにイベント通知する。 このイベント通知条件として、以下の条件判定機能を実装する。

- 事象種類(情報、警告、エラーの脅威重度で選択可能とする)
- 任意のロギング情報(例えば、管理ブロック飽和のロギング情報を個別指定可能とする)

SF_AUD.3.2:イベントの通知先

以下のようなイベント通知方法を実装する。

- RFC3164準拠形式でSyslogサーバに転送する。
- WELF形式(WebTrends Enhanced Log Format準拠)でSyslogサーバに転送する。
- 設定されたメールアカウント宛に、イベント毎(1件毎)でSMTPサーバに送信する。
- 設定されたメールアカウント宛に、数件をダイジェスト形式にまとめてSMTPサーバに送信する。
- SNMPマネージャに、イベント毎(1件毎)にSNMPトラップを発生させる。

6.2 保証手段

EAL1セキュリティ保証要件のコンポーネント及び各コンポーネントに対応する規約ドキュメントを以下に示す。

表6-2　セキュリティ保証要件の保証手段（EAL1）

クラス	コンポーネント名	保証手段
構成管理(ACM)	ACM_CAP.1	TOEの版数管理方法および、運用中TOEの版数確認方法は、以下のドキュメントに記載する。 - IPCOM EX1000/EX1200/EX2000 ソフトウェア説明書 - IPCOMEXの版数管理体系仕様書
配布と運用(ADO)	ADO_IGS.1	TOEを設置、生成、及び立上げるための要件（前提条件など）は、以下のドキュメントに記載する。 - IPCOM EX1000/EX1200/EX2000 取扱説明書 - IPCOM EX シリーズ 事例集 - IPCOM EX シリーズ ユーザーズガイド
開発(ADV)	ADV_FSP.1	TOEセキュリティ機能要件は、以下のドキュメントに詳細化する。 - ファイアウォール実装説明書 - IPCOM EX1000/EX1200/EX2000 ソフトウェア説明書 - IPCOM EX1000/1200/2000 基本設計書 ファイアウォール機能編 - IPCOM EX シリーズ E10L10 NTP 機能仕様書 - IPCOM EX シリーズ ユーザーズガイド - IPCOM EX シリーズ コマンド リファレンス ガイド - IPCOM EX シリーズ コンソール リファレンス ガイド - IPCOM EX シリーズ 保守ガイド
	ADV_RCR.1	仕様詳細化に関するドキュメントは、以下に記載する。 - ファイアウォール実装説明書
ガイダンス(AGD)	AGD_ADM.1	本TOEを構成し、保守し、管理する方法は、以下の管理者ガイダンスに記載する。 - IPCOM EX1000/EX1200/EX2000 ソフトウェア説明書 - IPCOM EX1000/EX1200/EX2000 取扱説明書 - IPCOM EX シリーズ 事例集 - IPCOM EX シリーズ 保守ガイド - IPCOM EX シリーズ ユーザーズガイド - IPCOM EX シリーズ コマンド リファレンス ガイド - IPCOM EX シリーズ コンソール リファレンス ガイド
	AGD_USR.1	利用者ガイダンスに記載すべき特機事項が無いため、保証要件としてのドキュメントは無い。
テスト(ATE)	ATE_IND.1	追加検証作業のための評価機器(ハードウェア)及び、関連機器(関連サーバ)を貸与する。

第7章　PP主張

7.1 PP参照

参照するPPはない。

7.2 PP修整

修整するPPはない。

7.3 PP追加

追加するPPはない。

第8章　根拠

本STの評価に使う論理的正当性の証拠を検証している。

8.1 セキュリティ対策方針根拠

以下に、“3. TOEセキュリティ環境”に示した、想定、脅威等に対して、“4. セキュリティ対策方針”に示した対策が有効であることを検証する。

8.1.1 脅威・前提条件に対抗するセキュリティ対策方針の説明

表8-1　セキュリティ対策方針と対抗する脅威及び前提条件

セキュリティ対策方針（第4章）	TOEのセキュリティ環境（第3章）									
	脅威		前提条件							
	T1	T2	ASM.1	ASM.2	ASM.3	ASM.4	ASM.6	ASM.8	ASM.SYSLOG	ASM.SLB
O.AC	○									
O.ADMIN		○								
O.AUDREC	○	○								
OE.1						○				
OE.2			○				○			
OE.3					○					
OE.6				○						
OE.11							○			
OE.12								○		
OE.SYSLOG									○	
OE.AUDVIEW	○	○								
OE.SLB										○

各脅威に対し、攻撃者を明示し、攻撃者が行う想定される攻撃方法を分析する。次に、攻撃方法に対抗するための有効な対策内容を示し、それがすべて満たされることで脅威に対抗できる十分な対策であることを示す。なお、対策内容は、一つ以上のセキュリティ対策方針がそれを満たし、脅威に対するセキュリティ対策方針として必要であることを示す。

T1（外部ネットワークから内部ネットワークへの不正アクセス）

この脅威は、外部ネットワーク上の攻撃者によって実行される。このような攻撃者がとり得る具体的な内部ネットワークへの脅威を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 利用を許可されていない者が、内部ネットワーク資産を利用しようとする。

許可されない内部ネットワークへの接続要求を制限することで対抗できる。 この対抗策に該当するセキュリティ対策方針は、O.ACである。

b. 利用を許可されていない者が、内部ネットワークを無作為に探索し、不正にアクセスしようとする。

この攻撃に対しては、許可されていない内部ネットワークへの接続要求を検出することが有効である。TOEで発生した事象についての正確な時刻に裏づけされた記録を採取し、その監査記録の中から不正アクセスの可能性をTOE管理者またはTOE監査者が確認した場合、TOEの保護のための適切な事前処置を促す。この対抗策に該当する、記録の採取と通知に関するセキュリティ対策方針はO.AUDRECであり、記録の参照に関する環境セキュリティ対策方針はOE.AUDVIEWである。また、TOE保護の責務に関する環境セキュリティ対策方針はOE.1である。

上記の a、bの攻撃方法に対抗することは、T1に対抗することである。 従って、それぞれの攻撃方法に対する対抗策として該当する O.AC、O.AUDREC、OE.1、OE.AUDVIEWによって、T1に対抗できる。

T2（TOEへの不正アクセスによるTOE関連資産の改ざん）

この脅威は、TOE管理者およびTOE監査者以外の攻撃者によって実行される。このような攻撃者がとり得る具体的なTOE関連資産の改ざん方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 利用を許可されていない者が、利用を許可されている者になりすまし、関連資産を改ざんする。

この攻撃に対しては、TOEの利用において識別認証を行い、TOEの利用を正当な者のみに制限することにより対抗できる。この対抗策に該当するセキュリティ対策方針は、O.ADMINである。

b. 正当な識別認証情報を不正に取得する。

aの対抗策が有効に働くためには、識別認証に用いられる情報を管理し、不正利用による利用許可者へのなりすましを防止する必要がある。識別認証情報の不正取得の方法は、TOE管理者またはTOE監査者からの取得と、攻撃者による類推の2種類がある。
正当なTOE管理者またはTOE監査者からの識別認証情報の取得、及び類推による識別認証情報の取得については、TOE管理者またはTOE監査者に対して認証情報の決定方法（認証情報を他人に教えない。認証情報は推測・類推されにくいものにする。認証情報は適切な間隔で変更する。）を教育することで対抗できる。この対抗策に該当する環境セキュリティ対策方針は、OE.3である。
また、関連装置に退避する構成定義情報やロギング情報の漏洩による識別認証情報の取得については、構成定義情報やロギング情報の通知経路および、退避先関連装置への不正アクセスを制限することで対抗できる。この対抗策に該当する環境セキュリティ対策方針は、OE.2、OE.11である。

c. 利用を許可されていない者が、識別認証を総当りで探索し、不正にアクセスしようとする。

この攻撃に対しては、許可されている識別認証を探索している操作を検出することが有効である。TOEで発生した事象についての正確な時刻に裏づけされた記録を採取し、その記録の中から攻撃の可能性を検知した時、その結果をTOEの保護に責務がある者に通知することにより、TOEの保護のための適切な事前処置を促す。この対抗策に該当する、記録の採取と通知に関するセキュリティ対策方針はO.AUDRECであり、記録の参照に関する環境セキュリティ対策方針はOE.AUDVIEWである。また、TOE保護の責務に関する環境セキュリティ対策方針はOE.1である。

上記の a、b、cの攻撃方法に対抗することは、T2に対抗することである。 従って、それぞれの攻撃方法に対する対抗策として該当する O.ADMIN、O.AUDREC、OE.1、OE.2、OE.3、OE.11、OE.AUDVIEWによって、T2に対抗できる。

ASM.1（物理的アクセス）

ASM.1は、TOEを動作させるハードウェア装置および保守端末は物理的に不正アクセスできない前提条件である。 これに対し、対策方針OE.2に従い、TOEを動作させるハードウェア装置および保守端末を施錠付き収納ラックやサーバ専用室に設置することで不正アクセスできなくなり、前提条件を実現できる。

ASM.2（接続形態）

ASM.2は、内部ネットワークと外部ネットワークを唯一の接点で接続する前提条件である。 これに対し、対策方針OE.6に従い、外部ネットワークと内部ネットワークを唯一の接続点としてネットワークを構築することで、TOEが唯一の接点となり、前提条件を実現できる。

ASM.3（信頼できるTOE管理者）

ASM.3は、TOE管理者およびTOE監査者は不正をしない前提条件である。 これに対し、対策方針OE.3に従い、システム運用管理部門の責任者により、不正のない運用管理ができるように教育することで、TOE管理者およびTOE監査者は不正をしないため、前提条件を実現できる。

ASM.4（TOEの構成の管理）

ASM.4は、TOE管理者は正しくTOEを運用管理する前提条件である。 これに対し、対策方針OE.1に従い、TOE管理者は、内部セキュリティポリシーに従った運用管理にすることで、TOEを正しく運用管理できるため、前提条件を実現できる。

ASM.6（データ漏洩不可）

ASM.6は、関連装置および運用管理専用ネットワークからTOE関連資産となるデータは漏洩しない前提条件である。 これに対し、対策方針OE.2に従い、関連装置や運用管理専用ネットワークを施錠付き収納ラックやサーバ専用室に設置することで、物理的な不正アクセスによる情報漏洩ができない。また、対策方針OE.11に従い、外部ネットワークや内部ネットワークを運用管理専用ネットワークと通信できない設定にすることで、論理的な通信手段による漏洩や流出ができないため、前提条件を実現できる。

ASM.8（時刻同期サーバ）

ASM.8は、時刻同期サーバは信用できる前提条件である。 これに対し、対策方針OE.12に従い、TOE管理者は時刻同期サーバに信頼できるNTPサーバを指定することで、時刻同期サーバは信頼できるため、前提条件を実現できる。

ASM.SYSLOG（ロギング情報）

ASM.SYSLOGは、TOEに補助記憶装置(Option)を実装するか、Syslogサーバを設置する前提条件である。これに対し、対策方針OE.SYSLOG従い、TOEが動作するハードウェアに補助記憶装置(Option)を実装するか、ロギング情報の維持監視機能を持つSyslogサーバを設置することで、前提条件を実現できる。

ASM.SLB（SLBモデル）

ASM.SLBは、IPフィルタ制御の例外動作を制限的(遮断)で運用する前提条件である。 これに対し、対策方針OE.SLBに従い、TOE管理者はIPフィルタ制御の例外動作に「パケット遮断」を指定することで、パケットフィルタ条件に合致しないIPパケットデータが破棄されるため、前提条件を実現できる。

8.2 セキュリティ要件根拠

以下では、“4. セキュリティ対策方針”に対して、“5. ITセキュリティ要件”に示した機能要件が有効であることを検証する。

8.2.1 セキュリティ機能要件の根拠

以下に、セキュリティ要件と機能要件との関係性について検証する。

表8-2　セキュリティ機能用件と対策方針

機能要件	セキュリティ対策方針		
	O.AC	O.ADMIN	O.AUDREC
FAU_GEN.1			○
FAU_STG.4			○
FDP_IFC.1	○		
FDP_IFF.1	○		
FIA_UAU.2		○	○
FIA_UID.2		○	○
FMT_MSA.1		○	
FMT_MSA.3		○	
FMT_MTD.1.a		○	
FMT_MTD.1.b		○	○
FMT_MTD.1.c		○	
FMT_SMF.1		○	
FMT_SMR.1		○	○
FPT_STM.1			○

O.AC

このTOEセキュリティ対策方針は、攻撃者による内部ネットワークへの侵入防止を求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 受信したIPパケットデータを識別する。

外部ネットワークから受信したIPパケットデータを解析し、受信LANインタフェース、接続元IPアドレス、接続先IPアドレス、接続元ポート番号、接続先ポート番号などのセキュリティ情報を識別する。この要件に該当するセキュリティ機能要件は、FDP_IFC.1、FDP_IFF.1である。

b. 通過許可されないIPパケットデータを破棄する。

識別されたIPパケットデータが、内部ネットワークへの許可されない通信要求の場合、IPパケットデータを破棄(遮断)する。この要件に該当するセキュリティ機能要件は、FDP_IFC.1、FDP_IFF.1である。

上記の全ての対策を満たすことは、O.ACを満たすことである。従って、それぞれの対策に必要な機能要件として該当する FDP_IFC.1、FDP_IFF.1の達成により、O.ACを実現できる。

O.ADMIN

このTOEセキュリティ対策方針は、環境設定操作が許可された管理者だけに制限されることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 管理者を識別認証する。

構成定義情報への許可利用者を識別するため、正当に許可されたTOE管理者またはTOE監査者であることを識別認証し、TOEへの接続処理中は、識別認証状態を維持しなければならない。この要件に該当するセキュリティ機能要件は、FIA_UAU.2、FIA_UID.2、FMT_SMR.1である。 また、TOEの動作に影響を及ぼす設定について、管理する権限を持つ者を制限した上で、セキュリティ機能の使用状況を管理しなければならない。この要件に該当するセキュリティ機能要件は、FMT_SMF.1である。

b. パスワード情報の更新操作を管理者だけに許可する。

パスワード情報の更新操作を含む、利用者アカウント情報の登録、更新、削除操作は、TOE管理者だけ許可し、他の利用者は制限しなければならない。この要件に該当するセキュリティ機能要件は、FMT_MTD1.aである。

c. 構成定義情報の更新操作や参照操作を管理者に許可する。

構成定義情報の更新操作および復旧操作は、TOE管理者だけ許可し、構成定義情報の参照操作は、TOE管理者とTOE監査者に許可する。他の利用者は構成定義情報へのアクセスを制限しなければならない。この要件に該当するセキュリティ機能要件は、FMT_MSA.1である。また、TOEの動作を決定するフィルタリング・ルールに対する例外動作の更新操作は、TOE管理者だけ許可し、他の利用者は制限しなければならない。この要件に該当するセキュリティ機能要件は、前者は、FMT_MSA.3である。

d. 構成定義情報のバックアップを管理者だけに許可する。

構成定義情報のバックアップ操作は、TOE管理者だけ許可し、他の利用者は制限しなければならない。この要件に該当するセキュリティ機能要件は、FMT_MTD1.cである。

e. ロギング情報ファイルの初期化操作および退避操作を管理者だけに許可する。

監査記録の改ざんを防止するため、ロギング情報ファイルの初期化操作および退避操作は、TOE管理者だけに制限されなければならない。この要件に該当するセキュリティ機能要件は、FMT_MTD.1.bである。

上記の全ての対策を満たすことは、O.ADMINを満たすことである。 従って、それぞれの対策に必要な機能要件として該当する FIA_UAU.2、FIA_UID.2、FMT_MSA.1、FMT_MSA.3、FMT_MTD1.a、FMT_MTD.1.b、FMT_MTD1.c、FMT_SMF.1、FMT_SMR.1の達成により、O.ADMINを実現できる。

O.AUDREC

このTOEセキュリティ対策方針は、監査記録操作が許可された管理者だけに制限されることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 監査記録を管理する。

外部ネットワークからの不正アクセス(T1)に関する監査記録と、TOEへの不正アクセス(T2)に関する監査記録は、基本的な監査記録レベルで、不正アクセス状況を監査できる。ただし、外部ネットワークからの不正アクセスに関しては、不正アクセスの兆候を詳細に分析可能とするため、詳細レベルの監視記録が要求される。この要件に該当するセキュリティ機能要件は、FAU_GEN.1である。なお、FAU_GEN.1で記録される監査対象事象において、以下の監査記録は、以下の理由で基本レベルの監査記録を要求しない。

FMT_SMF.1	TOE管理者の識別認証の監査記録(アカウントログ)で代行できるため、管理機能の使用状況監査は不要である。
FMT_MTD.1.b	TOE管理者だけが消去操作可能であり、かつ、OE.3の環境セキュリティ対策方針によりTOE管理者は不正をしないため、管理機能の使用状況監査は不要である。

b. 監査記録を管理者だけが退避可能とする。

TOE管理者として識別された場合、過去の監査記録の退避を許可する。この要件に該当するセキュリティ機能要件は、FIA_UAU.2、FIA_UID.2、FMT_SMR.1である。

c. 監査記録が消失しないように保護する。

過去の不正アクセス発生事象を保持するため、監査記録に対する不正な改ざんを防止しなければならない。また、格納領域破損や格納領域飽和が発生した場合でも、過去の監査記録を保護する機能を実装しなければならない。この要件に該当するセキュリティ機能要件は、前者はOE.2、FIA_UAU.2、FIA_UID.2、FMT_MTD.1bであり、後者はFAU_STG.4である。

d. 監査記録の事象発生時刻を正確に管理する。

不正アクセス事象の発生日時を正確に監査するため、正確な日時情報を管理しなければならない。この要件に該当するセキュリティ機能要件は、FPT_STM.1である。

上記の全ての対策を満たすことは、O. AUDRECを満たすことである。 従って、それぞれの対策に必要な機能要件として該当する FAU_GEN.1、FAU_STG.4、FIA_UAU.2、FIA_UID.2、FMT_MTD.1b、FMT_SMR.1、FPT_STM.1の達成により、O.AUDRECを実現できる。

8.2.2 セキュリティ機能要件の依存性

以下に、セキュリティ要件の依存性について検証する。

表8-3　セキュリティ機能要件の依存性

STコンポーネント		CCパート2で規定されている依存コンポーネント	TOE			
項番	項目		参照	TOEの依存コンポーネント	依存関係が満たされないコンポーネント	妥当性
1	FAU_GEN.1	FPT_STM.1	15	FPT_STM.1	なし	
5a	FAU_STG.4	FAU_STG.1	4	なし	FAU_STG.1	OK
6	FDP_IFC.1	FDP_IFF.1	7	FDP_IFF.1	なし	
7	FDP_IFF.1	FDP_IFC.1	6	FDP_IFC.1	なし	
		FMT_MSA.3	11	FMT_MSA.3	なし	
8	FIA_UAU.2	FIA_UID.1	ー	なし	FIA_UID.1	OK
9	FIA_UID.2	なし	ー	なし	なし	
10	FMT_MSA.1	FDP_IFC.1 または、FDP_ACC.1	6	FDP_IFC.1	なし	
		FMT_SMF.1	13	FMT_SMF.1	なし	
		FMT_SMR.1	14	FMT_SMR.1	なし	
11	FMT_MSA.3	FMT_MSA.1	10	FMT_MSA.1	なし	
		FMT_SMR.1	14	FMT_SMR.1	なし	
12a	FMT_MTD.1a	FMT_SMF.1	13	FMT_SMF.1	なし	
		FMT_SMR.1	14	FMT_SMR.1	なし	
12b	FMT_MTD.1b	FMT_SMF.1	13	FMT_SMF.1	なし	
		FMT_SMR.1	14	FMT_SMR.1	なし	
12c	FMT_MTD.1c	FMT_SMF.1	13	FMT_SMF.1	なし	
		FMT_SMR.1	14	FMT_SMR.1	なし	
13	FMT_SMF.1	なし	ー	なし	なし	
14	FMT_SMR.1	FIA_UID.1	ー	なし	FIA_UID.1	OK
15	FPT_STM.1	なし	ー	なし	なし	

FMT_SMR.1および、FIA_UAU.2の依存関係は満足されていないが、FIA_UAU.1の上位階層となるFIA_UID.2が存在するため、依存関係は妥当であると考える。

FAU_STG.4の依存関係は満足されていないが、FAU_STG.1に該当する監査記録の不正削除の脅威は、OE.2により物理的な不正アクセス保護と、FIA_UAU.2およびFIA_UID.2の論理的な不正アクセス保護により防止できるため、依存関係は妥当であると考える。

8.2.3 セキュリティ機能要件の相互補完性

前節より、TOEセキュリティ機能要件は、それぞれと依存関係のある機能要件と相互補完している。これらの機能要件以外で、明示的な依存関係はないが、セキュリティ対策方針で防御を提供している観点を列挙し、相互補完する機能要件について検証する。

表8-4　セキュリティ機能要件の相互補完性

機能要件	防御を提供している要件		
	認証や通信の バイパス防止	対策方針の 非活性化防止	TSFデータの 干渉防止
FAU_GEN.1	N/A	N/A	N/A
FAU_STG.4	N/A	N/A	N/A
FDP_IFC.1	N/A	N/A	N/A
FDP_IFF.1	N/A	N/A	N/A
FIA_UAU.2	N/A	N/A	N/A
FIA_UID.2	N/A	N/A	N/A
FMT_MSA.1	N/A	N/A	N/A
FMT_MSA.3	N/A	N/A	N/A
FMT_MTD.1.a	N/A	N/A	N/A
FMT_MTD.1.b	N/A	N/A	N/A
FMT_MTD.1.c	N/A	N/A	N/A
FMT_SMF.1	N/A	N/A	N/A
FMT_SMR.1	N/A	N/A	N/A
FPT_STM.1	N/A	N/A	N/A

N/A : Not Applicable

認証や通信のバイパス防止

N/A (FPT_RMV.1)

セキュリティ対策方針からの相互作用は無い。なお、本TOEと同居可能なコンポーネントは、同居における動作検証が実施された同時提供コンポーネントだけであるため、TOE内において、認証や通信のバイパスに関する脅威は存在しない。

対策方針の非活性防止

N/A

セキュリティ対策方針からの相互作用は無い。なお、情報フロー制御SFPを実現するFDP_IFC.1およびFDP_IFF.1の機能は、TOEのLANインタフェースと関連付けられ、IPパケットデータの送受信時に必ず呼び出されるため、FDP_IFC.1およびFDP_IFF.1の機能が非活性化されることは無い。また、考慮外の事態で、FDP_IFC.1およびFDP_IFF.1の非活性化状態が発生した場合でも、全通信遮断により、外部ネットワークの脅威から内部ネットワーク資産は保護される。従って、TOE内において、対策方針の非活性化に関する脅威は存在しない。

TSFデータの干渉(破壊)防止

N/A (FPT_SEP.1)

セキュリティ対策方針からの相互作用は無い。なお、本TOEと同居可能なコンポーネントは、同居における動作検証が実施された同時提供コンポーネントだけであるため、TOE内において、TSFデータの干渉（破壊）に関する脅威は存在しない。

8.2.4 セキュリティ保証要件の根拠

顧客要件（産業競争力のための情報基盤強化税制の創設）に対応するため、EAL1の品質保証レベルを保証する。

8.3 TOE要約仕様根拠

8.3.1 セキュリティ機能の根拠

第6.1節 TOEセキュリティ機能の表6-1で示したように、各TOEセキュリティ機能が1つ以上のセキュリティ機能要件に対応している。次に、各セキュリティ機能要件が、TOEセキュリティ機能により実現できることを説明する。

FAU_GEN.1

FAU_GEN.1は監査に関する要件で、SFP_ENV、SFP_IPPF、SFP_AUDで生成した監査記録をSFP_AUDで記録することで実現する。FAU_GEN.1の内容に関しては、監査機能の起動と終了、監査基本レベルの監査対象事象、ファイルタ制御のセキュリティ属性を元に監査記録を生成、記録する要件である。監査機能の起動と終了に関しては、SF_AUD.1.2によりTOE起動時に必須機能として起動するためTOE全体の起動/停止で確認でき、そのTOE全体の起動/停止はSF_AUD.1.5で監査を生成する。監査基本レベルの監査対象事象については、SF_ENV.1.3、SF_ENV.2.4で識別認証や構成定義情報の改変、SF_IPPF1.5でIPパケットデータの通過/破棄、SF_AUD.1.5で格納ブロック満杯や格納領域故障検出のロギング情報を生成する。ファイルタ制御のセキュリティ属性はSF_IPPF1.5、SF_IPPF.2.2で生成する。これらの監査事象は、事象の発生日時、種別、結果等を付随して生成し、SF_AUD.1.1で記録する。従って、SF_ENV.1.3、SF_ENV.2.4、SF_IPPF1.5、SF_IPPF2.2、SF_AUD.1.1、SF_AUD.1.2、SF_AUD.1.5の実装により、FAU_GEN.1を実現できる。

FAU_STG.4

FAU_STG.4は、補助記憶装置(Option)が実装されている環境における、補助記憶装置(Option)が故障したときのアクションと、監査証跡が満杯になったときのアクションの規定が要求される。SF_AUD.1.2は、ロギング情報格納領域の装置故障を検出した場合、TOEによる運用を強制停止する。SF_AUD.1.4は、ロギング情報格納領域の飽和事象が発生した場合、TOE管理者への事前警告が通知され、警告放置時は上書きとして最新のロギング情報が保持される。また、SF_AUD.3は、TOE管理者への通知方法を選択できる。これを実装することで、FAU_STG.4を実現できる。従って、SF_AUD.1.2、SF_AUD.1.4および、SF_AUD.3の実装により、FAU_STG.4を実現できる。

FDP_IFC.1

FDP_IFC.1は、適用可能な操作のサブセットに対し、識別された各情報フロー制御SFPが適切なものであることを要求する。SF_IPPF.1.2およびSF_IPPF.2は、設定されたファイルタリング・ルールに従った不正なIPパケットデータの破棄操作を実行する。これを実装することで、FDP_IFC.1を実現できる。従って、SF_IPPF.1.2および、SF_IPPF.2の実装により、FDP_IFC.1を実現できる。

FDP_IFF.1

FDP_IFF.1は、単純セキュリティ属性は、情報とその情報を流したり受け取ったりするサブジェクトにおけるセキュリティ属性を要求する。SF_IPPF.1.2およびSF_IPPF.2は、設定されたファイルタリング・ルールに従った不正なIPパケットデータの破棄操作を実行する。これを実装することで、FDP_IFF.1を実現できる。従って、SF_IPPF.1.2および、SF_IPPF.2の実装により、FDP_IFF.1を実現できる。

FIA_UAU.2

FIA_UAU.2は、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、利用者に認証が成功することを要求する。SF_ENV.1.1およびSF_ENV.1.2で採用するPAP方式の識別認証機能は、アカウント名とパスワードの組み合わせを一括認証するため、利用者認証前に使用者識別するような調停アクションは存在しない。これを実装することで、FIA_UAU.2を実現できる。従って、SF_ENV.1.1およびSF_ENV.1.2の実装により、FIA_UAU.2を実現できる。

FIA_UID.2

FIA_UID.2は、管理者を代行する他のTSF調停アクションを許可する前に、管理者に自分自身を識別することを要求する。SF_ENV.1.1およびSF_ENV.1.2により、TOE管理者およびTOE監査者の識別認証を行い、自分自身の識別を終えることにより、その他のアクションの開始が許可される。これを実装することで、FIA_UID.2を実現できる。従って、SF_ENV.1.1およびSF_ENV.1.2の実装により、FIA_UID.2を実現できる。

FMT_MSA.1

FMT_MSA.1は、セキュリティ属性の管理が許可された利用者に制限されることを要求する。SF_ENV.2.3.2は、

ファイルタリング条件の設定操作がTOE管理者に限定され、参照操作がTOE管理者とTOE監査者に限定される。これを実装することで、FMT_MSA.1を実現できる。従って、SF_ENV.2.3.2の実装により、FMT_MSA.1を実現できる。

FMT_MSA.3

FMT_MSA.3は、ファイアウォール製品としての適切なデフォルト値を要求する。SF_ENV.2.3は、IPフィルタ制御の例外動作の設定変更操作がTOE管理者に限定され、そのデフォルト値を「パケット遮断」とする。ただし、TOEを動作させるハードウェア装置がSLBモデルの場合、セキュリティ対策方針OE.SLBに従い、管理者ガイダンスでIPフィルタ制御の例外動作を「パケット遮断」に初期設定することを指導するため、ファイアウォール製品としての適切なデフォルト値が設定される。なお、TOEを動作させるハードウェア装置がSLBモデルの場合でも、SF_ENV.2.3でLANインタフェース情報の設定が完了するまで、LANインタフェースからIPパケットデータを受信することが無いため、TOE装置としてのセキュリティは確保される。これらを実装することで、FMT_MSA.3を実現できる。 従って、SF_ENV.2.3の実装とOE.SLBの対処実施により、FMT_MSA.3を実現できる。

FMT_MTD.1.a

FMT_MTD.1.aは、利用者認証用アカウント情報に対する改変操作を許可された者のみに制限することを要求する。SF_ENV.1.1はアカウント名やパスワード情報の改変操作が、SF_ENV.2.3.3は利用者認証用アカウント情報の復旧操作が、TOE管理者だけに許可される。これを実装することで、FMT_MTD.1.aを実現できる。従って、SF_ENV.1.1および、SF_ENV.2.3.3の実装により、FMT_MTD.1.aを実現できる。

FMT_MTD.1.b

FMT_MTD.1.bは、ロギング情報の消去操作および退避操作を許可された者のみに制限することを要求する。SF_ENV.1は、許可利用者がTOE管理者であることを識別する。SF_AUD.1.3は、ロギング情報の初期化操作がTOE管理者だけに許可される。また、SF_AUD.2は、補助記憶装置（Option）に格納されたロギング情報の退避操作がTOE管理者だけに許可される。これらを実装することで、FMT_MTD.1.bを実現できる。従って、SF_ENV.1、SF_AUD.1.3および、SF_AUD.2の実装により、FMT_MTD.1.bを実現できる。

FMT_MTD.1.c

FMT_MTD.1.cは、構成定義情報（基本動作情報、フィルタリング・ルール、利用者認証用アカウント情報）に対するバックアップ操作を許可された者のみに制限することを要求する。SF_ENV.2.3.3は、構成定義情報のバックアップ操作がTOE管理者だけに許可される。これを実装することで、FMT_MTD.1.cを実現できる。従って、SF_ENV.2.3.3の実装により、FMT_MTD.1.cを実現できる。

FMT_SMF.1

FMT_SMF.1は、セキュリティ管理機能を提供することを要求する。SF_ENV.1は、利用者識別認証処理を管理し、SF_ENV.2.3は、IPフィルタ制御の例外動作を管理する。また、SF_ENV.3は、時刻補正状況を管理する。これを実装することで、FMT_SMF.1で定義された管理要件を実現できる。従って、SF_ENV.1、SF_ENV.2.3および、SF_ENV.3の実装により、FMT_SMF.1を実現できる。

FMT_SMR.1

FMT_SMR.1は、認識するセキュリティに関する役割の特定を要求する。SF_ENV.1は、TOE管理者とTOE監査者の役割を識別し、維持管理する。これを実装することで、FMT_SMR.1を実現できる。従って、SF_ENV.1の実装により、FMT_SMR.1を実現できる。

FPT_STM.1

FPT_STM.1は、高信頼タイムスタンプを提供することを要求する。SF_ENV.3は、信頼された時刻同期サーバを利用し、定期的に時刻を自動補正できる。これを実装することで、FPT_STM.1を実現できる。従って、SF_ENV.3の実装により、FPT_STM.1を実現できる。

8.3.2 セキュリティ機能強度の根拠

セキュリティ機能強度の規定は無い。

8.3.3 セキュリティ保証手段の根拠

表6-2に示すように、すべてのTOEセキュリティ保証要件は “6.2 保証手段” により示されたドキュメントのセットによって対応付けられる。また、“6.2 保証手段” に示されたドキュメントによって、本STが規定した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。