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
セキュリティ ターゲット

2011年 9月 12日

バージョン: 2.1

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	2011.04.26	初版作成	初版
1.1	2011.05.27	記述内容変更	1.4.2、1.4.3、1.4.4章一部修正、第7章全般修正
1.2	2011.06.07	ASE001-01指摘対応	全般修正
1.3	2011.06.15	キックオフミーティング結果反映、ASE001-02指摘対応	全般修正、図修正
1.4	2011.06.20	指摘対応	全般修正
1.5	2011.0621	指摘対応	全般修正
1.6	2011.06.22	指摘対応	6章修正
1.7	2011.06.23	指摘対応	6章、7章修正
1.8	2011.06.27	指摘対応	6章、7章修正
1.9	2011.07.20	指摘対応	STタイトル訂正、1章、6章、7章修正
2.0	2011.08.10	指摘対応	TOEバージョン訂正、1章修正
2.1	2011.09.12	記述内容変更	1章ガイダンス版数修正

目次

図表目次

第1章　ST概説

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1 ST 参照

本節では、ST の識別情報を記述する。

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 セキュリティ ターゲット
バージョン	2.1
発行日	2011年 9月 12日
作成者	富士通株式会社

1.2 TOE 参照

本節ではTOE の識別情報を記述する。
TOE は、IPCOM EX シリーズとして動作する。TOE は以下の TOE 名とバージョンで識別する。

TOE 名	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	V 2.0.01
開発者	富士通株式会社

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（show system information）を実行することで確認できる。

1.3 TOE 概要

1.3.1 TOE 種別および主要セキュリティ機能

1.3.1.1 TOE の種別

TOE は、IP パケットデータを中継制御する IT 製品である統合型ネットワークサーバ（INS：Integrated Network Server）のファームウェアの内の、ファイアーウォールモジュール（IPパケットフィルタリング機能）である。

1.3.1.2 TOE が提供する機能

表 1 に TOE が提供する機能を記述する。

表 1　TOE が提供するセキュリティ機能

TOE が提供する機能
・IP パケットフィルタリング（ファイアーウォール）機能 ・環境設定管理機能 ・運用支援管理機能（監査記録管理機能）

1.3.1.3 TOE の使用法と主要セキュリティ機能

TOE の主な使用法とセキュリティを以下に示す。

(1) IP パケットフィルタリング（ファイアーウォール）機能
INS が中継する IP パケットデータを事前に定められたファイアーウォールの規則（IP パケットのフィルタリングルール）に則って、破棄、または通過させる。

(2) 環境設定管理機能
システム管理者端末から識別および認証されたシステム管理者が、TOE のセキュリティ機能に関する本TOE の構成設定の参照、および変更をシステム管理者、またはシステム監視者が行えるようにする機能である。

(3) 運用支援管理機能（監査記録管理機能）
本TOE が処理したIPパケットデータの破棄や通過のパケット処理記録や構成設定の設定データの変更や操作などのイベント（ロギング情報）を追跡記録（監査記録）するための機能である。

1.3.2 TOE 利用環境

本 TOE は、ネットワーク上を流れる IP パケットデータを中継する IT 製品として、外部ネットワークと内部ネットワークの境界上に設置して内部ネットワークを外部ネットワークの脅威から保護する利用を想定している。また運用管理専用ネットワークにより本 TOE の管理用ネットワークとして接続し、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利用する。
TOE の想定する利用環境を図 1 に記述する。

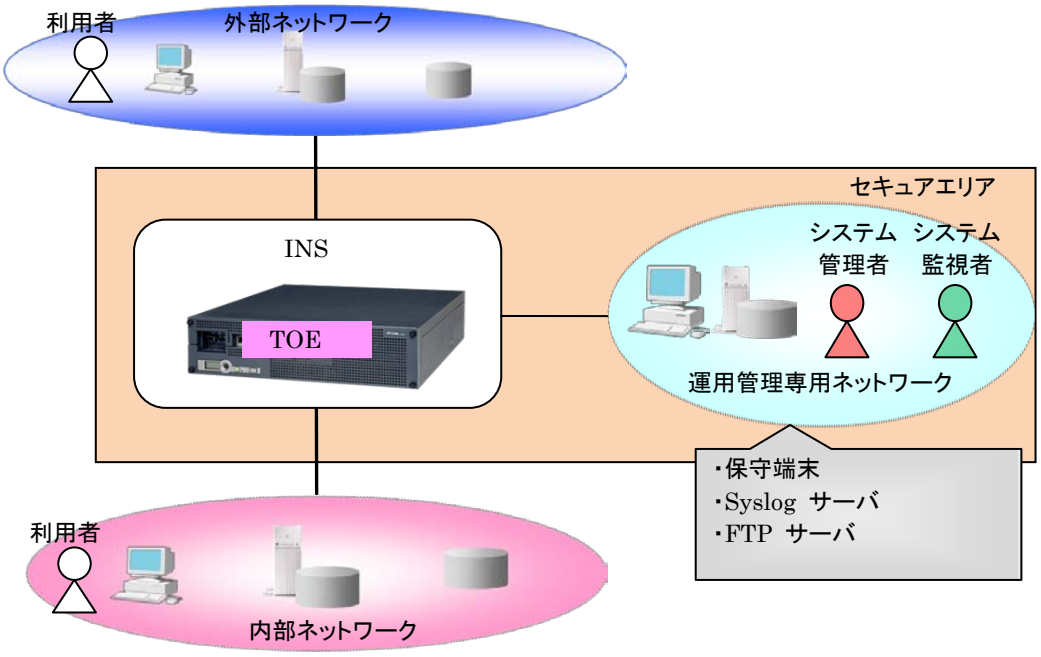

図 1 TOE 想定する利用環境

1.3.3 TOE 以外のハードウェア構成とソフトウェア構成

図 1 に示す利用環境の中で TOE は、コントローラファームウェアであり、下記の TOE 以外のハードウェアが存在する。

(1) INS 本体
INS は、コントローラボード、LAN インターフェース、不揮発性メモリ、補助記憶装置(Option)から構成され、INS 機能を提供するユーザーインターフェース、IP パケットデータ通信を中継するためのハードウェアを有する。

(2) 保守端末
ハードウェアは、汎用の PC であり、Telnet ソフトウェア 、または Web ブラウザ、またはシリアルインターフェース(RS232C) 接続した VT100 互換ソフトウェアを使用して TOE に対して TOE 構成設定データの参照や変更を行うことができる。

(3) Syslog サーバ
ハードウェア/OS は、汎用の PC、またはサーバであり、TOE は、ネットワーク管理プロトコルを用いて、Syslog サーバに TOE のロギング情報の送信を行う。

(4) FTP サーバ
ハードウェア/OS は、汎用のPC、またはサーバであり、TOE は、FTP プロトコルを用いて、FTP サーバに TOE の設定データ(構成設定情報ファイル)の送信を行う。

(5) 利用者端末
利用者が使用する装置については、特に限定されない。一般のPCやサーバ、ネットワーク機器などが行う通信が対象となる。

1.3.3.1 ハードウェア構成(INS 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。ハードウェア、ソフトウェア(ファームウェア)それぞれ独立した製品体系化されており、ハードウェアとソフトウェア(ファームウェア)を一体化した製品として提供される。装置概要を表 2 に、ファームウェアプラットフォームの依存仕様概要を表 3 に記述する。

富士通 IPCOM EXシリーズ

- ハードウェアプラットフォーム
  - IPCOM EX 1100
  - IPCOM EX 1300
  - IPCOM EX 2000A
  - IPCOM EX 2500
- ソフトウェア(ファームウェア)プラットフォーム
  - SC (セキュリティ シリーズ)
  - NW (ネットワーク シリーズ)
  - IN (システムフロント シリーズ)
  - LB (サーバロードバランス シリーズ)

表 2 TOE のハードウェアプラットフォーム概要(基本実装)

ハードウェアプラットフォーム 装置概要	EX 1100	EX 1300	EX 2000A		EX 2500
			標準	電源二重化	
保守インターフェース (LAN)	1	1	1		1
保守インターフェース (RS232C)	1	1	1		1
通信用 LAN インターフェース 標準	4	4	4		0
通信用 LAN インターフェース 最大 (Option搭載時)	4	4	12		20
不揮発性メモリ	○	○	○		○
導入用記憶装置	○	○	○		○
補助記憶装置 (標準/Option)	○	○	○		○
電源二重化(標準/Option)	−	−	−	○	○(*)
システムクロック(内部時計)	○	○	○		○

(*)EX2500 は、Option で電源二重化が搭載される。

シリーズ 装置概要	EX1100			EX1300			EX2000A				EX2500			
	SC	NW	LB	SC	NW	LB	SC	NW	IN	LB	SC	NW	IN	LB
補助記憶装置 (標準/Option)	Op	Op	標準	Op	Op	標準	Op	Op	標準	標準	Op	Op	標準	標準

*1:補助記憶装置(標準/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: IN/LBシリーズでは標準で、補助記憶装置が搭載される。

表 3 TOE ソフトウェアプラットフォーム概要(依存仕様)

ソフトウェアプラットフォーム 装置仕様概要	SC	NW	IN	LB
IP パケットフィルタ制御の例外動作 (設定定義のデフォルト値)	パケット拒否	パケット拒否	パケット拒否	パケット通過

パケットフィルタリング条件に合致しない場合の処置概要(例外動作は、設定定義でパケット拒否、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)。

1.3.3.2 ソフトウェア構成(TOE 対象外機能)

本 TOE 外の機能として、以下のコンポーネントが提供される。

- サーバ負荷分散
- QoS 制御(帯域制御)
- リンク負荷分散

- IPS
- Web アプリケーション・ファイアーウォール (WAF)
- プロキシ
- Web コンテンツ・フィルタリング
- アンチウィルス
- アドレス変換
- 証明書管理
- IPsec-VPN
- L2TP/IPsec
- SSL アクセラレーター
- SSL-VPN
- VPN タグマッピング
- HTTP コンテンツ圧縮
- FNA ルーティング
- ネットワークサービス
- 二重化制御
- 経路制御

1.3.3.3 保守端末(Webブラウザ)

保守端末で利用可能なWebブラウザを次に示す。

- Internet Explorer 6 (SP1,SP2,SP3)
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

1.4 TOE 記述

本章では、TOE の利用者役割、TOE の論理的範囲、および物理的範囲について記述する。

1.4.1 TOE 関連の利用者役割

本ST で、TOE に対して想定する利用者役割を表 4 に記述する。

表 4　TOE が想定する利用者役割

関連者	内容説明
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 を使用して運用する組織の責任者および管理者、監視者が所属する組織。
システム管理者 （管理者権限）	TOE の設置～運用～監視～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 の構成設定情報を設定し、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システム管理者に該当する。
システム監視者 （オペレーター権限）	TOE の運用～監視を担い、システム管理者を補佐する副管理者。システム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　の構成設定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システム監視者に該当する。
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、およ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。

1.4.2 TOE の論理的範囲

TOE の論理的範囲は、本 INS が中継する通信パケットのファイアーウォール処理を行う IP パケットフィルタリング機能（**TSF_IPPF**）、および IP パケットフィルタ制御や本 INS が動作するための動作環境の設定を行う環境設定管理機能（**TSF_ENV**）、IP パケットフィルタ制御や環境設定操作などの動作結果となる監査記録を処理する運用支援管理機能（**TSF_AUDT**）のコンポーネントである。
図 2 に TOE の論理的構成を記述する。

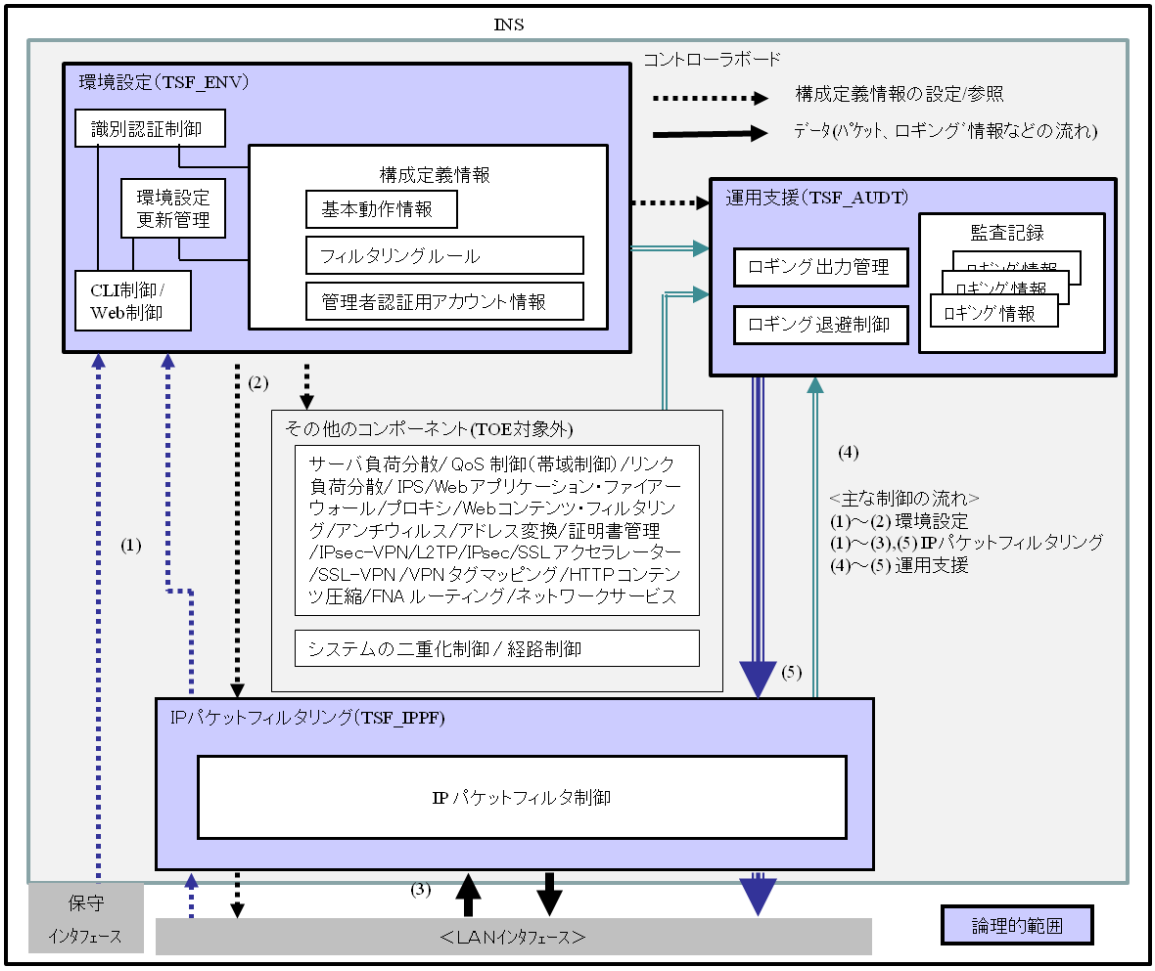

図 2 INS 内の TOE 論理的範囲

1.4.2.1 TOE が提供するセキュリティ機能

TOE は、利用者が行う通信に対して、INS が中継するネットワーク上の IP パケットデータをシステム管理者によって事前に定められたファイアーウォール（IP パケットフィルタリング）の規則（ルール）に則って、破棄、または通過させる機能を提供する。

(1) IP パケットフィルタリング（TSF_IPPF）

TSF_IPPF は、複数のLANインター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 インター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 インター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 インターフェースを利用して、IP パケットデータを送信する。

- IP パケットフィルタ制御
  LAN インターフェースから通知された 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 インターフェースに送信を指示する。

(2) 環境設定管理機能（TSF_ENV）

TSF_ENV は、TOE の動作環境を設定する機能を提供する。保守インターフェースか、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 インター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 システム管理者であれば、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、および Web 制御
  TOE を動作させるハードウェア装置の保守インターフェース（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。保守端末からの接続要求後、識別認証制御を利用し、システム管理者、またはシステム監視者であるかを識別検証する。なお、本制御部では、システム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、システム管理者やシステム監視者を識別する。

- 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）
  - 管理者認証用アカウント情報（システム管理者やシステム監視者のアカウント名やパスワード情報）

(3) 運用支援管理機能（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 の補助記憶装置に格納、または、指定された手段で監査記録を関連装置 Syslog サーバに転送する。 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、全消去が許可される。なお、監査記録を関連装置 Syslog サーバに転送する場合も、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(関連装置 Syslog サーバ宛ての通信を許可)していなければならない。

- ロギング出力管理
  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、関連装置 Syslog サーバ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、補助記憶装置に格納後、関連装置 Syslog サーバにもイベント転送する。

● ロギング退避制御
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。

1.4.3 TOE の物理的範囲

本 TOE の物理的範囲は、INSのコントローラボード上で動作するファームウェアが対象である。ファームウェアは、セキュリティコンポーネントとその他のコンポーネントがある。
TOE セキュリティコンポーネントやその他コンポーネントは、コントローラボードと内部インターフェースで接続されている LAN インターフェースや保守インターフェースを経由して外部ネットワークや内部ネットワーク、および運用管理専用ネットワークと接続され、ファイアーウォール（IP パケットフィルタリング）機能や TOE の動作環境を設定する環境設定管理機能、およびその他コンポーネントの機能を実現する。またファイアーウォール（IP パケットフィルタリング）機能や環境設定管理機能などの動作結果となる監査記録を処理する運用管理支援機能は、内部インターフェースで接続されている補助記録装置、または LAN インターフェース経由で Syslog サーバに格納する。
図 3 に TOE の物理的範囲を記述する。

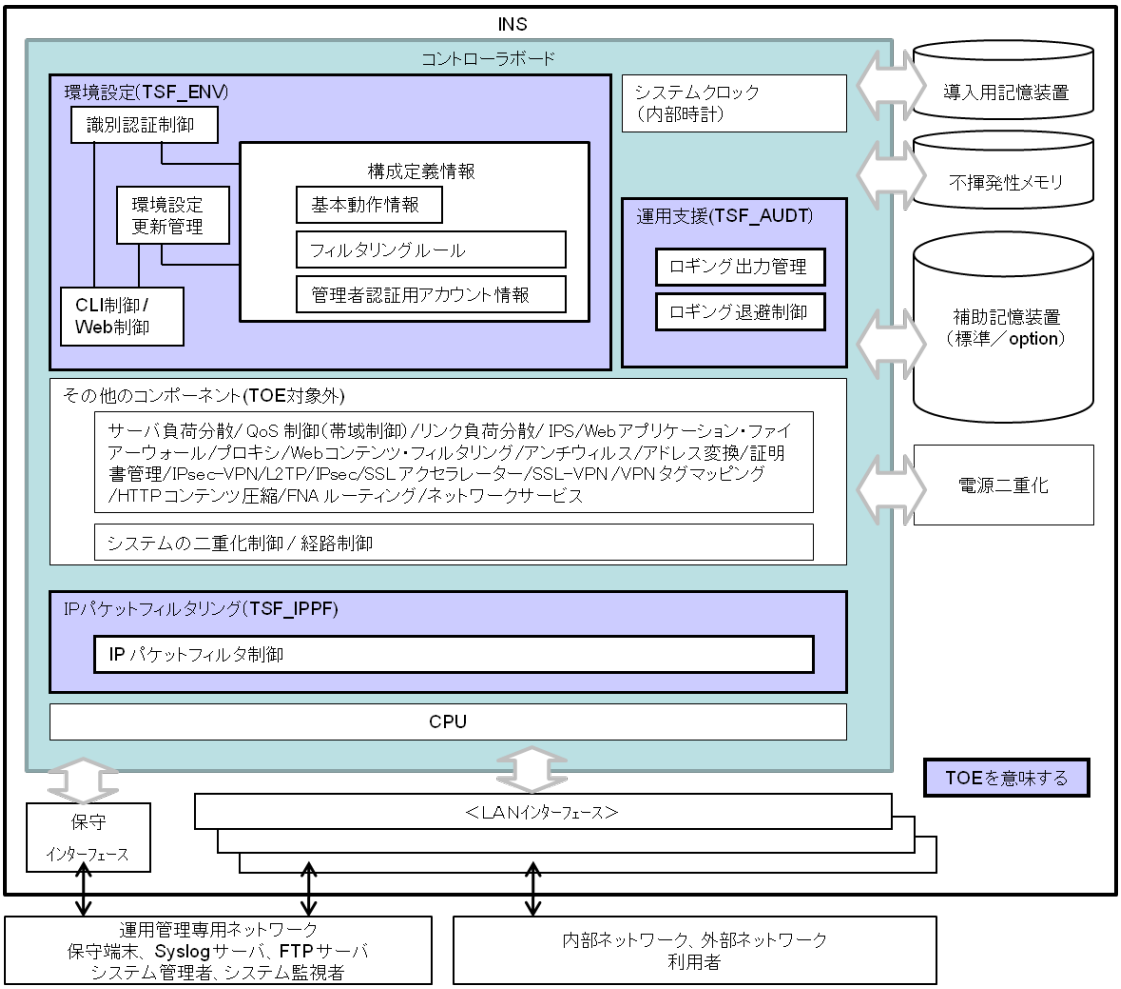

図 3 INS 内の TOE物理的範囲

1.4.4 ガイダンス

本 TOE を構成するガイダンス文書は、以下のとおりである。

ガイダンス文書名	版数
IPCOM EX シリーズ マニュアル体系と読み方	初版
IPCOM EX1100/EX1300 クイックスタートガイド(*)	Rev.1
IPCOM EX2000A（電源二重化タイプを除く）クイックスタートガイド(*)	Rev.1
IPCOM EX2000A（電源二重化タイプ）クイックスタートガイド(*)	Rev.1
IPCOM EX2500 クイックスタートガイド(*)	Rev.1
IPCOM EX1100/EX1300/EX2000A/EX2500 取扱説明書	初版
IPCOM EX シリーズ ユーザーズガイド	初版
IPCOM EX シリーズ 事例集	初版
IPCOM EX シリーズ コンソールリファレンスガイド	初版
IPCOM EX シリーズ コマンドリファレンスガイド	初版
IPCOM EX シリーズ 保守ガイド	初版
IPCOM EX1100/EX1300/EX2000A/EX2500 ソフトウェア説明書	2011年 9月

*クイックスタートガイドは、ハードウェアプラットフォームの機種により、対象のクイックスタートガイドが提供される。

第2章　適合主張

2.1 CC 適合主張

本 ST および TOE のCC適合主張は、以下のとおりである。
ST と TOE が適合を主張する CC のバージョン:

パート1: 概説と一般モデル 2009 年7 月 バージョン3.1 改訂第3 版 最終版 翻訳第1 版
パート2: セキュリティ機能コンポーネント 2009 年7 月 バージョン3.1 改訂第3 版 最終版 翻訳第1 版
パート3: セキュリティ保証コンポーネント 2009 年7 月 バージョン3.1 改訂第3 版 最終版 翻訳第1 版

CC パート2 に対するST の適合: CC パート2 適合
CC パート3 に対するST の適合: CC パート3 適合

2.2 PP主張

本 ST が適合している PP はない。

2.3 パッケージ主張

本 ST は、パッケージ EAL1 追加である。
EAL1 追加（EAL1+）コンポーネントは、ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1

2.4 適合根拠

本 ST は、PP 適合を主張しないので、PP 適合根拠はない。

第3章　セキュリティ課題定義

3.1 脅威

3.1.1 TOE 資産

本TOE が保護する資産は、以下のとおりである（図 4）。

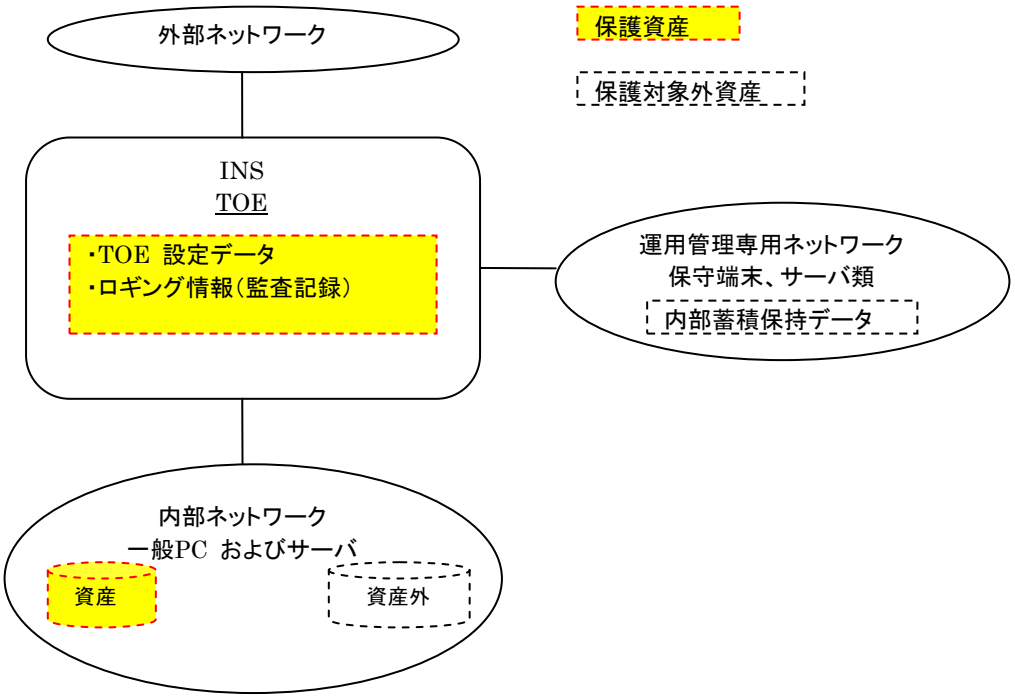

図 4　保護資産と保障対象外資産

(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。この定められた範囲が保護資産とする。

(2)　TOE 設定データ（構成設定情報）
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、TOE内に保存される（表 5）。この構成定義情報を保守端末などに退避した場合は、以下のファイル構成となり、退避時点の管理者用アカウント、パスワード情報も含まれる（図 5）。

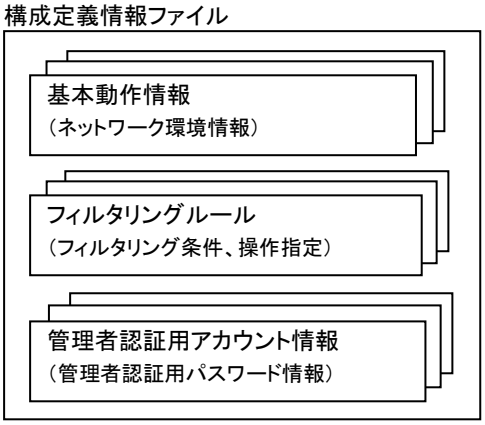

図 5　TOE 設定データ（構成定義情報ファイル）

(3)　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、または関連装置 Syslog サーバに格納される。
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 Syslog サーバにイベント情報を転送、または関連装置 FTP サーバに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。

注）内部ネットワーク資産に定められた保護資産であっても本 TOE を経由した場合にのみ保護対象となり、本 TOE を経由しない場合は、保護対象とはならない。運用管理ネットワークについても内部ネットワーク資産と同様に保護対象として内部ネットワークポリシーで定められる。

表 5 に TOE 設定データを記述する。

表 5　TOE 設定データ項目分類

TOE 設定データ項目分類（注）
INS 基本動作情報（ネットワーク環境情報）
ファイアーウォール（IP パケットフィルタリング）機能情報（フィルタリングルール、操作指定）
管理者認証用アカウント情報（システム管理者、およびシステム監視者アカウント、パスワード）

3.1.2 脅威

本 TOE に対する脅威を、表 6 に記述する。攻撃者は、低レベルの攻撃能力をもつものであり、TOE の動作について公開されている情報知識を持っていると想定する。

表 6 脅威

脅威（識別子）	内容説明
T.ATTK	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、外部ネットワークから内部ネットワーク上のサーバ(IP アドレス)やアプリケーション(ポート番号)などへの不正アクセスにより、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、または漏洩を図る恐れがある。
T.CNFD	TOE への不正アクセスによる TOE 関連資産の改ざん 外部ネットワーク上の攻撃者は、本 TOE に侵入、または盗聴し、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。内部ネットワーク上の利用者は、誤って構成定義情報やロギング情報の変更や消去を行う恐れがある。

3.2 組織のセキュリティ方針

本 TOE が順守しなければならない組織のセキュリティ方針はない。

3.3 前提条件

本 TOE の動作、運用、および利用に関する前提条件を、表 7 に記述する。

表 7 前提条件

前提条件 （識別子）	内容説明
物理的な信頼	
A.DACC	物理的アクセス 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、FTP サーバ）は、物理的に不正アクセスできない。
A.CNCT	接続形態 本 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。
A.SYSLOG	ロギング情報 ロギング情報を格納する補助記憶装置を TOE が動作するハードウェアに実装するか、ロギング情報の維持監視機能を持つ関連装置 Syslog サーバなどを設置する。
人的な信頼	
A.ADMN	信頼できる システム管理者 システム管理者およびシステム監視者は、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。
A.SSET	TOE の構成の管理 システム管理者は、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、TOE の構成定義情報を運用管理しなければならない。
A.SMRL	データ漏洩不可 関連装置（Syslog サーバ、FTP サーバ）、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。
A.SLB	**LB シリーズの設定** IP パケットフィルタ制御の例外動作は、制限的（拒否）で運用する。
A.TMM	時刻設定 システム管理者は、本 TOE が動作するハードウェア装置に実装されたシステムクロック（内部時計）にシステム運用に先立ち時刻を設定しなければならない。

第4章　セキュリティ対策方針

本章では、TOE セキュリティ対策方針、運用環境のセキュリティ対策方針、およびセキュリティ対策方針根拠について記述する。

4.1 TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表 8 に記述する。

表 8　TOE セキュリティ対策方針

セキュリティ対策方針（識別子）	詳細内容
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	システム管理者制御 TOE は、システム管理者およびシステム監視者だけがその動作環境の制御を行うことができるよう、システム管理者およびシステム監視者の 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 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を表 9 に記述する。

表 9 運用環境のセキュリティ対策方針

セキュリティ対策方針（識別子）	詳細内容
OE.PLCY	TOE の構成の管理 システム管理者は、内部セキュリティポリシーに従って、TOE、TOE を動作させるハードウェア装置、TOE の構成定義情報を管理、運用しなければならない。
OE.SECA	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、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、システム管理者が施錠可能な収納ラックやシステム管理者やシステム監視者だけが出入りできるセキュアなエリアに設置することで、物理的に保護しなければならない。
OE.MGR	システム管理者の教育 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、システム管理者およびシステム監視者を教育しなければならない。

OE.CNCT	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.NMG	運用管理専用ネットワークの管理 システム管理者は、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。システム管理者、システム監視者は、運用管理専用ネットワークから TOE 設定や監視を行わなければならない。システム管理者、システム監視者は、運用管理専用ネットワークから TOE 設定情報や関連装置（Syslog サーバや FTP サーバ）のデータを内部セキュリティポリシーに従って、持ち出さない。
OE.SYSLOG	ロギング情報の保持 システム管理者は、TOE が動作するハードウェアに補助記憶装置を実装するか、ロギング情報の維持監視機能を持つ Syslog サーバなどを設置する。
OE.AUDVIEW	ロギング情報の監査 システム管理者は、TOE が動作するハードウェア上に補助記憶装置が実装されていた場合、補助記憶装置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。また、関連装置である Syslog サーバへのイベント通知が指定されていた場合、Syslog サーバに格納されたロギング情報を Syslog サーバの機能で監査（参照）する。
OE.SLB	LB シリーズの設定 システム管理者は、IP パケットフィルタ制御の例外動作を制限的（拒否）に設定しなければならない。
OE.TMM	時刻設定 システム管理者は、本 TOE に時刻を設定しなければならない。

4.3 セキュリティ対策方針根拠

セキュリティ対策は、セキュリティ課題定義で規定した前提条件に対応するもの、あるいは脅威に対抗するため、あるいは組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対応する前提条件、対抗する脅威、実現する組織のセキュリティ方針の対応関係を表 10 に示す。また各セキュリティ課題定義がセキュリティ対策方針により保証されていることを表 11 に記述する。
表中の「✓」は、対応関係にあることを示す。

表 10 セキュリティ対策方針とセキュリティ課題定義の対応関係

セキュリティ課題定義 / セキュリティ対策方針	脅威		前提条件							
	T.ATTK	T.CNFD	A.DACC	A.CNCT	A.SYSLOG	A.ADMN	A.SSET	A.SMRL	A.SLB	A.TMM
O.AC	✓									
O.ADMIN		✓								
O.AUDREC	✓	✓								
OE.PLCY	✓	✓					✓			
OE.SECA			✓					✓		
OE.MGR		✓				✓				
OE.CNCT				✓						
OE.NMG		✓						✓		
OE.SYSLOG					✓					
OE.AUDVIEW	✓	✓								
OE.SLB									✓	
OE.TMM										✓

表 11 セキュリティ課題定義に対応するセキュリティ対策方針根拠

セキュリティ課題定義	セキュリティ対策方針根拠
T.ATTK	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システム管理者またはシステム監視者が確認した場合、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.PLCY である。 上記の a、bの攻撃方法に対抗することは、T.ATTK 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.PLCY、OE.AUDVIEW によって、T.ATTK に対抗できる。

T.CNFD	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、システム管理者、およびシステム監視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(盗聴)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、システム管理者またはシステム監視者からの取得と、攻撃者による類推の 2 種類がある。 正当なシステム管理者、またはシステム監視者からの識別認証情報の取得、および類推による識別認証情報の取得については、システム管理者、またはシステム監視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.MGR** である。また、不正に情報を取得させないために、システム管理者、およびシステム監視者は、運用管理専用ネットワークからのみ TOE の設定や監視を行うことにより盗聴に対抗できる。この対抗策に該当する環境セキュリティ対策方針は、**OE.NMG** 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(攻撃者への警告や該当通信の遮断)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.PLCY** である。 上記の a、b、c の攻撃方法に対抗することは、**T.CNFD** 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.PLCY**、**OE.MGR**、**OE.NMG**、**OE.AUDVIEW** によって、**T.CNFD** に対抗できる。
A.DACC	物理的アクセス **A.DACC** は、TOE を動作させるハードウェア装置、および保守端末、関連装置(Syslog サーバ、FTP サーバ)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.SECA** 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、関連装置(Syslog サーバ、FTP サーバ)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。
A.CNCT	接続形態 **A.CNCT** 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.CNCT** 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。
A.SYSLOG	ロギング情報 **A.SYSLOG** は、TOE が動作するハードウェアに補助記憶装置を実装するか、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** に従い、TOE が動作するハードウェアに補助記憶装置を実装するか、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。
A.ADMN	信頼できるシステム管理者

	A.ADMN は、システム管理者およびシステム監視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.MGR** 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、システム管理者およびシステム監視者は不正をしないため、前提条件を実現できる。
A.SSET	TOE の構成の管理 **A.SSET** は、システム管理者は正しく 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.PLCY** に従い、システム管理者は、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。
A.SMRL	データ漏洩不可 **ASMRL** は、関連装置（Syslog サーバ、FTP サーバ）、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.SECA** に従い、関連装置（Syslog サーバ、FTP サーバ）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.NMG** に従い、内部セキュリティポリシーにより、内部データを持ち出さないことや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。
A.SLB	**LB シリーズの設定** **A.SLB** は、IP パケットフィルタ制御の例外動作を制限的(拒否)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、システム管理者はIP パケットフィルタ制御の例外動作に「パケット拒否」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。
A.TMM	時刻設定 **A.TMM** は、本 TOE が動作するハードウェア装置にはシステムクロック（内部時計）があり、システム管理者が時刻を設定するのが前提条件である。これに対し、対策方針 **OE.TMM** にしたがい、システム管理者は、本 TOE に時刻を設定することで前提条件を実現できる。

第5章　　拡張コンポーネント

5.1 拡張コンポーネント

本 ST は、CC パート 2、および CC パート 3 に適合しており、拡張コンポーネントは定義しない。

第6章　セキュリティ要件

本章では、セキュリティ機能要件、セキュリティ保証要件、およびセキュリティ要件根拠について記述する。
なお、本章で使用する用語の定義は以下のとおりである。

サブジェクト	定義
IP パケットフィルタリング	IP パケットデータとフィルタリグルールを比較してパケットの通過、破棄の制御を行う制御部

情報	定義
IP パケットデータ	ネットワーク上を流れるデータ（Internet Protocol データ）。（外部ネットワークと内部ネットワーク間で送受信されるデータ）

操作	定義
IP パケットデータの通過（許可）	送受信されるデータの通過を許可。
IP パケットデータの破棄（拒否）	送受信されるデータの通過を破棄（拒否）。
消去	TOE 設定データの設定消去、およびセキュリティ属性の消去。
退避	TOE 設定データの設定退避（外部ファイルへ保存）、およびセキュリティ属性の退避（外部ファイルへ保存）。
復元	TOE 設定データの設定復元（外部保存ファイルから読み込み）、およびセキュリティ属性の復元（外部保存ファイルからの読み込み）。
追加	TOE 設定データの設定追加、およびセキュリティ属性の追加。
有効化	TOE 設定データ、およびセキュリティ属性の追加や改変など設定データを反映（適用）とする設定操作。

IP パケットフィルタリングのセキュリティ属性	定義
受信 LAN インターフェース名情報	フィルタリングルールの受信する LAN インターフェース名の情報。
送信 LAN インターフェース名情報	フィルタリングルールの送信する LAN インターフェース名の情報。
送信元 IP アドレス情報	フィルタリングルールの送信元 IP アドレス（ホスト、またはネットワーク）の情報。
送信先 IP アドレス情報	フィルタリングルールの送信先 IP アドレス（ホスト、またはネットワーク）の情報。
トランスポート層プロトコル情報	フィルタリングルールのトランスポート層プロトコル（TCP、UDP、ICMP）の情報。
送信元ポート番号情報	フィルタリングルールの送信元ポート番号（トランスポート層プロトコルが TCP、UDP の場合）の情報。
送信先ポート番号情報	フィルタリングルールの送信先ポート番号（トランスポート層プロトコルが TCP、UDP の場合）の情報。
IP パケットフィルタ制御の例外動作情報	IP パケットデータのパケットフィルタ制御ルールに合致しないときの例外動作の判断基準であり、パケットの通過の有効・無効（通過・拒否）の動作情報。

情報のセキュリティ属性	定義

TOE 上のIP パケットデータの受信 LAN インターフェース名情報	IP パケットデータを受信する LAN インターフェース名の情報。
TOE 上のIP パケットデータの送信 LAN インターフェース名情報	IP パケットデータを送信する LAN インターフェース名の情報。
送信元 IP アドレス情報	送信元 IP アドレス(ホスト、またはネットワーク)の情報。
送信先 IP アドレス情報	送信先 IP アドレス(ホスト、またはネットワーク)の情報。
トランスポート層プロトコル情報	トランスポート層プロトコル(TCP、UDP、ICMP)の情報。
送信元ポート番号情報	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)の情報。
送信先ポート番号情報	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)の情報。

その他の用語	定義
LAN インターフェース情報	本 TOE で使用する LAN インターフェースの設定情報(LAN インターフェース名や IP アドレスなどの設定情報)
保守インターフェース情報	本 TOE で使用する保守インターフェースの設定情報(シリアルインターフェース情報やIP アドレス情報などの設定情報)
時刻設定情報	本 INS のシステムクロック(内部時計)に設定する日付、時刻情報。
システム管理者 ID 情報	本 TOE のシステム管理者(管理者権限)認証のための ID 情報。
システム監視者 ID 情報	本 TOE のシステム監視者(オペレーター権限)認証のための ID 情報。
システム管理者パスワード情報	本 TOE のシステム管理者(管理者権限)認証のためのパスワード情報。
システム監視者パスワード情報	本 TOE のシステム監視者(オペレーター権限)認証のためのパスワード情報。
アカウントログ情報	システム管理者、またはシステム監視者のログイン、ログアウトの記録情報。
コマンドログ情報	システム管理者、またはシステム監視者によるコマンド(操作)実行履歴の記録情報。
セッションログ情報	IP パケットフィルタリング機能 (TSF_IPPF) による IP パケット処理結果の記録情報。
メッセージログ情報	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の記録情報。
エラーログ情報	本 TOE が動作する INS に関連する異常イベントや故障イベントの記録情報。
ロギング情報	IP パケット通過、遮断情報や設定操作などの事象や操作などの重要なイベントを追跡記録したデータの総称。(アカウントログ情報、コマンドログ情報、セッションログ情報、メッセージログ情報、エラーログ情報などのロギング情報。)
構成定義情報	TOE 設定データを含む本 INS を動作させるための設定情報。定義情報には、基本動作情報やフィルタリングルール、管理者認証用アカウント情報などが含まれる。
管理者認証用アカウント情報	システム管理者やシステム監視者を識別する情報。
基本動作情報	TOE が動作するための装置情報(LAN インターフェース情報や保守インターフェース情報など)。
フィルタリングルール(フィルタリング条件)	IP パケットデータのアクセス制御ルール(通過・破棄の条件、送受信 LAN インターフェース名やIP アドレス、プロトコル、ポート番号などのセキュリティ属性)の情報。
運用支援管理機能(補助記憶装置)	ロギング情報の格納場所であり、本 INS 上に実装される装置。

運用支援管理機能(Syslog サーバ)	ロギング情報の格納場所であり、本 INS 外に用意される装置。
システム停止	本 INS 装置(TOE を含む)の停止。
ブロック	補助記録装置のロギング情報を格納する領域。
イベント通知(転送)情報	本 TOE のロギング情報を関連装置であるSyslog サーバに通知(転送)する機能の有効・無効の情報。

6.1 セキュリティ機能要件

本 TOE が提供するセキュリティ機能要件を以下に記述する。セキュリティ機能要件は、CC パート 2 で規定されているクラス、およびコンポーネントに準拠している。

6.1.1 クラス FAU:セキュリティ監査

■ セキュリティ監査データ生成(FAU_GEN)

FAU_GEN.1 監査データ生成

下位階層

なし

依存性

FPT_STM.1 高信頼タイムスタンプ

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1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(ロギング情報として記録を残す事象)を表 12 に示す。

表 12 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	項	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	90	なし	―
FAU_STG.1	124	なし	―
FAU_STG.4	126	a) 基本:監査格納失敗によってとられるアクション。	＜基本＞ エラーログ:補助記録装置故障時に関する状況を監査する。 メッセージログ:監査記録領域に関するブロック満杯警告の発生状況を監査する。
FDP_IFC.1	183	なし	―
FDP_IFF.1	194	a) 最小: 要求された情報フローを許可する決	＜基本＞

機能要件	項	監査対象とすべきアクション(規約)	TOEの監査対象事象
		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: 情報フローの実施の決定をする上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的に基づいて流れた、情報の特定のサブセット(例えば、対象物の劣化の監査)。	セッションログ:IP パケットデータの通過/拒否を監査する。
FIA_UAU.2	269	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:システム管理者またはシステム監視者の認証成功／認証失敗を監査する。
FIA_UID.2	280	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:システム管理者またはシステム監視者の認証成功／認証失敗を監査する。
FMT_MSA.1	300	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:システム管理者の認証を監査する。 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	302	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:システム管理者の認証を監査する。 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	311	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:システム管理者の認証を監査する。 コマンドログ:管理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_SMF.1	325	a) 最小:管理機能の使用。	＜最小＞ 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_SMR.1	333	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:管理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	427	a) 最小:時間の変更 b) 詳細:タイムスタンプの提供	＜最小＞ 日付変更操作を監査する。

[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(該当する場合)、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

■ セキュリティ監査事象格納(FAU_STG)

FAU_STG.1 保護された監査証跡格納

下位階層

なし

依存性

FAU_GEN.1 監査データ生成

FAU_STG.1.1

TSFは、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

TSFは、監査証跡に格納された監査記録への不正な改変を[選択: 防止、検出: から1つのみ選択]できなければならない。

[選択: 防止、検出: から1つのみ選択]

- 防止

FAU_STG.4 監査データ損失の防止

下位階層

FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性

FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1

TSF は、監査証跡が満杯になった場合、[選択: 監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から1 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]を行わなければならない。

[選択: 監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き: から1 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]

- 補助記憶装置が故障した場合は、システム停止(本 INS 装置を停止)する。
- 監査記録領域のブロックが満杯の場合、警告の監査記録を残す。

監査対象としては、次のロギング情報がある。各ロギング種別毎に格納領域があり、上記のアクションは、格納領域毎に行なわれる。

- ●アカウントログ情報
- ●コマンドログ情報
- ●セッションログ情報
- ●メッセージログ情報
- ●エラーログ情報

6.1.2 クラス FDP:利用者データ保護

■ 情報フロー制御方針(FDP_IFC)

FDP_IFC.1 サブセット情報フロー制御

下位階層

なし

依存性

FDP_IFF.1 単純セキュリティ属性

FDP_IFC.1.1

TSFは、[割付: 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サブジェクト、情報及び操作のリスト]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: 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サブジェクト、情報及び操作のリスト]

＜サブジェクトのリスト＞
・IP パケットフィルタリング

＜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

＜操作のリスト＞
・IP パケットデータの通過(許可)
・IP パケットデータの破棄(拒否)

■ 情報フロー制御機能（FDP_IFF）

FDP_IFF.1 単純セキュリティ属性

下位階層

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

FDP_IFF.1.1

TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[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、及び各々に対応する、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、及び各々に対応する、セキュリティ属性]

＜サブジェクトのリスト＞
・IP パケットフィルタリング

＜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

＜操作のリスト＞
・IP パケットデータの通過（許可）
・IP パケットデータの破棄（拒否）

＜IP パケットフィルタリング（サブジェクト）のセキュリティ属性＞
・受信 LAN インターフェース名情報
・送信 LAN インターフェース名情報
・送信元 IP アドレス情報
・送信先 IP アドレス情報
・トランスポート層プロトコル情報
・送信元ポート番号情報
・送信先ポート番号情報
・IP パケットフィルタ制御の例外動作情報

＜情報のセキュリティ属性＞
・TOE 上のIP パケットデータの受信 LAN インターフェース名情報
・TOE 上のIP パケットデータの送信 LAN インターフェース名情報
・送信元 IP アドレス情報
・送信先 IP アドレス情報
・トランスポート層プロトコル情報
・送信元ポート番号情報
・送信先ポート番号情報

上記の操作のリストおよびIP パケットフィルタリングの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情報のセキュリティ属性と IP パケットフィルタリングのサブジェクトのセキュリティ属性が一致するか評価し、一致した場合に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 パケットデータは拒否する。条件に一致しない場合は、例外動作の情報に従って、通過、または破棄する。

表 13 セキュリティ属性の関係

情報	情報のセキュリティ属性	IP パケットフィルタリングのセキュリティ属性	操作
● TOE を介して送受信される IP パケットデータ	● TOE 上の IP パケットデータの受信 LAN インターフェース名情報 ● TOE 上の IP パケットデータの送信 LAN インターフェース名情報 ● 送信元 IP アドレス情報 ● 送信先 IP アドレス情報 ● トランスポート層プロトコル情報 ● 送信元ポート番号情報 ● 送信先ポート番号情報	● 受信 LAN インターフェース名情報 ● 送信 LAN インターフェース名情報 ● 送信元 IP アドレス情報 ● 送信先 IP アドレス情報 ● トランスポート層プロトコル情報 ● 送信元ポート番号情報 ● 送信先ポート番号情報 ● IP パケットフィルタ制御の例外動作情報	● IP パケットデータの通過(許可) ● IP パケットデータの破棄(拒否)

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、以下の規則、[割付: セキュリティ属性に基づいて情報フローを明示的に許可する規則]に基づいて、情報フローを明示的に許可しなければならない。

[割付: セキュリティ属性に基づいて情報フローを明示的に許可する規則]

なし。

FDP_IFF.1.5

TSF は、以下の規則、[割付: セキュリティ属性に基づいて情報フローを明示的に拒否する規則]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情報フローを明示的に拒否する規則]

なし。

6.1.3 クラス FIA:識別と認証

■ 利用者認証(FIA_UAU)

FIA_UAU.2 アクション前の利用者認証

下位階層

FIA_UAU.1 認証のタイミング

依存性

FIA_UID.1 識別のタイミング

FIA_UAU.2.1

TSF は、その利用者を代行する他のTSF 仲介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。

■ 利用者識別(FIA_UID)

FIA_UID.2 アクション前の利用者識別

下位階層

FIA_UID.1 識別のタイミング

依存性

なし

FIA_UID.2.1

TSF は、その利用者を代行する他のTSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.4 クラス FMT:セキュリティ管理

■ セキュリティ属性の管理(FMT_MSA)

FMT_MSA.1 セキュリティ属性の管理

下位階層

なし

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_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

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[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]

表 14 にセキュリティ属性を示す。

[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
- その他の操作:[消去、追加、退避、復元]

[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表 14 に示す。

表 14 セキュリティ属性の管理

IP パケットフィルタリングのセキュリティ属性	操作	許可された識別された役割
受信 LAN インターフェース名情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
送信 LAN インターフェース名情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
送信元 IP アドレス情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
送信先 IP アドレス情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
トランスポート層プロトコル情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
送信元ポート番号情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
送信先ポート番号情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者

	問い合わせ	システム監視者
IP パケットフィルタ制御の例外動作情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者

表 14 の操作における退避と復元は、構成定義情報一括で退避、または復元される。

[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 静的属性初期化

下位階層

なし

依存性

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

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に対して[選択: 制限的、許可的、[割付: その他の特性]: から1 つのみ選択]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、[割付: その他の特性]: から1 つのみ選択]

- 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特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]

- システム管理者

■ TSFデータの管理(FMT_MTD)

FMT_MTD.1　TSFデータの管理

下位階層

なし

依存性

FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1

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]

表 15 にTSFデータのリストを示す。

[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]]

- 問い合わせ
- 改変
- 消去
- その他の操作:[追加、退避、復元]

[割付:許可された識別された役割]

表 15 に役割を示す。

表 15　TSF データの管理

TSFデータ	操作	許可された識別された役割
LAN インターフェース情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
保守インターフェース情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
時刻設定情報	問い合わせ、改変	システム管理者
	問い合わせ	システム監視者
イベント通知(転送)情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
システム管理者 ID 情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
システム監視者 ID 情報	問い合わせ、改変、消去、追加、退避、復元	システム管理者
	問い合わせ	システム監視者
システム管理者パスワード情報	改変、消去、追加、退避、復元	システム管理者
システム監視者パスワード情報	改変、消去、追加、退避、復元	システム管理者
アカウントログ情報	消去、退避	システム管理者
コマンドログ情報	消去、退避	システム管理者
セッションログ情報	消去、退避	システム管理者
メッセージログ情報	消去、退避	システム管理者
エラーログ情報	消去、退避	システム管理者

表 15 の操作におけるロギング情報以外のTSFデータの退避と復元は、構成定義情報の一括データとして退避、または復元される。

■ 管理機能の特定(FMT_SMF)

FMT_SMF.1 管理機能の特定

下位階層

なし

依存性

なし

FMT_SMF.1.1

TSF は、以下の管理機能を実行することができなければならない。:[割付: TSF によって提供される管理機能のリスト]

[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]

- IPパケットフィルタリングのセキュリティ属性を管理する機能
- TSFデータ(LANインターフェース情報、保守インターフェース情報、イベント通知(転送)情報、システム管理者ID情報、システム監視者ID情報、時刻設定情報、システム管理者パスワード情報、システム監視者パスワード情報、アカウントログ情報、コマンドログ情報、セッションログ情報、メッセージログ情報、エラーログ情報)を管理する機能

表 16 セキュリティ管理機能リスト

機能要件	項	管理要件(CCの規定)	管理項目(TSFの実装)
FAU_GEN.1	88	なし	ー
FAU_STG.1	120	なし	ー
FAU_STG.4	123	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)。	a) 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	182	なし	ー
FDP_IFF.1	191	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。	a) 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	264	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) システム管理者アカウントの作成、参照、消去および、パスワード変更 b) システム監視者アカウントのパスワード変更
FIA_UID.2	279	a) 利用者識別情報の管理。	a) システム管理者およびシステム監視者のアカウントの作成、参照、消去
FMT_MSA.1	296	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。 b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a) なし(役割グループは固定であり、管理対象にならない) b) 値を引き継がない
FMT_MSA.3	298	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。 c) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a) なし(役割グループはシステム管理者だけであり、管理対象にならない) b) デフォルト通過禁止 c) 値を引き継がない
FMT_MTD.1	308	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。	a) なし(役割グループはシステム管理者だけであり、管理対象にならない)

FMT_SMF.1	324	なし	ー
FMT_SMR.1	330	a) 役割の一部をなす利用者のグループの管理。	a) 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	426	a) 時間の管理	a) システムクロック（内部時計）の設定

■ セキュリティ管理役割（FMT_SMR）

FMT_SMR.1 セキュリティの役割

下位階層

なし

依存性

FIA_UID.1 識別のタイミング

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]

- システム管理者
- システム監視者

FMT_SMR.1.2

TSF は、利用者を役割に関連付けなければならない。

6.1.5 クラス FPT：TSFの保護

■ タイムスタンプ（FPT_STM）

FPT_STM.1 高信頼タイムスタンプ

下位階層

なし

依存性

なし

FPT_STM.1.1

TSF は、高信頼タイムスタンプを提供できなければならない。

6.2 セキュリティ保証要件

本 TOE の評価保証レベルは、EAL1＋ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1である。すべてのセキュリティ保証要件コンポーネントは、CC パート3 で規定されている EAL1 コンポーネントとさらに追加した ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 コンポーネントを引用している。

表 17 EAL1+ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 保証要件

保証クラス	保証コンポーネント
ADV: 開発	ADV_FSP.1 基本機能仕様
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.1 TOE のラベル付け
	ALC_CMS.1 TOE のCM 範囲
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE: テスト	ATE_IND.1 独立テスト － 適合
AVA: 脆弱性評定	AVA_VAN.1 脆弱性調査

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応を、表 18 に記述する。この表で示すとおり、各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対応している。また各セキュリティ対策方針が、セキュリティ機能要件により保証されている根拠を、表 19 に記述する。

表 18 セキュリティ機能要件と対策方針の対応関係

セキュリティ対策方針 ＼ セキュリティ機能要件	O.AC	O.ADMIN	O.AUDREC
FAU_GEN.1			✓
FAU_STG.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		✓	✓
FMT_SMF.1		✓	
FMT_SMR.1		✓	

FPT_STM.1			✓

表 19 セキュリティ対策方針によるセキュリティ機能要件根拠

セキュリティ対策方針	セキュリティ機能要件根拠
O.AC （外部ネットワーク利用者の制限）	**O.AC** は、攻撃者による内部ネットワークへの侵入防止を提供する対策方針である。 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 インターフェース名、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（拒否）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 （システム管理者制御）	**O.ADMIN** は、環境設定操作が許可されたシステム管理者、およびシステム監視者だけに制限する対策方針である。 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、正当に許可されたシステム管理者、またはシステム監視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. 構成定義情報の基本動作情報（LAN インターフェース情報や保守インターフェース情報など）やフィルタリングルール（TOE 上の IP パケットデータの送受信 LAN インターフェース名など）、管理者用アカウント情報（システム管理者ID,パスワードなど）の改変や消去、退避、復元の更新操作を管理者だけに許可し、他の利用者は制限されなければならない。また、基本動作情報やフィルタリングルールの問い合わせ（参照）は、システム管理者、またはシステム監視者に許可し、他の利用者は制限しなければならない。ロギング情報ファイルの消去操作、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消去操作、および退避操作は、システム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要件は、**FMT_MSA.1**、**FMT_MSA.3**、**FMT_MTD.1**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。 したがって、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_MTD.1** 、**FMT_SMF.1** 、**FMT_SMR.1** の達成により、**O.ADMIN** を実現できる。
O.AUDREC （監査記録）	**O.AUDREC** は、監査記録操作が許可された管理者だけに制限する対策方針である。 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（**T.ATTK**）に関する監査記録と、TOE

	への不正アクセス(**T.CNFD**)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_MTD.1**、**FMT_SMF.1**:監査ロギング情報自身の消去では、システム管理者だけが消去操作可能であり、かつ、**OE.MGR** の環境セキュリティ対策方針によりシステム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.SECA**、**FIA_UAU.2**、**FIA_UID.2**、**FAU_STG.1**、**FMT_MTD.1** であり、後者は**FAU_STG.4** である。 c. 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監査するため、日時情報を管理しなければならない。日時情報は、INS に実装されているシステムクロック(内部時計)により得られる。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。したがって、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.1** 、 **FAU_STG.4** 、 **FIA_UAU.2** 、 **FIA_UID.2** 、**FMT_MTD.1**、**FPT_STM.1** の達成により、**O.AUDREC** を実現できる。

6.3.2 依存性の検証

セキュリティ機能要件が依存している機能要件、および依存関係を満足していない機能要件と依存関係が満たされていなくても問題がない根拠を、表 20 に記述する。

表 20 セキュリティ機能要件コンポーネントの依存性

機能要件コンポーネント	依存性の機能要件コンポーネント	
要件、および用件名称	満足している要件	依存性を満足していない要件とその正当性
FAU_GEN.1 監査データ生成	FPT_STM.1	なし
FAU_STG.1 保護された監査証跡格納	FAU_GEN.1	なし
FAU_STG.4 監査データ損失の防止	FAU_STG.1	なし
FDP_IFC.1 サブセット情報フロー制御	FDP_IFF.1	なし
FDP_IFF.1 単純セキュリティ属性	FDP_IFC.1	なし
	FMT_MSA.3	なし
FIA_UAU.2 アクション前の利用者認証	FIA_UID.2	**FIA_UID.1** F **FIA_UID.1**、および **FIA_UAU.2** の依存関係は満足されていないが、**FIA_UID.1** の上位階層となる **FIA_UID.2** が存在するため、不要である。
FIA_UID.2 アクション前の利用者識別	なし	なし
FMT_MSA.1 セキュリティ属性の管理	FDP_IFC.1	なし
	FMT_SMF.1	なし

	FMT_SMR.1	なし
FMT_MSA.3 静的属性初期化	FMT_MSA.1	なし
	FMT_SMR.1	なし
FMT_MTD.1 TSF データの管理	FMT_SMF.1	なし
	FMT_SMR.1	なし
FMT_SMF.1 管理機能の特定	なし	なし
FMT_SMR.1 セキュリティの役割	FIA_UID.2	**FIA_UID.1** **FMT_SMR.1**、および **FIA_UAU.1** の依存関係は満足されていないが、**FIA_UID.1** の上位階層となる **FIA_UID.2** が存在するため、不要である。
FPT_STM.1 高信頼タイムスタンプ	なし	なし

6.3.3 セキュリティ保証要件根拠

本 TOE は、ファイアーウォール製品であり、商用の製品である。第 1 章、および 3.3 前提条件の記述のとおり、物理的に保護されたエリアに設置され、信頼されるシステム管理者により適切に設定、および管理されている運用環境の下で外部ネットワーク、または内部ネットワークからのデータ盗聴や改ざんなどの不正アクセスが想定される。
このように保護された運用環境下での低レベルな攻撃を想定しているため、保証レベルとしては、EAL1＋ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 の選択は妥当であると言える。

第7章　TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の仕様を概説する。

7.1 セキュリティ機能

表 21 に、本 TOE が提供するセキュリティ機能とセキュリティ機能要件（SFR）の対応を示す。ここで示される通り、本節で説明するセキュリティ機能は、6.1 節に記述されているすべての SFR を満たすものである。

表 21　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

セキュリティ機能 / セキュリティ機能要件	SF_IPPF.1	SF_ENV.1	SF_AUD.1
FAU_GEN.1	✓	✓	✓
FAU_STG.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		✓	✓
FMT_SMF.1		✓	✓
FMT_SMR.1		✓	✓
FPT_STM.1		✓	

7.1.1 IP パケットフィルタリング機能 (SFP_IPPF)

TOE は、TOE 設定である環境管理機能(**TSF_ENV**)の設定データに基づき、TOE を通過する通信パケットの制御機能を提供する。以下では、IP パケットフィルタリング機能(**SFP_IPPF**)について、SFR実現方法という観点から説明する。

7.1.1.1 IP パケットフィルタ制御(SF_IPPF.1)に対応する SFR の実現方法

(1) FDP_IFC.1 サブセット情報フロー制御、FDP_IFF.1 セキュリティ属性による IP パケットフィルタ制御
TOE 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拒否する。通過または拒否は、以下のような処理で実装し、IP パケットフィルタ制御方針を実行する。

- 受信 LAN インターフェース名とフィルタリング条件の受信 LAN インターフェース名が一致するか評価する。
- 送信 LAN インターフェース名とフィルタリング条件の送信 LAN インターフェース名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。

上記のセキュリティ属性の評価(一致判定)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、IP 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、IP 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。
- 拒否指定の場合、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。

上記により、FDP_IFC.1、FDP_IFF.1 を実現する。

(2) FAU_GEN.1 監査データ生成
IP パケットフィルタ制御の処理結果として、システム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 22 IP パケット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:表 23 のコネクション情報

TCP/IP パケット破棄(拒否)	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:表 23 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:表 23 のコネクション情報
UDP/IP パケット破棄(拒否)	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:表 23 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:表 23 のコネクション情報
IP パケット破棄(拒否)	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:表 23 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 23 コネクション情報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 インターフェース名、または IP パケットデータを送信した LAN インターフェース名
	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元ポート番号
	IP パケットデータの送信先ポート番号
ICMP の場合	IP パケットデータを受信した LAN インターフェース名、または IP パケットデータを送信した LAN インターフェース名
	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)

上記により、FAU_GEN.1 を実現する。

7.1.2 環境設定管理機能 (SFP_ENV)

環境設定管理機能は、TOE にアクセスする操作員(システム管理者、またはシステム監視者)を識別し、登録されている操作員本人であることを確認するための機能を提供する。以下では、環境設定管理機能について、SFR の実現方法という観点から説明する。

7.1.2.1 環境設定管理 (SF_ENV.1)に対応する SFR の実現方法

(1) FIA_UAU2 アクション前の利用者認証、FIA_UID2 アクション前の識別

本 TOE では、TOE を管理する管理者識別認証機能(アカウント管理)を提供する。本 TOE に接続要求した場合、管理者識別機能および管理者認証機能により有効な管理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。管理者識別認証機能では、管理者ID(アカウント名)とパスワ

ード情報の両方を利用し、管理者識別と管理者認証を同時処理する PAP (Password Authentication Protocol) 方式を実装する。認証完了後、認証されたアカウントの役割(システム管理者やシステム監視者)を識別することで、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。
識別する利用者を以下に示す。

- システム管理者
- システム監視者

本 TOE への設定操作を行う保守端末の接続形態として、以下の接続形態を提供する。

- CLI接続(LAN 接続、または RS232C 接続:Telnet利用)
- Web接続(LAN 接続:Web ブラウザ利用)

上記により、FIA_UAU2、FIA_UID2 を実現する。

(2) FMT_SMR.1 セキュリティの役割
TOE は、管理者識別認証機能において、表 24 に示す識別された役割と許可された役割の機能を提供する。

表 24 管理者アカウント管理識別と状態管理、管理者インターフェース

利用識別	状態管理	管理者インターフェース
システム管理者	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、管理者認証用アカウント情報)の改変操作(復元を含む)、消去操作および、退避操作を許可する。 また、ロギング情報の消去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)
システム監視者	ー	

管理者識別認証機能では、システム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、以下に列挙された管理者認証用アカウント情報の操作を許可する。

- システム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。
- システム監視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。
- システム管理者のアカウント消去要求の場合、最後のシステム管理者であれば消去しない。
- システム管理者のアカウント消去要求の場合、アカウント情報(パスワードを含む)を消去する。
- システム監視者のアカウント消去要求の場合、アカウント情報(パスワードを含む)を消去する。
- システム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。
- システム監視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。

管理者アカウント管理機能では、システム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、管理者認証用アカウント情報の更新操作を拒否する。

上記により、FMT_SMR.1 を実現する。

(3) FMT_SMF.1 管理機能の特定
TOE は、環境設定管理において、表 25 に示すセキュリティ管理機能を含むIPパケットフィルタリングのセキュリティ属性、TSFデータの管理機能を提供する。

表 25 セキュリティ管理機能

セキュリティ管理項目	セキュリティ管理機能
管理者識別認証の管理	管理者識別認証の管理

	システム管理者、およびシステム監視者のID情報の問い合わせ、改変、消去、追加、退避、復元 システム管理者、およびシステム監視者のパスワード情報の改変、消去、追加、退避、復元
パケットフィルタリング機能の管理	パケットフィルタリング機能の管理 LANインターフェース情報、保守インターフェース情報、フィルタリングルールのデータを管理。
イベント通知の管理	イベント通知の管理 ロギング情報の通知有無を管理する。
時間の管理	システムクロック （内部時計）の管理 システムクロック（内部時計）の日時を管理。

上記により、FMT_SMF.1 を実現する。

(4) FMT_MTD.1 TSFデータの管理、FMT_MSA.1 セキュリティ属性の管理、FMT_MSA.3 静的属性初期化
TOE は、環境設定管理において、以下に示すセキュリティデータの管理、セキュリティ属性の管理、静的属性初期化を提供する。

- 基本動作情報と管理者認証アカウント情報（構成定義情報）
  基本動作情報と管理者認証アカウントの設定操作を、システム管理者に限り許可する。また、システム監視者には、アカウント情報（ID、パスワード情報を除き）参照（問い合わせ）操作に限り許可する。

表 26 基本動作情報と管理者認証アカウント情報データ

LAN インターフェース	LAN インターフェースに対して、有効化指定や IP アドレス割当て指定の設定変更操作（問い合わせ、改変、消去、追加）があった場合、構成定義情報の該当情報を更新する。
保守インターフェース	保守インターフェースに対する IP アドレスの設定変更操作（問い合わせ、改変、消去、追加）があった場合、構成定義情報の該当情報を更新する。
時刻設定	日付、および時刻に設定変更（問い合わせ、改変）があった場合、構成定義情報の該当情報を更新する。
イベント通知（転送）	ロギング情報を通知（転送）する関連装置 Syslog サーバのホスト情報と通知条件が設定（問い合わせ、改変、消去、追加）された場合、構成定義情報の該当情報を更新する。
システム管理者 ID 情報	システム管理者 ID に対して問い合わせ、改変、消去、追加の設定変更があった場合、構成定義情報の該当情報を更新する。
システム監視者 ID 情報	システム監視者 ID に対して問い合わせ、改変、消去、追加の設定変更があった場合、構成定義情報の該当情報を更新する。
システム管理者パスワード情報	システム管理者パスワードに対して改変、消去、追加の設定変更があった場合、構成定義情報の該当情報を更新する。
システム監視者パスワード情報	システム監視者パスワードに対して改変、消去、追加の設定変更があった場合、構成定義情報の該当情報を更新する。

- フィルタリングルール（構成定義情報）
  フィルタリングルールの設定操作を、システム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システム管理者およびシステム監視者に限り許可する。
  フィルタリングルールの設定において、ルールを省略した場合、またはルールを消去した場合は、IP パケットフィルタ制御の例外動作に従って、拒否（破棄）、または通過する。IP パケットフィルタリング制御の例外動作の初期値（デフォルト値）は、表 3 に示す。

表 27 フィルタリングルールデータ

受信 LAN インターフェー	IP パケットデータを受信する LAN インターフェース名を選択させ、フィ

ス名情報	ルタリングルールの受信インターフェース名情報を問い合わせ、改変、消去、追加する。なお、保守インターフェースは、この選択候補にしない。
送信 LAN インターフェース名情報	IP パケットデータを送信する LAN インターフェース名を選択させ、フィルタリングルールの送信インターフェース名情報を問い合わせ、改変、消去、追加する。なお、保守インターフェースは、この選択候補にしない。
送信元 IP アドレス情報	選択された LAN インタフェース名(親)に対して、送信元 IP アドレス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問い合わせ、改変、消去、追加する。
送信先 IP アドレス情報	選択された LAN インタフェース名(親)に対して、送信先 IP アドレス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問い合わせ、改変、消去、追加する。
トラスポート層プロトコル情報	選択された LAN インタフェース名(親)に対して、トランスポート層プロトコル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問い合わせ、改変、消去、追加する。
送信元ポート番号情報	選択された LAN インタフェース名(親)に対して、送信元ポート番号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問い合わせ、改変、消去、追加する。
送信先ポート番号情報	選択された LAN インタフェース名(親)に対して、送信先ポート番号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問い合わせ、改変、消去、追加する。

上記、設定されたフィルタリング条件に対して、許可(通過)や拒否(破棄)の処理動作を指定させ、フィルタリングルール、IP パケットフィルタ制御の例外動作情報の操作を更新する。

- 構成定義情報の退避と復元
  基本動作情報やフィルリングルールの構成定義情報の退避と復元操作を、システム管理者に限り許可する。

表 28 構成定義情報の退避と復元

退避	TOE 上の基本動作情報、フィルタリングルール、および管理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。
復元	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、および管理者認証用アカウント情報)を消去後、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。

上記により、FMT_MTD.1、FMT_MSA.1、FMT_MSA.3 を実現する。

(5) FPT_STM.1 高信頼スタンプ

TOE は、管理者識別認証機能において、システム管理者にかぎり高信頼スタンプを実現するために、日付、および時刻を設定する機能を提供する。日本国以外の国で設定する場合は、タイムゾーンを設定することができる。本 TOE は、この設定された日付、および時刻により時刻を管理するように実装する。
上記により、FPT_STM.1 を実現する。

(6) FAU_GEN.1 監査データ生成

TOE は、TOE がセキュアに運用されていることを監査するために必要なロギング情報の生成、および生成した情報の管理を行うために、監査対象となる事象が発生した場合、当該事象の監査証跡として、監査記録を生成する。

監査対象(ロギング情報の種別毎)を以下に示す。

・管理者アカウント認証(アカウントログ)

・構成定義更新操作(メッセージログ)
・構成定義更新操作(コマンドログ)

表 29 管理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:管理者識別情報、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:管理者識別情報、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:管理者識別情報、保守端末の IP アドレス

表 30 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 31 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 パケット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 パケットフィルタ制御の例外動作情報
管理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:管理者認証用アカウント情報
構成定義情報(LAN インターフェース情報、保守インターフェース情報、など)の改	日時情報:発生日時 事象種類:情報 (informational)

変	事象結果:設定変更 補助情報:構成定義情報

上記により、FAU_GEN.1 を実現する。

7.1.3 運用支援管理機能 (SFP_AUD)

運用支援管理機能は、TOE の稼働記録を維持するために、ロギング情報(監査記録)を管理する機能を提供する。この管理機能では、ロギング情報格納場所の選択や消去操作と退避操作を提供し、システム管理者だけに操作を許可する。以下では、運用支援管理機能について、SFRの実現方法という観点から説明する。

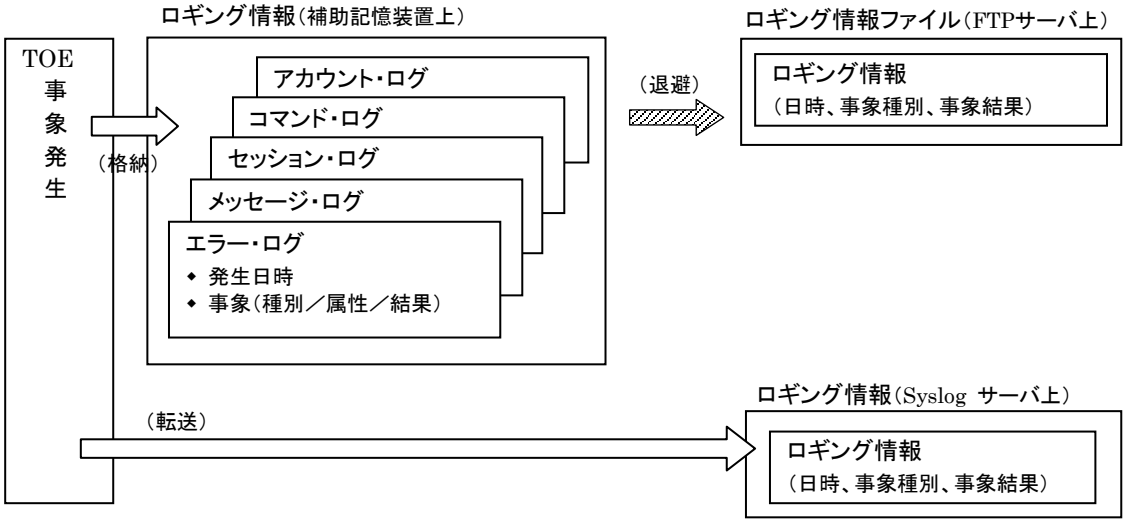

図 6 運用支援管理機能情報

7.1.3.1 運用支援管理 (SF_AUD.1)に対応する SFR の実現方法

(1) FAU_GEN.1 監査データ生成

TOE は、TOE がセキュアに運用されていることを監視するために必要な情報の記録や動作結果の管理を行うために、監査の対象となる事象が発生した場合、当該事象の監査証跡として、監査記録を生成する。

ロギング情報の種類

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

- アカウントログ
  システム管理者、またはシステム監視者による 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
  システム管理者、またはシステム監視者によるコマンド実行履歴を記録する。
- セッションログ
  IP パケットフィルタリング機能 (**SF_IPPF.1**) による IP パケット処理結果(通過または拒否)を記録する。
- メッセージログ
  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

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。

補助記憶装置が実装されている場合、記録依頼されたロギング情報を補助記憶装置に格納する。また補助記憶装置が実装されていない場合、ロギング情報を基本動作情報に設定されている Syslog サーバにロギング情報を転送する。

ロギング機能の開始

ロギング機能は、TOE 起動時に必須機能として自動起動するため、ロギ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、ロギ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、後述のロギング情報の消去時も、ロギング機能が一時停止することは無い。

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記録する。

表 32 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:ロギングファイルのローテーション通知 補助情報:なし

*1:システムの正常起動が機能単位の起動を兼ねる(機能単位の正常起動の監査事象は記録しない)。

上記により、FAU_GEN.1 を実現する。

(2) FAU_STG.4 監査データ損失の防止

TOE は、監査データの管理に関して、以下の機能を提供する。

ロギング機能の故障

ロギング情報を格納する補助記憶装置が実装されている環境で、ロギ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。

ロギング情報の格納

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 サーバへのイベント通知指定が存在すれば、イベント通知機能を呼び出すことで、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、最新のブロックに順次追加格納する。
③最新のブロックが満杯になった場合、ブロック飽和のロギング情報を生成する。
④ブロック飽和事象は、イベント通知機能を利用して、システム管理者に通知する。
⑤次のブロックを獲得し、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。

ロギング情報が満杯時

補助記憶装置の格納領域が満杯になった場合、ブロック飽和のロギング情報を生成し、監査記録に残す。

上記により、FAU_STG.4 を実現する。

(3) FAU_STG.1 保護された監査証跡格納、FMT_MTD.1 TSFデータの管理、FMT_SMF.1 管理機能の特定、FMT_SMR.1 セキュリティ役割

TOE は、運用管理支援において、TSFデータに関して以下の機能を提供する。

ロギング情報の消去

システム管理者に限り、ロギング情報の格納場所が補助記憶装置の場合、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。

ロギング情報の退避

システム管理者に限り、補助記憶装置が実装されている場合、補助記憶装置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 FTP サーバに退避(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(システム管理者またはシステム監視者によるコマンド実行履歴)
- セッションログ(通過または拒否の 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）

上記により、FAU_STG.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1 を実現する。

第8章　ST 略語・用語

8.1 略語

略語	定義内容
CC	コモンクライテリア（Common Criteria）
CLI	コマンドラインインターフェース(Command Line Interface)
EAL	評価保証レベル（Evaluation Assurance Level）
FTP	ファイル転送プロトコル（File Transfer Protocol）
ICMP	インターネット制御メッセージプロトコル（Internet Control Message Protocol）
INS	統合型ネットワークサーバ(Integrated Network Server)
IT	情報技術（Information Technology）
IP	インターネットプロトコル(Internet Protocol)
PP	プロテクションプロファイル（Protection Profile）
SAR	セキュリティ保証要件(Security Assurance Requirement)
SFP	セキュリティ機能方針(Security Function Policy)
SFR	セキュリティ機能要件(Security Functional Requirement)
ST	セキュリティターゲット（Security Target）
TCP	トランスミッション制御プロトコル（Trasmission Control Protocol）
TOE	評価対象（Target of Evaluation）
TSF	TOE セキュリティ機能（TOE Security Functionality）
UDP	ユーザデータグラムプロトコル（User Datagram Protocol）

8.2 用語

用語	定義内容
ネットワーク	外部ネットワークと内部ネットワークを包含する一般的に使用する場合の表現。
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、およ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。
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。
運用管理専用ネットワーク	本 TOE や基幹業務を担う機器の運用を管理するための独立させたネットワーク・セグメント。
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。
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。

システム管理者	TOE の設置～運用～監視～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システム管理者に該当する。
システム監視者	TOE の運用～監視を担い、システム管理者を補佐する副管理者。システム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システム監視者に該当する。
編集モード	システム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。
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、ネットワークのアドレス定義やフィルタリングルール、内部データの取り扱い（不正持ち出し不可）ルールで実現される。
IP パケットフィルタリング	TCP/IP4 階層のうち、インターネット層とトランスポート層にあたるパケットヘッダーをチェックし、事前に設定されたルールにしたがい、通過を許可するかどうかを処理する機能である。
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／拒否するための条件。
構成設定情報ファイル	フィルタリング条件などの動作条件が列挙された構成設定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 Syslog サーバ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。
不揮発性メモリ	コンピュータで使われるメモリの一種で、電源を供給しなくても記憶を保持するメモリの総称である。
ファイアーウォール	ファイアウォール（防火壁）とは、ある特定のコンピュータネットワークとその外部との通信を制御し、内部のコンピュータネットワークの安全を維持することを目的としたソフトウェア（あるいはそのソフトウェアを搭載したハードウェア）の技術概念である。
Syslog	システムの動作やメッセージ等の記録（ロギング情報）を取るプログラム。 Syslog サーバとは、記録を取るサーバをいう。

第9章　参考資料

本 ST 作成時の参考資料を以下に記述する。

ドキュメント名
情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル 2009 年7 月 バージョン3.1 改訂第3 版 最終版 CCMB-2009-07-001 平成21 年12 月翻訳第1.0 版 最終版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント 2009 年7 月 バージョン3.1 改訂第3 版 最終版 CCMB-2009-07-002 平成21 年12 月翻訳第1.0 版 最終版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント 2009 年7 月 バージョン3.1 改訂第3 版 最終版 CCMB-2009-07-003 平成21 年12 月翻訳第1.0 版 最終版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
情報技術セキュリティ評価のための共通方法 評価方法 2009 年7 月 バージョン3.1 改訂第3 版 最終版 CCMB-2009-07-00 平成21 年12 月翻訳第1.0 版 最終版 独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室