文書管理番号：P2NE-SSD01-02-0001

INTERSTAGE
Security Director 4.0
セキュリティターゲット

2002年10月21日
第2.7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	2001.12.03	初版	全般
1.1	2002.02.20	指摘結果反映	全般
1.2	2002.02.25	TOE関連装置の配置条件追加	2.3、3.1
1.3	2002.03.26	ASE2-001-01、ASE2-002-01、ASE2-003-01対応	5.1.1、6.1.3.4、8.1.1
1.4	2002.04.03	ASE2-001-01対応不備修正	5.1.1
		誤記訂正（メールサーバ→SNMPマネジャ）	2.3.2(SNMPマネジャ)
		誤記訂正（運用支援機能→環境設定機能）	2.3.3(TSF_ENV説明)
		誤記訂正（OE.1、OE.3説明）	4.2 OE.1、OE.3
		誤記訂正（Solaris OS提供機能）	8.3 TOE要約仕様根拠表
		誤記訂正（セキュリティ対策方針説明）	8.1.1.1 ASM.4、ASM.5、ASM.6
		版数	表紙、1.1 ST識別
1.5	2002.04.05	SFP_ACC追加対応	8.2、8.3
2.0	2002.04.16	誤記訂正（FDP_ACC.1、FDP_ACF.1）	5.1.1、8.3
		誤記訂正（OOE.AUDREC、OOE.AUDMON、OOE_ADMIN）	4.1、8.2.1.1
		機能強度追加	5.3、8.2.3
2.1	2002.04.22	誤記訂正	4.1、5.1(FAU_SEL.1)、8.2、8.3
2.2	2002.06.28	所見対応（ASE2-006～ASE2-009）	3.3、第5章、第8章
2.3	2002.07.11	誤記訂正等	全般
2.4	2002.08.01	誤記訂正等	全般
2.5	2002.08.23	誤記訂正等	全般
2.6	2002.10.02	ASM5削除、利用者ガイダンス削除	3.1、3.2、4.2、6.2、8.1
2.7	2002.10.21	ASE2-018-01対応	2.3.3、2.4.3、5.1.1、5.1.2、6.1.3.1、8.2

目次

第1章　ST概説

1.1 ST識別

名称

INTERSTAGE Security Director 4.0　セキュリティターゲット　第 2.7 版　富士通株式会社

対応TOE

本セキュリティターゲットは、以下のTOE(Target Of Evaluation)に対応する。

- INTERSTAGE Security Director　4.0　(製品コード：B23PDX4H0)

1.2 ST概要

本STは、富士通株式会社が提供するセキュリティ製品であるINTERSTAGE Security Directorのファイアウォール機能について記述している。
対象となるTOEは、上記機能のＩＰパケットフィルタリング機能、アドレス変換機能、運用支援機能、及び環境設定機能である。
上記ファイアウォール製品には、以下の機能が含まれているが、これらの機能については、TOE対象外である。

- アプリケーションゲートウェイ機能
- 暗号通信機能
- 認証機能
- システムの二重化機能

1.3 CC適合

- CC part-2適合
- CC part-3 EAL3適合

1.4 参照資料

- Common Criteria for Information Technology Security Evaluation
  Part 1:Introduction and general model Version 2.1 August 1999 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation
  Part 2:Security functional requirements Version 2.1 August 1999 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
- 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　1999年 8月　バージョン 2.1 CCIMB-99-031
  (平成13年 1月翻訳第1.2版　情報処理振興事業協会　セキュリティセンター)
- 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：セキュリティ機能要件　1999年 8月　バージョン 2.1 CCIMB-99-032
（平成13年 1月翻訳第1.2版　情報処理振興事業協会　セキュリティセンター）

- 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：セキュリティ保証要件　1999年 8月　バージョン 2.1 CCIMB-99-033
（平成13年 1月翻訳第1.2版　情報処理振興事業協会　セキュリティセンター）

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。それぞれの組織内部のイントラネット、及びインタ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」に該当します。

外部ネットワーク
組織の管理が及ばない、内部ネットワーク以外のネットワーク。

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門。

TOE管理者
TOEの設置～運用～監査～保守に渡って、本TOE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内部セキュリティポリシーに基づき、本TOEの環境設定ファイルを設定し、内部セキュリティポリシーを具体化する。

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に関する方針。

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、及びアドレス変換条件から構成される。

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。

アドレス変換条件
内部ネットワークと外部ネットワーク間でIPパケットデータのIPアドレス、及びポート番号を変換するための条件。

第2章　TOE記述

2.1 TOEの概要

TOEの種別

ファイアウォール製品

TOE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。また、別ネットワークへ配送する場合、通信パケット中のＩＰアドレスやポート番号を変換するアドレス変換機能を提供する。

本機能により、別ネットワーク上の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、特定のネットワーク上の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。

本TOEは、複数のネットワークの境界上に配置され、それぞれのネットワークを接続し、接続したそれぞれのネットワーク上のリソースを、安心して利用できる運用環境を享受するために利用される。ここで、安心してネットワーク上のリソースを利用するためには、接続するすべての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で策定された内部セキュリティポリシーの存在を前提とする。この識別された内部セキュリティポリシーに従って正しくTOEを構成することで、それぞれのネットワーク上のリソースを不正アクセスから保護しながら、ネットワーク上の有用なリソースを利用できるようになる。

利用目的

接続された、それぞれのネットワーク上のリソースを、安心して利用できる運用環境を享受することを目的に利用する。

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する。

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、この識別された内部セキュリティポリシーに従って、TOE管理者は正しくTOEを構成、維持、運用する。

具体的な利用環境として、利用者から物理的にアクセスできない場所に設置され、かつ、利用者からの論理的なアクセス（リモートからのアクセスなど）からも保護されている利用環境である。また、本TOE運用で連携する関連装置（メールサーバ、SNMPマネージャ）は、内部ネットワークに設置する。

運用

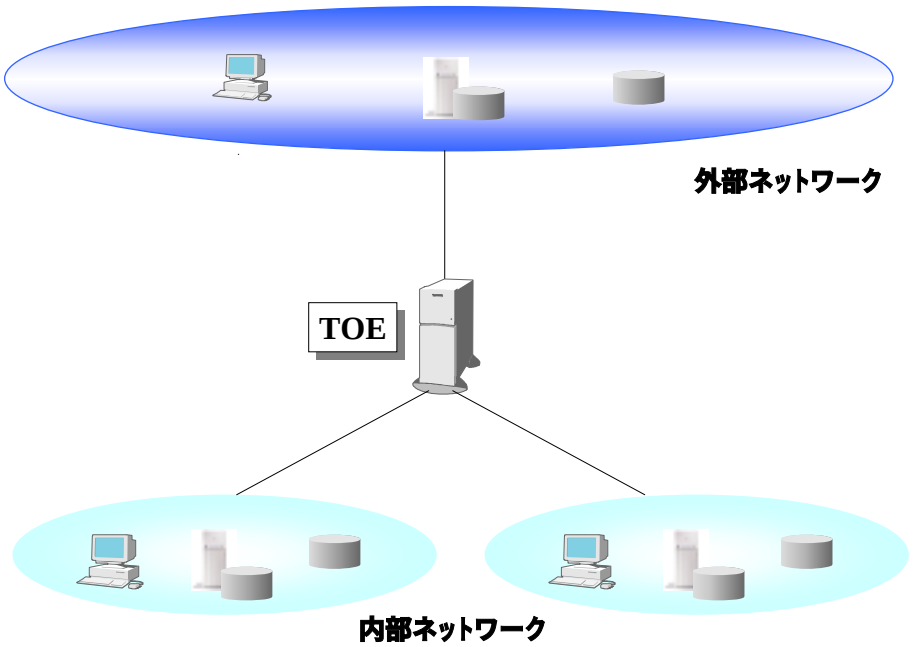
本TOEは、許可されたTOE管理者だけが運用可能である。

2.3 TOEの構成

本節では、TOEのネットワーク構成、及びハードウェア／ソフトウェア構成について説明する。

2.3.1 ネットワーク構成

本TOEは、複数のネットワークの境界点に位置する。
本TOEのネットワーク構成は、以下の通りである。



2.3.2 ハードウェア構成

本体装置／周辺装置

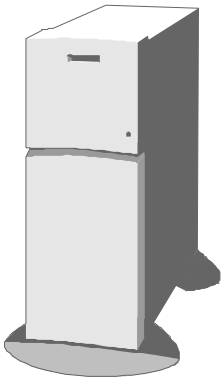
TOEは、Solaris OS(日本語Solaris 8) とともに以下の本体装置上で動作する。

- 富士通　GRANPOWER 7000Fシリーズ

TOE運用における上記本体装置上のハードウェア環境は、以下の通りである。

- CPU／メモリ
  CPUクロック数やMPシステム、メモリ容量など、TOEの運用要件に応じた構成
- ビットマップディスプレイ
  TOEの運用支援機能では、X－Windowシステム（Xサーバ）を利用して、ディスプレイケーブルで接続されたビットマップディスプレイ上にTOEの構成情報を表示している。
  なお、本ビットマップディスプレイ装置を用意できない場合、ネットワークで接続されたXサーバ機能を搭載した装置を利用することもできる。
- ハードディスク装置
  本TOEの構成情報（環境設定情報）、及び監査履歴を記録するためのハードディスク装置が必要である。
- ネットワークインタフェース
  本TOEに接続するネットワークインタフェース。
  １枚以上、８枚以下の制限がある。

その他の本体装置上のハードウェアについては、Solaris OSが動作するハードウェア構成であれば、TOEの動作のために特別なハードウェアを必要とはしない。



諸元		要件
CPU	主プロセッサ	運用要件に応じた選択要
	周波数	
	プロセッサ数	
キャッシュメモリ		
主記憶メモリ		
補助記憶	ディスク	TOE保護資産を格納するだけの容量が必要
	CD-ROM	TOEをインストールするために必要
	その他	外部媒体へTOE保護資産をバックアップするために、DAT、CD-R等が必要
I/O	ネットワーク	1以上8以下
	キーボード	TOE環境設定、監査機能を利用する場合に必要。ただし、Xサーバを利用する場合はXサーバで代替可能
	マウス	
ビットマップディスプレイ		

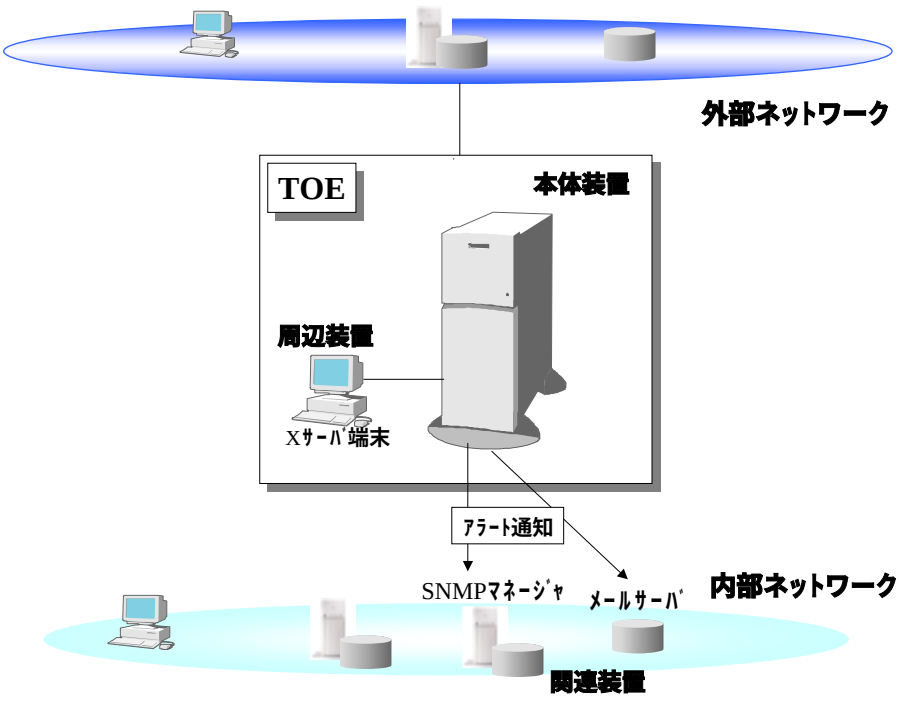
なお、Xサーバを利用する場合、TOEと同様、利用者から物理的にアクセスできない場所に設置され、かつ、利用者からの論理的なアクセス（リモートからのアクセスなど）からも保護されている利用環境である必要がある。

関連装置

本TOEの運用に応じて、以下の関連装置を利用する。

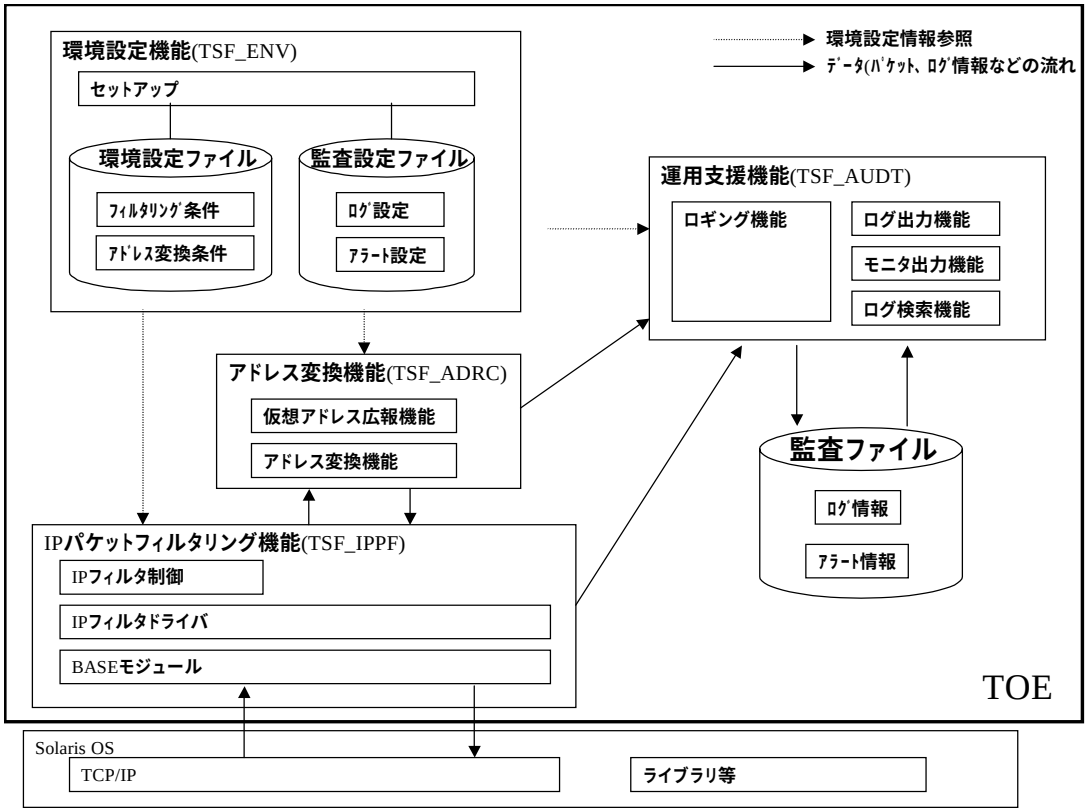
- メールサーバ
  本TOEの監査機能でアラートイベントを検出した場合に、アラートイベントを通知するメールサーバ
- SNMPマネージャ
  本TOEの監査機能でアラートイベントを検出した場合に、アラートイベントを通知するSNMPマネージャ

なお、上記ハードウェアは、「2.2 TOEの利用」に示すように、内部ネットワークに設置する必要がある。
以下に、本TOE、及び関連装置の構成を示す。



2.3.3 ソフトウェア構成

本TOEは、Solaris Operating System （日本語Solaris 8）上で動作する。
Solaris OSが標準で提供するライブラリ関数やシステムコール、又はデバイスドライバインタフェースを利用する。



2.4 ＴＯＥの機能

2.4.1 アクセス制御機能

(1) IPパケットフィルタリング機能(TSF_IPPF)

TSF_IPPFは、フィルタリング条件に従って、IPパケットデータを通過又は遮断する。

(2) アドレス変換機能(TSF_ADRC)

TSF_ADRCは、アドレス変換条件に従って、IPパケットデータのIPアドレスまたはポート番号を変換する。
本機能により、内部ネットワークアドレス、またはそのネットワークアドレス体系を保護しながらインターネットなどの外部ネットワークと通信することができる。

2.4.2 運用支援機能(TSF_AUDT)

TSF_AUDTは、TOEを通じてどのような通信が行われているかを解析／監視／通知する以下の機能を持ち、不正なアクセスを検出するための情報を提供する。

- ロギング機能
  TOEの動作状況を、ログ設定で指定された格納場所に格納する。
  また、アラートイベントの監視を行い、アラートイベントを検出した場合、アラート設定で指定された通知方法／通知先に対して、アラートイベントを通知する。
- ログ出力機能

格納されているログ情報を出力する。

- モニタ出力機能
  TOE の現在の動作状況を出力する。
- ログ検索機能
  ログ情報を検索する。

2.4.3 環境設定機能(TSF_ENV)

TSF_ENVは、TOEの動作環境を設定する機能を提供する。

- 環境設定機能
  TOEの実行環境に関する環境設定ファイル（フィルタリング条件、アドレス変換条件)、監査設定ファイル（ログ設定、アラート設定）を設定する。

2.5 TOEの保護資産

本TOEの保護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

本TOEは、複数のネットワークを接続する機能を持ち、かつ、不特定多数からアクセスのある特定の内部ネットワーク上の資産を保護する。内部ネットワーク上のどの資産を保護するかは、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システム運用管理部門が定める内部セキュリティポリシーによって決定される。

2.5.2 TOE関連資産

TOE関連資産には以下のものがある。

- 環境設定ファイル
- 監査ファイル

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

当TOEは、次のセキュアな使用環境を想定している。

識別子	タイトル	定義
ASM.1	物理的アクセス	TOE、及びXサーバ端末は、TOE管理者からしか物理的にアクセスできないように保護された環境に設置されている。
ASM.2	接続形態	TOE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形態で動作する。
ASM.3	信頼できるTOE管理者	TOE管理者は、TOE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を運用管理しなければならない。
ASM.6	関連装置の物理的アクセス	アラート情報のメール通知やSNMPマネージャ通知を行なう場合、通知先となるメールサーバ、及びSNMPマネージャは、内部ネットワークに設置する。

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、保護資産への想定される脅威について説明する。
想定される脅威は以下の通りである。

識別子	タイトル	定義
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利用者は、内部ネットワークに侵入し、内部ネットワークの保護資産の改ざん、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	外部ネットワーク及び内部ネットワークの利用者、またはTOE管理者がX端末を利用している場合、TOE管理者以外のX端末から、本TOEに侵入し、環境設定ファイルを改ざんして不正なIPパケットデータを通過させたり、監査ファイルを改ざん、又は破壊し、不正行為の証拠を隠滅する恐れがある。
T3	内部ネットワーク保護資産の意図しない漏洩	内部ネットワークの利用者が外部ネットワークへアクセスする場合、内部ネットワークのIPアドレス体系が外部ネットワークの利用者に漏洩する恐れがある。

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ない。

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

TOEに対するセキュリティ対策方針は、以下の通りである。

識別子	タイトル	定義
O.AC	外部ネットワーク利用者の制限	TOEは、TOE又は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の利用者を制限する。
O.ADRC	内部ネットワークのIPアドレスの隠遁	内部ネットワークの利用者が外部ネットワークにアクセスする場合、内部ネットワークの接続元IPアドレス情報を外部ネットワークに対して隠蔽できなければならない。
OOE.ADMIN	TOE管理者制御	TOEは、TOE管理者だけが環境設定ファイルの動作環境の制御を行うことができるよう、TOE管理者のアクセス制御機能を提供しなければならない。 なお、本セキュリティ対策方針は、環境のセキュリティ対策方針にも適用される。
OOE.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／時間を伴なって記録する機能を提供しなければならない。 なお、本セキュリティ対策方針は、環境のセキュリティ対策方針にも適用される。
O.AUDMON	監視機能	TOEは、監査記録を元に、外部ネットワークからの不正な侵入を監視する機能を提供しなければならない。
O.ACX	X端末からの接続の制限	TOE管理者がX端末を利用する場合は、特定のX端末からだけアクセスできるよう制限しなければならない。

注）識別子「OOE.」のセキュリティ対策方針は、TOE及び環境双方に適用されるセキュリティ対策方針である。

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。

識別子	タイトル	定義
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を管理、運用しなければならない。
OE.2	物理的保護	TOE管理者だけが、TOEに物理的にアクセスできるよう、TOEを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の管理、運用ができるよう、TOE管理者を教育しなければならない。
OE.5	提供サービス	TOE が搭載されたサーバ上では、TOE以外のアプリケーションサービスは提供してはならない。
OE.6	接続形態	本TOE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構成しなければならない。
OE.7	利用者の教育	TOE管理者は、内部ネットワークの利用者が内部ネットワークのアドレス体系を漏らさないよう、利用者を教育しなければならない。
OE.8	関連装置の設置	アラート情報のメール通知やSNMPマネージャ通知を行なう場合、通知先となるメールサーバ、及びSNMPマネージャは、内部ネットワークに設置しなければならない。
OE.9	X端末の接続	X端末はTOE管理者専用端末として、TOE管理者のみが物理的にアクセスできるように保護しなけれ

識別子	タイトル	定義
		ばいけない。

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

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

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

管理: FDP_IFC.1

このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_IFC.1

FAU_GEN セキュリティ監査データ生成がPP/ST に含まれている場合でも、監査対象とすべき識別された事象はない。

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]

IPパケットフィルタリング方針（SFP_IPPF）

[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、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は、以下の通りである。

- サブジェクト
  TOEのネットワークインタフェース
- 情報
  IPパケットデータ
- 操作
  通過または遮断

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）

FDP_IFF.1 単純セキュリティ属性

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

管理: FDP_IFF.1

以下のアクションはFMT 管理の管理機能と考えられる:

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。

監査: FDP_IFF.1

FAU_GEN セキュリティ監査データ生成がPP/ST に含まれていれば、以下の事象を監査対象にすべきである:

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)。

監査レベル：最小、基本、詳細（C）

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:セキュリティ属性の最小数及び種別]。

[割付：情報フロー制御SFP]

IPパケットフィルタリング方針（SFP_IPPF）

[割付：セキュリティ属性の最小数及び種別]

セキュリティ属性の最小数及び種別は、以下の通り。

- 最小数
  0（フィルタリング条件が設定されていない時に、無条件に遮断となるため）
- サブジェクトのセキュリティ属性
  - ネットワークインタフェース
- 情報のセキュリティ属性
  - 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）
  - ポート番号

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]

アドレス変換条件に従って、通過するIPパケットデータの内部ネットワークアドレスを外部ネットワークに公開するグローバルアドレスに変換する。

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

セキュリティ監査自動応答（FAU_ARP）

FAU_ARP.1 セキュリティアラーム

セキュリティアラームでは、TSF は、セキュリティ侵害の可能性が検出された場合にアクションをとらなければならない。

下位階層

なし

管理: FAU_ARP.1

以下のアクションはFMTの管理機能と考えられる:

a) アクションの管理（追加、除去、改変）。

監査: FAU_ARP.1

FAU_GEN セキュリティ監査データ生成がPP/ST に含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 切迫したセキュリティ侵害によってとられるアクション。

監査レベル：最小

FAU_ARP.1.1

TSFは、セキュリティ侵害の可能性が検出された場合、[割付:混乱を最小にするアクションのリスト]を実行しなければならない。

[割付:混乱を最小にするアクションのリスト]

- アラートイベントの通知

依存性

FAU_SAA.1 侵害の可能性の分析

セキュリティ監査事象選択（FAU_SEL）

FAU_SEL.1 選択的監査

選択的監査は、PP/ST 作成者によって特定される属性に基づき、監査される事象のセットから事象を含めたり除外する能力を要求する。

下位階層

なし

管理: FAU_SEL.1

以下のアクションは、FMTの管理機能と考えられる:

a) 監査事象を閲覧／改変する権限の維持。

監査: FAU_SEL.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小：監査データ収集機能が作動している間に生じる、監査設定へのすべての改変。

監査レベル：最小

FAU_SEL.1.1

TSFは以下のような属性に基づいて、監査事象のセットから監査対象事象を含めたり、除外したりすることができなければならない:

a) [選択:オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別]
b) [割付:監査の選択性の基礎となる追加属性リスト]。

[選択:オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別]

- サブジェクト識別情報

[割付:監査の選択性の基礎となる追加属性リスト]

- 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）
- ポート番号

依存性

FAU_GEN.1 監査データ生成
FMT_MTD.1 TSFデータの管理

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

監査データ生成は、監査対象事象のレベルを定義し、各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

管理: FAU_GEN.1

予見される管理アクティビティはない。

監査: FAU_GEN.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象とすべき識別されたアクションはない。

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]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

[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

● アドレス変換実施時のセキュリティ属性

以下の監査記録を生成する。

表 5.1

機能要件	監査レベル	監査対象事象	監査項目	監査方法	要約仕様
FDP_IFC.1	—	なし	—	—	—
FDP_IFF.1	最小、基本、詳細(C)	情報フローに対する要求に関するすべての決定 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	IPパケットデータに対する処理結果、およびその判定に使用されたセキュリティ属性	IPフィルタリング機能、及びアドレス変換機能のログ情報の参照	AUD.141 AUD.142
FAU_ARP.1	最小	切迫したセキュリティ侵害によってとられるアクション	TOE 管理者へのアラートイベントの通知事象	IPパケットフィルタリングログに記録されるアラート情報の参照	AUD.141
FAU_SEL.1	最小	監査データ収集機能が作動している間に生じる、監査設定へのすべての改変	環境設定機能の起動／終了事象	ファイアウォールサービスの起動／終了情報の参照	AUD.44
FAU_GEN.1	—	なし	—	—	—
FAU_SAA.1	最小(a)	すべての分析メカニズムの活性化／非活性化	運用支援機能の起動／終了事象	ファイアウォールサービスの起動／終了情報の参照	AUD.44
	最小(b)	ツールによって実行される自動応答	TOE 管理者へのアラートイベントの通知事象	IPパケットフィルタリングログに記録されるアラート情報の参照	AUD.141
FAU_SAR.1	基本	監査記録からの情報の読み出し	運用支援機能の起動／終了事象	ファイアウォールサービスの起動／終了情報の参照	AUD.44
FAU_STG.2	—	なし	—	—	—

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

セキュリティ監査分析（FAU_SAA）

FAU_SAA.1 侵害の可能性の分析

侵害の可能性の分析では、固定した規則セットに基づく基本閾値による検出が要求される。

下位層

なし

管理: FAU_SAA.1

以下のアクションはFMTの管理機能と考えられる:

a) 規則のセットから規則を（追加、改変、削除）することによる規則の維持。

監査: FAU_SAA.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきであ

る:

a) 最小:すべての分析メカニズムの活性化／非活性化。
b) 最小:ツールによって実行される自動応答。

監査レベル：最小

FAU_SAA.1.1

TSFは、監査事象のモニタに規則のセットを適用し、これらの規則に基づきTSP侵害の可能性を示すことができなければならない。

FAU_SAA.1.2

TSFは、監査事象をモニタするための以下の規則を実施しなければならない;

a) セキュリティ侵害の可能性を示すものとして知られている[割付:定義された監査対象事象のサブセット]をすべて合わせた、あるいは組み合わせたもの;
b) [割付:その他の規則]。

[割付:定義された監査対象事象のサブセット]

以下のいずれかの場合TSP侵害の可能性がある。

- 単位時間内に、同一の送信元IPアドレスからのIPパケットデータが、指定された回数分遮断。
- 単位時間内に、同一の送信先IPアドレスへのIPパケットデータが、指定された回数分遮断。
- 指定された送信先ポート番号へのIPパケットデータを検出。

[割付: その他の規則]

なし

依存性

FAU_GEN.1 監査データ生成

セキュリティ監査レビュー（FAU_SAR）

FAU_SAR.1 監査レビュー

監査レビューは、監査記録からの情報読み出し能力を提供する。

下位階層

なし

管理: FAU_SAR.1

以下のアクションはFMTの管理機能と考えられる:

a) 監査記録に対して読み出し権のある利用者グループの維持（削除、改変、追加）。

監査: FAU_SAR.1

セキュリティ監査データ生成（FAU_GEN）がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

a) 基本：監査記録からの情報の読み出し。

監査レベル：基本

FAU_SAR.1.1

TSFは、[割付:許可利用者]が、[割付:監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付:許可利用者]

TOE管理者

[割付:監査情報のリスト]

- IPパケットフィルタリング機能の稼動状況
- アドレス変換機能の稼動状況
- フィルタリング条件情報
- 各運用支援機能の動作履歴
- 環境設定機能の動作履歴
- パケット処理結果
- アラート情報

FAU_SAR.1.2

TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性

FAU_GEN.1 監査データ生成

セキュリティ監査事象格納（FAU_STG）

FAU_STG.2 監査データ可用性の保証

監査データ可用性の保証は、望ましくない条件の発生において、TSF が監査データに対して維持する保証を規定する。

下位階層

FAU_STG.1

管理: FAU_STG.2

以下のアクションはFMTの管理機能と考えられる:

a) 監査格納機能を制御するパラメタの維持。

監査: FAU_STG.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査すべき識別されたアクションはない。

FAU_STG.2.1

TSFは、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.2.2

TSFは、監査記録の改変を[選択：防止、検出]できねばならない。

[選択: 防止、検出]

防止

FAU_STG.2.3

TSFは、[選択：監査格納の領域枯渇、失敗、攻撃]という状況が生じた場合、[割付：救済する監査記録の数値尺度]の監査記録が維持されることを保証しなければならない。

[選択: 監査格納の領域枯渇、失敗、攻撃]

監査格納領域枯渇

[割付: 救済する監査記録の数値尺度]

TOE管理者が定めるディスク容量分

依存性

FAU_GEN.1 監査データ生成

5.1.2 TOEセキュリティ保証要件

本TOEは、一般のコマーシャルシステムの中で利用される。ただし、TOEが搭載されるシステムは管理専用であるために、運用／管理面で、セキュリティ確保ができる。このため、コマーシャルシステム用として、十分なレベルであるEAL3を品質保証レベルとする。

なお、EAL3を超える特定の保証対策はない。

クラス	コンポーネント名（ファミリ含む）	
ACM（構成管理）	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOEのCM範囲
ADO（配付と運用）	ADO_DEL.1	配付手続き
	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_HLD.2	セキュリティ実装上位レベル設計
	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

クラス	コンポーネント名（ファミリ含む）	
	AGD_USR.1	利用者ガイダンス
ALC（ライフサイクルサポート）	ALC_DVS.1	セキュリティ手段の識別
ATE（テスト）	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト：上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト－サンプル
AVA（脆弱性評定）	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOEセキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.1.3 機能強度

本STの最小機能強度レベルは、SOF-基本 とする。

5.2 IT環境に対するセキュリティ要件

ここでは、TOEのセキュリティ対策方針に対処するために、IT環境で応じるTOEのITセキュリティ要件の詳細について記述する。
以下のセキュリティ要件は、本TOEの環境設定データおよび監査データの管理に関連する。
そして各々のデータは、TOE管理者のみがアクセスを許され、それらへのアクセス制御機能は、Solaris OSによって提供される。

アクセス制御方針（FDP_ACC）

FDP_ACC.1 サブセットアクセス制御

サブセットアクセス制御は、TOE におけるオブジェクト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、識別された各アクセス制御SFP が適切なものであることを要求する。

下位階層

なし

FDP_ACC.1.1

TSF は、[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して、[割付: アクセス制御SFP]を実施しなければならない。

[割付：アクセス制御SFP]

アクセス制御方針（SFP_ACC）

[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

アクセス制御方針の対象とするサブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリストは、以下の通り。

- サブジェクト
  TOE管理者プロセス
- オブジェクト
  環境設定ファイル
- SFPで扱われるサブジェクトとオブジェクト間の操作のリスト
  - 問い合わせ
  - 改変

依存性

FDP_ACF.1 セキュリティ属性によるアクセス制御

アクセス制御機能（FDP_ACF）

FDP_ACF.1 セキュリティ属性によるアクセス制御

セキュリティ属性に基づくアクセス制御は、TSFが、セキュリティ属性と名前を付けられた属性グループに基づくアクセスを実施することを許可する。さらに、TSFは、セキュリティ属性に基づいてオブジェクトへのアクセスを明示的に正当化あるかは拒否する能力を持ってもよい。

下位階層

なし

FDP_ACF.1.1

TSF は、[割付: セキュリティ属性、名前付けされたセキュリティ属性のグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御SFP]を実施しなければならない。

[割付：アクセス制御SFP]

アクセス制御方針（SFP_ACC）

[割付: セキュリティ属性、名前付けされたセキュリティ属性のグループ]

TOE管理者プロセスに関連付けられる利用者属性

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない:[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

TOE 管理者プロセスに関連付けられる利用者属性がTOE 管理者の場合、サブジェクトはオブジェクトに対する操作（問合せ、又は改変）を許可され、それ以外であれば操作が拒否される。

FDP_ACF.1.3

TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセス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オブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]

なし

FDP_ACF.1.4

TSF は、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセス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オブジェクトに対するサブジェクトのアクセスを明示的拒否する規則]

なし

依存性

FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

利用者認証（FIA_UAU）

FIA_UAU.1 認証のタイミング

認証のタイミングは、利用者の識別情報の認証の前に、利用者があるアクションを実行することを認める。

下位階層

なし

FIA_UAU.1.1

TSFは、利用者が認証される前に利用者を代行して行なわれる[割付:TSF調停アクションのリスト]を許可しなければならない。

[割付:TSF調停アクションのリスト]

- 言語・デスクトップ環境等の設定、ヘルプの表示

FIA_UAU.1.2

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**識別のタイミング**

利用者識別（FIA_UID）

FIA_UID.1 識別のタイミング

識別のタイミングは、利用者がTSF によって識別される前に利用者があるアクションを実行することを認める。

下位階層

なし

FIA_UID.1.1

TSFは、利用者が識別される前に利用者を代行して実行される[割付:TSF調停アクションのリスト]を許可しなければならない。

[割付:TSF調停アクションのリスト]

- 言語・デスクトップ環境等の設定、ヘルプの表示

FIA_UID.1.2

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、各利用者に識別が成功することを要求しなければならない。

依存性

なし

TSF における機能の管理(FMT_MOF)

FMT_MOF.1 セキュリティ機能のふるまいの管理

セキュリティ機能のふるまいの管理は、許可利用者(役割)が、規則を使用するか、あるいは管理可能にし得る特定の条件を持つ、TSF における機能のふるまいを管理することを許可する。

下位階層

なし

FMT_MOF.1.1

TSFは、機能[割付: 機能のリスト][選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]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: 機能のリスト]

- IPパケットフィルタリング機能
- アドレス変換機能
- 運用支援機能
- 環境設定機能

[選択: のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]

TSFのふるまいを制御する、のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する行為

[割付: 許可された識別された役割]

TOE管理者

依存性

FMT_SMR.1 セキュリティ役割

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

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[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]

- 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）
- ポート番号
- ネットワークインタフェース

[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]

TOE管理者

[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（SFP_IPPF））

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 セキュリティ役割

FMT_MSA.3 静的属性初期化

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、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、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（SFP_IPPF））

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）

FMT_MTD.1 TSFデータの管理

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

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]

- 監査設定ファイル（ログ設定、アラート設定）

[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

[割付:許可された識別された役割]

TOE管理者

依存性

FMT_SMR.1 セキュリティ役割

セキュリティ管理役割（FMT_SMR）

FMT_SMR.1 セキュリティ役割

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

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

リファレンス調停（FPT_RVM）

FPT_RVM.1 TSPの非バイパス性

TSP の非バイパス性

下位階層

なし

FPT_RVM.1.1

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

依存性

なし

ドメイン分離（FPT_SEP）

FPT_SEP.1 TSFドメイン分離

TSF ドメイン分離は、TSF のための区分された保護ドメインを提供し、かつTSC 内のサブジェクト間の分

離を提供する。

下位階層

なし

FPT_SEP.1.1

TSFは、それ自身の実行のため、 信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2

TSFは、TSC内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性

なし

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

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

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要約仕様とセキュリティ機能要件の関係をしめす。

表 6.1

仕様概要 / 機能要件	IPPF.1	IPPF.2	ADRC.1	AUD.1	AUD.2	AUD.3	AUD.4	ENV.1
FAU_ARP.1					○			○
FAU_GEN.1				○			○	○
FAU_SAA.1					○			○
FAU_SAR.1				○		○	○	
FAU_SEL.1				○		○		○
FAU_STG.2				○				
FDP_IFC.1	○	○	○					○
FDP_IFF.1	○	○	○					○

6.1.1 IPパケットフィルタリング機能（SFP_IPPF)

IPパケットフィルタリング機能は、以下の機能を提供する。

IPPF.1

IPパケットフィルタリング機能（以降IPフィルタ機能と呼ぶ）は、TOE管理者が設定した条件に従って、IPパケットデータを通過／遮断する機能である。また、通過を許可されたIPパケットにアドレス変換処理を適用する必要がある場合、アドレス変換機能に当該IPパケットを転送する機能を保持している。
通過／遮断を決める条件を‘フィルタリング条件’といい、以下の指定が可能である。

- ネットワークインタフェース単位によりパケットの通過可否の設定
- 特定のあて先または特定のホストグループによりパケットの通過可否の設定
- 特定のサービス単位（telnet、ftpなど）によりパケットの通過可否の設定
- 特定のプロトコル（TCP、UDP、ICMP）によりパケットの通過可否の設定
- パケットの通過方向によりパケットの通過可否の設定
- 上記設定の組み合わせでパケットの通過可否の設定

IPパケットフィルタリング機能を実現するプログラムは、Solaris OSのSTREAMS機構上に実装され、ネットワークプロトコル(IP)層とネットワークドライバ（ネットワークインタフェースのデバイスドライバ）層の中間に挿入(push)されるSTREAMSモジュールである。
IPパケットフィルタリング機能では、通常、通過させたいIPパケット（IPアドレス、プロトコルサービスの詳細情報の組み合わせ）を“通過”条件として明示的に設定する。
ある範囲で一部だけを通過させたくない場合は、ある範囲で“通過”の設定を行った上で通過させたくない一部を“遮断”として設定する。

IPPF.2

上記のどの条件にも合致しなかった場合、パケットは遮断となる。

6.1.2 アドレス変換機能 (SFP_ADRC)

アドレス変換機能は、以下の機能を提供する。

ADRC.1

アドレス変換機能は、内部ネットワークのIPアドレスを隠蔽するために、別のIPアドレスに変換する。
アドレス変換の動作には、以下のものがある。

- NAT 方式
  外部ネットワーク上のホストと通信を行う内部ネットワーク上のホストのIPアドレスは、送信時に外部ネットワークに公開されたIPアドレスに変換され、受信時に元のIPアドレスに戻される。
- IPマスカレード方式
  外部ネットワーク上のホストと通信を行う内部ネットワーク上のホストのIPアドレス及びポート番号は、送信時にTOE の外部ネットワーク側のIPアドレス及びTOE 上の未使用のポート番号に変換され、受信時に元のIPアドレス及びポート番号に戻される。

これらの処理は本TSFが自動的に行うため、利用者は本TSFの存在を意識せずにサービスを利用できる。

6.1.3 運用支援機能 (SFP_AUD)

運用支援機能では、以下の機能を提供する。

- ロギング機能
- アラート機能
- モニタリング機能
- 稼動状況通知機能

以下に、それぞれの機能について説明する。
なお、それぞれの機能は、TOE管理者のみ実行できる。

6.1.3.1 ロギング機能 (AUD.1)

ロギング機能は、本TOE で処理した情報を記録する機能である。

AUD.11

ロギング機能の開始

ロギング機能は、TOE 起動時に自動的に起動され、起動された事象がログ情報に記録される。
ロギング機能を停止する場合には、停止操作を行います。このとき、停止された事象がログ情報に記録される。

AUD.12

ロギング情報の出力

記録されたロギング情報は、以下のいずれかの方法で参照することができる。

- ロギング情報の出力
  ロギング情報を標準出力に出力する。
  出力するロギング情報を選択することができる。
- ロギング情報の検索
  検索するロギング情報を指定し、画面上に出力する。

AUD.13

ロギング情報の記録

ロギング情報は、以下のように管理される。

- ロギング情報は監査ファイルに記録される。TOE管理者は、本TOEを通過するIPパケットデータのトラフィックに応じた適切な容量の監査ファイルを定義する。
- 監査ファイルの容量オーバとなった場合、TOEは最も古いロギング情報から上書きを行う。

AUD.14

ロギング情報の種類

記録されるロギング情報には、以下の種類がある。

- IPパケットフィルタリングログ

IPパケットフィルタリング機能（TSF_IPPF)のIPパケット処理状況を記録する。

- アドレス変換ログ
  アドレス変換機能（TSF_ADRC)で中継したIPパケットの処理状況を記録する。

AUD.141

IPパケットフィルタリングログ

IPパケットフィルタリング機能で処理したロギング情報である。
以下の情報が記録される。

- 統計情報
  ネットワークインタフェースごとの累積通過パケット数、累積破棄パケット数などが記録される。
- アラート情報
  アラート事象を検出した場合、アラート事象が記録される。
- コネクション情報
  IPプロトコルがTCP の場合、１対のTCPコネクションの確立／解放（強制解放を含む）の通信状況（通過、破棄など）が記録される。
  IPプロトコルがUDP/ICMPの場合、コネクションの概念はないため、すべてのIPパケットの通信状況（通過、破棄など）が記録される。

コネクション情報として記録される情報は、以下の通りである。

項目	説明
番号	ログ情報に対するレコード番号
日付・時刻	IPフィルタでパケットを処理した日付・時刻
インタフェース	IPパケットデータを検出したネットワークインタフェース
方向	IPパケットデータの入出力方向
送信元IP	IPパケットデータの送信元IPアドレス
送信先IP	IPパケットデータの送信先IPアドレス
プロトコル	IPプロトコル
送信元ポート	送信元ポート番号（IPプロトコルがTCP/UDPの場合)、又は メッセージタイプ・コード（IPプロトコルがICMPの場合）
送信先ポート	送信先ポート番号（IPプロトコルがTCP/UDPの場合)、又は メッセージタイプ・コード（IPプロトコルがICMPの場合）
結果	パケットの処理結果 pass：通過を許可されたIPパケットデータ block：遮断されたIPパケットデータ nat：アドレス変換機能で処理されたIPパケットデータ
TCPフラグ	IPプロトコルがTCPの場合、TCPパケットのデータ種別 なお、複数のビットがセットされている場合、すべての情報が列挙される。 S ：SYNビットセット F：FINビットセット R：RSTビットセット P：PUSHビットセット A：ACKビットセット U：Urgentビットセット

ロギング情報の選択

記録されるロギング情報は、ネットワークインタフェース、又はフィルタリング条件のなかで選択することができる。

- ネットワークインタフェース
  IPパケットデータを検出したネットワークインタフェースごとに、ロギング情報の採取有無を選択することができる。
- フィルタリング条件
  個々のフィルタリング条件（送信元IPアドレス／送信先IPアドレス、IPプロトコル、ポート番号、IPパケットデータの通過／遮断）ごとに、ロギング情報の採取有無を選択することができる。

AUD.142

アドレス変換ログ

アドレス変換機能 (TSF_ADRC)で中継したロギング情報である。
以下の情報が記録される。

- 統計情報
  送信元ポート番号（サービス）ごとの中継コネクション数および転送データ量。
- コネクション情報
  IPプロトコルがTCP の場合、１対のTCPコネクションの確立／解放（強制解放を含む）の中継情報。
  IPプロトコルがUDP/ICMPの場合、コネクションの概念はないため、すべてのIPパケットの通信情報。

コネクション情報として記録される情報は、以下の通りです。

項目	説明
番号	ログ情報に対するレコード番号
日付・時刻	透過ゲートウェイでパケットを処理した日付・時刻
送信元IP	IPパケットデータの送信元IPアドレス
送信元ポート	IPパケットデータの送信元ポート番号(IPプロトコルがTCP/UDPの場合)、又はメッセージタイプ・コード（IPプロトコルがICMPの場合）
（中継）送信元IP	中継処理後のIPパケットデータの送信元IPアドレス
（中継）送信元ポート	IPパケットデータの中継処理後の送信元ポート番号(IPプロトコルがTCP/UDPの場合)、又は中継処理後のメッセージタイプ・コード（IPプロトコルがICMPの場合）送信元ポート番号
送信先IP	IPパケットデータの送信先IPアドレス
送信先ポート	IPパケットデータの送信先ポート番号(IPプロトコルがTCP/UDPの場合)、又はメッセージタイプ・コード（IPプロトコルがICMPの場合）
プロトコル	IPプロトコル
種別	中継パケットの処理種別 con：コネクション確立 dis：コネクション解放

6.1.3.2 アラート機能 (AUD.2)

TOE 運用中に不正なパケットを検出した場合（これを、アラートイベントと呼びます）に、システムログ(syslog)に通知したり、ロギングしたりする機能である。また、アラートイベント発生時に実行するコマンドを登録しておくことで、TOE管理者はイベントログを常に監視していなくても、アラートイベントの発生に対して柔軟に対応することができる。
以下に、通知されるアラートの種類、アラートの通知方法、アラートの通知形式およびロギングについて説明する。

AUD.21

アラートの種類

アラートイベントには、以下の種類がある。

- 同一送信元アラート
  同一の送信元アドレスからのIPパケットデータがパケット監視単位時間内に規定数以上破棄された場合、アラートイベントが発生したものとみなす。
- 同一送信先アラート
  同一の送信先アドレスの同一送信先ポート番号に対するIPパケットデータがパケット監視単位時間内に規定数以上破棄された場合、アラートイベントが発生したものとみなす。
- 監視ポートアラート
  あらかじめ設定された監視対象ポート番号宛てのIPパケットデータを検出した場合、IPパケットデータの処理結果（通過、破棄など）に関わらず、アラートイベントが発生したものとみなす。

AUD.22

アラートイベントの通知方法

アラートイベントが発生した場合、以下のいずれかの方法でアラートイベントを通知する。

- コンソール出力
  アラートイベント発生時に、検出時刻、アラート種別などをコンソールに表示する。

- メール送信
  TOE管理者（アラート設定で指定した通知者リスト中に含まれている利用者）にメールで通知する。
- モニタリング機能通知
  本TOE のモニタリング機能に、アラートイベントが通知される。
- コマンド起動
  あらかじめ設定されているコマンドを起動する。
- SNMP マネージャ通知
  SNMP 連携機能を利用して、SNMPマネージャに通知することができる。
- システムログ（syslog）出力
  Solarisオペレーティングシステムのシステムログ（syslog）に出力することができる。

6.1.3.3 モニタリング機能 (AUD.3)

IPパケットフィルタリング機能、アドレス変換機能のIPパケットの処理状況をリアルタイムに表示する。

AUD.31

IPパケットフィルタリングモニタ機能

パケットフィルタリングモニタ機能では、IPパケットフィルタリング機能が処理しているネットワークアダプタ単位にパケットの通過、破棄状況がグラフ、又は表形式で表示される。
また、アラートイベントが発生した場合、アラート機能(AUD.2)から受信した情報が表示される。

AUD.32

アドレス変換モニタ機能

アドレス変換モニタ機能では、アドレス変換機能が処理しているそれぞれのコネクションの中継情報が表示される。

6.1.3.4 稼動状況通知機能 (AUD.4)

稼動状況通知機能は、IPパケットフィルタリング機能、アドレス変換機能に関する稼動状況を通知する。

AUD.41

通知情報

通知される稼動状況に関する情報には、以下のものがある。

通知情報	管理者インタフェース
環境設定情報更新時間 ファイアウォールサービス稼動状況	sgstatコマンド
ファイアウォールサービスの起動／終了情報	fwaudlogdspコマンド

AUD.42

環境設定情報更新時間

環境設定情報の更新時間と最終適用時間は、sgstatコマンドで参照することができる。
本機能では、以下の情報が通知される。

- 現在適用されている環境設定情報の最終更新時間
- 現在適用されている環境設定情報の最終適用時間

AUD.43

ファイアウォールサービス稼動状況

ファイアウォールサービスの稼動状況は、sgstatコマンドで参照することができる。
本機能では、以下の情報が通知される。

- ファイアウォールサービスの起動状況
- ファイアウォールサービスの最終起動時間

AUD.44

ファイアウォールサービスの起動／終了情報

ファイアウォールサービスの起動／終了情報は、fwaudlogdspコマンドで参照することができる。
本機能では、以下のファイアウォールサービスの起動／終了情報を参照することができる。

ファイアウォールサービス	情報種別	実行コマンド

ファイアウォールサービス	情報種別	実行コマンド
IPフィルタサービス	起動	/opt/FSUNfwip/bin/actipfil
	停止	/opt/FSUNfwip/bin/dactipfil
アドレス変換サービス	起動	（自動起動）
	停止	（自動起動）
セットアップ	起動	/opt/FSUNfwip/bin/sgsetup
ロギング機能	起動	/opt/FSUNfwip/bin/strfillog
	終了	/opt/FSUNfwip/bin/stpfillog
ログ出力（IPフィルタ）	起動	/opt/FSUNfwip/bin/prtfillog
ログ出力（アドレス変換）	起動	/opt/FSUNfwip/bin/prttrplog
ログ表示（IPフィルタ）	起動	/opt/FSUNfwip/bin/plog
ログ表示（アドレス変換）	起動	/opt/FSUNfwip/bin/tlog
モニタ（IPフィルタ）	起動	/opt/FSUNfwip/bin/pmon
モニタ（アドレス変換）	起動	/opt/FSUNfwip/bin/tmon

6.1.4 環境設定機能（SFP_ENV）

TOE の動作環境を設定する。
なお、本機能は、TOE管理者のみが環境設定ファイルや監査設定ファイルへの問合せ、改変の操作が可能である。

ENV.1

環境設定手順

以下の手順で環境設定を行う。

1. 環境設定機能（セットアップ）の起動
   環境設定を行う場合、環境設定機能（セットアップ）を起動する。
2. ネットワーク構成図の作成
   ネットワークシステムの構成要素の関係を表す構成図を作成する。
3. 要素設定
   ネットワークシステムを構成する以下の各要素（ネットワーク構成図で作成した各要素）に対し、設定情報や動作環境などを設定する。
   - インタフェース
     ネットワークインタフェースの情報を設定する。
   - ホスト
     パケットフィルタリングの条件を設定するホストおよび仮想アドレスを設定する。
   - ホストグループ
     複数のホストに対して同じパケットフィルタリング条件を設定する場合にホストグループを作成することができます。同じ条件を設定するホストをグループ化すると、パケットフィルタリング条件を設定する場合に、そのグループに対して一度に条件を設定することができる。
   - ネットワーク
     同一ネットワーク上の複数のホストに対して同じパケットフィルタリング条件を設定する場合に、ネットワークアドレスおよびサブネットを指定し、ネットワークを作成することができる。ネットワークを作成すると、パケットフィルタリング条件を設定する場合に、そのネットワークに対して一度に条件を設定することができる。
   - 透過ゲートウェイ動作環境
     アドレス変換機能（本TOEでは、アドレス変換機能を提供する機能を、“透過ゲートウェイ”と呼ぶ）を使用する場合、その動作環境を設定する。
4. サービス設定
   セキュリティポリシーを設定するサービスに関する設定を行う。
   - プロトコル
     利用できるIPプロトコルを参照できる。
   - サービス
     サービスを設定する。
   - サービスグループ
     複数のサービスに対して、同じセキュリティポリシーを設定する場合にサービスグループを作成できる。同じ条件を設定するサービスをグループ化すると、セキュリティポリシーを設定す

る場合に、そのサービスグループに対して一括して設定することができる。

5. ログ／アラート
   ロギング機能およびアラート機能に関する設定を行う。
   ロギング設定
   ロギング機能の動作環境が変更できる。
   アラート設定
   アラート機能の動作環境が変更できる。
6. パケットフィルタリング条件の設定
   要素設定およびサービス設定で定義した項目を組み合わせて、パケットフィルタリングを行う場合の条件を設定する。
7. セットアップの終了とシステムの再起動
   動作環境の設定後、セットアップを終了し、システムの再起動（IPパケットフィルタリング機能の活性化、アドレス変換機能の活性化等）を行う。

運用形態と設定項目

以下に、運用形態別に必要な設定項目について説明する。

表: IP フィルタリングおよび透過ゲートウェイを行う場合に必要な設定項目

運用形態 / 作業	IPパケットフィルタリング機能	IPパケットフィルタリング機能 アドレス変換機能
ネットワーク構成図	○	○
インタフェース設定	○	○
ホスト設定	○	○
ホストグループ設定	△	△
ネットワーク環境設定	△	△
透過GW動作環境設定	X	○
サービス設定	△	△
サービスグループ設定	△	△
ロギング設定	△	△
アラート設定	△	△
パケットフィルタリング条件設定	○	○

○：必須
△：運用に応じて設定
X：不要

6.1.5 TOE管理者インタフェース

TOE 管理者に提供されるインタフェースには、以下のものがある。
これらのインタフェースは、TOE管理者権限であるシステム管理者権限でのみ実行できる。

IPパケットフィルタリング機能

- IPパケットフィルタリング機能の活性化
- IPパケットフィルタリング機能の非活性化
- コネクション監視タイマのチューニング
- 最大コネクション数のチューニング
- SYN Attack防止機能有無のチューニング
- FTPプロトコルのサポートサブコマンドのチューニング
- TCPパケットブロック時の動作モードのチューニング
- IPフィルタ非活性時の動作モードのチューニング

アドレス変換機能

- アドレス変換機能の活性化
- アドレス変換機能の非活性化
- 仮想アドレス広報機能機能の活性化
- 仮想アドレス広報機能機能の非活性化

運用支援機能

- IPパケットフィルタログ出力

- IPパケットフィルタログ参照
- IPパケットフィルタモニタ出力
- IPパケットフィルタロギングの開始
- IPパケットフィルタロギングの停止
- アドレス変換ログ出力
- アドレス変換ログ参照
- アドレス変換モニタ出力
- ファイアウォール機能稼動状況表示
- ファイアウォール機能の全サービス起動
- ファイアウォール機能の全サービス停止
- ファイアウォール機能実行ログの表示

環境設定機能

- セットアップ
- インタフェース情報の設定
- リモートX 端末運用のための条件設定
- SNMP連携のための条件設定
- 環境設定情報（ポリシー）の移出
- 環境設定情報（ポリシー）の移入
- IPフィルタ非活性時のフィルタ動作モードの表示
- IPフィルタ非活性時のフィルタ動作モードの設定
- ファイアウォール機能実行ログ環境の設定

6.2 保証手段

EAL3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6.2.1 保証手段

クラス	コンポネント名	保証手段
構成管理(ACM)	ACM_CAP.3 ACM_SCP.1	TOE構成要素の完全性を保証するために、必要な規定・手順を遵守し、かつその運用履歴を記録する。 以下のドキュメントを参照のこと。 ソフトウェア基本開発プロセス運用規程 開発プロセスモデルガイドライン 商品化に関する手順規格 開発品質計画書運用規程 設計作業管理規格 進捗管理･工程管理および工程監査の手順 ピアレビュー実施ガイドライン マニュアル査読基準 コーディング規約 テスト実施（ＭＫ２からＣＴ）手順規格 ST作業手順規格 開発完了報告書運用規程 プログラムの受渡手続き ソフトウェア入試判定運用規定 ソフトウェア登録判定運用規程 構成管理手順規格 構成管理手順規定 文書管理手順規格 文書管理手順 品質記録管理規格 品質記録管理手順 テスト資材の管理手順規格 ２ソフトプロジェクト教育実施規定 是正処置／予防処置管理手順

クラス	コンポネント名	保証手段
		ソフトウェア障害レポート処理手続き パッチ受渡手続き 登録済み製品の重大障害管理手順 ツール管理
配付と運用(ADO)	ADO_DEL.1 ADO_IGS.1	開発元からユーザまでの配付手続きを遵守すること。また、TOEの安全な設置、生成、立ち上げのために必要なすべての手順を記述したドキュメントを作成すること。 以下のドキュメントを参照のこと。 配布規定
開発(ADV)	ADV_FSP.1 ADV_HLD.2 ADV_RCR.1	STを基に、機能仕様、上位レベル設計を作成する。また、セキュリティ機能要件、TOEサマリーファンクション、機能仕様、構成仕様書間での隣接する各TSF表現で、機能の対応付けを行うこと。 以下のドキュメントを参照のこと。 サブシステム説明書 開発品質計画書 機能仕様書 構成仕様書 構成仕様書　ポリシー移出入機能編 構成仕様書　仮想アドレス広報機能編 構成仕様書　正誤表 開発品質計画書レビュー報告書 機能仕様書レビュー報告書 構成仕様書レビュー報告書 マニュアルレビュー計画書 マニュアルレビュー査読依頼書
ガイダンス(AGD)	AGD_ADM.1 AGD_USR.1	管理者ガイダンスとして必要な要件を満たすドキュメントを作成すること。 以下のドキュメントを参照のこと。 インストールガイド ファイアウォール機能説明書 なお、本TOEを操作できるのは管理者のみに制限されるため、利用者ガイダンスはない。
ライフサイクルサポート(ALC)	ALC_DVS.1	開発環境のセキュリティを維持するために、必要な規定・手順を遵守し、かつその運用履歴を記録する。 以下のドキュメントを参照のこと。 設備管理および資産保全規格 開発マシン利用管理規定 開発場所管理規定 バックアップリストア手順 開発場所管理記録 開発マシン管理記録 バックアップ履歴 教育・訓練実施規準 教育訓練記録
テスト(ATE)	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	設計したプログラムが期待通りの機能を提供することを確認するため、テストを実施し、その結果を記録する。 以下のドキュメントを参照 CT計画書 CT項目兼結果記録表 ST計画書 ST項目兼結果記録表 CTテスト手順／仕様／項目書レビュー計画書 STテスト手順／仕様／項目書レビュー計画書 CTテスト手順／仕様／項目書レビュー報告書 STテスト手順／仕様／項目書レビュー報告書

クラス	コンポネント名	保証手段
		CTテスト結果記録 CTテスト報告書 STテスト結果記録 STテスト報告書 テスト分析 カバレッジ分析
脆弱性評定(AVA)	AVA_VLA.1 AVA_MSU.1 AVA_SOF.1	意図した環境では、TSFを迂回、干渉、不活性化されることがないことを保証するための脆弱性分析を行う。また、TOEが安全でない場合でも、TOE管理者がそれに気が付かないリスクを最小化することを保証するための誤使用分析を行う。さらに、強度分析の対象となるセキュリティメカニズムについて、直接的攻撃に対抗できる能力を分析し、強度分析を行う。 以下のドキュメントを参照 脆弱性評定

第7章　ＰＰ主張

該当する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、前提条件、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・前提条件に対応するセキュリティ対策方針の説明

セキュリティ対策方針	脅威			前提条件				
	T1	T2	T3	ASM.1	ASM.2	ASM.3	ASM.4	ASM.6
O.AC	○	○						
O.ADRC			○					
OOE.ADMIN		○						
OOE.AUDREC	○	○						
O.AUDMON	○	○						
OE.1	○	○					○	
OE.2				○				
OE.3	○	○				○		
OE.5		○						
OE.6	○				○			
OE.7			○					
OE.8	○	○						○
OE.9				○				
O.ACX		○						

T1

T1の脅威に対抗するためには、外部ネットワーク側のネットワークインタフェースから入ってくるIPパケットデータを識別し、その情報から、内部ネットワークに対する不正なアクセスを図ろうとするパケットであることを判別し、不正なアクセスであることを検出した場合、当該パケットの内部ネットワークへの侵入を防止する必要がある。
この脅威に対して、O.ACの対策方針、OOE.AUDREC、O.AUDMONによる監査ファイルを監視することで対抗することができる。すなわち、O.ACにより、内部ネットワークに侵入を試みようとする外部ネットワークからのIPパケットデータを識別し、この識別されたIPパケットに対して、内部ネットワーク、及び外部ネットワークで使用されるIPアドレスを適正な範囲に制限し、外部ネットワークからアクセスできる内部ネットワークの接続先IPアドレス、及び接続先ポート番号を制限することで、内部ネットワークへのアクセスが許可されないパケットの内部ネットワークへの侵入を防止する。さらに、OOE.AUDREC、O.AUDMONにより、監査ファイルを分析することで、内部ネットワークの保護資産の改ざん、破壊、又は漏洩を図ろうとする外部ネットワークの利用者からのアクセスの兆候を検出することができる。
また、OOE.AUDREC及びO.AUDMONを実施することによって得られる不正アクセスの情報を確実且つ迅速にO.ACの処理に反映することによってO.ACを確実に実施しなければならない。このためにはOE.1およびOE.3による不正のないTOEの管理・運用が実施され、OE.8によりO.AUDMONから発生するアラート情報が外部ネットワークの利

用者に漏れることを防止することによって実現できる。
なお、外部ネットワークから内部ネットワークへのアクセスは、OE.6の実施により必ずTOEを経由して行われ、TOEを迂回するバイパスが存在しないことが確認できる。

T2

T2の脅威に対抗するためには、TOE上のTOE保護資産へのアクセスをTOE管理者に制限する必要がある。この脅威に対して、O.AC、O.ACXによりTOEへのアクセスを制限し、OOE.ADMINによりTOE管理者を限定し、OOE.AUDREC、O.AUDMONにより監査ファイルを監視することで対抗することができる。すなわち、O.AC、O.ACXにより、TOEに侵入を試みようとする外部ネットワーク、又はTOE管理者がX端末を利用している場合、TOE管理者以外のX端末から、TOEへのアクセスを全面的に禁止することで、TOE上のTOE関連資産の改ざんを防止する。また、OOE.ADMINにより、TOEへのアクセス権限を持つTOE管理者のみがTOEの環境設定ファイルや監査ファイルを制御できるようにアクセス権限を限定させる。さらに、OOE.AUDREC、O.AUDMONにより、監査ファイルを分析することで、外部ネットワークの利用者が、本TOEに不正に侵入しようとしている兆候を検出することができる。
また、OOE.AUDREC及びO.AUDMONを実施することによって得られる不正アクセスの情報を確実且つ迅速にO.ACの処理に反映することによってO.ACを確実に実施しなければならない。このためにはOE.1およびOE.3による不正のないTOEの管理・運用が実施され、OE.8によりO.AUDMONから発生するアラート情報が外部ネットワークの利用者に漏れることを防止することによって実現できる。
さらに、OE.5の実施により、外部ネットワーク及び内部ネットワークからのIPパケットデータによりTOEが搭載されているサーバ上のTOE以外のサービスが起動され、TOE内の保護資源に対して不正なアクセスが行われることを防止できる。

T3

T3の脅威に対抗するためには、内部ネットワークから外部ネットワークへアクセス時、内部ネットワークのアドレス体系が外部に漏洩しないように保護する必要がある。
この脅威に対して、O.ADRCの対策方針で対抗することができる。すなわち、O.ACにより、内部ネットワークから外部ネットワークへのIPパケットデータを識別し、O.ADRCにより、内部ネットワークのIPアドレスを、外部に公開してもセキュリティ上の問題が発生しないIPアドレス（グローバルアドレス）に変換し、内部ネットワークのネットワークアドレス体系を外部に対して隠蔽する。また、OE.7により、内部ネットワークの利用者が外部ネットワークの利用者に内部ネットワークのIPアドレス体系に関する情報を漏洩することを防止できる。

ASM.1

ASM.1は、TOEに対する物理的な攻撃を防止する。OE.2は、TOE管理者以外によるTOEの直接的な操作を禁止できる。OE.9は、X端末からのTOEに対する直接的な攻撃を禁止できる。

ASM.2

ASM.2は、外部ネットワークからTOEを経由しない内部ネットワークへのアクセスを防止する。OE.6は、外部ネットワークから内部ネットワークに必ずTOE経由でアクセスすることを可能とする。

ASM.3

ASM.3は、TOE管理者による不正を防止する。OE.3は、TOE管理者が不正な操作を行わないことを実現する。

ASM.4

ASM.4は、TOEの正しい運用管理を実現する。OE.1は、内部セキュリティポリシーに従ったTOEの運用管理を実現できる。

ASM.6

ASM.6は、TOEから発行されるアラート情報の漏洩を防止する。OE.8は、アラート情報の通知先が内部ネットワーク内であることを確実にする。

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検証

8.2.1.1 セキュリティ対策方針を実現するセキュリティ機能要件の説明

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。

機能要件	セキュリティ対策方針					
	O.AC	O.ADRC	OOE.ADMIN	OOE.AUDREC	O.AUDMON	O.ACX
FDP_IFC.1	○	○				○
FDP_IFF.1	○	○				○
FDP_ACC.1			●			
FDP_ACF.1			●			
FAU_ARP.1					○	
FAU_GEN.1				○		
FAU_SAA.1					○	
FAU_SAR.1					○	
FAU_SEL.1			○			
FAU_STG.2				○		
FMT_MOF.1			●			
FMT_MSA.1			●			
FMT_MSA.3			●			
FMT_MTD.1			●			
FMT_SMR.1			●			
FIA_UAU.1			●			
FIA_UID.1			●			
FPT_STM.1				●		
FPT_RVM.1	「8.2.1.3 セキュリティ要件の相互作用」を参照					
FPT_SEP.1	「8.2.1.3 セキュリティ要件の相互作用」を参照					

○：TOE に対する機能要件

●：IT環境に対する機能要件

O.AC

FDP_IFC.1及びFDP_IFF.1の情報フロー制御方針により、外部ネットワークからのIPパケットデータから、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パケット情報及びIPパケットデータが送受信されるネットワークインタフェースを使用して内部ネットワークに対する不正アクセスを制限することができる。

O.ADRC

FDP_IFF.1は、内部ネットワーク上の利用者が外部ネットワークに IPパケットデータを送信する際に内部ネットワークのネットワーク体系に関する情報(内部ネットワークのIPアドレス、ポート番号等)を隠蔽しており、外部ネットワークの利用者が内部ネットワークの資源を不正にアクセスするために必要となる情報の漏洩を防止している。

OOE.ADMIN

まず、正当な許可されたTOE管理者をFIA_UID.1及びFIA_UAU.1によって識別認証する。TOE管理者は、本TOEの動作の決定についての役割をFMT_MOF.1によって任される。この役割は、FMT_SMR.1によって常に適切なTOE管理者に維持される。TOEの動作を決定するための利用者データである環境設定ファイルに対するアクセス制御は、FDP_ACC.1及びFDP_ACF.1によってTOE管理者のみに制限する。TSFデータであるログ設定及びアラート設定の情報もFMT_MTD.1によってTOE管理者のみにアクセスを制限する。TOE管理者はTOEの状況を把握してFAU_SEL.1により監査事象の選択を行う。外部ネットワークから内部ネットワークへの不正なアクセスを検出した場合、TOE管理者は、FMT_MSA.3及びFMT_MSA.1を使用して外部ネットワークの利用者を制限するよう関連するセキュリティ属性の管理を行う。以上によりTOEは適切に管理され良好な状態を維持することができる。

OOE.AUDREC

監査データはFAU_GEN.1により生成され、そのファイルはFAU_STG.2によって保護される。また、監査データ中に記録される情報の一つである日付時刻はFPT_STM.1により信頼できる。

O.AUDMON

FAU_SAA.1により侵害の可能性が検出できる。侵害の可能性が検出された場合、FAU_ARP.1によりTOEはTOE管理

者に警告メッセージを発行する。TOE管理者はこの分析結果を確認するためにFAU_SAR.1により監査データの内容を確認することができる。

O.ACX

TOE管理者がX端末を利用する場合、FDP_IFC.1及びFDP_IFF.1の情報フロー制御方針により、TOE管理者以外のX端末からのIPパケットデータから、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パケット情報及びIPパケットデータが送受信されるネットワークインタフェースを使用してTOEに対する不正アクセスを制限することができる。

8.2.1.2 セキュリティ要件の依存性分析

以下に、セキュリティ要件の依存性について検証する。
FDP_ACF.1を除いてすべての依存関係は満足されている。

コンポーネント		依存関係	
項番	項目	項目	参照
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	18
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SEL.1	FMT_MTD.1 FAU_GEN.1	14 2
6	FAU_STG.2	FAU_GEN.1	2
7	FDP_IFC.1	FDP_IFF.1	8
8	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	7 13
9	FIA_UAU.1	FIA_UID.1	10
10	FIA_UID.1	なし	—
11	FMT_MOF.1	FMT_SMR.1	15
12	FMT_MSA.1	FDP_IFC.1 FMT_SMR.1	7 15
13	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	12 15
14	FMT_MTD.1	FMT_SMR.1	15
15	FMT_SMR.1	FIA_UID.1	10
16	FPT_RVM.1	なし	—
17	FPT_SEP.1	なし	—
18	FPT_STM.1	なし	—
19	FDP_ACC.1	FDP_ACF.1	20
20	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	19 不要

FMT_MSA.3

TOE をアクセスできる利用者はTOE 管理者しかいないため、環境設定ファイルへのアクセスをTOE 管理者に制限するアクセス制御SFP において、セキュリティ属性（この場合は利用者）のデフォルト値自身が不要であり依存性FMT_MSA.3は不要である。

8.2.1.3 セキュリティ要件の相互作用

以下に、セキュリティ要件の相互作用の関係性について検証する。

機能要件	防御を提供している要件		
	迂回	破壊	非活性化
FAU_ARP.1	N/A	FPT_SEP.1	FMT_MOF.1
FAU_GEN.1	N/A	FPT_SEP.1	FMT_MOF.1
FAU_SAA.1	N/A	FPT_SEP.1	FMT_MOF.1
FAU_SAR.1	N/A	FPT_SEP.1	FMT_MOF.1
FAU_SEL.1	N/A	FPT_SEP.1	FMT_MOF.1
FAU_STG.2	N/A	FMT_MOF.1	N/A
FDP_IFC.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1

機能要件	防御を提供している要件		
	迂回	破壊	非活性化
FDP_IFF.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
FIA_UAU.1	N/A	N/A	N/A
FIA_UID.1	N/A	N/A	N/A
FMT_MOF.1	N/A	FPT_SEP.1	N/A
FMT_MSA.1	N/A	FMT_MOF.1	N/A
FMT_MSA.3	N/A	FMT_MOF.1	N/A
FMT_MTD.1	N/A	FMT_MOF.1	N/A
FMT_SMR.1	N/A	FMT_MOF.1	N/A
FPT_RVM.1	N/A	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A
FPT_STM.1	N/A	N/A	N/A
FDP_ACC.1	FPT_RVM.1	N/A	N/A
FDP_ACF.1	FPT_RVM.1	N/A	N/A

N/A ： Not Applicable

迂回

FPT_RVM.1

情報フロー制御SFPを実現するFDP_IFC.1/FDP_IFF.1の機能は、TOEホストのネットワークインタフェースドライバとIPレイヤの中間に挿入され、IPパケットの送受信時に必ず呼び出される。
さらに、呼び出されたFDP_IFC.1/FDP_IFF.1の機能内ではフィルタリング条件を適用する以外の事象はないため、必ず本機能は実施される。
また、アクセス制御SFPを実現するFDP_ACC.1/FDP_ACF.1の機能は、TOEの操作時は常に呼び出され、TOE管理者のみに操作を許可し、その他の利用者は操作を拒否するため、迂回できない。

破壊

FPT_SEP.1

セキュリティドメインが分離されることにより、TOEの破壊から保護されることを保証する。
FAU_ARP.1、FAU_GEN.1、FAU_SAA.1、FAU_SAR.1、FAU_SEL.1、FDP_IFC.1、FDP_IFF.1、FMT_MOF.1のそれぞれの機能を実現するプログラムは、メモリにロードされ実行される。ここで、メモリにロードされたTOEのプログラム、データが、他のプログラムからの妨害や破壊などから分離され、保護されたセキュリティドメイン内で実行される必要がある。FPT_SEP.1のSolaris OS機能では、不正なアプリケーションプログラムから、ドライバプログラムを保護する機能を有しており、結果、上記それぞれのセキュリティ機能は、保護されたセキュリティドメイン内で実行されることが保証される。

FMT_MOF.1

FAU_STG.2、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMR.1のそれぞれの機能要件は、FMT_MOF.1により、TOE管理者以外の利用者の破壊行為から保護されることを保証する。

非活性化

FMT_MOF.1

FAU_ARP.1、FAU_GEN.1、FAU_SAA.1、FAU_SAR.1、FAU_SEL.1、FDP_IFC.1、FDP_IFF.1のそれぞれの機能要件は、FMT_MOF.1により、TOE管理者以外の利用者の非活性化行為から保護されることを保証する。

8.2.2 セキュリティ保証要件の検証

本TOEは、一般のコマーシャルシステムの中で利用される。ただし、TOEが搭載されるシステムは管理専用であるために、運用／管理面で、セキュリティ確保ができる。このため、コマーシャルシステム用として、十分なレベルであるEAL3を品質保証レベルとする。
また、EAL3を超える特定の保証対策はない

8.2.3 機能強度の根拠

本TOEは、一般のコマーシャルシステムで利用されることを想定し、不正行為は公開インタフェースを利用した攻撃である。このため、攻撃力は“低レベル”であり、これに対応できる最小機能強度レベルは、“SOF-基

本”で満足される。ただし、本TOEには機能強度に関連するメカニズムはない。

8.3 TOE要約仕様根拠

8.3.1 TOEセキュリティ機能根拠

ここでは、“5. ITセキュリティ要件”に対する“6. セキュリティ仕様概要”の有効性について検証する。
下表は、個々の仕様概要と機能要件との関係性を示している。

仕様概要 / 機能要件	IPPF.1	IPPF.2	ADRC.1	AUD.1	AUD.2	AUD.3	AUD.4	ENV.1
FAU_ARP.1					○			○
FAU_GEN.1				○			○	○
FAU_SAA.1					○			○
FAU_SAR.1				○		○	○	
FAU_SEL.1				○		○		○
FDP_IFC.1	○	○	○					○
FDP_IFF.1	○	○	○					○
FAU_STG.2				○				

○：TOE の機能として提供される。

FAU_ARP.1

FAU_ARP.1は、ENV.1「環境設定機能」により設定されたセキュリティ侵害の判定基準に基づき、AUD.2「アラート通知機能」によりセキュリティ侵害を検出した場合、以下のいずれかの方法でセキュリティ侵害の発生を通知することにより、満足される。

- コンソール通知
- メール通知
- TSFが提供するモニタリング機能への通知
- TOE管理者が設定したコマンドの起動
- SNMPマネジャ通知
- システムログ(syslog)通知

FAU_GEN.1

FAU_GEN.1は、ENV.1「環境設定機能」により設定された監査記録の生成基準に基づき、表5.1に示すように各機能要件で必要な監査事象はすべて記録される。

FAU_SAA.1

FAU_SAA.1は、ENV.1「環境設定機能」により設定されたセキュリティ侵害の判定基準に基づき、AUD.2「アラート通知機能」により、以下の監査対象事象を検出することにより、満足される。

- 同一送信元アラート
  単位時間内に、同一の送信元IPアドレスからのパケットが、指定された回数分ブロックされた場合、同一送信元アラートとして、アラートイベントを検出する。
- 同一送信先アラート
  単位時間内に、同一の送信先IPアドレスへのパケットが、指定された回数分ブロックされた場合、同一送信先アラートとして、アラートイベントを検出する。
- 監視ポートアラート
  指定された送信先ポート番号へのパケットを検出した場合、監視ポートアラートとして、アラートイベントを検出する。

FAU_SAR.1

FAU_SAR.1は、AUD.1「ロギング機能」、AUD.3「モニタリング機能」、AUD.4「稼動状況通知機能」により、セキュリティ機能のロギング情報や稼動状況、動作履歴、フィルタリング条件情報、パケット処理結果、及びアラート情報などを、解釈するのに適した形式で監査記録から読み出されることにより、満足される。

FAU_SEL.1

FAU_SEL.1は、ENV.1「環境設定機能」により設定された監査記録の生成基準に基づくAUD.1「ロギング機能」によるロギング情報の選択により満足される。それぞれの監査イベントは、以下の情報に基づいて生成される。

- ネットワークインタフェース
- フィルタリング条件

FDP_IFC.1

FDP_IFC.1は、ENV.1「環境設定機能」により設定されたフィルタリング条件に基づき、IPPF.1及びIPPF.2によって不正なIPパケットデータを制限する。

FDP_IFF.1

FDP_IFF.1は、ENV.1「環境設定機能」により設定されたフィルタリング条件に基づき、IPPF.1及びIPPF.2によって不正なIPパケットデータを制限する。ADRC.1によって内部ネットワーク上の利用者が外部ネットワークにIPパケットデータを送信する際に内部ネットワークのネットワーク体系に関する情報(内部ネットワークのIPアドレス、ポート番号等)を隠蔽しており、外部ネットワークの利用者が内部ネットワークの資源を不正にアクセスするために必要となる情報の漏洩を防止している。

FAU_STG.2

FAU_STG.2は、AUD.1「ロギング機能」により、監査データの格納領域枯渇が発生した場合でも監査記録が保持されることにより満足される。

8.3.2 保証手段根拠

ここでは、“6.2 保証手段”の有効性について検証する。
表6.2.1に示すように、すべてのTOEセキュリティ保証要件は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、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。

8.4 PP主張根拠

本STでは、準拠するPPはない。