NEC

2008/3/24
1SS-SEC-QS-06-S020-01

NEC ファイアウォール SG コアユニット Ver 1.0.0

セキュリティターゲット

日本電気株式会社

Ver. 1.34

2008/3/24

Copyright © NEC Corporation 2007 All rights reserved.

目次

Copyright © NEC Corporation 2007 All rights reserved.

Copyright © NEC Corporation 2007 All rights reserved.

1 ST 概説

本章では、ST 識別、ST 概要、CC 適合の主張、参考資料、用語について記述する。

1.1 ST 識別

タイトル:NEC ファイアウォール SG コアユニット Ver 1.0.0 セキュリティターゲット
バージョン:1.34
発行日:2008 年 3 月 24 日
作成者:日本電気株式会社
TOE:NEC ファイアウォール SG コアユニット
TOE のバージョン:1.0.0
キーワード:ファイアウォール、パケットフィルタ
CC のバージョン: Common Criteria for Information Technology Security Evaluation,Ver.2.3
補足-0512 適用

1.2 ST 概要

このドキュメントは、「NEC ファイアウォール SG」と呼ばれるファイアウォールソフトウェア製品の一部をなす、「NEC ファイアウォール SG コアユニット Ver 1.0.0」のセキュリティターゲットである。本 ST における TOE は、NEC ファイアウォール SG コアユニット Ver 1.0.0 が提供する、次の機能を対象とする。

- 設定管理機能
- 管理者認証機能
- パケットフィルタ機能
- ログアラート機能

「NEC ファイアウォール SG」には「NEC ファイアウォール SG サブユニット」も同時提供されるが、この機能は、TOE の動作に影響を与えない独立した機能であり、TOE 範囲外である。

1.3 CC 適合

このSTは以下のCCに適合している。

- CC パート2適合
- CC パート3適合
- EAL1適合

このSTが適合しているPPはない。

1.4 参考資料

- 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 2005年8月 バージョン2.3 CCMB-2005-08-001
  平成17年12月翻訳第1.0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:
  セキュリティ機能要件 2005年8月 バージョン2.3 CCMB-2005-08-002

Copyright © NEC Corporation 2007 All rights reserved.

平成17年12月翻訳第1.0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:
  セキュリティ保証要件 2005年8月 バージョン2.3 CCMB-2005-08-003
  平成17年12月翻訳第1.0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

- 補足-0512 平成17年12月
  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

1.5 用語集

・ プラットフォーム
アプリケーションソフトを動作させる際の基盤となる OS の種類や環境、設定のこと。

・ ホスト
ネットワークに接続するコンピュータ。サーバや端末が該当する。

・ ID
Identifier の略。身分証明書という意味の英単語。IT の世界では、何らかの対象を集団の中で一意に識別するための識別符号のこと。コンピュータの利用者を識別するために一人一人に割り当てられたユーザ名がこれに当たる。

・ 内部ネットワーク
TOE により、外部ネットワークからの脅威に対して保護されるネットワーク。組織内部のイントラネット、および外部ネットワークに情報やサービスを公開するための公開セグメントがこれに該当する。

・ 外部ネットワーク
組織の管理が及ばない、インターネットなどの保護対象外のネットワーク。

・ プロトコル
ネットワークを介してコンピュータ同士が通信を行なう上で、相互に決められた約束事の集合。通信手順、通信規約と呼ばれることもある。

・ IP(Internet Protocol)アドレス
インターネットやイントラネットなどの IP ネットワークに接続されたコンピュータや通信機器 1 台 1 台に割り振られた識別番号。

・ IP
Internet Protocol の略。ネットワーク上のデータの形式や制御方法を定めたプロトコル。

・ TCP
Transmission Control Protocol の略。IP のうえに位置するコネクション指向のプロトコル。

Copyright © NEC Corporation 2007 All rights reserved.

・ UDP
User Datagram Protocol の略。IP のうえに位置するコネクションレス型のプロトコル。

・ ICMP
Internet Control Message Protocol の略。IP による通信を制御するためのもの。

・ ポート番号
インターネット上の通信において、複数の相手と同時に接続を行なうために IP アドレスの下に設けられたサブ(補助)アドレス。

・ パケット
ネットワーク上でやり取りされるひとまとまりのデータ。送信先のアドレスなどの各種通信属性情報をヘッダに持つ。

・ OS 標準フィルタリング制御
TOE がインストールされる、OS(Linux)が標準に装備している IP パケットのフィルタリング機能(netfilter)のことを指す。
TOE のパケットフィルタ機能は、OS 標準フィルタリング制御を介して、IP パケットの送受信を行う。

・ ルーティング
IP パケットのヘッダ情報である送信先 IP アドレスをルーティングテーブルに照らし、ローカル配信か他ホストへ転送すべきかを決定し、転送の場合は出力インタフェースを決定する処理のこと。

・ LAN ドライバ
周辺機器を動作させるためのソフトウェア。OS が周辺機器を制御するための橋渡しを行なう。
本 ST では、外側用、および内側用のネットワークインタフェースを動作させるソフトウェアを指す。

・ セッション
2 台のネットワーク機器間で使用される接続の単位のこと。

・ HTTP
HyperText Transfer Protocol の略。Web サーバと Web クライアントとの間でやり取りされる通信プロトコル。

・ SSL
Secure Sockets Layer の略。サーバとクライアント間の通信において、認証および暗号化をするプロトコル。

・ HTTPS
Hypertext Transfer Protocol Security の略。SSL の暗号化通信を HTTP に実装したもの。

・ SMTP
Simple Mail Transfer Protocol の略。インターネットやイントラネットで、電子メールを転送するためのプロトコル。

Copyright © NEC Corporation 2007 All rights reserved.

・ SSH
ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするためのプログラム。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

・ VPN
Virtual Private Network の略。インターネットを利用して仮想的に構築する独自ネットワーク。

・ Web（World Wide Web）ブラウザ
Web サーバがインターネットやイントラネット上に公開した Web ページを表示するためのソフトウェア。

・ Web サーバ
管理端末から TOE への各種設定要求を受け付け、その結果をファイアウォール管理者に提示するために使用される TOE 範囲外のソフトウェア。

・ メールサーバ
TOE からアラート通知としてファイアウォール管理者に送信されたメールを中継するために使用される、内部ネットワークに LAN 接続された TOE 範囲外のサーバ。

・ FTP
File Transfer Protocol の略。インターネットやイントラネットの TCP/IP ネットワークでファイルを転送するときに使われるプロトコル。

・ PING-SWEEP
ping ツールにより特定のネットワーク上の IP アドレス範囲に対し連続的に ping を送ること。

・ IP-SPOOFING
偽の IP アドレスを送信元にセットしたパケットを送り込む攻撃手法。

・ 二重化
複数の設備を用意しておき、1 つの設備が故障しても他の設備がサービスを続行できるようにした構成。
本 ST では、現在利用しているホストを現用ホスト、待機しているホストを待機ホスト、と呼ぶ。

・ P2P
peer-to-peer の略。不特定多数のホストが相互に接続され、直接ファイルなどの情報を送受信する接続形態。また、それを可能にするソフトウェアやシステムのこと。

・ ポリシ
組織のセキュリティ対策に対する根本的な考え方を表すもので、どのような情報資産をどのような脅威からどのように保護するのかを組織体制を含めて規定したもの。

・ 管理端末
ファイアウォール管理者が Web ブラウザを用いて TOE の運用管理を行うために使用する、内部ネットワークに LAN 接続された TOE 範囲外の端末。TOE には、管理端末を 4 台まで登録することがで

Copyright © NEC Corporation 2007 All rights reserved.

き、ファイアウォール管理者は、内部ネットワーク上のどの管理端末を使用しても TOE の設定・操作を行うことができる。

- 監査証跡
  TOE が生成した監査記録の集まりのことを指す。監査証跡には、イベントログとアラートログの 2 種類ある。ログアラート機能が、設定管理機能、管理者認証機能、およびパケットフィルタ機能からの監査記録の出力依頼に基づき生成し、格納する。

- イベントログ
  イベントログは、TOE の運用中に発生するイベント(アラートログと同一内容を含む)が記録された監査証跡を指す。
  TOE の運用中に発生するイベントは、設定管理機能、管理者認証機能、およびパケットフィルタ機能から、ログアラート機能に対して、監査記録として通知される。設定管理機能、管理者認証機能が通知する監査記録を運用イベントと呼び、パケットフィルタ機能が通知するイベントを通信イベントと呼ぶ。

- アラートログ
  アラートログは、アラートとして通知される可能性のあるイベントが記録された監査証跡を指す。
  アラートログに出力される監査記録をアラートイベントと呼ぶ。アラートイベントは、パケットフィルタ機能から、ログアラート機能に対して、監査記録として通知される。アラートログは、ログアラート機能から参照され、ログアラート設定(アラートアクション設定)で定義された方法で、ファイアウォール管理者にアラートを通知する。

- ログアラート設定
  TOE のログアラート機能に関する設定情報を指す。ログアラート設定は、ログアラート設定(監査証跡ファイル設定)、ログアラート設定(アラートアクション設定)の2種類に分類される。

- 監査証跡ファイル設定
  監査証跡のローテーションサイズ・監査証跡を格納するディスクの容量が設定される。

- アラートアクション設定
  アラートの通知方法(メール送付・syslog 出力・コマンド実行)・通知するアラートイベント(SYN-SCAN 検出・SYN-FLOOD 検出・PING-SWEEP 検出・パケット受付・パケット拒否・通信ログ・ファイル改ざん監視)毎のアラート通知の要否とアクションの通知方法の設定情報を指す。
  syslog 出力とは、アラートの通知をシステムログへ出力する。そのシステムログは、システム管理者が OS の機能を利用して、内容を確認する。コマンド実行とは、アラート情報の収集コマンドを実行し、保守サービス員がコマンドにて収集した情報を採取する。

- パケットフィルタルール
  フィルタリング条件(IPパケットのヘッダ情報(送信元IPアドレス・送信先IPアドレス・プロトコル種別・ポート番号・ネットワークインタフェース)、IP パケットに対する処理(通過・破棄・拒否)の指定、および監査記録の出力要否の指定)の組み合わせを指し、TOE のパケットフィルタ機能が参照する。パケットフィルタルールは「不正アクセス対策ルール」・「サイト共通ルール」・「管理端末接続ルール」・「暗黙のルール」の 4 種類のルールがある。

Copyright © NEC Corporation 2007 All rights reserved.

・ 不正アクセス対策ルール
不正アクセス対策ルールとは、不正アクセス対策レベルで設定された不正アクセスを検知するためのパケットフィルタルールを指す。TOE のインストール時に設定される。

・ 不正アクセス対策レベル
ファイアウォール管理者は、「ベーシック」・「アドバンス」の 2 種類のレベルを選択することができる。
「ベーシック」とは、PING-SWEEP 検知・IP-SPOOFING 対策を行う。
「アドバンス」とは、ベーシックの対策に通信流入量制限を追加した対策を行う。
TOE の不正アクセス対策レベルとして、「アドバンス」を選択した状態で TOE を運用しなければならない。

・ サイト共通ルール
サイト共通ルールとは、TOE を運用するネットワーク環境のポリシに合わせて設定するフィルタリングルールを指す。たとえば、「外部ネットワークから内部ネットワークへの FTP を廃棄する」のようなルールである。また、サイト共通ルールは、TOE の運用中に識別認証されたファイアウォール管理者が問い合わせ・改変・削除・追加、インポート/エクスポート、バックアップ／リストアすることができる。

・ 管理端末接続ルール
管理端末接続ルールとは、管理端末からの HTTPS 通信の IP パケットを許可するためのパケットフィルタルールを指す。TOE のインストール時に設定される。また、管理端末接続ルールは、TOE の運用中に識別認証されたファイアウォール管理者が問い合わせ・改変・削除・追加、インポート/エクスポート、バックアップ／リストアすることができる。

・ 暗黙のルール
暗黙のルールとは、開発者が開発段階で設定するパケットフィルタルールで、設定されているパケットフィルタルールのいずれにも該当しない（対象となる IP パケットに対する処理結果が判断できない）パケットを廃棄するためのパケットフィルタルールを指す。

・ ファイアウォール管理者情報
TOE の管理者認証機能が識別認証情報として使用するファイアウォール管理者の ID・パスワードを指す。

・ LAN アナライザ
ネットワークを流れるデータを捕捉して分析し、その結果を人間が理解できる形式に変換して表示するためのソフトウェアや機器のこと。

・ 初期導入設定ツール
TOE のインストール用 CD-ROM に格納されている Windows OS 上で動作するツールで、インストール時に使用するシステムの基本情報（ネットワーク設定など）の初期値を設定するツールのこと。

・ 流入量制限機能
単位時間当たりの IP パケット流入量を制限するための機能である。独立した機能であり、TOE が実装するセキュリティ機能の動作に影響を与えない。非セキュリティ機能として TOE により提供される。

Copyright © NEC Corporation 2007 All rights reserved.

・ SSH 機能
ファイアウォールサーバの OS に設定されているシステム管理者の ID とパスワードを変更するための機能である。非セキュリティ機能として TOE により提供される。

・ アドレスグループ設定機能
フィルタリングルールに記述する IP アドレスをグループにまとめて記述できるようにするための機能である。非セキュリティ機能として TOE により提供される。

・ サービス設定機能
フィルタリングルールに記述できる通信種別（プロトコル）ごとのタイプ（ポート番号、ICMP タイプなど）をグループ化するための機能である。非セキュリティ機能として TOE により提供される。

Copyright © NEC Corporation 2007 All rights reserved.

2 TOE 記述

本章では、TOE 概要、TOE 関連の利用者役割、TOE の論理的範囲、TOE の物理的範囲および TOE 資産について記述する。

2.1 TOE の概要

2.1.1 TOE 種別

TOE 種別は、ファイアウォール製品である。

2.1.2 サービス概要

内部ネットワークを、別のポリシで運用されている外部ネットワークに接続すると、外部ネットワークに存在する種々の資源が利用可能となる反面、内部ネットワークは外部ネットワークからの悪意を持った攻撃にさらされる恐れがある。
図 2-1に、ネットワーク構成を示す。

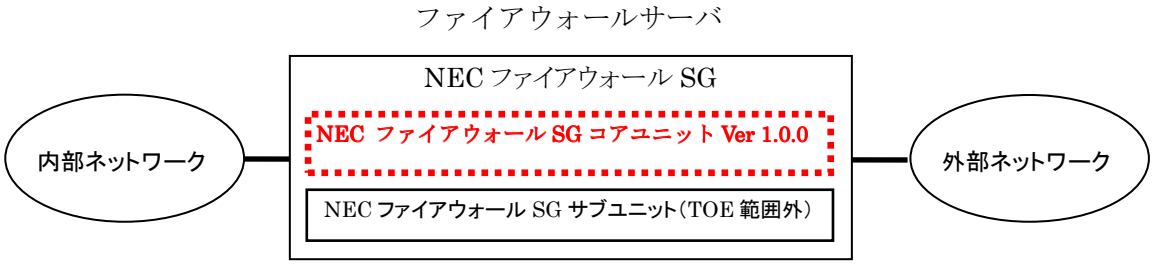

図 2-1 ネットワーク構成

図 2-1が示すように、NECファイアウォールSGは、内部ネットワークと外部ネットワークを接続する唯一の接点に配される。そして、パケットフィルタルールに基づいて通過しようとするIPパケットを評価し、そのパケットフィルタルールに反するIPパケットを拒否又は破棄することによって、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を防御する目的で利用される。

NECファイアウォールSGが提供する機能を大別すると「NEC ファイアウォールSGコアユニットVer 1.0.0」と「NECファイアウォールSGサブユニット」がある。

- NEC ファイアウォールSGコアユニットVer 1.0.0 が提供する機能
  設定管理機能、管理者認証機能、パケットフィルタ機能、ログアラート機能
  (上記の機能はTOE範囲内であり、セキュリティ機能及び非セキュリティ機能から構成される。TOEは、上記以外にOSが持つ機能であるOS標準フィルタリング制御とLANドライバも含んでいる。)

- NECファイアウォールSGサブユニットが提供する機能
  ホスト型IDS機能等のNECファイアウォールサブユニットが提供する機能は、TOEの動作に影響を与えない独立した機能であり、TOE範囲外である。

これらのうち、「NEC ファイアウォールSGコアユニットVer 1.0.0」が本STにおけるTOE 範囲である。
一方、「NECファイアウォールSGサブユニット」は、TOE範囲外であり、TOEに対する自律的なインタフェ

Copyright © NEC Corporation 2007 All rights reserved.

ースを持たずTOEの動作に影響を与えない。

2.2 TOE 関連の利用者役割

1）TOE を使用する利用者の役割

① ファイアウォール管理者

ファイアウォール管理者は、ファイアウォール管理責任者より1名任命される。ファイアウォール管理者は、管理端末のWebブラウザからTOEの設定管理機能に接続（TOE外で実装されるHTTPSを使用）し、設定管理機能が提供するWeb画面を使用して、TOEの運用管理を行う。識別認証されたファイアウォール管理者は、以下の操作を実行できる。

- ファイアウォール管理者情報（ID、パスワード）の改変
- パケットフィルタルールの問い合わせ、改変、削除、追加、、インポート/エクスポート、バックアップ／リストア
- ログアラート設定（監査証跡ファイル設定）の問い合わせ、改変
- ログアラート設定（アラートアクション設定）の問い合わせ、改変、削除、追加
- 監査証跡（イベントログ、アラートログ）の参照

② 保守サービス員

ファイアウォール管理者がログインした管理端末を用いて、ファイアウォール管理者の立会いのもと、アラート発生時の情報を収集するメーカの保守技術者である。

2）TOE の提供するサービスを使用して内部および外部ネットワークを利用する利用者の役割

① 内部の一般利用者

内部ネットワークにある端末から、TOEが動作するファイアウォールサーバを介して、外部ネットワークにあるホストが保有する情報、サービスを利用する。

② 外部の一般利用者

外部ネットワークにある端末から、TOEが動作するファイアウォールサーバを介して、内部ネットワークにあるホストが保有する情報、サービスを利用する。

3）その他の役割

① ファイアウォール管理責任者

ファイアウォールの設定の直接操作は行わないが、適切なファイアウォール管理者・システム管理者を任命する。

② システム管理者

システム管理者は、ファイアウォール管理責任者より1名任命される。システム管理者は、TOE外で実装されるSSHを用いてNECファイアウォールSGの動作に必要となるOSやNECファイアウォールSG以外の関連ソフトウェア群の運用を管理する。また、これらのソフトウェアが稼動するプラットフォームの運用を管理する。

Copyright © NEC Corporation 2007 All rights reserved.

2.3 TOE の物理的範囲

TOE の物理的ネットワーク構成を図 2-2 に示す。
図 2-2 に示すように、TOE は内部ネットワークと外部ネットワークとを結ぶ唯一の接点に位置するファイアウォールサーバ上で稼動する。TOE を設定管理するための管理端末が内部ネットワークに配置される。

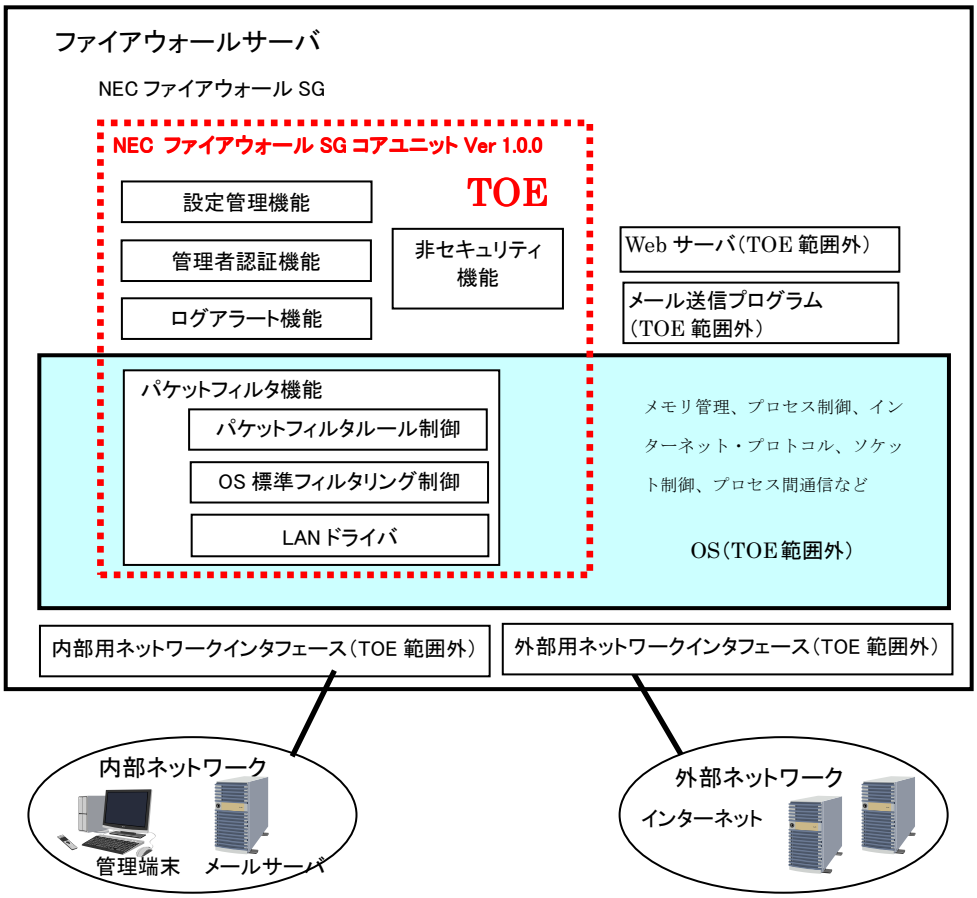

図 2-2 TOE の物理的ネットワーク構成

図 2-2 に示す破線で囲った範囲が TOE であり、ファイアウォールサーバ上で稼動する NEC ファイアウォール SG ソフトウェアの一部をなす「NEC ファイアウォール SG コアユニット Ver 1.0.0」である。

以下に、TOE が動作するハードウェア、管理端末、および関連装置について示す。

① ファイアウォールサーバ
管理端末が位置する内部ネットワークと外部ネットワークとを分離し、外部ネットワークから内部ネットワークへの不正侵入を防止するためのハードウェア。ファイアウォール管理責任者により任命されたシステム管理者及びファイアウォール管理者しか入室できず、かつ入退記録が残されるような、物理的に保護された環境に設置される。

② 管理端末
ファイアウォール管理者が Web ブラウザを用いて TOE の運用管理を行うために使用する、内部ネットワークに LAN 接続された TOE 範囲外の端末。

Copyright © NEC Corporation 2007 All rights reserved.

③ メールサーバ
TOE からアラート通知としてファイアウォール管理者に送信されたメールを中継するために使用される、内部ネットワークに LAN 接続された TOE 範囲外のサーバ。

④ 外部用ネットワークインタフェース、および内部用ネットワークインタフェース
外部ネットワーク、および内部ネットワークに接続するためのデバイス。TOE 範囲外である。

次に、ハードウェアごとに、TOE と TOE が動作するために必要なソフトウェアを示す。

＜ファイアウォールサーバ＞

① NEC ファイアウォール SG コアユニット Ver 1.0.0（TOE）
TOE であり、以下のセキュリティ機能と非セキュリティ機能で構成される。

●セキュリティ機能

- 設定管理機能
  ファイアウォール管理者が TOE の動作環境を設定する機能である。
- 管理者認証機能
  設定管理機能を利用するために管理端末から TOE に接続要求してきたファイアウォール管理者を識別認証する機能である。
- パケットフィルタ機能（パケットフィルタルール制御と、OS 内の OS 標準フィルタリング制御及び LAN ドライバから構成される）
  IP パケットを受け取り、パケットフィルタルールに基づいて IP パケットを評価し、通過・拒否・破棄の処理を行う。
- ログアラート機能
  監査記録（イベントログ、アラートログ）の形式を整えて監査証跡へ格納するログ格納機能と、ログアラート設定（アラートアクション設定）に基づいてファイアウォール管理者に対しアラート通知を行うアラート通知機能から構成される。

●非セキュリティ機能

TOE が提供する以下の機能は、TSF の動作に影響を与えない機能である。

- 流入量制限機能
- SSH 機能
- アドレスグループ設定機能
- サービス設定機能

② OS
TOE を動作させるための基盤となるソフトウェアである。OS が提供する OS 標準フィルタリング制御と LAN ドライバは、パケットフィルタ機能の一部として TOE 内に組み込まれる。OS が持つメモリ管理、プロセス管理、インターネット・プロトコル、ソケット制御、プロセス間通信などの他の機能は TOE 範囲外である。

③ Web サーバ
管理端末から TOE への各種設定要求を仲介し、その結果をファイアウォール管理者に提示するために使用される TOE 範囲外のソフトウェアである。

Copyright © NEC Corporation 2007 All rights reserved.

④ メール送信プログラム
TOE が、セキュリティ侵害の可能性を検知した場合に、その事実をファイアウォール管理者にアラート通知メールにより通知するために使用される TOE 範囲外のソフトウェアである。

＜管理端末＞

① OS
下記のソフトウェアを動作させるための基盤となるソフトウェアである。

② Web ブラウザ
ファイアウォールサーバに対して、ファイアウォール管理者が TOE の各種設定を要求し、その結果を得るためのソフトウェアである。

③ メールクライアント
TOE からのアラート通知のメールを受信するためのソフトウェアである。

次に、TOE が想定する上記ソフトウェアの製品名及びバージョンについて示す。

■ ソフトウェア

＜ファイアウォールサーバ＞

① OS
RedHat Enterprise Linux カーネルバージョン 2.4.21-32.0.1.ELsmp

② Web サーバ
wbmchttpd(Apache) 1.3.27

③ メール送信プログラム
Sendmail 8.12.11

＜管理端末＞

① OS
Microsoft Windows XP SP2

② Web ブラウザ
Internet Explorer 6.0 SP2

③ メールクライアント
特に指定なし

Copyright © NEC Corporation 2007 All rights reserved.

2.4 TOE の論理的範囲

TOE の論理的構成を図 2-3 に示す。

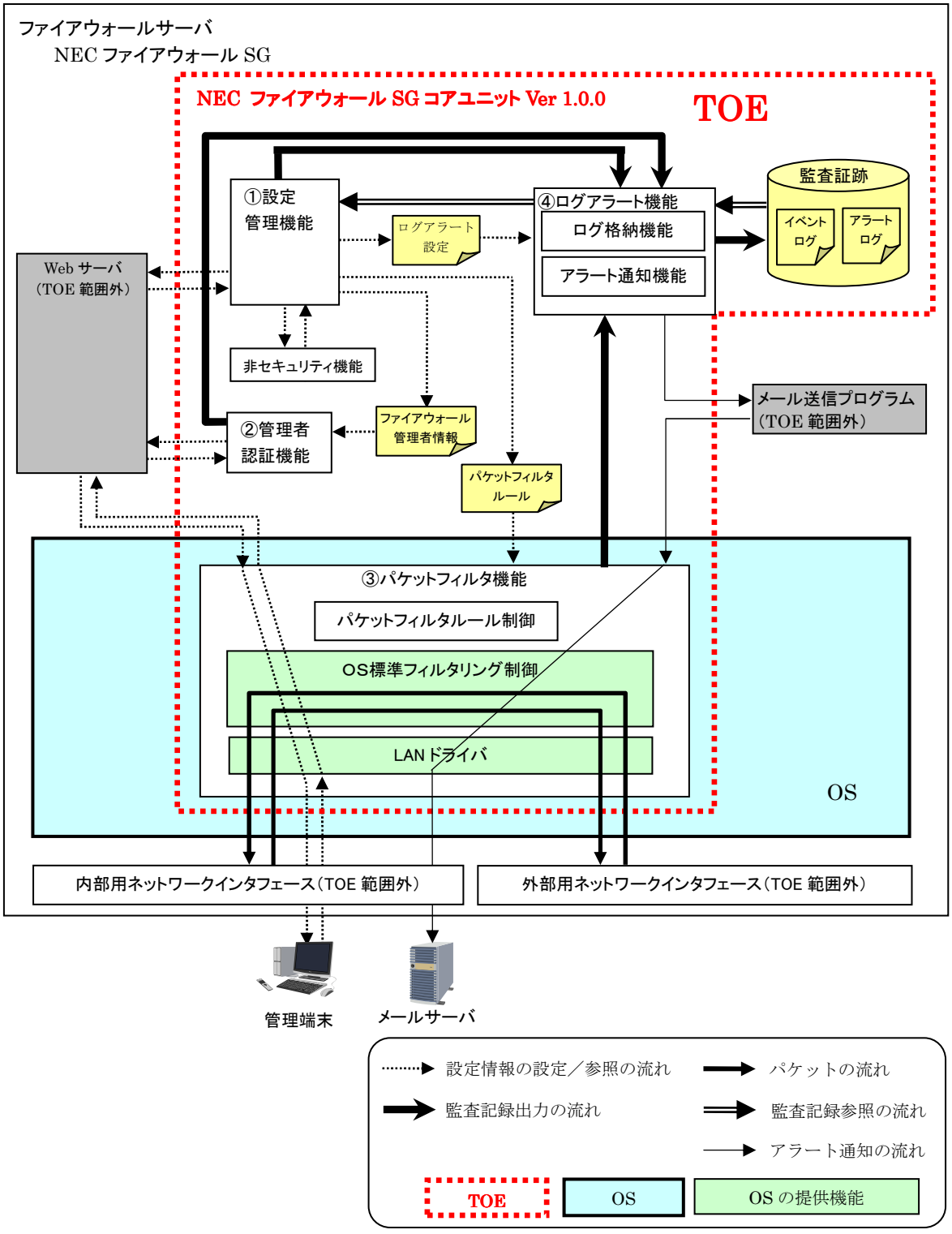

図 2-3 TOE の論理的構成

Copyright © NEC Corporation 2007 All rights reserved.

図 2-3 において、破線で囲まれた部分が TOE 範囲である。まず、TOE 範囲内の各機能について説明する。

1) TOE が提供する機能

TOE が提供する機能を以下に記述する。
①～④の説明は図 2-3 の①～④で示した機能に対応する。
TOE は OS の起動により開始され、OS の停止により終了する。

① 設定管理機能

設定管理機能は、ファイアウォール管理者が TOE の動作環境を設定する機能を提供する。パケットフィルタルールの管理端末接続ルールで許可されている内部ネットワークの IP アドレスを持つ管理端末を利用するファイアウォール管理者だけが、管理者認証機能により識別認証された後に本機能を利用できる。

識別認証に成功した場合、設定管理機能は、接続要求された URL を Web サーバ(TOE 範囲外)から受け取り、該当する Web 画面に表示する項目データを Web サーバ(TOE 範囲外)に返す。Web サーバ(TOE 範囲外)は、設定管理機能から受け取った項目データを用いて画面データを作成し、HTTPS パケットに分解して、パケットフィルタ機能に渡す。接続要求が許可され、識別認証が成功している場合、セッションは確立されており、パケットフィルタ機能では HTTPS パケットの通過が許可され、管理端末に送信される。その結果、管理端末上の Web ブラウザに要求した Web 画面が表示される。

また、設定管理機能は、以下の事象が発生した場合に、その監査記録をログアラート機能へ通知する。

- 監査記録の参照
- ファイアウォール管理者パスワード検証の成功／失敗
- パケットフィルタルール改変、削除、追加の成功
- ファイアウォール管理者パスワード改変の成功
- ファイアウォール管理者 ID 改変の成功
- ログアラート設定(監査証跡ファイル)改変の成功
- ログアラート設定(アラートアクション設定)改変、削除、追加の成功
- ログアラート設定(アラートアクション設定)の変更
- 設定管理機能の起動

Copyright © NEC Corporation 2007 All rights reserved.

② 管理者認証機能

管理者認証機能は、設定管理機能を利用するために管理端末から TOE に接続要求してきたファイアウォール管理者を識別認証する機能を提供する。

内部用ネットワークインタフェースにパケットフィルタルールの管理端末接続ルールで許可された管理端末から接続要求 IP パケットを受信した場合に限りパケットフィルタ機能が当該 IP パケットを Web サーバ(TOE 範囲外)に渡すため、Web サーバ(TOE 範囲外)との HTTPS のセッションが確立できる。セッション確立後、接続要求を受けた Web サーバ(TOE 範囲外)から本機能に識別認証の要求が渡される。管理者認証機能はファイアウォール管理者の識別認証状態を確認し、識別認証されていなければ識別認証の Web 画面の表示を Web サーバ(TOE 範囲外)に依頼する。
HTTPS のセッションが確立していない管理端末から新規に Web ブラウザを起動した場合、必ず識別認証が行われる。

管理者認証機能は、入力されたファイアウォール管理者の ID とパスワードを Web サーバ(TOE 範囲外)から受け取り、ファイアウォール管理者情報に登録されているものと比較する。一致する場合、管理者認証機能はアクセスを許可し、そうでない場合は拒否する。

ファイアウォール管理者は TOE の運用中に、設定管理機能を用いてファイアウォール管理者情報を管理端末上の Web ブラウザから変更することができる。変更した設定内容は、管理端末上の Web 画面に表示される設定ボタンの押下により、反映される。

また、管理者認証機能は、以下の事象が発生した場合に、その監査記録をログアラート機能へ渡し、監査証跡への格納を依頼する。

- ファイアウォール管理者の識別認証の成功／失敗

③ パケットフィルタ機能

パケットフィルタ機能は、外部用ネットワークインタフェース(TOE 範囲外)、内部用ネットワークインタフェース(TOE 範囲外)のそれぞれから受信する IP パケットを LAN ドライバで受け取り、パケットフィルタルールに基づいて IP パケットを評価し、通過・拒否・破棄の処理を行う。本機能は、以下の 3 つの機能から構成されている。

a) パケットフィルタルール制御

設定管理機能からの指示により、OS 標準フィルタリング制御が参照するメモリ上のパケットフィルタルールを書換える。

b) OS 標準フィルタリング制御

LAN ドライバから渡された受信 IP パケット、および Web サーバ(TOE 範囲外)、メール送信プログラム(TOE 範囲外)から渡された TOE が送信元であるパケット(HTTPS の応答パケット、SMTP パケット)をパケットフィルタルールに基づいて、評価する。
通過と判断された IP パケットは、宛先がファイアウォールサーバ自身である場合は、Web サーバ(TOE 範囲外)に渡し、宛先が他のホストである場合は、ルーティングにより転送先のネットワークインタフェースが決定され、LAN ドライバに送信を指示する。
拒否と判断れさた IP パケットは破棄し、LAN ドライバにエラーの送信を指示する。また、破棄と判断された IP パケットは破棄する。

Copyright © NEC Corporation 2007 All rights reserved.

c) LANドライバ
外部用ネットワークインタフェース、および内部用のネットワークインタフェースからIPパケットを受信し、OS標準フィルタリング機能に渡す。また、OS標準フィルタリング機能から受け取ったIPパケットを外部用ネットワークインタフェースまたは内部用ネットワークインタフェースから送信する。

次に、パケットフィルタルールについて説明する。パケットフィルタルールは以下の 4 種類のルールから構成されている。

① 不正アクセス対策ルール
② 管理端末接続ルール
③ サイト共通ルール
④ 暗黙のルール

TOE は IP パケットを評価する際に、該当するルールが現われるまで上記①→②→③→④のパケットフィルタルールを順に評価する。

不正アクセス対策ルールは、TOE が検出すべきセキュリティ侵害の可能性のパターンを指定するパケットフィルタルールであり、他のルールと異なり、個々の IP パケットだけでなく、複数の IP パケットのの受信パターンに関するルールを含んでいる。TOE は、不正アクセス対策ルールとして「アドバンス」が選択されている環境を想定しており、TOE 生成時に指定され、組み込まれる。

管理端末接続ルールは管理端末の IP アドレスを定義するパケットフィルタルールである。少なくとも 1 つの管理端末に関する定義が管理端末接続ルールとして TOE 生成時に指定される。

サイト共通ルールは、通過・拒否・破棄する IP パケットを明示的に指定するためのパケットフィルタルールである。TOE 運用中にファイアウォール管理者は必要に応じて本ルールを指定する。

暗黙のルールは設定されている他の種類のパケットフィルタルールのいずれにも該当しない IP パケットを破棄するパケットフィルタルールであり、TOE 開発時に組み込まれている。TOE はこのルール自身を変更する機能は持たないが、サイト共通ルール及び管理端末接続ルールを定義することにより、暗黙のルールによって破棄されない通過・拒否するIPパケットを指定することができる。パケットフィルタルールは、開発時に暗黙のルールが組み込まれることにより、全体が制限的ルールとなっている。

ファイアウォール管理者は、TOE の運用中にパケットフィルタルールを管理端末上の Web 画面から問い合わせ、改変、削除、追加、インポート／エクスポート（他のファイアウォールサーバにインストールされている TOE と同一のパケットフィルタルールを設定するための機能）、バックアップ／リストア（自ファイアウォールサーバ内のパケットフィルタルールを TOE の外部に取り出し・戻すための機能）することができる。
編集中のパケットフィルタルールは、設定管理機能により一時ファイルに保存される。確定した変更内容は、管理端末上の Web 画面に表示される設定ボタンの押下によりパケットフィルタル

Copyright © NEC Corporation 2007 All rights reserved.

ール・ファイルへ移され、パケットフィルタルール制御がメモリ内のパケットフィルタルールを書換えることにより反映される。

パケットフィルタ機能は定義されているパケットフィルタルールに基づいて、以下の事象が発生した場合、生成した監査記録をログアラート機能へ渡し、監査証跡への格納を依頼する。

- 不正アクセス対策ルールに基づく不正アクセスの可能性の検出
- サイト共通ルールに基づく IP パケットに対する処理

以下にパケットフィルタルールと監査記録の関係について説明する。表 2-1 にパケットフィルタルールと監査記録の関係について示す。

表 2-1 パケットフィルタルールと監査記録の関係

パケットフィルタルール	監査記録 (通信イベント)	監査記録 (アラートイベント)	備考
(ア)不正アクセス対策ルール	必ず生成される	必ず生成される	―
(イ)管理端末接続ルール	生成されない	生成されない	―
(ウ)サイト共通ルール	監査記録出力の要否の設定による	監査記録出力の要否の設定による	監査記録(アラートイベント)のみの生成はできない。
(エ)暗黙のルール	生成されない	生成されない	―

(ア)不正アクセス対策ルール

不正アクセス対策ルールが適用された通信は、必ず監査記録(通信イベント、アラートイベント)が生成される。

(イ)管理端末接続ルール

管理端末接続ルールが適用された IP パケットについては、監査記録は生成されない。

(ウ)サイト共通ルール

サイト共通ルールが適用された通信は、各ルールの監査記録出力要否設定に基づいて、監査記録が生成される。監査記録の出力要否として以下の選択が可能である。

- 監査記録(通信イベント)を生成しない
- 監査記録(通信イベントのみ)を生成する
- 監査記録(通信イベント、アラートイベント)を生成する

(エ)暗黙のルール

暗黙のルールが適用された IP パケットについては、監査記録は生成されない。

④ ログアラート機能

ログアラート機能は、以下の 2 つの機能を提供する。

a) ログ格納機能

ログ格納機能は、設定管理機能、管理者認証機能、パケットフィルタ機能から渡された監査記録(イベントログ、アラートログ)の形式を整えて監査証跡へ格納する。

Copyright © NEC Corporation 2007 All rights reserved.

監査記録格納時、ログ格納機能はログアラート設定(監査証跡ファイル設定)に基づいて残ディスク容量をチェックする。ディスク容量が満杯になると判断された場合は、最も古くに格納された監査記録に上書きする。
ログアラート設定(監査証跡ファイル設定)は、インストール時に初期値が設定され、運用中にも変更できる。

b) アラート通知機能
アラート通知機能は、定期的に監査証跡(アラートログ)を参照し、ログアラート設定(アラートアクション設定)に基づいてファイアウォール管理者に対しアラート通知を行う。通知するべきイベントを検出した場合、アラート通知機能はメール送信プログラム(TOE 範囲外)にメールの送信を依頼する。メール送信プログラム(TOE 範囲外)は、アラート通知のメールデータ(SMTP パケット)を作成し、パケットフィルタ機能に送信を依頼する。パケットフィルタ機能が受け取った SMTP パケットは、パケットフィルタルールに基づいて評価され、通過と判断された場合は LAN ドライバを経由してメールサーバへ送信される。

ファイアウォール管理者は、TOE の運用中にログアラート設定(監査証跡ファイル設定、アラートアクション設定)を管理端末上の Web 画面から変更することができる。変更した設定内容は、管理端末上の Web 画面に表示される設定ボタンの押下により反映される。

また、ログアラート機能は、以下の事象が発生した場合に、その監査記録を記録する。
- ログアラート機能の起動
- ログアラート機能の終了
- ファイアウォール管理者へのアラートの通知

監査記録出力の流れを図 2-4 に示す。

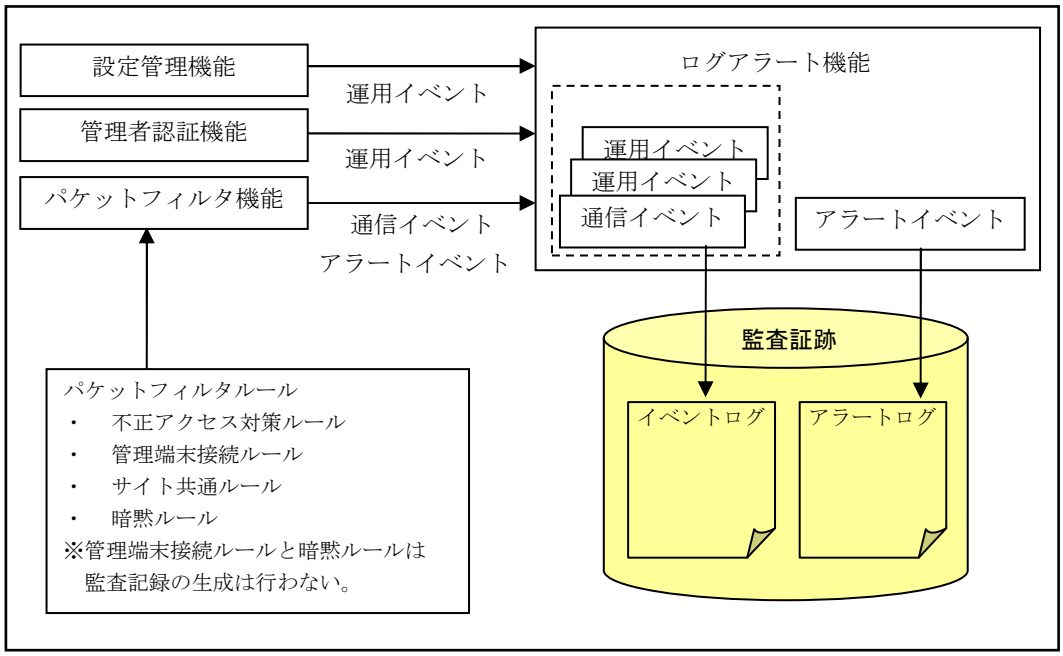

図 2-4 監査記録出力の流れ

Copyright © NEC Corporation 2007 All rights reserved.

設定管理機能、管理者認証機能から渡される監査記録は運用イベントである。パケットフィルタ機能から通知される監査記録は、通信イベント又はアラートイベントである。
ログアラート機能は、監査記録（運用イベント、通信イベント）を監査証跡（イベントログ）に格納し、監査記録（アラートイベント）を監査証跡（アラートログ）に格納する。

2.5 TOE 資産

TOE の保護資産は以下のとおりである。

1）ファイアウォールの各種設定情報
TOE の動作を決定する情報であり、パケットフィルタルール、ファイアウォール管理者情報、およびログアラート設定（監査証跡ファイル設定、アラート設定）を指す。
パケットフィルタルール（不正アクセス対策ルール、管理端末接続ルール）、およびファイアウォール管理者情報である ID とパスワードは、TOE 生成時に初期登録される。また、パケットフィルタルール（暗黙のルール）は、TOE 開発時に組み込まれる。
パケットフィルタルール、ファイアウォール管理者情報、およびログアラート設定（監査証跡ファイル設定、アラートアクション設定）は、TOE の運用中に更新することができる。

2）監査証跡
ファイアウォールの各種設定情報へのアクセス・IP パケット処理結果・識別認証結果を記録する情報であり、セキュリティ侵害の有無を監査するための資産となり、運用時に生成される。

3）内部ネットワークの情報
内部ネットワーク上に接続されている、ホストが保有する情報であり、TOE によって外部ネットワークからの脅威より守られる。

内部ネットワークの情報が利用者データであり、その他は TSF データである。

Copyright © NEC Corporation 2007 All rights reserved.

3 TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1 前提条件

A.SAFE_PLACE(安全な場所)
TOE および TOE がインストールされるファイアウォールサーバ、ハードウェア、及びパケットフィルタルールをバックアップした媒体は、システム管理者、およびファイアウォール管理者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・保管する。

A.NO_BYPASS(接続形態)
TOE を唯一の接点として、内部ネットワークと外部ネットワークを接続し、TOE 以外の迂回経路が存在しないネットワーク構成にする。

A.APPOINT(管理者の任命)
ファイアウォール管理責任者は信頼でき、信頼できるファイアウォール管理者、およびシステム管理者を任命する。

A.NO_EVIL(信頼できるシステム管理者、およびファイアウォール管理者)
システム管理者は、TOE の動作に必要となる TOE 外の OS や関連ソフトウェア、ハードウェア、管理端末の配付、設置、管理、運用に際して、TOE の正常動作が維持できるように管理する。
また、ファイアウォール管理者は、TOE が正しく動作するように、TOE を設定、監視、メンテナンスし、保守サービス員の作業に立ち会う。

A.PASSWORD_MANAGEMENT(システム管理者、およびファイアウォール管理者によるパスワードの管理)
ファイアウォール管理者は TOE にアクセスするためのファイアウォール管理者 ID とパスワードを、第三者に知られないように管理する。パスワードは推測・解析が容易でないものを設定し、適正な間隔で変更する。
また、システム管理者が TOE 以外の OS や各種サービスにアクセスする際に使用するシステム管理者の ID とパスワードも、TOE のファイアウォール管理者が使用する ID・パスワードと同様の基準で管理する。

A.OS(OS の選択とプラットフォームの要塞化)
TOE は、TOE のカーネルモジュールに悪影響を与えないことが実証されている、NEC が指定した OS にインストールする。
さらに、TOE が稼働するプラットフォームは、不要なサービスを停止し、不要なソフトウェアをインストールしない。

A.TRAINING(管理者の訓練)
システム管理者、およびファイアウォール管理者は、TOE および TOE の関連する周辺環境の運用に必要となる教育・訓練を受け、ガイダンスに則って TOE を運用する。

A.PASSWORD_INST(インストール時のパスワード設定)
ファイアウォール管理者は、TOE のインストール時に設定するパスワードをインストールガイダンスに則って設定する。

Copyright © NEC Corporation 2007 All rights reserved.

A.TRUSTED_PATH（高信頼チャネル）
ファイアウォール管理者は、管理端末と Web サーバ間の通信が盗聴されないように、Web サーバに HTTPS 通信のための設定を行う。

A.INJUSTICE_ACCESS_MEASURE（不正アクセス対策の設定）
ファイアウォール管理者は、「アドバンス」以外の不正アクセス対策レベルを選択しない。

3.2 脅威

本節に述べる攻撃者（悪意のある内部の一般利用者及び悪意のある外部の一般利用者）は、高度な専門知識を持たない低い攻撃能力を有するものとする。

T.INJUSTICE_LOGIN（不正ログイン）
悪意のある内部の一般利用者が、手当たり次第に ID とパスワードを試して TOE に不正ログインし、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定を破壊、改ざんしたり、監査記録を破壊、改ざんしたりする。

T.INVALID_NETWORK_ACCESS（内部サーバへの不正アクセス）
悪意のある外部の一般利用者が外部ネットワークから内部ネットワークに侵入し、内部ネットワークにある外部に公開されているサーバ上の情報を破壊、改ざんする。

T.SPOOFING（なりすまし）
悪意のある内部の一般利用者が、ファイアウォール管理者の離席時に管理端末を利用して、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定を破壊、改ざんする。

3.3 組織のセキュリティ方針

本 ST では、組織のセキュリティ方針はない。

Copyright © NEC Corporation 2007 All rights reserved.

4 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、環境セキュリティ対策方針について記述する。

4.1 TOE セキュリティ対策方針

O.SECURITY_MANAGEMENT(設定管理)
TOE は、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定の参照、更新を識別認証されたファイアウォール管理者に制限しなければならない。

O.ADMIN_ID_AUTH(識別認証)
TOE は、ID・パスワードを用いて TOE にアクセスする利用者を識別認証し、利用者がファイアウォール管理者であるか否かを判定する。

O.PACKET_FILTER(パケットフィルタ)
TOE は、ファイアウォール管理者がポリシにそって設定したパケットフィルタルールに基づいて、IP パケットの入出力を制御する。

O.AUDIT(監査)
TOE は、TOE に監査対象事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果、事象の内容を記録する。
また、ファイアウォール管理者は、監査記録を参照することによって、異常な動作を検出することが可能である。
さらに、TOE は、監査記録を出力する領域がファイアウォール管理者により設定されたディスク容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。

O.ALERT(アラート通知)
TOE は、TOE に対するセキュリティ侵害の可能性を検知した場合、ログアラート設定(アラートアクション設定)に基づき、ファイアウォール管理者へのアラートの通知を実行する。

4.2 環境セキュリティ対策方針

OEN.SAFE_PLACE(安全な場所)
TOE および TOE がインストールされるファイアウォールサーバ、ハードウェア、及びパケットフィルタルールをバックアップした媒体は、システム管理者、およびファイアウォール管理者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・保管しなければならない。

OEN.NO_BYPASS(接続形態)
TOE を唯一の接点として、内部ネットワークと外部ネットワークを接続し、TOE 以外の迂回経路が存在しないネットワーク構成にしなければならない。

OEN.APPOINT(管理者の任命)
ファイアウォール管理責任者は信頼でき、信頼できるファイアウォール管理者、およびシステム管理者を任命しなくてはならない。

OEN.NO_EVIL(信頼できるシステム管理者、およびファイアウォール管理者)

Copyright © NEC Corporation 2007 All rights reserved.

システム管理者は、TOE の動作に必要となる TOE 外の OS や関連ソフトウェア、ハードウェア、管理端末の配付、設置、管理、運用に際して、TOE の正常動作が維持できるように管理しなければならない。
また、ファイアウォール管理者は、TOE が正しく動作するように、TOE を設定、監視、メンテナンスし、保守サービス員の作業に立ち会わなければならない。

OEN.PASSWORD_MANAGEMENT（管理者によるパスワードの管理）
ファイアウォール管理者は TOE にアクセスするためのファイアウォール管理者 ID とパスワードを、第三者に知られないように管理しなければならない。パスワードは推測・解析が容易でないものを設定し、適正な間隔で変更しなければならない。
また、システム管理者が TOE 以外の OS や各種サービスにアクセスする際に使用するシステム管理者の ID とパスワードも、TOE のファイアウォール管理者が使用する ID・パスワードと同様の基準で管理しなければならない。

OEN.OS（OS の選択とプラットフォームの要塞化）
ファイアウォール管理者は TOE を、TOE のカーネルモジュールに悪影響を与えないことが実証されている、NEC が指定した OS にインストールしなくてはならない。
さらにシステム管理者は、TOE が稼働するプラットフォームは、不要なサービスを停止し、不要なソフトウェアをインストールしてはならない。

OEN.TRAINING（管理者の訓練）
システム管理者、およびファイアウォール管理者は、TOE および TOE の関連する周辺環境の運用に必要となる教育・訓練を受け、ガイダンスに則って TOE を運用しなければならない。

OEN.HOST_MANAGEMENT（管理端末の管理）
システム管理者及びファイアウォール管理者は、管理端末を設定画面が覗き見されないような場所に配置し、管理端末から離れるときには管理端末の操作をロックすることによって、離席時に第三者が管理端末を不正に利用することを防がなければならない。

OEN.PASSWORD_INST（インストール時のパスワード設定）
ファイアウォール管理者は、TOE のインストール時に設定するパスワードをインストールガイダンスに則って設定しなければならない。

OEN.TRUSTED_PATH（高信頼チャネル）
ファイアウォール管理者は、管理端末と Web サーバ間の通信が盗聴されないように、Web サーバに HTTPS 通信のための設定を行わなければならない。

OEN.INJUSTICE_ACCESS_MEASURE（不正アクセス対策の設定）
ファイアウォール管理者は、「アドバンス」以外の不正アクセス対策レベルを選択してはならない。

Copyright © NEC Corporation 2007 All rights reserved.

5 IT セキュリティ要件

本章では、TOE 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

5.1.1 TOE セキュリティ機能要件

TOE が提供するセキュリティ機能の機能要件を記述する。すべての機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用する。
セキュリティ機能要件の依存性を除去しているものは、以下の例の通り 2 重取消線を引いている。
2 重取消線の例:~~依存性の除去~~

◆ セキュリティ監査（FAU）

FAU_ARP.1 セキュリティアラーム

下位階層: なし

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*]

- ログアラート設定（アラートアクション設定）に基づく、ファイアウォール管理者へのアラートの通知

依存性: **FAU_SAA.1** 侵害の可能性の分析

FAU_GEN.1 監査データ生成

下位階層: なし

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

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

[選択: *最小、基本、詳細、指定なし*: から一つのみ選択**]**
指定なし
[割付: *上記以外の個別に定義した監査対象事象*]
以下の監査対象事象

- ファイアウォール管理者へのアラートの通知
- TSP 侵害の可能性の検出
- 監査記録の参照
- 対象となる IP パケットに対する処理結果、およびその判定に使用したセキュリティ属性
- ファイアウォール管理者パスワード検証の成功／失敗
- ファイアウォール管理者の識別認証の成功／失敗
- パケットフィルタルール（サイト共通ルール）の編集のための一時ファイルからの一括変更の成功
- ファイアウォール管理者パスワード改変の成功

Copyright © NEC Corporation 2007 All rights reserved.

- ファイアウォール管理者 ID 改変の成功
- ログアラート設定(監査証跡ファイル設定)改変の成功
- ログアラート設定(アラートアクション設定)改変、削除、追加の成功
- ログアラート設定(アラートアクション設定)の変更
- 設定管理機能の起動

各機能要件を選択した場合に、CC により規定された監査対象とすべきアクションと、それに対応する TOE の監査対象事象を表 5-1 に示す。

表 5-1 監査対象とすべきアクションと関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象	その他の監査関連情報
FAU_ARP.1	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。	[イベントログ] a) ファイアウォール管理者へのアラートの通知	なし
FAU_GEN.1	なし	なし	なし
FAU_SAA.1	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。	a)なし(分析メカニズムの活性化/非活性化はできないため。) b) なし(TSP 侵害の可能性の検出時点では、応答は返さないため。) [イベントログ、およびアラートログ] その他)TSP 侵害の可能性の検出	その他) 以下のいずれかの TSP 侵害の可能性の種別。 ・単位時間内に、同一の送信元 IP アドレスからの IP パケットを指定回数分破棄した。 ・単位時間内に、同一の送信先 IP アドレスへの IP パケットを指定回数分破棄した。 ・不正な送信元 IP アドレスを持つ IP パケットを検出した。
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	[イベントログ] a) 監査記録の参照	a)ファイアウォール管理者ID、および参照に使用した管理端末の IP アドレス
FAU_STG.4	a) 基本: 監査格納失敗によってとられるアクション。	なし(監査格納失敗時、TOE は停止するため。)	なし
FDP_IFC.1	なし	なし	なし

Copyright © NEC Corporation 2007 All rights reserved.

機能要件	監査対象とすべきアクション	監査対象事象	その他の監査関連情報
FDP_IFF.1	a) 最小: 要求された情報フローを許可する決定。 b) 基本: 情報フローに対する要求に関するすべての決定。 c) 詳細: 情報フローの実施を決定する上で用いられる特定のセキュリティ属性。 d) 詳細: 方針目的(policy goal)に基づいて流れた特定の情報のサブセット(例えば、対象物のレベル低下の監査)。	パケットフィルタルール(サイト共通ルール)に対する監査記録の出力要否の指定に基づいて生成される。 [イベントログ、アラートログ] b) 対象となる IP パケットに対する処理結果、およびその判定に使用したセキュリティ属性	b)対象となる IP パケットの送信元 IP アドレス・送信元ポート番号(TCP,UDP の場合)・送信先 IP アドレス・送信先ポート番号(TCP,UDP の場合)・プロトコル種別
FIA_SOS.1	a) 最小: TSF による、テストされた秘密の拒否; b) 基本: TSF による、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	[イベントログ] b)ファイアウォール管理者パスワード検証の成功／失敗	なし
FIA_UAU.2	a)最小: 認証メカニズムの不成功になった使用; b)基本: 認証メカニズムのすべての使用。	[イベントログ] b)ファイアウォール管理者の識別認証の成功／失敗	b)識別認証画面から入力されたファイアウォール管理者 ID
FID_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	[イベントログ] b)ファイアウォール管理者の識別認証の成功／失敗	b)識別認証画面から入力されたファイアウォール管理者 ID
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	[イベントログ] a)パケットフィルタルール(サイト共通ルール)の編集のための一時ファイルからの一括変更の成功	なし
FMT_MSA.3	a) 基本: 許可的あるいは制限的規則のデフォルト設定の改変。 b) 基本: セキュリティ属性の初期値の改変すべて。	[イベントログ] a)なし(デフォルト値設定は改変できないため) b)なし(FMT_MSA.1 で取得しているため)	なし

Copyright © NEC Corporation 2007 All rights reserved.

機能要件	監査対象とすべきアクション	監査対象事象	その他の監査関連情報
FMT_MTD.1	a) 基本: TSF データの値のすべての改変。	[イベントログ] a)ファイアウォール管理者パスワード改変の成功 a)ファイアウォール管理者 ID 改変の成功 a)ログアラート設定(監査証跡ファイル設定)改変の成功 a)ログアラート設定(アラートアクション設定)改変、削除、追加の成功	その他) [イベントログ] ログアラート設定(アラートアクション設定)の有無
FMT_SMF.1	a) 最小:管理機能の使用	[イベントログ] a)設定管理機能の起動	なし
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	a)なし(ファイアウォール管理者は一人しかいないため。)	なし
FPT_RVM.1	なし	なし	なし
FPT_SEP.1	なし	なし	なし
FPT_STM.1	a) 最小: 時間の変更; b) 詳細: タイムスタンプの提供。	a)なし(OS の機能によるため。)	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*]

その他の監査関連情報は、表 5-1 に示す通り。

依存性: **FPT_STM.1** 高信頼タイムスタンプ

FAU_SAA.1 侵害の可能性の分析

下位階層: なし

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、これらの規則にもとづき 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 パケットを指定回数分破棄した。

Copyright © NEC Corporation 2007 All rights reserved.

・ 単位時間内に、同一の送信先 IP アドレスへの IP パケットを指定回数分破棄した。
・ 不正な送信元 IP アドレスを持つ IP パケットを検出した。

[割付:*その他の規則*]
なし

依存性: **FAU_GEN.1** 監査データ生成

FAU_SAR.1 監査レビュー
下位階層: なし
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。

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。

[割付:*許可利用者*]
ファイアウォール管理者
[割付:*監査情報のリスト*]
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、その他の監査関連情報

依存性: **FAU_GEN.1** 監査データ生成

FAU_STG.4 監査データ損失の防止
下位階層: FAU_STG.3
FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[**選択:** ***監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択***]及び[**割付:** ***監査格納失敗時に取られるその他のアクション***]を行わねばならない。

[選択: ***監査対象事象の無視、特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き: から一つのみ選択***]
最も古くに格納された監査記録への上書き
[割付: ***監査格納失敗時に取られるその他のアクション***]
ハードディスクに障害が発生した場合は、TOE は停止する

依存性: ~~**FAU_STG.1** 保護された監査証跡格納~~

◆ **利用者データ保護(FDP)**
FDP_IFC.1 サブセット情報フロー制御
下位階層: なし
FDP_IFC.1.1 TSF は、[**割付:*サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト***]に対して[**割付:*情報フロー制御 SFP***]を実施しなければならない。
[**割付:*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***

Copyright © NEC Corporation 2007 All rights reserved.

たはサブジェクトから制御された情報の流れを引き起こす操作のリスト]

- サブジェクトのリスト
  ネットワークインタフェース
- 情報のリスト
  TOE を介して送受信される IP パケット
- 操作のリスト
  通過
  拒否(送信元へエラーを通知するとともに破棄)
  破棄(送信元へエラーを返さずに破棄)

[**割付:*情報フロー制御 SFP***]
パケットフィルタ方針

依存性: **FDP_IFF.1** 単純セキュリティ属性

FDP_IFF.1 単純セキュリティ属性
下位階層: なし
FDP_IFF.1.1 TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[**割付:*情報フロー制御 SFP***]を実施しなければならない: [**割付:*示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性***]。

[**割付: *情報フロー制御 SFP***]
パケットフィルタ方針
[**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、及び各々のセキュリティ属性***]

- サブジェクトのリスト
  ネットワークインタフェース
- サブジェクトのセキュリティ属性
  受信ネットワークインタフェース
  送信ネットワークインタフェース
- 情報のリスト
  TOE を介して送受信される IP パケット
- 情報のセキュリティ属性
  送信元 IP アドレス(ホスト、またはネットワーク)
  送信先 IP アドレス(ホスト、またはネットワーク)
  プロトコル種別(TCP、UDP、ICMP)
  送信元ポート番号(TCP、UDP の場合)
  送信先ポート番号(TCP、UDP の場合)

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もとづく関係***]。

[**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もとづく関係***]

Copyright © NEC Corporation 2007 All rights reserved.

TOE は、送受信される IP パケットを扱うサブジェクトのセキュリティ属性及び IP パケットから取得した情報のセキュリティ属性をパケットフィルタルールに基づいて評価し、当該 IP パケットの通過・拒否・破棄の処理を実施する。

FDP_IFF.1.3 TSF は、[**割付:*追加の情報フロー制御 SFP 規則***]を実施しなければならない。

[割付:*追加の情報フロー制御 SFP 規則*]
なし。

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

[割付:*追加の SFP 能力のリスト*]
なし。

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

[**割付:*セキュリティ属性に基づいて、明示的に情報フローを承認する規則***]
なし。

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

[**割付:*セキュリティ属性に基づいて、明示的に情報フローを拒否する規則***]
なし。

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

◆ **識別と認証(FIA)**

FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が[**割付:*定義された品質尺度***]に合致することを検証するメカニズムを提供しなければならない。

[割付: *定義された品質尺度*]
定義された品質尺度は、表 5-2 に示す通り。

表 5-2 パスワード規則

パスワード長	使用可能文字
6～8 文字	数字(0～9) 英文字(a～z、A～Z) 記号(# $ ' ( ) * + , - . / : = ? @ [¥] _ ` { } ~ !)

依存性: なし

Copyright © NEC Corporation 2007 All rights reserved.

FIA_UAU.2 アクション前の利用者認証
下位階層: **FIA_UAU.1**
FIA_UAU.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: **FIA_UID.1** 識別のタイミング

FIA_UID.2 アクション前の利用者識別
下位階層: **FIA_UID.1**
FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

◆ **セキュリティ管理(FMT)**
FMT_MSA.1 セキュリティ属性の管理
下位階層: なし
FMT_MSA.1.1 TSF は、セキュリティ属性[**割付:*セキュリティ属性のリスト***]に対し[**選択:** ***デフォルト値変更、問い合わせ、改変、削除***、[**割付:*その他の操作*]]をする能力を[**割付:*許可された識別された役割***]に制限するために[**割付:*アクセス制御 SFP、情報フロー制御 SFP***]を実施しなければならない。

[割付:*セキュリティ属性のリスト*]
パケットフィルタルールが対応するセキュリティ属性は下記の通り。
- 受信ネットワークインタフェース
- 送信ネットワークインタフェース
- 送信元 IP アドレス(ホスト、またはネットワーク)
- 送信先 IP アドレス(ホスト、またはネットワーク)
- プロトコル種別(TCP、UDP、ICMP)
- 送信元ポート番号(TCP、UDP の場合)
- 送信先ポート番号(TCP、UDP の場合)

[選択:*デフォルト値変更、問い合わせ、改変、削除*、[割付:*その他の操作*]]
パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除
[割付:*その他の操作*]
パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の追加、インポート/エクスポート、バックアップ/リストア
[割付:*許可された識別された役割*]
ファイアウォール管理者
[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(パケットフィルタ方針)

依存性: [**FDP_ACC.1** サブセットアクセス制御 または

Copyright © NEC Corporation 2007 All rights reserved.

FDP_IFC.1 サブセット情報フロー制御]
FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.3 静的属性初期化
下位階層: なし
FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性として、[**選択:*制限的、許可的 : から一つのみ選択***、[**割付:*その他の特性***]]デフォルト値を与える[**割付:*アクセス制御 SFP、情報フロー制御 SFP***]を実施しなければならない。

[**選択:*制限的、許可的 : から一つのみ選択***、[**割付:*その他の特性***]]
制限的
[**割付:*アクセス制御 SFP 、情報フロー制御 SFP***]
情報フロー制御 SFP(パケットフィルタ方針)

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成されるとき、[**割付:*許可された識別された役割***]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

[**割付:*許可された識別された役割***]
ファイアウォール管理者

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

FMT_MTD.1 TSF データの管理
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***]
- ファイアウォール管理者 ID
- ファイアウォール管理者のパスワード
- ログアラート設定(監査証跡ファイル設定)
- ログアラート設定(アラートアクション設定)

[**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**]]
TSF データの種別と操作の対応は表 5-3 に示す通り。

表 5-3 TSF データの種別と操作の対応

TSF データ	操作
ファイアウォール管理者 ID	改変
ファイアウォール管理者のパスワード	改変
ログアラート設定(監査証跡ファイル設定)	問い合わせ、改変
ログアラート設定(アラートアクション設定)	問い合わせ、改変、削除、追加

Copyright © NEC Corporation 2007 All rights reserved.

[割付:*許可された識別された役割*]
ファイアウォール管理者

依存性: **FMT_SMF.1** 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定
下位階層: なし
FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:**[割付:*TSF によって提供されるセキュリティ管理機能のリスト*]**。

[割付:*TSF によって提供されるセキュリティ管理機能のリスト*]
TOE における管理項目は以下のとおりである。
- ファイアウォール管理者 ID の改変
- ファイアウォール管理者のパスワードの改変
- ログアラート設定(監査証跡ファイル設定)の問い合わせ、改変
- ログアラート設定(アラートアクション設定)の問い合わせ、改変、削除、追加
- パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストア

表 5-4 機能要件に対して CC で規定している管理要件と TOE における管理項目を示す。

表 5-4 機能要件に対して CC で規定している管理要件と TOE における管理項目

機能要件	CC で規定している管理要件	TOE における管理項目
FAU_ARP.1	a) アクションの管理(追加、除去、改変)。	a)ログアラート設定(アラートアクション設定)の問い合わせ、改変、削除、追加
FAU_GEN.1	なし	なし
FAU_SAA.1	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。	なし(規則は固定であり、管理対象とならない)
FAU_SAR.1	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)。	なし(監査証跡の参照は、ファイアウォール管理者のみのため、管理対象とならない)
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	なし(監査格納失敗時は TOE が停止するため、管理対象とならない)
FDP_IFC.1	なし	なし
FDP_IFF.1	a) 明示的なアクセスに基づく決定に使われる属性の管理。	パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストア
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理。	なし(パスワードの文字数の尺度は、変更できないため、管理対象とならない)
FIA_UAU.2	管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	ファイアウォール管理者のパスワードの改変
FID_UID.2	a) 利用者識別情報の管理。	a)ファイアウォール管理者 ID の改変

Copyright © NEC Corporation 2007 All rights reserved.

機能要件	CC で規定している管理要件	TOE における管理項目
FMT_MSA.1	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	なし(役割のグループは固定であり、管理対象とならない)
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	a)なし(役割のグループは固定であり、管理対象とならない) b)なし(暗黙のルールは変更できないため、不正アクセス対策ルールは「アドバンス」以外選択されないため、管理端末接続ルールは設定されているIPアドレス以外のパケットを取り込まないため、管理対象とならない)
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし(役割のグループは固定であり、管理対象とならない)
FMT_SMF.1	なし	なし
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	なし(役割のグループは固定であり、管理対象とならない)
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし
FPT_STM.1	a) 時間の管理。	なし(TOE は時間を変更しないため、管理対象とならない)

依存性: なし

FMT_SMR.1 セキュリティ役割
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*]
ファイアウォール管理者

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

◆ **TSF の保護(FPT)**
FPT_RVM.1 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

FPT_SEP.1 TSFドメイン分離
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や改ざんからそ

Copyright © NEC Corporation 2007 All rights reserved.

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

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、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

5.1.2 最小機能強度レベル

この TOE の最小機能強度レベルは、低程度(SOF-基本)であり、確率的または順列的メカニズムを適用する TOE セキュリティ機能要件は FIA_SOS.1 である。

5.1.3 TOE セキュリティ保証要件

TOE の評価保証レベルは EAL1 である。すべての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 のコンポーネントを直接使用する。

[EAL1規定コンポーネント]

1) 構成管理
   ACM_CAP.1:バージョン番号
2) 配布と運用
   ADO_IGS.1:設置、生成、および立上げ手順
3) 開発
   ADV_FSP.1:非形式的機能仕様
   ADV_RCR.1:非形式的対応の実証
4) ガイダンス文書
   AGD_ADM.1:管理者ガイダンス
   AGD_USR.1:利用者ガイダンス
5) ライフサイクルサポート
   なし
6) テスト
   ATE_IND.1:独立テスト - 準拠
7) 脆弱性評定
   なし

5.2 IT 環境セキュリティ要件

5.2.1 IT 環境セキュリティ機能要件

本 ST では、IT 環境が提供するセキュリティ機能の機能要件は定義しない。

Copyright © NEC Corporation 2007 All rights reserved.

6 TOE 要約仕様

この章では、TOE の要約仕様を記述する。

6.1 TOE セキュリティ機能

この節では、TOE のセキュリティ機能を説明する。表 6-1 に示すように、本節で説明するセキュリティ機能は、5.1.1 節で記述した TOE セキュリティ機能要件を満たすものである。
「×」は、対応関係があることを表す。

表 6-1 TOE セキュリティ機能とセキュリティ機能要件の対応関係

セキュリティ機能要件 / TOE セキュリティ機能	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.4	FDP_IFC.1	FDP_IFF.1	FIA_SOS.1	FIA_UAU.2	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1
SF.MNG											×	×	×	×	×	×	×	
SF.I&A								×	×	×						×	×	
SF.PF						×	×									×	×	
SF.AUDIT	×	×	×	×	×											×	×	×

TOE は OS の起動により開始され、OS の停止により終了する。

6.1.1 設定管理機能(SF.MNG)

本機能は、SF.I&A(管理者認証機能)と同一プロセスであり、SF.I&A(管理者認証機能)による識別認証が成功した場合に限り動作する。
ファイアウォール管理者は管理端末上の Web ブラウザを操作して本機能にアクセスする。

TOE は、以下に示すセキュリティ管理機能を提供する(FMT_SMF.1)。

- ファイアウォール管理者 ID の改変
- ファイアウォール管理者のパスワードの改変
- ログアラート設定(監査証跡ファイル設定)の問い合わせ、改変
- ログアラート設定(アラートアクション設定)の問い合わせ、改変、削除、追加
- パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストア

TOE は、ファイアウォール管理者という役割を維持するとともに、利用者をファイアウォール管理者という役割に関連付ける(FMT_SMR.1)。

TOE は、パケットフィルタルールが対応する以下のセキュリティ属性に対し、パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ・リストアする操作をファイアウォール管理者に限り許可する(FMT_MSA.1)。

- 受信ネットワークインタフェース
- 送信ネットワークインタフェース
- 送信元 IP アドレス(ホスト、またはネットワーク)
- 送信先 IP アドレス(ホスト、またはネットワーク)

Copyright © NEC Corporation 2007 All rights reserved.

- プロトコル種別(TCP、UDP、ICMP)
- 送信元ポート番号(TCP、UDP の場合)
- 送信先ポート番号(TCP、UDP の場合)

TOE は、TOE 開発時に設定された暗黙のルール及び生成時に設定された不正アクセス対策ルールにより、全体が制限的ルールとなっているパケットフィルタルールに対する管理端末設定ルール及びサイト共通ルールによる指定を、ファイアウォール管理者に限り許可する(FMT_MSA.3)。

但し、パケットフィルタルール(不正アクセス対策ルール)については OEN.INJUSTICE_ACCESS_MEASURE により、「アドバンス」以外の不正アクセス対策レベルは選択されない。

TOE は、識別認証されたファイアウォール管理者のみに表 5-3 に示す操作を許可する(FMT_MTD.1)。

TOEは、SF.I&A(管理者認証機能)による識別認証に成功した場合に限り、その利用者を代行して動作する SF.MNG(設定管理機能)の動作が許可されることを保証する(FPT_RVM.1)。また、SF.MNG(設定管理機能)は、自身を保護し、干渉・改ざん・暴露から保護される(FPT_SEP.1)。

6.1.2 管理者認証機能(SF.I&A)

本機能は、SF.MNG(設定管理機能)と同一プロセスであり、SF.MNG の実行に先立って動作する。
ファイアウォール管理者は管理端末上の Web ブラウザを操作して、本機能にアクセスする。

TOE は、TOE へアクセスする利用者(ファイアウォール管理者)に対して、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、利用者に自分自身を識別し、認証が成功することを要求する(FIA_UID.2、FIA_UAU.2)。

TOEは、ファイアウォール管理者 ID とパスワードの変更時に、新たなパスワードの候補として入力された文字列が表 5-2 の規則を満たさない場合には、入力されたパスワードの受入れを拒否する(FIA_SOS.1)。

TOE は、SF.MNG(設定管理機能)の動作を許可する前に、SF.I&A(管理者認証機能)を呼び出し、ファイアウォール管理者 ID とパスワードによる識別認証が成功した場合に限って、業務の実行を許可することを保証する(FPT_RVM.1)。また、SF.I&A(管理者認証機能)は、自身を保護し、干渉・改ざん・暴露から保護される(FPT_SEP.1)。

6.1.3 パケットフィルタ機能(SF.PF)

本機能は、カーネルモジュールとして動作する。

TOE は、TOE を介して送受信される IP パケットに対して、以下の機能を提供する。

TOEは、TOEを介して送受信されるIPパケットに対して、パケットフィルタ方針を適用して通過・拒否(送信元へエラーを通知するとともに破棄)・破棄(送信元へエラーを返さずに破棄)の処理を実施する(FDP_IFC.1)。

Copyright © NEC Corporation 2007 All rights reserved.

TOE は、TOE を介して送受信される IP パケットから取得した、ネットワークインタフェースのセキュリティ属性と IP パケットのセキュリティ属性に基づいて、情報フロー制御 SFP(パケットフィルタ方針)に従って評価し、通過・拒否・破棄の処理を実施する(FDP_IFF.1)。
以下に、セキュリティ属性を示す。

ネットワークインタフェースのセキュリティ属性
- 受信ネットワークインタフェース
- 送信ネットワークインタフェース

IP パケットのセキュリティ属性
- 送信元 IP アドレス(ホスト、またはネットワーク)
- 送信先 IP アドレス(ホスト、またはネットワーク)
- プロトコル種別(TCP、UDP、ICMP)
- 送信元ポート番号(TCP、UDP の場合)
- 送信先ポート番号(TCP、UDP の場合)

TOE は、TOE を介して IP パケットが送受信される際に、受信した IP パケットを指定された送信先に送信する前に、SF.PF(パケットフィルタ機能)を呼び出すことにより、SF.PF(パケットフィルタ機能)が成功することを保証する(FPT_RVM.1)。また、SF.PF(パケットフィルタ機能)は、OEN.OS によりカーネルモジュールに悪影響を与えない OS にインストールされる。さらに不要なソフトウェアやサービスが存在しないことにより、干渉・改ざん・暴露から保護される(FPT_SEP.1)。

6.1.4 ログアラート機能(SF.AUDIT)

本機能は、デーモンモジュールとして動作する。

TOE は、TOE に対するセキュリティ侵害の可能性を検知するため、以下の監査対象事象が発生した場合、監査記録を生成する(FAU_GEN.1)。
- 監査機能の起動と終了(TOE の起動と終了として監査記録を生成する。)
- 表 5-1 に示す監査対象事象

TOE は、以下の項目をもつ監査記録を生成する(FAU_GEN.1)。
- 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
- 表 5-1 に示すその他の監査関連情報

TOE は、監査記録に付与される事象の日付・時刻として、OS から取得した日付・時刻を付与する(FPT_STM.1)。

TOE は、ファイアウォール管理者が以下の監査情報リストを解釈に適した形式で監査証跡参照機能を提供する(FAU_SAR.1)。
- 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
- 表 5-1 に示すその他の監査関連情報

Copyright © NEC Corporation 2007 All rights reserved.

TOE は、生成した監査記録が、ログアラート設定(監査証跡ファイル設定)に基づく規則に該当した場合、監査記録を下記の方法により維持し、監査データの損失を防止する(FAU_STG.4)。
・ 最も古くに格納された監査記録への上書き

TOE は、ハードディスクに障害が発生した場合は、TOE が停止することにより、監査データの損失を防止する(FAU_STG.4)。

TOE は、パケットフィルタルール(不正アクセス対策ルール)の設定に基づいて取得された監査データ中に、以下の事象を検知した場合、ログアラート設定(アラートアクション設定)が定義する方法により、ファイアウォール管理者に対してアラートを通知する(FAU_SAA.1、FAU_ARP.1)。
- 単位時間内に、同一の送信元 IP アドレスからの IP パケットを指定回数分破棄した
- 単位時間内に、同一の送信先 IP アドレスへの IP パケットを指定回数分破棄した
- 不正な送信元 IP アドレスを持つ IP パケットを検出した

各機能からの監査対象事象の記録依頼の仕組みは開発時に組み込まれている。TOE は、監査対象事象の記録依頼の仕組みを除去したり停止したりする機能を持たない。このため、必要なすべての監査対象事象の記録依頼に対し、監査記録が生成され、格納されることが保証される(FPT_RVM.1)。また、SF.AUDIT(ログアラート機能)のデーモンモジュールは自身を保護し、干渉・改ざん・暴露から保護される(FPT_SEP.1)。

6.2 セキュリティ機能強度

確率的または順列的メカニズムに基づくセキュリティ機能は、上述の SF.I&A である。
SF.I&A のパスワード照会メカニズムの機能強度レベルが SOF-基本である。

6.3 保証手段

この章では、TOE のセキュリティ保証手段を説明する。 表 6-2 に示すように、以下のセキュリティ保証手段は、5.1.3 節で記述した TOE セキュリティ保証要件を満たすものである。

表 6-2 保証手段と保証要件コンポーネントの対応関係

保証要件クラス	保証要件 コンポーネント	保証手段
ACM:構成管理	ACM_CAP.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 TOE NEC ファイアウォール SG コアユニット Ver 1.0.0 セキュリティターゲット
ADO:配布と運用	ADO_IGS.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 インストールガイダンス
ADV:開発	ADV_FSP.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 機能仕様書
	ADV_RCR.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 表現対応分析書
AGD: ガイダンス文書	AGD_ADM.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 運用管理・操作利用ガイダンス
	AGD_USR.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 運用管理・操作利用ガイダンス ※上記文書にて包括
ATE:テスト	ATE_IND.1	NEC ファイアウォール SG コアユニット Ver 1.0.0 TOE

Copyright © NEC Corporation 2007 All rights reserved.

7 PP 主張

この章では、PP 主張について記述する。

7.1 PP 参照

参照した PP はない。

7.2 PP 修整

修整した PP はない。

7.3 PP 追加

PP への追加はない。

Copyright © NEC Corporation 2007 All rights reserved.

8 根拠

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

8.1 セキュリティ対策方針根拠

セキュリティ対策は、TOE セキュリティ環境で規定した脅威に対抗するためのものである。あるいは、前提条件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抗する脅威および前提条件の対応関係を表 8-1 に示す。
「×」は、対応関係があることを表す。

表 8-1 セキュリティ対策方針と対抗する脅威および前提条件

	T.INJUSTICE_LOGIN	T.INVALID_NETWORK_ACCESS	T.SPOOFING	A.SAFE_PLACE	A.NO_BYPASS	A.APPOINT	A.NO_EVIL	A.PASSWORD_MANAGEMENT	A.OS	A.TRAINING	A.PASSWORD_INST	A. TRUSTED_PATH	A.INJUSTICE_ACCESS_MEASURE
O.SECURITY_MANAGEMENT	×												
O.ADMIN_ID_AUTH	×												
O.PACKET_FILTER		×											
O.AUDIT	×	×	×										
O.ALERT	×	×											
OEN.SAFE_PLACE				×									
OEN.NO_BYPASS					×								
OEN.APPOINT						×							
OEN.NO_EVIL							×						
OEN.PASSWORD_MANAGEMENT	×		×					×					
OEN.OS									×				
OEN.TRAINING			×							×			
OEN.HOST_MANAGEMENT			×										
OEN.PASSWORD_INST											×		
OEN.TRUSTED_PATH												×	
OEN.INJUSTICE_ACCESS_MEASURE													×

次節以降で、各脅威がセキュリティ対策方針で対抗できること、また各組織のセキュリティ方針・前提条件がセキュリティ対策方針で実現できることを説明する。

8.1.1 脅威に対するセキュリティ対策方針

T.INJUSTICE_LOGIN（不正ログイン）
T.INJUSTICE_LOGIN は、以下の記述である。
「悪意のある内部の一般利用者が、手当たり次第にIDとパスワードを試してTOEに不正ログインし、パケ

Copyright © NEC Corporation 2007 All rights reserved.

ットフィルタルール・ファイアウォール管理者情報・ログアラート設定を破壊、改ざんしたり、監査記録を破壊、改ざんしたりする。」
この脅威は、O.SECURITY_MANAGEMENT、O.ADMIN_ID_AUTH、O.AUDIT、O.ALERT 、OEN.PASSWORD_MANAGEMENT により対抗できる。根拠を以下に述べる。

O.SECURITY_MANAGEMENT では、以下を実施する。
・ TOE は、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定の参照、更新を識別認証されたファイアウォール管理者に制限しなければならない。
上記により、TSF データの参照・更新をファイアウォール管理者に限定することにより、破壊、改ざんを防止することができる。したがって、O.SECURITY_MANAGEMENT は T.INJUSTICE_LOGIN の軽減に寄与している。

O.ADMIN_ID_AUTH では、以下を実施する。
・ TOE は、ID・パスワードを用いて TOE にアクセスする利用者を識別認証し、利用者がファイアウォール管理者であるか否かを判定する。
上記により、ID・パスワードによる識別認証では、利用者は必ず識別認証されるため、ID・パスワードによる TOE の利用をファイアウォール管理者のみに制限することができる。したがって、O.ADMIN_ID_AUTH は T.INJUSTICE_LOGIN の軽減に寄与している。

O.AUDIT では、以下を実施する。
・ TOE は、TOE に監査対象事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果、事象の内容を記録する。
また、ファイアウォール管理者は、監査記録を参照することによって、異常な動作を検出することが可能である。
さらに、TOE は、監査記録を出力する領域がファイアウォール管理者により設定されたディスク容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。
上記により、ファイアウォール管理者は監査記録を参照することで、ID・パスワードによる識別・認証の連続試行、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定の改ざんを知ることができる。したがって、O.AUDIT は T.INJUSTICE_LOGIN の影響の緩和に寄与している。

O.ALERT では、以下を実施する。
・ TOE は、TOE に対するセキュリティ侵害の可能性を検知した場合、ログアラート設定(アラートアクション設定)に基づき、ファイアウォール管理者へのアラートの通知を実行する。
上記により、ファイアウォール管理者にアラート通知することで、不正行為の抑止効果を得ることができる。したがって、O.ALERT は T.INJUSTICE_LOGIN の影響の緩和に寄与している。

OEN.PASSWORD_MANAGEMENT では、以下を実施する。
・ ファイアウォール管理者は TOE にアクセスするためのファイアウォール管理者 ID とパスワードを、第三者に知られないように管理しなければならない。パスワードは推測・解析が容易でないものを設定し、適正な間隔で変更しなければならない。
・ システム管理者が TOE 以外の OS や各種サービスにアクセスする際に使用するシステム管理者の ID とパスワードも、TOE のファイアウォール管理者が使用する ID・パスワードと同様の基準で管理しなければならない。
上記により、ファイアウォール管理者は、パスワードを第三者に漏えいせず、推測・解析されにくいパスワ

Copyright © NEC Corporation 2007 All rights reserved.

ードを設定し、パスワードを適切な間隔で変更する。また、システム管理者は、ファイアウォール管理者と同様の基準で管理することにより、パスワードの不正入手することは困難になる。したがって、OEN.PASSWORD_MANAGEMENT は T.INJUSTICE_LOGIN の軽減に寄与している。

以上の対策により、T.INJUSTICE_LOGIN は、O.SECURITY_MANAGEMENT、O.ADMIN_ID_AUTH、O.AUDIT、O.ALERT、OEN.PASSWORD_MANAGEMENT により軽減され、その影響の緩和に寄与している。

T.INVALID_NETWORK_ACCESS(内部サーバへの不正アクセス)
T.INVALID_NETWORK_ACCESS は、以下の記述である。
「悪意のある外部の一般利用者が外部ネットワークから内部ネットワークに侵入し、内部ネットワークにある外部に公開されているサーバ上の情報を破壊、改ざんする。」
この脅威は、O.PACKET_FILTER、O.AUDIT、O.ALERT により対抗できる。根拠を以下に述べる。

O.PACKET_FILTER では、以下を実施する。
- TOE は、ファイアウォール管理者がポリシにそって設定したパケットフィルタルールに基づいて、IP パケットの入出力を制御する。

上記により、パケットフィルタルールに基づいて、IP パケットの入出力を制御することで、外部ネットワークより TOE を介して外部に公開されているサーバに対しての設定したルールに反する攻撃を防止することができる。したがって、O.PACKET_FILTER は T.INVALID_NETWORK_ACCESS の軽減に寄与している。

O.AUDIT では、以下を実施する。
- TOE は、TOE に監査対象事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果、事象の内容を記録する。
  また、ファイアウォール管理者は、監査記録を参照することによって、異常な動作を検出することが可能である。
  さらに、TOE は、監査記録を出力する領域がファイアウォール管理者により設定されたディスク容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。

上記により、ファイアウォール管理者は監査記録を参照することで、外部ネットワークからセキュリティ侵害されたことを知ることができる。したがって、O.AUDIT は T.INVALID_NETWORK_ACCESS の影響の緩和に寄与している。

O.ALERT では、以下を実施する。
- TOE は、TOE に対するセキュリティ侵害の可能性を検知した場合、ログアラート設定(アラートアクション設定)に基づき、ファイアウォール管理者へのアラートの通知を実行する。

上記により、ファイアウォール管理者にアラート通知することで、外部ネットワークからセキュリティ侵害の可能性に対して対策することができる。したがって、O.ALERT は T.INVALID_NETWORK_ACCESS の影響の緩和に寄与している。

以上の対策により、T.INVALID_NETWORK_ACCESS は、O.PACKET_FILTER、O.AUDIT、O.ALERT により軽減され、その影響の緩和に寄与している。

T.SPOOFING(なりすまし)

Copyright © NEC Corporation 2007 All rights reserved.

T.SPOOFING は、以下の記述である。
「悪意のある内部の一般利用者が、ファイアウォール管理者の離席時に管理端末を利用して、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定を破壊、改ざんする。」
この脅威は、O.AUDIT、OEN.PASSWORD_MANAGEMENT、OEN.TRAINING、OEN.HOST_MANAGEMENT により対抗できる。根拠を以下に述べる。

O.AUDIT では、以下を実施する。
- TOE は、TOE に監査対象事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果、事象の内容を記録する。
  また、ファイアウォール管理者は、監査記録を参照することによって、異常な動作を検出することが可能である。
  さらに、TOE は、監査記録を出力する領域がファイアウォール管理者により設定されたディスク容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。

上記により、なりすましによる不正行為を検出することができる。したがって、O.AUDIT は T.SPOOFING の影響の緩和に寄与している。

OEN.PASSWORD_MANAGEMENT では、以下を実施する。
- ファイアウォール管理者は TOE にアクセスするためのファイアウォール管理者 ID とパスワードを、第三者に知られないように管理しなければならない。パスワードは推測・解析が容易でないものを設定し、適正な間隔で変更しなければならない。
- システム管理者が TOE 以外の OS や各種サービスにアクセスする際に使用するシステム管理者の ID とパスワードも、TOE のファイアウォール管理者が使用する ID・パスワードと同様の基準で管理しなければならない。

上記により、ファイアウォール管理者は、パスワードを第三者に漏えいせず、推測・解析されにくいパスワードを設定し、パスワードを適切な間隔で変更する。また、システム管理者は、ファイアウォール管理者と同様の基準で管理することにより、パスワードの不正入手することは困難になる。したがって、OEN.PASSWORD_MANAGEMENT は T.SPOOFING の軽減に寄与している。

OEN.TRAINING では、以下を実施する。
- システム管理者、およびファイアウォール管理者は、TOE および TOE の関連する周辺環境の運用に必要となる教育・訓練を受け、ガイダンスに則って TOE を運用しなければならない。

上記により、離籍時の管理端末の取り扱いについて、十分な教育を受けているので管理端末の不正使用が困難となる。OEN.TRAINING は T.SPOOFING の軽減に寄与している。

OEN.HOST_MANAGEMENT では、以下を実施する。
- システム管理者及びファイアウォール管理者は、管理端末を設定画面が覗き見されないような場所に配置し、管理端末から離れるときには管理端末の操作をロックすることによって、離席時に第三者が管理端末を不正に利用することを防がなければならない。

上記により、管理端末の不正使用が困難となる。したがって、OEN.HOST_MANAGEMENT は T.SPOOFING の軽減に寄与している。

以上の対策により、T.SPOOFING は、O.AUDIT、OEN.PASSWORD_MANAGEMENT、OEN.TRAINING 、OEN.HOST_MANAGEMENT により軽減され、その影響の緩和に寄与している。

Copyright © NEC Corporation 2007 All rights reserved.

8.1.2 前提条件に対するセキュリティ対策方針

A.SAFE_PLACE(安全な場所)

A.SAFE_PLACE は、以下の記述である。

「TOE および TOE がインストールされるファイアウォールサーバ、ハードウェア、及びパケットフィルタルールをバックアップした媒体は、システム管理者、およびファイアウォール管理者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・保管する。」

この前提条件は、OEN.SAFE_PLACE によって満たされる。根拠を以下に述べる。

OEN.SAFE_PLACE では、以下を実施する。

- TOE および TOE がインストールされるファイアウォールサーバ、ハードウェア、及びパケットフィルタルールをバックアップした媒体は、システム管理者、およびファイアウォール管理者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・保管しなければならない。

上記により、A.SAFE_PLACE は、OEN.SAFE_PLACE により満たされる。

以上により、A.SAFE_PLACE は、OEN.SAFE_PLACE により意図する使用法が満たされ、環境が A.SAFE_PLACE と一貫する。

A.NO_BYPASS(接続形態)

A.NO_BYPASS は、以下の記述である。

「TOE を唯一の接点として、内部ネットワークと外部ネットワークを接続し、TOE 以外の迂回経路が存在しないネットワーク構成にする。」

この前提条件は、OEN.NO_BYPASS によって満たされる。根拠を以下に述べる。

OEN.NO_BYPASS では、以下を実施する。

- TOE を唯一の接点として、内部ネットワークと外部ネットワークを接続し、TOE 以外の迂回経路が存在しないネットワーク構成にしなければならない。

上記により、A.NO_BYPASS は、OEN.NO_BYPASS により満たされる。

以上により、A.NO_BYPASS は、OEN.NO_BYPASS により意図する使用法が満たされ、環境が A.NO_BYPASS と一貫する。

A.APPOINT(管理者の任命)

A.APPOINT は、以下の記述である。

「ファイアウォール管理責任者は信頼でき、信頼できるファイアウォール管理者、およびシステム管理者を任命する。」

この前提条件は、OEN.APPOINT によって満たされる。根拠を以下に述べる。

OEN.APPOINT では、以下を実施する。

- ファイアウォール管理責任者は信頼でき、信頼できるファイアウォール管理者、およびシステム管理者を任命しなくてはならない。

上記により、A.APPOINT は、OEN.APPOINT により満たされる。

以上により、A.APPOINT は、OEN.APPOINT により意図する使用法が満たされ、環境が A.APPOINT と一貫する。

Copyright © NEC Corporation 2007 All rights reserved.

A.NO_EVIL(信頼できるシステム管理者、およびファイアウォール管理者)
A.NO_EVIL は、以下の記述である。
「システム管理者は、TOE の動作に必要となる TOE 外の OS や関連ソフトウェア、ハードウェア、管理端末の配付、設置、管理、運用に際して、TOE の正常動作が維持できるように管理する。
また、ファイアウォール管理者は、TOE が正しく動作するように、TOE を設定、監視、メンテナンスし、保守サービス員の作業に立ち会う。」
この前提条件は、OEN.NO_EVIL によって満たされる。根拠を以下に述べる。

OEN.NO_EVIL では、以下を実施する。
- システム管理者は、TOE の動作に必要となる TOE 外の OS や関連ソフトウェア、ハードウェア、管理端末の配付、設置、管理、運用に際して、TOE の正常動作が維持できるように管理しなければならない。
  また、ファイアウォール管理者は、TOE が正しく動作するように、TOE を設定、監視、メンテナンスし、保守サービス員の作業に立ち会わなければならない。

上記により、A.NO_EVIL は、OEN.NO_EVIL により満たされる。

以上により、A.NO_EVIL は、OEN.NO_EVIL により意図する使用法が満たされ、環境が A.NO_EVIL と一貫する。

A.PASSWORD_MANAGEMENT(管理者によるパスワードの管理)
A.PASSWORD_MANAGEMENT は、以下の記述である。
「ファイアウォール管理者は TOE にアクセスするためのファイアウォール管理者 ID とパスワードを、第三者に知られないように管理する。パスワードは推測・解析が容易でないものを設定し、適正な間隔で変更する。
また、システム管理者が TOE 以外の OS や各種サービスにアクセスする際に使用するシステム管理者の ID とパスワードも、TOE のファイアウォール管理者が使用する ID・パスワードと同様の基準で管理する。」
この前提条件は、OEN.PASSWORD_MANAGEMENT によって満たされる。根拠を以下に述べる。

OEN.PASSWORD_MANAGEMENT では、以下を実施する。
- ファイアウォール管理者は TOE にアクセスするためのファイアウォール管理者 ID とパスワードを、第三者に知られないように管理しなければならない。パスワードは推測・解析が容易でないものを設定し、適正な間隔で変更しなければならない。
  また、システム管理者が TOE 以外の OS や各種サービスにアクセスする際に使用するシステム管理者の ID とパスワードも、TOE のファイアウォール管理者が使用する ID・パスワードと同様の基準で管理しなければならない。

上記により、A.PASSWORD_MANAGEMENT は、OEN.PASSWORD_MANAGEMENT により満たされる。

以上により、A.PASSWORD_MANAGEMENT は、OEN.PASSWORD_MANAGEMENT により意図する使用法が満たされ、環境が A.PASSWORD_MANAGEMENT と一貫する。

Copyright © NEC Corporation 2007 All rights reserved.

A.OS（**OS の選択とプラットフォームの要塞化**）
A.OS は、以下の記述である。
「TOE は、TOE のカーネルモジュールに悪影響を与えないことが実証されている、NEC が認めた OS にインストールする。
さらに、TOE が稼働するプラットフォームは、不要なサービスを停止し、不要なソフトウェアをインストールしない。」
この前提条件は、OEN.OS によって満たされる。根拠を以下に述べる。

OEN.OS では、以下を実施する。
- ファイアウォール管理者は TOE を、TOE のカーネルモジュールに悪影響を与えないことが実証されている、NEC が認めた OS にインストールしなくてはならない。
  さらにシステム管理者は、TOE が稼働するプラットフォームは、不要なサービスを停止し、不要なソフトウェアをインストールしてはならない。

上記により、A.OS は、OEN.OS により満たされる。

以上により、A.OS は、OEN.OS により意図する使用法が満たされ、環境が A.OS と一貫する。

A.TRAINING（管理者の訓練）
A.TRAINING は、以下の記述である。
「システム管理者、およびファイアウォール管理者は、TOE および TOE の関連する周辺環境の運用に必要となる教育・訓練を受け、ガイダンスに則って TOE を運用する。」
この前提条件は、OEN.TRAINING によって満たされる。根拠を以下に述べる。

OEN.TRAINING では、以下を実施する。
- システム管理者、およびファイアウォール管理者は、TOE および TOE の関連する周辺環境の運用に必要となる教育・訓練を受け、ガイダンスに則って TOE を運用しなければならない。

上記により、A.TRAINING は、OEN.TRAINING により満たされる。

以上により、A.TRAINING は、OEN.TRAINING により意図する使用法が満たされ、環境が A.TRAINING と一貫する。

A.PASSWORD_INST（インストール時のパスワード設定）
A.PASSWORD_INST は、以下の記述である。
「ファイアウォール管理者は、TOE のインストール時に設定するパスワードをインストールガイダンスに則って設定する。」
この前提条件は、OEN.PASSWORD_INST によって満たされる。根拠を以下に述べる。

OEN.PASSWORD_INST では、以下を実施する。
- ファイアウォール管理者は、TOE のインストール時に設定するパスワードをインストールガイダンスに則って設定しなければならない。

上記により、A.PASSWORD_INST は、OEN.PASSWORD_INST により満たされる。

以上により、A.PASSWORD_INST は、OEN.PASSWORD_INST により意図する使用法が満たされ、環境が A.PASSWORD_INST と一貫する。

Copyright © NEC Corporation 2007 All rights reserved.

A.TRUSTED_PATH（高信頼チャネル）
A.TRUSTED_PATH は、以下の記述である。
「ファイアウォール管理者は、管理端末と Web サーバ間の通信が盗聴されないように、Web サーバに HTTP 通信のための設定を行う。」
この前提条件は、OEN.TRUSTED_PATH によって満たされる。根拠を以下に述べる。

OEN.TRUSTED_PATH では、以下を実施する。
・ ファイアウォール管理者は、管理端末と Web サーバ間の通信が盗聴されないように、Web サーバに HTTP 通信のための設定を行わなければならない。
上記により、A.TRUSTED_PATH は、OEN.TRUSTED_PATH により満たされる。

以上により、A.TRUSTED_PATH は、OEN.TRUSTED_PATH により意図する使用法が満たされ、環境が A.TRUSTED_PATH と一貫する。

A.INJUSTICE_ACCESS_MEASURE（不正アクセス対策の設定）
A.INJUSTICE_ACCESS_MEASURE は、以下の記述である。
「ファイアウォール管理者は、「アドバンス」以外の不正アクセス対策レベルを選択しない。」
この前提条件は、OEN.INJUSTICE_ACCESS_MEASURE によって満たされる。根拠を以下に述べる。

OEN.INJUSTICE_ACCESS_MEASURE では、以下を実施する。
・ ファイアウォール管理者は、「アドバンス」以外の不正アクセス対策レベルを選択してはならない。
上記により、A.INJUSTICE_ACCESS_MEASURE は、OEN.INJUSTICE_ACCESS_MEASURE により満たされる。

以上により、A.INJUSTICE_ACCESS_MEASURE は、OEN.INJUSTICE_ACCESS_MEASURE により意図する使用法が満たされ、環境が A.INJUSTICE_ACCESS_MEASURE と一貫する。

Copyright © NEC Corporation 2007 All rights reserved.

8.2 セキュリティ要件根拠

8.2.1 TOE セキュリティ機能要件根拠

TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 8-2 に示す。
「×」は、対応関係があることを表す。
表 8-2 に示すように、各 TOE セキュリティ機能要件は一つ以上の TOE セキュリティ対策方針に対応している。

表 8-2 TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係

	O.SECURITY_MANAGEMENT	O.ADMIN_ID_AUTH	O.PACKET_FILTER	O.AUDIT	O.ALERT
FAU_ARP.1					×
FAU_GEN.1				×	
FAU_SAA.1					×
FAU_SAR.1				×	
FAU_STG.4				×	
FDP_IFC.1			×		
FDP_IFF.1			×		
FIA_SOS.1		×			
FIA_UAU.2		×			
FIA_UID.2		×			
FMT_MSA.1	×				
FMT_MSA.3	×				
FMT_MTD.1	×				
FMT_SMF.1	×				
FMT_SMR.1	×				
FPT_RVM.1	×	×	×	×	×
FPT_SEP.1	×	×	×	×	×
FPT_STM.1				×	

次に、各 TOE セキュリティ対策方針が TOE セキュリティ機能要件で実現できることを説明する。

O.SECURITY_MANAGEMENT（設定管理）
O.SECURITY_MANAGEMENT では、以下を実施する。
a) TOE は、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定の参照、更新を識別認証されたファイアウォール管理者に制限しなければならない。
O.SECURITY_MANAGEMENT のa）に定める「TOE は、パケットフィルタルール・ファイアウォール管理者情報・ログアラート設定の参照、更新を識別認証されたファイアウォール管理者に制限しなければならない。」は、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。根拠を以下に述べる。

Copyright © NEC Corporation 2007 All rights reserved.

- FMT_MSA.1 によって、パケットフィルタルールにかかわるセキュリティ属性の管理を、ファイアウォール管理者に制限することを保証するからである。
- FMT_MSA.3 によって、TOE 開発時に設定された暗黙のルール及び生成時に設定された不正アクセス対策ルールにより、全体が制限的ルールとなっているパケットフィルタルールに対する管理端末設定ルール及びサイト共通ルールによる指定を、ファイアウォール管理者に限り許可する。
- FMT_SMF.1 によって、TOE は管理機能を特定し、FMT_MTD.1 によって TOE は TSF データに対する操作をファイアウォール管理者に制限することを保証するからである。
- FMT_SMR.1 によって、利用者をファイアウォール管理者に関連づけ、その役割を維持することを保証するからである。
- FPT_RVM.1 によって、設定管理機能を動作させるために、事前にファイアウォール管理者認証機能が呼び出され、識別認証が成功することを保証する。
- FPT_SEP.1 によって、TOE は O.SECURITY_MANAGEMENT のセキュリティドメインを分離・維持し、信頼できないサブジェクトによる干渉と改ざんから保護するからである。

以上により、O.SECURITY_MANAGEMENT は、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。

O.ADMIN_ID_AUTH（識別認証）
O.ADMIN_ID_AUTH では、以下を実施する。
a) TOE は、ID・パスワードを用いて TOE にアクセスする利用者を識別認証し、利用者がファイアウォール管理者であるか否かを判定する。
O.ADMIN_ID_AUTH のa）に定める「TOE は、ID・パスワードを用いて TOE にアクセスする利用者を識別認証し、利用者がファイアウォール管理者であるか否かを判定する。」は、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。根拠を以下に述べる。

- FIA_SOS.1 によって、ファイアウォール管理者がパスワードを変更する際に、新たなパスワードとして入力された文字列が品質尺度にあっていることを TSF が検証する。
- FIA_UAU.2 によって、ファイアウォール管理者認証において、TSF がアクションを許可する前に、ファイアウォール管理者に対して認証が成功することを要求する。
- FIA_UID.2 によって、ファイアウォール管理者識別において、TSF がアクションを許可する前に、ファイアウォール管理者に対して識別が成功することを要求する。
- FPT_RVM.1 によって、TOE のファイアウォール管理を識別認証する前に O.ADMIN_ID_AUTH が必ず呼び出されることを保証する。
- FPT_SEP.1 によって、TOE は O.ADMIN_ID_AUTH のセキュリティドメインを分離・維持し、信頼できないサブジェクトによる干渉と改ざんから保護する。

以上により、O.ADMIN_ID_AUTH は、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。

O.PACKET_FILTER（パケットフィルタ）
O.PACKET_FILTER では、以下を実施する。
a) TOE は、ファイアウォール管理者がポリシにそって設定したパケットフィルタルールに基づいて、IP パケットの入出力を制御する。
O.PACKET_FILTER のa）に定める「TOE は、ファイアウォール管理者がポリシにそって設定したパケッ

Copyright © NEC Corporation 2007 All rights reserved.

トフィルタルールに基づいて、IP パケットの入出力を制御する」は、FDP_IFC.1、FDP_IFF.1、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。根拠を以下に述べる。

- FDP_IFC.1 によって、TOE を介して送受信する IP パケットに対してパケットフィルタルールに基づき、通過・拒否・破棄の情報フロー制御を実施する。
- FDP_IFF.1 によって、TOE を介して送受信する IP パケットに対してセキュリティ属性を条件として、パケットフィルタルールに基づき、通過、あるいは拒否、または破棄する。
- FPT_RVM.1 によって、TOE を介して IP パケットを送受信される際に、パケットフィルタ機能が呼び出されることを保証する。
- FPT_SEP.1 によって、TOE は O.PACKET_FILTER のOSや他のカーネルモジュールや、信頼できないサブジェクトによる干渉と改ざんから保護する。

以上により、O.PACKET_FILTER は、FDP_IFC.1、FDP_IFF.1、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。

O.AUDIT(監査)

O.AUDIT では、以下を実施する。

a) TOE は、TOE に監査対象事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果、事象の内容を記録する。

b) ファイアウォール管理者は、監査記録を参照することによって、異常な動作を検出することが可能である。

c) TOE は、監査記録を出力する領域がファイアウォール管理者により設定されたディスク容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。

O.AUDIT のa)に定める「TOE は、TOE に監査対象事象が発生した場合、監査記録を格納する。監査記録は、事象が生じた日時、事象の種別、事象の結果、事象の内容を記録する。」は、FAU_GEN.1、FPT_RVM.1、FPT_SEP.1、FPT_STM.1 の実現によって達成できる。根拠を以下に述べる。

- FAU_GEN.1 によって、TOE は、サービス運用中に監査対象事象が発生した場合、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、事象の内容を示すメッセージを含む監査記録を生成する。
- FPT_RVM.1 によって、TOE は、監査対象事象の発生時に O.AUDIT が必ず呼び出されることを保障する。
- FPT_SEP.1 によって、TOE は O.AUDIT のセキュリティドメインを分離・維持し、信頼できないサブジェクトによる干渉と改ざんから保護する。
- FPT_STM.1 によって、監査データ記録に必要な高信頼タイムスタンプを提供する。

O.AUDIT のb)に定める「ファイアウォール管理者は、監査記録を参照することによって、異常な動作を検出することが可能である。」は、FAU_SAR.1 の実現によって達成できる。根拠を以下に述べる。

- FAU_SAR.1 によって、TOE は、ファイアウォール管理者が監査記録を読み出せるようにする。

O.AUDIT のc)に定める「TOE は、監査記録を出力する領域がファイアウォール管理者により設定されたディスク容量に達した場合には、最も古くに格納された監査記録への上書きを行うことによって、ディスク容量分の監査記録を維持することを保証する。」は、FAU_STG.4 の実現によって達成できる。根拠を以下に述べる。

- FAU_STG.4 によって、TOEは、ファイアウォール管理者が定めるディスク容量に達した場合、最も古くに格納された監査記録への上書きを行う。

Copyright © NEC Corporation 2007 All rights reserved.

以上により、O.AUDIT は、FAU_GEN.1、FAU_SAR.1、FAU_STG.4、FPT_RVM.1、FPT_SEP.1、FPT_STM.1 の実現によって達成できる。

O.ALERT(アラート通知)
O.ALERT では、以下を実施する。
a) TOE は、TOE に対するセキュリティ侵害の可能性を検知した場合、ログアラート設定(アラートアクション設定)に基づき、ファイアウォール管理者へのアラートの通知を実行する。
O.ALERT のa)に定める「TOE は、TOE に対するセキュリティ侵害の可能性を検知した場合、ログアラート設定(アラートアクション設定)に基づき、ファイアウォール管理者へのアラートの通知を実行する。」は、FAU_ARP.1、FAU_SAA.1、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。根拠を以下に述べる。

- FAU_ARP.1、TOE へのセキュリティ侵害の可能性が検出された場合、ファイアウォール管理者が設定するログアラート設定(アラートアクション設定)に基づき、ファイアウォール管理者へアラートを通知する。
- FAU_SAA.1 によって、セキュリティ侵害の可能性を判断する規則を適用し、それを検出する。
- FPT_RVM.1 によって、TOE は、TOE に対するセキュリティ侵害の可能性の検知と、検知した場合に、ログアラート設定(アラートアクション設定)に基づいてファイウォール管理者へアラート通知を行うことを保証する。
- FPT_SEP.1 によって、TOE は O.ALERT のセキュリティドメインを分離・維持し、信頼できないサブジェクトによる干渉と改ざんから保護する。

以上により、O.ALERT は、FAU_ARP.1、FAU_SAA.1、FPT_RVM.1、FPT_SEP.1 の実現によって達成できる。

8.2.2 IT 環境セキュリティ機能要件根拠
本 ST は、IT 環境セキュリティ機能要件を記述しないため根拠は記述しない。

8.2.3 最小機能強度レベル根拠
TOE が想定する攻撃者は、3 章で述べたように「高度な専門知識を持たない」つまり低レベルの脅威エージェントを想定している。したがって、最小機能強度レベルは、SOF-基本が妥当であるといえる。本 ST は、TOE に対し最小機能強度レベルとして SOF-基本を求めており、一貫している。明示された機能強度が指定された機能要件は、FIA_SOS.1 である。

8.2.4 セキュリティ機能要件依存性
本節では、セキュリティ機能要件全体が相互に補完し、内部的に一貫している根拠として、セキュリティ機能要件が依存性を満足していることを説明する。
このため、セキュリティ機能要件には直接的および間接的に依存するセキュリティ機能要件が存在することを踏まえ、これらの依存性のすべてが満たされていることと、満たされていない依存性についてはその正当性の根拠を示す。
表 8-3 ではセキュリティ要件のコンポーネントの CC パート2における依存コンポーネントと TOE における依存コンポーネントを示すことにより、セキュリティ要件のコンポーネントの依存性が満たされている範囲を明確にする。さらに、満たされていない依存性についてはそれが正当である根拠を別途示す。以上により、全体として依存性が満たされていることを示す。

Copyright © NEC Corporation 2007 All rights reserved.

表 8-3 セキュリティ要件のコンポーネントの依存性

コンポーネント	CC パート 2 における 依存コンポーネント	TOE における 依存コンポーネント	依存性が満たされない コンポーネント	根拠
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1	なし	
FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし	
FAU_SAA.1	FAU_GEN.1	FAU_GEN.1	なし	
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし	
FAU_STG.4	FAU_STG.1	なし	FAU_STG.1	※1
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	なし	
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1	なし	
	FMT_MSA.3	FMT_MSA.3	なし	
FIA_SOS.1	なし	なし	なし	
FIA_UAU.2	FIA_UID.1	FIA_UID.2	なし	※2
FID_UID.2	なし	なし	なし	
FMT_MSA.1	FDP_ACC.1 または FDP_IFC.1	FDP_IFC.1	なし	
	FMT_SMF.1	FMT_SMF.1	なし	
	FMT_SMR.1	FMT_SMR.1	なし	
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	なし	
	FMT_SMR.1	FMT_SMR.1	なし	
FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	なし	
	FMT_SMR.1	FMT_SMR.1	なし	
FMT_SMF.1	なし	なし	なし	
FMT_SMR.1	FIA_UID.1	FIA_UID.2	なし	※2
FPT_RVM.1	なし	なし	なし	
FPT_SEP.1	なし	なし	なし	
FPT_STM.1	なし	なし	なし	

※1：FAU_STG.1 に該当する監査記録の不正削除の脅威は、OEN.SAFE_PLACE により物理的な不正アクセス保護と、FIA_UAU.2 および FIA_UID.2 の論理的な不正アクセス保護により防止できる。よって、依存関係にある FAU_STG.1 は不要である。

※2：FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである。

8.2.5 セキュリティ機能要件相互補完性

8.2.4 節より、TOE セキュリティ機能要件は、一部の例外を除き、それぞれと依存関係のある機能要件と相互補完している。これらの機能要件以外で明示的な依存関係はないが、バイパス防止、改ざん防止、非活性化防止、無効化検出のために相互補完している。以下にそれぞれの観点で相互補完する機能要件について記述する。

表 8-4 に、各セキュリティ機能要件に対し、バイパス防止、干渉阻止、非活性化防止、無効化検出の観点で相互補完が必要な機能要件を示す。
「×」は相互補完が必要な機能要件があることを表す。

Copyright © NEC Corporation 2007 All rights reserved.

表 8-4 セキュリティ要件のコンポーネントの相互補完性

コンポーネント	バイパス防止	干渉阻止	非活性化防止	無効化検出
FAU_ARP.1	×	×		×
FAU_GEN.1	×	×		×
FAU_SAA.1	×	×		×
FAU_SAR.1	×	×		×
FAU_STG.4	×	×		
FDP_IFC.1	×	×		
FDP_IFF.1	×	×		
FIA_SOS.1	×	×		
FIA_UAU.2	×	×		
FID_UID.2	×	×		
FMT_MSA.1	×	×		
FMT_MSA.3	×	×		
FMT_MTD.1	×	×	×	×
FMT_SMF.1	×	×		
FMT_SMR.1	×	×		
FPT_RVM.1	×	×		
FPT_SEP.1	×	×		
FPT_STM.1	×	×		×

＜バイパス防止＞

表 8-4 に示すすべてのセキュリティ機能要件は、自らがバイパスされることにより、セキュリティ機能が正常に動作しないため、自らがバイパスされることを防止しなければならない。すべての機能要件について、FPT_RVM.1 により、各セキュリティ機能が適切なタイミングで呼び出され成功することが保証される。
バイパス防止を考慮する必要がないセキュリティ機能要件は、本 ST では存在しない。

＜干渉阻止＞

表 8-4 に示すすべてのセキュリティ機能要件は、自らが改ざんされることにより、セキュリティ機能が正常に動作しないため、自らが改ざんされることを防止しなければならない。
すべての機能要件について、FPT_SEP.1 により、信頼できないサブジェクトから干渉と改ざんから自らを保護するためにセキュリティドメインを維持し、各セキュリティドメイン間の分離を実施することが保証される。
但し、パケットフィルタ機能は OEN.OS によって、TOE のカーネルモジュールに悪影響を与えないことが実証されている OS に TOE がインストールされることにより、信頼できないサブジェクトによる干渉と改ざんから保護される。

＜非活性化防止＞

FMT_MTD.1 により、ログアラート機能のアラート通知機能の非活性化行為を、ファイアウォール管理者に制限することを保障する。
また、ログアラート設定（アラートアクション設定）に基づく、ファイアウォール管理者へのアラート通知機能を非活性化することはできるが、ファイアウォール管理者は、監査記録を参照することにより、セキュリティ侵害を受けたことを検出することができる。したがって、アラート通知の非活性化に伴うセキュリティ侵害の見過ごしによる被害は発生しない。

Copyright © NEC Corporation 2007 All rights reserved.

＜無効化検出＞
FAU_ARP.1、FAU_GEN.1、FAU_SAA.1、FAU_SAR.1、FMT_MTD.1、FPT_STM.1 によってセキュリティ機能の無効化を目的とした攻撃の検出が可能となる。
TOE における監査機能の目的は、下記の 4 点である。

- TOE への不正ログイン
- 外部に公開されているサーバに対しての悪意を持ったパケットの検出
- なりすましによる TSF の不正改ざん
- セキュリティ機能の無効化検出

FAU_GEN.1 では、下記の監査事象の監査記録を生成する。

- 監査機能の起動と終了
- ファイアウォール管理者へのアラートの通知
- TSP 侵害の可能性の検出
- 監査記録の参照
- 対象となる IP パケットに対する処理結果、およびその判定に使用したセキュリティ属性
- ファイアウォール管理者パスワード検証の成功／失敗
- ファイアウォール管理者の識別認証の成功／失敗
- パケットフィルタルール（サイト共通ルール）の編集のための一時ファイルからの一括変更の成功
- ファイアウォール管理者パスワード改変の成功
- ファイアウォール管理者 ID 改変の成功
- ログアラート設定（監査証跡不ファイル設定）改変の成功
- ログアラート設定（アラートアクション設定）改変、削除、追加の成功
- ログアラート設定(アラートアクション設定)の変更
- 設定管理機能の起動

監査記録は、以下の項目で構成される。

- 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
- 表 5-1 に示すその他の監査関連情報

ログアラート機能の開始は OS の起動時であり、ログアラート機能の終了は OS の終了時である。但し、ログアラート情報の変更時は、再起動し変更情報を反映する。
FAU_SAR.1 により、ファイアウォール管理者が監査証跡を参照することで以下の不正行為を知ることできる。

- ファイアウォール管理者の識別認証の成功／失敗を参照することで、いつ手当たり次第 ID とパスワードを試して TOE へのログインを試みたのかを知ることできる。
- 監査記録の FAU_SAA.1 による分析結果を参照することで、いつ外部に公開されているサーバに対して悪意を持ったパケットの検出をしたのかを知ることできる。
  FAU_SAA.1 による分析結果をもとに、FAU_ARP.1 による、ログアラート設定（アラートアクション設定）に基づく、ファイアウォール管理者へのアラートの通知で知ることもできる。
- 離席の時間と監査記録の事象の日付・時刻をつき合わせることで、離席時に TSF データが改ざんされたかを知ることできる。

Copyright © NEC Corporation 2007 All rights reserved.

・ 監査記録の対象となるIPパケットに対する処理結果、およびその判定に使用したセキュリティ属性を見ることで、セキュリティ機能の無効化を試みる予兆を知ることができる。

したがって、上記の監査目的を達成できる。

また、FMT_MTD.1により、アラート通知機能を無効化する能力は、識別認証されたファイアウォール権利者に制限され、信頼できないサブジェクトによるアラート通知機能の無効化を防止している。アラート通知機能は、ログ格納機能を補強するものであり、仮にアラート通知機能が無効化されても監査の目的を達成できる。

8.2.6 セキュリティ機能要件内部一貫性

以下に、各機能要件が内部的に一貫しており、矛盾していない根拠を示す。

＜監査関連＞

FAU_ARP.1、FAU_GEN.1、FAU_SAA.1、FAU_SAR.1、FAU_STG.4、は監査機能に閉じたものであり、FMT_MTD.1、FPT_STM.1、FPT_RVM.1、FPT_SEP.1 以外の機能要件とは関連しない。

FAU_ARP.1 は、TSF がセキュリティ侵害の可能性を検出した場合、ログアラート設定（アラートアクション設定）に基づく、ファイアウォール管理者へのアラートを通知するものであり、他の機能要件との競合や矛盾はない。

FAU_GEN.1 は、取得する監査対象事象のレベルと、取得する監査対象事象のリストを定義するものであり、他の機能要件との競合や矛盾はない。

FAU_SAA.1 は、監査証跡をモニタするための規則により、セキュリティ侵害の可能性を検出する。このために必要となる情報は、FAU_GEN.1 で監査証跡に含まれる。以上より、FAU_GEN.1 は、FAU_SAA.1 の要求事項を満たすことが可能であり、これらの間に矛盾はない。

FAU_SAR.1 で監査証跡から監査情報(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、その他の監査関連情報）を読み出せることを要求している。このために必要となる情報は、FAU_GEN.1 で監査証跡として取得している情報(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、その他の監査関連情報）である。以上より、FAU_GEN.1 は、FAU_SAR.1 の要求事項を満たすことが可能であり、これらの間に矛盾はない。

FAU_STG.4 は、監査証跡がファイアウォール管理者の定めるディスク容量分を超えた場合、最も古くに格納された監査記録への上書きを行うものであり、他の機能要件との競合や矛盾はない。

FMT_MTD.1 は、TSF データであるログアラート設定（監査証跡ファイル設定）の問い合わせ、改変、及びログアラート設定（アラートアクション設定）の問い合わせ、改変、削除、追加の権限をファイアウォール管理者に限定すること要求する機能要件で、FAU_ARP.1、FAU_STG.4 の機能を補完するものであり、矛盾はない。

FPT_STM.1 は、FAU_GEN.1 を補完するものであり、矛盾はない。

FPT_RVM.1 は、監査記録の生成がバイパスされないための機能要件であり、矛盾はない。

FPT_SEP.1 は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜情報フロー制御関連＞

FDP_IFC.1、FDP_IFF.1、FMT_MSA.1、FMT_MSA.3 は情報フロー制御に関連する機能要件であり、FPT_RVM.1、FPT_SEP.1 以外の機能要件とは関連しない。

FDP_IFC.1 と FDP_IFF.1 において、サブジェクト、情報、SFP の名称を使用しているが、これらは一致しており矛盾はない。さらに、情報フロー制御の規則は一つであり、他の機能要件との競合や矛盾もない。

FMT_MSA.1 は、パケットフィルタルールの問い合わせ、改変、削除、追加、インポート／エクスポート、

Copyright © NEC Corporation 2007 All rights reserved.

バックアップ／リストアを行える権限をファイアウォール管理者に限定すること要求する機能要件で、FDP_IFC.1、FDP_IFF.1 の機能を補完するものでり、矛盾はない。
FMT_MSA.3 は、制限的パケットフィルタルールに対する管理端末設定ルール及びサイト共通ルールによる指定をファイアウォール管理者に限定すること要求する機能要件で、FDP_IFC.1、FDP_IFF.1 の機能を補完するものであり、矛盾はない。
FPT_RVM.1 は、情報フロー制御がバイパスされないための機能要件であり、矛盾はない。
FPT_SEP.1 は、TOE をカーネルモジュールに悪影響を与えない OS にインストールすることでセキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜識別認証関連＞
FIA_SOS.1、FIA_UAU.2、FIA_UID.2 は識別認証に関わるものであり、FMT_MTD.1、FPT_RVM.1、FPT_SEP.1 以外の機能要件とは関連しない。
FIA_SOS.1 は、秘密が表 5-2 に示す品質尺度に合致することを検証するメカニズムを提供するものであり、他の機能要件との競合や矛盾はない。
FIA_UAU.2 は、利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求するものであり、他の機能要件との競合や矛盾はない。
FIA_UID.2 は、利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に識別が成功することを要求するものであり、他の機能要件との競合や矛盾はない。
FMT_MTD.1 は、ファイアウォール管理者 ID 及びパスワードの変更を識別認証されたファイアウォール管理者に限定する機能要件である。また、パスワードを変更しても FIA_UAU.2、FIA_UID.2 の機能に影響はない。
以上より FMT_MTD.1 は、FIA_UAU.2、FIA_UID.2 を補完するものであり、矛盾はない。
FPT_RVM.1 は、識別認証がバイパスされないための機能要件であり、矛盾はない。
FPT_SEP.1 は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜セキュリティ管理関連＞
FMT_MTD.1、FMT_MSA.1、FMT_MSA.3、FMT_SMF.1、FMT_SMR.1 は、セキュリティ管理に関わるものであり、FIA_UID.2、FPT_RVM.1、FPT_SEP.1 以外の機能要件とは関連しない。
FMT_MTD.1 は、TSF データの管理を規定するものであり、定義された操作と対応する許可された役割は他の機能要件との競合や矛盾はない。
FMT_MSA.1 は、パケットフィルタルールに使用されるセキュリティ属性に対し、問い合わせ・改変・削除・追加・インポート／エクスポート、バックアップ／リストアする能力をファイアウォール管理者に制限するために情報フロー制御 SFP を実施することを要求するものであり、他の機能要件との競合や矛盾はない。
FMT_MSA.3 は、SFP を実施するために使われるセキュリティ属性として、制限的デフォルト値を与える情報フロー制御 SFP 実施するものであり、他の機能要件との競合や矛盾はない。
FMT_SMF.1 は、セキュリティ管理機能を特定するものであり、定義された TOE における管理項目は他の機能要件との競合や矛盾はない。
FMT_SMR.1 は、利用者をファイアウォール管理者に関連づけるものであり、他の機能要件との競合や矛盾はない。
FIA_UID.2 は、FMT_SMR.1 を補完するものであり、矛盾はない。
FPT_RVM.1 は、セキュリティ管理がバイパスされないための機能要件であり、矛盾はない。
FPT_SEP.1 は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜TSF 保護関連＞
FPT_RVM.1、FPT_SEP.1 は、TSF の保護に関わるものであり、他の機能要件との関係において競合

Copyright © NEC Corporation 2007 All rights reserved.

や矛盾はない。
FPT_RVM.1、FPT_SEP.1 は、各々独立した機能であり、競合や矛盾は生じない。

8.2.7 セキュリティ保証要件根拠

NEC ファイアウォール SG は、セキュリティ対策の重要なポジションを担う製品であるので、セキュリティ機能には高い信頼性が要求される。しかし、NEC ファイアウォール SG は物理的に不正侵入できないように保護された環境に設置され、さらに TOE の設定はファイアウォール管理者のみに限定されるため、攻撃レベルは“低”を想定している。
また、特定の組織からの評価保証レベルに対する要求はなく、外部の使用条件により評価保証レベルを定められることはない。それらを考慮すると、EAL1 は妥当な選択であるといえる。

8.3 TOE 要約仕様根拠

8.3.1 TOE セキュリティ機能根拠

表 6-1 で示したように、各 TOE セキュリティ機能が1つ以上のセキュリティ機能要件に対応している。次に、各セキュリティ機能要件が、TOE セキュリティ機能により実現できることを説明する。
なお、FPT_RVM.1 および FPT_SEP.1 は、すべてのセキュリティ機能によって実現される。
この例外を省き、各セキュリティ機能は独立しており、セキュリティ機能の組み合わせによって一つのセキュリティ機能要件を満たすものはない。

FAU_ARP.1 セキュリティアラーム

FAU_ARP.1 は、TSF に対して、セキュリティ侵害の可能性が検出された場合、以下のアクションを実行し、ファイアウォール管理者に対して TOE に対するセキュリティ侵害の可能性を通知することを要求する。

- ログアラート設定(アラートアクション設定)に基づく、ファイアウォール管理者へのアラートの通知

SF.AUDIT は、TOE に対するセキュリティ侵害の可能性を検出した場合、以下のアクションを実行し、ファイアウォール管理者に対して TOE に対するセキュリティ侵害の可能性があったことを通知する。

- ログアラート設定(アラートアクション設定)に基づく、ファイアウォール管理者へのアラートの通知

したがって、SF.AUDIT の実装によって FAU_ARP.1 を実現できる。

FAU_GEN.1 監査データ生成

FAU_GEN.1 は、TSF に対して、TOE が取得する監査対象事象として以下の事象を取得することを要求する。

- 監査機能の起動と終了
- 表 5-1 に示す監査対象事象

また、各監査記録において少なくとも、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)およびその他の監査関連情報を記録することを要求する。
SF.AUDIT は、以下の監査対象事象の監査記録を生成する。

- 監査機能の起動と終了(TOE の起動と終了として監査記録を生成する)
- 表 5-1 に示す監査対象事象

上記 FAU_GEN.1 に定める監査対象事象は、すべて SF.AUDIT において監査記録として生成される。

表 5-1 は、各機能要件を選択した場合に監査対象とすべきアクション(CC における規定)と、それに関連する監査対象事象とを示す。

Copyright © NEC Corporation 2007 All rights reserved.

FAU_GEN.1 に定める監査対象事象は、すべて SF.AUDIT において監査記録として生成される。
また、SF.AUDIT で生成する監査記録には少なくとも以下の情報が記録される。

- 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
- 表 5-1 に示すその他の監査関連情報

これらは、FAU GEN.1 に各監査記録に少なくとも記録すべきとした情報と一致する。
したがって、SF.AUDIT の実装により FAU_GEN.1 を実現できる。

FAU_SAA.1 侵害の可能性の分析

FAU_SAA.1 は、TSF に対して、監査事象のモニタに以下の規則を実施し、これらの規則に基づき TSP 侵害の可能性を示すことを要求する。

- 単位時間内に、同一の送信元 IP アドレスからの IP パケットを指定回数分破棄した。
- 単位時間内に、同一の送信先 IP アドレスへの IP パケットを指定回数分破棄した。
- 不正な送信元 IP アドレスを持つ IP パケットを検出した。

SF.AUDIT は、監査事象のモニタに以下の規則を実施し、TSP 侵害の可能性を示す。

- 単位時間内に、同一の送信元 IP アドレスからの IP パケットを指定回数分破棄した。
- 単位時間内に、同一の送信先 IP アドレスへの IP パケットを指定回数分破棄した。
- 不正な送信元 IP アドレスを持つ IP パケットを検出した。

したがって、SF.AUDIT の実装により FAU_SAA.1 は実現できる。

FAU_SAR.1 監査レビュー

FAU_SAR.1 は、TSF に対して、ファイアウォール管理者が以下の項目を解釈に適した形式で、監査記録を読み出せるようにすることを要求する。

- 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
- 表 5-1 に示すその他の監査関連情報

SF.AUDIT は、監査記録を取得し、ファイアウォール管理者が以下の項目を解釈に適した形式で、監査記録から参照できるようにしている。

- 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
- 表 5-1 に示すその他の監査関連情報

したがって、SF.AUDIT の実装により FAU_SAR.1 は実現できる。

FAU_STG.4 監査データ損失の防止

FAU_STG.4 は、TSF に対して、監査証跡がファイアウォール管理者の定めるディスク容量分を超えた場合、以下のアクションをとることを要求する。

- 最も古くに格納された監査記録への上書きを行う。

SF.AUDIT は、監査証跡が、ファイアウォール管理者が定めるディスク容量分を超えた場合、以下のアク

Copyright © NEC Corporation 2007 All rights reserved.

ションを行う。

- 最も古くに格納された監査記録への上書きを行う。

FAU_STG.4 は、TSF に対して、監査格納失敗時に以下のアクションをとることを要求する。

- ハードディスクに障害が発生した場合は、TOE が停止する。

SF.AUDIT は、監査格納失敗時に以下のアクションを行う。

- ハードディスクに障害が発生した場合は、TOE が停止する。

したがって、SF.AUDIT の実装により、FAU_STG.4 を実現できる。

FDP_IFC.1 サブセット情報フロー制御

FDP_IFC.1 は、TSF に対して TOE を介して送受信される IP パケットの流れを引き起こす以下の操作のリストに対して、情報フロー制御を実施することを要求する。

- 通過。
- 拒否(送信元へエラーを通知するとともに破棄)。
- 破棄(送信元へエラーを返さずに破棄)。

SF.PF は、TOE を介して送受信される IP パケットに対して、パケットフィルタルールに基づいて、以下の操作を行う情報フロー制御を実施する。

- 通過。
- 拒否(送信元へエラーを通知するとともに破棄)。
- 破棄(送信元へエラーを返さずに破棄)。

したがって、SF.PF の実装により FDP_IFC.1 は実現できる。

FDP_IFF.1 単純セキュリティ属性

FDP_IFF.1 は、TSF に対して、以下のネットワークインタフェースのセキュリティ属性および以下の情報(IP パケット)のセキュリティ属性の種別に基づいて、パケットフィルタ方針にしたがって、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することを要求する。

ネットワークインタフェースのセキュリティ属性

- 受信ネットワークインタフェース
- 送信ネットワークインタフェース

IP パケットのセキュリティ属性

- 送信元 IP アドレス(ホスト、またはネットワーク)
- 送信先 IP アドレス(ホスト、またはネットワーク)
- プロトコル種別(TCP、UDP、ICMP)
- 送信元ポート番号(TCP、UDP の場合)
- 送信先ポート番号(TCP、UDP の場合)

SF.PF は、送受信される IP パケットから取得したセキュリティ属性とネットワークインタフェースのセキュリティ属性に基づいて、パケットフィルタ方針に従って評価し、通過・拒否・破棄の処理を行う。

SF.PF は、以下のおよび以下の情報(IP パケット)のセキュリティ属性の種別に基づいて、パケットフィルタ方針にしたがって、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する。

ネットワークインタフェースのセキュリティ属性

- 受信ネットワークインタフェース
- 送信ネットワークインタフェース

IP パケットのセキュリティ属性

- 送信元 IP アドレス(ホスト、またはネットワーク)
- 送信先 IP アドレス(ホスト、またはネットワーク)
- プロトコル種別(TCP、UDP、ICMP)

Copyright © NEC Corporation 2007 All rights reserved.

- 送信元ポート番号(TCP、UDP の場合)
- 送信先ポート番号(TCP、UDP の場合)

したがって、SF.PF の実装により FDP_IFF.1 は実現できる。

FIA_SOS.1 秘密の検証

FIA_SOS.1 は、TSF に対して、秘密が表 5-2 の品質尺度に合致することを検証するメカニズムを提供することを要求する。

SF.I&A は、ファイアウォール管理者 ID とパスワードの変更時において、新たなパスワードの候補として入力された文字列が表 5-2 の規則を満たさない場合には、入力されたパスワードの受入れを拒否する。

したがって、SF.I&A の実装により FIA_SOS.1 は実現できる。

FIA_UAU.2 アクション前の利用者認証

FIA_UAU.2 は、TSF に対して、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する。

SF.I&A は、TOE へアクセスする利用者(ファイアウォール管理者)に対して、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する。

したがって、SF.I&A の実装により FIA_UAU.2 は実現できる。

FIA_UID.2 アクション前の利用者識別

FIA_UID.2 は、TSF に対して、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求する。

SF.I&A は、TOE へアクセスする利用者(ファイアウォール管理者)に対して、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求する。

したがって、SF.I&A の実装により FIA_UID2 は実現できる。

FMT_MSA.1 セキュリティ属性の管理

FMT_MSA.1 は、TSF に対して、以下のセキュリティ属性に対して、パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストアする能力をファイアウォール管理者に制限するために情報フロー制御 SFP を実施することを要求する。

- 受信ネットワークインタフェース
- 送信ネットワークインタフェース
- 送信元 IP アドレス(ホスト、またはネットワーク)。
- 送信先 IP アドレス(ホスト、またはネットワーク)。
- プロトコル種別(TCP、UDP、ICMP)。
- 送信元ポート番号(TCP、UDP の場合)。
- 送信先ポート番号(TCP、UDP の場合)。

SF.MNG は、パケットフィルタルールが対応する以下のセキュリティ属性に対して、パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストアする操作をファイアウォール管理者に限り許可する。

- 受信ネットワークインタフェース
- 送信ネットワークインタフェース
- 送信元 IP アドレス(ホスト、またはネットワーク)。
- 送信先 IP アドレス(ホスト、またはネットワーク)。

Copyright © NEC Corporation 2007 All rights reserved.

- プロトコル種別(TCP、UDP、ICMP)。
- 送信元ポート番号(TCP、UDP の場合)。
- 送信先ポート番号(TCP、UDP の場合)。

したがって、SF.MNG の実装により FMT_MSA.1 を実現できる。

FMT_MSA.3 静的属性初期化

FMT_MSA.3 は、TSF に対して、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、制限的デフォルト値を与える情報フロー制御 SFP を実施することを要求する。

SF.MNG は TOE 開発時に設定された暗黙のルール及び生成時に設定された不正アクセス対策ルールにより、全体が制限的ルールとなっているパケットフィルタルールに対する管理端末接続ルール及びサイト共通ルールによる指定を、ファイアウォール管理者に限り許可する。

したがって SF.MNG の実装により FMT_MSA.3 を実現できる。

FMT_MTD.1 TSF データの管理

FMT_MTD.1 は、TSF に対して、表 5-3 に示す TSF データのリストおよび操作をファイアウォール管理者に制限することを要求する。

SF.MNG は、表 5-3 に示す TSF データのリストおよび操作を、ファイアウォール管理者のみに制限する。

したがって SF.MNG の実装により FMT_MTD.1 を実現できる。

FMT_SMF.1 管理機能の特定

FMT_SMF.1 は、TSF に対して以下のセキュリティ管理機能を行う能力を持つことを要求する。

- ファイアウォール管理者 ID の改変
- ファイアウォール管理者のパスワードの改変
- ログアラート設定(監査証跡ファイル設定)の問い合わせ、改変
- ログアラート設定(アラートアクション設定)の問い合わせ、改変、削除、追加
- パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストア

SF.MNG は、以下のセキュリティ管理機能を提供する。

- ファイアウォール管理者 ID の改変
- ファイアウォール管理者のパスワードの改変
- ログアラート設定(監査証跡ファイル設定)の問い合わせ、改変
- ログアラート設定(アラートアクション設定)の問い合わせ、改変、削除、追加
- パケットフィルタルール(管理端末接続ルール、サイト共通ルール)の問い合わせ、改変、削除、追加、インポート/エクスポート、バックアップ/リストア

したがって、SF.MNG の実装により FMT_SMF.1 を実現できる。

FMT_SMR.1 セキュリティ役割

FMT_SMR.1 は、TSF に対して、利用者を以下の許可された識別された役割に関連づけ維持することを要求する。

- ファイアウォール管理者。

SF.MNG は、ファイアウォール管理者という役割を維持するとともに、利用者をファイアウォール管理者という役割に関連付ける。

したがって、SF.MNG の実装により FMT_SMR.1 を実現できる。

Copyright © NEC Corporation 2007 All rights reserved.

FPT_RVM.1 TSP の非バイパス性

FPT_RVM.1 は、TSF に対して、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することを要求する。

SF.MNG により、TOE は、SF.I&A（管理者認証機能）による識別認証に成功した場合に限り、その利用者を代行して動作する SF.MNG（設定管理機能）の動作が許可されることを保証する。

SF.I&A により、TOE は、SF.MNG（設定管理機能）の動作を許可する前に、SF.I&A（管理者認証機能）を呼び出し、ファイアウォール管理者 ID とパスワードによる識別認証が成功した場合に限って、業務の実行を許可することを保証する。

SF.PF により、TOE は、TOE を介して IP パケットが送受信される際に、受信した IP パケットを指定された送信先に送信する前に、SF.PF（パケットフィルタ機能）を呼び出すことにより、SF.PF（パケットフィルタ機能）が成功することを保証する。

SF.AUDIT により、各機能からの監査対象事象の記録依頼の仕組みは開発時に組み込まれている。TOE は、監査対象事象の記録依頼の仕組みを除去したり停止したりする機能を持たない。このため、必要なすべての監査対象事象の記録依頼に対し、監査記録が生成され、格納されることが保証される。

したがって、SF.MNG、SF.I&A、SF.PF、 SF.AUDIT の実装により FPT_RVM.1 を実現できる。

FPT_SEP.1 TSF ドメイン分離

FPT_SEP.1 は TSF に対して、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や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、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する事を要求する。

SF.MNG、SF.I&A、SF.AUDIT は、他の構成要素とは別の独立したプロセスとして実行されるため、セキュリティドメインとして他のドメインと分離される。

また SF.PF は、OEN.OS によりカーネルモジュールに悪影響を与えない OS にインストールすることで保護され、セキュリティドメインとして他のドメインと分離される。

したがって、SF.MNG、SF.I&A、SF.PF、SF.AUDIT の実装により FPT_SEP.1 を実現できる。

FPT_STM.1 高信頼タイムスタンプ

FPT_STM.1 は、TSF に対してそれ自身の使用のために、高信頼タイムスタンプを提供することを要求する。

SF.AUDIT は、監査記録に付与される事象の日付・時刻として、OS から取得した日付・時刻を付与する。

したがって、SF.AUDIT の実装により FPT_STM.1 を実現できる。

8.3.2 セキュリティ機能強度根拠

この TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、SF.I&A である。セキュリティ機能強度は、6.2 節において、SOF-基本を指定している。一方、この TOE の最小機能強度レベルは、5.1.2 節において SOF-基本を指定している。したがって、両者は一貫している。

8.3.3 セキュリティ保証手段根拠

表 6-2 で示したように、EAL1 で必要とするすべての TOE セキュリティ保証要件に対して、保証手段を対応付けている。また、保証手段によって、本 ST で規定した TOE セキュリティ保証要件が要求する証拠を網羅している。したがって、EAL1 における TOE セキュリティ保証要件が要求している証拠に合致している。

Copyright © NEC Corporation 2007 All rights reserved.

8.4 PP 主張根拠

本 ST は, PP 準拠を主張しない。

Copyright © NEC Corporation 2007 All rights reserved.

更新履歴

バージョン	作成・更新日	更新概要	更新箇所
第 1.0 版	2006/12/15	初版	
第 1.1 版	2006/12/20	内部レビュー指摘事項反映	全般
第 1.2 版	2007/01/19	6章、7章追加	6,7
第 1.3 版	2007/01/26	内部レビュー指摘事項反映	全般
第 1.4 版	2007/02/02	6章、7章不備事項追加	6,7
第 1.5 版	2007/02/06	8章追加	8
第 1.6 版	2007/02/07	内部レビュー指摘事項反映	全般
第 1.7 版	2007/02/23	8章不備事項追加	8
第 1.8 版	2007/02/28	内部レビュー指摘事項反映	全般
第 1.9 版	2007/04/09	監査ログ関連修正	5,6,7,8
第 1.10 版	2007/04/23	内部レビュー指摘事項反映	5,6,7,8
第 1.11 版	2007/06/01	ハードウェア情報修正	2.4
第 1.12 版	2007/07/27	所見報告書(PXO-EOR-0001-00)に基づき修正 [ASE_DES.1-3] －TOE の論理範囲および境界の明確化 [ASE_DES.1-4] －用語説明の追加と TOE との関係の明確化	全般
第 1.13 版	2007/08/28	問題点修正 －参考資料の修正 －TOE の論理範囲の各機能の説明を修正 サブユニットに関する記述の削除 －誤記の修正	全般
第 1.14 版	2007/09/14	問題点修正 －6 章の修正 －8 章修正 －6, 8章に関連する項目修正	全般
第 1.15 版	2007/09/28	問題点修正 －5.1.1 節の冒頭の修正 －5.1.1 節 FAU_GEN1.1 の修正 －6.1 節の冒頭の修正 －8.2.4 節 FPT_AMT.1 への依存が満たされない根拠の修正 －8.2.5 節セキュリティ機能相互補完性の修正 －8.2.6 節 セキュリティ機能要件内部一貫性の修正 －5, 8 章の誤記修正	5,6,8
第 1.16 版	2007/09/28	1.15 版に関する問題点修正 －5.1.1 節の冒頭の修正 －5.1.1 節 FAU_GEN1.1 の修正 －8.2.4 節 FPT_AMT.1 への依存が満たされない根拠の修正 －8.2.6 節 セキュリティ機能要件内部一貫性の修正	5,8

Copyright © NEC Corporation 2007 All rights reserved.

バージョン	作成・更新日	更新概要	更新箇所
第 1.17 版	2007/10/10	1.16 版に関する問題点修正 －2 章全般の見直し －3 章全般の見直し －4 章全般の見直し －5 章機能要件の見直し －6 章全般の見直し	2,3,4,5,6
第 1.18 版	2007/10/18	1.17 版に関する問題点修正 －2 章全般の表現変更 －3 章全般の表現変更 －4 章全般の表現変更 －5 章機能要件の見直し －5 章見直しに対しての 6 章の対応	2,3,4,5,6
第 1.19 版	2007/10/25	1.18 版に関する問題点修正 －2 章全般の表現変更 －3 章全般の表現変更 －4 章全般の表現変更 －5 章機能要件の見直し －5 章見直しに対しての 6 章の対応	2,3,4,5,6
第 1.20 版	2007/10/30	1.19 版に関する問題点修正 －2 章全般の表現変更 －3 章全般の表現変更 －4 章全般の表現変更 －5 章機能要件の見直し －5 章見直しに対しての 6 章の対応 －8 章全般の表現変更	2,3,4,5,6,8
第 1.21 版	2007/11/5	1.20 版に関する問題点修正 －2 章の表現変更（パケットフィルタ機能、ログアラート機能） －5 章機能要件の見直し －5 章見直しに対しての 6 章の対応 －8 章全般の表現変更	2,5,6,8
第 1.22 版	2007/11/7	1.21 版に関する問題点修正 －1 章の用語変更 －2 章の表現変更（ログアラート機能） －2 章追加 TOE（LAN ドライバ） －5 章機能要件の見直し －5 章見直しに対しての 6 章の対応 －8 章全般の表現変更	1,2,5,6,8
第 1.23 版	2007/11/12	1.22 に関する問題点修正 －1 章、用語集の見直し －2 章、全体の表現変更	1,2,5,6,8

Copyright © NEC Corporation 2007 All rights reserved.

バージョン	作成・更新日	更新概要	更新箇所
第 1.24 版	2007/11/15	1.22 に関する問題点修正 －1 章、用語集の見直し －2 章、全体の表現変更 －5 章、誤記の修正	1, 2, 5 p.23
第 1.25 版	2007/11/26	1 章～4 章の表現の見直し	1, 2, 3, 4
第 1.26 版	2007/11/30	5 章～8 章の表現の見直し	5, 6, 8
第 1.27 版	2007/12/4	OEN.HOST_MANAGEMENT の内容を追記 8 章(8.1, 8.2.1, 8.2.5, 8.2.6)の誤記修正	4, 8
第 1.28 版	2007/12/6	6.1.4, 8.1.3 **の表現不足部分を追記**	6, 8
第 1.29 版	2007/12/11	2.1.2, 8.1.5 **の表現不足部分を追記**	2, 8
第 1.30 版	2007/12/14	2.5 TOE **資産** **ー誤記修正（アラートアクション設定）** **－3）内部ネットワークの情報の記述を修正**	2
第 1.31 版	2008/1/22	**2～8 章の見直し**	2,3,4,5,6,8
第 1.32 版	2008/2/12	**2～8 章の誤記訂正**	2,3,4,5,6,8
第 1.33 版	2008/3/11	**1、6、8 章の記述見直し**	1, 6, 8
第 1.34 版	2008/3/24	指摘により修正	1,2

Copyright © NEC Corporation 2007 All rights reserved.