NEC

NEC ファイアウォール SG ソフトウェア Ver.3.0.1

セキュリティターゲット

日本電気株式会社

Ver. 1.18
2016/10/24

NEC

目次

1　ST 概説

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

1.1 ST 参照

本節では、ST の識別情報を記述する。

タイトル	NECファイアウォール SG ソフトウェア Ver.3.0.1 セキュリティターゲット
バージョン	1.18
発行日	2016 年 10 月 24 日
作成者	日本電気株式会社

1.2 TOE 参照

本節では TOE の識別情報を記述する。

TOE 名	NECファイアウォール SG ソフトウェア
TOE バージョン	3.0.1
開発者	日本電気株式会社

1.3 TOE 概要

1.3.1 TOE 種別および主要セキュリティ機能

1.3.1.1 TOE の種別

TOE は、「NEC ファイアウォール SG」と呼ばれるファイアウォールアプライアンス製品内のソフトウェア全体である。

1.3.1.2 TOE が提供する機能

TOE が提供する機能は下記である。

① 設定管理機能
② パケットフィルタ機能
③ ログアラート機能

1.3.1.3 TOE の使用法と主要セキュリティ機能

TOE の主な使用法とセキュリティ機能を以下に示す。

① 設定管理機能
管理端末上の Web 画面より識別認証されたファイアウォール管理者が TOE のセキュリティ機能に関する設定の参照、および変更を行えるようにする機能である。
本機能を実現するために必要となる下記機能を本機能のサブコンポーネントとして提供する。
・管理者認証機能
・通信保護機能

管理者認証機能は、管理者 ID、パスワードにより、ファイアウォール管理者、システム管理者を識別認証する機能を提供する。
通信保護機能は、管理端末と TOE 間のすべての通信を、SSL/SSH を使用し暗号化する機能である。

② パケットフィルタ機能
TOE が中継する IP パケットデータを事前に定められたパケットフィルタルールに則って、破棄、または通過させる。

③ ログアラート機能
設定管理機能、パケットフィルタ機能の操作・処理記録(ログ・アラート)を追跡記録(監査記録)するための機能である。アラートアクション設定を行うことにより出力されたアラートをメールなどにより通知することが可能である。

1.3.1.4 その他の機能

TOE のその他の機能を以下に示す。

① リモートメンテナンス機能
システム管理者がリモートコンソールで管理端末より TOE に接続し保守作業を行えるようにする機能である。

1.3.1.5 TOE 利用環境

本 TOE は、ネットワーク上を流れる IP パケットデータを中継する IT 製品として、外部ネットワークと内部ネットワークの境界上に設置して内部ネットワークを外部ネットワークの脅威から保護する利用を想定している。TOE の想定する利用環境を 図 1 に記述する。(メールサーバはログアラート機能でアラートをメールで通知する場合に必要)。

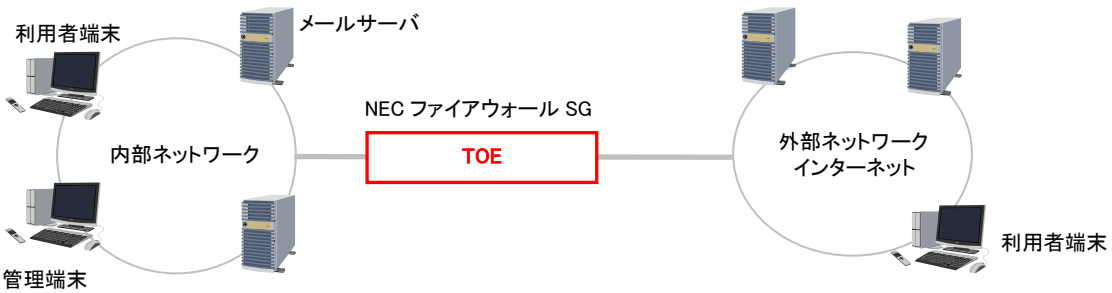


図1 TOE の想定する利用環境

1.3.1.6 TOE 以外のハードウェア構成とソフトウェア構成

図 1 利用環境における TOE 以外のハードウェア構成、およびソフトウェア構成については以下のとおりである。

（ア）NEC ファイアウォール SG（以降 SG）
SG は、TOE を動作させるための専用のハードウェアであり、以下のファイアウォールアプライアンス製品を指す。

- NEC SG3600LM
- NEC SG3600LG
- NEC SG3600LJ（認証評価では、このモデルを使用）
- NEC InterSecVM/SG

製品形態は、HW アプライアンス、仮想アプライアンスの2種類である。NEC SG3600LM、NEC SG3600LG、および NEC SG3600LJ が前者、NEC InterSecVM/SG が後者 である。
3つの HW アプライアンス製品では、HW 構成が異なる。
4製品で製品形態、HW 構成が異なるが、TOE であるソフトウェア全体は同一である。

（イ）管理端末
ハードウェアは、汎用の PC であり、Web ブラウザを使用して TOE に対して TOE 構成設定データの参照や変更を行うことができる。

ソフトウェアは、下記を使用する。
- Windows7 以降(評価では Windows7 を使用)
- Internet Explorer 8 以降(評価では Internet Explorer 11 を使用)
- SSH プロトコルバージョン2に対応した SSH クライアントソフトウェア
  （リモートコンソールを利用する場合）

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

（エ）メールサーバ
電子メールを配送するためのサーバコンピュータ。ログアラート機能でアラートをメールで通知する場合に必要。

1.4 TOE 記述

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

1.4.1 TOE 関連の利用者役割

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。

- 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（監査記録ファイル設定）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
- 管理者情報(ファイアウォール管理者ID、システム管理者ID)の問い合わせ、改変
- 管理者情報(ファイアウォール管理者パスワード、システム管理者パスワード)の改変
- 監査記録（イベントログ、アラートログ）の参照
- OSの日時情報の問い合わせ、改変

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、管理端末からTOEのリモートメンテナンス機能に接続し、識別認証された後にTOEの保守作業を行う。

2）その他の役割

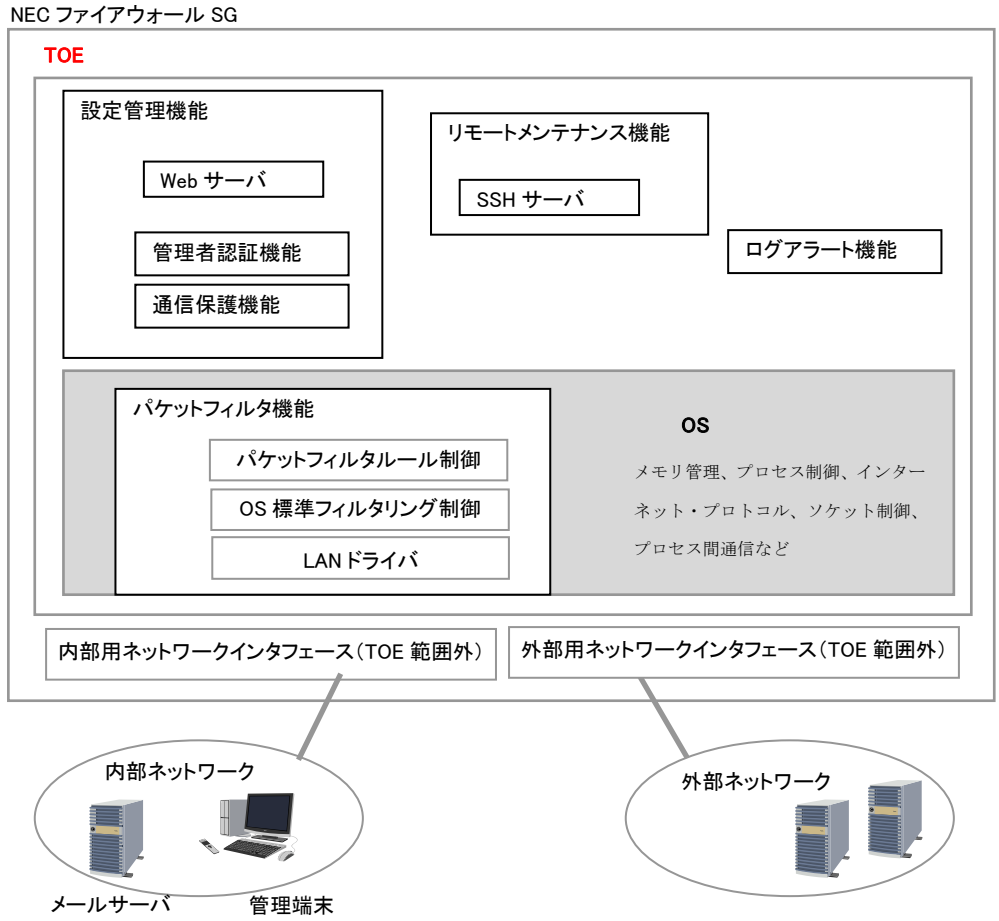
① ファイアウォール管理責任者

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。

1.4.2 TOE の物理的範囲

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 SG 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。
TOE の物理的範囲を図 2 に記述する。

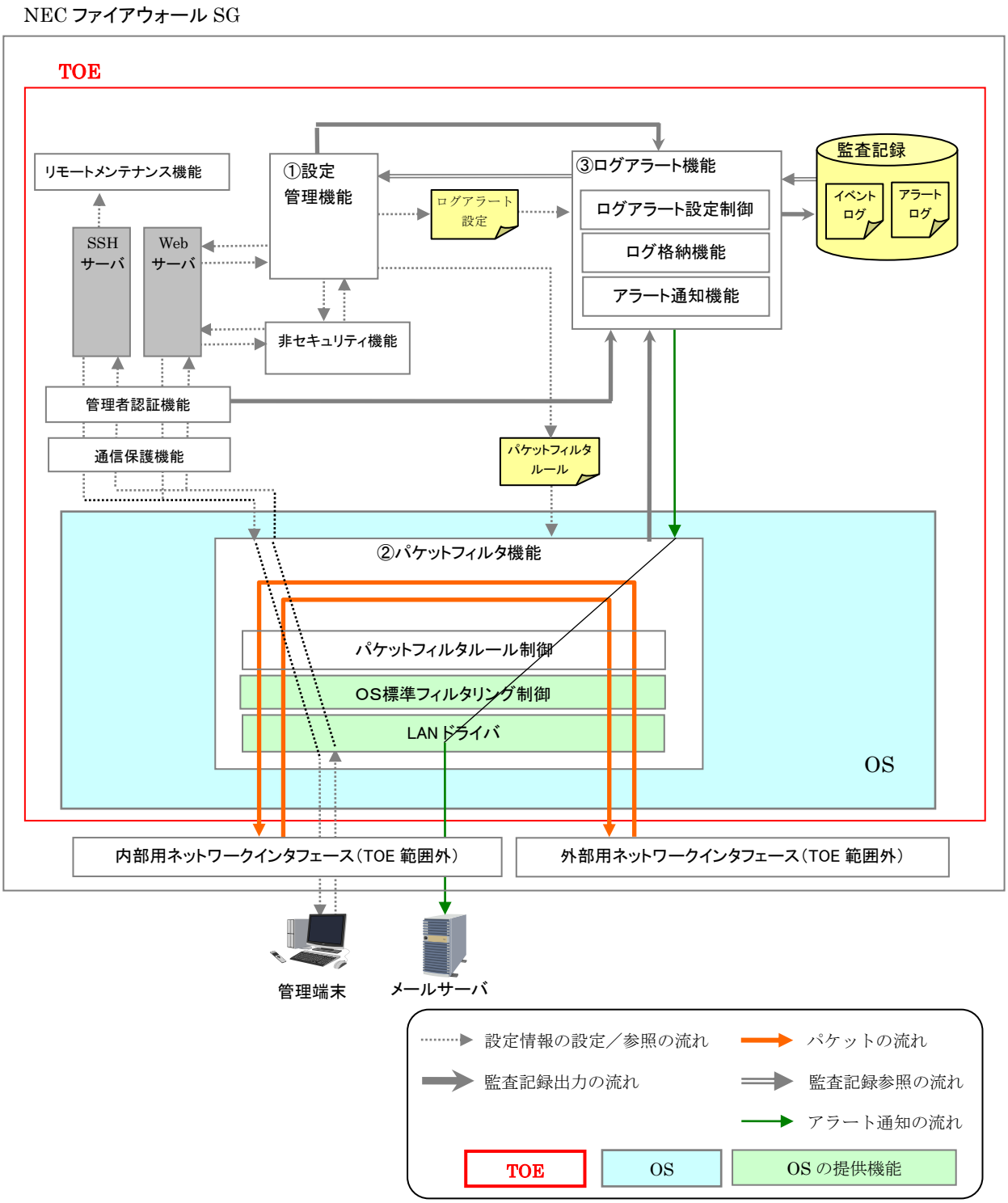
図 2 TOE 物理的範囲



1.4.3 TOE の論理的範囲

TOE の論理的範囲を図 3 に記述する。

図 3 TOE の論理的範囲



1.4.3.1 評価構成

TOE の評価対象の構成は以下の通りである。

TOE の設定および構成	
アドレス変換（NAT/NAPT）	なし
VPN 設定	なし
冗長構成	なし
仮想ファイアウォール	なし
AD 連携	なし
DMZ	なし
不正アクセス対策レベル	ベーシック
Management Console のセキュリティモード	レベル 2(パスワード+SSL)
SSH プロトコルバージョン	「2 に限定」
管理端末	登録した管理端末は 1 台

1.4.3.2 TOE が提供するセキュリティ機能

TOE が提供する機能を以下に記述する。
①～③の説明は図 3 TOE の論理的範囲の①～③で示した機能に対応する。

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。内部ネットワークに接続されている管理端末を利用するファイアウォール管理者だけが、識別認証された後に本機能を利用できる。
インタフェースは Web 画面である。

設定管理機能では下記を設定する機能を提供する。
設定完了時は、ログアラート機能、パケットフィルタ機能へ適用指示を行う。

- ログアラート設定（監査記録ファイル設定）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
- 管理者情報(ファイアウォール管理者 ID、システム管理者 ID)の問い合わせ、改変
- 管理者情報(ファイアウォール管理者パスワード、システム管理者パスワード)の改変
- パケットフィルタルール（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
- OS の日時情報の問い合わせ、改変

設定管理機能のサブコンポーネントとして下記を提供する。
・管理者認証機能
・通信保護機能

管理者認証機能は、ファイアウォール管理者、システム管理者が、管理端末より TOE に接続する際に管理者 ID、およびパスワードによる識別認証を行えるようにする機能である。
600 秒以内に 2 回連続して識別認証に失敗した場合は、識別認証機能を 600 秒間ロックアウトする機能を提供する。

通信保護機能は、設定管理機能、リモートメンテナンス機能で使用する全パケットを、SSL/SSH を使用し暗号化し、盗聴より保護する。
TOE 使用開始時の初期設定時にて、Management Console のセキュリティモードは、「レベル 2(パスワード+SSL)」を選択、SSH プロトコルバージョンは、「2 に限定」を選択することにより、SSL/SSH が使用される運用を想定している。

設定管理機能は、以下の事象が発生した場合に、その運用イベントをログアラート機能へ通知する。ログアラート機能は、受付けたイベントをイベントログとして記録する。

- 監査記録の参照
- パケットフィルタルール改変、削除、追加の成功
- ログアラート設定(監査記録ファイル)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
- 管理者情報(ファイアウォール管理者 ID、システム管理者 ID、パスワード)の改変の成功
- 設定管理機能の起動
- ファイアウォール管理者の識別認証の成功／失敗
- システム管理者の識別認証の成功／失敗
- OS の日時情報の改変の成功

② 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、及び TOE 自身が送信する IP 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 TOE 以外の場合は LAN ドライバに送信を指示し、宛先が TOE 自身の場合は上位プロトコルに渡す。
設定に従い拒否と判断れさた IP パケットは破棄し、パケットが TCP または UDP の場合は 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。
なお、一定の条件に合致するパケットは不正パケットとみなし、ルールに基づく評価を実施する前に破棄する。

c) LAN ドライバ
外部用ネットワークインタフェース、及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 3 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 サイト共通ルール
③ 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、不正アクセス対策レベルとして「ベーシック」が選択されている環境を想定しており、TOE 使用開始時の初期設定時に指定され、組み込まれる。

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・破棄する 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（パケットフィルタルールを移行するための機能）、バックアップ／リストアすることができる。
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、監査記録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。

（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、必ず監査記録が生成される。

（イ）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、必ず監査記録が生成される。

（ウ）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。

次に、ステートフルインスペクション機能について説明する。
ステートフルインスペクション機能は、OS 標準フィルタリング制御が動作する前に受信したパケットを下記4種類のステートに分類し、各ステートに応じたフィルタリング処理を実施する。

（ア）NEW
宛先・送信元、IP アドレス・ポートが、ステートフルインスペクション機能により保持されているセッション情報に存在しないパケット。
OS 標準フィルタリング制御による評価対象とする。通過と判定された場合はセッション情報を保持する。

（イ）ESTABLISHED
宛先・送信元、IP アドレス・ポートが、セッション情報に存在するパケット。
OS 標準フィルタリング制御による評価は行わずに通過と判定する。

（ウ）INVALID
プロトコル仕様に基づく正当な手順を踏んでいないと判定されたパケット。
不正パケットと判断され破棄する。

（エ）RELATED
FTP プロトコルでやりとりされる制御情報により認識したデータ転送セッションに該当するパケット、またはセッション情報に存在する宛先・送信元、IP アドレス情報をペイロードに格納している ICMP エラーパケット。
OS 標準フィルタリング制御による評価は行わずに通過と判定する。

最後に特定不正パケットの破棄について説明する。特定不正パケットについては、パケットフィルタルールによる判定を行う前に無条件に破棄する。

③ ログアラート機能
ログアラート機能は、以下の 3 つの機能を提供する。

a) ログアラート設定制御

設定管理機能からの指示により、ログアラート格納機能、アラート通知機能が参照するメモリ上のログアラート設定を書換える。

b) ログ格納機能

ログ格納機能は、設定管理機能、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記録へ格納する。
監査記録格納時、ログ格納機能はログアラート設定（監査記録ファイル設定）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（監査記録ファイル設定）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。
格納されたログは表形式での画面表示、CSV でのファイル出力が可能である。

c) アラート通知機能

アラート通知機能は、ログアラート設定（アラートアクション設定）に基づきアラート通知が必要であるかを判断し、必要であればファイアウォール管理者に対しアラート通知を行う。
通知方法がメール通知の場合は、アラート通知機能はメールデータ（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（監査記録ファイル設定、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 4 に示す。

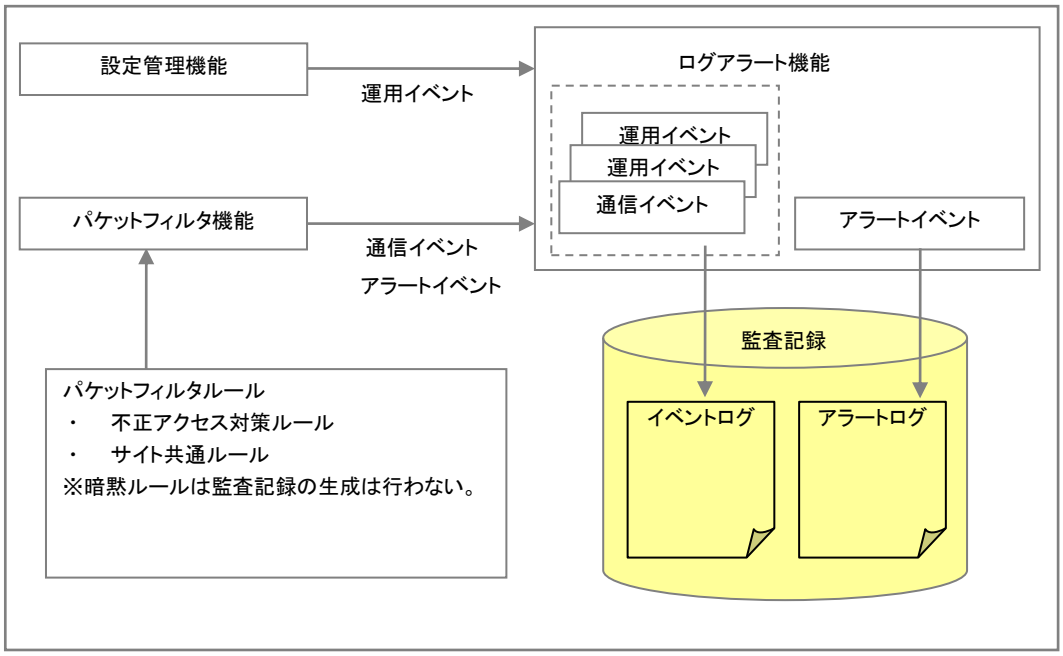


図 4 監査記録出力の流れ

設定管理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）を監査記録（イベントログ）に格納し、監査記録（アラートイベント）を監査記録（アラートログ）に格納する。

1.4.4 ガイダンス

本 TOE を構成するガイダンスは以下のとおりである。

表 1 ガイダンス

ガイダンス文書名	版数
NEC ファイアウォール SG ソフトウェア Ver.3.0.1 インストールガイダンス	1.08
NEC ファイアウォール SG ソフトウェア Ver.3.0.1 運用管理・操作利用ガイダンス	1.08

2　適合主張

2.1 CC 適合主張

本 ST および TOE の CC 適合主張は、以下のとおりである。

ST と TOE が適合を主張する CC のバージョン:
パート 1: 概説と一般モデルバージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
パート 2: セキュリティ機能コンポーネントバージョン 3.1 改訂第 4 版［翻訳第 1.0 版］
パート 3: セキュリティ保証コンポーネントバージョン 3.1 改訂第 4 版［翻訳第 1.0 版］

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

2.2 PP 主張

本 ST が適合している PP はない。

2.3 パッケージ主張

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

2.4 適合根拠

本 ST は、PP 適合を主張しないので、PP 適合根拠はない。

3　セキュリティ課題定義

3.1 脅威

3.1.1 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設定情報
以下の情報がある。
・パケットフィルタルール
・管理者情報
・ログアラート設定
・OS の日時情報

2）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および内部ネットワークで動作しているサービス

3.1.2 脅威

本 TOE に対する脅威を、**表** 3 に記述する。攻撃者は、基本的な攻撃能力をもつものであり、TOE の動作について公開されている情報知識を持っていると想定する。

表 2 脅威

脅威 識別子	説明
TOE への不正アクセス T.TOE_ACCESS	攻撃者が、ファイアウォール管理者、またはシステム管理者になりすましファイアウォールの設定情報を改ざんする。 ファイアウォールの設定情報の改ざんは不正な IP パケットや IP 通信サービスの通過につながる。
内部ネットワークへの不正アクセス T. NETWORK_ACCESS	攻撃者が、外部ネットワークから下記を行う恐れがある。 ・外部からのアクセスが許可されていないサービスにアクセスする。 ・Ping Flood、または SYN Flood により内部ネットワーク上のサービスを停止させる。
特定不正パケットによるアクセス T.INVALID_PACKET	攻撃者が、外部ネットワークから下記を行う恐れがある。 特定不正パケットを内部ネットワークに対して送信する。

3.2 組織のセキュリティ方針

本 TOE が順守しなければならない組織のセキュリティ方針はない。

3.3 前提条件

本 TOE の動作、運用、および利用に関する前提条件を、**表 4** に記述する。

表 3 前提条件

前提条件 識別子	説明
管理者の任命 A.APPOINT	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、及びシステム管理者を任命する。
安全な場所 A.SAFE_PLACE	ファイアウォール管理者は、TOE がインストールされるハードウェア(SG)をシステム管理者、及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する。 ファイアウォール管理者は、パケットフィルタルールをバックアップした媒体を、システム管理者、及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保管する。
接続形態 A.NO_BYPASS	ファイアウォール管理者は、TOE が動作する SG 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。
管理者によるパスワードの管理 A.PASSWORD_MANAGEMENT	ファイアウォール管理者は TOE にアクセスするためのパスワードを、第三者に知られないように管理する。 システム管理者は TOE にアクセスするためのパスワードを、第三者に知られないように管理する。
管理端末の保護 A.SAFE_TERMINAL	ファイアウォール管理者は、不正に使用されたり、不正なソフトウェアがインストールされたりしないように管理端末を管理する。
システム管理者による保守 A.SYSTEM_MANAGEMENT	システム管理者はリモートメンテナンス機能を使用して保守作業のみを行う。

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 のセキュリティ対策方針

TOE のセキュリティ対策方針を**表** 4 に記述する。

表 4 TOE セキュリティ対策方針

セキュリティ対策方針 識別子	内容
設定管理 O.SECURITY_MANAGEMENT	ファイアウォールの設定情報の管理機能を提供し、その実行を識別認証されたファイアウォール管理者およびシステム管理者に制限する。 また、識別認証機能の強度を高めるため、認証失敗時に識別認証機能をロックする機能を提供し、パスワードの盗聴を防止するため、TOE と管理端末間の通信を保護する。
パケットフィルタ O.PACKET_FILTER	外部からのアクセスが許可されていないサービスへのアクセス、Ping Flood、または SYN Flood によるサービス妨害を防止するためにパケットフィルタルールに基づいて、特定不正パケット除去後の IP パケットの入出力を制御する。
特定不正パケット破棄 O.INVALID_PACKET	特定不正パケットを破棄する。
監査 O.AUDIT	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、事象の発生日時、種別、結果、内容を記録する。
アラート O.ALERT	TOE は、ログアラート設定（アラートアクション設定）に基づきアラート通知が必要であるかを判断し、必要であればファイアウォール管理者に対しアラート通知を行い対応を促す。

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を**表** 5 に記述する。

表 5 運用環境のセキュリティ対策方針

セキュリティ対策方針 識別子	内容
管理者の任命 OEN.APPOINT	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、及びシステム管理者を任命しなくてはならない。
安全な場所 OEN.SAFE_PLACE	ファイアウォール管理者は、TOE がインストールされるハードウェア（SG）、システム管理者、及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しなければならない。 ファイアウォール管理者は、パケットフィルタルールをバックアップした媒体を、システム管理者、及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保管しなければならない。
接続形態 OEN.NO_BYPASS	ファイアウォール管理者は、TOE が動作する SG 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、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。
管理者によるパスワードの管理 OEN.PASSWORD_MANAGEMENT	ファイアウォール管理者は TOE にアクセスするためのパスワードを、第三者に知られないように管理しなければならない。 システム管理者は TOE にアクセスするためのパスワードを、第三者に知られないように管理しなければならない。
管理端末の保護 OEN.SAFE_TERMINAL	ファイアウォール管理者は、不正に使用されたり、不正なソフトウェアがインストールされたりしないように管理端末を管理しなければならない。
システム管理者による保守 OEN.SYSTEM_MANAGEMENT	システム管理者はリモートメンテナンス機能を使用して TOE の保守作業をおこない、それ以外の作業をおこなってはならない。

4.3 セキュリティ対策方針根拠

運用環境のセキュリティ対策方針を**表** 6 に記す。また、各セキュリティ課題定義がセキュリティ対策方針により保証されていることを**表** 7 に記す。

表 6 セキュリティ対策方針と対抗する脅威及び前提条件

セキュリティ対策方針 ＼ 脅威 前提条件	T.TOE_ACCESS	T. NETWORK_ACCESS	T.INVALID_PACKET	A.SAFE_PLACE	A.NO_BYPASS	A.APPOINT	A.PASSWORD_MANAGEMENT	A.SAFE_TERMINAL	A.SYSTEM_MAMAGEMENT
O.SECURITY_MANAGEMENT	✓								
O.PACKET_FILTER		✓							
O.INVALID_PACKET			✓						
O.AUDIT	✓	✓							
O.ALERT		✓							
OEN.SAFE_PLACE				✓					
OEN.NO_BYPASS					✓				
OEN.APPOINT						✓			
OEN.PASSWORD_MANAGEMENT							✓		
OEN.SAFE_TERMINAL								✓	
OE.SYSTEM_MANAGEMENT									✓

表 7 セキュリティ課題定義に対応するセキュリティ対策方針根拠

セキュリティ課題定義	セキュリティ対策方針根拠
T.TOE_ACCESS	ファイアウォール管理者、またはシステム管理者へなりすましによるファイアウォールの設定情報の改ざんは、O.SECURITY_MANAGEMENT により TOE と管理端末間の通信を保護することでパスワードの盗聴を防止し、設定情報へのアクセスを識別認証されたファイアウォール管理者およびシステム管理者に制限することで防止することができる。 また、O.AUDIT によって監査記録を生成し、参照可能とすることで、監査記録から識別認証機能への攻撃（なりすましの試行）の可能性を検出し、適切な対応を行うことができる。
T. NETWORK_ACCESS	外部からのアクセスが許可されていないサービスへのアクセス、Ping Flood、または SYN Flood による内部ネットワーク上のサービス停止については、O.ALERT による攻撃の可能性の通知とファイアウォール管理者の対応、および O.PACKET_FILTER による IP パケットの入出力の制御（不正なパケットの通過の防止）によって防止することができる。 また、O.AUDIT によって監査記録を生成し、参照可能とすることで、監査記録から、O.ALERT による通知の対象でない事象についても攻撃の可能性を検出し、適切な対応を行うことができる
T.INVALID_PACKET	特定不正パケットは標準のパケットフォーマットに従わないパケット等であり、O.INVALID_PACKET によって破棄することで内部ネットワークへの到達を防止する。
A.SAFE_PLACE	OEN.SAFE_PLACE により前提条件を満たすことができる。
A.NO_BYPASS	OEN.NO_BYPASS により前提条件を満たすことができる。
A.APPOINT	OEN.APPOINT により前提条件を満たすことができる。
A.PASSWORD_MANAGEMENT	OEN.PASSWORD_MANAGEMENT により前提条件を満たすことができる。
A.SAFE_TERMINAL	OEN.SAFE_TERMINAL により前提条件を満たすことができる。
A.SYSTEM_MANAGEMENT	OEN.SYSTEM_MANAGEMENT により前提条件を満たすことができる。

5　拡張コンポーネント定義

5.1 拡張コンポーネント定義

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

6　セキュリティ要件

本章では、セキュリティ機能要件、セキュリティ保証要件、及びセキュリティ要件根拠について記述する。

6.1 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。
例）依存性： ~~除去されるクラス~~

6.1.1 セキュリティ監査クラス(FAU)

FAU_ARP.1 セキュリティアラーム

下位階層： なし
依存性： **FAU_SAA.1** 侵害の可能性の分析

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:*アクションのリスト*]**を実行しなければならない。

[割付:*アクションのリスト*]
・ ファイアウォール管理者へのアラートの通知

FAU_GEN.1 監査データ生成

下位階層： なし
依存性： **FPT_STM.1** 高信頼タイムスタンプ

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない：
a） 監査機能の起動と終了；
b） 監査の**[選択: *最小*、*基本*、*詳細*、*指定なし*: から一つのみ選択]**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

表 8 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: 潜在的なセキュリティ侵害に	［イベントログ］	

	よってとられるアクション。	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動作/停止。 b) 最小: ツールによって実行される自動応答。	A)なし(分析メカニズムの動作/停止はできないため。) b) なし(セキュリティ侵害の可能性の検出時点では、応答は返さないため。)	なし
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、及び参照に使用した管理端末の IP アドレス
FAU_STG.1	なし	なし	なし
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.1a	なし	なし	なし
FDP_IFF.1a	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、情報の特定のサブセット(例えば、対象物の务化の監査)。	b) パケットフィルタルール(サイト共通ルール、不正アクセス対策ルール)に対する監査記録が生成される。	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・タイプ(ICMP、ICMPv6 の場合)・コード(ICMP、ICMPv6 の場合)
FDP_IFC.1b	なし	なし	なし
FDP_IFF.1b	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、情報の特定のサブセット(例えば、対象物の务化の監査)。	なし (特定不正パケット(標準のパケットフォーマットに従わないパケット等)を破棄する処理であるため)	なし
FIA_AFL.1	a) 最小: 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(たとえば端末の停止)、もし適切であれば、正常状態への復帰(たとえば端末の再稼動);	[イベントログ] a) ロックアウト開始／解除	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／システム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／システム管理者 ID
FIA_UID.2	a)最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b)基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用;	[イベントログ] b）ファイアウォール／システム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／システム管理者 ID
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
FPT_STM.1	a) 最小: 時間の変更; b) 詳細: タイムスタンプの提供。	[イベントログ] a）OS の日時情報の改変の成功	なし
FTP_TRP.1	なし	なし	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（該当する場合）、事象の結果(成功または失敗);及び

b） 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、**[割付:*その他の監査関連情報*]**

[割付:*その他の監査関連情報*]

その他の監査関連情報は、表 8 に示す通り。

FAU_SAA.1 侵害の可能性の分析

下位階層： なし

依存性： **FAU_GEN.1** 監査データ生成

FAU_SAA.1.1 TSF は、監査事象の監視に規則のセットを適用し、これらの規則に基づき SFR 実施の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、監査された事象を監視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*]**の集積、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*]

ログアラート設定（アラートアクション設定）

[割付: *その他の規則*]

なし

FAU_SAR.1 監査レビュー

下位階層: なし
依存性: **FAU_GEN.1** 監査データ生成

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*]
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

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。

FAU_STG.1 保護された監査証跡格納

下位階層: なし
依存性: **FAU_GEN.1** 監査データ生成

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を**[選択: *防止*、*検出*: から 1 つのみ選択]**できなければならない。

[選択:*防止*、*検出*: から一つのみ選択]
防止

FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション
依存性: **FAU_STG.1** 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、**[選択:*監査事象の無視*、*特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止*、*最も古くに格納された監査***

記録への上書き: から 1 つのみ選択]及び[**割付: *監査格納失敗時にとられるその他のアクション***]を行わなければならない。

[**選択: *監査対象事象の無視、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***]
なし(監査格納失敗時、TOE は停止するため。)

6.1.2 利用者データ保護クラス(FDP)

FDP_IFC.1a サブセット情報フロー制御

下位階層: なし
依存性: **FDP_IFF.1** 単純セキュリティ属性

FDP_IFC.1.1a TSF は、[**割付: *SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト***]に対して[**割付:*情報フロー制御 SFP***]を実施しなければならない。

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

- サブジェクトのリスト
  パケットフィルタ機能
- 情報のリスト
  TOE を介して送受信される IP パケット(特定不正パケット除去後)
- 操作のリスト
  IP パケットの通過
  IP パケットの拒否(パケットを破棄する。さらにパケットが TCP または UDP の場合は送信元へエラーを通知する)
  IP パケットの破棄

[**割付:*情報フロー制御 SFP***]
パケットフィルタ方針

FDP_IFC.1b サブセット情報フロー制御

下位階層: なし
依存性: **FDP_IFF.1** 単純セキュリティ属性

FDP_IFC.1.1b TSF は、[**割付: *SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こすサブジェクト、情報及び操作のリスト***]に対して[**割付:*情報フロー制御 SFP***]を実施しなければならない。

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

- サブジェクトのリスト

パケットフィルタ機能
- 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
  IP パケットの破棄

[割付:*情報フロー制御 SFP*]
パケットフィルタ方針

FDP_IFF.1a 単純セキュリティ属性

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

FDP_IFF.1.1a TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[**割付:** ***情報フロー制御 SFP***]を実施しなければならない。: [**割付:** ***示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性***]

[**割付:** ***情報フロー制御 SFP***]
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
  パケットフィルタ機能
- サブジェクト(パケットフィルタ機能)のセキュリティ属性

  設定管理機能で静的に設定する属性

  - 受信ネットワークインタフェース(外部、内部、または DMZ より選択)
  - 送信ネットワークインタフェース(外部、内部、または DMZ より選択)
  - 送信元 IP アドレス(ホスト、またはネットワークアドレスを指定)
  - 送信先 IP アドレス(ホスト、またはネットワークアドレスを指定)
  - プロトコル種別(TCP、UDP、ICMP、またはその他のプロトコルを指定)
  - タイプ(プロトコル種別が ICMP、または ICMPv6 の場合のみ指定可能)
  - コード(プロトコル種別が ICMP、または ICMPv6 の場合のみ指定可能)
  - 送信元ポート番号(プロトコル種別が TCP、または UDP の場合のみ指定可能)
  - 送信先ポート番号(プロトコル種別が TCP、または UDP の場合のみ指定可能)
  - 処理方法(許可、破棄、または拒否 より選択)
  - 記録方法(イベントログに記録、アラートログ、およびイベントログに記録、または記録しない より選択)

パケットフィルタ機能(ステートフルインスペクション機能)で動的に設定する属性

- 送信元 IP アドレス
- 送信元ポート番号
- 宛先 IP アドレス
- 宛先ポート番号
- 戻り送信元 IP アドレス
- 戻り送信元ポート番号
- 戻り宛先 IP アドレス
- 戻り宛先ポート番
- L3 プロトコル番号
- L4 プロトコル番号
- ステート
- TCP 前回状態
- タイムアウト値
- FTP データ転送用セッションで使用するアドレス・ポート番号・接続方向

パケットフィルタ機能固定値

- しきい値(不正アクセス対策ルールで使用)

・ 情報のリスト
TOE を介して送受信される IP パケット(特定不正パケット除去後)
・ 情報(IP パケット)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
送信元 IP アドレス
送信先 IP アドレス
プロトコル種別
タイプ
コード
送信元ポート番号
送信先ポート番号
TCP フラグ
IP ヘッダ
TCP ヘッダ
UDP ヘッダ
ICMP ヘッダ
FTP データ転送用セッションで使用するアドレス・ポート番号・接続方向

FDP_IFF.1.2a 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*]

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と IP パケット(特定不正パケットを除く)から取得した情報のセキュリティ属性が一致するかを比較し、一致する場合は、指定された処理方法による操作を実施し、それ以外の IP パケット(特定不正パケットを除く)は破棄する。

FDP_IFF.1.3a 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.1.4a TSF は、以下の規則、[割付:*セキュリティ属性に基づいて情報フローを明示的に許可する規則*]に基づいて、情報フローを明示的に許可しなければならない。

[割付:*セキュリティ属性に基づいて情報フローを明示的に許可する規則*]

なし。

FDP_IFF.1.5a TSF は、以下の規則、[割付: *セキュリティ属性に基づいて情報フローを明示的に拒否する規則*] に基づいて、情報フローを明示的に拒否しなければならない。

[割付:*セキュリティ属性に基づいて情報フローを明示的に拒否する規則*]

不正アクセス対策レベル[ベーシック]の場合に動作する以下の不正アクセス対策ルールを適用し、パケットを破棄する。

- しきい値に基づく Ping Flood の検出
- しきい値に基づく SYN Flood の検出

FDP_IFF.1b 単純セキュリティ属性

下位階層: なし

依存性: FDP_IFC.1 サブセット情報フロー制御

~~FMT_MSA.3 静的属性初期化~~

FDP_IFF.1.1b TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[割付:*情報フロー制御 SFP*]を実施しなければならない。:[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々に対応する、セキュリティ属性*]

[割付: *情報フロー制御 SFP*]

特定不正パケット条件

[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

パケットフィルタ機能
- サブジェクト（パケットフィルタ機能）のセキュリティ属性
  なし
- 情報のリスト
  TOE を介して送受信される IP パケット
- 情報(IP パケット)のセキュリティ属性
  送信元 IP アドレス
  送信先 IP アドレス
  IP ヘッダ
  TCP ヘッダ

FDP_IFF.1.2b 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*]
送受信される IP パケットが特定不正パケットに該当する場合（送受信される IP パケットから取得した情報のセキュリティ属性が特定不正パケットの条件に合致する場合）、当該パケットを破棄する。

FDP_IFF.1.3b 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.1.4b TSF は、以下の規則、**[割付:*セキュリティ属性に基づいて情報フローを明示的に許可する規則*]**に基づいて、情報フローを明示的に許可しなければならない。

[割付:*セキュリティ属性に基づいて情報フローを明示的に許可する規則*]
なし。

FDP_IFF.1.5b TSF は、以下の規則、**[割付: *セキュリティ属性に基づいて情報フローを明示的に拒否する規則*]** に基づいて、情報フローを明示的に拒否しなければならない。

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

6.1.3 識別と認証クラス(FIA)

FIA_AFL.1 認証失敗時の取り扱い

下位階層: **なし**
依存性: **FIA_UAU.1** 認証のタイミング

FIA_AFL.1.1
TSF は、**[割付:*認証事象のリスト*]**に関して、**[選択:*[割付:正の整数値]、[割付:許容可能な値の範囲]内における管理者設定可能な正の整数値]***]回の不成功認証試行が生じたときを検出しなければならない。

[割付:*認証事象のリスト*]
・ファイアウォール管理者認証操作における最後の認証成功以降の不成功認証試行
・システム管理者認証操作における最後の認証成功以降の不成功認証試行

[選択:*[割付:正の整数値]、[割付:許容可能な値の範囲]内における管理者設定可能な正の整数値]*
[割付:*正の整数値*]

[割付:*正の整数値*]
2

FIA_AFL.1.2
不成功の認証試行が定義した回数[選択:に達する、を上回った]とき、TSF は、[割付: *アクションのリスト*]をしなければならない。

[選択:に達する、を上回った]
に達する

[割付:*アクションのリスト*]
・不成功認証試行回数の到達が1回目の不成功から 600 秒以内である場合、識別認証機能を 600 秒間ロックアウトし 600 秒経過後不成功認証試行回数を0にしてロックを解除する。
・不成功認証試行回数の到達が1回目の不成功から 600 秒超である場合は不成功認証試行回数を 1 にする。

FIA_UAU.2 アクション前の利用者認証

下位階層: **FIA_UAU.1 認証のタイミング**
依存性: **FIA_UID.1** 識別のタイミング

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

FIA_UID.2 アクション前の利用者識別

下位階層: **FIA_UID.1 識別のタイミング**
依存性: なし

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.4 セキュリティ管理クラス(FMT)

FMT_SMF.1 管理機能の特定

下位階層: なし
依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。:**[割付: *TSF によって提供される管理機能のリスト*]**。

[割付:*TSF によって提供されるセキュリティ管理機能のリスト*]

- ログアラート設定(監査記録ファイル設定)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
- 管理者情報(ファイアウォール管理者 ID、システム管理者 ID)の問い合わせ、改変
- 管理者情報(ファイアウォール管理者パスワード、システム管理者パスワード)の改変
- パケットフィルタルール(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
- OS の日時情報の問い合わせ、改変

表 9 機能要件に対して CC で規定している管理要件と TOE における管理機能

機能要件	CC で規定している管理要件	TOE における管理機能
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。	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_SAR.1	a) 監査記録に対して読み出しアクセス権のある利用者グループの維持(削除、改変、追加)。	なし(監査記録の参照は、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.1	なし	なし
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、TOE は停止するため。)
FDP_IFC.1a	なし	なし
FDP_IFC.1b	なし	なし
FDP_IFF.1a	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(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
FDP_IFF.1b	a) 明示的なアクセスに基づく決定に使われる属性の管理。	なし(処理は固定であるため)。
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理; b) 認証失敗の事象においてとられるアクションの管理。	なし(閾値、アクションは固定であるため。)
FIA_UAU.2	a) 管理者による認証データの管理; b) このデータに関係する利用者による認証データの管理。	ファイアウォール管理者によるファイアウォール／システム管理者 ID の改変、およびパスワードの改変
FIA_UID.2	a) 利用者識別情報の管理。	ファイアウォール管理者によるファイアウォール／システム管理者 ID の改変
FMT_SMF.1	なし	なし
FPT_STM.1	a) 時間の管理。	OS の日時情報の問い合わせ、改変
FTP_TRP.1	a) もしサポートされていれば、高信頼パスを要求するアクションの構成。	なし(常に高信頼パス(SSL/SSH)が使用される運用を想定しているため)

6.1.5 TSF の保護クラス(FPT)

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし
依存性: なし

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

6.1.6 高信頼パス／チャネルクラス(FTP)

FTP_TRP.1 高信頼パス

下位階層: なし
依存性: なし

FTP_TRP.1.1 TSF は、それ自身と**[選択: *リモート*、*ローカル*]**利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、**[選択: *改変*、*暴露*、*[割付: ほかのタイプの完全性、または機密性侵害]*]**からの通信データの保護を提供する通信パスを提供しなければならない。

[選択: *リモート*、*ローカル*]
リモート

[選択: *改変*、*暴露*、*[割付: ほかのタイプの完全性、または機密性侵害]*]
暴露

FTP_TRP.1.2 TSF は、**[選択: *TSF*、*ローカル利用者*、*リモート利用者*]**が、高信頼パスを介して通信を開始することを許可しなければならない。

[選択: *TSF*、*ローカル利用者*、*リモート利用者*]
リモート利用者

FTP_TRP.1.3 TSF は、**[選択: *最初の利用者認証*、*[割付: 高信頼パスが要求される他のサービス]*]**に対して、高信頼パスの使用を要求しなければならない。

[選択: *最初の利用者認証*、*[割付: 高信頼パスが要求される他のサービス]*]
[割付: 高信頼パスが要求される他のサービス]

[割付: *高信頼パスが要求される他のサービス*]
TOE と管理端末間の通信

6.2 セキュリティ保証要件

TOE の評価保証レベルは EAL1, ASE_OBJ.2, ASE_REQ.2 及び ASE_SPD.1 であり、保証コンポーネントは以下のとおりである。

表 10 EAL1+ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 保証要件

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

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応関係を**表** 11 に示す。**表** 11 に示すように、各セキュリティ機能要件は一つ以上のセキュリティ対策方針に対応している。
また各セキュリティ対策方針が、セキュリティ機能要件により保証されている根拠を、**表** 12 に記述する。

表 11 セキュリティ機能要件とセキュリティ対策方針の対応関係

セキュリティ機能要件 ＼ セキュリティ対策方針	O.SECURITY_MANAGEMENT	O.PACKET_FILTER	O.INVALID_PACKET	O.AUDIT	O.ALERT
FAU_ARP.1					✓
FAU_GEN.1				✓	
FAU_SAA.1					✓
FAU_SAR.1				✓	
FAU_STG.1				✓	
FAU_STG.4				✓	
FDP_IFC.1a		✓			
FDP_IFF.1a		✓			
FDP_IFC.1b			✓		
FDP_IFF.1b			✓		
FIA_AFL.1	✓				
FIA_UAU.2	✓				
FIA_UID.2	✓				
FMT_SMF.1	✓				
FPT_STM.1				✓	
FTP_TRP.1	✓				

表 12 セキュリティ対策方針によるセキュリティ機能要件根拠

セキュリティ対策方針	セキュリティ機能要件根拠
O.SECURITY_MANAGEMENT	FIA_UAU.2、FIA_UID.2 によりファイアウォール管理者、およびシステム管理者が TOE にアクセスする際は必ず識別認証が実施される。FMT_SMF.1 により ファイアウォールの設定情報の管理機能を提供する。 また、FIA_AFL.1 により 600 秒以内に 2 回連続して識別認証に失敗した場合は、600 秒間識別認証機能をロックアウトすることで、識別認証機能の強度を高め、FTP_TRP.1 により、TOE、管理端末間の通信を保護する。
O.PACKET_FILTER	FDP_IFC.1a、FDP_IFF.1a により、パケットフィルタ機能のセキュリティ属性と TOE を介して送受信される IP パケットのセキュリティ属性を比較し、合致したパケットについてはパケットフィルタ方針に従いパケットの通過/拒否/破棄を行う。 FDP_IFF.1.2a による判定を行う前には FDP_IFF.1.5a の不正アクセス対策ルール適用により、Ping Flood、および SYN Flood の検出・破棄を行う。
O.INVALID_PACKET	FDP_IFC.1b、FDP_IFF.1b により、TOE を介して送受信される IP パケットのセキュリティ属性を参照し、特定不正パケットの条件に合致したパケットについては破棄を行う。
O.AUDIT	FAU_GEN.1、FPT_STM.1 により、監査記録を生成し、FAU_STG.1、FAU_STG.4 により生成された監査記録を保護し、FAU_SAR.1 により監査記録の参照を可能とする。
O.ALERT	FAU_SAA.1 によりセキュリティ侵害の可能性を分析することができ、セキュリティ侵害と判断した場合は FAU_ARP.1 により監視結果をファイアウォール管理者へアラート通知することを可能とする。

6.3.2 依存性の検証

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及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**表** 13 に示す。

表 13 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	依存コンポーネント	依存性が満たされない 要件とその根拠
FAU_ARP.1	FAU_SAA.1	なし
FAU_GEN.1	FPT_STM.1	なし
FAU_SAA.1	FAU_GEN.1	なし
FAU_SAR.1	FAU_GEN.1	なし
FAU_STG.1	FAU_GEN.1	なし
FAU_STG.4	FAU_STG.1	なし
FDP_IFC.1a	FDP_IFF.1a	なし
FDP_IFF.1a	FDP_IFC.1a	なし
	FMT_MSA.3	すべてのセキュリティ属性は TOE 外で情報が生成される時に決定されているため、初期化を必要としない。よって、FMT_MSA.3 は不要である。
FDP_IFC.1b	FDP_IFF.1b	なし
FDP_IFF.1b	FDP_IFC.1b	なし
	FMT_MSA.3	すべてのセキュリティ属性は TOE 外で情報が生成される時に決定されているため、初期化を必要としない。よって、FMT_MSA.3 は不要である。
FIA_AFL.1	FIA_UAU.2	なし
FIA_UAU.2	FIA_UID.1	なし FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである。
FIA_UID.2	なし	なし
FMT_SMF.1	なし	なし
FPT_STM.1	なし	なし
FTP_TRP.1	なし	なし

6.3.3 セキュリティ保証要件根拠

TOE 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、TOE 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“基本的な攻撃能力”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，ASE_OBJ.2，ASE_REQ.2 及び ASE_SPD.1 は妥当な選択であるといえる。

7　TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の仕様を記述する。

7.1 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** 14 に示すように、本節で説明するセキュリティ機能は、6.1 節で記述したセキュリティ機能要件を満たすものである。

表 14 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 / セキュリティ機能	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FAU_STG.4	FDP_IFC.1a	FDP_IFF.1a	FDP_IFC.1b	FDP_IFF.1b	FIA_UAU.2	FIA_AFL.1	FIA_UID.2	FMT_SMF.1	FPT_STM.1	FTP_TRP.1
SF.MNG											✓	✓	✓	✓		✓
SF.PF							✓	✓	✓	✓						
SF.AUDIT	✓	✓	✓	✓	✓	✓									✓	

7.1.1 設定管理機能（SF.MNG）

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。
インタフェースは Web 画面であり、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。

本機能では、下記サブコンポーネントが提供される。

- 管理者認証機能
- 通信保護機能

管理者認証機能は、管理者 ID、パスワードにより、ファイアウォール管理者、システム管理者を識別認証する機能を提供する。(FIA_UID.2、FIA_UAU.2)
なお、600 秒以内に 2 回連続して識別認証に失敗した場合は、識別認証機能を 600 秒間ロックアウトする機能を提供する。ロックアウトは、600 秒経過後解除される。前回の識別認証失敗から 600 秒超経過後の識別認証失敗は1回目とカウントする。(FIA_AFL.1)

通信保護機能は、TOE と管理端末間の通信の盗聴を防ぐために、高信頼パスを使用する。
(FTP_TRP.1)

TOE は、以下のセキュリティ管理機能を提供する。(FMT_SMF.1)

- ログアラート設定(監査記録ファイル設定)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
- 管理者情報(ファイアウォール管理者 ID、システム管理者 ID)の問い合わせ、改変
- 管理者情報(ファイアウォール管理者パスワード、システム管理者パスワード)の改変

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（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・リストアを行う機能を提供する（FMT_SMF.1）。

・ 受信ネットワークインタフェース(外部、内部、または DMZ より選択)
・ 送信ネットワークインタフェース(外部、内部、または DMZ より選択)
・ 送信元 IP アドレス（ホスト、またはネットワークアドレスを指定）
・ 送信先 IP アドレス（ホスト、またはネットワークアドレスを指定）
・ プロトコル種別（TCP、UDP、ICMP、またはその他のプロトコルを指定）
・ タイプ（プロトコル種別が ICMP、または ICMPv6 の場合のみ指定可能）
・ コード（プロトコル種別が ICMP、または ICMPv6 の場合のみ指定可能）
・ 送信元ポート番号（プロトコル種別が TCP、または UDP の場合のみ指定可能）
・ 送信先ポート番号（プロトコル種別が TCP、または UDP の場合のみ指定可能）
・ しきい値(設定管理機能で静的に設定する属性)
・ 処理方法(許可、破棄、または拒否 より選択)
・ 記録方法(イベントログに記録、アラートログ、およびイベントログに記録、または記録しない より選択)

パケットフィルタ機能には、パケットフィルタルールオブジェクトを介してセキュリティ属性が付加（結合）される。パケットフィルタルールオブジェクトは、TOE 起動時に生成され、サイト共通ルール、不正アクセス対策ルール、暗黙のルール より構成されるパケットフィルタルールが適用される。パケットフィルタルールの初期値は、変更を許可しない制限的な暗黙のルール、不正アクセス対策ルールのみが定義されている。ファイアウォール管理者は、サイト共通ルールを編集することによりパケットフィルタルールオブジェクトが生成されるときに適用されるパケットフィルタルールを変更することができる。

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）。

・ OS の日時情報の問い合わせ、改変

通信保護機能では、設定管理機能の Web 接続では SSL、リモートメンテナンス機能のリモートコンソール接続では SSH を使用しすべての IP パケットのペイロード・データ部を暗号化する。

プロトコルは下記のとおり。

プロトコル： TLS1.2

SSH で使用する暗号アルゴリズムは下記のとおり。

暗号アルゴリズム： AES 192/256 bit

7.1.2 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、破棄、または拒否の処理を実施する（FDP_IFC.1a、FDP_IFC.1b）。

本機能のインタフェースは、TOE を介して送受信される IP パケットであり、特定不正パケットについては、無条件に破棄する(FDP_IFF.1b)。その上で、TOE は、IP パケットの IP ヘッダ、および TCP ヘッダ、UDP ヘッダ、または ICMP ヘッダから取得したセキュリティ属性を、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、破棄、または拒否の処理を実施する(FDP_IFF.1a)。

パケットフィルタ方針は、下記3つのルールより構成される。
- サイト共通ルール
- 不正アクセス対策ルール
- 暗黙のルール

各ルールの実現方法は下記である。

サイト共通ルールは、パケットフィルタ機能の下記セキュリティ属性が、送受信する IP パケットのセキュリティ属性に合致する場合にパケットフィルタルールのセキュリティ属性として定義されている処理方法、記録方法を実施する。

- パケットフィルタ機能のセキュリティ属性
  受信ネットワークインタフェース(外部、内部、または DMZ より選択)
  送信ネットワークインタフェース(外部、内部、または DMZ より選択)
  送信元 IP アドレス(ホスト、またはネットワークアドレスを指定)
  送信先 IP アドレス(ホスト、またはネットワークアドレスを指定)
  プロトコル種別(TCP、UDP、ICMP、またはその他のプロトコルを指定)
  タイプ(プロトコル種別が ICMP、または ICMPv6 の場合のみ指定可能)
  コード(プロトコル種別が ICMP、または ICMPv6 の場合のみ指定可能)
  送信元ポート番号(プロトコル種別が TCP、または UDP の場合のみ指定可能)
  送信先ポート番号(プロトコル種別が TCP、または UDP の場合のみ指定可能)
  処理方法(許可、破棄、または拒否 より選択)
  記録方法(イベントログに記録、アラートログ、およびイベントログに記録、または記録しない より選択)
- IP パケッ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
  送信元 IP アドレス
  送信先 IP アドレス
  プロトコル種別
  タイプ
  コード
  送信元ポート番号
  送信先ポート番号

なお、処理方法に「拒否」を選択した場合の送信元へのエラー送信処理は パケットが TCP、または UDP の場合 のみ動作する。したがって、プロトコル種別に任意、または TCP、UDP 以外のプロトコルを指定する場合、送信元へのエラー送信処理は動作しない。

また、ステートフルインスペクション機能を実現するためにセッション情報を保持する。
ステートフルインスペクション機能では、パケット受信時にパケット中の下記情報をセッション情報より検索し、検索できなかった場合は新規セッションとしてセッション情報を作成する。

- 送信元 IP アドレス
- 送信元ポート番号
- 宛先 IP アドレス
- 宛先ポート番号

セッション情報には下記情報が含まれる。
「戻り」で始まる情報は受信したパケットの送信元・宛先を逆にして生成する。

- 送信元 IP アドレス
- 送信元ポート番号
- 宛先 IP アドレス
- 宛先ポート番号
- 戻り送信元 IP アドレス　<- 宛先 IP アドレスより生成
- 戻り送信元ポート番号　<- 宛先ポート番号より生成
- 戻り宛先 IP アドレス　<- 送信元 IP アドレスより生成
- 戻り宛先ポート番号　<- 送信元ポート番号より生成
- L3 プロトコル番号
- L4 プロトコル番号
- ステート
- TCP 前回状態
- タイムアウト値
- FTP データ転送用セッションで使用するアドレス・ポート番号・接続方向

パケット受信時にセッション情報が検索できなかった場合は、ステートに NEW を設定する。検索できた場合は、ステートに ESTABLISHED を設定する。

<u>パケットが TCP の場合</u>

- 受信したパケットの TCP フラグとセッション情報の TCP 前回状態より、通信状態が正しく遷移していることを確認する。正しく遷移している場合は、次回パケット受信時に備え TCP 前回状態を更新する。不正の場合は、ステートに INVALID を設定する。
- ステータスが NEW の場合は、ftp データ転送用セッションの syn パケットである可能性がある。直前に ftp 制御用セッション(tcp/21)上を流れるデータ転送用セッション情報通知パケットより読み取った IP アドレス、ポート番号、接続方向に該当しないか確認する。該当する場合は、ステートに RELATED を設定する。

<u>パケットが UDP の場合</u>

- パケット受信時に実施するセッション情報検索結果によるステート設定以外のステート設定は行わない。

<u>パケットが ICMP の場合</u>

・ メッセージタイプの種類がエラーの場合は、ICMP 以外を使用したパケットに対するエラー応答の可能性がある。ステートが NEW の場合は、ペイロード中に含まれるエラーの元となったパケットの IP ヘッダ、および L4 ヘッダより IP アドレス、ポート番号を取得しセッション情報を検索する。検索できた場合はステートに RELATED を設定する。

ステート変更後、L4 プロトコルに応じたタイムアウト値を設定する。
タイムアウト値を超える時間、該当セッションに対する継続パケット受信がなければタイムアウトとし、セッション情報を破棄する。
なお、ステートが ESTABLISHED、または RELATED と設定されたパケットはパケットフィルタリング機能の対象外となる。ステートが INVALID と設定された場合は無条件に破棄される。

暗黙のルールは、その他のルールで通過、破棄、または拒否されなかった IP パケットをすべて破棄する。

不正アクセス対策ルールは、パケットフィルタルールのセキュリティ属性であり、開発時に設定されるしきい値(パケットフィルタ機能固定値)を使用し、Ping Flood、SYN Flood の検出・破棄を実現する。

Ping Flood
受信できる ICMP Echo Request パケットは 1 件/200ms で、5 件までキューイング可能。
1 件/200ms を上回るペースでパケットを受信し、キューがあふれた場合に Ping Flood と判定し、キューからあふれたパケットを破棄する。

SYN Flood
受信できる SYN パケットは 1 件/100ms で、1024 件までキューイング可能。
1 件/100ms を上回るペースでパケットを受信し、キューがあふれた場合に SYN Flood と判定し、キューからあふれたパケットを破棄する。

7.1.3 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** 8 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** 8 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、RTC 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に対して以下の監査情報リストを表形式で表示する機能、CSV でファイル出力する機能を提供する（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** 8 に示すその他の監査関連情報

TOE は、監査記録を生成する際に、ログを出力するパーティションの空き容量を確認し、ログアラート設定（監査記録ファイル設定）で設定されているパーティション残量が確保できない場合は、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、ログアラート設定（設定）に基づき監査記録を監視し、アラート通知が必要であるかを判断する。(FAU_SAA.1)
アラート通知が必要であればファイアウォール管理者に対しアラート通知を行う（FAU_ARP.1）。

監査記録の削除をシステム管理者のみに制限することで不正な改ざんや削除を防止している(FAU_STG.1)。

8 用語

用語	説明
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。内部ネットワークインタフェース、および DMZ ネットワークインタフェースに接続されるネットワークより構成される。組織内部のイントラネット、及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。
特定不正パケット	下記のいずれかに該当するパケット - IP ヘッダのフラグメント制御情報に不整合がある - フラグメント化されたパケットの再構成に失敗する - 送信元アドレスがブロードキャストアドレスである - 送信元アドレスがマルチキャストアドレスである - 送信元アドレスがループバックアドレスで、かつ入力インタフェースがローカルインタフェース以外のインタフェースである - 送信元アドレスが予約アドレスである - 送信元アドレスが未指定アドレスである - 送信元アドレスへの経路がルーティングテーブルに登録されていない - 送信元アドレスへの経路がルーティングテーブルに登録されているが、パケットを受信したインタフェースが、ルーティングテーブルの該当経路で使用するインタフェースとは異なる - 送信元アドレスがローカルアドレスで、かつ入力インタフェースがローカルインタフェース以外のインタフェースである - 送信元アドレス、または送信先アドレスがリンクローカルアドレスで、かつ送信先アドレスが TOE に設定されているアドレスではない - IPv4 ソースルーティングが設定されている - IPv6 経路制御ヘッダが付加されていて、かつタイプに 0 が設定されている - TCP ヘッダの TCP フラグの値が不正である - ICMP パケットのペイロードが不正である。
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 の上位プロトコル。コネクション指向。
UDP	User Datagram Protocol の略。IP の上位プロトコル。コネクションレス型。
ICMP	Internet Control Message Protocol の略。IP による通信を制御するためのもの。
ICMPv6	Internet Control Message Protocol for IPv6 の略。IPv6 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。
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、及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、認証及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。
Management Console セキュリティモード	ファイアウォール管理者は、「レベル 1(パスワード)」・「レベル 2(パスワード+SSL)」の 2 種類を選択することができる。 「レベル 1(パスワード)」は SSL を使用せず、HTTP で TOE にアクセスする運用を指定する。 「レベル 2(パスワード+SSL)」は SSL を使用し、HTTPS で TOE にアクセスする運用を指定する。 TOE の Management Console セキュリティモードとして「レベル 2(パスワード+SSL)」を選択した状態で TOE を運用しなければならない。
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。
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。
SSH プロトコルバージョン	ファイアウォール管理者は、「1 と 2 に対応」・「2 に限定」の 2 種類のバージョンを選択することができる。 「1 と 2 に対応」はプロトコルバージョン 1、または 2 で接続が可能となる。「2 に限定」はプロトコルバージョン 2 のみの接続が可能となる。 TOE の SSH プロトコルバージョンとして「2 に限定」を選択した状態で TOE を運用しなければならない。
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 SMTP 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 Flood	攻撃対象のホストに対してICMP Echo Request パケットを大量に送りつけるサービス停

	止攻撃の 1 つ。
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。
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	内部ネットワークに LAN 接続された TOE 範囲外の端末。 ファイアウォール管理者は管理端末上の Web ブラウザを用いて TOE の運用管理を行う。 システム管理者は管理端末上のリモートコンソールを用いて TOE の保守作業を行う。 TOE には、管理端末を 4 台まで登録することができ、すべての管理端末の管理はファイアウォール管理者が行う。
監査記録	TOE が生成した監査記録の集まりのことを指す。監査記録には、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、及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）が記録された監査記録を指す。 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、及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記録を指す。 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）に基づきアラート通知が必要であるかを判断され、必要であればファイアウォール管理者に対しアラート通知される。
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（監査記録ファイル設定）、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。
監査記録ファイル設定	監査記録のローテーションサイズ・監査記録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（Ping Flood 検出、SYN Flood 検出※1、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、システム管理者がコマンドにて収集した情報を採取する。 ※1 Ping Flood 検出、SYN Flood 検出の判定は不正アクセス対策ルールにおける判定と同じ。
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・タイプ・コード・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、及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」・「暗黙のルール」の 3 種類のルールがある。
不正アクセス対策ルール	不正アクセス対策レベル「ベーシック」に含まれる対策のうち、脅威への対策である Ping Flood と SYN Flood の2つを不正アクセス対策ルールとする。

	Ping Flood、SYN Flood は、パケットフィルタルールのセキュリティ属性であり、開発時に設定されるしきい値(パケットフィルタ機能固定値)を使用し実現される。
不正アクセス対策レベル	保証された構成とするために TOE の不正アクセス対策レベルとして、「ベーシック」を選択した状態で TOE を運用しなければならない。 「ベーシック」とは、Ping Flood 検知・SYN Flood 対策・traceroute 対策・IP Spoofing 対策を行う。 traceroute はパケットの破棄は行わないため、SFR の対象としない。
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。
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。
管理者情報	管理者情報は下記情報である。 ・ ファイアウォール管理者 ID、パスワード ・ システム管理者 ID、パスワード ・ ファイアウォール管理者、システム管理者が連続して認証に失敗した場合に識別認証機能のロックアウトを行う累積認証失敗回数 ・ ロックアウトを自動解除するまでの時間 下記は固定値であり変更できない。 ・ ファイアウォール管理者、システム管理者が連続して認証に失敗した場合に識別認証機能のロックアウトを行う累積認証失敗回数:600 秒以内に 2 回 ・ ロックアウトを自動解除するまでの時間:600 秒
しきい値	TOE 開発時に組み込まれるパケットフィルタルールのセキュリティ属性のひとつである。不正アクセス対策ルールで Ping Flood、SYN Flood の検出を実現するために使用する。
Traceroute 対策	traceroute コマンドから TOE の存在を隠蔽する。 Traceroute はパケットの破棄は行わないため、SFR の対象としない。
SYN Flood	攻撃対象のホストに対して SYN パケットを大量に送りつけるサービス停止攻撃の 1 つ。
ステートフルインスペクション	パケットに含まれる TCP フラグなどを参照し、パケットの時間的な前後関係まで追跡し、プロトコル仕様に基づく正当な手順を踏んだパケットか、手続きを装った不正なものか見極め、不正なパケットの受信を破棄する機能、および FTP プロトコルでやりとりされる制御情報を認識し、動的にデータ転送セッションの通信を許可する機能を提供する。
ステート	ステートフルインスペクション機能により判定されたパケットの状態。下記4つの状態がある。 INVALID: 既存のコネクションとは関係のないパケット NEW: 新しいコネクションの接続に関するパケット ESTABLISHED: 接続済みコネクションのパケット RELATED: 接続済みコネクションに関連して発生した新たなコネクションパケット
静的ルーティング	パケットのルーティング情報をあらかじめ設定しておくこと。静的ルーティングを設定する場合は、宛先ネットワークアドレス、ネットマスク、ゲートウェイの IP アドレスを設定する。静的ルーティングを設定しない場

	合、パケットの転送先が不明なパケットは、すべてデフォルトゲートウェイに転送される。
仮想ファイアウォール	標準のファイアウォール機能に加え、1 台で複数の仮想ファイアウォールを最大 12 まで追加可能。 各仮想ファイアウォールに独立したファイアウォールルールを設定することができ、それぞれ管理者を分けることも可能。 1 つの仮想ファイアウォールには 4 つのインタフェースまで割り当て可能。
AD 連携	Active Directory と連携し、利用者のログオン情報をもとに、アクセス制御を実施。また、通信ログに利用者名を記録することが可能。
仮想アプライアンス	従来、ハードウェア上で実現したファイアウォール SG を仮想環境上で構築可能にしたもの。仮想環境ネットワークの容易な構築と効率的な運用を実現する。

9 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 2012 年 9 月バージョン 3.1 改訂第 4 版 CCMB-2012-09-001 平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構技術本部 セキュリティセンター情報セキュリティ認証室
情報技術セキュリティ評価のためのコモンクライテリア パート 2: セキュリティ機能コンポーネント 2012 年 9 月バージョン 3.1 改訂第 4 版 CCMB-2012-09-002 平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構技術本部 セキュリティセンター情報セキュリティ認証室
情報技術セキュリティ評価のためのコモンクライテリア パート 3: セキュリティ保証コンポーネント 2012 年 9 月バージョン 3.1 改訂第 4 版 CCMB-2012-09-003 平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構技術本部 セキュリティセンター情報セキュリティ認証室
情報技術セキュリティ評価のための共通方法 評価方法 2012 年 9 月バージョン 3.1 改訂第 4 版 CCMB-2012-09-004 平成 24 年 11 月翻訳第 1.0 版 独立行政法人情報処理推進機構技術本部 セキュリティセンター情報セキュリティ認証室

NEC

更新履歴

バージョン	作成・更新日	更新概要	更新箇所
第 1.00 版	2016/2/18	初版	ー
第 1.01 版	2016/4/19	TOE 資産より「監査記録」を削除 評価対象に実装されていない「不正アクセス対策設定」についての記述を削除 評価で使用する IE のバージョンを 8 から 11 に変更	3.1.1 1.4.3.1、8 1.3.1.6
第 1.02 版	2016/4/27	日時情報の記述を統一 O.SECURITY_MANAGEMENT 定義更新 ステートフルインスペクション機能についての説明更新	3.1.1、表 14、 4.1 6.1.2、7.1.2、8
第 1.03 版	2016/5/23	ファイアウォールの設定情報 定義変更 O.SECURITY_MANAGEMENT 定義変更 FDP_IFC.1.1 定義変更	3.1.1 表 5、表 14 6.1.2
第 1.04 版	2016/5/25	OS 標準フィルタリング制御 定義変更 パケットフィルタリング機能 定義にステートフルインスペクション機能追記 仮想アプライアンス 用語集追加	1.4.3.2 1.4.3.2 8
第 1.05 版	2016/6/8	T.NETWORK_ACCESS 定義変更 FDP_IFC.1.1 定義変更 ステートフルインスペクション機能説明変更	表 3 6.1.2 7.1.2
第 1.06 版	2016/6/14	T.NETWORK_ACCESS 説明変更 T.INVALID_PACKET 追加 O.PACKET_FILTER 説明変更 O.INVALID_PACKET 追加 T.NETWORK_ACCESS セキュリティ対策方針根拠変更 FIA_UID.2 誤植修正	表 3 表 3、7、8 表 5 表 5、7、8 表 8 7.1.1
第 1.07 版	2016/6/16	FDP_IFC.1、および FDP_IFF.1 から特定不正パケットルール部分を分離	表 9、6.1.2、 表 11、表 13、 表 14、表 15、 表 16、7.1.2、8
第 1.08 版	2016/6/20	T.INVALID_PACKET 説明変更	表 3
第 1.09 版	2016/6/21	T.INVALID_PACKET 識別子に対応する脅威を明記 O.PACKET_FILTER 内容変更 O.INVALID_PACKET 識別子に対応するセキュリティ方針を明記 FDP_IFC.1.1a 定義変更 FDP_IFC.1.1b 定義変更 FDP_IFF.1.1.a 定義変更 FDP_IFF.1.1.b 定義変更 O.INVALID_PACKET セキュリティ機能要件根拠変更	表 3 表 5 表 5 6.1.2 6.1.2 6.1.2 6.1.2 表 14
第 1.10 版	2016/7/1	特定不正パケットの説明変更	8
第 1.11 版	2016/7/11	SSH で使用する暗号アルゴリズムを変更	7.1.1
第 1.12 版	2016/7/27	TOE バージョン更新 ガイダンス版数更新	全体 表 2
第 1.13 版	2016/8/2	O.PACKET_FILTER、O.INVALID_PACKET セキュリティ機能要件根拠変更	表 14

バージョン	作成・更新日	更新概要	更新箇所
第 1.14 版	2016/8/25	ガイダンス版数更新 不正アクセス対策レベル説明変更 特定不正パケット説明変更	表 2 8 8
第 1.15 版	2016/10/4	サイト共通ルールでは必ず監査記録を生成するよう変更 ガイダンス版数更新 IP Spoofing を脅威とするよう変更	1.4.3.2 表 8 表 1 表 2 表 4 表 7 6.1.2 表 12 7.1.2 8
第 1.16 版	2016/10/13	ガイダンス版数更新 Ping Sweep を Ping Flood に訂正	表 1 表 2 表 4 表 7 6.1.2 表 12 7.1.2 8
第 1.17 版	2016/10/19	ガイダンス版数更新 IP Spoofing を脅威より削除 しきい値の説明変更	表 1 表 2 表 4 表 7 6.1.2 表 12 7.1.2 8 8
第 1.18 版	2016/10/24	ガイダンス版数更新	表 1