認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成19年3月14日** (IT**認証**7140)
認証番号	C0155
認証申請者	**日本電気株式会社**
TOE**の名称**	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
PP**適合**	**なし**
適合する保証パッケージ	EAL1
開発者	**日本電気株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成20年4月25日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「NEC ファイアウォールSG コアユニット Ver. 1.0.0」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「NEC ファイアウォールSG コアユニット Ver. 1.0.0」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所　評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である日本電気株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　NEC ファイアウォールSG コアユニット
バージョン：　1.0.0
開発者：　日本電気株式会社

1.2.2 製品概要

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、通過しようとするIPパケットをパケットフィルタルールに基づいて検査し、その結果により通信の許可・拒否を決定することで、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ファイアウォール製品である。

本TOEは、NECファイアウォールSGに含まれ、通過しようとするIPパケットをパケットフィルタルールに基づいて検査し、その結果により通信の許可・拒否を決定する機能を提供する。本TOEが提供するセキュリティ機能を以下に示す。

・ 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

なお、以下の機能は本TOEに含まれるが評価対象外である。
・流入量制限機能
・SSH機能

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの範囲及び動作環境

本TOEは、ファイアウォール製品であるNEC ファイアウォールSGに含まれる、通過しようとするIPパケットをパケットフィルタルールに基づいて検査し、その結果により通信の許可・拒否を決定する機能を提供する部分である。本TOEの動作環境概要を図1-1に示す。

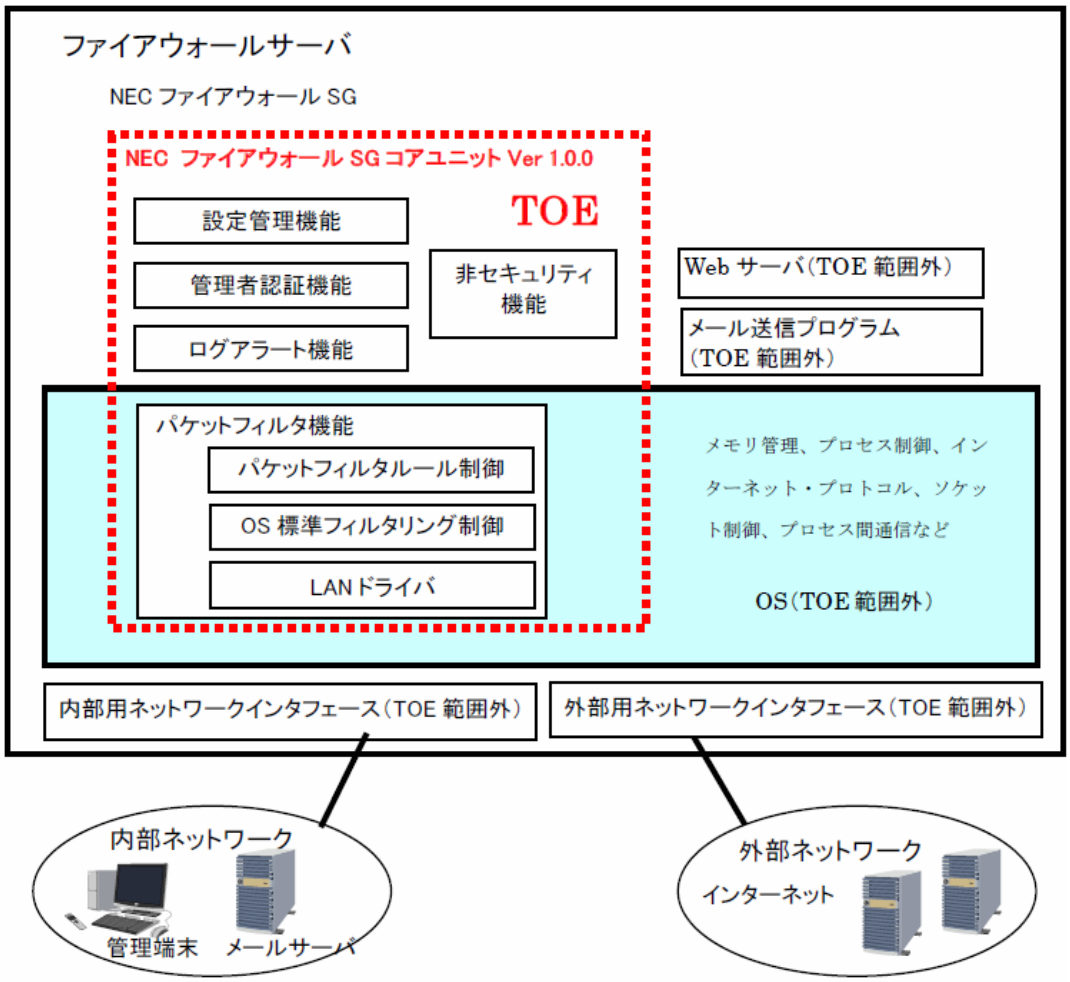

図1-1 TOEの動作環境概要

本TOEの動作に関わる構成要素の役割を以下に示す。

【ファイアウォールサーバ】（TOEを搭載）
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であり、ファイアウォールとして動作するために必要なOS、Webサーバ、メール送信プログラム等のソフトウェアがインストールされているサーバ。
許可されたもののみ入室可能で、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。

【OS】（一部がTOE）
本TOEを動作させるための基盤となるソフトウェア。
OSが提供するOS標準フィルタリング制御及びOSが周辺機器を制御するための橋渡しを行うLANドライバは、パケットフィルタ機能の一部として本TOE内に組み込まれる。

【管理端末】（TOE範囲外）
Webブラウザを用いて本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接続された端末。

【Webサーバ】（TOE範囲外）
管理端末から本TOEへの各種設定要求を仲介し、その結果をWebブラウザに提示するために使用されるソフトウェア。

【メール送信プログラム】（TOE範囲外）
本TOEが、セキュリティ侵害の可能性を検知した場合に、その事実をメールにより通知するために使用されるソフトウェア。

【メールサーバ】（TOE範囲外）
本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接続されたサーバ。

【内部ネットワーク】（TOE範囲外）
本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】（TOE範囲外）
内部ネットワークに接続するためのデバイス。内部ネットワークからの通信、及び内部ネットワークへの通信を受け渡す。

【外部ネットワーク】（TOE範囲外）
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。

【外部ネットワークインタフェース】（TOE範囲外）
外部ネットワークに接続するためのデバイス。外部ネットワークからの通信、及び外部ネットワークへの通信を受け渡す。

1.2.3.2 TOEの動作概要

本TOEは、内部ネットワーク及び外部ネットワーク上の端末から利用される。図1-1に示す動作環境において、本TOEは以下のとおりTOE以外のソフトウェア等と連動する。

① 本TOEの管理者は、内部ネットワーク上の管理端末上のWebブラウザを用いて、TOE外のWebサーバを介して本TOEへアクセスし、IDとパスワードによる識別・認証を経た上で、パケットの通過・拒否を行うためのパケットフィルタルールの設定、監査記録の設定、イベント発生時のアラート通知の設定を行う。
② 内部ネットワークや外部ネットワーク上の端末からの本TOEを経由した通信は管理者により設定済みのパケットフィルタルールに従ってフロー制御される。また、管理者により設定済みのイベントが発生した場合は、監査記録の取得や管理者へのアラート通知のためのメールが作成される。
③ アラート通知のためのメールは、本TOEがTOE外のメール送信プログラムを用いて送信し、内部ネットワーク上のTOE外のメールサーバを経由して管理端末に送信する。これにより管理者はアラート通知を受け取ることができる。

1.2.3.3 TOEに関係する利用者役割

本TOEに関係する利用者とその役割を以下に示す。

【ファイアウォール管理者】
ファイアウォール管理者は、管理端末のWebブラウザから本TOEに接続し、管理機能を用いて、本TOEの運用管理を行う。
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。

【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。

【一般利用者】
内部ネットワークや外部ネットワーク上の端末から、本TOEが動作するファイアウォールサーバを介して、他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。

【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。

【システム管理者】
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。
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。

1.2.4 TOEの機能

本TOEが保持する機能は、セキュリティ機能と非セキュリティ機能に分類される。図1-1に示す機能の本TOEが保持するセキュリティ機能を表1-1に、本TOEが保持する非セキュリティ機能（評価対象外の機能を含む）を表1-2に示す。なお、本TOEが提供する機能は、OSの起動により開始され、OSの停止により終了する。

表1-1　TOEのセキュリティ機能

セキュリティ機能	概要
設定管理機能	TOEの動作環境を設定する機能。 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。
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IDとパスワードにより識別認証する機能。
パケットフィルタ機能	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パケットを検査し、通過・拒否の処理を行う機能。 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 以下にそれぞれの概略を示す。 ①不正アクセス対策ルール： 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る。TOEのインストール時に指定される不正アクセス対策レベルに応じた内容が設定される。 ②管理端末接続ルール： 管理端末からの通信を許可するためのIPアドレスを定義するパケットフィルタルールである。TOEのインストール時に指定された管理端末からの通信を許可する。 ③サイト共通ルール： ファイアウォール管理者により、通過・拒否する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。ファイアウォール管理者は、TOE運用中に設定・変更することができる。 ④暗黙のルール： 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る。TOEのインストール時に設定され、ファイアウォール管理者であっても変更はできない。 パケットフィルタルールは①→②→③→④の順に検査され、IPパケットの内容と合致するルールが現れるまで検査が行われる。最終的にはすべてのIPパケットを破棄する④暗黙のルールが存在することにより、全体として明示的に指定されたIPパケットのみ通過を許可する制限的なルールを構成している。
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。 ログ格納機能： 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機能。

	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。 アラート通知機能： 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機能。

表1-2　TOEの非セキュリティ機能（評価対象外の機能を含む）

非セキュリティ機能	概要
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。
SSH機能	ファイアウォールの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。
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。
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。

1.3　評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。
(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
(3) 本TOEがセキュリティ設計に基づいて開発されていること。
(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「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 Ver. 1.34」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「NEC ファイアウォールSGコアユニット Ver.1.0.0 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年4月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL1適合である。

1.5.3 セキュリティ機能強度

本TOEの保証レベルは、EAL1であるため、AVA_SOF.1は含まれない。そのため、SOFを宣言する必要は無い。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能については、「1.2.4TOEの機能」を参照。

1.5.5 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3　想定する脅威

識別子	脅　威
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。

1.5.6　組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針はない。

1.5.7　構成条件

TOEが稼動するファイアウォールサーバに要求されるソフトウェア条件は以下のとおりである。

・OS： RedHat Enterprise Linux カーネルバージョン2.4.21-32.0.1.ELsmp
・Webサーバ： wbmchttpd(Apache) 1.3.27
・メール送信プログラム： Sendmail 8.12.11

TOEが稼動するための直接のソフトウェア条件ではないが、TOEを利用する管理端末に要求されるソフトウェア条件は以下のとおりである。

・OS： Microsoft Windows XP SP2
・Web ブラウザ： Internet Explorer 6.0 SP2
・メールクライアント： 特に指定なし

1.5.8　操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-4に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-4　TOE使用の前提条件

識別子	前提条件
A.SAFE_PLACE（安全な場所）	TOE及び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、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・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、及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、及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、及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、及びファイアウォール管理者は、TOE 及び 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。

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。

1.5.9 製品添付ドキュメント

本TOEの使用において提供されるガイダンスを以下に示す。

・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 Ver.1.4 2008/3/24
・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 Ver.1.7 2008/3/24

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成19年3月に始まり、平成20年4月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年1月及び2月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

本TOEでは、開発者テストは評価対象外である。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの環境を図2-1に、TOEの動作に関係する各構成要素についてのハードウェアの要件を表2-1、ソフトウェアの要件を表2-2、評価者テストに使用するツールの要件を表2-3に示す。

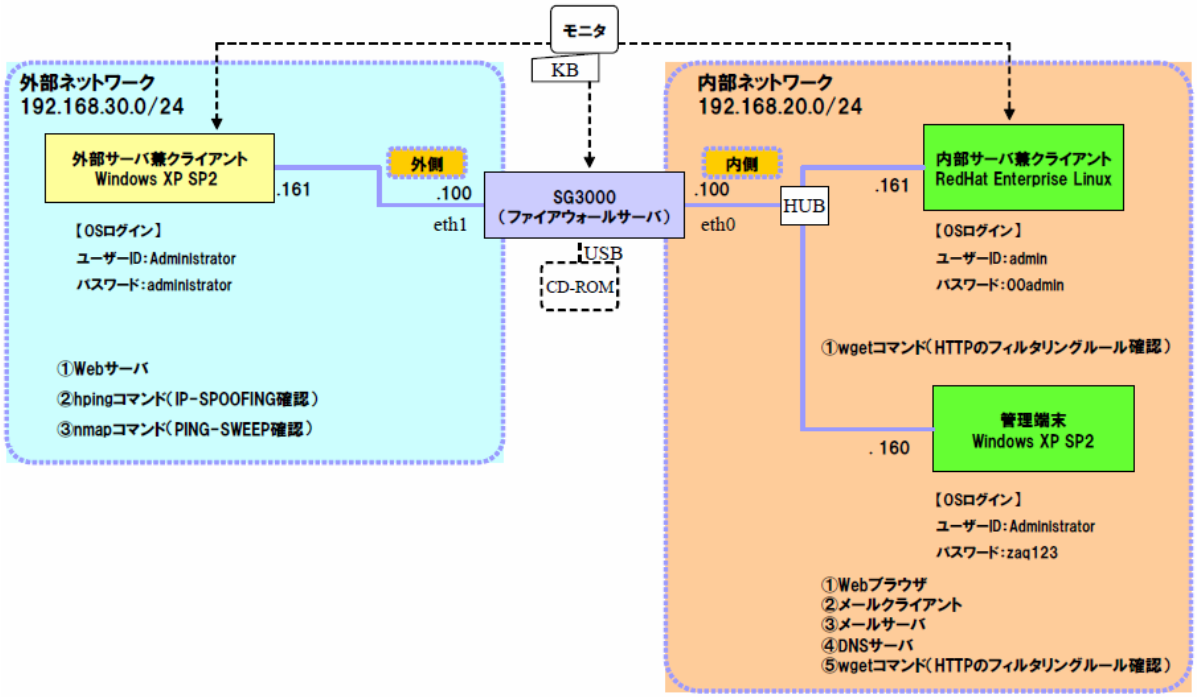

図2-1　評価者テストの環境

表2-1　評価者テストの環境における各構成要素のハードウェア要件

分類	メーカ	品番/型番等
ファイアウォールサーバ（外付けCD-ROM Reader）	NEC	UNIVERGE SG3000LG／ BTO125-002
	NEC	UJDB763X-NE
管理端末	NEC	PC-VA93JBHZH
外部サーバ兼クライアント	NEC	PC-MY30VBTESEDD
内部サーバ兼クライアント	NEC	110Rd-1 N8100-842
モニタ	NEC	MultiSync LCD1760V
KB（キーボード）	NEC	RT2900 128560-001
HUB（ハブ）	Allied Telesis	CentreCOM FH716XL
USBメモリ	NEC	Lumitas 128MB

表2-2　評価者テストの環境における各構成要素のソフトウェア要件

分類		名称	品番/型番等
ファイアウォールサーバ	OS	RedHat Enterprise Linux	カーネルバージョン 2.4.21-32.0.1.ELsmp
	TOE	NEC ファイアウォール SG コアユニット	1.0.0
	メール送信プログラム	sendmail	8.12.11
	Webサーバ	wbmchttpd(Appach)	1.3.27
管理端末	OS	Microsoft Windows XP	SP2
	Webブラウザ	Microsoft Internet Explorer	Version 6 SP2
	メールクライアント	Microsoft Office Outlook 2003	SP2

表2-3　評価者テストで使用するツール要件

分類		名称	品番/型番等
管理端末	メールサーバ	BlackJumboDog	4.0.7
	DNSサーバ	BlackJumboDog	4.0.7
	Telnet/SSHサーバ	PuTTY	Release 0.58-jp
外部サーバ兼クライアント	OS	Microsoft Windows XP	SP2
	Webサーバ	BlackJumboDog	4.0.7
	パケット送信ツール	hping	2.0.0-b1 Support for XP SP2
	ポートスキャンツール	nmap	V.3.00
内部サーバ兼クライアント	OS	RedHat Enterprise Linux	カーネルバージョン 2.4.21-32.0.1.ELsmp
	HTTP通信ツール	wget	1.9

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1に、TOEの動作に関係する各構成要素についてのハードウェアの要件を表2-1、ソフトウェアの要件を表2-2、評価者テストに使用するツールの要件を表2-3に示す。評価者テストはSTにおいて識別されているTOE構成を満たすテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①Webブラウザ、パケット送信ツール、HTTP通信ツール、ポートスキャンツールを用いて外部インタフェースからセキュリティ機能に刺激（パラメータ）を与え、外部インタフェースの表示、生成される監査記録、アラート通知メールの情報を参照してセキュリティ機能のふるまいを目視確認する。

c.実施テストの範囲

評価者が独自に考案した計13項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① STに識別されているセキュリティ機能要件に対応するセキュリティ機能は基本的にテストする。
② TOEの種別に一般的に関係する、知られている公知の弱点を持つセキュリティ機能をテストする。
③ 重要性及び複雑性を持つセキュリティ機能をテストする。
④ 異なるタイプのインタフェースを持つセキュリティ機能をテストする。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL1に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。

構成管理	適切な評価が実施された
ACM_CAP.1.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。

AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_IND.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.1.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用されたTOE特有の略語を以下に示す。

HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Security
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
OS	Operating System
SSH	Secure SHell
SSL	Secure Sockets Layer

本報告書で使用された用語を以下に示す。

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

ICMP	Internet Control Message Protocol の略。IP による通信を制御するためのもの。
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。
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。
IP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。
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。TOE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。
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。
SSH	Secure SHellの略。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。
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。
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Webブラウザに提示するために使用されるソフトウェア。
OS	TOEを動作させるための基盤となるソフトウェア。
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。
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。

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。
暗黙のルール	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る。TOEのインストール時に設定され、ファイアウォール管理者であっても変更はできない。
一般利用者	内部ネットワークや外部ネットワーク上の端末から、TOEが動作するファイアウォールサーバを介して、他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。
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、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。
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。
外部ネットワークインタフェース	外部ネットワークに接続するためのデバイス。外部ネットワークからの通信、及び外部ネットワークへの通信を受け渡す。
管理端末	Web ブラウザを用いて本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接続された端末。
管理端末接続ルール	管理端末からの通信を許可するためのスを定義するパケットフィルタルールである。TOEのインストール時に指定された管理端末からの通信を許可する。
サイト共通ルール	ファイアウォール管理者により、通過・拒否する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。ファイアウォール管理者は、TOE 運用中に設定・変更することができる。

システム管理者	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。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。
内部ネットワーク	本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	内部ネットワークに接続するためのデバイス。内部ネットワークからの通信、及び内部ネットワークへの通信を受け渡す。
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。
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・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」・「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。
ファイアウォール管理者	ファイアウォール管理者は、管理端末のWebブラウザから本TOEに接続し、管理機能を用いて、本TOEの運用管理を行う。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。
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。
ファイアウォールサーバ	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であり、ファイアウォールとして動作するために必要なOS、Webサーバ、メール送信プログラム等のソフトウェアがインストールされているサーバ。許可されたもののみ入出可能で、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。

不正アクセス対策ルール	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る。TOEのインストール時に指定される不正アクセス対策レベルに応じた内容が設定される。
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。
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。
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。
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。
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接続されたサーバ。
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、その事実をメールにより通知するために使用されるソフトウェア。
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。
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。

6 参照

[1] NEC ファイアウォールSG コアユニット セキュリティターゲット Ver. 1.34（2008年3月24日）日本電気株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 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 バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 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 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 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 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] NEC ファイアウォールSGコアユニット Ver.1.0.0 評価報告書 第1.7版 2008年4月9日 株式会社電子商取引安全技術研究所　評価センター