認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成28年4月1日 (IT認証6599)
認証番号	C0533
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ソフトウェア
TOEのバージョン	3.0.1
PP適合	なし
適合する保証パッケージ	EAL1及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
開発者	日本電気株式会社
評価機関の名称	みずほ情報総研株式会社 情報セキュリティ評価室

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28年12月9日

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
技術管理者　山里　拓己

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 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 バージョン3.1 リリース4
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「NECファイアウォールSGソフトウェア」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、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

この認証報告書は、日本電気株式会社が開発した「NEC ファイアウォール SG ソフトウェア、バージョン 3.0.1」（以下「本 TOE」という。）についてみずほ情報総研株式会社情報セキュリティ評価室（以下「評価機関」という。）が平成 28 年 11 月 2 日に完了した 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とともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書とともに提供されるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を購入する調達者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL1 及び追加の保証コンポーネント ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、ハードウェアとソフトウェアの一体型のファイアウォール製品「NEC ファイアウォール SG」のソフトウェア全体である。ハードウェア部分は含まない。

本 TOE は、管理者の許可していないネットワーク通信を遮断するパケットフィルタ機能と、管理者以外の者が不正に設定管理を行うことを防止する機能、及びそれらの監査機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本 TOE は、以下の脅威を想定しており、それに対抗するセキュリティ機能を提供する。

管理者の許可していないネットワーク通信は、不正アクセスをはじめとする悪影響を及ぼす恐れがある。そのため本 TOE は、あらかじめ設定されたパケットフィルタルールに従って、本 TOE が中継する IP パケットの通過と破棄を制御するパケットフィルタ機能を提供する。

本 TOE のパケットフィルタルール等の設定を行う管理機能は、管理者以外の者に不正に操作される恐れがある。そのため本 TOE は、管理機能の操作を正当な管理者に制限する識別認証機能と、管理者が本 TOE を操作する際の通信データを暗号化する通信保護機能を提供する。

また、それらのセキュリティ機能の運用を支援する監査機能を提供する。

1.1.2.2 構成要件と前提条件

本 TOE は、次のような構成及び前提で運用することを想定する。

- 本 TOE を搭載したファイアウォール装置は、2 つのネットワークを接続する唯一の接点であるようなネットワーク構成で使用される。
- 本 TOE を搭載したファイアウォール装置は、物理的な不正アクセスから保護された環境に設置される。

1.1.3 免責事項

本評価では、「7.5 評価構成について」の設定条件が適用された構成だけが TOE として評価されている。そのため、公開サーバ用の独立したネットワークセグメントやアドレス変換の使用など、設定条件と異なる構成は、本評価による保証の対象外である。

本 TOE は、一般に破棄することが推奨されている「レコードルート」オプションの指定された IP パケットについて、それを破棄する機能を提供していない。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 28 年 11 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。また、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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。

2 TOE識別

本 TOE は、以下のとおり識別される。

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

本 TOE は､ハードウェアとソフトウェアの一体型のファイアウォール製品｢NEC ファイアウォール SG｣のソフトウェア部分である。

製品が評価･認証を受けた本 TOE であることを､利用者はインストール媒体のラベルで確認することができる。上記の識別情報が付与されたインストール媒体を使って導入したソフトウェアが、評価･認証された本 TOE である。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、本 TOE を導入する組織の管理するネットワーク（これを「内部ネットワーク」という。）と、インターネットのように、内部ネットワークとは管理方針の異なるネットワーク（これを「外部ネットワーク」という。）を接続する際に、その境界に設置されるファイアウォール装置のソフトウェアである。

本 TOE は、あらかじめ本 TOE に設定されたパケットフィルタルールに従って、本 TOE が中継する IP パケットの通過と破棄を制御することで、管理者の許可していないネットワーク通信を遮断する。

さらに本 TOE は、本 TOE の管理機能を操作する管理者を識別認証し、管理者が本 TOE を操作する際の通信データに暗号通信プロトコルを適用することで、本 TOE の提供する管理機能が第三者によって不正に操作されることを防止する。

本 TOE は、管理者として以下の役割を想定している。他の利用者役割はない。

・ファイアウォール管理者
　本 TOE の設定管理を行う。

・システム管理者
　本 TOE の保守作業を行う。

3.1 セキュリティ機能方針

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1　想定する脅威

識別子	脅威
T.NETWORK_ACCESS (内部ネットワークへの不正アクセス)	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。

識別子	脅威
T.INVALID_PACKET (特定不正パケットによるアクセス)	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。 注)「特定不正パケット」とは、インターネットプロトコルの規約に従っていないパケットや、一般に悪用防止のために破棄することが推奨されているパケットである。ただし、レコードルートのオプションが指定されたIPパケットは含まれていない。詳細は「11 用語」を参照。
T.TOE_ACCESS (TOEへの不正アクセス)	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。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。なお、各セキュリティ機能の詳細は、5 章に示す。

⑴ 脅威「T.NETWORK_ACCESS」への対抗

本 TOE は「パケットフィルタ機能」で本脅威に対抗し、「ログアラート機能」でその運用を支援する。

本 TOE の「パケットフィルタ機能」は、本 TOE が中継する IP パケットに対して、以下の制御を行う。

- 本 TOE に設定されたパケットフィルタルールに従って、本 TOE が中継する IP パケットの通過と破棄を制御する。
- Ping Flood、SYN Flood を検出した場合には、しきい値を超えたパケットを破棄する。

本 TOE の「ログアラート機能」は、パケットフィルタ機能の監査記録を格納する。さらに、設定された監査イベントが発生した場合には、電子メール等によりファイアウォール管理者に通知する。

⑵ 脅威「T.INVALID_PACKET」への対抗

本 TOE は「パケットフィルタ機能」で本脅威に対抗する。

本 TOE の「パケットフィルタ機能」は、特定不正パケットを破棄する。

なお、本 TOE では、特定不正パケットの破棄の場合は、ファイアウォール管理者による特別な管理は必要としないという考え方がされており、監査記録は生成されない。

(3) 脅威「T.TOE_ACCESS」への対抗

本 TOE は「設定管理機能」で本脅威に対抗し、「ログアラート機能」でその運用を支援する。

本 TOE の「設定管理機能」は、識別認証の成功したファイアウォール管理者とシステム管理者だけに、本 TOE の設定管理機能と保守のための機能の使用を許可する。さらに、暗号通信プロトコルを使用し、識別認証に使用するパスワードの盗聴を防止する。これらの機能により、本 TOE はファイアウォール管理者やシステム管理者以外の者が、ファイアウォールの設定情報を改ざんすることを防止する。

本 TOE の「ログアラート機能」は、設定管理機能の監査記録を格納する。さらに、設定された監査イベントが発生した場合には、電子メール等によりファイアウォール管理者に通知する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

本 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。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 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4-1 前提条件

識別子	前提条件
A.APPOINT	TOEを運用管理する組織の責任者は、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ければならない。
A.SAFE_PLACE	ファイアウォール管理者は、TOEを搭載したファイアウォール装置を、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。
A.NO_BYPASS	ファイアウォール管理者は、TOEを搭載したファイアウォール装置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。
A.PASSWORD_MANAGEMENT	ファイアウォール管理者及びシステム管理者は、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。
A.SAFE_TERMINAL	ファイアウォール管理者は、管理端末が、不正に使用されたり、不正なソフトウェアをインストールされたりしないように、管理しなければならない。 注）本評価では、管理端末は1台だけが接続できるように制限されている。システム管理者の保守作業は、ファイアウォール管理者の管理する管理端末を使用する。
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い、それ以外の作業を行ってはならない。

4.2 運用環境と構成

本 TOE を搭載したファイウォール装置は、外部ネットワークと内部ネットワークの境界に設置される。ファイアウォール管理者及びシステム管理者は、内部ネットワークの管理端末から本 TOE の運用管理と保守を行う。本 TOE の一般的な運用環境を図 4-1 に示す。

図 4-1 TOE の運用環境

図 4-1 で、本 TOE は、NEC ファイアウォール SG に搭載されているソフトウェア全体である。TOE の運用環境の構成品について以下に示す。

(1) NEC ファイアウォール SG（ハードウェア部分）

本 TOE を動作させるための専用ハードウェアである。本評価では、以下のモデルを使用する。

・NEC SG3600LJ

(2) 管理端末

本 TOE の設定管理及び保守作業のために使用する PC である。ファイアウォール管理者は、管理端末の Web ブラウザを使用して設定管理を行い、システム管理者は、管理端末の SSH クライアントを使用して保守作業を行う。本評価では、以下のソフトウェアを使用する。

・OS: Windows 7
・Web ブラウザ: Internet Explorer 11
・SSH クライアント: SSH プロトコルバージョン 2 対応ソフトウェア

また、本評価では、管理端末は 1 台だけが接続可能である。

(3) メールサーバ

本 TOE のログアラート機能で、電子メールによる通知を設定した場合に必要である。

なお、本構成に示されているハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本 TOE の提供するセキュリティ機能には以下の制約がある。

- PING Flood や SYN Flood は、しきい値を用いて判定される（詳細は「11 用語」を参照）。判定条件に合致する IP パケットは、正当な通信であっても PING Flood や SYN Flood とみなされ破棄されるので、本 TOE の管理者は注意が必要である。なお、本 TOE は、しきい値を変更する機能は提供していない。
- 特定不正パケットが破棄された場合は、監査記録は生成されない。本 TOE では、特定不正パケットが破棄された場合、管理者による特別な管理は必要としないという考え方がされている。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

本 TOE は NEC ファイアウォール SG のソフトウェア全体である。本 TOE は以下のセキュリティ機能とその他の機能を提供する。

・セキュリティ機能：パケットフィルタ機能、設定管理機能、ログアラート機能
・その他の機能：リモートメンテナンス機能

リモートメンテナンス機能は、本 TOE の保守のための機能であり、評価対象のセキュリティ機能ではない。

以下、本 TOE のセキュリティ機能について説明する。

(1) パケットフィルタ機能

本機能は､本 TOE が中継する IP パケットの通過と破棄を制御する機能である。制御内容の概要は以下のとおりである。

・特定不正パケットを検出した場合には、無条件に破棄する。

・Ping Flood、SYN Flood を検出した場合には、しきい値を超えたパケットを破棄する。

・本 TOE に設定されたパケットフィルタルールに従って、TOE が中継する IP パケットの通過と破棄を制御する。その際、送信パケットと応答パケットの関係に着目して以下の処理を行う。（これを「ステートフルインスペクション機能」という。）

- TCP、UDP、ICMP の送信を許可すると、その応答パケットは自動的に許可される。

- 許可された送信パケットに対して、宛先経路が存在しない等の ICMP エラーが送信元に返却された場合、その ICMP エラーの通知パケットは、応答パケットの場合と同様に自動的に許可される。

- FTP プロトコルの場合、制御コネクションを許可すると、データ転送のコネクションは自動的に許可される。

(2) 設定管理機能

本機能には、管理者認証機能、通信保護機能、及びセキュリティ機能の設定管理機能が含まれている。

①管理者認証機能

本機能は、ファイアウォール管理者とシステム管理者を、それぞれの ID とパスワードで識別認証する機能である。識別認証は以下のインタフェースに適用される。

・ファイアウォール管理者：管理端末(Web ブラウザ)からの本 TOE 利用
・システム管理者：管理端末(SSH クライアント)からの本 TOE 利用

識別認証を補強するために、本 TOE は以下の機能を備えている。

・600 秒以内に 2 回連続して識別認証に失敗した場合は、識別認証を 600 秒間停止する。

②通信保護機能

本機能は、管理端末と本 TOE との間の通信に、暗号通信プロトコルを適用する機能である。使用する暗号通信プロトコルは以下のとおりである。

・管理端末(Web ブラウザ)：TLS 1.2
・管理端末(SSH クライアント)：SSH バージョン 2

③セキュリティ機能の設定管理機能

本機能は、識別認証の成功したファイアウォール管理者が、本 TOE のセキュリティ機能で使用する設定データを管理する機能である。対象となる設定データは以下のとおりである。

・パケットフィルタルール
・ログアラート機能の設定
・ファイアウォール管理者の ID とパスワード
・システム管理者の ID とパスワード
・日時

(3) ログアラート機能

本機能には、ログ格納機能とアラート通知機能が含まれている。

①ログ格納機能

本機能は、パケットフィルタ機能及び設定管理機能に関する監査記録を格納する機能である。ただし、特定不正パケットが破棄される場合は、監査記録は生成されない。格納領域が満杯の場合には、最も古い監査記録が上書きされる。

ファイアウォール管理者は、格納された監査記録の読み出しと削除が可能である。

②アラート通知機能

本機能は、ログ格納機能で格納される監査記録を監視し、アラート通知するように設定された監査イベントが発生した場合には、アラートを通知する機能である。通知方法としては、電子メール送信や任意のコマンドの実行等が設定可能である。

5.2 IT環境

本 TOE は、NEC ファイアウォール SG のハードウェア上で動作する。

ログアラート機能で電子メールによる通知を設定した場合、アラート通知のために、本 TOE はメールサーバに電子メールを送信する。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。本 TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

・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

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報セキュリティ評価室は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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た。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 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 28 年 4 月に始まり、平成 28 年 11 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 28 年 8 月から 10 月に、評価機関内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。

7.4 製品テスト

評価者は、評価の過程で示された証拠を検証した結果から、必要と判断された評価者独立テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

本評価において、開発者テストは保証要件には含まれない。

7.4.2 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることを確認するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成を図 7-1 に示す。

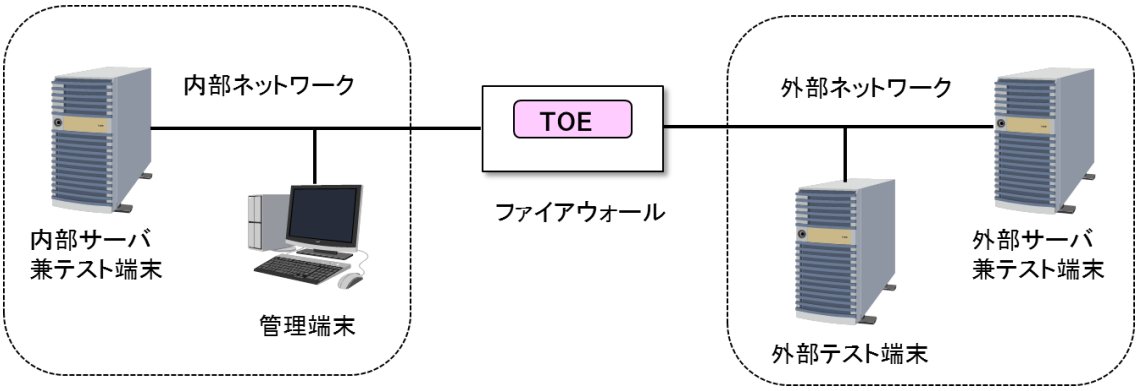

図7-1　独立テストの構成図

独立テストの構成要素を表 7-1 に示す。

表7-1　独立テストの構成要素

名称	詳細
ファイアウォール (TOE搭載)	TOEを搭載したファイアウォール装置 ・ソフトウェア (TOE) : NECファイアウォールSGソフトウェア バージョン3.0.1 ・ハードウェア : NEC SG3600LJ
管理端末	TOEの管理端末として使用 ・Windows7 Professional SP1搭載PC ・Webブラウザ: Internet Explorer 11 ・SSHクライアント: OpenSSH_7.2p2

名称	詳細
内部サーバ兼 テスト端末	内部ネットワーク上のサーバ及びテスト用端末として使用 ・Red Hat Enterprise Linux Server release 6.2搭載PC (Kernel 2.6.32-220.el6.i686) ・メールサーバ: Postfix 2.6.6 ・テストツール（表7-2参照）
外部サーバ兼 テスト端末	外部ネットワーク上のサーバ及びテスト用端末として使用 ・Red Hat Enterprise Linux Server release 6.2搭載PC (Kernel 2.6.32-220.el6.i686) ・テストツール（表7-2参照）
外部テスト端末	外部ネットワーク上のテスト用端末として使用 ・CentOS Linux release 7.2搭載PC (Kernel 3.10.0-327.13.1.el7.x86_64) ・テストツール（表7-2参照）

評価の対象の TOE は、2 章の TOE 識別と同一である。また、各構成要素は、IPv4 と IPv6 の両方の場合がテストされている。

独立テストは、本 ST において識別されている TOE の構成と同じ環境で実施された。なお、独立テスト環境の構成品やテストツールの妥当性確認及び動作試験は、評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者は、すべての外部インタフェースとセキュリティ機能を確認するという方針のもと、以下の観点で独立テストを考案した。

＜独立テストの観点＞

① すべてのセキュリティ機能とインタフェースを確認する。

② パケットフィルタ機能で特別な処理を行うすべての条件を確認する。

③ 特定不正パケット等とは異なるパケットに、特定不正パケット等の場合の特別な処理が適用されないことを確認する。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

TOE の外部インタフェースについて、管理端末からの入力や、各種のテストツールを使用して通信データの送受信を行い、そのふるまいの確認を行った。ふるまいの確認には、入力に対する応答やテストツールの出力、監査記録、ネットワーク上の通信データが用いられた。

＜独立テストツール＞

独立テストにおいて利用したツールを表 7-2 に示す。

表7-2　独立テストで使用したツール

機器	ツール名称	概要・利用目的
内部サーバ兼テスト端末	Webサーバ、DNSサーバ、FTPサーバ、SSHサーバ（OSに付属）	各種プロトコル（HTTP、DNS、FTP、SSH）のテストに使用
	Nmap Version 7.12	様々な構成のパケットの送出に使用
	FTester Version 1.0	ファイアウォールのフィルタリング動作を検査する。外部サーバ兼クライアント上のFTesterとペアで使用して、指定されたパケットの送信と受信を行い、両者の記録を比較する。
外部サーバ兼テスト端末	SSHサーバ（OSに付属）	SSHプロトコルのテストに使用
	FTester Version 1.0	ファイアウォールのフィルタリング動作を検査する。内部サーバ兼クライアント上のFTesterとペアで使用して、指定されたパケットの送信と受信を行い、両者の記録を比較する。
	cURL Version 7.19.7-26	HTTPプロトコルの送受信に使用
	Wget Version 1.12	
	hping3 Version 3.0.0-alpha-1	TCPプロトコルのSYNやACKなどのフラグを任意の値に設定したパケットを生成し送出する
	synk4 Release 1997/04/29	SYN Floodの送出に使用
	Nmap Version 7.12	SYN Scanの送出に使用
外部テスト端末	Nmap Version 7.12	様々な構成のパケットの送出に使用
	Scapy Version 2.3.2	様々な構成のパケットの送出に使用（Nmapでは生成することが困難なパケットをテストする場合に使用）

各テスト端末共通	tcpdump（OSに付属）	ネットワーク上のパケットを取得し、確認するために使用
	dig，ping，ping6，ftp，telnet, ssh（OSに付属）	各種プロトコル（DNS、ICMP Echo、FTP、TELNET、SSH）の送受信に使用

＜独立テストの実施内容＞

独立テストは、評価者によって 17 項目実施された。

独立テストの観点とそれに対応した主なテスト内容を表 7-3 に示す。

表7-3　実施した主な独立テスト

観点	テスト概要
観点①	・ファイアウォール管理者とシステム管理者について、識別認証、アカウントロック、暗号通信プロトコルが仕様どおりに動作することを確認した。 ・ファイアウォール管理者に提供されている管理機能が、仕様どおりに動作することを確認した。 ・監査記録の格納、格納領域が満杯時の動作、アラート通知が、仕様どおりに動作することを確認した。
観点②	・パケットフィルタルールの設定のとおりに、パケットの通過と破棄が制御されることを確認した。 ・TCP、UDP、ICMPの応答パケットが、仕様どおりに自動的に制御されることを確認した。 （許可された送信パケットの応答待ちの場合のみ、応答パケットの通過が許可される。） ・FTPのデータ転送が、仕様どおりに自動的に制御されることを確認した。 ・Ping Flood、SYN Floodが、仕様どおりに破棄されることを確認した。 ・すべての特定不正パケットが仕様どおりに破棄されることを確認した。
観点③	・SYN Scanが、Ping FloodやSYN Floodとは異なり、破棄されないことを確認した。 ・レコードルートオプションの指定されたIPパケットが、特定不正パケットとは異なり、破棄されないことを確認した。 ・IPv6経路制御ヘッダで、タイプ0以外のタイプが指定された場合は、特定不正パケットとは異なり、破棄されないことを確認した。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① TOEの管理画面にWebアプリケーションの各種脆弱性が存在する可能性がある。

② TOEに組み込まれているOS等のソフトウェアに脆弱性が存在する可能性がある。

③ 電源オン直後の初期化処理において、パケットフィルタ機能が有効になるまでの間に、許可されていないパケットが通過する可能性がある。

④ TOEのTCPプロトコルの状態管理が厳格でない場合、TCPのハンドシェイクを悪用し、許可されていないパケットが通過する可能性がある。

⑤ 不正なパケットを処理中にTOEが予期しない状態に陥る可能性がある。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは、独立テストの環境に検査用 PC を追加した環境で実施した。検査用 PC は、Windows7 Professional SP1 を搭載した PC である。

侵入テストで使用したツールの詳細を表 7-4 に示す。

表7-4　侵入テストで使用したツール

ツール名称	概要・利用目的
Burp Suite Version 1.7.03	Webデバッガ。WebブラウザとWebサーバ(TOE)の間の通信を仲介し、その間の通信データの参照と変更を行う
OWASP zap Version 2.5.0	Webアプリケーションの脆弱性診断ツール
XSS Me Version 0.4.6	Webアプリケーションのクロスサイトスクリプティング脆弱性の診断ツール
Nessus Version 6.7.0	セキュリティスキャナ（脆弱性データベースは2016年7月29日時点で最新のもの）
ISIC Version 0.07	ファイアウォールのIPプロトコルスタック（IP, ICMP, TCP, UDP）の安定性を検査するツール
Wireshark Version 2.0.2	ネットワーク上のパケットを収集し、プロトコルを解析するツール。Web関連のテストで使用
fakestack.rb	TCPのハンドシェイクを悪用する攻撃を行うプログラム

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-5 に示す。

表7-5　侵入テスト概要

脆弱性	テスト概要
脆弱性①	・WebブラウザやWebデバッガを使用して、攻撃として知られている文字列をTOEに入力しても、攻撃が成功しないことを確認した。 ・OWASP zap、XSS MeをTOEに実施し、公知の脆弱性がないことを確認した。
脆弱性②	・NessusをTOEに実施し、公知の脆弱性がないことを確認した。
脆弱性③	・TOEの停止時からパケットを連続的に送出し、その状態でTOEの電源をオンにしても、破棄対象のパケットが通過しないことを確認した。
脆弱性④	・TCPのハンドシェイクを悪用するパケットを送出しても、攻撃パケットが通過しないことを確認した。
脆弱性⑤	・ISICを使用して、正常及び異常なパケットをランダムに大量に生成し送出しても、TOEが正常に動作することを確認した。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5 評価構成について

本評価で評価されたネットワーク構成は、「7.4.2 評価者独立テスト」の図 7-1 に示す構成である。IPv4 と IPv6 の両方の構成が含まれている。

また、評価された TOE の構成条件は表 7-5 のとおりである。

表7-5　TOEの構成条件（設定値）

設定項目	設定値
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 (1 台の物理的なファイアウォール装置上で、仮想的に複数のファイアウォールを実現する機能)	なし
AD連携 (Active Directoryと連携し、利用者のアクセスを制御する機能)	なし
DMZ (「DeMilitarized Zone: 非武装地帯」の略。公開サーバ用の独立したネットワークセグメントのこと)	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 (「Management Console」はTOEの設定管理機能を提供するツール)	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	1台だけを登録

TOE を、上記とは異なる構成や設定値で運用する場合には、本評価による保証の対象ではない。

7.6 評価結果

評価者は、評価報告書をもって本 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。

評価では以下について確認された。

・セキュリティ機能要件：　コモンクライテリア　パート２　適合
・セキュリティ保証要件：　コモンクライテリア　パート３　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

・EAL1 パッケージのすべての保証コンポーネント
・追加の保証コンポーネント　ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 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 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

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。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL1 及び追加の保証コンポーネント ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 に対する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の制約事項や評価対象範囲が、各自の想定する運用条件に合致しているかどうか注意が必要である。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

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, 2016 年 10 月 24 日, 日本電気株式会社

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された用語の定義を以下に示す。

特定不正パケット　インターネットプロトコルの規約に従っていないパケットや、一般に悪用防止のために破棄することが推奨されているパケットであり、下記のパケットが該当する。
- 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

Ping Flood	大量のICMP Echo Requestパケットを送付するサービス停止攻撃。本TOEでは、1件/200msを上回るペースでICMP Echo Requestパケットを受信し、5件まで保持可能なキューがあふれた場合、Ping Floodと判定し、キューからあふれたICMP Echo Requestパケットを破棄する
SYN Flood	大量のTCP SYNパケットを送付するサービス停止攻撃。本TOEでは、1件/100msを上回るペースでSYNパケットを受信し、1024件まで保持可能なキューがあふれた場合、SYN Floodと判定し、キューからあふれたSYNパケットを破棄する
SYN Scan	TCP SYNパケットを利用して、TCPの接続を確立せずに、TCPのポートが開いているかどうかを調べる行為。本TOEは、SYN Scanを破棄する特別な機能は提供していない

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 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3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[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, 2012年9月, CCMB-2012-09-002, (平成24年11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, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 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3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] 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, 2016年10月24日, 日本電気株式会社

[13] NECファイアウォールSGソフトウェア Ver.3.0.1 評価報告書, 第2版, 2016年11月2日, みずほ情報総研株式会社 情報セキュリティ評価室