認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日(受付番号)	**平成18年10月10日(IT認証6105)**
認証番号	C0088
認証申請者	**富士通株式会社**
TOE**の名称**	IPCOM EX**シリーズ ファームウェア セキュリティ コンポーネント**
TOE**のバージョン**	V1.0.00
PP**適合**	**なし**
適合する保証要件	EAL1
TOE**開発者**	**富士通株式会社**
評価機関の名称	**社団法人 電子情報技術産業協会 ITセキュリティセンター**

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19年3月22日

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
技術管理者　田渕　治樹

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

「IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、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、「IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（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富士通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: IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント
バージョン: V1.00.00
開発者: 富士通株式会社

1.2.2 製品概要

本TOEは、複数のネットワークの境界点に位置し、あるネットワークから受信した通信パケットを、事前に定められた規則（フィルタリングルール）に従って、別ネットワークへ配送、又は破棄するIPパケットフィルタリング機能を提供するファームウェアである。本機能により、外部ネットワーク上の通信リソースを利用できる利点を活かしながら、不正アクセスなどの脅威から、内部ネットワーク上の通信リソースを保護することができるようになる。

1.2.3 TOEの範囲と動作概要

TOEは、ファイアウォール装置であるIPCOM EXシリーズのファームウェアであり、以下のコンポーネントで構成される。このコンポーネントは、セキュリティ コンポーネントとして版数管理される。

- ●IPパケットフィルタリング
- ●運用支援
- ●環境設定

IPCOM EXシリーズ ファームウェアとして以下のコンポーネントも提供されるが、本TOEの対象外である。

- ●システムの二重化制御（装置の二重化機能、LAN二重化機能）
- ●経路制御（RIP、OSPF、FNAルーティング、他）
- ●暗号通信（IPSec-VPN機能、SSL-VPN機能、SSLアクセラレータ機能、認証機能）
- ●アドレス変換
- ●サーバ負荷分散
- ●リンク負荷分散
- ●QoS制御（帯域制御機能）
- ●簡易サーバ（DNSサーバ機能、DHCPサーバ機能）

本ファームウェアは、専用ハードウェア装置の不揮発性メモリ領域に格納される。

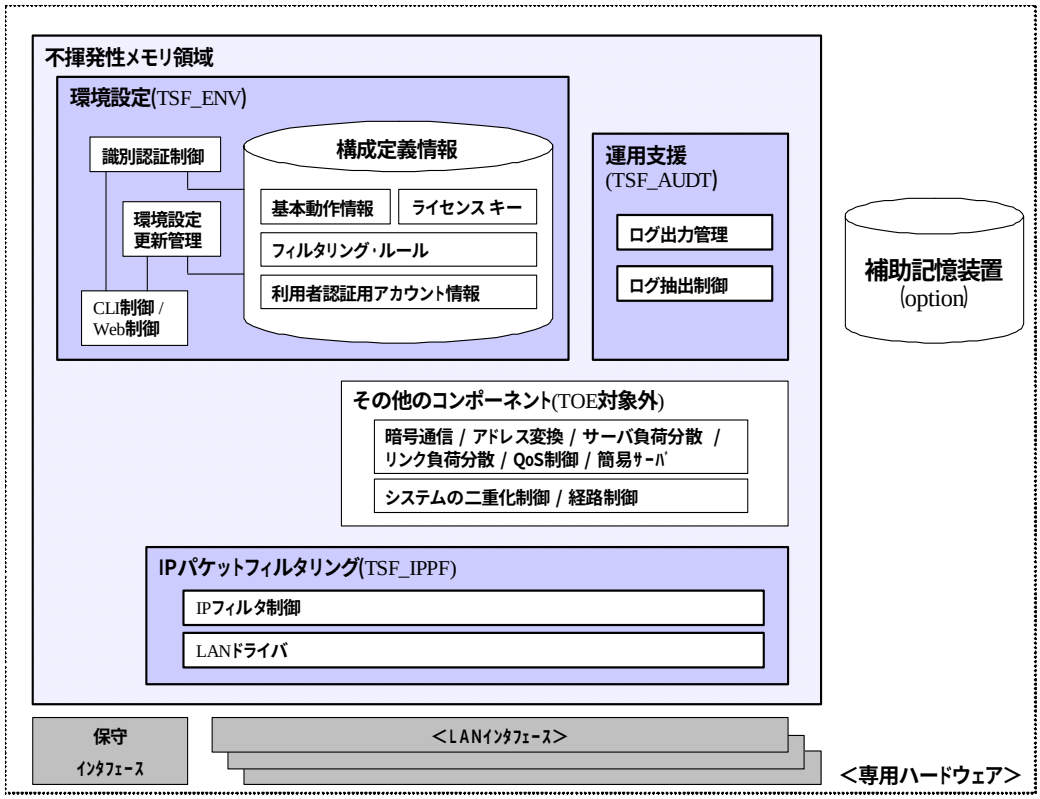

図 1-1　　TOE の物理構成

そして本TOEを動作させるハードウェア装置は、複数のネットワークの境界点に位置し、以下のようなネットワーク構成になる。

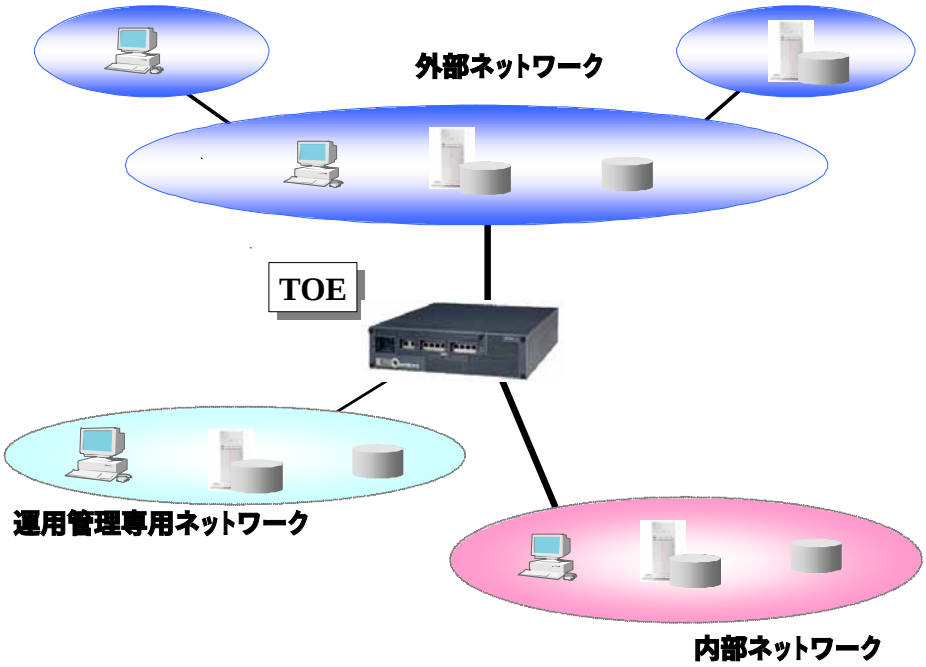

図 1-2　　TOE のネットワーク構成

上記のネットワーク構成では、外部ネットワークと内部ネットワークにおいて、相互のIPアドレス体系を隠蔽しない運用を想定している。

例えば、外部ネットワークがグローバルIPアドレス体系（インターネット）であれば、内部ネットワークもグローバルIPアドレス体系（インターネット）で運用する（SCモデルで想定されるネットワーク環境である）。また、外部ネットワークがプライ ベートIPアドレス体系（イントラネット）であれば、内部ネットワークもプライベート IPアドレス体系（イントラネット）で運用する（SLBモデルで想定されるネット ワーク環境である）。

運用管理専用ネットワークは、TOEの管理通信セグメントに利用し、外部ネットワーク および内部ネットワークと通信できない独立したネットワークとして構築する。

1.2.4　　TOEの機能

TOEが持つ機能を以下に示す。

（1）環境設定(TSF_ENV)

TSF_ENVは、TOEの動作環境を設定する機能を提供する。保守インタフェースか、IPパケットフィルタリング(TSF_IPPF)でパケット通過を設定したLANインタフェースに保守端末を接続することで、本TOEに通信することができる。本TOEに通信開始後、利用者識別認証が実行され、許可されたTOE管理者であれば、TOEの構成定義情報を設定または変更することができる。設定された構成定義情

報は、構成定義情報の有効化操作により、IPパケットフィルタリング(TSF_IPPF)や運用支援(TSF_AUDT)に配布される。

（2）IPパケットフィルタリング(TSF_IPPF)

TSF_IPPFは、複数のLANインタフェース間で送受信されるIPパケットデータを評価し、通過または破棄の処理を行う。LANインタフェースから取得したIPパケットデータは、配布された構成定義情報に基づき、通過と判断したIPパケットデータだけ受信（内部転送）が許可される。通過と判断され受信が許可されたIPパケットデータは、その他のコンポーネント（TOE 対象外）に内部転送され、経路制御により中継先のLANインタフェースが特定され、IPパケットフィルタリング(TSF_IPPF)に戻される。IPパケットフィルタリング(TSF_IPPF)は、経路制御で特定されたLANインタフェースを利用してIPパケットデータを送信する。

（3）運用支援(TSF_AUDT)

TSF_AUDT は、通過または破棄のパケット処理記録や、TOEの動作結果となる監査記録を保管および退避する機能を提供する。 環境設定(TSF_ENV)やIPパケットフィルタリング(TSF_IPPF)から受け取ったロギング情報を、環境設定(TSF_ENV)で定義された方法でTOEの補助記憶装置(Option)に格納、または、指定された手段で監査記録を遠隔装置に転送する。

TOE に格納された監査記録は、保守端末を利用して参照または、全削除が許可される。なお、監査記録を遠隔装置に転送する場合も、IPパケットフィルタリング(TSF_IPPF)による評価が実施されるため、IPパケットフィルタリング指定で明示的に送信を許可(指定遠隔装置宛ての通信を許可)していなければならない。

● ログ出力管理

TOEを動作させるハードウェア装置に補助記憶装置（Option）が増設されている場合、この補助記憶装置にロギング情報を格納する。 また、遠隔関連装置へのイベント通知が指定されていれば、その装置にロギング情報をイベントとして転送する。 両方の定義が有効であれば、補助記憶装置（Option）に格納後、遠隔関連装置にもイベント転送する。

● ログ退避制御

TOEを動作させるハードウェア装置に補助記憶装置（Option）が実装されている場合、この補助記憶装置に格納されているロギング情報を参照する機能を提供する。

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セキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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「IPCOM EX シリーズ ファームウェア セキュリティ コンポーネント セキュリティターゲット」（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及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書C、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・製造・出荷環境が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、「IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント 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19年3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

STはAVA_SOF.1を含まないため、最小機能強度を主張しない。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

（1）環境設定(TSF_ENV)

TSF_ENVは、TOEの動作環境を設定する機能を提供する。保守インタフェースか、IPパケットフィルタリング(TSF_IPPF)でパケット通過を設定したLANインタフェースに保守端末を接続することで、本TOEに通信することができる。本TOEに通信開始後、利用者識別認証が実行され、許可されたTOE管理者であれば、TOEの構成定義情報を設定または変更することができる。設定された構成定義情報は、構成定義情報の有効化操作により、IPパケットフィルタリング(TSF_IPPF)や運用支援(TSF_AUDT)に配布される。

（2）IPパケットフィルタリング(TSF_IPPF)

TSF_IPPF は、複数のLANインタフェース間で送受信されるIPパケットデータを評価し、通過または破棄の処理を行う。LANインタフェースから取得したIPパケットデータは、配布された構成定義情報に基づき、通過と判断したIPパケットデータだけ受信（内部転送）が許可される。通過と判断され受信が許可されたIPパケットデータは、その他のコンポーネント（TOE 対象外）に内部転送され、経路制御により中継先のLANインタフェースが特定され、IPパケットフィルタリング(TSF_IPPF)に戻される。IPパケットフィルタリング(TSF_IPPF)は、経路制御で特定されたLANインタフェースを利用してIPパケットデータを送信する。

（3）運用支援(TSF_AUDT)

TSF_AUDTは、通過または破棄のパケット処理記録や、TOEの動作結果となる監査記録を保管および参照する機能を提供する。 環境設定(TSF_ENV)やIPパケットフィルタリング(TSF_IPPF)から受け取ったロギング情報を、環境設定(TSF_ENV)で定義された方法でTOEの補助記憶装置(Option)に格納、または、指定された手段で監査記録を遠隔装置に転送する。

TOEに格納された監査記録は、保守端末を利用して参照または、全削除が許可される。なお、監査記録を遠隔装置に転送する場合も、IPパケットフィルタリング(TSF_IPPF)による評価が実施されるため、IPパケットフィルタリング指定で明示的に送信を許可(指定遠隔装置宛ての通信を許可)していなければならない。

● ログ出力管理

TOEを動作させるハードウェア装置に補助記憶装置（Option）が実装されている場合、この補助記憶装置にロギング情報を格納する。 また、遠隔関連

装置へのイベント通知が指定されていれば、その装置にログング情報をイベントとして転送する。 両方の定義が有効であれば、補助記憶装置（Option）に格納後、遠隔関連装置にもイベント転送する。

● ログ退避制御

TOEを動作させるハードウェア装置に補助記憶装置（Option）が実装されている場合、この補助記憶装置に格納されているロギング情報を参照する機能を提供する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.1	･外部ネットワークから内部ネットワークへの不正アクセス 外部ネットワークの攻撃者は、内部ネットワークに侵入し、内部ネットワークの資産の不正使用、改ざん、破壊、又は漏洩を図る恐れがある。
T.2	･TOEへの不正アクセスによるTOE関連資産の改ざん 外部ネットワークまたは内部ネットワーク上の攻撃者は、本TOEに侵入し、構成定義情報を改ざんして不正なIPパケットデータやIP通信サービスを通過可能にする恐れがある。また、ロギング情報を改ざん、または、破壊し、不正行為の証拠を隠滅する恐れもある。

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存在しない。

1.5.7 構成条件

本セキュリティーターゲットは富士通株式会社製の以下の製品のファームウェアとして標準実装され、提供される。

● 富士通　IPCOM-EX1000 SCモデル
● 富士通　IPCOM-EX1200 SCモデル
● 富士通　IPCOM-EX2000 SCモデル
● 富士通　IPCOM-EX1000 SLBモデル
● 富士通　IPCOM-EX1200 SLBモデル

● 富士通　IPCOM-EX2000 SLBモデル

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1-3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1-2　TOE使用の前提条件

識別子	前提条件
ASM.1 **(物理的アクセス)**	TOEを動作させるハードウェア装置および保守端末は、物理的に不正アクセスできない。
ASM.2 **(接続形態)**	TOEを動作させるハードウェア装置は、内部ネットワークと外部ネットワークまたは、内部ネットワークと内部ネットワークを唯一の接点で接続する形態でネットワークを構築する。
ASM.3 **(信頼できる**TOE**管理者)**	TOE管理者およびTOE監査者は、TOEおよびTOEを動作させるハードウェア装置に関して不正をしない。
ASM.4 **(**TOE**の構成の管理)**	TOE管理者は、TOEが正しく動作するよう、TOEおよびTOEを動作させるハードウェア装置を運用管理しなければならない。
ASM.6 **(データ漏洩不可)**	関連装置および運用管理専用ネットワークから、TOE関連資産となるデータは漏洩しない。
ASM.8 **(時刻同期サーバ)**	時刻同期サーバは、信用できる。
ASM.SYSLOG **(ロギング情報)**	ロギング情報を格納する補助記憶装置(Option)をTOEが動作するハードウェアに実装するか、ログの維持監視機能を持つSyslogサーバを設置する。
ASM.SLB **(**SLB**モデル)**	IPフィルタ制御の例外動作は、制限的（遮断）で運用する。

1.5.9　製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

日本語マニュアル	
1	IPCOM EX シリーズ E10L10ユーザーズガイド 2006年11月第2版
2	IPCOM EX シリーズ E10L10　コマンド リファレンス ガイド 2006年11月第2版
3	IPCOM EX シリーズ E10 L10コンソール リファレンス ガイド 2006年11月第2版
4	IPCOM EX シリーズ E10L10　事例集 2006年11月第2版
5	IPCOM EX シリーズ E10L10　保守ガイド 2006年11月第2版
6	IPCOM EX1000/EX1200/EX2000　E10 取扱説明書［C120-E321-01] 2006年9月初版
7	IPCOM EX1000/EX1200/EX2000　E10L10 ソフトウェア説明書 2007年3月

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18年10月に始まり、平成19年3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18年12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 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構成を以下に示す。

TOE管理者端末は、MNTポートにてTOEの初期設定をした後、管理ネットワークに接続しリモートにてTOEの設定を行った。

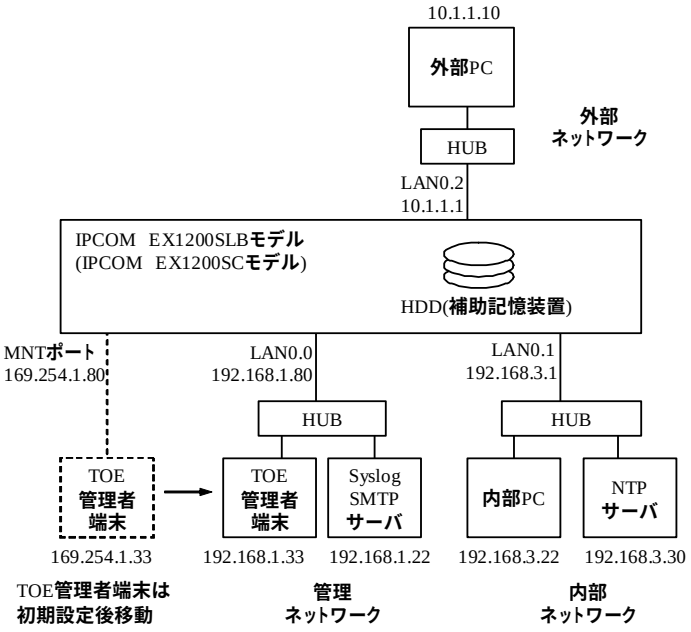

図2-1　評価者テスト構成

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に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

内容としてはST に記載されたTOEセキュリティ機能は全て網羅したテストを考案した。

c.実施テストの範囲

本TOE では複雑なセキュリティ機能や革新的で一般的ではないセキュリティ機能は存在しないため「セキュリティ機能の重要性」に着目しテストを実施する。その結果、評価者は以下の合計21項目のテストを考案した。

・環境設定機能(SFP_ENV)：12項目

・IPパケットフィルタリング機能(SFP_IPPF)：5項目

・運用支援機能(SFP_AUD)：4項目

これらのテストは1 項目をテストすることにより、複数のTOE 機能がテストされる。例えば、IPパケットフィルタリング機能をテストする場合、フィルタリングを設定するための環境設定機能も同時にテストされ、更にログ情報も記録されることから運用支援機能もテストされる。

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

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識別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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、機能拡張要件が適切に定義されていることを確認している。保証要件はCCの範囲内であるため、対象外である。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、機能拡張要件の依存性が全て識別されていることを確認している。保証要件はCCの範囲内であるため、対象外である。

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り、上位レベル設計が機能仕様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用語を以下に示す。

内部ネットワーク	本TOEにより、外部ネットワークからのセキュリティの脅威に対して保護されるネットワーク・セグメント。それぞれの組織内部のイントラネット・セグメント、サーバ管理通信専用の運用管理専用ネットワーク・セグメント及び、インターネットに情報を公開するために設置された公開セグメント（DMZ：De-Militarized Zone 非武装セグメント）が「内部ネットワーク」に該当する。
運用管理専用ネットワーク	サーバ管理通信専用として独立させたネットワーク・セグメント。
外部ネットワーク	組織のセキュリティポリシーが及ばないインターネットや、自部門と異なる方針で運営管理されているイントラネットのネットワーク・セグメントで、保護対象となる内部ネットワーク以外のネットワーク・セグメント。
保守端末	TOEの運用～監査～保守において、TOE管理者またはTOE監査者が利用する専用端末。
コマンド操作端末	TOEとの通信にSSHプロトコルやTelnetプロトコルを利用し、コマンド形式(CLI)で操作する保守端末。

Webブラウザ端末	TOEとの通信にHTTPSプロトコルを利用し、Webブラウザ形式(GUI)で操作する保守端末。
システム運用管理部門	組織に属する内部ネットワークの運用管理責任を担う部署。
TOE管理者	TOEの設置～運用～監査～保守に渡って、本TOE及び運用管理専用ネットワークの運用全般の管理責任を担う管理者。主に、システム運用管理部門で策定されたセキュリティポリシーに基づき、本TOEの構成定義情報を設定し、セキュリティポリシーを具体化する。本TOEのユーザ認証機能では、管理者権限クラスがTOE管理者に該当する。
TOE監査者	TOEの運用～監査を担い、TOE管理者を補佐する副管理者。TOE 管理者より権限が低く、本TOEの運用状況監視権限が許可され、本TOEの構成定義情報を変更する権限を持たない。本TOEのユーザ認証機能では、オペレーター権限クラスがTOE監査者に該当する。
編集モード	TOE管理者の権限に対する現在のステータスを意味する。このステータスには、通常モードと編集モードが存在し、編集モードは通常モードの権限を包含し、TOEを設定変更できる状態を意味する。
利用者	内部ネットワークに接続され、外部ネットワークにアクセスするユーザ、及び外部ネットワークに接続され、内部ネットワークにアクセスするユーザ。
IPパケットデータ	内部ネットワークと外部ネットワーク間で、送受信されるデータ
内部セキュリティポリシー	システム運用管理部門が設定する内部ネットワークのセキュリティ方針であり、フィルタリングルールで実現される。
フィルタリングルール	内部セキュリティポリシーを具体化したルール。フィルタリングルールは、フィルタリング条件の組み合わせから構成される。
フィルタリング条件	IPパケットデータを内部ネットワークと外部ネットワーク間で通過／遮断するための条件
構成定義情報ファイル	フィルタリング条件などの動作条件が列挙された構成定義

	情報を退避したファイル。
ロギング情報	TOEの監査記録において、任意の実行結果を意味する。 また、関連装置にロギング情報を転送する場合、イベント転送と表現する。
ロギング情報ファイル	TOEの監査記録において、格納または保存されたロギング情報の集まりを意味する。

6 参照

[1] IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント バージョン 2.5（2007年3月12日）富士通株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成18年9月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-05

[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] IPCOM EXシリーズ ファームウェア セキュリティ コンポーネント 評価報告書 第1.6版 2007年3月14日
社団法人 電子情報技術産業協会 ITセキュリティセンター