認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成23年5月20日 (IT認証1351)
認証番号	C0330
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	V2.0.01
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	富士通株式会社
評価機関の名称	一般社団法人 ITセキュリティセンター 評価部

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23年11月29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３
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

この認証報告書は、富士通株式会社が開発した「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、V2.0.01」（以下「本 TOE」という。）について一般社団法人 IT セキュリティンター 評価部（以下「評価機関」という。）が平成 23 年 11 月 10 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富士通株式会社に報告するとともに、本 TOE に関心を持つ消費者や調達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、本書の付属書であ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、市販される本 TOE が搭載された統合型ネットワークサーバ IPCOM EX を購入する一般消費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、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、または破棄する「IP パケットフィルタリング機能」を提供する、IPCOM EX のファームウェア内の、ファイアーウォールモジュールである。

本 TOE は、上記の「IP パケットフィルタリング機能」の他、識別・認証された管理者のみがセキュリティ機能に関する設定を行える「環境設定管理機能」、IP パケットデータの破棄や通過などのイベントを監査証跡として記録する「運用支援管理機能」などのセキュリティ機能を提供する。

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､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

組織内部のイントラネット・セグメント、およびインターネットに情報を公開するため設置された公開セグメント（以下「内部ネットワーク」という）に対して、インターネットや異なる方針で運営管理されているイントラネット・セグメント（以下､「外部ネットワーク」という）から、不正な IP パケットデータを用いた、内部セキュリティポリシーにおいて許可されていないアクセスなどの脅威がある。

この脅威に対抗するために、本 TOE は、「IP パケットフィルタリング機能」を提供する。

また､本TOEを設置した際には､本TOEへの許可されていない侵入によるセキュリティに影響する設定情報の改ざんの脅威もある。

この脅威に対抗するために、本 TOE は、TOE 管理者の識別認証、TOE 設定データに対するアクセス制御等の機能を提供する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

TOE を動作させるハードウェア装置は、不正な物理的アクセスから保護されるセキュアなエリアに設置すること。

TOE を動作させるハードウェア装置は、外部ネットワークと内部ネットワークを接続する唯一の接続点としてネットワークを構成すること。

本 TOE の監査記録であるロギング情報を格納するため、TOE が動作するハードウェアに補助記憶装置を実装するか、TOE と通信する Syslog サーバを設置すること。

1.1.3 免責事項

本 TOE は IPCOM EX シリーズ ファームウェア内の「IP パケットフィルタリング機能」と、その設定や監査証跡の記録に関連した特定のコンポーネントである。

IPCOM EX シリーズには、TOE 以外にも IPS や Web アプリケーション・ファイアーウォールなど複数のセキュリティ機能が実装されているが、それらは TOE の範囲外であるため、本評価による保証はされない。

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 セキュリティ認証申請手続等に関する規程」[1]、「IT セキュリティ評価機関承認申請手続等に関する規程」[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 23 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。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。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[3][4][5]または[6][7][8]）及び CEM（[9][10]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：	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：	V2.0.01
開発者：	富士通株式会社

TOE は IPCOM EX1100/EX1300/EX2000A/EX2500 のファームウェアに含まれる IP パケットフィルタリングを実現するモジュールである。

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

TOE にログイン後、「IPCOM EX1100/EX1300/EX2000A/EX2500 ソフトウェア説明書」に記載された手順に従い、show system information コマンドを実行することで、TOE のバージョンを確認することができる。

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 の保護資産は以下のものである。TOE は、内部ネットワークへの接続制限を行う IP パケットフィルタリング、識別認証された正当な管理者にのみ TOE へのアクセスを許可することにより、保護資産に対する脅威に対抗する。

●内部ネットワーク資産

外部ネットワークからアクセスされる可能性がある、内部ネットワークの運用管理部門が定めた内部セキュリティポリシーによって特定される、内部ネットワーク上の資産である。

●TOE 設定データ（構成定義情報）

本 TOE の動作を決定する定義情報であり、内部ネットワーク上の資産を保護する内部セキュリティポリシーを保証するための関連資産になる。ネットワーク環境情報、フィルタリングルール、管理者認証用アカウント情報などが該当する。

IPCOM EX 内の不揮発性メモリに格納される。

●ロギング情報（監査記録）

本 TOE の動作状況や処理結果を記録する情報であり、内部ネットワーク上の資産に対する侵害発生有無を監査するための関連資産になる。

IPCOM EX に実装された補助記憶装置、または関連装置である Syslog サーバに格納される。

また､TOE へのアクセスが許可される管理者には以下の 2 つの役割が存在する。

●システム管理者

TOE の設置～運用～監視～保守に渡って、本 TOE 及び、本 TOE などの機器管理のために独立させた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内部セキュリティポリシーに基づき、本 TOE の構成設定情報を設定し、内部セキュリティポリシーを具体化する。

●システム監視者

TOE の運用～監視を担い、システム管理者を補佐する副管理者。

システム管理者と同様に､本 TOE の運用状況の監視権限は付与される｡ただし､システム管理者とは異なり、本 TOE の構成定義情報を変更する権限を持たない。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗する。

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.ATTK （外部ネットワークから内部ネットワークへの許可されないアクセス）	外部ネットワークの攻撃者は、外部ネットワークから内部ネットワーク上のサーバのIP アドレスや、アプリケーションが使用するポートなどに対して、内部セキュリティポリシーでは許可されていないアクセスを図る恐れがある。
T.CNFD （TOE への許可されないアクセスによるTOE 関連資産の改ざん）	外部ネットワーク上の攻撃者は、本TOEに侵入、または盗聴し、TOEの設定データである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。内部ネットワーク上の利用者は、誤って構成定義情報やロギング情報の変更や消去を行う恐れがある。

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。

(1) 脅威「T.ATTK」への対抗

本脅威に対して TOE は「IP パケットフィルタリング機能」、「運用支援管理機能（監査記録管理機能）」で対抗する。

「IP パケットフィルタリング機能」により、システム管理者が事前に定めた IP パケットのフィルタリングルールに則って、IP パケットデータを破棄、または通過させる。

「運用支援管理機能」により、TOE は TOE で発生した事象の監査証跡を記録する。システム管理者及びシステム監視者は監査証跡を分析することにより、許可されていない内部ネットワークへの接続要求を検出することができる。

(2) 脅威「T.CNFD」への対抗

本脅威に対して TOE は「環境設定管理機能」、「運用支援管理機能（監査記録管理機能）」で対抗する。

「環境設定管理機能」により、TOE はシステム管理者・システム監視者を識別認証し、構成定義情報やロギング情報の参照を正当なシステム管理者・システム監視者に許可する。また、システム管理者にのみ構成定義情報の設定及び変更が許可される。

「運用支援管理機能」により、識別認証操作を監査証跡に記録することで、TOE に対する許可されない侵入の可能性を検出することが可能となる。

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を運用する際の物理的前提条件を表 4-1、人的前提条件を表 4-2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 物理的前提条件

識別子	前提条件
A.DACC 物理的アクセス	TOEを動作させるハードウェア装置、保守端末、構成定義情報やロギング情報を転送する関連装置（Syslogサーバ、FTPサーバ）は、物理的に不正アクセスできない。
A.CNCT 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。
A.SYSLOG ロギング情報	ロギング情報を格納する補助記憶装置をTOEが動作するハードウェアに実装するか、ロギング情報の維持監視機能を持つSyslogサーバなどを設置する。

表 4-2 人的前提条件

識別子	前提条件
A.ADMN 信頼できるシステム管理者	システム管理者およびシステム監視者は、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。
A.SSET TOEの構成の管理	システム管理者は、内部セキュリティポリシーに従って、TOE、およびTOEを動作させるハードウェア装置、TOEの構成定義情報を運用管理しなければならない。

識別子	前提条件
A.SMRL データ漏洩不可	関連装置（Syslogサーバ、FTPサーバ）、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。 【本前提条件を達成するには以下の手順が必要となる。】 システム管理者は、関連装置を設置する運用管理専用ネットワークを、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設定する。 また、システム管理者及びシステム監視者が、運用管理専用ネットワークからTOE設定情報や関連装置のデータを持ち出さないよう、組織として内部セキュリティポリシーを設定する。
A.SLB LBシリーズの設定	IP パケットフィルタ制御の例外動作は、制限的（パケット拒否）で運用する。 【本前提条件を達成するには以下の手順が必要となる。】 IPCOM EXのソフトウェアプラットフォームがLBの場合、IPパケットフィルタ制御の例外動作の初期設定がパケット通過を許可する設定となっているため、導入時にシステム管理者は「IPCOM EX1100/EX1300/EX2000A/EX2500 ソフトウェア説明書」に記載されている手順に従い、設定を変更する。 なお、LB以外のソフトウェアプラットフォームでは、初期設定がパケット通過を拒否する設定となっているため、変更の必要は無い。
A.TMM 時刻設定	システム管理者は、本TOEが動作するハードウェア装置に実装されたシステムクロック（内部時計）にシステム運用に先立ち時刻を設定しなければならない。

4.2 運用環境と構成

本 TOE 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、システム管理者・システム監視者は運用管理専用ネットワークの保守端末から TOE の運用管理を行う。

本 TOE の一般的な運用環境を図 4-1 に示す。

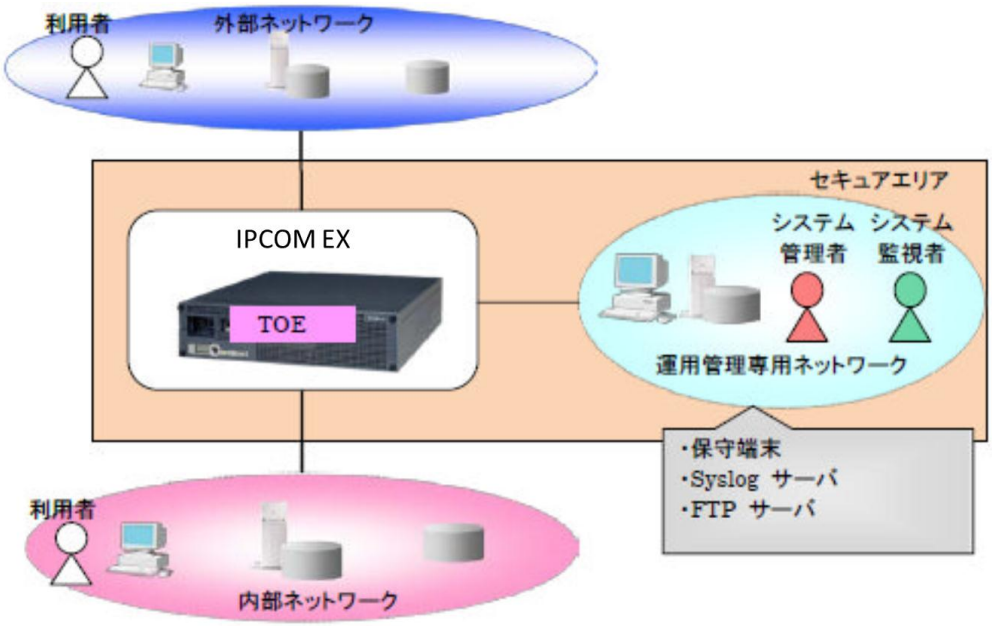

図 4-1 TOEの運用環境

(1) IPCOM EX

TOE が動作する IPCOM EX にはそれぞれ 4 種類のハードウェアプラットフォーム、ソフトウェアプラットフォームが存在する。

各ハードウェアプラットフォーム間では、通信用 LAN インターフェース数や、オプションである電源二重化装置の有無が異なる。

ソフトウェアプラットフォームとは、TOE の機能とは別に、帯域制御やサーバ負荷分散機能などを提供するソフトウェアである。なお、いずれのソフトウェアプラットフォームにおいても、TOE を含むファームウェアは同一のバイナリである。

ハードウェアプラットフォームとソフトウェアプラットフォームの組み合わせは以下の表 4-3 に示す 14 通りが存在し、消費者が自身の利用環境に合わせて選択可能である。

組み合わせごとに、監査証跡を記録するための補助記憶装置が標準装備されているものと、オプションとして消費者が実装の選択が可能なものが存在するため、補助記憶装置を実装しない場合には、消費者は後述の Syslog サーバを設置する必要がある。

表 4-3 ハードウェア・ソフトウェアプラットフォームの組み合わせ

ハードウェア プラットフォーム	ソフトウェア プラットフォーム	補助記憶装置
IPCOM EX 1100	SC	オプション
	NW	オプション

	LB	標準装備
IPCOM EX 1300	SC	オプション
	NW	オプション
	LB	標準装備
IPCOM EX 2000A	SC	オプション
	NW	オプション
	IN	標準装備
	LB	標準装備
IPCOM EX 2500	SC	オプション
	NW	オプション
	IN	標準装備
	LB	標準装備

(2) 保守端末

ハードウェアは、汎用の PC であり、Telnet ソフトウェア 、または Web ブラウザ、またはシリアルインターフェース（RS232C）接続した VT100 互換ソフトウェアを使用して 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。

なお、利用可能な Web ブラウザは以下のバージョンである。

- Internet Explorer 6 （SP1,SP2,SP3）
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

(3) Syslog サーバ

ハードウェア/OS は、汎用の PC、またはサーバであり、TOE はネットワーク管理プロトコルを用いて、Syslog サーバに TOE のロギング情報の送信を行う。

(4) FTP サーバ

ハードウェア/OS は、汎用 PC、またはサーバであり、TOE は FTP プロトコルを用いて、FTP サーバに TOE の設定データ（構成設定情報ファイル）の送信を行う。

(5) 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。

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 は補助記憶装置内の格納領域が満杯になったときの上書き機能や、監査記録への許可されないアクセスに対する保護機能を提供している。しかし、Syslog サーバ内の監査記録に対しては本機能による保護がされないため、システム管理者及びシステム監査者は、「IPCOM EX1100/EX1300/EX2000A/EX2500 ソフトウェア説明書」に従った Syslog サーバの設置・運用が必要となる。

内部セキュリティポリシーにおいて許可された、内部ネットワークへのアクセスによる脅威（内部ネットワーク資産の不正使用、改ざん、破壊、漏えいなど）への対抗は、本評価の対象外である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な機能を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。IPCOM EX ファームウェア内の「IP パケットフィルタリング機能」、「環境設定管理機能」、「運用支援管理機能」の各コンポーネントが TOE である。

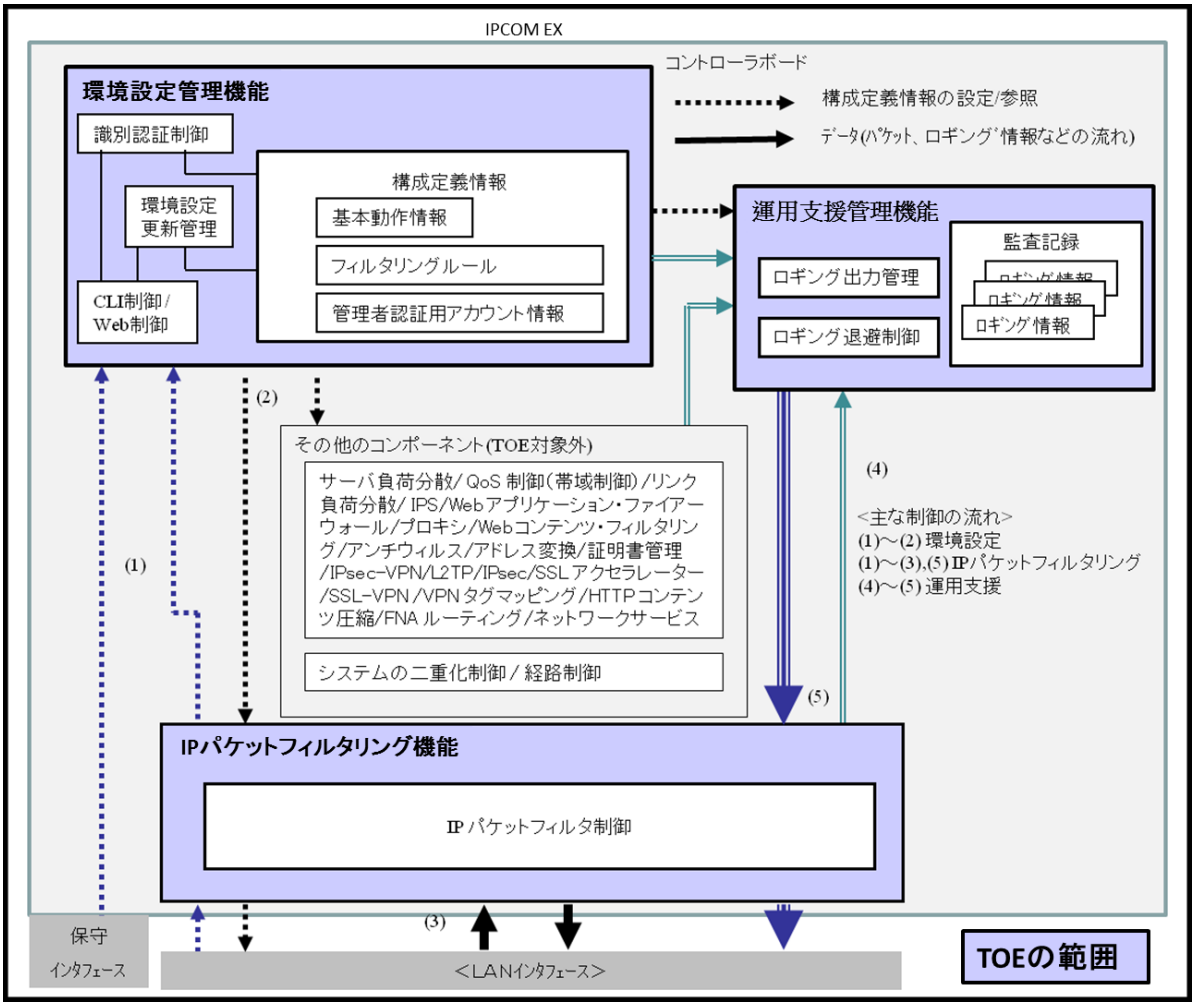

図 5-1 TOE境界

以下に TOE を構成する各コンポーネントとコンポーネント間の関係について説明する。

IP パケットフィルタリング機能

「IPパケットフィルタリング機能」は、複数のLANインター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インターフェースから取得した IPパケットデータは、システム管理者に

より設定されたフィルタリングルールに基づき、通過と判断したIPパケットデータだけ内部ネットワークへの転送が許可される。

通過と判断された IPパケットデータは、TOE対象外である「その他のコンポーネント」に内部転送され、経路制御により中継先の LANインターフェースが特定され、「IPパケットフィルタリング機能」に戻される。「IP パケットフィルタリング機能」は、経路制御で特定された LANインターフェースを利用して、IPパケットデータを送信する。

環境設定管理機能

「環境設定管理機能」は、TOEの動作環境を設定する機能を提供する。保守インターフェースか、「IPパケットフィルタリング機能」でパケット通過を設定したLANインター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。なお、本TOEは保守端末の接続形態として、telnetを利用したCLI（コマンド）接続、Webブラウザを利用したWebコンソール接続、VT100互換ソフトウェアを利用したシリアルインターフェース（RS232C）接続を提供する。

本TOEに通信開始後、利用者の識別認証が実行され、許可されたシステム管理者であれば、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機能」や「運用支援管理機能」に配布される。

なお、TOEの動作を決定する構成定義情報には以下の情報が含まれる。

- 基本動作情報
  IPCOM EX をルータまたはブリッジとして動作させるためのネットワーク情報など

- フィルタリングルール
  内部セキュリティポリシーとなるフィルタリング条件と動作

- 管理者認証用アカウント情報
  システム管理者やシステム監視者のアカウント名やパスワード情報

運用支援管理機能

「運用支援管理機能」は、「環境設定管理機能」や「IPパケットフィルタリング機能」から受け取った、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。

TOEに格納された監査記録は、運用管理専用ネットワークに設置された保守端末を利用して退避または、全消去が許可される。

5.2 IT環境

「環境設定管理機能」は、ロギング情報をIPCOM EXに実装された補助記憶装置に格納、または運用管理専用ネットワークに設置されたSyslogサーバに転送する。なお、Syslogサーバに転送する場合にも、転送データに対して「IPパケットフィルタリング機能」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Syslogサーバ宛ての通信を許可していなければならない。

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。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。

ガイダンス文書名	版数
IPCOM EX シリーズ マニュアル体系と読み方	初版
IPCOM EX1100/EX1300 クイックスタートガイド(*)	Rev.1
IPCOM EX2000A（電源二重化タイプを除く）クイックスタートガイド(*)	Rev.1
IPCOM EX2000A（電源二重化タイプ）クイックスタートガイド(*)	Rev.1
IPCOM EX2500 クイックスタートガイド(*)	Rev.1
IPCOM EX1100/EX1300/EX2000A/EX2500 取扱説明書	初版
IPCOM EX シリーズ ユーザーズガイド	初版
IPCOM EX シリーズ 事例集	初版
IPCOM EX シリーズ コンソールリファレンスガイド	初版
IPCOM EX シリーズ コマンドリファレンスガイド	初版
IPCOM EX シリーズ 保守ガイド	初版
IPCOM EX1100/EX1300/EX2000A/EX2500 ソフトウェア説明書	2011 年 9 月

*クイックスタートガイドは、ハードウェアプラットフォームの機種により、対象のクイックスタートガイドが提供される。

7 評価機関による評価実施及び結果

7.1 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。

7.2 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 23 年 5 月に始まり、平成 23 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 23 年 8 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、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.3 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。

7.3.1 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。

7.3.2 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より確信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、テストに使用した機器の概要を表 7-1 に示す。

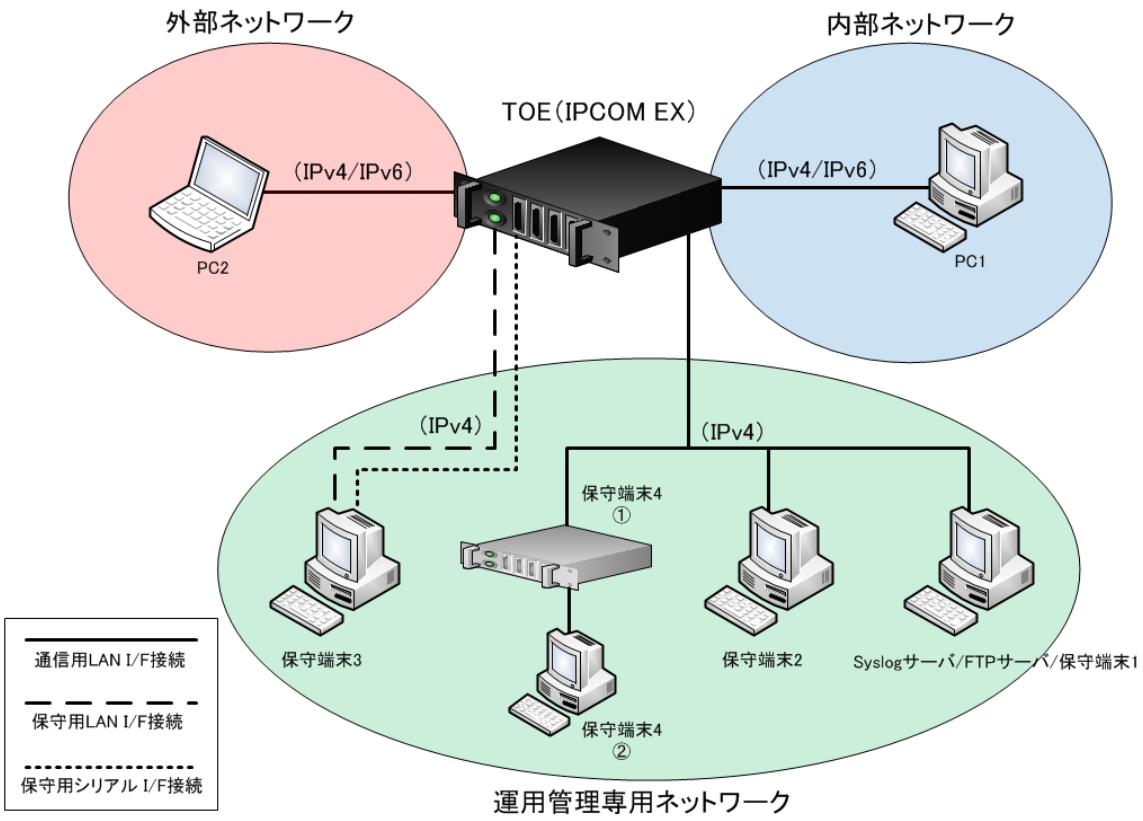

図 7-1　独立テストの構成図

表 7-1　テストに使用した機器

機器	概要
syslogサーバ/ FTPサーバ/ 保守端末1(CLI用)	マシン：DELL INSPIRON 1150 OS：Window XP ソフトウェア： 簡易ロギングユーティリティ、Tera Term IIS（インターネットインフォメーションサービス） Web ブラウザ：IE7
保守端末2 (CLI/Web コンソール用)	マシン：DELL VOSTRO1000 OS：Windows Vista Web ブラウザ：IE8
保守端末3 (TOE設置・生成用)	マシン：SONY VAIO PCG-V505R OS：Windows XP ソフトウェア：Tera Term Web ブラウザ：IE6
保守端末4 (VMware上にIE6、7、8、9を搭載し、VMクライアントから切り替えて利用)	①マシン：DELL PowerEdge2950 OS：Windows XP、Windows Vista ソフトウェア：VMware Web ブラウザ：IE6、IE7、IE8、IE9
	②マシン：DELL VOSTRO1000 OS：Windows Vista ソフトウェア： VM クライアント
PC1 (IP パケットデータの受信用)	マシン：Fujitsu FMV-B8250 OS：Windows Vista ソフトウェア： IIS（インターネットインフォメーションサービス）
PC2 (IP パケットデータの送信用)	マシン：Fujitsu FMV-C8250 OS：Windows Vista ソフトウェア： Netmi NT Ver.1.14（ネットワークスループット測定） Ping Web ブラウザ：IE8

独立テストにおける IPCOM EX の TOE 以外の評価構成、及びロギング情報を格納する補助記憶装置と Syslog サーバの有無を表 7-2 に示す。

表 7-2　TOE以外の評価構成

No.	ハードウェアプラットフォーム	ソフトウェアプラットフォーム	補助記憶装置	Syslogサーバ	搭載オプションファームウェア
①	IPCOM EX 1100	SC	なし	あり	なし
②	IPCOM EX 1300	NW	なし	あり	WCF AV（プロキシ含む） IPsec-VPN FNA
③	IPCOM EX 2000A	IN	あり	あり	SSL-VPN L2TP/IPsec VPN タグマッピング
④	IPCOM EX 2500	LB	あり	なし	WAF SSLアクセラレーター 電源二重化

TOE の機能はハードウェアプラットフォームとソフトウェアプラットフォーム間の組み合わせ、オプションファームウェアの搭載/非搭載による影響は受けないと評価者によって確認されており、独立テスト環境は ST において識別されている全ての TOE の構成をカバーしている。

⑵ 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

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

評価者は、すべてのTOEセキュリティ機能に対してテストを実施するという方針のもと以下の観点で独立テストを実施した。特に、本TOEではフィルタリングルールを設定することにより、通過するIPパケットのフローを制御する機能および制御のための管理者機能が重要なセキュリティ機能であり、フィルタリングルールの設定および通過するIPパケットの組合せに着目したテストを実施した。

＜独立テストの観点＞

①「IP パケットフィルタリング機能」及び「環境設定管理機能」に関して、フィルタリングルールを設定し、設定どおりに通信制御が実施されるかを確認する。

②「環境設定管理機能」に関して管理者アカウントに関する操作が仕様通りであること、構成定義情報の退避・復元やロギング情報の採取・消去など保守機能が仕様通りであることを確認する。

③「運用支援管理機能」に関して、ロギング情報が仕様通りに生成できることを確認する。

④コマンドと Web コンソールでは、同一の機能が実施できるため、双方のインターフェース利用で異なる結果とならないことを確認する。

b) 独立テスト概要

評価者は、提供された評価証拠資料から、以下の観点で20項目の独立テストを考案した。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＞

フィルタリングルールの設定については、全てのコマンド、Web コンソールをカバーするようにテストケースを設定した。また、IPv4 ネットワークと IPv6 ネットワークの両方を確認するよう実施された。

＜独立テストツール＞

独立テストは表 7-1 のソフトウェアを用いて実施された。

＜独立テストの実施内容＞

独立テストは、評価者によって 20 項目実施された。

独立テストの観点とそれに対応したテスト内容を表 7-3 に示す。

表 7-3 実施した独立テスト

観点	テスト概要
① ④	全てのコマンド、Webコンソールがカバーされるよう、評価者が考案した18パターンのフィルタリングルールを設定し、設定どおりに通信制御が実施されていることを、ログの確認により行った。 上記のテストをコマンドとWebコンソールの両方のインターフェースで

	実施した。 また、初期設置時にIPパケットの通過が全て拒否されることを確認した。
② ④	構成定義情報を退避する際にその時点の管理者情報等を記録しておき、復元後に管理者のログイン操作が正常に動作すること及び、復元後の構成定義情報が退避時に記録したものと一致することを確認した。また、ロギング情報の採取・消去に関する操作が正常に実施されることを確認した。 上記のテストをコマンドとWebコンソールの両方のインターフェースで実施した。
③	実行したコマンド、Web コンソール操作、IP パケット送信に関連したロギング情報が記録されていることを、実際にログ参照することにより確認した。 ログイン、ログアウトを大量に実施し、ログファイルの満杯時に一番古いログファイルから上書きされていることを確認した。

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。

7.3.3 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及び公知の情報より、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公知の一般的攻撃に関する脆弱性を識別した。

①「IPパケットフィルタリング機能」に関する以下の脆弱性

- ガイダンス文書の手順に従ったTOEの設定後に、意図しないパケットの通過を許してしまう潜在的脆弱性
- 異常なIPパケットの入力により、当該パケットや後続パケットが正しく制御されない潜在的脆弱性

②「環境設定管理機能」に関する以下の脆弱性

- 保守インターフェースについて本来許可されていないIPルーティングが有効になることにより、外部ネットワークから保守インターフェースを経由して運用管理専用ネットワークに侵入される潜在的脆弱性
- FTPコマンドによりFTPサーバ上の許可されないファイルへのアクセスが可能となる潜在的脆弱性
- 退避した構成定義情報が破壊されていた場合、これを復元した際にシステムの誤動作を招く潜在的脆弱性
- パスワード照合が正しく行われない潜在的脆弱性

③「運用支援管理機能」に関する以下の脆弱性

- ログインやユーザ登録時のパスワードが平文でロギング情報に含まれる潜在的脆弱性

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＞

評価者が実施した侵入テストは、独立テスト環境に侵入テスト用 PC を追加で外部ネットワークに接続した環境で実施された。

侵入テスト用 PC と用いたツールの詳細を表 7-4 に示す。

表 7-4　侵入テスト用PCと用いたツール

構成品	概要・
侵入テスト用PC	マシン：FMV-BIBLO MG/G75N CPU：Intel Core i7 2.67GHz メモリ：4GB HDD　：140GB × 2 OS：Windows 7 Professional SP1 ブラウザ：IE9.02
使用ツール	nmap Version 5.51（ポートスキャンツール） Wireshark Version 1.4.2（パケットキャプチャツール） ipsendwin Version 2.4（パケットジェネレータ）

＜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
①	・新規にネットワーク設定をした後に、TOEの外部ネットワーク用として用いるインターフェースについてポートスキャンを実施し、開いているポートが存在しないことを確認した。 ・異常なIPパケットデータを生成し、TOEに対して入力することで、IPパケットデータが異常と認識され、破棄されたことを、記録されたロギング情報の内容より確認した。
②	・保守インターフェースについてIPルーティング指定のコマンドを実施し、無効となることを確認した。 ・FTPサーバにログインし、ガイダンス文書に記載されていないファイルが表示されないこと、システム監視者には操作が制限されることを確認した。 ・TOEの構成定義情報ファイルを保守端末に退避した後、当該ファイルの一部を変更した後、復元しようとするとエラーとなり、構成定義情報が更新されないことを確認した。 ・パスワード入力において、英文字の大文字/小文字を識別すること、空白文字を識別すること、最大長を超えたパスワード入力に対するエラー処理に関して、誤処理が行われないことを確認した。
③	・ログイン時にはアカウントログにパスワードが記録されないこと、コマンドログ上ではパスワード部分がマスクされていることを確認した。

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。

7.4　評価構成について

本 TOE は、IPv4 ネットワークと IPv6 ネットワークの両方をサポートしているため、IPv4、IPv6 両方の構成において、評価を行った。

本評価では、「7.3.2 評価者独立テスト」及び図 7-1 に示す構成において、評価を行った。

本 TOE は、上記と構成要素が大きく異なる構成において、運用される場合はない。よって、評価者は、上記の評価構成は、適切であると判断した。

7.5 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。

7.6 評価者コメント/勧告

消費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。

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、本 ST 及び評価報告書において、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、本認証報告書を発行した。

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

IPCOM EX シリーズに実装される以下の機能は本評価の範囲外であり保証されない。以下の機能を利用する場合には、消費者は注意する必要がある

- サーバ負荷分散
- QoS 制御（帯域制御）
- リンク負荷分散
- IPS
- Web アプリケーション・ファイアーウォール (WAF)
- プロキシ
- Web コンテンツ・フィルタリング
- アンチウィルス
- アドレス変換
- 証明書管理

- IPsec-VPN
- L2TP/IPsec
- SSL アクセラレーター
- SSL-VPN
- VPN タグマッピング
- HTTP コンテンツ圧縮
- FNA ルーティング
- ネットワークサービス
- 二重化制御
- 経路制御

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。

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　バージョン：2.1　2011 年 9 月 12 日　富士通株式会社

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 TOE に関する略語を以下に示す。

AV	Antivirus
CLI	Command Line Interface
FNA	Fujitsu Network Architecture
FTP	File Transfer Protocol
IIS	Internet Information Service
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
SSL	Secure Socket Layer
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
WCF	Windows Communication Foundation

本報告書で使用された用語の定義を以下に示す。

Syslog	システムの動作やメッセージ等の記録（ロギング情報）を取るプログラム。
フィルタリングルール	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／拒否するための条件を組み合わせた、内部セキュリティポリシーを具体化したルール。
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。本TOEを利用するそ

	れぞれの組織内部のイントラネット・セグメント、およ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。
外部ネットワーク	本TOEを利用する組織の内部セキュリティ ポリシーが及ばないインターネットや、本TOEを利用する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。
運用管理専用ネットワーク	本TOEや基幹業務を担う機器の運用を管理するための独立させたネットワーク・セグメント。
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、ネットワークのアドレス定義やフィルタリングルール、内部データの取り扱い（不正持ち出し不可）ルールで実現される。

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23年2月, 独立行政法人 情報処理推進機構, CCS-01

[2] ITセキュリティ認証申請手続等に関する規程, 平成23年2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申請手続等に関する規程, 平成23年2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 Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[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3版, 2009年7月, CCMB-2009-07-001, (平成21年12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3版, 2009年7月, CCMB-2009-07-002, (平成21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3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[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3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] 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, バージョン：2.1, 2011年9月12日, 富士通株式会社

[13] 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1.8版, 2011年11月10日, 一般社団法人 ITセキュリティセンター 評価部