認　証　報　告　書

評価対象

申請受付年月日(受付番号)	平成14年６月７日（IT認証2003）
認証申請者	富士通株式会社
TOEの名称	INTERSTAGE Security Director 4.0
ＰＰ適合	なし
適合する保証要件	EAL3
TOE開発者	**富士通株式会社　ソフトウェア事業本部ネットワークソフトウェア事業部第三開発部**
評価機関の名称	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１４年１２月２０日

独立行政法人製品評価技術基盤機構
適合性評価センター管理課情報セキュリティ室
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価機関に対する要求事項」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999 Information technology － Security techniques － Evaluation criteria for IT security.
② JIS X 5070(2000) セキュリティ技術 － 情報技術セキュリティの評価基準。
③ Common Criteria for Information Technology Security Evaluation.
④ JIS TR X 0049(2001) 情報技術セキュリティ評価のための共通方法
⑤ Common Methodology for Information Technology Security Evaluation
⑥ 認証機関が公開する③および⑤の翻訳文書

評価結果：合格

INTERSTAGE Security Director 4.0は、独立行政法人製品評価技術基盤機構が定めるIT製品等のセキュリティ認証業務実施規程に従い、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。

その他：

本報告書には、認証申請の受理以前に評価が開始されているような日付の記載がある。これは、評価認証制度に関わる正式な手続が確定した後に、認証申請書が提出されたことによるものである。認

証は、実際の評価の開始と同時に実施している。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「INTERSTAGE Security Director 4.0」（以下「本TOE」という。）について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「ファイアウォール機能説明書　第2.1版(D07)」および「インストールガイド INTERSTAGE Security Director 4.0 ファイアウォール機能 for Solaris Environment, B23PDX4-G-02-1」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、動作条件および機能仕様は本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。

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: INTERSTAGE Security Director
- バージョン: 4.0
- 開発者: 富士通株式会社　ソフトウェア事業本部
  ネットワークソフトウェア事業部　第三開発部

1.2.2 製品概要

本TOEは、Solaris OS上で動作するファイアウォールソフトウェアである。

本TOEは、「図 1ネットワーク構成」に示すように複数のネットワークの境界点に設置されたサーバ上で動作し、本TOEを経由するIPパケットを、事前に設定されたフィルタリング条件(IPアドレス、ポート番号、プロトコル、パケット方向、ネットワークインタフェース及びその組合せ)に従い、転送または破棄を行う。同様に、本TOEを経由するIPパケットのIPアドレス及びポート番号を、事前に設定されたアドレス変換条件に従い変換する。

本TOEは、あらかじめ設定したイベントに関連するログの収集や、SNMPあるいはメールを用いたアラーム通知を行うことができる。

本TOEは、内部ネットワークに対する外部ネットワークからのアクセスの制限や、外部ネットワークとの通信時における内部ネットワークのアドレス体系の隠匿を目的に使用される。

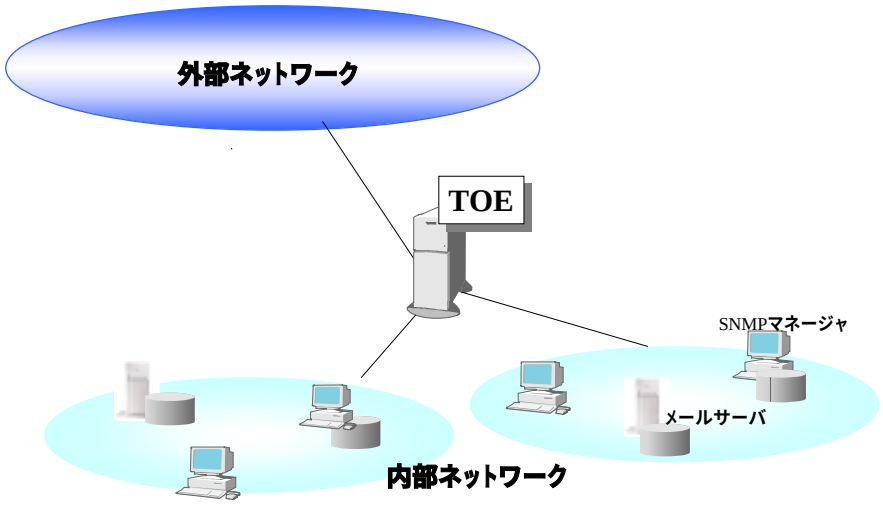

図 1 ネットワーク構成

1.3 評価の実施

INTERSTAGE Security Director　4.0のセキュリティ評価は、独立行政法人製品評価技術基盤機構が独立した認証機関として運営する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セキュリティ認証申請等の手引き (平成14年4月)」[2]、「ITセキュリティ評価機関に対する要求事項 (平成14年4月)」[3]、「ITセキュリティ認証申請者・登録者に対する要求事項 (平成14年4月)」[4]に規定された内容に従って実施された。

本評価の目的は、以下のとおりである。

(1)　本TOEのセキュリティの基本設計が適切であること。

(2)　本TOEのセキュリティ機能が、基本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がセキュリティの基本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、本TOEのセキュリティの基本設計である「INTERSTAGE Security Director 4.0 セキュリティターゲット 第2.7版」（以下「本ST」という。）[1]、本TOE開発に関連する評価用提供物件及び本TOEの開発環境・製造・出荷の現場を検証し、本TOEとその開発環境等がCCパート1 ([5][8][11][14]のいずれか)附属書C、CCパート2（[6][9][12][15]のいずれか）の機能要件及びCCパート3（[7][10][13][16]のいずれか）の保証要件を満たしていることを評価することである。この評価手順及び結果は、「INTERSTAGE Security Director 4.0 評価報告書」（以下「本評価報告書」という。）［20］に示されている。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関である電子情報技術産業協会　ITセキュリティセンターが作成した、本評価報告書、当該所見報告書[21]及び関連する評価証拠資料を検証し、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[22][23][24]を作成した。評価は、平成14年10月21日の評価機関によるINTERSTAGE Security Director 4.0 評価報告書　第1.7版[20]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、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が判明した。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

TOEの評価保証レベルは、EAL3である。

1.5.3 セキュリティ機能強度

最小機能強度として、”SOF-基本”を主張する。

本TOEは、一般の商用システムで利用されることを想定する。TOEへの直接的なセキュリティは管理・運用で確保されるため、攻撃は公開インタフェースを利用したものとなる。このため、低レベルの攻撃力に対抗できるレベルである”SOF-基本”で満足される。ただし、本TOEには機能強度に関連するセキュリティメカニズムはない。

1.5.4 セキュリティ機能

TOEは、以下のセキュリティ機能を有する。
図 2にTOEのセキュリティ機能を示す。

(1)　IPパケットフィルタリング機能

管理者が設定したフィルタリング条件に従って、本TOEを経由するIPパケットを通過または遮断する機能。フィルタリング条件には、以下の指定が可能。

・ネットワークインタフェース単位
・IPアドレス
・ポート番号
・プロトコル
・パケット方向
・上記組合せ

また、アドレス変換機能が設定されている場合には、通過IPパケットをアドレス変換機能へ転送する。

(2)　アドレス変換機能

本TOEを通過するIPパケットに対し、内部ネットワーク上のホストやネットワークのアドレスと外部ネットワークとの通信用のIPアドレスとの変換を行う。変換には以下のものがある。

・　内部IPアドレスの変換(送信元NAT)

外部ネットワークとの通信に際して、内部IPアドレスに対応した外部公開用IPアドレスに変換し通信を行う。

・　内部IPアドレス/内部ポート番号変換(IPマスカレード)

外部ネットワークとの通信に際して、内部IPアドレスを本TOEの外部ネットワーク向けインタフェースのIPアドレスに変換し、内部ポート番号を当該通信識別のためのユニークな本TOEの未使用ポート番号に変換し通信を行う。

(3)　運用支援機能

本TOEを通じて行われている通信の解析・監視及び特定事象の通知を行う機能であり、管理者を通じてセキュアな運用を支援するものである。運用支援機能には以下のものがある。

・　ロギング機能

あらかじめ定められたTOEのセキュリティ機能(IPパケットフィルタリング機能及びアドレス変換機能)の処理結果の情報を、定められたログ格納ファイルに格納する。

・　アラート機能

あらかじめ定められた事象（アラートイベント）を検出した場合、その情報と発生時刻を通知する。アラートイベントとその通知方法には以下の種類がある。

アラートイベント	同一送信元IPアドレスからのIPパケットが、単位時間あたりにあらかじめ定められた規定回数以上破棄された場合。
	同一送信先IPアドレスかつ同一送信先ポート番号へのIPパケットが、単位時間あたりにあらかじめ定められた規定回数以上破棄された場合。
	あらかじめ定められたポート番号宛てのIPパケットを受信した場合。
アラートイベント通知方法	コンソールにアラートを表示する。
	あらかじめ定められた通知者リスの通知者に対し、メールで通知する。
	モニタリング機能にアラートを通知する。
	SNMP連携機能を通じ、SNMPマネージャに通知する。
	システムログ(syslog)に出力する。
	あらかじめ定められたコマンドを実行する。

・ モニタリング機能

TOEでのパケットの処理状況をリアルタイムに表示する。IPフィルタリング機能でのパケットの通過、破棄状況をネットワークインタフェースごとにグラフまたは表形式で表示する。アドレス変換機能で処理しているそれぞれのコネクション状況を表示する。

・ 稼動状況通知機能

TOEの稼動状況をコマンドにより得ることができる。稼動状況として通知される情報は、環境設定情報の更新・適用に関する時間情報、TOEの起動状態・最終起動時刻、TOEのセキュリティ機能の起動・終了に関する情報である。

(4) 環境設定機能

本TOEを運用するために必要とされる環境設定ファイルへの操作を行う。この機能で、本TOEが接続するネットワークの構成を入力し、IPフィルタイリング機能の対象となるインタフェース、ホスト、ホストグループ、ネットワークの情報を設定する。アドレス変換機能の条件の設定も行う。また、セキュリティポリシーに従ったフィルタリング条件、ロギングの対象と格納場所、アラートイベントの種類と通知方法の設定も行う。

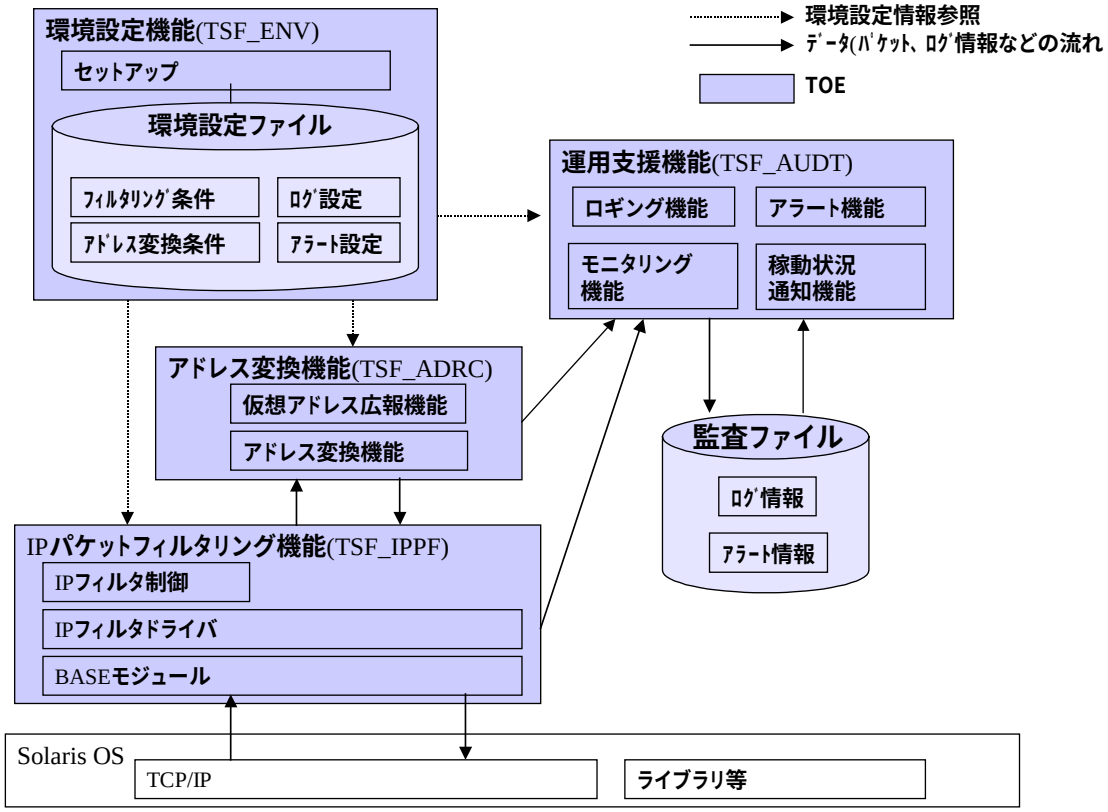

図 2 TOEのセキュリティ機能

1.5.5 脅威

本TOEは、表 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 想定する脅威

識別子	脅威
T1	外部ネットワークの利用者は、内部ネットワークに侵入し、内部ネットワークの保護資産の改ざん、破壊、又は漏洩を図る恐れがある。
T2	外部ネットワーク及び内部ネットワークの利用者、またはTOE管理者がX端末を利用している場合、TOE管理者以外のX端末から、本TOEに侵入し、環境設定ファイルを改ざんして不正なIPパケットデータを通過させたり、監査ファイルを改ざん、又は破壊し、不正行為の証拠を隠滅する恐れがある。
T3	内部ネットワークの利用者が外部ネットワークへアクセスする場合、内部ネットワークのIPアドレス体系が外部ネットワークの利用者に漏洩する恐れがある。

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ない。

1.5.7 構成条件

本TOEは、ファイアウォール製品である。本TOEは、複数のネットワークの境界に設置される。また、運用に応じてメールサーバあるいはSNMPマネージャを内部ネット内に配置する（図 1)。本TOEが必要とするサーバの構成条件は、以下のとおりである。

■本TOEの構成条件

OS:	日本語 Solaris 8
HW:	富士通　GRANDPOWER 7000Fシリーズ
CPU:	上記HWにてTOEの運用に応じて対応
Memory:	上記HWにてTOEの運用に応じて対応
Display:	X-Windowシステム表示可能なビットマップディスプレイ
Network:	ネットワーク構成に応じインタフェースボード1～8枚

1.5.8 動作環境の前提条件

本TOEを使用する環境において有する前提条件を表 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 2　TOE使用の前提条件

識別子	前提条件
ASM.1	**TOE、及びXサーバ端末は、TOE管理者から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定されている。**
ASM.2	**TOEは、内部ネットワークと外部ネットワークを唯一の接点で接続する形態で動作する。**
ASM.3	**TOE管理者は、TOEに関して不正をしない。**
ASM.4	**TOE管理者は、TOEが正しく動作するよう、TOEを運用管理しなければならない。**
ASM.6	**アラート情報のメール通知やSNMPマネージャ通知を行う場合、通知先となるメールサーバ、及びSNMPマネージャは、内部ネットワークに設置する。**

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。

■「ファイアウォール機能説明書　第2.1版(D07)」
　管理者ガイドとして提供され、TOEのセキュアな管理・運用に必要な事項が述べられている。提供形態はCD-ROM。

■「インストールガイド INTERSTAGE Security Director 4.0 ファイアウォール機能 for Solaris Environment, B23PDX4-G-02-1」
　インストールガイドとして提供され、セキュアな設置、生成及び立ち上げの手順が述べられている。

なお、本TOEは一般利用者が利用するインタフェースを有しておらず、利用者ガイドに相当するものは提供されない。

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パート2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、本評価報告書において報告されている。本評価報告書では、TOEの概要説明、CEMパート2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、本評価報告書による評価実施の履歴を示す。

評価は、平成13年12月に始まり、平成14年10月本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検証した。また、平成14年2月及び4月に開発・製造現場へ赴き、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の認証を、記録及びスタッフへのヒアリングにより実施し、同現場で開発者のテスト環境と同等の環境を構築し開発者サンプリングテスト及び評価者テストも実施している。

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記録され、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、評価に反映された。

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

1) 開発者テスト環境

開発者が実施したテストのシステム構成を図 3に示す。また、テストシステムの各機器の構成を表 3に示す。

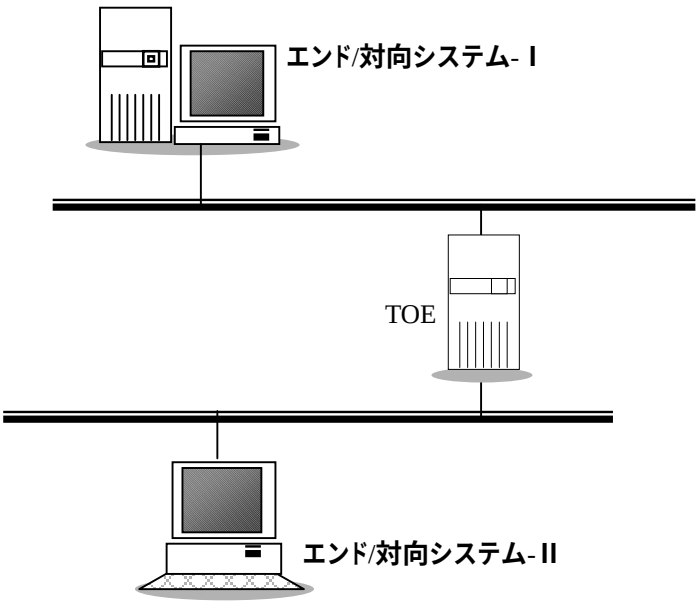

図 3 開発者テストシステム構成図

表 3 開発者テスト構成機器概要

TOE搭載機	
ハードウェア機種	GRANDPOWER 7000F M25
CPU	256MHz x 2CPU
Memory	512MB
OS	日本語Solaris 8
エンド/対向システム-Ⅰ	
ハードウェア機種	GP-S (S7/7000U)

CPU	256MHz x 1CPU
Memory	512MB
OS	Solaris 8
エンド/対向システム-Ⅱ	
ハードウェア機種	FMV DESKPOWER
CPU	256MHz x 2CPU
Memory	256MB
OS	Windows NT Server

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

1. テスト構成

開発者が実施したテストの構成は図 3及び表 3に示す。本構成は本STの記述と一致している。

2. テスト手法

開発者はコンポーネントテスト(CT)を実施している。CTはTOEを構成する各モジュールに対する単体テストである。

CTは一方のエンド/対抗システムからTOEを介しもう一方のエンド/対向システムに向けてパケットを送信することにより実施している(図 3参照)。

パケットの方向(仮想的な内部ネットワークと外部ネットワークを想定)、プロトコル(TCP/UDP/ICMP)、サービス(TELNET、FTPなど)及び送信先アドレスの組合せを変化させ、TOEで設定されているフィルタリング条件、アドレス変換条件が正しく機能していることの確認を行った。

3. 実施テストの範囲

TOEセキュリティ機能(IPパケットフィルタリング機能、アドレス変換機能、運用支援機能、環境設定機能)は、管理者の外部インタフェースの各設定に対しパケットが期待されるようにフィルタリングあるいはアドレス変換されるかを確認することによりテストが可能である。開発者テストでは、すべてのTOE管理者インタフェースに対して代表的な組合せが少なくともひとつ以上テストされ、また各機能と外部インタフェースの対応も確認されている。

CTの総数は4000項目であるが、個々のモジュールにおいて設定値のパラメタを変更しながらテストを行ったためであり、開発者テスト数としては妥当と判断した。

4. 結果

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法

及び実施結果がテスト計画書に示されたものと一致することを確認した。

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システム構成を図 4に示す。また、テストシステムの各機器の構成を表 4に示す。

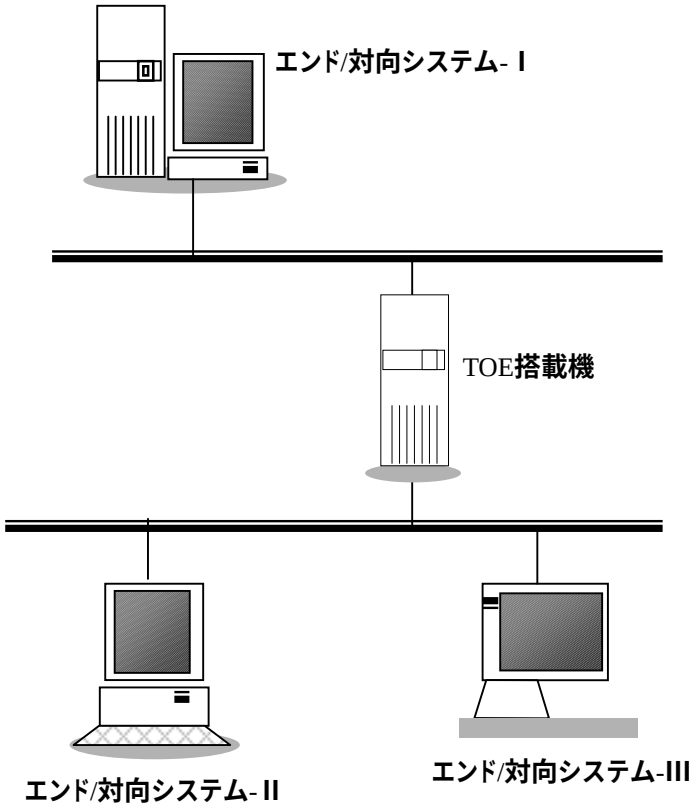

図 4 評価者テストシステム構成図

表 4 評価者テスト構成機器概要

TOE搭載機	
ハードウェア機種	GRANDPOWER 7000F
CPU	SPARC64-Ⅲ 248MHz 2CPU
Memory	512MB
OS	日本語Solaris 8
エンド/対向システム-Ⅰ	

ハードウェア機種	GP-S (S7/7000U)
CPU	UltraSPARCⅡ 248MHz × 2CPU
Memory	512MB
OS	Solaris 2.6
エンド/対向システム-Ⅱ	
ハードウェア機種	FMV DESKPOWER
CPU	PentiumⅡ 266MHz
Memory	98MB
OS	Windows 2000
エンド/対向システム-Ⅲ	
ハードウェア機種	FMV-N5200
CPU	Pentium MMX 200MHz
Memory	64MB
OS	Free BSD

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。

1. テスト構成

評価者が実施したテストの構成は図 4及び表 4に示す。本構成は本STの記述と一致しており、開発者のテスト環境とも一致する。なお、テスト効率を上げるため、クライアント2台で実施した。

2. テスト手法

評価者は、開発者テストのCTの実施方法がTOEのセキュリティ機能全体をカバーできるテストと考え踏襲した。TOEでフィルタリング及びアドレス変換の設定可能な代表的パターンを設定し、一方のエンド/対向マシンから他方のエンド/対向マシンへパケットの方向、プロトコル、サービス、宛先アドレスの組合せを変えて送信することで実施している(図 4参照)。

3. 実施テストの範囲

評価者テストは、CTの実施方法のなかで、各サブシステムの機能での特殊なケースを中心に実施された。TOEのセキュリティ機能が機能非活性である場合、パケットフィルタリング・アドレス変換条件が未設定の場合、設定された境界値を上回るパケット数送信が行われた場合のパケット処理が、想定された結果となるかなどがテストされた。実施されたテスト数は11種類25パターンである。

また、サブシステムごとに開発者テスト項目を抽出し、セキュリティ機能単

位に最低１つのテスト項目を選び、78パターンを実施した。

4. 結果

評価者テストを実施し、実施結果が評価者テストは期待される結果となり、開発者テストのサンプリングテストはテスト計画書に示されたものと一致することを確認した。

2.4 評価結果

本評価報告書をもって、評価者は本TOEがCEMパート2の所定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 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本評価報告書で示されたように評価されていること。

④ 本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 本評価報告書に示された評価者の評価方法がCEMに適していること。

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[22][23][24]として作成し、評価機関に送付した。

認証機関は、本ST及び本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

提出された本評価報告書、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、本TOEがCCパート3（[7][10][13][16]のいずれか）に規定されたEAL3で要求されてい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アクションエレメントについての認証結果を表 5にまとめる。

表 5　評価者アクションエレメント認証結果

評価者アクションエレメント	認証結果
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指摘(所見報告書ASE004-01、ASE2-011-01)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記述が理路整然と一貫性のあ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。また、当評価に至るまでなされた指摘(所見報告書ASE002-01)も適切と判断される。
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。また、当評価に至るまでになされた指摘(所見報告書ASE2-010-01、ASE2-016-01、ASE007-01、ASE006-01、ASE2-014-01、ASE2-006-01)も適切と判断される。
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。また、当評価に至るまでになされた指摘(所見報告書ASE005-01)も適切と判断される。
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。また、当評価に至るまでになされた指摘(所見報告書ASE001-01)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書ASE017-01)も適切と判断される。
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明記され、それらが脅威、組織のセキュリティ、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。また、当評価に至るまでなされた指摘(所見報告書ASE2-004-01、ASE009-01、ASE010-01、ASE2-008-01、ASE2-014-01)も適切と判断される。
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理路整然とし、完結しており、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。また、当評価に至るまでなされた指摘(所見報告書ASE011-01、ASE016-01、ASE018-01、ASE2-012-01、ASE012-01、ASE014-01、ASE-020-01、ASE2-007-01、ASE2-018-01、ASE2-002-01、ASE021-01、ASE2-005-01、ASE024-01、ASE026-01、ASE019-01、ASE030-01、ASE025-01、ASE021-01、ASE2-009-01)も適切と判断される。
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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書ASE013-01、ASE022-01、ASE2-018-01)も適切と判断される。
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、セキュリティメカニズムが存在せず関連するワークユニットが非適用であることを確認している。また、当評価に至るまでなされた指摘(所見報告書ASE013-01、ASE027-01、ASE2-015-01、ASE027-01、ASE028-01、ASE-015-01、ASE2-003-01、ASE2-017-01、ASE2-017-01、ASE2-013-01)も適切と判断される。
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結しており、理路整然とし、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書ASE2-013-01、ASE2-018-01)も適切と判断される。
構成管理	**適切な評価が実施された**
ACM_CAP.3.1E	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。また、当評価に至るまでなされた指摘(所見報告書ACM0001-01)も適切と判断される。
ACM_SCP.1.1E	評価はワークユニットに沿って行われ、CMシステムにCCで必要とされるものが含まれており、CM証拠資料に各ライフサイクルを通して構成要素のステータスの追跡、割当ての方法、構成要素変更に伴う関連する構成要素が記述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_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
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を確認している。また、当評価に至るまでなされた指摘(所見報告書ADV011-01、ADV003-01、ADV001-01、ADV010-01、ADV006-01、ADV007-01、ADV013-01、ADV014-01)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書ADV002-01、ADV004-01、ADV005-01)も適切と判断される。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。また、当評価に至るまでなされた指摘(所見報告書ADV009-01、ADV012-01)も適切と判断される。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全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。また、当評価に至るまでなされた指摘(所見報告書ADV015-01)も適切と判断される。
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、他のドキュメントと一貫しており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。また、当評価に至るまでなされた指摘(所見報告書AGD002-01、AGD001-01、AGD003-01)も適切と判断される。

AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者が利用可能なセキュリティ機能やインタフェースが提供されておらず、利用者ガイダンスは存在しないため、非適用であることを確認している。また、当評価に至るまでなされた指摘(所見報告書AGD004-01)も適切と判断される。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.2Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での認証方法も適切と判断される。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。また、当評価に至るまでなされた指摘(所見報告書ATE002-01)も適切と判断される。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。また、当評価に至るまでなされた指摘(所見報告書ATE003-01)も適切と判断される。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果が含まれておりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。また、当評価に至るまでなされた指摘(所見報告書ATE001-01)も適切と判断される。
ATE_IND.2.1E	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.2.2E	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サイト訪問でのテスト実施方法も適切と判断される。

ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、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、本評価のサンプリング方針及びサイト訪問でのテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.1.1E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていることを確認している。
AVA_MSU.1.2E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドのみの情報でTOEを構成でき、セキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.1.3E	評価はワークユニットに沿って行われ、管理者ガイド及びインストールガイドが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法が記述されていることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、該当するセキュリティメカニズムは存在しないため非適用であることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、該当するセキュリティメカニズムは存在しないため非適用であることを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が明らかな脆弱性に関する情報を考慮していること、明らかな脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト内容を記述し、脆弱性分析とあわせて悪用可能な明らかな脆弱性が存在しないことを確認している。また、実施したテストの詳細と悪用され得る脆弱性及び残存脆弱性について報告がなされている。

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

6 参照

[1] INTERSTAGE Security Director 4.0 セキュリティターゲット　第2.7版 2002年10月21日 富士通株式会社

[2] ITセキュリティ認証申請等の手引き 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター

[3] ITセキュリティ評価機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT機関要求－02

[4] ITセキュリティ認証申請者・登録者に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－IT申請要求－02

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部:

セキュリティ機能要件
[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件
[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999
[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月
[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法
[20] INTERSTAGE Security Director 4.0 評価報告書 第1.7版 2002年10月21日 01ITSC-E004 電子情報技術産業協会　ITセキュリティセンター
[21] 所見報告書　ASE001-01～ASE018-01、ACM001-01、ADV001-01～AV15-01、AGD001-01～AGD004-01、ATE001-01～ATE004-01、AVA001-01
[22] 認証レビュー CRV-T003-001 2002年6月20日発行
[23] 認証レビュー CRV-T003-002 2002年8月15日発行
[24] 認証レビュー CRV-T003-003 2002年10月11日発行