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

申請受付日（受付番号）	**平成18年10月16日（IT認証6107）**
認証番号	C0114
認証申請者	**株式会社 日立製作所**
TOEの名称	JP1/Base **認証サーバ**
TOEのバージョン	08-10（Windows版）
PP適合	**なし**
適合する保証パッケージ	EAL2+ALC_FLR.1
開発者	**株式会社 日立製作所**
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19年8月30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　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

「JP1/Base 認証サーバ バージョン 08-10（Windows版）」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、「JP1/Base 認証サーバ バージョン 08-10（Windows版）」（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株式会社 日立製作所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： JP1/Base 認証サーバ
バージョン： 08-10（Windows版）
開発者： 株式会社 日立製作所

1.2.2 製品概要

JP1/Baseは、システム運用管理のソフトウェア製品であるJP1製品群に対し、基盤機能を提供するソフトウェア製品である。評価対象は、JP1/Baseの基盤機能の一つであるユーザー管理／認証機能を提供するソフトウェアコンポーネント（「JP1/Base 認証サーバ」という。）である。

JP1/Base 認証サーバが有するセキュリティ機能を以下に示す。

- 識別・認証機能
- アクセス制御機能（識別・認証されたJP1ユーザー自身のデータにのみアクセスできるように制御する機能）
- JP1ユーザーの登録等に関するセキュリティ管理機能

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの範囲

TOEは、ソフトウェア製品であるJP1/Baseに含まれる、ユーザー管理/認証機能を提供するソフトウェアコンポーネントである。

1.2.3.2 TOEの動作環境

TOEはすべてのJP1/Baseに含まれるが、JP1/Baseを認証サーバとして設定した場合のみ、その機能が有効となる。また、TOEが提供する機能は、JP1製品群の一つである統合管理用ソフトウェアであるJP1/IM（JP1/IM-View及びJP1/IM-Manager）を介して、または認証サーバから直接利用される。TOEを使用した動作環境を図1-1に示す。

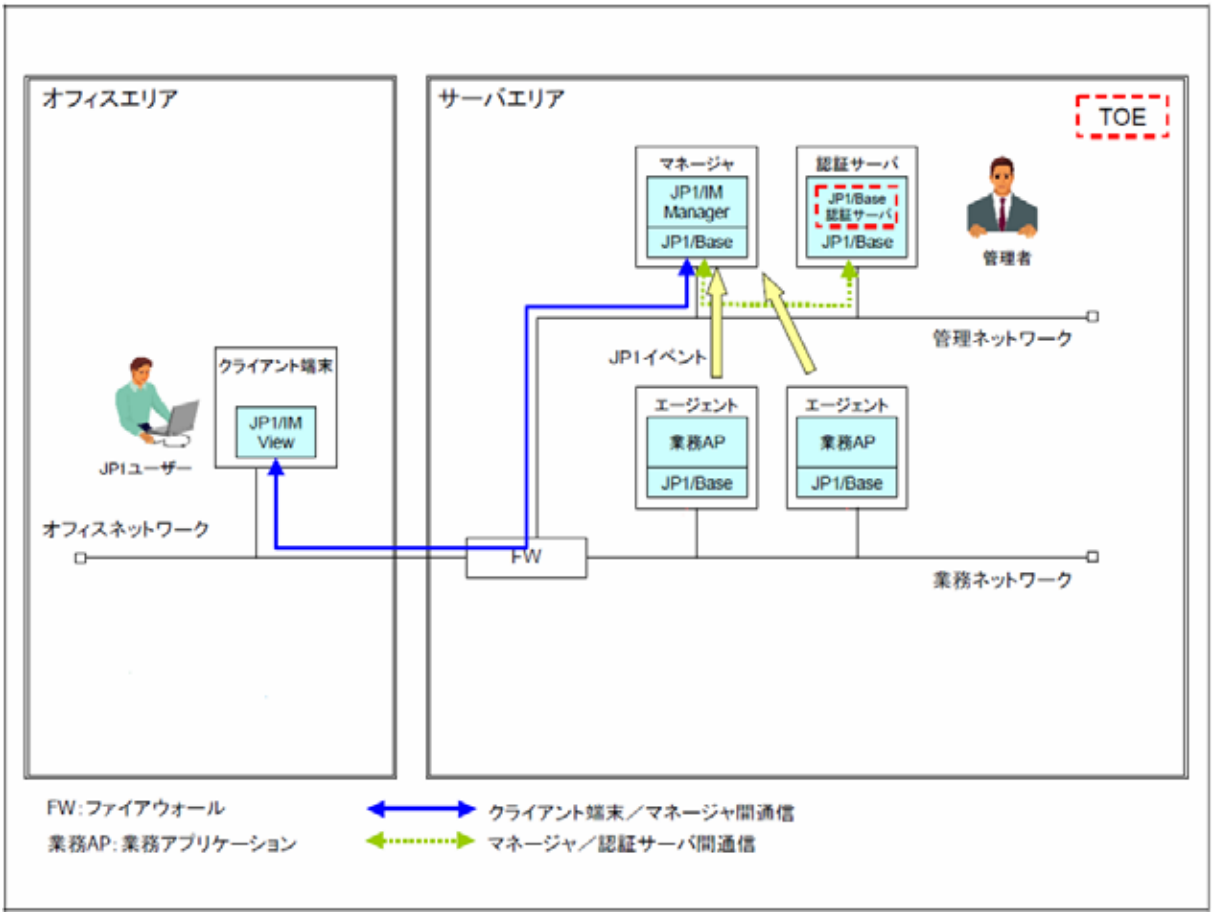

図1-1　TOEを使用したシステム概要

TOEの動作に関わる構成要素の役割を以下に示す。

【認証サーバ】（TOEを搭載）
JP1/Baseがインストールされ、認証サーバとして設定されているマシンである。マネージャ、エージェントにインストールされているJP1/Baseは、認証サーバとしてこのマシンを利用するように設定されている。認証サーバは、JP1ユーザー情報、JP1資源グループ/JP1権限レベルの管理を行う。また、マネージャからの要求に応じ、ユーザーの識別・認証、及びJP1資源グループ/JP1権限レベルの提供を行う。TOEは、認証サーバ上で動作する。

【クライアント端末】（TOE範囲外）
JP1/IM-Viewがインストールされているマシンである。JP1ユーザーは、クライアント端末にインストールされたJP1/IM-Viewを経由してマネージャに接続してJP1/IM-Managerの機能を利用する。JP1ユーザーが行う操作に先立ち、JP1/IM-Viewは入力画面を表示し、JP1ユーザーに対して、JP1ユーザー名・パスワードの入力を要求する。入力されたJP1ユーザー情報は、JP1/IM-Managerを経由して認証サーバに送信され、識別・認証が行われる。識別・認証が成功した後は、識別・認証されたJP1ユーザーは、許可された操作のみが利用可能となる。クライアント端末はTOEの範囲外である。

【マネージャ】（TOE範囲外）
JP1/IM-Manager及びJP1/Baseがインストールされているマシンである。JP1/IM-Managerには、システム構築時に管理者によって管理対象ホスト（エージェント）が登録される。JP1/IM-Managerは、自身が管理する各エージェントが送信するイベント情報の一元的管理や、JP1/IM-Managerで設定した定義の各エージェントへの配布・各エージェントからの定義の収集を行う。また、クライアント端末上のJP1/IM-Viewからの要求に応じ、認証サーバに対してJP1ユーザーの認証要求や権限取得要求、自身が管理するイベント情報の提供などを行う。マネージャはTOEの範囲外である。

各構成要素の設置環境について以下に示す。

TOEを搭載する認証サーバは、入退出管理が行われたサーバエリアに設置され、サーバエリア内にはTOEに関連する機器のみが設置される。また、サーバエリアには、管理作業を行う管理者及び業務管理者のみが入室可能である。

サーバエリア内のネットワークは、ファイアウォールを介してサーバエリア外のネットワークであるオフィスネットワークと接続されている。

TOEは、クライアント端末を操作するJP1ユーザー及び認証サーバの管理者が利用する。TOEの利用にあたって、JP1ユーザーはTOEが管理するパスワードを、管理者は認証サーバのOSのパスワードを要求されるが、それぞれのパスワードは管理者により推測困難なものが設定される。また、JP1ユーザー及び管理者はパスワードが第三者に知られないように秘密に管理するための各種対策を行う。

JP1/IM（JP1/IM-View及びJP1/IM-Manager）間の通信はSSL等により暗号化されている。

1.2.3.3 TOEの動作概要

TOEは、JP1製品群の一つであるJP1/IM（JP1/IM-View及びJP1/IM-Manager）を介して、または認証サーバから直接利用される。図1-1に示す動作環境において、TOEは以下のとおり、他のJP1製品群と連動する。

① 管理者はシステム構築を行い、サーバエリア内で認証サーバに直接アクセスし、JP1ユーザーの登録及びJP1資源グループ/JP1権限レベルに対するJP1ユーザー名を、TOEへ登録する。
② JP1ユーザーは、管理者から与えられたJP1ユーザー名・パスワードにより、クライアント端末上のJP1/IM-Viewからマネージャ上のJP1/IM-Managerに対してログイン要求を行う。
③ クライアント端末上のJP1/IM-ViewからJP1ユーザー名・パスワードを受け取ったマネージャ上のJP1/IM-Managerは、認証サーバに対して認証要求を行う。
④ 認証サーバ上のTOEはマネージャ上のJP1/IM-Managerから受け取ったJP1ユーザー名・パスワードと、登録された認証情報が一致することを確認し、一致した場合はログイン許可及びセッション情報をマネージャ上のJP1/IM-Managerに返信する。また、一致しない場合はログイン不許可を返信する。
⑤ マネージャ上のJP1/IM-Managerは認証サーバから受け取ったログイン許可/不許可の情報を基に判断を行い、ログイン許可の場合は受け取ったセッション情報をJP1/IM-Manager自身で保持し、さらにクライアント端末上のJP1/IM-Viewに返信する。ログイン不許可の場合は、該当するメッセージをクライアント端末上のJP1/IM-Viewに返信する。
⑥ JP1ユーザーのログインが成功した場合、マネージャ上のJP1/IM-Managerは、当該JP1ユーザーに対応するセッション情報を用いて、TOEから当該JP1ユーザーに関連付けられているJP1資源グループ/JP1権限レベルを取得し、その内容に基づいてJP1製品群に関する操作の許可/不許可の制御を行う。
⑦ JP1製品群に関する操作が許可された場合、JP1ユーザーはその操作を実行することが可能となる。

1.2.3.4 TOEに関係する利用者役割

TOEに関係する利用者とその役割を以下に示す。

【管理者】
サーバエリア内のハードウェア、ソフトウェア、ネットワークに対して責任を持ち、マネージャ、エージェント、ファイアウォール、認証サーバを含むサーバエリア内のTOEに関連するシステムの設定・運用・管理を行う。OSの管理者権限を持ち、システムの構成変更の権限を持つ。基本的にシステム構築時や構成変更時のみアクセスする。

【JP1ユーザー】
TOEの直接の利用者ではないが、クライアント端末上のJP1/IM-Viewを使用してマネージャ上のJP1/IM-Managerを介して、認証サーバ上のTOEに要求を出す。また、クライアント端末上のJP1/IM-Viewを使用し、マネージャ上のJP1/IM-Managerを介して、エージェント上の業務アプリケーションの監視を行う。

【マネージャ】
JP1/IM-Manager及びJP1/Baseがインストールされているマシンであり、JP1ユーザーからの要求に対して、登録済みのJP1ユーザーであるか、JP1/IMに対する操作の要求を行う権限があるか、などを確認するためにTOEに問い合わせを行う。
サーバエリア内に設置され、管理者によって設定・運用・管理される。

1.2.4 TOEの機能

TOEは、システム運用管理のソフトウェアであるJP1製品群の操作権限を一元的に管理するためのユーザー管理/認証機能を有している。ユーザー管理/認証機能は、JP1ユーザー情報、JP1資源グループ/JP1権限レベルを管理する機能である。TOEのセキュリティ機能を表1-1に示す。

表1-1　TOEのセキュリティ機能

セキュリティ機能	概要
識別・認証機能	JP1製品へのログイン時に、JP1ユーザー名・パスワードに基づいて一元的に識別・認証を行う機能である。
アクセス制御機能	識別・認証されたJP1ユーザーに対し、関連付けられているJP1資源グループ/JP1権限レベルを提供する機能である。識別・認証されたJP1ユーザー自身のデータのみアク

	セスを許可する。
セキュリティ管理機能	管理者に対して、JP1ユーザー名・パスワードの登録・変更、JP1資源グループ/JP1権限レベルに対するJP1ユーザー名の登録・削除・表示などの管理機能を提供する。

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「JP1/Base セキュリティターゲット Version 1.13」（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・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、「JP1/Base 認証サーバ 08-10（Windows版） 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8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、EAL2追加である。

追加されるコンポーネントはALC_FLR.1である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、“ SOF-基本 ”を主張する。

本TOEは、高度な専門知識を持たず、クライアント端末からのインタフェースを利用する低レベルの脅威エージェントを想定している。このため、最小機能強度レベルは“ SOF-基本 ”で妥当であると言える。

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1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2　想定する脅威

識別子	脅　威
T.UNDEFINED_USERS	TOEに登録されていない者が、クライアント端末上のJP1/IM-Viewを利用することにより、JP1資源グループ/JP1権限レベルにアクセスするかもしれない。
T.UNAUTHORIZED_ACCESS	TOEに登録されているJP1ユーザーが、クライアント端末上のJP1/IM-Viewを利用することにより、別のJP1ユーザーのJP1資源グループ/JP1権限レベルにアクセスするかもしれない。

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が稼動する認証サーバに要求されるハードウェア及びソフトウェア条件は以下のとおりである。

＜TOEが搭載される認証サーバのハードウェア条件＞

・Microsoft Windows 2000 Server以降のWindowsが搭載できるPC/AT互換機
　ディスク占有量： 約300MB
　標準メモリ量：256MB以上

＜TOEが搭載される認証サーバのソフトウェア条件＞

・Microsoft Windows 2000 ServerまたはWindows Server 2003
・日立製作所 JP1/Base 08-10（TOEが含まれる）

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JP1/IM（JP1/IM-View及びJP1/IM-Manager）に関するソフトウェア条件は以下のとおりである。

＜JP1/IM Viewが搭載されるクライアント端末のソフトウェア条件＞

・Microsoft Windows XP Professional
・日立製作所 JP1/Integrated Management － View 08-10（JP1/IM-Managerを利用するためのGUI）

＜JP1/IM Managerが搭載されるマネージャ端末のソフトウェア条件＞

・Microsoft Windows Server 2003
・日立製作所 JP1/Integrated Management － Manager 08-10
・日立製作所 JP1/Base 08-10（JP1/IM-Managerの前提となる製品）

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1-3　TOE使用の前提条件

識別子	前提条件
A.PHYSICAL	TOEが稼動するハードウェア、マネージャ、エージェント、ファイアウォール、及び業務ネットワーク、管理ネットワークは、物理的に外部から隔離されたサーバエリアに設置され、管理者及び業務管理者以外は入室できない。
A.MANAGE	TOE及びTOEが稼動するために必要なサーバエリア内の

識別子	前提条件
	ハードウェア、ソフトウェア及び業務ネットワーク、管理ネットワークは、管理者によって運用・管理が行われるものとする。また、ガイダンスに従って、JP1製品のログの内容が管理者によって定期的に監査されるものとする。
A.PERSONNEL	管理者は信頼できる人物であり、サーバエリア内のTOEに関連するシステムに対して責任を持っている。また、業務管理者は信頼できる人物であり、サーバエリア内のエージェント上で稼働する業務アプリケーションに対して責任を持っている。管理者及び業務管理者は、故意によりセキュリティに支障をきたすような操作は行わないことを想定する。
A.ADMIN_LOGIN	管理者はサーバエリア内でTOEがインストールされているサーバマシンに管理者アカウントでログインするものと想定する。
A.PROTOCOL	不特定のクライアント端末からサーバエリア内のマシンへの攻撃及び認証サーバに対する直接の攻撃を防ぐため、クライアント端末を接続するオフィスネットワークから、サーバエリア内の業務ネットワーク及び管理ネットワークに対するプロトコル及びIPアドレスはファイアウォールにより制限されているものと想定する。また、業務クライアントからの操作による業務ネットワークに接続されたエージェントからの通信攻撃を防ぐため、業務ネットワークから管理ネットワークに対するプロトコル及びIPアドレスもファイアウォールにより制限されているものと想定する。ファイアウォールの設定については、ガイダンスに従って管理者が設定する。
A.PASSWORD	管理者は、不正な利用者によるログインを防止するため、ガイダンスに従った十分強度のあるパスワードを設定しなければならない。

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。

・取扱説明書 036952 JP1/Base 08-10 認証サーバセキュリティ機能 初版

・JP1/Base 運用ガイド 解説・手引・文法・操作書 第2版

・JP1/Base メッセージ 操作書 第2版

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8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19年4月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、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調査を行った。また、平成19年5月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び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

1) 開発者テスト環境

開発者テストは、表2-1に示す各OSの環境で実施された。

表2-1 開発者テストの構成

TOE	備考
JP1/Base 認証サーバ 08-10 (Windows 版)	JP1/Base 08-10 に含まれ

	る
認証サーバマシン	備考
Microsoft Windows 2000 Server 及び Microsoft Windows Server 2003	OS 左記の2種類のOSにて テストを実施
JP1 Version8 JP1/Base 08-10	Windows 版 インストール時に、認証 サーバとして機能する ように設定
マネージャマシン	備考
Microsoft Windows Server 2003	OS
JP1 Version8 JP1/Base 08-10	Windows 版 認証サーバの設定はしな い
JP1 Version8 JP1/IM-Manager 08-10	Windows 版
クライアント端末	備考
Microsoft Windows XP Professional	OS
JP1 Version8 JP1/IM-View 08-10	Windows 版

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。

a.テスト構成

開発者テストはSTにおいて識別されているTOE構成から以下の要素を取り除いたTOEテスト環境で実施されている。

・ファイアウォールの設置
・業務クライアント及びエージェントマシンの設置
・クライアント端末とマネージャマシン間の保護通信の設定

取り除かれた要素については、TOEの動作に影響を与えないものであることが開発者及び評価者により確認されている。

b.テスト手法

テストには、以下の手法が使用された。

①クライアント端末上のJP1/IM-Viewの操作画面からの操作、画面・ログ出力の確認。

②認証サーバマシン上のコンソール画面からの操作、画面・ログ出力の確認。

③マネージャマシン上のJP1/IM-Managerから特定の入力パラメタをTOE

に送信するための、開発者作成のテストツールの使用と、ログ出力の確認。

c.実施テストの範囲

テストは開発者によって各OSの環境ごとに55項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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

評価者テストは、表2-2に示す各OSの環境で実施された。

表2-2 評価者テストの構成

TOE	備考
JP1/Base 認証サーバ 08-10 (Windows 版)	JP1/Base 08-10 Windows 版(形名：P-242C-6L84)に含まれる
認証サーバマシン	備考
Microsoft Windows 2000 Server 及び Microsoft Windows Server 2003	OS 左記の2種類のOSにてテストを実施 （CPU：Pentium4 mobile 1.5 GHz）
JP1 Version8 JP1/Base 08-10	Windows 版 (形 名 ： P-242C-6L84) インストール時に、認証サーバとして機能するように設定
マネージャマシン	備考
Microsoft Windows Server 2003	OS （CPU：Pentium4 mobile 1.8 GHz）
JP1 Version8 JP1/Base 08-10	Windows 版 (形 名 ：

	P-242C-6L84) 認証サーバとしての設定はしない
JP1 Version8 JP1/IM-Manager 08-10	Windows 版 (形 名 ： P-242C-8E84)
クライアント端末	備考
Microsoft Windows XP Professional	OS （CPU：Pentium4 mobile 1.6 GHz）
JP1 Version8 JP1/IM-View 08-10	Windows 版 (形 名 ： P-242C-6H84)

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

評価者テストはSTにおいて識別されているTOE構成から以下の要素を取り除いたTOEテスト環境で実施されており、開発者テストの環境と同一である。

・ファイアウォールの設置
・業務クライアント及びエージェントマシンの設置
・クライアント端末とマネージャマシン間の保護通信の設定

取り除かれた要素については、TOEの動作に影響を与えないものであることが評価者により確認されている。

b.テスト手法

テストには、以下の手法が使用された。

① クライアント端末上のJP1/IM-Viewの操作画面からの操作、画面・ログ出力の確認。
② 認証サーバマシン上のコンソール画面からの操作、画面・ログ出力の確認。
③ マネージャマシン上のJP1/IM-Managerから特定の入力パラメタをTOE に送信するための、開発者作成のテストツールの使用と、ログ出力の確認。

c.実施テストの範囲

評価者が独自に考案したテストを8項目、開発者テストのサンプリングによるテストを22項目、評価者が独自に考案した侵入テストを7項目、計37項目のテストを各OSの環境で実施した。テスト項目の選択基準として、下記を考慮

している。

① 全てのセキュリティ機能を含める。
② 各セキュリティ機能のインタフェースにおいて、テストされていないパラメタ(限界値)はないか。
③ セキュリティ管理機能においてセキュリティパラメタの変更をした場合、即時に反映されるか。
④ 脆弱性が悪用できないという開発者の根拠のうち、開発者テストでその根拠の検証がされていないもの。
⑤ 開発者の脆弱性分析の十分性の確認の補助として、評価者が有益であると判断したもの。

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EAL2及びALC_FLR.1の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。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。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_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所見報告書による指摘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。
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。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_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。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_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。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_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.2.1E	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_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。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。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、インタビュー及び実地検査により確認している。
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、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_HLD.1.1E	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環境としてのソフト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。
ADV_HLD.1.2E	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、当評価に至るまでになされた所見報告書による指摘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。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。
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。

ライフサイクルサポート	適切な評価が実施された
ALC_FLR.1.1E	評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供され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。
テスト	**適切な評価が実施された**
ATE_COV.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機能仕様に正確に対応していることを確認している。
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を含んで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。
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_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされてい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、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しい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、脆弱性分析が脆弱性に関する情報を考慮していること、識別された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。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。
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。実施したテスト結果とテスト概要について報告がなされている。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。

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
GUI	Graphical User Interface
JP1/IM	JP1/Integrated Management
OS	Operating System
PP	Protection Profile
SOF	Strength of Function
SSL	Secure Socket Layer
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。

JP1/IM	JP1/Baseを基盤として利用するJP1製品の一つで、ITシステム全体の一元的な監視と操作を実現することにより、ITシステムを統合管理するための製品である。 JP1/IM-ManagerとJP1/IM-Viewで構成される。 JP1/IM-Managerはシステム全体を統合管理するためのマネージャ機能を提供する。JP1/IM-Viewはシステムの管理者がJP1/IM-Managerの機能を利用するためのGUIを提供する。 JP1/IMのシステムにおいて、JP1ユーザーを認証するために、JP1/Baseの認証サーバを利用する。またJP1/IMは、JP1/Baseの稼働するホストをエージェントとして監視することができる。
JP1ユーザー情報	JP1ユーザー名とパスワードからなる、JP1ユーザーに関する情報。
JP1資源	JP1/Baseを基盤として利用する各JP1製品が運用管理の対象と

	するリソースである。ジョブ、ジョブネット、イベントなどを含む。
JP1資源グループ	JP1資源の集合に対して付与した名称。
JP1権限レベル	各JP1資源グループに対してどのような操作ができるか（定義、実行、編集、参照など）を、定義したもの。JP1権限レベルによって行える操作は、JP1/Baseを基盤として利用する各JP1製品によってあらかじめ定義されている。
業務管理者	TOEの利用者ではない。サーバエリア内のエージェント上で稼働する業務アプリケーションに対して責任を持ち、業務アプリケーションの運用管理を行う。基本的に障害発生時や業務アプリケーションの設定変更時にサーバエリア内で作業を行う。JP1ユーザーと兼務することができる。
セッション情報	JP1ユーザーが認証サーバによって識別・認証されてから、ログアウトを行うまでの間の接続を識別するためにTOEが生成する情報。

6 参照

[1] JP1/Base セキュリティターゲット Version 1.13（2007年8月9日）
株式会社 日立製作所

[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] JP1/Base 認証サーバ 08-10（Windows版） 評価報告書 第3.0版 2007年8月10日 株式会社電子商取引安全技術研究所 評価センター