JP1/Base
セキュリティターゲット

2007/08/09

Version 1.13

(株)日立製作所

「JP1/Base セキュリティターゲット」

－ 変更歴 －

項番	作成／変更年月日	ST バージョン	更新内容 （概要）	作成／変更者
1	2006/09/12	1.00	新規作成	山下部
2	2007/02/19	1.01	キックオフ会議の結果を反映、及び ENK-EOR-0001-00 の指摘事項を修正	山下部
3	2007/03/09	1.02	ENK-EOR-0002-00 の指摘事項及び評価者の指摘事項、設計内での指摘事項を修正	山下部
4	2007/03/22	1.03	評価者の指摘事項を修正	山下部
5	2007/03/28	1.04	ENK-EOR-0003-00 の指摘事項及び評価者の指摘事項を修正	山下部
6	2007/04/27	1.05	ENK-EOR-0004-00、ENK-EOR-0005-00 の指摘事項及び評価者の指摘事項、設計内での指摘事項を修正	山下部
7	2007/05/08	1.06	評価者の指摘事項を修正	山下部
8	2007/05/21	1.07	評価者の指摘事項を修正	山下部
9	2007/05/28	1.08	評価者の指摘事項を修正	山下部
10	2007/06/04	1.09	評価者の指摘事項を修正	山下部
11	2007/06/13	1.10	評価者の指摘事項を修正	山下部
12	2007/07/06	1.11	評価者の指摘事項を修正	山下部
13	2007/08/08	1.12	評価者の指摘事項を修正	山下部
14	2007/08/09	1.13	評価者の指摘事項の修正	山下部

「JP1/Base セキュリティターゲット」

－ 目次 －

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、用語の定義について記述する。

1.1. ST 識別

ST 名称： JP1/Base セキュリティターゲット
バージョン： 1.13
発行日： 2007 年 8 月 9 日
作成者 株式会社　日立製作所　ソフトウェア事業部
TOE : JP1/Base 認証サーバ
TOE のバージョン： 08-10（Windows 版）
キーワード： 運用管理、認証
適合する CC のバージョン : Common Criteria for Information Technology Security Evaluation Ver2.3 補足-0512 適用

1.2. ST 概要

本ドキュメントは、JP1/Base の認証サーバ機能のセキュリティターゲットである。

JP1/Base は、システム運用管理のソフトウェアである JP1 製品群に対して基盤機能を提供するソフトウェアであり、JP1 製品群のユーザー管理／認証を行う認証サーバ機能を中核として、サービス起動管理機能、イベント発行機能、定義収集・配布機能、プロセス監視機能などを持ち、業務システムの可用性、信頼性を高め、効率良くシステムの運用管理を行うための基盤機能を提供する。

TOE は、JP1/Base の認証サーバ機能である、ユーザー管理／認証機能のソフトウェアコンポーネントである。

TOE のセキュリティ機能には次のものが含まれる。

- 識別・認証機能（JP1 ユーザー名、パスワードによるログイン機能）
- 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・削除、パスワードの変更、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・表示などを行うためのセキュリティ管理機能

1.3. CC 適合の主張

- CC パート 2 適合
- CC パート 3 適合

評価保証レベルは、EAL2 追加（EAL2＋ALC_FLR.1）である。

1.4. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August Version 2.3
  CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 2005 Version 2.3
  CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 2005 Version 2.3
  CCMB-2005-08-003
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology August 2005 Version 2.3
- 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 2005 年 8 月 バージョン 2.3 CCMB-2005-08-001
  平成 17 年 12 月翻訳第 1.0 版
  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
- 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 2005 年 8 月 バージョン 2.3 CCMB-2005-08-002
  平成 17 年 12 月翻訳第 1.0 版
  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
- 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 2005 年 8 月 バージョン 2.3 CCMB-2005-08-003
  平成 17 年 12 月翻訳第 1.0 版
  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
- 情報技術セキュリティ評価のための共通方法
  評価方法 2005 年 8 月 バージョン 2.3 CCMB-2005-08-004
  平成 17 年 12 月翻訳第 1.0 版
  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
- 補足-0512

1.5. 用語

1.5.1. 本 ST における用語

用語	定義内容
JP1 ユーザー	JP1/Base を基盤として利用する各 JP1 製品を操作するユーザー。
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。
※ どの JP1 ユーザーが、どの JP1 資源グループに対して、どのような JP1 権限レベルを持っているかを意味する JP1 資源グループ／JP1 権限レベルのペアが各 JP1 ユーザーと関連付けられて TOE に登録されている。 ※ 本 TOE では、この JP1 ユーザーに関連付けられた、JP1 資源グループ／JP1 権限レベルのペアを利用者データとして取り扱う。 ※ ある JP1 ユーザーが、ある JP1 資源グループに対して実際にアクセスしてよいかどうかを JP1 権限レベルに基づいて判定するのは、JP1/Base を基盤として利用する各 JP1 製品である。	
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。 JP1 ユーザーのログイン中は TOE 内部の JP1 ユーザーを代行するスレッド等によって保持される。ログアウト時に TOE から削除され、セッションは無効になる。
管理者	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管理を行う者である。TOE に関連する各ホストの OS 管理者権限を保持する。 JP1 ユーザーの管理、及び各 JP1 ユーザーに対して JP1 資源グループ／JP1 権限レベルのペアの関連付けを行う。
業務管理者	サーバエリア内のエージェント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管理を行う者である。
業務ユーザー	オフィスエリアの業務クライアントから、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を利用する者である。
JP1/IM	JP1/Integrated Management の略。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。
マネージャ	JP1/IM-Manager 及び JP1/Base がインストールされているホスト。
エージェント	マネージャが管理対象とするホストであり、JP1/Base がインストールされているホスト。

クライアント端末	JP1/IM-View がインストールされたホスト。本端末上の JP1/IM-View からマネージャに接続して JP1/IM-Manager の機能を利用する。

1.5.2. 略語

<CC 関連略語>
CC（Common Criteria）：コモンクライテリア
EAL（Evaluation Assurance Level）：評価保証レベル
IT（Information Technology）：情報技術
PP（Protection Profile）：プロテクションプロファイル
SF（Security Function）：セキュリティ機能
SFP（Security Function Policy）：セキュリティ機能ポリシー
SOF（Strength Of Function）：機能強度
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 Functions）：TOE セキュリティ機能

<TOE 関連略語>
OS（Operating System）：基本ソフト
SNMP（Simple Network Management Protocol）：通信機器等をネットワーク経由で監視・制御するためのプロトコル

2. TOE 記述

本章では、TOE 概要、TOE 関連の利用者役割、TOE の機能、TOE の範囲及び TOE の保護資産について記述する。

2.1. TOE の概要

2.1.1. TOE 種別

JP1/Base は、システム運用管理のソフトウェアである JP1 製品群に対して基盤機能を提供するソフトウェア製品である。TOE は、認証サーバ上で動作する JP1/Base のユーザー管理／認証機能である。

2.1.2. TOE を利用したシステム概要

TOE を利用したシステム概要を図 2-1 に示す。TOE が提供する基盤機能は、JP1/IM によって利用される。ここでは JP1/IM を利用したシステム構成を示す。

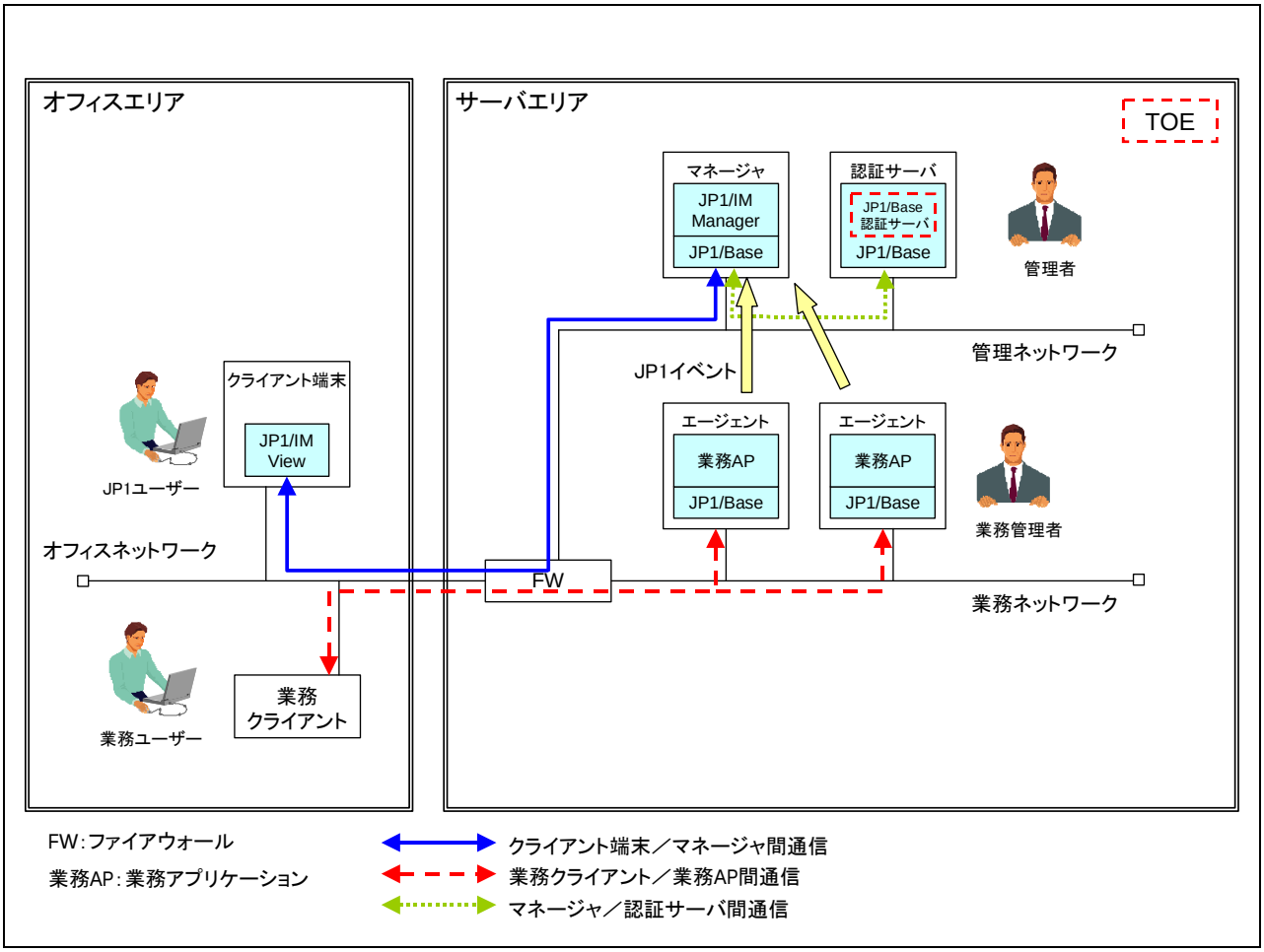

図 2-1 TOE を利用したシステム概要

図 2-1 に示したシステムを構成する構成要素について説明する。

【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。

【エージェント】
マネージャが管理対象とする業務アプリケーション及び JP1/Base がインストールされ、マネージャによって管理されている管理対象ホストである。エージェント上で通知すべき事象（JP1 イベント）が発生した場合、マネージャに対してイベント通知を行う。また、マネージャからの指示に従い、定義ファイルの送受信を行う。エージェントは TOE の範囲外である。

【認証サーバ】
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、及び 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】
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 ユーザーに対して、許可された操作のみ利用可能である。クライアント端末は TOE の範囲外である。

【業務クライアント】
マネージャが管理対象とする業務アプリケーションを操作するためのクライアントである。業務ユーザーは、業務クライアントを使用して、エージェント上の業務アプリケーションにアクセスし、サービスを利用する。業務クライアントは TOE の範囲外である。

マネージャ、エージェント、認証サーバは、オフィスエリアから隔離され、入退出管理のされたサーバエリアに設置される。サーバエリアには、TOE に関連する機器のみ設置される。サーバエリアには、サーバエリア内のハードウェア・ソフトウェア・ネットワークの管理を行う管理者及び業務アプリケーションの管理を行う業務管理者のみが入室できる。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は、ファイアウォールを介してオフィスネットワークに接続されている。

クライアント端末及び業務クライアントは通常の業務などを行うオフィスエリアに設置する。
JP1 ユーザーはクライアント端末上の JP1/IM-View を使用して、オフィスネットワーク・管理ネットワークを介してマネージャにアクセスする。
業務ユーザーは業務クライアントを使用して、オフィスネットワーク・業務ネットワークを介してエージェント上の業務アプリケーションにアクセスする。

クライアント端末とマネージャ間の通信路は、SSL などにより漏洩・改ざんから保護されているものとする。

次に、図 2－1 に示したシステムにおける動作の流れを以下に示す。

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 権限レベルに対して JP1 ユーザー名を登録する。
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は、認証サーバに対して認証要求を行う。
4) 認証サーバはマネージャから受け取った 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マネージャ自身で保持し、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に成功した場合は、マネージャが保持するセッション情報を用いて以後の操作を行う。
   ※JP1/IM-View とマネージャの間のセッションは、TCP/IP によるセッションであり、セッション情報は利用しない。
7) 例えば、ある JP1 資源グループの参照操作を行おうとすると、この要求は JP1/IM-View からマネージャに送信される。
8) マネージャは当該 JP1 ユーザーが当該操作を行ってよいかどうかを、マネージャ自身が保持している、要求元の JP1/IM-View に対応するセッション情報と伴に認証サーバに問い合わせる。
9) 認証サーバは、セッション情報を基に当該 JP1 ユーザーに関連付けられている JP1 資源グループ／JP1 権限レベルをマネージャに返信する。
10) マネージャは、認証サーバから受け取った JP1 資源グループ／JP1 権限レベルの情報を基に当該操作の許可／不許可を判断する。

- 業務ユーザーは、業務クライアントからエージェント上の業務アプリケーションにアクセスして、サービスを利用する。
- エージェント上で通知すべき事象（JP1 イベント）が発生した場合、マネージャに対してイベント通知を行う。

2.2. TOE 関連の利用者役割

TOE に関連する利用者とその役割を以下に説明する。

【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。

TOE に対しては、以下のような操作を行う。

- JP1 ユーザー名・パスワードの登録・削除，及びパスワードの変更
- 各 JP1 ユーザーに対する JP1 資源グループ／JP1 権限レベルの登録・削除・変更
- JP1/Base が提供するサービスの起動・停止順序の変更や，サービスの起動・停止
- イベントサービスの定義収集・配付やイベントサービスの起動・停止
- イベント変換機能の設定や起動・停止

【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を介して、認証サーバに要求を出す。また、クライアント端末上の JP1/IM-View を使用してマネージャを介して、エージェント上の業務アプリケーションの監視を行う。

以下のような操作を行う。

- イベント情報を閲覧し，業務システムに異常が発生していないか監視を行う
- 特定のイベント発生時の対処法を示すイベントガイドに従い，問題の調査・対策を行う
- 異常発生時の問題を調査・対策するためのエージェントに対するコマンド実行要求や，コマンド実行状態の確認及びコマンドの削除を行う
- 特定のイベントが発生した時に自動的にコマンドを実行する自動アクションの設定，キャンセル，結果や状態の確認を行う

【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。

JP1 ユーザーに対して、以下のサービスを提供する。

- 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 にログインする際に，認証サーバに対してユーザー識別・認証要求を行う
- クライアント端末上の JP1/IM-View からの要求により，認証サーバに対して JP1 資源グループ／JP1 権限レベルの取得要求を行う
- クライアント端末上の JP1/IM-View からの要求により，認証サーバに対して JP1 資源グループ／JP1 権限レベルのチェック要求を行う
- クライアント端末上の JP1/IM-View からの要求により，認証サーバに対してログアウト要求を行う
- クライアント端末上の JP1/IM-View からの要求により，マネージャが保持するイベント DB に保存されているイベント情報を送信する
- エージェントから特定のイベントを受信した場合に実行する自動アクションの設定を行う

次に、TOE に関係しない利用者とその役割を以下に記述する。

【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。

【業務ユーザー】

TOE の利用者ではない。オフィスエリアに設置された業務クライアントから、エージェント上で稼働する業務アプリケーションを利用する。

2.3. TOE の機能

JP1/Base は、システムの運用管理製品群に対して基盤機能を提供する。JP1/Base は各運用管理製品のユーザー管理／認証を一元的に行う認証サーバ機能を中核として、サービスの起動／停止を管理したり、イベントを収集・管理したりすることができる。

JP1/Base によって提供されるメイン機能及び TOE によって提供されるセキュリティ機能を次に示す。

2.3.1. JP1/Base によって提供される機能

JP1/Base が提供する機能とその概要を示す。TOE は、表 2-1 に示すユーザー管理／認証機能である。

表 2-1 JP1/Base が提供するメイン機能

機能	概要
ユーザー管理／認証機能	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。この機能により、JP1 ユーザーのエージェントに対する、JP1/Base を利用する各 JP1 製品の操作権限を一元的に管理することが出来る。
サービスの起動管理機能	サービスの起動順序や終了順序を制御する機能である。 あらかじめ定義した順序に従ってサービスを起動したり、終了したりすることができる。
イベントサービス機能	システムで何らかの事象が発生したときに JP1/Base に通知される事象（JP1 イベント）を管理したり，運用管理対象のホスト間で JP1 イベントを送受信したりする機能である。
イベント変換機能	管理対象の業務アプリケーションのログメッセージや、OS のイベントログ、SNMP トラップなどを JP1 イベントに変換する機能である。この機能を使って，ログメッセージや SNMP トラップを JP1/Base の管理形式である JP1 イベントに変換できる。
定義収集・配布機能	JP1 製品で定義した情報を収集および配布する機能である。この機能を利用すると、イベントサービスの定義情報の収集・配布や，JP1 製品が管理する定義情報を収集することができる。
プロセス管理機能	JP1/Base 自身の起動・停止などの動作を行う機能である。

2.3.2. TOE によって提供されるセキュリティ機能

本 TOE が提供するセキュリティ機能とその概要を示す。

表 2-2 TOE が提供するセキュリティ機能

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。

2.3.3. TOE によって提供されないセキュリティ機能

- TOE の管理者の識別･認証には、OS の識別･認証機能を利用する。
- クライアント端末、業務クライアント、マネージャ、エージェント間の情報フロー制御には、ファイアウォールを利用する。管理者は、サーバエリア内にファイアウォールを設置し、以下に示すルールに従って設定を行う。

発信元	宛先
クライアント端末	マネージャ：JP1/IM-Manager のサービスポート
業務クライアント	エージェント：業務アプリケーションのサービスポート
エージェント	マネージャ：イベントサービスポート

2.4. TOE の範囲

2.4.1. TOE の範囲

TOE は、第 2.1.2 節の図 2-1 において、認証サーバ上に TOE として破線で囲まれた部分であり、第 2.3.1 節の表 2-1 において、「ユーザー管理／認証機能」として示したソフトウェアコンポーネントである。

2.4.2. ハードウェア条件

TOE が稼動するためのハードウェア条件を以下に示す。

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

2.4.3. ソフトウェア条件

TOE が稼動するためのソフトウェア条件を以下に示す。

ベンダ名	製品名	説明
Microsoft	Windows 2000 Server または Windows Server 2003	オペレーティングシステムである。
(株)日立製作所	JP1/Base 08-10	TOE を含む製品である。

※ 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、本 ST では以下のソフトウェアを前提としている。

＜マネージャ＞

ベンダ名	製品名	説明
Microsoft	Windows Server 2003	オペレーティングシステムである。
(株)日立製作所	JP1/Integrated Management － Manager 08-10	TOE を利用するソフトウェアである。
	JP1/Base 08-10	JP1/Integrated Management - Manager の前提製品である。

＜クライアント端末＞

ベンダ名	製品名	説明
Microsoft	Windows XP Professional	オペレーティングシステムである。
(株)日立製作所	JP1/Integrated Management － View 08-10	JP1/Integrated Management - Manager を利用するための GUI である。

2.5. TOE の保護資産

第 2.3.1 節で示したように、JP1/Base は JP1 製品群に対して各種基盤機能を提供するが、中核となるのは、JP1 製品群のユーザー管理／認証を行う認証サーバ機能であり、表 2-1 に示したユーザー管理機能が取り扱うデータが主要な保護資産となる。

従って、TOE は、以下の JP1 資源グループ／JP1 権限レベルを権限外の参照から保護する。

- JP1 資源グループ／JP1 権限レベル

本データは、JP1/Base を利用する各 JP1 製品の権限情報に関する重要なデータであり、JP1 ユーザーによって変更されてはならない。JP1 ユーザーは自身に割り当てられたデータのみ参照できる。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティポリシーについて記述する。

3.1. 前提条件

本 TOE が想定する前提条件を次に示す。

ID	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。

3.2. 脅威

本 TOE が想定する脅威を次に示す。

ID	想定する脅威
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。

3.3. 組織のセキュリティポリシー

本 TOE が想定する組織のセキュリティポリシーは無い。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針及び環境セキュリティ対策方針について記述する。

4.1. TOE セキュリティ対策方針

O.I&A

TOE は、登録されていないユーザーから、JP1 資源グループ／JP1 権限レベルへのアクセスを保護するために識別・認証を行う。

O.ACC

TOE は、登録されている JP1 ユーザーが、別の JP1 ユーザーの、JP1 資源グループ／JP1 権限レベルへのアクセスを保護するために、アクセス制御を行う。

O.MGT

TOE は、JP1 ユーザーの識別・認証情報、及び JP1 資源グループ／JP1 権限レベルに対応付けられる JP1 ユーザー名を管理者のみが管理できるように制御する。

4.2. 環境セキュリティ対策方針

4.2.1. IT 環境のセキュリティ対策方針

OE.I&A

正当な管理者に対してのみ TOE の管理を許可するために、TOE が動作する OS の識別・認証機能を利用する。

OE.SECURE_CHANNEL

クライアント端末とマネージャ間の通信路は、暗号化などがなされた保護通信路を用い，暴露・改ざんから保護する。

4.2.2. 運用により実現するセキュリティ対策方針

OM.PHYSICAL

管理者は、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、管理ネットワークを、物理的に外部から隔離されたサーバエリアに設置する。また、管理者及び業務管理者以外がサーバエリアに入室できないように、入退室管理を行わなければならない。

OM.FIREWALL

管理者は、オフィスネットワークと、業務ネットワーク及び管理ネットワークの境界にファイアウォールを設置し、業務ネットワークと管理ネットワークを論理的に分離し、許可されたプロトコル及び IP アドレス宛の通信のみ通過させるように設定・維持・管理する。

OM.ADMIN

- 管理者には、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おり、悪意のある行為は行わず、信頼できる者を選定する。
- 管理者は、TOE に関するトレーニングをすることにより、TOE の運用・管理について熟知する。
- 管理者は、IT 環境として利用するそれぞれの機器の運用・管理について熟知する。
- 管理者は、TOE、及び IT 環境の運用・管理において、セキュリティ面での注意点を考慮して、運用・管理を行う。
- 管理者は、ガイダンスに従って定期的に JP1 製品のログを確認する。
- 管理者は、JP1 ユーザーに対して、クライアント端末に不要なアプリケーションがインストールされないような対策をとるよう周知・徹底する。
- 管理者は、JP1 ユーザー及び管理者自身の OS ユーザーの登録に際して、推測されにくく、十分強

度のあるパスワードを設定する。

- 管理者は、JP1 ユーザーに対して、JP1 ユーザー自身のパスワードを他人に知られないように管理するよう指導する。
- 管理者は、業務管理者の選出において、業務アプリケーションに対して責任を持ち、悪意のある行為を行わず、信頼できる者を選定する。

5. IT セキュリティ要件

本章では、TOE のセキュリティ要件、IT 環境セキュリティ要件について記述する。

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

TOE が提供するセキュリティ機能の機能要件を記述する。すべての機能要件コンポーネントは、CC パート 2 で規定されているものを直接使用する。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1 TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]

	サブジェクト	オブジェクト	操作
1	JP1/Base ログインスレッド	JP1資源グループ／JP1権限レベル コンテナ	参照

[割付: アクセス制御SFP]
JP1/Baseアクセス制御ポリシー

依存性: **FDP_ACF.1** セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1 TSF は、以下の[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

[割付: 示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ]

	サブジェクト	サブジェクト属性	オブジェクト	オブジェクト属性
1	JP1/Base ログインスレッド	JP1ユーザー名	JP1資源グループ／ JP1権限レベルコンテナ	JP1ユーザー名

[割付: アクセス制御SFP]
JP1/Baseアクセス制御ポリシー

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

a) サブジェクトに関連付けられたJP1ユーザー名が、オブジェクトに関連付けられたJP1ユーザー名と一致した場合のみ、当該JP1ユーザー及び指定したJP1資源グループに関するJP1権限レベルを参照できる
b) サブジェクトに関連付けられたJP1ユーザー名が、オブジェクトに関連付けられたJP1ユーザー名と一致した場合のみ、当該JP1ユーザーが指定したJP1資源グループに対して指定したJP1権限レベルを保持しているかどうかを問い合わせできる
c) 上記以外の場合、JP1資源グループ／JP1権限レベルコンテナへのアクセスは許可しない

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則]
なし

FDP_ACF.1.4 TSF は、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェ

クトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]
なし

依存性: **FDP_ACC.1** サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FIA_UAU.2a アクション前の利用者認証

下位階層: **FIA_UAU.1**

FIA_UAU.2.1a TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性: **FIA_UID.1** 識別のタイミング

FIA_UID.2a アクション前の利用者識別

下位階層: **FIA_UID.1**

FIA_UID.2.1a TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:セキュリティ属性のリスト]を維持しなければならない。

[割付：セキュリティ属性のリスト]

- JP1ユーザー名

依存性: なし

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1 TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: 利用者セキュリティ属性のリスト]

[割付：利用者セキュリティ属性のリスト]

- JP1ユーザー名

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: 属性の最初の関連付けに関する規則]

[割付：属性の最初の関連付けに関する規則]
なし

FIA_USB.1.3 TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: 属性の変更に関する規則]

[割付：属性の変更に関する規則]
なし

依存性: **FIA_ATD.1** 利用者属性定義

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割]
管理者

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

依存性: **FIA_UID.1** 識別のタイミング

FMT_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

上述の割付及び選択を下表に示す。

TSFデータ	選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]	許可された識別された役割
JP1ユーザー名	追加、削除、問い合わせ	管理者
パスワード	変更，追加，削除	管理者

依存性: **FMT_SMF.1** 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1 TSF は、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付: 許可された識別された役割]に制限するために[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

上述の割付及び選択を下表に示す。

セキュリティ属性のリスト	選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]	許可された識別された役割	アクセス制御SFP 情報フロー制御SFP
オブジェクトに関連付けられたJP1ユーザー名	追加、削除、問い合わせ	管理者	JP1/Baseアクセス制御ポリシー

依存性: [**FDP_ACC.1** サブセットアクセス制御または
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層： なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付： TSF によって提供されるセキュリティ管理機能のリスト]。

[割付： TSF によって提供されるセキュリティ管理機能のリスト]

表 5-1 TSF によって提供されるセキュリティ管理機能のリスト

機能要件	管理要件	管理項目
FDP_ACC.1	なし	なし
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	なし(明示的なアクセスまたは拒否に関する規則は無いため、管理対象とならない)
FIA_UAU.2a	a)管理者による認証データの管理 b)このデータに関係する利用者による認証データの管理。	a)JP1ユーザーのパスワードの登録・削除・変更 b)なし(JP1ユーザーは、自身のパスワードを変更できないため、管理対象とならない)
FIA_UID.2a	利用者識別情報の管理。	JP1ユーザー名の登録・削除・参照
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし(利用者に対する追加のセキュリティ属性は無いため、管理対象とならない)

FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	a) なし(デフォルトのサブジェクト属性は無いため、管理対象とならない) b) なし(デフォルトのサブジェクト属性は無いため、管理対象とならない)
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	なし(利用者のグループの概念が無いため、管理対象とならない)
FMT_MTD.1	TSFデータと相互に影響を及ぼし得る役割のグループを管理すること。	なし(役割のグループの概念が無いため、管理対象とならない)
FMT_MSA.1	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	なし(役割のグループの概念が無いため、管理対象とならない)
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし

依存性： なし

FPT_RVM.1　TSP の非バイパス性

下位階層 ： なし

FPT_RVM.1.1　TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性 ：　なし

FPT_SEP.1　TSF ドメイン分離

下位階層 ： なし

FPT_SEP.1.1　TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2　TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性 ：　なし

5.1.2. 最小機能強度レベル

本 TOE の最小機能強度レベルは、低程度(SOF-基本)である。

5.1.3. TOE セキュリティ保証要件

TOE のセキュリティ保証要件を記述する。

本 TOE の評価保証レベルは EAL2 であり、追加する保証コンポーネントは ALC_FLR.1 である。すべての保証要件コンポーネントは、CC パート 3 で既定されている評価コンポーネントを直接使用する。EAL2＋ALC_FLR.1 の評価コンポーネントを表 5-1 に示す。

表 5-2 EAL2＋ALC_FLR.1 評価コンポーネント一覧

保証クラス	保証コンポーネント	
構成管理（ACM クラス）	**ACM_CAP.2**	構成要素
配付と運用（ADO クラス）	**ADO_DEL.1**	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
開発（ADV クラス）	**ADV_FSP.1**	非形式的機能仕様
	ADV_HLD.1	記述的上位レベル設計
	ADV_RCR.1	非形式的対応の実証
ガイダンス文書（AGD クラス）	**AGD_ADM.1**	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート（ALC クラス）	**ALC_FLR.1**	基本的な欠陥修正
テスト（ATE クラス）	**ATE_COV.1**	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定（AVA クラス）	**AVA_SOF.1**	TOE セキュリティ機能強度評価
	AVA_VLA.1	開発者脆弱性分析

5.2. IT 環境セキュリティ機能要件

FIA_UAU.2b アクション前の利用者認証

下位階層: **FIA_UAU.1**

FIA_UAU.2.1b TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

【詳細化】: TSF は → OS は

依存性: **FIA_UID.1** 識別のタイミング

FIA_UID.2b アクション前の利用者識別

下位階層: **FIA_UID.1**

FIA_UID.2.1b TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

【詳細化】: TSF は → OS は

依存性: なし

FTP_ITC.1 TSF 間高信頼チャネル

下位階層 : なし

FTP_ITC.1.1 TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC.1.2 TSF は、[選択: TSF、リモート高信頼 IT 製品]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

[選択: TSF、リモート高信頼 IT 製品]

リモート高信頼 IT 製品

FTP_ITC.1.3 TSF は、[割付: 高信頼チャネルが要求される機能のリスト]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付: 高信頼チャネルが要求される機能のリスト]

JP1 ユーザーの識別・認証に使用する JP1 ユーザー名・パスワードの送信

【詳細化】: TSF は → JP1/IM – Manager は

依存性 : なし

6. TOE 要約仕様

6.1. TOE セキュリティ機能

本節では、TOEのセキュリティ機能を説明する。本節で説明するセキュリティ機能は、第 5.1.1節で記述したTOEセキュリティ機能要件を満たすものである。

表 6-1 TOE セキュリティ機能とセキュリティ機能要件の対応関係

TOE セキュリティ機能要件 / TOE セキュリティ機能	FDP_ACC.1	FDP_ACF.1	FIA_UAU.2a	FIA_UID.2a	FIA_ATD.1	FIA_USB.1	FMT_SMR.1	FMT_MTD.1	FMT_MSA.1	FMT_SMF.1	FPT_RVM.1	FPT_SEP.1
SF.I&A			○	○		○					○	○
SF.MGT					○		○	○	○	○		○
SF.ACC	○	○									○	○

6.1.1. 識別・認証機能 (SF.I&A)

JP1 ユーザーは、JP1 製品の操作を開始する際、ログイン操作を行う。このログイン操作により、マネージャを経由して TOE にログイン要求が行われる。

SF.I&A は、ログイン要求で受信した JP1 ユーザー名・パスワードが、TOE に登録済みの JP1 ユーザー名・パスワードと一致することの確認を行う。識別・認証に成功した場合は認証済みのサブジェクト、すなわち JP1/Base ログインスレッドを生成し、JP1 ユーザー名を関連付ける。識別・認証に使用する JP1 ユーザー名・パスワードは、**SF.MGT** により TOE に登録される。

識別・認証に成功した場合、**SF.I&A** は、セッション情報を生成しログイン要求元に返信する。

識別・認証に失敗した場合、**SF.I&A** は、エラーを返信する。

JP1 製品に対する操作が完了した場合、JP1 ユーザーはログアウト操作を行う。このログアウト操作により、マネージャを経由して TOE にログアウト要求が行われる。

SF.I&A は、ログアウト要求で受信したセッション情報をもとに、TOE で管理するセッション情報を削除する。

JP1 ユーザーからマネージャを経由して、ログイン要求が行われた場合、**SF.I&A** が必ず実施されることを保証する。

また JP1/Base ログインスレッド毎にサブジェクトに関連付けられた JP1 ユーザー名とセッション情報を管理するため、**SF.I&A** は、別の JP1/Base ログインスレッドからサブジェクトに関連付けられた JP1 ユーザー名が変更されないことを保証する。

6.1.2. セキュリティ管理機能 (SF.MGT)

SF.MGT は、以下の JP1 ユーザーの管理機能を管理者に提供する。

- JP1 ユーザー名・パスワードの登録
- JP1 ユーザー名・パスワードの削除
- パスワードの変更
- JP1 ユーザー一覧表示
- 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
- JP1 資源グループ／JP1 権限レベルに対する JP1 ユーザー名の削除
- JP1 資源グループ／JP1 権限レベルに対する JP1 ユーザー名**の表示**

SF.MGT は、これらの機能を管理コマンドとして提供し、管理コマンドを実行できる役割を、管理者に制限する。

また、管理者は、JP1 資源グループ／JP1 権限レベルを、JP1 ユーザー毎に登録するため、**SF.MGT** は、別のオブジェクトに関連付けられた JP1 ユーザー名が変更されないことを保証する。

SF.MGT は、セキュリティ属性である JP1 ユーザー名を維持・管理する。

SF.MGT は、本機能の利用に際して、管理コマンドを実行した役割を維持する。

SF.MGT は、サブジェクトである JP1/Base ログインスレッドが、サブジェクトに関連付けられた JP1 ユーザー名に直接アクセスすることが無いことを保証する。

6.1.3. アクセス制御機能 (SF.ACC)

サブジェクトである JP1/Base ログインスレッドがオブジェクトである JP1 資源グループ／JP1 権限レベルコンテナにアクセスする際に、**SF.ACC** は、JP1/Base ログインスレッドに割り付けられた JP1 ユーザー名に基づいて、以下のルールに従いアクセス制御を行う。

a) サブジェクトに関連付けられたJP1ユーザー名が、オブジェクトに関連付けられたJP1ユーザー名と一致した場合のみ、当該JP1ユーザー及び指定したJP1資源グループに関するJP1権限レベルを参照できる

b) サブジェクトに関連付けられたJP1ユーザー名が、オブジェクトに関連付けられたJP1ユーザー名と一致した場合のみ、当該JP1ユーザーが指定したJP1資源グループに対して指定したJP1権限レベルを保持しているかどうかを問い合わせできる

c) 上記以外の場合、JP1資源グループ／JP1権限レベルコンテナへのアクセスは許可しない

アクセスが許可された場合のみ、**SF.ACC** は、当該 JP1 ユーザーが JP1 資源グループに対してどのような JP1 権限レベルを持っているかを返信する。

また、アクセスが許可された場合のみ、**SF.ACC** は、当該 JP1 ユーザーが指定された JP1 資源グループに対して指定された JP1 権限レベルを保持しているかを判定し、結果を返信する。

JP1/Base ログインスレッドが JP1 資源グループ／JP1 権限レベルコンテナにアクセスする際、**SF.ACC** が必ず実施されることを保証する。

また、JP1 資源グループ／JP1 権限レベルは、管理者が JP1 ユーザー名毎に登録するため、**SF.ACC** は、別の JP1/Base ログインスレッドからオブジェクトに関連付けられた JP1 ユーザー名が変更されないことを保証する。

6.2. セキュリティ機能強度

確率的かつ順列的メカニズムを使用したセキュリティ機能は、**SF.MGT** 及び **SF.I&A** で実現する JP1 ユーザーのパスワードに関する機能であり、機能強度レベルは SOF-基本である。

6.3. 保証手段

本 ST で適用するセキュリティ保証要件とセキュリティの保証手段の対応を表 6-2 に示す。本 ST で適用するセキュリティ保証手段として、以下に示すドキュメントを提供する。以下のセキュリティ保証手段は、第 5.1.3 節で記述した TOE セキュリティ保証要件を満たすものである。

表 6-2 保証手段と保証要件コンポーネントの対応関係

保証要件クラス	保証要件コンポーネント	保証手段
ACM：構成管理	**ACM_CAP.2**	JP1/Base 構成管理文書
ADO：配付と運用	**ADO_DEL.1**	JP1/Base 配付文書
	ADO_IGS.1	取扱説明書 JP1/Base 08-10 認証サーバセキュリティ機能 JP1 Version 8 JP1/Base 運用ガイド
ADV：開発	**ADV_FSP.1**	JP1/Base 機能仕様書
	ADV_HLD.1	JP1/Base 構造設計書
	ADV_RCR.1	JP1/Base 対応分析書
AGD：ガイダンス文書	**AGD_ADM.1**	取扱説明書 JP1/Base 08-10 認証サーバセキュリティ機能 JP1 Version 8 JP1/Base 運用ガイド JP1 Version 8 JP1/Base メッセージ
	AGD_USR.1	
ALC：ライフサイクルサポート	**ALC_FLR.1**	JP1/Base セキュリティ欠陥修正規程書
ATE：テスト	**ATE_COV.1**	JP1/Base テスト分析書
	ATE_FUN.1	JP1/Base テスト仕様書／報告書
	ATE_IND.2	JP1/Base 08-10
AVA：脆弱性評定	**AVA_SOF.1**	JP1/Base セキュリティ機能強度分析書
	AVA_VLA.1	JP1/Base 脆弱性分析書

7. PP 主張

本章では、PP 主張について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修整

修整した PP はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

8.1. セキュリティ対策方針根拠

セキュリティ対策方針は、TOE セキュリティ環境で規程した脅威に対抗するためのものであり、前提条件と組織のセキュリティポリシーを実現するためのものである。セキュリティ対策方針と対応する前提条件・脅威および組織のセキュリティポリシーの対応関係を表 8-1 に示す。

表 8-1 セキュリティ対策方針と対応する前提条件・脅威・組織のセキュリティポリシー

前提条件 脅威 組織のセキュリティポリシー セキュリティ対策方針	T.UNDEFINED_USERS	T.UNAUTHORIZED_ACCESS	A.PHYSICAL	A.MANAGE	A.PERSONNEL	A.ADMIN_LOGIN	A.PROTOCOL	A.PASSWORD
O.I&A	○							
O.ACC		○						
O.MGT	○	○						
OE.I&A	○	○				○		
OE.SECURE_CHANNEL	○							
OM.PHYSICAL			○			○		
OM.FIREWALL						○	○	
OM.ADMIN	○			○	○	○		○

表 8-1 により、各セキュリティ対策方針は、１つ以上の脅威、前提条件、または組織のセキュリティポリシーに対応している。

次に、各脅威・前提条件・組織のセキュリティポリシーがセキュリティ対策方針で実現できることを説明する。

＜脅威＞

T.UNDEFINED_USERS

O.I&A により、TOE は、登録されている JP1 ユーザーを識別・認証する。また、**O.MGT** により、JP1 ユーザーの識別・認証情報を管理者のみが管理できるように制御する。この管理機能を正当な管理者のみに制限するために、**OE.I&A** により OS の識別・認証機能を利用する。

オフィスネットワーク上での JP1 ユーザーの識別・認証情報の盗聴により、この脅威が発生する可能性があるが、**OE.SECURE_CHANNEL** により IT 環境であるクライアント端末とマネージャ間で SSL などの暗号化通信を使用し、通信路の保護を行う。

OM.ADMIN により、JP1 ユーザーは、JP1 ユーザー自身のパスワードを他人に知られないように管理し、またクライアント端末には不要なアプリケーションがインストールされないように管理する。

以上により、**T.UNDEFINED_USERS** は、**O.I&A**、**O.MGT**、**OE.I&A**、**OE.SECURE_CHANNEL**、**OM.ADMIN** により対抗できる。

T.UNAUTHORIZED_ACCESS

O.ACC により、TOE は、登録されている権限のない JP1 ユーザーから JP1 資源グループ／JP1 権限レベルコンテナを保護するためにアクセス制御を行う。また、**O.MGT** により、アクセス制御に用いるセキュリティ属性情報を管理者のみが管理できるように制御する。この管理機能を正当な管理者のみに制限するために、**OE.I&A** により OS の識別・認証機能を利用する。

以上により、**T.UNAUTHORIZED_ACCESS** は、**O.ACC**、**O.MGT**、**OE.I&A** により対抗できる。

＜前提条件＞

A.PHYSICAL

OM.PHYSICAL により、管理者は、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、管理ネットワークを、物理的に外部から隔離されたサーバエリアに設置する。また、管理者及び業務管理者以外がサーバエリアに入室できないように、入退室管理を行う。

以上により、**A.PHYSICAL** は、**OM.PHYSICAL** により実現できる。

A.MANAGE

OM.ADMIN により、

- 管理者は、TOE のガイダンス文書を読み、TOE の運用・管理について熟知する。
- 管理者は、IT 環境として利用するそれぞれの機器の取扱説明書を読み、当該機器の運用・管理について熟知する。
- 管理者は、TOE のガイダンス文書に従い、TOE、及び IT 環境の運用・管理において、セキュリティ面での注意点を考慮して、運用・管理を行う。

- 管理者は、ガイダンスに従って、JP1 製品のログを定期的に確認する。

以上により、**A.MANAGE** は、**OM.ADMIIN** により実現できる。

A.PERSONNEL

OM.ADMIN により、

- 管理者には、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おり、悪意のある行為は行わず、信頼できる者を選定する。
- 管理者は、TOE のガイダンス文書を読み、TOE の運用・管理について熟知する。
- 管理者は、IT 環境として利用するそれぞれの機器の取扱説明書を読み、当該機器の運用・管理について熟知する。
- 業務管理者は、業務アプリケーションに対して責任を持ち、悪意のある行為を行わず、信頼できる者が管理者によって選定される。

以上により、**A.PERSONNEL** は、**OM.ADMIN** により実現できる。

A.ADMIN_LOGIN

OM.PHYSICAL により、サーバエリアは物理的に外部から隔離されており、管理者及び業務管理者のみ入室が可能である。また、**OM.FIREWALL** により、管理者はオフィスネットワークと業務ネットワーク及び管理ネットワークの境界にファイアウォールを設置し、オフィスネットワークからサーバエリア内のネットワークへの通信プロトコルを制限することにより、telnet や ftp などによる外部からのログインを防ぐことができる。さらに **OE.I&A** により、管理者は OS の管理者アカウントで識別認証を行う。**OM.ADMIN** により、管理者はサーバエリア内の TOE に関連するシステムに対して責任を持っており、悪意のある行為は行わず、信頼できる。また、業務管理者はサーバエリア内のエージェント上の業務アプリケーションに対して責任を持っており、悪意のある行為は行わず、信頼できる。

以上により、**A.ADMIN_LOGIN** は **OM.PHYSCAL**、**OM.FIREWALL**、**OE.I&A**、**OM.ADMIN** により実現できる。

A.PROTOCOL

OM.FIREWALL により、管理者はオフィスネットワークと業務ネットワーク及び管理ネットワークの境界にファイアウォールを設置し、クライアント端末からマネージャへの通信及び、業務クライアントからエージェントへの通信、エージェントからマネージャへの通信を必要最小限のプロトコル及び IP アドレスに制限することができる。

以上により、**A.PROTOCOL** は **OM.FIREWALL** により実現できる。

A.PASSWORD

OM.ADMIN により、管理者は、JP1 ユーザー及び管理者自身の OS ユーザーの登録に際して，推測され

にくく、十分強度のあるパスワードを設定する。

以上により、**A.PASSWORD** は、**OM.ADMIN** により実現できる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

本 ST で選択した TOE 及び IT 環境のセキュリティ機能要件とセキュリティ対策方針の対応関係を表 8-2 に示す。

表 8-2 セキュリティ機能要件とセキュリティ対策方針の対応関係

TOE セキュリティ対策方針 / TOE セキュリティ機能要件	O.I&A	O.ACC	O.MGT	OE.I&A	OE.SECURE_CHANNEL
FDP_ACC.1		○			
FDP_ACF.1		○			
FIA_UAU.2a	○				
FIA_UID.2a	○				
FIA_ATD.1			○		
FIA_USB.1	○				
FMT_SMR.1			○		
FMT_MTD.1			○		
FMT_MSA.1			○		
FMT_SMF.1			○		
FPT_RVM.1	○	○			
FPT_SEP.1	○	○	○		
FIA_UAU.2b				○	
FIA_UID.2b				○	
FTP_ITC.1					○

表 8-2 により、TOE の各セキュリティ機能要件は、1 つ以上の TOE セキュリティ対策方針に対応している。また、IT 環境の各セキュリティ機能要件は、1 つ以上の IT 環境のセキュリティ対策方針に対応している。

次に、TOE の各セキュリティ対策方針が、TOE のセキュリティ機能要件で実現できることを説明す

る。

O.I&A

TOE は、利用者が TOE の保護対象資産にアクセスする前に、利用者が正規の JP1 ユーザーであることを **FIA_UID.2a** により識別し、JP1 ユーザー本人であることを **FIA_UAU.2a** で認証することで、正当な JP1 ユーザーであることが確認できる。また、**FIA_USB.1** により、JP1 ログインスレッドに対して JP1 ユーザーを関連付ける。

また、TOE は、**FPT_RVM.1**、**FPT_SEP.1** により、セキュリティ機能のバイパス、干渉・改ざんを防ぐ。

O.ACC

TOE は、**FDP_ACC.1**、**FDP_ACF.1** により、認証済みの JP1 ユーザーのセキュリティ属性および JP1 資源グループ／JP1 権限レベルコンテナにおけるセキュリティ属性に基づいてアクセス制御を実施する。

また、TOE は、**FPT_RVM.1**、**FPT_SEP.1** により、セキュリティ機能のバイパス、干渉・改ざんを防ぐ。

O.MGT

TOE は、**FMT_MTD.1** により JP1 ユーザーの JP1 ユーザー名・パスワードを管理者のみが管理できるように制限する。また、**FIA_ATD.1** により、TOE は JP1 ユーザーのセキュリティ属性を維持する。

TOE は、**FMT_MSA.1** により、JP1 資源グループ／JP1 権限レベルコンテナのセキュリティ属性を、管理者のみが管理できるように制限する。

TOE は、FMT_SMR.1 により管理者という役割を維持する。この管理者という役割を識別するために、FIA_UAU.2b、FIA_UID.2b に示す OS の識別・認証機能を利用する。

TOE は、**FMT_SMF.1** により、管理項目に示したセキュリティ管理機能を行う能力を持つ。

また、TOE は、**FPT_SEP.1** により、セキュリティ機能の干渉・改ざんを防ぐ。

以上により、TOE の各セキュリティ対策方針は、TOE のセキュリティ機能要件で実現できる。

次に、IT 環境の各セキュリティ対策方針が、IT 環境のセキュリティ機能要件で実現できることを説明する。

OE.I&A

TOE は、**FIA_UAU.2b**、**FIA_UID.2b** により、OS に対して管理者の識別・認証が成功するまで、TOE の管理機能にアクセスすることを許可しない。

OE.SECURE_CHANNEL

FTP_ITC.1 により、TOE は、TOE を利用する JP1/IM - Manager に対し、改変や暴露から保護する通信チャネルを提供することを要求する。

以上により、IT 環境の各セキュリティ対策方針は、IT 環境のセキュリティ機能要件で実現できる。

8.2.2. 最小機能強度レベル根拠

本 TOE が想定する攻撃者は、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”が妥当であると言える。本 ST は TOE に対し最小機能強度レベルとして SOF-基本を求めており、一貫している。

8.2.3. セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 8-3 に示す。

表 8-3 セキュリティ要件のコンポーネントの依存性

セキュリティ機能要件	CC Part2 で規定されている依存コンポーネント	本 ST で選択したコンポーネント	充足性
FDP_ACC.1	**FDP_ACF.1**	**FDP_ACF.1**	○
FDP_ACF.1	**FDP_ACC.1**	**FDP_ACC.1**	○
	FMT_MSA.3	－	※1
FIA_UAU.2a	**FIA_UID.1**	**FIA_UID.2a**	※2
FIA_UID.2a	なし	－	－
FIA_ATD.1	なし	－	－
FIA_USB.1	**FIA_ATD.1**	**FIA_ATD.1**	○
FMT_SMR.1	**FIA_UID.1**	**FIA_UID.2b**	※2
FMT_MTD.1	**FMT_SMF.1**	**FMT_SMF.1**	○
	FMT_SMR.1	**FMT_SMR.1**	○
FMT_MSA.1	**FDP_ACC.1** または **FDP_IFC.1**	**FDP_ACC.1**	○
	FMT_SMF.1	**FMT_SMF.1**	○
	FMT_SMR.1	**FDP_SMR.1**	○
FMT_SMF.1	なし	－	－
FPT_RVM.1	なし	－	－
FPT_SEP.1	なし	－	－
FIA_UAU.2b	**FIA_UID.1**	**FIA_UID.2b**	※2
FIA_UID.2b	なし	－	－
FTP_ITC.1	なし	－	なし

※1：**FDP_ACF.1** において、JP1 資源グループ／JP1 権限レベルコンテナに対するアクセス制御ルールを定義しているが、これらオブジェクトの生成は、JP1 資源グループ／JP1 権限レベルの登録時に行われるものであり、これらオブジェクトのセキュリティ属性は、第 2.2 節に示したように、管理者が属

性値を設定するものである。従ってオブジェクト生成時のデフォルトセキュリティ属性の管理は本 TOE に適用しないため、**FMT_MSA.3** は選択しない。

※２：**FMT_MTD.1**、**FMT_MSA.1** において、管理操作を行える役割を管理者に制限しているが、役割を維持する機能要件である **FMT_SMR.1** において、この管理者という役割を識別する機能として OS の識別機能 **FIA_UID.2b** を利用する。**FIA_UID.1** は **FIA_UID.2** の下位階層である。

以上により各セキュリティ機能要件は、必要な依存関係をすべて満たしている。

8.2.4. セキュリティ機能要件相互補完性

前節より、TOE のセキュリティ機能要件は、IT 環境のセキュリティ機能要件も含めると、それぞれと依存関係のある機能要件と相互に補完している。これらの機能要件以外で、明示的な依存関係はないが、以下の観点から相互補完する機能要件について記述する。

セキュリティ対策方針を大別すると、識別・認証、アクセス制御、セキュリティ管理に分類できる。識別・認証に関するセキュリティ対策方針や、アクセス制御に関するセキュリティ対策方針を実施するためには、常にそれらが実施されるように、バイパス防止の仕組みが必要である。また、各セキュリティ対策方針を実施するためには、それらに関わる TSF データの干渉・改ざんを防止する仕組みが必要であり、またセキュリティ機能の無効化を防止する必要がある。

本 TOE では、セキュリティ機能がバイパスされたり、改ざん・干渉されたり、無効化されたりすることがないように、セキュリティ機能要件として、**FPT_RVM.1**、**FPT_SEP.1** を選択しており、以下のように相互補完を行っている。

迂回防止：

FIA_UAU.2a、**FIA_UID.2a** および **FDP_ACC.1**、**FDP_ACF.1** は、**FPT_RVM.1** により、迂回防止の要件が適用されているため、攻撃者がこれらのセキュリティ機能を迂回することが防止される。

干渉防止：

FIA_UAU.2a、**FIA_UID.2a** および **FDP_ACC.1**、**FDP_ACF.1** は、**FPT_SEP.1** により、干渉防止の要件が適用されているため、攻撃者がこれらのセキュリティ機能を改ざん・干渉されることが防止される。

非活性化防止：

FMT_SMF.1 セキュリティ機能の管理において、**FIA_UAU.2a** 管理者による認証データの管理および **FIA_UID.2a** 利用者識別情報の管理以外にセキュリティ機能を管理する機能要件を必要としない。また、**FIA_UAU.2a** は、JP1 ユーザーのパスワードの変更・削除に関する要件であり、**FIA_UID.2a** は JP1 ユーザーの識別・認証情報の登録・変更・削除に関する要件であるため、セキュリティ機能を非活性化するものではない。このことから、本 TOE は稼働後、セキュリティ機能を非活性化する管理は必要としないことが言える。したがって、**FMT_MOF.1** の機能要件を含む必要が無く、セ

キュリティ機能が不正に非活性化されることにつながることはない。

8.2.5. セキュリティ機能要件内部一貫性

各セキュリティ機能要件が内部的に一貫しており、矛盾しない根拠を記述する。

重複して使用するサブジェクト、オブジェクト、セキュリティ属性等に対して競合や矛盾が無いこと、TSF データに対して競合や矛盾が無いこと、機能要件の内容そのものに競合がある複数の機能要件を選択していないこと、もし選択している場合は矛盾が無いことを適切に正当化しているかという観点から、調査を行った。

＜アクセス制御関連＞

FDP_ACC.1、**FDP_ACF.1**、**FMT_MSA.1** はアクセス制御に関する機能要件であり、**FPT_RVM.1**、**FPT_SEP.1** 以外の機能要件とは関連しない。

FDP_ACC.1 と **FDP_ACF.1** では、サブジェクト、オブジェクト、SFP の名称を使用しているが、これらに矛盾は無い。

FMT_MSA.1 で記述される役割は、**FMT_SMR.1** で定義されている管理者のみであり、矛盾は無い。

FPT_RVM.1 は、アクセス制御がバイパスされないための機能要件であり、矛盾は無い。

FPT_SEP.1 は、セキュリティドメインが干渉されないための機能要件であり、矛盾は無い。

＜識別・認証関連＞

FIA_UID.2a、**FIA_UAU.2a**、**FIA_ATD.1**、**FIA_USB.1** は識別・認証に関する機能要件であり、**FMT_SMR.1**、**FPT_RVM.1**、**FPT_SEP.1** 以外の機能要件とは関連しない。

FIA(識別と認証)に関する 4 つの機能要件には、記述内容が重複する部分は無い。したがって、この部分には矛盾は無い。

FMT_SMR.1 は、利用者の役割を定義したものであり、これと重複する内容は **FIA**(識別と認証)に含まれていないため、競合や矛盾は無い。

FPT_RVM.1 は、識別・認証がバイパスされないための機能要件であり、矛盾は無い。

FPT_SEP.1 は、セキュリティドメインが干渉されないための機能要件であり、矛盾は無い。

＜セキュリティ管理関連＞

FMT_SMR.1、**FMT_MTD.1**、**FMT_MSA.1**、**FMT_SMF.1** は、セキュリティ管理に関する機能要件であり、**FPT_SEP.1** 以外の機能要件とは関連しない。

FMT_MSA.1、**FMT_MTD.1** では、セキュリティ属性及び TSF データの管理を重複せずに規定しており、競合や矛盾は無い。

FMT_SMF.1 は、セキュリティ機能を特定するものであり、他の機能要件との競合や矛盾は無い。

FMT_SMR.1 は、利用者の役割を規定するものであり、他の機能要件との競合や矛盾はない。

FPT_SEP.1 は、セキュリティドメインが干渉されないための機能要件であり、矛盾は無い。

＜TSF 保護関連＞

FPT_RVM.1 及び **FPT_SEP.1** は、TSF の保護に関するものであり、他の機能要件との関係においては競合や矛盾は無い。

FPT_RVM.1、**FPT_SEP.1** は、これらの関係において、その内容から競合や矛盾は生じない。

以上より、それぞれのカテゴリ内では競合や矛盾はない。

さらに、各カテゴリ間について、競合や矛盾の可能性を調査した。

まず、機能要件の観点では、FPT_RVM.1, FPT_SEP.1, FMT_SMR.1, FMT_MSA.1 が上記４つのカテゴリにまたがっているが、FPT_RVM.1, FPT_SEP.1 は TOE の構造に関する要件であるため矛盾しない。また、FMT_SMR.1 は単に役割を列挙しているだけであるため、矛盾することは考えられない。さらに FMT_MSA.1 は、セキュリティ属性の管理を管理者のみが行うことを規定しているが、他の機能要件と競合や矛盾は無い。

次に、TSF データ及びセキュリティ属性の観点では、＜アクセス制御関連＞（アクセス制御 SFP のサブジェクト属性、オブジェクト属性)、＜識別・認証関連＞（サブジェクトに結合される利用者属性)、及び＜セキュリティ管理関連＞（管理すべき TSF データとセキュリティ属性）の間で矛盾が懸念されるが、いずれも「JP1 ユーザー名」と一貫しており、矛盾はない。

以上より、各セキュリティ機能要件が内部的に一貫しており、矛盾は無い。

8.2.6. 監査対象事象根拠

JP1 ユーザーのパスワードには、信頼できる管理者が、ガイダンスに従って十分強度のあるパスワードを設定することを前提としている。また、ガイダンスに従って、管理者は JP1 製品のログを定期的に確認することとしている。

以上のことから、本 ST では、TOE に登録されていないユーザーのログインの繰り返し試行などは、IT 環境のログを定期的に確認することによって検出することとし、TOE のセキュリティ対策方針としてはあげていない。従って、セキュリティ機能要件 **FAU_GEN.1** を選択していないため、監査対象事象の根拠は対象とはならない。

8.2.7. セキュリティ管理機能根拠

表 5-1 に本 ST で選択した TOE セキュリティ機能要件について CC Part2 で規定された、管理要件と TSF で管理する管理項目との対応を示している。

表 8-4 に、表 5-1 で示した TSF の管理項目と 第 6.1 節で述べた TOE セキュリティ機能との対応を示す。

表 8-4 TSF の管理項目と TOE セキュリティ機能との対応

機能要件	管理項目	TOEのセキュリティ機能
FDP_ACC.1	なし	－
FDP_ACF.1	なし(明示的なアクセスまたは拒否に関する規則は無いため、管理対象とならない)	－
FIA_UAU.2a	a)JP1ユーザーのパスワードの登録・削除・変更 b)なし(JP1ユーザーは、自身のパスワードを変更できないため、管理対象とならない)	a) **SF.MGT** b) －
FIA_UID.2a	JP1ユーザー名の登録・削除・参照	**SF.MGT**
FIA_ATD.1	なし(利用者に対する追加のセキュリティ属性は無いため、管理対象とならない)	－
FIA_USB.1	a) なし(デフォルトのサブジェクト属性は無いため、管理対象とならない) b) なし(デフォルトのサブジェクト属性は無いため、管理対象とならない)	a) － b) －
FMT_SMR.1	なし(利用者のグループの概念が無いため、管理対象とならない)	－
FMT_MTD.1	なし(役割のグループの概念が無いため、管理対象とならない)	－
FMT_MSA.1	なし(役割のグループの概念が無いため、管理対象とならない)	－
FPT_RVM.1	なし	－
FPT_SEP.1	なし	－

8.2.8. セキュリティ保証要件根拠

本 TOE の評価保証レベルは、EAL2＋ALC_FLR.1 である。

本 TOE を使用したシステムは、外部のネットワークから隔離された社内ネットワークに接続されることを想定しており、また本 TOE を使用したシステムのユーザーは、業務アプリケーションの稼動状況を監視する社内ユーザーを想定している。

EAL2 は、このような TOE の特性に対して、構造設計の観点での評価、セキュアな配布手続き、脆弱性評定を含むことから妥当な選択である。

また、昨今、セキュリティ脆弱性問題への対応が重要となってきているため、セキュリティ欠陥の修正を含む **ALC_FLR.1** を追加することも妥当な選択である。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

第 6.1 節TOEセキュリティ機能の表 6-1で示したように、各TOEセキュリティ機能は 1 つ以上のセキュリティ機能要件に対応している。

FDP_ACC.1

FDP_ACF.1

SF.ACC により、TOE は、サブジェクトに関連付けられた JP1 ユーザー名と、オブジェクトに関連付けられた JP1 ユーザー名に基づいて、アクセス制御を行う。TOE は、サブジェクトに関連付けられた JP1 ユーザー名とオブジェクトに関連付けられた JP1 ユーザー名が一致する場合にのみ要求されたアクセスを許可する。

以上により、**FDP_ACC.1**、**FDP_ACF.1** は、**SF.ACC** により実現できる。

FIA_UAU.2a

FIA_UID.2a

SF.I&A により、TOE は、ログイン要求に対して識別・認証を行う。ログイン要求で受信した JP1 ユーザー名・パスワードが、TOE に登録済みの JP1 ユーザー名・パスワードと一致する場合のみ識別・認証が成功したものとし、JP1/Base ログインスレッドを生成し、利用者を代行して動作するサブジェクトとして取り扱う。識別・認証に失敗した場合は、エラーを返信する。TOE は、JP1 ユーザーの識別・認証が成功するまで、セキュリティ機能の利用を許可しない。

以上により、**FIA_UAU.2a**、**FIA_UID.2a** は、**SF.I&A** により実現できる。

FIA_ATD.1

SF.MGT により、TOE は、セキュリティ属性である JP1 ユーザー名を維持・管理する。

以上により、**FIA_ATD.1** は、**SF.MGT** により実現できる。

FIA_USB.1

SF.I&A により、TOE は、識別・認証に成功した場合、JP1/Base ログインスレッドを生成し、JP1 ユーザー名を関連付ける。なお、本 TOE では、上述した関連付けルール以外に、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する規則、変更に関する規則はない。

以上により、**FIA_USB.1** は、**SF.I&A** により実現できる。

FMT_SMR.1

SF.MGT により、セキュリティ管理機能を利用するために、管理コマンドを実行した役割は維持される。また、これらセキュリティ管理機能の利用者は、管理者に関連付けられる。

以上により、**FMT_SMR.1** は、**SF.MGT** により実現できる。

FMT_MTD.1

SF.MGT により、TOE は、以下のデータを管理する機能を提供する。

- JP1 ユーザー名・パスワードの登録
- JP1 ユーザー名・パスワードの削除
- パスワードの変更
- JP1 ユーザー一覧表示

また、TOE は、**SF.MGT** により、これらの管理機能を管理者に制限する。

以上により、**FMT_MTD.1** は、**SF.MGT** により実現できる。

FMT_MSA.1

SF.MGT により、TOE は、JP1 資源グループ／JP1 権限レベルに対して JP1 ユーザー名を追加・削除・参照する機能を提供する。また、TOE は、**SF.MGT** により、これらの管理機能を管理者に制限する。

以上により、**FMT_MSA.1** は、**SF.MGT** により実現できる。

FMT_SMF.1

第 8.2.6 節に示したように、本 ST で選択した機能要件に対して CC Part2 で規定された管理すべき要件のうち、TOE で管理すべき項目は、**SF.MGT** にて管理している。

以上により、**FMT_SMF.1** は、**SF.MGT** により実現できる。

FPT_RVM.1

SF.I&A において、JP1 ユーザーからマネージャを経由して、ログイン要求が行われた場合、**SF.I&A** が必ず実施されることを保証している。

SF. ACC において、JP1/Base ログインスレッドが JP1 資源グループ／JP1 権限レベルコンテナにアクセスする際、**SF.ACC** が必ず実施されることを保証している。

以上により、**FPT_RVM.1** は、**SF.I&A**、**SF. ACC** において実現される。

FPT_SEP.1

この機能要件は、TOE のすべてのセキュリティ機能において実現される。

SF.I&A において、ログインに成功した利用者を代行する JP1/Base ログインスレッドごとに JP1 ユーザー名が対応付けられており、別の JP1/Base ログインスレッドによりこの属性が変更されないことを保証している。

SF. ACC において、JP1/Base ログインスレッドは JP1 ユーザー名に対応付けられており、別の JP1/Base ログインスレッドによりこの属性が変更されないことを保証している。

SF.MGT において、管理者のコマンド入力プロセスによってのみ TSF データの変更を許可し、JP1/Base ログイ

ンスレッドが TSF データを変更することが無いことを保証している。

以上により、**FPT_SEP.1** は、TOE のすべての機能において実現される。

第 6.1 節の表 6-1 に示した TOE セキュリティ機能要件は、**FPT_RVM.1**、**FPT_SEP.1** を除き、対応関係にある、それぞれ独立したセキュリティ機能において実施される。従ってセキュリティ機能の組み合わせが、TOE セキュリティ機能要件を満たすために一緒に機能する場合は、**FPT_RVM.1**、**FPT_SEP.1** に限定される。

(1) **SF.I&A**、**SF.ACC** はそれぞれバイパスされない実装を行うことが記述されこれらが一緒に機能して **FPT_RVM.1** を満たす。

(2) またすべてのセキュリティ機能は、前述の記述からセキュリティ属性が信頼出来ないサブジェクトからのアクセスができない実装を行うため **FPT_SEP.1** を満たしている。

(3) 機能要件がセキュリティ機能と 1 対 1 の関係にあるセキュリティ機能はそれぞれ独立しており機能要件を弱めたり、非活性化したりすることはない。

以上により、すべての TOE セキュリティ機能要件が必要とする機能を、TOE セキュリティ機能が提供していることが示される。

8.3.2. セキュリティ機能強度根拠

本TOEにおいて、セキュリティ機能強度は、第6.2節において機能強度レベルSOF-基本を指定している。また、本TOEの最小機能強度レベルは、第5.1.2節において、SOF-基本を指定している。従って両者は一貫している。

8.3.3. セキュリティ保証手段根拠

第6.3節保証手段の表 6-2に示したように、EAL2 およびALC_FLR.1 で必要とするすべてのTOEセキュリティ保証要件に対して、保証手段を対応付けている。また、保証手段によって、本STで規定したTOEセキュリティ保証要件が要求する証拠を網羅している。従ってEAL2＋ALC_FLR.1 におけるTOEセキュリティ保証要件が要求している証拠に合致している。

8.4. PP 主張根拠

本 ST では、PP との適合を主張しない。