uCosminexus Application Server
セキュリティターゲット

2007/03/12

Version 1.07

株式会社 日立製作所

「uCosminexus Application Server 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）
1	2006/07/31	1.00	新規作成
2	2006/09/13	1.01	VTL-EOR-0001-00, VTL-EOR-0002-00, VTL-EOR-0004-00, VTL-EOR-0005-00 の指摘事項反映。
3	2006/09/21	1.02	VTL-EOR-0003-00, VTL-EOR-0001-01, VTL-EOR-0001-02 の指摘事項反映。
4	2006/09/29	1.03	VTL-EOR-0006-00 の指摘事項反映。
5	2006/11/13	1.04	VTL-EOR-0007-00 の指摘事項反映。
6	2006/12/25	1.05	VTL-EOR-1102-00 の指摘事項反映。
7	2007/01/11	1.06	AGD_ADM.1、AGD_USR.1 で、保証手段のドキュメント名を修正。
8	2007/03/12	1.07	評価者指摘事項の修正。

■ 商標類

Java 及びすべての Java 関連の商標及びロゴは，米国及びその他の国における米国 Sun Microsystems，Inc.の商標または登録商標です。

Linux は，Linus Torvalds の米国およびその他の国における登録商標あるいは商標です。

Microsoft は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。

Netscape は，米国およびその他の国における Netscape Communications Corporation の登録商標です。

Red Hat は，米国およびその他の国で Red Hat，Inc. の登録商標若しくは商標です。

Sun Microsystems は，米国 Sun Microsystems，Inc. の米国およびその他の国における商標または登録商標です。

UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

Windows は，米国およびその他の国における米国 Microsoft Corp.の登録商標です。

Windows Server は， 米国およびその他の国における米国 Microsoft Corp.の商標です。

■ 著作権

「uCosminexus Application Server 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

本 ST(セキュリティターゲット)の識別情報を以下に示す。

名称: uCosminexus Application Server セキュリティターゲット
バージョン: 1.07
識別名: uCosmiAS-ST-1.07
作成日: 2007 年 03 月 12 日
作成者: 株式会社 日立製作所 ソフトウェア事業部
TOE: uCosminexus Application Server
TOE のバージョン: 07-00
キーワード: Application Server
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、uCosminexus Application Server のセキュリティターゲットである。

TOE は、サーバサイド Java の規格である J2EE 1.4 に準拠した Web アプリケーションサーバの実行・運用環境を提供するソフトウェアである。TOE を含む製品は、Web コンテナ／EJB コンテナと呼ばれる、J2EE 準拠の Java アプリケーションの実行基盤を中核とし、Web サーバ、データベース連携、運用管理など、J2EE アプリケーションの実行および運用に関する複数のソフトウェアで構成されている。これらの構成ソフトウェアは、業務システムの可用性、信頼性を高め、効率良く運用するためのさまざまな機能を提供する。

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
- アクセス制御機能
- セキュリティ管理機能

1.3. CC 適合

本 ST は以下の CC に適合している。

- 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

- Java™ 2 Platform Enterprise Edition Specification, v1.4
- Java™ Servlet Specification Version 2.4
- JavaServer Pages™ Specification Version 2.0
- Enterprise JavaBeans™ Specification, Version 2.1

1.5. 用語の定義

1.5.1. 本 ST における用語

用語	意味
J2EE	Web ベースのアプリケーションを開発するための機能を実現するための API のセット及びサーバの仕様。Sun Microsystems, Inc.から仕様が公開されている。
Web	WWW（World Wide Web）と同義。主に HTML（Hyper Text Markup Language）と呼ばれるマークアップ言語で記述された Web ページを Web サーバから読み出し、Web ブラウザで閲覧する技術。
アプリケーションサーバ	情報システムの中間に位置し、ユーザの要求（プレゼンテーション層）と業務システム（データ層）の処理を橋渡しするためのアプリケーション層を構築するためのミドルウェア。
製品	uCosminexus Application Server Standard または uCosminexus Application Server Enterprise を指す。
Web コンテナ	Web アプリケーションが動作する実行環境。
Web アプリケーション	Web ブラウザを備えたクライアントを対象に作成されたアプリケーション。具体的には、Servlet、JSP、HTML ドキュメントなどの集合体を指す。
EJB コンテナ	EJB が動作する実行環境。
EJB	業務ロジックをプログラムとして記述したビジネスロジックを Java コンポーネント化したもの。Sun Microsystems, Inc.から仕様が公開されている。
Web サーバ	Web ブラウザからのリクエスト受信および Web ブラウザへのデータ送信に関連する処理を実行するプログラム。
J2EE アプリケーション	J2EE 仕様に準拠したアプリケーション。
HTTP	クライアントとサーバ間の通信に使うインターネットプロトコル。
HTTPS	SSL を含むインターネット上で情報を暗号化して送受信するプロトコル。
SSL	Netscape Communications 社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。
JSP	HTML ファイルに拡張タグやスクリプトを挿入することで、Web クライアントに動的な Web ページを提供する機能。Servlet 技術をベースとしている。
Servlet	Web サーバの機能を拡張して、動的に Web ページを生成したり、Web クライアントとの対話処理を実行したりする Java プログラム。
J2EE サーバ	J2EE コンテナを生成、実行する環境。
J2EE コンテナ	J2EE アプリケーションを実行するためのサーバ基盤。J2EE アプリケーションへ各種 API を提供する、Web コンテナ、EJB コンテナから構成される。
配備者（デプロイヤ）	J2EE サーバ内にインポートした J2EE アプリケーションを、クライアントから実

	行可能な状態にする者。
静的コンテンツ	HTML ファイルや画像ファイルなど、エンドユーザからの要求に対する応答に使用するファイルのうち、リクエスト内容に影響されない、常に同じ内容になるコンテンツ。
Basic 認証	Web ブラウザが持つ機能により、ユーザ名・パスワードの入力ダイアログを提示し、入力されたユーザ名・パスワードをサーバ側で照合する認証方式。
Form 認証	ユーザ名・パスワードを入力するログイン用の HTML ページを提示し、入力されたユーザ名・パスワードをサーバ側で照合する認証方式。

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

TSC（TSF Scope of Control）：TSF 制御範囲

TSF（TOE Security Functions）：TOE セキュリティ機能

TSP（TOE Security Policy）：TOE セキュリティポリシー

<TOE 関連略語>

OS：（Operating System）

J2EE：（Java™ 2 Platform, Enterprise Edition）

HTTP：（Hypertext Transfer Protocol）

HTTPS：（Hypertext Transfer Protocol Security）

SSL：（Secure Socket Layer）

JSP：（JavaServer Pages™）

EJB：（Enterprise JavaBeans™）

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 の種別

TOE は、サーバサイド Java の規格である J2EE 1.4 に準拠した Web アプリケーションサーバの実行・運用環境を提供するソフトウェアである。

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構成の一例を図 2-1 に示す。

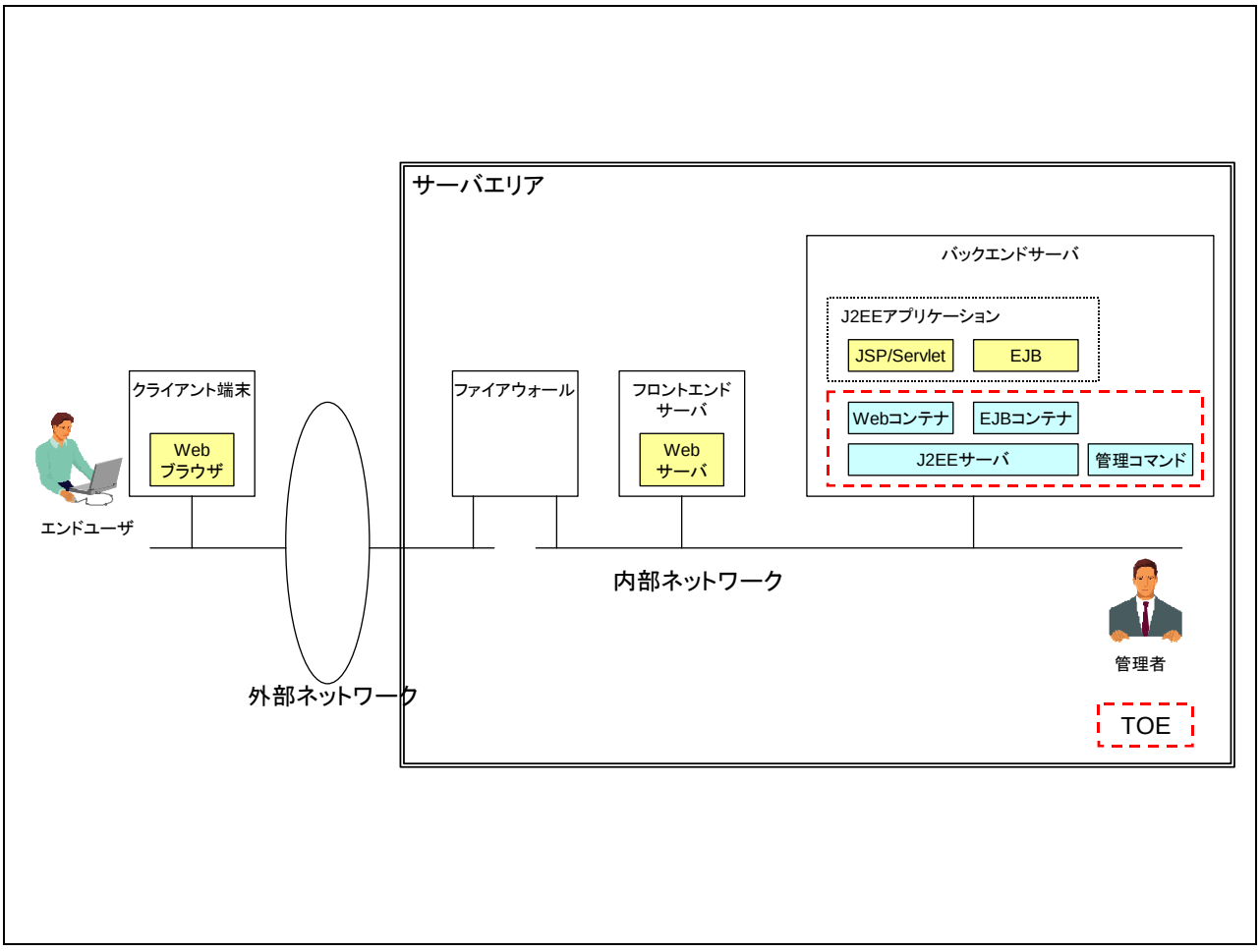

図 2-1 TOE を利用したシステム構成の一例

なお、上図は、システム構成の一例を示したものであり、製品のすべてのコンポーネントを記載しているわけではない。

以下に、システムを構成する各要素について説明する。

【 クライアント端末 】

エンドユーザは、クライアント端末上の Web ブラウザを使用し、外部ネットワーク経由で、TOE にアクセスし、J2EE アプリケーションのサービスを利用する。クライアント端末は、TOE の範囲外である。

【 サーバエリア 】

以下に示す、ファイアウォール、フロントエンドサーバ、バックエンドサーバは、サーバエリア内に設置され、サーバエリアを管理する管理者によって管理されている。サーバエリアは、物理的に隔離され、入退室管理されており、サーバエリアに入室できるのは、管理者のみである。

【 ファイアウォール 】

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る。外部ネットワークと内部ネットワークの間は、TOE を利用するために必要なプロトコルすなわち、HTTP および HTTPS のみ通過させるように管理者によって管理されている。ファイアウォールは TOE の範囲外である。

【 フロントエンドサーバ 】

Web サーバが稼動しているマシンである。エンドユーザからの要求を受付け、バックエンドサーバに受け渡し、またバックエンドサーバからの応答をエンドユーザに返信する。TOE におけるエンドユーザの識別・認証に使用するデータを送受信する際には、クライアント端末上の Web ブラウザとフロントエンドサーバ上の Web サーバの間で、HTTPS 通信により通信路の保護を行なう。また、Web アプリケーションを利用する際にも、管理者が静的コンテンツおよび JSP/Servlet に対して HTTPS を使用するという設定を行なっていた場合のみ、HTTPS 通信により通信路の保護を行なう。フロントエンドサーバは、TOE の範囲外である。

【 バックエンドサーバ 】

TOE が稼動するマシンである。 業務を提供する J2EE アプリケーションが稼動するために必要な Web コンテナ、EJB コンテナ、J2EE サーバが動作している。また、管理者はバックエンドサーバ上で管理コマンドを実行し、TOE の運用を管理する。バックエンドサーバのうち、図 2-1 の破線で囲んだ範囲が TOE である。

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、ネットワークおよび J2EE アプリケーションを管理する者である。本 ST で定義する管理者は、J2EE の仕様における配備者(Deployer)及びシステム管理者(System Administrator)を兼ねている。管理者は、バックエンドサーバ上の管理コマンドを用いて TOE の管理を行なう。具体的には以下のような管理を行なう。

- サーバエリア内のハードウェアの設置及び内部ネットワークの構築。
- サーバエリア内のソフトウェアのインストール及びコンフィギュレーション。
- TOE にアクセスするエンドユーザの管理。
- J2EE アプリケーションの配備・再配備及び運用。

J2EE アプリケーションの配備や、修正あるいは機能エンハンスが行なわれた J2EE アプリケーションの再配備においては、管理者は、当該 J2EE アプリケーションのプロパティを見直し、十分テストを行なった後に、この J2EE アプリケーションを開始する。

具体的には、以下の操作を行なう。

1) J2EE アプリケーションのインポート
2) J2EE アプリケーションのプロパティの見直し、定義
3) J2EE アプリケーションの開始
4) 当該 J2EE アプリケーションのテストの実施
5) J2EE アプリケーションの停止
6) 必要に応じて、2)の J2EE アプリケーションのプロパティ見直し、定義を繰り返す
7) 本番サービスとして、J2EE アプリケーションを開始する

TOE にアクセスするエンドユーザの管理において、TOE にアクセスするエンドユーザのパスワードは、以下に示す文字種を併用して、十分強度があるものを管理者が設定する。なお、管理者は、設定したエンドユーザのパスワードを、漏洩や改ざんから保護された手段でエンドユーザに通知する。

項目	品質尺度
パスワード長	8～64 文字
使用可能な文字種	数字: 0～9 英字大文字: A～Z 英字小文字: a～z 記号: ! $ @ ~ ? ` ( ) { }

管理者は、ハードウェア、ソフトウェア、ネットワーク、および J2EE アプリケーションなどのサーバエリア内のシステム全体に対して責任を持っており、信頼してよい。

また、管理者はバックエンドサーバ上の管理コマンドによる操作以外の運用は禁止されなければならない。

【エンドユーザ】

エンドユーザは、クライアント端末上の Web ブラウザを使用し、外部ネットワーク経由で、TOE にアクセスし、J2EE アプリケーションのサービスを利用する。

2.3. TOE の機能

2.3.1. TOE の動作

TOE の動作の概要を図 2-2 に示す。

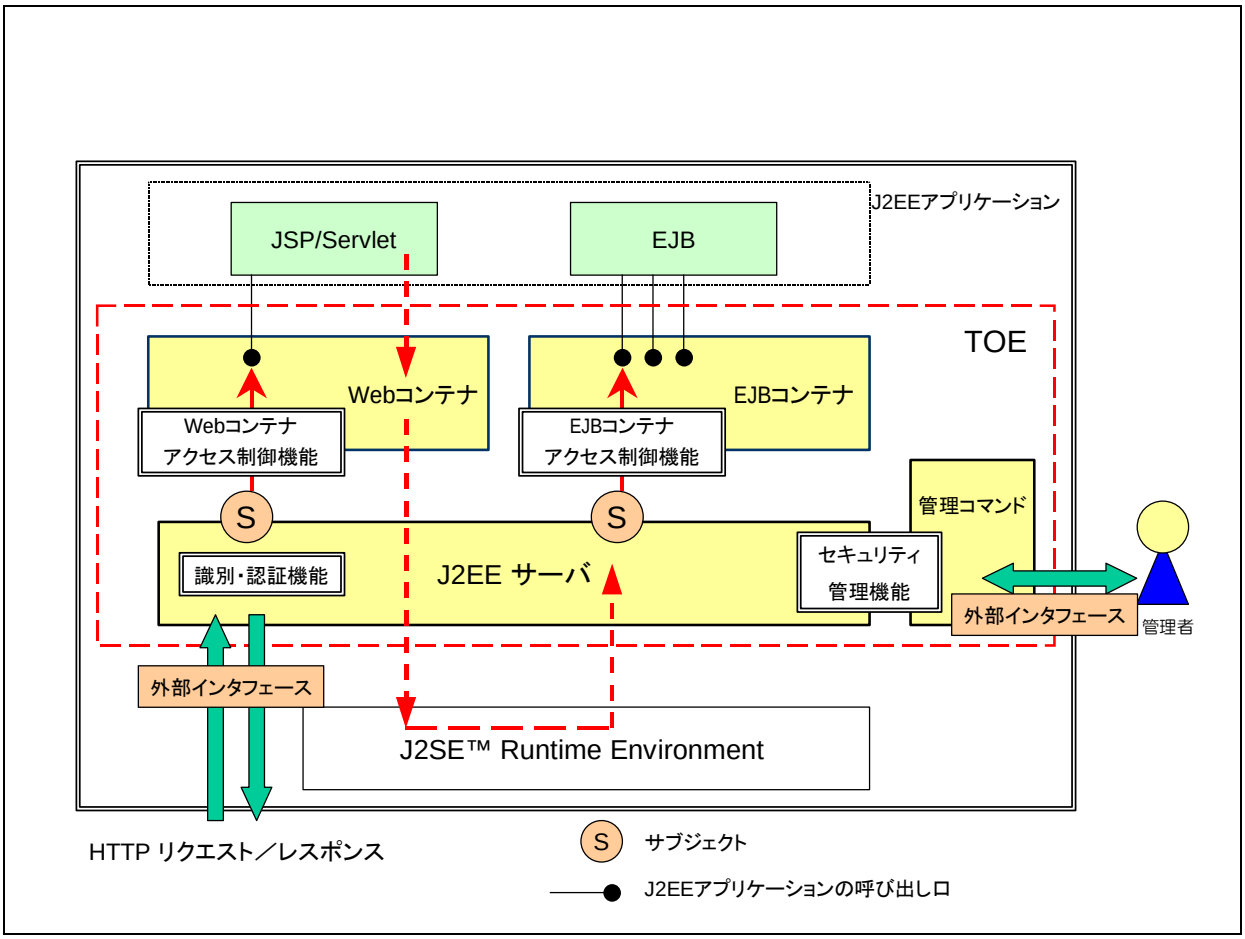

図 2-2 TOE の動作

1) TOE は、エンドユーザの Web ブラウザから Web サーバ経由で HTTP リクエストを受信する。TOE は、これに対して、最初に必ずエンドユーザの識別認証を行なう。識別認証が成功した後は、当該 URL を閉じるまで、TOE は認証状態を維持する。
2) TOE は、認証したユーザのロールおよび該当する Web コンテナオブジェクトのセキュリティ属性に従って、ユーザを代行するサブジェクトの、Web コンテナオブジェクトである JSP/Servlet の呼び出し口または静的コンテンツの読み出し口に対するアクセスを制御する。
3) JSP/Servlet は、Web コンテナ上で動作するが、これは TOE の範囲外である。
4) JSP/Servlet は、処理の実行中に、必要に応じて EJB コンテナ上で動作する EJB のメソッドを呼び出すことができる。この場合 TOE は、JSP/Servlet の処理コンテクストを引き継ぎ、ユーザのロールおよび該当する EJB コンテナオブジェクトのセキュリティ属性に従って、ユーザを代行するサブジェクトの、EJB コンテナオ

ブジェクトである EJB メソッドの呼び出し口に対するアクセスを制御する。

5) EJB は、EJB コンテナ上で動作するが、これは TOE の範囲外である。

6) TOE は、管理者が J2EE アプリケーションの登録、削除、開始、終了を行なうための管理機能を提供する。

7) Web コンテナおよび EJB コンテナは、管理者による J2EE アプリケーションの登録・開始によって生成されており、エンドユーザがアクセスする際には、既に生成されたものが使用される。

8) TOE 内のコンポーネントである J2EE サーバ、Web コンテナ、EJB コンテナにおいて、処理がコンポーネント間で遷移する際に性能解析情報を記録する。

9) 上記は、J2SE™ Runtime Environment 上で動作する。J2SE™ Runtime Environment は TOE の範囲外である。

2.3.2. TOE によって提供されるセキュリティ機能

【 識別・認証機能 】

TOE は、エンドユーザから要求を受け取ると、その実行に先立ちエンドユーザに対してユーザ ID とパスワードの入力を要求する。TOE は、エンドユーザから渡されたユーザ ID とパスワードにより認証を行なう。TOE は、認証済みのユーザ情報を、処理コンテクストに関連付ける。

【 アクセス制御機能 】

- Web コンテナオブジェクト(JSP/Servlet 呼び出し口または静的コンテンツの読み出し口)に対するアクセス制御

Webコンテナは処理コンテクストに関連付けられた、認証済みのユーザ情報からユーザのロールを取得し、Web コンテナオブジェクト(JSP/Servlet 呼び出し口または静的コンテンツの読み出し口)に関連付けられたロール情報との対応関係を検証し、アクセスが許可されている場合のみ呼び出しを行なう。

- EJB コンテナオブジェクト(EJB メソッドの呼び出し口)に対するアクセス制御

EJB コンテナは処理コンテクストに関連付けられた、認証済みのユーザ情報からユーザのロールを取得し、EJB コンテナオブジェクト(EJB メソッドの呼び出し口)に関連付けられたロール情報との対応関係を検証し、アクセスが許可されている場合のみ呼び出しを行なう。

【 セキュリティ管理機能 】

- 識別・認証情報とセキュリティ属性の管理

TOE は、エンドユーザの識別・認証を行なうため、ユーザ ID とパスワード、およびロールの対応関係を維持・管理する。管理者は、管理コマンドによりこの対応関係を管理することができる。

- J2EE アプリケーションのセキュリティ属性の管理

TOE は、管理者が J2EE アプリケーションを登録する際に指定したロール情報を維持・管理する。管理者は、管理コマンドによりこの対応関係を管理することができる。

2.3.3. TOE によって提供される非セキュリティ機能

【Web アプリケーション実行機能】

JSP/Servlet で構成される Web アプリケーションを実行する機能である。Web コンテナ上で動作する。

【EJB 実行機能】

業務処理プログラムを実装した EJB のメソッドを実行する機能である。EJB コンテナ上で動作する。

【性能解析情報出力機能】

リクエストが TOE 内のコンポーネント間を遷移する際に、性能解析情報を記録する。TOE 外である性能トレース機能を用いてトレースファイルが出力できる。

2.3.4. TOE によって提供されないセキュリティ機能

- TOE を管理するための管理コマンドの保護には、OS のファイルシステムの機能を利用する。
- 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。

2.4. TOE の範囲

2.4.1. TOE の範囲

TOE は、第 2.1.2 節の図 2-1 においてバックエンドサーバと示した部分において動作する。なお、図 2-1 において、フロントエンドサーバ、バックエンドサーバを同一マシンで動作させるシステム構成も可能である。

また、第 2.3.1 節の図 2-2 の破線内で示したコンポーネントである Web コンテナ、EJB コンテナ、J2EE サーバ、管理コマンドが TOE の範囲である。

これらのコンポーネントから構成される TOE は、TOE 名称とバージョンで識別され、利用者が参照できる。

製品を構成する TOE の範囲外のコンポーネントを表 2-1 に示す。

表 2-1 TOE の範囲外のコンポーネント

TOE の範囲外のコンポーネント	機能概要
Web サーバ	Secure Socket Layer (SSL) をサポートした HTTP/HTTPS リクエストの処理を行なうサーバ機能を提供する。
運用管理	アプリケーションサーバを運用管理するための機能を提供する。アプリケーションサーバの一括構築やアプリケーションサーバの各機能が出力するログの収集などを行なうことができる。
性能トレース	処理性能のボトルネックを解析するためのトレース情報を出力する機能を提供する。
J2SE™ Runtime Environment	Java™ 2 Platform Standard Edition に準拠した Java の仮想実行環境を提供する。
スケジューラ	クライアントからのリクエストをスケジューリングして、負荷分散や流量制御を実現する機能を提供する。 本コンポーネントは、uCosminexus Application Server Enterprise にのみ含まれる。

2.4.2. ハードウェア条件

以下に TOE の評価構成であるハードウェア条件を示す。OS は、本 TOE のテストを実施した OS を示しており、複数のハードウェア条件を示している。

本 TOE の動作環境としてテストを実施した OS

(1) Windows の場合
下記シリーズ中で Windows Server 2003 Standard x64 Edition が稼動する機種
BladeSymphony
FLORA 700 シリーズ
HA8000 シリーズ
他社 PC/AT 互換機

ディスク占有量: 約 410MB
標準メモリ量: 約 890MB

(2) Linux の場合
下記シリーズ中で Red Hat Enterprise Linux AS 4(AMD64 & Intel EM64T)が稼動する機種
BladeSymphony
HA8000 シリーズ
他社 PC/AT 互換機

ディスク占有量: 約 440MB
標準メモリ量: 約 1370MB

2.4.3. ソフトウェア条件

以下に TOE の評価構成であるソフトウェア条件を示す。OS は、本 TOE のテストを実施した OS を示している。

(1) Windows の場合

- Windows Server 2003 Standard x64 Edition
  本 ST の TOE 外であり、IT 環境である。
- uCosminexus Application Server Standard 07-00 または
  uCosminexus Application Server Enterprise 07-00
  本 ST の TOE を含む製品である。

(2) Linux の場合

- Red Hat Enterprise Linux AS 4(AMD64 & Intel EM64T)
  本 ST の TOE 外であり、IT 環境である。
- uCosminexus Application Server Standard 07-00 または
  uCosminexus Application Server Enterprise 07-00
  本 ST の TOE を含む製品である。

2.5. TOE の保護資産

第 2.3.1 節に示したように、登録されたエンドユーザが、ロールに従って、許可された J2EE アプリケーションを利用できる環境を提供することが TOE の機能である。従って、TOE は、Web コンテナオブジェクトおよび EJB コンテナオブジェクトである、以下の J2EE アプリケーションの呼び出し口を権限外の呼び出しから保護する。

- J2EE アプリケーションの呼び出し口
  - HTML ファイル、画像ファイルなどの静的コンテンツの読み出し口
  - JSP/Servlet の呼び出し口
  - EJB メソッドの呼び出し口

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方針について記述する。

3.1. 前提条件

A. PHYSICAL

TOE が稼動するハードウェア、ファイアウォール、フロントエンドサーバ及び内部ネットワークは、物理的に外部から隔離されたサーバエリアに設置され、管理者以外は入室できないように管理される。また、TOE が稼動するために不要なハードウェア及びソフトウェアは、サーバエリア内には持ち込まれないものとする。

A. MANAGE

TOE と TOE が稼動するために必要なサーバエリア内の各ハードウェア、ソフトウェア、内部ネットワーク及び TOE を利用して動作する J2EE アプリケーションは、管理者によって運用・管理が行なわれるものとする。

A. PERSONNEL

管理者は、IT 環境及び TOE に精通しており、またサーバエリア内のシステム全体に対して責任を持っており、信頼できるものとし、悪意のある行為は行なわない。

A. FIREWALL

TOE が稼動する内部ネットワークと、外部ネットワークの境界に、ファイアウォールが設置され、Web アプリケーションが利用する HTTP/HTTPS プロトコルのみ通過させるように設定・維持・管理されるものとする。

3.2. 脅威

T.UNDEFINED_USERS

高度な専門知識を持たない TOE に登録されていないエンドユーザが、HTTP 電文を覗き見たり、不正にHTTP リクエストを送信したりすることにより、J2EE アプリケーションにアクセスするかもしれない。

T.UNAUTHORIZED_ACCESS

高度な専門知識を持たない TOE に登録されているエンドユーザが、不正に HTTP リクエストを送信することにより、アクセス権限の無い J2EE アプリケーションにアクセスするかもしれない。

3.3. 組織のセキュリティ方針

P.PASSWORD

管理者は、推測されにくく、十分強度のあるパスワードを設定しなければならない。

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、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(識別・認証)

TOE は、登録されていないエンドユーザから、J2EE アプリケーションへのアクセスを保護するために識別・認証を行なう。

O.ACC (J2EE アプリケーションへのアクセス制御)

TOE は、登録されているがアクセス権限を持っていないエンドユーザから、J2EE アプリケーションへのアクセスを保護するために、アクセス制御を行なう。

O.MANAGE(TOE の管理)

TOE は、エンドユーザの識別・認証情報及びセキュリティに関連する情報を、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

OE.I&A (OS による識別・認証)

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(セキュア通信)

エンドユーザを認証するための識別・認証情報を送受信する際には, Web ブラウザと Web サーバ間で HTTPS プロトコルを使用し、通信路の保護を行なう。

OM.PHYSICAL(サーバエリアの保護)

管理者は、TOE が稼動するハードウェア、ファイアウォール、フロントエンドサーバ及び内部ネットワークは、物理的に外部から隔離されたサーバエリアに設置する。また、TOE が稼動するために不要なハードウェア及びソフトウェアは、サーバエリア内には持ち込まない。さらに、管理者以外がサーバエリアに入室できないように、入退出管理を行なう。

OM.FIREWALL(ファイアウォールの設置)

管理者は、外部ネットワークと内部ネットワークの境界にはファイアウォールを設置し、Web アプリケーションが利用する HTTP 及び HTTPS プロトコルのみ通過させるよう設定・維持・管理する。

OM. ADMIN(管理者)

- 管理者には、システム全体に責任を持っており、悪意のある行為は行なわず、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・管理を行なう。
- 管理者は、管理者自身の OS パスワード及びエンドユーザの登録に際して、推測されにくく、十分強度のあるパスワードを設定する。

5. IT セキュリティ要件

本章では、TOE 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使用する。

FIA_UAU.2 アクション前の利用者認証

下位階層 : なし

FIA_UAU.2.1 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.2 アクション前の利用者識別

下位階層 : FIA_UID.1

FIA_UID.2.1 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_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]
ユーザ ID およびユーザ ID に対応付けられたロール

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

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]
ユーザ ID およびユーザ ID に対応付けられたロールのペア

依存性 : なし

FDP_ACC.1a Webコンテナにおけるサブセットアクセス制御

下位階層 : なし

FDP_ACC.1.1a 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：Web コンテナサブジェクトインスタンス
オブジェクト：静的コンテンツの読み出し口
JSP/Servlet の呼び出し口
操作： 呼び出し

[割付: アクセス制御 SFP]
Web コンテナアクセス制御方針

依存性 ： FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1b EJBコンテナにおけるサブセットアクセス制御

下位階層 ： なし

FDP_ACC.1.1b 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：EJB コンテナサブジェクトインスタンス
オブジェクト：EJB メソッドの呼び出し口
操作： 呼び出し

[割付: アクセス制御 SFP]
EJB コンテナアクセス制御方針

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.1a Webコンテナにおける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.1.1a 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]
サブジェクト属性：ユーザ ID に対応付けられたロール
オブジェクト属性：Web コンテナオブジェクトに対応付けられたロール

[割付: アクセス制御 SFP]
Web コンテナアクセス制御方針

FDP_ACF.1.2a 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]
ユーザ ID に対応付けられたロールと Web コンテナオブジェクトに対応付けられたロールが対応付けられている場合のみ、サブジェクトのオブジェクトに対する要求されたアクセスを許可する。

[Note] ユーザ ID に対応付けられたロールと Web コンテナオブジェクトに対応付けられたロールの対応付けはオブジェクトの配備時に管理者によって定義される。

FDP_ACF.1.3a 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]
Web コンテナオブジェクトに対するアクセス制御ルールが無い場合は、サブジェクトのオブジェクトに対する要求されたアクセスを許可する。

FDP_ACF.1.4a 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

FDP_ACF.1b EJBコンテナにおける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.1.1b 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]
サブジェクト属性：ユーザ ID に対応付けられたロール
オブジェクト属性：EJB コンテナオブジェクトに対応付けられたロール

[割付: アクセス制御 SFP]
EJB コンテナアクセス制御方針

FDP_ACF.1.2b 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]
ユーザ ID に対応付けられたロールと EJB コンテナオブジェクトに対応付けられたロールが対応付けられている場合のみ、サブジェクトのオブジェクトに対する要求されたアクセスを許可する。

[Note] ユーザ ID に対応付けられたロールと EJB コンテナオブジェクトに対応付けられたロールの対応付けはオブジェクトの配備時に管理者によって定義される。

FDP_ACF.1.3b 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]
EJB コンテナオブジェクトに対するアクセス制御ルールが無い場合は、サブジェクトのオブジェクトに対する要求されたアクセスを許可する。

FDP_ACF.1.4b 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

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付けなければならない。

依存性 : FIA_UID.1 識別のタイミング

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な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
FIA_UAU.2	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) エンドユーザのパスワードの作成・削除 b) なし(エンドユーザは、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.2	利用者識別情報の管理	エンドユーザのユーザIDの作成・削除
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セキュリティ属性は無いため、管理対象とならない) b) なし(デフォルトのサブジェクトセキュリティ属性は無いため、管理対象とならない)
FIA_ATD.1	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。 ユーザIDに対するロールの追加	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)
FDP_ACC.1a	なし	なし
FDP_ACC.1b	なし	なし
FDP_ACF.1a	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	Webコンテナオブジェクトに対応付けられたロールの管理
FDP_ACF.1b	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	EJBコンテナオブジェクトに対応付けられたロールの管理
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_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)
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)
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし

依存性 ： なし

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
Web コンテナオブジェクトに対応付けられたロール	選択: 問い合わせ、改変、削除 割付: 登録	管理者	Web コンテナアクセス制御方針
EJB コンテナオブジェクトに対応付けられたロール	選択: 問い合わせ、改変、削除 割付: 登録	管理者	EJB コンテナアクセス制御方針

依存性 ： FDP_ACC.1 サブセットアクセス制御
FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

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
ユーザ ID	選択: 問い合わせ、削除 割付: 登録	管理者
パスワード	選択: 削除 割付: 登録	管理者
ユーザ ID に関連付けられたロール	選択: 問い合わせ、削除 割付: 登録	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

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 で規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 5-2 に示す。

表 5-2 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 環境のセキュリティ要件

5.2.1. セキュリティ機能要件

IT 環境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使用する。

FIA_UAU.2E　アクション前の利用者認証

下位階層 ： FIA_UAU.1

FIA_UAU.2.1E　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.2E　アクション前の利用者識別

下位階層 ： FIA_UID.1

FIA_UID.2.1E　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間高信頼性チャネル

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]
エンドユーザの識別・認証に使用するユーザ ID・パスワードの送信

[詳細化] : TSF は、→Web サーバは、

依存性 : なし

6. TOE 要約仕様

本章では、TOE セキュリティ機能、セキュリティ機能強度、セキュリティ保証手段について記述する。

6.1. TOE セキュリティ機能

本節では、TOE セキュリティ機能について記述する。表 6-1 に示すように、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足している。

表 6-1 TOE セキュリティ機能と TOE 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	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FIA_ATD.1	FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a	FDP_ACF.1b	FMT_SMR.1	FMT_SMF.1	FMT_MSA.1	FMT_MTD.1	FPT_RVM.1	FPT_SEP.1
SF.I&A	○	○	○										○	○
SF.WEB_ACC					○		○						○	○
SF.EJB_ACC						○		○					○	○
SF.USER_MNG				○					○	○		○		○
SF.RULE_MNG									○	○	○			○

6.1.1. 識別・認証機能(**SF.I&A**)

SF.I&A は、エンドユーザから Web コンテナ上の J2EE アプリケーションにアクセスが要求されると、Web コンテナオブジェクトのアクセス制御情報を取得する。認証方式は、Basic 認証または Form 認証から選択する。Web コンテナオブジェクトのアクセス制御情報は、**SF.RULE_MNG** で管理され、設定される。

決定した認証方式をエンドユーザに返信すると、認証方式に応じてエンドユーザの Web ブラウザ上にユーザ ID・パスワードの入力画面が表示され、エンドユーザは、ユーザ ID・パスワードを入力する。
なお、Web ブラウザ上の機能は、TOE の範囲外である。

SF.I&A は、エンドユーザが入力したユーザ ID・パスワードに対して、登録されたユーザ ID・パスワードにより識別・認証を行ない、識別・認証に成功した場合、認証済みのサブジェクト、すなわち Web コンテナサブジェクトインスタンスを生成する。識別・認証に使用するユーザ ID・パスワードの TOE への登録は、**SF.USER_MNG** により設定される。

SF.I&A は、Web コンテナサブジェクトインスタンスにユーザ ID 及びユーザ ID に対応付けられたロールを関連付ける。ユーザ ID とユーザ ID に対応付けられたロールの対応付けは、**SF.USER_MNG** により設定される。

SF.I&A は、識別・認証に失敗した場合、エンドユーザにエラーを返信する。

エンドユーザから Web コンテナ上の J2EE アプリケーションへのアクセスが要求された場合、**SF.I&A** が必ず実施されることを保証する。

また、Web コンテナサブジェクトインスタンスごとにユーザ ID 及びユーザ ID に対応付けられたロールを管理するため、**SF.I&A** は、別の Web コンテナサブジェクトインスタンスからこれらの属性が変更されないことを保証する。

6.1.2. Web アクセス制御機能(**SF.WEB_ACC**)

SF.WEB_ACC は、Web コンテナオブジェクトに設定されているアクセス制御ルールおよび Web コンテナオブジェクトに対応したロールを利用してアクセス制御を行なう。

SF.WEB_ACC は、Web コンテナサブジェクトインスタンスに設定されている、ユーザ ID に対応付けられたロールが、Web コンテナオブジェクトに設定されている、Web コンテナオブジェクトに対応付けられたロールに関連付けられている場合のみアクセスを許可する。
また **SF.WEB_ACC** は、Web コンテナオブジェクトに対するアクセス制御ルールが存在しない場合は、アクセスを許可する。

ユーザ ID に対応付けられたロールと Web コンテナオブジェクトに対応付けられたロールの関連付けは、**SF.RULE_MNG** により設定される。

Web コンテナサブジェクトインスタンスが Web コンテナオブジェクトにアクセスする際に、**SF.WEB_ACC** が必ず実施されることを保証する。

また、Web コンテナサブジェクトインスタンスごとにユーザ ID 及びユーザ ID に対応付けられたロールを管理するため、**SF.WEB_ACC** は、別の Web コンテナサブジェクトインスタンスからこれらの属性が変更されないことを保証する。

SF.WEB_ACC は、アクセスが許可されなかった場合、エンドユーザにその旨を通知する。

6.1.3. EJB アクセス制御機能(**SF.EJB_ACC**)

Web コンテナ上で動作する JSP/Servlet は、処理の実行中に必要に応じて EJB コンテナ上で動作する EJB のメソッドを呼び出すことができる。JSP/Servlet が Web コンテナを経由して EJB コンテナ上で動作する EJB のメソッドへアクセスする際に、Web コンテナ内で Web コンテナサブジェクトインスタンスに関連付けられた、ユーザ ID 及びユーザ ID に対応付けられたロールは、EJB コンテナへ伝播され、これらは EJB コンテナサブジェクトインスタンスに関連付けられる。

SF.EJB_ACC は、EJB コンテナオブジェクトに設定されているアクセス制御ルールおよび EJB コンテナオブジェクトに対応したロールを利用してアクセス制御を行なう。

SF.EJB_ACC は、EJB コンテナサブジェクトインスタンスに設定されている、ユーザ ID に対応付けられたロールが、EJB コンテナオブジェクトに設定されている、EJB コンテナオブジェクトに対応付けられたロールに関連付けられている場合のみアクセスを許可する。
また **SF.EJB_ACC** は、EJB コンテナオブジェクトに対するアクセス制御ルールが存在しない場合は、アクセス

を許可する。

ユーザ ID に対応付けられたロールと EJB コンテナオブジェクトに対応付けられたロールの関連付けは、**SF.RULE_MNG** により設定される。

EJB コンテナサブジェクトインスタンスが EJB コンテナオブジェクトにアクセスする際に、**SF.EJB_ACC** が必ず実施されることを保証する。

また、EJB コンテナサブジェクトインスタンスごとにユーザ ID 及びユーザ ID に対応付けられたロールを管理するため、**SF.EJB_ACC** は、別の EJB コンテナサブジェクトインスタンスからこれらの属性が変更されないことを保証する。

SF.EJB_ACC は、アクセスが許可されなかった場合、Web コンテナにその旨を通知する。

6.1.4. ユーザ・ロール管理機能(**SF.USER_MNG**)

SF.USER_MNG は、以下のデータを管理する機能を提供する。

- ユーザ ID の登録・削除・問い合わせ
- パスワードの登録・削除
- ユーザ ID に対応付けられたロールの登録・削除・問い合わせ

SF.USER_MNG は、ユーザ ID とユーザ ID に対応付けられたロールを関連付ける機能を提供する。

SF.USER_MNG は、ユーザ ID とユーザ ID に対応付けられたロールの関連付けを解除する機能を提供する。

SF.USER_MNG は、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。

管理者が、管理コマンドを使用してユーザ ID とユーザ ID に対応付けられたロールの関連付けを行なうことにより、TOE のアクセス制御機能、すなわち、**SF.WEB_ACC** 及び **SF.EJB_ACC** を利用することができる。

SF.USER_MNG は、サブジェクトがユーザ ID とユーザ ID に対応付けられたロールに直接アクセスすることが無いことを保証する。

SF.USER_MNG 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。

6.1.5. アクセスルール管理機能(**SF.RULE_MNG**)

SF.RULE_MNG は、以下の設定を管理する機能を提供する。

- サブジェクトの認証方式の設定
- Web コンテナオブジェクトに対応付けられたロールの登録・削除・問い合わせ・改変
- EJB コンテナオブジェクトに対応付けられたロールの登録・削除・問い合わせ・改変
- Web コンテナオブジェクトに対するアクセス制御ルールの設定
- EJB コンテナオブジェクトに対するアクセス制御ルールの設定

SF.RULE_MNG は、Web コンテナオブジェクトに対応付けられたロールとユーザ ID に対応付けられたロールを関連付ける機能を提供する。

SF.RULE_MNG は、EJB コンテナオブジェクトに対応付けられたロールとユーザ ID に対応付けられたロールを関連付ける機能を提供する。

SF.RULE_MNG は、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。

SF.RULE_MNG は、管理コマンドからアクセス制御ルール情報取得要求があった場合、アクセス制御ルールをファイルに書き出し管理コマンドで指定されたパスへ出力する。

SF.RULE_MNG は、**SF.RULE_MNG** で管理しているデータにサブジェクトが直接アクセスすることが無いことを保証する。

SF.RULE_MNG 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。

6.2. セキュリティ機能強度

確率的または順列的メカニズムに基づくセキュリティ機能は、上述の **SF.I&A** である。このセキュリティ機能のうち、ID、パスワード方式の機能強度レベルが 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 セキュリティ保証要件(EAL2+ALC_FLR.1)とセキュリティ保証手段の対応表

セキュリティ保証要件（EAL2＋FLR_ALC.1）	セキュリティ保証手段
ACM_CAP.2	uCosminexus Application Server 構成管理文書
ADO_DEL.1	uCosminexus Application Server 配付文書
ADO_IGS.1	Cosminexus セキュリティ構築・運用ガイド
ADV_FSP.1	uCosminexus Application Server 機能仕様書
ADV_HLD.1	uCosminexus Application Server 構造設計書
ADV_RCR.1	uCosminexus Application Server 対応分析書
AGD_ADM.1	Cosminexus セキュリティ構築・運用ガイド
AGD_USR.1	Cosminexus セキュリティ構築・運用ガイド
ALC_FLR.1	uCosminexus Application Server セキュリティ欠陥修正規程書
ATE_COV.1	uCosminexus Application Server テスト仕様書／報告書
ATE_FUN.1	uCosminexus Application Server テスト仕様書／報告書
ATE_IND.2	uCosminexus Application Server 07-00
AVA_SOF.1	uCosminexus Application Server セキュリティ機能強度分析書
AVA_VLA.1	uCosminexus Application Server 脆弱性分析書

7. PP 主張

本章では、PP 参照、PP 修正、PP 追加について記述する。

7.1. PP 参照

参照した PP は無い。

7.2. PP 修正

PP への修正は無い。

7.3. PP 追加

PP への追加は無い。

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定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方針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抗する脅威、実現する前提条件及び組織のセキュリティ方針の対応関係を表 8-1 に示す。

表 8-1 セキュリティ対策方針と脅威、前提条件、組織のセキュリティ方針の対応表

	T.UNDEFINED_USERS	T.UNAUTHORIZED_ACCESS	A.PHYSICAL	A.MANAGE	A.PERSONNEL	A.FIREWALL	P.PASSWORD
O.I&A	○						
O.ACC		○					
O.MANAGE	○	○					○
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方針に対応している。

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

T.UNDEFINED_USERS:

O.I&A により、TOE は、登録されているエンドユーザを識別・認証する。また、**O.MANAGE** により、エンドユーザの識別・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。

外部ネットワーク上でのエンドユーザの識別・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 Web ブラウザと Web サーバ間で HTTPS プロトコルを使用し、通信路の保護を行なう。

以上により、**T.UNDEFINED_USERS** は、**O.I&A**、**O.MANAGE**、**OE.I&A**、**OE.SECURE_CHANNEL** 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無いエンドユーザから J2EE アプリケーションへのアクセスを保護するためにアクセス制御を行なう。また、**O.MANAGE** 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.MANAGE**、**OE.I&A** により対抗できる。

A.PHYSICAL:

OM.PHYSICAL により、管理者は、TOE が稼動するハードウェア、ファイアウォール、フロントエンドサーバ及び内部ネットワークを、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、TOE が稼動するために不要なハードウェア及びソフトウェアは、サーバエリア内には持ち込まない。さらに、管理者以外がサーバエリアに入室できないように、入退出管理を行なう。

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 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・管理を行なう。

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、システム全体に責任を持っており、悪意のある行為は行なわず、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。

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

A.FIREWALL:

OM.FIREWALL により、管理者は、外部ネットワークと内部ネットワークの境界にはファイアウォールを設置し、Web アプリケーションが利用する HTTP 及び HTTPS プロトコルのみ通過させるよう設定・維持・管理する。

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

P.PASSWORD:

O.MANAGE により、TOE は、エンドユーザのパスワードを管理者のみが管理できるように制御する。また、**OM.ADMIN** により、管理者は、エンドユーザの登録に際して、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、**P.PASSWORD** は、**O.MANAGE**、**OM.ADMIN** により実施される。

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 および 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.MANAGE	OE.I&A	OE.SECURE_CHANNEL
FIA_UAU.2	○				
FIA_UID.2	○				
FIA_USB.1	○				
FIA_ATD.1			○		
FDP_ACC.1a		○			
FDP_ACC.1b		○			
FDP_ACF.1a		○			
FDP_ACF.1b		○			
FMT_SMR.1			○		
FMT_SMF.1			○		
FMT_MSA.1			○		
FMT_MTD.1			○		
FPT_RVM.1	○	○			
FPT_SEP.1	○	○	○		
FIA_UAU.2E				○	
FIA_UID.2E				○	
FTP_ITC.1					○

表 8-2 より、TOE の各セキュリティ機能要件は、1つ以上の TOE の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、**FIA_UAU.2**、**FIA_UID.2** により、エンドユーザの識別・認証が成功するまでいかなる J2EE アプリケーションへのアクセスを許可しない。また、**FIA_USB.1** により、TOE は認証済みのエンドユーザのセキュリティ属性を Web コンテナおよび EJB コンテナのサブジェクトインスタンスに関連付ける。

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.1a**、**FDP_ACF.1a** により、認証済みのエンドユーザのセキュリティ属性および Web コンテナオブジェクト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。同様に TOE は、**FDP_ACC.1b**、**FDP_ACF.1b** により、認証済みのエンドユーザのセキュリティ属性および EJB コンテナオブジェクト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.MANAGE:

TOE は、**FMT_MTD.1** によりエンドユーザのユーザ ID、パスワード及びユーザ ID に対応付けられたロールを管理者のみが管理できるように制限する。また、ユーザ ID 及びユーザ ID に対応付けられたロールのペアは、**FIA_ATD.1** により、維持される。

また、TOE は、**FMT_MSA.1** により、Web コンテナおよび EJB コンテナにおける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.2E**、**FIA_UID.2E** 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なう能力を持つ。

また、TOE は、**FPT_SEP.1** により、セキュリティデータの干渉・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.2E**、**FIA_UID.2E** 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:

TOE は、**FTP_ITC.1** により、Web サーバに対し、エンドユーザの識別・認証に使用するユーザ ID とパスワードを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 が稼動する環境は、第 2 章で記述したように、外部ネットワークは HTTPS により保護されており、HTTPS を攻略することは、高レベルの攻撃でなければ成功しない。内部ネットワーク、フロントエンドサーバおよび TOE が動作するサーバは、サーバエリアに設置され、信頼できる管理者以外のアクセスは制限される。従って、本 TOE が想定する攻撃者は、Web ブラウザあるいは HTTP コマンドを利用する、「高度な専門知識を持たない」すなわち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 TOE セキュリティ機能要件のコンポーネントの依存性

本 ST で選択した機能要件コンポーネント	CC パート2で規定されている依存コンポーネント	本 ST で選択した依存コンポーネント	依存性が満たされないコンポーネント
FIA_UAU.2	**FIA_UID.1**	**FIA_UID.2**	なし
FIA_UID.2	なし	—	なし
FIA_USB.1	**FIA_ATD.1**	**FIA_ATD.1**	なし
FIA_ATD.1	なし	—	なし
FDP_ACC.1a	**FDP_ACF.1**	**FDP_ACF.1a**	なし
FDP_ACC.1b	**FDP_ACF.1**	**FDP_ACF.1b**	なし
FDP_ACF.1a	**FDP_ACC.1**	**FDP_ACC.1a**	なし
	FMT_MSA.3	**—**	※1
FDP_ACF.1b	**FDP_ACC.1**	**FDP_ACC.1b**	なし
	FMT_MSA.3	**—**	※1
FMT_SMR.1	**FIA_UID.1**	**FIA_UID.2E**	※2
FMT_SMF.1	なし	—	なし
FMT_MSA.1	**FDP_ACC.1**	**FDP_ACC.1a, FDP_ACC.1b**	なし
	FMT_SMF.1	**FMT_SMF.1**	なし
	FMT_SMR.1	**FMT_SMR.1**	なし
FMT_MTD.1	**FMT_SMR.1**	**FMT_SMR.1**	なし
	FMT_SMF.1	**FMT_SMF.1**	なし
FPT_RVM.1	なし	—	なし

FPT_SEP.1	なし	—	なし

※1:**FDP_ACF.1a**、**FDP_ACF.1b** において、Webコンテナオブジェクト、EJBコンテナオブジェクトに対するアクセス制御ルールを定義しているが、これらのオブジェクトの生成は、J2EE アプリケーションの配備および再配備時に行なわれるものであり、これらの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り、また当該 J2EE アプリケーションのテストを行なった後に、運用が開始される。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、管理操作を行な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.2E** を利用する。

以上により、TOE の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。

表 8-4 IT 環境セキュリティ機能要件のコンポーネントの依存性

機能要件コンポーネント	CC パート2で規定されている依存コンポーネント	IT 環境の依存コンポーネント	依存性が満たされないコンポーネント
FIA_UAU.2E	**FIA_UID.1**	**FIA_UID.2E**	なし
FIA_UID.2E	なし	—	なし
FTP_ITC.1	なし	—	なし

表 8-4 より、IT 環境の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. セキュリティ保証要件依存性

ALC_FLR.1 から依存される保証コンポーネントは無い。

8.2.5. セキュリティ機能要件相互補完性

前節より、TOE 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無いが、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。

これら 識別・認証、アクセス制御、セキュリティ管理の分類に関連する個々のセキュリティ機能要件は、分類内において独立している。また、各分類に関連するセキュリティ機能要件は、他の分類のどの要件とも矛盾する内容ではない。このため、本 TOE セキュリティ機能要件が相互に競合・矛盾することはない。

また、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なっている。

迂回防止:

FIA_UAU.2、**FIA_UID.2** 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.2、**FIA_UID.2** 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:

本 ST には、**FMT_MOF.1** を含んでいないため、セキュリティ機能が不正に非活性化されることはない。

8.2.6. 監査対象事象根拠

本 TOE の使用環境として、エンドユーザのパスワードは、信頼できる管理者が十分強度のあるパスワードを TOE に設定することを前提としている。パスワード長は、8 文字以上であり、パスワードに使用する文字種は、第 2.2 節に示したように、英数字及び記号を想定している。

以上のことから、本 ST では、TOE に登録されていないユーザのログインの繰り返し試行などを監査手段によって検出することをセキュリティ対策方針としてあげていない。このため、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
FIA_UAU.2	a) エンドユーザのパスワードの作成・削除 b) なし(エンドユーザは、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.USER_MNG** b) －
FIA_UID.2	エンドユーザのユーザIDの作成・削除	**SF.USER_MNG**

FIA_USB.1	a) なし(デフォルトのサブジェクトセキュリティ属性は無いため、管理対象とならない) b) なし(デフォルトのサブジェクトセキュリティ属性は無いため、管理対象とならない)	a) － b) －
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)	－
FDP_ACC.1a	なし	－
FDP_ACC.1b	なし	－
FDP_ACF.1a	Webコンテナオブジェクトに対応付けられたロールの管理	**SF.RULE_MNG**
FDP_ACF.1b	EJBコンテナオブジェクトに対応付けられたロールの管理	**SF.RULE_MNG**
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_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)	－
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)	－
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 が想定する利用者は、一般的な Web ブラウザを用いた Web アプリケーションを利用するような一般的な利用者であり、自宅などの通常の環境で利用している。外部ネットワークから TOE にアクセスするためには HTTPS 経由で識別・認証が成功する必要があり、また TOE の利用者は、事前に管理者によって TOE に登録されている必要があり、不特定多数の利用者は想定していない。

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。本製品のような Web アプリケーションサーバは、特にセキュリティ欠陥を追跡し、脆弱性に対する迅速な対応が求められるため、セキュリティ欠陥に対する保証は、利用者に対する安心を担保する上で重要である。このため、ALC_FLR.1 を選択する。

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。

次に、TOE セキュリティ機能要件が各 TOE セキュリティ機能で満たされていることを説明する。

FIA_UAU.2:

FIA_UID.2:

SF.I&A により、TOE は、エンドユーザからの要求に対して、ユーザ ID、パスワードの入力を要求する。エンドユーザが入力したユーザ ID、パスワードが登録済みのユーザ ID、パスワードと一致した場合のみ、識別・認証が成功したものとし、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、エンドユーザにエラーを返信する。

以上により、**FIA_UAU.2**、**FIA_UID.2** は、**SF.I&A** 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、Web コンテナサブジェクトインスタンスに ユーザ ID 及びユーザ ID と対応付けられたロールを関連付ける。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、変更管理に関する規則は無い。

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

FIA_ATD.1:

SF.USER_MNG により、TOE はユーザ ID とユーザ ID に対応付けられたロールの関連を管理する。

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

FDP_ACC.1a:

FDP_ACF.1a:

SF.WEB_ACC により、TOE は、Web コンテナサブジェクトインスタンスに設定されている、ユーザ ID に対応付けられたロールと、Web コンテナオブジェクトに設定されている、Web コンテナオブジェクトに対応付けられたロールに基づいて、アクセス制御を行なう。

TOE は、ユーザ ID に対応付けられたロールが、Web コンテナオブジェクトに対応付けられたロールに関連付けられている場合のみ、要求されたアクセスを許可する。

TOE は、Web コンテナオブジェクトに対するアクセス制御ルールが存在しない場合は、要求されたアクセスを許可する。

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

FDP_ACC.1b:

FDP_ACF.1b:

SF.EJB_ACC により、TOE は、EJB コンテナサブジェクトインスタンスに設定されている、ユーザ ID に対応付けられたロールと、EJB コンテナオブジェクトに設定されている、EJB コンテナオブジェクトに対応付けられたロールに基づいて、アクセス制御を行なう。

TOE は、ユーザ ID に対応付けられたロールが、EJB コンテナオブジェクトに対応付けられたロールに関連付けられている場合のみ、要求されたアクセスを許可する。

TOE は、EJB コンテナオブジェクトに対するアクセス制御ルールが存在しない場合は、要求されたアクセスを許可する。

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

FMT_SMR.1:

SF.USER_MNG 及び **SF.RULE_MNG** により、これらの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.USER_MNG**、**SF.RULE_MNG** により実現できる。

FMT_SMF.1:

第 8.2.7 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.USER_MNG**、**SF.RULE_MNG** にて管理している。

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

FMT_MSA.1:

TOE は、**SF.RULE_MNG** により、Web コンテナオブジェクトに対応付けられたロール及び EJB コンテナオブジェクトに対応付けられたロールを登録・削除・問い合わせ・改変する機能を、管理者に制限する。

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

FMT_MTD.1:

TOE は、**SF.USER_MNG** により、以下のデータを管理する機能を提供する。

- ユーザ ID の登録・削除・問い合わせ
- パスワードの登録・削除
- ユーザ ID に対応付けられたロールの登録・削除・問い合わせ

また、TOE は、**SF.USER_MNG** 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.USER_MNG** により実現できる。

FPT_RVM.1:

SF.I&A において、エンドユーザから Web コンテナ上の J2EE アプリケーションへのアクセスが要求された場合、**SF.I&A** が必ず実施されることを保証している。

SF.WEB_ACC において、Web コンテナサブジェクトインスタンスが Web コンテナオブジェクトにアクセスする際に、**SF.WEB_ACC** が必ず実施されることを保証している。
SF.EJB_ACC において、EJB コンテナサブジェクトインスタンスが EJB コンテナオブジェクトにアクセスする際に、**SF.EJB_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.WEB_ACC**、**SF.EJB_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、Web コンテナサブジェクトインスタンスごとにユーザ ID 及びユーザ ID に対応付けられたロールを管理するため、別の Web コンテナサブジェクトインスタンスからこれらの属性が変更されないことを保証している。
SF.WEB_ACC において、Web コンテナサブジェクトインスタンスごとにユーザ ID 及びユーザ ID に対応付けられたロールを管理するため、別の Web コンテナサブジェクトインスタンスからこれらの属性が変更されないことを保証している。
SF.EJB_ACC において、EJB コンテナサブジェクトインスタンスごとにユーザ ID 及びユーザ ID に対応付けられたロールを管理するため、別の EJB コンテナサブジェクトインスタンスからこれらの属性が変更されないことを保証している。
SF.USER_MNG において、サブジェクトがユーザ ID とユーザ ID に対応付けられたロールに直接アクセスすることが無いことを保証している。
SF.RULE_MNG において、**SF.RULE_MNG** で管理しているデータにサブジェクトが直接アクセス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 TOE セキュリティ機能の表 6-1 に示したように、TOE セキュリティ機能要件は、**FMT_SMR.1**、**FMT_SMF.1**、**FPT_RVM.1**、**FPT_SEP.1** を除き、それぞれ対応関係にある1つの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併せて機能する場合は、**FMT_SMR.1**、**FMT_SMF.1**、**FPT_RVM.1**、**FPT_SEP.1** に限定される。

- **FMT_SMR.1**、**FMT_SMF.1** は **SF.USER_MNG** と **SF.RULE_MNG** で実現される。**SF.USER_MNG** と **SF.RULE_MNG** はいずれも管理コマンドを実行する管理者役割を特定し、ユーザの登録・削除などの管理や、WEB コンテナオブジェクト及び EJB コンテナオブジェクトのセキュリティ属性の管理を分担して実現するセキュリティ機能である。両機能は干渉せず、他方を非活性化することは無く、併せて機能して **FMT_SMR.1**、**FMT_SMF.1** を満たす。
- **SF.I&A**、**SF.WEB_ACC**、**SF.EJB_ACC** はそれぞれバイパスされない実装を行なうことが記述されており、これらが併せて機能して **FPT_RVM.1** を満たす。
- 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できないサブジェクトからのア

クセスができない実装を行なうため **FPT_SEP.1** を満たしている。

- 機能要件と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、他のセキュリティ機能を干渉・したり、非活性化したりすることは無い。

8.3.2. セキュリティ機能強度根拠

本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、**SF.I&A** のユーザ ID、パスワード方式である。これらのセキュリティ機能強度は、第 6.2 節において、SOF-基本を指定している。一方、この 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. 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。