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

2009/07/28

Version 2.04

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.	2009/03/17	2.00	新規作成
2.	2009/04/17	2.01	誤記修正，他
3.	2009/05/25	2.02	前提条件 A.APP の追加
4.	2009/06/18	2.03	システム構成例の変更，誤記修正
5.	2009/07/28	2.04	用語を追記

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

— 目次 —

1. ST概説 1
1.1 ST参照 1
1.2 TOE参照 1
1.3 TOE概要 1
1.3.1 TOEの種別およびセキュリティ機能 1
1.3.2 TOEの構成 2
1.3.3 TOEの動作環境 3
1.4 TOE記述 5
1.4.1 TOEの論理的範囲 5
1.4.2 TOEの物理的範囲 7
1.4.3 TOEの利用者役割 7
2. 適合主張 9
2.1 CC適合主張 9
2.2 PP主張，パッケージ主張 9
2.2.1 PP主張 9
2.2.2 パッケージ主張 9
3. セキュリティ課題定義 10
3.1 脅威 10
3.1.1 保護対象資産 10
3.1.2 脅威 10
3.2 前提条件 10
3.3 組織のセキュリティ方針 11
4. セキュリティ対策方針 12
4.1 TOEのセキュリティ対策方針 12
4.2 運用環境のセキュリティ対策方針 12
4.3 セキュリティ対策方針根拠 13
5. 拡張コンポーネント定義 16
6. セキュリティ要件 17
6.1 セキュリティ機能要件 17
6.2 セキュリティ保証要件 23
6.3 セキュリティ要件根拠 24
6.3.1 セキュリティ機能要件根拠 24
6.3.2 セキュリティ機能要件依存性 25
6.3.3 セキュリティ保証要件根拠 26
7. TOE要約仕様 28

7.1 識別・認証機能(SF.I&A) 28
7.2 Webアクセス制御機能(SF.WEB_ACC) 28
7.3 EJBアクセス制御機能(SF.EJB_ACC) 29
7.4 ユーザ・ロール管理機能(SF.USER_MNG) 30
7.5 アクセスルール管理機能(SF.RULE_MNG) 30
7.6 TOEセキュリティ機能要件とTOEセキュリティ機能の対応関係 31
8. 参考資料・用語 35
8.1 参考資料 35
8.2 用語 35
8.2.1 本STにおける用語 35
8.2.2 略語 37

1. ST 概説

本章では，ST 参照，TOE 参照，TOE 概要，および TOE 記述について記述する。

1.1 ST 参照

ST 名称	: uCosminexus Application Server セキュリティターゲット
バージョン	: 2.04
発行日	: 2009 年 7 月 28 日
作成者	: 株式会社 日立製作所 ソフトウェア事業部

1.2 TOE 参照

TOE	: uCosminexus Application Server
TOE バージョン	: 08-00
キーワード	: Application Server
開発者	: 株式会社 日立製作所

1.3 TOE 概要

1.3.1 TOE の種別およびセキュリティ機能

(1) TOE 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。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。

(2) セキュリティ機能

TOE が提供するセキュリティ機能を以下に示す。

- 識別・認証機能

ユーザ ID とパスワードによりエンドユーザの識別と認証を行なう機能。

- アクセス制御機能

認証済みのユーザ情報を用いて、Web コンテナ上のオブジェクトと EJB コンテナ上のオブジェクトに対するアクセス制御を行なう機能。

- セキュリティ管理機能

エンドユーザの識別・認証情報とアクセス権限情報の管理と、アプリケーションに対して許可されるアクセス権限の管理を行なう機能。

1.3.2 TOE の構成

uCosminexus Application Serverは、複数のソフトウェアコンポーネントにより構成される。uCosminexus Application Serverに含まれる代表的なソフトウェアコンポーネントの構成を図 1-1に示す。これらのソフトウェアコンポーネントのうち、TOEはComponent Containerである。

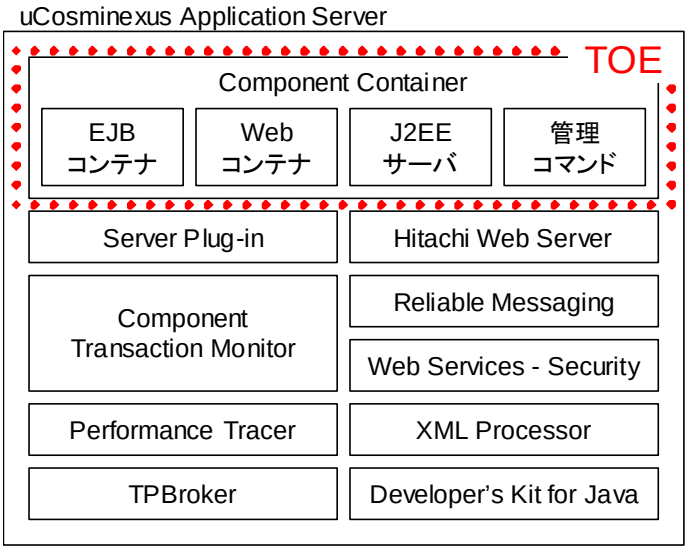

図 1-1 uCosminexus Application Server の構成

各ソフトウェアコンポーネントについて、表 1-1を用いて説明する。

表 1-1 uCosminexus Application Server を構成するソフトウェアコンポーネント

ソフトウェアコンポーネント	概要説明
Component Container	TOE が提供するセキュリティ機能を提供するソフトウェアコンポーネント。 J2EE 準拠の Java アプリケーションの実行基盤を提供するソフトウェアコンポーネント。
Hitachi Web Server	Web ブラウザからのリクエストの受信および Web ブラウザへのデータ送信を行う Web サーバ。
Developer's Kit for Java	J2SE 準拠の Java アプリケーションの開発・実行環境を提供するコンポーネント。
TPBroker	分散システムの通信制御機能などの開発・実行環境を提供するコンポーネント。
Performance Tracer	リクエストの処理トレースの出力機能を提供するコンポーネント。
Component Transaction Monitor	Component Container への処理リクエストの流量制御機能などを提供するコンポーネント。

XML Processor	XML 形式のデータの解析機能などを提供するコンポーネント。
Web Services – Security	XML 署名および XML 暗号を利用した XML セキュリティ機能などを提供するコンポーネント
Reliable Messaging	高信頼のメッセージ管理機能やメッセージ通信機能などを提供するコンポーネント
Server Plug-in	Component Container の運用・管理機能を提供するコンポーネント

なお，パッケージ構成は，製品のエディションによって内容が異なる。以下に，違いをまとめる。

表 1-2 製品エディションによる違い

製品エディション	説明
uCosminexus Application Server Enterprise	表 1-1記載のすべてのソフトウェアコンポーネントが含まれる。
uCosminexus Application Server Standard	表 1-1記載のソフトウェアコンポーネントのうち，Component Transaction Monitorを除くすべてのコンポーネントが含まれる。

1.3.3 TOE の動作環境

(1) TOE 運用環境

TOEを利用したシステム構成の一例を図 1-2に示す。

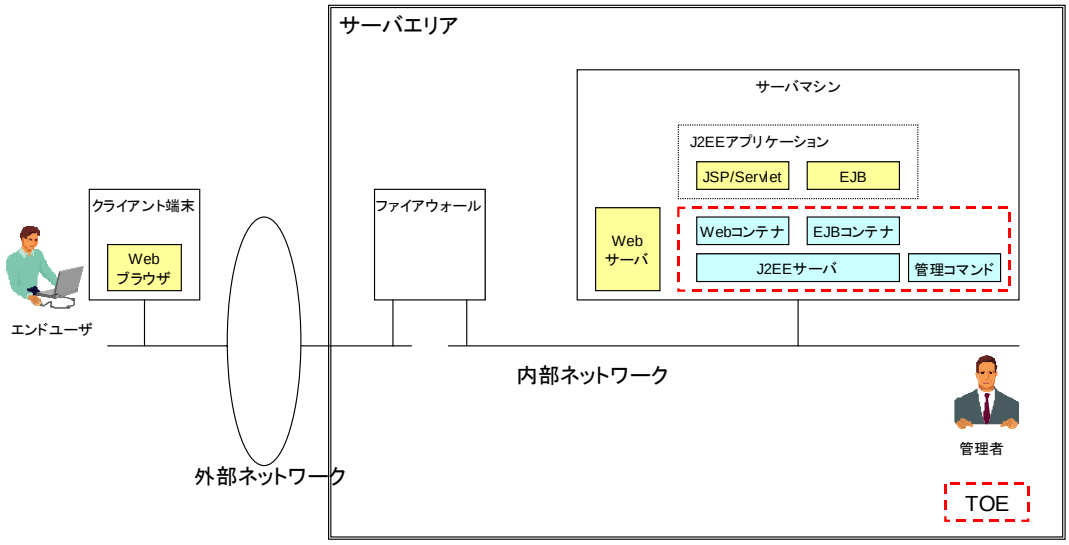

図 1-2 TOE を利用したシステム構成の一例

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、サーバマシンは、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。

【サーバマシン】

TOEとWebサーバ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、管理者はサーバマシン上で管理コマンドを実行し、TOEの運用を管理する。Webサーバは, エンドユーザからの要求を受付け、J2EEサーバを介してJ2EEアプリケーションに受け渡し、またJ2EEサーバ経由で受け取ったJ2EEアプリケーションからの応答をエンドユーザに返信する。サーバマシンのうち、図 1-2の破線で囲んだ範囲がTOEである。

(2) 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。

[Windows の場合]

- Windows Server 2003, Standard Edition (32bit)
  本 ST の TOE 外であり、IT 環境である。
- uCosminexus Application Server Standard 08-00 または uCosminexus Application Server Enterprise 08-00
  本 ST の TOE を含む製品である。

[Linux の場合]

- Red Hat Enterprise Linux 5 (x86)
  本 ST の TOE 外であり、IT 環境である。
- uCosminexus Application Server Standard 08-00 または uCosminexus Application Server Enterprise 08-00
  本 ST の TOE を含む製品である。

(3)　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。

[Windows の場合]

下記シリーズ中で Windows Server 2003, Standard Edition (32bit)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 410 MB

標準メモリ量： 約 1220 MB

[Linux の場合]

下記シリーズ中で Red Hat Enterprise Linux 5 (x86)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 520 MB

標準メモリ量： 約 2570 MB

1.4　TOE 記述

1.4.1　TOE の論理的範囲

本節では，TOEの論理的範囲について記述する。TOEの論理構成の一例を図 1-3に示す。

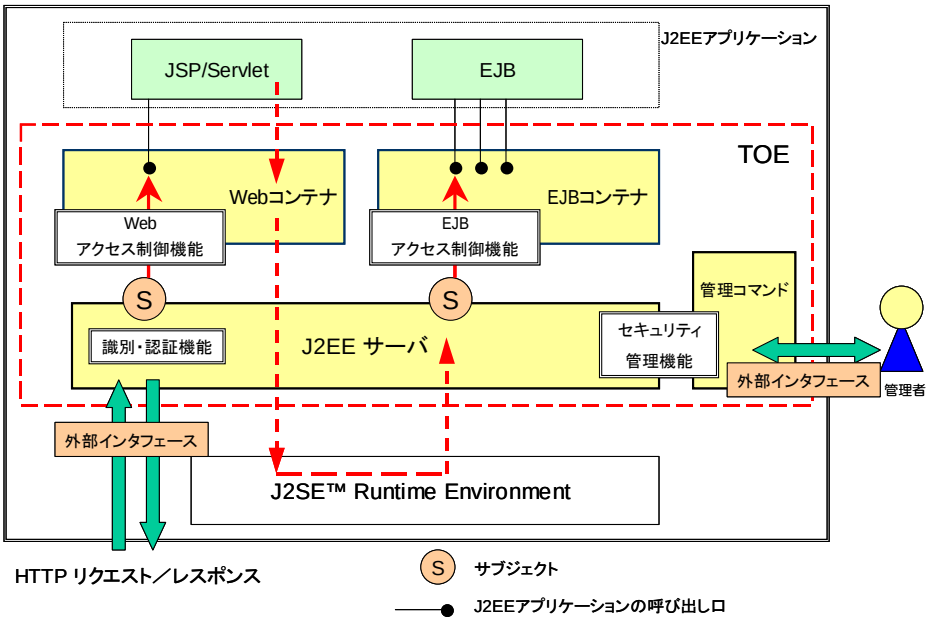

図 1-3 TOE の論理構成

(1) TOE によって提供される基本機能
TOE が提供する基本機能を以下に示す。

【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) TOE によって提供されるセキュリティ機能
TOE が提供するセキュリティ機能を以下に示す。

【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】
以下の 2 種類のアクセス制御を行なう。

- **【Web アクセス制御】**（Web コンテナオブジェクト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 アクセス制御】**（EJB コンテナオブジェクト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】
以下の 2 種類のセキュリティ管理を行なう。

- **【ユーザ・ロール管理】**（識別・認証情報とロール情報の管理）

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。

- **【アクセスルール管理】**（J2EE アプリケーションのロール情報の管理）

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。

(3) 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。

1.4.2 TOE の物理的範囲

図 1-3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。

また，TOE に付属のガイダンス文書は以下の通りである。

- 日立ソフトウェアマニュアル
- Cosminexus アプリケーションサーバ V8 セキュリティ構築・運用ガイド

1.4.3 TOE 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、サーバマシン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、管理者はサーバマシン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. 適合主張

2.1 CC 適合主張

本 ST は以下の CC に適合している。

- ST が適合主張する CC のバージョン
  - パート 1 : 概説と一般モデル 2007 年 4 月 バージョン 3.1 改訂第 1 版 ［翻訳第 1.2 版］
  - パート 2 : セキュリティ機能コンポーネント 2008 年 3 月 バージョン 3.1 改訂第 2 版 ［翻訳第 2.0 版］
  - パート 3 : セキュリティ保証コンポーネント 2008 年 3 月 バージョン 3.1 改訂第 2 版 ［翻訳第 2.0 版］
- CC パート 2 に対する適合
  - CC パート 2 適合
- CC パート 3 に対する適合
  - CC パート 3 適合

2.2 PP 主張，パッケージ主張

2.2.1 PP 主張

本 ST が適合主張する PP はない。

2.2.2 パッケージ主張

本 ST の評価保証レベルは EAL2 追加である。
追加されるセキュリティ保証要件は ALC_FLR.1 である。

3. セキュリティ課題定義

本章では，脅威，前提条件，組織のセキュリティ方針について記述する。

3.1 脅威

3.1.1 保護対象資産

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

3.1.2 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、不正に HTTP リクエストを送信することにより、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。

3.2 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、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。

A. APP

TOE を利用して動作する J2EE アプリケーションに含まれる Enterprise Beans は，Session Bean であるものとする。

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 のセキュリティ対策方針、運用環境のセキュリティ対策方針，およびセキュリティ対策方針の根拠について記述する。

4.1 TOE の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 運用環境の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。

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、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。

4.3 セキュリティ対策方針根拠

セキュリティ対策方針は、セキュリティ課題定義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 4-1に示す。

表 4-1 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	A.APP	P.PASSWORD
O.I&A	○							
O.ACC		○						
O.MANAGE	○	○						○
OE.I&A	○	○						
OM.PHYSICAL			○					
OM.FIREWALL						○		
OM.ADMIN				○	○		○	○

表 4-1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。

以上により、T.UNDEFINED_USERS は、O.I&A、O.MANAGE、OE.I&A 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、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。

A.APP：

OM.ADMIN により，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.APP は、OM.ADMIIN 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。

5. 拡張コンポーネント定義

本 ST では，拡張コンポーネントを定義しない。

6. セキュリティ要件

6.1 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: FIA_UAU.1 認証のタイミング
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 TSF は、その利用者を代行する他の TSF 仲介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。

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング
依存性: なし

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FIA_USB.1 利用者-サブジェクト結合

下位階層: なし
依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 TSF は、以下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、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: 属性の最初の関連付けの規則]

[割付: 属性の最初の関連付けの規則]
なし

FIA_USB.1.3 TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を

代行して動作するサブジェクトと共に実施しなければならない。: [割付: 属性の変更の規則]

[割付: 属性の変更の規則]
なし

FIA_ATD.1 利用者属性定義

下位階層: なし
依存性: 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]

[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

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
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.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

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
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.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

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

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.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を決定するために、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、次の追加規則、[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許可する規則]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許可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許可する規則]
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

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
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.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を決定するために、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、次の追加規則、[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許可する規則]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許可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許可する規則]
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

FMT_SMR.1 セキュリティの役割

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

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。

FMT_SMF.1 管理機能の特定

下位階層: なし
依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。: [割付: TSF によって提供される管理機能のリスト]

[割付: TSF によって提供される管理機能のリスト]

表 6-1 TSF によって提供される管理機能のリスト

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	a) エンドユーザのパスワードの作成・削

	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	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・問い合わせ
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。	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）

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

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_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定

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[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。

[割付: 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]]	[割付: 許可された識別された役割]	[割付: 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

FMT_MTD.1 TSF データの管理

下位階層: なし
依存性: FMT_SMR.1 セキュリティの役割 FMT_SMF.1 管理機能の特定

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。

[割付: TSF データのリスト]	[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]]	[割付: 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

6.2 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 の保証コンポーネントを表 6-2に示す。

表 6-2 保証コンポーネント一覧

保証クラス	保証コンポーネント

ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP.2 セキュリティ実施機能仕様
	ADV_TDS.1 基本設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.2 CM システムの使用
	ALC_CMS.2 TOE の一部の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_FLR.1 基本的な欠陥修正
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE: テスト	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
AVA: 脆弱性評定	AVA_VAN.2 脆弱性分析

6.3 セキュリティ要件根拠

6.3.1 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6-3に示す。

表 6-3 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
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			○

表 6-3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。

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。

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。

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。

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。

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。

6.3.2 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 6-4に示す。

表 6-4 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	—	※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

※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。

6.3.3 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。本 TOE はセキュアな環境に構築されるシステムの一部であり，物理的に隔離されたサーバエリアで運用され，外部ネットワークと内部ネットワークの間はファイアウォールによって TOE を利用するために必要なプロトコルのみを通過させるように管理されている。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。

7. TOE 要約仕様

本節では、TOE セキュリティ機能について記述する。

7.1 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、維持されている。

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・パスワードは、SF.USER_MNG で管理され、維持されている。

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関連付けは、SF.USER_MNG で管理され、維持されている。

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。

7.2 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。

7.3 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。

7.4 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管理コマンドとして提供する。

- 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、管理コマンドの利用に際して、実行できる役割を管理者に制限し、維持する。

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維持しており、TOE のアクセス制御機能、すなわち、SF.WEB_ACC 及び SF.EJB_ACC はこの関連付けを利用している。

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。

7.5 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管理コマンドとして提供する。

- 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、管理コマンドの利用に際して、実行できる役割を管理者に制限し、維持する。

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。

7.6 TOE セキュリティ機能要件と TOE セキュリティ機能の対応関係

本節では，TOE セキュリティ機能要件と TOE セキュリティ機能の対応関係について記述する。
表 7-1に示すとおり，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。

表 7-1 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
SF.I&A	○	○	○									
SF.WEB_ACC					○		○					
SF.EJB_ACC						○		○				
SF.USER_MNG				○					○	○		○
SF.RULE_MNG									○	○	○	

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維持する。

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、管理コマンドを実行する管理者の役割が維持される。また、管理コマンドの利用者は、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：

表 7-2に，表 6-1で示したTSFの管理項目とTOEセキュリティ機能との対応関係を示す。

表 7-2 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・問い合わせ	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）	－

表 7-2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。

8. 参考資料・用語

8.1 参考資料

- Common Criteria for Information Technology Security Evaluation Version 3.1
  Part 1: Introduction and general model Revision 1 (CCMB-2006-09-001)
- Common Criteria for Information Technology Security Evaluation Version 3.1
  Part 2: Security functional components Revision 2 (CCMB-2007-09-002)
- Common Criteria for Information Technology Security Evaluation Version 3.1
  Part 3: Security assurance components Revision 2 (CCMB-2007-09-003)
- Common Methodology for Information Technology Security Evaluation Version 3.1
  Evaluation methodology Revision 2 (CCMB-2007-09-004)
- 情報技術セキュリティ評価のためのコモンクライテリア バージョン 3.1
  パート 1: 概説と一般モデル 改訂第 1 版 ［翻訳第 1.2 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 バージョン 3.1
  パート 2: セキュリティ機能コンポーネント 改訂第 2 版 ［翻訳第 2.0 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 バージョン 3.1
  パート 3: セキュリティ保証コンポーネント 改訂第 2 版 ［翻訳第 2.0 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 バージョン 3.1
  評価方法 改訂第 2 版 ［翻訳第 2.0 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

8.2 用語

8.2.1 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。
ロール	アクセス許可に関する情報。エンドユーザに付与されるアクセス権限と，アプリケーションへのアクセス許可範囲を指定するための情報がある。
ディスク占有量	製品に含まれる全てのソフトウェアコンポーネントをインストールするのに必要となるディスク容量をあらわしている。
標準メモリ量	製品に含まれる全てのソフトウェアコンポーネントを利用した場合に必要となるメモリ量をあらわしている。

8.2.2 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™）