Cosminexus セキュリティ構築・運用ガイド

解説・手引・操作書

3020-3-N37-10

マニュアルの購入方法

このマニュアル，および関連するマニュアルをご購入の際は，巻末の「ソフトウェアマニュアルのサービス ご案内」をご参照ください。

HITACHI

■対象製品

●適用 OS：Windows 2000 Server，Windows Server 2003，Windows Server 2003 R2，Windows Server 2003（x64），Windows Server 2003 R2（x64）
P-2443-7D74 uCosminexus Application Server Standard 07-00
P-2443-7K74 uCosminexus Application Server Enterprise 07-00
●適用 OS：AIX 5L V5.1，AIX 5L V5.2，AIX 5L V5.3
P-1M43-7D71 uCosminexus Application Server Standard 07-00
P-1M43-7K71 uCosminexus Application Server Enterprise 07-00
●適用 OS：HP-UX 11i V2（IPF）
P-1J43-7D71 uCosminexus Application Server Standard 07-00
P-1J43-7K71 uCosminexus Application Server Enterprise 07-00
●適用 OS：Red Hat Enterprise Linux AS 3（x86），Red Hat Enterprise Linux AS 4（x86），Red Hat Enterprise Linux ES 3（x86），Red Hat Enterprise Linux ES 4（x86），Red Hat Enterprise Linux AS 3（AMD64 & Intel EM64T），Red Hat Enterprise Linux AS 4（AMD64 & Intel EM64T）
P-9S43-7D71 uCosminexus Application Server Standard 07-00
P-9S43-7K71 uCosminexus Application Server Enterprise 07-00
●適用 OS：Solaris 8，Solaris 9，Solaris 10
P-9D43-7D71 uCosminexus Application Server Standard 07-00
P-9D43-7K71 uCosminexus Application Server Enterprise 07-00
本製品では日立トレース共通ライブラリをインストールします。

■ ISO/IEC 15408 の認証

この製品は，ISO/IEC 15408 に基づき EAL2 + ALC_FLR.1 の認証を取得しました。
なお，この認証は，製品そのものを保証しているのではなく，ISO/IEC 15408 による評価結果がその保証要件を満たしていることを意味するものです。

■輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標類

■発行

2007 年 1 月（第 1 版）3020-3-N37
2007 年 3 月（第 2 版）3020-3-N37-10

■著作権

変更内容

変更内容（3020-3-N37-10**）** uCosminexus Application Server Standard　07-00，uCosminexus Application Server Enterprise　07-00

追加・変更機能	変更個所
ISO/IEC 15408 に基づき EAL2 + ALC_FLR.1 の認証を取得した。	中表紙裏

単なる誤字・脱字などはお断りなく訂正しました。

はじめに

このマニュアルは，Cosminexus（コズミネクサス）のセキュリティを考慮したシステム構築手順，システムの運用方法，およびシステム構築・運用で使用するファイルやコマンドについて説明したものです。
Cosminexus では，次に示すプログラムプロダクトを使用して，アプリケーションサーバをセキュアに構築・運用できます。

- P-1J43-7D71　uCosminexus Application Server Standard　07-00
- P-1J43-7K71　uCosminexus Application Server Enterprise　07-00
- P-1M43-7D71　uCosminexus Application Server Standard　07-00
- P-1M43-7K71　uCosminexus Application Server Enterprise　07-00
- P-2443-7D74　uCosminexus Application Server Standard　07-00
- P-2443-7K74　uCosminexus Application Server Enterprise　07-00
- P-9D43-7D71　uCosminexus Application Server Standard　07-00
- P-9D43-7K71　uCosminexus Application Server Enterprise　07-00
- P-9S43-7D71　uCosminexus Application Server Standard　07-00
- P-9S43-7K71　uCosminexus Application Server Enterprise　07-00

なお，オペレーティングシステム（OS）の種類によって，機能が異なる場合があります。OSごとの違いがある場合の表記方法については，「適用 OS の違いによる機能相違点の表記」を参照してください。

■対象読者

このマニュアルは，Cosminexus のアプリケーションサーバをセキュアに構築・運用したい方を対象としています。
次の内容を理解されていることを前提としています。

- OS（Windows または UNIX）のシステム構築および運用に関する知識
- J2EE に関する知識

また，このマニュアルは，マニュアル「Cosminexus 機能解説」を理解していることを前提としていますので，あらかじめお読みいただくことをお勧めします。

■マニュアルの構成

このマニュアルは，次に示す章と付録から構成されています。

第１章　セキュリティ構築・運用の概要

Application Server のセキュリティ機能を使用して構築・運用するシステムの概要について説明しています。また，マニュアルの使い方，セキュリティポリシーの制定，および構築・運用の流れについて説明しています。

第２章　システム構成の検討

セキュアなアプリケーションサーバを実現するシステム構成について，ハードウェア，ソフト

ウェアに分けて説明しています。

第３章　システム構築前の準備
システムを構築する前に必要な準備作業について説明しています。

第４章　システムの構築
システムを構築する方法について，例に基づいて説明しています。

第５章　システム運用前の準備
システムを運用する前に必要な準備作業について説明しています。

第６章　システムの運用
システム運用に必要な作業のうち，アプリケーションサーバをセキュアに保つために必要な作業について説明しています。

第７章　リファレンス
Cosminexus が提供するファイルおよびコマンドのうち，このマニュアルで説明する操作に必要なものを一覧で説明しています。また，Application Server のセキュリティ機能で使用するファイルやコマンドの詳細について説明しています。

付録 A　用語解説
このマニュアルで使用している用語について説明しています。

■関連マニュアル

関連マニュアルを次に示します。必要に応じてお読みください。

- Cosminexus 概説（3020-3-M01）
- Cosminexus 機能解説（3020-3-M03）
- Cosminexus システム設計ガイド（3020-3-M04）
- Cosminexus システム構築ガイド（3020-3-M06）
- Cosminexus システム運用ガイド（3020-3-M07）
- Cosminexus アプリケーション設定操作ガイド（3020-3-M08）
- Cosminexus リファレンス コマンド編（3020-3-M10）
- Cosminexus リファレンス 定義編（3020-3-M11）
- Cosminexus メッセージ 1 KDJE 編（3020-3-M12）
- Hitachi Web Server（3020-3-M15）
- TPBroker ユーザーズガイド（3020-3-M16）

■読書手順

このマニュアルは，利用目的に合わせて章を選択して読むことができます。利用目的別にお読みいただくことをお勧めしますが，最初は必ず通読してください。

マニュアルを読む目的		記述個所
このマニュアルで説明することの概要について知りたい。	このマニュアルの使い方を知りたい。	1.1
	構築・運用するシステムの概要，および使用するセキュリティ機能について知りたい。	1.2
	構築・運用に当たってのセキュリティポリシーについて知りたい。	1.3
	構築・運用の流れを知りたい。	1.4
システム構築について知りたい。	構築するシステムの構成を知りたい。	2 章
	構築前の準備作業について知りたい。	3 章
	Application Server のセキュリティ機能を使用した，Cosminexus のシステム構築方法について知りたい。	4 章
システム運用について知りたい。	運用前の準備作業について知りたい。	5 章
	Application Server のセキュリティ機能を使用して，システムをセキュアに保つ運用方法について知りたい。	6 章
このマニュアルで説明する Cosminexus のファイルやコマンドについて知りたい。		7 章
このマニュアルで使用する用語について知りたい。		付録 A

■このマニュアルでの表記

このマニュアルで使用している表記と，対応する製品名を次に示します。

表記		製品名
Application Server	Application Server Enterprise	uCosminexus Application Server Enterprise
	Application Server Standard	uCosminexus Application Server Standard
Internet Explorer		Microsoft(R) Internet Explorer
IPF		Itanium(R) Processor Family
UNIX	AIX	AIX 5L V5.1
		AIX 5L V5.2
		AIX 5L V5.3
	HP-UX	HP-UX 11i V2（IPF）
	Linux	Red Hat Enterprise Linux AS 3（x86）
		Red Hat Enterprise Linux AS 4（x86）
		Red Hat Enterprise Linux ES 3（x86）
		Red Hat Enterprise Linux ES 4（x86）

表記		製品名
		Red Hat Enterprise Linux AS 3（AMD64 & Intel EM64T）
		Red Hat Enterprise Linux AS 4（AMD64 & Intel EM64T）
	Solaris	Solaris 8
		Solaris 9
		Solaris 10
Windows 2000 Server		Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Microsoft(R) Windows(R) 2000 Datacenter Server Operating System
		Microsoft(R) Windows(R) 2000 Server Operating System
Windows Server 2003		Microsoft(R) Windows Server(TM) 2003, Enterprise Edition Operating System（x86）
		Microsoft(R) Windows Server(TM) 2003, Standard Edition Operating System（x86）
Windows Server 2003 R2		Microsoft(R) Windows Server(TM) 2003 R2 Enterprise Edition Operating System（x86）
		Microsoft(R) Windows Server(TM) 2003 R2 Standard Edition Operating System（x86）
Windows Server 2003（x64）		Microsoft(R) Windows Server(TM) 2003, Enterprise x64 Edition Operating System
		Microsoft(R) Windows Server(TM) 2003, Standard x64 Edition Operating System
Windows Server 2003 R2（x64）		Microsoft(R) Windows Server(TM) 2003 R2, Enterprise x64 Edition Operating System
		Microsoft(R) Windows Server(TM) 2003 R2, Standard x64 Edition Operating System

Windows 2000 Server，Windows Server 2003，Windows Server 2003 R2，Windows Server 2003（x64），および Windows Server 2003 R2（x64）を総称して Windows と表記することがあります。

このマニュアルで使用している表記と，対応する Cosminexus の機能名を次に示します。

表記	Cosminexus の機能名
Cosminexus Developer's Kit for Java	Cosminexus Developer's Kit for Java™
Management Server	Cosminexus Management Server
PRF	Cosminexus Performance Tracer

このマニュアルで使用している表記と，対応する Java 関連用語を次に示します。

表記	Java 関連用語
EAR	Enterprise ARchive
EJB または Enterprise JavaBeans	Enterprise JavaBeans™
J2EE	Java™ 2 Platform, Enterprise Edition
JAR	Java™ Archive
Java	Java™
JSP	JavaServer Pages™
Servlet またはサーブレット	Java™ Servlet
WAR	Web ARchive

■適用 OS の違いによる機能相違点の表記

このマニュアルは，適用 OS が Windows，AIX，HP-UX，Linux，および Solaris の製品に対応します。OS によって記述を書き分ける場合，次に示す表記を使用して，それぞれの説明に OS 名を明記しています。

表記	意味
Windows の場合	Windows に該当する表記です。
AIX の場合	AIX に該当する表記です。
HP-UX の場合	HP-UX に該当する表記です。
Linux の場合	Linux に該当する表記です。
Solaris の場合	Solaris に該当する表記です。
UNIX の場合	UNIX（AIX，HP-UX，Linux，Solaris）に該当する表記です。

■このマニュアルで使用している略語

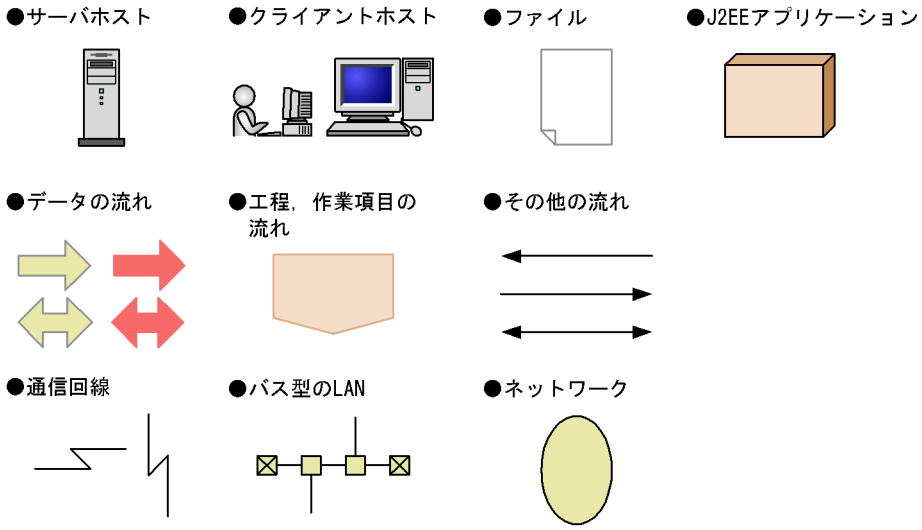
このマニュアルで使用している英略語を次に示します。

英略語	英字での表記
CD-ROM	Compact Disk - Read Only Memory
CSR	Certificate Signing Request
DD	Deployment Descriptor
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Security
I/O	Input/Output

英略語	英字での表記
IP	Internet Protocol
JST	Japan Standard Time
LAN	Local Area Network
OS	Operating System
PC/AT	Personal Computer/Advanced Technology
PP	Program Product
RSA	Rivest Shamir Adleman
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
XML	Extensible Markup Language

■このマニュアルの図中で使用している記号

このマニュアルの図中で使用している記号を，次のように定義します。



■このマニュアルで使用している記号

注意事項

操作時に遵守する必要がある項目や，誤るとトラブルが発生するような項目について説明しています。

■このマニュアルの GUI の説明で使用している記号

このマニュアルでは，次に示す記号を使用して GUI を説明しています。

記号	意味
[　]	画面の名称および画面に表示されている項目を表します。

■このマニュアルのコマンドの説明で使用している記号

このマニュアルでは，次に示す記号を使用してコマンドの文法を説明しています。

記号	意味
[ ]	この記号で囲まれている項目は省略してもよいことを示します。複数の項目が横に並べて記述されている場合には，すべてを省略するか，記号{ }と同じくどれか一つを選択します。 （例）[A] " 何も指定しない " か "A を指定する " ことを示します。
< >	この記号で囲まれている項目は，該当する要素やファイルを指定することを示します。 （例） < ユーザ ID> ユーザ ID を指定します。
...	この記号の直前に示す記号を繰り返し，複数個指定できることを示します。 （例） < ユーザ ID>... ユーザ ID は複数個，繰り返して指定できます。

■常用漢字以外の漢字の使用について

このマニュアルでは，常用漢字を使用することを基本としていますが，次に示す用語については，常用漢字以外の漢字を使用しています。

鍵（かぎ） 個所（かしょ） 全て（すべて）

■ KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイトです。

目次

図目次

表目次

1 セキュリティ構築・運用の概要

Application Server のセキュリティ機能とは，セキュアなシステムを構築・運用するために必要なユーザ認証，およびアクセス制御の仕組みです。
この章では，Application Server のセキュリティ機能を使用して構築・運用するシステムの概要について説明します。また，マニュアルの使い方，セキュリティポリシーの制定，および構築・運用の流れについて説明します。

1.1 このマニュアルの使い方

このマニュアルは，Cosminexus のアプリケーションサーバをセキュアに構築・運用することを目的としています。このマニュアルに沿った操作で構築・運用をすれば，外部の脅威からアプリケーションサーバを保護できます。

ただし，このマニュアルで説明するセキュアなシステム環境では，使用できる Cosminexus の機能が限定されます。このマニュアルで説明しないシステム環境については，マニュアル「Cosminexus システム設計ガイド」を参照してください。

ここでは，マニュアルの対象読者，およびマニュアルの読み方について説明します。

1.1.1 マニュアルの対象読者

このマニュアルの対象読者は，システムを構築・運用するシステム管理者です。システム管理者は，次に示す作業を実施します。

- セキュリティポリシーの制定
- ハードウェアの設置，および内部ネットワークの構築
- システムに必要なソフトウェアのインストール，および設定
- アプリケーションサーバにアクセスするエンドユーザの管理
- アプリケーションサーバで動作させる J2EE アプリケーションの配備，および管理

このマニュアルでは，システム管理者のことを**管理者**と呼びます。また，エンドユーザを**利用者**，J2EE アプリケーションを開発して管理者に提供する人を**開発者**と呼びます。

1.1.2 マニュアルの読み方

このマニュアルは，記述してあるとおりに作業を進めることが前提条件です。なお，このマニュアルは，構築時と運用時で読み方が異なります。それぞれの読み方について説明します。

構築時のマニュアルの読み方

マニュアルの 1 ～ 4 章を通読してください。また，必要に応じて 7 章を参照してください。

このマニュアルは，システムをセキュアに構築するために必要な作業はすべて記載しています。このマニュアルで説明しない作業については，マニュアル「Cosminexus システム構築ガイド」を参照してください。

運用時のマニュアルの読み方

運用開始時は，マニュアルの 5，6 章を通読してください。運用中は，1，5，6 章の中から必要な個所を参照してください。また，必要に応じて 7 章を参照してください。

このマニュアルは，運用中に発生する作業のうち，Application Server のセキュリティ機能に関係する作業についてだけ記載しています。Application Server のセ

キュリティ機能に関係しない作業については，マニュアル「Cosminexus システム運用ガイド」を参照してください。

1.2　構築・運用するシステムの概要

システムをセキュアに構築・運用するためには，外部からの脅威に対してセキュリティ対策を実施する必要があります。Cosminexus では，Application Server がセキュリティ機能を提供しています。

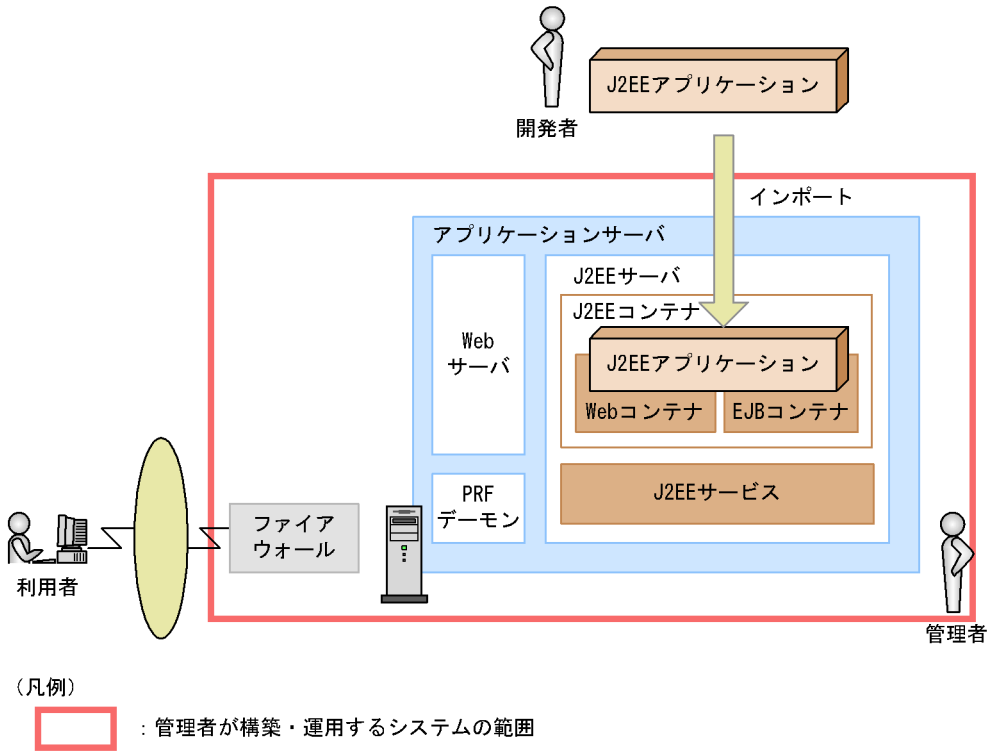
ここでは，Application Server のセキュリティ機能を使用して構築・運用するシステムの全体像，およびセキュリティ機能の概要について説明します

1.2.1　システムの全体像

構築・運用するシステムは，利用者がインターネットを使用してアプリケーションサーバにアクセスする，Web **クライアント構成**です。

システムの全体像を次の図に示します。

図 1-1　システムの全体像



このマニュアルで説明するのは，図中に示した管理者が構築・運用するシステムの範囲です。ここでは，管理者が構築・運用するシステムの範囲のうち，アプリケーションサーバについて説明します。

（1） J2EE サーバ

J2EE アプリケーションの実行基盤であり，Application Server のセキュリティ機能を提供するプロセスです。J2EE サーバは，次のプログラムモジュールで構成されます。

● **J2EE アプリケーション**
利用者のリクエストに応じて業務サービスを提供するアプリケーションで，複数の J2EE コンポーネントで構成されます。J2EE サーバにインポートする J2EE アプリケーションは，開発者から入手します。

● **J2EE コンテナ**
J2EE コンポーネントが動作する基盤です。Web アプリケーションが動作する Web コンテナと，EJB が動作する EJB コンテナで構成されます。

● **J2EE サービス**
J2EE コンテナの部品機能として利用され，Application Server のセキュリティ機能の基盤となります。

（2） Web サーバ

利用者の Web ブラウザからのリクエスト受信，および利用者の Web ブラウザへのレスポンス送信に関連する処理を実行するプロセスです。このマニュアルで説明するシステムでは，Web サーバとして，Application Server の構成ソフトウェアである Hitachi Web Server を使用します。

（3） PRF デーモン

バッファに出力されたトレース情報をファイルに出力する I/O プロセスです。

1.2.2 Application Server のセキュリティ機能

このマニュアルで説明するシステムに適用する Application Server のセキュリティ機能は，J2EE サーバによるユーザ認証とアクセス制御の 2 種類です。ユーザ認証とアクセス制御は，登録された利用者が，その利用者に許可されたコンテンツだけにアクセスするための仕組みです。

ここでは，このマニュアルで説明するシステムに適用する Application Server のセキュリティ機能について説明します。

（1） ユーザ認証

不正なアクセスを防ぐために，J2EE サーバの Web コンテナは，利用者の**ユーザ認証情報**（ユーザ ID，パスワード）を用いてユーザ認証をします。

認証方式には次の種類があります。

● HTTP（Basic 認証）

認証インタフェースとして，Web ブラウザの機能を使用します。

● HTTP（Form 認証）
認証の機能は HTTP（Basic 認証）と同じです。認証インタフェースを開発者が自由にデザインできます。

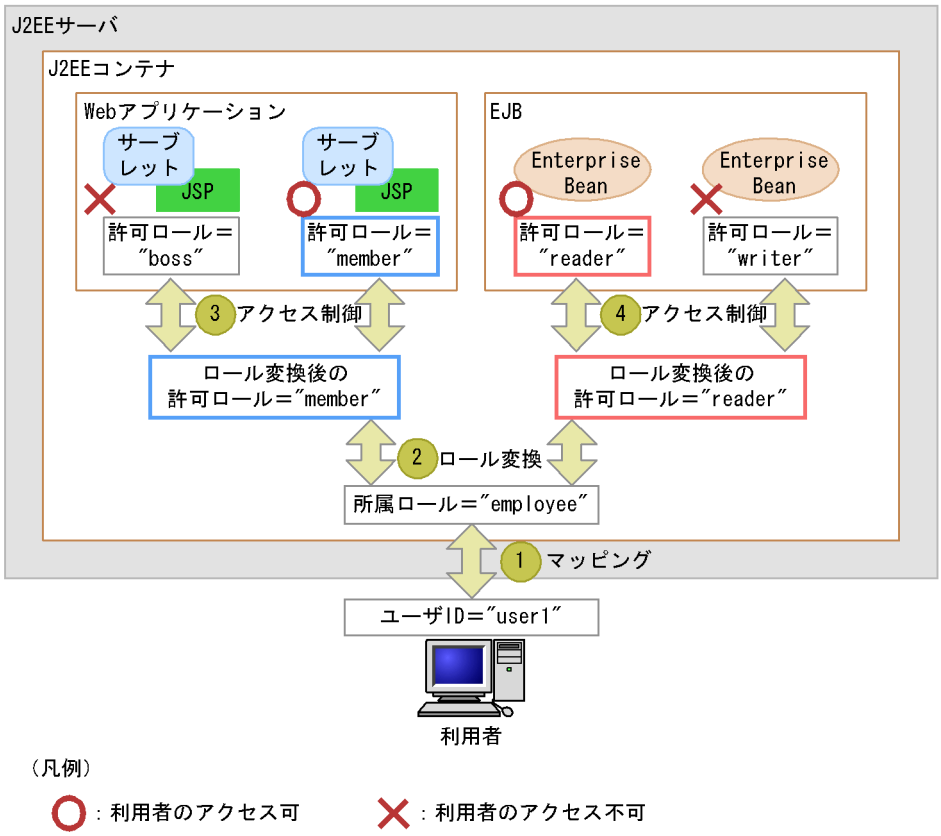
(2) アクセス制御

利用者の役割に応じた業務サービスを提供するために，J2EE サーバの J2EE コンテナは，**セキュリティロール**によるアクセス制御をします。

セキュリティロールによるアクセス制御とは，リクエストを送信した利用者が所属するロール（**所属ロール**）と，J2EE アプリケーションがアクセスを許可するロール（**許可ロール**）とを比べることで，そのリクエストを許可するかどうかを制御する仕組みです。

セキュリティロールによるアクセス制御の流れを，簡単な例を用いて次の図に示します。図中の記号は，図の説明 1. ～ 4. に対応します。

図 1-2 セキュリティロールによるアクセス制御の概要



1. **マッピング（ユーザ ID ←→所属ロール）**
各利用者のユーザ ID と，対応する所属ロールをマッピングします。一つのユーザ ID

に対して複数の所属ロールをマッピングさせることもできます。
この例では，利用者のユーザ ID は「user1」，所属ロールは「employee」です。

2. **ロール変換（所属ロール←→許可ロール）**
   マッピングした所属ロールを，対応する許可ロールにロール変換します。一つの所属ロールに対して複数の許可ロールを対応させることもできます。
   この例では，所属ロール「employee」を，許可ロール「member」および「reader」にロール変換しています。

3. **アクセス制御（ロール変換後の許可ロール←→ Web アプリケーションの許可ロール）**
   ロール変換した許可ロールと，Web アプリケーションに設定された許可ロールを比較します。比較した結果が同じ場合は利用者のアクセス可，異なる場合は利用者のアクセス不可です。
   この例では，利用者は許可ロール「member」が設定された Web アプリケーションにアクセスできます。許可ロール「boss」が設定された Web アプリケーションにはアクセスできません。

4. **アクセス制御（ロール変換後の許可ロール←→ EJB の許可ロール）**
   ロール変換した許可ロールと，EJB に設定された許可ロールを比較します。比較した結果が同じ場合は利用者のアクセス可，異なる場合は利用者のアクセス不可です。
   この例では，利用者は許可ロール「reader」が設定された EJB にアクセスできます。許可ロール「writer」が設定された EJB にはアクセスできません。

1.3 構築・運用に当たってのセキュリティポリシー

システムを外部の脅威から確実に保護するためには，セキュリティポリシーに従ってシステムを構築・運用し，Application Server のセキュリティ機能を正しく使用することが前提です。

セキュリティポリシーとして必要な項目を次の表に示します。

表 1-1 セキュリティポリシーとして必要な項目

項番	項目	詳細の参照先	セキュリティポリシーに従って実施する作業
1	信頼でき，かつ必要な知識を持つ管理者によるシステム構築・運用	1.3.1	―
2	サーバエリア内でのハードウェアの管理	1.3.2	「3.1 ハードウェアの設置」
3	適切なソフトウェアの管理	1.3.3	―
4	内部ネットワークと外部ネットワーク間の通信路の保護	1.3.4	「3.1 ハードウェアの設置」 「3.3 SSL 通信で使用する証明書および秘密鍵の検討」
5	使用する J2EE アプリケーションのセキュリティの確認，設定	1.3.5	「3.4 J2EE アプリケーションの入手」 「3.5 セキュリティ機能の設定に関する検討」
6	ユーザ認証情報の設定，管理	1.3.6	「3.2 OS の設定」 「3.5 セキュリティ機能の設定に関する検討」 「5.1 運用ルールの決定」 「5.2 利用者への通知」
7	パスワードの設定，管理	1.3.7	「3.2 OS の設定」 「3.5 セキュリティ機能の設定に関する検討」 「5.1 運用ルールの決定」 「5.2 利用者への通知」

（凡例）―：構築・運用時は，常に念頭に置いて作業してください。

1.3.1 管理者の選定

管理者は，構築・運用時に発生するすべての作業に責任を持つ人物です。したがって，管理者には，悪意を持ってシステムを操作しない，信頼できる人物を選定します。

選定された管理者は，システムの構築・運用を開始する前に次のことをしてください。

- アプリケーションサーバを搭載するマシン，ファイアウォール，およびネットワーク機器のマニュアルを読み，システムで使用するハードウェアの運用・管理について熟

知する。
- このマニュアルを通読し，Application Server のセキュリティ機能について熟知する。

また，システムの構築・運用時は，このマニュアルに従って作業を進めてください。

1.3.2 ハードウェアの管理

構築・運用するシステムに必要なハードウェアは，**サーバエリア**で管理します。サーバエリアとは，企業のマシン室に該当する物理的な領域のことです。サーバエリアは，次の規定に従って管理してください。

- 厳密に入退室の管理をして，管理者以外の人間がサーバエリアに侵入しないように制限する。
- サーバエリア内のネットワークと外部ネットワーク（社内 LAN を含む）との境界に，ファイアウォールを設置する。
- システムに必要なハードウェア以外の機器を持ち込まない。
  システムに必要なハードウェア構成については，「2.1　ハードウェア構成」を参照してください。

1.3.3 ソフトウェアの管理

構築・運用するシステムに必要なソフトウェアは，次の規定に従って管理してください。

- システムに必要なソフトウェアを，このマニュアルに記載されているとおりにインストール，および設定する。
  OS の設定のうち，このマニュアルで記載を省略している個所については，OS のマニュアルに従って設定してください。
- システムに必要でないソフトウェアを，サーバエリア内のハードウェアにインストールしない。また，決められた構成以外のソフトウェア構成にしない。
  システムに必要なソフトウェア，およびインストール先のハードウェアとの対応については，「2.2　ソフトウェア構成」を参照してください。

1.3.4 ネットワークの管理

サーバエリア内のネットワークと外部ネットワーク間の通信路は，外部の脅威から保護される必要があります。ネットワークの管理について注意事項を次に示します。

通信プロトコル

HTTP および HTTPS だけに制限します。ファイアウォールおよび Web サーバで設定してください。

SSL 通信

Web サーバで SSL 通信（サーバ認証）をするよう設定します。SSL 通信の設定については，マニュアル「Hitachi Web Server」の「6.　SSL による認証，暗号化」を参照してください。

SSL 通信に使用するサーバ証明書と秘密鍵は，次の規定に従って設定してください。
- 秘密鍵生成時の乱数生成用ファイルの内容は，予測されにくいものを使用する。
- 秘密鍵を暗号化する。
- 秘密鍵の鍵長を十分に長くする。
- CSR の署名アルゴリズムに sha1WithRSAEncryption を使用する。
- 生成したサーバ証明書および秘密鍵は，公開ディレクトリ以外に格納する。

EJB コンテナの通信ポートと IP アドレスの固定

J2EE サーバで EJB コンテナの通信ポートと IP アドレスを固定するよう設定します。EJB コンテナの通信ポートと IP アドレスの固定については，マニュアル「Cosminexus 機能解説」の「4.13.2　EJB コンテナの通信ポートと IP アドレスの固定（TPBroker のオプション）」を参照してください。

1.3.5　J2EE アプリケーションの管理

J2EE アプリケーションは，開発者から入手するプログラムです。したがって，信頼できる開発者に発注し，適切な方法で入手してください。

ここでは，J2EE アプリケーションのセキュリティの管理について説明します。

入手時のセキュリティ確認

入手した J2EE アプリケーションが，次に示す条件を満たしていることを確認してください。
- Enterprise Bean の種類は，Session Bean である。
- データベースに接続しない。

構築時のセキュリティ設定

通常，Application Server のセキュリティ機能を使用できるように設定するのは開発者です。セキュリティ機能を使用するための設定がない J2EE アプリケーションを入手した場合は，システム構築時に管理者が設定する必要があります。
J2EE アプリケーションに設定するセキュリティ機能の条件を次に示します。
- ユーザ認証をするよう設定されている。
- J2EE アプリケーションを構成する全 URL パターン，および EJB の全メソッドにセキュリティロールが設定されている。

セキュリティロールの構成管理

セキュリティロールによるアクセス制御を正しく機能させるには，セキュリティロールの構成を適切に管理する必要があります。管理者は，J2EE アプリケーションに設定された許可ロールの構成を基に，セキュリティロールの構成を検討します。また，J2EE アプリケーションの入れ替えや利用者の増減などの理由で構成を見直す場合，変更後の構成を正しく把握しておく必要があります。

1.3.6 ユーザ認証情報の管理

アプリケーションサーバにアクセスできる人物は，管理者と利用者だけです。ほかの人物による侵入を防ぐために，管理者は自分自身のユーザ認証情報と，全利用者のユーザ認証情報を管理する必要があります。

ここでは，管理者と利用者のユーザ認証情報について，それぞれ説明します。

管理者のユーザ認証情報

OS のアカウントを利用します。

Windows の場合は Administrator 権限を持つユーザ，UNIX の場合は root 権限を持つユーザが，管理者のアカウントとなります。管理者のアカウント以外の，不要なアカウントは削除してください。

また，アカウントのパスワードは，「1.3.7　パスワードの管理」に従って，強度があるものを設定してください。

利用者のユーザ認証情報

Application Server のセキュリティ機能で設定するユーザ認証情報を利用します。

利用者のユーザ認証情報は，ユーザ ID，パスワードおよび所属ロールで構成されます。

利用者のユーザ認証情報を設定するときは，次のことを守ってください。

- 利用者間でユーザ ID が重複しないように設定する。
- アカウントのパスワードは，「1.3.7　パスワードの管理」に従って，強度があるものを設定する。
- ユーザ ID と所属ロールの対応づけを適切に管理する。一人の利用者が持つ所属ロールを増やし過ぎないよう注意する。
- 運用中，不要になったユーザ認証情報は直ちに削除する。
- 設定した全ユーザ認証情報のリストは，第三者に漏えいしないよう，適切に管理する。
- 利用者本人のユーザ ID およびパスワードを，確実かつ安全な手段で利用者に通知する。ネットワーク経由ではなく，郵送などの手段を検討する。
- 利用者に，ユーザ ID およびパスワードの管理を徹底させる。紙に書いたりデータ化したりしないよう，注意を促す。

1.3.7 パスワードの管理

管理者は，自分自身のパスワードと全利用者のパスワードを管理します。ここでは，パスワードの管理方法について説明します。

強度があるパスワードの設定

パスワードは，次の規定に従って強度があるものを設定してください。

- 誕生日や名前など，第三者が推測しやすいパスワードを避ける。
- 管理者のパスワードは，OS の規定に従って設定する。
- 利用者のパスワードは，次の表に従って設定する。

表 1-2 利用者のパスワードの規定

項番	規定がある項目	規定内容
1	パスワードの長さ	8 ～ 64 文字
2	使用できる文字種	• 数字（0 ～ 9） • 英大文字（A ～ Z） • 英小文字（a ～ z） • 記号（半角） 「!」「$」「@」「~」「?」「`」「(」「)」「{」「}」

設定したパスワードの扱い

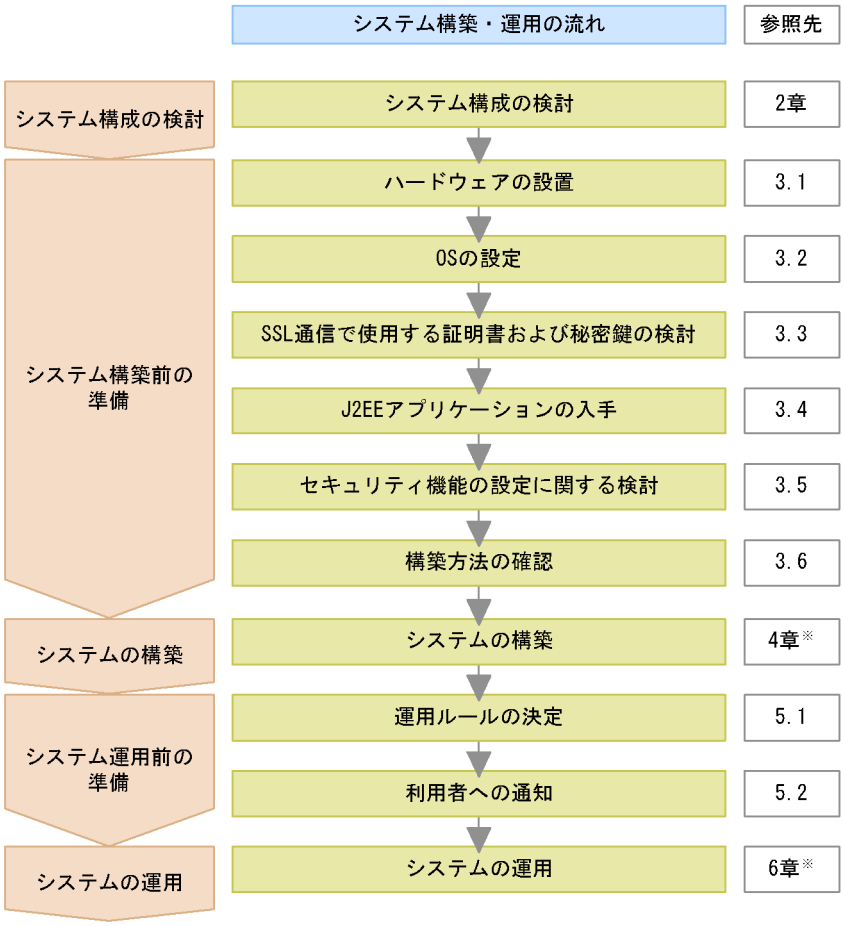
設定したパスワードは，第三者に漏えいしないように扱ってください。パスワードの扱い方についての注意事項を次に示します。

- 管理者のパスワードは，管理者自身が正しく記憶する。紙に書いたりデータ化したりしない。
- 利用者のパスワードは，確実かつ安全な手段で利用者に通知する。ネットワーク経由ではなく，郵送などの手段を検討する。
- 設定したパスワードは，定期的に変更する。
- 利用者にパスワードの管理を徹底させる。紙に書いたりデータ化したりしないよう，注意を促す。

1.4　構築・運用の流れ

システム構成の検討から，構築したシステムの運用までの流れを次の図に示します。

図 1-3　システム構築・運用の流れ



注※　構築の流れの詳細は4.1，運用の流れの詳細は6.1を参照してください。

2 システム構成の検討

システムを構築する前に，まず，システム構成を検討します。この章では，セキュアなアプリケーションサーバを実現するシステム構成について，ハードウェア，ソフトウェアに分けて説明します。

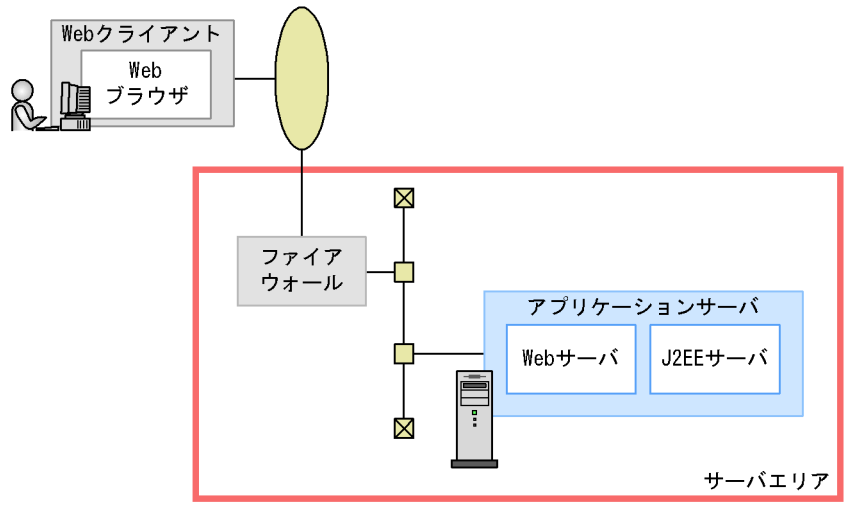
2.1 ハードウェア構成

このマニュアルで説明するシステムは，次のようなハードウェア構成です。

- Web クライアント構成である。
- J2EE サーバと Web サーバが 1 台のマシンに搭載され，アプリケーションサーバを構成している。
- アプリケーションサーバはサーバエリアに設置されている。
- 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ている。

ハードウェア構成を次の図に示します。

図 2-1 ハードウェア構成



図中に示した「サーバエリア」が，このマニュアルで説明するシステムの範囲です。サーバエリアには，ファイアウォールとアプリケーションサーバのマシンを 1 台ずつ用意します。

アプリケーションサーバに使用できるマシンの機種は，前提 OS によって異なります。前提 OS と使用できるマシンの機種の対応を次の表に示します。

表 2-1　前提 OS と使用できるマシンの機種の対応

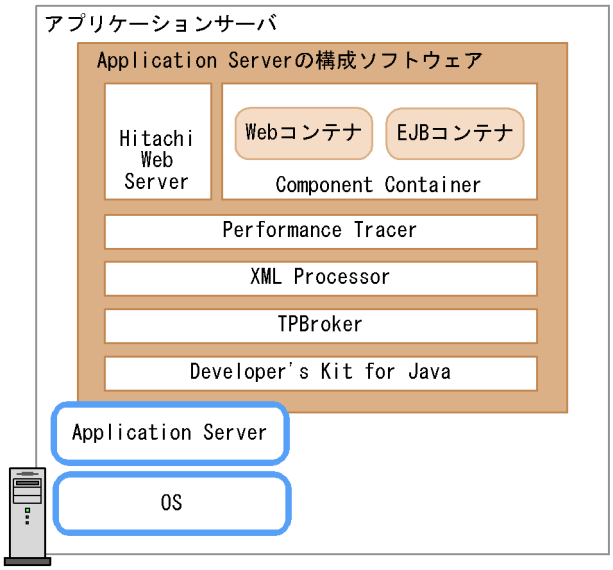
項番	前提 OS	使用できるマシンの機種
1	Windows	• BladeSymphony • FLORA 700 シリーズ • HA8000 シリーズ • 他社 PC/AT 互換機
2	AIX	• EP8000 シリーズ（POWER4+ 以前） • EP8000 シリーズ（POWER5） • IBM System p5 • IBM pSeries • IBM RS/6000 サーバ • IBM RS/6000 ワークステーション
3	HP-UX	• BladeSymphony • HA8500 シリーズ • HP Integrity サーバ • HP Integrity サーバ互換機
4	Linux	• BladeSymphony • HA8000 シリーズ • 他社 PC/AT 互換機
5	Solaris	• Sun SPARCstation シリーズ • Sun Blade シリーズ • Sun Fire シリーズ • Sun Fire 互換機 • Sun Netra • Sun Netra 互換機 • Sun Ultra シリーズ • Sun Ultra Enterprise シリーズ • Sun Ultra Enterprise 互換機 • Sun Ultra 互換機 • 富士通 PRIMEPOWER シリーズ

注　前提 OS の詳細については，「2.2　ソフトウェア構成」を参照してください。また，前提 OS と使用できるマシンの機種の対応を詳細に知りたい場合は，マシンのマニュアルをお読みください。

2.2　ソフトウェア構成

構築するアプリケーションサーバのソフトウェア構成を次の図に示します。

図 2-2　ソフトウェア構成



（凡例）

：インストールするソフトウェア

注　図中では，構成ソフトウェア名の「Cosminexus」は省略しています。

アプリケーションサーバのマシンには，Application Server と前提 OS をインストールします。また，Application Server では，図中に示す構成ソフトウェアが動作します。

ここでは，インストールするソフトウェアについて説明します。Application Server の各構成ソフトウェアの機能概要については，マニュアル「Cosminexus 概説」の「2.3.2　構成ソフトウェアの機能概要」を参照してください。

Application Server

アプリケーションサーバの機能を提供するソフトウェアです。次のどちらかが必要です。どちらを使用しても Application Server のセキュリティ機能（ユーザ認証，アクセス制御）に差異はありません。

- uCosminexus Application Server Standard　07-00
- uCosminexus Application Server Enterprise　07-00

OS

Application Server の前提 OS です。前提 OS を次の表に示します。

表 2-2 Application Server の前提 OS

項番	前提 OS	前提 OS のバージョン
1	Windows	• Windows 2000 Server（SP3 または SP4 を適用） • Windows Server 2003（SP1 を適用） • Windows Server 2003 R2（SP1 を適用） • Windows Server 2003（x64）（SP1 を適用） • Windows Server 2003 R2（x64）（SP1 を適用）
2	AIX	• AIX 5L V5.1 • AIX 5L V5.2 • AIX 5L V5.3
3	HP-UX	• HP-UX 11i V2（IPF）
4	Linux	• Red Hat Enterprise Linux AS 3（x86） • Red Hat Enterprise Linux AS 4（x86） • Red Hat Enterprise Linux ES 3（x86） • Red Hat Enterprise Linux ES 4（x86） • Red Hat Enterprise Linux AS 3（AMD64 & Intel EM64T） • Red Hat Enterprise Linux AS 4（AMD64 & Intel EM64T）
5	Solaris	• Solaris 8 • Solaris 9 • Solaris 10

3 システム構築前の準備

この章では，システムを構築する前に必要な準備作業について説明します。

3.1 ハードウェアの設置

「1.3.2 ハードウェアの管理」と「2.1 ハードウェア構成」に従って，システムのハードウェアを設置します。ハードウェアは，サーバエリア内に設置してください。

ファイアウォールの構築

外部ネットワークからアプリケーションサーバへの不正なアクセスを禁止するために，使用するポートは HTTP（通常は 80），および HTTPS（通常は 443）だけを許可してください。

構築方法の詳細は，ファイアウォールのマニュアルをお読みください。

3.2 OS の設定

「1.3.3 ソフトウェアの管理」と「2.2 ソフトウェア構成」に従って，アプリケーションサーバのマシンに前提 OS をインストールし，必要な設定をします。

ここでは，OS のインストールが完了したあとの設定について説明します。

管理者のユーザ認証情報の設定

「1.3.6 ユーザ認証情報の管理」に従って，管理者のアカウントを設定します。アカウントのパスワードは，「1.3.7 パスワードの管理」に従って，強度があるものにしてください。

Web サーバとの連携の設定（UNIX の場合）

UNIX の場合，Hitachi Web Server を動作させるためのアカウントを追加します。ユーザとグループを，新規に登録してください。

セキュリティパッチの適用

システムに必要な最新のセキュリティパッチを適用し，OS の状態を常に適切に保ちます。

パッケージのインストール（Linux の場合）

Linux の場合，ncompress パッケージがインストールされている必要があります。ncompress パッケージがインストールされているかを確認してください。

ネットワークの設定

IP アドレス，およびホスト名の設定をして，ネットワークと接続できるようにします。

3.3 SSL 通信で使用する証明書および秘密鍵の検討

「1.3.4 ネットワークの管理」に従って，SSL 通信で使用するサーバ証明書の記述内容，および秘密鍵の設定内容を検討します。サーバ証明書の記述内容および秘密鍵の設定内容については，マニュアル「Hitachi Web Server」の「6.2 証明書取得手順」を参照してください。

ここで検討した情報は，システム構築時にファイルやコマンドで設定します。

3.4 J2EE アプリケーションの入手

J2EE サーバにインポートする J2EE アプリケーションを，開発者から入手します。
J2EE アプリケーションを入手したら，次のことを確認してください。

- 発注時の仕様書と同じ内容かどうか。
- セキュリティポリシーに従っているか。
  「1.3.5　J2EE アプリケーションの管理」に従って確認してください。
- ユーザ認証方式は何か。
  HTTP（Form 認証）の場合，カスタマイズされた認証インタフェースの URL を調査しておきます。カスタマイズされた認証インタフェースがない場合，システム構築時にユーザ認証方式として HTTP（Basic 認証）を設定します。
- 各 J2EE コンポーネントに許可ロールが設定されているかどうか。
  設定されている場合，各コンポーネントに設定された許可ロールの構成を調査します。設定されていない場合，「3.5　セキュリティ機能の設定に関する検討」で許可ロールの構成検討が必要です。

3.5 セキュリティ機能の設定に関する検討

Application Server のセキュリティ機能を使用するために必要な設定について検討します。ここで検討した内容は，システム構築時にファイルやコマンドで設定します。なお，システム運用時の設定変更に備えて，あらかじめセキュリティ機能の設定について運用ルールを決めておくことをお勧めします。運用ルールの決定については，「5.1　運用ルールの決定」を参照してください。

ここでは，セキュリティ機能を使用するに当たっての検討項目について説明します。

セキュリティロールの構成

「1.3.5　J2EE アプリケーションの管理」に従って，次の項目を検討してください。

- J2EE アプリケーションの許可ロール
  Web アプリケーションの全 URL パターン，および EJB の全メソッドに許可ロールを割り当てます。開発者が許可ロールを割り当てていない場合，または既定の許可ロールの割り当てを編集したい場合に検討が必要です。
- システムで使用する所属ロール
  システムで使用する所属ロールの総数，および所属ロールの名称を，社内の職制などに応じて決定します。
- 所属ロールから許可ロールへのロール変換
  各所属ロールを，どの許可ロールと対応させるかを決定します。

利用者のユーザ認証情報

ユーザ認証情報を，各利用者に割り当てます。次の情報を割り当ててください。

- ユーザ ID
- パスワード
  「1.3.7　パスワードの管理」に従って，強度があるものにしてください。
- 所属ロール
  セキュリティロールの構成に基づき，利用者の役割に応じて所属ロールを割り当てます。

3.6　構築方法の確認

システム構築は，ファイル編集とコマンド実行で行います。アプリケーションサーバのマシンで，J2EE サーバや Web サーバのファイルを編集したりコマンドを実行したりして，システムを構築します。

J2EE サーバが提供するファイルについては，マニュアル「Cosminexus リファレンス 定義編」を，コマンドについては，マニュアル「Cosminexus リファレンス コマンド編」を参照してください。Web サーバが提供するファイルおよびコマンドについては，マニュアル「Hitachi Web Server」を参照してください。

また，このマニュアルで説明する構築作業に必要なファイルとコマンドの概要，および関連マニュアルとの対応については，「7.　リファレンス」を参照してください。

4 システムの構築

構築前に必要な準備作業が完了したら，システムの構築作業を実施します。
この章では，システムを構築する方法について，例に基づいて説明します。

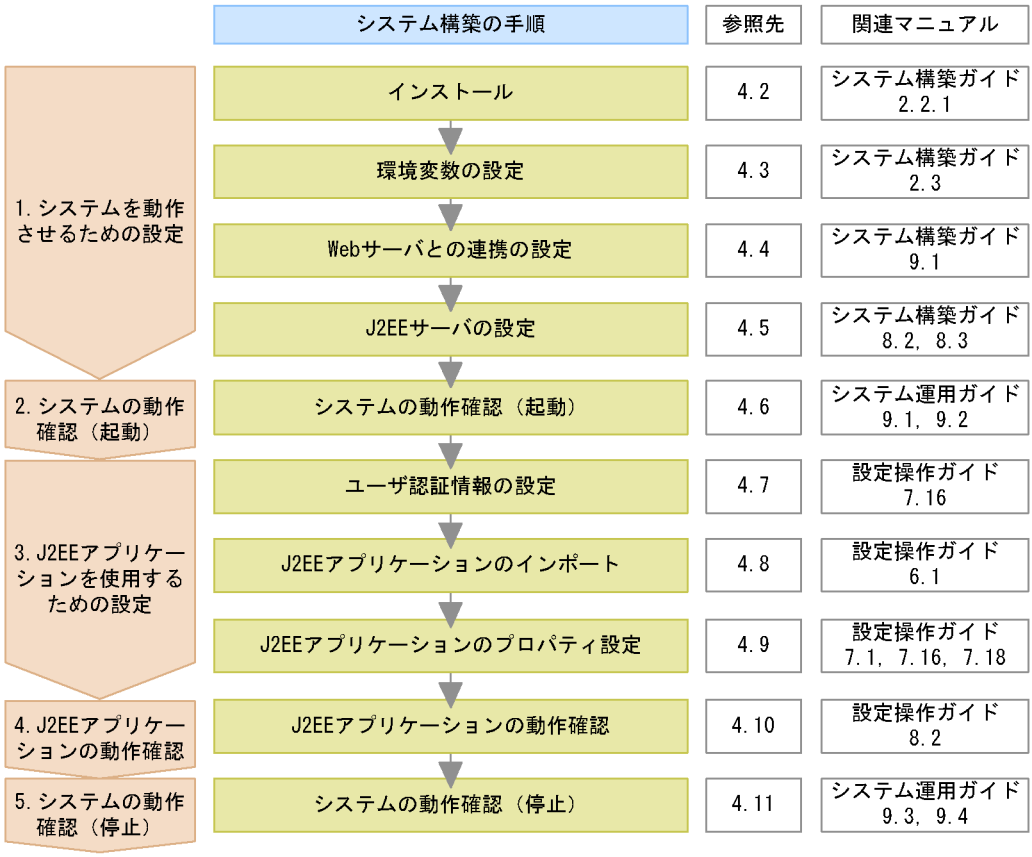
4.1　システム構築の概要

ここでは，Application Server のセキュリティ機能を使用したシステム構築の概要を説明します。Application Server のセキュリティ機能に関係ない，システムを動作させるための構築作業の概要については，マニュアル「Cosminexus システム構築ガイド」の「2.1　インストールと初期設定の概要」および「8.1　システム構築の概要」を参照してください。

4.1.1　システム構築の流れ

システム構築の流れを次の図に示します。

図 4-1　システム構築の流れ



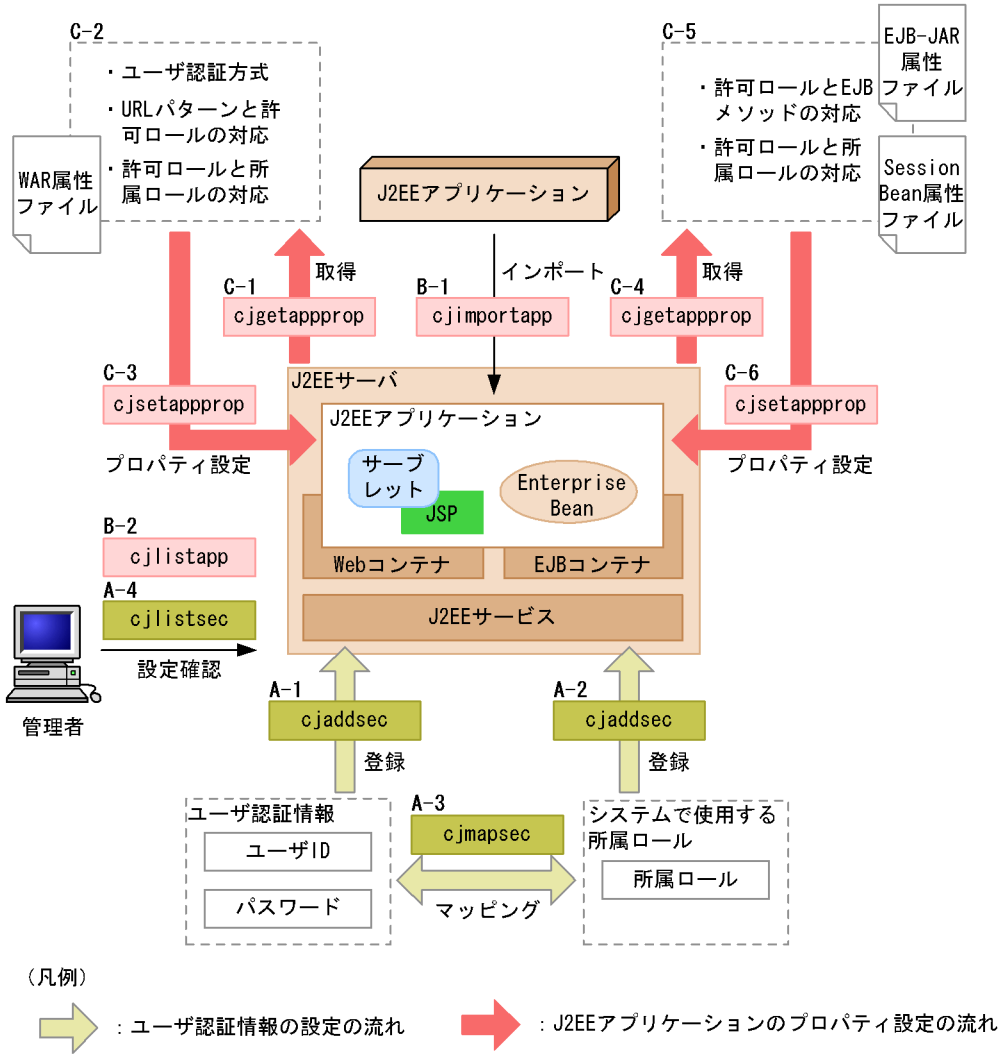
注　各手順の具体的な説明については「参照先」を，各手順の概要については「関連マニュアル」を参照してください。なお，関連マニュアルの名称は，次のとおりに省略しています。
・Cosminexus システム構築ガイド→「システム構築ガイド」
・Cosminexus システム運用ガイド→「システム運用ガイド」
・Cosminexus アプリケーション設定操作ガイド→「設定操作ガイド」

1. **システムを動作させるための設定**
   アプリケーションサーバをシステムで稼働させるための設定をします。
2. **システムの動作確認（起動）**
   流れ 1. での設定が正しいかを確認するために，アプリケーションサーバを起動します。
3. J2EE **アプリケーションを使用するための設定**
   Application Server のセキュリティ機能によって J2EE アプリケーションをセキュアに動作させるための設定をします。J2EE アプリケーションを使用するための設定は，サーバ管理コマンド，および属性ファイルを使用します。使用するコマンド，ファイルとセキュリティ設定の関係については，「4.1.2　コマンド，ファイルとセキュリティ設定の関係」を参照してください。
4. J2EE **アプリケーションの動作確認**
   流れ 3. での設定が正しいかを確認するために，J2EE アプリケーションを開始したあと，アプリケーションサーバのマシンから J2EE アプリケーションにアクセスします。
5. **システムの動作確認（停止）**
   正しく停止できるかを確認するために，アプリケーションサーバを停止します。

4.1.2　コマンド，ファイルとセキュリティ設定の関係

Application Server のセキュリティ機能は，サーバ管理コマンド，および属性ファイルを使用して設定します。Application Server のセキュリティ機能の設定で使用するコマンド，ファイルとセキュリティ設定との関係を，次の図に示します。

図 4-2 コマンド，ファイルとセキュリティ設定の関係



図中の記号（A-1 ～ C-6）について説明します。

図中の記号	操作の流れ	操作の詳細	使用するコマンド，ファイル
A-1	ユーザ認証情報の設定	利用者のユーザ ID，およびパスワードを J2EE サーバに登録します。	cjaddsec コマンド
A-2		システムで使用する所属ロールを J2EE サーバに登録します。	
A-3		ユーザ ID と所属ロールをマッピングすることで，利用者に所属ロールを割り当てます。	cjmapsec コマンド
A-4		ユーザ認証情報の設定を確認します。	cjlistsec コマンド

図中の記号	操作の流れ	操作の詳細	使用するコマンド，ファイル
B-1	J2EE アプリケーションのインポート	使用する J2EE アプリケーションをインポートします。	cjimportapp コマンド
B-2		インポートした J2EE アプリケーションの状態を確認します。	cjlistapp コマンド
C-1	J2EE アプリケーションのプロパティ設定※	Web アプリケーションの属性を設定する WAR 属性ファイルを取得します。	cjgetappprop コマンド
C-2		WAR 属性ファイルに次の情報を記述します。 • ユーザ認証方式 • URL パターンと Web アプリケーションの許可ロールの対応 • Web アプリケーションの許可ロールと，利用者の所属ロールの対応	WAR 属性ファイル
C-3		WAR 属性ファイルに記述した情報を，J2EE サーバに設定します。	cjsetappprop コマンド
C-4		EJB の属性を設定する EJB-JAR 属性ファイル，および Session Bean 属性ファイルを取得します。	cjgetappprop コマンド
C-5		EJB-JAR 属性ファイル，および Session Bean 属性ファイルに，次の情報を記述します。 • EJB の許可ロールとメソッドの対応 • EJB の許可ロールと，利用者の所属ロールの対応	• EJB-JAR 属性ファイル • Session Bean 属性ファイル
C-6		EJB-JAR 属性ファイル，および Session Bean 属性ファイルに記述した情報を，J2EE サーバに設定します。	cjsetappprop コマンド

注　この表で説明している操作は，Cosminexus のシステムを動作させる設定が完了していることが前提です。
注※　この章では三つの属性ファイルを使用した設定方法を説明しますが，アプリケーション統合属性ファイルを使用しても設定できます。アプリケーション統合属性ファイルの詳細については，マニュアル「Cosminexus リファレンス 定義編」の「8.2　アプリケーション統合属性ファイル」を参照してください。

4.1.3　この説明で使用するシステム構成の例

この章では，ここで示す例に基づいて構築方法の説明をします。

注意事項

ここに示すのは一つの例であり，実際はお使いのシステムに合わせて構成を決定してください。なお，構成を決定するときは，「1.3　構築・運用に当たってのセキュリティポリシー」で制定したセキュリティポリシーに従ってください。

Windows の場合

Windows の場合の説明で使用するシステム構成例を次の表に示します。なお，インポートする J2EE アプリケーションの例の詳細は，「4.1.4　この説明で使用する J2EE アプリケーションの例」を参照してください。

表 4-1　構築方法の説明で使用するシステム構成例（Windows の場合）

項番	項目	値
1	OS の種類	Windows 2000 Server
2	Application Server の種類	uCosminexus Application Server Standard 07-00
3	インストールディレクトリ	C:¥Program Files¥Hitachi¥Cosminexus ※1
4	インストール時に登録するユーザ名と会社名	• ユーザ名：日立　太郎 • 会社名：（株）日立製作所
5	ホスト名	MyServer
6	J2EE サーバ名	MyServer
7	Web サーバ名	MyServer
8	Web サーバのポート番号	• HTTP：80 ※1 • HTTPS：443
9	SSL 通信に使用する秘密鍵ファイル名	C:¥Program Files¥Hitachi¥Cosminexus¥httpsd¥conf¥httpsdkey.pem
10	SSL 通信に使用する証明書ファイル名	C:¥Program Files¥Hitachi¥Cosminexus¥httpsd¥conf¥httpsd.pem
11	EJB コンテナのポート番号と IP アドレス	• ポート番号：30000 • IP アドレス：192.1.1.xxx ※2
12	インポートする J2EE アプリケーション名	sample
13	構築時に使用するブラウザ	Internet Explorer
14	Management Server の使用有無	使用しない

注※ 1　デフォルトを使用します。
注※ 2　「xxx」の部分は数字です。実際の IP アドレスは，システム構成に合わせて設定してください。

UNIX の場合

UNIX の場合の説明で使用するシステム構成例を次の表に示します。なお，インポートする J2EE アプリケーションの例の詳細は，「4.1.4　この説明で使用する J2EE アプリケーションの例」を参照してください。

表 4-2　構築方法の説明で使用するシステム構成例（UNIX の場合）

項番	項目	値
1	OS の種類	Red Hat Enterprise Linux AS 3（x86）
2	Application Server の種類	uCosminexus Application Server Standard 07-00
3	インストールディレクトリ	/opt/Cosminexus ※1
4	ホスト名	MyServer
5	J2EE サーバ名	MyServer
6	Web サーバ名	MyServer
7	Web サーバのポート番号	• HTTP：80 ※2 • HTTPS：443
8	Web サーバのユーザ名，グループ名	• ユーザ名：wwwuser • グループ名：wwwgroup
9	Web サーバのコアダンプの出力先	/opt/hitachi/httpsd/logs
10	SSL 通信に使用する秘密鍵ファイル名	/opt/hitachi/httpsd/conf/httpsdkey.pem
11	SSL 通信に使用する証明書ファイル名	/opt/hitachi/httpsd/conf/httpsd.pem
12	EJB コンテナのポート番号と IP アドレス	• ポート番号：30000 • IP アドレス：192.1.1.xxx ※3
13	インポートする J2EE アプリケーション名	sample
14	Management Server の使用有無	使用しない

注※1　UNIX の場合，インストールディレクトリは固定です。
注※2　デフォルトを使用します。
注※3　「xxx」の部分は数字です。実際の IP アドレスは，システム構成に合わせて設定してください。

4.1.4　この説明で使用する J2EE アプリケーションの例

この章では，ここで示すサンプルアプリケーションをシステムにインポートするものとして，構築方法の説明をします。

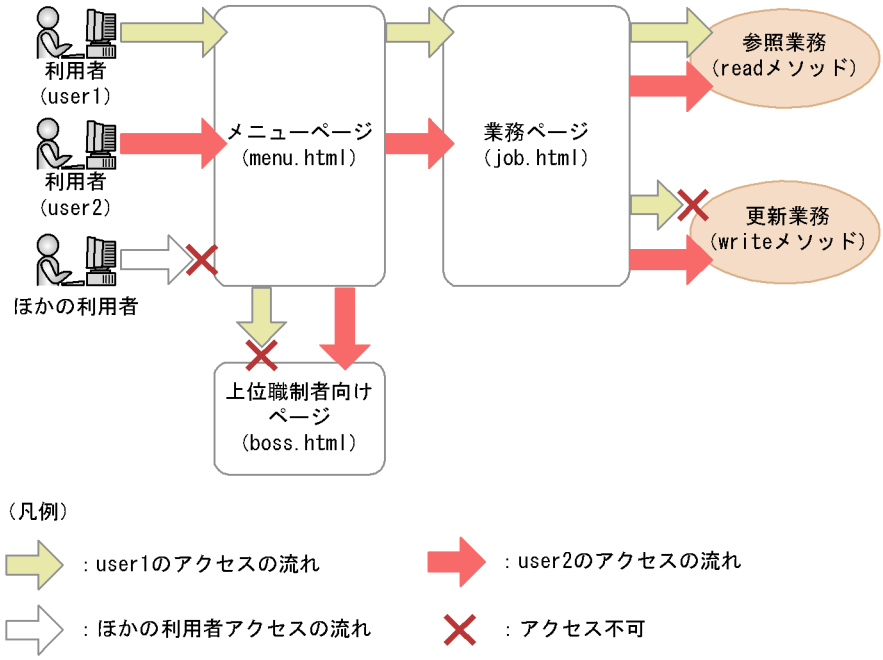
このサンプルアプリケーションには，開発者によるセキュリティ機能の設定が一切されていない，という前提で説明します。したがって，必要なセキュリティ機能の設定は，すべて管理者が行います。セキュリティ機能の設定値は，「3.4　J2EE アプリケーションの入手」および「3.5　セキュリティ機能の設定に関する検討」で決定した値を使用します。

（1）画面遷移とセキュリティ設定の概要

サンプルアプリケーションの画面遷移と，セキュリティ機能の設定の概要を，次の図に

示します。

図 4-3 サンプルアプリケーションの画面遷移とセキュリティ設定の概要



画面遷移

メニューページ（menu.html）から，業務ページ（job.html）および上位職制者向けページ（boss.html）にリンクしています。業務ページでは，参照業務（read メソッド）および更新業務（write メソッド）を実行できます。

ユーザ認証

HTTP（Basic 認証）によって認証します。システムに登録されている利用者は，下位職制の利用者（user1）と上位職制の利用者（user2）の 2 名です。ほかの利用者は，ユーザ認証時に拒否されます。

アクセス制御

各 URL パターン，および各メソッドのアクセス制御の設定は次のとおりです。

- メニューページ（menu.html）および業務ページ（job.html）には，登録されているすべての利用者がアクセスできるよう設定されているため，ユーザ認証に成功した利用者（user1，user2）がアクセスできる。
- 上位職制者向けページ（boss.html）には，上位職制の利用者（user2）だけがアクセスできる。
- 参照業務（read メソッド）には，すべての職制の利用者（user1，user2）がアクセスできる。
- 更新業務（write メソッド）には，上位職制の利用者（user2）だけがアクセスできる。

(2) 基本構成

この説明で使用するサンプルアプリケーションは，アーカイブ形式のアプリケーションです。この説明で使用するサンプルアプリケーションの基本構成を，次の表に示します。

表 4-3 サンプルアプリケーションの基本構成

項番	項目	値
1	J2EE アプリケーション名	sample
2	EAR ファイル名	sample.ear
3	J2EE アプリケーションのリソースの表示名	• WAR：sample_war • EJB-JAR：sample_ejb • Session Bean：Business
4	取得する属性ファイル名	• WAR 属性ファイル：prop_war.xml • EJB-JAR 属性ファイル：prop_ejbjar.xml • Session Bean 属性ファイル：prop_session.xml
5	URL パターン	• boss.html • job.html • menu.html
6	EJB のメソッド名	• read • write
7	ユーザ認証時に使用するレルム名	SAMPLE
8	アクセス制御時に使用する Web リソース名	• 全ページ：ALL • 上位職制者向けページ：BOSS
9	作業用ディレクトリ	• Windows の場合：C:¥sample¥ • UNIX の場合：/sample/

(3) セキュリティロールの構成とユーザ認証情報

ここでは，サンプルアプリケーションのセキュリティロールの構成とユーザ認証情報について説明します。

注意事項

ここに示すのは一つの例であり，実際はお使いのシステムに合わせて構成やユーザ認証情報を決定してください。なお，構成やユーザ認証情報を決定するときは，「1.3 構築・運用に当たってのセキュリティポリシー」で制定したセキュリティポリシーに従ってください。

システムで使用する所属ロール

次の所属ロールを使用します。

- employee
  下位職制者に割り当てる所属ロールです。
- manager
  上位職制者に割り当てる所属ロールです。

サンプルアプリケーションの許可ロール

Web アプリケーションおよび EJB は，次の許可ロールで構成されます。

- Web アプリケーションの許可ロール
  全利用者向けの「member」と，上位職制者向けの「boss」の 2 種類です。
- EJB の許可ロール
  参照業務ができる「reader」と，更新業務ができる「writer」の 2 種類です。

Web アプリケーションのセキュリティロールの構成

各 URL パターンに，アクセスを許可する Web アプリケーションの許可ロールを割り当てます。また，Web アプリケーションの各許可ロールと，アクセスを許可する所属ロールとを対応づけます。Web アプリケーションのセキュリティロールの構成を，次の表に示します。

表 4-4　Web アプリケーションのセキュリティロールの構成例

項番	URL パターン	Web アプリケーションの許可ロール	システムで使用する所属ロール
1	/*（全ページ※）	member	employee
		boss	manager
2	/boss/*（上位職制者向けページ）		

注※　ほかにアクセス制御の設定がないすべてのページを指します。この例では，メニューページ（menu.html），および業務ページ（job.html）を含みます。

EJB のセキュリティロールの構成

EJB の各許可ロールに，アクセスを許可するメソッドを割り当てます。また，EJB の各許可ロールと，アクセスを許可する所属ロールとを対応づけます。EJB のセキュリティロールの構成を，次の表に示します。

表 4-5　EJB のセキュリティロールの構成例

項番	EJB の許可ロール	メソッド	システムで使用する所属ロール
1	reader	read（参照メソッド）	employee
2	writer		manager
		write（更新メソッド）	

ユーザ認証情報

各利用者のユーザ ID，パスワード，および所属ロールを，次の表に示します。

表 4-6　利用者のユーザ認証情報の例

項番	ユーザ ID	パスワード※	所属ロール
1	user1	password1	employee
2	user2	password2	manager

注※　実際のパスワードは，「1.3.7　パスワードの管理」に従って，強度があるものに設定してください。

4.2 インストール

ここでは，Application Server のインストール方法について説明します。

管理者は，Application Server をインストールする前に次のことを確認してください。

- 「3.1 ハードウェアの設置」に従って，ハードウェアが適切に設置されているか。
- 「3.2 OS の設定」に従って，前提 OS のインストール，および設定が完了しているか。
- 動作中のソフトウェアがないか。
- インストール先にファイル，またはディレクトリがないか。
- ディスクの空き容量が十分にあるか。
- インストールに必要なファイル，またはディレクトリに，必要なアクセス権限が設定されているか。
- インストール実行時の言語種別と実行するマシンの言語が一致しているか。

なお，インストール時の注意事項については，マニュアル「Cosminexus システム構築ガイド」の「2.2.1 インストール方法」を参照してください。

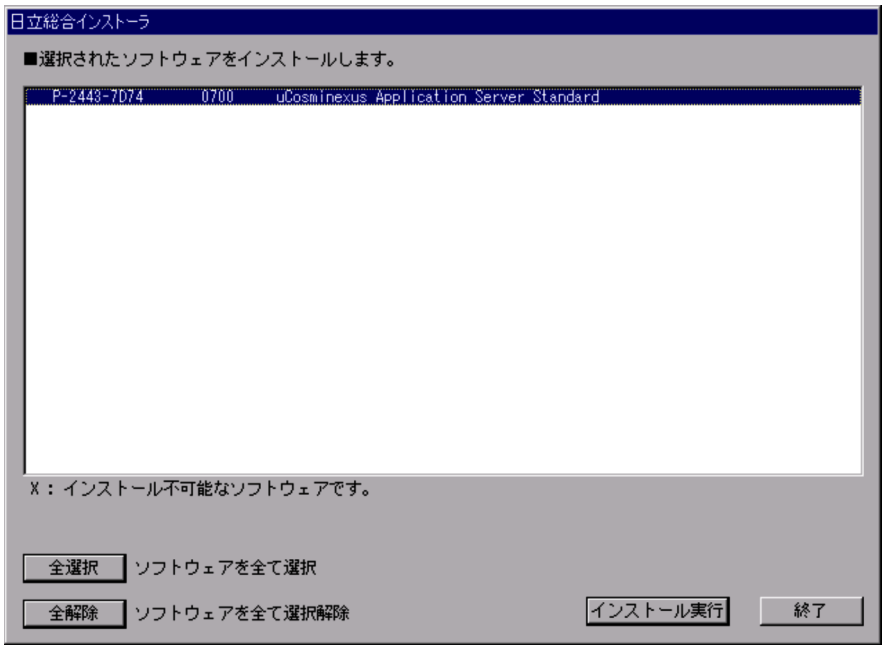
4.2.1 Windows の場合

ここでは，Windows の場合の操作手順，インストール後の確認手順，およびディレクトリ構成について説明します。

(1) 操作手順

Application Server のインストール手順を次に示します。

1. **インストールに使用する** CD-ROM **に，インストールするソフトウェアが格納されていることを確認します。**
   この例では，次のソフトウェアが格納されていることを確認します。
   - P-2443-7D74　07-00　uCosminexus Application Server Standard
2. Application Server **をインストールするマシンに** Administrator **権限でログインします。**
3. **手順** 1. **の** CD-ROM **を，**CD-ROM **ドライブに入れます。**
   インストーラが自動起動されます。
4. **手順** 1. **で確認したソフトウェアを選択し，［インストール実行］ボタンをクリックします。**
   この例では，次のソフトウェアを選択します。
   - P-2443-7D74　07-00　uCosminexus Application Server Standard



5. **［インストール処理開始の確認］画面で［OK］ボタンをクリックします。**

6. **［ようこそ］画面で，手順 4. で選択したソフトウェア名が表示されていることを確認し，［次へ］ボタンをクリックします。**
   この例では，「uCosminexus Application Server Standard セットアッププログラムへようこそ」と表示されていることを確認します。

7. **［インストール先の選択］画面でインストール先を選択し，［次へ］ボタンをクリックします。**
   この例では，デフォルトの設定のまま，次のディレクトリをインストール先とします。
   `C:¥Program Files¥Hitachi¥Cosminexus`

8. **［コンポーネントの選択］画面で［カスタム］ボタンをクリックします。**

9. **［プログラムの選択］画面で必要なプログラムを選択し，［OK］ボタンをクリックします。**
   次に示すプログラムだけを選択してください。ほかのプログラムは，選択を解除してください。
   - P-2441-E374 - Hitachi Web Server - 0300
   - P-2443-8174 - Cosminexus Component Container - 0700
   - P-245Z-D174 - Cosminexus XML Processor - 0700
   - P-2464-AF64 - Cosminexus TPBroker - 0517
   - P-2464-EB14 - Cosminexus Performance Tracer - 0700

10. **[ユーザ情報] 画面でユーザ名および会社名を入力し，[次へ] ボタンをクリックします。**
    この例では，次のとおりに入力します。
    - ユーザ名：日立　太郎
    - 会社名：（株）日立製作所
11. **[プログラムフォルダの選択] 画面でプログラムフォルダを選択し，[次へ] ボタンをクリックします。**
    この例では，デフォルトの設定のままとします。
12. **[インストールの開始] 画面でこれまでの設定内容を確認し，[次へ] ボタンをクリックします。**
    インストールが実行されます。
13. **[セットアップの完了] 画面で [完了] ボタンをクリックします。**
14. **OS を再起動するかどうかを確認するダイアログで，[はい] ボタンをクリックします。**
    OS が再起動されます。これでインストール作業は完了です。

(2) 確認手順

Application Server が正しくインストールされているか，確認する手順を次に示します。

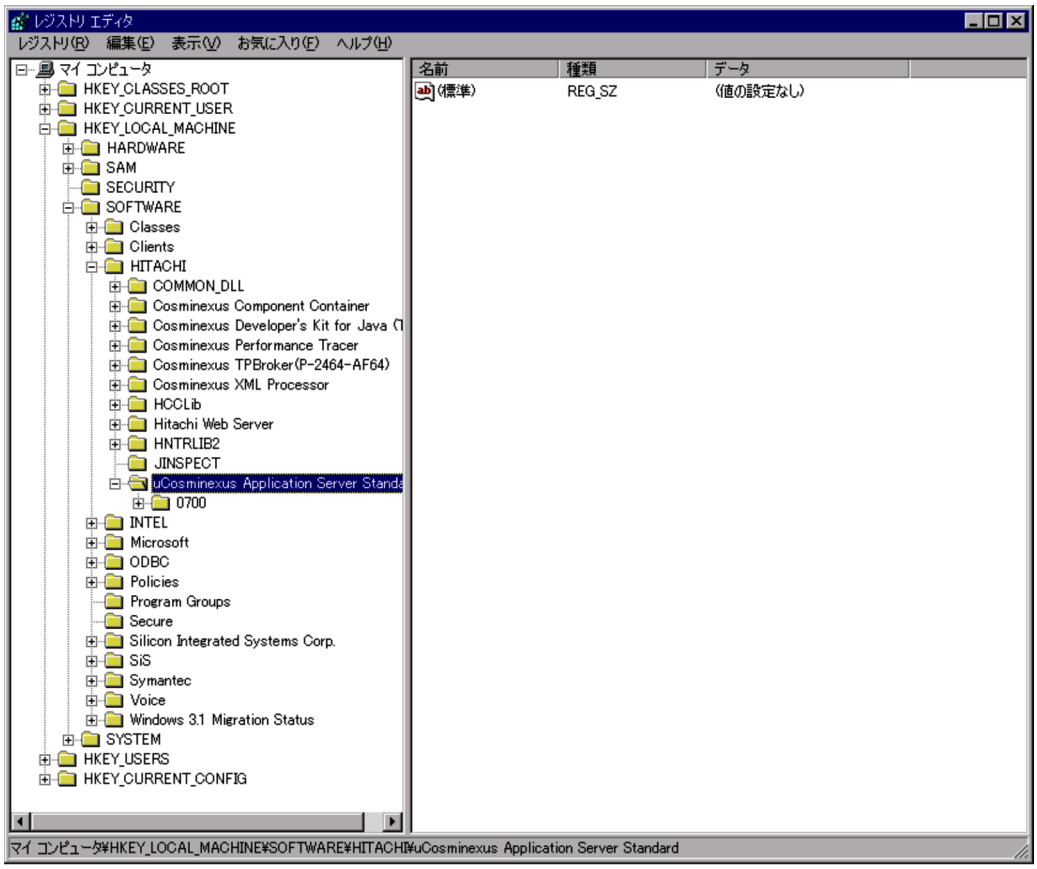
1. **OS の regedit コマンドでレジストリエディタを起動します。**
   regedit コマンドの実行例を次に示します。

```
C:¥>regedit
```

2. **レジストリエディタの画面で，**[HKEY_LOCAL_MACHINE¥SOFTWARE]**キーに** Application Server**（バージョン番号：**0700**）が存在することを確認します。**

この例では，次のキーが存在することと，下位に［0700］キーが存在することを確認します。

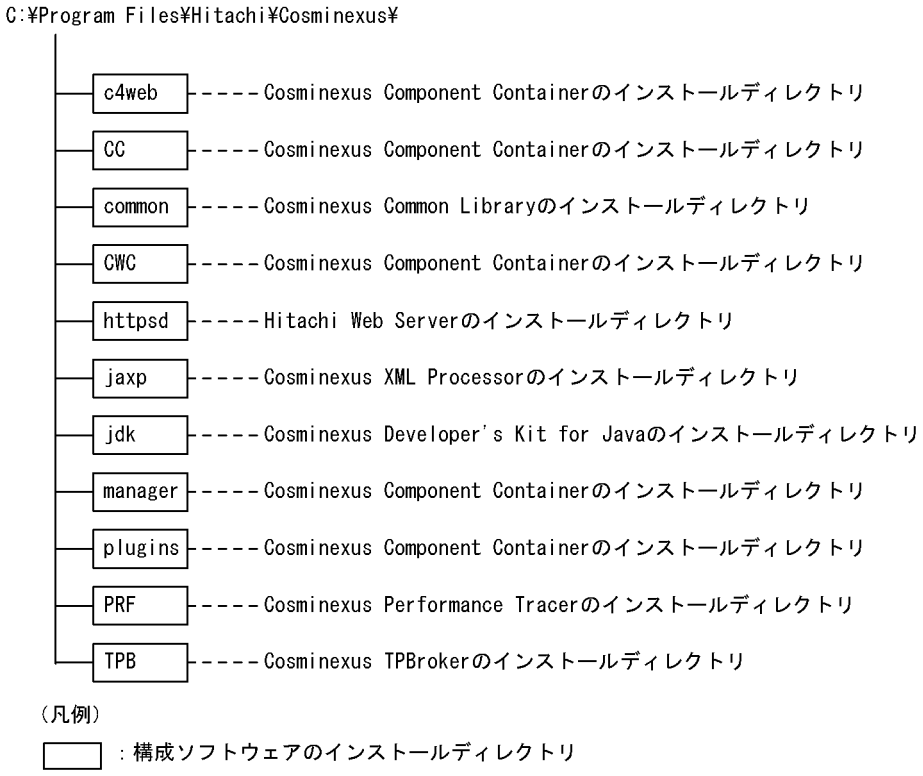
- HKEY_LOCAL_MACHINE¥SOFTWARE¥HITACHI¥uCosminexus Application Server Standard



(3) ディレクトリ構成

この例でのディレクトリ構成を次の図に示します。各ディレクトリの説明については，マニュアル「Cosminexus システム構築ガイド」の「2.9.1　Application Server のディレクトリ構成」を参照してください。

図 4-4 ディレクトリ構成（Windows の場合）



4.2.2 UNIX の場合

ここでは，UNIX の場合の操作手順，インストール後の確認手順，およびディレクトリ構成について説明します。

(1) 操作手順

Application Server のインストール手順を次に示します。

1. **インストールに使用する** CD-ROM **に，インストールするソフトウェアが格納されていることを確認します。**
   この例では，次のソフトウェアが格納されていることを確認します。
   - P-9S43-7D71　　07-00　　uCosminexus Application Server Standard
2. Application Server **をインストールするマシンに** root **権限でログインします。**
3. **手順** 1. **の** CD-ROM **を，**CD-ROM **ドライブに入れます。**
4. OS **の** mount **コマンドで，**CD-ROM **ファイルシステムをマウントします。**
   mount コマンドの実行例を次に示します。下線部には，CD-ROM ファイルシステムのマウントディレクトリ名を指定します。

```
# mount -r -o mode=0544 /dev/cdrom /mnt/cdrom
```

5. **日立 PP インストーラの setup コマンドで，セットアッププログラムを起動します。**
   setup コマンドの実行例を次に示します。下線部には，CD-ROM ファイルシステムのマウントディレクトリ名を指定します。

```
# /mnt/cdrom/linux/setup /mnt/cdrom
```

   注　CD-ROM ファイルシステムのディレクトリ名やファイル名は，OS の ls コマンドの実行結果をそのまま指定してください。マシン環境によっては，ls コマンドの実行結果とツリーの表示内容が異なる場合があります。

6. **日立 PP インストーラのメインメニューで，[I] キーを押します。**

```
Hitachi PP Installer  04-05

   L) List Installed Software.
   I) Install Software.
   D) Delete  Software.
   Q) Quit.

   Select Procedure ===>
```

7. **PP インストール画面で，必要なプログラムにカーソルを移動させ，[スペース] キーを押します。**
   次に示すプログラムだけを選択してください。ほかのプログラムは選択しないでください。選択したプログラムの左側には「@」が表示されます。
   - P-9S3Z-7151　0700　Cosminexus Developer's Kit for Java(TM)
   - P-9S41-E171　0300　Hitachi Web Server
   - P-9S43-7D71　0700　uCosminexus APS Standard - Base ※
   - P-9S43-8171　070001 Cosminexus Component Container
   - P-9S5Z-D171　0700　Cosminexus XML Processor
   - P-9S64-AF61　0517　Cosminexus TPBroker
   - P-9S64-EB11　0700　Cosminexus Performance Tracer

   注※　この例は，Application Server Standard をインストールする場合を説明しています。Application Server Enterprise をインストールする場合，「P-9S43-7K71　0700　uCosminexus APS Enterprise - Base」を選択してください。

8. **必要なすべてのプログラムの左側に「@」が表示されていることを確認し，[I] キーを押します。**

9. **インストールするかどうかを確認する次のメッセージが出力されたら，[y] キーまたは [Y] キーを押します。**

```
Install PP? (y: install,  n: cancel)==>
```

10. **インストール終了を示す次のメッセージが出力されたら，[Q] キーを押します。**

```
Installation completed.
```

11. **日立 PP インストーラのメインメニューで，[Q] キーを押します。**
    これでインストール作業は完了です。

(2) 確認手順

Application Server が正しくインストールされているか，確認する手順を次に示します。

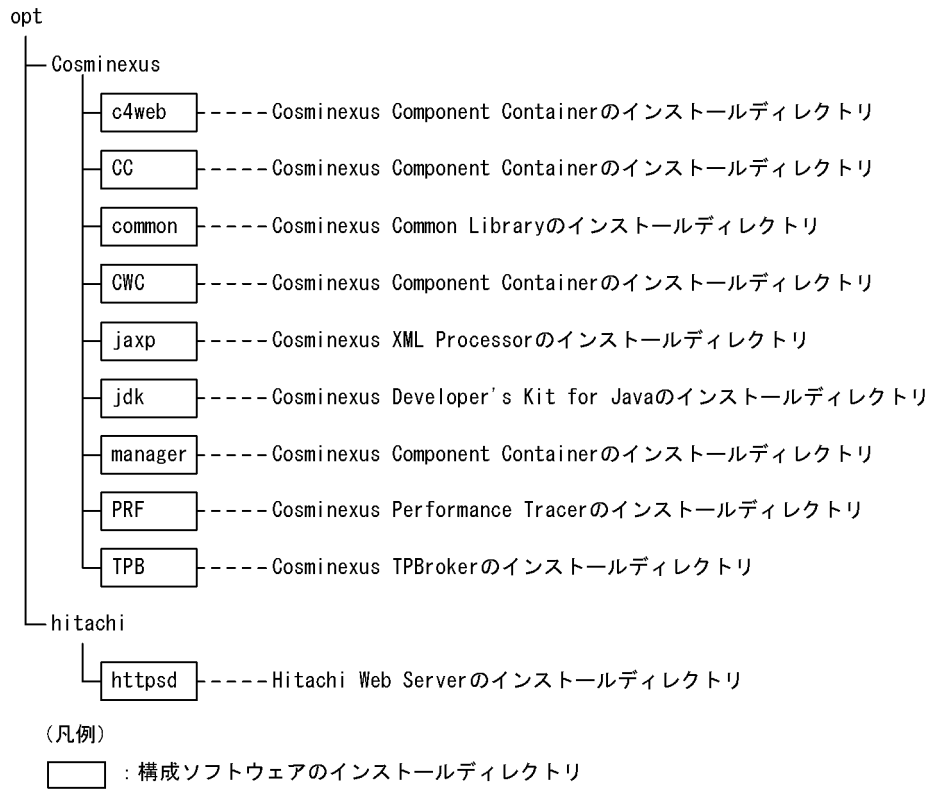
1. **/opt/Cosminexus/common/cosmicom.dat をテキストエディタなどで開きます。**
2. **インストールした Application Server の情報が記述されていることを確認します。**
   この例では，次の情報が記述されていることを確認します。

```
CosmiProductID = P-9S43-7D71
CosmiProductName = uCosminexus Application Server Standard
CosmiVersion = 07-00
   :
```

(3) ディレクトリ構成

この例でのディレクトリ構成を次の図に示します。各ディレクトリの説明については，マニュアル「Cosminexus システム構築ガイド」の「2.9.1　Application Server のディレクトリ構成」を参照してください。

図 4-5 ディレクトリ構成（UNIX の場合）



4.3 環境変数の設定

Application Server のインストールが完了したら，環境変数を設定します。

注意事項

システムが正しく動作しなくなるおそれがあるため，環境変数は誤りがないように設定してください。

4.3.1 Windows の場合

ここでは，Windows の場合の操作手順，および設定後の確認手順について説明します。

(1) 操作手順

環境変数の設定手順を次に示します。

1. **アプリケーションサーバのマシンに** Administrator **権限でログインします。**
2. **環境変数（**PATH**，**TPDIR**，**TZ**，**VBROKER_ADM**）を設定します。**
   この例での環境変数の設定値を，次の表に示します。

表 4-7 **必要な環境変数と設定値（**Windows **の場合）**

項番	環境変数名	設定値
1	PATH	C:¥Program Files¥Hitachi¥Cosminexus¥jdk¥bin ※
		C:¥Program Files¥Hitachi¥Cosminexus¥TPB¥bin
		C:¥Program Files¥Hitachi¥Cosminexus¥PRF¥bin
		C:¥Program Files¥Hitachi¥Cosminexus¥CC¥admin¥bin
		C:¥Program Files¥Hitachi¥Cosminexus¥CC¥server¥bin
		C:¥Program Files¥Hitachi¥Cosminexus¥httpsd
2	TPDIR	C:¥Program Files¥Hitachi¥Cosminexus¥TPB
3	TZ	JST-9
4	VBROKER_ADM	C:¥Program Files¥Hitachi¥Cosminexus¥TPB¥adm

設定するときの注意事項を次に示します。

- <Cosminexus のインストールディレクトリ >¥jdk¥bin（この例では表中の※）は，PATH の先頭に指定してください。
- CLASSPATH の値は空にしてください。

(2) 確認手順

環境変数が正しく設定されているか，確認する手順を次に示します。

1. OS を再起動し，Administrator 権限でログインします。
2. OS の set コマンドで環境変数が正しく設定されていることを確認します。
   set コマンドの実行結果で，設定した環境変数名の値に設定値が表示されているかを確認してください。この例での set コマンドの実行結果を次に示します。

```
C:¥Program Files¥Hitachi¥Cosminexus>set
   :
Path=C:¥WINNT¥system32;C:¥WINNT;C:¥WINNT¥System32¥Wbem;C:¥Program Files¥Common
Files¥Hitachi;C:¥Program Files¥Hitachi¥Cosminexus¥jdk¥bin;C:¥Program
Files¥Hitachi¥Cosminexus¥TPB¥bin;C:¥Program
Files¥Hitachi¥Cosminexus¥PRF¥bin;C:¥Program
Files¥Hitachi¥Cosminexus¥CC¥admin¥bin;C:¥Program
Files¥Hitachi¥Cosminexus¥CC¥server¥bin;C:¥Program
Files¥Hitachi¥Cosminexus¥httpsd
   :
TPDIR=C:¥Program Files¥Hitachi¥Cosminexus¥TPB
   :
TZ=JST-9
   :
VBROKER_ADM=C:¥Program Files¥Hitachi¥Cosminexus¥TPB¥adm
   :
```

4.3.2 UNIX の場合

ここでは，UNIX の場合の操作手順，および設定後の確認手順について説明します。

(1) 操作手順

環境変数の設定手順を次に示します。

1. アプリケーションサーバのマシンに root 権限でログインします。
2. 環境変数（LD_LIBRARY_PATH，CSCCFJ_SERVER_HOME，PATH，TPDIR，VBROKER_ADM，PRFSPOOL，TZ）を設定します。
   この例での環境変数の設定値を，次の表に示します。

表 4-8 必要な環境変数と設定値（UNIX の場合）

項番	環境変数名	設定値
1	LD_LIBRARY_PATH	/opt/Cosminexus/TPB/lib
		/opt/Cosminexus/PRF/lib
		/opt/hitachi/common/lib
2	CSCCFJ_SERVER_HOME	/opt/Cosminexus/CC
3	PATH	/opt/Cosminexus/jdk/bin
		/opt/Cosminexus/CC/admin/bin
		/opt/Cosminexus/CC/server/bin
		/opt/Cosminexus/TPB/bin
		/opt/Cosminexus/PRF/bin
		/opt/hitachi/httpsd/sbin

項番	環境変数名	設定値
		/bin
4	TPDIR	/opt/Cosminexus/TPB
5	VBROKER_ADM	/opt/Cosminexus/TPB/adm
6	PRFSPOOL	/opt/Cosminexus/PRF/spool
7	TZ	JST-9

設定するときの注意事項を次に示します。

- /opt/Cosminexus/jdk/bin は，PATH の先頭に指定してください。
- CLASSPATH の値は空にしてください。
- この例は，前提 OS が Linux の場合を説明しています。前提 OS が AIX の場合，設定が必要な環境変数が異なります。AIX とほかの UNIX の差異については，マニュアル「Cosminexus システム構築ガイド」の「2.3.1(2)　UNIX の場合」を参照してください。ただし，AIX 固有の環境変数 LDR_CNTRL と LC__FASTMSG の設定は不要です。

(2) 確認手順

環境変数が正しく設定されているか，確認する手順を次に示します。

1. **OS を再起動し，root 権限でログインします。**
2. **OS の env コマンドで環境変数が正しく設定されているかを確認します。**
   env コマンドの実行結果で，設定した環境変数名の値に設定値が表示されているかを確認してください。この例での env コマンドの実行結果を次に示します。

```
[root@MyServer root]# env
   :
VBROKER_ADM=/opt/Cosminexus/TPB/adm
   :
LD_LIBRARY_PATH=/opt/Cosminexus/TPB/lib:/opt/Cosminexus/PRF/lib:/opt/hitachi/
common/lib
   :
PATH=/opt/Cosminexus/jdk/bin:/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/
sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:/root/bin:/
opt/Cosminexus/CC/admin/bin:/opt/Cosminexus/CC/server/bin:/opt/Cosminexus/TPB/
bin:/opt/Cosminexus/PRF/bin:/bin:/opt/hitachi/httpsd/sbin
   :
CSCCFJ_SERVER_HOME=/opt/Cosminexus/CC
   :
PRFSPOOL=/opt/Cosminexus/PRF/spool
   :
TZ=JST-9
   :
TPDIR=/opt/Cosminexus/TPB
   :
```

4.4 Web サーバとの連携の設定

環境変数の設定が完了したら，Web サーバとの連携の設定をします。Web サーバとの連携は，ファイルを使用して設定します。Web サーバとの連携のための設定項目，使用するファイル，および設定個所を，次の表に示します。

表 4-9 Web サーバとの連携の設定

項番	設定項目	ファイル名	設定個所
1	URL パターンとワーカのマッピング定義	mod_jk.conf	JkMount
2	Hitachi Web Server の動作環境の設定	httpsd.conf	• User ※1 • Group ※1 • ServerName • CoreDumpDirectory ※2 • Include
3	Hitachi Web Server の SSL 通信の設定		• Listen • SSLEnable • SSLCertificateFile • SSLCertificateKeyFile • SSLRequireSSL

注　この例では，この表で示していない設定項目やファイルはデフォルトのまま使用するため，編集しません。
注※1　UNIX の場合だけ必要です。
注※2　Linux の場合だけ必要です。

注意事項

設定内容が正しいかを機械的に確認する方法はないため，各ファイルは誤りがないように編集してください。

4.4.1 Windows の場合

Web サーバとの連携の設定手順を次に示します。

操作手順

1. mod_jk.conf をテキストエディタなどで開きます。
   この例での mod_jk.conf の格納先を次に示します。

```
C:¥Program
Files¥Hitachi¥Cosminexus¥CC¥web¥redirector¥mod_jk.conf
```

2. mod_jk.conf に，URL パターンとワーカのマッピングを定義します。
   この例では，JkMount パラメタを次のとおりに編集します。

< 変更前 >

```
   :
JkMount /examples/* worker1
   :
```

< 変更後 >

```
   :
JkMount /sample/* worker1
   :
```

3. mod_jk.conf を上書き保存します。

4. httpsd.conf をテキストエディタなどで開きます。
   この例での httpsd.conf の格納先を次に示します。
   C:¥Program Files¥Hitachi¥Cosminexus¥httpsd¥conf¥httpsd.conf

5. httpsd.conf に，Hitachi Web Server の動作環境の設定をします。
   この例では，ServerName ディレクティブを次のとおりに編集します。

< 変更前 >

```
   :
ServerName www.example.com
   :
```

< 変更後 >

```
   :
ServerName MyServer
   :
```

また，ファイルの末尾に次の行を追加します。

```
Include "C:/Program Files/Hitachi/Cosminexus/CC/web/redirector/mod_jk.conf"
```

6. httpsd.conf に，Hitachi Web Server の SSL 通信の設定をします。
   この例では，ファイルの末尾に次の行を追加します。

```
Listen 443
<VirtualHost MyServer:443>
  SSLEnable
  SSLCertificateFile "C:/Program Files/Hitachi/Cosminexus/httpsd/conf/
httpsd.pem"
  SSLCertificateKeyFile "C:/Program Files/Hitachi/Cosminexus/httpsd/conf/
httpsdkey.pem"
</VirtualHost>
<Location /sample/>
  SSLRequireSSL
</Location>
```

注 1　この例では，<VirtualHost> ディレクティブで SSL 通信を適用する Web サーバ名，および SSL 通信に使用するポート番号を設定しています。また，<Location> ディレクティブで SSL 通信を適用する URL パターンを設定しています。

注 2　SSLCertificateFile ディレクティブおよび SSLCertificateKeyFile ディレクティブの指定値は，「3.3　SSL 通信で使用する証明書および秘密鍵の検討」で決定した内容に従ってください。

7. **httpsd.conf を上書き保存します。**

4.4.2　UNIX の場合

Web サーバとの連携の設定手順を次に示します。

操作手順

1. **mod_jk.conf をテキストエディタなどで開きます。**
   mod_jk.conf の格納先を次に示します。
   /opt/Cosminexus/CC/web/redirector/mod_jk.conf
2. **mod_jk.conf に，URL パターンとワーカのマッピングを定義します。**
   この例では，JkMount パラメタを次のとおりに編集します。

   < 変更前 >

```
   :
JkMount /examples/* worker1
   :
```

   < 変更後 >

```
   :
JkMount /sample/* worker1
   :
```

3. **mod_jk.conf を上書き保存します。**
4. **httpsd.conf をテキストエディタなどで開きます。**
   httpsd.conf の格納先を次に示します。
   /opt/hitachi/httpsd/conf/httpsd.conf
5. **httpsd.conf に，Hitachi Web Server の動作環境の設定をします。**
   この例では，User ディレクティブ，Group ディレクティブ，および ServerName ディレクティブを次のとおりに編集します。User ディレクティブおよび Group ディレクティブの指定値は，「3.2　OS の設定」で設定したアカウントと同じにしてください。

   < 変更前 >

```
   :
User nobody
Group nogroup
   :
ServerName www.example.com
   :
```

< 変更後 >

```
    :
User wwwuser
Group wwwgroup
    :
ServerName MyServer
    :
```

また，ファイルの末尾に次の行を追加します。CoreDumpDirectory ディレクティブには，すでに存在するディレクトリを指定してください。

```
CoreDumpDirectory /opt/hitachi/httpsd/logs
Include /opt/Cosminexus/CC/web/redirector/mod_jk.conf
```

6. **httpsd.conf に，Hitachi Web Server の SSL 通信の設定をします。**

この例では，ファイルの末尾に次の行を追加します。

```
Listen 443
<VirtualHost MyServer:443>
  SSLEnable
  SSLCertificateFile /opt/hitachi/httpsd/conf/httpsd.pem
  SSLCertificateKeyFile /opt/hitachi/httpsd/conf/httpsdkey.pem
</VirtualHost>
<Location /sample/>
  SSLRequireSSL
</Location>
```

注 1　この例では，<VirtualHost> ディレクティブで SSL 通信を適用する Web サーバ名，および SSL 通信に使用するポート番号を設定しています。また，<Location> ディレクティブで SSL 通信を適用する URL パターンを設定しています。

注 2　SSLCertificateFile ディレクティブおよび SSLCertificateKeyFile ディレクティブの指定値は，「3.3　SSL 通信で使用する証明書および秘密鍵の検討」で決定した内容に従ってください。

7. **httpsd.conf を上書き保存します。**

4.5　J2EE サーバの設定

Web サーバとの連携の設定が完了したら，J2EE サーバの設定を実施します。ここでは，J2EE サーバのセットアップ，および J2EE サーバの動作設定のカスタマイズについて説明します。

4.5.1　J2EE サーバのセットアップ

J2EE サーバは，製品のインストール時にホスト名と J2EE サーバ名とが同じ設定でセットアップ済みです。この例では，ホスト名と J2EE サーバ名が同じ「MyServer」であるため，J2EE サーバのセットアップは実行しません。

J2EE サーバのセットアップ手順を知りたい場合は，マニュアル「Cosminexus システム構築ガイド」の「8.2.1　J2EE サーバのセットアップ」を参照してください。

4.5.2　J2EE サーバの動作設定のカスタマイズ

J2EE サーバの動作設定のカスタマイズは，ファイルを使用して設定します。J2EE サーバの動作設定のカスタマイズをするための設定項目，使用するファイル，および設定個所を，次の表に示します。

表 4-10　J2EE サーバの動作設定のカスタマイズ

項番	設定項目	ファイル名	設定個所
1	EJB コンテナの通信ポートと IP アドレスの固定	usrconf.properties（J2EE サーバ用ユーザプロパティファイル）	• vbroker.se.iiop_tp.scm.iiop_tp.listener.port • vbroker.se.iiop_tp.host
2	Management Server の使用有無		ejbserver.instrumentation.enabled
3	サーバ管理コマンドの接続先の設定	usrconf.properties（サーバ管理コマンド用システムプロパティファイル）	ejbserver.naming.host

注　この例では，この表で示していない設定項目やファイルはデフォルトのまま使用するため，編集しません。

注意事項

- 設定内容が正しいかを機械的に確認する方法はないため，各ファイルは誤りがないように編集してください。
- ここで編集する usrconf.properties は，J2EE サーバ用ユーザプロパティファイルとサーバ管理コマンド用システムプロパティファイルの 2 種類あり，それぞれ設定内容が異なります。各ファイルに指定するキーや値を取り違えないよう，注意してください。

J2EE サーバの設定方法を次に示します。

操作手順

1. usrconf.properties（J2EE **サーバ用ユーザプロパティファイル）をテキストエディタなどで開きます。**
   - Windows の場合の，この例での usrconf.properties の格納先を次に示します。

     ```
     C:¥Program
     Files¥Hitachi¥Cosminexus¥CC¥server¥usrconf¥ejb¥MyServer¥usrconf.properties
     ```
   - UNIX の場合の，usrconf.properties の格納先を次に示します。

     ```
     /opt/Cosminexus/CC/server/usrconf/ejb/MyServer/
     usrconf.properties
     ```
2. usrconf.properties（J2EE **サーバ用ユーザプロパティファイル）に，**EJB **コンテナの通信ポートと** IP **アドレスの値，および** Management Server **の使用有無を設定します。**

   この例では，次のとおりに編集します。

   < 変更前 >

```
   :
#vbroker.se.iiop_tp.scm.iiop_tp.listener.port=0
#vbroker.se.iiop_tp.host=
   :
#ejbserver.instrumentation.enabled=true
   :
```

   < 変更後 >

```
   :
vbroker.se.iiop_tp.scm.iiop_tp.listener.port=30000
vbroker.se.iiop_tp.host=192.1.1.xxx
   :
ejbserver.instrumentation.enabled=false
   :
```

3. usrconf.properties（J2EE **サーバ用ユーザプロパティファイル）を上書き保存します。**
4. usrconf.properties**（サーバ管理コマンド用システムプロパティファイル）をテキストエディタなどで開きます。**
   - Windows の場合の，この例での usrconf.properties の格納先を次に示します。

     ```
     C:¥Program
     ```

Files¥Hitachi¥Cosminexus¥CC¥admin¥usrconf¥usrconf.properties

- UNIX の場合の，usrconf.properties の格納先を次に示します。
  /opt/Cosminexus/CC/admin/usrconf/usrconf.properties

5. usrconf.properties（サーバ管理コマンド用システムプロパティファイル）に，サーバ管理コマンドの接続先の設定をします。
   usrconf.properties（J2EE サーバ用ユーザプロパティファイル）の vbroker.se.iiop_tp.host キーに指定した，EJB コンテナの IP アドレスと同じ値を設定してください。この例では，次のとおりに編集します。

   < 変更前 >

```
   :
#ejbserver.naming.host=localhost
   :
```

   < 変更後 >

```
   :
ejbserver.naming.host=192.1.1.xxx
   :
```

6. usrconf.properties（サーバ管理コマンド用システムプロパティファイル）を上書き保存します。

注意事項

IP アドレスに含まれる「xxx」の部分は数字です。実際の IP アドレスは，システム構成に合わせて設定してください。

4.6 システムの動作確認（起動）

J2EE サーバの設定が完了したら，アプリケーションサーバが正常に起動するかどうかを確認します。

注意事項

アプリケーションサーバの起動の各手順でコマンドの実行に失敗した場合，表示されるメッセージおよび操作内容を見直して，再実行してください。

4.6.1 Windows の場合

アプリケーションサーバの起動手順を次に示します。

この例では，ホスト名と J2EE サーバ名が同じ「MyServer」であるため，J2EE サーバ名の指定を省略しています。

操作手順

1. cprfstart コマンドで PRF デーモンを起動します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cprfstart
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KFCT73412-I cprfd is now online.
```

2. cjstartsv コマンドで J2EE サーバを起動します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjstartsv
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，この例では，起動した J2EE サーバ名が「MyServer」になっていることを確認します。

```
KDJE30028-I The J2EE server has started. Server name = MyServer
```

3. 別のコマンドプロンプトを開きます。
これまで使用していたコマンドプロンプトは，閉じないでそのままにしておいてください。

4. httpsd コマンドで Hitachi Web Server を起動します。

```
C:¥Program Files¥Hitachi¥Cosminexus>httpsd -k start
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してくださ

い。

```
The Hitachi Web Server service is running.
```

4.6.2 UNIX の場合

アプリケーションサーバの起動手順を次に示します。

この例では，ホスト名と J2EE サーバ名が同じ「MyServer」であるため，J2EE サーバ名の指定を省略しています。

操作手順

1. cprfstart コマンドで PRF デーモンを起動します。

```
# cprfstart
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KFCT73412-I cprfd is now online.
```

2. cjstartsv コマンドで J2EE サーバを起動します。

```
# cjstartsv
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，この例では，起動した J2EE サーバ名が「MyServer」になっていることを確認します。

```
KDJE30028-I The J2EE server has started. Server name = MyServer
```

3. 別のコンソールを開きます。
これまで使用したコンソールは，閉じないでそのままにしておいてください。

4. httpsdctl ユティリティで Hitachi Web Server を起動します。

```
# httpsdctl start
```

5. 制御プロセス ID を格納するファイルを開いて，Hitachi Web Server の制御プロセス ID を確認します。
この例では，デフォルト値の /opt/hitachi/httpsd/logs/httpd.pid を開いて確認します。

6. OS の ps コマンドで Hitachi Web Server のプロセスの状態を確認します。
ps コマンドの実行結果で，手順 5. で確認した制御プロセス ID の状態を確認してください。ps コマンドの実行例を次に示します。

```
# ps 2841
  PID TTY      STAT   TIME COMMAND
 2841 ?        S      0:00 /opt/hitachi/httpsd/sbin/httpsd -k start
```

4.7 ユーザ認証情報の設定

アプリケーションサーバが正常に起動するかどうかを確認したら，利用者のユーザ認証情報を設定します。

管理者は，「3.5 セキュリティ機能の設定に関する検討」で決定した内容に従って，ユーザ ID，パスワード，および所属ロールを J2EE サーバに登録します。そして，ユーザ ID と所属ロールをマッピングします。

ここでは，ユーザ認証情報の設定手順について説明します。なお，説明する手順では，Windows での操作例を記載しています。UNIX の場合，表示されるコマンドプロンプト「C:¥Program Files¥Hitachi¥Cosminexus>」を「#」に置き換えてください。

注意事項

ユーザ認証情報の設定の各手順でコマンドの実行に失敗した場合，表示されるメッセージおよび操作内容を見直して，再実行してください。

4.7.1 ユーザ ID とパスワードの登録

この例で想定している 2 名の利用者に対して，ユーザ ID とパスワードを登録します。

(1) 操作手順

ユーザ ID とパスワードの登録手順を次に示します。

1. cjaddsec **コマンドで，下位職制の利用者のユーザ** ID **とパスワードを登録します。**
   この例では，下位職制の利用者のユーザ ID として「user1」，パスワードとして「password1」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjaddsec -type user -name user1 -password
password1
```

   コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[user1]」が表示されていることを確認してください。

```
KDJE37503-I User has been added successfully. (name = [user1])
```

2. cjaddsec **コマンドで，上位職制の利用者のユーザ** ID **とパスワードを登録します。**
   この例では，上位職制の利用者のユーザ ID として「user2」，パスワードとして「password2」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjaddsec -type user -name user2 -password
password2
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[user2]」が表示されていることを確認してください。

```
KDJE37503-I User has been added successfully. (name = [user2])
```

注意事項

- 実際に設定するパスワードは，「1.3.7　パスワードの管理」に従って，強度があるものにしてください。
- パスワードが正しく登録されたかどうかを確認するコマンドはありません。cjaddsec コマンド実行時，指定したパスワードに誤りがないかを十分確認してください。

(2) 確認手順

ユーザ ID が正しく登録されているか，確認する手順を次に示します。

1. cjlistsec **コマンドで，ユーザ** ID **が正しく登録されているか確認します。**
   コマンドの実行結果として，登録したユーザ ID「user1」および「user2」が表示されていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistsec -type user
   :
user1
user2
KDJE37508-I All users have been listed successfully. (number = [2])
```

4.7.2 所属ロールの登録

この例で使用する 2 種類の所属ロールを設定します。

(1) 操作手順

所属ロールの登録手順を次に示します。

1. cjaddsec **コマンドで，下位職制の利用者に対応づける所属ロールを登録します。**
   この例では，下位職制の利用者に対応づける所属ロールとして「employee」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjaddsec -type role -name employee
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[employee]」が表示されていることを確認してください。

```
KDJE37503-I Role has been added successfully. (name = [employee])
```

2. cjaddsec **コマンドで，上位職制の利用者に対応づける所属ロールを登録します。**

この例では，上位職制の利用者に対応づける所属ロールとして「manager」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjaddsec -type role -name manager
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[manager]」が表示されていることを確認してください。

```
KDJE37503-I Role has been added successfully. (name = [manager])
```

(2) 確認手順

所属ロールが正しく登録されているか，確認する手順を次に示します。

1. cjlistsec **コマンドで，所属ロールが正しく登録されているか確認します。**
   コマンドの実行結果として，登録した所属ロール「employee」および「manager」が表示されていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistsec -type role
   :
employee
manager
KDJE37508-I All roles have been listed successfully. (number = [2])
```

4.7.3 ユーザ ID と所属ロールのマッピング

「4.7.1 ユーザ ID とパスワードの登録」で登録したユーザ ID と「4.7.2 所属ロールの登録」で登録した所属ロールをマッピングします。

(1) 操作手順

ユーザ ID と所属ロールのマッピング手順を次に示します。

1. cjmapsec **コマンドで下位職制の利用者のユーザ ID と下位職制用の所属ロールをマッピングします。**
   この例では，下位職制用の所属ロールとして「employee」，下位職制の利用者のユーザ ID として「user1」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjmapsec -role employee -user user1
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[user1]」が表示されていることを確認してください。

```
KDJE37514-I User has been mapped successfully. (name = [user1])
```

2. cjmapsec **コマンドで上位職制の利用者のユーザ ID と上位職制用の所属ロールをマッ**

ピングします。
この例では，上位職制用の所属ロールとして「manager」，上位職制の利用者のユーザ ID として「user2」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjmapsec -role manager -user user2
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[user2]」が表示されていることを確認してください。

```
KDJE37514-I User has been mapped successfully. (name = [user2])
```

(2) 確認手順

ユーザ ID と所属ロールが正しくマッピングされているか，確認する手順を次に示します。

1. cjlistsec **コマンドで，ユーザ** ID**「**user1**」に対して所属ロール「**employee**」が正しくマッピングされているか確認します。**
   コマンドの実行結果として，ユーザ ID「user1」にマッピングした所属ロール「employee」が表示されていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistsec -type user -name user1
   :
employee
KDJE37509-I Role has been listed successfully. (name = [user1])
```

2. cjlistsec **コマンドで，ユーザ** ID**「**user2**」に対して所属ロール「**manager**」が正しくマッピングされているか確認します。**
   コマンドの実行結果として，ユーザ ID「user2」にマッピングした所属ロール「manager」が表示されていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistsec -type user -name user2
   :
manager
KDJE37509-I Role has been listed successfully. (name = [user2])
```

4.8 J2EE アプリケーションのインポート

利用者のユーザ認証情報を設定したら，J2EE アプリケーションをインポートします。

管理者は，「3.4 J2EE アプリケーションの入手」に従って，入手および確認した J2EE アプリケーションをインポートします。

ここでは，J2EE アプリケーションのインポート手順について説明します。なお，説明する手順では，Windows での操作例を記載しています。UNIX の場合，表示されるコマンドプロンプト「C:¥Program Files¥Hitachi¥Cosminexus>」を「#」に置き換えてください。また，作業用ディレクトリのパス「C:¥sample¥」を「/sample/」に置き換えてください。

(1) 操作手順

J2EE アプリケーションのインポート手順を次に示します。

1. **入手した** J2EE **アプリケーションを，作業用ディレクトリに格納します。**
   この例では，J2EE アプリケーション「sample.ear」を，作業用ディレクトリ「C:¥sample¥」に格納します。
2. cjimportapp **コマンドで** J2EE **アプリケーションをインポートします。**
   この例では，J2EE アプリケーション名として「sample.ear」，作業用ディレクトリとして「C:¥sample¥」を指定しています。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjimportapp -f C:¥sample¥sample.ear
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「Name =」のあとに，「[sample]」が表示されていることを確認してください。

```
KDJE37041-I Application has been imported successfully. Name=[sample]
```

注意事項

コマンドの実行に失敗した場合，表示されるメッセージおよび操作内容を見直して，再実行してください。

(2) 確認手順

J2EE アプリケーションが正しくインポートされているか，確認する手順を次に示します。

1. cjlistapp **コマンドで** J2EE **アプリケーションがインポートされていることを確認します。**
   コマンドの実行結果で，インポートした J2EE アプリケーション「sample」が表示さ

れ，状態が「stopped」になっていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistapp
   :
stopped sample
KDJE37508-I All applications have been listed successfully. (number = [1])
```

4.9 J2EE アプリケーションのプロパティ設定

インポートした J2EE アプリケーションに対して，ユーザ認証方式，およびセキュリティロールの構成を設定します。

管理者は，J2EE アプリケーションの属性ファイルを取得し，「3.4 J2EE アプリケーションの入手」および「3.5 セキュリティ機能の設定に関する検討」で決定した内容に従って，属性ファイルを編集します。そのあと，属性ファイルの値を J2EE アプリケーションに反映します。

ここでは，J2EE アプリケーションのプロパティを設定する手順について説明します。なお，説明する手順では，Windows での操作例を記載しています。UNIX の場合，表示されるコマンドプロンプト「C:¥Program Files¥Hitachi¥Cosminexus>」を「#」に置き換えてください。また，作業用ディレクトリのパス「C:¥sample¥」を「/sample/」に置き換えてください。

注意事項

- J2EE アプリケーションのプロパティ設定の各手順でコマンドの実行に失敗した場合，表示されるメッセージおよび操作内容を見直して，再実行してください。
- J2EE アプリケーションを開始できなくなるおそれがあるため，各属性ファイルは誤りがないように編集してください。

4.9.1 アプリケーション属性ファイルの編集

アプリケーション属性ファイルはデフォルトのまま使用します。編集しないでください。

4.9.2 WAR 属性ファイルの編集

WAR 属性ファイルでは，次の三つの項目を設定します。

- ログイン時のユーザ認証方式
- URL パターンと Web アプリケーションの許可ロールの対応
- Web アプリケーションの許可ロールと所属ロールの対応

WAR 属性ファイルの編集手順を次に示します。

操作手順

1. cjgetappprop コマンドで WAR 属性ファイルを取得します。
   この例では，J2EE アプリケーション名として「sample」，WAR の表示名として「sample_war」，WAR 属性ファイルの出力先として「C:¥sample¥prop_war.xml」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjgetappprop -name sample -type war
-resname sample_war -c C:¥sample¥prop_war.xml
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KDJE37505-I WAR has been obtained successfully. (name = [sample_war])
```

また，「C:¥sample」の下に「prop_war.xml」が取得されていることを確認してください。

2. **prop_war.xml をテキストエディタなどで開きます。**

3. **ログイン時のユーザ認証方式を定義します。**
   prop_war.xml の <login-config> タグを編集してください。この例では，ユーザ認証方式として「BASIC」，レルム名として「SAMPLE」を指定します。

```
  :
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>SAMPLE</realm-name>
</login-config>
 :
```

4. **URL パターンと Web アプリケーションの許可ロールの対応を定義します。**
   prop_war.xml の <security-constraint> タグを編集してください。この例では，次の二つを定義します。
   - Web リソース名として「ALL」を指定する。URL パターン「/*」と，Web アプリケーションの許可ロール「member」および「boss」を対応づける。
   - Web リソース名として「BOSS」を指定する。URL パターン「/boss/*」と，Web アプリケーションの許可ロール「boss」を対応づける。

```
  :
<security-constraint>
  <web-resource-collection>
    <web-resource-name>ALL</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>member</role-name>
    <role-name>boss</role-name>
  </auth-constraint>
  <original-name/>
</security-constraint>

<security-constraint>
  <web-resource-collection>
    <web-resource-name>BOSS</web-resource-name>
    <url-pattern>/boss/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>boss</role-name>
  </auth-constraint>
  <original-name/>
</security-constraint>
 :
```

5. Web アプリケーションの許可ロールと所属ロールの対応を定義します。
   prop_war.xml の <security-role> タグを編集してください。この例では，次の二つを定義します。
   - Web アプリケーションの許可ロール「member」を所属ロール「employee」と対応づける。
   - Web アプリケーションの許可ロール「boss」を所属ロール「manager」と対応づける。

```
 :
<security-role>
  <role-name>member</role-name>
  <linked-to>employee</linked-to>
</security-role>

<security-role>
  <role-name>boss</role-name>
  <linked-to>manager</linked-to>
</security-role>
 :
```

6. prop_war.xml を上書き保存します。

7. cjsetappprop コマンドで WAR 属性ファイルの値を反映します。
   この例では，J2EE アプリケーション名として「sample」，WAR の表示名として「sample_war」，WAR 属性ファイルの入力元として「C:¥sample¥prop_war.xml」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjsetappprop -name sample -type war
-resname sample_war -c C:¥sample¥prop_war.xml
```

   コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[sample_war]」が表示されていることを確認してください。

```
KDJE37506-I WAR has been set successfully. (name = [sample_war])
```

4.9.3 EJB-JAR 属性ファイルの編集

EJB-JAR 属性ファイルでは，次の項目を設定します。

● EJB の許可ロールと所属ロールの対応

EJB-JAR 属性ファイルの編集手順を次に示します。

操作手順

1. cjgetappprop コマンドで EJB-JAR 属性ファイルを取得します。
   この例では，J2EE アプリケーション名として「sample」，EJB-JAR の表示名として「sample_ejb」，EJB-JAR 属性ファイルの出力先として「C:¥sample¥prop_ejbjar.xml」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjgetappprop -name sample -type ejb
-resname sample_ejb -c C:¥sample¥prop_ejbjar.xml
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KDJE37505-I EJB-JAR has been obtained successfully. (name = [sample_ejb])
```

また，「C:¥sample」の下に「prop_ejbjar.xml」が取得されていることを確認してください。

2. prop_ejbjar.xml **をテキストエディタなどで開きます。**
3. EJB **の許可ロールと所属ロールの対応を定義します。**

   prop_ejbjar.xml の <security-role> タグを編集してください。この例では，次の二つを定義します。
   - EJB の許可ロール「reader」と所属ロール「employee」を対応づける。
   - EJB の許可ロール「writer」と所属ロール「manager」を対応づける。

```
  :
<security-role>
  <role-name>reader</role-name>
  <linked-to>employee</linked-to>
</security-role>

<security-role>
  <role-name>writer</role-name>
  <linked-to>manager</linked-to>
</security-role>
 :
```

4. prop_ejbjar.xml **を上書き保存します。**
5. cjsetappprop **コマンドで** EJB-JAR **属性ファイルの値を反映します。**

   この例では，J2EE アプリケーション名として「sample」，EJB-JAR の表示名として「sample_ejb」，EJB-JAR 属性ファイルの入力元として「C:¥sample¥prop_ejbjar.xml」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjsetappprop -name sample -type ejb
-resname sample_ejb -c C:¥sample¥prop_ejbjar.xml
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[sample_ejb]」が表示されていることを確認してください。

```
KDJE37506-I EJB-JAR has been set successfully. (name = [sample_ejb])
```

4.9.4 Session Bean 属性ファイルの編集

Session Bean 属性ファイルでは，次の項目を設定します。

● EJB の許可ロールとメソッドの対応

Session Bean 属性ファイルの編集手順を次に示します。

操作手順

1. cjgetappprop **コマンドで** Session Bean **属性ファイルを取得します。**
   この例では，J2EE アプリケーション名として「sample」，EJB-JAR の表示名として「sample_ejb」，Session Bean の表示名として「Business」，Session Bean 属性ファイルの出力先として「C:¥sample¥prop_session.xml」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjgetappprop -name sample -type ejb
-resname sample_ejb/Business -c C:¥sample¥prop_session.xml
```

   コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KDJE37505-I EJB-JAR has been obtained successfully. (name = [sample_ejb/
Business])
```

   また，「C:¥sample」の下に「prop_session.xml」が取得されていることを確認してください。

2. prop_session.xml **をテキストエディタなどで開きます。**

3. EJB **の許可ロールとメソッドの対応を定義します。**
   prop_session.xml の <method-permission> タグを編集してください。この例では，次の二つを定義します。
   - EJB の許可ロール「reader」とメソッド「read」を対応づける。
   - EJB の許可ロール「writer」とメソッド「write」および「read」を対応づける。

```
 :
<method-permission>
  <role-name>reader</role-name>
  <method>
    <method-name>read</method-name>
  </method>
</method-permission>

<method-permission>
  <role-name>writer</role-name>
  <method>
    <method-name>write</method-name>
  </method>
  <method>
    <method-name>read</method-name>
  </method>
</method-permission>
 :
```

4. prop_session.xml **を上書き保存します。**

5. cjsetappprop **コマンドで** Session Bean **属性ファイルの値を反映します。**
   この例では，J2EE アプリケーション名として「sample」，EJB-JAR の表示名として

「sample_ejb」，Session Bean の表示名として「Business」，Session Bean 属性ファイルの入力元として「C:¥sample¥prop_ejbjar.xml」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjsetappprop -name sample -type ejb
-resname sample_ejb/Business -c C:¥sample¥prop_session.xml
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「name =」のあとに，「[sample_ejb/Business]」が表示されていることを確認してください。

```
KDJE37506-I EJB-JAR has been set successfully. (name = [sample_ejb/Business])
```

4.10 J2EE アプリケーションの動作確認

J2EE アプリケーションのプロパティ設定が完了したら，J2EE アプリケーションが正常に動作するか確認をします。次の観点で確認をしてください。

- J2EE アプリケーションを開始できるかどうか。
- J2EE アプリケーションを正常に実行できるかどうか。
- ユーザ認証とアクセス制御が正しく設定されているかどうか。

それぞれの確認方法について，次に示します。

4.10.1 J2EE アプリケーションの開始確認

設定した J2EE アプリケーションが正しく開始されるかどうかを確認します。ここでは，操作手順，および開始後の確認手順について説明します。

なお，この手順では，Windows での操作例を記載しています。UNIX の場合，表示されるコマンドプロンプト「C:¥Program Files¥Hitachi¥Cosminexus>」を「#」に置き換えてください。また，作業用ディレクトリのパス「C:¥sample¥」を「/sample/」に置き換えてください。

注意事項

J2EE アプリケーションの開始に失敗した場合，表示されるメッセージおよび操作内容を見直して，再実行してください。

(1) 操作手順

J2EE アプリケーションの開始手順を次に示します。

1. cjstartapp コマンドで J2EE アプリケーションを開始します。
   この例では，J2EE アプリケーション名として「sample」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjstartapp -name sample
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，このメッセージの「Name =」のあとに，「[sample]」が表示されていることを確認してください。

```
KDJE37045-I Application has been started successfully. Name=[sample]
```

(2) 確認手順

J2EE アプリケーションが開始されているか，確認する手順を次に示します。

1. cjlistapp コマンドで J2EE アプリケーションが開始されていることを確認します。
   コマンドの実行結果で，起動した J2EE アプリケーション「sample」の状態が，「running」になっていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistapp
   :
running sample
KDJE37508-I All applications have been listed successfully. (number = [1])
```

4.10.2 J2EE アプリケーションの実行確認

設定した J2EE アプリケーションが正常に実行されるかどうかを確認します。ここでは，J2EE アプリケーションの実行確認をする場合の観点，および J2EE アプリケーションが正しく実行できないときの見直し観点を，次に示します。

(1) 確認の観点

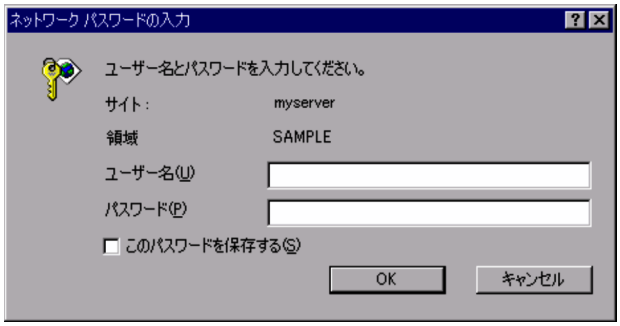
アプリケーションサーバのマシンから，次の観点で確認をしてください。

- ログイン画面にアクセスできるか。
- SSL 通信を使用してアクセスしているか。

この例の場合，次の URL にアクセスして，ログイン画面にアクセスできるかどうか，確認してください。

```
https://MyServer/sample/menu.html
```

正常に実行された場合，次のようなログイン画面が表示されます。



(2) 見直しの観点

ログイン画面にアクセスできなかった場合は，次の点を見直して再実行してください。

- システムが正しく動作しているか。
  システムの動作確認については，「4.6　システムの動作確認（起動）」を参照してください。
- J2EE アプリケーションが開始されているか。

J2EE アプリケーションの開始については，「4.10.1　J2EE アプリケーションの開始確認」を参照してください。

- 指定した URL が正しいか。
- WAR 属性ファイルで，ユーザ認証方式が正しく定義されているか。
  WAR 属性ファイルについては，「4.9.2　WAR 属性ファイルの編集」を参照してください。
- Web サーバとの連携の設定が正しいか。
  次の定義ファイルが正しく定義されているかを確認してください。Web サーバとの連携の設定については，「4.4　Web サーバとの連携の設定」を参照してください。
  - mod_jk.conf
  - httpsd.conf
- J2EE サーバの動作設定が正しいか。
  次の定義ファイルが正しく定義されているかを確認してください。J2EE サーバの動作設定については，「4.5.2　J2EE サーバの動作設定のカスタマイズ」を参照してください。
  - usrconf.properties（J2EE サーバ用ユーザプロパティファイル）
  - usrconf.properties（サーバ管理コマンド用システムプロパティファイル）

4.10.3　ユーザ認証とアクセス制御の設定確認

ログイン画面に正常にアクセスできたら，登録した全ユーザ ID について，ユーザ認証とアクセス制御が正しく設定されているかどうかを確認します。

ここでは，ユーザ認証とアクセス制御の設定を確認する場合の観点，および正しく設定されていないときの見直し観点について説明します。

(1) 確認の観点

ユーザ認証とアクセス制御のそれぞれの観点について説明します。

ユーザ認証

次の観点で確認してください。

- 登録したユーザ ID およびパスワードでログインできるか。
- 登録していないユーザ ID でログインしようとした場合，ログインが拒否されるか。

アクセス制御

次の観点で確認してください。

- アクセスが許可されているページにアクセスできるか。
- アクセスが許可されていないページにアクセスしようとした場合，アクセスが拒否されるか。
- 実行が許可されているメソッドを実行できるか。
- 実行が許可されていないメソッドを実行しようとした場合，拒否されるか。

この例では，各ユーザ ID に対する設定は，次の表のようになっています。

表 4-11　この例での J2EE アプリケーションのアクセス制御

項番	ユーザ ID	URL パターンへのアクセス許可		メソッドに対する許可	
		/*	/boss/*	read	write
1	user1	○	×	○	×
2	user2	○	○	○	○

（凡例）　○：アクセス可　×：アクセス不可

注意事項

異なるユーザ ID に対してユーザ認証とアクセス制御の確認を実施する場合は，必ずブラウザを再起動してください。

(2) 見直しの観点

ユーザ認証およびアクセス制御が正しく設定されていない場合は，次の点を見直して再実行してください。

- ユーザ認証情報が正しく設定されているか。
  ユーザ認証情報の設定については，「4.7　ユーザ認証情報の設定」を参照してください。
- WAR 属性ファイルで，セキュリティロールの構成が正しく設定されているか。
  次の項目が正しく設定されているかを確認してください。WAR 属性ファイルについては，「4.9.2　WAR 属性ファイルの編集」を参照してください。
  - URL パターンと Web アプリケーションの許可ロールの対応
  - Web アプリケーションの許可ロールと所属ロールの対応
- EJB-JAR 属性ファイルで，セキュリティロールの構成が正しく設定されているか。
  EJB の許可ロールと所属ロールの対応が正しく設定されているかを確認してください。EJB-JAR 属性ファイルについては，「4.9.3　EJB-JAR 属性ファイルの編集」を参照してください。
- Session Bean 属性ファイルで，セキュリティロールの構成が正しく設定されているか。
  EJB の許可ロールとメソッドの対応が正しく設定されているかを確認してください。Session Bean 属性ファイルについては，「4.9.4　Session Bean 属性ファイルの編集」を参照してください。

4.11 システムの動作確認（停止）

J2EE アプリケーションの動作確認が完了したら，アプリケーションサーバが正常に停止するかどうかを確認します。

アプリケーションサーバの停止方法を，適用 OS 別に次に示します。

注意事項

アプリケーションサーバの停止の各手順でコマンドの実行に失敗した場合，表示されるメッセージおよび操作内容を見直して，再実行してください。

4.11.1 Windows の場合

アプリケーションサーバの停止手順を次に示します。

この例では，ホスト名と J2EE サーバ名が同じ「MyServer」であるため，J2EE サーバ名の指定を省略しています。

操作手順

1. httpsd コマンドで Hitachi Web Server を停止します。

```
C:¥Program Files¥Hitachi¥Cosminexus>httpsd -k stop
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
The Hitachi Web Server service has stopped.
```

2. cjstopapp コマンドで J2EE アプリケーションを停止します。
この例では，J2EE アプリケーション名として「sample」を指定します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjstopapp -name sample
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，この例では，停止した J2EE アプリケーション名が「sample」であることを確認します。

```
KDJE37046-I Application has been stopped successfully. Name=[sample]
```

3. cjlistapp コマンドで J2EE アプリケーションが停止されていることを確認します。
コマンドの実行結果で，停止した J2EE アプリケーション「sample」の状態が，「stopped」になっていることを確認してください。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjlistapp
   :
stopped sample
KDJE37508-I All applications have been listed successfully. (number = [1])
```

4. cjstopsv コマンドで J2EE サーバを停止します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cjstopsv
```

コマンドの実行結果として，cjstartsv コマンドを実行したコマンドプロンプトに次のメッセージが表示されていることを確認してください。また，この例では，停止した J2EE サーバ名が「MyServer」になっていることを確認します。

```
KDJE30034-I The J2EE server shut down. Server name = MyServer
```

5. cprfstop コマンドで PRF デーモンを停止します。

```
C:¥Program Files¥Hitachi¥Cosminexus>cprfstop
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KFCT73414-I CPRFD stop.
```

4.11.2 UNIX の場合

アプリケーションサーバの停止手順を次に示します。

この例では，ホスト名と J2EE サーバ名が同じ「MyServer」であるため，J2EE サーバ名の指定を省略しています。

操作手順

1. httpsdctl ユティリティで Hitachi Web Server を停止します。

```
# /opt/hitachi/httpsd/sbin/httpsdctl stop
```

2. OS の ps コマンドで，Hitachi Web Server のプロセスの状態を確認します。
ps コマンドの実行結果で，「4.6.2　UNIX の場合」の手順 5. で確認した Hitachi Web Server の制御プロセス ID が表示されないことを確認してください。ps コマンドの実行例を次に示します。

```
# ps 2841
  PID TTY      STAT   TIME COMMAND
```

3. cjstopapp コマンドで J2EE アプリケーションを停止します。
この例では，J2EE アプリケーション名として「sample」を指定します。

```
# cjstopapp -name sample
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。また，この例では，停止した J2EE アプリケーション名が「sample」であることを確認します。

```
KDJE37046-I Application has been stopped successfully. Name=[sample]
```

4. cjlistapp **コマンドで** J2EE **アプリケーションが停止されていることを確認します。**
   この例では，コマンドの実行結果で，停止した J2EE アプリケーション「sample」の状態が，「stopped」になっていることを確認します。

```
# cjlistapp
   :
stopped sample
KDJE37508-I All applications have been listed successfully. (number = [1])
```

5. cjstopsv **コマンドで** J2EE **サーバを停止します。**

```
# cjstopsv
```

コマンドの実行結果として，cjstartsv コマンドを実行したコンソールに次のメッセージが表示されていることを確認してください。また，この例では，停止した J2EE サーバ名が「MyServer」であることを確認します。

```
KDJE30034-I The J2EE server shut down. Server name = MyServer
```

6. cprfstop **コマンドで** PRF **デーモンを停止します。**

```
# cprfstop
```

コマンドの実行結果として，次のメッセージが表示されていることを確認してください。

```
KFCT73414-I CPRFD stop.
```

5 システム運用前の準備

この章では，システムを運用する前に必要な準備作業について説明します。

5.1 運用ルールの決定

運用作業を円滑に実施するために，あらかじめ運用ルールを決定しておきます。

ここでは，Application Server のセキュリティ機能を使用したシステムの運用ルールについて説明します。

セキュリティロールの構成

セキュリティロールによるアクセス制御を正しく機能させるために，管理者はセキュリティロールの構成を適切に管理する必要があります。セキュリティロールの構成は，「1.3.5　J2EE アプリケーションの管理」のセキュリティロールの構成管理に関する説明に従って管理します。

ここでは運用ルールとして，次のことを決定しておいてください。

- 構築時に設定した情報を，最新に保つための管理方法
- 利用者を追加登録する場合の，ユーザ認証情報の決定方針
- 社内の職制変更や J2EE アプリケーションの入れ替えに伴う，セキュリティロールの構成の変更方針

利用者のユーザ認証情報

- システムに登録した利用者のユーザ認証情報は，常に最新であるよう管理する必要があります。利用者のユーザ認証情報は，「1.3.6　ユーザ認証情報の管理」の利用者のユーザ認証情報に関する説明に従って管理します。
  ここでは運用ルールとして，ユーザ認証情報の管理方法について決定しておいてください。
- 利用者のパスワードは，不正なアクセスを防ぐため，管理者が定期的に変更する必要があります。利用者のパスワードは，「1.3.7　パスワードの管理」に従って変更します。
  ここでは運用ルールとして，パスワードを変更する頻度を決定しておいてください。

5.2 利用者への通知

利用者がシステムを利用するために必要な情報や，利用に当たっての注意事項を通知します。利用者への通知は，確実で安全な手段，および手順を選んで実施してください。

ここでは，管理者が利用者に通知する必要がある項目について説明します。

システムを利用するために必要な情報

- アクセスする Web ページの URL
- アクセス時のユーザ認証画面で入力する情報（ユーザ ID，パスワード）
- システムにアクセス後，ユーザ認証が完了してログインするまでの手順

利用に当たっての注意事項

- 「1.3.6　ユーザ認証情報の管理」の利用者のユーザ認証情報に関する説明に従って，各利用者が自分のユーザ認証情報を適切に管理するよう，注意を促してください。
- 管理者が運用作業のためにシステムを停止する場合は，必ずシステム停止期間を通知してください。
- セキュリティ上，管理者がパスワードを定期的に変更することを通知してください。また，実際にパスワードを変更するときは，変更後のパスワードを適用する前に，変更後のパスワードと適用開始時期を利用者に通知してください。

5.3 運用方法の確認

システム運用は，ファイル編集とコマンド実行で行います。アプリケーションサーバのマシンで，J2EE サーバや Web サーバのファイルを編集したりコマンドを実行したりして，システムを運用します。

J2EE サーバが提供するファイルについては，マニュアル「Cosminexus リファレンス 定義編」を，コマンドについては，マニュアル「Cosminexus リファレンス コマンド編」を参照してください。Web サーバが提供するファイルおよびコマンドについては，マニュアル「Hitachi Web Server」を参照してください。

また，このマニュアルで説明する運用作業に必要なファイルとコマンドの記述形式，および関連マニュアルとの対応については，「7. リファレンス」を参照してください。

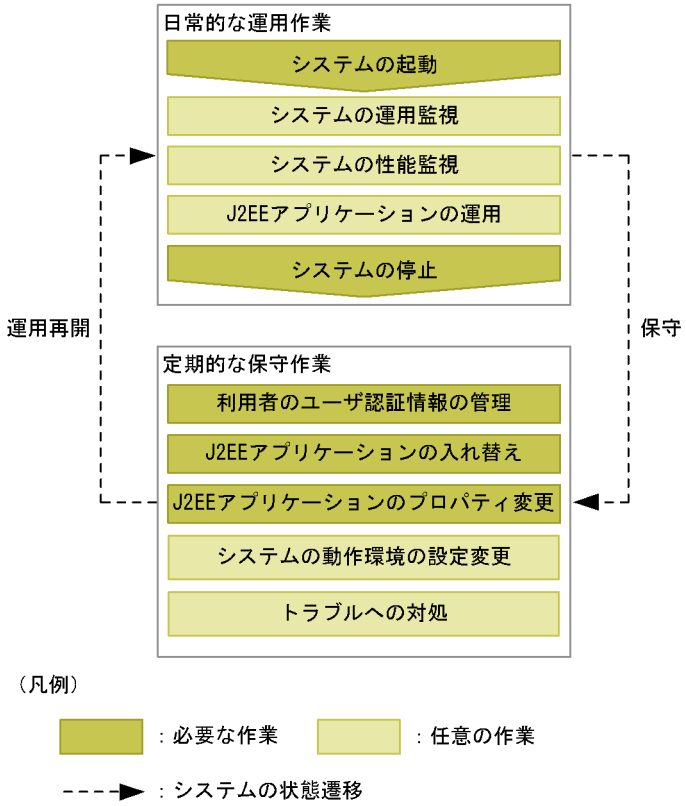
6 システムの運用

運用前の準備作業が完了したら，システムの運用を開始します。
この章では，システム運用に必要な作業のうち，アプリケーションサーバをセキュアに保つために必要な作業について説明します。

6.1　システム運用の概要

Cosminexus のシステム運用では，日常的な運用作業と定期的な保守作業を繰り返します。Cosminexus のシステムの運用サイクルを次の図に示します。

図 6-1　システムの運用サイクル



図中に示した「必要な作業」とは，Application Server のセキュリティ機能を使用してアプリケーションサーバをセキュアに保つために必要な作業のことです。

ここでは，アプリケーションサーバをセキュアに保つために必要な作業の概要について説明します。

日常的な運用作業

アプリケーションサーバをセキュアに保つために必要な，日常的な運用作業の概要を次に示します。ほかの運用作業については，マニュアル「Cosminexus システム運用ガイド」の「1.4　システム運用の作業」を参照してください。

- システムの起動
  運用を開始するときに実施する作業です。このマニュアルでは，アプリケーションサーバを起動し，J2EE アプリケーションを通常モードで開始する手順を説明し

ます。

- システムの停止
  運用を終了するときに実施する作業です。このマニュアルでは，アプリケーションサーバを停止し，J2EE アプリケーションを通常モードで停止する手順を説明します。

定期的な保守作業

アプリケーションサーバをセキュアに保つために必要な，定期的な保守作業の概要を次に示します。ほかの保守作業については，マニュアル「Cosminexus システム運用ガイド」の「1.5　システム保守の作業」を参照してください。

- 利用者のユーザ認証情報の管理
  利用者を追加・削除する場合，パスワードを変更する場合，セキュリティロールの構成を変更する場合などに，必要に応じて実施します。
- J2EE アプリケーションの入れ替え
  J2EE アプリケーションの仕様が変更されたり，バージョンアップされたりした場合に実施します。このマニュアルでは，アーカイブ形式の J2EE アプリケーションを入れ替える手順を説明します。
- J2EE アプリケーションのプロパティ変更
  社内の職制が変更になった場合，J2EE アプリケーションを入れ替える場合などに，必要に応じて実施します。

注意事項

ここで説明する運用・保守作業を実施する場合や，システム構成を変更する作業を実施する場合，「1.3　構築・運用に当たってのセキュリティポリシー」で制定したセキュリティポリシーに従ってください。

6.2 システムの起動，停止

ここでは，システムを起動する方法，および停止する方法について説明します。

6.2.1 システムの起動

システムの起動手順を次に示します。

1. cprfstart **コマンドで** PRF **デーモンを起動します。**

```
cprfstart
```

コマンド実行後，メッセージ（KFCT73412-I）で PRF デーモンが起動されたことを確認してください。

2. cjstartsv **コマンドで** J2EE **サーバを起動します。**

```
cjstartsv
```

コマンド実行後，メッセージ（KDJE30028-I）で起動した J2EE サーバ名に誤りがないことを確認してください。

3. **別のコマンドプロンプトを開きます。**
これまで使用していたコマンドプロンプトは，閉じないでそのままにしておいてください。

4. cjstartapp **コマンドで** J2EE **アプリケーションを開始します。**

```
cjstartapp -name <J2EEアプリケーション名>
```

コマンド実行後，メッセージ（KDJE37045-I）で開始した J2EE アプリケーション名に誤りがないことを確認してください。

5. cjlistapp **コマンドで** J2EE **アプリケーションの稼働状況を確認します。**

```
cjlistapp
```

コマンド実行後，開始した J2EE アプリケーションの状態が「running」であることを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

6. Hitachi Web Server **を起動します。**
   - Windows **の場合**
     httpsd コマンドで起動します。

```
httpsd -k start
```

コマンド実行後，「The Hitachi Web Server service is running.」というメッセージ

が出力されることを確認してください。

- **UNIX の場合**

  httpsdctl ユティリティで起動します。

```
httpsdctl start
```

ユティリティ実行後，OS の ps コマンドを実行して Hitachi Web Server の制御プロセス ID が起動状態であることを確認してください。

6.2.2 システムの停止

システムの停止手順を次に示します。

1. **Hitachi Web Server を停止します。**

   - **Windows の場合**

     httpsd コマンドで停止します。

```
httpsd -k stop
```

コマンド実行後，「The Hitachi Web Server service has stopped.」というメッセージが出力されることを確認してください。

- **UNIX の場合**

  httpsdctl ユティリティで停止します。

```
httpsdctl stop
```

ユティリティ実行後，OS の ps コマンドを実行して Hitachi Web Server の制御プロセス ID が表示されないことを確認してください。

2. **cjstopapp コマンドで J2EE アプリケーションを停止します。**

```
cjstopapp -name <J2EEアプリケーション名>
```

コマンド実行後，メッセージ（KDJE37046-I）で停止した J2EE アプリケーション名に誤りがないことを確認してください。

3. **cjlistapp コマンドで J2EE アプリケーションの稼働状況を確認します。**

```
cjlistapp
```

コマンド実行後，停止した J2EE アプリケーションの状態が「stopped」であることを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

4. **cjstopsv コマンドで J2EE サーバを停止します。**

```
cjstopsv
```

コマンド実行後，メッセージ（KDJE30034-I）で停止した J2EE サーバ名に誤りがないことを確認してください。

5. cprfstop コマンドで PRF デーモンを停止します。

```
cprfstop
```

コマンド実行後，メッセージ（KFCT73414-I）が出力されることを確認してください。

6.3 利用者のユーザ認証情報の管理

ここでは，利用者のユーザ認証情報の管理作業について説明します。利用者のユーザ認証情報の管理作業を実施するのは，次のような場合です。

- 利用者を追加，削除する場合
- 利用者のパスワードを変更する場合
- 利用者にマッピングする所属ロールを追加，削除する場合
- システムで使用する所属ロールを追加，削除する場合

注意事項

ここで説明する作業を実施するときは，Web サーバおよび J2EE アプリケーションを停止する必要があります。あらかじめ業務サービスが停止する期間を利用者に通知しておいてください。
なお，Web サーバおよび J2EE アプリケーションの停止手順については，「6.2.2　システムの停止」の手順 1. ～手順 3. を参照してください。

6.3.1 利用者の追加

利用者の追加手順を次に示します。

1. cjaddsec **コマンドで追加する利用者のユーザ** ID **およびパスワードを登録します。**

```
cjaddsec -type user -name <ユーザID> -password <パスワード>
```

コマンド実行後，メッセージ（KDJE37503-I）で登録したユーザ ID に誤りがないことを確認してください。

2. cjmapsec **コマンドで追加した利用者のユーザ** ID **に所属ロールをマッピングします。**

```
cjmapsec -role <所属ロール名> -user <ユーザID>
```

コマンド実行後，メッセージ（KDJE37514-I）でマッピングしたユーザ ID に誤りがないことを確認してください。複数の所属ロールをマッピングするときは，所属ロールの数だけコマンドを実行してください。

3. cjlistsec **コマンドで登録結果を確認します。**

```
cjlistsec -type user -name <ユーザID>
```

コマンド実行後，表示された所属ロール一覧に，ユーザ ID にマッピングした所属ロールがあることを確認してください。また，メッセージ（KDJE37509-I）が出力されることを確認してください。

注意事項

パスワードが正しく登録されたかどうかを確認するコマンドはありません。cjaddsec コマンド実行時，指定したパスワードに誤りがないかを十分確認してください。

6.3.2 利用者の削除

利用者をシステムから削除するには，削除する利用者のユーザ ID を削除します。このとき，ユーザ ID とともにパスワードや所属ロールとのマッピングの情報も削除されます。

利用者の削除手順を次に示します。

1. cjdeletesec **コマンドで削除する利用者のユーザ** ID **を削除します。**

```
cjdeletesec -type user -name <ユーザID>
```

コマンド実行後，メッセージ（KDJE37504-I）で削除したユーザ ID に誤りがないことを確認してください。

2. cjlistsec **コマンドで削除結果を確認します。**

```
cjlistsec -type user
```

コマンド実行後，表示されたユーザ ID 一覧に，削除した利用者のユーザ ID がないことを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

6.3.3 利用者のパスワード変更

利用者のパスワードを変更するには，いったん，対象の利用者を削除したあと，変更後のパスワードで登録し直します。

パスワードの変更手順を次に示します。

1. **パスワードを変更する利用者を削除します。**
   利用者の削除手順については，「6.3.2　利用者の削除」を参照してください。
2. **パスワードを変更する利用者を再度追加します。**
   変更後のパスワードを指定して，利用者を再度追加します。利用者の追加手順については，「6.3.1　利用者の追加」を参照してください。

6.3.4 ユーザ ID と所属ロールのマッピング追加

ユーザ ID と所属ロールのマッピングを追加する手順を次に示します。

1. cjmapsec **コマンドで利用者のユーザ** ID **と所属ロールをマッピングします。**

```
cjmapsec -role <所属ロール名> -user <ユーザID>
```

コマンド実行後，メッセージ（KDJE37514-I）でマッピングしたユーザ ID に誤りがないことを確認してください。
一つの所属ロールに対して複数のユーザ ID をマッピングするときは，「-user」オプションを複数指定してコマンドを実行してください。また，一つのユーザ ID に対して複数の所属ロールをマッピングするときは，所属ロールの数だけコマンドを実行してください。

2. cjlistsec **コマンドで登録結果を確認します。**
   次のどちらかの方法で確認してください。
   - あるユーザ ID にマッピングされている全所属ロールを表示する方法

```
cjlistsec -type user -name <ユーザID>
```

コマンド実行後，表示された所属ロール一覧に，マッピングを追加した所属ロールがあることを確認してください。また，メッセージ（KDJE37509-I）が出力されることを確認してください。

   - ある所属ロールにマッピングされている全ユーザ ID を表示する方法

```
cjlistsec -type role -name <所属ロール名>
```

コマンド実行後，表示されたユーザ ID 一覧に，マッピングを追加したユーザ ID があることを確認してください。また，メッセージ（KDJE37509-I）が出力されることを確認してください。

6.3.5 ユーザ ID と所属ロールのマッピング削除

利用者にマッピングした所属ロールを削除するには，利用者のユーザ ID と削除する所属ロールをアンマッピングします。

利用者にマッピングした所属ロールの削除手順を次に示します。

1. cjunmapsec **コマンドで利用者のユーザ** ID **と削除する所属ロールをアンマッピングします。**

```
cjunmapsec -role <所属ロール名> -user <ユーザID>
```

コマンド実行後，メッセージ（KDJE37515-I）でアンマッピングしたユーザ ID に誤りがないことを確認してください。
一つの所属ロールに対して複数のユーザ ID をアンマッピングするときは，「-user」オプションを複数指定してコマンドを実行してください。また，一つのユーザ ID に対して複数の所属ロールをアンマッピングするときは，所属ロールの数だけコマンドを実行してください。

2. cjlistsec **コマンドで削除結果を確認します。**
   次のどちらかの方法で確認してください。
   - あるユーザ ID にマッピングされている全所属ロールを表示する方法

```
cjlistsec -type user -name <ユーザID>
```

   コマンド実行後，表示された所属ロール一覧に，マッピングを削除した所属ロールがないことを確認してください。また，メッセージ（KDJE37509-I）が出力されることを確認してください。
   - ある所属ロールにマッピングされている全ユーザ ID を表示する方法

```
cjlistsec -type role -name <所属ロール名>
```

   コマンド実行後，表示されたユーザ ID 一覧に，マッピングを削除したユーザ ID がないことを確認してください。また，メッセージ（KDJE37509-I）が出力されることを確認してください。

6.3.6 システムで使用する所属ロールの追加

ここでは，システムで使用する所属ロール追加時の操作手順，およびコマンド実行の流れについて説明します。

なお，所属ロールを追加した場合，セキュリティロールの構成（所属ロールから許可ロールへのロール変換）を見直し，J2EE アプリケーションのプロパティ変更をしてください。J2EE アプリケーションのプロパティ変更については，「6.5 J2EE アプリケーションのプロパティ変更」を参照してください。

システムで使用する所属ロール追加時の操作手順を次に示します。

1. cjaddsec **コマンドで所属ロールを登録します。**

```
cjaddsec -type role -name <所属ロール名>
```

   コマンド実行後，メッセージ（KDJE37503-I）で登録した所属ロールに誤りがないことを確認してください。

2. cjlistsec **コマンドで登録結果を確認します。**

```
cjlistsec -type role
```

   コマンド実行後，表示された所属ロール一覧に，登録した所属ロールがあることを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

6.3.7 システムで使用する所属ロールの削除

システムで使用する所属ロールを削除すると，削除対象の所属ロールにマッピングされている利用者はアンマッピングされます。ここでは，システムで使用する所属ロール削除時の操作手順について説明します。

なお，所属ロールを削除した場合，セキュリティロールの構成（所属ロールから許可ロールへのロール変換）を見直し，J2EE アプリケーションのプロパティ変更をしてください。J2EE アプリケーションのプロパティ変更については，「6.5　J2EE アプリケーションのプロパティ変更」を参照してください。

システムで使用する所属ロール削除時の操作手順を次に示します。

1. cjdeletesec **コマンドで所属ロールを削除します。**

```
cjdeletesec -type role -name <所属ロール名>
```

コマンド実行後，メッセージ（KDJE37504-I）で削除した所属ロールに誤りがないことを確認してください。

2. cjlistsec **コマンドで削除結果を確認します。**

```
cjlistsec -type role
```

コマンド実行後，表示された所属ロール一覧に，削除した所属ロールがないことを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

6.4 J2EE アプリケーションの入れ替え

J2EE アプリケーションの仕様が変更されたり，バージョンアップされたりした場合，J2EE アプリケーションの入れ替え作業を実施します。ここでは，古い J2EE アプリケーションをいったん削除したあと，新しい J2EE アプリケーションをインポートする手順について説明します。

注意事項

ここで説明する作業を実施するときは，Web サーバおよび J2EE アプリケーションを停止する必要があります。あらかじめ業務サービスが停止する期間を利用者に通知しておいてください。

J2EE アプリケーション入れ替え時の操作手順を次に示します。

操作手順

1. Hitachi Web Server を停止します。
   - Windows の場合

     httpsd コマンドで停止します。

```
httpsd -k stop
```

     コマンド実行後，「The Hitachi Web Server service has stopped.」というメッセージが出力されることを確認してください。
   - UNIX の場合

     httpsdctl ユティリティで停止します。

```
httpsdctl stop
```

     ユティリティ実行後，OS の ps コマンドを実行して Hitachi Web Server の制御プロセス ID が表示されないことを確認してください。
2. cjstopapp コマンドで J2EE アプリケーションを停止します。

```
cjstopapp -name <J2EEアプリケーション名>
```

   コマンド実行後，メッセージ（KDJE37046-I）で停止した J2EE アプリケーション名に誤りがないことを確認してください。
3. cjdeleteapp コマンドで停止した J2EE アプリケーションを削除します。

```
cjdeleteapp -name <J2EEアプリケーション名>
```

   コマンド実行後，メッセージ（KDJE37047-I）で削除した J2EE アプリケーション名に誤りがないことを確認してください。

4. cjlistapp **コマンドで** J2EE **アプリケーションの稼働状況を確認します。**

```
cjlistapp
```

コマンド実行後，削除した J2EE アプリケーションが表示されないことを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

5. cjimportapp **コマンドで入れ替える** J2EE **アプリケーションをインポートします。**

```
cjimportapp -f <EARファイルパス>
```

コマンド実行後，メッセージ（KDJE37041-I）でインポートした J2EE アプリケーション名に誤りがないことを確認してください。

6. **入れ替えた** J2EE **アプリケーションのプロパティ設定をします。**
プロパティの設定手順については，「6.5.1　J2EE アプリケーションのプロパティ変更手順」の手順 4. ～手順 6. を参照してください。

7. **入れ替えた** J2EE **アプリケーションの動作確認をします。**
動作確認手順については，「6.5.1　J2EE アプリケーションのプロパティ変更手順」の手順 7. ～手順 11. を参照してください。

6.5 J2EE アプリケーションのプロパティ変更

社内の職制が変更になった場合や J2EE アプリケーションを入れ替える場合，J2EE アプリケーションのプロパティを変更します。J2EE アプリケーションのプロパティを変更するには，J2EE アプリケーションの属性ファイルを編集したあと，編集した内容を J2EE アプリケーションに反映する必要があります。

ここでは，次に示す変更の手順，および属性ファイルの編集内容について説明します。

- ユーザ認証方式の変更
- セキュリティロールの構成変更

6.5.1 J2EE アプリケーションのプロパティ変更手順

J2EE アプリケーションのプロパティ変更時の操作手順を次に示します。

1. Hitachi Web Server を停止します。
   - Windows の場合
     httpsd コマンドで停止します。

```
httpsd -k stop
```

     コマンド実行後，「The Hitachi Web Server service has stopped.」というメッセージが出力されることを確認してください。
   - UNIX の場合
     httpsdctl ユティリティで停止します。

```
httpsdctl stop
```

     ユティリティ実行後，OS の ps コマンドを実行して Hitachi Web Server の制御プロセス ID が表示されないことを確認してください。
2. cjstopapp コマンドで J2EE アプリケーションを停止します。

```
cjstopapp -name <J2EEアプリケーション名>
```

   コマンド実行後，メッセージ（KDJE37046-I）で停止した J2EE アプリケーション名に誤りがないことを確認してください。
3. cjlistapp コマンドで J2EE アプリケーションの稼働状況を確認します。

```
cjlistapp
```

   コマンド実行後，停止した J2EE アプリケーションの状態が「stopped」であることを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認し

てください。

4. cjgetappprop **コマンドで属性ファイルを取得します。**
   - EJB-JAR 属性ファイルを取得する場合

```
cjgetappprop -name <J2EEアプリケーション名> -type ejb -resname <EJB-JARの表示名> -c
<属性ファイルの出力先パス>
```

   コマンド実行後，メッセージ（KDJE37505-I）で，プロパティを取得した EJB-JAR の表示名が正しいことを確認してください。
   - Session Bean 属性ファイルを取得する場合

```
cjgetappprop -name <J2EEアプリケーション名> -type ejb -resname <EJB-JARの表示名>/
<Session Beanの表示名> -c <属性ファイルの出力先パス>
```

   コマンド実行後，メッセージ（KDJE37505-I）で，プロパティを取得した EJB-JAR の表示名と Session Bean の表示名が正しいことを確認してください。
   - WAR 属性ファイルを取得する場合

```
cjgetappprop -name <J2EEアプリケーション名> -type war -resname <WARの表示名> -c <属
性ファイルの出力先パス>
```

   コマンド実行後，メッセージ（KDJE37505-I）で，プロパティを取得した WAR の表示名が正しいことを確認してください。

5. **取得した属性ファイルを編集して，プロパティを変更します。**
   変更後のユーザ認証方式，またはセキュリティロールの構成に合わせて，属性ファイルを編集します。編集内容については，「6.5.2　属性ファイルの編集内容」を参照してください。

6. cjsetappprop **コマンドで属性ファイルの内容を** J2EE **アプリケーションに反映します。**
   - EJB-JAR 属性ファイルの内容を反映する場合

```
cjsetappprop -name <J2EEアプリケーション名> -type ejb -resname <EJB-JARの表示名> -c
<属性ファイルのパス>
```

   コマンド実行後，メッセージ（KDJE37506-I）で，プロパティを設定した EJB-JAR の表示名が正しいことを確認してください。
   - Session Bean 属性ファイルの内容を反映する場合

```
cjsetappprop -name <J2EEアプリケーション名> -type ejb -resname <EJB-JARの表示名>/
<Session Beanの表示名> -c <属性ファイルのパス>
```

   コマンド実行後，メッセージ（KDJE37506-I）で，プロパティを設定した EJB-JAR の表示名と Session Bean の表示名が正しいことを確認してください。
   - WAR 属性ファイルの内容を反映する場合

```
cjsetappprop -name <J2EEアプリケーション名> -type war -resname <WARの表示名> -c <属性ファイルのパス>
```

コマンド実行後，メッセージ（KDJE37506-I）で，プロパティを設定した WAR の表示名が正しいことを確認してください。

7. cjstartapp **コマンドで** J2EE **アプリケーションを開始します。**

```
cjstartapp -name <J2EEアプリケーション名>
```

コマンド実行後，メッセージ（KDJE37045-I）で開始した J2EE アプリケーション名に誤りがないことを確認してください。

8. cjlistapp **コマンドで** J2EE **アプリケーションの稼働状況を確認します。**

```
cjlistapp
```

コマンド実行後，開始した J2EE アプリケーションの状態が「running」であることを確認してください。また，メッセージ（KDJE37508-I）が出力されることを確認してください。

9. Hitachi Web Server **を起動します。**
   - Windows **の場合**

     httpsd コマンドで起動します。

```
httpsd -k start
```

     コマンド実行後，「The Hitachi Web Server service is running.」というメッセージが出力されることを確認してください。
   - UNIX **の場合**

     httpsdctl ユティリティで起動します。

```
httpsdctl start
```

     ユティリティ実行後，OS の ps コマンドを実行して Hitachi Web Server の制御プロセス ID が起動状態であることを確認してください。

10. **アプリケーションサーバのマシンから** J2EE **アプリケーションの** URL **にアクセスします。**

ユーザ認証方式を変更した場合，変更後の認証方式のログイン画面が表示されることを確認してください。アクセスできなかった場合，または変更後の認証方式のログイン画面が表示されなかった場合は，「4.10.2(2)　見直しの観点」に従って操作し直してください。

11. **必要に応じて，ユーザ認証およびアクセス制御の確認をします。**

セキュリティロールの構成を変更した場合，ユーザ認証およびアクセス制御の確認をして，変更内容が正しく反映されているかどうかを確認してください。

ユーザ認証およびアクセス制御の確認方法の詳細については，「4.10.3　ユーザ認証とアクセス制御の設定確認」を参照してください。

6.5.2　属性ファイルの編集内容

J2EE アプリケーションのプロパティ変更時に検討する必要がある項目と，属性ファイルの編集個所の対応を，次に示します。

（1）ユーザ認証方式の変更

WAR 属性ファイルの <login-config> タグを編集します。認証方式や認証時に必要な情報を設定します。

HTTP（Form）認証に変更する場合，あらかじめ認証インタフェースが準備されている必要があります。

（2）セキュリティロールの構成変更

J2EE アプリケーションの許可ロール

- Web アプリケーションの許可ロールと URL パターンの構成
  WAR 属性ファイルの <security-constraint> タグを編集します。各 URL パターンに許可ロールを対応づけます。
- EJB の許可ロールとメソッドの構成
  Session Bean 属性ファイルの <method-permission> タグを編集します。各許可ロールにメソッドを対応づけます。

システムで使用する所属ロール

属性ファイルの編集は不要です。
システムで使用する所属ロールは，サーバ管理コマンドの実行によって変更します。
システムで使用する所属ロールの追加方法については「6.3.6　システムで使用する所属ロールの追加」を，削除方法については「6.3.7　システムで使用する所属ロールの削除」を参照してください。

所属ロールから許可ロールへのロール変換

- Web アプリケーションの許可ロールと，アクセスを許可する所属ロールの対応づけ
  WAR 属性ファイルの <security-role> タグを編集します。各許可ロールと所属ロールとを対応づけます。
- EJB の許可ロールと，アクセスを許可する所属ロールの対応づけ
  EJB-JAR 属性ファイルの <security-role> を編集します。各許可ロールと所属ロールとを対応づけます。

7 リファレンス

この章では，Cosminexus が提供するファイルおよびコマンドのうち，このマニュアルで説明する操作に必要なものを一覧で説明します。また，Application Server のセキュリティ機能で使用するファイルやコマンドの詳細について説明します。

7.1 ファイル

ここでは，システム構築・運用で使用するファイルのうち，このマニュアルで説明する操作に必要なファイルを一覧で示します。また，属性ファイルについて，編集，追加する必要がある項目を説明します。

このマニュアルで説明しないファイルについては，次のマニュアルを参照してください。

● マニュアル「Cosminexus リファレンス 定義編」

● マニュアル「Hitachi Web Server」

7.1.1 このマニュアルで説明する操作に必要なファイル一覧

このマニュアルで説明する操作に必要なファイル一覧を，次の表に示します。

表 7-1 このマニュアルで説明する操作に必要なファイル一覧

項番	ファイル名	ファイルの用途	詳細な説明の参照先
1	EJB-JAR 属性ファイル	**J2EE アプリケーションのプロパティ設定** EJB の属性を編集して，Application Server のセキュリティ機能の設定をします。	「7.1.2 EJB-JAR 属性ファイル」
2	httpsd.conf	**Web サーバとの連携の設定** • Hitachi Web Server の動作環境を設定します。 • SSL 通信の設定をします。	マニュアル「Hitachi Web Server」の「7. ディレクティブ」
3	mod_jk.conf	**Web サーバとの連携の設定** URL パターンとワーカのマッピングを定義します。	マニュアル「Cosminexus リファレンス 定義編」の「4.3 mod_jk.conf (Hitachi Web Server 用リダイレクタ動作定義ファイル)」にあるマッピング定義の説明
4	Session Bean 属性ファイル	**J2EE アプリケーションのプロパティ設定** Session Bean の属性を編集して，Application Server のセキュリティ機能の設定をします。	「7.1.3 Session Bean 属性ファイル」
5	usrconf.properties	**J2EE サーバの動作設定のカスタマイズ** • EJB コンテナのポート番号と IP アドレスを固定します。 • Management Server の使用有無を設定します。	マニュアル「Cosminexus リファレンス 定義編」の「2.4 usrconf.properties (J2EE サーバ用ユーザプロパティファイル)」

項番	ファイル名	ファイルの用途	詳細な説明の参照先
6	usrconf.properties	J2EE サーバの動作設定のカスタマイズ サーバ管理コマンドの接続先の設定をします。	マニュアル「Cosminexus リファレンス 定義編」の「2.10　usrconf.properties（サーバ管理コマンド用システムプロパティファイル）」
7	WAR 属性ファイル	J2EE アプリケーションのプロパティ設定 Web アプリケーションの属性を編集して，Application Server のセキュリティ機能の設定をします。	「7.1.4　WAR 属性ファイル」

7.1.2　EJB-JAR 属性ファイル

EJB-JAR 属性ファイルは，EJB の属性を編集するためのファイルです。このマニュアルで説明するシステムでは，Application Server のセキュリティ機能を使用するために，次の内容を設定します。

● EJB の許可ロールとシステムで使用する所属ロールの対応

Application Server のセキュリティ機能の設定に必要なタグを，次の表に示します。

表 7-2　Application Server のセキュリティ機能の設定に必要なタグ（EJB-JAR 属性ファイル）

項番	タグ名	説明
1	<security-role>	－
2	<role-name>	EJB の許可ロールを指定します。J2EE アプリケーションが持つ EJB の全許可ロールを，それぞれ指定する必要があります。
3	<linked-to>	<role-name> タグに指定した許可ロールに対応する所属ロールを指定します。
4	</security-role>	－

（凡例）－：開始タグまたは終了タグです。値は設定しません。
注　<security-role> タグ下のタグのうち，セキュリティ設定に関係ないタグは省略しています。

ここで説明しない EJB-JAR 属性ファイルの説明については，マニュアル「Cosminexus リファレンス 定義編」の「8.4　EJB-JAR 属性ファイル」を参照してください。

7.1.3　Session Bean 属性ファイル

Session Bean 属性ファイルは，Session Bean の属性を編集するためのファイルです。このマニュアルで説明するシステムでは，Application Server のセキュリティ機能を使用するために，次の内容を設定します。

● EJB の許可ロールとメソッドの対応

Application Server のセキュリティ機能の設定に必要なタグを，次の表に示します。

表 7-3　Application Server のセキュリティ機能の設定に必要なタグ（Session Bean 属性ファイル）

項番	タグ名	説明
1	<method-permission>	—
2	<role-name>	EJB の許可ロール名を指定します。J2EE アプリケーションが持つ EJB の全許可ロールを，それぞれ指定する必要があります。
3	<method>	—
4	<method-intf>	<method-name> タグに指定した EJB のメソッドが属するインタフェース種別を指定します。 このタグを省略した場合，すべての種別が指定されます。
5	<method-name>	<role-name> タグに指定した許可ロールに対応する EJB のメソッド名を指定します。 「*」を指定した場合，すべてのメソッドを表します。
6	<method-params>	<method-name> タグに「*」以外を指定した場合で，パラメタが異なる同名メソッドを区別するときに指定します。 <method-name> タグに指定した EJB のメソッドのパラメタを指定します。 このタグを省略した場合，<method-intf> タグに指定したインタフェースに属し，かつ <method-name> タグに指定したメソッド名を持つすべての EJB メソッドが指定されます。
7	<method-param>	<method-params> タグに指定したパラメタのデータ型を指定します。 このタグは省略できます。
8	</method-params>	—
9	</method>	—
10	</method-permission>	—

（凡例）－：開始タグまたは終了タグです。値は設定しません。
注　<method-permission> タグ下のタグのうち，セキュリティ設定に関係ないタグは省略しています。

ここで説明しない Session Bean 属性ファイルの説明については，マニュアル「Cosminexus リファレンス 定義編」の「8.5　Session Bean 属性ファイル」を参照してください。

7.1.4　WAR 属性ファイル

WAR 属性ファイルは，WAR の属性を編集するためのファイルです。このマニュアルで

説明するシステムでは，Application Server のセキュリティ機能を使用するために，次の内容を設定します。

● ユーザ認証方式

● Web アプリケーションの許可ロールと URL パターンの対応

● Web アプリケーションの許可ロールとシステムで使用する所属ロールの対応

Application Server のセキュリティ機能の設定に必要なタグを，次の表に示します。

表 7-4 Application Server のセキュリティ機能の設定に必要なタグ（WAR 属性ファイル）

項番	タグ名	説明
1	<login-config>	—
2	<auth-method>	ユーザ認証方式を指定します。次のどちらかを指定してください。 • BASIC • FORM このタグを省略した場合，「BASIC」が指定されます。
3	<realm-name>	<auth-method> タグに「BASIC」を指定した場合に，レルム名（<login-config> タグに設定した情報の識別子）として任意の値を設定します。Web ブラウザのユーザ認証画面などで表示されます。 <auth-method> タグに「BASIC」を指定した場合，このタグは省略できません。
4	<form-login-config>	—
5	<form-login-page>	<auth-method> タグに「FORM」を指定した場合に，ログイン時の認証ページの URL を指定します。 <auth-method> タグに「FORM」を指定した場合，このタグは省略できません。
6	<form-error-page>	<auth-method> タグに「FORM」を指定した場合に，ログイン時の認証エラーページの URL を指定します。 <auth-method> タグに「FORM」を指定した場合，このタグは省略できません。
7	</form-login-config>	—
8	</login-config>	—
9	<security-constraint>	—
10	<web-resource-collection>	—
11	<web-resource-name>	Web リソース名（<web-resource-collection> タグで設定する情報の識別子）として，任意の値を設定します。 このタグは省略できません。

項番	タグ名	説明
12	<url-pattern>	<security-constraint> タグでの設定を有効にする URL パターンを指定します。J2EE アプリケーションが持つ全 URL パターンを，それぞれ指定する必要があります。
13	<http-method>	<security-constraint> タグでの設定を有効にする HTTP メソッドの種別を指定します。 このタグを省略した場合，すべての種別に対して設定が有効になります。
14	</web-resource-collection>	—
15	<auth-constraint>	—
16	<role-name>	<url-pattern> タグに指定した URL パターンに対応する Web アプリケーションの許可ロール名を指定します。
17	</auth-constraint>	—
18	</security-constraint>	—
19	<security-role>	—
20	<role-name>	Web アプリケーションの許可ロールを指定します。J2EE アプリケーションが持つ Web アプリケーションの全許可ロールを，それぞれ指定する必要があります。
21	<linked-to>	<role-name> タグに指定した許可ロールに対応する所属ロールを指定します。
22	</security-role>	—

（凡例）—：開始タグまたは終了タグです。値は設定しません。
注　<login-config> タグ，<security-constraint> タグ，および <security-role> タグ下のタグのうち，セキュリティ設定に関係ないタグは省略しています。

ここで説明しない WAR 属性ファイルの説明については，マニュアル「Cosminexus リファレンス 定義編」の「8.8　WAR 属性ファイル」を参照してください。

7.2 コマンド

ここでは，システム構築・運用で使用するコマンドのうち，このマニュアルで説明する操作に必要なコマンドを一覧で示します。また，Application Server のセキュリティ機能の設定に必要なコマンドについて，記述形式や機能を説明します。

コマンドの入力形式，およびこのマニュアルで説明しないコマンドについては，次のマニュアルを参照してください。

● マニュアル「Cosminexus リファレンス コマンド編」

● マニュアル「Hitachi Web Server」

7.2.1 このマニュアルで説明する操作に必要なコマンド一覧

このマニュアルで説明する操作に必要なコマンド一覧を，次の表に示します。

表 7-5 このマニュアルで説明する操作に必要なコマンド一覧

項番	コマンド名	コマンドの用途	詳細な説明の参照先
1	cjaddsec	**ユーザ認証情報の設定，管理** • 利用者（ユーザ ID，パスワード）を追加します。 • システムで使用する所属ロールを追加します。	「7.2.2(1) cjaddsec（利用者のユーザ認証情報の登録）」
2	cjdeleteapp	J2EE **アプリケーションの入れ替え** J2EE アプリケーションを削除します。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2 J2EE サーバで使用するコマンドの詳細」
3	cjdeletesec	**ユーザ認証情報の設定，管理** • 利用者（ユーザ ID，パスワード）を削除します。 • システムで使用する所属ロールを削除します。	「7.2.2(2) cjdeletesec（利用者のユーザ認証情報の削除）」
4	cjgetappprop	J2EE **アプリケーションのプロパティ設定** J2EE アプリケーションの属性ファイルを取得します。	「7.2.3(1) cjgetappprop（属性ファイルの取得）」
5	cjimportapp	J2EE **アプリケーションのインポート** J2EE アプリケーションを J2EE サーバにインポートします。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2 J2EE サーバで使用するコマンドの詳細」
6	cjlistapp	J2EE **アプリケーションの一覧表示** J2EE サーバに登録されている J2EE アプリケーションを一覧表示します。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2 J2EE サーバで使用するコマンドの詳細」

項番	コマンド名	コマンドの用途	詳細な説明の参照先
7	cjlistsec	**ユーザ認証情報の設定，管理** • J2EE サーバに登録されている全ユーザ ID を一覧表示します。 • J2EE サーバに登録されている全所属ロールを一覧表示します。 • あるユーザ ID にマッピングされている全所属ロールを一覧表示します。 • ある所属ロールにマッピングされている全ユーザ ID を一覧表示します。	「7.2.2(3)　cjlistsec（利用者のユーザ認証情報の一覧表示）」
8	cjmapsec	**ユーザ認証情報の設定，管理** ユーザ ID と所属ロールのマッピングを追加します。	「7.2.2(4)　cjmapsec（ユーザ ID と所属ロールのマッピング）」
9	cjsetappprop	J2EE **アプリケーションのプロパティ設定** J2EE アプリケーションの属性ファイルの内容を J2EE アプリケーションに反映して，Application Server のセキュリティ機能の設定をします。	「7.2.3(2)　cjsetappprop（属性ファイルの内容の反映）」
10	cjstartapp	**システムの起動** J2EE アプリケーションを開始します。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2　J2EE サーバで使用するコマンドの詳細」
11	cjstopapp	**システムの停止** J2EE アプリケーションを停止します。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2　J2EE サーバで使用するコマンドの詳細」
12	cjunmapsec	**ユーザ認証情報の設定，管理** ユーザ ID と所属ロールをアンマッピングします。	「7.2.2(5)　cjunmapsec（ユーザ ID と所属ロールのアンマッピング）」
13	cjstartsv	**システムの起動** J2EE サーバを起動します。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2　J2EE サーバで使用するコマンドの詳細」
14	cjstopsv	**システムの停止** J2EE サーバを停止します。	マニュアル「Cosminexus リファレンス コマンド編」の「2.2　J2EE サーバで使用するコマンドの詳細」
15	cprfstart	**システムの起動** PRF デーモンを起動します。	マニュアル「Cosminexus リファレンス コマンド編」の「3.2　性能解析トレースで使用するコマンドの詳細」
16	cprfstop	**システムの停止** PRF デーモンを停止します。	マニュアル「Cosminexus リファレンス コマンド編」の「3.2　性能解析トレースで使用するコマンドの詳細」

項番	コマンド名	コマンドの用途	詳細な説明の参照先
17	httpsd	**システムの起動** Windows の場合に，Hitachi Web Server を起動します。 **システムの停止** Windows の場合に，Hitachi Web Server を停止します。	マニュアル「Hitachi Web Server」の「3.4.1(3) コマンドプロンプトからの起動，停止，及び再起動」
18	httpsdctl	**システムの起動** UNIX の場合に，Hitachi Web Server を起動します。 **システムの停止** UNIX の場合に，Hitachi Web Server を停止します。	マニュアル「Hitachi Web Server」の「2.4.1 Hitachi Web Server を起動，停止する（httpsdctl ユティリティ）」

7.2.2 ユーザ認証情報の設定，管理で使用するコマンド

ここでは，利用者のユーザ認証情報の設定，管理で使用するコマンドについて説明します。各コマンドの引数，入力例，戻り値，および注意事項の詳細については，マニュアル「Cosminexus リファレンス コマンド編」の「2.2 J2EE サーバで使用するコマンドの詳細」を参照してください。

ユーザ認証情報の設定，管理で使用するコマンドの格納先を次に示します。

Windows の場合

```
<Cosminexusのインストールディレクトリ>¥CC¥admin¥bin¥
```

UNIX の場合

```
/opt/Cosminexus/CC/admin/bin/
```

（1）cjaddsec（利用者のユーザ認証情報の登録）

ここでは，cjaddsec コマンドの形式，機能，および注意事項について説明します。

形式

利用者を追加する場合

```
cjaddsec [<J2EEサーバ名>] -type user -name <ユーザID> -password
<パスワード>
```

所属ロールを追加する場合

```
cjaddsec [<J2EEサーバ名>] -type role -name <所属ロール名>
```

機能

利用者のユーザ認証情報を，J2EE サーバに登録するコマンドです。利用者を追加したり，システムで使用する所属ロールを追加したりするときに使用します。このコマンドで登録できる情報の種別を次に示します。

- ユーザ ID およびパスワード

  利用者を追加する場合に指定する情報です。

- 所属ロール
  システムで使用する所属ロールを追加する場合に指定する情報です。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- すでに存在するユーザ ID または所属ロール名は指定できません。
- このコマンドの引数に指定する内容は，「3.5　セキュリティ機能の設定に関する検討」で決定したことに従ってください。

（2） cjdeletesec（利用者のユーザ認証情報の削除）

形式

ユーザ ID を削除する場合

```
cjdeletesec [<J2EEサーバ名>] -type user -name <ユーザID>
```

所属ロールを削除する場合

```
cjdeletesec [<J2EEサーバ名>] -type role -name <所属ロール名>
```

機能

利用者のユーザ認証情報を，J2EE サーバから削除するコマンドです。利用者をシステムから削除したり，システムで使用する所属ロールを削除したりするときに使用します。このコマンドで削除できる情報の種別を次に示します。

- ユーザ ID
  利用者を削除する場合に指定する情報です。ユーザ ID を削除すると，ユーザ ID とともにパスワードや所属ロールとのマッピングの情報も削除されます。
- 所属ロール
  システムで使用する所属ロールを削除する場合に指定する情報です。所属ロールを削除すると，削除対象の所属ロールにマッピングされているユーザ ID もアンマッピングされます。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- セキュリティロールの構成変更などで不要になった利用者の認証情報は，このコマンドを使って必ず削除してください。

（3） cjlistsec（利用者のユーザ認証情報の一覧表示）

形式

J2EE サーバに登録されている全ユーザ ID を表示する場合

```
cjlistsec [<J2EEサーバ名>] -type user
```

J2EE サーバに登録されている全所属ロールを表示する場合

```
cjlistsec [<J2EEサーバ名>] -type role
```

あるユーザ ID にマッピングされている全所属ロールを表示する場合

```
cjlistsec [<J2EEサーバ名>] -type user -name <ユーザID>
```

ある所属ロールにマッピングされている全ユーザ ID を表示する場合

```
cjlistsec [<J2EEサーバ名>] -type role -name <所属ロール名>
```

機能

ユーザ認証情報が正しく設定されているかどうかを確認するときに使用するコマンドです。J2EE サーバに登録されているユーザ認証情報を，標準出力に一覧表示します。このコマンドで一覧表示できる情報の種別を次に示します。

- J2EE サーバに登録されている全ユーザ ID
  利用者を追加，削除したあとの確認をする場合に指定する情報です。
- J2EE サーバに登録されている全所属ロール
  システムで使用する所属ロールを追加，削除したあとの確認をする場合に指定する情報です。
- あるユーザ ID にマッピングされている全所属ロール
  ユーザ ID と所属ロールのマッピングを追加，削除したあとの確認をする場合に指定する情報です。
- ある所属ロールにマッピングされている全ユーザ ID
  ユーザ ID と所属ロールのマッピングを追加，削除したあとの確認をする場合に指定する情報です。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- 一覧は大文字小文字の区別なしで，昇順でソートされます。

（4） cjmapsec（ユーザ ID と所属ロールのマッピング）

形式

```
cjmapsec [<J2EEサーバ名>] -role <所属ロール名>
         -user <ユーザID> [-user <ユーザID> ...]
```

機能

利用者のユーザ ID と所属ロールをマッピングするときに使用するコマンドです。一つの所属ロールに対して，複数のユーザ ID を指定できます。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- このコマンドの引数に指定する内容は，「3.5　セキュリティ機能の設定に関する検討」で決定したことに従ってください。

（5） cjunmapsec（ユーザ ID と所属ロールのアンマッピング）

形式

```
cjunmapsec [<J2EEサーバ名>] -role <所属ロール名>
           -user <ユーザID> [-user <ユーザID> ...]
```

機能

セキュリティロールの構成変更などで，不要になったマッピングを削除するときに使用するコマンドです。利用者のユーザ ID と所属ロールをアンマッピングします。一つの所属ロールに対して，複数のユーザ ID を指定できます。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- セキュリティロールの構成変更などで不要になったマッピングは，このコマンドを使って必ず削除してください。

7.2.3 J2EE アプリケーションのプロパティ設定で使用するコマンド

ここでは，J2EE アプリケーションに Application Server のセキュリティ機能の設定をするために使用するコマンドについて説明します。各コマンドの引数，入力例，戻り値，および注意事項の詳細については，マニュアル「Cosminexus リファレンス コマンド編」の「2.2　J2EE サーバで使用するコマンドの詳細」を参照してください。

J2EE アプリケーションのプロパティ設定で使用するコマンドの格納先を次に示します。

Windows の場合

```
<Cosminexusのインストールディレクトリ>¥CC¥admin¥bin¥
```

UNIX の場合

```
/opt/Cosminexus/CC/admin/bin/
```

（1） cjgetappprop（属性ファイルの取得）

形式

EJB-JAR 属性ファイルを取得する場合

```
cjgetappprop [<J2EEサーバ名>] -name <J2EEアプリケーション名>
             -type ejb -resname <EJB-JARの表示名>
             [-encoding <属性ファイル出力時のエンコーディング名>]
             -c <属性ファイルの出力先パス>
```

Session Bean 属性ファイルを取得する場合

```
cjgetappprop [<J2EEサーバ名>] -name <J2EEアプリケーション名>
             -type ejb
             -resname <EJB-JARの表示名>/<Session Beanの表示名>
             [-encoding <属性ファイル出力時のエンコーディング名>]
             -c <属性ファイルの出力先パス>
```

WAR 属性ファイルを取得する場合

```
cjgetappprop [<J2EEサーバ名>] -name <J2EEアプリケーション名>
```

```
-type war -resname <WARの表示名>
[-encoding <属性ファイル出力時のエンコーディング名>]
-c <属性ファイルの出力先パス>
```

機能

J2EE アプリケーションのプロパティを，属性ファイルとして取得するときに使用するコマンドです。属性ファイルの出力先は，管理者が任意で指定します。
このコマンドで取得できる属性ファイルのうち，Application Server のセキュリティ機能の設定に関係する属性ファイルの種別を次に示します。

- EJB-JAR 属性ファイル
- Session Bean 属性ファイル
- WAR 属性ファイル

各属性ファイルの設定については，「7.1　ファイル」を参照してください。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- 「-encoding < 属性ファイル出力時のエンコーディング名 >」は，JavaVM のデフォルトのエンコーディングを使用しない場合に指定する必要がある引数です。
- 指定したパスにすでに属性ファイルが存在する場合，上書きします。

（2） cjsetappprop（属性ファイルの内容の反映）

形式

EJB-JAR **属性ファイルの内容を反映する場合**

```
cjsetappprop [<J2EEサーバ名>] -name <J2EEアプリケーション名>
             -type ejb -resname <EJB-JARの表示名>
             -c <属性ファイルのパス>
```

Session Bean **属性ファイルの内容を反映する場合**

```
cjsetappprop [<J2EEサーバ名>] -name <J2EEアプリケーション名>
             -type ejb
             -resname <EJB-JARの表示名>/<Session Beanの表示名>
             -c <属性ファイルのパス>
```

WAR **属性ファイルの内容を反映する場合**

```
cjsetappprop [<J2EEサーバ名>] -name <J2EEアプリケーション名>
             -type war -resname <WARの表示名>
             -c <属性ファイルのパス>
```

機能

属性ファイルの内容を，J2EE アプリケーションに反映するときに使用するコマンドです。
このコマンドで内容を反映できる属性ファイルのうち，Application Server のセキュリティ機能の設定に関係する属性ファイルの種別を次に示します。

- EJB-JAR 属性ファイル
- Session Bean 属性ファイル

- WAR 属性ファイル

各属性ファイルの設定については,「7.1　ファイル」を参照してください。

注意事項

- 「<J2EE サーバ名 >」は，ホスト名と J2EE サーバ名を異なる値に設定した場合に指定する必要がある引数です。
- 指定した J2EE アプリケーション，またはリソース（EJB-JAR，Session Bean，WAR）は存在している必要があります。

付録

付録 A　用語解説

付録 A　用語解説

(英字)

Application Server

Cosminexus の実行環境を構築する基盤製品です。Application Server Standard と，Application Server Enterprise の総称です。

Application Server のセキュリティ機能

システムに登録された利用者が，その利用者に許可されたコンテンツだけにアクセスするための仕組みです。ユーザ認証とアクセス制御の 2 種類の機能があります。

Cosminexus

アプリケーションサーバを中核とした，性能や信頼性が高い J2EE アプリケーションを実行・開発するためのシステム構築基盤製品です。J2EE アプリケーションを実行し，利用者に業務サービスを提供する基盤を実行環境，実行環境で動作する J2EE アプリケーションを開発する基盤を開発環境といいます。

DD

J2EE アプリケーションを運用環境に配置するときの定義情報を記述した XML 形式のファイルです。Sun Microsystems, Inc. から EJB 用 DD，Web アプリケーション用 DD などの仕様が公開されています。

EAR ファイル

J2EE アプリケーションを構成する複数の EJB-JAR ファイル，WAR ファイル，および DD を EAR ファイル形式でパッケージ化したものです。

EJB

Enterprise JavaBeans の略です。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です。Sun Microsystems, Inc. から EJB 仕様が公開されています。

EJB-JAR 属性ファイル

EJB の属性を編集するためのファイルです。EJB-JAR 属性ファイルには，Application Server のセキュリティ機能を使用するために必要な，J2EE アプリケーションのプロパティを設定します。

EJB-JAR ファイル

Enterprise Bean，DD などを JAR ファイル形式に圧縮したものです。

EJB コンテナ

J2EE コンテナの構成要素で，Enterprise Bean を制御します。Enterprise Bean の実体は，EJB コンテナの中で実行されます。

Enterprise Bean

ビジネスロジックを EJB アーキテクチャに従って作成したものです。業務処理プログラムに該当します。

J2EE

Java™ 2 Platform, Enterprise Edition の略です。Sun Microsystems, Inc. から J2EE 仕様が公開されています。

J2EE アプリケーション

利用者のリクエストに応じて業務サービスを提供するアプリケーションです。EAR ファイル形式でパッケージ化されていて，複数の EJB-JAR ファイル，複数の WAR ファイル，および一つの DD から構成されます。J2EE アプリケーションの形式には，アーカイブ形式と展開ディレクトリ形式があります。

J2EE コンテナ

J2EE コンポーネントが動作する基盤です。Web アプリケーションが動作する Web コンテナと，EJB が動作する EJB コンテナで構成されます。

J2EE コンポーネント

J2EE アプリケーションの構成要素であるサーブレット，JSP，Enterprise Bean などのユーザアプリケーションプログラムのことです。J2EE コンポーネントは，J2EE コンテナや J2EE サービスで実行，管理されます。

J2EE サーバ

J2EE アプリケーションの実行基盤であり，Application Server のセキュリティ機能を提供するプロセスです。J2EE サーバは，次のプログラムモジュールで構成されます。

- J2EE アプリケーション
- J2EE コンテナ
- J2EE サービス

J2EE サービス

J2EE コンテナの部品機能として利用され，Application Server のセキュリティ機能の基盤となります。

PRF デーモン

バッファに出力された PRF トレースを PRF トレースファイルに出力する I/O プロセスです。

Session Bean

主に業務処理を実行するための Enterprise Bean です。クライアントが終了すると，対応する Session Bean も終了します。クライアントとのセッションの間だけ動作するため，一時的であり，非永続的です。Session Bean は，Stateless Session Bean と Stateful Session Bean に分類されます。

Session Bean 属性ファイル

Session Bean の属性を編集するためのファイルです。Session Bean 属性ファイルには，Application Server のセキュリティ機能を使用するために必要な，J2EE アプリケーションのプロパティを設定します。

WAR 属性ファイル

WAR の属性を編集するためのファイルです。WAR 属性ファイルには，Application Server のセ

キュリティ機能を使用するために必要な，J2EE アプリケーションのプロパティを設定します。

WAR ファイル

Web アプリケーションの構成要素を JAR ファイル形式に圧縮したファイルです。
Web アプリケーション実行に必要なサーブレット，JSP，HTML，Java クラスファイル，JAR ファイル，および Web アプリケーション配置記述子が含まれます。

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です。具体的には，サーブレット，JSP，HTML などの集合体です。

Web クライアント構成

利用者が，インターネットを使用してアプリケーションサーバにアクセスする構成です。サーブレットと JSP がアクセスポイントになります。

Web コンテナ

J2EE コンテナの構成要素で，J2EE アーキテクチャの Web コンポーネント規約を実装しています。
Web アプリケーションは，Web コンテナで動作します。
Java Servlet2.4 仕様，および JavaServer Pages Specification v2.0 仕様に準拠した Web アプリケーションを実行できます。

Web サーバ

利用者の Web ブラウザからのリクエスト受信，および利用者の Web ブラウザへのレスポンス送信に関連する処理を実行するプロセスです。

（ア行）

アーカイブ形式

J2EE アプリケーションの構成要素を，J2EE サーバの作業ディレクトリに持つ J2EE アプリケーションの形式です。

アクセス制御

Application Server のセキュリティ機能の一つです。利用者の役割に応じた業務サービスを提供するために，J2EE サーバはセキュリティロールの仕組みを使ってアクセス制御します。

アプリケーションサーバ

J2EE サーバを中心とした，アプリケーションの実行環境になるサーバ基盤です。
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）とデータベースなどの業務システム（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です。
日立のアプリケーションサーバ Cosminexus は，業務の開発から運用まで一貫した環境を提供します。

（カ行）

開発者
J2EE アプリケーションを開発して管理者に提供する人のことです。

管理者
アプリケーションサーバを構築・運用するシステム管理者のことです。

許可ロール
J2EE アプリケーションがアクセスを許可するロールのことです。Application Server のセキュリティ機能であるアクセス制御に使用されます。

構成ソフトウェア
Application Server で動作する個々のソフトウェアのことです。構成ソフトウェアは，単体で動作させるのではなく，ほかの構成ソフトウェアの機能と組み合わせて動作させることによって，Application Server としての機能を実現します。

（サ行）

サーバエリア
システムのハードウェアを管理するための，物理的な領域です。

サーバ管理コマンド
J2EE サーバで管理している J2EE アプリケーションの設定をするためのコマンド群です。

サーブレット
サーバ側で Java を実行させる方法の一つです。
サーブレットは，Web サーバに対して，単に HTML 文書や画像ファイルを送るだけではなく，Web サーバと連携して，アプリケーションを実行し，その結果を HTML 文書として送り返す機能を提供します。

所属ロール
リクエストを送信した利用者が所属するロールのことです。

セキュリティポリシー
セキュリティに関する基本方針です。システムの管理者が制定し，システムの利用者や J2EE アプリケーションの開発者を含めて，システム構築・運用にかかわる全員が遵守するように運用します。

セキュリティロール
J2EE サーバによるアクセス制御に必要なセキュリティの仕組みで，受信したリクエストをアクセス許可するかどうかを決定します。セキュリティロールは，リクエストを送信した利用者の所属ロールと，リクエスト送信先の J2EE アプリケーションが持つ許可ロールから構成され，J2EE サーバと J2EE アプリケーションにそれぞれセキュリティロールの設定が必要です。

属性ファイル
J2EE アプリケーションに対して，Application Server のセキュリティ機能の設定をするためのファ

イルです。

（タ行）

展開ディレクトリ形式

J2EE アプリケーションの構成要素を，J2EE サーバの外部にある一定のルールに従ったファイル，ディレクトリに持つ J2EE アプリケーションの形式です。

（ヤ行）

ユーザ認証

Application Server のセキュリティ機能の一つです。第三者による不正なアクセスを防ぐために，J2EE サーバは利用者のユーザ認証情報を使ってユーザ認証をします。

ユーザ認証情報

システムにユーザがログインするための情報です。管理者のユーザ認証情報は OS のアカウントとパスワード，利用者のユーザ認証情報は J2EE サーバで定義するユーザ ID，パスワード，および所属ロールです。

（ラ行）

利用者

Web クライアントのマシンから J2EE アプリケーションを利用するエンドユーザのことです。

索引

記号

A

C

D

E

H

J

O

P

S

W

あ

い

う

か

き

こ

さ

し

せ

そ

つ

て

ね

は

ふ

へ

ま

ゆ

り

ソフトウェアマニュアルのサービス ご案内

ソフトウェアマニュアルについて，３種類のサービスをご案内します。ご活用ください。

１．マニュアル情報ホームページ

ソフトウェアマニュアルの情報をインターネットで公開しております。

URL　http://www.hitachi.co.jp/soft/manual/

ホームページのメニューは次のとおりです。

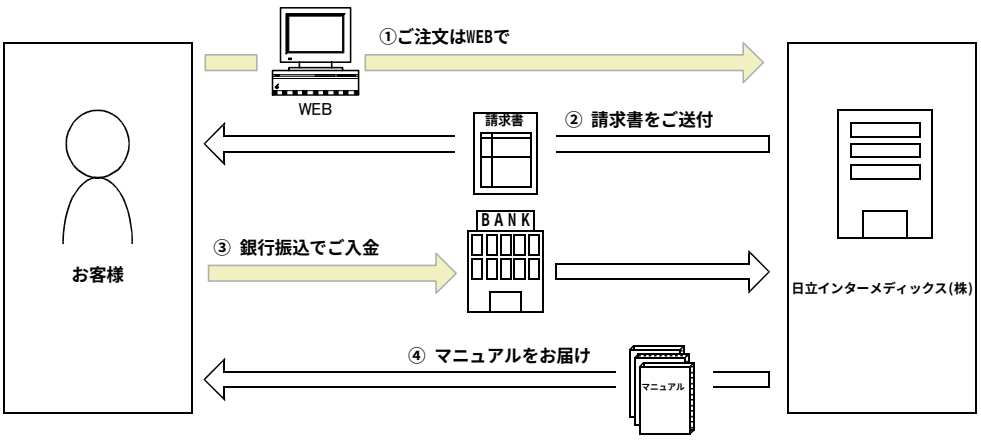
■マニュアル一覧	日立コンピュータ製品マニュアルを製品カテゴリ，マニュアル名称，資料番号のいずれかから検索できます。
■CD-ROMマニュアル情報	複数マニュアルを格納したCD-ROMマニュアルを提供しています。どの製品に対応したCD-ROMマニュアルがあるか，を参照できます。
■マニュアルのご購入	日立インターメディックス(株)の「日立コンピュータ製品マニュアルサイト」からお申し込みできます。 (詳細は「３．マニュアルのご注文」を参照してください。)
■Web提供マニュアル一覧	インターネットで参照できるマニュアルの一覧を提供しています。 (詳細は「２．インターネットからのマニュアル参照」を参照してください。)
■ご意見・お問い合わせ	マニュアルに関するご意見，ご要望をお寄せください。

２．インターネットからのマニュアル参照(ソフトウェアサポートサービス)

ソフトウェアサポートサービスの契約をしていただくと，インターネットでマニュアルを参照できます。
本サービスの対象となる契約の種別，及び参照できるマニュアルは，マニュアル情報ホームページでご確認ください。なお，ソフトウェアサポートサービスは，マニュアル参照だけでなく，対象製品に対するご質問への回答，問題解決支援，バージョン更新版の提供など，お客様のシステムの安定的な稼働のためのサービスをご提供しています。まだご契約いただいていない場合は，ぜひご契約いただくことをお勧めします。

３．マニュアルのご注文

日立インターメディックス(株)の「日立コンピュータ製品マニュアルサイト」からご注文ください。



① 下記 URL にアクセスして必要事項を入力してください。

URL　http://www2.himdx.net/manual/privacy.asp?purchase_flag=1

② ご注文いただいたマニュアルについて，請求書をお送りします。

③ 請求書の金額を指定銀行へ振り込んでください。なお，送料は弊社で負担します。

④ 入金確認後，７日以内にお届けします。在庫切れの場合は，納期を別途ご案内いたします。