WebSphere® Application Server V4.0 for z/OS and OS/390

インストールおよびカスタマイズ

GA88-8652-00
(英文原典：GA22-7834-00)

WebSphere® Application Server V4.0 for z/OS and OS/390

インストールおよびカスタマイズ

GA88-8652-00
(英文原典：GA22-7834-00)

お願い

本書および本書で紹介する製品をご使用になる前に、427ページの『付録D. 特記事項』に記載されている一般情報をお読みください。

本書は、WebSphere Application Server V4.0 for z/OS and OS/390 (5655-F31) に適用されます。また、新版で特に断りのない限り、これ以降のすべてのリリースとモディフィケーション・レベルにも適用されます。

WebSphere Application Server V4.0 for z/OS and OS/390 に関する資料の最新版は、
http://www.ibm.com/jp/software/websphere/appserv/ の Web サイトにあります。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

原　典： GA22–7834–00
WebSphere® Application Server V4.0 for z/OS and OS/390
Installation and Customization

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2001.6

この文書では、平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

図

表

本書について

本書 (*WebSphere Application Server V4.0 for z/OS and OS/390: インストールおよびカスタマイズ*) では、以下の方法について説明します。

- WebSphere for z/OS ランタイム環境の計画、インストール、およびカスタマイズ
- WebSphere Application Server の前のリリースからのマイグレーション
- シスプレックスなどの拡張システム構成内での WebSphere for z/OS のセットアップ

WebSphere for z/OS による使用のための eNetwork Communication Server (TCP/IP)、セキュリティー・サーバー (RACF)、およびワークロード管理など、必要な OS/390 または z/OS 機能のセットアップの説明が含まれています。

注: 正式なプロダクト名は『WebSphere Application Server V4.0 for z/OS and OS/390』ですが、本書では、これを単に『WebSphere for z/OS』と表記します。

本書の対象読者

本書は、OS/390 または z/OS サブシステムの構成および WebSphere for z/OS のインストールを行うシステム・プログラマー、セキュリティー管理者、ネットワーク管理者、またはデータベース管理者を対象としています。

本書の構成

WebSphere for z/OS の計画およびインストールには、ビジネス・アプリケーションのインストールを行う前に実行しなければならないタスクが含まれています。これには、システム構成の計画および WebSphere for z/OS ランタイム環境のインストールなどのタスクが含まれます。1ページの『第1章 インストールおよびカスタマイズの概要』には、インストール手順を行う前の簡単な概要が提供されています。

ランタイム環境をインストールするには、以下の 2 つの一般領域でタスクを実行しなければなりません。

1. OS/390 または z/OS の基本システム。WebSphere for z/OS をセットアップする前に、さまざまな OS/390 または z/OS サブシステムおよびネットワークを準備する必要があります。たとえば、セキュリティー管理をセットアッ

プして、ワークロード管理 (WLM) のワークロードの定義および DB2 for OS/390 のセットアップを行うなどのタスクを実行しなければなりません。詳細については、9ページの『第2章 OS/390 または z/OS の基本環境の準備』を参照してください。

2. WebSphere for z/OS ランタイム環境本体。これには、コードのロード、parmlib メンバーの変更、環境ファイルの作成、および構成ジョブ (ブートストラップ・ジョブとも呼ばれます) の実行が含まれます。詳細については、55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』を参照してください。

WebSphere の別のリリースからマイグレーションする場合は、205ページの『第4章 WebSphere for z/OS の新規リリースへのマイグレーション』を参照し、その説明に従ってください。

285ページの『第5章 インストール後のタスク』では、システムのバックアップなどのタスクを扱っています。これは、インストールおよびカスタマイズのすぐ後に行うとよいでしょう。

WebSphere for z/OS をモノプレックス・システム上で開始してから、拡張セキュリティー、ワークロード管理、データベース、およびシスプレックス・オペレーションを後でインプリメントすることができます。これらの拡張タスクについては、301ページの『第6章 拡張トピック』を参照してください。

参照情報は、本書の以下の付録にあります。

- 383ページの『付録A. 環境ファイル』では、WebSphere for z/OS 環境変数について説明しています。
- 413ページの『付録B. ネーム・スペースの構成』では、WebSphere for z/OS ネーミング・スペースの構成方法について説明しています。
- 421ページの『付録C. DCE のセットアップ』では、DCE セキュリティーのセットアップ方法について説明しています。

関連情報の参照先

WebSphere for z/OS ライブラリーに含まれる資料のリストを次に示します。これらの資料は、次の Web サイトにもあります。

`http://www.ibm.com/jp/software/websphere/appserv/`

- *WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 には、WebSphere for z/OS のエレメントと、インストールの方法が記載されています。

- *WebSphere Application Server V4.0 for z/OS and OS/390: License Information*, LA22-7855 には、WebSphere for z/OS のライセンス情報が記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: インストールおよびカスタマイズ*, GA88-8652 には、WebSphere for z/OS についての計画、インストール、カスタマイズの各タスクとガイドラインが記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 には、WebSphere for z/OS に関連した診断情報、メッセージ、およびコードが記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: 操作および管理*, SA88-8653 には、システム操作と管理タスクに関する説明が記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 には、WebSphere for z/OS J2EE サーバーでの J2EE アプリケーションの開発、アセンブル、およびインストールの方法が記載されています。また、前のリリースの WebSphere Application Server for OS/390 またはその他の WebSphere ファミリー・プラットフォームからアプリケーションをマイグレーションする方法も記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: CORBA アプリケーションのアセンブル*, SA88-8658 には、WebSphere for z/OS (MOFW) サーバーでの CORBA アプリケーションの開発、アセンブル、および配置の方法が記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 には、システム管理ユーザー・インターフェースで提供されるシステム管理タスクと操作タスクについての説明が記載されています。
- *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スクリプト API*, SA88-8657 には、WebSphere for z/OS システム管理スクリプト API 製品の機能に関する説明が記載されています。

場合によっては、その他の z/OS または OS/390 のエレメントと製品に関する情報を参照する必要があります。これらすべての情報は、次のインターネットの場所にあるリンクを通じて入手できます。

```
http://www.ibm.com/servers/eserver/zseries/zos/
http://www.ibm.com/servers/s390/os390/
```

特に役立つ資料は、次のとおりです。

- *Getting Started with WebSphere Application Server*, SC09-4581。この資料には WebSphere for z/OS の概要と、その環境をセットアップするための要件が記載されています。
- *WebSphere* ビジネス構築のソリューション, SD88-7362

第1章 インストールおよびカスタマイズの概要

WebSphere Application Server V4.0 for z/OS and OS/390 (以後、WebSphere for z/OS と呼びます) は、WebSphere Application Server for OS/390 バージョン 3 スタンダード版とエンタープライズ版の機能を単一の製品にまとめたものです。

この資料では、WebSphere for z/OS の計画、インストール、カスタマイズの各タスクを扱っています。

WebSphere for z/OS の計画、インストール、およびカスタマイズには、ビジネス・アプリケーションをインストールする前に実行しなければならないタスクが含まれています。これらのタスクには、システム構成の計画および WebSphere for z/OS ランタイム環境のインストールが含まれます。この章の内容は次のとおりです。

- WebSphere for z/OS を最初にインストールおよびカスタマイズする場合に実行しなければならないタスクの一般的な概要が記載されています。
- 最初のインストールおよびカスタマイズの後のランタイム環境の図および説明が提供されています。最初のインストールおよびカスタマイズは、モノプレックス上で実行されるか、シスプレックス内の単一のシステム上で実行されます。
- WebSphere for z/OS の最初のインストールで考慮すべきことがらのチェックリスト、アプリケーション開発およびクライアント・システム、およびシスプレックス内の WebSphere for z/OS などの拡張システム構成が提供されています。

ランタイム環境を最初にインストールするには、以下の 2 つの一般的な領域でタスクを実行しなければなりません。

1. OS/390 または z/OS の基本システム。WebSphere for z/OS をセットアップする前に、さまざまな OS/390 または z/OS エレメント、製品、およびネットワークを準備する必要があります。たとえば、TCP/IP ネットワークの更新、セキュリティー管理のセットアップ、およびワークロード管理 (WLM) のワークロードの定義などのタスクを実行しなければなりません。詳細については、9ページの『第2章 OS/390 または z/OS の基本環境の準備』を参照してください。

2. WebSphere for z/OS ランタイム環境本体。これには、コードのロード、parmlib メンバーの変更、環境ファイルの作成、および構成ジョブ (ブートストラップ・ジョブとも呼ばれます) の実行が含まれます。詳細については、55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』を参照してください。

すでに WebSphere のいずれかのリリースをインストールし、カスタマイズしてある場合は、そのリリースを WebSphere for z/OS にマイグレーションできます。205ページの『第4章 WebSphere for z/OS の新規リリースへのマイグレーション』を参照してください。

インストールおよびカスタマイズの後に、アプリケーション開発者およびビジネス・アプリケーション用のクライアント環境のためのアプリケーション開発環境をインストールすることができます。この詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

最初のシステム上で WebSphere for z/OS を安定させたら、シスプレックス上で WebSphere for z/OS を使用可能にすることができます。ビジネス・アプリケーションを IMS または CICS データベースに接続するなど、その他の拡張システム構成をインプリメントすることも可能です。これらのトピック、およびその他のトピックは、301ページの『第6章 拡張トピック』に記載されています。

WebSphere for z/OS ランタイム構成の図

3ページの図1 は、モノプレックス上、またはシスプレックス内の単一のシステム上に製品を最初にインストールした後の WebSphere for z/OS ランタイム構成を表しています。

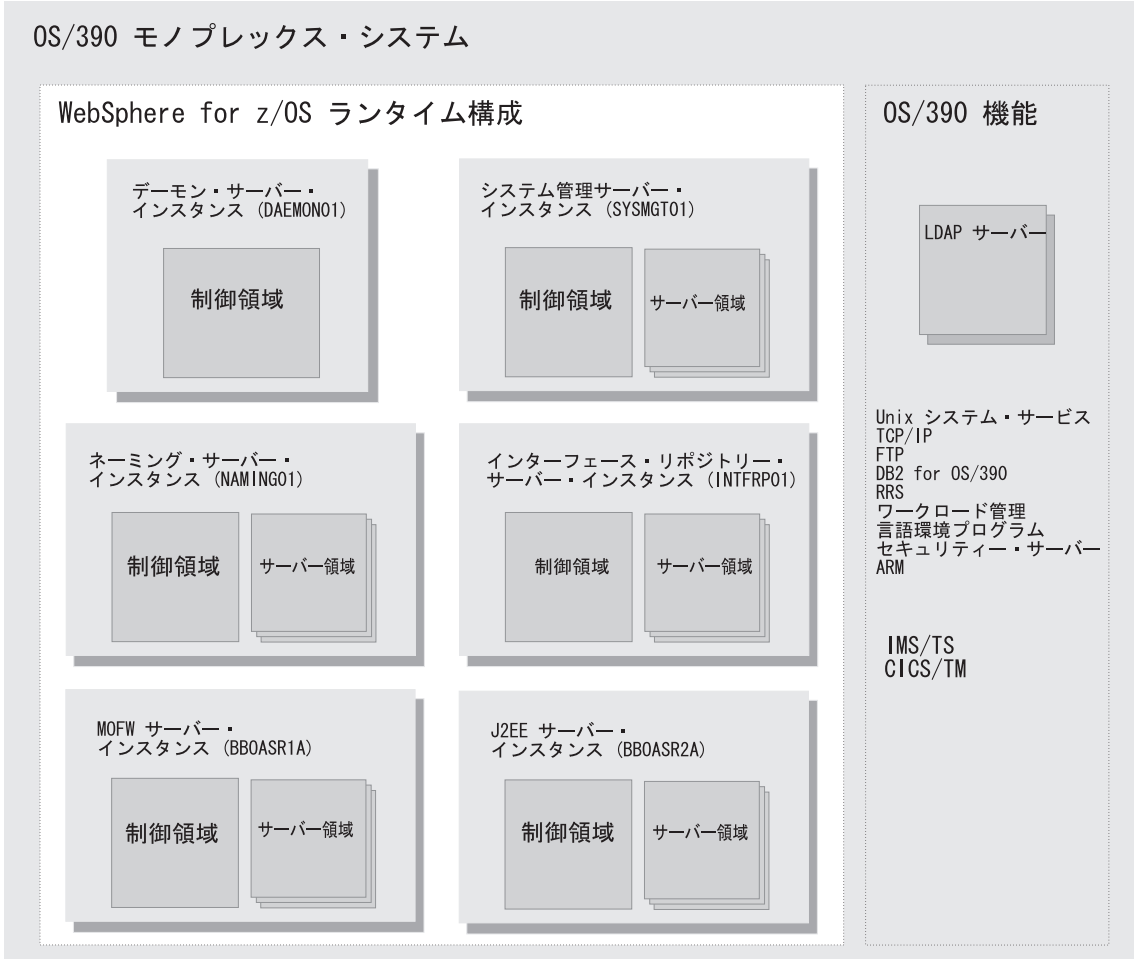


図 1. モノプレックス・システム上の WebSphere for z/OS ランタイム

先へ続ける前に、いくつかの用語について、特にサーバー という語の使用について説明します。WebSphere for z/OS では、アプリケーションが稼働している機能コンポーネントは、サーバー・インスタンス と呼ばれています。サーバー・インスタンスは、OS/390 または z/OS の、実際にコードを実行するアドレス・スペースを構成しています。

一方、サーバー は、複製されたサーバー・インスタンスの*論理グループ* です。これは何を意味するのか、説明します。サーバーは、ワークロードを別々のサーバー・インスタンスに区分することを可能にしますが、それでも、これらのワークロードを単一の単位として参照します。これは、シスプレックス環境では特に重要です。シスプレックス環境では、シスプレックス内の各 OS/390

または z/OS システムは、複製されたサーバー・インスタンスを実行している場合がありますが、シスプレックス外のクライアントは、それらを単一のサーバーとしてアドレッシングします。クライアントは、どのサーバー・インスタンスが実際にそれに代わって作業を行っているかを知りません。実際、クライアントからの後続の作業要求が、ワークロードの平衡化のために、シスプレックス内の異なるサーバー・インスタンスによって実行されることもあります。

各サーバー・インスタンス内には、制御領域およびサーバー領域の 2 種類のアドレス・スペースがあります。*制御領域* は、システム許可プログラムの実行と、サーバー・インスタンス用の通信などの管理を行います。各サーバー・インスタンスには、制御領域が 1 つずつあります。*サーバー領域* は、ビジネス・アプリケーションなどの非許可プログラムを実行します。ワークロードに応じて、サーバー・インスタンスは、1 度に 1 つまたは複数のサーバー領域を稼働させることができます (特殊サーバー・インスタンスで、サーバー領域を持たないデーモンを除く)。作業が構築される際、追加のサーバー領域は動的に開始され、要求を処理します。

3ページの図1 に示すように、完全な WebSphere for z/OS ランタイムには、デーモン・サーバー、システム管理サーバー、ネーミング・サーバー、およびインターフェース・リポジトリー・サーバーの各インスタンスが含まれています。ランタイムは、WebSphere for z/OS の直接の一部ではありませんが、Lightweight Directory Access Protocol (LDAP) サーバーを必要とします。また、次の 2 つの汎用アプリケーション・サーバー・インスタンスも組み込まれています。

- J2EE サーバー・インスタンス (BBOASR2A)。これは、弊社のインストール検査プログラム (IVP) の J2EE 部分が、J2EE コンポーネント・サポートをテストするために使用します。このサーバー・インスタンスは、サーブレット、JSP (Java Server Pages)、Enterprise (EJB) bean サーバー・インスタンスのパターンとして使用できます。
- MOFW サーバー・インスタンス (BBOASR1A)。これは、弊社のインストール検査プログラムの MOFW 部分が MOFW コンポーネント・サポートをテストするために使用します。MOFW (マネージド・オブジェクト・フレームワーク) は、CORBA 準拠コンポーネントを WebSphere for z/OS' にインプリメントしたものです。このサーバー・インスタンスは、MOFW コンポーネント用のパターンとして使用できます。

3ページの図1 に記載されているように、ランタイム・サーバー・インスタンスは、OS/390 UNIX や TCP/IP など、他の OS/390 または z/OS 機能を使用します。WebSphere for z/OS のインストールの一部には、ランタイムが使用する

これらの機能の構成が含まれています (詳細は 9ページの『第2章 OS/390 または z/OS の基本環境の準備』にあります)。

3ページの図1 にあるサーバー・インスタンスは、最初の OS/390 または z/OS イメージのインストール中に自動的に作成されます。表1 は、デフォルト・サーバーおよびそれに対応するサーバー・インスタンスおよびサーバー名をリストしています。

表 1. サーバー・インスタンスおよびサーバー名

サーバー	サーバー・インスタンス名	サーバー名
デーモン	DAEMON01	CBDAEMON
システム管理	SYSMGT01	CBSYSMGT
ネーミング	NAMING01	CBNAMING
インターフェース・リポジトリー	INTFRP01	CBINTFRP

インストールとカスタマイズのとき、LDAP サーバーをセットアップします。また、どの IVP を実行するかに応じて、MOFW サーバー・インスタンス (BBOASR1A) とそれに対応するアプリケーション・サーバー (BBOASR1)、または J2EE サーバー・インスタンス (BBOASR2A) とそれに対応するサーバー (BBOASR2) のどちらか、または両方を作成します。

WebSphere for z/OS をインプリメントするための計画の作成

WebSphere for z/OS の配置を正しく行うには、OS/390 または z/OS のシステムへの変更の計画および WebSphere for z/OS のインストールおよびカスタマイズの計画が必要です。この節では、考慮すべきタスクについてのチェックリストを提供しています。

インプリメント計画の作成のためのステップ

はじめに、すべての WebSphere for z/OS ランタイム・サーバー・インスタンスを 1 つのシステム上に作成してから、シスプレックスに拡張する際にそれらを他のシステム上に複製するように計画します。この手順では、モノプレックス上の WebSphere for z/OS の初期計画およびインプリメントの全体をガイドします。その後、アプリケーション開発およびクライアント環境のセットアップ全体をガイドします。最後に、オプションの拡張システム構成の計画全体をガイドします。

この作業を始める前に: WebSphere for z/OS をインプリメントする OS/390 または z/OS システムがあることを前提とします。

計画にそってインプリメントするために、以下のステップを実行します。

1. モノプレックス上に WebSphere for z/OS、またはマルチシステム・シスプレックス内に単一の OS/390 または z/OS をインプリメントする計画をします。以下を完了したらチェックマークを付けてください。

✔	項目	詳細情報
☐	必要なスキルを決定する。	9ページの『必要なスキルの決定』
☐	WebSphere for z/OS のシステム要件を確定する。	10ページの『WebSphere for z/OS のシステム要件の決定』
☐	TCP/IP ネットワーク用に実行する必要のあるカスタマイズの変更を理解および計画する。	16ページの『TCP/IP ネットワークの更新』
☐	セキュリティー・オプションを理解し、システムを保護するための準備をする。	19ページの『セキュリティーのセットアップ』
☐	WebSphere for z/OS ランタイム・サーバーのワークロード管理環境をセットアップする。	37ページの『ワークロード管理 (WLM) のセットアップ』
☐	WebSphere for z/OS が使用するためのリソース・リカバリー・サービスをカスタマイズする。	42ページの『リソース・リカバリー・サービスに関する推奨』
☐	パフォーマンスおよびシステムをモニターするための計画を立てる。	44ページの『RMF および他のモニター・システムについてのガイドライン』
☐	DB2 for OS/390 および LDAP の変更の計画を立てる。	44ページの『DB2 for OS/390 データベースおよび LDAP』
☐	メモリーの使用効率に対する推奨に従う。	49ページの『メモリーの使用に関する推奨』
☐	問題診断手順を計画および定義する。	50ページの『問題診断についての計画』
☐	WebSphere for z/OS をインストールする前に、自動再始動管理を考慮する。	53ページの『自動再始動管理 (ARM) についてのヒント』

2. WebSphere for z/OS をインストールおよびカスタマイズします。

✔	項目	詳細情報
☐	WebSphere for z/OS の初回のインストールとカスタマイズを行う。	55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』
☐	WebSphere for z/OS にマイグレーションする。	205ページの『第4章 WebSphere for z/OS の新規リリースへのマイグレーション』

---

3. さまざまなインストール後のタスクを実行します。

✔	項目	詳細情報
☐	システムのバックアップ・プロシージャーを計画および定義する。	285ページの『WebSphere for z/OS システムのバックアップのためのガイドライン』
☐	必要であれば、LDAP アクセス制御リストを更新する。	289ページの『管理アプリケーションの新規管理者の追加』
☐	ソフトウェアのサービス手順を計画および定義する。	292ページの『製品サービス』
☐	必要であれば、DB2 for OS/390 の RACF 保護をセットアップする。	292ページの『DB2 for OS/390 の RACF 保護のセットアップ』
☐	必要であれば、自動化制御をインプリメントし、WebSphere for z/OS の自動再始動管理をセットアップする。	295ページの『自動化および自動再始動管理のセットアップ』
☐	アカウンティングをセットアップする。	300ページの『アカウンティング』

---

4. アプリケーション開発およびクライアント環境の計画を立てます。

✔	項目	詳細情報
☐	アプリケーション開発およびクライアント環境のための WebSphere for z/OS の要件を検討する。	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

---

5. (オプション) 拡張システム構成を計画およびインプリメントします。

✓	項目	詳細情報
☐	WebSphere for z/OS をシスプレックス内に配置する計画を立てる。	301ページの『シスプレックスでの WebSphere for z/OS の使用可能化』
☐	複数の TCP/IP スタックを持つよう計画し、接続の最適化を使用、IBM Network Dispatcher を使用、またはバインドを特定するサポートを使用する。	320ページの『拡張 TCP/IP ネットワークのインプリメント』
☐	SSL や Kerberos などの拡張セキュリティー管理をインプリメントする。	324ページの『拡張セキュリティーのインプリメント』
☐	システム・パフォーマンスを調整する。	352ページの『拡張パフォーマンス制御のインプリメント』
☐	IMS データベース内のデータを使用する。2 つのオプションがあります。 a. OTMA インターフェースを使用する。 b. APPC を使用する。	• 361ページの『IMS-OTMA 手続き型アプリケーション・アダプター』 • 365ページの『IMS-APPC 手続き型アプリケーション・アダプター』
☐	CICS データベース内のデータを使用する。	364ページの『CICS-EXCI 手続き型アプリケーション・アダプターのセットアップ』
☐	WebSphere for z/OS の機能レベルをマイグレーションする。	376ページの『WebSphere for z/OS の機能レベルのマイグレーション』

すべての適用できる項目にチェックを入れたら完了です。

第2章 OS/390 または z/OS の基本環境の準備

WebSphere for z/OS 用に実行する必要のある OS/390 または z/OS の機能のカスタマイズ・ステップの一部は、WebSphere for z/OS 本体をインストールおよびカスタマイズする前に完了することができます。これらのタスクをこの章に入れ、作業を分割できるようにしました。

他の OS/390 または z/OS の機能のカスタマイズ・ステップは、必ず WebSphere for z/OS 本体と共に実行しなければなりません。これらのステップは、55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』に記載しています。

どちらの場合でも、本章では、OS/390 または z/OS の使用についての WebSphere for z/OS のバックグラウンド情報を記載しており、計画のガイドラインおよび WebSphere for z/OS のインプリメントに関するヒントを提供しています。

必要なスキルの決定

プロジェクト・チームを構成する場合、WebSphere for z/OS のインプリメントに必要なスキルを考慮に入れる必要があります。以下は、必要な機能スキル領域です。

以下のシステム・スキルを持つチームを構成することによって、WebSphere for z/OS を始めることができます。

- OS/390 UNIX システム・サービスおよび階層ファイル・システム (HFS)
- eNetwork Communications Server (TCP/IP) または同等のサーバー
- Lightweight Directory Access Protocol (LDAP)
- DB2 for OS/390
- ワークロード管理 (WLM)
- システム・ロガーおよびリソース・リカバリー・サービス (RRS)
- SMP/E および JCL
- セキュリティー・サーバー (RACF)、またはユーザーが使用するセキュリティー製品

システムを実稼働環境へ向けて移行する際、以下のシステム・スキルが必要になります。

- 自動再始動管理 (ARM)

- システム・オートメーション (インストールしてある場合)、またはユーザーが使用するオートメーション
- シスプレックス
- 分散ネットワーク内にセキュリティーを持つ計画の場合は、Secure Sockets Layer (SSL) Kerberos または分散コンピューティング環境 (DCE)
- RMF またはその他のパフォーマンス測定システム
- HTTP クライアントをサポートする計画の場合は、Web サーバー
- C++ または Java

アプリケーション開発環境の場合は、以下のスキルが必要です。
- オブジェクト指向アプリケーション・プログラミングのスキル
- Java ベースのコンポーネントの使用を計画している場合は、Java 2 Platform エンタープライズ版 (J2EE) と Enterprise JavaBeans (EJB) コンポーネントのアーキテクチャーに関する知識
- CORBA コンポーネントの使用を計画している場合は、Common Object Request Broker Architecture (CORBA) に関する知識
- 使用するアプリケーション開発ツール、たとえば、VisualAge for Java および IBM WebSphere Studio などに関する知識
- Windows のスキル
- ネットワーク・ファイル・システム (NFS) またはファイル転送プロトコル (FTP) のスキル

WebSphere for z/OS のシステム要件の決定

以下は、WebSphere for z/OS 用のシステム要件です。

OS/390 または z/OS のハードウェア要件

この製品のハードウェア要件は、OS/390 または z/OS バージョン 2 リリース 8 または z/OS、およびこれらの製品のそれ以降のリリースをサポートするハードウェアであれば、何でもかまいません。ただし、S/390 並列エンタープライズ・サーバーの第 5 世代以降のシステムなど、バイナリー浮動小数点ハードウェアを備えたマシンであれば、浮動小数点数演算を行うアプリケーションでパフォーマンスが大幅に向上します。

WebSphere for z/OS 用の OS/390 または z/OS ソフトウェア要件

以下は、WebSphere for z/OS 用のソフトウェア要件です。必要な修正サービスについては、プログラム・ディレクトリーを参照してください。

- シスプレックスとして構成された OS/390 バージョン 2 リリース 8 (またはそれ以降) または z/OS (最低でもモノプレックスは必要)。詳細は、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

- 階層ファイル・システム (HFS) 付きの OS/390 または z/OS UNIX システム・サービス (OS/390 UNIX)。詳細は、*z/OS UNIX システム・サービス 計画*, GA88-8639 を参照してください。

  注: WebSphere for z/OS システム管理サーバーには、読み取り / 書き込み HFS が必要です。シスプレックス内に WebSphere for z/OS を配置する計画の場合は、そのシスプレックス全体で読み取り / 書き込みモードで HFS を共用する手段を確立しなければなりません。OS/390 または z/OS バージョン 2 リリース 8 の場合は、ネットワーク・ファイル・システムを使用しなければなりません。OS/390 または z/OS バージョン 2 リリース 9 以降の場合は、ネットワーク・ファイル・システムを選択するか、共用 HFS 機能を使用することができます。

- eNetwork Communications Server (TCP/IP) または同等のサーバー。この資料では、eNetwork Communications Server に言及しますが、これと同等の製品に置き換えても構いません。詳細は、*z/OS Communications Server: IP マイグレーション*, GC88-8924 を参照してください。

- DB2 for OS/390 バージョン 7.1。

  注:

  1. シスプレックスおよび共用のワークロード内の複数システム上で WebSphere for z/OS を稼働している場合は、DB2 for OS/390 をデータ共用モードで構成しなければなりません。これは、カップリング・ファシリティーを必要とします。
  2. モノプレックス内で DB2 for OS/390 を稼働している場合は、データ共用モードで稼働する必要はありません。詳細は、*DB2 データ共用 : 計画および管理*, SC88-7380 を参照してください。

- ゴール・モードでのワークロード管理 (WLM) のセットアップ。詳細は、*z/OS MVS 計画 : ワークロード管理*, SA88-8574 を参照してください。

- OS/390 または z/OS システム・ロガー。詳細は、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

- リソース・リカバリー・サービス (RRS)。詳細は、*z/OS MVS プログラミング : リソース・リカバリー*, SA88-8582 を参照してください。

- セキュリティー・サーバー (RACF) などのセキュリティー製品。この資料では、例の中で、セキュリティー・サーバーに言及しますが、同等のセキュリティー製品と置き換えて構いません。詳細は、*z/OS SecureWay Security Server (RACF) マイグレーション*, GA88-8619 を参照してください。

- Secure Sockets Layer (SSL) のセキュリティーを使用する計画の場合は、暗号サービス・ベース (OS/390 または z/OS のエレメント) の暗号サービス・システム SSL が必要です。*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください。
- Kerberos セキュリティーを使用する計画の場合は、OS/390 SecureWay Security Server Network Authentication and Privacy Service for OS/390 が必要です。OS/390 V2R8 および V2R9 の場合、このサポートは次の Web サイトで入手できます。

  `http://www.software.ibm.com`

  OS/390 V2R10 および z/OS の場合、このサポートは SecureWay Security Server に組み込まれています。
- DCE セキュリティーを使用する計画の場合は、セキュリティー・サーバーの DCE コンポーネント (OS/390 または z/OS のオプションのエレメント) が必要です。詳細は、*z/OS DCE Administration Guide*, SC24-5904 を参照してください。
- LDAP (OS/390 または z/OS セキュリティー・サーバー内のコンポーネント)。詳細は、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。
- Java for OS/390 1.3.0 (WebSphere for z/OS のエレメント)。ただし、別々での使用も可能です。

  注: Java for OS/390 の以降のリリースは、サポートされていません。
- WebSphere for z/OS IMS-OTMA または IMS-APPC 手続き型アプリケーション・アダプターのサポートを使用する計画の場合は、IMS/TM 6.1.0 が必要です。

  WebSphere for z/OS での IMS のセットアップについて、詳しくは、361ページの『IMS-OTMA 手続き型アプリケーション・アダプター』を参照してください。
- WebSphere for z/OS CICS-EXCI 手続き型アプリケーション・アダプターのサポートを使用する計画の場合は、CICS/TS 1.3 が必要です。

  WebSphere for z/OS での CICS のセットアップについて、詳しくは、364ページの『CICS-EXCI 手続き型アプリケーション・アダプターのセットアップ』を参照してください。

ワークステーション要件

管理アプリケーションおよび操作アプリケーションは、WebSphere for z/OS に同梱されています。このアプリケーションは、以下を必要とします。

プロセッサー
200 MHz (最低)

メモリー
128 MB (最低)

ディスク
20 MB (最低構成)

50 MB (すべての構成オプション付きの場合)

一時ディスク・スペース
50 MB (インストール後削除)

モニター
800x600 対応モニター (最低)

オペレーティング・システム
Microsoft Windows NT 4.0 (サービス・パック 3)、Microsoft Windows 95 (サービス・パック 1 または 2)、Windows 98、または Windows 2000

通信 TCP/IP (オペレーティング・システム提供のもの)

Web ブラウザー
HTML 3.2 対応 (Netscape Navigator 4.0 または Microsoft Internet Explorer 4.0 など)

Java 仮想マシン
IBM Java Runtime Environment 1.3 以上 (インストール・パッケージを含む)

プロセッサーの速度およびメモリーの増強は、ワークステーションのパフォーマンスを向上する場合があります。

WebSphere for z/OS アプリケーションの開発のためのソフトウェア要件

アプリケーション開発環境に必要な製品は、J2EE と CORBA (MOFW) のどちらのコンポーネントを開発するかによって異なります。MOFW は Managed Object Framework (マネージド・オブジェクト・フレームワーク) の略で、IBM による CORBA の標準のインプリメンテーションです。

J2EE コンポーネントの要件: J2EE コンポーネントを開発する場合は、ワークステーション上に次のものが必要です。

表 2. *Java 2 Enterprise Edition* アプリケーション・コンポーネントのソフトウェア要件

J2EE アプリケーション・コンポーネント	**使用するソフトウェア**
Enterprise beans	**開発およびテスト用:** • 次のフィーチャーを備えた VisualAge for Java 3.5 とパッチ 2: – Data Access Beans 3.5 – IBM EJB Development Environment 3.5 – IBM Enterprise Extension Libraries 3.5 – IBM WebSphere Test Environment 3.5 – IBM Common Connector Framework 3.5 – IBM Enterprise Access Builder Library 3.5 – IBM Java Record Library 3.5 **ヒント:** VisualAge for Java を使用する代わりに、IBM 以外のツール、たとえば JBuilder や Visual Cafe などをアプリケーション開発に使用できます。それらの製品の文書を使用して、ハードウェア要件とソフトウェア要件を判別してください。 • IBM または Sun Microsystems Java 2 Standard Edition (J2SE) ソフトウェア開発キット (SDK)V1.3。 • アプリケーション・コンポーネントのテスト用に WebSphere Application Server Advanced Edition V3.5。 • (オプション) DB2 ユニバーサル・データベース バージョン 7.1。これは、パーシスタント・データストアの使用を必要とする bean のテストにのみ必要です。
	アセンブリー用: WebSphere for z/OS アプリケーション組み立てツール。
	J2EE サーバーでのインストール用: WebSphere for z/OS 管理アプリケーション。

表 2. Java 2 Enterprise Edition アプリケーション・コンポーネントのソフトウェア要件 (続き)

J2EE アプリケーション・コンポーネント	使用するソフトウェア
サーブレットおよび JSP (JavaServer Pages)	**開発およびテスト用:** • WebSphere Studio 3.5.2 **ヒント:** WebSphere Studio を開始した時点で、このツールは、VisualAge for Java と WebSphere Application Server Advanced Edition がワークステーションにインストールされているかどうかを検査します。 • IBM または Sun Microsystems Java 2 Standard Edition (J2SE) ソフトウェア開発キット (SDK)V1.3。
	アセンブリー用: WebSphere for z/OS アプリケーション組み立てツール。
	J2EE サーバーでのインストール用: WebSphere for z/OS 管理アプリケーション。

J2EE コンポーネント用に、OS/390 または z/OS 上に次のものが必要です。

- 階層ファイル・システム (HFS) に書き込みができる FTP サーバー

CORBA (MOFW) コンポーネントの要件: CORBA (MOFW) コンポーネントを開発する場合は、ワークステーション上に次のものが必要です。

- Component Broker for Windows NT 3.5
- VisualAge C++
- 手続き型アプリケーション・アダプターを開発する場合は VisualAge for Java エンタープライズ版 3.5

CORBA (MOFW) コンポーネント用に、OS/390 または z/OS 上に次のものが必要です。

- C/C++ IBM オープン・クラス・ライブラリー (OS/390 または z/OS のオプション機構。実行時には必要ありませんが、コンパイルに必要です)。*z/OS 言語環境プログラム カスタマイズ*, SA88-8552 および *z/OS インストール計画*, GA88-8520 を参照してください。

TCP/IP ネットワークの更新

WebSphere for z/OS は、通信に関しては、CORBA 標準の Internet Inter-ORB Protocol (IIOP) に従っています。したがって、TCP/IP への変更点を考慮し、TCP/IP の構成を変更しなければなりません。

この節では、ドメイン・ネーム・サーバー (DNS) および TCP/IP に対して行う必要のある変更点についてのバックグラウンド情報を提供しています。実際に実行するステップは、77ページの『TCP/IP ネットワークのセットアップ』に記載されています。

TCP/IP および WebSphere for z/OS についてのヒント

TCP/IP ネットワークについて、以下を考慮に入れてください。

OS/390 または z/OS の場合:

- シンプルなドメイン・ネーム・サービス (DNS) のネーム・サーバーおよび単一の OS/390 または z/OS イメージで始めることができますが、初期構成は成長するものと考えて設計する必要があります。たとえば、パフォーマンス上の理由、または単一障害ポイントを防ぐという理由でビジネス・アプリケーションをモノプレックスを超えて完全シスプレックス構成に拡張するという意図がある場合があります。いくつかの考慮事項がここに生じてきます。

  ネットワーク・トラフィックを複製されたサーバー・インスタンスへ動的にルーティングする一方で、いくつかの DNS のインプリメントおよびネットワーク・ルーターのインプリメントによって、汎用のデーモン IP 名の使用が可能になります。システムをモノプレックスを超えて拡張するつもりがある場合は、始めからこれらのインプリメントのうちの 1 つを使用する価値があるかもしれません。非ラウンドロビン DNS ネーム・サーバーは、動的ネットワーク・トラフィック・ルーティングを可能にするネーム・サーバーを改造せずに拡張する能力を制限します。

  OS/390 または z/OS 上またはそれ以外での DNS およびルーター・インプリメントを以下のように選択することができます。

  – 非ラウンドロビン DNS ネーム・サーバー。
  – ラウンドロビン DNS ネーム・サーバー。
  – 接続の最適化 (OS/390 または z/OS が使用する、DNS およびワークロード管理 (WLM) を使用する技法)。WebSphere for z/OS は、接続の最適化を使用して、単一障害ポイントを防ぎます。接続の最適化を使用するに

は、OS/390 または z/OS 上で DNS ネーム・サーバーを実行しなければなりません。詳しくは、321ページの『接続の最適化』を参照してください。

– IBM Network Dispatcher などのネットワーク・ルーター。詳しくは、322ページの『IBM Network Dispatcher』を参照してください。

- **デーモン・サーバー用のデーモン IP 名を慎重に選択します。**希望する任意の名前を選択することができますが、一度選択すると、変更するのは困難です。また、インストールとカスタマイズの最中にデーモン IP 名を変更することはできません。

  インストール時のデーモン・ブートストラップ・プロセスを開始する前に、DAEMON_IPNAME 環境変数を定義しなければなりません。値については、選択したデーモン IP 名を使用します。383ページの『付録A. 環境ファイル』を参照してください。

  ブートストラップ・プロセスは、特に、システム管理データベース内のデーモン IP 名を設定します。ブートストラップの後、WebSphere for z/OS は、システム管理データベース内のこの値を使用し、環境ファイル内の値は無視します。ブートストラップの後で、DAEMON_IPNAME 環境変数の値がシステム管理データベース内にある値とは別の値に変わることがあり得ます。このようなことが起こった場合は、エラー・メッセージが発行されますが、デーモンは、システム管理データベースからの値で初期化します。
- デーモン・サーバー用のポートを選択します。これは変更しないでください。オブジェクト参照にはポートを含んでいます。ポートを変更すると、既存のオブジェクトにはアクセスできなくなります。WebSphere for z/OS は、デフォルトとしてポート 5555 を使用します。
- WebSphere for z/OS では、システム管理サーバーが解決ポートを処理します。クライアントは解決 IP 名で構成され、サーバーはネーミング・サーバー・ルートまたはインターフェース・リポジトリー参照などの項目を戻すため、サーバーは、変更に対してより柔軟性があります。

  推奨: CORBA および IBM は、解決ポート用にデフォルトのポート 900 をお勧めします。解決ポート用の別のポートを使用する場合は、分散ネットワーク内のあらゆる個所で変更しなければなりません。

  ブートストラップ・サーバーをローカルの OS/390 または z/OS (これは、実際に WebSphere for z/OS 内のシステム管理サーバーです) 上や、あるいは別のシステム上に構成しても構いません。ポートを 900 以外に構成して、OS/390 または z/OS 上の複数の ORB を容易にすることができます。
- すべての接続に固定ポート番号を設定して、ファイアウォールの背後にあるサーバーの構成を可能にすることができます。Internet Inter-ORB Protocol

(IIOP) をファイアウォール経由で使用する必要がある場合は、そのファイアウォールが IIOP をサポートすることを確認してください。

- 他のすべてのポートは、動的に取得されます。
- ルート・ネーミング・コンテキスト用の TCP/IP ホスト・アドレスを確立します。
- その他の TCP/IP 関連の活動には、NFS、LDAP、Web サーバー (オプション)、Kerberos (オプション)、および DCE (オプション) のセットアップが含まれています。

  LDAP の場合は、システム上にすでに LDAP サーバーを持っていても、WebSphere for z/OS 専用に LDAP サーバーをセットアップすることをお勧めします。この専用の LDAP サーバーには、専用のポートが必要です (推奨は 1389)。94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』を参照してください。
- OS/390 または z/OS 上で DNS を使用する場合は、ネーム・デーモンに関連したリフレッシュ・タイマー・インターバル (-t 値) を変更したい場合があります。-t 値は、シスプレックスの名前およびアドレスのリフレッシュと、それらの名前およびアドレスに関連する待機のリフレッシュとの間の時間 (nn、秒単位) を指定します。デフォルトは、60 秒です。-t 値を減らすと、DNS での DAEMON_IPNAME および RESOLVE_IPNAME の登録に必要な経過時間が短くなりますが、DNS プロセッシング・オーバーヘッドも増加します。当社のテストでは、10 秒のインターバルを使用しました。詳細は、*z/OS Communications Server: IP Configuration Reference*, SC31-8776 を参照してください。

管理アプリケーションおよび操作アプリケーションを稼働するワークステーションの場合:

管理アプリケーションおよび操作アプリケーション (Windows NT 上で稼働するシステム管理サーバーのクライアント) には、TCP/IP のセットアップが必要です。ドメイン・ネーム・サーバー (DNS) または ワークステーション HOSTS ファイル内のブートストラップ・サーバーの IP 名およびネーミング・サーバーの IP 名を定義しなければなりません。ブートストラップ・サーバーの IP 名は、ホストへの初期接続に関連する名前です。これは、WebSphere for z/OS 環境ファイルの RESOLVE_IPNAME パラメーターで定義されます。ネーミング・サーバーの IP 名はネーミング・サーバーに関連する総称名で、WebSphere for z/OS 環境ファイルの DAEMON_IPNAME パラメーターで定義されます。複数のネーム・サーバーがある場合 (連合ネーム・スペース)、ワークステーションが必要とするすべてのネーム・サーバーのホスト名が解決可能でなければなりません。ワークステーションには HOSTS ファイルがある場合

があります。これは、TCP/IP ホスト名を TCP/IP アドレスと関連付けする場合に使用されます。通常、TCP/IP アドレスは、システムのドメイン・ネーム・サーバー (DNS) によってホスト名と関連付けされます。ホスト名がドメイン・ネーム・サーバーを使用しても解決できない場合、ワークステーションは HOSTS ファイルを使用します。117ページの『ワークステーションの Hosts ファイルを更新するためのステップ』に、HOSTS ファイルの更新方法についての説明があります。

セキュリティーのセットアップ

WebSphere for z/OS は、分散ネットワークでのクライアントとサーバーによるリソースへのアクセスをサポートしています。このため、セキュリティー戦略の一部として、それらのリソースへのアクセスを制御する方法を決定し、故意または偶然によるシステムまたはデータの破壊を防止する必要があります。

分散ネットワークで考慮する必要がある要素は、次のとおりです。

- サーバーに OS/390 または z/OS の基本オペレーティング・システム・サービスに対する権限を与える必要があります。それらのサービスは、RACF セキュリティー、データベース管理、およびトランザクション管理です。
  - サーバーの場合、制御領域とサーバー領域を区別しなければなりません。制御領域は、許可されたシステム・コードを実行します。このため、制御領域は信頼されています。サーバー領域はアプリケーション・コードを実行し、リソースへのアクセスができます。したがって、サーバー領域に与える権限は、慎重に考慮する必要があります。
  - また、ランタイム・サーバーと自己のアプリケーション・サーバーが備える権限のレベルを区別する必要があります。たとえば、システム管理サーバーには他のサーバーを起動する権限が必要ですが、自己のアプリケーション・サーバーにその権限は必要ありません。
- クライアント (ユーザー) にサーバーとサーバー内のオブジェクトに対する権限を与える必要があります。各クライアントの特性には、特別に次の点を考慮する必要があります。
  - そのクライアントはローカル・システム上にあるのか、それともリモート・クライアントか。ネットワークのセキュリティーは、リモート・クライアントについての考慮事項となります。
  - 識別できない (認証されていない) クライアントがシステムにアクセスするのを許可するかどうか。システム上のリソースには、パブリック・アクセス用に意図されているものと、保護を必要とするものがあります。保護されたリソースにアクセスするためには、クライアントは ID を確立し、それらのリソースを使用する権限を持たなければなりません。

– どのような種類のオブジェクトにクライアントはアクセスするのか。Enterprise bean オブジェクトと CORBA オブジェクトの許可メカニズムは、互いに異なります。

リソースを保護する必要がある場合は、それらのリソースにだれがアクセスするかを識別することが非常に重要です。このため、どのセキュリティー・システムにも、認証と呼ばれるクライアント (ユーザー) 識別機能が必要です。WebSphere for z/OS がサポートする分散ネットワークでは、クライアントは次の場所からリソースにアクセスできます。

- サーバーと同じシステムの中からアクセスする
- サーバーと同じシスプレックスの中からアクセスする
- リモート OS/390 または z/OS システムからアクセスする
- 異機種混合のシステム (たとえば分散プラットフォーム上の WebSphere)、CICS システム、またはその他の CORBA 準拠システムからアクセスする

さらに、クライアントがあるサービスを要求し、サーバーがその要求を別のサーバーへ転送しなければならない場合もあります。その場合、システムは、委任 (クライアント ID を中間サーバーとターゲット・サーバーが使用できること) を処理する必要があります。

最後に、分散ネットワークで、渡されるメッセージが機密情報であり、悪用されていないことをどのように保証しますか。クライアントが本当にそのクライアントであることを、どのように保証しますか。ネットワーク ID を OS/390 または z/OS の ID に、どのようにマップしますか。これらの問題は、WebSphere for z/OS では次の方法で処理されます。

- SSL とディジタル証明書の使用
- Kerberos
- 分散コンピューティング環境 (DCE)

ネットワーク・セキュリティーは WebSphere for z/OS の初期インストールとカスタマイズには必要ないので、これらのトピックの詳細については、301ページの『第6章 拡張トピック』で説明します。現時点のトピックは、WebSphere for z/OS のセキュリティーの概要を紹介し、読者がシステムのセキュリティーに関する初期計画について決定を下せるようにすることを狙いとしています。55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』に、WebSphere for z/OS が提供しているサンプルの使用を通して、初期の RACF セキュリティー管理をセットアップするための特定の指示があります。

RACF サンプルは、ユーザー ID および他のカスタマイズ・サンプルで使用されているグループで作成されています。したがって、RACF サンプルを変更しないことをお勧めします。

以下のトピックでは、WebSphere for z/OS がどのようにセキュリティーをサポートするかを説明しています。説明は、以下のサブトピックで編成されています。

- 許可検査
- ユーザー識別、認証、およびネットワーク・セキュリティーの問題

注: 例としてセキュリティー・サーバー (RACF) を使用していますが、これと同等の製品を使用することもできます。

セキュリティー監査とセキュリティー管理のためのサポートに関する注が含まれています。

許可検査

それぞれの制御領域、サーバー領域、およびクライアントは、独自の MVS ユーザー ID を備えている必要があります (ユーザー識別と認証については、後で詳しく説明します)。要求がクライアントからサーバーへ、またはサーバーからサーバーへ流れる場合、WebSphere for z/OS は、その要求と一緒にユーザーの ID を渡します。したがって、各要求は、そのユーザー ID のために実行され、システムは、そのユーザー ID がそのような要求を行う権限を持っているかどうかを検査します。

制御のまとめ

表3 は、リソースに対する認可を与えるために使用される制御を要約したものです。これらの制御を理解し、使用することにより、WebSphere for z/OS におけるすべてのリソース・アクセスを制御できます。

表 3. 制御と許可のまとめ

制御	許可
LDAP でのアクセス制御リスト	WebSphere for z/OS のネーミングおよびインターフェース・リポジトリー・データへの LDAP 制御アクセス
CBIND クラス	サーバーへのアクセス
DATASET クラス	データ・セットへのアクセス
DCEUUIDS クラスと FACILITY クラス	RACF ユーザー ID への DCE 証明書のマッピング
DSNR クラス	DB2 for OS/390 へのアクセス

表 3. 制御と許可のまとめ (続き)

制御	許可
EJBROLE クラス	Enterprise bean 内のメソッドへのアクセス
FACILITY クラス (IRR.DIGTCERT.LIST および IRR.DIGTCERT.LISTRING)	SSL 鍵リング、証明書、およびマッピング
FACILITY クラス (IMSXCF.OTMACI)	IMS アクセスのための OTMA へのアクセス
FACILITY クラス (IRR.RUSERMAP)	Kerberos 証明書
ファイル・アクセス権	HFS ファイルへのアクセス
GRANT (DB2 for OS/390)	計画およびデータベースへの DB2 for OS/390 アクセス
LOGSTRM クラス	ログ・ストリームへのアクセス
OPERCMDS クラス	デーモンによるサーバーの始動と停止
PTKTDATA クラス	シスプレックスでのパスチケットの使用可能化
SERVER クラス	サーバー領域による制御領域へのアクセス
SOMDOBJS クラス	CORBA オブジェクト内のメソッドへのアクセス
STARTED クラス	ユーザー ID (およびオプションとしてグループ ID) と開始プロシージャーとの関連付け
SURROGAT クラス (*.DFHEXCI)	CICS アクセスのための EXCI へのアクセス

サーバー許可

23ページの図2は、WebSphere for z/OS がサーバーについて行う許可検査の種類を示しています。

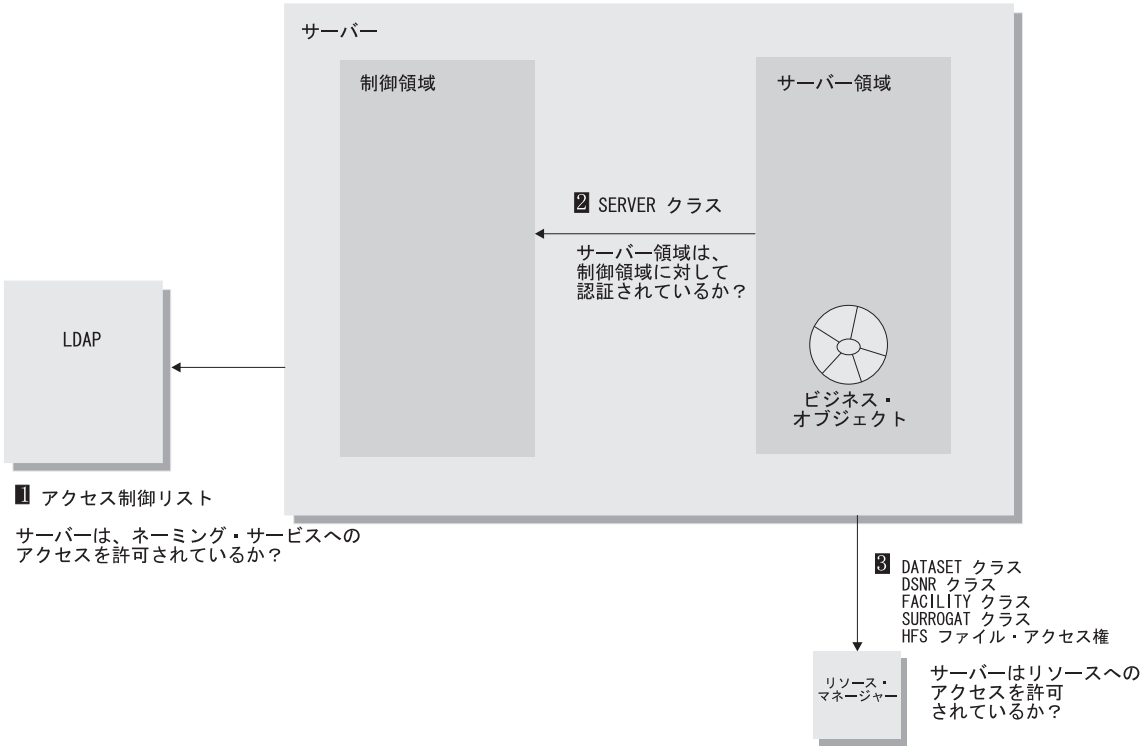


図 2. サーバー許可検査

以下は、図2 の番号付きの項目についての説明です。

1. LDAP をオブジェクト用のアクセス制御リスト (ACL) を使用できるようにセットアップすることができます。この場合、ネーミング・サーバーはこれらのオブジェクトに対して許可される必要があります。詳しくは、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。
2. サーバー領域は、RACF SERVER クラス内のプロファイルへのアクセスを持っていなければなりません。これは、サーバー領域が制御領域内の許可ルーチンを呼び出すことができるかどうかを制御します。

   制御領域には、このようなアクセス制御は必要ありません。許可プログラム機能 (APF) のライブラリーからロードされた許可プログラムのみが、制御領域内で稼働します。
3. DB2 for OS/390、IMS、および CICS などのリソース・マネージャーは、独自のリソース制御をインプリメントしています。これらのリソース制御は、サーバーがリソースにアクセスする機能を制御します。

DB2 for OS/390 がリソース制御を使用している場合、すべての制御領域およびサーバー領域は、関係のあるリソースへのアクセスを認可される必要があります。DSNR RACF クラスを使用するか (RACF サポートがある場合)、または関連する DB2 for OS/390 GRANT ステートメントを発行することによって、これを行うことができます。

IMS アクセスのための OTMA へのアクセスは、FACILITY クラス (IMSXCF.OTMACI) を通じて行われます。CICS のための EXCI へのアクセスは、SURROGAT クラス (*.DFHEXCI) を通じて行われます。

データ・セットへのアクセスは、DATASET クラスを通じて制御でき、HFS ファイルへのアクセスは、ファイル・アクセス権を通じて制御できます。

サーバー許可検査についての指定: WebSphere for z/OS リソースへのアクセスを制御するには、以下のように行います。

- 経験法則として、制御領域により大きな権限を、サーバー領域により小さい権限を与えてください。

表 4. 領域に対する信頼と権限のレベル

領域	信頼およびアクセス権限のレベル
制御領域	WebSphere for z/OS システム・コードを含んでいます。信頼されています。複数のユーザーとやり取りします。より大きな許可。APF 許可を実行します。
サーバー領域	アプリケーション・コードを含んでいます。信頼されていません。作業するための、およびデータ・ストアへ付加するための許可を持たずに、無許可で実行します。

- 以下の表で説明しているように、WebSphere for z/OS ランタイム・サーバーに関しては、経験法則として、デーモンおよびネーミング・サーバーにより小さい権限を、システム管理サーバーにより大きい権限を与えてください。

表 5. WebSphere for z/OS ランタイム・サーバー制御領域およびサーバー領域への権限の割り当て

ランタイム・サーバー	領域	必要な権限
デーモン・サーバー	制御	STARTED クラス、WLM サービスへのアクセス、DNS へのアクセス、他のサーバーを START、STOP、 CANCEL、FORCE、および MODIFY するための OPERCMDS アクセス

表 5. WebSphere for z/OS ランタイム・サーバー制御領域およびサーバー領域への権限の割り当て (続き)

ランタイム・サーバー	領域	必要な権限
ネーミング・サーバー	制御	STARTED クラス、WLM サービスへのアクセス
	サーバー	STARTED クラス、SERVER クラスへの READ 権限、LDAP データベース用の DBADM
システム管理サーバー	制御	STARTED クラス
	サーバー	STARTED クラス、SERVER クラスに対する READ 権限、他のサーバーを START、STOP、CANCEL、FORCE、および MODIFY するための OPERCMDS アクセス
インターフェース・リポジトリー・サーバー	制御	STARTED クラス
	サーバー	STARTED クラス、SERVER クラスへの READ 権限、LDAP データベース用の DBADM

- RRS ログ・ストリームの保護を忘れないでください。デフォルトでは、UACC は READ です。
- WebSphere for z/OS 環境ファイルを、特にパスワードを持っている場合には、保護します。環境ファイルについての詳細は、383ページの『付録A. 環境ファイル』を参照してください。

クライアント許可

26ページの図3 は、WebSphere for z/OS がクライアントについて行う許可検査の種類を示しています。

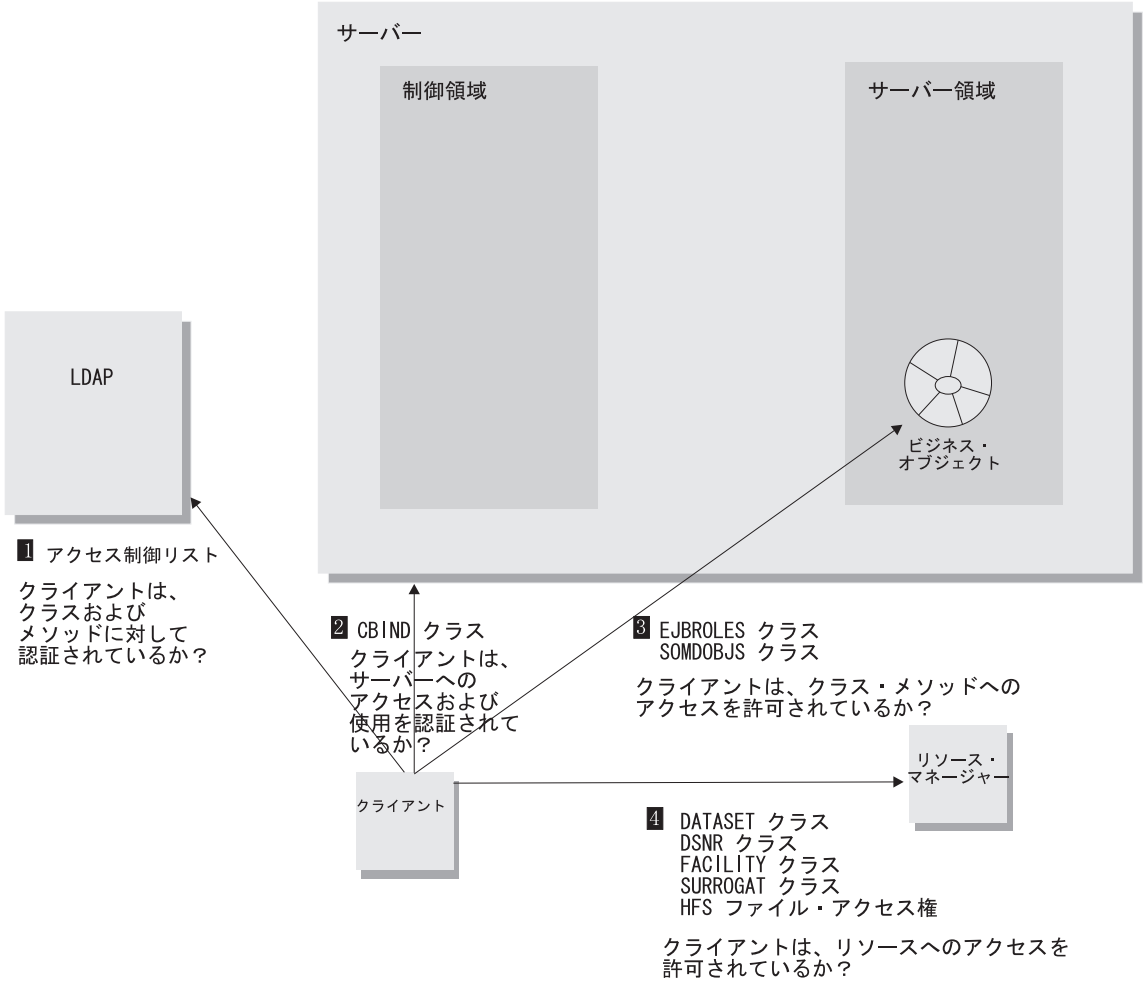


図3. クライアント許可検査

以下は、図3 の番号付きの項目についての説明です。

1. LDAP は、アクセス制御リストを使用して、ネーミング・サービスへのクライアント・アクセスを制御します。通常では、汎用の ANYBODY ユーザー ID を LDAP ネーム・スペースへの読み取りアクセス権付きでセットアップし、すべてのクライアントがネーミング・サービスにアクセスできるようにします。
2. RACF (オプション) 内の CBIND クラスを使用して、サーバーへアクセスするクライアントの能力を制限することができます。または、この種のアク

セス制御を必要としない場合は、このクラスを非活動化することができます。WebSphere for z/OS が CBIND クラスで使用するプロファイルには、以下の 2 つのタイプがあります。

- ローカルまたはリモート・クライアントがサーバーにアクセスできるかどうかを制御するもの。このプロファイルの名前は、以下の形式です。

  ```
  CB.BIND.server_name
  ```

  server_name は、サーバーの名前です。
- クライアントがサーバー内でオブジェクトを使用することができるかどうかを制御するもの。このプロファイルの名前は、以下の形式です。

  ```
  CB.server_name
  ```

  server_name は、サーバーの名前です。

注: 新規のサーバーを追加する場合は、すべてのシステム管理ユーザー ID (たとえば CBADMIN) に、CB.**server_name** および CB.BIND.**server_name** RACF プロファイルへの読み取りアクセスを持つことを許可しなければなりません。たとえば、以下のように、CBADMIN は CB.BBOASR1 および CB.BIND.BBOASR1 プロファイルへの読み取り権限が必要です。

```
PERMIT CB.BBOASR1      CLASS(CBIND) ID(CBADMIN) ACCESS(READ)
PERMIT CB.BIND.BBOASR1 CLASS(CBIND) ID(CBADMIN) ACCESS(READ)
```

3. RACF 内の EJBROLE (または GEJBROLE) クラスを使用して、Enterprise bean へのクライアントのアクセスを制御します。EJBROLE のプロファイル名は、以下の形式です。

   ```
   role_name
   ```

   ここで、*role_name* は、jar ファイル内かアプリケーション用に指定されたセキュリティー役割属性に一致します。役割名にブランクを含めることはできず、役割名は 245 文字を超えることができません。しかし、役割名には大文字と小文字を混在させることができます。

   RACF 内の SOMDOBJS クラスを使用して、CORBA オブジェクトへのクライアントのアクセスを制御します。SOMDOBJS 内のプロファイル名は、以下の形式です。

   ```
   server_name.home.method
   ```

   server_name
   サーバーの名前です。8 文字以下でなければなりません。

home
ホームの名前です。192 文字以下でなければなりません。

method
メソッドの名前です。244 からサーバーとホームの名前の長さの合計を引いた残りの長さまで、可能です。たとえば、サーバー名が 8 文字で、ホーム名が 128 文字の場合、メソッド名は、108 (244 - (8 + 128)) 文字まで可能です。

メソッドが SOMDOBJS で保護されており、かつ、

- クライアント・プログラムがそのメソッドを使用してオブジェクトの属性を更新する場合は、そのクライアントにそのメソッド用の UPDATE 許可を与えます。
- クライアント・プログラムがそのメソッドを使用してオブジェクトの属性を読み取る場合は、そのクライアントにそのメソッド用の READ 許可を与えます。

すべての名前は、ユーザーがどのように入力しても、大文字に変換されます。したがって、MY_server.MY_home.MY_method と MY_SERVER.MY_HOME.MY_METHOD の間には違いはありません。

RACF SOMDOBJS 定義に加えて、WebSphere for z/OS 管理アプリケーションを経由してメソッド・レベルのアクセス検査を指定しなければなりません。アプリケーションのコンテナーを定義する場合は、メソッド・レベルのアクセス検査のボックスをチェックします。

4. DB2 for OS/390、IMS、および CICS などのリソース・マネージャーは、独自のリソース制御をインプリメントしています。これらのリソース制御は、クライアントがリソースにアクセスする機能を制御します。

   DB2 for OS/390 によってリソース制御を使用する場合は、DSNR RACF クラスを使用するか (RACF サポートがある場合)、関連する DB2 for OS/390 GRANT ステートメントを発行します。

   IMS アクセスのための OTMA へのアクセスは、FACILITY クラス (IMSXCF.OTMACI) を通じて行われます。CICS のための EXCI へのアクセスは、SURROGAT クラス (*.DFHEXCI) を通じて行われます。

   データ・セットへのアクセスは、DATASET クラスを通じて制御でき、HFS ファイルへのアクセスは、ファイル・アクセス権を通じて制御できます。

ユーザー識別、認証、およびネットワーク・セキュリティーの問題

どのようなシステムでも正常なセキュリティーであれば、ユーザーまたはプログラムに自分自身を識別させ、本人であることを証明する (自分自身を認証す

る) よう要求します。図4 に、システム内およびシステム間で WebSphere for z/OS が使用するユーザー識別および認証の種類が記載されています。

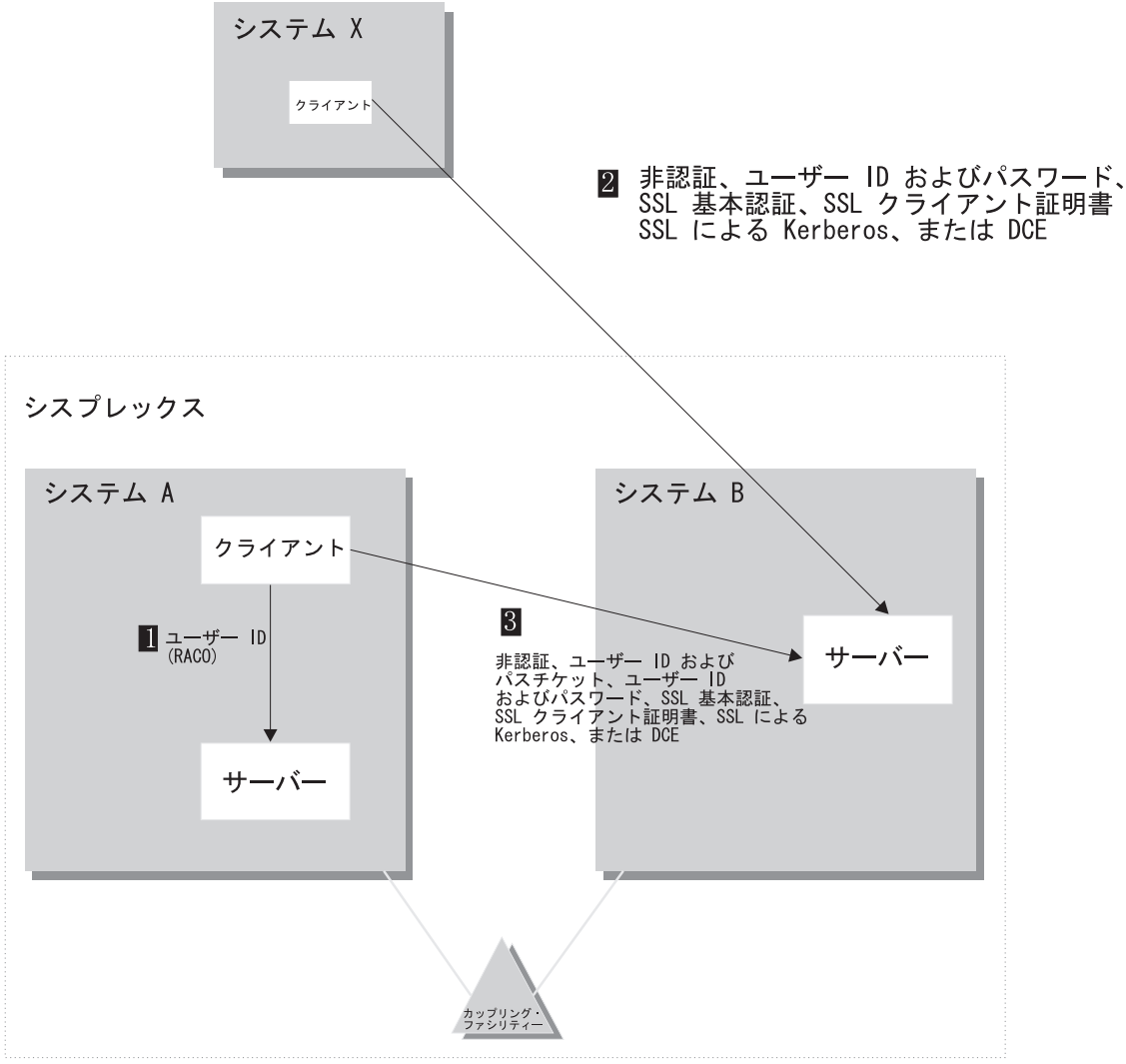


図 4. 識別および認証

以下は、図4 の番号付きの項目についての説明です。

1. ローカル・クライアントおよびサーバーは、サービスを要求する際にユーザー ID を使用して自分自身を識別します。WebSphere for z/OS は、同一のシスプレックス内で稼働しているローカル・クライアントおよびサーバーに

対して、RACO と呼ばれる、ユーザーのアクセス機能環境エレメント (ACEE) の移送可能な形式を使用します。RACO は WebSphere for z/OS システム全体で使用され、すべてのタスクが要求元の ID の下で実行されることを保証します。ユーザーの ID がオペレーティング・システムによってすでに確立されているため、認証は要求されません。他の OS/390 アプリケーションと同様に、WebSphere for z/OS は、オペレーティング・システムを使用してユーザー ID を追跡し、作業の実行中にセキュリティー・サービスを呼び出します。

2. 交換されるすべてのメッセージがトラステッド・ネットワーク内だけを流れることに確信が持てる場合以外、クライアントとサーバーの確実性、メッセージの機密性、およびメッセージの保全性は重要な問題となります。クライアントは、正当なサーバーからサービスを受け取っていることを確認する必要があり、サーバーはクライアントがだれであるかを確認する必要があります。また双方とも、交換するメッセージが悪意の第三者による悪用やスヌープから保護されていることに確信を持ちたいと望むので、移送メディアのセキュリティー (メッセージの保護) に無関心ではいられません。WebSphere for z/OS は複数の認証機構を備えており、そのいくつかはメッセージ保護に関与しています。使用するネットワークの性格に基づいて、どの認証機構が必要であるかを決定する必要があります。
   - 非認証クライアントを受け入れるようサーバーを構成すると、セキュリティーのないネットワークを作成することができます。この方法でサーバーを構成すると、ID のないすべての要求が、サーバーによって確立されたデフォルトの ID の下で実行されます。
   - WebSphere for z/OS クライアントから、ユーザー ID / パスワードのセキュリティーを使用することができます。これは、クライアントの妥当性検査は行いますが、メッセージの保護も、またサーバーが許可されている保証もありません。ユーザー ID / パスワードのセキュリティーを決して非トラステッド・ネットワークで使用しないでください。なぜなら、ユーザー ID とパスワードを傍受して再使用すれば、システムに簡単に侵入できるからです。
   - ネットワーク内の保護されている通信およびユーザー認証にセキュリティーを追加したい場合は、Secure Sockets Layer (SSL) のセキュリティーを使用することができます。SSL は、暗号化テクノロジーによって通信リンクのセキュリティーを提供し、ネットワーク内のメッセージの保全性を確保します。双方の当事者間で通信が暗号化されているので、第三者はメッセージを悪用できません。

また、SSL は、通信する当事者たちの ID を証明するメソッドも提供します。WebSphere for z/OS での SSL サポートを通じて、サーバーとクライアントの ID を証明するのに次の 3 つの方法があります。

- 基本認証 (SSL タイプ 1 認証)。この場合、サーバーはクライアントにディジタル証明書を渡すことによってサーバーの ID を証明します。ちょうど、外国に入国するのにパスポートを提示するのと同じことです。クライアントは、ターゲット・サーバーに既知のユーザー ID とパスワードを渡すことによって、サーバーに対してクライアントの ID を証明します。
- クライアント証明書サポート。この場合、サーバーとクライアントの両者は、ディジタル証明書を提供して互いに自己の ID を証明します。

  クライアント証明書サポートは、アサート ID と呼ばれる機能も提供します。この機能では、中間サーバーがターゲット・サーバーにクライアントの ID を安全かつ効率的な方法で送信できます。この機能では、中間サーバーを SSL セッションの所有者として確立するために、クライアント証明書サポートが必要です。RACF を通じて、システムは中間サーバーをトラステッドにできるかどうかを検査できます (特殊な RACF アクセス権が制御領域などのアドレス・スペースに与えられ、それらのアドレス・スペースは安全なシステム・コードを実行します)。この中間サーバーに対する信頼が確立されれば、ターゲット・サーバーがクライアント ID (MVS ユーザー ID) を別個に検証する必要はありません。クライアント ID は単にアサートされるだけで、認証は必要ありません。
- SSL 上の Kerberos は、使用できるもう 1 つの認証機構です。WebSphere for z/OS では、完全な認証機構を提供するために Kerberos クライアント認証が SSL と一緒に使用されます。その場合、SSL はメッセージのセキュリティーを提供し、クライアントに対してサーバーを認証します。Kerberos 自体は、サーバーがクライアントを認証する能力を提供します。

SSL と Kerberos サポートはオプションです。これらを使用せずに WebSphere for z/OS を実行した場合、暗号化機能と認証機能だけが影響を受けます。それでも、その他の認証機構を使用できます。

SSL についての詳細は、327ページの『WebSphere for z/OS 用の SSL セキュリティーのセットアップ』を参照してください。Kerberos の詳細については、346ページの『WebSphere for z/OS 用の Kerberos セキュリティーのセットアップ』を参照してください。

- 分散コンピューティング環境 (DCE) のセキュリティーは、信頼されていないネットワーク内の別々のシステム上のクライアントおよびサーバーに対して使用できる、もう 1 つのオプションです。DCE は、第三者の検証技法を使用します。これは、クライアントが正しいサーバーと通信しており、サーバーが正しいクライアントと通信していることを検証します。DCE を使用すると、ユーザーはメッセージを暗号化したり、メッセージの悪用を検査することもできます。

  DCE サポートはオプションです。DCE をインストールせずに WebSphere for z/OS を実行した場合、DCE 暗号化機能と認証機能だけが影響を受けます。DCE のインストールおよび活動化をしない場合、WebSphere for z/OS は、DCE を使用してリモート・クライアントを認証することはできません。

  DCE の使用およびその要件についての詳細は、421ページの『付録C. DCE のセットアップ』を参照してください。

3. シスプレックス内でのクライアントとサーバーのセキュリティー・サポートは、ローカルとネットワークの両方の場合のプロパティーをいくつか備えています。すべてのネットワーク・プロトコルは、シスプレックスの内部において、クライアントとサーバーの間でサポートされます。また、パスチケットがサポートされており、その場合は、クライアントのユーザー ID が識別に使用され、パスチケットが認証に使用されます。パスチケットは、動的に生成される 1 回限りの使用のパスワードです。

   シスプレックス内での通信は、一般に、保護されたネットワークを通じて直接流されるので、WebSphere for z/OS は、通常、それらの通信ではメッセージの暗号化によるオーバーヘッドを回避します。

クライアントがサーバーに接続する場合、接続処理の一部として、クライアントとサーバーの間で、どのセキュリティー・プロトコルを使用するかについての折衝が行われます。これは、上級のトピックです。セキュリティー・プロトコルの折衝の詳細については、324ページの『クライアントおよびサーバーのセキュリティー・プロトコルの折衝方法』に説明があります。

識別および認証についての指定

識別について、各制御領域およびサーバー領域開始プロシージャーは、独自のユーザー ID を持っていなければならず、ユーザーはそれを STARTED クラスに定義しなければなりません。制御領域は信頼されていますが、サーバー領域は信頼されていません。これについては、21ページの『許可検査』で説明しています。それぞれに対して異なるリソース許可を与える必要があるため、制御領域およびサーバー領域に対して異なるユーザー ID を与える必要があります。

インストール用に、追加のユーザー ID が必要になります。RACF サンプル内にこれらのユーザー ID 用の定義が提供されています。84ページの『RACF セキュリティーをセットアップするためのステップ』を参照してください。

- 制御領域とサーバー領域のユーザー ID。
- インストール検査プログラムおよびそのアプリケーション・サーバー用のユーザー ID。RACF サンプルでは CBIVP を使用しています。
- 管理アプリケーションが使用する CBADMIN と呼ばれるユーザー ID。
- 管理アプリケーションを経由して各サーバーに関連付けられたデフォルトのローカルおよびリモート・ユーザー ID。ここでは、CBGUEST を使用しています。

WebSphere for z/OS ランタイム用の必要なユーザー ID および RACF 定義は、RACF サンプルで提供されています。

認証に関しては、オペレーターが START コマンドおよび制御領域開始プロシージャーを使用してサーバーを開始します。開始プロシージャーのユーザー ID の認証は、オペレーターが開始プロシージャーを開始したという事実の効果によって行われます。つまり、パスワードは必要ありません。サーバーを開始するオペレーターの能力を制限したい場合は、RACF 内の OPERCMDS クラスを経由して行います。

セキュリティー監査

セキュリティー監査は、セキュリティー製品によって通常の方法で処理されます。WebSphere for z/OS は、システム許可機能 (SAF) を使用します。これは、OS/390 または z/OS 内の他の機能と一貫性のある監査機構を提供します。

セキュリティー管理

セキュリティー管理は、セキュリティー製品によって通常の方法で処理される必要があります。

必要なシステム・セキュリティーの選択

必要なセキュリティーと、インストールおよびカスタマイズしなければならないコンポーネントを決定します。どのセキュリティー機構が要件に最も適合するかを判断する前に、使用するアプリケーション、サーバー間の対話、およびネットワーク・トポロジーに基づいて、必要なセキュリティーを判別する必要があります。

この作業を始める前に: WebSphere for z/OS が、ランタイムにどのように基礎セキュリティー・システムを使用するか理解している必要があります。19ページの『セキュリティーのセットアップ』に WebSphere for z/OS セキュリティーの概要が記載されています。

次のステップに従って、必要なセキュリティーを選択してください。

1. 使用するアプリケーションに保護が必要かどうかを判断します。

   使用するアプリケーションで機密データの交換を行わず、参加者の ID が必要でない場合は、ほとんどのセキュリティー制御を回避することができ、このトピックの残りの部分を無視してもかまいません。

   注: 管理アプリケーションを通じてサーバーが非認証要求を認めるようにし、RACF を通じて非認証要求を処理するために使用される OS/390 または z/OS ユーザー ID をセットアップする必要があります。

---

2. 使用するアプリケーションが非トラステッド・ネットワークで動作し、しかも、それらのアプリケーションで機密データや主幹業務データを処理する場合は、メッセージの保全性や機密性をサポートするいずれかのセキュリティー機構を選択してください (表6)。

表 6. ネットワーク内の信頼に基づいた推奨セキュリティー機構

	非 SSL セキュリティー				SSL ベースのセキュリティー			
ネットワークのタイプ	**ローカル**	**パスチケット**	**ユーザー ID / パスワード**	**DCE**	**基本認証**	**Kerberos**	**クライアント証明書**	**アサート ID**
トラステッド	✔	✔	✔	✔	✔	✔	✔	✔[a]
非トラステッド		[b]	[c]	✔	✔	✔	✔	

注:

a. アサート ID を管理するには、中間サーバー上で信頼について管理上の協議が行われる必要があります。

b. 一般に、シスプレックス内の通信は XCF 接続を通じて保護されます。パスチケット・セキュリティーは、シスプレックスのメンバー間でのみ使用されるので、ネットワークの残りの部分の構成は関係がありません。

c. **決して**、非トラステッド・ネットワーク上でユーザー ID とパスワードを**送信しないでください。**管理アプリケーションはワークステーションから WebSphere for z/OS に、ユーザー ID とパスワードを通じて接続することに注意してください。

3. アプリケーションに、リモート・サーバーへの要求を発行するサーバー・コンポーネント (Enterprise bean または CORBA コンポーネント) が存在する場合は、認証された ID をリモート・サーバーへ伝送することに対処できるセキュリティー機構を考慮してください。一部の機構を使用すると、リモート・サーバーにクライアント ID を伝搬する (委任する) ことができ、一部の機構は、中間サーバーの ID を伝送します (表7)。

表 7. ユーザー ID を伝搬する必要に基づいた推奨セキュリティー機構

	非 SSL セキュリティー				SSL ベースのセキュリティー			
伝搬のタイプ	**ローカル**	**パス チケット**	**ユーザー ID / パスワード**	**DCE**	**基本 認証**	**Kerberos**	**クライアント 証明書**	**アサート ID**
サーバーはクライアント ID を転送できる	✔	✔		✔		✔		✔

4. 最後に、使用するソフトウェア構成と、サーバーとの対話を行うクライアントのタイプに応じて、使用するセキュリティー機構のタイプを決定します (表8)。

表 8. ソフトウェア構成とクライアントの特性に基づいた推奨セキュリティー機構

	非 SSL セキュリティー				SSL ベースのセキュリティー			
クライアントの 特性	**ローカル**	**パス チケット**	**ユーザー ID / パスワード**	**DCE**	**基本 認証**	**Kerberos**	**クライアント 証明書**	**アサート ID**
同じ OS/390 または z/OS システム上	✔							
同じシスプレックス内		✔	✔	✔	✔	✔	✔	✔
リモート共用 RACF データベース内に登録済み			✔	✔	✔	✔	✔	✔
共用でないリモート RACF データベース内に登録済み				✔		✔	✔	
WebSphere Application Server エンタープライズ版 (分散) C++				✔			✔	
WebSphere Application Server エンタープライズ版 (分散) Java				✔	✔			
CICS							✔	
OEM ORB							✔	

ここで、選択したコンポーネント用のセキュリティー管理をインプリメントすることができます。

システム・セキュリティーの選択の例

これは、システムのセキュリティー機構をどのように選択すればよいかを考慮する方法の一例です。

この例では、あるシスプレックス内に 2 台の J2EE サーバー (CBSRV1 と CBSRV2) を配置します。クライアントは CBSRV1 を通じてシステムと通信し、CBSRV1 は保護されたシスプレックスを通じてクライアント ID を CBSRV2 へ伝搬します。クライアントは WebSphere Application Server エンタープライズ版 (分散) 上で実行され、シスプレックスとの対話はトラステッドでないネットワーク上で行われます。アプリケーションで使用するデータは、保護されて機密が保たれた状態であることが必要です。

1. データの機密性を保護し、クライアント ID を知る必要があるので、最初の判断は明らかです。つまり、ネットワークが非トラステッドなので、メッセージの保全性と機密性をサポートするセキュリティー機構を使用しなければなりません (34ページの表6 を参照)。
2. 使用するアプリケーションは、クライアント ID が他のサーバーへ伝搬されることを必要とします。この場合は、パスチケット、アサート ID、Kerberos、DCE のいずれかを使用できます (35ページの表7 を参照)。
   - パスチケットのセキュリティーは、一般に、シスプレックス内で最も簡単にセットアップできますが、1 つのアドレス・スペースで 1 秒当たり 1 つのパスチケットしか使用できないという制限があります。
   - アサート ID のセキュリティーは共用 RACF データベースを必要とし、このデータベースはシスプレックス内にインプリメントできます。この場合は、CBSRV1 と CBSRV2 用に、RACF を通じて SSL 証明書と鍵リングを定義する必要があります。また、CBSRV1 と CBSRV2 の間に信頼関係を定義するために、CBSRV1 に CB.BIND.CBSRV2.* プロファイルについての RACF CONTROL 権限を与えなければなりません。
   - Kerberos のセキュリティーは、WebSphere for z/OS で最も堅固なセキュリティー機構です。Kerberos はスケーラブルで、Kerberos ネットワーク ID を安全に委任でき、OS/390 または z/OS ユーザー ID を必要としません。しかし、Kerberos と SSL のインストールと構成を行う必要があり、これは重要なタスクです。
   - DCE セキュリティーは、すでに DCE セキュリティーをインプリメントしてある場合にはオプションです。

ここでは、パスチケットのセキュリティーを選択します。その理由は、アプリケーションのトランザクションのボリュームが小さくなることがわかっており、セキュリティー・タスクと管理を最小にしたいからです。

3. 最後に、ネットワークの対話用に SSL 基本認証を選択します。その理由は、WebSphere Application Server エンタープライズ版がこのセキュリティー機構をサポートするからです。

この例では、CBSRV1 にパスチケットと SSL タイプ 1 (基本認証) を定義し、CBSRV2 にパスチケットを定義します。

ワークロード管理 (WLM) のセットアップ

WebSphere for z/OS は、OS/390 または z/OS 内のワークロード管理 (WLM) 機能を使用して、ワークロードを管理します。この節は、それを始めるための手助けを提供しており、WebSphere for z/OS システムを機能させるには十分です。ワークロード管理の拡張トピックは、301ページの『第6章 拡張トピック』にあります。

ワークロード管理 (WLM) のゴール・モードでのセットアップ

WebSphere for z/OS は、OS/390 または z/OS がゴール・モードでワークロード管理を実行することを必要とします。システムが互換モードで稼働している場合は、ゴール・モードをインプリメントしなければなりません。ワークロード管理の詳細については、*z/OS MVS 計画 : ワークロード管理*, SA88-8574 を参照してください。

ランタイム・サーバー用のワークロード管理のセットアップ

ワークロード管理のゴール・モードでのセットアップに加えて、WebSphere for z/OS サーバーおよびビジネス・アプリケーション用にワークロード管理ポリシーを定義する必要があります。この節では、ランタイム・サーバー用の指定について説明しています。ワークロード管理およびビジネス・アプリケーションについての詳細は、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

ワークロード管理およびランタイム・サーバーについてのバックグラウンド

システム管理サーバー、ネーミング・サーバー、およびインターフェース・リポジトリー・サーバー用のアプリケーション環境を定義する必要があります (デーモン・サーバー用のアプリケーション環境は定義しません)。これらの定義なしでは、WebSphere for z/OS は始動しません。

注: これらを開始するには、専用の種別規則および作業修飾子を定義する必要はありませんが、実動システム用にこれを行いたい場合があります。詳しくは、352ページの『拡張パフォーマンス制御のインプリメント』を参照してください。

インストール検査プログラムにはサーバーが必要なので、MOFW と J2EE のどちらのコンポーネントの使用を計画しているかに応じて、MOFW アプリケーション・サーバーか J2EE アプリケーション・サーバー、またはその両方について、アプリケーション環境を定義する必要もあります。このサーバーは、以下の表に含まれています。

ビジネス・アプリケーション用のサーバーと同様に、WebSphere for z/OS ランタイム・サーバー (デーモンを除く) には、1 つの制御領域および 1 つまたは複数のサーバー領域があります。これらの領域は、表9 に示されている開始プロシージャーによって開始されます。

表 9. ランタイム制御およびサーバー領域の開始プロシージャー

サーバー	サーバー名	制御領域の開始プロシージャー	サーバー領域の開始プロシージャー
ネーミング・サーバー	CBNAMING	BBONM	BBONMS
システム管理サーバー	CBSYSMGT	BBOSMS	BBOSMSS
インターフェース・リポジトリー・サーバー	CBINTFRP	BBOIR	BBOIRS
MOFW アプリケーション・サーバー	BBOASR1	BBOASR1	BBOASR1S
J2EE アプリケーション・サーバー	BBOASR2	BBOASR2	BBOASR2S

ビジネス・アプリケーション・サーバーの場合、自分で制御領域を開始しなければなりません。ただし、WebSphere for z/OS ランタイム・サーバーの場合は、デーモンのみを開始する必要があります。デーモンは、次にシステム管理サーバー、ネーミング・サーバー、およびインターフェース・リポジトリー・サーバー用の制御領域を開始します。ワークロード管理は、作業要求が到着すると同時にサーバー領域を動的に開始します。したがって、39ページの表10 に示すように、**サーバー**領域の開始プロシージャーを開始するよう指定する

WLM アプリケーション環境を作成しなければなりません。たとえば、ワークロード管理が BBOASR1 サーバーを開始する開始プロシージャー名として BBOASR1S を指定します。

また、ビジネス・アプリケーション用に作成した新規のサーバーごとに、ワークロード管理を定義する必要があります。*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

ランタイム・サーバー用のワークロード管理ポリシーの定義

ISPF アプリケーション IWMARIN0 を使用して、以下の表に従って、WLM アプリケーション環境を定義します。

表 10. ランタイム・サーバー用のアプリケーション環境の仕様

ランタイム・サーバー	アプリケーション環境	サブシステム・タイプ	ランタイム・サーバー領域用のプロシージャー名	開始パラメーター	サブシステム・インスタンス[1] 用の開始サーバーのアドレス・スペース制限
ネーミング・サーバー	CBNAMING	CB	BBONMS	IWMSSNM=&IWMSSNM	制限なし
システム管理サーバー	CBSYSMGT	CB	BBOSMSS	IWMSSNM=&IWMSSNM	制限なし
インターフェース・リポジトリー・サーバー	CBINTFRP	CB	BBOIRS	IWMSSNM=&IWMSSNM	制限なし
MOFW アプリケーション・サーバー	BBOASR1	CB	BBOASR1S	IWMSSNM=&IWMSSNM	システム[2]ごとの単一アドレス・スペース
J2EE アプリケーション・サーバー	BBOASR2	CB	BBOASR2S	IWMSSNM=&IWMSSNM	システムごとの単一アドレス・スペース

表 10. ランタイム・サーバー用のアプリケーション環境の仕様 (続き)

ランタイム・サーバー	アプリケーション環境	サブシステム・タイプ	ランタイム・サーバー領域用のプロシージャー名	開始パラメーター	サブシステム・インスタンス[1] 用の開始サーバーのアドレス・スペース制限

注:

1. 「制限なし」か、または「システムごとの単一アドレス・スペース」を指定することができます。「シスプレックスごとの単一アドレス・スペース」は指定できません。
2. MOFW インストール検査プログラムは、BBOASR1 内で稼働し、他のトランザクションに対して使用可能な一時オブジェクトの状態を作り出すプログラムの一例です。これは、すべてのトランザクションが同一のアドレス・スペース (サーバー領域) 内で稼働する必要があります。すべてのトランザクションが同一のサーバー領域内で稼働しない場合、あるトランザクションはあるサーバー領域内で処理を行い、一時オブジェクトの状態に依存する 2 つ目のトランザクションは別のサーバー領域内で処理を行います。ただし、一時オブジェクトの状態は、2 番目のトランザクションに対しては使用可能にはなりません。BBOASR1 のようなサーバーをセットアップするには、以下を行わなければなりません。
   a. サーバー用に 1 つのサーバー・インスタンスのみをセットアップします。複数のサーバー領域 (アドレス・スペース) を作ることになるため、サーバー・インスタンスの複製を作ることはできません。
   b. ワークロード管理の「サブシステム・インスタンス用の開始サーバーのアドレス・スペース制限」を「システムごとの単一アドレス・スペース」に設定します。複数のサーバー領域 (アドレス・スペース) を作ることになるため、「制限なし」は使用できません。
   c. 管理アプリケーションを使用して、アプリケーション・サーバー用に以下のサーバー属性を設定します。
      - 「実動 (Production)」チェック・ボックスをチェックします。
      - 「分離ポリシー (Isolation policy)」を「サーバー領域につき複数トランザクション (multiple transactions per server region)」に設定します。

ワークロード管理に対するアプリケーション環境の定義についての詳細は、*z/OS MVS 計画：ワークロード管理*, SA88-8574 を参照してください。

以下の例は、BBOASR1 用のアプリケーション環境の作成方法を示しています。39ページの表10 のサーバーごとに、例中のステップを実行しなければなりません。

IWMARIN0 の使用例: 以下は、アプリケーション環境を定義する場合に IWMARIN0 内で使用する画面を示しています。

この作業を始める前に: IWMARIN0 のユーザーは、RACF FACILITY クラスのプロファイル MVSADMIN.WLM.POLICY への更新アクセスを持っていなければなりません。

以下のステップを実行して、BBOASR1 アプリケーション環境を作成します。

1. 以下のように、IWMARIN0 を発行してメイン画面を開き、オプション 9 を選択します。

```
  File  Utilities  Notes  Options  Help
-------------------------------------------------------------------------------
Functionality LEVEL003         Definition Menu         WLM Appl LEVEL004
Command ===> ____________________________________________________________

Definition data set  . . : 'CB.MYCB.WLM'

Definition name  . . . . . CB390      (Required)
Description  . . . . . . . WLM Setup for WebSphere for z/OS

Select one of the
following options. . . . . 9__  1.  Policies
                               2.  Workloads
                               3.  Resource Groups
                               4.  Service Classes
                               5.  Classification Groups
                               6.  Classification Rules
                               7.  Report Classes
                               8.  Service Coefficients/Options
                               9.  Application Environments
                              10.  Scheduling Environments
```

2. 以下に示すように、次の画面上のフィールドを埋めます。

```
  Application-Environment  Notes  Options  Help
-------------------------------------------------------------------------------
                    Create an Application Environment
Command ===> ____________________________________________________________

Application Environment  . . . BBOASR1_____________________________  Required
Description  . . . . . . . . . . CB IVP Server_____________________
Subsystem Type . . . . . . . . . CB__                                Required
Procedure Name . . . . . . . . . BBOASR1S
Start Parameters . . . . . . . . IWMSSNM=&IWMSSNM_____________________
                                 ___________________________________
                                 ___________________________________

Limit on starting server address spaces for a subsystem instance:
2   1.  No limit
    2.  Single address space per system
    3.  Single address space per sysplex



   .-------------------------------------------------------------------.
   | Selection List empty. Define an application environment. (IWMAM600) |
   '-------------------------------------------------------------------'
```

3. アプリケーション環境を保存します。以下の画面が表示されます。

```
  Application-Environment  Notes  Options  Help
------------------------------------------------------------------------------
                  Application Environment Selection List     Row 1 to 12 of 12
Command ===> ____________________________________________________________

Action Codes: 1=Create, 2=Copy, 3=Modify, 4=Browse, 5=Print, 6=Delete,
              /=Menu Bar

Action  Application Environment Name      Description
  __     BBOASR1                          CB IVP Server
****************************** Bottom of data ********************************
```

4. 「ユーティリティー (Utilities)」メニューから、「インストール (Install)」定義を選択します。

5. 「ユーティリティー (Utilities)」メニューから、「サービス・ポリシーを活動化する (Activate service policy)」を選択します。

6. 「ファイル (File)」メニューから「終了 (exit)」を選択します。

リソース・リカバリー・サービスに関する推奨

WebSphere for z/OS は、リソース・リカバリー・サービス (RRS) のセットアップを必要とします。これは、次に、RRS 付加機能 (RRSAF) および DB2 for OS/390 の使用を必要とします。RRS をセットアップする場合は、以下を考慮に入れてください。

1. WLM 管理の DB2 ストアード・プロシージャーのアドレス・スペースを活用するために、OS/390 または z/OS 用の RRS をすでに構成してある場合があります。しかし、DB2 for OS/390 が、トランザクション・コミットに加わっている、RRS にのみ準拠のリソース・マネージャーである場合、最適化は、システムがシステム・ロガーの RRS の使用をう回する原因となります。つまり、インストールが RRS を構成している間は、ログ・ストリームに最小の活動しかないことを意味します。WebSphere for z/OS は、RRS 準拠のリソース・マネージャーで、DB2 for OS/390 とのトランザクション・コミットに加わります。したがって、WebSphere for z/OS は、システム・ロガー・ログ・ストリームへのデータの書き込みを開始するための RRS を必要とします。ログ・ストリームのサイズを調整する必要がある場合があります。
   - WebSphere for z/OS は、RM.DATA ログへの重大な影響は与えません。

- クライアントおよびコンテナー両方のトランザクション・ポリシーによっては、MAIN.UR ログ内に何の活動もない場合があります。このように活動がなくても、問題ありません。
- コンテナー用に定義されたトランザクション・ポリシーによっては、MAIN.UR ログ・ストリームより DELAYED.UR ログ・ストリーム内により多くの活動がある場合があります。一般に、WebSphere for z/OS は、単一のサーバー領域内でアクセスまたは変更された保護リソースに対してさえも、変更済みの分散コミットを実行します。ユーザーは、これらのグローバル・トランザクションを未確定状態で監視することができます。未確定とは、トランザクションが指定されたアプリケーション・サーバーに対してローカルな場合の、非常に短期間の状態を言います。ただし、トランザクションが未確定状態に入るため、RRS は強化されたデータを DELAYED.UR ログにログ記録します。

  WebSphere for z/OS のすべての RRS トランザクション・ログは、DELAYED.UR ログ・ストリーム内で単独で発生します。このようなロギングは、WebSphere for z/OS の今後のリリースで変更される場合があります。そのため、MAIN.UR ログ・ストリームを構成しておくのも良いかと思われます。そうすることによって、新規のコンテナーを配置したり、または WebSphere for z/OS の基盤の構造が変更した場合にも、実動ワークロードを処理することができます。
- WebSphere for z/OS は、RESTART ログへの重大な影響は与えません。
- ARCHIVE ログについてのポリシーを変更する理由はありません。オプションではありますが、ARCHIVE ログの使用をお勧めします。これには、パフォーマンスに関して小さなマイナスの影響があります。ログの保存期間を通常の期間に設定してください。

2. WebSphere for z/OS のオブジェクト・トランザクション・サービスは、異なるロギング・グループ内で再始動された場合は検出されません。これは、トランザクション・リカバリーに影響します。再始動位置を制御する自動再始動管理 (ARM) の使用をお勧めします。
3. 構造サイズについては、初期セットアップ値として以下をお勧めします。経験を重ねるにつれ、以下を調整する必要がある場合があります。

表 11. ログ・ストリームの推奨サイズ

ログ・ストリーム	初期サイズ	サイズ
RM.DATA	1 MB	1 MB
MAIN.UR	5 MB	50 MB
DELAYED.UR	5 MB	50 MB
RESTART	1 MB	5 MB

表 11. ログ・ストリームの推奨サイズ (続き)

ログ・ストリーム	初期サイズ	サイズ
ARCHIVE	5 MB	50 MB

ログ・ストリーム上で MAXBUFSIZE を検査してください。このサイズが小さすぎると、DB2 for OS/390 の障害が発生するおそれがあります。

リソース・リカバリーについての詳細は、*z/OS MVS プログラミング : リソース・リカバリー*, SA88-8582 にあります。RRS 付加機能についての詳細は、*DB2 (OS/390 版) 適用業務プログラミングおよび SQL の手引き*, SC88-7377 に記載されています。

RMF および他のモニター・システムについてのガイドライン

選択するいずれのパフォーマンスおよびモニター・システムを使用することができます。

DB2 for OS/390 データベースおよび LDAP

この節では、WebSphere for z/OS がどのように DB2 for OS/390 および LDAP (Lightweight Directory Access Protocol) を使用するかの説明、これら 2 つの機能のガイドラインの提供、DB2 for OS/390 操作上の考慮事項についての説明、および LDAP セキュリティーについての規則の説明を記載しています。

インストールおよびカスタマイズが完了したら、RACF を使用して DB2 for OS/390 リソースを保護できます。詳しくは、292ページの『DB2 for OS/390 の RACF 保護のセットアップ』を参照してください。

DB2 for OS/390 および LDAP についてのバックグラウンド

この節では、WebSphere for z/OS、DB2 for OS/390、および LDAP の関係について説明します。

WebSphere for z/OS の場合、OS/390 または z/OS Security Server の LDAP コンポーネントは、Java Naming and Directory Interface (JNDI) と CORBA (MOFW) ネーミングおよびインターフェース・リポジトリー・サービス用にディレクトリー・サービスを提供します。ディレクトリーのコンテンツは、DB2 for OS/390 表に格納されます。

インストールとカスタマイズのときに、LDAP サーバーを作成 (または既存の LDAP サーバーを使用) し、LDAP データベースを作成し、バインド・ジョブ

を実行し、DB2 for OS/390 の認可を設定し、LDAP ディレクトリーを初期化する必要があります。94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』に、これらの説明が記載されています。

実行時に、EJB コンポーネントは LDAP サーバーがネーム・サービス用に実行されていることを必要とします。インストールとカスタマイズのときに作成した LDAP サーバーをこの目的に使用することをお勧めします。MOFW コンポーネントは LDAP サーバーが実行されていることを必要としません。なぜなら、MOFW コンポーネントはネーミング・サーバーに頼り、ネーミング・サーバーは独自のアドレス・スペースで LDAP DLL を実行するからです。どちらの場合でも、LDAP アクセス制御リストへのユーザーの追加など、管理の目的で LDAP サーバーが必要です。

DB2 for OS/390 および LDAP についてのガイドライン

以下のガイドラインに従って、DB2 for OS/390 および LDAP をセットアップしてください。

- DB2 for OS/390 ログのサイズを検査します。WebSphere for z/OS が生成するトランザクションの数によっては、サイズを大きくする必要があります。
- BP32K バッファー・プールを少なくとも 100 に増やします。
- DSNDB07 データベースのサイズを検査します。
- DB2 for OS/390 用の 32K 一時ワークスペースを検査します。ユーザーのインストールでは、このワークスペースを使用したことがないかもしれませんが、WebSphere for z/OS はこれを使用します。DB2 for OS/390 のインストール中に DNSTIJTM と呼ばれる DB2 for OS/390 ジョブを実行して、このワークスペースを割り振らなければなりません。この割り振りの大きさが十分でない場合、LDAP サーバー、システム管理サーバー、またはネーミング・サーバーを立ち上げる際に SQL -904 戻りコードを受け取る場合があります。
- WebSphere for z/OS は、行レベルのロックおよびタイプ 2 索引を使用しますので、注意してください。
- 可能であれば、WebSphere for z/OS LDAP テーブルを他の LDAP テーブルとは別に保持してください。LDAP テーブルのこれらのセットを別々に保持する理由は、WebSphere for z/OS LDAP テーブルを WebSphere for z/OS システム管理と共にユニットとしてバックアップする必要があるからです。WebSphere for z/OS LDAP テーブルが他の LDAP テーブルと別々になっていれば、このような整合バックアップの実行がより簡単になります。さらに、WebSphere for z/OS 環境を復元する必要がある場合、WebSphere for

z/OS LDAP テーブルの復元が、他のアプリケーションで使用している LDAP によって妨害されることはありません。

- LDAP データベースの管理に使用するパスワードを変更することもできます。その場合は、LDAP LDIF ファイル (この例では、bboldif.cb という名前です) の中でパスワードを設定し、LDAPBINDPW 環境変数を変更する必要があります。94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』を参照してください。

Java Database Connectivity および静的 SQL についてのガイドライン

Java Database Connectivity (JDBC) は、動的 SQL を使用してデータベース内の関連データにアクセスするための、Java アプリケーション・プログラム用のインターフェースを提供しています。静的 SQL (SQLJ) は、Java アプリケーションおよびアプレット内の組み込み済み静的 SQL のサポートを提供しています。DB2 for OS/390 は、これらのアプリケーション・プログラミング・インターフェースをサポートしています。JDBC、SQLJ、および DB2 for OS/390 の完全な情報については、*DB2 for OS/390 Application Programming Guide and Reference for Java* を参照してください。このトピックでは、JDBC および SQLJ の WebSphere for z/OS による使用に関連するガイドラインを扱っています。

- サーバー・アプリケーション内の JDBC (動的 SQL) および SQLJ (静的 SQL) を使用することができます。
- すべての J2EE サーバーとシステム管理サーバーに、DSNJDBC 計画に対する EXECUTE 権限を付与する必要があります。使用するインストールが DSNJDBC 計画へのパブリック・アクセスを許可する場合は、次のコマンドを発行するだけで済みます。

  ```
  GRANT EXECUTE ON PLAN DSNJDBC TO PUBLIC
  ```

  インストールが DSNJDBC 計画へのパブリック・アクセスを許可しない場合は、すべての J2EE サーバーとシステム管理サーバーに EXECUTE 権限を付与する必要があります。DB2 for OS/390 のセカンダリー許可 ID を使用する場合は、サーバー ID の所属先であるグループにこの権限を付与できます。

  注: インストールとカスタマイズのときに、サンプルの BBOCBGRT ジョブを使用して、さまざまなユーザー ID に、DB2 for OS/390 へのアクセス権限を付与します。この GRANT ジョブは、次のコマンドを発行します。

  ```
  GRANT EXECUTE ON PLAN DSNJDBC TO PUBLIC
  ```

このステートメントは、更新または除去してもかまいません。

- RRSAF 接続機構インターフェース (CAF ではありません) を使用しなければなりません。
- 複数コンテキストのサポートを使用することはできません。
- DSNAOINI 環境変数を DB2 for OS/390 DSNAOINI ファイルを指すように設定しなければなりません。

JDBC および SQLJ のセットアップ、およびアプリケーション・プログラムについての考慮事項の詳細は、*DB2 for OS/390 Application Programming Guide and Reference for Java* を参照してください。

DB2 for OS/390 の操作についての計画

操作について計画する場合は、以下に注意してください。

- WebSphere for z/OS は、制御情報として DB2 for OS/390 を使用します。したがって、WebSphere for z/OS ランタイム・サーバーが稼働するためには、DB2 for OS/390 が稼働していなければなりません。保守を行うために DB2 for OS/390 を停止しようとしている場合は、WebSphere for z/OS も停止しなければなりません。また、LDAP を停止してから、DB2 for OS/390 をシャットダウンする必要があります。
- `-dis thd(*)` コマンドで DB2 for OS/390 スレッドを表示する場合、相関 ID は `CB390` です。AUTHID の列には、活動状態の要求または直前の要求のユーザー ID が入っています。**例:**

```
NAME     ST A   REQ   ID        AUTHID   PLAN     ASID TOKEN
RRSAF    T      9     CB390     DINGES   ?RRSAF   0045 436
RRSAF    T      841   CB390     CBNAMSR1 ?RRSAF   0044 435
RRSAF    T      1457  CB390     CBNAMSR1 ?RRSAF   0031 434
RRSAF    T      83    CB390     CBINTSR1 ?RRSAF   001E 433
RRSAF    T      221   CB390     CBIVP    ?RRSAF   0015 432
RRSAF    T      3709  CB390     CBNAMSR1 ?RRSAF   0038 431
RRSAF    T      1923  CB390     CBSYMCR1 ?RRSAF   0040 12
RRSAF    T      2078  CB390     CBSYMCR1 ?RRSAF   0040 13
RRSAF    DI     2300  CB390     CBSYMCR1 ?RRSAF   0040 14
RRSAF    T      1285  CB390     CBSYMCR1 ?RRSAF   0040 350
RRSAF    T      452   CB390     CBDMNCR1 ?RRSAF   003F 10
RRSAF    T      31    CB390     CBDMNCR1 ?RRSAF   003F 11
```

JDBC 接続の場合、相関 ID はジョブの名前です。**例:**

```
NAME     ST A   REQ   ID        AUTHID   PLAN     ASID TOKEN
RRSAF    T  *   3     BBOASR1S  CBASRU1  DSNJDBC  0039 438
```

LDAP セキュリティーの規則

アクセス制御リスト (ACL) を使用して、LDAP ディレクトリー、サブディレクトリー、または項目へのアクセスを制御することができます。ACL は、どのユーザーが各 LDAP 項目へのアクセスを許可されているか、また、それらのユーザーがどのタイプの操作を実行してよいかを指定します。詳細は、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。LDAP セキュリティーに関連する以下の規則に従ってください。

- CORBA (MOFW) コンポーネント用に、IBM では、LDAP DLL をネーミング・サーバーおよびインターフェース・リポジトリー・サーバーのインスタンス内で稼働するように構成しています。したがって、WebSphere for z/OS ランタイムで稼働している別の LDAP サーバーは必要ありません。

  LDAP DLL をネーミング・サーバーおよびインターフェース・リポジトリー・サーバーのインスタンス内で実行する標準構成に従わず、WebSphere for z/OS ランタイムで稼働している LDAP サーバーに頼る場合は、ACL ベースのアクセス制御を WebSphere for z/OS データにインプリメントしないでください。このような構成で、ACL ベースのアクセス制御をインプリメントすると、WebSphere for z/OS は、データにアクセスできなくなります。

- LDAP アクセス制御リスト内の RACF ユーザー ID を使用することができます。

  例: USER1 が RACF ユーザー ID の場合は、以下の ACL 文を使用します。指定された LDAP 項目に対する最高のアクセス権限が USER1 に与えられます。

  ```
  aclSource: cn=DEPT_A, o=IBM, c=US
  aclEntry: access-id:USER1:object:ad:normal:rwsc
  ```

  ただし、この方法では RACF グループ名は使用できません。これについての詳細、および LDAP がどのように RACF データベースにアクセスするかについては、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。グループ名を使用する場合は、インストールは、WebSphere for z/OS ライブラリー、DB2 for OS/390 ライブラリー、および SYS1.LINKLIB をプログラム制御下に配置しなければなりません。

  推奨: LDAP の初期構成については、LDAP を RACF グループ名でセットアップしないことをお勧めします。

メモリーの使用に関する推奨

WebSphere for z/OS は、メモリーの使用において、従来のアプリケーション・サーバーとは異なります。WebSphere for z/OS をインプリメントすることによって、OS/390 または z/OS の効率のよいメモリー管理を有効利用することができますが、昨今の多くの新しいアプリケーション・サーバーおよび言語と同様、これは、メモリーを大量に消費します。既存のメモリー使用パターンからの変化を感じるかもしれません。この節では、行う必要がありそうな変更についてのアウトラインを提供しています。以下の推奨に従ってください。

1. ロード・モジュールのサイズが大規模で、多くのアドレス・スペースがこれらのロード・モジュールを参照する必要があるため、ランタイムをリンク・パック域 (LPA) 内に動的にロードすることをお勧めします。ランタイムのロード・モジュールは、約 200 MB のサイズを含んでいます。忘れずに、CSA ページ・データ・セットのサイズをそれ相当に増加してください。

   動的 LPA を使用しているので、IPL 時の CSA を増やさなかった場合は、IPL の後、ECSA が使い果たされます。LPA にランタイムを動的にロードした後、ECSA をモニターしてください。
2. ロード・モジュールを steplib またはリンク内に配置することにした場合、追加の 200 MB を各アドレス・スペースの領域の一部として許可しなければなりません。標準的な WebSphere for z/OS の基本インストールは、9 個のアドレス・スペースから成っており、それぞれロード・モジュールの 200 MB のほとんどを参照します。
3. ロード・モジュールをリンク・パック域内に配置するだけでなく、各アドレス・スペースに少なくとも 128 MB の動的区域を与えます。
4. IEFUSI 出口、JES 出口、または TSO セグメントのデフォルトを通して、インストールで領域サイズを制限しているかどうかを確認します。すべての WebSphere for z/OS JCL プロシージャーは、デフォルト REGION=0M で提供されており、これは、できる限り大きな領域を与える必要があることを意味しています。リンク・パック域から実行する場合は、動的区域に最低 128 MB が必要となります。リンク・リストから実行する場合は、最低 328 MB (ロード・モジュール用に 200 MB、動的区域用に 128 MB) が必要となります。

   IEFUSI 出口ルーチンが、最大領域を必要なサイズ (リンク・パック域から実行する場合は最低 128 MB、リンク・リストから実行する場合は最低 328 MB) より小さいサイズに制限している場合は、異常終了となります。この問題を修正するには、IEFUSI 出口ルーチンを変更して、より大きなデフォルト領域を許可するか、あるいは JCL REGION= パラメーターを必要なサイズに変更します。

インストールは、通常、JES2 EXIT06 出口または JES3 IATUX03 出口を経由して、REGION= の指定を制限 (制御) します。このような場合は、WebSphere for z/OS JCL プロシージャーのこの制限を緩めてください。

最後に、TSO セグメントのデフォルト領域サイズを検査して、必要があれば変更します。

アプリケーションのメモリーの使用についての追加情報は、352ページの『拡張パフォーマンス制御のインプリメント』に記載されています。

問題診断についての計画

この節では、以下について説明します。

- WebSphere for z/OS のコンポーネント・トレースの使用
- WebSphere for z/OS エラー・ログ・ストリーム
- ダンプ・データ・セット

問題診断についてのバックグラウンド

WebSphere for z/OS は、コンポーネント・トレース (CTRACE) を使用して、トレース・データ・セット内のトレース・データを取り込み、表示します。WebSphere for z/OS は、コンポーネント名「SYSBBOSS」で CTRACE に対して自分を識別します。CTRACE は、ユーザーに対して以下を許可します。

- ブラウズ・ツールを経由して、TCP/IP および OS/390 UNIX などのその他のコンポーネントを含む複数のトレースをマージする。
- トレース・データを sysprint ではなくデータ・セットに書き込む。これによって、スプール・スペースをフリーに保ちます。
- トレース・データをラップする、またはラップしないことを可能にする。これによって、システム・リソースをよりよく管理することができます。
- CTRACE を使用して、トレース・データを複数のアドレス・スペースから 1 つのデータ・セットに集めるか、または、CTRACE にトレース・データを各アドレス・スペースから別々のデータ・セットへ送信させる。
- WebSphere for z/OS アドレス・スペースの停止および再始動をせずに、トレースを開始および停止する。
- 1 つまたは複数のデータ・セットを使用して、トレース・データを取り込む。これによって、I/O をより効果的に管理することができます。

また、WebSphere for z/OS には、自分のコード内に予期しない状態または障害を検出した場合に、以下のような、エラー情報を記録するエラー・ログ・ストリームがあります。

- 障害の表明
- 回復不能エラー状態
- メモリーなどの、重要なリソースの障害
- オペレーティング・システムの例外
- WebSphere for z/OS コード内のプログラミングの欠陥

使用可能な他の機能に関連するエラー・ログ・ストリームを使用して、活動記録ログ、トレース・データ、システム・ログ記録、およびジョブ・ログなどのエラー情報や状況情報を取り込みます。

WebSphere for z/OS のエラー・ログ・ストリームは、システム・ロガー・アプリケーションです。エラー・ログ・ストリームはシステム・ロガーを使用するため、以下のことがらを行うことができます。

- エラー情報をカップリング・ファシリティー・ログ・ストリームに書き込むことができます。これによって、シスプレックスごとにエラー・ロギングが得られます。あるいは、エラー情報を DASD のみのログ・ストリームに書き込むことができます。これによって、単一システムのみのエラー・ロギングが得られます。

  注: DASD のみのエラー・ロギングを使用している場合は、重大なパフォーマンスへの影響が発生します。
- すべての WebSphere for z/OS の共通ログ・ストリームか、またはサーバーおよびサーバー・インスタンスの個々のログ・ストリームのどちらかをセットアップします。ローカル OS/390 または z/OS クライアント ORB は、ログ・ストリーム内のデータをログに記録することもできます。システム・ロガー API は許可されていないため、いずれのアプリケーションでもこれらを使用することができます。RACF などのセキュリティー製品を通して、ログ・ストリームへのアクセスを制御する必要があります。

WebSphere for z/OS は、REXX EXEC (BBORBLOG) を提供しており、これを使用すると、エラー・ログ・ストリームを表示することができます。デフォルトでは、EXEC がエラー・レコードを 3270 ディスプレイに合うように形式設定します。

この資料では、エラー・ログ・ストリームおよびそのセットアップ方法について説明しています。問題を診断するためのエラー・ログ・ストリームの使用についての情報は、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 に記載されています。システム・ロガーについての一般情報およびガイダンスは、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 に記載されています。52ページの表12 は、エラー・ログ・ストリ

ームに関係のある情報を記載している箇所を示しています。

表 12. WebSphere for z/OS エラー・ログ・ストリーム情報の検索

目的	参照箇所
システム・ロガーについて学習し、その要件を理解する	*z/OS MVS シスプレックスのセットアップ*, SA88-8591
WebSphere for z/OS エラー・ログ・ストリームについて学習する	50ページの『問題診断についてのバックグラウンド』
WebSphere for z/OS エラー・ログ・ストリームを計画し、セットアップする	*z/OS MVS シスプレックスのセットアップ*, SA88-8591 81ページの『エラー・ログ・ストリームをセットアップするためのステップ』
WebSphere for z/OS エラー・ログ・ストリームに必要なカップリング・ファシリティーの構造スペースのサイズを設定する	*z/OS MVS シスプレックスのセットアップ*, SA88-8591
WebSphere for z/OS エラー・ログ・ストリーム用のシステム・ロガー・リソースへのアクセス許可を定義する	81ページの『エラー・ログ・ストリームをセットアップするためのステップ』
WebSphere for z/OS エラー・ログ・ストリームを定義する	81ページの『エラー・ログ・ストリームをセットアップするためのステップ』
WebSphere for z/OS エラー・ログ・ストリームを表示する	*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655
Java アプリケーションがどのようにしてエラー・ログ・ストリーム内にメッセージおよびトレース・データを記録するかについて学習する	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

問題診断の詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 を参照してください。

コンポーネント・トレースについての計画

CTRACE を使用するには、以下のように行います。

- トレース・データ・セットを識別する、および WebSphere for z/OS アドレス・スペースを parmlib メンバー内のデータ・セットに接続するためのトレース・オプションを指定します。
- 初期トレース・パラメーターを考慮に入れて WebSphere for z/OS 環境変数を更新します。

- 通常のエディターではトレース・データを読み取ることはできないため、IPCS-CTRACE を使用して、トレース・データを表示します。

WebSphere for z/OS 用の CTRACE のセットアップについて、詳しくは、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 を参照してください。

ダンプに関する推奨

システム・ダンプについては通常どおり計画します。

自動再始動管理 (ARM) についてのヒント

システム上で自動再始動管理 (ARM) を使用可能にしている場合は、WebSphere for z/OS をインストールおよびカスタマイズする前に、WebSphere for z/OS アドレス・スペース用の ARM を使用不可にしたい場合があります。カスタマイズ中、ジョブ・エラーが、WebSphere for z/OS アドレス・スペースの不必要な再始動を起こす原因となる場合があります。インストールおよびカスタマイズの後で、ARM の使用可能化について検討してください。詳しくは、295ページの『自動化および自動再始動管理のセットアップ』を参照してください。

第3章 WebSphere for z/OS のインストールおよびカスタマイズ

この章の内容は、ここに書かれている順序に従って実行してください。

1. 56ページの『インストールおよびカスタマイズの準備』では、WebSphere for z/OS のカスタマイズおよびランタイム・サーバーの構成を開始する前に、完了しておかなければならないことについて述べています。
2. 64ページの『SMP/E を使用したコードのインストールと、データ・セットのコピー』では、製品コードのインストールに関する情報を示し、次に、WebSphere for z/OS のカスタマイズに使用するデータ・セットをコピーするためのステップについて説明します。
3. 72ページの『OS/390 または z/OS の基本機能のカスタマイズ』では、OS/390 または z/OS の基本機能 (SCHEDxx、PROGxx、LPA、MVS メッセージ・サービス、TCP/IP、エラー・ログ・ストリーム、RACF など) をカスタマイズする方法について説明します。
4. 86ページの『システム管理データベースの定義』では、WebSphere for z/OS がサーバーを管理する際に使用するデータベースを作成する方法について説明します。
5. 88ページの『システム管理 HFS 構造を作成するためのステップ』では、ブートストラップ・プロセス中に使用される、重要な HFS ディレクトリーと初期環境ファイルを作成する方法について説明します。
6. 94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』では、LDAP サーバーのセットアップ方法について説明します。このサーバーは、WebSphere for z/OS のネーム・スペースを作成する際に使用されます。
7. 105ページの『ブートストラップの準備と実行』では、ランタイム・サーバーをセットアップし、WebSphere for z/OS のネーム・スペースを初期化する、ブートストラップ・ジョブおよびその他の関連ジョブを実行する方法について説明します。
8. 116ページの『管理アプリケーションおよび操作アプリケーションのインストール』では、管理アプリケーションおよび操作アプリケーションのインストールに関する情報を提供します。管理アプリケーションは、BBOASR1 サーバーを定義する際また、インストール検査プログラムを実行する際に使用します。

9. 120ページの『インストール検査プログラム用のアプリケーション・サーバーの定義』では、管理アプリケーションを実行して、BBOASR1 および BBOASR2 サーバーを作成する方法について説明します。
10. 192ページの『WebSphere for z/OS インストール検査プログラム (IVP) の実行』では、インストール検査プログラムを実行する方法について説明します。
11. 198ページの『2 番目のインターフェース・リポジトリー・クライアント・ブートストラップの実行』は最終タスクで、2 番目のインターフェース・リポジトリー・ブートストラップを実行する方法について説明します。

インストールとカスタマイズの途中で問題が発生した場合は、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 のトラブルシューティング情報を参照してください。

インストールおよびカスタマイズの準備

インストールおよびカスタマイズを開始する前に、OS/390 または z/OS のサブシステムを作成し、この節のその他のタスクを実行しなければなりません。さらに、カスタマイズを開始する前には、WebSphere for z/OS および OS/390 または z/OS サブシステムに関する重要な情報を決定する必要があります。この節での手順は次のとおりです。

- 『OS/390 または z/OS サブシステムを作成するためのステップ』
- 57ページの『開始に先立って重要な情報を決定するためのステップ』

OS/390 または z/OS サブシステムを作成するためのステップ

この作業を始める前に: 1ページの『第1章 インストールおよびカスタマイズの概要』を読んでおいてください。

以下のステップに従ってください。

1. OS/390 または z/OS サブシステムを作成する (9ページの『第2章 OS/390 または z/OS の基本環境の準備』を参照)。特に、以下の指示およびヒントには必ず従うようにしてください。
   - システム要件。10ページの『WebSphere for z/OS のシステム要件の決定』を参照してください。
   - TCP/IP。16ページの『TCP/IP ネットワークの更新』に記載されているバックグラウンド情報とヒントを参照してください。
   - セキュリティー・サーバー (RACF)。19ページの『セキュリティーのセットアップ』を参照してください。

- ワークロード管理 (WLM)。37ページの『ワークロード管理 (WLM) のセットアップ』を参照してください。
- リソース・リカバリー・サービス。42ページの『リソース・リカバリー・サービスに関する推奨』を参照してください。
- DB2 for OS/390。DB2 for OS/390 と LDAP (まだインストールされていないはずですので、この章でインストールします) に関するバックグラウンド、ガイドライン、および規則については、44ページの『DB2 for OS/390 データベースおよび LDAP』を参照してください。

---

2. RACF ユーザー ID がまだない場合はそれをセットアップし、WebSphere for z/OS ファイル (BBO.* データ・セットおよび HFS ファイル) への読み取り / 書き込みアクセスの許可を得る。ユーザー ID には、DB2 表を作成する機能が備わっていなくてはなりません。

以上の準備が正常に完了すれば、このステップは終了です。

開始に先立って重要な情報を決定するためのステップ

この節の表に重要情報を記録して、システムをカスタマイズする方法に関する重要な決定を行います。

次のステップに従ってください。

⇔表13 に、カスタマイズの際に使用する値を記入していってください。

表 13. カスタマイズに使用する構成データ

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
作業用の JCL データ・セット	サンプルの JCL メンバーをコピーする場合	(値は提供されていない)	
作業用の PROCLIB	サンプルの開始プロシージャーをコピーする場合	(値は提供されていない)	
作業用の SPUFI データ・セット	サンプルの SPUFI ジョブをコピーする場合	(値は提供されていない)	
作業用の変数ブロック・データ・セット	サンプルの REXX EXEC をコピーする場合	(値は提供されていない)	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
RACF 特殊権限を持つユーザー ID	以下を実行する場合 • BBOCBRAJ • BBOLDRAJ	(値は提供されていない)	
DB2 for OS/390 SYSADM 権限を持つユーザー ID	以下を実行する場合 • BBOBIND • BBOCBGRT • BBOIBN • BBOICD • BBOIGRT • BBOLDGRT • BBOLDTBC • BBOLDTBD • BBOMCRDB • BBO1JCL • BBO2JCL	(値は提供されていない)	
WebSphere for z/OS データ・セット用の上位修飾子	• BBOBIND • BBOCBRAJ • BBOIBN • BBOLDRAJ • BBOMCFG	BBO	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
DB2 for OS/390 サブシステム名	• BBOBIND • BBOCBGRT • BBOIBN • BBOICD • BBOIGRT • BBOLDGRT • BBOLDTBC • BBOLDTBD • BBOMCRDB • BBO1JCL • BBO2JCL • dsnaoini • SYS_DB2_SUB_SYSTEM_NAME 環境変数	(値は提供されていない)	
DB2 for OS/390 の SDSNLOAD、SDSNLOD2 および SDSNDBRM データ・セットの上位修飾子 (接頭部)	• BBOASR2S • BBOBIND • BBOCBGRT • BBOIBN • BBOICD • BBOIGRT • BBOLD2DB • BBOLDAP • BBOLDGRT • BBOLDTBC • BBOLDTBD • BBOMCRDB • BBOSMSS • BBO1JCL • BBO2JCL	(値は提供されていない)	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
DB2 for OS/390 システム上の DSNTIAD プログラムの計画名	• BBOCBGRT • BBOICD • BBOIGRT • BBOLDGRT • BBOLDTBC • BBOLDTBD • BBOMCRDB	(値は提供されていない)	
DB2 for OS/390 データ・ソース・ロケーション名。Z パラメーターで検出されます。	• bboslapd.conf (サーバー名のキーワード) • dsnaoini	(値は提供されていない)	
システム管理データベースの記憶域グループ	• BBOMCRDB	• BBOMG01 • BBOMG02	
4K DB2 for OS/390 バッファー・プール *	• BBOLDTBC • BBOMCRDB	BP0	
* インストール時にユーザー・データを BP0 に置くことができない場合は、適当なバッファー・プールを指定してください。			
32K DB2 for OS/390 バッファー・プール	• BBOLDTBC • BBOMCRDB	BP32K	
DB2 for OS/390 表および VCAT 用のボリューム	• BBOLDTBC • BBOMCRDB	(値は提供されていない)	
LDAP ロード・モジュールの上位修飾子	• BBOIRS • BBOLD2DB • BBOLDAP • BBONMS	GLD	
DB2 for OS/390 LDAP データベースの記憶域グループ	• BBOLDTBC	BBOLDSTO	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
SMP/E インストール後に WebSphere for z/OS のファイルが常駐するディレクトリーの名前	• BBOMCFG (-INSTALLDIR 変数) • jcivp.sh (CLASSPATH ステートメント) • patchenv.in • 環境ファイル (IVB_DRIVER_PATH、CLASSPATH、および LIBPATH) • HTTP サーバーの envvars ファイルおよび httpd.conf ファイル	/usr/lpp/WebSphere	
アプリケーション・データと環境ファイルが書き込まれる読み取り / 書き込み HFS ディレクトリー・マウント・ポイント (88ページの『システム管理 HFS 構造を作成するためのステップ』を参照)	• BBOASR1 • BBOASR1S • BBOASR2 • BBOASR2S • BBODMN • BBOIR • BBOIRC • BBOIRC3 • BBOIRC3A • BBOIRS • BBOIVP • BBOMCFG (-TARGETDIR 変数) • BBONDUTL • BBONM • BBONMC • BBONMS • BBOSMS • BBOSMSS	/WebSphere390/CB390	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
Java ライブラリー・パス	• HTTP サーバーの envvars ファイル	/usr/lpp/java/IBM/J1.3/bin and /usr/lpp/java/IBM/J1.3/bin/classic	
LDAP データベース名	• BBOCBGRT • BBOLDTBC • BBOLDTBD • bboslapd.conf (データベース名のキーワード) • BBOLDGRT	BBOLDAP	
LDAP テーブル・スペース名	• BBOLDTBC • bboslapd.conf (tbspaceentry、tbspace32k、tbspace4k および tbspacemutex キーワード)	• BBOENT • BBO32K • BBO4K • BBOMUTX	
LDAP データベースでテーブルを作成するときに LDAP が使用する接頭部。この接頭部により、WebSphere for z/OS に関連する LDAP テーブルを、ユーザーが所有する他の LDAP テーブルと区別することになります。	bboslapd.conf (dbuserid キーワード)	(値は提供されていない) 推奨: BBO	
LDAP データベースへの書き込みアクセスを与えられた LDAP アクセス ID	bboldif.cb	• CBAdmin • WASAdmin	
LDAP サーバーの開始プロシージャー名	BBOLDRAC (STARTED クラスの RACF 権限)	BBOLDAP	
LDAP サーバー・アドレス・スペースのユーザー ID	• BBOLDRAC (STARTED クラス用に RACF で設定されるユーザー識別) • BBOLDGRT	CBLDAP	
LDAP サーバー・アドレス・スペースのグループ	BBOLDRAC	CBLDAPGP	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
環境ファイルなど、HFS ファイルのグループ名。BBOCBRAC がこのグループを作成します (デフォルトは CBCFG1)。このグループの目的は、ランタイム・サーバーのユーザー ID、特に HFS ディレクトリーを所有するシステム管理領域のユーザー ID (CBSYMSR1) と、アプリケーションのインストーラーが、同じ RACF グループにない場合でも、これらの HFS ファイルを管理できるようにすることです。	• BBOCBRAC • BBOMCFG (-GROUP 変数)	CBCFG1	
ネーム・スペースへの更新アクセスを必要とするユーザー ID。実行時に、WebSphere for z/OS 管理者およびシステム管理サーバー制御領域は、更新アクセスを必要とします。	BBOCBRAC	• CBADMIN • CBSYMCR1 • CBGUEST (EJB bean の場合)	
J2EE コンポーネント用の LDAP における WsnName ツリーの開始点	• bboslapd.conf (接尾部キーワード) • com.ibm.ws.naming .ldap.containerdn 環境変数	「o=WASNaming,c=US」	
WebSphere for z/OS のルート・ネーミング・コンテキスト	• bboslapd.conf (接尾部キーワード) • bboldif.cb (dn キーワード) • LDAPROOT 環境変数 • LDAPIRROOT 環境変数	「o=BOSS,c=US」	
デーモン用の使用可能ポート	• TCP/IP プロファイル	(値は提供されていない) 推奨: 5555	
システム管理サーバー用の使用可能ポート	• TCP/IP プロファイル	(値は提供されていない) 推奨: 900	

表 13. カスタマイズに使用する構成データ (続き)

項目	使用する場合	例の値	ユーザーの値 (ここに書きこむ)
LDAP サーバー用の使用可能ポート。LDAP のデフォルトは 389 ですが、排他的 LDAP サーバーを作成しているので、別のポートが必要です。	• bboslapd.conf (ポート・キーワード) • TCP/IP プロファイル • ネーミング・サーバー用の com.ibm.ws.naming.ldap .masterurl 環境変数	(値は提供されていない) 推奨: 1389	

NLSPATH 環境変数	• BBOLD2DB で使用される slapd.envvars
	• HTTP サーバーの envvars ファイル
		以下のいずれかで**なければならない**
		`/usr/lib/nls/msg/En_US.IBM-1047/%N`
		または
		`/usr/lib/nls/msg/C/%N`	

エラー・ログ・ストリーム名	サーバー用の環境ファイル	(なし)	

表13 の空欄をすべて埋めたら、このステップは終了です。

SMP/E を使用したコードのインストールと、データ・セットのコピー

SMP/E を使用してコードをインストールするには、*WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 に従ってください。

注: インストールしたデータ・セットの上位修飾子 (推奨はしません)、または中位修飾子は変更することができます。本資料では、データ・セット名に上位修飾子を付けずに使用します。ただし、明確に区別するために完全なデータ・セット名が必要な場合は別で、その場合は、`BBO` を修飾子として使用します。

参照のために、65ページの表14 に、重要なデータ・セットと、インストールおよびカスタマイズの際に使用されるそのメンバーを示します。すべてではありませんが、大部分は、ユーザー自身のデータ・セットにコピーすることになります。

表 14. 製品で提供されるデータ・セット

ソース	説明
BBO.SBBOJCL では	
BBOACASH	BECASHAC の COBOL プログラムの例、すなわち CICS EXCI PAA で使用される例を、コンパイルおよびリンクするジョブ。
BBOADEFS	BCASHAC サンプルの CICS 領域をセットアップするジョブ。
BBOAFILS	CASHACCT トランザクションの例が使用するファイルを、削除したり再作成したりするジョブ。
BBOASR1	MOFW アプリケーション・サーバー制御領域の開始プロシージャー。このアプリケーション制御領域は、MOFW インストール時のインストール検査プログラムに使用されます。
BBOASR1S	MOFW アプリケーション制御領域のワークロード管理が開始する、アプリケーション・サーバー領域の開始プロシージャー。
BBOASR2	J2EE アプリケーション・サーバー制御領域の開始プロシージャー。この制御領域は、J2EE インストール時のインストール検査プログラムに使用されます。
BBOASR2S	J2EE アプリケーション制御領域のワークロード管理が開始する、アプリケーション・サーバー領域の開始プロシージャー。
BBOBIND	WebSphere for z/OS の諸機能のために DB2 for OS/390 パッケージをインストールするバインド・ジョブ。
BBOCBGRT	WebSphere for z/OS ランタイム・サーバーのために DB2 for OS/390 GRANT を発行するジョブの例。
BBOCBRAJ	REXX コード (BBOCBRAC) を呼び出して、WebSphere for z/OS ランタイム・サーバー用の RACF 定義をセットアップするジョブ。
BBOCTI00	WebSphere for z/OS がコンポーネント・トレース (Ctrace) を使用する場合のデフォルトを設定するのに使用される、PARMLIB メンバーの例。
BBODMCCB	WebSphere for z/OS およびそれに関連するアドレス・スペースのダンプに使用される、PARMLIB メンバーの例。
BBODMN	デーモンの開始プロシージャー。この開始プロシージャーは、インストール段階でランタイムをブートストラップします。また、通常の操作の際、デーモン、システム管理、ネーミング、およびインターフェース・リポジトリーの制御領域を開始します。
BBOIBN	インストール検査プログラムのバインド・ジョブ。
BBOICD	インストール検査プログラムのデータベース作成ジョブ。

表 14. 製品で提供されるデータ・セット (続き)

ソース	説明
BBOIGRT	WebSphere for z/OS の IVP サーバーとクライアントのために DB2 for OS/390 GRANT を発行するジョブの例。
BBOIPCSP	WebSphere for z/OS IPCS 処理のモデル。
BBOIR	インターフェース・リポジトリー・サーバー制御領域の開始プロシージャー。初期設定の際にデーモンによって開始されます。
BBOIRC	最初のインターフェース・リポジトリー・クライアント・ブートストラップ開始プロシージャー。これによって、ルートおよびその他のインターフェース・リポジトリー名がネーム・スペースに配置されます。
BBOIRC2	2 番目のインターフェース・リポジトリー・クライアント・ブートストラップ・ジョブ。これは、パブリック・インターフェースを伴うインターフェース・リポジトリーを移植する際に使用されます。
BBOIRC3	ローダーが PDS または PDSE にインストールされているときに、クライアントのサーバー・オブジェクト・インターフェース情報をインターフェース・リポジトリー・データベースに移植するために使用されるインターフェース・リポジトリー・クライアント・ブートストラップ JCL。WebSphere for z/OS 上にインストールされているすべてのサーバー・オブジェクトに対して使用します。
BBOIRC3A	ローダーが HFS にインストールされているときに、クライアントのサーバー・オブジェクト・インターフェース情報をインターフェース・リポジトリー・データベースに移植するために使用されるインターフェース・リポジトリー・クライアント・ブートストラップ JCL。WebSphere for z/OS 上にインストールされているすべてのサーバー・オブジェクトに対して使用します。
BBOIRS	インターフェース・リポジトリー・サーバーのサーバー領域の開始プロシージャー。ワークロード管理によって開始されます。
BBOIVP	BBOASR1 MOFW サーバー用のインストール検査プログラム・クライアント・ジョブ。
BBOIVPE	BBOASR2 J2EE サーバー用のインストール検査プログラム・クライアント・ジョブ。
BBOLDAP	LDAP サーバーを開始する LDAP サーバー開始プロシージャーの例。

表 14. 製品で提供されるデータ・セット (続き)

ソース	説明
BBOLDGRT	LDAP サーバー用に DB2 for OS/390 GRANT を発行するジョブの例。
BBOLDRAJ	REXX コード (BBOLDRAC) を呼び出して、LDAP サーバー用の RACF 定義をセットアップするジョブ。
BBOLDTBC	WebSphere for z/OS 用の LDAP データベースを作成するジョブ。LOCKSIZE は ROW で、通常の PAGE の LOCKSIZE とは異なります。
BBOLDTBD	WebSphere for z/OS 用の LDAP データベースを除去するジョブ。 **重要:** このジョブを使用すると、LDAP データベースが破棄されます。
BBOLD2DB	LDAP LDIF2DB バルク・ローダーを実行するジョブの例。
BBOMCFG	管理アプリケーションに必要な HFS 構造 (ディレクトリー、ファイル、およびリンク) をセットアップするジョブ。
BBOMCRDB	システム管理データベース作成ジョブ。
BBOMDUMP	DB2 for OS/390 の SQL ステートメント。SPUFI を使用してシステム管理表の内容をダンプします。
BBOMMIG	使用している XML 構成ファイルと環境ファイルをエンタープライズ版 V3.02 からアップグレードするジョブ。
BBONDUTL	ネーミング・ダンプ・ユーティリティーの JCL。
BBONM	ネーミング・サーバー制御領域 (CORBA 互換のネーミング・サーバー) の開始プロシージャー。デーモンによって開始されます。
BBONMC	ネーミング・クライアント・ブートストラップ開始プロシージャー。これは、WebSphere for z/OS のデフォルト・ネーム・スペースを確立します。
BBONMS	ネーミング・サーバーのサーバー領域の開始プロシージャー。ワークロード管理によって開始されます。
BBORCLGS	カップリング・ファシリティー・ログ・ストリームのセットアップに使用される JCL の例。
BBORDLGS	DASD のみのログ・ストリームのセットアップに使用される JCL の例。
BBOSCHED	WebSphere for z/OS の SCHEDxx PARMLIB メンバーの例。
BBOSMS	システム管理サーバー制御領域の開始プロシージャー。初期設定の際にデーモンによって開始されます。

表 14. 製品で提供されるデータ・セット (続き)

ソース	説明
BBOSMSS	システム管理サーバーのサーバー領域の開始プロシージャー。ワークロード管理によって開始されます。
BBOWTR	外部書き出しプログラムの開始プロシージャー。このプログラムは、PROCLIB の CTRACE メンバー (CTIBBOxx) で識別されます。
BBO1JCL	WebSphere for z/OS で使用される LDAP サーバー用の、DSNT1JCL バインド・ジョブの例。
BBO2JCL	WebSphere for z/OS で使用される LDAP サーバーに必要な、DSNT2JCL バインド・ジョブの例。
BBO.SBBOEXEC では	
BBOCBRAC	WebSphere for z/OS ランタイム・サーバーの RACF 定義をセットアップする REXX コード。BBOCBRAJ から呼び出します。
BBOCNFG	ネーミング・クライアント構成ファイルの例。
BBOHFSWR	REXX コード。OE UNIX シェル内部で動作する Java クライアント・テスト・ケース出力を、SYSOUT に書き込みます。
BBOLDRAC	LDAP サーバーの RACF 定義をセットアップする REXX コード。BBOLDRAJ から呼び出します。
BBOLSDEL	LDAP 項目を削除する CLIST の例。
BBOLSRCH	LDAP 項目を表示する CLIST の例。
BBOMKDIR	WebSphere for z/OS に必要な静的製品ディレクトリーおよびその他のファイルを作成する REXX EXEC。
BBONDSMP	ネーミング・ダンプ・ユーティリティーの構成ファイルの例。この例は、ローカル (ホスト) ネーム・スペース全体をダンプするものです。
BBORBLOG	エラー・ログ・ストリームを参照できるようにする REXX EXEC。
BBOXPC	DB2 プリコンパイラーを実行する EXEC。この EXEC は、階層ファイル・システムから C ソースをコピーし、それを、DB2 プリコンパイラーが処理するための一時データ・セットに置きます。DB2 プリコンパイラーからの出力 (変更済みの C ソース) はコピーされ、階層ファイル・システムに戻されます。
BBO.SBBOMSG では	
BBOUMSEN	英語のインストール・メッセージ・スケルトン。
BBOUMSJP	日本語のインストール・メッセージ・スケルトン。

表 14. 製品で提供されるデータ・セット (続き)

ソース	説明
/usr/lpp/WebSphere/samples ディレクトリーでは	
bboaoini	WebSphere for z/OS 用の LDAP をセットアップする、DB2 for OS/390 初期設定ファイルの例。DB2 for OS/390 の DSNAOINI ファイルからコピーされます。
bboldif.cb	LDAP テーブルの作成に必要な LDIF ファイル。BBOLD2DB によって使用されます。
bboslapd.conf	LDAP サーバー用の slapd.conf ファイルの例。このファイルは、BBOLDAP、BBONMS、および BBOLD2DB によって使用されます。
patchenv.in	BBOMMIG ジョブの新規または変更されたコード・ディレクトリーとサーバー名を定義している入力ファイルの例。

製品とともに提供されるファイルをコピーするためのステップ

インストールした WebSphere for z/OS をカスタマイズする際には、製品とともに配布されているサンプル・ファイルのコピーが必要です。以下の手順では、サンプルの内容とそのコピー先について説明します。

この作業を始める前に: SMP/E を使用してインストールした WebSphere for z/OS の、製品コードを用意する必要があります。

データ・セットをコピーするには、以下のステップを実行してください。

1. 次のデータ・セット・メンバーの例を、BBO.SBBOJCL から作業中の JCL データ・セットにコピーする。
   BBOACASH
   BBOADEFS
   BBOAFILS
   BBOBIND
   BBOCBGRT
   BBOCBRAJ
   BBOIBN
   BBOICD
   BBOIGRT
   BBOIRC
   BBOIRC2
   BBOIRC3
   BBOIRC3A

BBOIVP
BBOIVPE
BBOLDGRT
BBOLDRAJ
BBOLDTBC
BBOLDTBD
BBOLD2DB
BBOMCFG
BBOMCRDB
BBONMC
BBORCLGS
BBORDLGS
BBO1JCL
BBO2JCL

---

2. 次のデータ・セット・メンバーの例を、BBO.SBBOJCL から作業中の PROCLIB にコピーする。
   BBOASR1
   BBOASR1S
   BBOASR2
   BBOASR2S
   BBODMN
   BBOIR
   BBOIRS
   BBOLDAP
   BBONM
   BBONMS
   BBOSMS
   BBOSMSS

---

3. 次のものを、マスター・スケジューラー JCL にリストされた PROCLIB、たとえば SYS1.PARMLIB(MSTJCL00) にコピーする。
   BBOWTR

---

4. 次のものを、BBO.SBBOJCL から PARMLIB にコピーする。
   - BBOCTI00。このメンバーの名前を CTIBBO00 に変更します。

- BBODMCCB。このメンバーの名前を IEADMC*xx* に変更します。ここで、*xx* はユーザーが選択する接尾部です。

  例: IEADMCCB

---

5. BBOMDUMP データ・セット・メンバーを、BBO.SBBOJCL から作業中の SPUFI データ・セットにコピーする。

---

6. BBO.SBBOEXEC のすべてのメンバーを、作業中の変数ブロック・データ・セットにコピーする。

---

7. BBO.SBBOMSG の BBOUMSEN メンバーを、それ自身の区分データ・セット、または SYS1.MSGENU にコピーする。

---

8. BBO.SBBOMSG の BBOUMSJP メンバーを、それ自身の区分データ・セット、または SYS1.MSGJPN にコピーする。

---

9. BBORBLOG (エラー・ログ・ストリーム・ブラウザー) を BBO.SBBOEXEC から適当なライブラリーにコピーする。これを使用する場合は、データ・セット名全体を提供して BBORBLOG を直接呼び出すことも、ユーザー・ログオン開始プロシージャーの SYSEXEC 連結にデータ・セット名を追加することもできます。後者の方が、BBORBLOG を簡単に呼び出すことができます。BBORBLOG の使用に関する詳細は、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 を参照してください。

注: これ以降のステップでは、これらの例の変更を行います。大文字と小文字の区別が重要な場合がしばしばあるので注意してください。つまり、小文字を使用している例を変更する場合は、変更にも小文字を使用するようにしてください。

OS/390 または z/OS の基本機能のカスタマイズ

この節では、APF 権限の設定や LPA のロード、TCP/IP のカスタマイズなど、OS/390 または z/OS の基本機能をカスタマイズする方法について説明します。

基本システムを変更するためのステップ

この作業を始める前に: SMP/E を使用して WebSphere for z/OS の製品コードをインストールし、製品のサンプル・ファイルのコピーを作成する必要があります。

基本システムを変更するには、以下のステップを実行します。

1. BBO.SBBOJCL 内の SCHEDxx を変更して、BBOSCHED サンプル・ファイルに入っているステートメントを組み込みます。

---

2. BBO.SBBOLOAD、BBO.SBBOLD2、および BBO.SBBOLPA データ・セットの、APF 許可を行います。

   例: PROGxx PARMLIB メンバーには次のものを組み込むことができます。

```
APF FORMAT(DYNAMIC)
/**********************************************************************/
/* BOSS LOCAL DATASETS                                                */
/**********************************************************************/
APF ADD
    DSNAME(BBO.SBBOLOAD)
    VOLUME(vvvvvv)
APF ADD
    DSNAME(BBO.SBBOLD2)
    VOLUME(vvvvvv)
APF ADD
    DSNAME(BBO.SBBOLPA)
    VOLUME(vvvvvv)
```

   ここで、vvvvvv はユーザーのボリューム ID です。

---

3. 言語環境プログラム・データ・セット SCEERUN、および DB2 for OS/390 データ・セット SDSNLOAD が許可済みであることを確認します。

---

4. BBO.SBBOULIB または SBBOMIG は、クライアント・ユーザーの権限の下で実行されるべきものなので、APF 許可を行っては**なりません**。

---

5. 次の表を使用して、WebSphere for z/OS のモジュールを配置します。

表 15. LPA またはリンク・リストでのモジュールの配置

モジュール	注
BBO.SBBOLPA	すべてのメンバーを LPA にロードします。
BBO.SBBOLOAD	すべてのメンバーを、LPA に動的にロードすることをお勧めします。仮想記憶域がコンストレインドである場合は、メンバーをリンク・リストに置いてください。
BBO.SBBOLD2(BBORSMCT)	WebSphere for z/OS で Web サーバー・サーブレットを使用する計画の場合は、SBBOLD2(BBORSMCT) を、LPA またはリンク・リストに配置しなければなりません。
BBO.SBBOLD2	BBORSMCT は別として、SBBOLD2 からのメンバーは、LPA には配置**しないでください**。これらのメンバーは、リンク・リストに配置します。
BBO.SBBOULIB	これらのメンバーは、LPA またはリンク・リストの**いずれにも、配置しないでください**。

注:

a. メンバーは PDSE に常駐しているため、LPA に動的にロードしなければなりません。また OS/390 または z/OS は、システムの初期設定時には PDSE のメンバーをロードすることができません。**例:** 以下のコマンドを発行してください。

```
SETPROG LPA,ADD,MASK=*,DSNAME=hlq.SBBOLOAD
SETPROG LPA,ADD,MASK=*,DSNAME=hlq.SBBOLPA
```

ここで、*hlq* は、使用している WebSphere for z/OS データ・セットの上位修飾子です。

重要: LPA のサイズが、WebSphere for z/OS のモジュールを保持できる大きさであることを確認してください。49ページの『メモリーの使用に関する推奨』を参照してください。

b. すでに LPA に入っている BBO.SBBOLPA、BBO.SBBOLOAD、または BBO.SBBOLD2 からのモジュールと同じ名前のモジュールは、必ず除去してください。

c. WebSphere for z/OS のモジュールを、IPL 後に LPA にロードするには、自動化更新することをお勧めします。COMMNDxx は、コマンドが使用可能にされる DFSMS サービスに先だって実行されるため、このタスクには適していません。

6. APF 許可または LPA に PROGxx ファイルを使用した場合は、必ず次のコマンドを発行してください。

```
SET PROG=xx
```

ここで、xx は PROGxx メンバーの接尾部です。

---

7. すべての BBO.* データ・セットおよびすべての LDAP データ・セットが、カタログを作成していることを確認してください。これは必須ではありませんが、そうすることを強くお勧めします。

---

8. SYS1.PARMLIB(BLSCUSER) メンバーを、BBO.SBBOJCL 内のメンバー BBOIPCSP によって提供された IPCS モデルで更新します。BLSCUSER の詳細は、*z/OS MVS 対話式問題管理システム (IPCS) ユーザーズ・ガイド*, SA88-8568 を参照してください。

---

9. SMF 記録を開始して、WebSphere for z/OS システムについて、システムとジョブに関連した情報を収集したい場合は、次のようにします。
   a. SMFPRMxx parmlib メンバーを編集します。
      1) ACTIVE ステートメントを挿入して、SMF の記録を指示します。
      2) システムに作成させたい SMF レコードのタイプを示すために、SYS ステートメントを挿入します。たとえば、タイプ 120 のレコードだけを選択するには、SYS(TYPE(120:120)) を使用します。パフォーマンスへの影響を最小にするために、選択したレコード・タイプの数は少なくしておいてください。
   b. DASD へのレコードの書き込みを開始するために、次のコマンドを発行します。

      ```
      t smf=xx
      ```

      ここで、xx は SMF parmlib メンバー (SMFPRMxx) の接尾部です。SMF parmlib メンバーの詳細については、*z/OS MVS システム管理機能 (SMF)*, SA88-8596 を参照してください。

      DASD への書き込みを活動状態にすると、データが (SMFPRMxx で指定した) データ・セットの中に記録されます。

注: その後、管理アプリケーションのインストールが完了した時点で、いくつかのプロパティーをサーバー・プロパティー・フォーム上で定義することにより、サーバーに SMF レコードを収集させることができます。

WebSphere for z/OS と SMF 記録の使用の詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: 操作および管理*, SA88-8653 を参照してください。

変換メッセージのセットアップ (オプション)

MVS メッセージ・サービス (MMS) を使用すると、インストール時に、メッセージ変換のためのメッセージ・ファイルを使用することができます。MMS は、米国英語のメッセージを、別の言語に変換された同等のメッセージに置換します。MMS が活動中であれば、TSO/E 上の拡張 MCS コンソールの許可ユーザーは、使用可能言語を選択してメッセージを変換し、変換されたメッセージを画面に表示させることができます。

MMS が変換メッセージを処理するためには、MMS メッセージ・コンパイラーを使用して、英語のメッセージ・スケルトンおよび変換済みのメッセージ・スケルトンを含む、インストール・メッセージ・ファイルの形式を設定しなければなりません。

WebSphere for z/OS は、次の 2 つのメッセージ・スケルトンを提供します。

表 16. インストール・メッセージ・スケルトン

BBOUMSEN	英語
BBOUMSJP	日本語

これら 2 つのファイルを、次のどちらかの方法によって MMS メッセージ・コンパイラーで処理します。次のいずれかを実行します。

1. BBOUMSEN をそれ自身の PDS にコピーし、この PDS を、英語のランタイム・メッセージ・ファイルを生成する際に、MMS メッセージ・コンパイラーへの入力データとして使用される、PDS ファイルの連結に追加します。

   BBOUMSJP をそれ自身の PDS にコピーし、この PDS を、日本語の実行時メッセージ・ファイルを生成する際に、MMS メッセージ・コンパイラーへの入力データとして使用される、PDS ファイルの連結に追加します。

   あるいは、

2. BBOUMSEN を SYS1.MSGENU にコピーし、PDS を、英語の実行時メッセージ・ファイルを作成する際の、MMS メッセージ・コンパイラーへの入力データとして指定します。

   BBOUMSJP を SYS1.MSGJPN にコピーし、PDS を、日本語の実行時メッセージ・ファイルを作成する際の、MMS メッセージ・コンパイラーへの入力データとして指定します。

変換メッセージを提供するステップについては、*z/OS MVS 計画 : 操作*, SA88-8573 の変換メッセージの処理に関する節を参照してください。

TCP/IP ネットワークのセットアップ

16ページの『TCP/IP ネットワークの更新』では、WebSphere for z/OS 用に TCP/IP をカスタマイズする際の、バックグラウンド情報とヒントを提供しています。次のステップでは、OS/390 または z/OS システム上で TCP/IP を変更する方法について説明します。

OS/390 または z/OS 上で TCP/IP を更新するためのステップ

この作業を始める前に: 使用しているドメイン・ネーム・サーバー (DNS) のタイプを、インプリメントしてください。これに関するヒントは、16ページの『TCP/IP および WebSphere for z/OS についてのヒント』を参照してください。

OS/390 または z/OS で DNS をインプリメントする場合、詳細は *z/OS Communications Server: IP マイグレーション*, GC88-8924 を参照してください。`resolv.conf` ファイルと BPXPRM parmlib メンバーの入手方法を知っている必要があります。詳しくは、*z/OS Communications Server: IP Configuration Reference*, SC31-8776、および *z/OS UNIX システム・サービス 計画*, GA88-8639 を参照してください。

TCP/IP を更新するには、以下のステップを実行してください。

1. 解決構成ファイルに、使用している DNS の項目があることを確認する。ない場合は、適切な更新を行ってください。ドメイン・ネーム・サーバーの、解決構成ファイルへの追加に関する情報は、*z/OS Communications Server: IP Configuration Reference*, SC31-8776 を参照してください。

   ドメイン・ネーム・サーバーがない場合は、`etc/hosts` ファイルを更新してください。

   注:

   a. `etc` ディレクトリーの `resolv.conf` を更新すると、IP は、ユーザーが順次データ・セットを持っている可能性があっても、その項目を検索しなくなります。したがって、`etc/resolv.conf` を更新する場合は、DNS 項目がすべてそのファイルに含まれていることを確認してください。

   b. `etc/resolv.conf` を構成ファイルとして使用する場合は、アクセス権ビットが 755 に設定されていることを確認してください。

---

2. OS/390 または z/OS 上に `etc/hosts` ファイルがない場合は、このファイルを作成する。ファイルの中身は重要ではありませんが、このファイルは存在していなければなりません。アクセス権ビットが 755 に設定されていることを確認してください。

3. **重要:** TCP/IP プロファイルで、解決 IP ポート用にポート 900 を追加し、それをシステム管理サーバーのインスタンス名へ関連付ける。WebSphere for z/OS がインストールされているシスプレックス内の最初のシステムには、SYSMGT01 を使用します。サーバー・インスタンスの説明については、2ページの『WebSphere for z/OS ランタイム構成の図』を参照してください。たとえば、項目は次のようになります。

   ```
   900   TCP    SYSMGT01
   ```

4. TCP/IP プロファイルでデーモン用のポートを予約し、それをデーモン・サーバーのインスタンス名へ関連付ける。WebSphere for z/OS がインストールされているシスプレックス内の最初のシステムには、DAEMON01 を使用します。ポートは 5555 にすることをお勧めします。たとえば、この項目は次のようになります。

   ```
   5555  TCP    DAEMON01
   ```

   規則: 一度選択したデーモン・ポートは、**絶対に**変更することはできません。すべてのオブジェクト参照にそのポートが組み込まれるからです。ポートを変更すると、以後既存のオブジェクトにアクセスすることができなくなります。

   現行のお客様への注: 以前のリリースでは、ポート 5555 を BBODMN へ関連付けていましたが、この関連付けをデーモン・サーバーのインスタンス名に変更しなければなりません。関連付けを変更しても、オブジェクト参照に問題は起きません。変更した後、次のコマンドでデーモンを始動してください。

   ```
   S BBODMN.DAEMON01
   ```

   これについては、この後に説明があります。

5. 必要に応じて、TCP/IP ツールの組をセットアップする。
   - WebSphere for z/OS が使用する LDAP サーバーのポートを予約します。ポート 1389 をお勧めします。使用されていなければどのポートでもかまいませんが、389 は使用できません。ポート 389 は汎用 LDAP サーバーのデフォルト・ポートなので、インストール・プロセスでは別の LDAP サーバーを作成します。

- OS/390 または z/OS 階層ファイル・システムに、ワークステーション上のローカル・ドライブとしてアクセスするための、ネットワーク・ファイル・システム。オブジェクト・ビルダーにはこれをお勧めします。
- OS/390 UNIX シェルにコマンドを送信する REXEC。REXEC を使用して、オブジェクト・ビルダーから自動的にコンパイラーを立ち上げます。
- ネットワーク内でファイルを移動するための FTP。
- OS/390 または z/OS にリモート・ログインするための Telnet。

---

6. TCP/IP プロファイルで、すでに予約したデーモン・ポートをブロックするポート範囲 (PORTRANGE ステートメント) を、予約していないかどうか検査します。

---

7. BPXPRM parmlib メンバーで、許可されるソケットおよびファイル・ハンドルの数を増やす。
   - ソケットの場合、NETWORK ステートメントの MAXSOCKETS パラメーターで、システムに同時にアクセスするクライアントの 4 倍の数を、既存のソケット数に追加します。つまり、同時にシステムにアクセスするクライアントが 250 あり、すでに 1,000 のソケットが定義されている場合は、2,000 のソケット (4 x 250 + 1,000) を指定する必要があります。
   - ファイル・ハンドルの場合、MAXFILEPROC パラメーターで、同時にシステムにアクセスするクライアントの数を、ファイル・ハンドルの現行数に追加します。つまり、同時にシステムにアクセスするクライアントが 250 あり、ファイル・ハンドルの現在の数が 1,000 である場合は、1,250 のファイル・ハンドル (250 + 1,000) を指定する必要があります。

     注: 使用中のシステムで設定されるソケットまたはファイル・ハンドルの、最大数を超えないように注意してください。
   - INADDRANYPORT および INADDRANYCOUNT の NETWORK ステートメントの値を検査します。この 2 つの値は予約ポートの範囲 (INADDRANYPORT が開始点) を表します。この範囲には、デーモン・ポートの値を含むことはできません。たとえば、デーモン・ポートが 5555 の場合、INADDRANYPORT は 6000 以上の値から開始することになります。

---

8. 次の IP 名が、etc/hosts ファイル、またはドメイン・ネーム・サーバーを使用している場合は etc/resolv.conf ファイルのいずれかで、定義されていることを確認する。

   注: etc/hosts 内のホスト名には、24 バイトという制限があります。etc/hosts の中でこの限度を超えると、管理アプリケーション (この後に使用します) はホストに接続しません。

   - 解決 IP 名。RESOLVE_IPNAME 環境変数の値と同じです。
   - デーモン IP 名。DAEMON_IPNAME 環境変数の値と同じです。
   - 解決 IP 名でもデーモン IP 名でもない場合は、システムのホスト IP 名。

   環境変数に関する詳細は、383ページの『付録A. 環境ファイル』を参照してください。

---

9. oping コマンドを使用して、解決 IP 名、デーモン IP 名、およびホスト IP 名をテストする。IP 名が解決しない場合は、解決構成ファイルを更新してください。

---

oping コマンドが正常に動作したら、このステップは終了です。

エラー・ログ・ストリームをセットアップするためのステップ

インストール時に WebSphere for z/OS のブートストラップを実行する前に、エラー・ログ・ストリームをセットアップしてください。エラー・ログ・ストリームのバックグラウンド情報については、50ページの『問題診断についてのバックグラウンド』を参照してください。

この作業を始める前に: システムがカップリング・ファシリティーに記録するか、それとも DASD のみのロギングを使用するかを決定します。

注: DASD のみのエラー・ロギングを使用する場合は、パフォーマンスがかなり低下します。

- カップリング・ファシリティーを使用する場合は、SYS1.MIGLIB にある、カップリング・ファシリティー・データの形式設定ユーティリティー、IXCL1DSU に対するアクセス権がなければなりません。
- SYS1.MIGLIB にある管理データ・ユーティリティー、IXCMIAPU に対するアクセス権がなければなりません。
- 結合データ・セットの作成権限が必要です。
- これまでのステップで述べたアクセス権を与える RACF 管理者権限が必要です。

WebSphere for z/OS のエラー・ログ・ストリームをセットアップするには、次のステップを実行してください。

1. カップリング・ファシリティーに記録する場合は、ログ・ストリーム (たとえば CB_ERRORLOG) に対応するカップリング・ファシリティー構造を定義する。結合データの形式設定ユーティリティー、IXCL1DSU を使用します。*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

   ---

2. BBORCLGS サンプル (カップリング・ファシリティー・ログ・ストリームを作成)、あるいは BBORDLGS (DASD のみのログ・ストリームを作成) のいずれかを使用して、ログ・ストリームを構成する。

   ファイルのコメントに従って、ジョブの 1 つを変更してください。BBORDLGS を使用する場合は、次のように設定します。

   - MAXBUFSIZE は 255 ～ 4096 バイト
   - STG_SIZE は 900: `STG_SIZE(900)`
   - LS_SIZE は 900: `LS_SIZE(900)`

注: ログ・ストリーム保存期間および自動削除のガイドラインについては、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

---

3. 選択して更新したジョブを実行する。

ログ・ストリームが正常に定義されれば、このステップは終了です。

エラー・ログに関するインストール後の注意

インストール・ブートストラップが完了したら、管理アプリケーションを使用してログ・ストリームの名前を変更するか、あるいは、サーバーまたはサーバー・インスタンスのための新規のログ・ストリーム名を作成してください。

注:

1. サーバー・エラー・ログ・ストリームを設定すると、WebSphere for z/OS の一般設定がオーバーライドされます。またサーバー・インスタンスの設定は、サーバーの設定をオーバーライドします。したがって、一般のエラー・ロギングはセットアップできますが、特定のログ・ストリームに対するサーバーまたはサーバー・インスタンスの直接エラー・ロギングは、セットアップできません。
2. 管理アプリケーションを介して新規のログ・ストリーム名を作成した場合は、OS/390 または z/OS 上でその新規ログ・ストリームを構成しなければなりません。カップリング・ファシリティーを使用した場合は、それに対応する新規のカップリング・ファシリティー・ログ・ストリームを定義してください。
3. 既存のログ・ストリームを変更した場合、あるいは新規のログ・ストリームを作成した場合は、おそらく、WebSphere for z/OS の再始動が必要になります。管理アプリケーションを介してログ・ストリームの名前を変更するとほとんどの場合は、変更を有効にするために WebSphere for z/OS の再始動が必要です。変更が自動的に有効になるのは、ログ・ストリームの名前が、サーバーの再始動を引き起こす他の変更と一緒に変更される場合だけです。

エラー・ログ・ストリームに記録される OS/390 または z/OS クライアントの実行中に発生する、WebSphere for z/OS メッセージを入手したい場合は、環境ファイルの CLIENTLOGSTREAMNAME 環境変数をコーディングし、その後クライアントを初期化します。CLIENTLOGSTREAMNAME に関する詳細は、383ページの『付録A. 環境ファイル』を参照してください。

RACF の BBOCBRAC の例は、ランタイム制御、およびユーザーが作成したログ・ストリームのサーバー領域ユーザー ID に、更新権限を与えます (ログ・ストリームの名前を提供する必要があります)。インストールおよびカスタマイズ後に、ログ・ストリームへのアクセスを認可する場合は、次のようにします。

- ログ・ストリームに書き込む個々のサーバー識別 (あるいは、クライアントにエラー・ログ・ストリームへの書き込みを許可している場合は、クライアント識別) では、ログ・ストリームに更新アクセスを割り当てます。
- エラー・ログ・ストリームを表示する個々のユーザーには、読み取りアクセスを割り当てます。

BBOCBRAC の RACF コマンドの例に従ってください。

RACF セキュリティーをセットアップするためのステップ

ここでの各ステップは、ランタイム・サーバーおよびアプリケーション・サーバーの、ユーザー ID と RACF 権限をセットアップします。ここではサンプル・ジョブ BBOCBRAJ を提供します。このジョブは、REXX EXEC、すなわち BBOCBRAC を呼び出しますが、これには RACF コマンドが含まれていて、初期インストールに必要な権限のセットアップに役立ちます。実際に運用する場合には、これらの権限を検証する必要があります。

BBOCBRAC は、次のいずれかを実行します。

- 一連の RACF コマンドを、ファイルに格納した REXX EXEC の形で生成します。それらの RACF コマンドを格納するファイルを指定するには、BBOCBRAJ ジョブの中で RACFCMDS DD ステートメントを使用します。このオプションを使用した場合は、出力を編集でき、その後、調整した EXEC を実行できます。
- RACF コマンドを作成し、即時に実行します。

EXEC は、SSL や Kerberos などの拡張セキュリティー制御を組み込むかどうかも尋ねてきます。BBOCBRAC のコードを検討してください。使用できるオプションがコード内のコメントによって説明されています。

BBOCBRAC で確立される重要な権限はシステム管理サーバー領域のユーザー ID (REXX 変数の `default_sysmgt_SR_userid` によって CBSYMSR1 として定義されます) と、デフォルトの構成グループ (REXX 変数の `default_CB_CFG_group` によって CBCFG1 として定義されます) です。このユーザー ID は、システム管理サーバーが保守する HFS ファイルとディレクトリーの所有者になります。88ページの『システム管理 HFS 構造を作成するためのステップ』を参照してください。システム管理 HFS ファイルおよびディレクトリーへのアクセスを必要とするすべてのユーザー ID は、このグループ (READ アクセス権を持つことを許可されます) に接続していなければなりません。

この作業を始める前に: BBOCBRAC および BBOCBRAJ のコピーが必要です。

RACF セキュリティーをセットアップするには、以下のステップを実行してください。

1. BBOCBRAC のコピーを、そのファイルのコメントに従って変更する。指定しなければならないログ・ストリーム名には、81ページの『エラー・ログ・ストリームをセットアップするためのステップ』で定義したのと同じログ・ストリームを使用してください。

推奨: 例の中のユーザー ID およびグループは変更しないでください。変更すると、あとで他のカスタマイズ・ジョブも変更しなければならなくなります。

---

2. 必要な場合は、ファイルのコメントに従って BBOCBRAJ のコピーを変更する。

---

3. 適切な RACF 権限を持つユーザー ID から BBOCBRAJ のコピーを実行依頼し、ユーザー ID およびグループを作成する。

ジョブが正常に実行されれば、このステップは終了したことになります。

システム管理データベースの定義

この節では、WebSphere for z/OS がサーバーを管理する際に使用する、システム管理データベースをセットアップする方法について説明します。

RRS および DB2 for OS/390 を初期化するためのステップ

この作業を始める前に: RRS および DB2 for OS/390 のセットアップを行わなければなりません。42ページの『リソース・リカバリー・サービスに関する推奨』および 44ページの『DB2 for OS/390 データベースおよび LDAP』を参照してください。

次のステップを実行してください。

⇔ RRS および DB2 for OS/390 を開始する。RRS を初期化しなければ、DB2 for OS/390 を開始することはできません。

WebSphere for z/OS システム管理データベースをセットアップするためのステップ

この手順では、WebSphere for z/OS が使用するデータベースの作成とバインディングに関して説明します。

この作業を始める前に: BBOMCRDB および BBOBIND のコピーをとる必要があります。

システム管理データベースをセットアップするには、次のステップを実行してください。

1. JCL のコメントに従って、システム管理データベース作成ジョブ、BBOMCRDB を更新し、ユーザーの DB2 for OS/390 環境に合わせる。

   注:

   a. WebSphere for z/OS は、DB2 for OS/390 表の接頭部として、BBO を使用します。接頭部は変更できません。

   b. BBOMCRDB が使用する DBRMLIB は、DB2 for OS/390 によって提供されるものです。

---

2. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、BBOMCRDB を実行依頼する。このジョブにより、最初にジョブを実行するときには存在しない表が削除されます。最初にジョブを実行するときには戻りコード 8 が、2 回目以降の実行では戻りコード 0 が戻されます。

---

3. JCL のコメントに従って、表バインド・ジョブ、BBOBIND を更新する。

   注: BBOBIND が使用する DBRMLIB は、WebSphere for z/OS によって提供されるものです。

---

4. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、BBOBIND を実行依頼する。

バインド・ジョブが正常に完了すれば、このステップは終了したことになります。

システム管理 HFS 構造を作成するためのステップ

この手順では、BBOMCFG というジョブを使用して、ブートストラップのフェーズ 1 と LDAP で使用する必須の HFS ディレクトリーと初期環境ファイル (環境ファイルの configuration.env を含む) を作成します。configuration.env ファイルは、この後の手順で編集します。

重要: configuration.env ファイルを直接編集できるのは、ブートストラップが完了する前**だけ**です。ブートストラップの後に環境変数を変更するには、**必ず**管理アプリケーションを使用しなければなりません。

ブートストラップの完了後、WebSphere for z/OS は環境変数データをシステム管理データベースで保管および管理し、システム管理データベースのデータから、HFS のサーバーおよびサーバー・インスタンス用の環境変数を作成します。ブートストラップ後に環境変数ファイルを直接編集しても、新しいシステム管理構成が活動化されたときに編集内容が上書きされ、これを避けることはできません。

BBOMCFG ジョブは、WebSphere for z/OS ファイル・システムのマウント・ポイントにシステム管理 HFS 構造を作成します。そのマウント・ポイントは、TARGETDIR という変数で指定されます。デフォルトは `/WebSphere390/CB390` です。

規則:

1. TARGETDIR は、読み取り / 書き込みディレクトリーでなければなりません。シスプレックス内に WebSphere for z/OS をセットアップする計画の場合は、このディレクトリーを共用する必要があるので、シスプレックス全体で HFS を読み取り / 書き込みモードで共用する何らかの手段を確立しなければなりません。OS/390 バージョン 2 リリース 8 の場合は、ネットワーク・ファイル・システムを使用しなければなりません。OS/390 バージョン 2 リリース 9 以降、および z/OS の場合は、ネットワーク・ファイル・システムを選択するか、共用 HFS 機能を使用できます。
2. システム管理サーバー領域で HFS 構造を保守するためには、システム管理サーバー領域のユーザー ID (BBOCBRAC REXX 変数 `default_sysmgt_SR_userid` によって CBSYMSR1 として定義されます) が TARGETDIR ディレクトリーの所有者でなければなりません。システム管理サーバー領域は、このディレクトリーにファイルを書き込みます。BBOMCFG はアクセス権ビットを 750 に設定し、他のサーバー領域のユーザー ID がそのディレクトリーに読み取りアクセス権を持つようにします。

サブディレクトリー構造全体は、次のようになります。

```
/TARGETDIR
   /controlinfo
      /envfile
         /SYSPLEX
           /DAEMON01
              current.env -> /TARGETDIR/SYSPLEX/initial/configuration.env
           /INTFRP01
              current.env -> /TARGETDIR/SYSPLEX/initial/configuration.env
           /NAMING01
              current.env -> /TARGETDIR/SYSPLEX/initial/configuration.env
           /SYSMGT01
              current.env -> /TARGETDIR/SYSPLEX/initial/configuration.env
   /SYSPLEX
      /conversations
         /cb302
         /current
           configuration.xml -> /TARGETDIR/SYSPLEX/initial/configuration.xml
      /etc
      /ldap
           SYS1.bboldif.cb
           SYS1.bboslapd.conf
           SYS1.dsnaoini
      /initial
         configuration.env
         configuration.xml
      /resources
         /templates
           CICSEXCIConnectionFactory.xml
           DB2datasource.xml
           IMSAPPCConnectionFactory.xml
      /temp
   /apps
      /SYSPLEX
```

ここで

TARGETDIR
BBOMCFG で TARGETDIR というジョブ変数を使用して指定したマウント・ポイントです。

SYSPLEX
WebSphere for z/OS システムを実行するシスプレックスの名前です。シスプレックス名は、SYSPLEX というジョブ変数の中で指定します。

インストールとカスタマイズに重要なディレクトリーは、次のとおりです。

- *TARGETDIR*/*SYSPLEX*/initial。ランタイム・サーバー用の環境ファイルは、このディレクトリーに置かれます。
- *TARGETDIR*/*SYSPLEX*/etc/ldap. カスタム LDAP 構成ファイルは、このディレクトリーに入っています。

この作業を始める前に: 以下の作業が必要です。

- BBOMCFG のコピーを作成しておく必要があります。
- BBOMCFG を実行するために、UID 0 のユーザー ID と、環境ファイルの格納先となるディレクトリーへの書き込みアクセス権を持っていなければなりません。
- BBOMCFG によって作成されたサブディレクトリーのマウント・ポイントになるターゲット読み取り / 書き込みディレクトリー (TARGETDIR) を持っていなければなりません。

次のステップを実行してください。

1. 表17 に記入する。ここでは、BBOMCFG が使用する変数とその意味が説明されています。

表 17. ジョブ BBOMCFG の変数

変数	説明	デフォルト値	ユーザーの値
-INSTALLDIR	SMP/E インストール後に WebSphere for z/OS のファイルが常駐するディレクトリーの名前	/usr/lpp/WebSphere	

表 17. ジョブ BBOMCFG の変数 (続き)

変数	説明	デフォルト値	ユーザーの値
-TARTGETDIR	WebSphere for z/OS マウント・ポイントの名前。 -TARTGETDIR は、BBOMCFG がディレクトリー構造をセットアップするベース・ディレクトリーとして使用されます。そのディレクトリー構造の中に、HFS に関連したすべての構成データとアプリケーション・データが保持されます。 -TARTGETDIR の値は、環境ファイルの中で指定されている CBCONFIG 環境変数、および WebSphere for z/OS サーバーを始動する開始プロシージャーの中で使用された CBCONFIG JCL 変数の値と同じでなければなりません。 -TARTGETDIR の値は、-INSTALLDIR と同じであっては**なりません**。	/WebSphere390/CB390	
-SYSPLEX	WebSphere for z/OS を実行するモノプレックスまたはシスプレックスの名前。この値は、システム・コンソールで `D SYMBOLS` コマンドを入力すると入手できます。	(なし)	
-SYSNAME	WebSphere for z/OS を実行する OS/390 または z/OS システムの名前。この値は、システム・コンソールで `D SYMBOLS` コマンドを入力すると入手できます。	(なし)	

表 17. ジョブ BBOMCFG の変数 (続き)

変数	説明	デフォルト値	ユーザーの値
-DM_NAME	ブートストラップに使用される初期デーモン・サーバー・インスタンスの名前。	DAEMON01	
-IR_NAME	ブートストラップに使用される初期インターフェース・リポジトリー・サーバー・インスタンスの名前。	INTFRP01	
-NM_NAME	ブートストラップに使用される初期ネーミング・サーバー・インスタンスの名前。	NAMING01	
-SM_NAME	ブートストラップに使用される初期システム管理サーバー・インスタンスの名前。	SYSMGT01	
-OWNER	システム管理サーバーに関連付けられるユーザー ID。これが HFS ファイルの所有者になります。	CBSYMSR1	
-GROUP	HFS ファイルの RACF グループ名。BBOCBRAC がこのグループを作成します (デフォルトは CBCFG1)。このグループの目的は、ランタイム・サーバーのユーザー ID、特に HFS ディレクトリーを所有するシステム管理領域のユーザー ID (CBSYMSR1) と、アプリケーションのインストーラーが、同じ RACF グループにない場合でも、これらの HFS ファイルを管理できるようにすることです。	CBCFG1	

2. 90ページの表17 に従って、BBOMCFG のコピーの変数を更新する。

3. 0 の UID を持ち、-TARGETDIR で指定したディレクトリーとそれにマウントするファイル・システムへの書き込みアクセス権を持っているユーザー ID で、BBOMCFG を実行依頼する。

4. セクション MCFGB の下にあるジョブ・ログを検査する。ログには実行エラー、状況情報、および BBOMCFG が作成したディレクトリーが記録されます。

ジョブが正常に実行されれば、このステップは終了したことになります。

LDAP および WebSphere for z/OS ネーム・スペースのセットアップ

インストールのこの部分では、WebSphere for z/OS の LDAP サーバーをセットアップします。EJB コンポーネントを使用する場合は、クライアントが JNDI を使用できるよう、実行時に LDAP サーバーが必要です。CORBA (MOFW) コンポーネントは、実行時に LDAP サーバーを必要としません。なぜなら、CORBA コンポーネントをサービスする WebSphere for z/OS ランタイム・サーバーは、実際には LDAP サーバーを使用せず、独自のアドレス・スペースで LDAP DLL を実行するからです。いずれの場合でも、管理の目的で LDAP サーバーをセットアップする必要があります。

推奨: システム上にすでに LDAP サーバーがある場合でも、前リリースの WebSphere for z/OS 用の LDAP サーバーがある場合でも、WebSphere for z/OS V4.0 Early Availability 用に新規の LDAP サーバーとデータベースを作成してください。それは次の理由によります。

- ユーザーがデータベースに書き込むデータは、WebSphere for z/OS だけに関連のあるもので、WebSphere for z/OS サービスからアクセス可能であるため。
- 専用の LDAP サーバーとデータベースは、WebSphere for z/OS データベースの同期を保つのに役立つため。

注: 既存の WebSphere Application Server エンタープライズ版 for OS/390 V3.02 LDAP データベースがある場合、スキーマを変更するには、アンロードと再ロードの操作を使用してそのデータベースをマイグレーションする必要があります。269ページの『LDAP データベースを再作成するステップ』を参照してください。

この節の手順は簡単で、すばやく実行できるように記述されています。LDAP のセットアップに関する詳しい説明については、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。

LDAP 構成ファイルと LDAP 初期設定ファイルを変更するためのステップ

このステップでは、この節の後の部分で使用する開始プロシージャーとジョブに備えて、LDAP の構成ファイルと初期設定ファイル (bboldif.cb) を準備する方法について説明します。LDAP サーバー、ネーミング・サーバー領域、およびインターフェース・リポジトリー・サーバー領域の開始プロシージャーでは、LDAP 構成ファイルが使用されます。BBOLD2DB ジョブは、初期設定ファイルを使用してデータベースを準備します。

推奨: LDAP ファイルについては次の推奨事項に従ってください。

- カスタム LDAP ファイル (bboslapd.conf、bboldif.cb、および dsnaoini) は、HFS ファイル・システムに入れてください。弊社のサンプルの開始プロシージャーは、これら 3 つのファイルがすべて、HFS のサブディレクトリー、*TARGETDIR*/*SYSPLEX*/etc/ldap に入っていることを想定しています。
- ネーミング・サービスへのアクセスは LDAP アクセス制御リストによって制御され、管理されます。弊社が提供するサンプルの LDIF ファイル (bboldif.cb) は、CBAdmin と WASAdmin というネーム・スペースへの書き込みアクセス権を備えた 2 つの LDAP アクセス ID を提供します。これらの ID は、書き込みアクセス権を備えているので、LDIF ファイル内の管理パスワードを変更することもできます。
  - CBAdmin のパスワードを変更する場合は、ネーミング・サーバーの LDAPBINDPW 環境変数と、インターフェース・リポジトリー・サーバーの LDAPIRBINDPW 環境変数を更新しなければなりません。各サーバーの current.env ファイルの中で、環境変数を更新してください。詳しくは、383ページの『付録A. 環境ファイル』を参照してください。

  注: 汎用ランタイム名前検索には、ネーム・スペースへの読み取りアクセス権が必要です。サンプルの LDIF ファイルは、読み取りアクセス権を備えた ANYBODY というアクセス ID を提供します。

LDAP のメイン構成ファイル、*system*.bboslapd.conf は、include ステートメントを使用して、他の構成ファイルを組み込みます。一般的な LDAP 構成ファイルには、dsnaoini ステートメントも含まれています。このステートメントは、DSNAOINI データ・セット、つまり DB2 for OS/390 初期設定ファイルを指しています。しかし、弊社のバージョンの DSNAOINI を HFS に入れるには、LDAP、ネーミング・サーバー領域、およびインターフェース・リポジトリー・サーバー領域の開始プロシージャーが、DD ステートメントを通じて DSNAOINI を指していなければなりません (弊社のサンプルでは、すでにそうなっています)。開始プロシージャーでこのような DD ステートメントを使用した場合は、LDAP 構成ファイルの中で dsnaoini ステートメントを使用する必要はありません。したがって、bboslapd.conf の中の dsnaoini ステートメントはコメント化されています。

構造は次のようになります。

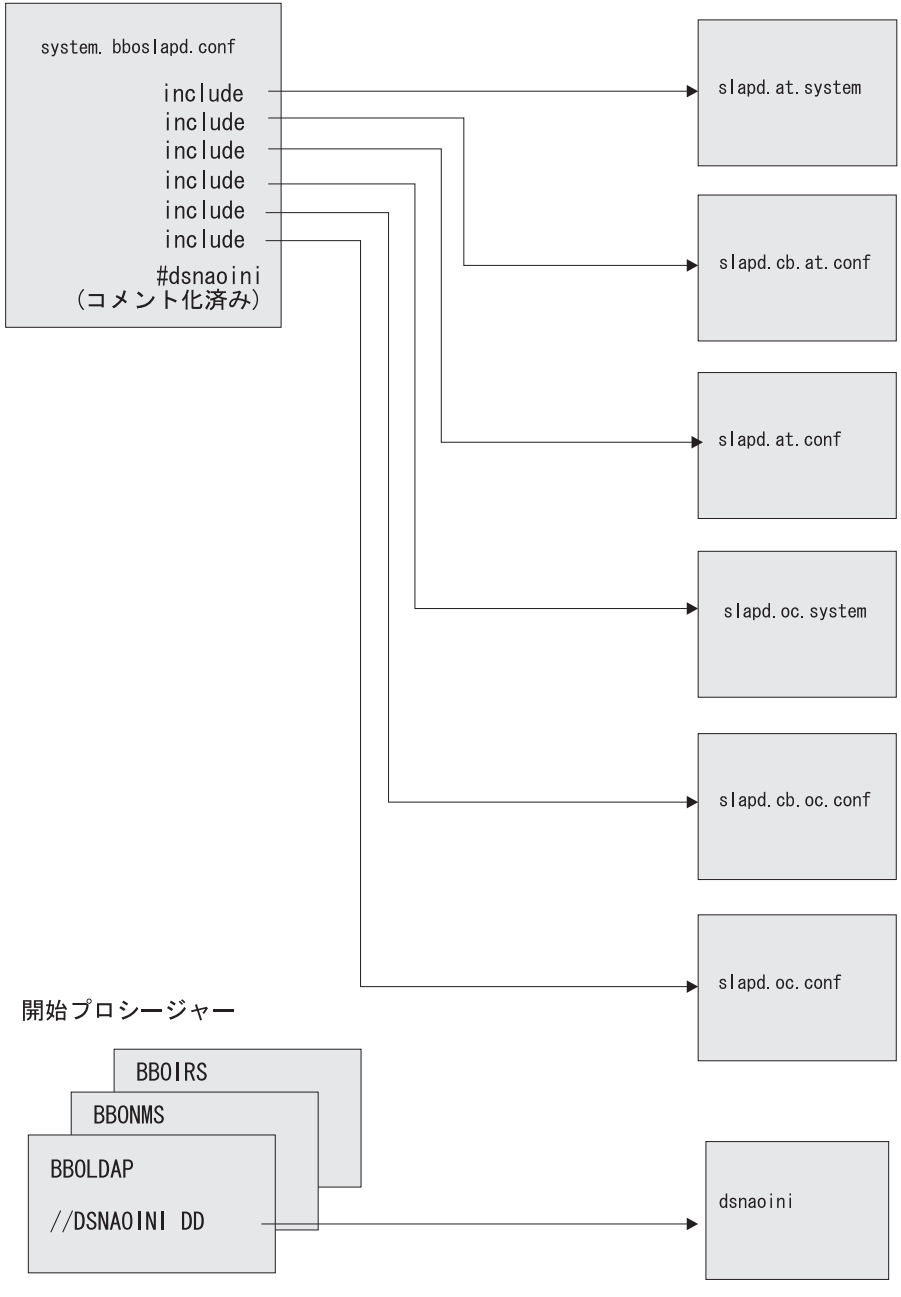


図 5. LDAP 構成ファイルの構造

この作業を始める前に: OS/390 または z/OS バージョン 2 リリース 8 以降で、LDAP とともに提供されているファイルが必要です。このファイル

は、/usr/lpp/ldap/etc ディレクトリーにあります。次の各ファイルです。

ファイル	注
slapd.at.system	一般に使用される属性定義
slapd.cb.at.conf	WebSphere for z/OS の属性定義
slapd.at.conf	一般に使用される属性定義
slapd.oc.system	一般に使用されるオブジェクト・クラス定義
slapd.cb.oc.conf	WebSphere for z/OS のオブジェクト・クラス定義
slapd.oc.conf	一般に使用されるオブジェクト・クラス定義

重要: 通常、これらのファイルを変更する必要はありません。これらの構成ファイルの LDAP スキーマに対する LDAP サービスおよびリリースの変更は、下位互換なので、IBM 提供の変更が WebSphere for z/OS に影響することはありません。ただし、ユーザー自身がスキーマを変更した場合は、この限りではありません。LDAP スキーマを変更する場合は、LDAP ファイルを別のディレクトリーにコピーしてください。コピーしないと、IBM のサービスおよびリリースの変更により、ユーザーの変更が削除され、WebSphere for z/OS に影響が出る場合があります。

ユーザーは、DB2 for OS/390 をインストールする必要があります。重要なガイドラインおよび規則については、44ページの『DB2 for OS/390 データベースおよび LDAP』を参照してください。

ユーザーは、57ページの表13 を完了する必要があります。

LDAP 構成ファイルを変更するには、以下のステップを実行します。

1. ファイル内のコメントに従って、使用している *system*.dsnaoini ファイル (*TARGETDIR*/*SYSPLEX*/etc/ldap に入っている) を変更する。提供する必要のある値については、57ページの表13 を参照してください。

---

2. 使用しているバージョンの *system*.bboldif.cb ファイルと *system*.bboslapd.conf ファイルを、それぞれのファイル内のコメントに従って変更する。提供する必要のある値については、57ページの表13 を参照してください。次のステートメントは、必ず更新してください。

   ```
   suffix          "<ws_rdn>"
   ```

   これを、J2EE コンポーネント用の LDAP における WsnName ツリーの開始点に置き換えます。**例:**

   ```
   suffix          "o=WASNaming, c=US"
   ```

これで、LDAP 構成ファイルの完全セットができました。

LDAP データベースおよび表スペースを作成するためのステップ

この作業を始める前に: 以下のことが必要です。

- BBOLDTBC をコピーする。
- RRS および DB2 for OS/390 を開始する。RRS を初期化しなければ、DB2 for OS/390 を開始することはできません。
- DB2 for OS/390 SYSADM データベース権限を持つユーザー ID を取得する。

注: その時点で表がある場合は、それを削除しなければなりません。 BBOLDTBD のコピーを使用してください。

LDAP データベースを作成するには、以下のステップを実行します。

1. BBOLDTBC のコピーを、そのファイルのコメントに従って変更する。提供する必要のある値については、57ページの表13 を参照してください。

---

2. DB2 for OS/390 SYSADM 権限を持つユーザー ID で、ユーザーのバージョンの BBOLDTBC を実行依頼する。

ジョブが正常に実行されれば、このステップは終了したことになります。

DB2 for OS/390 パッケージをバインドするためのステップ

次の指示に従うと、LDAP サーバーのバインド・ジョブが実行されます。

この作業を始める前に: BBO1JCL および BBO2JCL のコピーが必要です。

DB2 for OS/390 SYSADM データベース権限を持つユーザー ID が必要です。

重要: 次のステップでは、BBO1JCL というジョブを実行することになります。**すでにこのジョブを実行している場合、または DSNACLI 計画がすでにシステム上にある場合は、再び実行しないようにしてください。このジョブは、DB2 for OS/390 用に設定されたすべての GRANT 特権を破棄するからです。**

DB2 for OS/390 のエキスパートでないユーザーは、エキスパートに相談して、BBO1JCL がすでに実行されているか、あるいは DSNACLI がすでにある

かを判断してください。これを判別するためには、次の SPUFI 照会を実行します。この照会は、DSNACLI 計画がすでにバインドされているかどうかを見るテストを行います。

```
select * from sysibm.sysplan where name='DSNACLI';
```

SQLCODE=100 という結果が出たら、DSNACLI はバインドされていません。BBO1JCL を実行できます。

BBO1JCL がすでに実行されているか、DSNACLI がすでに存在している場合は、次のような複数の選択肢があります。

- 既存の特権が失われないように RETAIN を指定して、計画を再びバインドする。
- 計画に関する実行特権を持つユーザーを検出し、再び BBO1JCL を実行し、特権を再度認可する。計画に関する実行特権を持つユーザーを検出するには、次の SPUFI 照会を実行します。

  ```
  select  * from sysibm.sysplanauth where name='DSNACLI';
  ```

- 新しい計画名 (たとえば BBOACLI) を作成し、BBOLDAP および WebSphere for z/OS が使用する dsnaoini ファイルをその新規計画名で更新し、BBO1JCL の場合と同じパッケージ名および DBRM を使用して、新しい計画をバインドする。次に、BBOLDAP、BBOIRS、および BBONMS、あるいは PUBLIC (ユーザーのインストール・ポリシーによって異なります) の実行許可を、適切に更新する。

パッケージをバインドするには、以下のステップを実行します。

1. BBO1JCL のコピーを、そのファイルのコメントに従って変更する。提供する必要のある値については、57ページの表13 を参照してください。

---

2. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、BBO1JCL を実行依頼する。

   結果: 次のメッセージを伴う戻りコード 4 が受け入れ可能です。

   ```
   WARNING, ONLY IBM-SUPPLIED COLLECTION-IDS SHOULD BEGIN WITH  "DSN"
   WARNING, ONLY IBM-SUPPLIED PACKAGE-IDS SHOULD BEGIN WITH  "DSN"
   DSNX100I BIND SQL WARNING USING authorization_id AUTHORITY
   PLAN=(NOT APPLICABLE) DBRM=DSNCLIF4 STATEMENT=statement_number
   SYSIBM.SYSLOCATIONS IS NOT DEFINED
   ```

   ここで、

   authorization_id
   BIND プロセスで使用される許可 ID です。

statement_number
SYSIBM.SYSLOCATIONS を参照する SQL ステートメントのステートメント番号です。

他のエラー・メッセージまたは条件を受け取った場合は、分析が必要です。

---

3. BBO2JCL のコピーを、そのファイルのコメントに従って変更する。提供する必要のある値については、57ページの表13 を参照してください。

---

4. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、BBO2JCL を実行依頼する。

   結果: 次のメッセージを伴う戻りコード 4 が受け入れ可能です。

```
WARNING, ONLY IBM-SUPPLIED COLLECTION-IDS SHOULD BEGIN WITH  "DSN"
WARNING, ONLY IBM-SUPPLIED PACKAGE-IDS SHOULD BEGIN WITH  "DSN"
DSNX100I BIND SQL WARNING USING authorization_id AUTHORITY
PLAN=(NOT APPLICABLE) DBRM=DSNCLIF4 STATEMENT=statement_number
SYSIBM.SYSLOCATIONS IS NOT DEFINED
```

   ここで、

   authorization_id
   BIND プロセスで使用される許可 ID です。

   statement_number
   SYSIBM.SYSLOCATIONS を参照する SQL ステートメントのステートメント番号です。

   他のエラー・メッセージまたは条件を受け取った場合は、分析が必要です。

バインド・ジョブが正常に実行されれば、このステップは終了したことになります。

LDAP テーブルを作成するためのステップ

WebSphere for z/OS は SBBOJCL(BBOLD2DB) と呼ばれるサンプル・ジョブを提供して、LDAP テーブルを初期化します。

この作業を始める前に: BBOLD2DB のコピーおよび、LDAP 構成ファイルの変更済みコピーが必要です。

LDAP サーバーが稼働して**いない**ことを確認してください。

LDAP テーブルを作成するには、以下のステップを実行します。

1. BBOLD2DB のコピーを、そのファイルのコメントに従って変更する。提供する必要のある値については、57ページの表13 を参照してください。

---

2. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、ユーザー・バージョンの BBOLD2DB を実行依頼する。

ジョブが終了したとき、ジョブ内の出力データ・セットによって、2 つのオブジェクトが正常に追加されたことが知らされれば、このステップは終了したことになります。

```
GLD2004I ldif2db: 5 entries have been successfully added out of 5 attempts
```

LDAP の RACF 権限を設定するためのステップ

以下のステップでは、WebSphere for z/OS LDAP サーバーの RACF 権限をセットアップする方法を説明します。

この作業を始める前に: BBOLDRAC および BBOLDRAJ のコピーが必要です。

LDAP サーバーの保護に関する詳細は、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。

RACF 権限をセットアップするには、以下のステップを実行してください。

1. BBOLDRAC および BBOLDRAJ のコピーを、そのファイルのコメントに従って変更する。提供する必要のある値については、57ページの表13 を参照してください。

---

2. 適切な RACF 権限を持つユーザー ID で、ユーザー・バージョンの BBOLDRAJ のコピーを実行依頼する。

BBOLDRAJ ジョブが正常に実行されれば、このステップは完了です。LDAP サーバー開始手順および RACF 権限は、その後、103ページの『LDAP サーバー開始プロシージャーを作成し、オプションでそれをテストするためのステップ』でテストします。

システム管理および LDAP データベースへのアクセスを認可するためのステップ

サーバー識別および新規 LDAP サーバーには、ユーザーが作成したデータベースへの DB2 for OS/390 アクセス権限が必要です。この手順では、必要な GRANT ステートメントを発行します。

この作業を始める前に: システム管理データベース、および LDAP データベースのセットアップを完了しておかなければなりません。86ページの『WebSphere for z/OS システム管理データベースをセットアップするためのステップ』および 94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』を参照してください。BBOCBGRT および BBOLDGRT のコピーをとる必要があります。

注:

1. 計画 DSNACLI の使用許可は、BBOCBGRT および BBOLDGRT ジョブで指定され、PUBLIC に認可されます。この計画へのアクセスを制限したい場合は、最低限、DSNACLI 計画の、WebSphere for z/OS LDAP サーバーの排他的 EXECUTE 権限に関連したユーザー ID (BBOLDRAC の例では、LDAP ユーザー ID として CBLDAP を使用します) を認可しなければなりません。

   ネーミング・サーバー領域およびインターフェース・リポジトリー領域は、DSNACLI 計画を使用しませんが、LDAP データベースへのアクセスは必要なので、CBLIFECYCLE_PKG コレクションを介して入手します。これらのサーバー領域と関連付けられたユーザー ID (BBOCBRAC の例では、CBNAMSR1 および CBINTSR1) にも、排他的な WebSphere for z/OS LDAP サーバーと関連したユーザー ID と同じ SELECT および DBADM 権限が必要です。BBOCBGRT の例では、これらに必要な GRANT ステートメントが提供されます。
2. ここで提供される例では、従来の DB2 for OS/390 セキュリティーが使用されています。DB2 for OS/390 の RACF 保護 (DSNR クラス) および 2 次許可 ID を使用する場合は、計画およびパッケージに対する使用権限を認可するすべてのジョブについて、ユーザーは独自のスクリプトを作成しなければなりません。
3. すべての J2EE サーバーとシステム管理サーバーに、DSNJDBC 計画に対する EXECUTE 権限を付与する必要があります。使用するインストールが DSNJDBC 計画へのパブリック・アクセスを許可する場合は、次の GRANT を BBOCBGRT の中で使用します。

   ```
   GRANT EXECUTE ON PLAN DSNJDBC TO PUBLIC;
   ```

インストールが DSNJDBC 計画へのパブリック・アクセスを許可しない場合は、BBOCBGRT から上記の権限付与を除去し、すべての J2EE サーバーとシステム管理サーバーに個別の EXECUTE 権限を付与する必要があります。DB2 for OS/390 の 2 次許可 ID を使用する場合は、サーバー ID の所属先であるグループにこの権限を付与できます。

データベースへのアクセスを認可するには、以下のステップを実行します。

1. BBOCBGRT のコピーを、そのファイルのコメントに従って変更する。必要な値については、57ページの表13 を参照してください。

   _____

2. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、ユーザー・バージョンの BBOCBGRT を実行依頼する。

   _____

3. BBOLDGRT のコピーを、そのファイルのコメントに従って変更する。必要な値については、57ページの表13 を参照してください。

   _____

4. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、ユーザー・バージョンの BBOLDGRT を実行依頼する。

   _____

2 つの GRANT ジョブが正常に実行されれば、このステップは終了したことになります。

LDAP サーバー開始プロシージャーを作成し、オプションでそれをテストするためのステップ

この手順により、LDAP サーバー開始プロシージャーを作成し、LDAP サーバーを始動し、サーバーが機能していることを検証します。

この作業を始める前に: この節でこれまで述べてきたすべての手順を、完了していなければなりません。

LDAP サーバーを始動し、それが機能していることを検証するには、次のステップを実行してください。

1. BBOLDAP のコピーを、そのファイルのコメントに従って変更する。必要な値については、57ページの表13 を参照してください。

   _____

2. DSNAOINI ファイルが標準 OS データ・セットである場合は、RACF を使用して、グループ CBLDAPGP にファイルへの READ アクセス権を与える。

---

3. (オプション) 次のコマンドを発行する。

```
S BBOLDAP
```

結果: 次のメッセージを待機してください。

```
GLD0122I Slapd is ready for requests
```

---

4. (オプション) OS/390 または z/OS シェルから、次の ldapsearch コマンドを発行する。

```
ldapsearch -v -p 1389 -h 127.0.0.1 -D  "cn=CBAdmin" -w pw -b "your_root" "objectclass=*"
```

ここで

pw
CBADMIN のパスワードです。

your_root
ユーザーのルート・ネーミング・コンテキスト (たとえば ″o=BOSS,c=US″) です。

結果: 次のようなメッセージが表示されます。

```
ldap_init(127.0.0.1, 1389)
filter pattern: objectclass=*
returning: ALL
filter is: (objectclass=*)
o=BOSS, c=US
o=BOSS
objectclass=top
objectclass=organization
description=CBServer Name Tree Root
userpassword=pw
cn=BOSSAdmin, o=BOSS, c=US
objectclass=person
cn=BOSSAdmin
sn=BOSS
userpassword=pw
2 matches
```

---

ldapsearch からメッセージが表示されると、このステップは終了したことになります。

ブートストラップの準備と実行

この節では、ブートストラップ・ジョブおよび、WebSphere for z/OS のカスタマイズに関連したその他のジョブを実行する方法について説明します。

configuration.env ファイルを変更するためのステップ

configuration.env 内の環境変数を更新する。提供されている例には、推奨される値がありますが、ユーザーが変更しなければならない値もいくつかあります。ファイルは、*TARGETDIR*/*SYSPLEX*/initial に入っています。

ここで、

TARGETDIR
90ページの表17 でユーザーが -TARGETDIR のために指定した値です。

SYSPLEX
90ページの表17 でユーザーが -SYSPLEX のために指定した値です。

環境変数についての詳細は、383ページの『付録A. 環境ファイル』を参照してください。

この作業を始める前に: 88ページの『システム管理 HFS 構造を作成するためのステップ』を完了していなければなりません。

configuration.env ファイルを変更するには、以下のステップを実行します。

1. configuration.env ファイルを開く。

---

2. CLASSPATH ステートメントと LIBPATH ステートメントを検査する。/usr/lpp/WebSphere を製品のマウント・ポイントとして使用しなかった場合は、CLASSPATH と LIBPATH の中でパスを変更しなければなりません。
   - 次に示してある CLASSPATH は、製品のマウント・ポイントが /usr/lpp/WebSphere であるときに使用するものです。場合によっては、パスを変更し、以下のファイルが CLASSPATH 環境変数に入るようにする必要があります。

     ```
     CLASSPATH=db2_install_path/classes/db2j2classes.zip
     :/usr/lpp/WebSphere/samples/PolicyIVP/PRODUCTION/bboplc.jar
     :/usr/lpp/WebSphere/samples/PolicyIVP/PRODUCTION/bboplsj.jar
     ```

     ここで、*db2_install_path* は DB2 for OS/390 をインストールしたパスです。

手続き型のアプリケーション・アダプターを使用する計画の場合は、次のものを CLASSPATH に追加します。

```
/usr/lpp/WebSphere/lib/bboadptr.jar:
/usr/lpp/WebSphere/lib/bbokeart.jar:
/usr/lpp/WebSphere/lib/bbokpart.jar
```

CLASSPATH ステートメントは、全体が 1 行になければなりません。

- LIBPATH を、JDBC ライブラリーが組み込まれるようにコード化します。**例:**

```
LIBPATH=:/usr/lpp/java/IBM/J1.3/bin
:/usr/lpp/java/IBM/J1.3/bin/classic
:/usr/lpp/WebSphere/lib
:db2_install_path/lib/
```

ここで、*db2_install_path* は DB2 for OS/390 をインストールしたパスです。LIBPATH ステートメントは、全体が 1 行になければなりません。

---

3. 次の環境変数を検査し、必要であれば設定を変更する。

環境変数	ファイル内の値
注	
詳細については、383ページの『付録A. 環境ファイル』を参照してください。	
com.ibm.ws.naming.ldap. masterurl= ldap://*IP_name:port*	ldap://*local_host*:1389
IP_name:port は、LDAP の IP 名とポートです。使用している LDAP サーバーが 1389 以外のポートを使用している場合は、com.ibm.ws.naming.ldap.masterurl 環境変数を更新します。**例:** `com.ibm.ws.naming.ldap.masterurl=ldap://wsldap:1389` 弊社の推奨事項に従った場合、使用している LDAP ポートは 1389 です。	
CBCONFIG	/WebSphere/CB390
90ページの表17 に示した -TARGETDIR の値に一致させてください。	
DAEMON_IPNAME	DOMAIN_QUALIFICATION.COM
使用しているシステムの IP 名に変更してください。	
DAEMON_PORT	5555
TCP/IP 解決構成ファイルで定義したものと同じでなければなりません。	
LDAPCONF	/WebSphere390/CB390/*sysplex* /etc/ldap/*system*.bboslapd.conf
sysplex と *system* を変更してください。	

環境変数	ファイル内の値
注	
LDAPIRCONF	/WebSphere390/CB390/*sysplex* /etc/ldap/*sysplex*.bboslapd.conf
sysplex を変更してください。	
LDAPROOT	o=BOSS,c=US
LDAPIRROOT	o=BOSS,c=US
LD_LIBRARY_PATH	*path*/lib
path は、DB2 for OS/390 のインストール・パスです。**例:** `/usr/lpp/db2/db2710/lib` DB2 for OS/390 ディレクトリーが classpath と libpath に入っていれば (弊社の指示ではそうなります)、LD_LIBRARY_PATH は必要ありません。この環境変数の詳細については、*DB2 for OS/390 Application Programming Guide and Reference for Java* を参照してください。	
LOGSTREAMNAME	

81ページの『エラー・ログ・ストリームをセットアップするためのステップ』で作成したログ・ストリームの名前を使用します。これにより、デーモンおよびシステム管理サーバーがエラー情報を書き込むログ・ストリームが決定されます。
 	
例:
`LOGSTREAMNAME=MY.CB.ERROR.LOG`
 	
特に指定されていなければ、デフォルト値は次のようになります。
`BBO.derived_name`
 	
ここで、*derived_name* は、デーモン・サーバーの IP 名から派生したログ・ストリームの名前です。
 	
ヒント: 引用符のないログ・ストリーム名をコード化します。ログ・ストリーム名はデータ・セット名ではありません。	

RESOLVE_IPNAME	DOMAIN_QUALIFICATION.COM
使用しているシステムの IP 名に変更してください。	
RESOLVE_PORT	900
SYS_DB2_SUB_ SYSTEM_NAME	DB2
使用している DB2 for OS/390 サブシステム名に一致させてください。	
TRACEALL	1
推奨: 環境ファイルの TRACEALL 環境変数を、例外トレース用に設定してください (デフォルト設定では、`TRACEALL=1`)。	

4. configuration.env ファイルに対する所有権とアクセス権を検査する。正しくない場合、ブートストラップは失敗します。所有権とアクセス権が次のようになっているかどうかを確認してください。

```
-rw-r-----   1 CBSYMSR1 CBCFG1      2356 Jan 24 09:45 configuration.env
```

所有権とアクセス権を変更する必要がある場合は、次のコマンドを発行します。

```
chmod 640 configuration.env
chown CBSYMSR1:CBCFG1 configuration.env
```

configuration.env ファイルを正常に更新できれば、このステップは完了です。

コンソールからブートストラップのフェーズ 1 を準備し、開始するためのステップ

この作業を始める前に: SBBOJCL の開始プロシージャーのコピーが必要です。88ページの『システム管理 HFS 構造を作成するためのステップ』のステップに従ってください。

RRS および DB2 for OS/390 が動作していることを確認してください。動作していない場合は、RRS を開始し、その初期化を待って、DB2 for OS/390 を開始してください。

注: デーモンは Ctrace に PARMLIB(CTIBBO00) を使用するので、デーモンの初期化の際に Ctrace の外部書き出しプログラム (サンプルでは BBOWTR) が動作していない場合は、警告メッセージが表示されます。ユーザーは、オプションで BBOWTR を開始することができます。その場合は、コンポーネント・トレース・データ・セットを割り振ってカタログを作成し、ファイルのコメントに従って BBOWTR を編集する必要があります。そうしてから、BBOWTR を開始しなければなりません。

データ・セットを割り振り、それに以下の DCB 属性を与えます。

- DSORG=PS (順次データ・セット)
- ブロック・サイズ 27998
- Lrecl 27994
- レコード・フォーマット VB

BBOWTR の例を、データ・セット名に DISP=OLD を組み込むように変更してください。

Ctrace 外部書き出しプログラムを開始するには、次のコマンドを発行します。

```
TRACE CT,WTRSTART=BBOWTR
```

コンポーネント・トレース (Ctrace) および、Ctrace 外部書き出しプログラムのセットアップに関する情報は、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 を参照してください。

ブートストラップのフェーズ 1 を準備し、開始するには、次のステップを実行してください。

1. 以下の開始プロシージャーのコピーを、各ファイルのコメントに従って更新する。
   - BBODMN

     注: BBOMCFG で -DM_NAME のデフォルト値を変更した場合は、必ず、BBODMN のコピーで SVRNAME パラメーターを変更してください。
   - BBONM
   - BBONMS
   - BBOSMS
   - BBOSMSS
   - BBOIR
   - BBOIRS

---

2. ブートストラップのフェーズ 1 を開始する。**パラメーター、PARMS='-ORBCBI COLD' に注意してください。このパラメーターは必ず使用しなければなりません。**

   ```
   S BBODMN.DAEMON01,PARMS='-ORBCBI COLD'
   ```

   注:

   a. コマンドは、表示されるとおりに入力してください。

   b. 何らかの理由で BBODMN がキャンセルされた場合は、再始動することができます。その場合、ブートストラップは中断したステップから再開します。

c. インストール中およびカスタマイズ中は、自動再始動管理 (ARM) を使用可能にしないことをお勧めします。終了するまで待ってください。ARM をセットアップしない場合は、BBODMN を実行すると、デーモン、ネーミング・サーバー、システム管理サーバー、およびインターフェース・リポジトリー・サーバーに、ARM 登録エラーが生じる可能性があります。これは問題ありません。ただし、サーバーの自動再始動は使用できません。自動再始動管理のセットアップ方法については、295ページの『自動再始動管理のセットアップ』を参照してください。

d. BBODMN がエラーで終了し、メッセージ、

```
IEF188I PROBLEM PROGRAM ATTRIBUTES ASSIGNED
```

が表示された場合は、BBO.SBBOLOAD、BBO.SBBOLD2、BBO.SBBOLPA の各データ・セットに対する APF 許可があるかどうかを確認してください。72ページの『基本システムを変更するためのステップ』を参照してください。

弊社のテストでは、このステップが完了するのに約 10 分かかりました。

BBOSMS のジョブ出力に次のメッセージが表示されれば、このステップは終了したことになります。

```
BBOU0134I WS BOOTSTRAP PHASE 1 IS COMPLETE.
```

WebSphere for z/OS のアドレス・スペースをすべてキャンセルし、デーモンを再始動するためのステップ

この作業を始める前に: ブートストラップのフェーズ 1 を完了していなければなりません。

次のステップを実行してください。

1. デーモンをキャンセルする。その結果、他のサーバー・インスタンスもキャンセルされます。

   ```
   C DAEMON01
   ```

   注: 次のコマンドを発行してデーモンをキャンセルすることもできます。

   ```
   C BBODMN.DAEMON01
   ```

   他の WebSphere for z/OS アドレス・スペースが残っている場合は、それらをキャンセルしてください。

---

2. デーモンをパラメーターを伴わずに再始動する。

   ```
   S BBODMN.DAEMON01
   ```

   BBONM、BBOSMS、または BBOIR を開始する必要はありません。これは、デーモン・サーバーが自動的に行います。ランタイム・サーバー・インスタンスがすべて初期化されるまで待ってください。

オペレーターのコンソールまたはジョブ・ログに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBOU0016I INITIALIZATION COMPLETE FOR DAEMON DAEMON01.
BBOU0020I INITIALIZATION COMPLETE FOR CB SERIES CONTROL REGION  SYSMGT01.
BBOU0020I INITIALIZATION COMPLETE FOR CB SERIES CONTROL REGION  NAMING01.
BBOU0020I INITIALIZATION COMPLETE FOR CB SERIES CONTROL REGION  INTFRP01.
```

ネーミング・クライアントを実行するためのステップ

ネーミング・クライアント・ジョブは、WebSphere for z/OS のデフォルト・ネーミング・スペースを確立します。インストール検査プログラムが正常に動作するには、まず、このジョブが正常に動作しなければなりません。ユーザーに必要なのは、コールド・スタートごとに 1 度、ネーミング・クライアントを実行することだけです。ただし、ネーミング・クライアントが正常に動作しない場合は、LDAP 項目を削除してから、再びネーミング・クライアントを実行してください。201ページの『LDAP 項目を削除するためのステップ』を参照してください。

この作業を始める前に: 94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』の指示に従っていることを確認してください。

BBONMC および BBOCNFG のコピーをとる必要があります。BBONMC は、ジョブとしてでも開始プロシージャーとしてでも実行できますが、ジョブとして実行してください。BBONMC に関連したユーザーには、LDAP データベースを更新する権限がなければなりません。システム管理の管理者ユーザー ID (CBADMIN) の使用をお勧めします。別のユーザー ID を使用する場合は、289ページの『管理アプリケーションの新規管理者の追加』の指示に従ってください。

ネーミング・クライアントを実行するには、次のステップに従ってください。

1. 使用している作業用変数ブロック・データ・セット内のネーミング構成ファイル BBOCNFG のコピーを、インストール構成に従って更新するか、また

は製品に添付されている BBOCNFG を使用する。ネーミング構成ファイルをコード化する方法については、413ページの『付録B. ネーム・スペースの構成』を参照してください。

2. ネーミング・クライアント、BBONMC のコピーを、そのファイルのコメントに従って更新する。

3. LDAP データベースを更新する適切な権限を持つユーザー ID (たとえば CBADMIN) と、そのパスワードを、ジョブ・カード上に配置する。

4. BBONMC を実行依頼する。

コンソールまたは BBONMC のジョブ出力に次のメッセージが表示されれば、このステップは完了です。

```
BBOU0126I: The configuration of the global NameSpace has succeeded.
           NameSpace configuration has been committed.
```

最初のインターフェース・リポジトリー・クライアント・ブートストラップを実行するためのステップ

インターフェース・リポジトリー・クライアント・ジョブ BBOIRC は、インターフェース・リポジトリーを初期化します。

この作業を始める前に: LDAP データベースのセットアップを行わなければなりません。

BBOIRC のコピーをとる必要があります。BBOIRC は、ジョブとしてでも開始プロシージャーとしてでも実行できますが、ジョブとして実行してください。BBOIRC に関連したユーザーには、LDAP データベースを更新する権限がなければなりません。システム管理の管理者ユーザー ID (CBADMIN) の使用をお勧めします。別のユーザー ID を使用する場合は、289ページの『管理アプリケーションの新規管理者の追加』の指示に従ってください。

最初のインターフェース・リポジトリー・クライアント・ブートストラップを開始するには、次のステップを実行してください。

1. インターフェース・リポジトリー・クライアント、BBOIRC のコピーを、そのファイルのコメントに従って更新する。

2. LDAP データベースを更新する適切な権限を持つユーザー ID (たとえば CBADMIN) と、そのパスワードを、ジョブ・カード上に配置する。

---

3. BBOIRC を実行依頼する。

BBOIRC のジョブ出力に次のメッセージが表示されれば、このステップは終了したことになります。

```
BBOU0185I IR Bootstrap completed sucessfully for INTFRP01
```

WebSphere for z/OS のアドレス・スペースをすべてキャンセルし、ブートストラップのフェーズ 2 を開始するためのステップ

この作業を始める前に: DAEMON01、SYSMGT01、NAMING01、および INTFRP01 が稼働していなければなりません。

次のステップを実行してください。

1. デーモンをキャンセルする。その結果、他のサーバー・インスタンスもキャンセルされます。

   ```
   C DAEMON01
   ```

   注: 次のコマンドを発行してデーモンをキャンセルすることもできます。

   ```
   C BBODMN.DAEMON01
   ```

   他の WebSphere for z/OS アドレス・スペースが残っている場合は、それらをキャンセルしてください。

---

2. ブートストラップのフェーズ 2 を開始する。**パラメーター、PARMS='-ORBCBI COLD' に注意してください。このパラメーターは必ず使用しなければなりません。**

   ```
   S BBODMN.DAEMON01,PARMS='-ORBCBI COLD'
   ```

   注:

   a. コマンドは、表示されるとおりに入力してください。

   b. インストール中およびカスタマイズ中は、自動再始動管理 (ARM) を使用可能にしないことをお勧めします。終了するまで待ってください。ARM をセットアップしない場合は、BBODMN を実行すると、デーモン、ネーミング・サーバー、システム管理サーバー、およびインターフェース・リポジトリー・サーバーに、ARM 登録エラーが生じる可能性

があります。これは問題ありません。ただし、サーバーの自動再始動は使用できません。自動再始動管理のセットアップ方法については、295ページの『自動再始動管理のセットアップ』を参照してください。

BBOSMS のジョブ出力に次のメッセージが表示されれば、このステップは終了したことになります。

```
BBOU131I  THE WEBSPHERE BOOTSTRAP HAS COMPLETED.
```

ブートストラップが正常であることを検査するためのステップ (オプション)

この作業を始める前に: 以下のことを確認してください。

- WebSphere for z/OS ブートストラップが完了している。システム・ログのジョブ出力で、メッセージ BBOU0131I を待機してください。
- LDAP サーバーが稼働している。稼働していない場合は、103ページの『LDAP サーバー開始プロシージャーを作成し、オプションでそれをテストするためのステップ』で作成した開始プロシージャーを使用して、LDAP サーバーを始動してください。たとえば、作成した開始プロシージャーが BBOLDAP である場合は、次のコマンドを発行します。

  ```
  S BBOLDAP
  ```

ブートストラップが正常であることを検査するには、次のステップを実行してください。

1. OMVS セッションで次のコマンドを発行する。

   ```
   export LDAP_BASEDN="root_naming_context"
   ldapsearch -v -p port -h 127.0.0.1 "objectclass=*" >name.space
   ```

   ここで、

   root_naming_context
   bboslapd.conf 構成ファイルの接尾部ステートメントで、ユーザーが指定したルート・ネーミング・コンテキスト (たとえば o=BOSS,c=US) です。

   port
   LDAP サーバー用に定義した使用可能なポートです。1389 の使用をお勧めします。-p *port* を指定しない場合、LDAP サーバーのデフォルト・ポートは 389 です。

---

2. CBADMIN を検出できるかどうか確認する。次のコマンドを発行してください。

```
grep CBADMIN name.space
```

CBADMIN が検出されれば、ブートストラップは正常です。

WebSphere for z/OS のアドレス・スペースをすべてキャンセルし、デーモンを再始動するためのステップ

この作業を始める前に: ブートストラップのフェーズ 2 を完了し、それが正常であることを検証しなければなりません。

次のステップを実行してください。

1. デーモンをキャンセルする。その結果、他のサーバー・インスタンスもキャンセルされます。

```
C DAEMON01
```

注: 次のコマンドを発行してデーモンをキャンセルすることもできます。

```
C BBODMN.DAEMON01
```

他の WebSphere for z/OS アドレス・スペースが残っている場合は、それらをキャンセルしてください。

---

2. デーモンをパラメーターを伴わずに再始動する。

```
S BBODMN.DAEMON01
```

BBONM、BBOSMS、または BBOIR を開始する必要はありません。これは、デーモン・サーバーが自動的に行います。

オペレーターのコンソールまたはジョブ・ログに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBOU0016I INITIALIZATION COMPLETE FOR DAEMON DAEMON01.
BBOU0020I INITIALIZATION COMPLETE FOR CB SERIES CONTROL REGION  SYSMGT01.
BBOU0020I INITIALIZATION COMPLETE FOR CB SERIES CONTROL REGION  NAMING01.
BBOU0020I INITIALIZATION COMPLETE FOR CB SERIES CONTROL REGION  INTFRP01.
```

管理アプリケーションおよび操作アプリケーションのインストール

この節のプロシージャーでは、管理アプリケーションおよび操作アプリケーションをインストールする方法と、ワークステーションがドメイン・ネーム・サーバー (DNS) を使用しない場合は、ワークステーションの Hosts ファイルを更新する方法について、説明します。

管理アプリケーションおよび操作アプリケーションをインストールするためのステップ

以下のステップでは、管理アプリケーションおよび操作アプリケーションのパッケージを Windows ワークステーションにダウンロードしてインストールします。プログラム・パッケージは、自己解凍方式の EXE ファイルです。

この作業を始める前に: 10ページの『WebSphere for z/OS のシステム要件の決定』のワークステーション要件を確認してください。

管理アプリケーションおよび操作アプリケーションをインストールするには、以下のステップを実行します。

1. コマンド・プロンプトを開き、プログラム・パッケージをダウンロードするディレクトリーに移動する。

   例:

   ```
   C:¥>cd temp

   C:¥TEMP>
   ```

   ---

2. WebSphere for z/OS が動作しているシステムに FTP コマンドを発行する。システムにログオンしてください。OMVS セグメントが定義されている任意のユーザー ID を使用してログオンできます。弊社の例では CBGUEST を使用していますが、ユーザー自身のユーザー ID を使用することをお勧めします。

   例:

   ```
   C:¥TEMP>ftp boss.my.com
   Connected to boss.my.com.
   220-FTPD1 IBM FTP CS V2R8 at OS390CBSERIES, 15:18:44 on 2000-04-18.
   220 Connection will close if idle for more than 5 minutes.
   User (boss.my.com:(none)): cbguest
   331 Send password please.
   Password:
   230 CBGUEST is logged on.  Working directory is "CBGUEST.".
   ```

   ---

3. プログラム・パッケージがあるディレクトリー (デフォルトでは /usr/lpp/WebSphere/bin) に移動する。

   例:

   ```
   ftp> cd /usr/lpp/WebSphere/bin
   250 HFS directory /usr/lpp/WebSphere/bin is the current working directory
   ```

---

4. bin コマンドを発行し、プログラム・パッケージを入手する。

   例:

   ```
   ftp> bin
   200 Representation type is Image
   ftp> get bboninst.exe
   200 Port request OK.
   125 Sending data set /usr/lpp/WebSphere/bin/bboninst.exe
   250 Transfer completed successfully.
   16725648 bytes received in 35.16 seconds (475.70 Kbytes/sec)
   ```

---

5. FTP を終了する。

   例:

   ```
   ftp> quit
   221 Quit command received. Goodbye.
   ```

---

6. 「スタート」メニューから、「ファイル名を指定して実行」をクリックし、次に「参照」を使用して、プログラム・パッケージを検索する。「OK」をクリックする。

---

7. InstallShield ウィザードに従って、インストールを完了する。

InstallShield ウィザードが正常に完了すれば、このステップは終了したことになります。

ワークステーションの Hosts ファイルを更新するためのステップ

管理アプリケーションおよび操作アプリケーションが動作しているワークステーションが、ドメイン・ネーム・サーバー (DNS) に接続されていない場合、あるいは WebSphere for z/OS と同じドメインにない場合は、ワークステーションの Hosts ファイルを更新しなければなりません。ワークステーションは、

Hosts ファイルを介して、WebSphere for z/OS が動作しているシステムを検出することができます。ワークステーションが DNS に接続されている場合は、この手順はスキップしてください。

この作業を始める前に: Windows システムが稼働していなければなりません。

Windows で Hosts ファイルを更新するには、以下のステップを実行してください。

1. Hosts ファイルを検出する。Windows NT では、通常は、`c:¥winnt¥system32¥drivers¥etc` にあります。Windows 95 では、通常は `c:¥windows` にあります。

   ヒント: Hosts ファイルがない場合は、テキスト・エディターを使用して作成し、それを適当なディレクトリーに置いてください。Hosts ファイルの例、Lmhosts.sam があれば、それを、新規 Hosts ファイルのモデルに使用することができます。

---

2. そのファイルに項目を追加して、TCP/IP のホスト名とアドレスを関連付ける。Hosts ファイルの各項目は、IP アドレスに完全修飾 IP 名が続き、オプションで、1 つまたは複数の別名という構成になっています。適切なアドレス解決を確保するには、完全修飾名が IP アドレスの直後になければなりません。各項目は間にブランクを入れ、1 行で表示する必要があります。

   例:

   ```
   #
   #  The following entries allow the workstation to access CB on OS390 without
   #  the workstation being in the same domain.
   #
   9.82.93.2 wsccb.washington.ibm.com  wsccb #CB Daemon_IPname and alias
   #
   #  The CB Resolve_IPname is the same for this installation or it, too, must
   #  be added.
   #
   ```

---

3. Hosts ファイルを保管し、テストする。コマンド・ウィンドウを開き、追加したばかりの名前で PING コマンドを発行して、変更をテストすることができます。

   例:

   ```
   ping wsccb
   ```

PING コマンドからの応答があれば、このステップは終了したことになります。

インストール検査プログラム用のアプリケーション・サーバーの定義

BBOASR2 サーバーか BBOASR1 サーバー、またはその両方を定義するには、管理アプリケーションを使用します。BBOASR2 サーバーは J2EE サーバーであり、弊社のインストール検査プログラム (IVP) の 1 つは、このサーバーを使用して J2EE コンポーネント・サポートをテストします。BBOASR1 サーバーは MOFW サーバーであり、その他の IVP は、このサーバーを使用して MOFW コンポーネント・サポートをテストします。これらのサーバーは、IVP を実行できるようにするだけでなく、ユーザー独自のビジネス・アプリケーション・サーバーをセットアップする例を提供します。

後に示すこのトピックの 2 つの主要な節では、管理アプリケーションを開始する方法と、新規会話を追加する方法について説明します。*会話* は、WebSphere for z/OS の構成を表示し、変更することができるシステム管理オブジェクトです (会話と 管理アプリケーションの詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 を参照してください)。その後、それぞれの節でアプリケーション・サーバーの定義方法、IVP アプリケーションのインストール方法、会話を活動化する方法について説明します。会話を活動化することは、WebSphere for z/OS のシステム管理機能で使用するためにサーバー構成が更新されることを意味しています。

使用することを計画しているコンポーネント・タイプに応じて、いずれかのサーバー、または両方のサーバーを定義できます。どれを選択するかは、どのコンポーネント・タイプのサーバーが必要であるかに基づいて決めてください。

セットアップしたいもの	サーバーの定義方法の説明
J2EE サーバー	121ページの『BBOASR2 J2EE サーバーの定義』
MOFW サーバー	149ページの『BBOASR1 MOFW サーバーの定義』
J2EE サーバーと MOFW サーバー	121ページの『BBOASR2 J2EE サーバーの定義』、および 149ページの『BBOASR1 MOFW サーバーの定義』 (2 つの異なる会話を使用)

この時点で、決定に合ったステップを実行できます。

管理アプリケーションは、システム管理サーバーと対話して作業を行います。この対話が完了するのにはしばらく時間がかかります。

BBOASR2 J2EE サーバーの定義

J2EE コンポーネントの使用を計画している場合は、この節に述べるステップを実行して BBOASR2 をセットアップしてください。BBOASR2 は、IVP が J2EE コンポーネント・サポートをテストするために使用する J2EE サーバーです。

管理アプリケーションを開始するためのステップ

この作業を始める前に: WebSphere for z/OS ランタイム・サーバー・インスタンスを初期化し、管理アプリケーションをインストールしておかなければなりません。

管理アプリケーションを開始するには、以下のステップを実行してください。

1. ワークステーションで、「スタート」、「プログラム」、「IBM WebSphere for z/OS Administration」を順にクリックする。

   ---

2. ダイアログにブートストラップ・サーバー IP 名、ポート 900、ユーザー ID cbadmin およびパスワードを入力する (パスワードについては、RACF のサンプル BBOCBRAC を参照)。「OK」をクリックする。

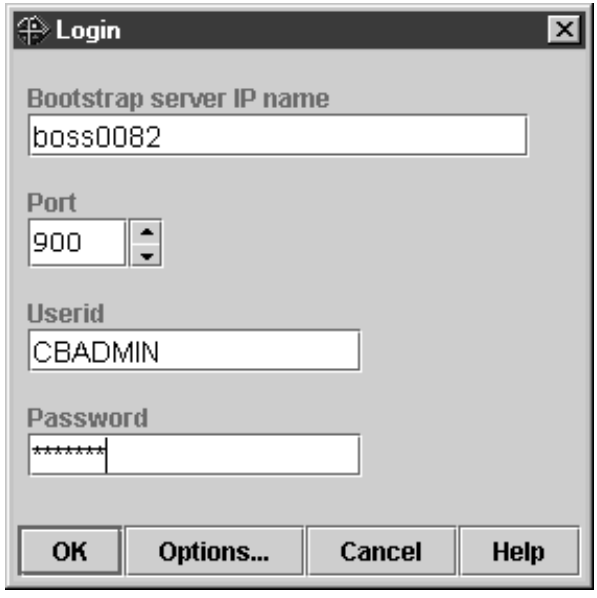
   推奨:

   a. 単一のワークステーションからであれ、複数のワークステーションからであれ、同じ管理者 ID を使用して、アプリケーションの複数並行セッションにログオン**しない**ことを強くお勧めします。たとえば、ユーザー ID に CBADMIN を使用して、ワークステーションで 管理アプリケーションを開始する場合、そのワークステーションからでも別のワークステーションからでも、CBADMIN を使用して別のセッションを開始することはできません。

   b. 複数の管理者ユーザー ID を定義した場合、それらすべてが同時にログオンできますが、会話の更新および活動化を行うのは、一度に **1 つだけ** にしてください。

      複数の管理者が会話を活動化しようとした場合には、予期しない結果が生じます。ある管理者が新規の会話を開始すると、現在活動状態にある会話のコピーがベース・レベルとして使用されます。複数の管理者が、現在活動状態にある同じ会話に基づいて新規会話を作成した場合は、最初に活動化を行った管理者が成功します。その他の活動化を試みたすべての管理者は、それらの管理者による変更が現在活動状態にある会話に基づくものではないので (現在活動状態の会話は、それらの管理者の下にあったものから変化してしまったため)、活動化に失敗します。2 番目以降の管理者は、新しい現行会話を使用して、やり直さなければなりま

せん。これは、変更の量によっては大きな混乱を起こします。このため、ある管理者が会話を更新して活動化しようとしている間、それ以外の管理者は、読み取りまたは表示機能に限定して管理アプリケーションを使用しなければなりません。



メインウィンドウにブートストラップの会話が表示されれば、このステップは終了したことになります。接続にトラブルがある場合は、ヘルプ・システムまたは *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 で、詳しい情報を入手してください。

新しい会話を開始するためのステップ

この作業を始める前に: ログインして管理アプリケーションを開始しなければなりません。

新規会話を開始するには、以下のステップを実行してください。

1. 左マウス・ボタンで会話 (Conversations) フォルダーを選択する。次に、右マウス・ボタンを使用して、会話 (Conversations) フォルダーをクリックし、「追加 (Add)」を選択する。

---

2. 「特性 (properties)」フォーム (右側のパネル) で、新規会話に名前を付ける。たとえば、ここではこの会話に「BBOASR2 SERVER DEFINITION」という名前を付けました。説明も加えてください (オプション)。

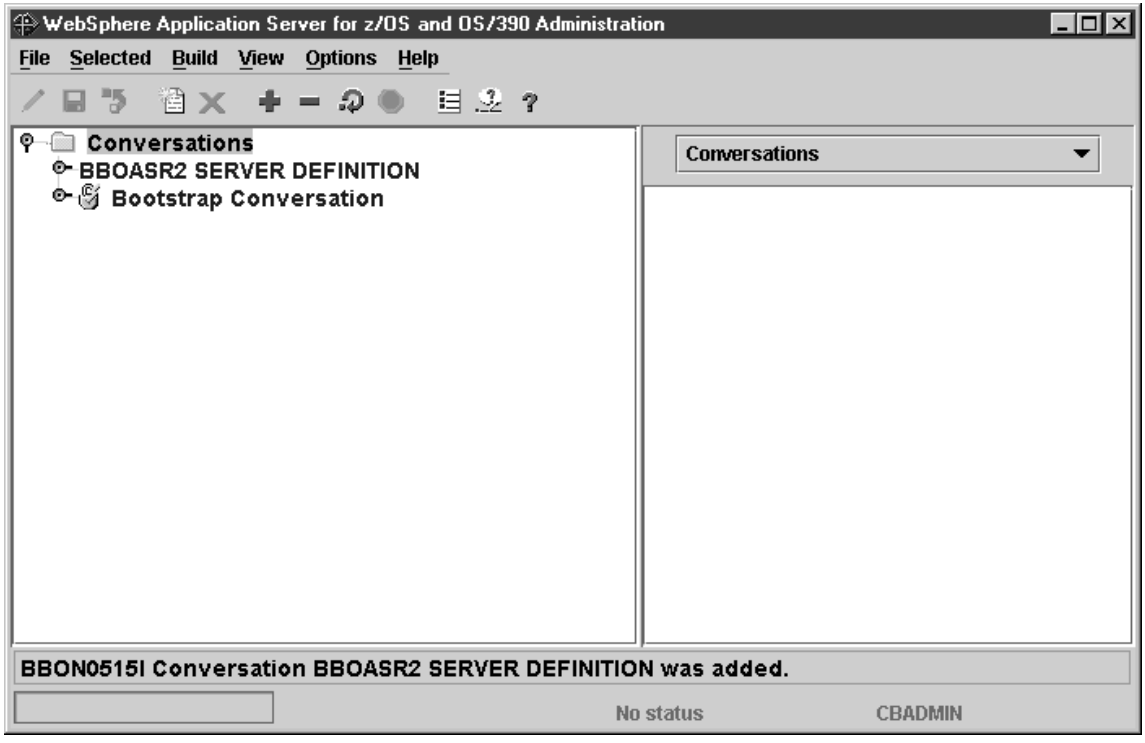
---

3. ディスケットへの保管を表すアイコンをクリックする。「... 会話の追加 (Adding... Conversations)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Conversation BBOASR2 SERVER DEFINITION was added.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
Conversations
BBON0515I Conversation BBOASR2 SERVER DEFINITION was added.
No status
CBADMIN

BBOASR2 J2EE サーバーを追加するためのステップ
この作業を始める前に: 現行会話で作業している必要があります。

新規サーバーを追加するには、以下のステップを実行します。

1. 会話名の左のノードをクリックして、新しい会話ツリーを展開する。

   _____

2. シスプレックスを展開し、次にユーザーのシスプレックスを展開する。

   _____

3. 左マウス・ボタンで J2EE サーバーのフォルダーを選択する。次に、右マウス・ボタンを使用して J2EE サーバーのフォルダーをクリックし、「追加 (Add)」を選択する。

   _____

4. 「プロパティー (properties)」フォームで、使用しているインストールに合わせて、値を入力するか選択する。

サーバー名	BBOASR2
サーバーの説明	オプション・サーバーの説明
制御領域識別	制御領域が動作するユーザー ID。これは RACF STARTED クラスの項目と一致し、制御領域用の適切な RACF 権限を有していなければなりません。BBOCBRAC のデフォルト値は CBACRU1 です。
サーバー領域識別	サーバー領域が動作するユーザー ID。これは RACF STARTED クラスの項目と一致し、サーバー領域用の適切な RACF 権限を有していなければなりません。BBOCBRAC のデフォルト値は CBASRU1 です。
サーバー領域のスタック・サイズ (バイト)	0
実動 J2EE サーバー	チェック・ボックスにチェックマークを付ける
許可されるデバッガー	チェックなしのまま
分離ポリシー	1 つのサーバー領域につき 1 トランザクション
レプリカ生成ポリシー	サーバーごとに 1 つ
サーバー領域には JVM が必要	チェック・ボックスをクリアする
サーバー領域の JVM 名	ブランクのまま
ローカル識別	CBGUEST
リモート識別	CBGUEST

登録トランザクション・ファクトリー	チェック・ボックスのクリア *

* トランザクション・ファクトリーとして登録するサーバーは、いつでも使用可能でなければなりません。BBOASR2 はインストール検査の間だけ使用可能なので、このサーバーを、トランザクション・ファクトリーとして登録することはできません。

ネーミング・サーバーは、トランザクション・ファクトリーとして定義されています。ネーミング・サーバーを構成から除去する場合は、トランザクション・ファクトリーに別のサーバーを作成する必要があります。複数のトランザクション・ファクトリーを持つこともできますが、そのようなサーバーは、常に使用可能でなければならないことを覚えておく必要があります。

サーバー領域ガーベッジ・コレクションの許可	チェック・ボックスにチェックマークを付ける
ガーベッジ・コレクション・インターバル	50000
ログ・ストリーム名	エラー情報を取り込むためにセットアップするログ・ストリームの名前。81ページの『エラー・ログ・ストリームをセットアップするためのステップ』を参照してください。ここはブランクでもかまいませんが、その場合、システムはデーモンのログ・ストリームを使用します。
制御領域の proc 名	BBOASR2 (デフォルト)
不許可クライアントの許可	チェック・ボックスにチェックマークを付ける
許可されるユーザー ID のパスワード	チェック・ボックスにチェックマークを付ける
許可されるユーザー ID のパスチケット	チェック・ボックスをクリアする
許可される DCE	チェック・ボックスをクリアする
DCE の保護品質	保護なし
DCE キータブ・ファイル	ブランクのまま
SSL 許可	チェック・ボックスをクリアする
Kerberos の許可	チェック・ボックスをクリアする
セキュリティー優先リスト	パスワードを優先順位 1 に設定
環境変数リスト	環境変数を確認する**

** BBOASR2 サーバー用に以下の環境変数が設定されていることを確認します。current.env をブラウズして、値を検索してください。次に、既存の値をパネルにカット・アンド・ペーストし、必要な場合は、それに追加します。切り取り、コピーおよび貼り付けには、クイック・キー (コピーは

[ctrl]+c、切り取りは [ctrl]+x、貼り付けは [ctrl]+v) を使用してください。これらの機能は、環境変数表のポップアップ・メニューからは利用できません。

- LIBPATH。LIBPATH 変数は、階層ファイル・システム (HFS) 内の Java と JDBC の DLL 検索パスを指定します。システム、WebSphere for z/OS、Java、および JDBC DLL を指定してください。たとえば次のようになります。

  ```
  LIBPATH=/db2_install_path/lib
  :/usr/lpp/java/J1.3/bin
  :/usr/lpp/java/J1.3/bin/classic
  :/usr/lpp/WebSphere/lib
  ```

  ここで、*db2_install_path* は DB2 for OS/390 をインストールした HFS です。

  LIBPATH ステートメントは、全体が 1 行になければなりません。

- CLASSPATH。CLASSPATH ステートメントは、サーバー領域内の Java アプリケーションで使用する Java クラス・ファイルを指定します。CLASSPATH に次の指定があることを確認してください。

  ```
  CLASSPATH=db2_install_path/classes/db2j2classes.zip
  ```

  ここで、*db2_install_path* は DB2 for OS/390 をインストールした HFS です。

  CLASSPATH ステートメントは、全体が **1 行になっていなければなりません**。

  注: この会話を活動化した後、システム管理はユーザーに代わって自動的にアプリケーション・サーバーの CLASSPATH の前に ws390srt.jar、 waswebc.jar、および xerces.jar を付加します。

  手続き型アプリケーション・アダプターを使用する計画の場合は、次のものを CLASSPATH に追加します。

  ```
  /usr/lpp/WebSphere/lib/bboadptr.jar:
  /usr/lpp/WebSphere/lib/bbokeart.jar:
  /usr/lpp/WebSphere/lib/bbokpart.jar
  ```

- JVM_LOGFILE。ログを入手したいファイルに設定します。たとえば次のようになります。

  ```
  /serverdir/jvm.log
  ```

  ここで、*serverdir* は、BBOASR2 の制御およびサーバー領域が書き込みアクセス権を持つディレクトリーです。

- TRACEALL。サーバーのパフォーマンスを向上させるため、TRACEALL 環境変数を必ず 1 に設定してください。
- DB2SQLJPROPERTIES。これは、JDBC のプロパティー・ファイルを指すように設定します。この環境変数の詳細については、*DB2 for OS/390 Application Programming Guide and Reference for Java* を参照してください。

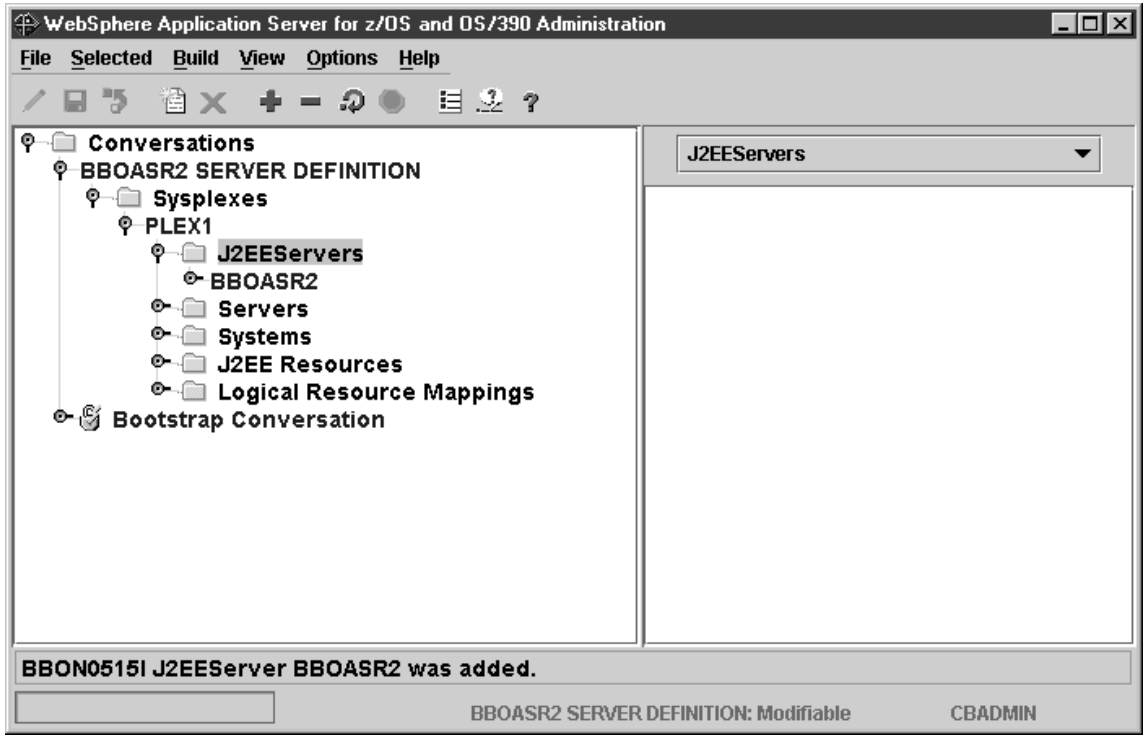
---

5. ディスケットへの保管を表すアイコンをクリックする。ツリーの中に「...J2EE サーバーの追加 (Adding... J2EE servers)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは完了です。

```
BBON0515I J2EEServer BBOASR2 was added.
```

画面は次のようになります。



BBOASR2A サーバー・インスタンスを追加するためのステップ
この作業を始める前に: BBOASR2 サーバーを定義しておく必要があります。

サーバー・インスタンスを追加するには、以下のステップを実行してください。

1. 必要であれば、J2EEServers と BBOASR2 の左側にあるノードをクリックして、ツリーを展開する。

   _____

2. 左マウス・ボタンでサーバー・インスタンスを選択する。次に、右マウス・ボタンを使用して、サーバー・インスタンスをクリックし、「追加 (Add)」を選択する。

   _____

3. 「プロパティー (properties)」フォームで、サーバー・インスタンス名として BBOASR2A を入力する。

   _____

4. オプション: サーバー・インスタンスの説明を入力する。

   _____

5. オプション: ログ・ストリーム名を指定する。指定しなかった場合のデフォルトは、BBOASR2 サーバー用に選択したログ・ストリーム名です。

   _____

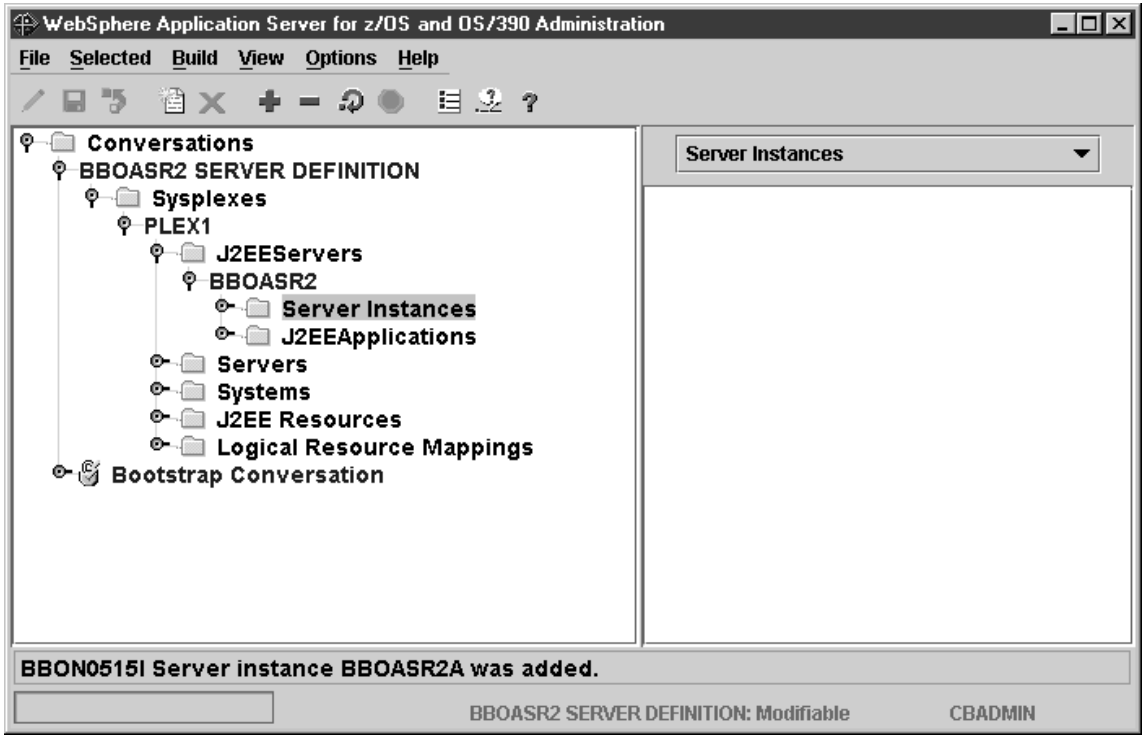
6. ディスケットへの保管を表すアイコンをクリックする。ツリーの中に「...サーバー・インスタンスの追加 (Adding... Server Instances)」が表示されます。

   _____

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Server instance BBOASR2A was added.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR2 SERVER DEFINITION
Sysplexes
PLEX1
J2EEServers
BBOASR2
Server Instances
J2EEApplications
Servers
Systems
J2EE Resources
Logical Resource Mappings
Bootstrap Conversation
Server Instances
BBON0515I Server instance BBOASR2A was added.
BBOASR2 SERVER DEFINITION: Modifiable
CBADMIN

J2EE リソースを追加するためのステップ

この作業を始める前に: 現行会話で作業している必要があります。

J2EE リソースを追加するには、以下のステップを実行します。

1. 左マウス・ボタンで J2EE リソースを選択する。次に、右マウス・ボタンを使用して J2EE リソースをクリックし、「追加 (Add)」を選択する。

   ---

2. 「プロパティー (properties)」フォームで、J2EE リソースの名前を入力する。この例では、『BBOASR2_EJB_IVP_RESOURCE』を使用しています。

   ---

3. オプション: J2EE リソースの説明を入力する。

   ---

4. 「J2EE リソース・タイプ」という名前の特性を見つけ、「DB2 データ・ソース」を選択する。

   管理アプリケーションは、上記の各フィールドに DB2 データ・ソースに適した情報を入力します。

   ---

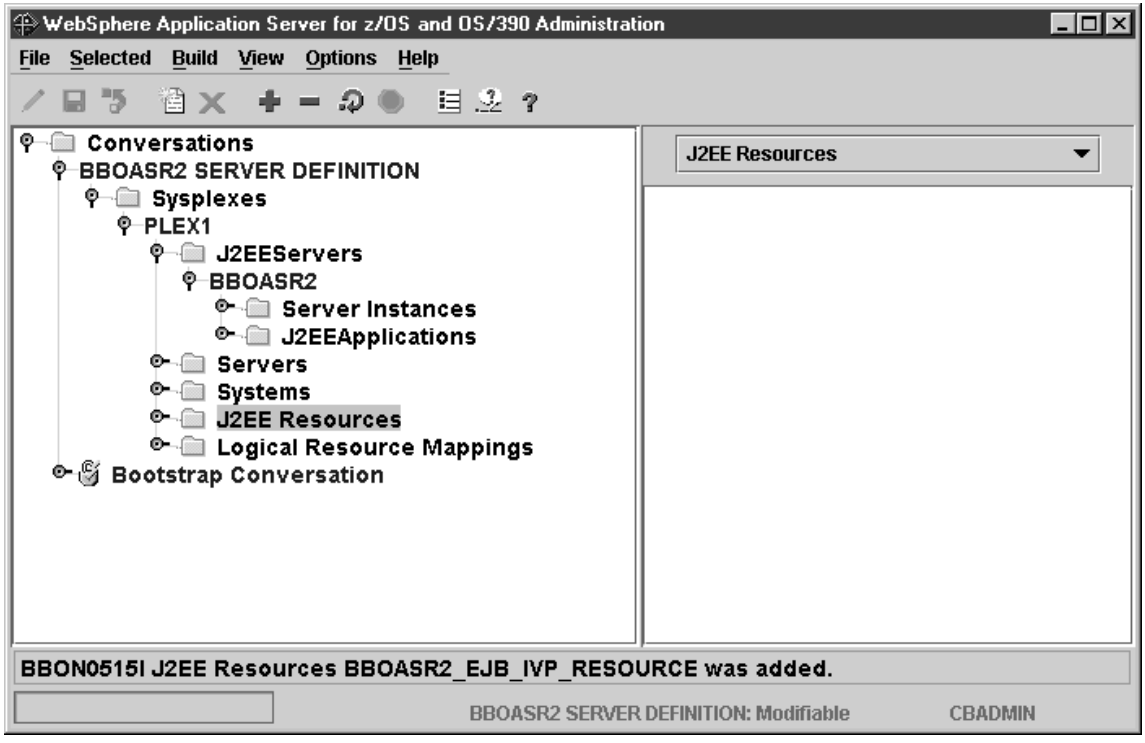
5. ディスケットへの保管を表すアイコンをクリックする。ツリーの中に「...J2EE リソースの追加 (Adding... J2EE resources)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I J2EE Resources name was added.
```

ここで、*name* は J2EE リソース用に選択した名前です。

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR2 SERVER DEFINITION
Sysplexes
PLEX1
J2EEServers
BBOASR2
Server Instances
J2EEApplications
Servers
Systems
J2EE Resources
Logical Resource Mappings
Bootstrap Conversation
J2EE Resources
BBON0515I J2EE Resources BBOASR2_EJB_IVP_RESOURCE was added.
BBOASR2 SERVER DEFINITION: Modifiable
CBADMIN

J2EE リソース・インスタンスを追加するためのステップ

この作業を始める前に: J2EE リソースを定義しなければなりません。

J2EE リソース・インスタンスを追加するには、以下のステップを実行します。

1. 必要であれば、J2EE リソース名の左側にあるノードをクリックして、新規に作成した J2EE リソースのツリーを展開する。

---

2. 左マウス・ボタンで J2EE リソース・インスタンスを選択する。次に、右マウス・ボタンで「J2EE リソース・インスタンス (J2EE Resource Instances)」をクリックし、「追加 (Add)」をクリックする。

---

3. 「プロパティー (properties)」フォームで、次のように適切な値を入力する。
   - J2EE リソース・インスタンス名。**例:** `BBOASR2_EJB_IVP_RESOURCE_system`。ただし、*system* は使用しているシステムの名前です。
   - J2EE リソース・インスタンスの説明 (オプション)。
   - データベース名: DB2 for OS/390 ロケーション名を指定します。

---

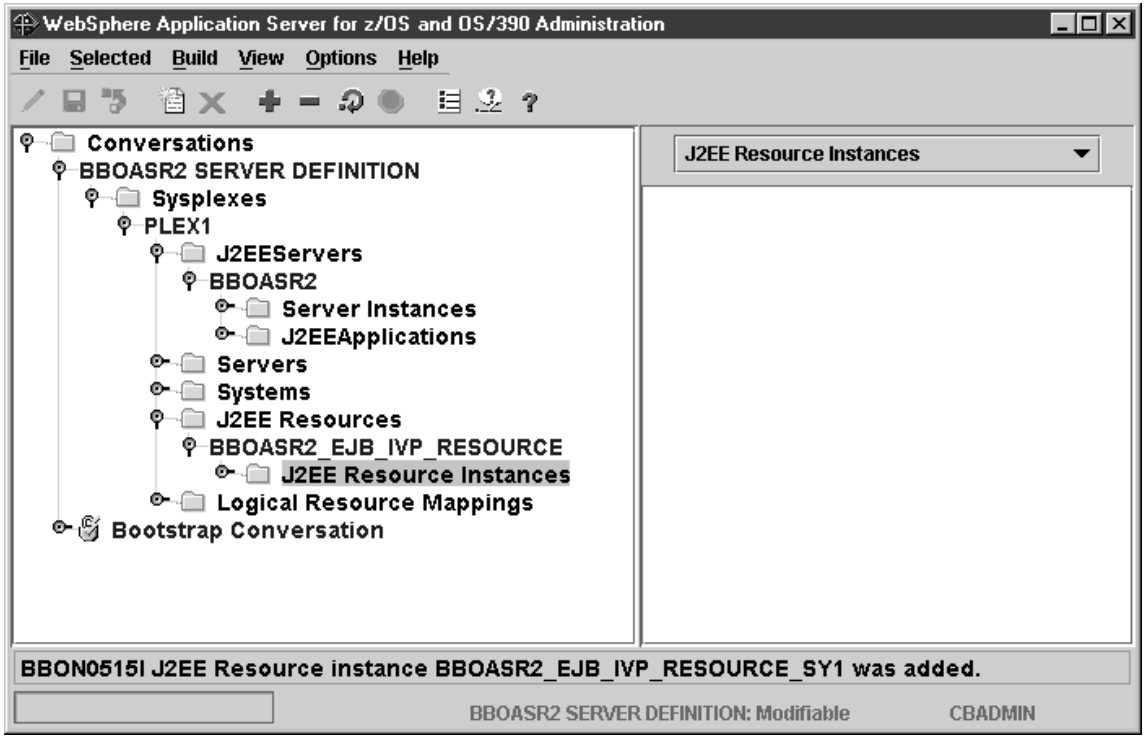
4. ディスケットへの保管を表すアイコンをクリックする。ツリーの中に「...J2EE リソース・インスタンスの追加 (Adding... J2EE resource instances)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I J2EE resource Instance name was added.
```

ここで、*name* は J2EE リソース・インスタンス用に選択した名前です。

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR2 SERVER DEFINITION
Sysplexes
PLEX1
J2EEServers
BBOASR2
Server Instances
J2EEApplications
Servers
Systems
J2EE Resources
BBOASR2_EJB_IVP_RESOURCE
J2EE Resource Instances
Logical Resource Mappings
Bootstrap Conversation
J2EE Resource Instances
BBON0515I J2EE Resource instance BBOASR2_EJB_IVP_RESOURCE_SY1 was added.
BBOASR2 SERVER DEFINITION: Modifiable
CBADMIN

J2EE コンテナーにサーバー・アプリケーションをインストールするためのステップ

この作業を始める前に: 以下の作業が必要です。

- OS/390 または z/OS 上で FTP サーバーが稼働していることを確認する。
- その FTP サーバーが次の一時ディレクトリーに対する書き込みアクセス権を備えていることを確認する。

  targetdir/*sysplex*/temp/*administrator_ID*

  ここで、

  targetdir
  マウント・ポイントです。

  sysplex
  シスプレックスの名前です。

  administrator_ID
  管理者です (通常は CBADMIN)。

- PolicyIVP.ear ファイルを WebSphere for z/OS システムからバイナリーでダウンロードする。このファイルのデフォルトの位置は、次のとおりです。

  /usr/lpp/WebSphere/samples/PolicyIVP/ejb

WebSphere for z/OS 管理アプリケーションを使用してアプリケーション用の EAR ファイルをインストールするには、以下のステップを実行します。

1. ツリーの中で、BBOASR2 サーバーを選択する。

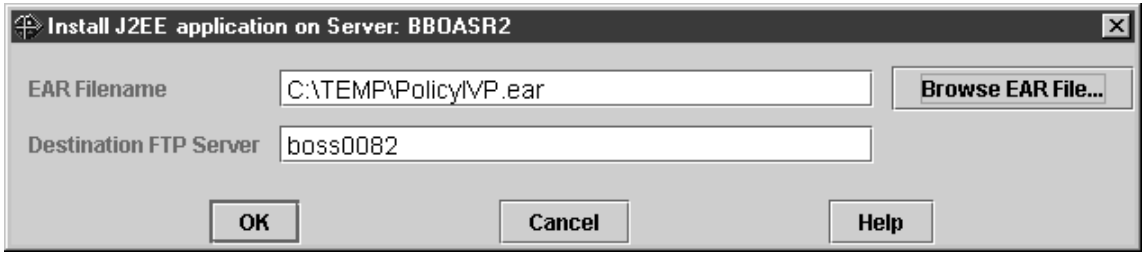
---

2. 「選択 (Selected)」メニュー・バーから「J2EE アプリケーションのインストール... (Install J2EE Application...)」を選択する。「J2EE アプリケーションのインストール (Install J2EE Application)」ダイアログ・ボックスが表示されます。

---

3. ダイアログ・ボックスに次の値を入力する。
   - J2EE アプリケーションが入っている EAR ファイルの名前。「参照 (Browse)」ボタンを使用して、ワークステーション・ファイル・システム内を PolicyIVP.ear ファイルまでナビゲートしてください。
   - アプリケーションをインストールしたいシスプレックスの FTP サーバーの名前。通常、これはログオンしたシステムの IP 名です (これは、デフォルトとして表示されます)。

例:



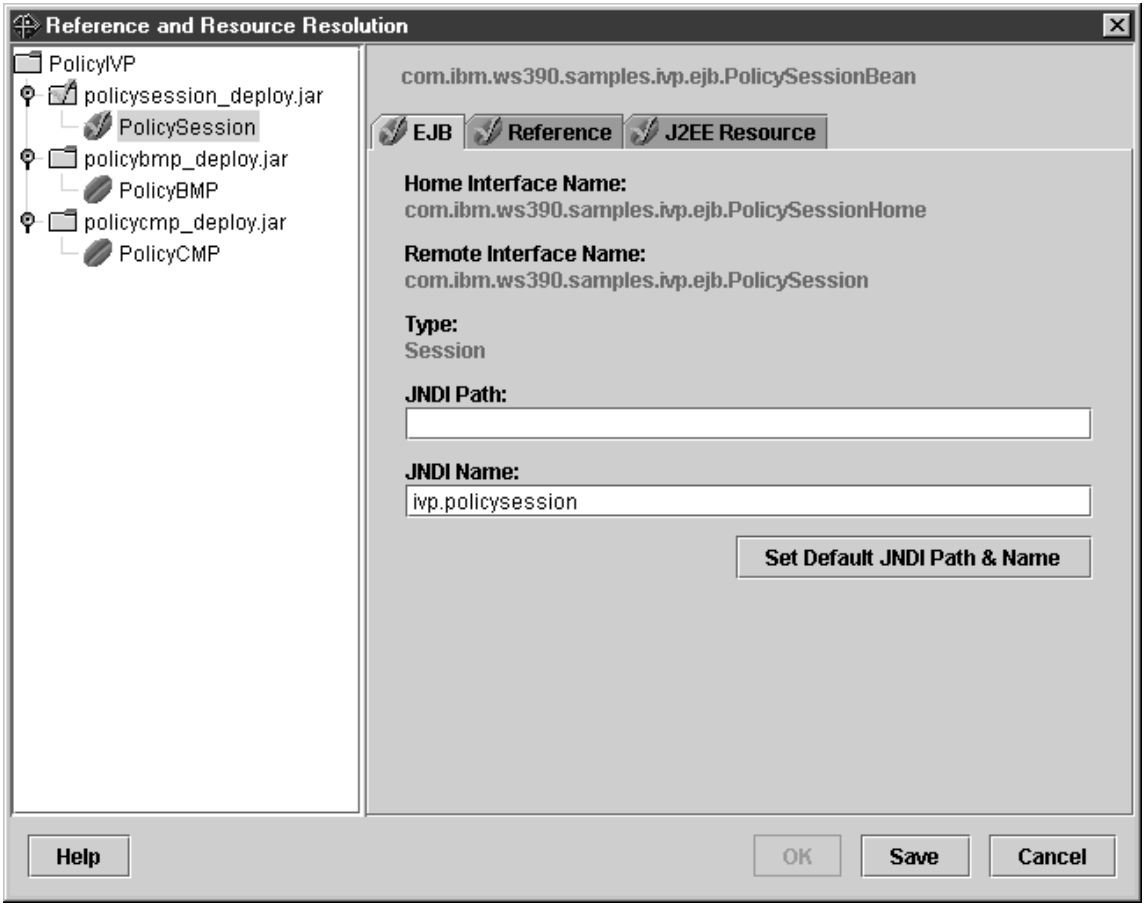
「OK」をクリックする。**結果:** 『Loading ear file』というポップアップが表示された後、「参照とリソースの解決 (Reference and Resource Resolution)」ウィンドウが表示され、ear ファイル内のアプリケーション・コンテンツが表示されます。

---

4. 「参照とリソースの解決 (Reference and Resource Resolution)」ウィンドウにリストされた各フォルダーを展開する。次に、それぞれの bean について、次の操作を行います。
   a. bean 名をクリックして、その bean の詳細をウィンドウの右側に表示する。
   b. 「EJB」タブをクリックし、「JNDI パス (JNDI Path)」の値を消去する。
   c. 次の表に従って、bean の「JNDI 名 (JNDI Name)」を入力する。

bean	入力する JNDI 名
PolicySessionBean	ivp.policysession
PolicyBMPBean	ivp.policybmp
PolicyCMPBean	ivp.policycmp

例:



結果: bean 名の左側にある bean シンボルの上にチェックマークが付いた時点で、このプロセスは完了です。すべての bean について JNDI 選択プロセスが完了すると、「OK」ボタンが選択可能になります。

ヒント: 「参照とリソースの解決 (Reference and Resource Resolution)」ウィンドウのデータは、配置のためにサーバーへ転送される前に、*application_name*_resolved.ear という名前の新しい ear ファイルのコピーに保管されます。このファイル・コピーを後で再オープンすれば、情報を再度入力する必要はありません。

5. 「参照 (Reference)」と「リソース (Resource)」のタブはそのままにする。

6. すべての bean の左側にチェックマークが付いたら、「OK」をクリックする。**結果:** このアクションによって、EAR ファイルの内容のワークステーションから OS/390 または z/OS への自動 FTP 転送が開始されます。ポップアップが表示され、そこに FTP 転送のステージを記述したメッセージが表示されます。たとえば次のようになります。

その後、ツリーの中に「Deploying... BBOASR2」が表示されます。

FTP 転送は、以下のステージに従います。

ステージ	説明
1	ear ファイルをインポートするとき、システムはこのファイルを次の位置へ FTP します。 *targetdir*/*sysplex*/temp/*administrator_ID*/PolicyIVP.ear *targetdir* はマウント・ポイント、*sysplex* はシスプレックスの名前、および *administrator_ID* は管理者のユーザー ID (通常は CBADMIN) です。
2	ear ファイルが、次の位置へコピーされます。 *targetdir*/apps/BBOASR2/L*n*/PolicyIVP.ear *n* はレベル番号です。
3	ear ファイルが処理されます。ear ファイルの処理のとき、ear ファイルは次のディレクトリーへ展開されます。 *targetdir*/apps/BBOASR2/L*n*/*app_name*/ *app_name* は、アプリケーションの名前です (必ずしも ear ファイル名に等しくはなりません)。

ステージ	説明
4	足場となるディレクトリーの *targetdir*/apps/BBOASR2/L*n*/A/ が作成され、この下にすべての配置情報が格納されます。

注: 会話の活動化と同時に、

targetdir/apps/BBOASR2/L*n*/

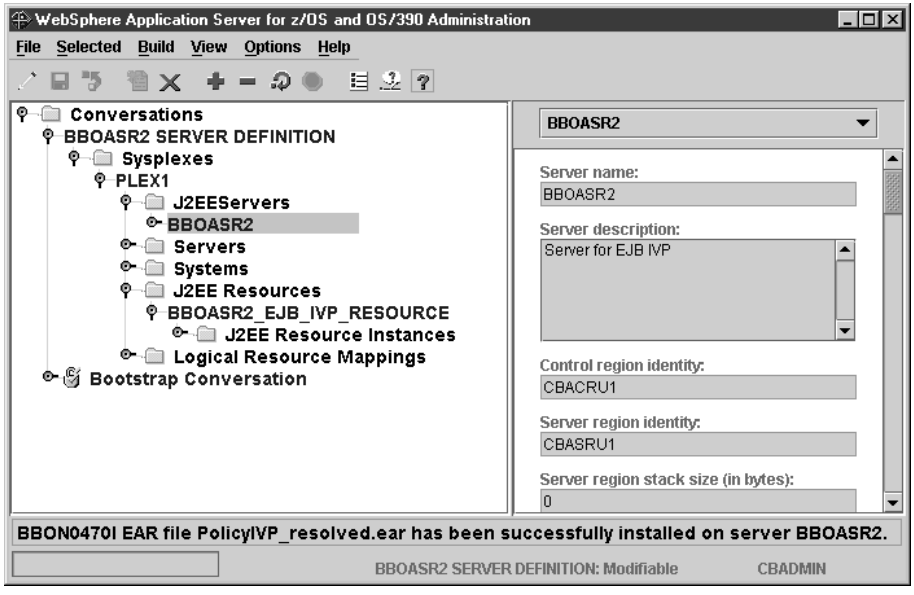
の下にあるすべてのものが、1 レベル上の次のディレクトリーまで移動します。

targetdir/apps/BBOASR2/

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0470I EAR file PolicyIVP_resolved.ear has been successfully installed on server BBOASR2.
```

IVP のインストールが正常に完了した場合、画面は次のようになります。



会話の妥当性検査をするためのステップ

この作業を始める前に: 現行会話のこれまでのステップを、すべて完了していなければなりません。

会話の妥当性を検査するには、以下のステップを実行します。

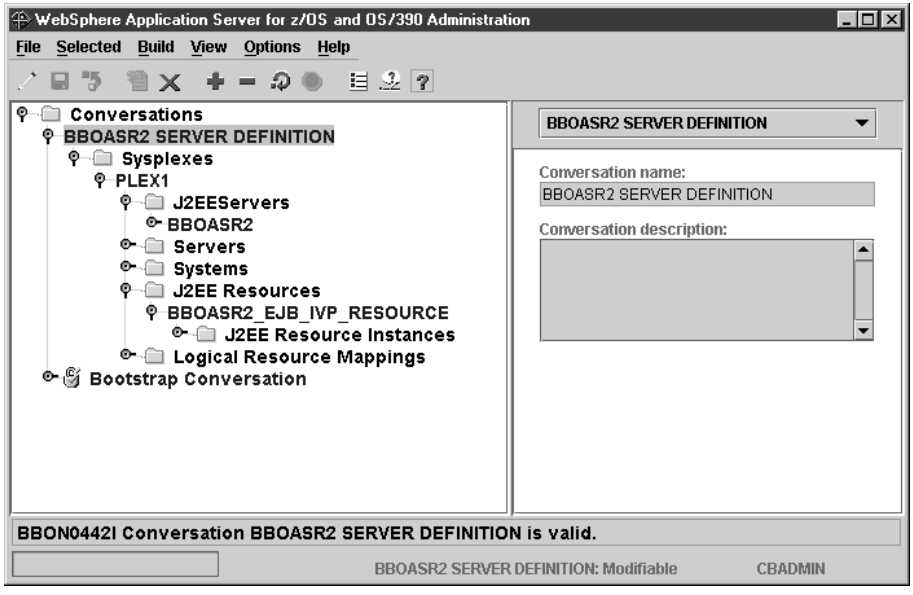
1. 必要であれば、ツリーを BBOASR2 SERVER DEFINITION 会話名までスクロールアップする。

   ---

2. 左マウス・ボタンで会話を選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「検査 (Validate)」を選択する。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0442I Conversation BBOASR2 SERVER DEFINITION is valid.
```



会話をコミットするためのステップ
この作業を始める前に: 現行会話の妥当性検査をしなければなりません。

⇔ 左マウス・ボタンで会話を選択します。次に、右マウス・ボタンを使用してその会話をクリックし、「コミット (Commit)」を選択します。以下の質問に「はい (Yes)」と答えてください。

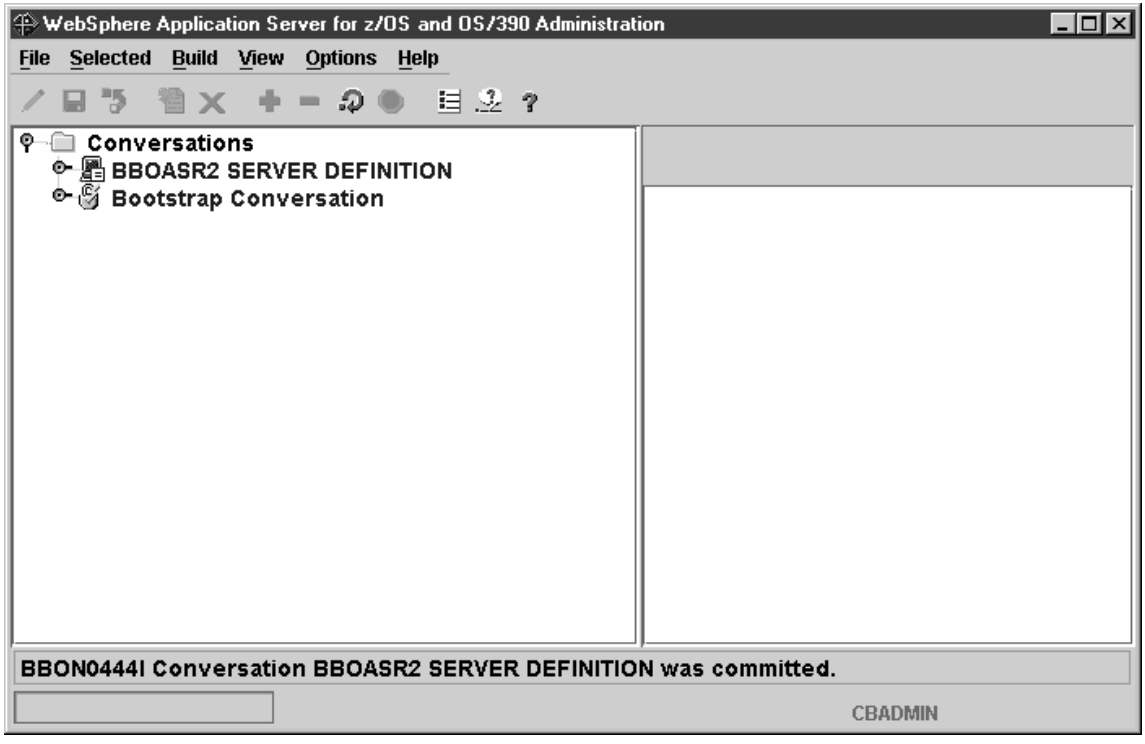
```
BBON0534I You cannot undo Commit.  Do you still want to commit?
```

ツリーの中に、「...BBOASR2 SERVER DEFINITION のコミット (Committing... BBOASR2 SERVER DEFINITION)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0444I Conversation BBOASR2 SERVER DEFINITION was committed.
```

画面は次のようになります。



OS/390 または z/OS タスクを完了する指示に従うためのステップ

この作業を始める前に: 現行会話の妥当性検査およびコミットを行わなければなりません。

OS/390 または z/OS タスクを完了する指示に従うには、以下のステップを実行してください。

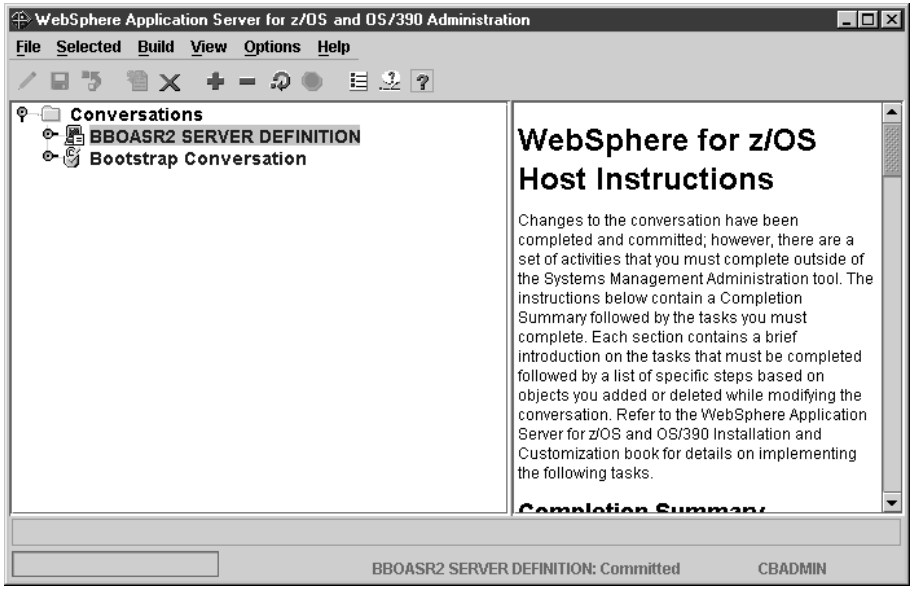
1. BBOASR2 SERVER DEFINITION 会話を左マウス・ボタンで選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「指示 (Instructions) 」を選択する。

   ---

2. 管理アプリケーションが提供する、OS/390 または z/OS タスクを完了するための指示をすべて完了する。

必要な OS/390 または z/OS タスクがすべて完了すれば、このステップは終了したことになります。

画面は次のようになります。



すべてのタスクの完了をマークするためのステップ

この作業を始める前に: 必要な OS/390 または z/OS タスクをすべて完了していなければなりません。

すべてのタスクの完了をマークするには、以下のステップを実行してください。

1. BBOASR2 SERVER DEFINITION 会話を左マウス・ボタンで選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「完了 (Complete)」に続いて「すべてのタスク (All tasks)」を選択する。

   ---

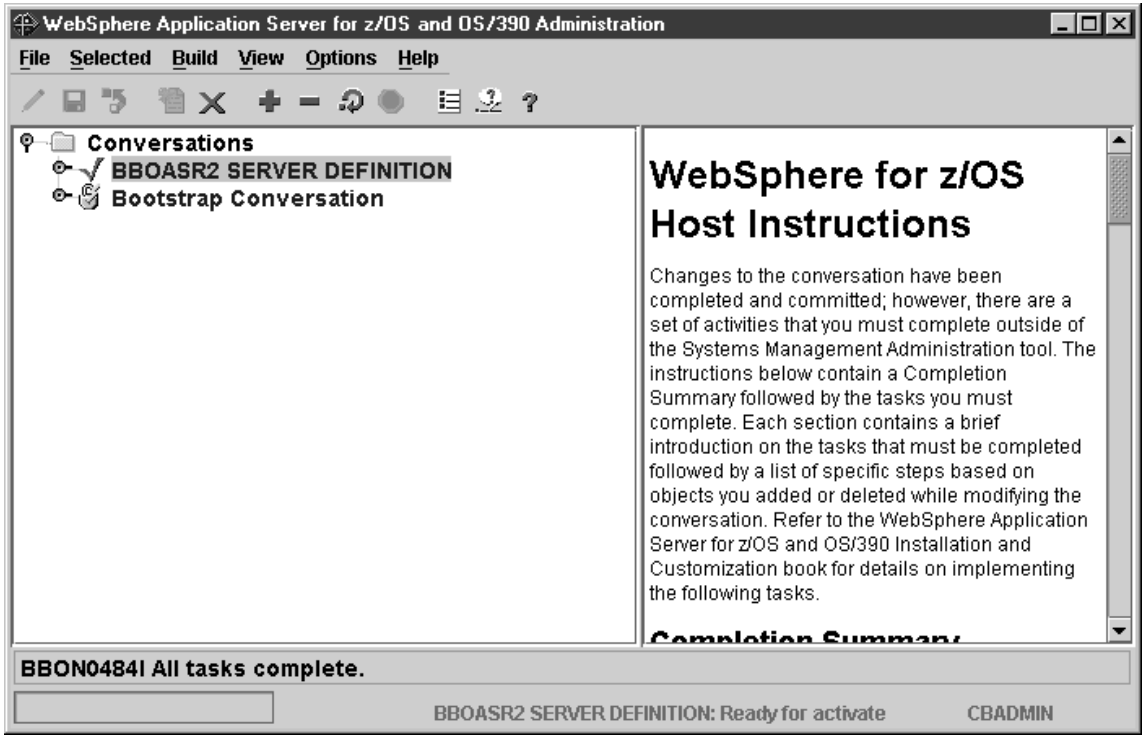
2. 以下の質問に「はい (Yes)」と答える。

   ```
   BBON0550I  Are you sure that all tasks have been completed?
   ```

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0484I All tasks complete.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
WebSphere for z/OS Host Instructions
Changes to the conversation have been completed and committed; however, there are a set of activities that you must complete outside of the Systems Management Administration tool. The instructions below contain a Completion Summary followed by the tasks you must complete. Each section contains a brief introduction on the tasks that must be completed followed by a list of specific steps based on objects you added or deleted while modifying the conversation. Refer to the WebSphere Application Server for z/OS and OS/390 Installation and Customization book for details on implementing the following tasks.
BBON0484I All tasks complete.
BBOASR2 SERVER DEFINITION: Ready for activate
CBADMIN

新しい会話を活動化するためのステップ

この作業を始める前に: この節でこれまで述べてきた指示をすべて完了していなければなりません。

新規会話を活動化するには、以下のステップを実行してください。

1. BBOASR2 SERVER DEFINITION 会話を左マウス・ボタンで選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「活動化 (Activate)」を選択する。

---

2. 以下の質問に「はい (Yes)」と答える。

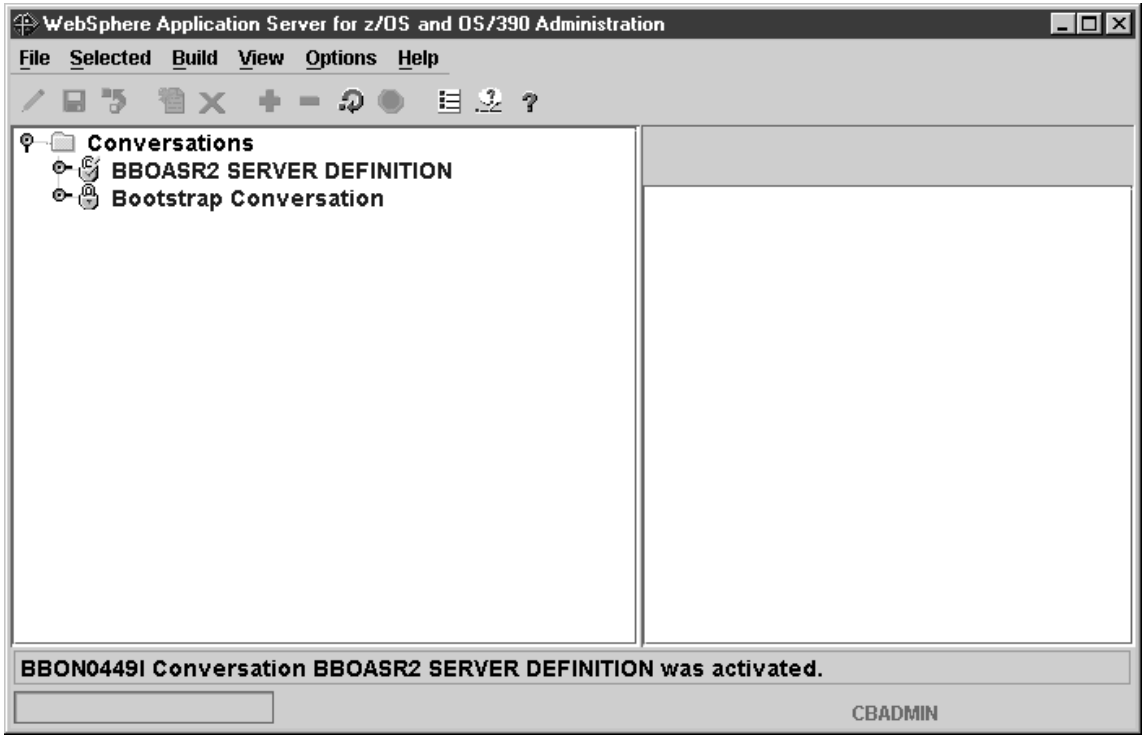
   ```
   BBON0539I  Activate cannot undone.  Do you want to activate conversation
              BBOASR2 SERVER DEFINITION?
   ```

   結果: ツリーの中に、「...BBOASR2 SERVER DEFINITION の活動化 (Activating... BBOASR2 SERVER DEFINITION)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0449I Conversation BBOASR2 SERVER DEFINITION was activated.
```

画面は次のようになります。

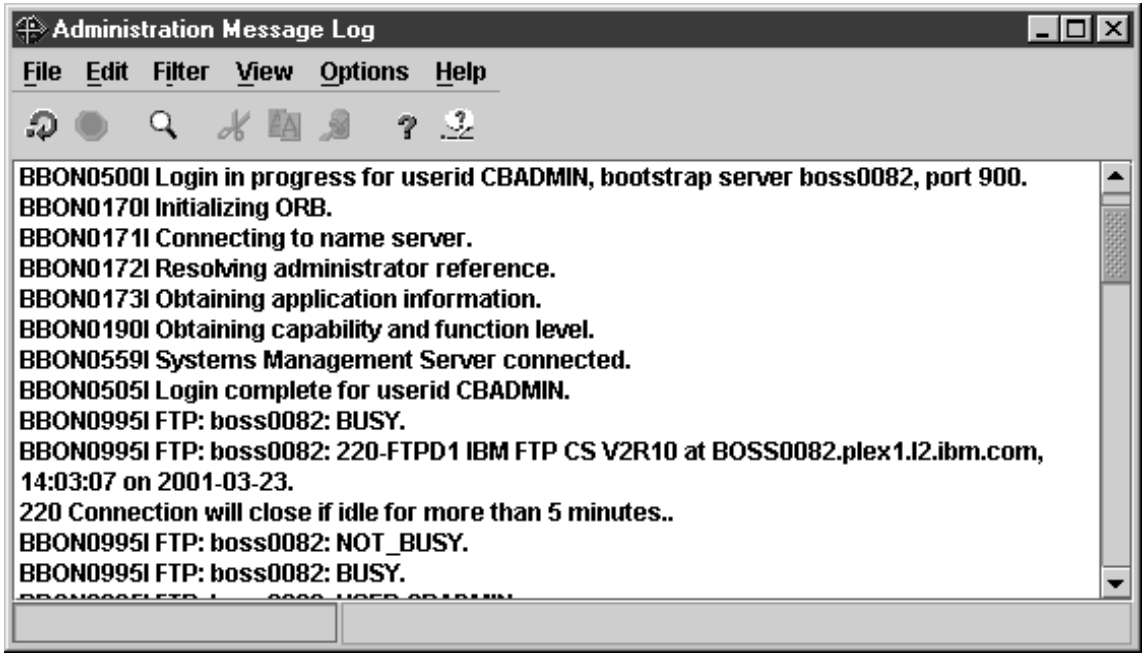

WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
BBON0449I Conversation BBOASR2 SERVER DEFINITION was activated.
CBADMIN

管理メッセージ・ログを印刷するためのステップ
この作業を始める前に: 会話を活動化しなければなりません。

管理メッセージ・ログを印刷するには、次のステップに従ってください。

1. 「ファイル (File)」、続いて「メッセージ・ログ... (Message log...)」をクリックする。

   結果: 画面は次のようになります。



---

2. 「管理メッセージ・ログ (Administration Message Log)」ウィンドウから、「ファイル (File)」をクリックし、次に「印刷 (Print)...」をクリックする。

結果: Windows の印刷ダイアログが表示されます。プリンターを選択して「OK」をクリックします。次のポップアップが表示されます。

管理メッセージ・ログの印刷出力が取得されれば、このステップは終了したことになります。プログラムを終了してかまいません。

BBOASR2 サーバーの定義が完了しました。

MOFW IVP を実行したい場合は、149ページの『BBOASR1 MOFW サーバーの定義』へ進んでください。それ以外の場合は、191ページの『インストール検査プログラム (IVP) 用のデータベースを作成するためのステップ』へ進んでください。

BBOASR1 MOFW サーバーの定義

MOFW コンポーネントの使用を計画している場合は、この節に述べるステップを実行して BBOASR1 をセットアップしてください。BBOASR1 は、IVP が MOFW コンポーネント・サポートをテストするために使用する MOFW サーバーです。

管理アプリケーションを開始するためのステップ

この作業を始める前に: WebSphere for z/OS ランタイム・サーバー・インスタンスを初期化し、管理アプリケーションをインストールしておかなければなりません。

管理アプリケーションを開始するには、以下のステップを実行してください。

1. ワークステーションで、「スタート」、「プログラム」、「IBM WebSphere for z/OS Administration」を順にクリックする。

   ---

2. ダイアログにブートストラップ・サーバー IP 名、ポート 900、ユーザー ID cbadmin およびパスワードを入力する (パスワードについては、RACF のサンプル BBOCBRAC を参照)。「OK」をクリックする。

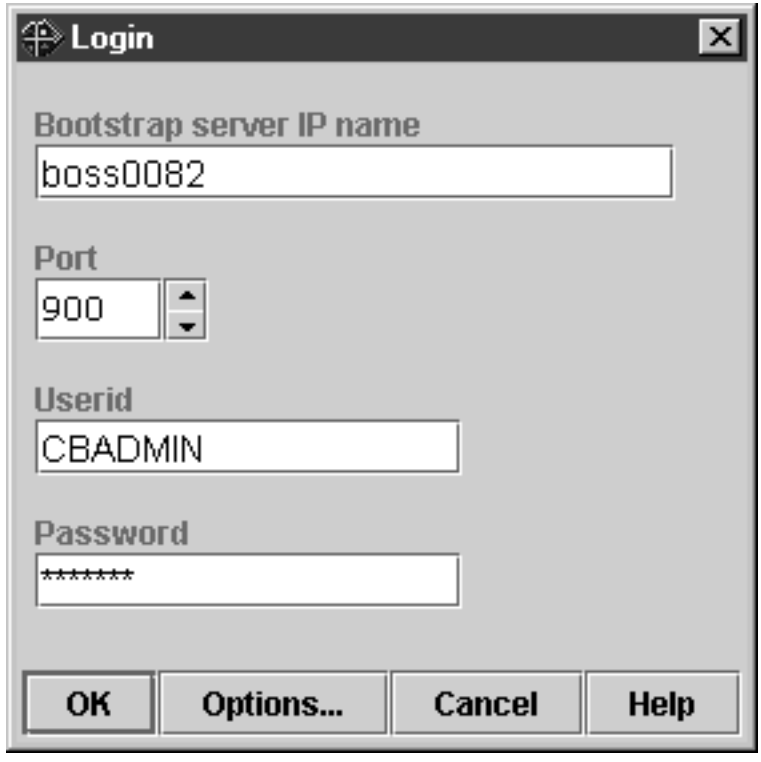
   推奨:

   a. 単一のワークステーションからであれ、複数のワークステーションからであれ、同じ管理者 ID を使用して、アプリケーションの複数並行セッションにログオン**しない**ことを強くお勧めします。たとえば、ユーザー ID に CBADMIN を使用して、ワークステーションで 管理アプリケーションを開始する場合、そのワークステーションからでも別のワークステーションからでも、CBADMIN を使用して別のセッションを開始することはできません。

   b. 複数の管理者ユーザー ID を定義した場合、それらすべてが同時にログオンできますが、会話の更新および活動化を行うのは、一度に **1 つだけ** にしてください。

      複数の管理者が会話を活動化しようとした場合には、予期しない結果が生じます。ある管理者が新規の会話を開始すると、現在活動状態にある会話のコピーがベース・レベルとして使用されます。複数の管理者が、現在活動状態にある同じ会話に基づいて新規会話を作成した場合は、最初に活動化を行った管理者が成功します。その他の活動化を試みたすべての管理者は、それらの管理者による変更が現在活動状態にある会話に基づくものではないので (現在活動状態の会話は、それらの管理者の下にあったものから変化してしまったため)、活動化に失敗します。2 番目以降の管理者は、新しい現行会話を使用して、やり直さなければなりま

せん。これは、変更の量によっては大きな混乱を起こします。このため、ある管理者が会話を更新して活動化しようとしている間、それ以外の管理者は、読み取りまたは表示機能に限定して管理アプリケーションを使用しなければなりません。



メインウィンドウにブートストラップの会話が表示されれば、このステップは終了したことになります。接続にトラブルがある場合は、ヘルプ・システムまたは *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 で、詳しい情報を入手してください。

新しい会話を開始するためのステップ

この作業を始める前に: ログインして管理アプリケーションを開始しなければなりません。

新規会話を開始するには、以下のステップを実行してください。

1. 左マウス・ボタンで会話 (Conversations) フォルダーを選択する。次に、右マウス・ボタンを使用して、会話 (Conversations) フォルダーをクリックし、「追加 (Add)」を選択する。

   ---

2. 「プロパティー (properties)」フォーム (右側のパネル) で、新規会話に名前を付ける。たとえば、ここではこの会話に「BBOASR1 (BBOASR1 Server Definition)」という名前を付けました。説明も加えてください (オプション)。

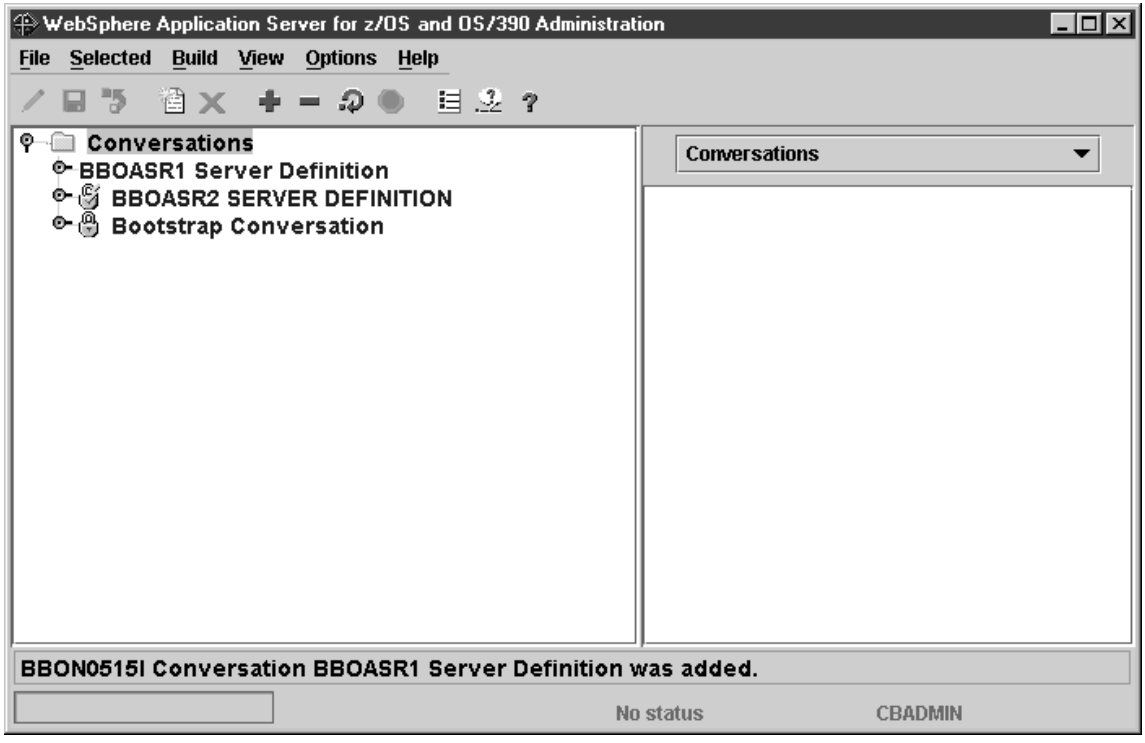
   ---

3. ディスケットへの保管を表すアイコンをクリックする。「... 会話の追加 (Adding... Conversations)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Conversation BBOASR1 Server Definition was added.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR1 Server Definition
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
Conversations
BBON0515I Conversation BBOASR1 Server Definition was added.
No status
CBADMIN

BBOASR1 MOFW サーバーを追加するためのステップ

この作業を始める前に: 現行会話で作業している必要があります。

BBOASR1 サーバーを追加するには、以下のステップを実行してください。

1. 必要であれば、会話名の左側にあるノードをクリックして、新しい会話ツリーを展開する。

   _____

2. シスプレックスを展開し、次にユーザーのシスプレックスを展開する。

   _____

3. 左マウス・ボタンでサーバー (Servers) フォルダーを選択する。次に、右マウス・ボタンを使用して、サーバー (Servers) フォルダーをクリックし、「追加 (Add)」を選択する。

   _____

4. 「プロパティー (properties)」フォームで、以下のとおり値を入力するか選択する。

サーバー名	BBOASR1
サーバーの説明	オプション・サーバーの説明
制御領域識別	制御領域が動作するユーザー ID。これは RACF STARTED クラスの項目と一致し、制御領域用の適切な RACF 権限を有していなければなりません。BBOCBRAC のデフォルト値は CBACRU1 です。
サーバー領域識別	サーバー領域が動作するユーザー ID。これは RACF STARTED クラスの項目と一致し、サーバー領域用の適切な RACF 権限を有していなければなりません。BBOCBRAC のデフォルト値は CBASRU1 です。
サーバー領域のスタック・サイズ (バイト)	0
運用サーバー	チェック・ボックスにチェックマークを付ける
許可されるデバッガー	チェックなしのまま
分離ポリシー	サーバー領域ごとに複数のトランザクション
レプリカ生成ポリシー	サーバーごとに 1 つ
サーバー領域には JVM が必要	チェック・ボックスをクリアする
サーバー領域の JVM 名	ブランクのまま
ローカル識別	CBGUEST
リモート識別	CBGUEST

登録トランザクション・ファクトリー	チェック・ボックスのクリア *

* トランザクション・ファクトリーとして登録するサーバーは、いつでも使用可能でなければなりません。BBOASR1 はインストール検査の間だけ使用可能なので、このサーバーを、トランザクション・ファクトリーとして登録することはできません。

ネーミング・サーバーは、トランザクション・ファクトリーとして定義されています。ネーミング・サーバーを構成から除去する場合は、トランザクション・ファクトリーに別のサーバーを作成する必要があります。複数のトランザクション・ファクトリーを持つこともできますが、そのようなサーバーは、常に使用可能でなければならないことを覚えておく必要があります。

サーバー領域ガーベッジ・コレクションの許可	チェック・ボックスにチェックマークを付ける
ガーベッジ・コレクション・インターバル	50000
ログ・ストリーム名	エラー情報を取り込むためにセットアップするログ・ストリームの名前。81ページの『エラー・ログ・ストリームをセットアップするためのステップ』を参照してください。ここはブランクでもかまいませんが、その場合、システムはデーモンのログ・ストリームを使用します。
制御領域の開始プロシージャー名	BBOASR1 (デフォルト)
不許可クライアントの許可	チェック・ボックスにチェックマークを付ける
許可されるユーザー ID のパスワード	チェック・ボックスにチェックマークを付ける
許可されるユーザー ID のパスチケット	チェック・ボックスのクリア
許可される DCE	チェック・ボックスのクリア
DCE の保護品質	保護なし
DCE キータブ・ファイル	ブランクのまま
SSL 許可	チェック・ボックスのクリア
Kerberos の許可	チェック・ボックスのクリア
セキュリティー優先リスト	パスワードを優先順位 1 に設定
サーバー活動 SMF レコードの書き込み	サーバー活動レコードを収集したい場合は、チェック・ボックスにチェックマークを付ける。
コンテナー活動 SMF レコードの書き込み	コンテナー活動レコードを収集したい場合は、チェック・ボックスにチェックマークを付ける。

サーバー・インターバル SMF レコードの書き込み	サーバー・インターバル・レコードを収集したい場合は、チェック・ボックスにチェックマークを付ける。
コンテナー・インターバル SMF レコードの書き込み	コンテナー・インターバル・レコードを収集したい場合は、チェック・ボックスにチェックマークを付ける。
SMF インターバル長	SMF の記録間隔の長さを設定する。「サーバー・インターバル SMF レコードの書き込み」または「コンテナー・インターバル SMF レコードの書き込み」を指定したときに有効です。デフォルトのインターバルは 1 時間です。このインターバルは、15 〜 86400 秒 (24 時間) に設定できます。この値を 0 に設定すると、SMFPRMxx parmlib メンバーの INTERVAL ステートメントに入っている値が使用されます。SMFPRMxx に INTERVAL ステートメントがない場合のデフォルトのインターバルは 30 分です。
環境変数リスト	環境変数を確認する **

** BBOASR1 サーバー用に以下の環境変数が設定されていることを確認します。current.env をブラウズして、値を検索してください。次に、既存の値をパネルにカット・アンド・ペーストし、必要な場合は、それに追加します。切り取り、コピーおよび貼り付けには、クイック・キー (コピーは [ctrl]+c、切り取りは [ctrl]+x、貼り付けは [ctrl]+v) を使用してください。これらの機能は、環境変数表のポップアップ・メニューからは利用できません。

- LIBPATH:

  ```
  /usr/lpp/java/IBM/J1.3/bin:/usr/lpp/java/IBM/J1.3/bin/classic:/usr/lpp/WebSphere/lib
  ```

- CLASSPATH には次のファイルが含まれています。
  - *path*/bboplsj.jar。
  - *path*/bboplc.jar。この 2 つのファイルのデフォルト・パスは、`/usr/lpp/WebSphere/samples/PolicyIVP/PRODUCTION` です。

  注: この会話を活動化した後、システム管理はユーザーに代わって自動的にアプリケーション・サーバーの CLASSPATH の前に ws390srt.jar、waswebc.jar、および xerces.jar を付加します。
- JAVA_COMPILER。JAVA_COMPILER を指定する必要はありません。その場合、デフォルトは `JITC` です。あるいは次のようにコード化することもできます。

  ```
  jitc
  ```

- JVM_LOGFILE。ログを入手したいファイルに設定します。たとえば次のようになります。

  /*serverdir*/jvm.log

  ここで、*serverdir* は、BBOASR1 の制御およびサーバー領域が書き込みアクセス権を持つディレクトリーです。
- PATH。JDK の bin ディレクトリーを組み込むように設定します。

  一部のお客様は、IVP の実行可能ファイル (bbopls、bboplsj、および bboplc の DLL) を HFS の中へ移動しています。その場合は、それらのファイルが入っているディレクトリーを PATH の**先頭**に追加してください。

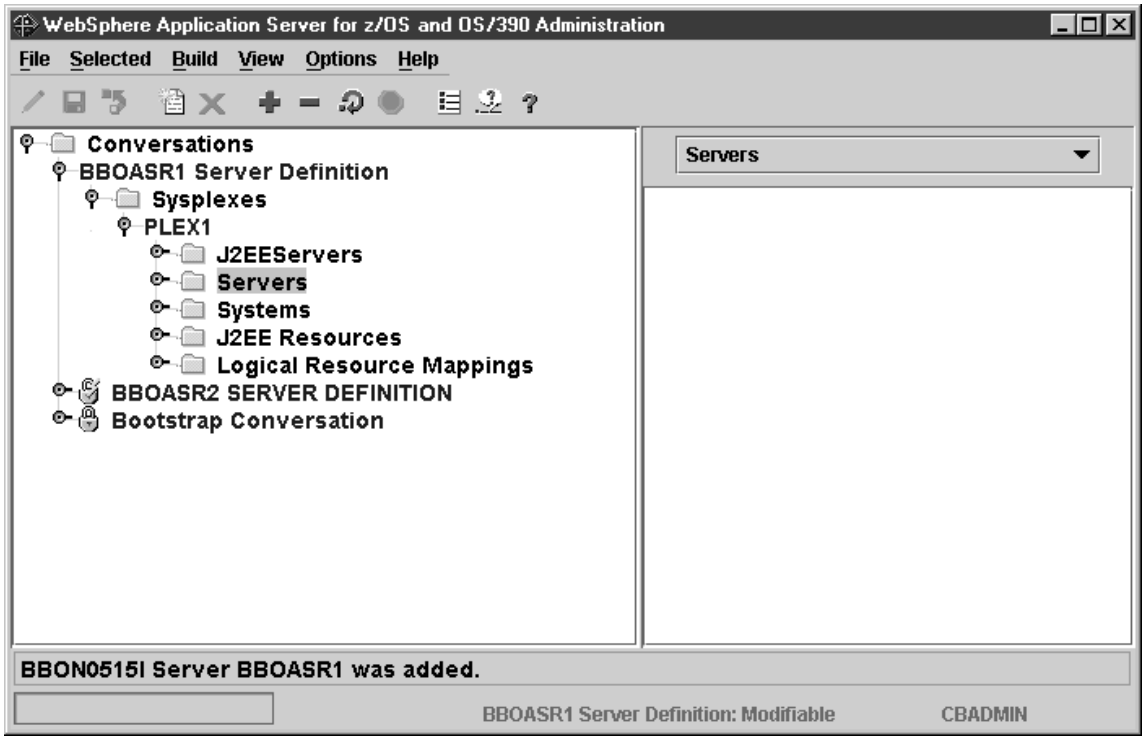
---

5. ディスケットへの保管を表すアイコンをクリックする。「... サーバーの追加 (Adding... Servers)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Server BBOASR1 was added.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR1 Server Definition
Sysplexes
PLEX1
J2EEServers
Servers
Systems
J2EE Resources
Logical Resource Mappings
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
Servers
BBON0515I Server BBOASR1 was added.
BBOASR1 Server Definition: Modifiable
CBADMIN

BBOASR1A サーバー・インスタンスを追加するためのステップ

この作業を始める前に: BBOASR1 サーバーの定義を行わなければなりません。

BBOASR1A サーバー・インスタンスを追加するには、以下のステップを実行してください。

1. フォルダー・アイコンの左側にあるノードをクリックして、サーバー (Servers) フォルダーと BBOASR1 フォルダーを展開する。

   ---

2. 左マウス・ボタンでサーバー・インスタンスを選択する。次に、右マウス・ボタンを使用して、サーバー・インスタンスをクリックし、「追加 (Add)」を選択する。

   ---

3. 「プロパティー (properties)」フォームで、サーバー・インスタンス名として BBOASR1A を入力する。

   ---

4. オプション: サーバー・インスタンスの説明を入力する。

   ---

5. (オプション) ログ・ストリーム名を提供し、LOGSTREAMNAME 環境変数を更新する。そうしない場合、デフォルトは、BBOASR1 サーバーで選択したログ・ストリーム名です。

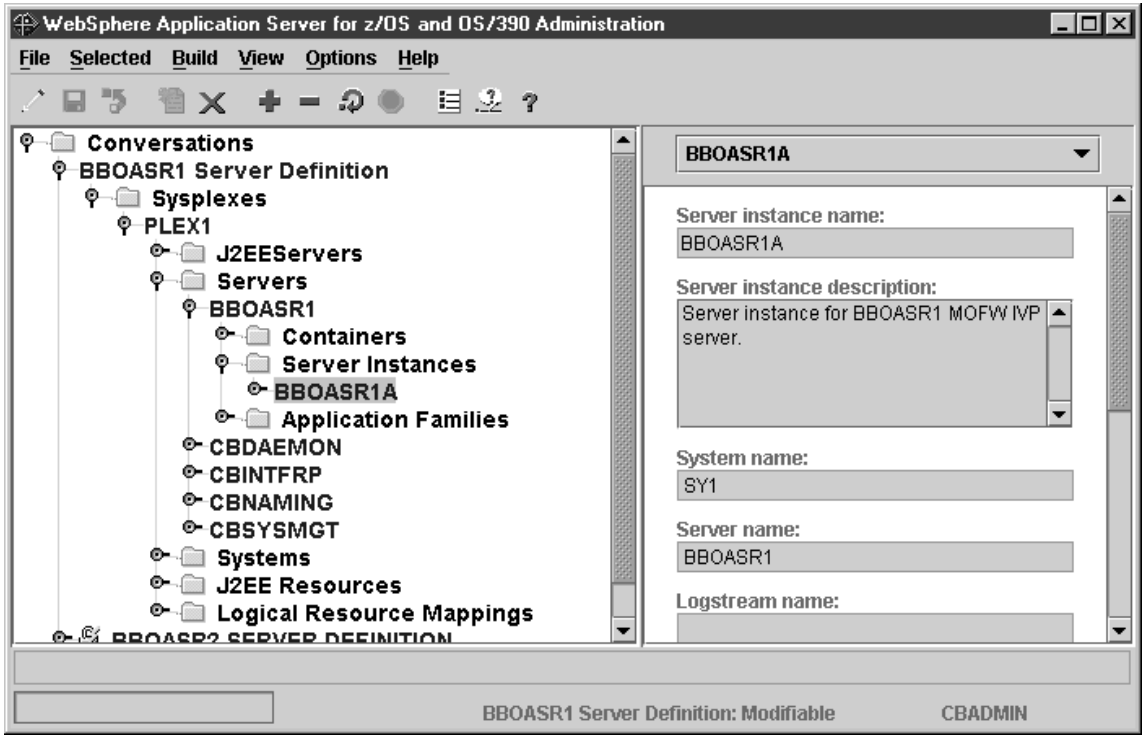
   ---

6. ディスケットへの保管を表すアイコンをクリックする。「... サーバー・インスタンスの追加 (Adding... Server Instance)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Server instance BBOASR1A was added.
```

この手順の最後に、ツリーでサーバー・インスタンスを展開し、BBOASR1A を選択すると、次のような画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR1 Server Definition
Sysplexes
PLEX1
J2EEServers
Servers
BBOASR1
Containers
Server Instances
BBOASR1A
Application Families
CBDAEMON
CBINTFRP
CBNAMING
CBSYSMGT
Systems
J2EE Resources
Logical Resource Mappings
BBOASR1A
Server instance name:
BBOASR1A
Server instance description:
Server instance for BBOASR1 MOFW IVP server.
System name:
SY1
Server name:
BBOASR1
Logstream name:
BBOASR1 Server Definition: Modifiable
CBADMIN

論理リソース・マッピングを追加するためのステップ
この作業を始める前に: 現行会話で作業している必要があります。

論理リソース・マッピングを追加するには、以下のステップを実行してください。

1. 左マウス・ボタンで「論理リソース・マッピング (Logical Resource Mappings)」を選択する。次に、右マウス・ボタンを使用して「論理リソース・マッピング (Logical Resource Mappings)」をクリックし、「追加 (Add)」を選択する。

   ---

2. 「プロパティー (properties)」フォームで、論理リソース・マッピング名として CB_OS/390_IVP_DB2 を入力する。

   ---

3. (オプション) 論理リソース・マッピングの説明を入力する。

   ---

4. 「プロパティー (properties)」フォームを LRM サブシステム・タイプまでスクロールし、DB2 を選択する。

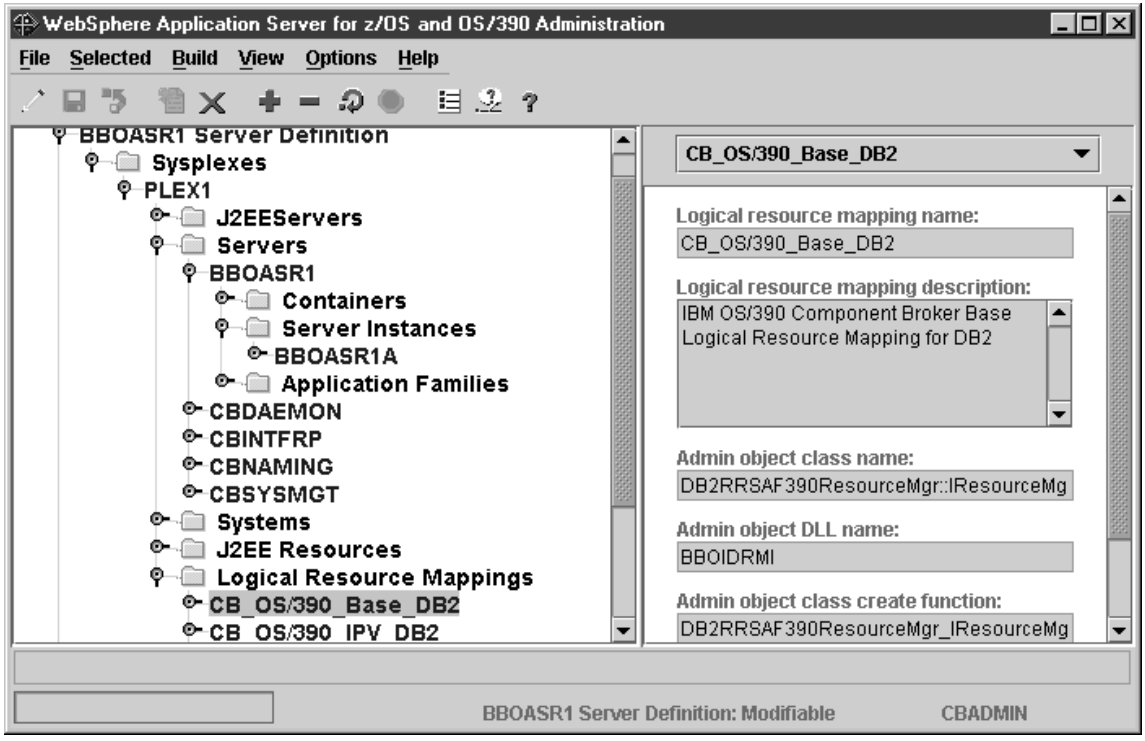
   ---

5. ディスケットへの保管を表すアイコンをクリックする。「... 論理リソース・マッピングの追加 (Adding... Logical Resource Mappings)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Logical resource mapping CB_OS/390_IVP_DB2  was added.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
BBOASR1 Server Definition
Sysplexes
PLEX1
J2EEServers
Servers
BBOASR1
Containers
Server Instances
BBOASR1A
Application Families
CBDAEMON
CBINTFRP
CBNAMING
CBSYSMGT
Systems
J2EE Resources
Logical Resource Mappings
CB_OS/390_Base_DB2
CB_OS/390_IPV_DB2
CB_OS/390_Base_DB2
Logical resource mapping name:
CB_OS/390_Base_DB2
Logical resource mapping description:
IBM OS/390 Component Broker Base
Logical Resource Mapping for DB2
Admin object class name:
DB2RRSAF390ResourceMgr::IResourceMg
Admin object DLL name:
BBOIDRMI
Admin object class create function:
DB2RRSAF390ResourceMgr_IResourceMg
BBOASR1 Server Definition: Modifiable
CBADMIN

論理リソース・マッピング・インスタンスを追加するためのステップ

この作業を始める前に: CB_OS/390_IVP_DB2 論理リソース・マッピングを定義しなければなりません。

論理リソース・マッピング・インスタンスを追加するには、以下のステップを実行してください。

1. 必要なら、フォルダー・アイコンの左のノードをクリックして、論理リソース・マッピング (Logical Resource Mappings) フォルダーを展開する。

   _____

2. フォルダー・アイコンの左のノードをクリックして、CB_OS/390_IVP_DB2 を展開する。

   _____

3. 左マウス・ボタンで LRM インスタンスを選択する。次に、右マウス・ボタンを使用して、LRM インスタンスをクリックし、「追加 (Add)」を選択する。

   _____

4. 「プロパティー (properties)」フォームで、LRM インスタンス名として、CB_OS/390_IVP_DB2_*system_name* を入力する。*system_name* で提供する値は、規則により、BBOASR1A が動作するシステムのシステム名です。

   例: システム名が SY1 なら、LRM インスタンス名は `CB_OS/390_IVP_DB2_SY1` になります。

   _____

5. オプション: LRM インスタンスの説明を入力する。

   _____

6. この LRM インスタンスを適用するシステムを選択する。

   _____

7. 接続データ・テーブルで、名前の列から「DB2 サブシステム名 (DB2 Subsystem Name)」を見つける。それと関連した値の列に、DB2 サブシステム名、またはグループ接続名を入力する。名前の列に「集合 ID (CollectionId)」が表示されたら、関連した値の列に「CBIVP_PKG」と入力してください。

   _____

8. ディスケットへの保管を表すアイコンをクリックする。「... LRM インスタンスの追加 (Adding... LRM Instances)」がツリーに表示されます。

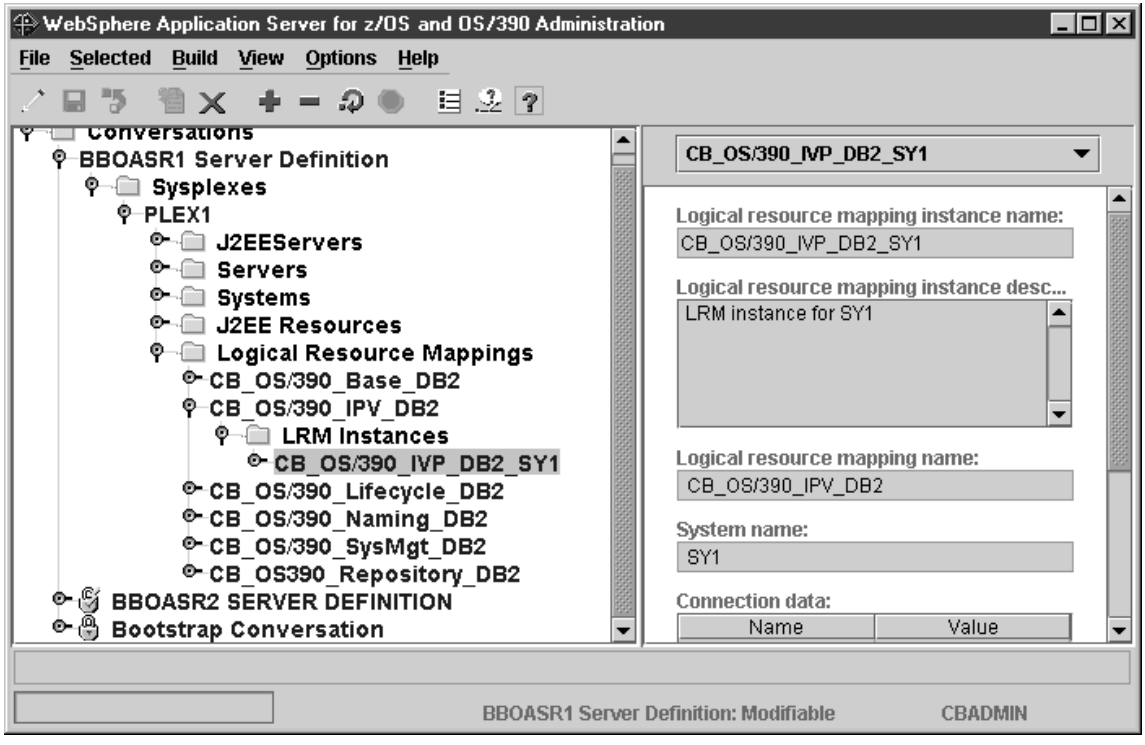
   _____

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I LRM instance CB_OS/390_IVP_DB2_system_name was added.
```

ここで、*system_name* はユーザーが選択したシステム名です。

この手順の最後に、LRM インスタンスを展開し、CB_OS/390_IVP_DB2_SY1 を選択すると、次のような画面が表示されます。



PolicyHomeObjects コンテナーを追加するためのステップ

この作業を始める前に: 現行会話で作業している必要があります。

PolicyHomeObjects コンテナーを追加するには、以下のステップを実行します。

1. 必要な場合は、フォルダー・アイコンの左のノードをクリックして、BBOASR1 フォルダーを展開する。

   ---

2. 左マウス・ボタンでコンテナーを選択する。次に、右マウス・ボタンを使用して、コンテナーをクリックし、「追加 (Add)」を選択する。

   ---

3. 「プロパティー (properties)」フォームで、コンテナー名を次のとおりに入力する。名前には大文字小文字の区別があります。

   ```
   PolicyHomeObjects
   ```

   ---

4. オプション: コンテナーの説明を入力する。

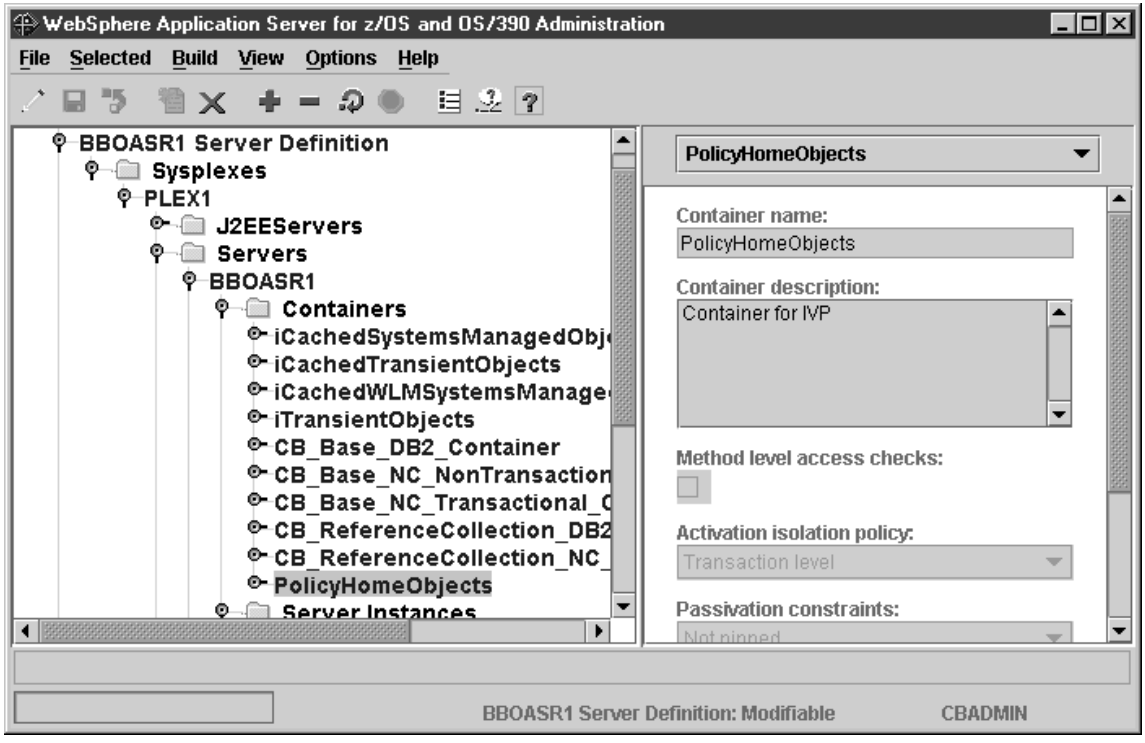
   ---

5. ディスケットへの保管を表すアイコンをクリックする。「... コンテナーの追加 (Adding... Containers)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Container PolicyHomeObjects was added.
```

この手順の最後に、ツリーでコンテナーを展開し、PolicyHomeObjects を選択すると、次のような画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
BBOASR1 Server Definition
Sysplexes
PLEX1
J2EEServers
Servers
BBOASR1
Containers
iCachedSystemsManagedObj
iCachedTransientObjects
iCachedWLMSystemsManage
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransaction
CB_Base_NC_Transactional_C
CB_ReferenceCollection_DB2
CB_ReferenceCollection_NC_
PolicyHomeObjects
Server Instances
PolicyHomeObjects
Container name:
PolicyHomeObjects
Container description:
Container for IVP
Method level access checks:
Activation isolation policy:
Transaction level
Passivation constraints:
Not pinned
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicyHomeObjects コンテナーの論理リソース・マネージャー (LRM) 接続を追加するためのステップ

この作業を始める前に: PolicyHomeObjects コンテナーを追加しなければなりません。

PolicyHomeObjects コンテナーの論理リソース・マネージャー接続を追加するには、以下のステップを実行してください。

1. 必要な場合は、フォルダー・アイコンの左のノードをクリックして、BBOASR1 サーバーの下にあるコンテナー・フォルダーを展開する。

   ---

2. PolicyHomeObjects の左のノードをクリックする。

   ---

3. 左マウス・ボタンで「LRM 接続 (LRM Connections)」を選択する。次に、右マウス・ボタンを使用して「LRM 接続 (LRM Connections)」をクリックし、「追加 (Add)」を選択する。

   ---

4. 論理リソース・マッピング名として、次を選択する。

   ```
   CB_OS/390_IVP_DB2
   ```

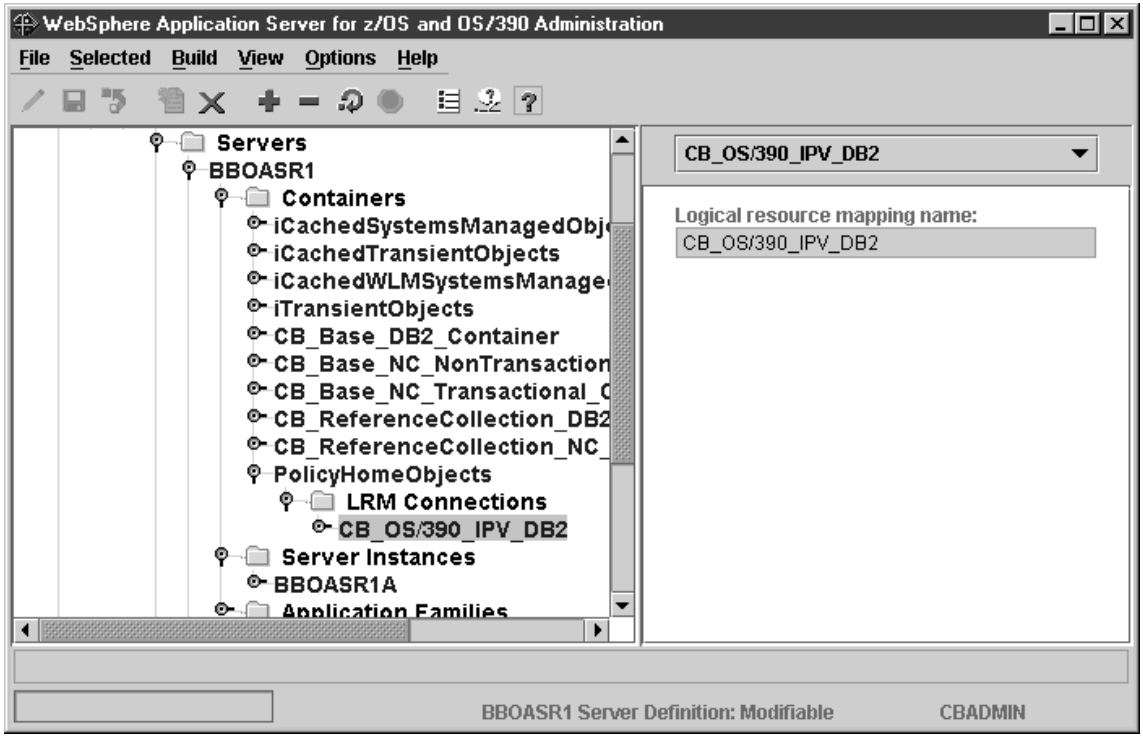
   ---

5. ディスケットへの保管を表すアイコンをクリックする。「... LRM 接続の追加 (Adding... LRM Connections)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0547I LRM connection CB_OS/390_IVP_DB2 was added.
```

この手順の最後に、ツリーで LRM 接続を展開し、CB_OS/390_IVP_DB2 を選択すると、次のような画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Servers
BBOASR1
Containers
iCachedSystemsManagedObj
iCachedTransientObjects
iCachedWLMSystemsManage
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransaction
CB_Base_NC_Transactional_C
CB_ReferenceCollection_DB2
CB_ReferenceCollection_NC_
PolicyHomeObjects
LRM Connections
CB_OS/390_IPV_DB2
Server Instances
BBOASR1A
Application Families
CB_OS/390_IPV_DB2
Logical resource mapping name:
CB_OS/390_IPV_DB2
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicySQLObjects コンテナーを追加するためのステップ

この作業を始める前に: 現行会話で作業している必要があります。

PolicySQLObjects コンテナーを追加するには、以下のステップを実行します。

1. 左マウス・ボタンでコンテナーを選択する。次に、右マウス・ボタンを使用して、コンテナーをクリックし、「追加 (Add)」を選択する。

   _____

2. 「プロパティー (properties)」フォームで、コンテナー名を次のとおりに入力する。名前には大文字小文字の区別があります。

   ```
   PolicySQLObjects
   ```

   _____

3. オプション: コンテナーの説明を入力する。

   _____

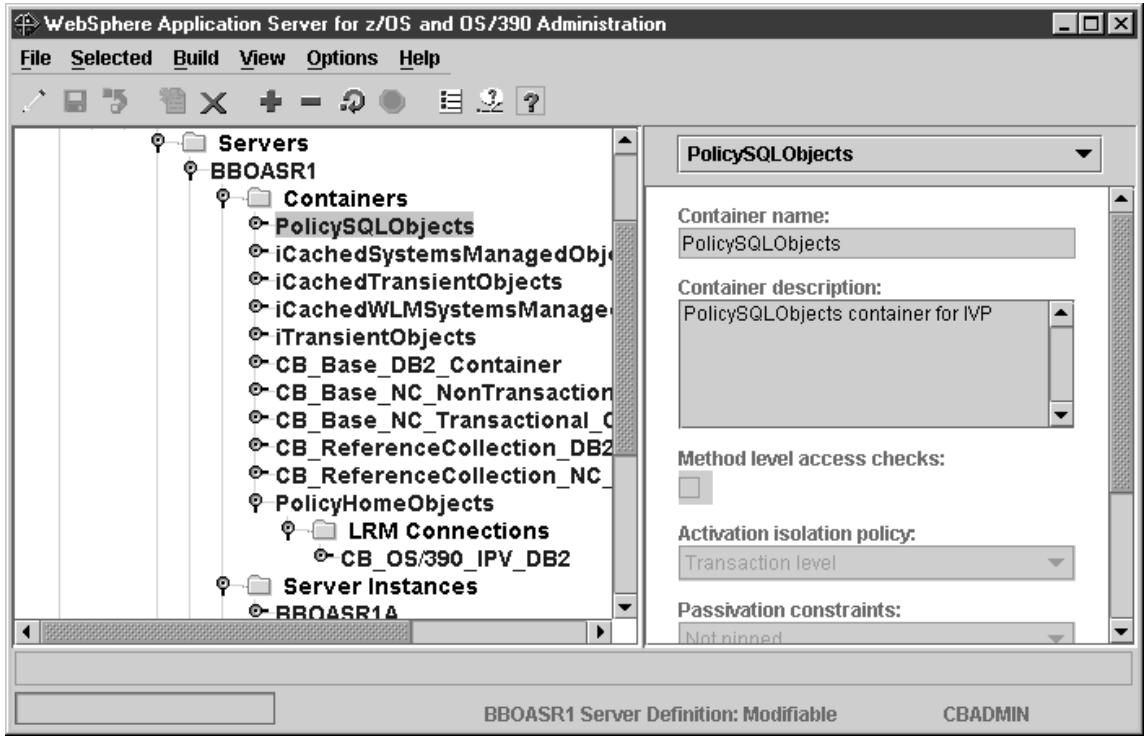
4. ディスケットへの保管を表すアイコンをクリックする。「... コンテナーの追加 (Adding... Containers)」がツリーに表示されます。

   _____

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Container PolicySQLObjects was added.
```

この手順の最後に、ツリーでコンテナーを展開し、PolicySQLObjects を選択すると、次のような画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Servers
BBOASR1
Containers
PolicySQLObjects
iCachedSystemsManagedObj
iCachedTransientObjects
iCachedWLMSystemsManage
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransaction
CB_Base_NC_Transactional_C
CB_ReferenceCollection_DB2
CB_ReferenceCollection_NC_
PolicyHomeObjects
LRM Connections
CB_OS/390_IPV_DB2
Server Instances
BBOASR1A
PolicySQLObjects
Container name:
PolicySQLObjects
Container description:
PolicySQLObjects container for IVP
Method level access checks:
Activation isolation policy:
Transaction level
Passivation constraints:
Not pinned
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicySQLObjects コンテナーの論理リソース・マネージャー (LRM) 接続を追加するためのステップ

この作業を始める前に: PolicySQLObjects コンテナーを追加しなければなりません。

PolicySQLObjects コンテナーの論理リソース・マネージャーを追加するには、以下のステップを実行してください。

1. 必要な場合は、フォルダー・アイコンの左のノードをクリックして、BBOASR1 サーバーの下にあるコンテナー・フォルダーを展開する。

   ---

2. フォルダー・アイコンの左のノードをクリックして、PolicySQLObjects を展開する。

   ---

3. 左マウス・ボタンで「LRM 接続 (LRM Connections)」を選択する。次に、右マウス・ボタンを使用して「LRM 接続 (LRM Connections)」をクリックし、「追加 (Add)」を選択する。

   ---

4. 論理リソース・マッピング名として、次を選択する。

   ```
   CB_OS/390_IVP_DB2
   ```

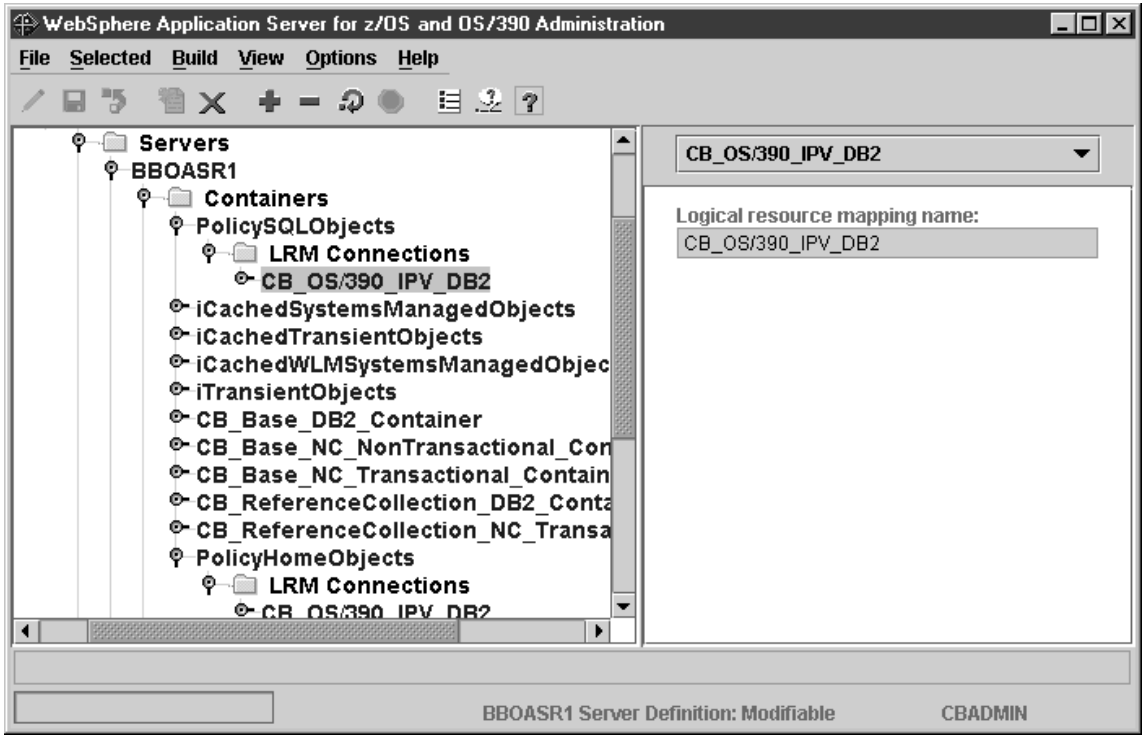
   ---

5. ディスケットへの保管を表すアイコンをクリックする。「... LRM 接続の追加 (Adding... LRM Connections)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0547I LRM connection CB_OS/390_IVP_DB2 was added.
```

この手順の最後に、ツリーで LRM 接続を展開し、CB_OS/390_IVP_DB2 を選択すると、次のような画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Servers
BBOASR1
Containers
PolicySQLObjects
LRM Connections
CB_OS/390_IPV_DB2
iCachedSystemsManagedObjects
iCachedTransientObjects
iCachedWLMSystemsManagedObjec
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransactional_Con
CB_Base_NC_Transactional_Contain
CB_ReferenceCollection_DB2_Conta
CB_ReferenceCollection_NC_Transa
PolicyHomeObjects
LRM Connections
CB_OS/390_IPV_DB2
CB_OS/390_IPV_DB2
Logical resource mapping name:
CB_OS/390_IPV_DB2
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicyTransientObjects コンテナーを追加するためのステップ
この作業を始める前に: 現行会話で作業している必要があります。

PolicyTransientObjects コンテナーを追加するには、以下のステップを実行します。

1. 左マウス・ボタンでコンテナーを選択する。次に、右マウス・ボタンを使用して、コンテナーをクリックし、「追加 (Add)」を選択する。

---

2. 「プロパティー (properties)」フォームで、コンテナー名を次のとおりに入力する。名前には大文字小文字の区別があります。

   ```
   PolicyTransientObjects
   ```

---

3. オプション: コンテナーの説明を入力する。

---

4. 「プロパティー (properties)」フォームで、活動化分離ポリシーのために、「**コンテナー・レベル (Container level)**」を選択する。

> **重要!**
> 「**コンテナー・レベル (Container level)**」を選択してください。これはデフォルトではありません。

---

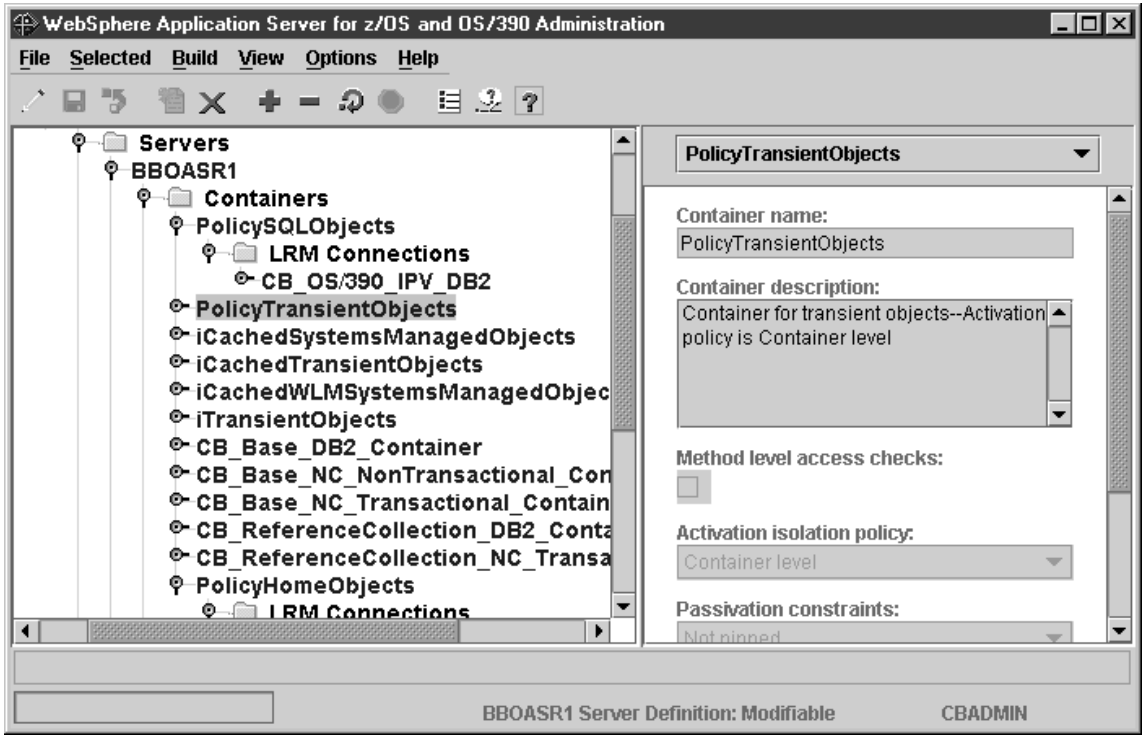
5. ディスケットへの保管を表すアイコンをクリックする。「... コンテナーの追加 (Adding... Containers)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Container PolicyTransientObjects was added.
```

注: LRM 接続は、このコンテナーでは必須ではありません。

この手順の最後に、ツリーでコンテナーを展開し、PolicyTransientObjects を選択すると、次のような画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Servers
BBOASR1
Containers
PolicySQLObjects
LRM Connections
CB_OS/390_IPV_DB2
PolicyTransientObjects
iCachedSystemsManagedObjects
iCachedTransientObjects
iCachedWLMSystemsManagedObjec
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransactional_Con
CB_Base_NC_Transactional_Contain
CB_ReferenceCollection_DB2_Conta
CB_ReferenceCollection_NC_Transa
PolicyHomeObjects
LRM Connections
PolicyTransientObjects
Container name:
PolicyTransientObjects
Container description:
Container for transient objects--Activation policy is Container level
Method level access checks:
Activation isolation policy:
Container level
Passivation constraints:
Not pinned
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicySQLLocalObjects コンテナーを追加するためのステップ
この作業を始める前に: 現行会話で作業している必要があります。

PolicySQLLocalObjects コンテナーを追加するには、以下のステップを実行します。

1. 左マウス・ボタンでコンテナーを選択する。次に、右マウス・ボタンを使用して、コンテナーをクリックし、「追加 (Add)」を選択する。

---

2. 「プロパティー (properties)」フォームで、コンテナー名を次のとおりに入力する。名前には大文字小文字の区別があります。

   ```
   PolicySQLLocalObjects
   ```

---

3. オプション: コンテナーの説明を入力する。

---

4. 「トランザクション (Transaction)」ポリシーの下で、「**同じサーバー・ハイブリッド・グローバルをサポート (Supports Same-Server Hybrid Global)**」を選択する。

   重要!
   「**同じサーバー・ハイブリッド・グローバルをサポート (Supports Same-Server Hybrid Global)**」を選択してください。

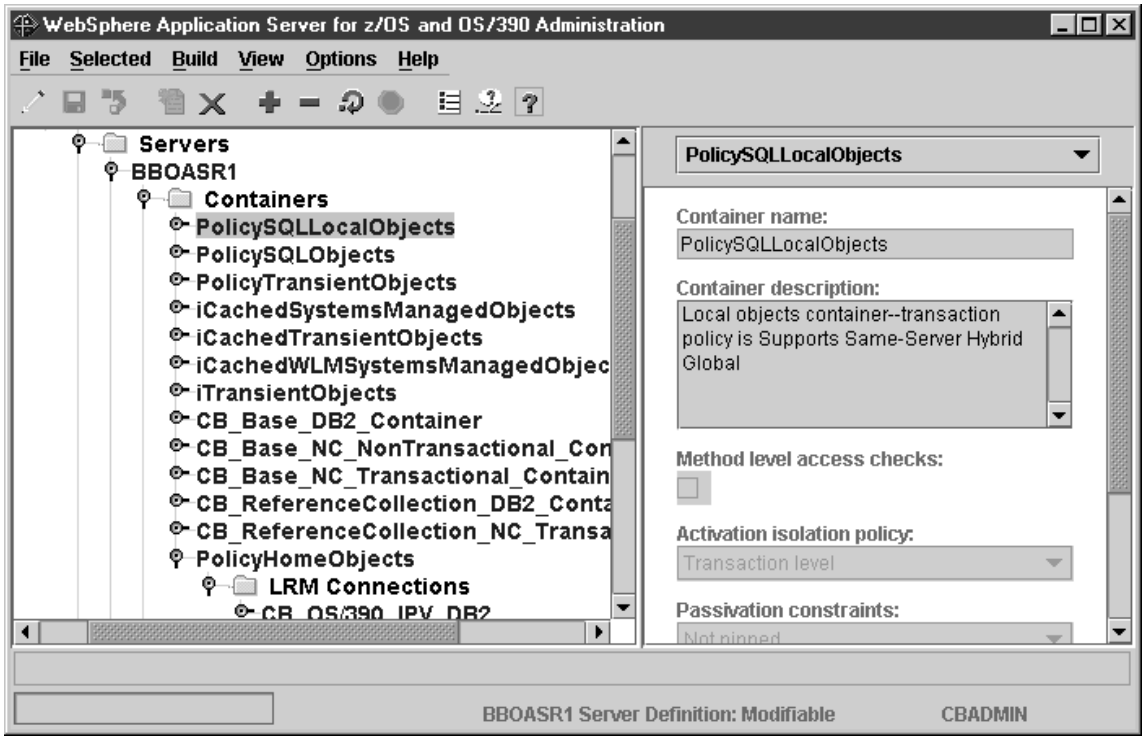
---

5. ディスケットへの保管を表すアイコンをクリックする。「... コンテナーの追加 (Adding... Containers)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Container PolicySQLLocalObjects was added.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Servers
BBOASR1
Containers
PolicySQLLocalObjects
PolicySQLObjects
PolicyTransientObjects
iCachedSystemsManagedObjects
iCachedTransientObjects
iCachedWLMSystemsManagedObjec
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransactional_Con
CB_Base_NC_Transactional_Contain
CB_ReferenceCollection_DB2_Conta
CB_ReferenceCollection_NC_Transa
PolicyHomeObjects
LRM Connections
CB_OS/390_IPV_DB2
PolicySQLLocalObjects
Container name:
PolicySQLLocalObjects
Container description:
Local objects container--transaction policy is Supports Same-Server Hybrid Global
Method level access checks:
Activation isolation policy:
Transaction level
Passivation constraints:
Not pinned
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicySQLLocalObjects コンテナーの論理リソース・マネージャー (LRM) 接続を追加するためのステップ

この作業を始める前に: PolicySQLLocalObjects コンテナーを追加しておかなければなりません。

PolicySQLLocalObjects コンテナーの論理リソース・マネージャーを追加するには、以下のステップを実行します。

1. 必要な場合は、フォルダー・アイコンの左のノードをクリックして、BBOASR1 サーバーの下にあるコンテナー・フォルダーを展開する。

   ---

2. フォルダー・アイコンの左側にあるノードをクリックして、PolicySQLLocalObjects を展開する。

   ---

3. 左マウス・ボタンで「LRM 接続 (LRM Connections)」を選択する。次に、右マウス・ボタンを使用して「LRM 接続 (LRM Connections)」をクリックし、「追加 (Add)」を選択する。

   ---

4. 論理リソース・マッピング名として、次を選択する。

   ```
   CB_OS/390_IVP_DB2
   ```

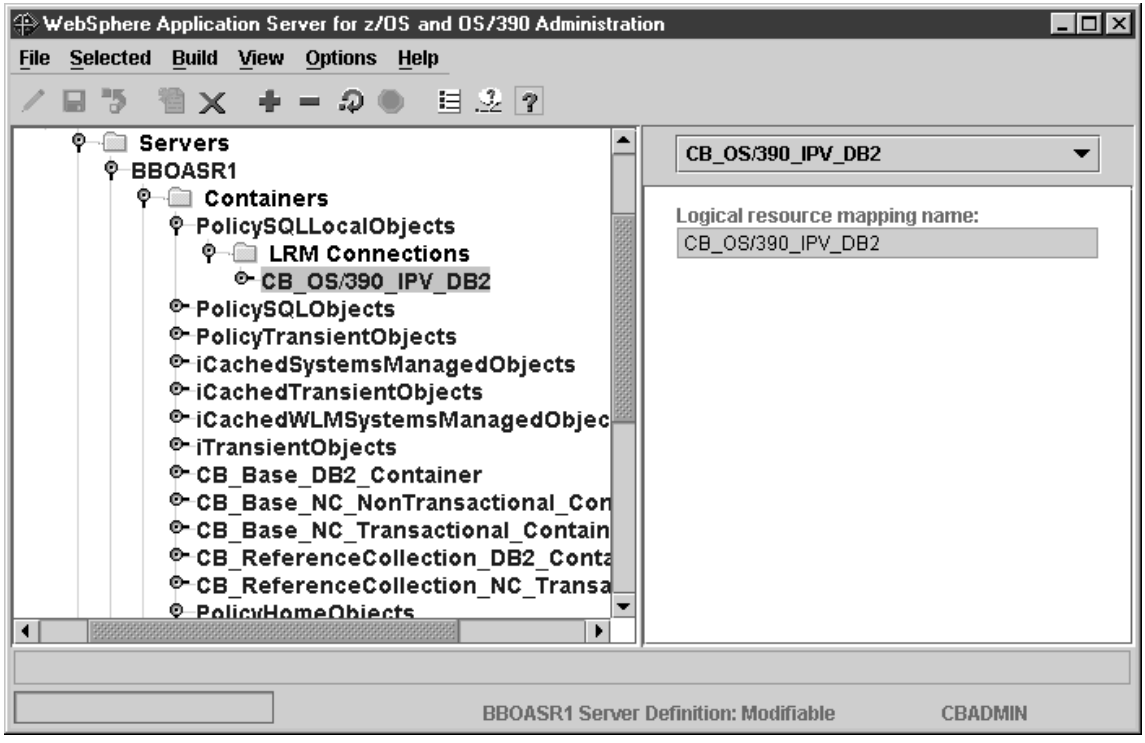
   ---

5. ディスケットへの保管を表すアイコンをクリックする。「... LRM 接続の追加 (Adding... LRM Connections)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0547I LRM connection CB_OS/390_IVP_DB2 was added.
```

この手順の最後に、LRM 接続を展開し、CB_OS/390_IVP_DB2 を選択すると、次の画面が表示されます。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Servers
BBOASR1
Containers
PolicySQLLocalObjects
LRM Connections
CB_OS/390_IPV_DB2
PolicySQLObjects
PolicyTransientObjects
iCachedSystemsManagedObjects
iCachedTransientObjects
iCachedWLMSystemsManagedObjec
iTransientObjects
CB_Base_DB2_Container
CB_Base_NC_NonTransactional_Con
CB_Base_NC_Transactional_Contain
CB_ReferenceCollection_DB2_Conta
CB_ReferenceCollection_NC_Transa
PolicyHomeObjects
CB_OS/390_IPV_DB2
Logical resource mapping name:
CB_OS/390_IPV_DB2
BBOASR1 Server Definition: Modifiable
CBADMIN

PolicyTransientLocalObjects コンテナーを追加するためのステップ
この作業を始める前に: 現行会話で作業している必要があります。

PolicyTransientLocalObjects コンテナーを追加するには、以下のステップを実行します。

1. 左マウス・ボタンでコンテナーを選択する。次に、右マウス・ボタンを使用して、コンテナーをクリックし、「追加 (Add)」を選択する。

---

2. 「プロパティー (properties)」フォームで、コンテナー名を次のとおりに入力する。名前には大文字小文字の区別があります。

   ```
   PolicyTransientLocalObjects
   ```

---

3. オプション: コンテナーの説明を入力する。

---

4. 「プロパティー (properties)」フォームで、活動化分離ポリシーのために、「**コンテナー・レベル (Container level)**」を選択する。

> **重要!**
> 「**コンテナー・レベル (Container level)**」を選択してください。これはデフォルトではありません。

---

5. 「トランザクション (Transaction)」ポリシーの下で、「**同じサーバー・ハイブリッド・グローバルをサポート (Supports Same-Server Hybrid Global)**」を選択する。

> **重要!**
> 「**同じサーバー・ハイブリッド・グローバルをサポート (Supports Same-Server Hybrid Global)**」を選択してください。

---

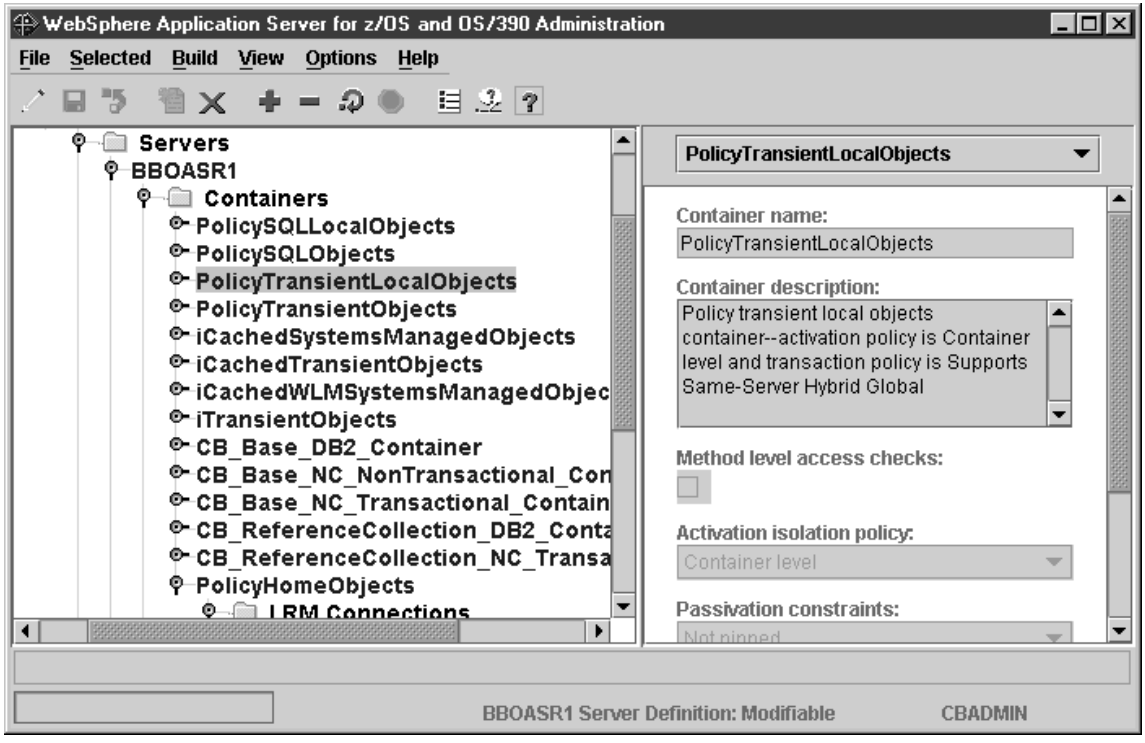
6. ディスケットへの保管を表すアイコンをクリックする。「... コンテナーの追加 (Adding... Containers)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0515I Container PolicyTransientLocalObjects was added.
```

注: LRM 接続は、このコンテナーでは必須ではありません。

この手順の最後に、コンテナーを展開し、PolicyTransientLocalObjects を選択すると、次のような画面が表示されます。



PolicyFamily アプリケーションをインポートするためのステップ

この作業を始める前に: BBOASR1 サーバーを定義しなければなりません。

PolicyFamily アプリケーションをインポートするには、以下のステップを実行してください。

1. OS/390 または z/OS で、WebSphere for z/OS HFS をマウント・ポイント /usr/lpp/WebSphere にマウントする。

---

2. 必要な場合は、会話ツリーを BBOASR1 サーバーまでスクロールアップする。左マウス・ボタンで BBOASR1 を選択する。次に、右マウス・ボタンを使用して BBOASR1 をクリックし、「アプリケーションのインポート (Import application)」を選択する。

---

3. 「インポート (Import)」ダイアログに、PolicyFamily アプリケーションの入出力ファイルを入力する。入力ファイルは次のとおりです。

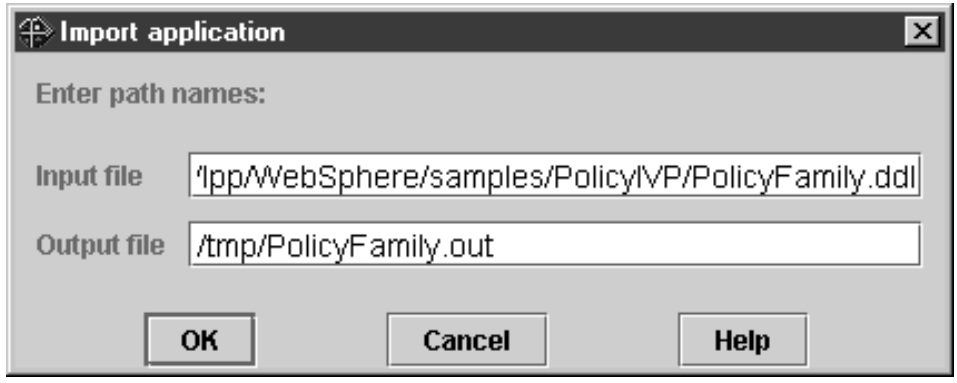
   ```
   /usr/lpp/WebSphere/samples/PolicyIVP/PolicyFamily.ddl
   ```

   規則:

   a. インポートおよび出力データ・セットは、BBOSMSS アドレス・スペースのユーザー ID (BBOCBRAC の例では CBSYMSR1) に関連付けられます。

      - データ・セットを使用する場合、このユーザー ID には、入力データ・セットに対する読み取りアクセス権と、出力データ・セットに対する更新アクセス権がなければなりません。
      - HFS ファイルを使用する場合は、このユーザー ID には、ディレクトリーを検索して入力ファイルを見つける機能、入力ファイルを読み取る機能、および出力ファイルを書き込む機能が備わっていなければなりません。

   b. インポート・プロセス中に使用されるインポートまたは出力データ・セットを、別のプロセスが同時に使用することはできません。たとえば、ISPF を使用して、インポートを開始するのと同時に、データ・セットまたはデータ・セット・メンバーを、編集または参照することはできません。



---

4. 「OK」をクリックする。「... BBOASR1 のインポート (Importing... BBOASR1)」がツリーに表示されます。次のメッセージが出るのを待ってください。

```
BBON0467I Package file '/usr/lpp/WebSphere/samples/PolicyIVP/PolicyFamily.ddl'
          was imported.
```

---

5. 「ファイル (File)」、「メッセージ・ログ... (Message log...)」の順にクリックする。詳細なエラー・メッセージについては、「エラー (Error)」という言葉を検索し、その後に続くメッセージを読んで、メッセージ・ログを検査してください。

インポートがエラーを起こさずに正常に終了すれば、このステップは終了したことになります。

会話の妥当性検査をするためのステップ

この作業を始める前に: 現行会話のこれまでのステップを、すべて完了していなければなりません。

会話の妥当性を検査するには、以下のステップを実行します。

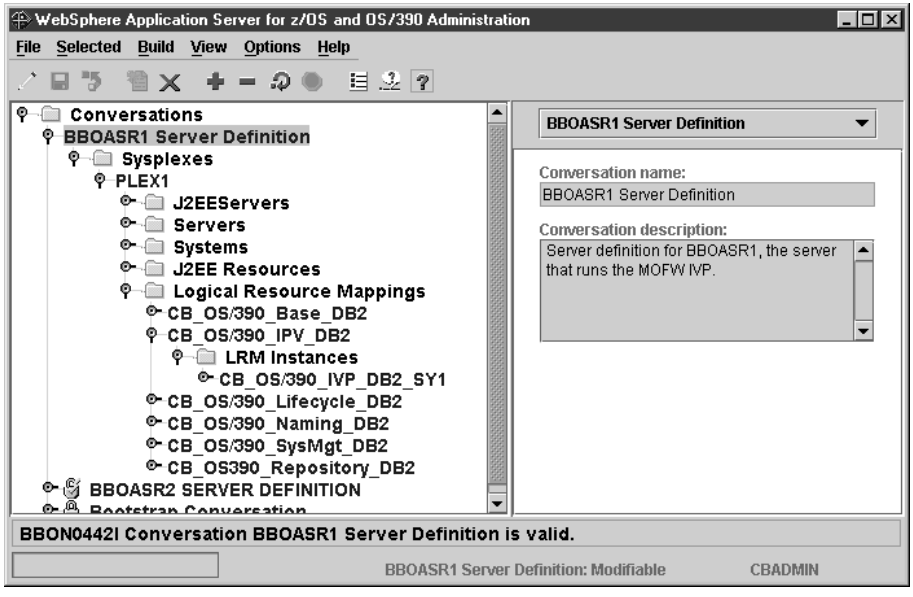
1. 必要なら、ツリーを BBOASR1 Server Definition までスクロールアップする。

---

2. 左マウス・ボタンで会話を選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「検査 (Validate)」を選択する。**結果:** ツリーの中に「...BBOASR1 Server Definition の検査 (Validating... BBOASR1 Server Definition)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0442I Conversation BBOASR1 Server Definition is valid.
```



会話をコミットするためのステップ
この作業を始める前に: 現行会話の妥当性検査をしなければなりません。

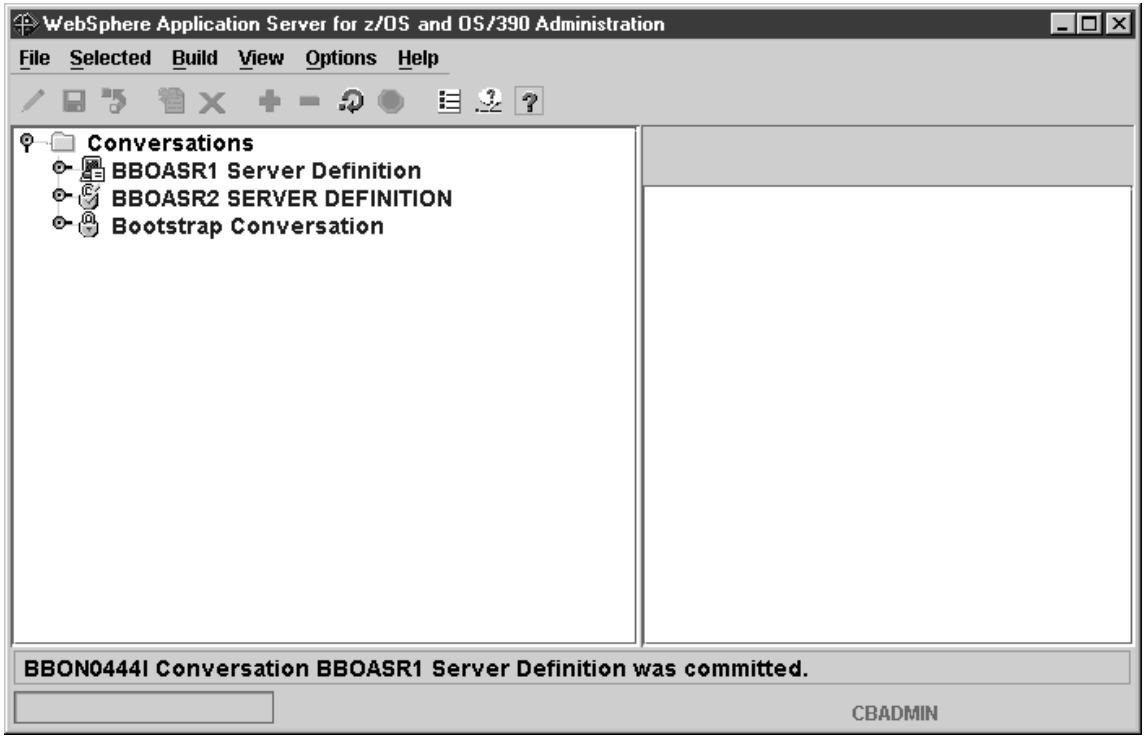
⇔ 左マウス・ボタンで会話を選択します。次に、右マウス・ボタンを使用してその会話をクリックし、「コミット (Commit)」を選択します。以下の質問に「はい (Yes)」と答えてください。

```
BBON0534I You cannot undo Commit.  Do you still want to commit?
```

「... BBOASR1 Server Definition のコミット (Committing... BBOASR1 Server Definition)」がツリーに表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0444I Conversation BBOASR1 Server Definition was committed.
```



OS/390 または z/OS タスクを完了する指示に従うためのステップ

この作業を始める前に: 現行会話の妥当性検査およびコミットを行わなければなりません。

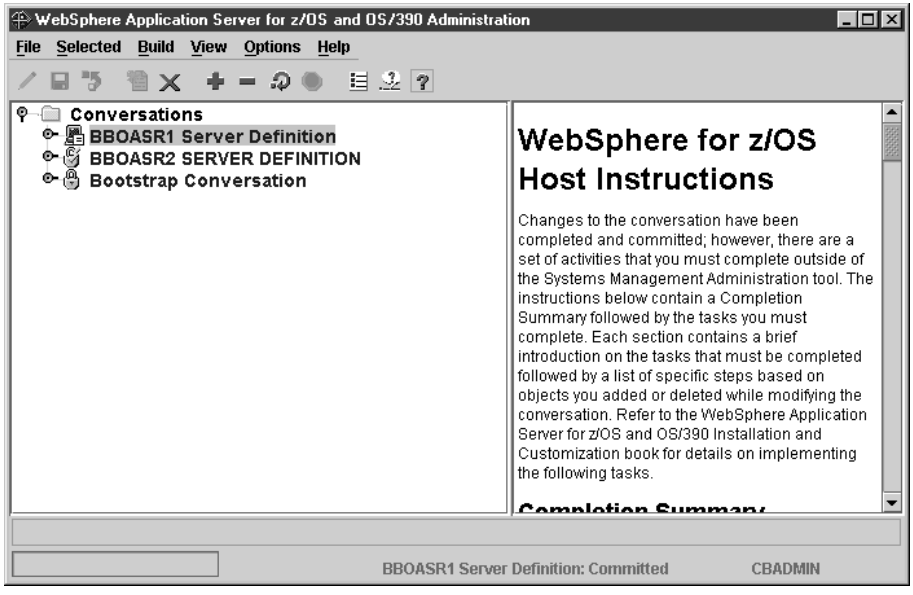
OS/390 または z/OS タスクを完了する指示に従うには、以下のステップを実行してください。

1. 左マウス・ボタンで BBOASR1 Server Definition の会話を選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「指示 (Instructions) 」を選択する。**結果:** ツリーの中に「...指示の取得 (Getting instructions...)」が表示されます。

   ---

2. 管理アプリケーションが提供する、OS/390 または z/OS タスクを完了するための指示をすべて完了する。

必要な OS/390 または z/OS タスクがすべて完了すれば、このステップは終了したことになります。



すべてのタスクの完了をマークするためのステップ

この作業を始める前に: 必要な OS/390 または z/OS タスクをすべて完了していなければなりません。

すべてのタスクの完了をマークするには、以下のステップを実行してください。

1. 左マウス・ボタンで BBOASR1 Server Definition の会話を選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「完了 (Complete)」に続いて「すべてのタスク (All tasks)」を選択する。

---

2. 以下の質問に「はい (Yes)」と答える。

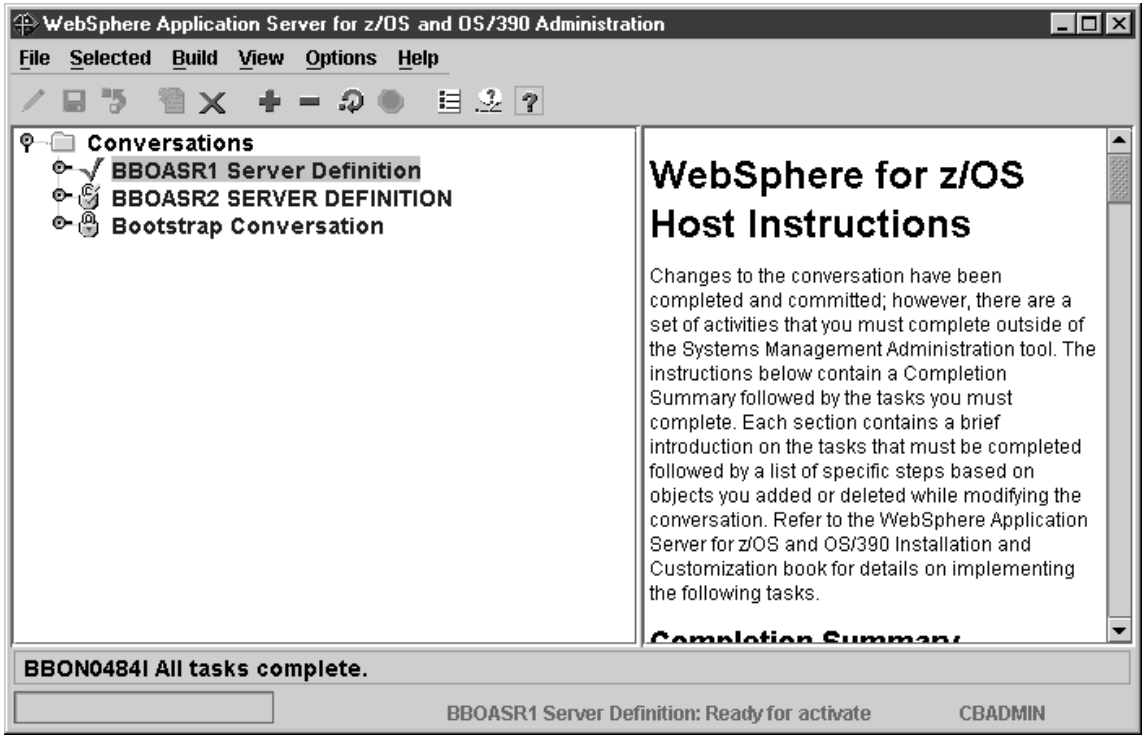
   ```
   BBON0550I  Are you sure that all tasks have been completed?
   ```

   結果: ツリーの中に「...BBOASR1 Server Definition タスクの完了 (Completing tasks... BBOASR1 Server Definition)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0484I All tasks complete.
```

画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR1 Server Definition
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
WebSphere for z/OS Host Instructions
Changes to the conversation have been completed and committed; however, there are a set of activities that you must complete outside of the Systems Management Administration tool. The instructions below contain a Completion Summary followed by the tasks you must complete. Each section contains a brief introduction on the tasks that must be completed followed by a list of specific steps based on objects you added or deleted while modifying the conversation. Refer to the WebSphere Application Server for z/OS and OS/390 Installation and Customization book for details on implementing the following tasks.
BBON0484I All tasks complete.
BBOASR1 Server Definition: Ready for activate
CBADMIN

新しい会話を活動化するためのステップ

この作業を始める前に: この節でこれまで述べてきた指示をすべて完了していなければなりません。

新規会話を活動化するには、以下のステップを実行してください。

1. 左マウス・ボタンで BBOASR1 Server Definition の会話を選択する。次に、右マウス・ボタンを使用してその会話をクリックし、「活動化 (Activate)」を選択する。

   ---

2. 以下の質問に「はい (Yes)」と答える。

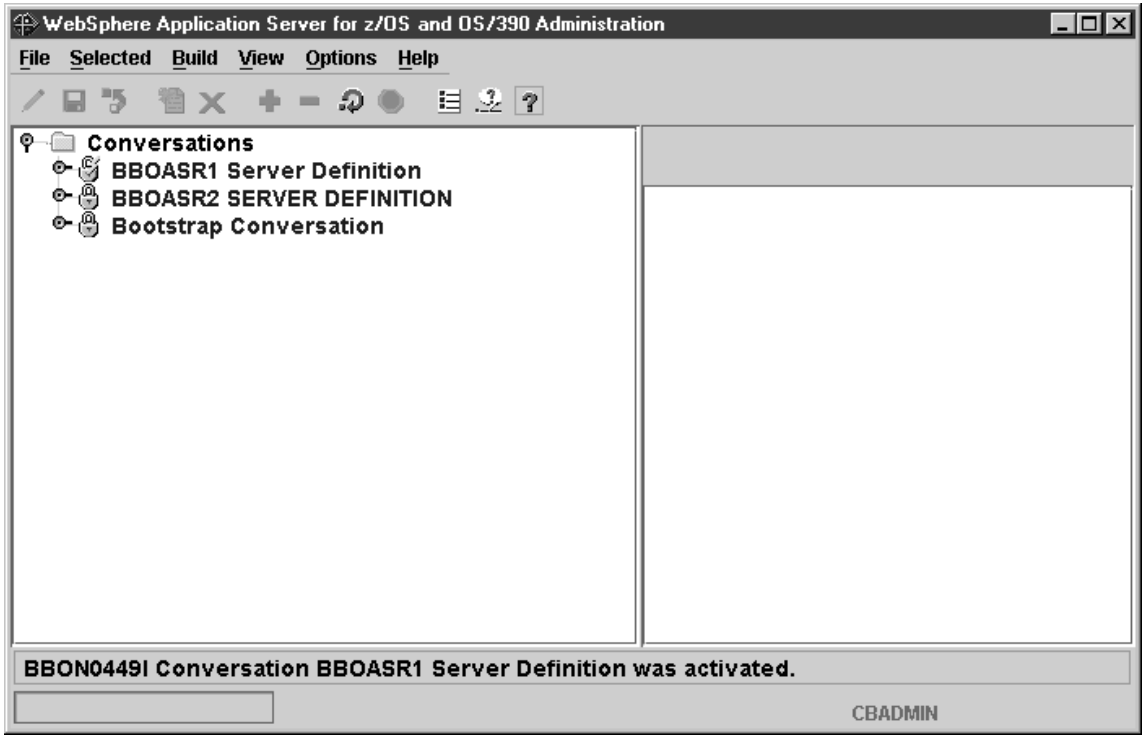
   ```
   BBON0539I  Activate cannot undone.  Do you want to activate conversation
              BBOASR1 Server Definition?
   ```

   結果: ツリーの中に「...BBOASR1 Server Definition の活動化 (Activating... BBOASR1 Server Definition)」が表示されます。

ステータス・バーに次のメッセージが表示されれば、このステップは終了したことになります。

```
BBON0449I Conversation BBOASR1 Server Definition was activated.
```

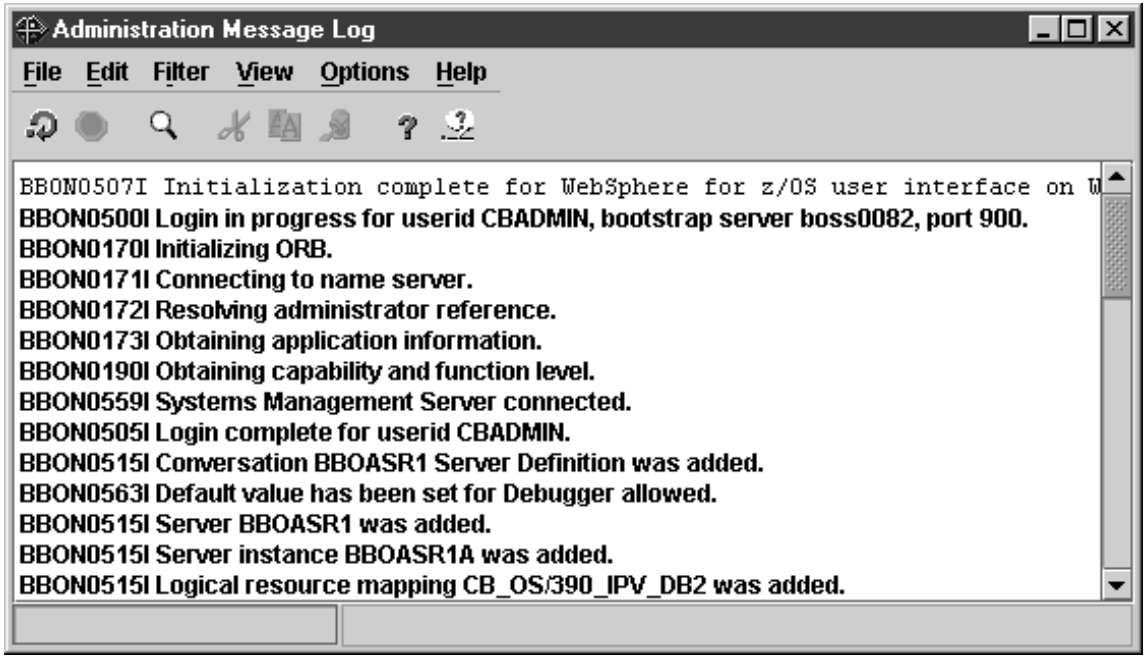
画面は次のようになります。


WebSphere Application Server for z/OS and OS/390 Administration
File Selected Build View Options Help
Conversations
BBOASR1 Server Definition
BBOASR2 SERVER DEFINITION
Bootstrap Conversation
BBON0449I Conversation BBOASR1 Server Definition was activated.
CBADMIN

管理メッセージ・ログを印刷するためのステップ
この作業を始める前に: 会話を活動化しなければなりません。

管理メッセージ・ログを印刷するには、次のステップに従ってください。

1. 「ファイル (File)」に続いて「メッセージ・ログ **...** (Message log...)」をクリックする。
   結果: 画面は次のようになります。



2. 「管理メッセージ・ログ (Administration Message Log)」ウィンドウから、「ファイル (File)」をクリックし、次に「印刷 (Print...)」をクリックする。
   結果: Windows の印刷ダイアログが表示されます。
   プリンターを選択して「OK」をクリックする。次のポップアップが表示されます。

管理メッセージ・ログの印刷出力が取得されれば、このステップは終了したことになります。プログラムを終了してかまいません。

インストール検査プログラム (IVP) 用のデータベースを作成するためのステップ

この作業を始める前に: BBOICD、BBOIBN、および BBOIGRT のコピーが必要です。

IVP 用のデータベースを作成するには、以下のステップを実行します。

1. ポリシー・データベース・ジョブ、BBOICD のコピーを、そのファイルのコメントに従って更新する。

   _____

2. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、BBOICD のコピーを実行依頼する。

   _____

3. ポリシー PO パッケージ・ジョブ、BBOIBN のコピーを、そのファイルのコメントに従って更新する。

   _____

4. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、ユーザー・バージョンの BBOIBN を実行依頼する。

   _____

5. IVP のサーバーとクライアントの GRANT ジョブ、BBOIGRT のコピーを、そのファイル内のコメントに従って更新する。

   _____

6. DB2 for OS/390 の SYSADM 権限を持つユーザー ID で、ユーザー・バージョンの BBOICD を実行依頼する。

   _____

これらのジョブが正しく実行された時点で、このステップは完了です。

WebSphere for z/OS インストール検査プログラム (IVP) の実行

WebSphere for z/OS のカスタマイズが完了した時点で、BBOASR2 と BBOASR1 のどちらのアプリケーション・サーバーをセットアップしたかに応じて、BBOIVPE (J2EE 機能をテストする IVP) か BBOIVP (MOFW 機能をテストする IVP)、またはその両方を実行できます。

- BBOIVPE を実行する場合は、『BBOIVPE (J2EE) インストール検査プログラムを実行するためのステップ』を参照してください。
- BBOIVP を実行する場合は、195ページの『BBOIVP (MOFW) インストール検査プログラム (IVP) を実行するためのステップ』を参照してください。

どちらの IVP も、前もってパッケージ化されたアプリケーションです。すべてのアプリケーション開発作業は、ユーザーに代わって、すでに済まされています。WebSphere for z/OS 用のアプリケーションの開発方法については、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

BBOIVPE (J2EE) インストール検査プログラムを実行するためのステップ

以下の指示は、BBOIVPE (J2EE) インストール検査プログラムの実行方法を説明したものです。SMP/E インストールの完了後、ファイル・システムの `usr/lpp/WebSphere/samples/PolicyIVP/ejb` ディレクトリーで、IVP に使用されるサンプル・ソースを見ることができます。このサンプルは、Enterprise bean を実行します。

この作業を始める前に: IVP を実行するユーザー ID は、RACF OMVS セグメント (サンプルの RACF では、CBIVP) を持っていなければなりません。このユーザー ID が Java 仮想マシン (JVM) に対する読み取りアクセス権を持っていることを確認してください。

BBOIVPE IVP を実行するには、以下のステップを実行します。

1. LDAP サーバーをまだ始動していなければ、この時点で始動する。**例:**

   ```
   S BBOLDAP
   ```

   結果: 次のメッセージを待機してください。

   ```
   GLD0122I Slapd is ready for requests
   ```

2. IVP クライアントに必要なファイルを保持するディレクトリーを作成する。**例:**

   ```
   mkdir /tmp/CBIVP
   ```

3. PolicyIVP_resolved.ear ファイルと ejbivp.sh ファイルをそのディレクトリーにコピーし、IVP ユーザー ID がこれらのファイルにアクセスできることを確認する。**例:**

```
cp  targetdir/apps/BBOASR2/PolicyIVP_resolved.ear         /tmp/CBIVP
cp  /usr/lpp/WebSphere/samples/PolicyIVP/ejb/ejbivp.sh    /tmp/CBIVP
chown  CBIVP   /tmp/CBIVP/*
```

ここで、*targetdir* はマウント・ポイントです。

4. 新規に作成したディレクトリーへ移動し、ファイルの unjar を行う。**例:**

```
cd  /tmp/CBIVP
jar -xvf PolicyIVP_resolved.ear
```

ヒント: SDK がデフォルトのパスに入っていない場合は、jar コマンドの中で SDK のディレクトリーを指定する必要があります。

```
/usr/lpp/java/IBM/J1.3/bin/jar  -xvf  PolicyIVP_resolved.ear
```

5. 必要に応じて、次のように ejbivp.sh シェル・スクリプトを更新する。
   - デフォルトのインストール・パス、/usr/lpp/WebSphere を使用しない場合は、シェル・スクリプトの中でこのパスが参照されている箇所に変更を加えます。
   - CLASSPATH を、ステップ 4 で unjar を行った jar ファイルを指すように更新します。
   - SDK へのデフォルトの PATH がない場合は、PATH ステートメントを追加します。

     ```
     export PATH=<SDK_install_path>/bin:$PATH
     ```

     ここで、<*SDK_install_path*> は使用したい JDK へのパスです。

6. BBOASR2 と BBOASR2S のコピーを、これらのファイル内のコメントに従って更新する。

7. 次のようにして BBOASR2A サーバーを始動する。

```
s bboasr2.bboasr2a
```

BBOASR2A が完全に初期化され、コンソールに次のメッセージが表示されるまで待ってください。

```
BBOU0695I Naming registration completed for server BBOASR2
```

---

8. BBOIVPE のコピーを、そのファイルのコメントに従って変更する。

---

9. BBOIVPE を実行依頼する。

BBOIVPE が正常に実行されれば、このステップは完了です。

BBOIVP (MOFW) インストール検査プログラム (IVP) を実行するためのステップ

以下の指示は、BBOIVP (MOFW) インストール検査プログラムの実行方法を説明したものです。SMP/E インストールの完了後、ファイル・システムの usr/lpp/WebSphere/samples/PolicyIVP ディレクトリーで、IVP に使用されるサンプル・ソースを見ることができます。このサンプルは C++ プログラムを実行し、続いて Java プログラムを実行します。

この作業を始める前に: IVP を実行するユーザー ID は、RACF OMVS セグメント (サンプルの RACF では、CBIVP) を持っていなければなりません。このユーザー ID が Java 仮想マシン (JVM) に対する読み取りアクセス権を持っていることを確認してください。

IVP をセットアップして実行するには、以下のステップを実行してください。

1. サーバー・インスタンスを実行する OS/390 または z/OS 開始プロシージャーを準備する。次のファイルを、そのファイルのコメントに従って更新してください。
   - BBOASR1
   - BBOASR1S

   ---

2. 次のようにして BBOASR1A サーバーを始動する。

   ```
   s bboasr1.bboasr1a
   ```

   BBOASR1A が完全に初期化され、コンソールに次のメッセージが表示されるまで待ってください。

   ```
   BBOU0695I Naming registration completed for server BBOASR1
   ```

   ---

3. BBOASR1A サーバー・インスタンス用の環境ファイル (*targetdir*/controlinfo/envfile/*SYSPLEX*/BBOASR1A/current.env) を、IVP クライアント・ユーザー ID (CBIVP) が読み取りアクセス権を持っているディレクトリーへコピーする。この環境ファイルは、BBOIVP ジョブが実行する IVP クライアントの環境ファイルになります。
   a. IVP クライアント環境ファイルを編集します。
   b. RESOLVE_IPNAME の値 (クライアントには必須です) を検査してください。
   c. CLIENTLOGSTREAMNAME を追加することもできます。

環境変数の詳細については、383ページの『付録A. 環境ファイル』を参照してください。

---

4. jcivp.sh をコピーする。製品バージョンの jcivp.sh のデフォルト・ディレクトリーは、/usr/lpp/WebSphere/samples/PolicyIVP/ です。

---

5. 必要に応じて、次のように jcivp.sh スクリプトを更新する。
   a. デフォルトのインストール・パス、/usr/lpp/WebSphere を使用しない場合は、シェル・スクリプトの中でこのパスが参照されている箇所に変更を加えます。
   b. SDK 1.3 がデフォルト・パスに入っていない場合は、シェル・スクリプトに次のステートメントを追加します。

      ```
      export PATH=<SDK_install_path>
      ```

      例: `export PATH=/usr/lpp/java/IBM/J1.3`
   c. 変更した jcivp.sh スクリプトを保存します。

---

6. インストール検査プログラム・ジョブ、BBOIVP のコピーを、そのファイルのコメントに従って更新する。確実に次を指すようにしてください。
   - BBOENV DD ステートメント上の IVP クライアント環境ファイル
   - 使用する jcivp.sh のコピー

   注: BBOASR1 以外のサーバー名を使用した場合は、BBOIVP 内の IVP1 および IVP2 ステップの PARM= ステートメントを更新しなければなりません。PARM= ステートメントの構文は、次のとおりです。

   ```
   PARM='[java] [serverSERVERNAME] [timeout=xxxx]'
   ```

   ここで

   java
   そのステップで C++ BO でなく Java BO を使用することを示します。このパラメーターは、IVP2 ステップで使用されます。

   serverSERVERNAME
   サーバー名を指定します。デフォルトは BBOASR1 です。

   timeout=xxxx
   トランザクションのタイムアウト値です。

例:

```
PARM=('java serverMYSERVER timeout=500')
```

同様の変更をシェル・スクリプトの中でも行う必要があります。

---

7. BBOIVP を実行依頼して、クライアント IVP プログラムを実行する。

IVP クライアントから、SYSPRINT 出力ファイルに次のメッセージが表示されれば、このステップは終了したことになります。最初のメッセージは C++ ビジネス・オブジェクト用、2 番目のメッセージは Java ビジネス・オブジェクト用、3 番目のメッセージは Java クライアント用です。

```
All tests completed successfully
All tests completed successfully
Java Client test complete and successful
```

BBOIVP のステップ 3A が、次のようなメッセージで失敗する場合があります。

```
CORBA::INTERNAL.  Error code is C9C21118.
The data from jcivp.out is:
       Your JDK installation is incomplete, java may fail
       (file JDK_INSTALL_OK not found)
The data from jcivp.err is:  java was not found in <directory>
```

ここで、<*directory*> はディレクトリー・パスです。jcivp.sh を検査し、Java がデフォルト・パスに入っているかどうかを確認してください。シェル・スクリプトを更新し、IVP を再度実行してください。

使用している環境が jcivp.sh の想定するデフォルトの環境に一致しない場合は、これ以外のエラーが起きることもあります。たとえば、jcivp.sh 内の CLASSPATH ステートメントが指すパスに jar ファイルが入っていない場合などです。

2 番目のインターフェース・リポジトリー・クライアント・ブートストラップの実行

2 番目のインターフェース・リポジトリー・ブートストラップは、完了までに時間を要する場合があるので、最後に実行してください。

2 番目のインターフェース・リポジトリー・クライアント・ブートストラップを開始するためのステップ

この作業を始める前に: 時間が十分あるときに、2 番目のインターフェース・リポジトリー・クライアント・ブートストラップを実行しておきます。弊社で BBOIRC2 を実行したときには、完了までに 2 時間かかりました。

LDAP を更新できるユーザー ID でログオンしてください。BBOIRC2 に関連したユーザーには、LDAP データベースを更新する権限がなければなりません。システム管理の管理者ユーザー ID (CBADMIN) の使用をお勧めします。別のユーザー ID を使用する場合は、289ページの『管理アプリケーションの新規管理者の追加』の指示に従ってください。

2 番目のインターフェース・リポジトリー・クライアント・ブートストラップを開始するには、次のステップを実行してください。

1. 2 番目のインターフェース・リポジトリー・クライアント・ブートストラップ、BBOIRC2 のコピーを、そのファイルのコメントに従って更新する。

   _____

2. BBOIRC2 のコピーをジョブとして実行依頼する。

   _____

3. 戻りコード 0 を検査する。完了前にジョブが失敗した場合は、
   a. ジョブ・ログを検査して、障害がどのステップで発生したかを判別する。
   b. 障害の原因となった問題を解決する。
   c. ジョブ内で START 変数を変更し、障害が起こったステップから再始動する。たとえば、ジョブがステップ 39 で失敗した場合は、START 変数を、START=39 を読み取るように変更します。
   d. ジョブを再度実行依頼する。

   _____

ジョブがエラーを起こさずに完了すれば、このステップは終了したことになります。

お疲れさまでした

これで WebSphere for z/OS のインストールおよびカスタマイズは完了しました。次は、インストール後のタスクの実行です。285ページの『第5章 インストール後のタスク』を参照してください。

本章の補足

この節では、インストール時に必要となる可能性がある操作とジョブの、一般的な参照事項を提供しています。

RRS をコールド・スタートするためのステップ

RRS をコールド・スタートするには、次のステップを実行してください。

⇔ 次のジョブを実行します。

```
//ATRCOLD  JOB  MSGLEVEL=(1,1),REGION=4M
//*
//*01* FUNCTION: DELETES AND REDEFINES THE RRS RESOURCE MANAGER
//*              DATA LOGSTREAM FOR TESTING
//*********************************************************************
//STEP1    EXEC PGM=IXCMIAPU
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD  *
DATA TYPE(LOGR) REPORT(YES)      /* DEFAULT TO SHOW OUTPUT OF JOB */
DELETE LOGSTREAM NAME(ATR.xxxx.RM.DATA)     xxxx = group name
DEFINE LOGSTREAM NAME(ATR.xxxx.RM.DATA)
```

注: このログ・ストリームの作成に使用されるのと同じログ・ストリーム属性を使用します。

このジョブが正常に完了すれば、このステップは終了したことになります。

ネーム・スペースの内容を検査するためのステップ

この作業を始める前に: LDAP サーバーのインストールを行わなければなりません。

ネーム・スペースの内容を検査するには、以下のステップを実行してください。

1. LDAP サーバーを始動する。たとえば次のようになります。

   ```
   S BBOLDAP
   ```

   メッセージ「Starting slapd (slapd を開始します)」が、オペレーターのコンソールに表示され、「Listening on 0 (0 で listen します)」などのメッセージが、ジョブで定義される SLAPDOUT データ・セットに表示されます。

   ---

2. ジョブ出力を検査して、`done with initial namespace` という語句を探す。

   ---

3. LDAP の内容を検索するための CLIST を作成する (たとえば BOSS.SLAPD.CLIST(BBOLSRCH))。次のものを CLIST に入れてください。

```
/* REXX */
queue('GLDSRCH  -h 127.0.0.1 -p 1389 -b "o=BOSS,c=US"  "objectclass=*"')
```

---

4. CLIST を実行する。たとえば、ISPF オプション 6 を使用して、次のように入力して LDAP の内容を表示します。

```
ex 'boss.slapd.clist(bbolsrch)'
```

いくつかの出力画面があります。

CLIST から画面出力が表示されれば、このステップは終了したことになります。

LDAP 項目を削除するためのステップ

インストールとカスタマイズのときに、ネーミング・クライアント・ジョブが失敗した場合は、この手順を使用して回復してください。

インターフェース・リポジトリーのネーム・スペースの構造上、この手順を使用してインターフェース・リポジトリーの項目を削除することはできません。

重要: インストールとカスタマイズが完了した後は、絶対に必要な場合以外、この手順を使用してネーミング・サーバーまたはインターフェース・リポジトリー・サーバーの LDAP テーブルを回復しないでください。インストールとカスタマイズの後にこの手順を使用するには、WebSphere for z/OS を再カスタマイズする (つまり、コールド・スタートを行う) 必要があります。LDAP テーブルには、正規のバックアップ手順とデータ・マイグレーション手順を使用してください。

この作業を始める前に: SDELETE モジュールが必要です。SDELETE モジュールは、BBO.SBBOLOAD(BBOLSDEL) に入っています。SDELETE に関する詳細は、*z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923 を参照してください。

LDAP サーバーをインストールしておかなければなりません。

項目を削除するには、次のようにします。

1. LDAP サーバーを始動する。たとえば次のようになります。

```
S BBOLDAP
```

---

2. LDAP 項目を削除するための CLIST を作成する (たとえば BOSS.SLAPD.CLIST(BBOLSDEL))。次のものを CLIST に入れてください。

```
/* REXX */
queue('sdelete -h 127.0.0.1 -p 1389 -D "cn=admin,cn=localhost" -w secret
"TypelessRDN=/,o=BOSS,c=US"')
```

---

3. CLIST を実行する。たとえば、ISPF オプション 6 を使用して、次のように入力して CLIST を実行します。

```
ex 'boss.slapd.clist(bbolsdel)'
```

---

4. BBOLSDEL の実行が正常に行われない場合は、
   a. BBOLDTBD を使用して LDAP テーブルを除去する。
   b. BBOLDTBC を使用して LDAP テーブルを再作成する。
   c. バインド・ジョブ、BBO1JCL および BBO2JCL を再実行する。
   d. GRANT ジョブの BBOCBGRT と BBOLDGRT を再実行する。
   e. LDAP バルク・ローダー (サンプル BBOLD2DB) を再実行する。

BBOLD2DB ジョブが正常に実行されれば、このステップは終了です。

ワークロード管理およびサーバー障害の処理

操作中に、アプリケーションが繰り返し障害を起こし、アプリケーション・サーバー領域を終了させる場合は、ワークロード管理によって、アプリケーションのアプリケーション環境が終了させられることがあります。WebSphere for z/OS は、障害が発生したアプリケーション環境を使用しようとする場合には、次のようなメッセージを発行します。

```
BBOU199E Unable to schedule work.  WLM application environment applenv has
         stopped.
```

アプリケーションで問題を修正し、VARY WLM コマンドの RESUME オプションで、アプリケーション環境を再始動しなければなりません。

ワークロード管理アプリケーション環境を検査および開始するためのステップ
ワークロード管理アプリケーション環境を検査し、開始するためには、以下のステップを実行してください。

1. アプリケーション環境を表示するために、次のコマンドを発行する。

   ```
   d wlm,applenv=*
   ```

---

2. アプリケーション環境を開始するために、次のコマンドを発行する。

   ```
   v wlm,applenv=environment_name,resume
   ```

   ここで、**environment_name** はアプリケーション環境の名前です。

アプリケーション環境を再表示し、環境が使用可能であれば、このステップは終了したことになります。

第4章 WebSphere for z/OS の新規リリースへのマイグレーション

現在、WebSphere Application Server for OS/390 の古いリリースを使用しており、WebSphere Application Server V4.0 for z/OS and OS/390 にマイグレーションする場合、または J2EE アプリケーションを別の WebSphere プラットフォームから WebSphere for z/OS に移動することを計画している場合は、この章を読み、その指示に従ってください。

マイグレーションの概要

新しいレベルの WebSphere for z/OS へマイグレーションする計画には、さまざまな情報源からの情報を組み込んでください。ここに示す情報源には、共存、サービス、ハードウェアとソフトウェアの要件、インストールとマイグレーションの手順、インターフェースの変更などのトピックが説明されています。

次の資料は、製品とともに提供されるもので、OS/390 システムのインストールに関する情報を提供します。

- *WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549

  この文書は、OS/390 製品とともに提供されるもので、WebSphere for z/OS の詳しいインストール・ステップを説明しています。

- *ServerPac: オーダーのインストール*

  これは、ServerPac Installation メソッドを使用するための、オーダーでカスタマイズされたインストール資料です。必ず、付録の製品情報を検討してください。ここには、提供されるデータ・セット、すでにユーザーに代わって実行されているジョブまたはプロシージャー、および製品の状況が記述されています。すでに IBM がジョブを実行しているか、PARMLIB またはその他のシステム制御データ・セットを更新している場合があります。それらの更新によって、マイグレーションが影響を受ける場合もあります。

この資料の中に、本リリースの WebSphere for z/OS に適用される特定の更新と考慮事項に関する情報が記載されています。

• 210ページの『マイグレーション・ロードマップ』

ここでは、現行レベルの WebSphere for z/OS でサポートされるマイグレーション・パスが示されています。また、現行レベルへのマイグレーションに役立つ追加資料も記載されています。

- 217ページの『マイグレーション・パスの概要』

  ここでは、現行リリース用に WebSphere for z/OS に加えられた更新内容が詳しく説明されています。それぞれの項目について、変更の概要、考慮できるマイグレーション・タスクおよび共存タスクの説明、WebSphere for z/OS ライブラリーまたはその他のエレメントのライブラリーのどこに詳細な情報があるか、が記載されています。

- 276ページの『インターフェースの変更の要約』

  ここには、WebSphere for z/OS のユーザー・インターフェースとプログラミング・インターフェースに加えられた変更の要約が記載されています。

知っておく必要がある用語

ここでは、本書を使用するときに知っておく必要があるいくつかの用語について説明します。

マイグレーション
古いレベルのプログラムに代わる新しいバージョンまたはリリースのインストールに関連した活動。これらの活動を完了することによって、システム上のアプリケーションとリソースが新しいレベルで正しく機能するようになります。

共存
異なるレベル (たとえば、ソフトウェア・レベル、サービス・レベル、または操作レベル) にありながら、リソースを共用する複数のシステム。共存には、リソースを共用している別のシステム上に導入された新しい機能に対して、その新しい機能を無視するか、終了するか、または新しい機能をサポートすることによって応答するシステムの能力が含まれます。リソースの共用が可能な構成の例を次に示します。

- WebSphere Application Server スタンダード版 for OS/390 V3.02 と WebSphere Application Server V4.0 for z/OS and OS/390
- WebSphere Application Server スタンダード版 for OS/390 V3.5 と WebSphere Application Server V4.0 for z/OS and OS/390

活用
あるリリースに対する、オプションの機能拡張を利用することに関連した活動。

相互協調処理
異なるプラットフォーム上にあり、互いに通信する複数のシス

テム。たとえば、WebSphere 分散プラットフォーム上のクライアントは、WebSphere for z/OS 上のサーバーと相互協調処理を行います。

マイグレーション戦略の開発

WebSphere for z/OS の新しいリリースへマイグレーションするための推奨されるステップは、次のとおりです。

1. そのリリースのマイグレーションとインストールをサポートする資料を熟読します。

   IBM が提供する製品、システム・ライブラリー、および IBM 以外の製品に、どの更新が必要であるかを判別してください。WebSphere for z/OS については、210ページの『マイグレーション・ロードマップ』と 217ページの『マイグレーション・パスの概要』を検討してください。

2. インストール用のマイグレーション計画を作成します。

   新しいリリースの WebSphere for z/OS へのマイグレーションを計画する場合は、マシンとプログラミングの制約事項、マイグレーション・パス、およびプログラム互換性など、高レベルのサポート要件を考慮する必要があります。

3. 必要なプログラム一時修正 (PTF) または更新されたバージョンのオペレーティング・システムを入手し、インストールします。

   弊社ソフトウェア営業担当員に連絡し、WebSphere for z/OS の予防保守計画 (PSP) アップグレードを入手します。これには、WebSphere for z/OS 用の PTF に関する最新情報が記載されています。WebSphere for z/OS をテストする直前に、再度 RETAIN を検査します。予防保守計画については、*WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 を参照してください。*プログラム・ディレクトリー*に、必要な PTF のリストが入っていますが、最新情報は弊社ソフトウェア営業担当員にお問い合わせください。

4. *WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 または *ServerPac オーダーのインストール* の資料を使用して、製品をインストールします。

5. 55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』または 262ページの『コールド・スタート』の手順に従って、製品をカスタマイズします。

6. 使用しているインストールでアプリケーションの更新に責任を負うプログラマーに連絡します。

インストールのアプリケーションを引き続き実行できるかどうかを検証し、必要であれば、新しいリリースとの互換性を維持するための変更を加えます。

7. 使用しているアプリケーションのさまざまなマイグレーション方法から、いずれかを選択します。
8. 必要であれば、使用するインストール用に新しい機能をカスタマイズします。
9. 新しい機能を試してみます。

WebSphere for z/OS の処理に対する変更の検討

インストールのマイグレーション計画を決定するときに、新規および変更された WebSphere for z/OS サポートが WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があることを考慮してください。217ページの『マイグレーション・パスの概要』で述べる各項目について、『変更によって影響を受ける領域』と『マイグレーション手順』の項を検討し、使用するインストールで実行するタスクにこのサポートがどのように影響するか、または影響の有無を判別してください。

管理

管理者は、新しい製品リリースによって導入された変更が、インストールのデータ処理リソースにどのような影響を及ぼすかを認識しておく必要があります。実記憶域と仮想記憶域の要件、パフォーマンス、セキュリティー、および保全性に対する変更は、プログラムで使用されるコンピューター・システム・リソースについて決定を下す責任を負う管理者やシステム・プログラマーにとって、関心のある事項です。

アプリケーション開発

アプリケーション開発プログラマーは、WebSphere for z/OS の新しいリリースで導入された新機能を認識しておく必要があります。既存プログラムが以前のように動作するかどうか確認するために、アプリケーション・プログラマーはアプリケーション・プログラミング・インターフェースと処理要件の変更について知っておく必要があります。本書には、既存のアプリケーション・プログラムに影響を及ぼす可能性がある変更について、その概要が記載されています。

監査

一般に、監査担当者はインストールの適正なア

クセス制御と責任能力に責任を負っています。本書には、セキュリティー・オプション、監査レコード、およびレポート生成ユーティリティーに対する変更が示されています。

カスタマイズ

使用しているインストールの特定の要件を満たすために、製品をインストールした後、WebSphere for z/OS の機能をカスタマイズして、新しいサポートを利用できます。たとえば、WebSphere for z/OS を調整し、パフォーマンスを向上させることができます。本書には、使用しているインストールで製品を調整する必要がある WebSphere for z/OS への変更がリストされており、そのような調整によって、WebSphere for z/OS を以前と同様に動作させたり、インストールに必要となる新しいセキュリティー制御を使用できます。

一般ユーザー

本書には、一般ユーザー向けの既存の手順に影響を及ぼす可能性がある変更について、その概要が記載されています。

操作

新しい WebSphere for z/OS のリリースは、コマンドの変更、新規または変更されたメッセージ、または新しい機能をインプリメントする方法など、操作特性に変更をもたらす可能性があります。本書にはそれらの変更が示されており、それらの変更について、このリリースの製品を実行する前に、ユーザー研修を行ってください。

WebSphere for z/OS のインターフェースに対する変更の検討

使用しているインストールのマイグレーション計画を定義するときに、このリリースで導入される新しい機能または変更された機能によって、WebSphere for z/OS のインターフェースが影響を受ける可能性があることを考慮してください。それらのインターフェースは、次のとおりです。

- コマンド
- データベース・テンプレート
- メッセージ
- 画面
- SMF レコード
- ユーティリティー

276ページの『インターフェースの変更の要約』に、上に示したこのリリースのインターフェースに影響を及ぼす変更の要約が記載されています。この情報は、217ページの『マイグレーション・パスの概要』の各リリースの拡張機能について述べた『変更によって影響を受ける領域』の項にもリストされています。

マイグレーション・ロードマップ

ここでは、WebSphere for z/OS の現行リリースがサポートしているマイグレーション・パスについて説明します。また、WebSphere for z/OS の前のリリースからのマイグレーション情報を入手する方法についても説明します。

WebSphere for z/OS には次のリリースからマイグレーションできます。

- WebSphere Application Server スタンダード版 for OS/390 V3.02 (以後、『スタンダード版 V3.02』と呼びます)。
- WebSphere Application Server スタンダード版 for OS/390 V3.5 (以後、『スタンダード版 V3.5』と呼びます)。
- WebSphere Application Server エンタープライズ版 for OS/390 V3.02 (以後、『エンタープライズ版 V3.02』と呼びます)。

これ以外のプラットフォームから J2EE アプリケーションを WebSphere Application Server V4.0 for z/OS and OS/390 にマイグレーションすることもできます。

ここで示すロードマップには、それぞれのマイグレーションの概要が示されています。

スタンダード版 V3.02 または V3.5 から WebSphere for z/OS への要約

以下は、WebSphere for z/OS V4.0 で導入された更新の概要を示します。各項目の詳細を示した項の情報も検討してください。

スタンダード版 V3.02 とスタンダード版 V3.5 からのマイグレーションは、ほとんど同じですが、次の点が異なります。

- スタンダード版 V3.02 からマイグレーションする場合は、アプリケーションを直接 V4.0 へマイグレーションするか、いったんスタンダード版 V3.5 へマイグレーションしてから V4.0 へマイグレーションすることができます。V3.5 アプリケーションは V4.0 環境でも実行できますが、そのためには、V3.5 was.conf ファイルの完全修飾された名前を、ホストとなっている Web サーバーの httpd.conf 構成ファイルの中で、ServerInit ディレクティブの第 2 パラメーターとして指定する必要があります。

WebSphere Application Server スタンダード版 for OS/390 V3.5 へのマイグレーションの詳細については、*WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895 を参照してください。

- スタンダード版 V3.02 から WebSphere for z/OS へマイグレーションするには、Java 環境とアプリケーションを次のレベルへマイグレーションします。
  - JDK を更新して SDK 1.3 にします。
  - サーブレットを更新して Java サーブレット仕様 V2.2 にします。
  - JSP を更新して JavaServer Pages V1.1 仕様にします。
  - アプリケーションを .war ファイルとして再パッケージ化します。
- スタンダード版 V3.5 から WebSphere for z/OS V4.0 へマイグレーションするには、次のことを確認する必要があります。
  - サーブレットが Java サーブレット仕様 V2.2 に合わせて書かれている。
  - JSP が JavaServer Pages V1.1 仕様に合わせて書かれている。
  - アプリケーションが .war ファイルとしてパッケージ化されている。

参照情報	参照先
オペレーティング・システムとデータベースの要件	218ページの『オペレーティング・システムとデータベースの要件』
プロセス / 実行モデルの相違点	223ページの『プロセス / 実行モデルの相違点』
アプリケーションのアセンブリーと配置の相違点	226ページの『アプリケーションのアセンブリーと配置の相違点』
WebSphere HTTP セッション状態データベース・リポジトリー	229ページの『WebSphere HTTP セッション状態データベース・リポジトリー』
セキュリティー機構	231ページの『セキュリティー機構』
Common Connector Framework サポート	235ページの『Common Connector Framework サポート』
CICS へのアクセス	237ページの『CICS へのアクセス』
IMS へのアクセス	241ページの『IMS へのアクセス』

参照情報	参照先
JDBC による DB2 for OS/390 へのアクセス	245ページの『JDBC V2.0 Standard Extension DataSource API による DB2 for OS/390 へのアクセス』
WebSphere for z/OS へのアプリケーションのマイグレーション	251ページの『WebSphere for z/OS へのアプリケーションのマイグレーション』
JRas サポート	254ページの『JRas サポート』
JVM プロパティー	278ページの『JVM プロパティーの変更』

エンタープライズ版 V3.02 から WebSphere for z/OS への要約

以下は、WebSphere for z/OS で導入された更新の概要を示します。エンタープライズ版 V3.02 システムからマイグレーションする場合は、各項目の詳細を示した項の情報を検討する必要があります。

参照情報	参照先
基本オペレーティング・システムとデータベースの要件	258ページの『オペレーティング・システムとデータベースの要件』
システムのコールド・スタート	262ページの『コールド・スタート』
システム管理スクリプト API	271ページの『システム管理スクリプト API』
JRas サポート	273ページの『JRas サポート』
メッセージ	279ページの『メッセージ、コード、および異常終了』

SE V3.02、SE V3.5、および V4.0 J2EE サーバーの特性の要約

表18 は、WebSphere Application Server for OS/390 および WebSphere for z/OS の各リリースについて、J2EE サーバーの特性を要約したものです。

表 18. SE V3.02、SE V3.5、および V4.0 J2EE サーバーの特性の要約

特性	SE V3.02	SE V3.5	V4.0
最小システム要件			

表 18. SE V3.02、SE V3.5、および V4.0 J2EE サーバーの特性の要約 (続き)

特性	SE V3.02	SE V3.5	V4.0
オペレーティング・システム	• z/OS V1R1、または • OS/390 または z/OS V2R7 以上	• z/OS V1R1、または • OS/390 または z/OS V2R8 以上	• z/OS V1R1、または • OS/390 または z/OS V2R8 以上
システム構成	OS/390 または z/OS HTTP サーバー	OS/390 または z/OS HTTP サーバー	• OS/390 または z/OS HTTP サーバー • シスプレックス (モノプレックス最小) • ゴール・モードでのワークロード管理 • RRS • システム・ロガー • LDAP • DB2 for OS/390 V7.1
ソフトウェア開発キット (SDK)	Sun または IBM JDK 1.1.8	IBM Java 2 Standard Edition (J2SE) V1.3 for OS/390	IBM Java 2 Standard Edition (J2SE) V1.3 for OS/390
プロセス / 実行モデル	Go Web Server (GWAPI) プラグイン・ルーチンを提供します。相違点の詳細については、223ページの『プロセス / 実行モデルの相違点』を参照してください。	Go Web Server (GWAPI) プラグイン・ルーチンを提供します。相違点の詳細については、223ページの『プロセス / 実行モデルの相違点』を参照してください。	J2EE サーバーは Web コンテナーを含んでいます。

表 18. SE V3.02、SE V3.5、および V4.0 J2EE サーバーの特性の要約 (続き)

特性	SE V3.02	SE V3.5	V4.0
WebSphere 管理データベース	データベースは必要ありません。 サーバー構成は、構成ファイルで提供されます。 サーバー操作は、HTTP サーバー機能を介して行われます。	データベースは必要ありません。 サーバー構成は、構成ファイルで提供されます。 サーバー操作は、HTTP サーバー機能を介して行われます。	管理データベースは、常駐している必要があり、DB2 V7.1 の中でアクセスされる必要があります。 J2EE サーバーおよびシステム・サーバーの構成と管理のために、管理アプリケーションが提供されます。 Web 要求を J2EE サーバーへ経路指定するよう構成されている HTTP サーバーは、既存の HTTP サーバー機能を使用して管理されます。
アプリケーションのアセンブリーと配置	Web アプリケーションの概念がサポートされます。226ページの『アプリケーションのアセンブリーと配置の相違点』を参照してください。	Web アプリケーションの概念がサポートされます。226ページの『アプリケーションのアセンブリーと配置の相違点』を参照してください。	WebSphere for z/OS は、エンタープライズ・アプリケーションを Enterprise archive (.ear) ファイルの形で受け入れます。
WebSphere HTTP セッション状態データベース・リポジトリー	データベースは DB2 for OS/390 V5 (PTF 付き) または V6 (PTF 付き) の中に存在していなければなりません。229ページの『WebSphere HTTP セッション状態データベース・リポジトリー』を参照してください。	データベースは DB2 for OS/390 V5 (PTF 付き) または V6 (PTF 付き) の中に存在していなければなりません。229ページの『WebSphere HTTP セッション状態データベース・リポジトリー』を参照してください。	データベースは DB2 for OS/390 V7.1 の中に存在していなければなりません。

表 18. SE V3.02、SE V3.5、および V4.0 J2EE サーバーの特性の要約 (続き)

特性	SE V3.02	SE V3.5	V4.0
セキュリティー機構	SAF ベースのローカル OS。231ページの『セキュリティー機構』を参照してください。	SAF ベースのローカル OS。231ページの『セキュリティー機構』を参照してください。	SAF ベースのローカル OS。
Common Connector Framework (CCF) サポート	IBM Common Connector Framework V1.1 に準拠。最低限の品質のサービスとランタイム統合が提供されます。235ページの『Common Connector Framework サポート』を参照してください。	IBM Common Connector Framework V1.1 に準拠。最低限の品質のサービスとランタイム統合が提供されます。235ページの『Common Connector Framework サポート』を参照してください。	IBM Common Connector Framework V1.1 に準拠。最低限の品質のサービスとランタイム統合が提供されます。
CICS へのアクセス	CICS Transaction Gateway (CTG) 製品 (5648-B43) は CCF ベースのコネクターを提供し、これを使用して、CommArea ベースの CICS トランザクション・プログラムにアクセスできます。237ページの『CICS へのアクセス』を参照してください。	CICS Transaction Gateway (CTG) 製品 V4.0 は CCF ベースのコネクターを提供し、これを使用して、CommArea ベースの CICS トランザクション・プログラムにアクセスできます。237ページの『CICS へのアクセス』を参照してください。	CICS Transaction Gateway (CTG) 製品 V4.0 は CCF ベースのコネクターを提供し、これを使用して、CommArea ベースの CICS トランザクション・プログラムにアクセスできます。
IMS へのアクセス	IMS Connect (5655-E51) は CCF ベースのコネクターを提供し、これを使用して、IMS トランザクション・プログラムにアクセスできます。241ページの『IMS へのアクセス』を参照してください。	詳細については、241ページの『IMS へのアクセス』を参照してください。	

表 18. SE V3.02、SE V3.5、および V4.0 J2EE サーバーの特性の要約 (続き)

特性	SE V3.02	SE V3.5	V4.0
JDBC V2.0 Standard Extension DataSource API による DB2/ESA アクセス	データベースは、V5 レベル (PTF 付き) または V6 レベル (PTF 付き) の DB2 サブシステム内に存在していなければなりません。詳細については、245 ページの『JDBC V2.0 Standard Extension DataSource API による DB2 for OS/390 へのアクセス』を参照してください。	データベースは、V5 レベル (PTF 付き) または V6 レベル (PTF 付き) の DB2 サブシステム内に存在していなければなりません。詳細については、245 ページの『JDBC V2.0 Standard Extension DataSource API による DB2 for OS/390 へのアクセス』を参照してください。	DB2 V7.1

マイグレーション・パスの概要

スタンダード版 V3.02 または V3.5 から WebSphere for z/OS への概要

以下の項では、WebSphere for z/OS の新機能と変更された機能について説明します。

- 説明
- 影響を受ける可能性がある WebSphere for z/OS のタスクまたはインターフェースの要約
- その項目に関連した共存に関する考慮事項
- その項目に関連したマイグレーション手順
- 追加の詳細情報が記載されているその他の資料

オペレーティング・システムとデータベースの要件

説明: ここでは、マイグレーションに影響を及ぼすオペレーティング・システムとデータベースの新規要件について説明します。サーブレットと JSP の WebSphere for z/OS へのマイグレーションについては、251ページの『WebSphere for z/OS へのアプリケーションのマイグレーション』を参照してください。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	なし
監査	なし
カスタマイズ	221ページの『マイグレーション・タスク』を参照してください。
一般ユーザー	なし
操作	サーバーを実行するための新規の操作手順。*WebSphere Application Server V4.0 for z/OS and OS/390: 操作および管理*, SA88-8653 を参照してください。
インターフェース	なし

依存関係: WebSphere for z/OS の要件の完全なリストについては、10ページの『WebSphere for z/OS のシステム要件の決定』を参照してください。

依存に関する考慮事項: 以下は、J2EE ランタイムによってもたらされる互換性と共存に関する事項です。

- スタンダード版 V3.02 または V3.5 システムは、同じシステムまたはシスプレックス上で WebSphere for z/OS と共存できます。ただし、マウント・ポイントが異なっていなければなりません (両方の製品にデフォルトのマウント・ポイントを使用することはできません)。テストの目的で分離するために、別々のテスト・システムまたは LPAR を作成することもできます。
- ランタイムに DB2 for OS/390 V7.1 が必要です。以下の点を考慮してください。
  - DB2 for OS/390 V7.1 は、同じイメージ上にあり、固有のテスト・データを持つ旧 DB2 と共存できます。
  - DB2 for OS/390 V7.1 は、テスト・データにアクセスするために、旧 DB2 へ分散呼び出しを行うことができます。

– DB2 for OS/390 V7.1 は、テスト・データにアクセスするために、旧 DB2 とデータ共用を行うことができます。同じデータ共用グループに所属できるのは 2 つのレベルの DB2 for OS/390 だけである点に注意してください。データ共用を行う場合は、DB2 for OS/390 の互換性 APAR をインストールしなければなりません。

  推奨: DB2 for OS/390 の複数のリリース間でのデータ共用は、限られた時間枠だけにとどめてください。

220ページの図6 は、DB2 for OS/390 V7.1 へのマイグレーションが考えられる DB2 for OS/390 の各構成を示しています。

スタンダード版 V3.02 または V3.5

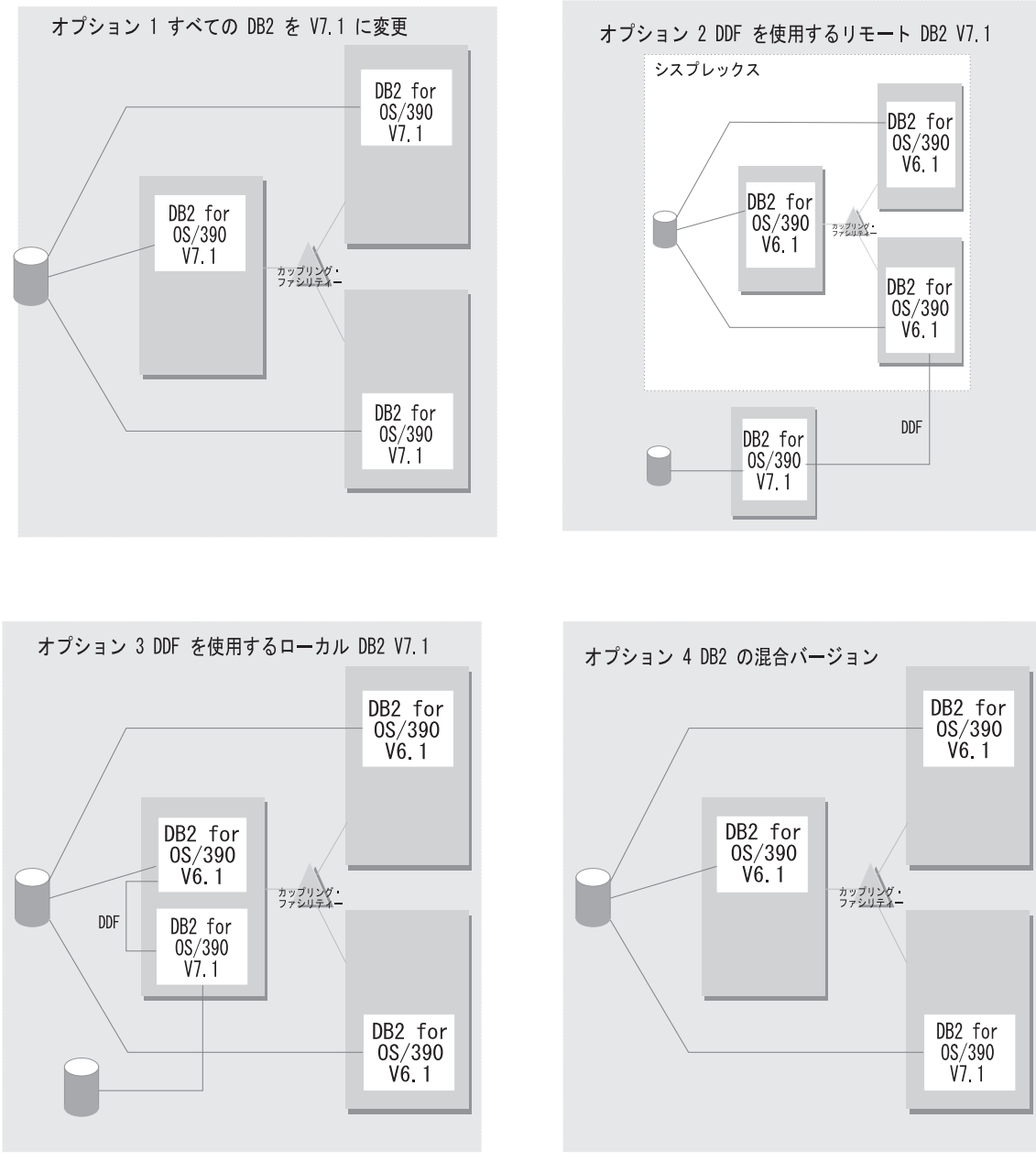


図 6. DB2 for OS/390 V7.1 へのマイグレーションが考えられる構成

- スタンダード版 V3.5 システムとの相互協調処理を行いたい場合は、V3.5 用の SDK に互換性 PTF をインストールしなければなりません。最新の PTF 情報は、PSP バケットを参照してください。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

タスク	条件	参照情報
必要であれば、ハードウェアをアップグレードする。S/390 並列エンタープライズ・サーバーの第 5 世代以降のシステムなど、バイナリー浮動小数点ハードウェアを備えたマシンであれば、浮動小数点数演算を行うアプリケーションでパフォーマンスが大幅に向上します。	強く推奨	
オペレーティング・システムをアップグレードする。WebSphere for z/OS は、OS/390 V2R8 以降または z/OS を必要とします。シスプレックス内にいる場合は、使用する OS/390 V2R8 システムがシスプレックス内にある別レベルの OS/390 または z/OS と共存しなければなりません。すべての OS/390 または z/OS イメージは N±4 リリースと共存できるので、OS/390 V2R8 システムは、古いものでは V2R5、新しいものでは V2R10 または z/OS と共存できます。	必須	*z/OS インストール計画*, GA88-8520
PTF をインストールする。PSP バケットで次のものに必要な PTF を調べてください。 • ワークロード管理 • RACF • LDAP • XML パーサー • SSL / セキュリティー • RRS • OS/390 または z/OS. シスプレックス内で稼働する各種リリースのオペレーティング・システムに必要な PTF を検討してください。	必須	PTF の添付資料

スタンダード版 V3.02 または V3.5

タスク	条件	参照情報
DB2 for OS/390 V7.1 へマイグレーションする。	必須	*DB2 リリースの手引き*, SC88-7383
WebSphere for z/OS をインストールおよびカスタマイズする。次のようなオペレーティング・システム要件があります。 • シスプレックス (最小: モノプレックス) • ゴール・モードでのワークロード管理 • RRS およびロガー • LDAP • FTP サーバー	必須	9ページの『第2章 OS/390 または z/OS の基本環境の準備』および 55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』

詳細情報: このサポートの詳細については、次の WebSphere for z/OS 資料を参照してください。

- *WebSphere Application Server V4.0 for z/OS and OS/390: インストールおよびカスタマイズ*, GA88-8652 (本書)
- *z/OS インストール計画*, GA88-8520
- *DB2 リリースの手引き*, SC88-7383
- *z/OS MVS 計画：ワークロード管理*, SA88-8574
- *z/OS MVS シスプレックスのセットアップ*, SA88-8591
- *z/OS MVS プログラミング：リソース・リカバリー*, SA88-8582
- *z/OS Communications Server: IP Configuration Guide*, SC31-8775

プロセス / 実行モデルの相違点

説明: この節では、WebSphere for z/OS のプロセス / 実行モデルと、Application Server のバージョン 3.02 および 3.5 のプロセス / 実行モデルを比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	アプリケーションのインストール・プロセスが変更されました。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	JVM を定義する方式が変更されました。
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、SE V3.02、SE V3.5、および V4.0 のプロセス / 実行モデルにおける相違点を要約したものです。

スタンダード版 V3.02 または V3.5

表 19. プロセス / 実行モデルの比較

SE V3.02	SE V3.5	V4.0
次のことができる Go Web Server (GWAPI) プラグイン・ルーチンを提供します。 • HTTP サーバーのアドレス・スペース内で、Java 1 ベース (JDK 1.1.8) の仮想マシンを初期化します。 • その JVM 内で、was.conf 構成ファイルで提供される構成データを使用して、WebSphere Application Server の Web コンテナーを初期化します。 • その Web コンテナーへ HTTP 要求を処理のために経路指定します。	次のことができる Go Web Server (GWAPI) プラグイン・ルーチンを提供します。 • HTTP サーバーのアドレス・スペース内で、Java 2 ベース (J2SE V1.3) の仮想マシンを初期化します。 • その JVM 内で、was.conf 構成ファイルで提供される構成データを使用して、WebSphere Application Server の Web コンテナーを初期化します。 • その Web コンテナーへ HTTP 要求を処理のために経路指定します。	J2EE サーバーは、デフォルトで Web コンテナーを含んでいます。 その Web コンテナーのプロパティーは、webcontainer.conf 構成ファイルに入っています。この構成ファイルは J2EE サーバーに環境変数として提供されます。 Web アプリケーションは、WebSphere V4.0 for z/Os and OS/390 システム管理機能によって J2EE サーバーにインストールされます。 WebSphere V4.0 プラグイン・ルーチンが入った 1 台以上の HTTP サーバーが、インストール済み Web アプリケーションが入った J2EE サーバーと同じシスプレックス内に構成されている必要があります。HTTP サーバーは Web クライアントからのトラフィックを処理します。 WebSphere for z/OS および Go Web Server (GWAPI) プラグイン・ルーチンでは、次の処理を行うことができます。 • HTTP サーバーのアドレス・スペース内で、Java 2 ベース (J2SE V1.3) の仮想マシンを初期化します。 • 同じシスプレックスの J2EE サーバー内にある Web コンテナーへ、要求を処理するために経路指定します。 このプラグイン・ルーチンには、J2EE サーバーとその構成の変更をリアルタイムで検出するロジックが含まれています。

表 19. プロセス / 実行モデルの比較 (続き)

SE V3.02	SE V3.5	V4.0
プラグイン・ルーチンは、HTTP サーバーの httpd.conf ファイルの中に ServerInit、Service、ServerTerm の各ディレクティブを追加することによって、HTTP サーバー・アドレス・スペースに対して構成されます。	プラグイン・ルーチンは、HTTP サーバーの httpd.conf ファイルの中に ServerInit、Service 、ServerTerm の各ディレクティブを追加することによって、HTTP サーバー・アドレス・スペースに対して構成されます。	プラグイン・ルーチンは、HTTP サーバーの httpd.conf ファイルに ServerInit、Service、ServerTerm の各ディレクティブを追加することによって、HTTP サーバー・アドレス・スペースに対して構成されます。
1 つの実行システムに、同時に複数の WebSphere Application Server スタンダード版製品レベルをインストールし、マウントすることができますが、1 つの Web サーバー・アドレス・スペースに対して構成できる WebSphere プラグイン・ルーチンは 1 つだけです。	1 つの実行システムに、同時に複数の WebSphere Application Server スタンダード版製品レベルをインストールし、マウントすることができますが、1 つの Web サーバー・アドレス・スペースに対して構成できる WebSphere プラグイン・ルーチンは 1 つだけです。	1 つの実行システムに、同時に複数の WebSphere Application Server スタンダード版製品レベルをインストールし、マウントすることができますが、1 つの Web サーバー・アドレス・スペースに対して構成できる WebSphere プラグイン・ルーチンは 1 つだけです。
管理者は、1 つのシステム上で同時に複数のレベルの WebSphere Application Server スタンダード版を実行する場合、別々の HTTP サーバー・アドレス・スペースの中でプラグイン・ルーチンを構成しなければなりません。	管理者は、1 つのシステム上で同時に複数のレベルの WebSphere Application Server スタンダード版を実行する場合、別々の HTTP サーバー・アドレス・スペースの中でプラグイン・ルーチンを構成しなければなりません。	管理者は、1 つのシステム上で同時に複数のレベルの WebSphere Application Server スタンダード版を実行する場合、別々の HTTP サーバー・アドレス・スペースの中でプラグイン・ルーチンを構成しなければなりません。

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

アプリケーションのアセンブリーと配置の相違点

説明: この節では、WebSphere for z/OS のアプリケーションのアセンブリーおよび配置プロセスと、Application Server バージョン 3.02 および 3.5 のアプリケーションのアセンブリーおよび配置プロセスを比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	アプリケーションのアセンブリーおよび配置プロセスが変更されました。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、スタンダード版 V3.02、SE V3.5、および WebSphere for z/OS V4.0 アプリケーションのアセンブリーおよび配置プロセスにおける相違点を要約したものです。

表 20. アプリケーションのアセンブリーと配置の比較

SE V3.02	SE V3.5	V4.0
Web アプリケーションの概念がサポートされます。Web アプリケーションの物理的プロパティー (HTML および JSP が格納されている HFS の文書ルート。サーブレットと Java bean のインプリメンテーションを見つけるための classpath) と、そのアドレス (そのホスト内の rootURI 指定) は、was.conf 構成ファイル内の **deployedwebapp** プロパティーで指定されます。 Web アプリケーションのプロパティー (サーブレット定義、init プロパティーなど) は、was.conf ファイル内の **webapp** プロパティーを使用して指定されます。または、Application Server の classpath 内に存在する別個の .webapp XML 文書として指定されます。この別個の文書構造を使用して、開発者はアプリケーションの前提事項を正式な方法で管理者に提供できます。	Web アプリケーションの概念がサポートされます。Web アプリケーションの物理的プロパティー (HTML および JSP が格納されている HFS の文書ルート。サーブレットと Java bean のインプリメンテーションを見つけるための classpath) と、そのアドレス (そのホスト内の rootURI 指定) は、was.conf 構成ファイル内の **deployedwebapp** プロパティーで指定されます。 Web アプリケーションのプロパティー (サーブレット定義、init プロパティーなど) は、was.conf ファイル内の **webapp** プロパティーを使用して指定されます。または、Application Server の classpath 内に存在する別個の .webapp XML 文書として指定されます。この別個の文書構造を使用して、開発者はアプリケーションの前提事項を正式な方法で管理者に提供できます。	WebSphere V4.0 for z/Os and OS/390 は、エンタープライズ・アプリケーションを Enterprise archive (.ear) ファイルの形で受け入れます。 .ear ファイルは、V4.0 に添付されたシステム管理アプリケーションへの入力として提供されます。管理アプリケーションは、リソース解決と物理ファイルのインストールも含め、アプリケーションの完全な配置を行うことができます。 .ear ファイルには、ゼロ個以上の Web アプリケーションを含めることができます。Web アプリケーションは、.ear ファイルの中に業界標準の .war ファイルとして存在します。アプリケーション・レベルの配置記述子を使用して、アプリケーション内の個々の .war ファイルに「コンテキスト・ルート」を割り当てることができます。このテキスト・ルートは、旧バージョンの Application Server で配置された Web アプリケーションに対する root.URI 指定と同等のものです。

表 20. アプリケーションのアセンブリーと配置の比較 (続き)

SE V3.02	SE V3.5	V4.0
仮想ホスト定義と、それによってサービスされる配置済み Web アプリケーションへのバインディングは、was.conf ファイル内の **host** プロパティーの中で指定されます。	仮想ホスト定義と、それによってサービスされる配置済み Web アプリケーションへのバインディングは、was.conf ファイル内の **host** プロパティーの中で指定されます。 WebSphere V3.5 スタンダード版は、業界標準の Web アプリケーション・アーカイブ (.war ファイル) から必要な配置情報 (was.conf ファイル用の deployedwebapp プロパティーである .webapp ファイル) を作成するユーティリティーも備えています。これにより、アプリケーション開発ツールを使用して開発され .war ファイル形式でパッケージ化されたアプリケーションを、簡単に Application Server の中に配置できます。 Web アプリケーションの配置記述子に入っている関数の完全セットは、WebSphere V3.5 ではサポートされません。	製品に添付されているアプリケーション組み立てツールを使用して、複数の Web アプリケーションをインポートし、1 つのエンタープライズ・アプリケーションにアセンブルすることができます。 アプリケーションを J2EE サーバーにインストールした後、webcontainer.conf ファイルの中で定義されている仮想ホストを通じて、そのアプリケーションを公開できます。

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

WebSphere HTTP セッション状態データベース・リポジトリー

説明: この節では、スタンダード版 V3.02、V3.5、および WebSphere for z/OS V4.0 で使用される WebSphere HTTP セッション状態データベース・リポジトリーを比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	セッション・データを格納するために使用される DB2 for OS/390 データベースは、異なる方法でセットアップされます。
アプリケーション開発	なし
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、セッション・データを格納する DB2 for OS/390 データベースのスタンダード版 V3.02、V3.5、および WebSphere for z/OS V4.0 の環境におけるセットアップ方法について、その相違点を要約したものです。

スタンダード版 V3.02 または V3.5

表 21. WebSphere HTTP セッション状態データベース・リポジトリーのセットアップの相違点

SE V3.02	SE V3.5	V4.0
パーシスタント HTTP セッション状態を使用する場合、DB2 for OS/390 データベースを *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895 で述べるように定義しなければなりません。	パーシスタント HTTP セッション状態を使用する場合は、DB2 for OS/390 データベースを *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895 で述べるように定義しなければなりません。	パーシスタント HTTP セッション状態を使用する場合は、DB2 データベースを *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 で述べるように定義しなければなりません。
データベースは、V5 レベル (PTF 付き) または V6 レベル (PTF 付き) の DB2 for OS/390 サブシステム内に存在していなければなりません。	データベースは、V5 レベル (PTF 付き) または V6 レベル (PTF 付き) の DB2 for OS/390 サブシステム内に存在していなければなりません。	データベースは、V7.1 レベルの DB2 サブシステム内に存在していなければなりません。
セッション状態データベースは、Websphere V3.02 スタンダード版 for OS/390、WebSphere V3.5 スタンダード版 for OS/390、および WebSphere V4.0 for z/OS and OS/390 の Web コンテナー間で並行して共用できます。	セッション状態データベースは、Websphere V3.02 スタンダード版 for OS/390、WebSphere V3.5 スタンダード版 for OS/390、および WebSphere V4.0 for z/OS and OS/390 の Web コンテナー間で並行して共用できます。	セッション状態データベースは、Websphere V3.02 スタンダード版 for OS/390、WebSphere V3.5 スタンダード版 for OS/390、および WebSphere V4.0 for z/OS and OS/390 の Web コンテナー間で並行して共用できます。

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

セキュリティー機構

説明: この節では、スタンダード版 V3.02、V3.5、および WebSphere for z/OS V4.0 のセキュリティー機構を比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	セキュリティーの相違点
アプリケーション開発	なし
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、SE V3.02、SE V3.5、および V4.0 環境でのセキュリティー処理の相違点を要約したものです。

表 22. セキュリティー・メカニズムの比較

SE V3.02	SE V3.5	V4.0
SAF ベースの LocalOS。	SAF ベースの LocalOS。	SAF ベースの LocalOS。
ユーザー・レジストリー: ユーザーは、オペレーティング・システムの SAF リポジトリーで定義されます。	**ユーザー・レジストリー:** ユーザーは、オペレーティング・システムの SAF リポジトリーで定義されます。	**ユーザー・レジストリー:** ユーザーは、オペレーティング・システムの SAF リポジトリーで定義されます。

表 22. セキュリティー・メカニズムの比較 (続き)

SE V3.02	SE V3.5	V4.0
認証のためのユーザー確認機構: HTTP 基本認証 - HTTP 基本認証によって、ユーザーに確認のためのユーザー ID とパスワードを提供させることができます。 HTTPS SSL 接続を通じてクライアント証明書が提供されます。クライアント証明書は、SAF ユーザー・レジストリー内でユーザー ID へ解決されなければなりません。 ユーザー確認機構は、httpd.conf ファイル内の HTTP サーバー保護ディレクティブを介して構成されます。	**認証のためのユーザー確認機構:** HTTP 基本認証 - HTTP 基本認証によって、ユーザーに確認のためのユーザー ID とパスワードを提供させることができます。 HTTPS SSL 接続を通じてクライアント証明書が提供されます。クライアント証明書は、SAF ユーザー・レジストリー内でユーザー ID へ解決されなければなりません。 ユーザー確認機構は、httpd.conf ファイル内の HTTP サーバー保護ディレクティブを介して構成されます。	**認証のためのユーザー確認機構:** HTTP 基本認証 - HTTP 基本認証によって、ユーザーに確認のためのユーザー ID とパスワードを提供させることができます。 HTTPS SSL 接続を通じてクライアント証明書が提供されます。クライアント証明書は、SAF ユーザー・レジストリー内でユーザー ID へ解決されなければなりません。 ユーザー ID とパスワードは、サーブレット V2.2 仕様で規定されているように、フォーム・ベースのログインを介して入手できます。 Web アプリケーションのコンポーネントのユーザー確認機構は、配置された Web アプリケーションの一部である .webapp ファイル内の情報を介して構成できます。 ユーザー確認機構は、httpd.conf ファイル内の HTTP サーバー保護ディレクティブを介して構成できます。
URL アクセス検査: 認証された ID を使用して、URL アクセス検査を行うことができます。これらの検査は、httpd.conf ファイル内の HTTP サーバー保護ディレクティブを介して構成できます。	**URL アクセス検査:** 認証された ID を使用して、URL アクセス検査を行うことができます。これらの検査は、httpd.conf ファイル内の HTTP サーバー保護ディレクティブを介して構成できます。	**URL アクセス検査:** 認証された ID を使用して、URL アクセス検査を行うことができます。これらの検査は、httpd.conf ファイル内の HTTP サーバー保護ディレクティブを介して構成できます。

表 22. セキュリティー・メカニズムの比較 (続き)

SE V3.02	SE V3.5	V4.0
実行 ID (オペレーティング・システム): 要求を実行するシステム ID は、HTTP サーバー内の保護ディレクティブによって決定されます。厳密に言えば、HTTP サーバー認証プロセスの結果として生じた ID を表す ACEE が、実行スレッド上に存在します。	**実行 ID (オペレーティング・システム):** 要求を実行するシステム ID は、HTTP サーバー内の保護ディレクティブによって決定されます。厳密に言えば、HTTP サーバー認証プロセスの結果として生じた ID を表す ACEE が、実行スレッド上に存在します。	**実行 ID (オペレーティング・システム):** V4.0 Web コンテナーの内部にあるすべての要求は、HTTP サーバーのシステム ID と同じシステム ID を使用して実行されます。特に、サーブレットまたは JSP (JavaServer Pages) などの Web コンポーネントの内部での実行中に、リクエスターを表す ACEE は実行スレッド上に存在しません。
実行 ID (J2EE): サーブレット仕様で義務付けられているように、WebSphere はリクエスターに関する情報を保守し、実行時に Web コンポーネントが使用できるようにします。特に、入力要求オブジェクトに対する API が提供され、サーブレットはそれらの API を使用して、要求のサブジェクトに関する情報、たとえば、X509 証明書に入っている情報やユーザー ID などを取り出すことができます。 J2EE サービス、たとえば JDBC コネクターや Java 2 コネクターは、リクエスターに関する正しい情報を実行時に入手し、サービス・レベルのセキュリティー検査に使用できます。	**実行 ID (J2EE):** サーブレット仕様で義務付けられているように、WebSphere はリクエスターに関する情報を保守し、実行時に Web コンポーネントが使用できるようにします。特に、入力要求オブジェクトに対する API が提供され、サーブレットはそれらの API を使用して、要求のサブジェクトに関する情報、たとえば、X509 証明書に入っている情報やユーザー ID などを取り出すことができます。 J2EE サービス、たとえば JDBC コネクターや Java 2 コネクターは、リクエスターに関する正しい情報を実行時に入手し、サービス・レベルのセキュリティー検査に使用できます。	**実行 ID (J2EE):** サーブレット仕様で義務付けられているように、WebSphere はリクエスターに関する情報を保守し、実行時に Web コンポーネントが使用できるようにします。特に、入力要求オブジェクトに対する API が提供され、サーブレットはそれらの API を使用して、要求のサブジェクトに関する情報、たとえば、X509 証明書に入っている情報やユーザー ID などを取り出すことができます。 J2EE サービス、たとえば JDBC コネクターや Java 2 コネクターは、リクエスターに関する正しい情報を実行時に入手し、サービス・レベルのセキュリティー検査に使用できます。
WebSphere アクセス制御検査: WebSphere は、SOMDOBJ 機能クラス内のリソースに対して SAF 検査を行います。どのリソースを検査するかの定義は、スタンダード版構成ファイルの was.conf の中で構成ディレクティブとして提供されます。	**WebSphere アクセス制御検査:** WebSphere は、SOMDOBJ 機能クラス内のリソースに対して SAF 検査を行います。どのリソースを検査するかの定義は、スタンダード版構成ファイルの was.conf の中で構成ディレクティブとして提供されます。	**WebSphere アクセス制御検査:** Web コンポーネントへのアクセスについてのアクセス制御検査は、要求のサブジェクトである役割に基づいて行うことができます。

表 22. セキュリティー・メカニズムの比較 (続き)

SE V3.02	SE V3.5	V4.0
シングル・サインオン機能: WebSphere V3.02 スタンダード版は、この機能をサポートしません。	**シングル・サインオン機能:** WebSphere V3.02 スタンダード版は、この機能をサポートしません。	**シングル・サインオン機能:** Web アプリケーションへのシングル・サインオンは、サーブレット V2.2 仕様の記述のとおりにサポートされます。
推奨と使用法: 認証は、HTTP サーバーが行わなければなりません。許可検査は、HTTP サーバー保護ディレクティブか was.conf ファイルのプロパティー、またはその両方によって行うことができます。	**推奨と使用法:** 認証は、HTTP サーバーが行わなければなりません。許可検査は、HTTP サーバー保護ディレクティブか was.conf ファイルのプロパティー、またはその両方によって行うことができます。	**推奨と使用法:** 管理者は、J2EE によって規定されている配置機能を利用することをお勧めします。特に、Web アプリケーションと一緒にパッケージ化されている配置記述子を、認証と権限の検査の基礎とすることを強くお勧めします。 HTTP サーバー内で構成されているセキュリティー処理は、WebSphere V4.0 に入る前に実行されます。これは独立した一連の処理であり、WebSphere の処理に影響を及ぼしません。 管理者は、J2EE サーバーの使用へ移行するときに、既存の保護ディレクティブを HTTP サーバーの中にそのまま残してもかまいません。その後、Web 配置記述子の中で指定されている冗長な処理 (たとえば、認証など) を行うときに、それらのステートメントを HTTP サーバーの httpd.conf ファイルから除去することをお勧めします。

詳細情報: このサポートの詳細については、次の資料を参照してください。

- 19ページの『セキュリティーのセットアップ』
- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

Common Connector Framework サポート

説明: この節では、Commone Connector Framework サポートについて説明します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	なし
監査	なし
カスタマイズ	236ページの『マイグレーション・タスク』を参照してください。
一般ユーザー	なし
操作	なし
インターフェース	236ページの『マイグレーション・タスク』を参照してください。

依存関係: 236ページの『マイグレーション・タスク』を参照してください。

依存に関する考慮事項: 236ページの『マイグレーション・タスク』を参照してください。

マイグレーション・タスク:

表 23. Common Connector Framework の比較

SE V3.02	SE V3.5	V4.0
IBM Common Connector Framework V1.1 に準拠。	IBM Common Connector Framework V1.1 に準拠。	IBM Common Connector Framework V1.1 に準拠。
最低限の品質のサービスとランタイム統合が提供されます。CCF コネクター・サポートは、ユーザー・トランザクションを認識する設定にはなっていません。	最低限の品質のサービスとランタイム統合が提供されます。CCF コネクター・サポートは、ユーザー・トランザクションを認識する設定にはなっていません。	最低限の品質のサービスとランタイム統合が提供されます。CCF コネクター・サポートは、ユーザー・トランザクションを認識する設定にはなっていません。
コネクターは、そのインプリメンテーション・ファイルを Application Server の classpath にインストールすることによって、ランタイムに対して構成されます。	コネクターは、そのインプリメンテーション・ファイルを Application Server の classpath にインストールすることによって、ランタイムに対して構成されます。	コネクターは、そのインプリメンテーション・ファイルを Application Server の classpath にインストールすることによって、ランタイムに対して構成されます。
クライアント・プログラムは、ランタイムが提供する CCF コネクション・ファクトリーへの静的アクセスを介して、コネクターへのアクセスを取得します。	クライアント・プログラムは、ランタイムが提供する CCF コネクション・ファクトリーへの静的アクセスを介してコネクターへのアクセスを取得します。	クライアント・プログラムは、ランタイムが提供する CCF コネクション・ファクトリーへの静的アクセスを介してコネクターへのアクセスを取得します。
推奨と使用法: CCF コネクター・サポートは、Web コンポーネント用にのみ提供されます。これは、既存の WebSphere Application Server スタンダード版 for OS/390 のお客様向けのマイグレーション・エイドとして意図されています。WebSphere V4.0 for z/OS and OS/390 J2EE サーバー内では、これらのコネクター用にそれ以上の品質のサービスは提供されません。お客様は、Javasoft 準拠 J2C コネクターが使用可能になったときに、それらのコネクターを使用するために移行を開始することをお勧めします。		

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

CICS へのアクセス

説明: この節では、スタンダード版 V3.02、V3.5、および WebSphere for z/OS V4.0 での CICS へのアクセス方法を比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	238ページの表24を参照してください。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、SE V3.02、SE V3.5、および V4.0 環境での CICS へのアクセス方法を要約したものです。

スタンダード版 V3.02 または V3.5

表 24. CICS へのアクセスの比較

SE V3.02	SE V3.5	V4.0
CICS Transaction Gateway (CTG) 製品 (5648-B43) は CCF ベースのコネクターを提供し、これを使用して、CommArea ベースの CICS トランザクション・プログラムにアクセスできます。 このコネクターは、スタンダード版ランタイム内で使用した場合には、トランザクションを認識しません。 このコネクターは、CICS トランザクションに対するアクセス制御検査を実行するために、実行スレッド上のシステム ID (ACEE) を利用します。このシステム ID は、HTTP 保護ディレクティブを介した Web コンポーネントへのアクセス用に構成された認証プロセスの結果です。	CICS Transaction Gateway (CTG) 製品 V4.0 は CCF ベースのコネクターを提供し、これを使用して、CommArea ベースの CICS トランザクション・プログラムにアクセスできます。 このコネクターは、スタンダード版ランタイム内で使用した場合には、トランザクションを認識しません。 このコネクターは、CICS トランザクションに対するアクセス制御検査を実行するために、実行スレッド上のシステム ID (ACEE) を利用します。このシステム ID は、HTTP 保護ディレクティブを介した Web コンポーネントへのアクセス用に構成された認証プロセスの結果です。	CICS Transaction Gateway (CTG) 製品 V4.0 は CCF ベースのコネクターを提供し、これを使用して、CommArea ベースの CICS トランザクション・プログラムにアクセスできます。 このコネクター・インプリメンテーションは、J2EE サーバー・ランタイム内で使用した場合には、トランザクションを認識しません。 このコネクターは、CICS トランザクションに対するアクセス制御検査を実行するために、実行スレッド上のシステム ID (ACEE) を利用します。V4.0 Web コンテナー内のすべての要求は、サーバーのシステム ID と同じシステム ID を使用して実行されます。このことは、このコンテナーが許可検査に使用する ID は、このコネクターを実行しているサーバー・アドレス・スペース (つまり、J2EE サーバー) の ID になることを意味しています。

表 24. CICS へのアクセスの比較 (続き)

SE V3.02	SE V3.5	V4.0
推奨と使用法: クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。また、HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。 この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルに Application Server インスタンスからのアクセス制御だけを許可させることができます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。	**推奨と使用法:** クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。また、HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。 この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルに Application Server インスタンスからのアクセス制御だけを許可させることができます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。	**推奨と使用法:** クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。WebSphere V4.0 J2EE ランタイム内のすべての Web コンポーネントは、J2EE サーバーのシステム ID と同じシステム ID を使用して実行されます。 この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルに Application Server インスタンスからのアクセス制御だけを許可させることができます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 J2EE サーバーは、最小限のアクセス権限と特権を使用して構成できます。

詳細情報: このサポートの詳細については、次の資料を参照してください。

スタンダード版 V3.02 または V3.5

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

IMS へのアクセス

説明: この節では、スタンダード版 V3.02、V3.5、および WebSphere for z/OS V4.0 での IMS へのアクセス方法を比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	『依存に関する考慮事項』を参照してください。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、SE V3.02、SE V3.5、および V4.0 環境での IMS へのアクセス方法を要約したものです。

表 25. IMS へのアクセスの比較

SE V3.02	SE V3.5	V4.0
IMS Connect (5655-E51) は、IMS トランザクション・プログラムにアクセスできる CCF ベースのコネクターを提供します。このコネクターは、スタンダード版ランタイム内で使用した場合には、トランザクションを認識しません。このコネクターは、IMS トランザクションに対するアクセス制御検査を実行するために、実行スレッド上のシステム ID (ACEE) を利用します。このシステム ID は、HTTP 保護ディレクティブを介した Web コンポーネントへのアクセス用に構成された認証プロセスの結果です。	このコネクターは、スタンダード版ランタイム内で使用した場合には、ユーザー・トランザクションを認識しません。このコネクターは、IMS トランザクションに対するアクセス制御検査を実行するために、実行スレッド上のシステム ID (ACEE) を利用します。このシステム ID は、HTTP 保護ディレクティブを介した Web コンポーネントへのアクセス用に構成された認証プロセスの結果です。	このコネクターは、IMS トランザクションに対するアクセス制御検査を実行するために、実行スレッド上のシステム ID (ACEE) を利用します。V4.0 Web コンテナー内のすべての要求は、サーバーのシステム ID と同じシステム ID を使用して実行されます。このことは、このコンテナーが許可検査に使用する ID は、このコネクターを実行しているサーバー・アドレス・スペース (つまり、J2EE サーバー) の ID になることを意味しています。

表 25. IMS へのアクセスの比較 (続き)

SE V3.02	SE V3.5	V4.0
推奨と使用法: クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。 HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。 この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルに Application Server インスタンスからのアクセス制御だけを許可させることができます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。	**推奨と使用法:** クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。 HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。 この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルに Application Server インスタンスからのアクセス制御だけを許可させることができます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。	**推奨と使用法:** クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。 HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。 この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルに Application Server インスタンスからのアクセス制御だけを許可させることができます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 J2EE サーバーは、最小限のアクセス権限と特権を使用して構成できます。

表 25. IMS へのアクセスの比較 (続き)

SE V3.02	SE V3.5	V4.0
必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。	必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。	

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895
- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

JDBC V2.0 Standard Extension DataSource API による DB2 for OS/390 へのアクセス

説明: この節では、スタンダード版 V3.02、V3.5、および WebSphere for z/OS V4.0 の JDBC V2.0 Standard Extension DataSource API による DB2 for OS/390 へのアクセス方法を比較します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	DB2 表の変更が必要になる場合があります。
アプリケーション開発	なし
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: スタンダード版 V3.02、V3.5、および WebSphere for z/OS 4.0 J2EE サーバーの特性の完全なリスト (マイグレーション用) については、212 ページの表18 を参照してください。

依存に関する考慮事項: 次の表は、SE V3.02、SE V3.5、および V4.0 環境での JDBC V2.0 Standard Extension DataSource API による DB2/ESA へのアクセス方法を要約したものです。

スタンダード版 V3.02 または V3.5

表 26. JDBC による DB2 for OS/390 へのアクセスの比較

SE V3.02	SE V3.5	V4.0
was.conf ファイル内のディレクティブを使用して、データベース接続プールを構成できます。プールの構成には、最小および最大接続数、アイドル接続タイムアウト、接続のファクトリーとして使用するデータベース・ドライバーの名前などが含まれます。	was.conf ファイル内のディレクティブを使用して、データベース接続プールを構成できます。プールの構成には、最小および最大接続数、アイドル接続タイムアウト、接続のファクトリーとして使用するデータベース・ドライバーの名前などが含まれます。	WebSphere Application Server V4.0 for z/Os and OS/390 では、システム管理ユーティリティーを使用してデータ・ソースを構成する必要があります。 WebSphere for z/OS では、システム管理ユーティリティーを使用してデータ・ソースを構成する必要があります。 JDBC を利用したい Web アプリケーションには、JDBC がアクセス対象の外部リソースであることを示す配置記述子を組み込む必要があります。

表 26. JDBC による DB2 for OS/390 へのアクセスの比較 (続き)

SE V3.02	SE V3.5	V4.0
物理プール特性に加えて、JDBC の取得と解放に使用できるデータ・ソース・オブジェクトの JNDI 名も指定できます。 アプリケーションの実行時に、構成済みの JNDI 名を介してデータ・ソースへの参照を取得できます。JNDI ネーム・スペースへのアクセスを取得するための初期コンテキスト・ファクトリーは、com.ibm.ejs.ns.jndi.CNInitialContextFactory クラスを介して提供されます。ネーム・スペースから戻されたデータ・ソース・インプリメンテーションには、次のメソッドのインプリメンテーションが入っています。 • getConnection(userid,Password) • getConnection() データ・ソースの getConnection メソッドへ有効なユーザー ID とパスワードを明示的に提供した場合、戻された JDBC ハンドルは、入力したユーザー ID が表すシステム ID と同じ 1 次許可 ID を使用して確立されています。この 1 次許可 ID は、データベース・アクセスの検査に使用されます。	物理プール特性に加えて、JDBC の取得と解放に使用できるデータ・ソース・オブジェクトの JNDI 名も指定できます。 アプリケーションの実行時に、構成済みの JNDI 名を介してデータ・ソースへの参照を取得できます。JNDI ネーム・スペースへのアクセスを取得するための初期コンテキスト・ファクトリーは、com.ibm.ejs.ns.jndi.CNInitialContextFactory クラスを介して提供されます。ネーム・スペースから戻されたデータ・ソース・インプリメンテーションには、次のメソッドのインプリメンテーションが入っています。 • getConnection(userid,Password) • getConnection() データ・ソースの getConnection メソッドへ有効なユーザー ID とパスワードを明示的に提供した場合、戻された JDBC ハンドルは、入力したユーザー ID が表すシステム ID と同じ 1 次許可 ID を使用して確立されています。この 1 次許可 ID は、データベース・アクセスの検査に使用されます。	アプリケーション配置の一部として、システム管理アプリケーションは、J2EE のプログラミング技法を使用した Web コンポーネントが実行時にデータ・ソースを見つけることができるよう、参照を解決し、ネーム・スペースを確立します。 com.ibm.ejs.ns.jndi.CNInitialContextFactory クラスは、J2EE ランタイム内ではアプリケーション用に提供されません。ネーム・スペースから戻されたデータ・ソース・インプリメンテーションには、次のメソッドのインプリメンテーションが入っています。 • getConnection(userid,Password) • getConnection() データ・ソースの getConnection メソッドへ有効なユーザー ID とパスワードを明示的に提供した場合、戻された JDBC ハンドルは、入力したユーザー ID が表すシステム ID と同じ 1 次許可 ID を使用して確立されています。この 1 次許可 ID は、データベース・アクセスの検査に使用されます。

表 26. JDBC による DB2 for OS/390 へのアクセスの比較 (続き)

SE V3.02	SE V3.5	V4.0
入力パラメーターを指定せずに getConnection を実行した場合、結果としての JDBC ハンドルは、要求を実行している HTTP サーバー・プロセスのシステム ID と同じ 1 次許可 ID を使用して確立されます。	入力パラメーターを指定せずに getConnection を実行した場合、結果としての JDBC ハンドルは、要求を実行している HTTP サーバー・プロセスのシステム ID と同じ 1 次許可 ID を使用して確立されます。	入力パラメーターを指定せずに getConnection を実行した場合、結果としての JDBC ハンドルは、要求を実行している HTTP サーバー・プロセスのシステム ID と同じ 1 次許可 ID を使用して確立されます。
スタンダード版ランタイム内の JDBC 接続を、ユーザー・トランザクションと結合して使用することはできません。	スタンダード版ランタイム内の JDBC 接続を、ユーザー・トランザクションと結合して使用することはできません。	スタンダード版ランタイム内の JDBC 接続を、ユーザー・トランザクションと結合して使用することはできません。

表 26. JDBC による DB2 for OS/390 へのアクセスの比較 (続き)

SE V3.02	SE V3.5	V4.0
推奨と使用法: クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルは、Application Server インスタンスからのアクセス制御を許可するだけで済みます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。	**推奨と使用法:** クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルは、Application Server インスタンスからのアクセス制御を許可するだけで済みます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。	**推奨と使用法:** クライアント認証およびアクセス制御検査を、HTTP クライアントを介してアクセスされる Web コンポーネントに適用することをお勧めします。HTTP サーバーのシステム ID と同じシステム ID を使用して要求を実行することをお勧めします。このことは、要求を %%SERVER として実行できるようにする HTTP 保護ディレクティブを管理者が構成する必要があることを意味しています。この技法により、既存の CICS、IMS、DB2 などのシステム・リソースとファイルは、Application Server インスタンスからのアクセス制御を許可するだけで済みます。Application Server 自体には、アクセスされる外部コンポーネント (たとえば、サーブレットなどの Web コンポーネントを表す URL) に対するアクセス権限の管理、認証、および妥当性検査を行うためのポリシーとサポートが入っています。 必要な PTF がインストールされていれば、HTTP サーバーをそれ以上、UID=0 の UNIX システム・サービス ID を使用して構成する必要はありません。このことは、ユーザー・レベルのアクセス権限だけを提供する UID を使用して HTTP サーバーを構成できることを意味しています。

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server for OS/390 Application Server 計画、インストールおよび使用の手引き*, GD88-7895

- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

WebSphere for z/OS へのアプリケーションのマイグレーション

説明: オペレーティング・システムとサブシステムを必要なレベルと WebSphere for z/OS ランタイムへマイグレーションした後、アプリケーションをスタンダード版 V3.02 または V3.5 からマイグレーションしなければなりません。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	いくつかの新規タスクと、新規ツールの管理アプリケーションがあります。このツールは、アプリケーションをインストールするために使用します。V3.5 の was.conf ファイルの中で設定する必要があったプロパティーのほとんどは、管理アプリケーションによって処理されるようになりました。仮想ホストとセッション・トラッキングの構成設定の一部は、以前と同様に webcontainer.conf ファイルの中で指定する必要があります。*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 および *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 を参照してください。
アプリケーション開発	252ページの『マイグレーション・タスク』を参照してください。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	なし
インターフェース	Application Server プラグインのホストとなるすべての Web サーバーの httpd.conf 構成ファイルに、ServerInit、Service、および ServerTerm ディレクティブを追加し、それらの Web サーバーに、このプラグインの初期化、要求処理、および終了ルーチンのエントリー・ポイントを提供してください。前バージョンの Application Server 用の ServerInit、Service、ServerTerm ディレクティブがすでに httpd.conf ファイルに存在する場合は、それらを削除しなければなりません。*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

依存関係: このサポートに必要となる追加のハードウェアやソフトウェアはありません。

依存に関する考慮事項: スタンダード版 V3.5 アプリケーションは、WebSphere for z/OS サーバーと共存し、対話することができます。ただし、それらのアプリケーションに含まれているサーブレットが Java サーブレット V2.2 仕様レベルに合わせて書かれており、それらのアプリケーションに含まれている JSP が JSP V1.1 仕様レベルに合わせて書かれていなければなりません。さらに、アプリケーションは .war ファイルとしてパッケージ化されていなければなりません (http://www.javasoft.com の URL で Java サーブレット仕様 V2.2 を参照してください)。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

タスク	条件	参照情報
次のアプリケーション開発ツールをアップグレードする。 • VisualAge for Java 3.5 • Websphere Studio 3.5.2	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
これらのツールのどちらかを使用するか、手動で、アプリケーションを .war ファイルとして再パッケージ化する。	必須	WebSphere Studio の資料 http://www.javasoft.com の URL にある Java サーブレット仕様 V2.2
新規ツールのアプリケーション組み立てツールを使用して、アプリケーションのアセンブルと配置を行う。	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
JDBC レベルを 2.0 へマイグレーションする (1.x のままでもかまいません)。	オプション	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
J2EE リソースを事前構成する。	オプション (接続プール機能には必須)	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

タスク	条件	参照情報
アプリケーションを J2EE サーバーにインストールする。	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654

詳細情報: このサポートの詳細については、次の WebSphere for z/OS 資料を参照してください。

- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
- *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656

JRas サポート

説明: JRas サポートは、以下のように変更されました。
- 新規インターフェースにより、Java アプリケーションでメッセージ・ロガーまたはトレース・ロガーを取得できます。
- ランタイム環境変数でなく、ユーザー提供のトレース設定ファイルによって、トレース・データの収集を使用可能または使用不可にできます。
- メッセージの収集は、常に使用可能になっています。

変更によって影響を受ける領域: このサポートは、次の処理領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	Java アプリケーションについてトレース・データの収集を使用可能にするには、次のようにします。 • トレース設定ファイルを提供する。 • その設定ファイルを指すように、アプリケーション・サーバー・ランタイム環境変数を変更する。
アプリケーション開発	新規 Java アプリケーションの場合は、新規 JRas インターフェースを使用してメッセージ・ロガーとトレース・ロガーを取得します。以前のインターフェースは使用すべきではありませんが、現在それらのインターフェースを使用している Java アプリケーションを変更する必要はありません。詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 で Java アプリケーションのメッセージとトレース・データのロギングに関するトピックを参照してください。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	Java アプリケーションのメッセージまたはトレース・データは、エラー・ログか CTRACE データ・セット、またはその両方の中に現れる場合があります。また、メッセージの収集は常に使用可能にされているので、このサポートは、マスター・コンソール上のメッセージ・トラフィックを増加させる場合があります。
インターフェース	新規および変更されたインターフェースの詳細については、以下のトピックを参照してください。 • 277ページの『JRas サポート用のインターフェース』 • 278ページの『JVM プロパティーの変更』

依存関係: このサポートに関連したハードウェア、ソフトウェア、または機能の依存関係はありません。

依存に関する考慮事項: このサポートに関連した共存に関する考慮事項はありません。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

表 27. マイグレーション・タスク

タスク	条件	手順参照
新規 JRas インターフェースを使用するように Java アプリケーションを再コーディングする。	オプション	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
Java アプリケーションのメッセージとトレース要求をログに記録するよう、次のようにランタイム環境を準備する。 • トレース設定プロパティー・ファイルを作成する。 • アプリケーション・サーバー用の JVM プロパティー・ファイルを更新する。 既存アプリケーションで JRas サポートを使用する場合は必須。	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
アプリケーション・サーバー用の環境変数を更新し、古くなった JRas 変数を除去する。	オプション	

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
- *WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655

- 使用している WebSphere ワークステーションのインフォセンターに入っている JRas のトピック

エンタープライズ版 V3.02 から WebSphere for z/OS への概要

以下では、WebSphere for z/OS の新機能と変更された機能について説明します。

- 説明
- 影響を受ける可能性がある WebSphere for z/OS のタスクまたはインターフェースの要約
- その項目に関連した共存に関する考慮事項
- その項目に関連したマイグレーション・プロシージャー
- 追加の詳細情報が記載されているその他の資料

オペレーティング・システムとデータベースの要件

説明: ここでは、マイグレーションに影響を及ぼすオペレーティング・システムとデータベースの新規要件について説明します。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	なし
監査	なし
カスタマイズ	261ページの『マイグレーション・タスク』を参照してください。
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: WebSphere for z/OS の要件の完全なリストについては、10ページの『WebSphere for z/OS のシステム要件の決定』を参照してください。

依存に関する考慮事項: 以下は、統合ランタイムによってもたらされる互換性と共存に関する事項です。

- エンタープライズ版 V3.02 と WebSphere for z/OS を同じシステム上、または同じシスプレックス内に置くことはできません。実動システムの完全なミラーリングを行うテスト・システムをセットアップする場合は、テスト・システムと実動システムのイメージを分離する必要があります。
- ランタイム時に DB2 for OS/390 V7.1 が必要です。以下の点を考慮してください。
  - DB2 for OS/390 V7.1 は、同じイメージ上にあり、固有のテスト・データを持つ旧 DB2 と共存できます。
  - DB2 for OS/390 V7.1 は、旧 DB2 へ分散呼び出しを行ってテスト・データにアクセスすることができます。
  - DB2 for OS/390 V7.1 は、旧 DB2 とデータ共用を行ってテスト・データにアクセスできます。同じデータ共用グループに所属できるのは 2 つのレベルの DB2 for OS/390 だけである点に注意してください。データ共用を行う場合は、DB2 for OS/390 の互換性 APAR をインストールしなければなりません。

推奨: DB2 for OS/390 の複数のリリース間でのデータ共用は、限られた時間枠だけにとどめてください。

260ページの図7 は、DB2 for OS/390 V7.1 へのマイグレーションが考えられる DB2 for OS/390 の各構成を示しています。

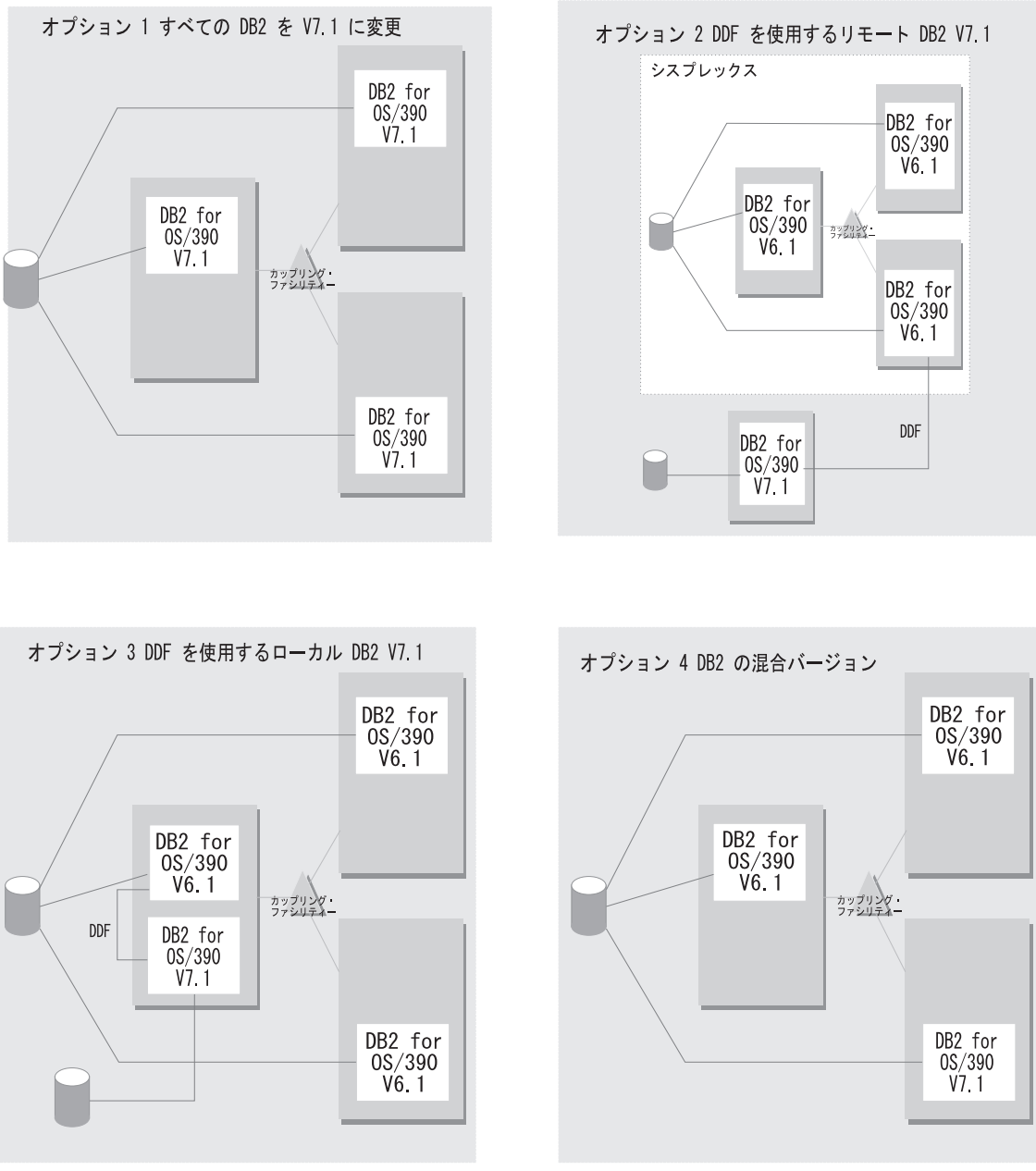


図 7. DB2 for OS/390 V7.1 へのマイグレーションが考えられる構成

- スタンダード版 V3.5 システムとの相互協調処理を行ないたい場合は、V3.5 用の SDK に互換性 PTF をインストールしなければなりません。最新の PTF 情報は、PSP バケットを参照してください。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

タスク	条件	参照情報
必要であれば、ハードウェアをアップグレードする。S/390 並列エンタープライズ・サーバーの第 5 世代以降のシステムなど、バイナリー浮動小数点ハードウェアを備えたマシンであれば、浮動小数点数演算を行うアプリケーションでパフォーマンスが大幅に向上します。	強く推奨	
DB2 for OS/390 V7.1 へマイグレーションする。	必須	*DB2 インストレーションの手引き*, GC88-7385
Java 1.1.8 JDK から 1.3 SDK へマイグレーションする。	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549

詳細情報: このサポートの詳細については、次の WebSphere for z/OS 資料を参照してください。

- *WebSphere Application Server V4.0 for z/OS and OS/390: インストールおよびカスタマイズ*, GA88-8652 (本書)
- *DB2 リリースの手引き*, SC88-7383

コールド・スタート

説明: エンタープライズ版 V3.02 から WebSphere Application Server V4.0 for z/OS and OS/390 へ移行するには、ランタイムを完全に置換する必要があります。次の作業を行わなければなりません。

- エンタープライズ版 V3.02 をコールド・スタート用に準備する。
- コールド・スタートの準備プロシージャーで生成された構成 XML ファイルを更新する。
- 各環境ファイルを更新して、Java SDK、DB2 for OS/390、LDAP、および CLASSPATH の新しい値を取得する。
- エンタープライズ版 V3.02 用の LDAP データベースを除去し、新しい V4.0 スキーマを使用して LDAP データベースを再作成する。
- V3.02 用のシステム管理データベースを除去し、新しい V4.0 スキーマを使用してシステム管理データベースを作成する。
- 更新した構成 XML ファイルを使用して WebSphere for z/OS V4.0 のコールド・スタートを実行する。

変更によって影響を受ける領域: このサポートは、WebSphere for z/OS 処理の次の領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	なし
アプリケーション開発	オブジェクト・ビルダー V3.5 を使用して、C++ Enterprise Edition V3.02 アプリケーションを再コンパイルしてください。Java BO アプリケーションをオブジェクト・ビルダー V3.5 で再コンパイルすることもできます。詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。
監査	なし
カスタマイズ	263ページの『マイグレーション・タスク』を参照してください。
一般ユーザー	なし
操作	なし
インターフェース	なし

依存関係: コールド・スタートには、ハードウェアとソフトウェアで追加の依存関係はありません。

依存に関する考慮事項: エンタープライズ版 V3.02 は、同じシステムまたは同じシスプレックス内の WebSphere Application Server V4.0 for z/OS and OS/390 とは共存できません。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

タスク	条件	参照情報
コールド・スタートの準備をする	必須	264ページの『システムのコールド・スタートを準備するステップ』
DB2 for OS/390 を V7.1 へマイグレーションする	必須	*DB2 インストレーションの手引き*, GC88-7385
SMP/E を通じて WebSphere for z/OS コードをインストールする	必須	265ページの『SMP/E を通じて WebSphere for z/OS コードをインストールするステップ』
システム管理 HFS 構造をアップグレードする	必須	266ページの『システム管理 HFS 構造をアップグレードするステップ』
コールド・スタートの XML 構成ファイルおよび環境ファイルをアップグレードする	必須	267ページの『XML 構成ファイルと環境ファイルをアップグレードするステップ』
システム管理データベースを再作成する	必須	269ページの『システム管理データベースを再作成するステップ』
LDAP データベースを再作成する	必須	269ページの『LDAP データベースを再作成するステップ』
WebSphere for z/OS ブートストラップを実行し、アプリケーション・サーバーを再初期化する	必須	269ページの『WebSphere for z/OS ブートストラップを実行し、アプリケーション・サーバーを再初期化するステップ』

弊社では、エンタープライズ版 V3.02 システムを WebSphere for z/OS へ移行するためのジョブと手順を提供しています。それらは次のとおりです。

- 管理アプリケーション。これを使用すると、現在の構成データを保管できます。
- BBOMMIG。使用している XML 構成ファイルと環境ファイルをアップグレードするジョブです。
- BBOMCRDB および BBOBIND。システムの初期のインストールとカスタマイズに使用するのと同じジョブです。

エンタープライズ版 V3.02 を復元する必要がある場合は、LDAP データベース、システム管理データベース、および V3.02 コードをバックアップしてください。詳しくは、285ページの『WebSphere for z/OS システムのバックアップのためのガイドライン』を参照してください。

システムのコールド・スタートを準備するステップ: この手順では、エンタープライズ版 V3.02 をコールド・スタート用に準備します。後で エンタープライズ版 V3.02 とすべてのアプリケーション・サーバーをシャットダウンするので、これらのステップは最も影響が少ないときに実行してください。

この作業を始める前に: 管理アプリケーションの V3.02 をインストールしておかなければなりません。

以下のステップを実行して、コールド・スタートを実行します。

1. 管理アプリケーションを開始し、ログインします。

---

2. 現在アクティブな会話をクリックし、「コールド・スタートの準備 (Prepare for cold start)」を選択します。

---

3. BBON0536I のメッセージに「はい (Yes)」と答えます。デーモン IP 名を変更**しない**でください。**結果:** 次のように表示されます。

---

4. すべてのアプリケーション・サーバーをシャットダウンします。**例:**

   ```
   C server_instance
   ```

   ここで、*server_instance* はサーバー・インスタンスの名前です。

---

5. シスプレックス内で実行されているすべてのデーモンをシャットダウンします。残っているエンタープライズ版 V3.02 アドレス・スペースがあれば、それらをキャンセルしてください。**例:**

   ```
   C DAEMON01
   ```

すべてのエンタープライズ版 V3.02 アドレス・スペースがキャンセルされると、このステップは完了です。

DB2 for OS/390 の V71 へのマイグレーション: WebSphere for z/OS は、実行時に DB2 for OS/390 V7.1 を必要とします。V7.1 へのマイグレーションについては、*DB2 インストレーションの手引き*, GC88-7385 を参照してください。

SMP/E を通じて WebSphere for z/OS コードをインストールするステップ:
この作業を始める前に: WebSphere for z/OS コードと *WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 が必要です。

以下のステップを実行して、コードをインストールします。

1. *WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 の説明に従って、WebSphere for z/OS コードをインストールします。

---

2. 新しい SDK をマウントします。

---

3. 69ページの『製品とともに提供されるファイルをコピーするためのステップ』で述べたように、製品に添付されているすべてのファイルをコピーします。

ファイルのコピーが終了すれば、このステップは完了です。

システム管理 HFS 構造をアップグレードするステップ: **この作業を始める前に:** HFS 構造と WebSphere for z/OS に必要な初期システム管理ファイルを作成したジョブ、BBOMCFG のコピーが必要です。

以下のステップを実行して、システム管理 HFS 構造をアップグレードします。

1. 88ページの『システム管理 HFS 構造を作成するためのステップ』の説明に従って、BBOMCFG ジョブを実行します。

   ---

2. SYSPRINT で BBOMCFG を検査します。

   ---

3. エンタープライズ版 V3.02 ベースの HFS マウント・ポイント (古い *TARGETDIR*) が /WebSphere390/CB390/controlinfo ならば、SYSPRINT に次のメッセージがあります。

   ```
   Existing environment files will be retained!
   Migrating existing files finished
   ```

   これらのメッセージがあれば、この手順は完了です。次の手順へ進んでください。

   ---

4. エンタープライズ版 V3.02 ベースの HFS マウント・ポイント (古い *TARGETDIR*) が /WebSphere390/CB390/controlinfo でない場合は、次のようにします。

   a. 次の表に従ってください。

エンタープライズ版 V3.02 からコピーするファイル	WebSphere for z/OS V4.0 でのコピー先
V3.02_TARGETDIR/configuration/ に入っている current.xml	*V4.0_TARGETDIR*/*SYSPLEX*/conversations/cb302/
V3.02_TARGETDIR/envfile/*SYSPLEX* 内の全ファイル	*V4.0_TARGETDIR*/controlinfo/envfile/*SYSPLEX*

エンタープライズ版 V3.02 からコピーするファイル	WebSphere for z/OS V4.0 でのコピー先

ここで、

V3.02_TARGETDIR
エンタープライズ版 V3.02 のターゲット・ディレクトリーです。

V4.0_TARGETDIR
WebSphere for z/OS V4.0 のターゲット・ディレクトリーです。

SYSPLEX
ユーザーのシスプレックスの名前です。

b. コピーしたファイルを調べて、ファイル所有者、グループ・アクセス、ファイル・アクセス権を確認してください。

---

current.xml と環境ファイルが正しいディレクトリーに入っていれば、このステップは完了です。

XML 構成ファイルと環境ファイルをアップグレードするステップ: この手順では、XML 構成ファイルと環境ファイルを更新する BBOMMIG ジョブを実行します。

1. BBOMMIG のステップ 1 と 2 では、エンタープライズ版 V3.02 上でコールド・スタートの準備を行ったときに作成された XML 構成ファイルを更新します。これらの更新には、ランタイム・サーバー (デーモン、ネーミング、システム管理、およびインターフェース・リポジトリー) 用のアプリケーション変更と、ネーミング・サーバー用のトランザクション・ポリシー、および、オプションとしてすべてのアプリケーション・サーバー用のトランザクション・ポリシーが含まれます。

   V4.0_TARGETDIR/*SYSPLEX*/conversations/cb302/ 内の current.xml は configuration.xml へマイグレーションされます。また、*V4.0_TARGETDIR*/*SYSPLEX*/conversations/current/ の中に configuration.xml へのリンクが設定されるので、ブートストラップ・プロセスで変更が読み込まれます。

2. BBOMMIG のステップ 3 と 4 では、古いエンタープライズ版 V3.02 環境ファイルが更新されます。これらのステップはシステム管理データベースにバインドし、環境データを取り出します。

   これらのステップでは、新規または変更されたコード・ディレクトリーとサーバー名を定義している入力ファイルを提供する必要があります。IBM では、サンプル・ファイルの *INSTALLDIR*/samples/patchenv.in を提供してい

ます。ここで、*INSTALLDIR* は、SMP/E インストール後に WebSphere for z/OS のファイルが常駐するディレクトリーの名前です。

この作業を始める前に: 266ページの『システム管理 HFS 構造をアップグレードするステップ』のステップを実行する必要があります。また、BBOMMIG と patchenv.in のコピーも必要です。

UID が 0 であるユーザー ID には、環境変数が格納されているディレクトリーへの書き込みアクセス権、および、PLAN とこのジョブ内の PACKAGES へバインドする許可が必要です。

以下のステップを実行して、XML 構成ファイルと環境ファイルをアップグレードします。

1. patchenv のコピーを、このファイル内のコメントに従って更新します。このファイルが HFS 内の読み取り / 書き込みディレクトリーに入っていることを確認してください。

   ---

2. BBOMMIG のコピーを、このファイル内のコメントに従って更新します。#INPUTFILE# の出現箇所は、すべて、更新した patchenv.in ファイルの位置に必ず置き換えてください。

   ---

3. BBOMMIG を実行します。**結果:** 次のようなメッセージが表示されます。

```
=====================================================
Input parameters are:
=====================================================
Installation dir    : /usr/lpp/WebSphere
Target dir          : /WebSphere390/CB390
Sysplex name        : MONOS20
Parameter file      : /WebSphere390/CB390/patch/patchenv.in
Change TP           : YES
=====================================================

=> Now executing XML Migration tool....
.
.
.
=> XML Migration tool finished!
=> Creating symbolic link for migrated cb3.02 conversation configuration file
=> ....
=> Finished!

 BIND PACKAGE(CBSYSMGT_PKG) MEMBER(BBOMPAT)  ....
 ....
DSNT232I  - SUCCESSFUL BIND FOR
           PACKAGE = LOC1.CBSYSMGT_PKG.BBOMPAT.(version)
 ....
```

```
 BIND PACKAGE(CBSYSMGT_PKG) MEMBER(BBOMPDB2) ....
 ....
DSNT232I  - SUCCESSFUL BIND FOR
           PACKAGE = LOC1.CBSYSMGT_PKG.BBOMPDB2.(version)
 ....
 BIND PLAN(<plan>) PKLIST(CBSYSMGT_PKG.*) ....
 ....
DSNT200I  -  BIND FOR PLAN plan SUCCESSFUL
....patch program starts...
processing step STEP6
Start migrateEnvironment using fileName = filename_from_job.
Start migrateEnvFiles
Done migrateEnvFiles
Done migrateEnvironment
patch program ends...
```

BBOMMIG が戻りコード CC=00 で終了し、/tmp/bbommig.err ファイルが空であれば、このステップは完了です。

システム管理データベースを再作成するステップ: **この作業を始める前に:** DB2 for OS/390 V7.1 のインストールを完了しておかなければなりません。

⇔ 86ページの『システム管理データベースの定義』の手順を実行します。

すべての手順が正常に終了すれば、このステップは完了です。

LDAP データベースを再作成するステップ: **重要:** この手順では、LDAP データベースを除去して再作成します。WebSphere for z/OS ランタイムは、以前のランタイムが使用していたネーミング項目だけを再確立します。独自に作成したネーミング項目は手動で復元する必要があります。それらの項目は、ランタイム項目以外の項目で、既存アプリケーションの内部で使用されて いた項目です。

この作業を始める前に: 復元を計画している独自のネーミング項目があれば、そのバックアップを作成しておく必要があります。

⇔ 94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』の手順を実行します。

すべての手順が正常に終了すれば、このステップは完了です。

WebSphere for z/OS ブートストラップを実行し、アプリケーション・サーバーを再初期化するステップ: **この作業を始める前に:** この節で述べたこれ以外のマイグレーション手順とタスクをすべて完了していなければなりません。

以下のステップを実行して WebSphere for z/OS ブートストラップを実行し、アプリケーション・サーバーを再初期化します。

1. 『ブートストラップの準備と実行』で述べた手順を、108ページの『コンソールからブートストラップのフェーズ 1 を準備し、開始するためのステップ』から開始します (つまり、『configuration.env ファイルを変更するためのステップ』をスキップします)。

---

2. ブートストラップが完了し、デーモンの再初期化が済んだら、それぞれのアプリケーション・サーバーごとに 1 つのサーバー・インスタンスを始動します。初期化が完了するのを待ってから、新しいサーバー・インスタンスを始動します。**結果:** 次のようなメッセージが表示されます。

```
BBOU0694I Naming registration started for server server
BBOU0696I Registering home home for server server
.
.
.
BBOU0698I Registering server server
BBOU0695I Naming registration completed for server server
```

ここで、

server
アプリケーション・サーバーの名前です。

home
ホームの名前です。

---

3. 198ページの『2 番目のインターフェース・リポジトリー・クライアント・ブートストラップの実行』で述べたように、2 番目のインターフェース・リポジトリー・クライアント・ブートストラップを稼働します。

すべてのランタイム・サーバーとアプリケーション・サーバーが初期化され、2 番目のインターフェース・リポジトリー・クライアント・ブートストラップが正常に動作したら、このステップは完了です。

詳細情報: このサポートの詳細については、次の WebSphere for z/OS 資料を参照してください。

- *WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656

システム管理スクリプト API

説明: 新規アクションは、現時点で CB390CFG スクリプトを通じて使用できます。このスクリプトは、WebSphere for z/OS の構成とアプリケーションを定義し管理する機能を提供するシステム管理スクリプト API です。つまり、SM スクリプト API は、WebSphere for z/OS の構成を管理する代替の方法となります。これらの新規アクションは、シスプレックスとシステム定義を管理する機能を提供します。

変更によって影響を受ける領域: このサポートは、次の処理領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	278ページの表31 の新規および変更されたインターフェース情報を検討し、新機能を活用するかどうかを判断してください。
アプリケーション開発	なし
監査	なし
カスタマイズ	新規の CB390CFG アクションを使用するには、デフォルトの XML ファイルの変更が必要になる場合があります。詳しくは、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スプリクト API*, SA88-8657 を参照してください。
一般ユーザー	なし
操作	なし
インターフェース	新規および変更されたインターフェースの詳細については、278ページの表31 を参照してください。

依存関係: このサポートに関連したソフトウェア依存関係、または機能的な依存関係はありません。

依存に関する考慮事項: このサポートに関連した共存に関する考慮事項はありません。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

表 28. マイグレーション・タスク

タスク	条件	手順参照
クライアント環境をセットアップする手順に変更があるかどうかを調べる。	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スプリクト API*, SA88-8657
新機能を活用するために既存のクライアント・スクリプトを編集する。たとえば、XMLGEN スクリプトを使用して、デフォルトの XML ファイルに新規属性を追加します。	オプション	*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スプリクト API*, SA88-8657

詳細情報: このサポートの詳細については、次の資料を参照してください。
WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スプリクト API, SA88-8657

JRas サポート

説明: JRas サポートは、以下のように変更されました。
- 新規インターフェースにより、Java アプリケーションでメッセージ・ロガーまたはトレース・ロガーを取得できます。
- ランタイム環境変数でなく、ユーザー提供のトレース設定ファイルによって、トレース・データの収集を使用可能または使用不可にできます。
- メッセージの収集は、常に使用可能になっています。

変更によって影響を受ける領域: このサポートは、次の処理領域に影響を及ぼす可能性があります。

領域	考慮事項
管理	Java アプリケーションについてトレース・データの収集を使用可能にするには、次のようにします。 • トレース設定ファイルを提供する。 • その設定ファイルを指すようにアプリケーション・サーバー・ランタイム環境変数を変更する。
アプリケーション開発	新規 Java アプリケーションの場合は、新規 JRas インターフェースを使用してメッセージ・ロガーとトレース・ロガーを取得します。以前のインターフェースは使用すべきではありませんが、現在それらのインターフェースを使用している Java アプリケーションを変更する必要は、まったくありません。詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 で Java アプリケーションのメッセージとトレース・データのロギングに関するトピックを参照してください。
監査	なし
カスタマイズ	なし
一般ユーザー	なし
操作	Java アプリケーションのメッセージまたはトレース・データは、エラー・ログか CTRACE データ・セット、またはその両方の中に現れる場合があります。また、メッセージの収集は常に使用可能にされているので、このサポートはマスター・コンソール上のメッセージ・トラフィックを増加させる場合があります。
インターフェース	新規および変更されたインターフェースの詳細については、以下のトピックを参照してください。 • 277ページの『JRas サポート用のインターフェース』 • 278ページの『JVM プロパティーの変更』

依存関係: このサポートに関連したソフトウェア依存関係、または機能的な依存関係はありません。

依存に関する考慮事項: このサポートに関連した共存に関する考慮事項はありません。

マイグレーション・タスク: 環境への影響を詳しく知るためには、次のような高レベルのマイグレーション・タスクを検討してください。**必須**タスクは、この機能を使用可能にするすべてのインストールに適用されます。**オプション**のタスクは、所定の稼働環境だけに適用されるか、この機能をセットアップまたは使用可能にするのに複数の方法がある状況に適用されます。タスクに関連する手順の詳細については、リストされた参考資料を参照してください。

表 29. マイグレーション・タスク

タスク	条件	手順参照
新規 JRas インターフェースを使用するように Java アプリケーションを再コーディングする。	オプション	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
Java アプリケーションのメッセージとトレース要求をログに記録するよう、次のようにランタイム環境を準備する。 • トレース設定プロパティー・ファイルを作成する。 • アプリケーション・サーバー用の JVM プロパティー・ファイルを更新する。 既存アプリケーションで JRas サポートを使用する場合は必須。	必須	*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
アプリケーション・サーバー用の環境変数を更新し、古くなった JRas 変数を除去する。	オプション	383ページの『付録A. 環境ファイル』

詳細情報: このサポートの詳細については、次の資料を参照してください。

- *WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654
- *WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655

- 使用している WebSphere ワークステーションのインフォセンターに入っている JRas のトピック

インターフェースの変更の要約

ここでは、WebSphere for z/OS の新規インターフェースと変更されたインターフェースの概要を示します。

参照事項	参照先
アプリケーション・プログラミング・インターフェース	
J2EE アプリケーション・コンポーネント仕様	『J2EE アプリケーション・コンポーネント仕様』
JDBC	277ページの『JDBC 2.0 API』
JRas サポート	277ページの『JRas サポート用のインターフェース』
システム・インターフェース	277ページの『システム・インターフェース』
アプリケーション開発ツール	
オブジェクト・ビルダー	278ページの『オブジェクト・ビルダー』
アプリケーションのインストールとランタイム	
システム管理スクリプト API	278ページの『システム管理スクリプト API』
JVM プロパティー	278ページの『JVM プロパティーの変更』
Web サーバーの構成の変更	279ページの『Web サーバーの構成の変更』
メッセージ、コード、および異常終了	279ページの『メッセージ、コード、および異常終了』

J2EE アプリケーション・コンポーネント仕様

スタンダード版 V3.02 アプリケーションを WebSphere for z/OS サーバー上で実行することはできません。これらのアプリケーションに含まれているサーブレットは、Java サーブレット V2.2 仕様レベルまでアップグレードする必要があります。また、これらのアプリケーションに含まれている JSP は、JSP V1.1 仕様レベルまでアップグレードする必要があります。さらに、アプリケーションは .war ファイルとしてパッケージ化されていなければなりません。

スタンダード版 V3.5 アプリケーションは、WebSphere for z/OS サーバーと共存し、対話することができます。ただし、それらのアプリケーションに含まれているサーブレットが Java サーブレット V2.2 仕様レベルに合わせて書かれ

ており、それらのアプリケーションに含まれている JSP が JSP V1.1 仕様レベルに合わせて書かれていなければなりません。さらに、アプリケーションは .war ファイルとしてパッケージ化されていなければなりません。

Java サーブレットの詳細については、http://www.javasoft.com の URL で Java サーブレット仕様 V2.2 を参照してください。

JDBC 2.0 API

データ・ソースにアクセスし、JDBC 2.0 API を使用するには、Java コードを修正しなければなりません。ただし、JDBC 2.0 は JDBC 1.x API をサポートしており、オブジェクトを『更新』してプログラム内で初期化する代わりに、管理アプリケーションを使用してデータ・ソースを構成できます。

JRas サポート用のインターフェース

Java アプリケーション用の JRas インターフェースは、com.ibm.websphere.ras パッケージ内のクラスを通じて提供されます。表30 は、JRas サポート用の新規インターフェースと変更されたインターフェースのリストです。詳細については、使用している WebSphere ワークステーションのインフォセンターを参照してください。

表 30. JRas サポート用の新規インターフェースと変更されたインターフェースの要約

API	リリース	説明
RASIMessageLogger インターフェース	V4.0	**新規インターフェース:** Java アプリケーションで、メッセージを発行できるようにします。それらのメッセージは、マスター・コンソール上、エラー・ログ内、または CTRACE データ・セット内に収集され、表示されます。
RASITraceLogger インターフェース	V4.0	**新規インターフェース:** CTRACE データ・セット内に記録するトレース項目を Java アプリケーションで定義できるようにします。

システム・インターフェース

スタンダード版 V3.02 および V3.5 では、JDBC や JNDI などのシステム・インターフェースへのアクセスは、was.conf ファイル内の設定を通じて確立されていました。WebSphere for z/OS V4.0 では、これらのインターフェースへのアクセスは、J2EE サーバーによって提供されます。しかし、DB2 を使用してセッション・データを格納する場合は、webcontainer.conf ファイル内で **session.dbjdbcpoolname session.datasourcename**、および **session.dbtablename** プロパティーの値を指定する必要があります。

オブジェクト・ビルダー

オブジェクト・ビルダー V3.5 を使用して、C++ Enterprise Edition V3.02 アプリケーションを再コンパイルしてください。Java BO アプリケーションをオブジェクト・ビルダー V3.5 で再コンパイルすることもできます。詳しくは、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

システム管理スクリプト API

表31 は、新規および変更されたシステム管理スクリプト API のリストです。それぞれのインターフェースの詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スクリプト API*, SA88-8657 を参照してください。

表 31. 新規および変更された SM スクリプト API の要約

API	リリース	説明
CB390CFG	V4.0	**新規のアクション:** • `changesysplex` を使用して、シスプレックス定義の属性を変更できます。 • `createsystem`、`deletesystem`、`changesystem`、および `listsystem` を使用して、システム定義の作成と管理ができます。
		変更されたアクション: サーバーの定義または変更について、追加の XML ファイル属性を指定します。

JVM プロパティーの変更

スタンダード版 V3.5 では、JVM プロパティー・ファイルの位置、実行するロギングのレベル、作業ディレクトリーの位置など、ランタイム設定は was.conf ファイルの中で設定されていました。WebSphere for z/OS V4.0 では、J2EE サーバー構成用に確立されたランタイム設定は、そのサーバー内のコンテナーに適用されます。したがって、**appserver.jvmpropertiesfile** や **appserver.loglevel** などのプロパティーは、webcontainer.conf ファイルの中に存在しません。

それでも、IBM が設定したデフォルト値の使用を選択する場合以外は、webcontainer.conf ファイルの中で **host.**<*virtual-hostname*>**.alias**<*hostname*>|localhost、**host.**<*virtual-hostname*>**.mimetypefile**、**host.**<*virtual-hostname*>**.contextroots** の各プロパティーに値を指定する必要があります。

Web サーバーの構成の変更

V4.0 Application Server プラグインのホストとなるすべての Web サーバーの httpd.conf 構成ファイルに新規の ServerInit、Service、および ServerTerm ディレクティブを追加し、それらの Web サーバーにこのプラグインの初期化、要求処理、および終了ルーチンのエントリー・ポイントを提供する必要があります。前バージョンの Application Server 用の ServerInit、Service、ServerTerm ディレクティブがすでに httpd.conf ファイルに存在する場合は、それらを削除しなければなりません。

メッセージ、コード、および異常終了

ここでは、新規、変更または削除されたメッセージ、コード、および異常終了のリストを示します。

これらのメッセージの詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 を参照してください。

表 32. 新規メッセージ、変更または削除されたメッセージ

新規メッセージ	BBOU0618W	BBOU0711E
	BBOU0705W	BBOU0712E
	BBOU0706W	BBOU0713W
	BBOU0707W	BBOU0714E
	BBOU0708W	BBOU0715E
	BBOU0709E	BBOU0716E
	BBOU0710E	

表 32. 新規メッセージ、変更または削除されたメッセージ (続き)

変更されたメッセージ	BBOU0000I	BBOU0651E
	BBOU0039E	BBOU0652E
	BBOU0130I	BBOU0670I
	BBOU0131I	BBOU0673I
	BBOU0133I	BBOU0677I
	BBOU0134I	BBOU0678I
	BBOU0168E	BBOU0679I
	BBOU0334I	BBOU0692I
	BBOU0505E	BBOU0694I
	BBOU0604I	BBOU0695I
	BBOU0610E	BBOU0696I
	BBOU0611E	BBOU0697I
	BBOU0612E	BBOU0698I
	BBOU0623E	BBOU0699I
	BBOU0628E	BBOU0700I
	BBOU0648E	
	BBOU0649E	
	BBOU0650E	
削除されたメッセージ	BBOU0519W	BBOU0669I
	BBOU0520W	BBOU0693I
	BBOU0521W	

表 33. 新規コード、変更または削除されたコード

新規コード	C9C20CDA	C9C22831
	C9C2122F	C9C22832
	C9C21230	C9C22833
	C9C21231	C9C22834
	C9C21232	C9C22835
	C9C21233	C9C22836
	C9C21234	C9C240B8
	C9C21235	C9C240B9
	C9C21236	C9C240BA
	C9C21237	C9C240BB
	C9C21238	C9C240BC
	C9C21239	C9C240C0
	C9C2123A	C9C240C1
	C9C2123B	C9C240C2
	C9C2123C	C9C240C3
	C9C21457	C9C240C4
	C9C21458	C9C240C5
	C9C21C05	C9C240C6
	C9C21C06	C9C240C7
	C9C21C3F	C9C240C8
	C9C21C40	C9C240C9
	C9C21C41	C9C240CA
	C9C21C42	C9C240CB
	C9C21C43	C9C240CC
	C9C21C44	C9C240CD
	C9C2281D	C9C240CE
	C9C2281E	C9C240CF
	C9C2281F	C9C240D0
	C9C22820	C9C240D2
	C9C22821	C9C240D3
	C9C22822	C9C240D4
	C9C22823	C9C240D5
	C9C22824	C9C240D6
	C9C22825	C9C240D7
	C9C22826	C9C240D8
	C9C22827	C9C240D9
	C9C22828	C9C240DA
	C9C22829	C9C240DB
	C9C2282A	C9C240DC
	C9C2282B	C9C240DD
	C9C2282C	C9C240DE
	C9C2282D	C9C240DF
	C9C2282E	C9C2EA01
	C9C2282F	C9C2EA02
	C9C22830	

表 33. 新規コード、変更または削除されたコード (続き)

変更されたコード	C9C21111 C9C21208	C9C2120A
削除されたコード	C9C20C00 C9C20C03 C9C20C22 C9C20C36 C9C20C6E	C9C20C73 C9C22801 C9C22802 C9C22803

表 34. 新規の異常終了、変更または削除された異常終了

新規の異常終了	CC3 0A020004	CC3 0A080014
	CC3 0A020005	CC3 0A080015
	CC3 0A060001	CC3 0A080016
	CC3 0A060002	CC3 0A080017
	CC3 0A060003	CC3 0A080018
	CC3 0A060004	CC3 0A080019
	CC3 0A060005	CC3 0A08001A
	CC3 0A060006	CC3 0A08001B
	CC3 0A060007	CC3 0A08001C
	CC3 0A070001	CC3 0A090001
	CC3 0A080001	CC3 0A090002
	CC3 0A080002	CC3 0A090003
	CC3 0A080003	CC3 0A090004
	CC3 0A080004	CC3 0A090005
	CC3 0A080005	CC3 0A090006
	CC3 0A080006	CC3 0A090007
	CC3 0A080007	CC3 0A090008
	CC3 0A080008	CC3 0A090009
	CC3 0A080009	CC3 0A0A0001
	CC3 0A08000A	CC3 0A0A0002
	CC3 0A08000B	CC3 0A0A0003
	CC3 0A08000C	DC3 0204000A
	CC3 0A08000D	DC3 0204000B
	CC3 0A08000E	DC3 0205000F
	CC3 0A08000F	DC3 02050010
	CC3 0A080010	DC3 04010006
	CC3 0A080011	DC3 04010007
	CC3 0A080011	DC3 04010008
	CC3 0A080012	EC3 0402000B
	CC3 0A080013	EC3 0402000C
変更された異常終了	(なし)	

表 34. 新規の異常終了、変更または削除された異常終了 (続き)

削除された異常終了	EC3 04230004

第5章 インストール後のタスク

この章では、WebSphere for z/OS のインストール後に発生するトピックやタスクを扱います。扱うトピックは次のとおりです。

- システムをバックアップするためのガイドライン
- LDAP アクセス制御リストの更新
- 製品サービス
- DB2 for OS/390 の RACF 保護のセットアップ
- 自動化および自動再始動管理のセットアップ
- アカウンティング

WebSphere for z/OS システムのバックアップのためのガイドライン

WebSphere for z/OS システムの各部分をバックアップするには、次のガイドラインに従ってください。

1. 必ず、RRS の RMDATA ログをバックアップしてください。そうしないと、障害が発生して RRS のコールド・スタートを余儀なくされる場合があります。
2. アーカイブ・ログの保存期間を 1 日にします。
3. ユーザー自身のバックアップ手順に従って、ネーミングおよびインターフェース・リポジトリーのデータを含む、LDAP データベースをバックアップします。

   LDAP データを復元する場合は、必ず、統合ネーミング・スペース内の他の WebSphere システムとの間で復元の調整を行います。調整を行わないと、ネーミング・スペースの一貫性が保たれません。
4. 次のものを、通常のバックアップ手順に取り込みます。
   - WebSphere for z/OS proclib
   - WebSphere for z/OS loadlib
   - WebSphere for z/OS 環境ファイル
   - 管理アプリケーションがアプリケーションを書き込むディレクトリー (CBCONFIG 環境変数の値。デフォルトは `/WebSphere390/CB390` です。)
5. 次の DB2 for OS/390 表の参照コレクション・データをバックアップします。

- BBO.RCTABLE
- BBO.KRCTABLE
- BBO.RCHMTABLE

6. ユーザー所有アプリケーションの実行可能プログラム、およびバインディングをバックアップします。
7. 会話を活動化する場合は、システム管理が自動的に、/*path*/envfile/*sysplex*/*server_instance*/backup/ にある、個々のサーバー・インスタンスの現行環境ファイルをバックアップします。ここで、

   path
   CBCONFIG 環境変数の値 (デフォルトは、/WebSphere390/CB390) です。

   sysplex
   ユーザーのシスプレックスの名前です。

   server_instance
   サーバー・インスタンスの名前です。

   バックアップ・ファイルには、名前にタイム・スタンプが含まれています。バックアップ・ディレクトリーが満杯になると、古いバックアップ・ファイルを消去することができます。
8. コールド・スタートの準備をする場合は、システム管理が、/*path*/configuration/backup/ にある、XML 形式の制御情報をバックアップします。ここで、

   path
   CBCONFIG 環境変数の値 (デフォルトは、/WebSphere390/CB390) です。

   バックアップ・ファイルには、名前にタイム・スタンプが含まれています。バックアップ・ディレクトリーが満杯になると、古いバックアップ・ファイルを消去することができます。
9. 単一のサーバー・インスタンスをバックアップしたい場合は、管理アプリケーションのエクスポート / インポート機能を使用することができます。この実行方法に関する詳細は、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。
10. システム管理データベースに関しては、次の表に従って、バックアップするものを決定します。

条件	バックアップの対象となるもの	
管理者を追加した場合	次の表スペース	
	BBOMDB01.BBOMS51	
	BBOMDB01.BBOMS54	
新規会話またはコミットを作成した場合	次の表スペース	
	BBOMDB01.BBOMS00	BBOMDB01.BBOMS56
	BBOMDB01.BBOMS02	BBOMDB01.BBOMS58
	BBOMDB01.BBOMS04	BBOMDB01.BBOMS60
	BBOMDB01.BBOMS06	BBOMDB01.BBOMS62
	BBOMDB01.BBOMS10	BBOMDB01.BBOMS64
	BBOMDB01.BBOMS15	BBOMDB01.BBOMS66
	BBOMDB01.BBOMS19	BBOMDB01.BBOMS68
	BBOMDB01.BBOMS23	BBOMDB01.BBOMS70
	BBOMDB01.BBOMS25	BBOMDB01.BBOMS72
	BBOMDB01.BBOMS27	BBOMDB01.BBOMS74
	BBOMDB01.BBOMS29	BBOMDB01.BBOMS76
	BBOMDB01.BBOMS31	BBOMDB01.BBOMS80
	BBOMDB01.BBOMS33	BBOMDB01.BBOMS81
	BBOMDB01.BBOMS35	BBOMDB01.BBOMS82
	BBOMDB01.BBOMS37	BBOMDB01.BBOMS83
	BBOMDB01.BBOMS39	BBOMDB01.BBOMS84
	BBOMDB01.BBOMS41	BBOMDB01.BBOMS85
	BBOMDB01.BBOMS43	BBOMDB01.BBOMS86
	BBOMDB01.BBOMS45	BBOMDB01.BBOMS87
	BBOMDB01.BBOMS48	BBOMDB01.BBOMS90
	BBOMDB01.BBOMS52	

条件	バックアップの対象となるもの	
会話を活動化した場合	次の表スペースまたはデータベース	
		BBOMDB01.BBOMS53
	BBOMDB01.BBOMS00	BBOMDB01.BBOMS55
	BBOMDB01.BBOMS02	BBOMDB01.BBOMS56
	BBOMDB01.BBOMS04	
		BBOMDB01.BBOMS58
	BBOMDB01.BBOMS06	BBOMDB01.BBOMS60
	BBOMDB01.BBOMS10	BBOMDB01.BBOMS62
	BBOMDB01.BBOMS15	
		BBOMDB01.BBOMS64
	BBOMDB01.BBOMS19	BBOMDB01.BBOMS66
	BBOMDB01.BBOMS23	BBOMDB01.BBOMS68
	BBOMDB01.BBOMS25	
		BBOMDB01.BBOMS70
	BBOMDB01.BBOMS27	BBOMDB01.BBOMS72
	BBOMDB01.BBOMS29	BBOMDB01.BBOMS74
	BBOMDB01.BBOMS31	
		BBOMDB01.BBOMS76
	BBOMDB01.BBOMS33	BBOMDB01.BBOMS80
	BBOMDB01.BBOMS35	BBOMDB01.BBOMS81
	BBOMDB01.BBOMS37	
		BBOMDB01.BBOMS82
	BBOMDB01.BBOMS39	BBOMDB01.BBOMS83
	BBOMDB01.BBOMS41	BBOMDB01.BBOMS84
	BBOMDB01.BBOMS43	
		BBOMDB01.BBOMS85
	BBOMDB01.BBOMS45	BBOMDB01.BBOMS86
	BBOMDB01.BBOMS48	BBOMDB01.BBOMS87
	BBOMDB01.BBOMS52	
		BBOMDB01.BBOMS90
	LDAP データベース	BBOMDB01.BBOSLS01
		BBOMDB01.BBOSLS02

注:

a. バックアップした WebSphere for z/OS 表スペースを、他の WebSphere システム管理 (たとえば Windows NT 上のもの) と調整してください。

b. ネーミング・ツリーを別のシステム (たとえば Windows NT) と統合した場合は、バックアップした LDAP データベースと Windows NT 上のバックアップとを同期化しなければなりません。同期化しないと、統合ネーミング・スペースの一貫性が保たれません。

管理アプリケーションの新規管理者の追加

管理アプリケーションのデフォルトの管理者は CBADMIN です。管理者を追加したい場合は、次のタスクを実行する必要があります。

サブタスク	関連手順 (参照箇所)
MVS ユーザー ID を作成するか、現行の MVS ユーザー ID を使用する。 **注:** 新規管理者ユーザー ID に CBADMIN と同じ RACF 権限を与えます。	*z/OS TSO/E 管理*, SA88-8626 または *z/OS SecureWay Security Server (RACF)* セキュリティー管理者のガイド, SA88-8613
LDAP 用アクセス制御リストを更新する。	『LDAP 用アクセス制御リスト更新のためのステップ』
管理アプリケーションに対して新規管理者を定義する。	*WebSphere Application Server V4.0 for z/OS and OS/390:* システム管理ユーザー・インターフェース, SA88-8656
管理者ユーザー ID にシステム管理データベース権限を付与する。	291ページの『新規管理者にデータベース権限を付与するためのステップ』

LDAP 用アクセス制御リスト更新のためのステップ

管理アプリケーションの管理者を追加する場合は、その管理者を LDAP 内のアクセス制御リストに追加する必要があります。

この作業を始める前に: LDAP サーバーのセットアップが必要です。ここでは、WebSphere for z/OS を管理する目的で、排他的 LDAP サーバーがすでにセットアップされていることを前提にします。LDAP サーバーのセットアップに関する詳細は、94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』を参照してください。

LDAP サーバーが現在使用している bboslapd.conf ファイルも必要です。

LDAP のアクセス制御リストを変更するには、以下のステップを実行します。

1. bboslapd.conf ファイルを表示し、次の項目に注目する。
   a. 管理者の識別名。**例:**

```
adminDN         "cn=CBAdmin"
```

b. 管理者のパスワード。**例:**

```
adminPW         mypass
```

c. WebSphere for z/OS ネーム・スペース構造のルート・ネーミング・コンテキスト (RDN)。**例:**

```
suffix          "o=BOSS,c=US"
```

---

2. 次のコマンドで LDAP サーバーを始動する。

```
S BBOLDAP
```

---

3. ldapcp コマンドで、現行のアクセス制御リストを抽出する。**例:**

```
/u/myself-> ldapcp -p 1389
GLD4005I Environment variable file not found.  Environment variables not set.
GLD6009I No DN entered.  Enter DN now.
ldapcp> cn=CBAdmin
GLD6010I No password entered.  Enter password now.
ldapcp>

GLD6019I Communicating with server on port 1389.
ldapcp> acl q ob "o=boss,c=us"
 object = o=boss,c=us
 aclSource = O=BOSS,C=US
 aclPropagate = TRUE

 acl = access-id:CBADMIN:object:ad:normal:rwsc

 acl = access-id:CBSYMCR1:object:ad:normal:rwsc

 acl = group:CN=ANYBODY:normal:rsc

 acl = access-id:CN=BOSSAdmin,O=BOSS,C=US:object:ad:normal:rwsc

ldapcp>quit
```

---

4. ホーム・ディレクトリーに新規ファイル (たとえば acl_update.txt) を作成する。そのファイルに次の行を追加する。

```
dn: o=boss, c=us
changetype:modify
replace:x
```

---

5. ファイルに追加した最初の 3 行に続けて、ステップ 3 で抽出した ACL 行のそれぞれに対し、aclentry ステートメントを追加する。USER1 用に、新規の aclentry ステートメントを追加する。

注:

a. 末尾にダッシュ (「-」) を追加することが重要です。

b. ldapcp コマンドの出力形式は、入力した aclentry 行と同じではありません (たとえば、「acl=」は「aclentry:」に変更しなければなりません)。

c. この例では、USER1 の aclentry は、CBADMIN と同じ権限を USER1 に与えています。

例:

```
aclentry: access-id:cn=BOSSAdmin, o=boss, c=us:normal:rwsc:object:ad
aclentry: access-id:USER1:normal:rwsc:object:ad
aclentry: access-id:CBADMIN:normal:rwsc:object:ad
aclentry: access-id:CBSYMCR1:normal:rwsc:object:ad
aclentry: group:CN=ANYBODY:normal:rsc
-
```

---

6. 更新ファイルを保管し、次の ldapmodify コマンドを発行する。

```
u/myself-> ldapmodify -v -p 1389 -D "cn=CBAdmin" -w mypass -f acl_update.txt
```

結果: ldapmodify が次のように応答します。

```
modifying entry o=BOSS, c=US
```

---

7. 290ページの3 ステップを繰り返し、アクセス制御リストに新規ユーザーが追加されたことを確認する。

アクセス制御リストに新規ユーザーが表示されれば、このステップは終了したことになります。

新規管理者にデータベース権限を付与するためのステップ

新規管理者は、CBSYSMGT_PKG の実行権限と、管理者が J2EE アプリケーションをシステム管理データベース内に配置するために必要なテーブルの選択、更新、挿入、および削除の権限を必要とします。

この作業を始める前に: DB2 for OS/390 SYSADM 権限を備えたユーザー ID を持っている必要があります。

新規管理者にデータベース権限を付与するために、次のステップを実行します。

⇔ 以下のコマンドを発行します。

```
GRANT EXECUTE ON PACKAGE CBSYSMGT_PKG.*    TO user_ID

GRANT SELECT,UPDATE,INSERT,DELETE ON TABLE
BBO.BBOMT80_J2EEAPP TO user_ID;

GRANT SELECT,UPDATE,INSERT,DELETE ON TABLE
BBO.BBOMT81_MODULE TO user_ID;

GRANT SELECT,UPDATE,INSERT,DELETE ON TABLE
BBO.BBOMT82_COMPONENT TO user_ID;

GRANT SELECT,UPDATE,INSERT,DELETE ON TABLE
BBO.BBOMT83_METHOD TO user_ID;

GRANT SELECT,UPDATE,INSERT,DELETE ON TABLE
BBO.BBOMT86_DATASI TO user_ID;

GRANT SELECT,UPDATE,INSERT,DELETE ON TABLE
BBO.BBOMT87_COMP_DS TO user_ID;
```

ここで、*user_ID* は、定義した管理者ユーザー ID です。

GRANT コマンドが正常に終了すれば、このステップは完了です。

製品サービス

WebSphere for z/OS 用の予防保守計画 (PSP) アップグレードについては、弊社ソフトウェア営業担当員にお問い合わせください。PSP アップグレードの詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: プログラム・ディレクトリー*, GI88-8549 を参照してください。*プログラム・ディレクトリー* に、必要な PTF のリストが入っていますが、最新情報は弊社ソフトウェア営業担当員にお問い合わせください。

DB2 for OS/390 の RACF 保護のセットアップ

RACF DSNR リソース・クラスを使用すると、DB2 for OS/390 のリソースを保護することができます。この機能は、セキュリティー管理を一元化するのに役立ちます。この節では、DB2 for OS/390 の RACF 保護のセットアップに関する一般情報への参照箇所、および WebSphere for z/OS が使用するリソース、グループ、ユーザー ID、アクセス権に関する特定情報への参照箇所を提供します。

RACF には、DB2 for OS/390 の保護に関して考慮すべき機能領域が 3 つあります。

- RACF DSNR クラスは、DB2 サブシステムへのアクセスを制御します。DSNR クラスが活動中の場合、WebSphere for z/OS の制御領域およびサーバー領域には、*db2_ssn*.RRSAF プロファイルへのアクセスが必要になります。ここで、*db2_ssn* は、ユーザーの DB2 for OS/390 サブシステム名です。制御領域またはサーバー領域にアクセス権がない場合は、その領域は初期化されません。
- DB2 識別およびサインオン出口 (DSN3@ATH および DSN3@SGN) は、許可 ID を割り当てます。2 次許可 ID (RACF グループ名) を使用する場合は、デフォルトの出口を、上の 2 つのルーチン例に置き換えなければなりません。これらのルーチン例のインストール方法に関する詳細は、*DB2 管理の手引き*, SC88-7376 を参照してください。
- WebSphere for z/OS は、DSNX@XAC 出口による DB2 for OS/390 オブジェクトの保護はサポートしていません。DB2 for OS/390 オブジェクトを保護するには、GRANT ステートメントを使用しなければなりません。

必要な RACF コマンドを使用して、WebSphere for z/OS が使用する DB2 for OS/390 のリソースを保護する BBOCBRAC の例には、コメント付きセクションが含まれています。RACF コマンドの例を使用すると、アプリケーション・サーバー用に、WebSphere for z/OS ランタイムまたはモデル権限を許可することができます。例では、

- DSNR クラス・プロファイル *db2_ssn*.RRSAF が定義されます。ここで、*db2_ssn* は、ユーザーの DB2 for OS/390 のサブシステム名です。

  注: シスプレックスの場合は、シスプレックス内の DB2 for OS/390 サブシステムごとに、固有のサブシステム名を使用して、*db2_ssn*.RRSAF クラス・プロファイルを定義しなければなりません。
- 以下に、*db2_ssn*.RRSAF クラス・プロファイルに対する読み取り権限が与えられます。
  - デーモン制御領域
  - システム管理サーバー制御領域
  - すべてのサーバー領域

次の表は、WebSphere for z/OS が必要とする DB2 for OS/390 の RACF 保護をセットアップするための、サブタスクおよび関連手順を示したものです。

サブタスク	関連手順 (参照箇所)
RACF ルーター・テーブルに項目を追加する	*DB2 管理の手引き*, SC88-7376

サブタスク	関連手順 (参照箇所)
識別およびサインオン出口 (DSN3@ATH および DSN3@SGN) をインストールする	*DB2 管理の手引き*, SC88-7376
DB2 for OS/390 の開始済みタスクで RACF ユーザー ID を定義する	*DB2 管理の手引き*, SC88-7376
WebSphere for z/OS が RACF で必要とする DB2 for OS/390 のリソースおよび許可を定義する	『RACF で DB2 for OS/390 の許可を定義するためのステップ』

RACF で DB2 for OS/390 の許可を定義するためのステップ

この作業を始める前に: DB2 for OS/390 システムの RACF 保護を使用可能にするための、一般タスクを完了しなければなりません。一般タスクには、RACF ルーター・テーブルへの項目の追加、識別およびサインオン出口のインストール、DB2 for OS/390 の開始済みタスクでの RACF ユーザー ID の定義などがあります。WebSphere for z/OS で提供している BBOCBRAJ および BBOCBRAC の例のコピーもとっておかなければなりません。

DB2 for OS/390 のリソースおよび許可を RACF で定義するには、以下のステップを実行してください。

1. 例 BBOCBRAC を編集し、「DSNR PROFILES」のラベルの付いたセクションをコピーして、そのセクションを新規ファイルに貼り付ける。

   _____

2. REXX および RACF コマンドを囲むコメント・マークを除去する。出荷時には、DSNR プロファイル・セクションはコメント化されています。

   _____

3. BBOCBRAJ ジョブを新規ファイルにコピーする。

   _____

4. BBOCBRAJ の BBOCBRAC メンバー名を、DSNR プロファイル・コマンドを持つ新規のメンバー名に変更する。

   _____

5. RACF 特殊権限を持つユーザー ID でジョブを実行依頼する。

   _____

このジョブが正常に完了すれば、このステップは終了したことになります。

自動化および自動再始動管理のセットアップ

この節では、自動化の推奨と、自動再始動管理をセットアップするためのステップについて説明します。

WebSphere for z/OS およびそのアプリケーションの自動化に対する推奨

ユーザーは、システム IPL で WebSphere for z/OS サーバーを自動的に始動するかどうかを決定し、この決定をシステム自動化にインプリメントする必要があります。自動化ポリシーでは、WebSphere for z/OS および関連機能の初期設定を、必ず次の順序で行う必要があります。

1. システム・ロガー
2. RRS
3. DB2 for OS/390
4. TCP/IP
5. LDAP (オプション)
6. DCE (使用されている場合)
7. デーモン・サーバー。これが、システム管理サーバー、ネーミング・サーバー、およびインターフェース・リポジトリー・サーバーを自動的に始動します。
8. ユーザーのビジネス・アプリケーション・サーバー

WebSphere for z/OS サーバーの自動化に関する詳細は、*WebSphere Application Server V4.0 for z/OS and OS/390: 操作および管理*, SA88-8653 を参照してください。

自動再始動管理のセットアップ

ビジネスにとって重要なアプリケーションがある場合、障害を管理する機能が必要になります。OS/390 または z/OS には豊富な自動化インターフェースがあり、これを使用すると、障害を検出し、障害から回復することができます。ただし、複雑すぎて自動化では処理できないリカバリー状態もいくつかあります。そのような状態に備えて、OS/390 または z/OS には自動再始動管理の機能があります。この機能により、障害が発生したサーバーの再始動が処理されます。WebSphere for z/OS は自動再始動管理を使用します。

個々の WebSphere for z/OS サーバー・インスタンス (ユーザーが、ビジネス・アプリケーション用に作成するサーバー・インスタンスを含む) は、自動的に、自動再始動管理のデフォルト・グループに登録されます。各登録では、SYSCB と呼ばれる特殊なエレメント・タイプが使用されます。自動再始動管

理はこのエレメント・タイプを再始動レベル 3 として扱い、RRS と DB2 for OS/390 が、確実にどのサーバー・インスタンスよりも先に再始動するようにします。

サーバー・インスタンスは自動的に自動再始動管理の対象となりますが、機能自体はユーザーが活動化しなければなりません。つまり、以下のことを行う必要があります。

1. ARM 結合データ・セットを割り振る
2. 自動再始動管理ポリシーを開始する

自動再始動管理が活動状態にない場合は、WebSphere for z/OS はハードコピー・ログにエラー・メッセージを発行します。

WebSphere for z/OS サーバー・インスタンスに対する自動再始動管理ポリシーのデフォルトの変更も、検討しなければなりません。WebSphere for z/OS とともに開始されるポリシーを変更する必要はありませんが、アプリケーションを運用する際には、その変更を検討すべきです。自動再始動管理ポリシーに対する WebSphere for z/OS の要件に関する情報は、297ページの『WebSphere for z/OS の自動再始動管理ポリシーを変更するためのガイドラインと制限』にあります。ポリシーの変更方法についての詳細な情報は、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

自動再始動管理を活動化するためのステップ

次の手順は、自動再始動管理を実行するのに十分な情報を提供するためのものです。自動再始動管理ポリシーの定義は、本資料には含まれていません。自動再始動管理に対する WebSphere for z/OS の要件は、297ページの『WebSphere for z/OS の自動再始動管理ポリシーを変更するためのガイドラインと制限』で定義されていますが、自動再始動管理ポリシーの定義に関する一般情報については、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

この作業を始める前に: SYS1.MIGLIB にある、結合データ・セットのフォーマット・ユーティリティー、IXCL1DSU に対するアクセス権がなければなりません。自動再始動管理ポリシーを変更する予定の場合は、やはり SYS1.MIGLIB にある、管理データ・ユーティリティー、IXCMIAPU に対するアクセス権を取得し、RACF FACILITY クラス MVSADMIN.XCF.ARM に対する更新許可を得る必要があります。ポリシーを開始するためには、RACF FACILITY クラス MVSADMIN.XCF.ARM に対する読み取り許可を得る必要があります。

WebSphere for z/OS の自動再始動管理を活動化するには、以下のステップに従ってください。

1. ポリシー用の結合データ・セットをまだフォーマットしていない場合は、ここでフォーマットを行う。詳細は、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

---

2. ARM 結合データ・セットをフォーマットするジョブを実行依頼する。

---

3. この時点で自動再始動管理ポリシーを変更したくない場合は、このステップはスキップして次のステップに進む。開始するのに、ポリシーを変更する必要はありません。

   自動再始動管理ポリシーを変更したい場合は、まず、『WebSphere for z/OS の自動再始動管理ポリシーを変更するためのガイドラインと制限』で、自動再始動管理ポリシーのための WebSphere for z/OS の要件を読み、次に、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 に進んで、その資料の指示に従ってください。

---

4. 次のオペレーター・コマンドを発行して、自動再始動管理ポリシーを開始する。

   ```
   SETXCF COUPLE,TYPE=ARM,PCOUPLE=(dsname,vvvvvv)
   SETXCF START,POLICY,TYPE=ARM
   ```

   ここで

   dsname
   結合データ・セットのデータ・セット名です。

   vvvvvv
   結合データ・セットが常駐するボリュームのボリューム通し番号です。

SETXCF コマンドが正常に完了すれば、このステップは終了です。

WebSphere for z/OS の自動再始動管理ポリシーを変更するためのガイドラインと制限

295ページの『自動再始動管理のセットアップ』は、WebSphere for z/OS の自動再始動管理をセットアップするステップを取り上げていますが、自動再始動管理ポリシーの変更については扱っていませんでした。自動再始動管理ポリシーの変更は必須ではありませんが、ポリシーを変更してカスタム再始動グループを作成することもできます。サーバー・インスタンスがデフォルトの再始動グループに登録されているため、システム障害が発生すると、自動再始動管理

は、シスプレックスの別のシステムにあるデフォルト・グループ全体を再始動しようとします。ここで、デフォルト以外の再始動グループを作成することができます。

この節では、WebSphere for z/OS が自動再始動管理ポリシーを使用する際の、ガイドラインと制限について説明します。ポリシーの変更方法については、本資料では説明しません。自動再始動管理ポリシーの変更に関する詳細は、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

以下のガイドラインおよび制限に従ってください。

バージョン 4.0 の制約事項

1. WebSphere for z/OS のサーバー・インスタンスでは、システム間再始動を使用可能に**しない**ことをお勧めします。ワークロードは、障害が起こったシステムから稼働中のシステムに移動できますが、一度復元したワークロードを、オリジナル・システムに戻すことはできません。WebSphere for z/OS サーバーが設定したデフォルトの ARM ポリシーを変更するには、管理データ・ユーティリティー (IXCMIAPU) を使用します。詳しくは、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

バージョン 4.0 の制約事項の終り

2. 障害が発生すると、自動再始動管理により、WebSphere for z/OS および、同一システム上の関連のあるサーバー・インスタンスを、再始動することができます。
3. ポリシーを変更するためには、WebSphere for z/OS ランタイム・サーバー・インスタンスの既存エレメントの名前、および追加のランタイム・サーバー・インスタンスの新規エレメントの名前の命名規則を、知っている必要があります。

   WebSphere for z/OS ランタイム・サーバー・インスタンスのエレメント名を、表35 に示します。

表 35. WebSphere for z/OS ランタイム・サーバー・インスタンスの自動再始動管理エレメント名

サーバー・インスタンス	エレメント名 *
デーモン	CBDMNDAEMON01
システム管理	CBSRVSYSMGT01
ネーミング	CBSRVNAMING01
インターフェース・リポジトリー	CBSRVINTFRP01

表 35. WebSphere for z/OS ランタイム・サーバー・インスタンスの自動再始動管理エレメント名 (続き)

サーバー・インスタンス	エレメント名 *

* 最初のサーバー・インスタンスの接尾部は 01 です。その後のサーバー・インスタンスのレプリカの接尾部は、それぞれ 1 ずつ増えていきます。

298ページの表35 で示されているように、WebSphere for z/OS は、サーバー・インスタンスのエレメント名を、サーバー・インスタンス名に接頭部 CBSRV を付けて作成します。デーモン・サーバー・インスタンスは例外で、サーバー・インスタンス名に付く接頭部は CBDMN です。たとえば、SYSMGT01 というシステム管理サーバー・インスタンスのエレメント名は CBSRVSYSMGT01 ですが、DAEMON01 というデーモン・サーバー・インスタンスのエレメント名は CBDMNDAEMON01 です。

4. アプリケーションのサーバー・インスタンスの名前に、CBSRV という接頭部を付けます。たとえば、MYSERVER というサーバー・インスタンスの場合、エレメント名は CBSRVMYSERVER になります。
5. シスプレックスで WebSphere for z/OS がデータ非共用の構成になっている場合 (つまり、複数の個別の WebSphere for z/OS システムがシスプレックス上で動作していながら、データ共用を行っていない場合) は、ARM を使用可能にしないでください。
6. 再始動グループを作成する場合は、以下のものを同じ再始動グループに入れ、以下に示すようにエレメントの再始動順序を設定してください。
   a. RRS
   b. IRLM を伴う DB2 for OS/390
   c. 再始動グループでアプリケーション・サーバーによって使用される場合は、IMS、CICS、およびその他のトランザクションまたはリソース・マネージャー
   d. WebSphere for z/OS デーモン・サーバー・インスタンス
   e. WebSphere for z/OS システム管理、ネーミング、およびインターフェース・リポジトリー・サーバー・インスタンス

      注: デーモン・サーバー・インスタンスは、通常はシステム管理、ネーミング、およびインターフェース・リポジトリー・サーバー・インスタンスを開始しますが、再始動時にはこれらを開始しません。これらのサーバー・インスタンスは自動再始動管理によって再始動されます。したがって、再始動ポリシーを変更する場合は、そのポリシーにこれらが組み込まれていることを確認してください。

f. ユーザーのアプリケーション・サーバー・インスタンス

アカウンティング

WebSphere for z/OS はエンクレーブを使用するので、サーバー・インスタンスおよびクライアントに与えられるサービスは、集計すると SMF 30 および SMF 72 レコードになります。

- 個々のエンクレーブ (システム内を移動するクライアント作業要求を記録するもの) は、個別の SRM トランザクションで、分類、制御および報告を個別に行います。
- エンクレーブ・トランザクションのカウントおよびリソース使用は、エンクレーブのサービス・クラスまたはパフォーマンス・グループ番号、およびインストール・アカウンティングおよびチャージ・バックのレポート・クラス、およびパフォーマンス・グループ番号に関して、SMF 72 レコードで記録されています。
- エンクレーブ・トランザクションのカウントおよびリソース使用は、そのエンクレーブを作成したアドレス・スペース (所有者アドレス・スペース) では、SMF 30 レコードで記録されます。エンクレーブ用の SMF 30 レコードはありません。
- エンクレーブにスケジュールされる SRB は、タスクと同じ優先権です。
- 既存のアカウンティング・パッケージは、SMF 30 レコードでも SMF 72 でも、変更する必要はありません。
- サーバーのアカウンティングについて
  - 分散作業の場合、CPU サービスは、サーバー・インスタンス制御領域のアドレス・スペースでは SMF 30 レコードに、エンクレーブのサービス・クラス期間では SMF 72 レコードに、組み込まれています。
  - ローカルに発生する作業の場合、CPU および MSO サービスは、クライアントのアドレス・スペースの SMF 30 レコードに、クライアントのサービス・クラス期間では SMF 72 レコードに、組み込まれています。
  - IOC および SRB サービスは、サーバー・インスタンスのアドレス・スペースでは、SMF 30 および SMF 72 レコードに組み込まれています。

エンクレーブのリソース・アカウンティングに関する詳細は、*z/OS MVS プログラミング : ワークロード管理サービス*, SA88-8585 を参照してください。

第6章 拡張トピック

この章では、シスプレックスのセットアップ、拡張 TCP/IP のセットアップ、手続き型アプリケーション・アダプターのセットアップなどの、拡張トピックを扱います。

シスプレックスでの WebSphere for z/OS の使用可能化

WebSphere for z/OS ランタイムおよびそれに関連したビジネス・アプリケーション・サーバーを、モノプレックスにインストールしたら、ランタイムおよびそれに関連したアプリケーション・サーバーを、シスプレックス構成にマイグレーションすることができます。シスプレックスにマイグレーションするメリットは、次のとおりです。

- 複数システムにわたるワークロードのバランスを取ることができ、したがって、アプリケーションのパフォーマンス管理が改善されます。
- ワークロードが大きくなるにつれて、新規システムを追加して要求を満たすことができ、したがって、処理に必要なスケーラブル・ソリューションが得られます。
- ランタイムおよびそれに関連したアプリケーション・サーバーのレプリカを生成することにより、ユーザーの可用性を保証するために必要なシステムの冗長度が得られます。したがって、たとえ 1 つのシステムに障害が発生しても、別のシステムを利用して作業を続けることができます。

シスプレックスの外側にあるシステムおよびアプリケーション・プログラムにとっては、WebSphere for z/OS シスプレックス構成は、そのシスプレックス内に複数の物理システムがあるとしても、単一のシステムのように見えます。このような構成は、ホスト・クラスター と呼ばれます。また、ホスト・クラスター内の WebSphere for z/OS サーバーの単一セットは、クラスター・ホスト・インスタンス と呼ばれます。

302ページの図8 はホスト・クラスターの一例を示すものです。ここでは、シスプレックス内の 3 つの OS/390 または z/OS システムのそれぞれが、WebSphere for z/OS のクラスター・ホスト・インスタンスをサポートしています。図の三角形は、3 つの OS/390 または z/OS システムをリンクするカップリング・ファシリティーを表します。

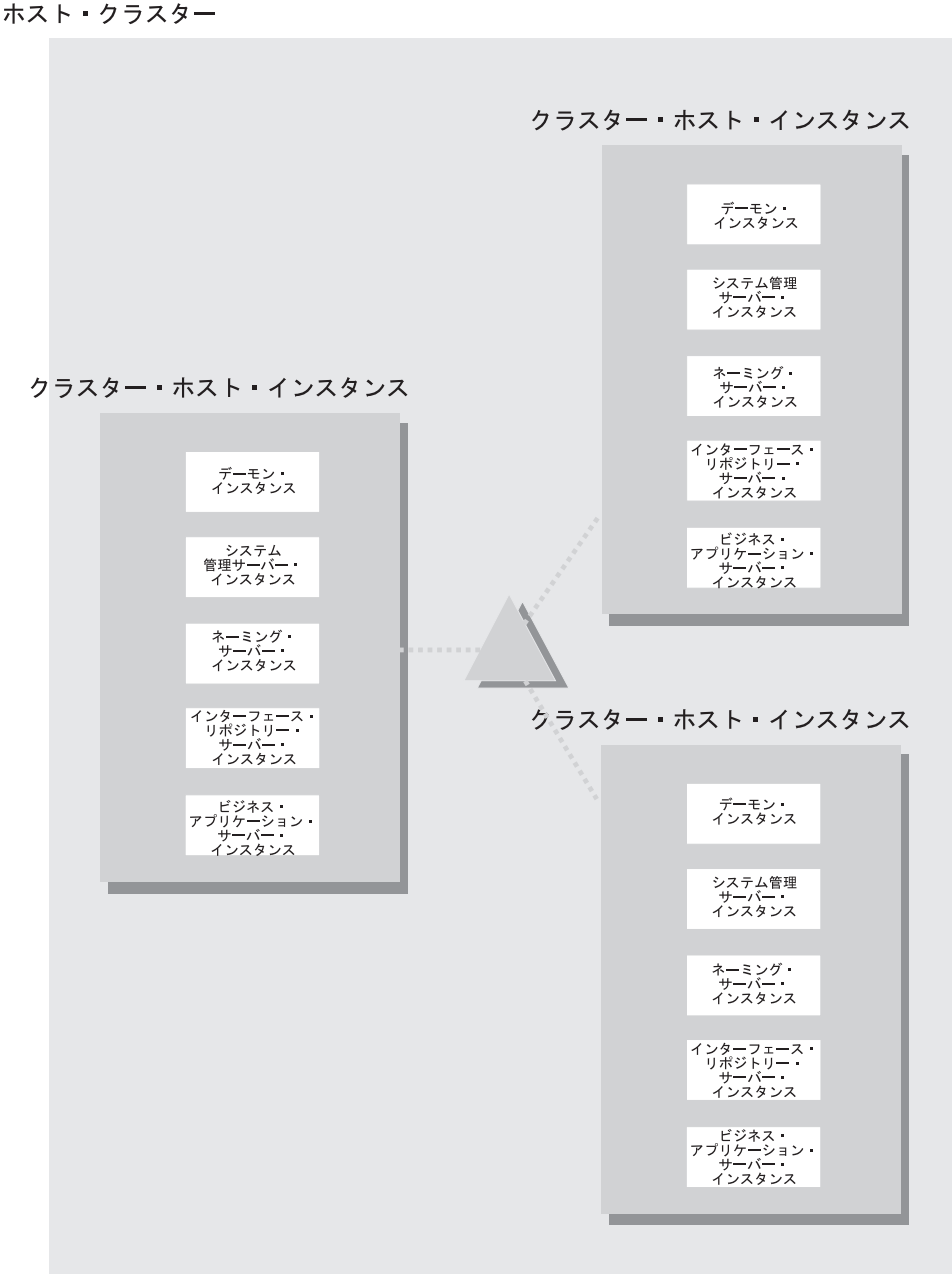


図 8. ホスト・クラスター

ホスト・クラスターは、ホストとして WebSphere for z/OS ネーム・スペースに構成され、単一のデーモン IP 名として表されます。単一のデーモン IP 名

があるために、シスプレックスの外側のシステムおよびアプリケーションは、シスプレックスを単一ホストとして扱います。WebSphere for z/OS の機能は、OS/390 または z/OS のサブシステム (TCP/IP、ドメイン・ネーム・サーバー (DNS)、ワークロード管理など) と連携して、サーバー・インスタンスの可用性およびワークロードの平衡化規則に従って、シスプレックスを介した作業の経路を定めます。

次の表は、WebSphere for z/OS を使用可能化するための、サブタスクおよび関連手順を示したものです。

サブタスク	関連手順 (参照箇所)
シスプレックスをセットアップする	*z/OS MVS シスプレックスのセットアップ*, SA88-8591
WebSphere for z/OS 構成およびシスプレックスに関する決定を下す	304ページの『WebSphere for z/OS およびシスプレックスの計画のためのステップ』
セキュリティー・システムを作成する	306ページの『セキュリティー・システムを作成するためのステップ』
データ共用をセットアップする	*DB2 データ共用 : 計画および管理*, SC88-7380 307ページの『データ共用をセットアップするためのステップ』
シスプレックスの他のシステムで、OS/390 または z/OS 基本機能をカスタマイズする	307ページの『シスプレックス内の他のシステムで OS/390 または z/OS の基本機能をカスタマイズするためのステップ』
TCP/IP を変更する	311ページの『TCP/IP を変更するためのステップ』
シスプレックス内の他のシステム用の LDAP ファイルをセットアップする	312ページの『シスプレックス内の他のシステム用の LDAP ファイルをセットアップするためのステップ』
シスプレックスで、WebSphere for z/OS の新規クラスター・ホスト・インスタンスを定義する	314ページの『シスプレックス内での WebSphere for z/OS の新規クラスター・ホスト・インスタンスの定義』
WebSphere for z/OS システムの最新表示を行う	319ページの『2 番目のシステムで WebSphere for z/OS をキャンセルおよび再始動するためのステップ』
インストール検査プログラムを使用して構成を検査する	319ページの『インストール検査プログラムを実行するためのステップ』

WebSphere for z/OS およびシスプレックスの計画のためのステップ

モノプレックス、あるいはシスプレックスの 1 つのシステム上に WebSphere for z/OS をインストールしたら、今度はそれをシスプレックスで使用可能にすることができます。このトピックでは、シスプレックス配置のための計画ステップを取り上げます。

この作業を始める前に: モノプレックス、あるいはシスプレックスの 1 つのシステム上で、WebSphere for z/OS のインストールおよびカスタマイズを完了していなければなりません。また、OS/390 または z/OS シスプレックスを使用可能にしていなければなりません。シスプレックスに関する詳細は、*z/OS MVS シスプレックスのセットアップ*, SA88-8591 を参照してください。

WebSphere for z/OS およびシスプレックスを計画するには、以下のステップに従ってください。

1. エラー・ログの単一システム表示が必要かどうかを決定する。エラー・ログの単一システム表示が必要であり、最初にシステム・ロガーおよびロギングに使用する DASD でエラー・ログをセットアップする場合は、ここで、カップリング・ファシリティーを使用してエラー・ログを構成しなければなりません。

   ---

2. シスプレックス内で、読み取り / 書き込みモードで HFS を共用する方法を確立する。WebSphere for z/OS は、サーバー開始プロシージャーが使用する環境ファイルの書き込みに、この HFS を使用します (詳しくは、383 ページの『付録A. 環境ファイル』を参照してください)。 OS/390 または z/OS バージョン 2 リリース 8 では、ネットワーク・ファイル・システムを使用しなければなりません。OS/390 または z/OS バージョン 2 リリース 9 では、ネットワーク・ファイル・システムまたは、共用 HFS 機能のいずれかを選択することができます。

   ---

3. シスプレックスでアプリケーション実行可能プログラムを共用する方法を決定する。ヒントと推奨については、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

   ---

4. ARM をセットアップする。本リリースは、システム間再始動をサポートしていません。したがって、ユーザーの ARM ポリシーをそれに応じてセットアップする必要があります。個々のエレメントが動作するシステム上で、

TARGET_SYSTEM が指定されていることを確認してください (デフォルトの TARGET_SYSTEM=* を指定していれば、システム間再始動が利用できます)。

---

5. すべての WebSphere for z/OS ランタイム・サーバーのレプリカを生成するかどうかを決定する。次の表は、シスプレックスでサーバー・インスタンスのレプリカを生成する際の、推奨と要件を示すものです。

表 36. シスプレックスでのサーバー・インスタンスのレプリカ生成

サーバー	シスプレックスでサーバー・インスタンスのレプリカを生成する際の推奨と要件
デーモン・サーバーおよびシステム管理サーバー	• シスプレックスの各システムで WebSphere for z/OS 作業を実行したい場合は、どちらのサーバー・インスタンスでもレプリカを生成しなければなりません。つまり、シスプレックス内に、WebSphere for z/OS も WebSphere for z/OS アプリケーションも実行しないシステムがあっても差し支えありません。しかし、WebSphere for z/OS アプリケーションを実行したいシステムには、デーモン・サーバーおよびシステム管理サーバー・インスタンスが必要です。 • サーバーが、クライアントとの対話にはパスチケットが望ましいと指示する場合は、OS/390 または z/OS クライアントが常駐するシステム上で、デーモン・サーバーおよびシステム管理サーバー・インスタンスを開始する必要があります。
ネーミング・サーバー	• シスプレックスには、ネーミング・サーバー・インスタンスが少なくとも 1 つはなければなりません。しかもそれは、ユーザーが WebSphere for z/OS ブートストラップを実行するシステム上にある必要があります。 • IBM は、シスプレックス内の個々のシステムで、ネーミング・サーバー・インスタンスのレプリカを生成することを強くお勧めします。シスプレックス内のすべてのシステムで、ネーミング・サーバー・インスタンスのレプリカが生成されていない場合は、可用性のために、少なくとも 1 つの別のシステムにそのレプリカを生成することをお勧めします。

表 36. シスプレックスでのサーバー・インスタンスのレプリカ生成 (続き)

サーバー	シスプレックスでサーバー・インスタンスのレプリカを生成する際の推奨と要件
インターフェース・リポジトリー・サーバー	• インターフェース・リポジトリー・サーバー・インスタンスは、少なくとも 1 つはなければなりません。しかもそれは、ユーザーが WebSphere for z/OS ブートストラップを実行するシステム上にある必要があります。 • 可用性のために、このサーバー・インスタンスのレプリカを生成することができます。 • 述部評価を照会するアプリケーションがある場合は、IBM は、シスプレックス内の各システムで、このサーバー・インスタンスのレプリカを生成することをお勧めします。

6. 共用の PROCLIB を使用するかどうかを決定する。

   推奨: 共用デーモン、システム管理、ネーミング、およびインターフェース・リポジトリーの開始プロシージャーを含む、共用の PROCLIB を作成してください。開始プロシージャーを実行する際には、START コマンドでステップ修飾を使用することができます。これを使用すると、これまでより簡単に、システム・ログでサーバー・インスタンスの名前を認識することができるようになります。また、サーバー・インスタンスが SRVNAME パラメーターを介して始動するよう、指定することもできます。

   例:

```
S BBODMN.DAEMON01,SRVNAME='DAEMON01'
S BBODMN.DAEMON02,SRVNAME='DAEMON02'
```

セキュリティー・システムを作成するためのステップ

この作業を始める前に: 19ページの『セキュリティーのセットアップ』の、セキュリティーに関するバックグラウンド情報を読んでおいてください。

セキュリティー・システムを作成するには、以下のステップに従ってください。

1. WebSphere for z/OS をシスプレックスの複数のシステムに置く場合は、共用の RACF データベースをインプリメントする。WebSphere for z/OS は、ユーザー ID が、シスプレックスのすべてのシステムで、同じユーザー識別を表すものと想定します。

2. 個々の制御領域およびサーバー領域のレプリカは、シスプレックス全体で同じ権限を持っていなければなりません。これは、次の方法で達成できます。
   - 共用の開始プロシージャーを使用して、RACF に対するユーザー識別を、STARTED クラスを介して定義します。その他の RACF 権限は、STARTED クラスで定義されるユーザー識別に対して認可されます。したがって、制御領域およびサーバー領域のレプリカは、シスプレックス内で同じユーザー ID で動作し、同じ権限を有します。
   - 個々のシステムに固有の開始プロシージャーを使用して、STARTED クラスを介して新規のユーザー識別を作成します。その後、制御領域およびサーバー領域のレプリカに、最初のシステムで認可したのと同じ権限を認可します。制御領域およびサーバー領域のレプリカは、他のシステムとは異なるユーザー ID で動作しますが、レプリカに対する権限も持っています。

データ共用をセットアップするためのステップ

この作業を始める前に: カップリング・ファシリティーを持っていなければなりません。

データ共用をセットアップするには、以下のステップを実行してください。

1. DB2 for OS/390 のデータ共用をセットアップします。詳細は、*DB2 データ共用 : 計画および管理*, SC88-7380 を参照してください。

---

2. カップリング・ファシリティーに BP32K バッファー・プールがなければなりません。所有する BP32K バッファー・プールの数と、DSNDB07 データベースのサイズを調べてください。

データ共用が機能していれば、このステップは終了したことになります。

シスプレックス内の他のシステムで OS/390 または z/OS の基本機能をカスタマイズするためのステップ

WebSphere for z/OS の最初のインストールおよびカスタマイズで行ったのと同じカスタマイズを、OS/390 または z/OS の基本機能に対しても繰り返します。ここでは、便宜上ステップを繰り返しています。

この作業を始める前に: SMP/E を使用して WebSphere for z/OS の製品コードをインストールし、製品のサンプル・ファイルのコピーを作成する必要があります。

基本システムを変更するには、以下のステップを実行します。

1. BBO.SBBOJCL 内の SCHEDxx を変更して、BBOSCHED サンプル・ファイルに入っているステートメントを組み込みます。

---

2. BBO.SBBOLOAD、BBO.SBBOLD2、および BBO.SBBOLPA データ・セットの、APF 許可を行います。

   例: PROGxx PARMLIB メンバーには次のものを組み込むことができます。

```
APF FORMAT(DYNAMIC)
/*********************************************************************/
/* BOSS LOCAL DATASETS                                               */
/*********************************************************************/
APF ADD
    DSNAME(BBO.SBBOLOAD)
    VOLUME(vvvvvv)
APF ADD
    DSNAME(BBO.SBBOLD2)
    VOLUME(vvvvvv)
APF ADD
    DSNAME(BBO.SBBOLPA)
    VOLUME(vvvvvv)
```

   ここで、vvvvvv はユーザーのボリューム ID です。

---

3. 言語環境プログラム・データ・セット SCEERUN、および DB2 for OS/390 データ・セット SDSNLOAD が許可済みであることを確認します。

---

4. BBO.SBBOULIB または SBBOMIG は、クライアント・ユーザーの権限の下で実行されるべきものなので、APF 許可を行っては**なりません**。

---

5. 次の表を使用して、WebSphere for z/OS のモジュールを配置します。

表 37. LPA またはリンク・リストでのモジュールの配置

モジュール	注
BBO.SBBOLPA	すべてのメンバーを LPA にロードします。
BBO.SBBOLOAD	すべてのメンバーを、LPA に動的にロードすることをお勧めします。仮想記憶域がコンストレインドである場合は、メンバーをリンク・リストに置いてください。

表 37. LPA またはリンク・リストでのモジュールの配置 (続き)

モジュール	注
BBO.SBBOLD2(BBORSMCT)	WebSphere for z/OS で Web サーバー・サーブレットを使用する計画の場合は、SBBOLD2(BBORSMCT) を、LPA またはリンク・リスト に配置しなければなりません。
BBO.SBBOLD2	BBORSMCT は別として、SBBOLD2 からのメンバーは、LPA には配置**しないでください**。これらのメンバーは、リンク・リストに配置します。
BBO.SBBOULIB	これらのメンバーは、LPA またはリンク・リストの**いずれにも、配置しないでください**。

注:

a. メンバーは PDSE に常駐しているため、LPA に動的にロードしなければなりません。また OS/390 または z/OS は、システムの初期設定時には PDSE のメンバーをロードすることができません。**例:** 以下のコマンドを発行してください。

```
SETPROG LPA,ADD,MASK=*,DSNAME=hlq.SBBOLOAD
SETPROG LPA,ADD,MASK=*,DSNAME=hlq.SBBOLPA
```

ここで、*hlq* は、使用している WebSphere for z/OS データ・セットの上位修飾子です。

重要: LPA のサイズが、WebSphere for z/OS のモジュールを保持できる大きさであることを確認してください。49ページの『メモリーの使用に関する推奨』を参照してください。

b. すでに LPA に入っている BBO.SBBOLPA、BBO.SBBOLOAD、または BBO.SBBOLD2 からのモジュールと同じ名前のモジュールは、必ず除去してください。

c. WebSphere for z/OS のモジュールを、IPL 後に LPA にロードするには、自動化更新することをお勧めします。COMMNDxx は、コマンドが使用可能にされる DFSMS サービスに先だって実行されるため、このタスクには適していません。

---

6. APF 許可または LPA に PROGxx ファイルを使用した場合は、必ず次のコマンドを発行してください。

```
SET PROG=xx
```

ここで、xx は PROGxx メンバーの接尾部です。

---

7. すべての BBO.* データ・セットおよびすべての LDAP データ・セットが、カタログを作成していることを確認してください。これは必須ではありませんが、そうすることを強くお勧めします。

---

8. SYS1.PARMLIB(BLSCUSER) メンバーを、BBO.SBBOJCL 内のメンバー BBOIPCSP によって提供された IPCS モデルで更新します。BLSCUSER の詳細は、*z/OS MVS 対話式問題管理システム (IPCS) ユーザーズ・ガイド*, SA88-8568 を参照してください。

---

9. SMF 記録を開始して、WebSphere for z/OS システムについて、システムとジョブに関連した情報を収集したい場合は、次のようにします。
   a. SMFPRMxx parmlib メンバーを編集します。
      1) ACTIVE ステートメントを挿入して、SMF の記録を指示します。
      2) システムに作成させたい SMF レコードのタイプを示すために、SYS ステートメントを挿入します。たとえば、タイプ 120 のレコードだけを選択するには、SYS(TYPE(120:120)) を使用します。パフォーマンスへの影響を最小にするために、選択したレコード・タイプの数は少なくしておいてください。
   b. DASD へのレコードの書き込みを開始するために、次のコマンドを発行します。

      ```
      t smf=xx
      ```

      ここで、xx は SMF parmlib メンバー (SMFPRMxx) の接尾部です。SMF parmlib メンバーの詳細については、*z/OS MVS システム管理機能 (SMF)*, SA88-8596 を参照してください。

      DASD への書き込みを活動状態にすると、データが (SMFPRMxx で指定した) データ・セットの中に記録されます。

   注: その後、管理アプリケーションのインストールが完了した時点で、いくつかのプロパティーをサーバー・プロパティー・フォーム上で定義することにより、サーバーに SMF レコードを収集させることができます。WebSphere for z/OS と SMF 記録の使用の詳細については、*WebSphere Application Server V4.0 for z/OS and OS/390: 操作および管理*, SA88-8653 を参照してください。

TCP/IP を変更するためのステップ

この作業を始める前に: TCP/IP のインストールおよび構成を行っていなければなりません。

TCP/IP を変更するには、以下のステップを実行してください。

1. DNS 項目を変更する。サーバー・インスタンスのレプリカを動的に解決する、汎用 IP 名の使用を許可する DNS のインプリメンテーションを使用していることを前提とすると、DNS での IP 名を調整する必要があります。デーモンの汎用 IP 名は保持しますが、2 番目以降のデーモン・サーバー・インスタンスには新規の IP 名を追加します。これは、ワークロードの平衡化だけでなく、サーバー・インスタンスに障害が発生した場合にも重要です。これで、DNS は、作業を他のサーバー・インスタンスに送信することができます。

   詳しくは、321ページの『接続の最適化』、および 322ページの『IBM Network Dispatcher』を参照してください。

---

2. シスプレックスの個々の追加システム用 TCP/IP プロファイルで、解決 IP ポート用にポート 900 を追加し、それを、新規のシステム管理サーバー・インスタンスの名前と関連付ける。デフォルトでは、WebSphere for z/OS は最初のシステム管理サーバー・インスタンスに SYSMGT01 という名前を付け、新規にシステム管理サーバー・インスタンスが作成されるたびに、その名前の接尾部を増分します (SYSMGT02、SYSMGT03、など)。したがって、シスプレックスの 2 番目のシステムでは、ポート 900 を追加して、それを SYSMGT02 に関連付けます。

   例:

   ```
   900   TCP     SYSMGT02
   ```

   シスプレックスの 3 番目以降のシステムでも、同じパターンに従ってください。

---

3. シスプレックスの個々の追加システム用 TCP/IP プロファイルの中で、デーモン用のポートを追加し、それを、新規のデーモン・サーバー・インスタンス名へ関連付ける。デフォルトでは、WebSphere for z/OS はデーモン用にポート 5555 を使用します。また、WebSphere for z/OS は最初のデーモン・サーバー・インスタンスに DAEMON01 という名前を付け、新しいデーモン・サーバー・インスタンスごとに、この名前の接尾部を

(DAEMON02、DAEMON03 などのように) 増分します。したがって、シスプレックスの 2 番目のシステムでは、ポートを追加して、それを DAEMON02 に関連付けます。

例:

```
5555   TCP     DAEMON02
```

シスプレックスの 3 番目以降のシステムでも、同じパターンに従ってください。

---

4. 管理アプリケーションを実行するワークステーション上のワークステーション・ホスト・ファイルを更新し、シスプレックスとシスプレックス内で実行されているシステムの IP 名を組み込む。**例:** シスプレックス名は WSCCB で、このシスプレックス内に WSCCB1 と WSCCB2 という 2 つのシステムが存在します。ワークステーション・ホスト・ファイル内の項目は、次のようになります。

```
#
9.82.93.1 wsccb1.washington.ibm.com  wsccb1 #CB Daemon_IPname and alias for wsccb1
#
9.82.93.2 wsccb2.washington.ibm.com  wsccb2 #CB Daemon_IPname and alias for wsccb2
#
9.82.93.1 wsccb.washington.ibm.com   wsccb #CB Daemon_IPname and alias for wsccb
#
```

これで、TCP/IP の更新は完了しました。

シスプレックス内の他のシステム用の LDAP ファイルをセットアップするためのステップ

最初のインストールおよびカスタマイズの際にしたように、新規の LDAP サーバーを作成する必要はありません。ネーミング・サーバーとインターフェース・リポジトリー・サーバーのインスタンスを実行するそれぞれの新規システムについて、固有の bboslapd.conf、bboldif.cb、および dsnaoini ファイルを作成する必要があります。これは、個々の dsnaoini ファイルがシステム特有のもので、固有の DB2 for OS/390 サブシステムを参照するためです。マルチシステム構成で複数のサーバー・インスタンスが存在する場合、個々のネーミングおよびインターフェース・リポジトリー・サーバー領域は、システム特有の dsnaoini ファイルを参照する必要があります。

WebSphere for z/OS の最初のインストールおよびカスタマイズの際には、これらのファイルのために設定された命名規則に従います。つまり、ファイル名に

はシステム名を、これらのファイルおよびデータ・セットにはデータ・セット名を使用します。以下のステップで、その方法を説明します。

この作業を始める前に: LDAP を WebSphere for z/OS 用に構成しておかなければなりません。

重要: すでに、最初のインストールおよびカスタマイズでセットアップするように、LDAP をセットアップしている場合は、LDAP のテーブル作成、バインド、またはバルク・ローダー・ジョブを、再実行**しないで**ください。これらのジョブを実行すると、既存のネーム・スペースが破棄されます。94ページの『LDAP および WebSphere for z/OS ネーム・スペースのセットアップ』を参照してください。

この手順では、ユーザーが、最初のインストールおよびカスタマイズ時に、LDAP ファイル用の共用 HFS ディレクトリーを作成していることを前提としています。このディレクトリーは BBOMCFG ジョブによって作成され、デフォルト・ディレクトリーは `/WebSphere390/CB390/etc` です。

シスプレックスで他のシステム用の LDAP ファイルをセットアップするには、以下のステップを実行してください。

1. `/WebSphere390/CB390/etc` の中に、新しい bboslapd.conf、bboldif.cb、および dsnaoini ファイルを作成します。次の命名規則に従うことをお勧めします。
   - *system*.bboslapd.conf
   - *system*.bboldif.cb
   - *system*.dsnaoini

   ここで、*system* はシスプレックス内の 2 番目のシステムの名前です。シスプレックス内の 3 番目以降のシステムに WebSphere for z/OS を配置したい場合は、このステップを繰り返してください。

   ---

2. 個々の新規 dsnaoini ファイルを、そのシステム上の DB2 for OS/390 のサブシステム名を参照するように変更します。DB2 for OS/390 のグループ接続名は使用できません。

これで、必要な LDAP ファイルができました。

シスプレックス内での WebSphere for z/OS の新規クラスター・ホスト・インスタンスの定義

シスプレックスの追加システムを、そのシステムのサーバー・インスタンスを使用して定義するには、管理アプリケーションを使用します。最初の WebSphere for z/OS システムは、アプリケーション・サーバー BBOASR1 (インストール検査プログラムで使用される、アプリケーション・サーバー) を使用してすでに作成されているものとします。

ここでは、2 番目のシステムを定義する方法を説明します。3 番目以降のシステムについても、これと同じステップを実行してください。

2 番目の WebSphere for z/OS システムを定義するためのステップ

この手順では、管理アプリケーションを使用して、2 番目の WebSphere for z/OS ランタイム・システムを作成する方法について説明します。

この作業を始める前に: 最初の WebSphere for z/OS システムがインストールされ、稼働していなければなりません。そうなっていない場合は、RRS、次いで DB2 for OS/390 を始動してください。その後、次のように WebSphere for z/OS を始動します。

```
S BBODMN.DAEMON01
```

2 番目の WebSphere for z/OS システムを定義するには、以下のステップに従ってください。

1. 管理アプリケーションにログオンする。

   _____

2. 会話を追加する。

   _____

3. シスプレックスで 2 番目のシステムを定義する。ランタイム・サーバー・インスタンスは自動的に定義されます。

   _____

4. 2 番目のシステム上にある個々のランタイム・サーバー・インスタンスの環境変数を検査する。環境変数は、シスプレックス、サーバー、サーバー・インスタンスの順序で、階層的に定義されます。階層の低い環境変数は、それとマッチングする階層の高い環境変数を上書きします。しかし、環境変数は特にサーバー・インスタンス・レベルで定義されていない限り、「プロパティー (properties)」フォームには表示されません。したがって、サーバー・インスタンス・レベルでは環境変数が見えない場合もあります。環境変数の一部を上書きするかどうかを決定するためには、サーバーおよびシスプレッ

クス・レベルで、環境変数を検査してください。環境変数には、シスプレックス内のすべてのシステムに共通するものと、各システムに固有のものとがあります。

以下の環境変数をサーバー・インスタンス・レベルで上書きしなければなりません。それぞれのランタイム・サーバー・インスタンスのプロパティー・フォームへ進み、表38 に示すように環境変数の値をコード化してください。

表 38. シスプレックス内のサーバー・インスタンス環境変数

サーバー	サーバー・インスタンス	変更する環境変数	値
デーモン	DAEMON02	DM_SPECIFIC_SERVER_NAME	DAEMON02
		SM_SPECIFIC_SERVER_NAME	SYSMGT02
		NM_SPECIFIC_SERVER_NAME	NAMING02
		IR_SPECIFIC_SERVER_NAME	INTFRP02
		SYS_DB2_SUB_SYSTEM_NAME	使用している DB2 for OS/390 サブシステムの名前
システム管理	SYSMGT02	DM_SPECIFIC_SERVER_NAME	DAEMON02
		SM_SPECIFIC_SERVER_NAME	SYSMGT02
		NM_SPECIFIC_SERVER_NAME	NAMING02
		IR_SPECIFIC_SERVER_NAME	INTFRP02
		SYS_DB2_SUB_SYSTEM_NAME	使用している DB2 for OS/390 サブシステムの名前
ネーミング	NAMING02	DM_SPECIFIC_SERVER_NAME	DAEMON02
		SM_SPECIFIC_SERVER_NAME	SYSMGT02
		NM_SPECIFIC_SERVER_NAME	NAMING02
		IR_SPECIFIC_SERVER_NAME	INTFRP02
		SYS_DB2_SUB_SYSTEM_NAME	使用している DB2 for OS/390 サブシステムの名前
インターフェース・リポジトリー	INTFRP02	DM_SPECIFIC_SERVER_NAME	DAEMON02
		SM_SPECIFIC_SERVER_NAME	SYSMGT02
		NM_SPECIFIC_SERVER_NAME	NAMING02

表 38. シスプレックス内のサーバー・インスタンス環境変数 (続き)

サーバー	サーバー・インスタンス	変更する環境変数	値
		IR_SPECIFIC_SERVER_NAME	INTFRP02
		SYS_DB2_SUB_SYSTEM_NAME	使用している DB2 for OS/390 サブシステムの名前
ビジネス・サーバー・インスタンス (BBOASR1B、BBOASR1C など)	INTFRP02	DM_SPECIFIC_SERVER_NAME	DAEMON02
		SM_SPECIFIC_SERVER_NAME	SYSMGT02
		NM_SPECIFIC_SERVER_NAME	NAMING02
		IR_SPECIFIC_SERVER_NAME	INTFRP02
		SYS_DB2_SUB_SYSTEM_NAME	使用している DB2 for OS/390 サブシステムの名前

5. デーモン・サーバーが使用する開始プロシージャーを指定して、2 番目のシステムで、システム管理、ネーミング・サーバー、およびインターフェース・リポジトリー・サーバー・インスタンス (制御領域) を開始する。デーモンの開始後は、デーモンが自動的にこれらのサーバー・インスタンス制御領域を開始します。SMPROC、NMPROC、および IRPROC 環境変数で、これらの開始プロシージャーを指定してください。

   シスプレックスで、ネーミングおよびインターフェース・リポジトリー・サーバー・インスタンスを追加する必要がない場合は、NMPROC および IRPROC 環境変数を NULL に設定します。ネーミングおよびインターフェース・リポジトリー・サーバー・インスタンスの、レプリカ生成に関するガイドラインについては、305ページの表36 を参照してください。

6. LDAPCONF 環境変数で、適切な LDAP bboslapd.conf ファイルを指定する。この bboslapd.conf ファイルが、今度は DB2 for OS/390 CLI 初期設定ファイル (ユーザーが、312ページの『シスプレックス内の他のシステム用の LDAP ファイルをセットアップするためのステップ』で作成した固有の

DSNAOINI ファイル) を指します。bboslapd.conf ファイルが正しい初期設定ファイルを指していることを確認してください。

推奨: LDAP の構成はシスプレックス内で行うことをお勧めします。そうすれば、ネーミング・サービスが完全なトランザクションであることが保証されます。LDAP をシスプレックスの外側のサーバーとして構成することも可能です。この場合は、LDAPCONF 環境変数は指定しません。

---

7. デフォルトの各 LRM (CB_OS/390_Base_DB2、CB_OS/390_Naming_DB2、CB_OS390_Repository_DB2、および CB_OS/390_SysMgt_DB2) で、2 番目のシステムに関連付けられている LRM インスタンスを開き、その 2 番目のシステム上で、DB2 for OS/390 サブシステムの接続データを追加する。

---

8. 2 番目のシステムの CB_OS/390_IVP_DB2 で、新規の LRM インスタンスを作成する。

これで、新しい WebSphere for z/OS ランタイムの定義が完了しました。『新規サーバー・インスタンスを定義し、会話を活動化するためのステップ』へ進んでください。

新規サーバー・インスタンスを定義し、会話を活動化するためのステップ

この手順では、新規サーバー・インスタンスの作成方法と、新規の会話を活動化する方法について説明します。

この作業を始める前に: 新規 WebSphere for z/OS ランタイム・サーバーを 管理アプリケーションによって定義しなければなりません。

以下のステップを実行して、新規サーバー・インスタンスを定義し、会話を活動化してください。

1. 2 番目のシステム上の新規サーバー・インスタンス (たとえば、サーバー・インスタンス BBOASR1B) を定義する。

---

2. 個々の新規サーバー・インスタンスのプロパティー・フォームで、サーバー・インスタンスの必要に応じて環境変数の設定を上書きする。SM_SPECIFIC_SERVER_NAME の値を SYSMGT02 に変更する。

---

3. 個々の新規サーバー・インスタンスに対する適当な論理リソース・マネージャー・インスタンスを、新システム上の DB2 for OS/390 のサブシステム名と関連付ける。

   _____

4. 新規会話の妥当性を検査する。

   _____

5. 新規会話をコミットする。

   _____

6. すべてのタスクを完了する。

   _____

7. すべてのタスクに完了のマークを付ける。

   _____

8. 新規会話を活動化する。

   _____

活動化が成功すれば、このステップは終了です。『2 番目の WebSphere for z/OS システムで失敗した会話を再活動化するためのステップ』はスキップしてください。

活動化に失敗したとしても、問題ありません。WebSphere for z/OS は、2 番目のシステムではサーバー・インスタンスを初期化できなかったということです。『2 番目の WebSphere for z/OS システムで失敗した会話を再活動化するためのステップ』に進んでください。

2 番目の WebSphere for z/OS システムで失敗した会話を再活動化するためのステップ

直前の手順の 8 のステップで、活動化に失敗した場合は、このプロシージャーのステップに従って、失敗した会話を活動化してください。

この作業を始める前に: 314ページの『2 番目の WebSphere for z/OS システムを定義するためのステップ』を完了しておかなければなりません。

2 番目のシステム上で新規サーバー・インスタンスを定義するには、以下のステップに従ってください。

1. 2 番目のシステムで RRS および DB2 for OS/390 を開始する。

   _____

2. 2 番目のシステムで以下を発行する。

   ```
   SET PROG=XX
   ```

ここで、xx は PROGxx メンバーの接尾部です。

---

3. 2 番目のシステムで WebSphere for z/OS を開始する。

```
S BBODMN.DAEMON02,SRVNAME='DAEMON02'
```

---

4. 直前の手順の 8 のステップで失敗した会話を活動化する。

注: 活動化プロセスにより、新規のサーバー・インスタンスが始動します。すでに始動しているサーバー・インスタンスがある場合は、活動化プロセスはそれをシャットダウンした後、再始動します。

2 番目のシステムで WebSphere for z/OS をキャンセルおよび再始動するためのステップ

この作業を始める前に: この節でこれまで述べてきたすべての手順を、完了していなければなりません。

WebSphere for z/OS システムをキャンセルおよび再始動するには、以下のステップに従ってください。

1. シスプレックスの 2 番目のシステムでデーモンをキャンセルする。

```
C BBODMN.DAEMON02
```

---

2. 2 番目のシステムで WebSphere for z/OS を再始動する。

```
S BBODMN.DAEMON02,SRVNAME='DAEMON02'
```

---

2 番目のシステムで WebSphere for z/OS が初期化されれば、このステップは終了です。

インストール検査プログラムを実行するためのステップ

この作業を始める前に: シスプレックス内のすべての WebSphere for z/OS システムを、再初期化しなければなりません。

BBOIVP クライアント・ジョブのコピーを取得している必要があります。

インストール検査プログラムを実行するには、次のステップに従ってください。

1. ユーザーが定義した新規システムで、BBOIVP を実行する。

   ---

2. ローカルの BBOASR1 サーバー・インスタンスをキャンセルし、BBOIVP をローカルで実行して、シスプレックスの別のシステムのサーバー・インスタンスに、作業を移す。**例:** 2 番目のシステムの BBOASR1B サーバー・インスタンスをキャンセルします。BBOASRIA を最初のシステムで実行しておきます。管理アプリケーション、またはキャンセル・コマンドを使用します。

   ```
   c BBOASR1.BBOASR1B
   ```

   2 番目のシステムで BBOIVP を実行依頼します。

インストール検査プログラムが正常に動作すれば、このステップは終了です。

拡張 TCP/IP ネットワークのインプリメント

このトピックでは、次のような、拡張 TCP/IP の構成について説明します。

- OS/390 または z/OS での、複数の TCP/IP スタックの使用。
- 接続の最適化。これは OS/390 または z/OS の機能で、これによって、ワークロード管理と DNS が連携して、要求の経路を定めます。
- IBM Network Dispatcher。ネットワーク・ルーターです。
- バインド特有のサポート。これにより、WebSphere for z/OS での TCP/IP リソースの使用を制御することができます。

複数の TCP/IP スタック

複数の TCP/IP スタックを同一システム上で実行して、単一ポイントの障害でシステム全体がダウンする可能性を削減することができます。たとえば、ユーザーの System/390 をネットワークに接続する OSA 機構が複数あり、それぞれに TCP/IP スタックを割り当てたい場合があります。そのためには、共通の INET 物理ファイル・システム (C_INET PFS) を使用します。この物理ファイル・システムを使用すると、複数の物理ファイル・システム (ネットワーク・ソケット) を構成し、それらを並行して活動化することができます。

SYS1.PARMLIB(BPXPRMxx) の NETWORK DOMAINNAME パラメーターを介して、共通の INET を指定します。詳しくは、*z/OS UNIX システム・サービス 計画* および *z/OS Communications Server: IP Configuration Reference*, SC31-8776 を参照してください。

接続の最適化

322ページの図9 は、ドメイン・ネーム・サーバーがワークロード管理 (WLM) と連携して、シスプレックス内でクライアント要求の経路を定める際の構成を示しています。この構成の特性は以下のとおりです。

- 2 次 DNS のセットアップによって、シスプレックス内の複数のシステムで、ドメイン・ネーム・サーバー (DNS) のレプリカが生成されます。
- WebSphere for z/OS に接続するためには、クライアントがデーモンの IP 名を知っている必要があります。
- シスプレックス内の各システムのデーモン IP 名および解決 IP 名は、同じです。クライアント要求が実際にどのシステムに到達するかは、ワークロード管理およびドメイン・ネーム・サーバーが決定します。クライアントはシスプレックスを単一システムと見なしますが、その要求は、シスプレックス内のシステム間に均等に配分されます。
- ワークロード平衡化およびパフォーマンス最大化という目標の一環として、ワークロード管理はまた、作業要求の経路をシスプレックス内のシステムに定めます。この機能が可能となるのは、WebSphere for z/OS がワークロード管理と連携するためです (詳しくは、352ページの『ワークロード管理と WebSphere for z/OS』を参照してください)。クライアントが見るシステム参照は、間接的なものなので、その同じクライアントからの要求であっても、シスプレックス内の別のシステムが応答することもあります。
- クライアントは、失敗した接続から回復できない限り、IP アドレスはキャッシュに入れられないと考えます。つまり、接続が失敗した場合、クライアントは要求を再発行できるはずですが、IP アドレスが間接アドレスであるため、要求を再発行してもシスプレックス内の別のシステムが応答する可能性があります。

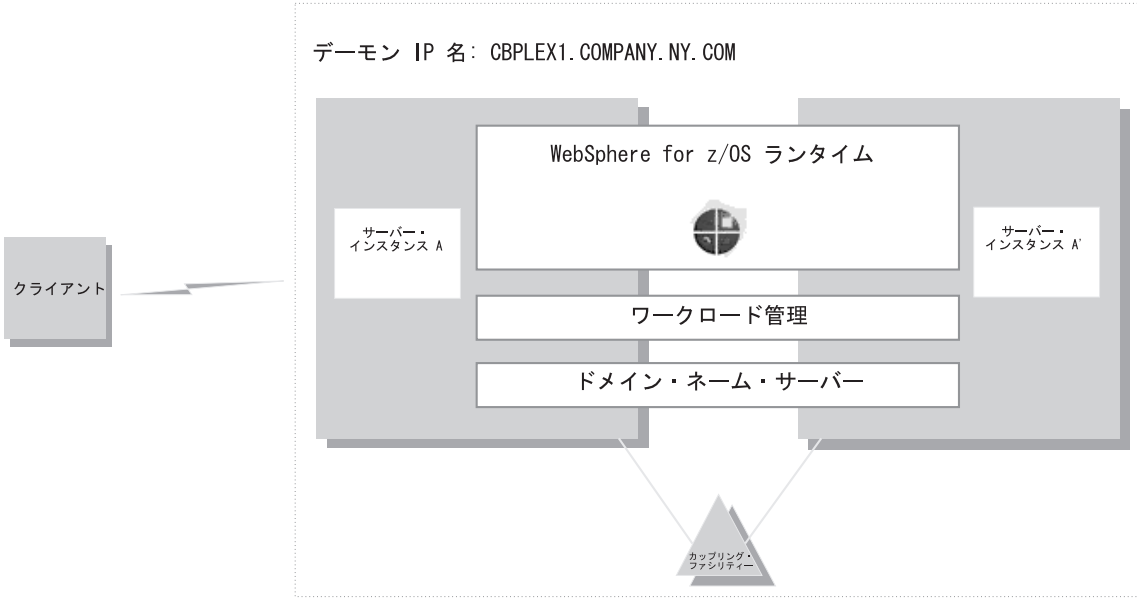


図 9. 接続最適化の構成

接続最適化のためのサーバーのセットアップに関する詳細は、*z/OS Communications Server: IP Configuration Reference*, SC31-8776 を参照してください。

IBM Network Dispatcher

IBM Network Dispatcher (323ページの図10 を参照) は、シスプレックスに対するネットワーク要求を処理するルーターです。この種の構成の特性は次のとおりです。

- デーモンの IP 名が、ルーターの IP アドレスと関連付けられます。
- IBM Network Dispatcher はワークロード管理と連携して、シスプレックスを介して要求の経路を定めます。クライアントには、IP アドレスの変更は認識されません。
- クライアントは、IP アドレスをキャッシュに入れることができると考えています。この構成が、IP アドレスを動的に変更しないためです。

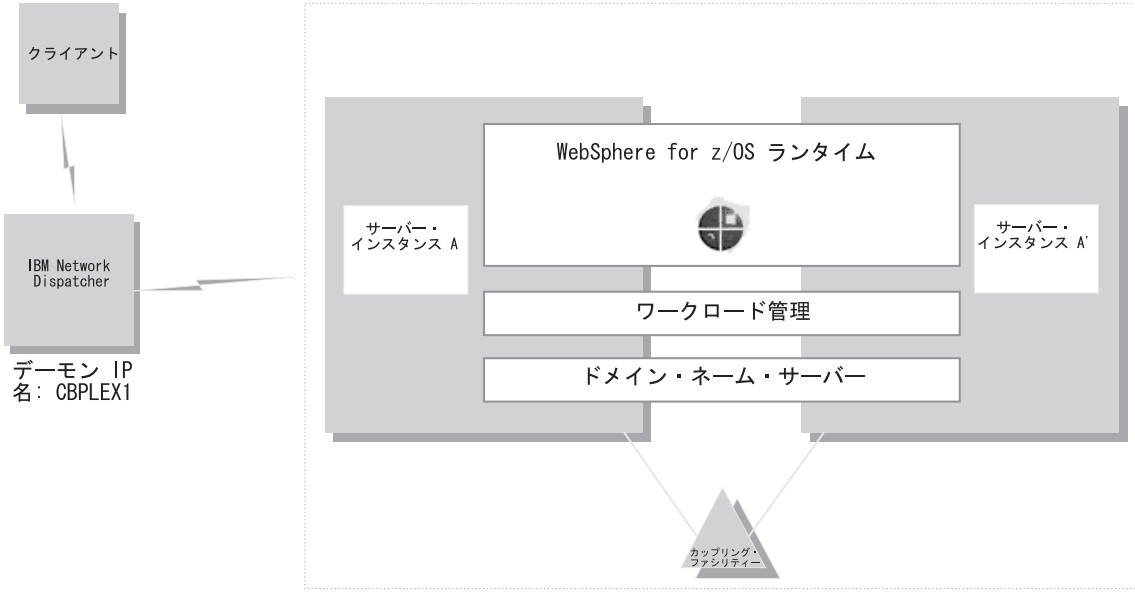


図 10. IBM Network Dispatcher の構成

WebSphere for z/OS でのバインド特有のサポート

WebSphere for z/OS でバインド特有のサポートを使用すると、WebSphere for z/OS での TCP/IP リソースの使用を制御することができます。このサポートにより、ユーザーは、固有ポートを構成するクライアント・コードを必要とすることなく、WebSphere for z/OS ORB およびその他の製品やアプリケーションを、同一の OS/390 または z/OS 上で所有することができます。つまり、このサポートにより、WebSphere for z/OS とその他の製品およびアプリケーションが、同一システム上でポート 900 を使用することができます。またこのサポートによって、WebSphere for z/OS ORB による複数 TCP/IP スタック (共通 INET) の利用、および同じ TCP/IP スタックでの複数 IP アドレスの使用も、可能になります。

バインド特有サポートを使用するには、SRVIPADDR 環境変数を使用してください。この環境変数は、ドット付き 10 進数形式で IP アドレスを指定します。WebSphere for z/OS サーバーは、この IP アドレス上のクライアント接続要求を listen します。

任意の IP アドレスは任意の TCP/IP スタックと関連付けられるので、WebSphere for z/OS サーバーが特定の TCP/IP スタックを使用するように、環境ファイルで SRVIPADDR 変数を指定することができます。

さらに、任意の TCP/IP スタックで複数の IP アドレスを定義できるため、WebSphere for z/OS のポート 900 サーバーは、ポート 900 を必要とする他の製品およびアプリケーションと、同じ TCP/IP スタックを共用することもできます。それらの IP アドレスを、SRVIPADDR を使用して固有のものにしたためです。

また別の選択肢として、バインド特有のサポートを使用せずに、ポート 900 の代替ポートとデーモンを定義することもできます。これらは、CORBA 標準で定義される唯一の値です。ただし、すべてのクライアント ORB が、ブートストラップ・ポートを 900 以外のポートに構成することを容易にサポートするかどうかは、明らかではありません。DAEMON_PORT および RESOLVE_PORT 環境変数でポート番号を指定して、デーモンおよびシステム管理サーバーのポートを構成してください。

環境変数に関する詳細は、383ページの『付録A. 環境ファイル』を参照してください。

複数 TCP/IP スタック (共通 INET) に関する詳細は、*z/OS UNIX システム・サービス 計画*, GA88-8639 を参照してください。同一 TCP/IP スタック上の複数 IP アドレスに関する詳細は、*z/OS Communication Server IP 構成解説書*, SC31-8776 を参照してください。

拡張セキュリティーのインプリメント

このトピックでは、次のような拡張セキュリティーに関する事柄について説明します。

- クライアントおよびサーバーのセキュリティー・プロトコルの折衝方法
- SSL セキュリティーのセットアップ
- アサート ID 機能のセットアップ
- Kerberos セキュリティーのセットアップ

クライアントおよびサーバーのセキュリティー・プロトコルの折衝方法

クライアントおよびサーバーがサポートするセキュリティー・プロトコルはいくつかあるため、クライアントおよびサーバーが通信を保護する方法は多数あります。サーバーは、多数のセキュリティー機構を同時にサポートする場合があります。実行時に、クライアントおよびサーバーは、対話に使用するセキュ

リティーの種類を動的に折衝します。たとえば、あるクライアントはユーザー ID およびパスワードのセキュリティーをサポートしており、別のクライアントは SSL セキュリティーをサポートしている場合に、これらのクライアントが対話するサーバーは SSL、DCE、およびユーザー ID およびパスワードのセキュリティーをサポートしているとします。各クライアントおよびサーバーは、選択項目の番号付きリストに基づいて、使用するセキュリティーのタイプを折衝します。折衝は、リストのトップから開始されます。クライアントおよびサーバーがリストのトップでセキュリティーのタイプに同意できない場合は、折衝はリストの 2 番目のセキュリティー・タイプへ継続され、3 番目へと順に続きます。この折衝は、クライアントおよびサーバーが、使用するセキュリティーのタイプに同意するまで継続されます。使用するセキュリティーのタイプの折衝に成功すると、認証段階が始まります。認証に失敗すると、通信は終了し、クライアントの要求は失敗します。

注:

1. 現時点では、管理アプリケーションを通じて指定されたサーバーのセキュリティー設定の優先順位は、クライアントによって無視されます。
2. クライアントとサーバー間の折衝が、セキュリティーが使用されることなく終わることは、あり得ます。

クライアントが使用する選択項目の番号付きリストは、クライアントとサーバー間の対話の種類によって変化します。326ページの図11 には、クライアントとサーバー間の対話のタイプが記載されています。図の中の番号ラベルが付いているものについては、326ページの表39 で説明しています。

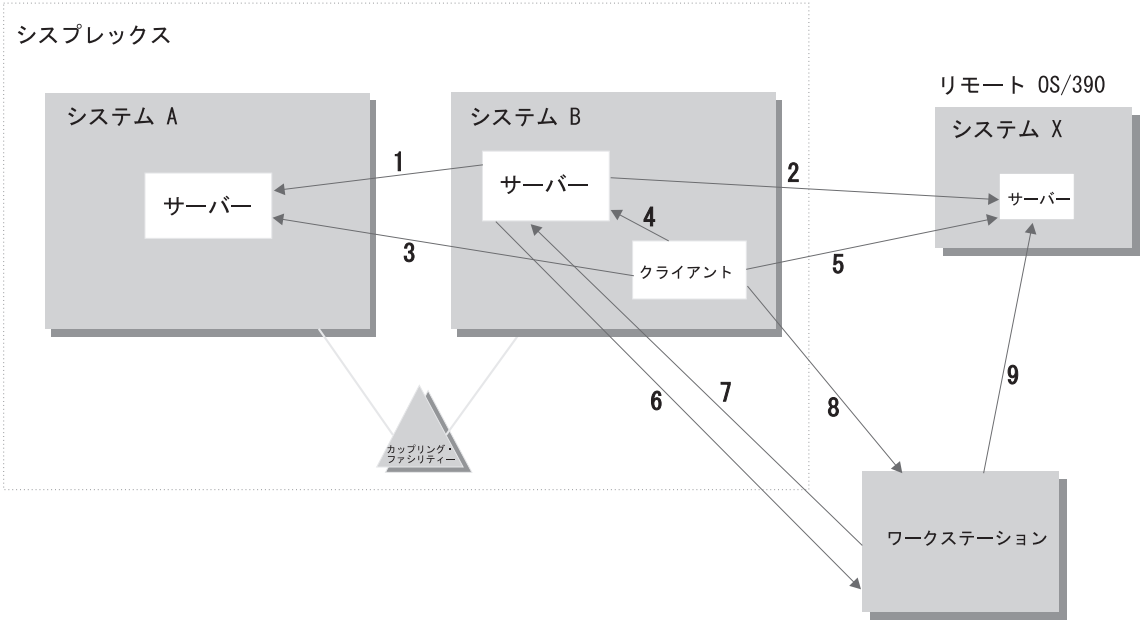


図 11. クライアントおよびサーバー間の対話

表 39. 対話に基づいた選択項目の番号付きリスト

項目	対話のタイプ	この対話に使用される番号付きリスト
1	シスプレックス内でのサーバーからサーバーへ	1. SSL 上の Kerberos 2. アサート ID 3. ユーザー ID / パスチケット 4. DCE 5. SSL クライアント証明書 (サーバー ID のみを使用) 6. ユーザー ID / パスワード 7. セキュリティーなし
2	サーバーからリモート OS/390 または z/OS サーバーへ	1. SSL 上の Kerberos 2. アサート ID 3. DCE 4. SSL クライアント証明書 (サーバー ID のみを使用) 5. ユーザー ID / パスワード 6. セキュリティーなし

表 39. 対話に基づいた選択項目の番号付きリスト (続き)

項目	対話のタイプ	この対話に使用される番号付きリスト
3	シスプレックス内でのクライアントからサーバーへ	1. SSL クライアント証明書 2. SSL 上の Kerberos 3. SSL 基本認証 4. ユーザー ID / パスチケット 5. DCE 6. ユーザー ID / パスワード 7. セキュリティーなし
4	OS/390 または z/OS システム内でのクライアントからサーバーへ	ユーザー ID (RACO) が必ず使用されます。
5	クライアントからリモート OS/390 または z/OS サーバーへ	1. SSL クライアント証明書 2. SSL 上の Kerberos 3. SSL 基本認証 4. DCE 5. ユーザー ID / パスワード 6. セキュリティーなし
6	サーバーからワークステーションへ	1. DCE 2. SSL クライアント証明書 (サーバー ID を使用) 3. セキュリティーなし
7 および 9	ワークステーションから OS/390 または z/OS サーバーへ	ワークステーション・クライアントの構成によって決定されます。
8	クライアントからワークステーションへ	1. DCE プリンシパル / パスワード認証での SSL 2. DCE 3. セキュリティーなし

WebSphere for z/OS 用の SSL セキュリティーのセットアップ

このトピックでは、ユーザーは、SSL プロトコルおよび OS/390 または z/OS 上で暗号サービス・システム SSL がどのように機能するかを理解していることを前提としています。SSL プロトコルについての情報は、以下の Web サイトを参照してください。

`http://home.netscape.com/eng/ssl3/ssl-toc.html`

暗号サービス・システム SSL について、詳しくは、*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください。

ネットワーク内の保護されている通信およびユーザー認証にセキュリティーを追加したい場合は、Secure Sockets Layer (SSL) のセキュリティーを使用することができます。WebSphere for z/OS での SSL サポートには、次のような目的があります。

- ネットワーク上を流れるメッセージのセキュリティーを保護するために業界で認めているいくつかの手段を提供するため。このセキュリティーは、多くの場合、*トランスポート層セキュリティー* と呼ばれています。トランスポート層セキュリティーは、通信する 2 つのアプリケーション間でプライバシーとデータ保全性を提供する機能です。この保護は、基本トランスポート・プロトコルの最上部 (たとえば、TCP/IP の最上部) にあるソフトウェア層で発生します。

  SSL は、暗号化テクノロジーによって通信リンクのセキュリティーを提供し、ネットワーク内のメッセージの保全性を確保します。双方の当事者間で通信が暗号化されているので、第三者はメッセージを改ざんできません。また、SSL は機密性 (メッセージの内容が読まれないことを保証する)、再生の検出機能、および順不同の検出機能を提供します。
- さまざまな認証プロトコルを運用でき、機密が保護される通信媒体を提供するため。1 つの SSL セッションで複数の認証プロトコルを使用できます。認証プロトコルとは、通信する当事者たちの ID を証明する方式のことです。

  SSL サポートは、サーバーがそれ自体の ID を証明する機構を必ず備えています。WebSphere for z/OS 上の SSL サポートでは、クライアントは以下の方法によってそれ自体の ID を証明できます。
  - 基本認証 (SSL タイプ 1 認証とも呼ばれます)。クライアントは、ターゲット・サーバーに既知のユーザー ID とパスワードを渡すことによって、サーバーに対してクライアントの ID を証明します。

    SSL 基本認証によって、次のことができます。
    - OS/390 または z/OS クライアントは、ユーザー ID とパスワードを使用することによって、WebSphere for z/OS サーバーと安全に通信できます。
    - OS/390 または z/OS クライアントは、DCE プリンシパルとパスワードを使用することによって、WebSphere 分散プラットフォーム上のサーバーと安全に通信できます。

- 分散プラットフォーム・クライアントは、MVS ユーザー ID とパスワードを使用することによって、WebSphere for z/OS サーバーと安全に通信できます。
- 要求にあたって常にパスワードが必要となるので、単純なクライアント対サーバー接続だけを行うことができます。つまり、サーバーはクライアントのユーザー ID を別のサーバーへ送信して要求に応答することはできません。そのような機能は、*ID アサーション* またはトラステッド・アソシエーション と呼ばれます。詳細は後述します。

– クライアント証明書サポート。この場合、サーバーとクライアントの両者は、ディジタル証明書を提供して互いに自己の ID を証明します。

  Web アプリケーションは数千のクライアントを持つ場合があり、その場合、クライアント認証は管理の重荷となります。RACF の*証明書名フィルター (certificate name filtering)* によって、WebSphere for z/OS 上の SSL サポートでは、クライアント証明書を (格納せずに) MVS ユーザー ID へマップできます。証明署名フィルターを通じて、MVS ユーザー ID を作成したり、すべてのユーザーのクライアント証明書を管理したりせずに、サーバーにアクセスするユーザー集合を認可できます。

– Kerberos セキュリティー。この場合、サーバーはクライアントにディジタル証明書を渡すことによって、サーバーの ID を証明します。クライアントは Kerberos 認証を使用して、サーバーに対して自己の ID を証明します。

– ID アサーションまたはトラステッド・アソシエーション。この場合、中間サーバーはクライアントの ID を安全かつ効率的な方法でターゲット・サーバーへ送信できます。このサポートは、クライアント証明書を使用して、中間サーバーを SSL セッションの所有者として確立します。RACF を通じて、システムは中間サーバーをトラステッドにできるかどうかを検査できます (特殊な SAF アクセス権が制御領域などのアドレス・スペースに与えられ、それらのアドレス・スペースは安全なシステム・コードを実行します)。この中間サーバーに対する信頼が確立されれば、ターゲット・サーバーがクライアント ID (MVS ユーザー ID) を別個に検証する必要はありません。クライアント ID は単にアサートされるだけで、認証は必要ありません。

- 次のような製品と安全に相互協調処理ができるようにするため。
  – CICS Transaction Server for z/OS
  – 分散プラットフォーム上の WebSphere
  – CORBA に準拠したオブジェクト・リクエスト・ブローカー

SSL サポートはオプションです。SSL を使用せずに WebSphere for z/OS を実行すると、通信の保護およびクライアントとサーバーの認証を行う SSL 機能だけが影響を受けます。

以下は、SSL 接続がどのように機能するかを説明しています。

ステージ	説明
折衝	クライアントがサーバーを見つけると、クライアントとサーバーは通信のためのセキュリティーのタイプを折衝します。SSL が使用される場合、クライアントは専用の SSL ポートに接続するよう伝えられます。
ハンドシェーク	クライアントは SSL ポートに接続すると、SSL ハンドシェークが発生します。成功した場合は、暗号化された通信が開始されます。クライアントは、サーバーのディジタル証明書を検査することによってサーバーを認証します。 ハンドシェークのときにクライアント証明書が使用された場合、サーバーは、クライアントのディジタル証明書を検査することによってクライアントを認証します。
基本認証を使用する場合	SSL ハンドシェークが発生した後、クライアントはサーバーに対して自己の ID を確立するために、SSL 暗号化パイプを通じてユーザー ID とパスワードを提供します。サーバーが OS/390 または z/OS 上にある場合、クライアントはユーザー ID およびパスワードを提供します。サーバーがワークステーション上にある場合は、クライアントは DCE プリンシパルおよびパスワードを提供します。
最初のクライアント要求	サーバーが最初のクライアント要求を受信した時点で、サーバーと RACF はクライアント証明書用の OS/390 または z/OS ユーザー ID を確立し、そのクライアント ID の下で要求を実行します。 RACF がユーザー ID の認証を行う場合、サーバーはそのクライアント ID の下で作業要求を実行します。クライアント認証が失敗した場合は、通信は停止します。
通信の進行中	SSL ハンドシェークのとき、クライアントとサーバーは、通信の暗号化に使用する暗号化スペックについて折衝します。

規則:

- サーバー制御領域と OS/390 または z/OS クライアントだけが、暗号サービス・システム SSL へのアクセスを必要とします。ユーザーの制御領域と OS/390 または z/OS クライアントは、*hlq*.SGSKLOAD データ・セットへの

アクセスを必要とします。SGSKLOAD を LPA に配置してください。詳しくは、*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください。

- OS/390 または z/OS 上の Java または C++ クライアントのいずれかは、WebSphere for z/OS またはワークステーション・サーバーとの相互協調処理ができ、また SSL を使用することができます。
- ハンドシェークの一部は、メッセージ保護用の SSL が使用する暗号スペックを折衝するためのものです。システム上にインストールされている暗号サービスのセキュリティー・レベルは、WebSphere for z/OS に使用可能な暗号スペックおよび鍵のサイズを決定します (詳しくは、*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください)。
- ディジタル証明書および鍵の保管には、RACF かそれと同等のものを使用しなければなりません。ディジタル証明書と鍵の HFS 内のキー・データベースへの配置は、オプションではありません。
- デーモン・サーバーは SSL を使用しません。

アプリケーション・サーバーとクライアント用の SSL 基本認証セキュリティーの概要

SSL 基本認証セキュリティーを定義するには、まずサーバー用の署名済み証明書と、そのサーバー証明書に署名した認証局からの認証局 (CA) 証明書を要求しなければなりません。証明書要求のプロセスは、本書では説明しません。証明書要求について、詳しくは、*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください。

サーバー用の署名済み証明書および CA 証明書を認証局から受け取ったら、RACF を使用してディジタル証明書の使用を許可し、サーバー証明書およびサーバー鍵リングを RACF に保管し、管理アプリケーションを通してサーバー用の SSL セキュリティー・プロパティーを定義しなければなりません。

クライアント用には、鍵リングを作成し、それにサーバーの証明書を発行した認証局からの CA 証明書を添付する必要があります。OS/390 または z/OS クライアントの場合は、RACF を使用してクライアント鍵リングを作成し、その鍵リングに CA 証明書を添付する必要があります。

332ページの図12 は、SSL 基本認証に関与する証明書を整理したものです。

- **クライアントがサーバーを認証するためには:** サーバー (実際には制御領域ユーザー ID) が、認証局 (CA) によって作成された署名済み証明書を所有していなければなりません。サーバーは、その署名済み証明書をクライアントに渡して、自己の ID を証明します。クライアントは、サーバーの証明書を発行した認証局からの CA 証明書を所有していなければなりません。クライ

アントは、その CA 証明書を使用して、サーバーの証明書が信頼できるものであるかどうかを検証します。検証できれば、クライアントはそのメッセージが間違いなくそのサーバーから来たものであることを確認できます。

- **サーバーがクライアントを認証するためには:** クライアントがサーバーに対して自己の ID を証明するために渡すクライアント証明書が存在しないことに注意してください。SSL 基本認証方式では、サーバーはクライアントのユーザー ID とパスワードを調べることによってクライアントを認証します。

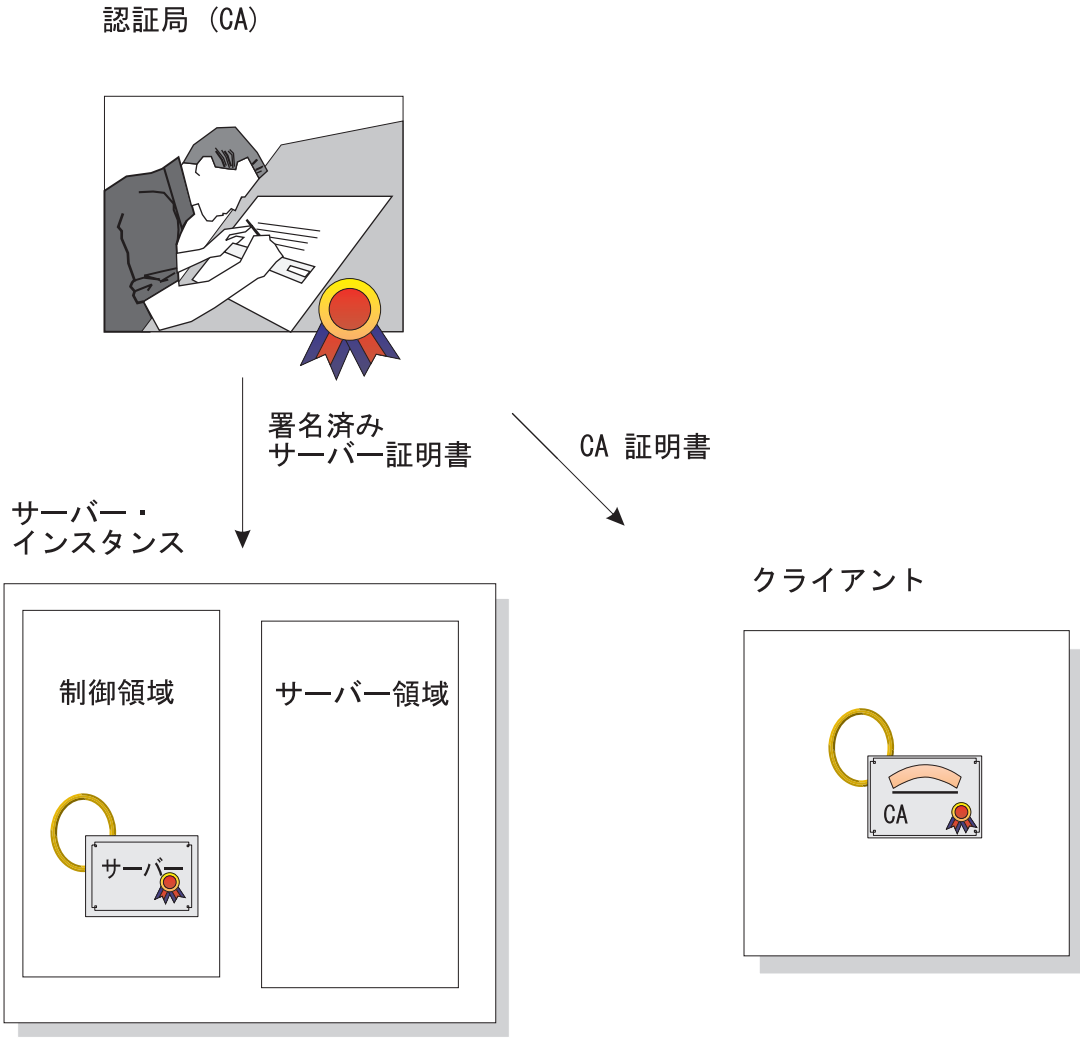


図 12. SSL 基本認証の証明書

規則:

- OS/390 または z/OS 以外のプラットフォーム上にある Java クライアントで WebSphere for z/OS サーバーとの相互協調処理を行い、SSL 基本認証を使用するためには、それらのプラットフォーム上に WebSphere Application Server エンタープライズ版 3.5 が存在しなければなりません。他のプラットフォーム上の C++ クライアントは、WebSphere for z/OS と相互協調処理をしているときは SSL を使用できません。
- SSL 基本認証の場合、クライアントは次のようにして認証されます。
  - リモート OS/390 または z/OS サーバーと通信している OS/390 または z/OS クライアントは、クライアント環境ファイル内のリモートのユーザー ID およびパスワード (REM_USERID および REM_PASSWORD) 環境変数を使用して、クライアントの ID を認証します。
  - OS/390 または z/OS クライアントは、他のプラットフォーム上の Component Broker サーバーで SSL を使用する場合、REM_DCEPRINCIPAL および REM_DCEPASSWORD 環境変数を使用して、定義済みの DCE プリンシパルとパスワードをそのサーバーに渡さなければなりません。
  - また、OS/390 または z/OS クライアントは、SSL_KEYRING 環境変数を通じて自己の鍵リングを示さなければなりません。
  - OS/390 または z/OS サーバーと通信する WebSphere Application Server 分散プラットフォーム上のクライアントは、ORB が提供するユーザー・ダイアログを使用し、その中で、ユーザーはユーザー ID とパスワードを指定します。

次の表は、SSL 基本認証セキュリティーを定義するためのサブタスクとそれに関連した手順を示しています。

サブタスク	関連手順 (参照項目資料)
サーバー証明書および認証局 (CA) 証明書を要求する	*z/OS System Secure Sockets Layer Programming*, SC24-5901
サーバー用の SSL 基本認証セキュリティーをセットアップする	338ページの『RACF を使用してサーバーにディジタル証明書の使用を許可するステップ』 340ページの『SSL セキュリティー用のサーバー・セキュリティー・プロパティーを定義するステップ』

サブタスク	関連手順 (参照項目資料)
クライアント用の SSL 基本認証セキュリティーをセットアップする	341ページの『クライアント用の SSL セキュリティーをセットアップするステップ』

アプリケーション・サーバーとクライアント用の SSL クライアント証明書セキュリティーの概要

SSL クライアント証明書セキュリティーを定義するには、まずサーバーとクライアント用の署名済み証明書と、それらの証明書に署名した認証局からの認証局 (CA) 証明書を要求しなければなりません。証明書要求のプロセスは、本書では説明しません。証明書要求について、詳しくは、*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください。

署名済み証明書と CA 証明書を認証局から受け取ったら、RACF を使用してディジタル証明書の使用を許可し、証明書と鍵リングを RACF に保管し、管理アプリケーションを通じてサーバーの SSL セキュリティー・プロパティーを定義しなければなりません。

ディジタル証明書によって識別された各クライアントは、最終的にターゲットの WebSphere for z/OS サーバーによって MVS ユーザー ID に変換されなければなりません。クライアントとサーバーが同じ RACF データベースを共用している場合は、このマッピングのための追加構成を行う必要はありません。クライアントとサーバーが同じ RACF データベースを共用していない場合は、次のようにしてマッピングを構成できます。

- クライアント証明書をターゲット・サーバーの RACF データベースに追加する。ほとんどの場合、これは現実性がないと考えられます。
- RACF 証明書名フィルターを使用して、クライアントのグループを RACF ID にマップする。
- 上記の 2 つを組み合わせて使用する。

337ページの図13 は、SSL クライアント証明書による認証に関与する証明書を整理したものです。

- **クライアントがサーバーを認証するためには:** サーバー (実際には制御領域ユーザー ID) が認証局 (CA) によって作成された署名済み証明書を所有していなければなりません。サーバーは、その署名済み証明書をクライアントに渡して、自己の ID を証明します。クライアントは、サーバーの証明書を発行した認証局からの CA 証明書を所有していなければなりません。クライアントは、その CA 証明書を使用して、サーバーの証明書が信頼できるものであるかどうかを検証します。検証できれば、クライアントはそのメッセージが間違いなくそのサーバーから来たものであることを確認できます。
- **サーバーがクライアントを認証するためには:** クライアントが認証局 (CA2) によって作成された署名済み証明書を所有していなければなりません (337ページの図13 では、わかりやすくするために 2 つの異なる認証局を示してありますが、同じ認証局がサーバーとクライアントの両方に署名済み証明書を

提供する場合も考えられます)。サーバーは、クライアントの証明書を発行した認証局からの CA2 証明書を所有していなければなりません。サーバーは、その CA2 証明書を使用して、クライアントの証明書が信頼できるものであるかどうかを検証します。検証できれば、サーバーはそのメッセージが間違いなくそのクライアントから来たものであることを確認できます。

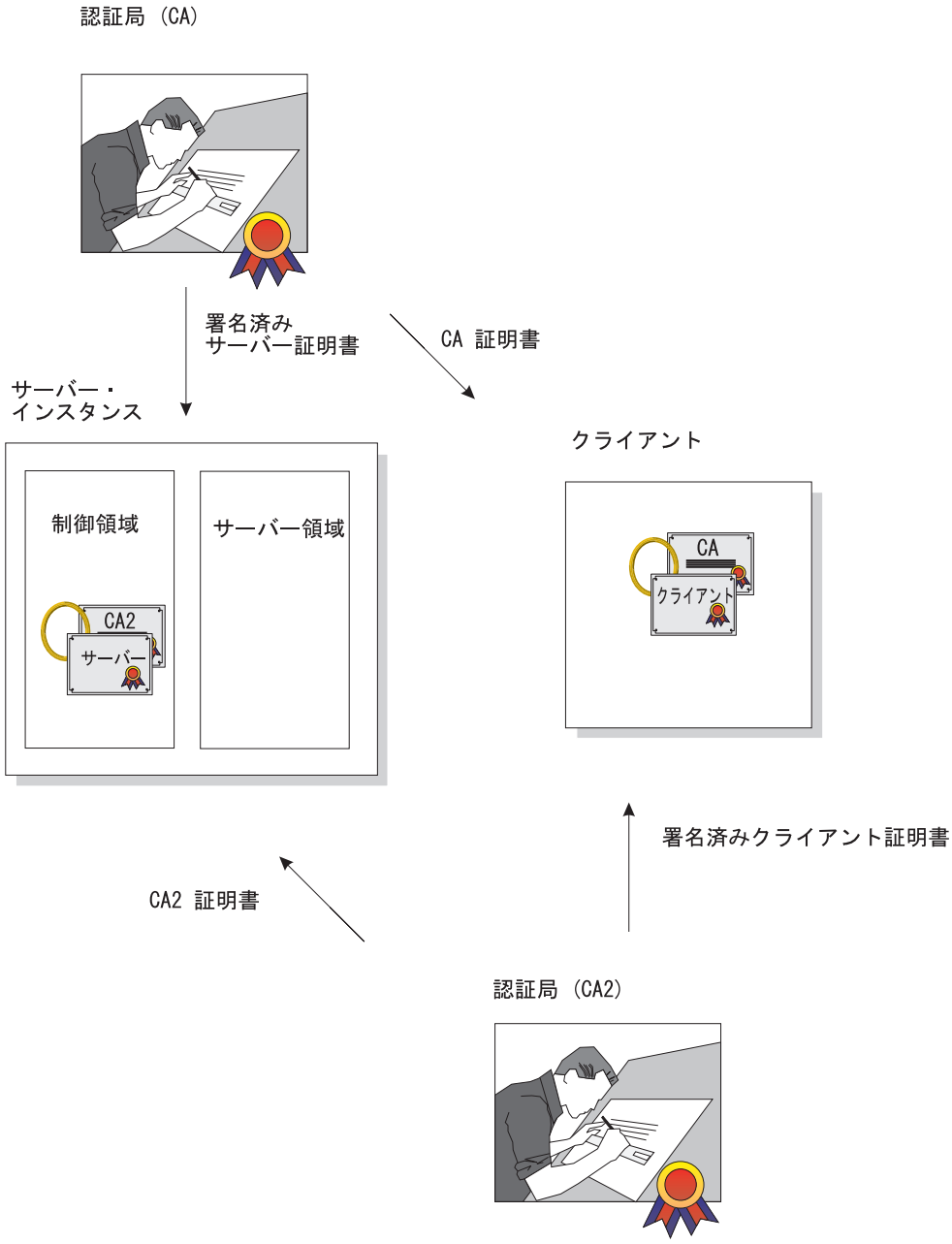


図 13. SSL クライアント証明書セキュリティーの証明書

次の表は、SSL クライアント証明書セキュリティーを定義するためのサブタスクとそれに関連した手順を示しています。

サブタスク	関連手順 (参照項目資料)
サーバー証明書および認証局 (CA) 証明書を要求する	*z/OS System Secure Sockets Layer Programming*, SC24-5901
サーバー用の SSL クライアント証明書セキュリティーをセットアップする	『RACF を使用してサーバーにディジタル証明書の使用を許可するステップ』 340ページの『SSL セキュリティー用のサーバー・セキュリティー・プロパティーを定義するステップ』
クライアント用の SSL クライアント証明書セキュリティーをセットアップする	341ページの『クライアント用の SSL セキュリティーをセットアップするステップ』
クライアント・ディジタル証明書をサーバーのシステム上の MVS ユーザー ID へマッピングする	343ページの『クライアント・ディジタル証明書をサーバーのシステム上の MVS ユーザー ID へマッピングするステップ』

クライアントおよびサーバー用の SSL セキュリティーの定義

この節には、SSL ベースのすべての認証機構をインプリメントするために実行しなければならない手順が含まれています。

RACF を使用してサーバーにディジタル証明書の使用を許可するステップ:

SSL は、ディジタル証明書および公開 / 秘密鍵を使用します。アプリケーション・サーバーが SSL を使用する場合は、RACF を使用して、サーバー制御領域を実行しているユーザー ID 用のディジタル証明書と公開 / 秘密鍵を格納しなければなりません。

この作業を始める前に: 認証局 (CA) 証明書およびサーバー用の署名済み証明書を要求する必要があります。

SSL クライアント証明書サポートのインプリメントを計画している場合は、クライアント証明書を検証する各認証局からの認証局 (CA) 証明書も持っていなければなりません。*z/OS System Secure Sockets Layer Programming*, SC24-5901 を参照してください。

RACF 内の RACDCERT コマンドを使用するための権限 (たとえば、特殊権限など) のある、ユーザー ID を持っている必要があります。RACDCERT の詳細については、*z/OS SecureWay Security Server (RACF) コマンド言語 解説書*, SA88-8617 および *z/OS SecureWay Security Server (RACF) セキュリティー管理者のガイド*, SA88-8613 を参照してください。

以下のステップを実行して、ディジタル証明書の使用を許可します。

1. SSL を使用するサーバーごとに、そのサーバーの制御領域ユーザー ID 用の鍵リングを作成します。

   例: 制御領域は、CBACRU1 と呼ばれるユーザー ID と関連付けられています。以下のように発行します。

   ```
   RACDCERT ADDRING(ACRRING) ID(CBACRU1)
   ```

---

2. アプリケーション・サーバー用の証明書を認証局から受け取ります。

   例: 証明書を要求したところ、認証局から署名済みの証明書が戻されてきました。これを CBACRU1.CA というファイルに格納しました。以下のように発行します。

   ```
   RACDCERT ID (CBACRU1) ADD('CBACRU1.CA') WITHLABEL('ACRCERT') PASSWORD('password')
   ```

---

3. 署名済みの証明書を制御領域ユーザー ID の鍵リングに接続し、その証明書をデフォルトの証明書にします。

   例: ACRCERT というラベルの付いた証明書を CBACRU1 が所有する鍵リング ACRRING に接続します。以下のように発行します。

   ```
   RACDCERT ID(CBACRU1) CONNECT (ID(CBACRU1) LABEL('ACRCERT') RING(ACRRING) DEFAULT)
   ```

---

4. サーバーにクライアントを認証させること (SSL クライアント証明書サポート) を計画している場合は、次のようにします。
   - クライアント証明書を検証する各認証局 (CA) 証明書を受信します。それぞれの CA 証明書に CERTAUTH 属性を与えます。

     例: ユーザー ID が CLIENT1 であるクライアントを検証する CA 証明書を受信します。この証明書は、ファイル内では USER.CLIENT1.CA という名前です。以下のように発行します。

     ```
     RACDCERT ADD('USER.CLIENT1.CA') WITHLABEL('CLIENT1 CA') CERTAUTH
     ```

   - 各クライアントの認証局 (CA) 証明書を制御領域ユーザー ID の鍵リングに接続します。

     例: CLIENT1 の CA 証明書を、CBACRU1 が所有する鍵リング ACRRING に接続します。

     ```
     RACDCERT ID(CBACRU1) CONNECT(CERTAUTH LABEL('CLIENT1 CA') RING(ACRRING))
     ```

---

5. RACF FACILITY クラス内の IRR.DIGTCERT.LIST および IRR.DIGTCERT.LISTRING の読み取りアクセスを制御領域ユーザー ID に与えます。

   例: ユーザーの制御領域ユーザー ID は CBACRU1 です。以下のように発行します。

   ```
   PERMIT IRR.DIGTCERT.LIST     CLASS(FACILITY) ID(CBACRU1) ACC(READ)
   PERMIT IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(CBACRU1) ACC(READ)
   ```

RACF コマンドが成功したら、RACF での作業は完了です。続けて『SSL セキュリティー用のサーバー・セキュリティー・プロパティーを定義するステップ』を行ってください。

SSL セキュリティー用のサーバー・セキュリティー・プロパティーを定義するステップ: この手順では、管理アプリケーションによってサーバーが SSL クライアント証明書セキュリティーを使用することを指定する方法を説明しています。

この作業を始める前に: 管理アプリケーションを開始してログオンし、新規の会話を作成する必要があります。詳しくは、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 を参照してください。

以下のステップを実行して、サーバー用のセキュリティー特性を定義します。

1. 会話ツリー内のサーバーを展開します。

---

2. 新規のサーバーを作成するか、または既存のサーバーの名前をクリックします。

---

3. プロパティー・フォームで次のようにします。
   - SSL 基本認証をインプリメントする場合は、「SSL タイプ 1 (基本認証)(SSL Type 1 (basic authentication))」チェック・ボックスをクリックします。
   - SSL クライアント証明書をインプリメントする場合は、「SSL クライアント証明書 (SSL Client Certificates)」チェック・ボックスをクリックします。
   - Kerberos をインプリメントする場合は、「Kerberos」チェック・ボックスをクリックします。

- アサート ID をインプリメントする場合は、「アサート ID (Asserted identity)」チェック・ボックスをクリックします。必ず、「SSL クライアント証明書 (SSL client certificates)」チェック・ボックスもクリックしてください。

---

4. SSL RACF 鍵リングを指定します。これは、338ページの『RACF を使用してサーバーにディジタル証明書の使用を許可するステップ』のステップ 1 で定義した鍵リングです。

   注: 間違った RACF 鍵リングを指定すると、サーバーは実行時にエラー・メッセージを受け取ります。

---

5. SSL V2 タイムアウト値を指定します。これは、システムがセッション・キーを保持する時間の長さで、秒単位で表します。範囲は 0 〜 100 秒です。デフォルトは 100 秒です。

---

6. SSL V3 タイムアウト値を指定します。これは、システムがセッション・キーを保持する時間の長さで、秒単位で表します。範囲は 0 〜 86400 秒 (1 日) です。デフォルトは 600 秒です。

---

7. セキュリティー・プリファレンス・リストを配列します。セキュリティー・プリファレンス・リストの詳細については、324ページの『クライアントおよびサーバーのセキュリティー・プロトコルの折衝方法』を参照してください。

---

8. サーバーに対する他のすべての指定を完了してから、妥当性検査およびコミットを行い、すべてのタスクを完了して、この会話を活動化します。

会話が活動化したことをシステムが通知してきたら、完了したことがわかります。

クライアント用の SSL セキュリティーをセットアップするステップ: すべてのクライアントは、SSL ハンドシェーク時にサーバーを認証できるよう、サーバーの認証局 (CA) 証明書へのアクセス権を持っていなければなりません。さらに、SSL クライアント証明書サポートのインプリメントを計画している場合

は、クライアントが自己の証明書をデフォルト証明書としてクライアントの鍵リング上に持っていなければなりません。

- クライアントがワークステーション上の WebSphere から WebSphere for z/OS へ接続する場合は、ワークステーション・システムに SSL 証明書をインポートする必要があります。詳しい説明については、*WebSphere Application Server エンタープライズ版 Component Broker システム管理の手引きバージョン 3.0*, SD88-7375 を参照してください。
- OS/390 または z/OS では、クライアントは RACF 内の鍵リングに証明書が添付されていなければなりません。

この手順は、OS/390 または z/OS クライアントに証明書を添付する方法を説明したものです。

この作業を始める前に: SSL 基本認証の場合は、アプリケーション・サーバー用の署名済み証明書を発行した認証局と同じ認証局からの CA 証明書を要求しなければなりません。さらに、SSL クライアント証明書サポートのインプリメントを計画している場合は、認証局からのクライアント用の署名済み証明書を要求しなければなりません。

RACF 内の RACDCERT コマンドを使用するための権限 (たとえば、特殊権限など) のあるユーザー ID を持っている必要があります。RACDCERT の詳細については、*z/OS SecureWay Security Server (RACF) コマンド言語 解説書*, SA88-8617 および *z/OS SecureWay Security Server (RACF) セキュリティー管理者のガイド*, SA88-8613 を参照してください。

以下のステップを実行して、OS/390 または z/OS クライアントによるディジタル証明書の使用を許可します。

1. OS/390 または z/OS クライアント用の鍵リングを作成します。

   例: クライアントのユーザー ID は CLIENT1 です。以下のように発行します。

   ```
   RACDCERT ADDRING(C1RING) ID(CLIENT1)
   ```

---

2. サーバーの認証局 (CA) 証明書を受け取り、それに CERTAUTH 属性を与えます。

   例: ユーザーは CA 証明書を要求し、認証局は、自分の証明書をユーザーに戻しました。ユーザーはこれを USER.CBSERVER.CA と呼ばれるファイル内に保管しました。以下のコマンドを発行します。

   ```
   RACDCERT ADD('USER.CBSERVER.CA') WITHLABEL('VERI CA') CERTAUTH
   ```

3. CA 証明書をクライアントの鍵リングに接続します。

   例: VERI CA 証明書を CLIENT1 が所有する C1RING 鍵リングに接続します。

   ```
   RACDCERT ID(CLIENT1) CONNECT(CERTAUTH LABEL('VERI CA') RING(C1RING))
   ```

4. クライアントの環境ファイル内で、SSL_KEYRING 環境変数をクライアントの鍵リングに対応するようコード化します。

   詳しくは、383ページの『付録A. 環境ファイル』を参照してください。

5. SSL クライアント証明書サポートをインプリメントする場合は、次のようにします。
   - アプリケーション・サーバー用の証明書を認証局から受け取ります。

     例: 証明書を要求したところ、署名済み証明書が認証局から戻されてきました。これを CLIENT1.SIGNED.CERT というファイルに格納しました。以下のように発行します。

     ```
     RACDCERT ID (CLIENT1) ADD('CLIENT1.SIGNED.CERT') WITHLABEL('CLIENT1 CERT') PASSWORD('password')
     ```

   - クライアントの署名済み証明書をクライアントのユーザー ID の鍵リングに接続し、その証明書をデフォルトの証明書にします。

     例: CLIENT1 というラベルの付いた証明書を CLIENT1 が所有する鍵リング C1RING に接続します。以下のように発行します。

     ```
     RACDCERT ID(CLIENT1) CONNECT (ID(CLIENT1) LABEL('CLIENT1 CERT') RING(C1RING) DEFAULT)
     ```

RACF コマンドが成功し、環境を保存したら、完了です。

クライアント・ディジタル証明書をサーバーのシステム上の MVS ユーザー ID へマッピングするステップ: 自己の ID を認証するためのディジタル証明書を提示した Component Broker の各クライアントは、個々の証明書がターゲット・サーバーのシステムまたはシスプレックス上の RACF に登録されていなければ、有効な MVS ユーザー ID へのマッピングを持っていなければなりません。このマッピングは、RACF 証明書名フィルターを使用して作成できます。

RACF 証明書名フィルターは、X.509 ディジタル証明書に含まれているような、クライアントまたは証明書発行者の識別名に基づいて作成できます。

この作業を始める前に: ディジタル証明書を提示するクライアント集合をどのように編成するか、およびそれらのクライアントがどのような種類のアクセスを必要とするかを知っておかなければなりません。

RACDCERT MAP コマンドを発行する権限を持っている必要があります。

以下のステップを実行して、証明書名フィルターをセットアップします。

1. 証明書名フィルターへ関連付ける各ユーザー ID に MVS ユーザー ID を定義します。それぞれのユーザー ID に PROTECTED 属性と RESTRICTED 属性を割り当てることを考慮してください。PROTECTED 属性は、そのユーザー ID がシステムへの直接のログオンに使用されるのを防止し、不正なパスワードの試みによってユーザー ID が取り消されるのを防止します。RESTRICTED 属性は、そのユーザー ID が明示的にアクセスを許可されていない保護されたリソースへのアクセスに使用されないようにします。**例:**

   ```
   ALTUSER WEBUSER NOPASSWORD RESTRICTED
   ```

   ---

2. 証明書名フィルターを活動化します。**例:**

   ```
   SETROPTS CLASSACT(DIGTNMAP) RACLIST(DIGTNMAP)
   ```

   ---

3. 証明書名フィルターを作成します。**例:** 次のフィルターは、ユーザー ID WEBUSER を、VeriSign Class 1 によって発行された証明書を提示するすべてのユーザー (ただし、個別の証明書がシステム上の RACF に登録されていないユーザー) へ関連付けます。

   ```
   RACDCERT ID(WEBUSER) MAP WITHLABEL('INTERNET OTHERS') +
            IDNFILTER('OU=VeriSign Class 1 Individual Subscriber.O=VeriSign, Inc.L=Internet')
   ```

   このフィルターは、発行者の名前に基づいています。その他のフィルターを、サブジェクト名、または発行者名とサブジェクト名の組み合わせに基づいて作成することもできます。証明書名フィルターの詳細については、*z/OS SecureWay Security Server (RACF) セキュリティー管理者のガイド*, SA88-8613 を参照してください。

   ---

4. DIGTNMAP クラスをリフレッシュします。**例:**

   ```
   SETROPTS RACLIST(DIGTNMAP) REFRESH
   ```

SETROPTS コマンドが完了すれば、作業は完了です。

アサート ID 機能のセットアップ

SSL クライアント証明書サポートは、アサート ID と呼ばれる機能を提供します。この機能では、中間サーバーがターゲット・サーバーにクライアントの ID を安全かつ効率的な方法で送信できます。この機能では、中間サーバーを SSL セッションの所有者として確立するために、クライアント証明書サポートが必要です。RACF を通じて、システムは中間サーバーをトラステッドにできるかどうかを検査できます (特殊な RACF アクセス権が制御領域などのアドレス・スペースに与えられ、それらのアドレス・スペースは安全なシステム・コードを実行します)。この中間サーバーに対する信頼が確立されれば、ターゲット・サーバーがクライアント ID (MVS ユーザー ID) を別個に検証する必要はありません。クライアント ID は単にアサートされるだけで、認証は必要ありません。

アサート ID 機能をセットアップするためのステップ

この作業を始める前に: SSL クライアント証明書サポートをセットアップしておかなければなりません。335ページの『アプリケーション・サーバーとクライアント用の SSL クライアント証明書セキュリティーの概要』を参照してください。

アサート ID 機能をセットアップするには、次のステップを実行してください。

1. 管理アプリケーションを開き、ログオンします。新規会話を開始します。必要であれば、新規サーバーを定義します。

   ---

2. アサート ID を受信するサーバー (ターゲット・サーバー) のプロパティー・フォームで、以下のプロパティーを追加します。
   - アサート ID の受信を許可
   - SSL クライアント証明書を許可

   ---

3. アサート ID を送信するサーバー (中間サーバー) のプロパティー・フォームで、「アサート ID の送信を許可 (Send asserted identity allowed)」を指定します。

   ---

4. 会話の妥当性を検査し、会話をコミットし、活動化します。

   ---

5. OS/390 または z/OS で、中間サーバーの制御領域のユーザー ID に CB.BIND.*servername* についての CONTROL 権限を与えます。ここで、*servername* は**ターゲット・サーバー**の名前です。

   _____

6. CBIND クラスを活動化します。

   _____

RACF コマンドが終了したら、作業は完了です。

WebSphere for z/OS 用の Kerberos セキュリティーのセットアップ

WebSphere for z/OS では、Kerberos は SSL と一緒に機能して完全な認証機構を提供します。

- SSL は、メッセージを保護するためにトランスポート層を保護します。また、SSL はクライアントがサーバーを認証する機構も提供します。
- Kerberos は、サーバーがクライアントを認証する機構を提供します。つまり、クライアントはサーバーへ Kerberos Generic Security Service Application Program Interface (GSS_API) トークンを送信し、サーバーはそのトークンを使用して、クライアントの ID を認証します。
- GSS_API トークンを通じて、サーバーはクライアントの ID を別のサーバーへ渡し、クライアントの要求を満たすことができます。これを委任と呼びます。

以下は、SSL 接続がどのように機能するかを説明しています。

ステージ	説明
折衝	クライアントがサーバーを見つけると、クライアントとサーバーは通信のためのセキュリティーのタイプを折衝します。SSL が使用される場合、クライアントは専用の SSL ポートに接続するよう伝えられます。
ハンドシェーク	クライアントは SSL ポートに接続すると、SSL ハンドシェークが発生します。成功した場合、SSL のメッセージ保護が開始されます。クライアントは、サーバーのディジタル証明書を検査することによってサーバーを認証します。

ステージ	説明
クライアント認証	SSL ハンドシェークが発生した後、クライアントは自己の Kerberos ID を確立し、この ID とサーバーの Kerberos プリンシパルに基づいて、Kerberos GSS_API トークンを取得します。クライアントはそのトークンを、固有の SSL 接続 ID と一緒にサーバーへ送信します。サーバーは、GSS_API トークンを使用して、クライアントを表す Kerberos プリンシパルを認証します。 クライアントが認証された後、システムは RACF を使用して、クライアントの Kerberos プリンシパルへマップされている z/OS ユーザー ID を取得します。この z/OS ユーザー ID は、将来の許可検査で使用されます。 デフォルトでは、クライアントは委任が可能になるように GSS_API トークンを構成します。これによって、サーバーはクライアントの名前を使用して、クライアントの代わりに要求を出せるようになります。 z/OS ユーザー ID、Kerberos 委任証明書、および固有の SSL 接続 ID は、将来この SSL Kerberos 接続を通じて出される要求で使用できるように、保管されます。 Kerberos クライアント認証または認証プリンシパルのマッピングが失敗した場合、通信は停止します。
通信の進行中	クライアントとサーバー間の通信では、メッセージの保護のために SSL サービスが使用されます。それぞれのメッセージには固有の SSL 接続 ID が含まれているので、サーバーはこの ID を使用して、要求を、サーバーに保管してある z/OS ユーザー ID および Kerberos 委任証明書と突き合わせることができます。

このサポートを使用するには、SSL セキュリティーをセットアップしておく必要があります。SSL の要件に加えて、Kerberos は、OS/390 または z/OS システムに以下のものがインストールされ構成されていることを必要とします。

- OS/390 SecureWay Security Server Network Authentication and Privacy Service for OS/390。OS/390 V2R8 および V2R9 の場合、このサポートは次の Web サイトで入手できます。

  `http://www.software.ibm.com`

  OS/390 V2R10 および z/OS の場合、このサポートは SecureWay Security Server に組み込まれています。

- 使用している OS/390 または z/OS システム用の各 PTF。詳しくは、PSP バケットを参照してください。
- このサポートを使用するクライアント・システムとサーバー・システム上で、Kerberos セキュリティー・サーバーが活動状態になっていなければなりません。
- Kerberos 認証に参加するすべての (クライアントとサーバーの) OS/390 または z/OS ユーザー ID は、Kerberos プリンシパルを定義した Kerberos RACF セグメントを備えている必要があります。
- Kerberos サーバーは、そのサーバーの Kerberos 秘密鍵が入ったファイルを持っている必要はありません。OS/390 または z/OS の Kerberos では、この要件は除去され、現行システム ID へ関連付けられた Kerberos プリンシパルを使用してサーバー・チケットを解読できます。WebSphere for z/OS サーバーは、この機能を使用する必要があります。
- WebSphere for z/OS サーバーは、RACF FACILITY クラス内の IRR.RUSERMAP リソースに対する READ アクセス権を備えていなければなりません。
- Kerberos セキュリティーは、参加者間での時刻調整に頼っています。Kerberos セキュリティー管理者は時刻提供者を選択し、Kerberos セキュリティーの参加者がその時刻源を使用して各自のシステム時刻を保守するようにしなければなりません。

次の表は、Kerberos セキュリティーを定義するためのサブタスクとそれに関連した手順を示しています。

サブタスク	関連手順 (参照項目)
基本認証用の SSL をセットアップする	327ページの『WebSphere for z/OS 用の SSL セキュリティーのセットアップ』
Kerberos サーバーを使用可能にする	*z/OS SecureWay Security Server Network Authentication Service Administration*, SC24-5926
サーバー ID と Kerberos プリンシパルを関連付ける	349ページの『サーバー ID と Kerberos プリンシパルの関連付けのステップ』
Kerberos 用のサーバー属性を定義する	349ページの『Kerberos 用のサーバー・セキュリティー属性を定義するステップ』
クライアントが Kerberos を使用するようにセットアップする	350ページの『Kerberos を使用するようクライアントをセットアップするステップ』

サーバー ID と Kerberos プリンシパルの関連付けのステップ

この作業を始める前に: サーバーの制御領域用に RACF ユーザー ID を確立しておく必要があります。

次のステップを実行して、サーバー ID を Kerberos プリンシパルへ関連付けます。

⇔ 次の ALTUSER コマンドを発行して関連付けを作成します。**例:**

```
ALTUSER ctl_ID PASSWORD(new_password) NOEXPIRED
        KERB(KERBNAME(kerberos_principal))
```

ここで

ctl_ID
STARTED クラスを通じてサーバーの制御領域へ割り当てられたユーザー ID です。

new_password
OS/390 または z/OS および Kerberos の共用パスワードです。

kerberos_principal
この OS/390 または z/OS ユーザー ID へ関連付ける Kerberos プリンシパル名です。

ジョブが正常に実行されると、このステップは終了したことになります。

Kerberos 用のサーバー・セキュリティー属性を定義するステップ

この手順は、管理アプリケーションによってサーバーが Kerberos セキュリティーを使用することを指定する方法を説明しています。

この作業を始める前に: 管理アプリケーションを開始してログオンし、新規の会話を作成する必要があります。詳しくは、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 を参照してください。

以下のステップを実行して、サーバー用のセキュリティー特性を定義します。

1. 会話ツリー内のサーバーを展開します。

   ---

2. 新規のサーバーを作成するか、または既存のサーバーの名前をクリックします。

   ---

3. プロパティー・フォーム内で、「Kerberos 許可 (Kerveros allowed)」チェック・ボックスをクリックします。

---

4. SSL RACF 鍵リングを指定します。これは、338ページの『RACF を使用してサーバーにディジタル証明書の使用を許可するステップ』のステップ 1 で定義した鍵リングです。

   注: 間違った RACF 鍵リングを指定すると、サーバーは実行時にエラー・メッセージを受け取ります。

---

5. SSL V2 タイムアウト値を指定します。これは、システムがセッション・キーを保持する時間の長さで、秒単位で表します。範囲は 0 ～ 100 秒です。デフォルトは 100 秒です。

---

6. SSL V3 タイムアウト値を指定します。これは、システムがセッション・キーを保持する時間の長さで、秒単位で表します。範囲は 0 ～ 86400 秒 (1 日) です。デフォルトは 600 秒です。

---

7. セキュリティー・プリファレンス・リストを配列します。セキュリティー・プリファレンス・リストの詳細については、324ページの『クライアントおよびサーバーのセキュリティー・プロトコルの折衝方法』を参照してください。

---

8. サーバーに対する他のすべての指定を完了してから、妥当性検査およびコミットを行い、すべてのタスクを完了して、この会話を活動化します。

会話が活動化したことをシステムが通知してきたら、完了したことがわかります。

Kerberos を使用するようクライアントをセットアップするステップ

この作業を始める前に: SSL 基本認証をセットアップしておく必要があります。

OS/390 SecureWay Security Server Network Authentication and Privacy Service for OS/390 (Kerberos) をインストールし、構成する必要があります。クライアントが Kerberos を使用する予定の各 OS/390 または z/OS イメージ上で、

SecureWay Security Server (KDC) を使用可能にしてください。詳しくは、*z/OS SecureWay Security Server Network Authentication Service Administration*, SC24-5926 を参照してください。

以下のステップを実行して、クライアントが Kerberos を使用するようにセットアップします。

1. RACF を使用して、Kerberos クライアントとして参加するそれぞれの OS/390 または z/OS ユーザーをローカル・レルム上の Kerberos プリンシパルにマップします。**例:**

   ```
   ALTUSER client_ID PASSWORD(CBIVP) NOEXPIRED KERB(KERBNAME(kerberos_principal))
   ```

   ここで

   client_ID
   クライアントのユーザー ID です。

   kerberos_principal
   この OS/390 または z/OS ユーザー ID へ関連付ける Kerberos プリンシパル名です。

   ヒント: あるユーティリティーを使用すると、セキュリティー管理者が OS/390 または z/OS RACF レジストリーを Kerberos へマイグレーションするのに役立ちます。そのユーティリティーは、次の Web サイトにあります。

   ```
   http://sandbox.s390.ibm.com/products/racf/kmigrate.html
   ```

---

2. RACF を使用して、ターゲット・サーバーが常駐するレルムとクライアントが常駐するレルムの間で信頼関係をセットアップします。**例:** あるクライアントが Kerberos レルム CLIENTREALM にあり、サーバーが SERVERREALM にある場合:

   ```
   RDEFINE REALM /.../CLIENTREALM/krbtgt/SERVERREALM KERB(PASSWORD(password1))
   RDEFINE REALM /.../SERVERREALM/krbtgt/CLIENTREALM KERB(PASSWORD(password2))
   ```

   ここで、*password1* と *password2* はパスワードです。この 2 つのコマンドをそれぞれの RACF データベースに対して発行しなければなりません。

---

3. RACF を使用して、サーバー・レルム内に外部ユーザー・マッピングをセットアップします。**例:**

   a. 外部レルムにあるすべてのプリンシパルを単一のユーザー ID にマップするには、次のコマンドを発行します。

```
RDEFINE KERBLINK /.../foreign_realm APPLDATA('user_ID')
```

b. 外部レルムにある 1 つのプリンシパルを 1 つのユーザー ID にマップするには、次のコマンドを発行します。

```
RDEFINE KERBLINK /.../foreign_realm/principal APPLDATA('user_ID')
```

ここで

foreign_realm
外部レルムです。

user_ID
MVS ユーザー ID です。

principal
プリンシパルです。

RACF コマンドが正常に終了すれば、このステップは完了です。

拡張パフォーマンス制御のインプリメント

この節では、次の項目に対するパフォーマンスの問題について述べます。

- リソースの逐次化
- WLM 分類規則および作業修飾子

リソースの逐次化に対する推奨

パフォーマンス上の理由で、グローバル・リソース逐次化のスター型複合システムの使用をお勧めします。詳細については *z/OS MVS 計画：グローバル・リソース逐次化*, SA88-8572 を参照してください。

ワークロード管理と WebSphere for z/OS

このトピックでは、WebSphere for z/OS が OS/390 または z/OS ワークロード管理サブシステムを使用する方法について述べ、ワークロード管理制御のセットアップ方法について説明します。

ワークロード管理と WebSphere for z/OS のバックグラウンド情報

WebSphere for z/OS は、次の一般機能でワークロード管理を活用します。

- 作業要求のシスプレックス経路指定
- 作業要求のアドレス・スペース管理

作業要求のシスプレックス経路指定: WebSphere for z/OS は、ドメイン・ネーム・サーバー (DNS) を使用して、シスプレックス全体の作業要求の経路を定めます。354ページの図14 は、作業がシスプレックスでどのように経路指定されるかを示しています。DNS は、クライアントから汎用ホスト名を受信し、その名前を特定のシステムにマップします。使用可能な最良のシステムを選択するために、DNS は、ワークロード管理 (WLM) の勧告を求めます。ワークロード管理は、シスプレックスの現状を分析し、CPU、メモリー、入出力使用率など、多数の要因を考慮して、新規作業に最も適した配置を決定します。次に DNS は、実行に最適なシステムにクライアント要求の経路を定めます。ワークロード管理および DNS のこのような使用はオプションですが、こうすれば、単一ポイントの障害によってシステム全体がダウンするのを防ぐことができるため、この方法を強くお勧めします。

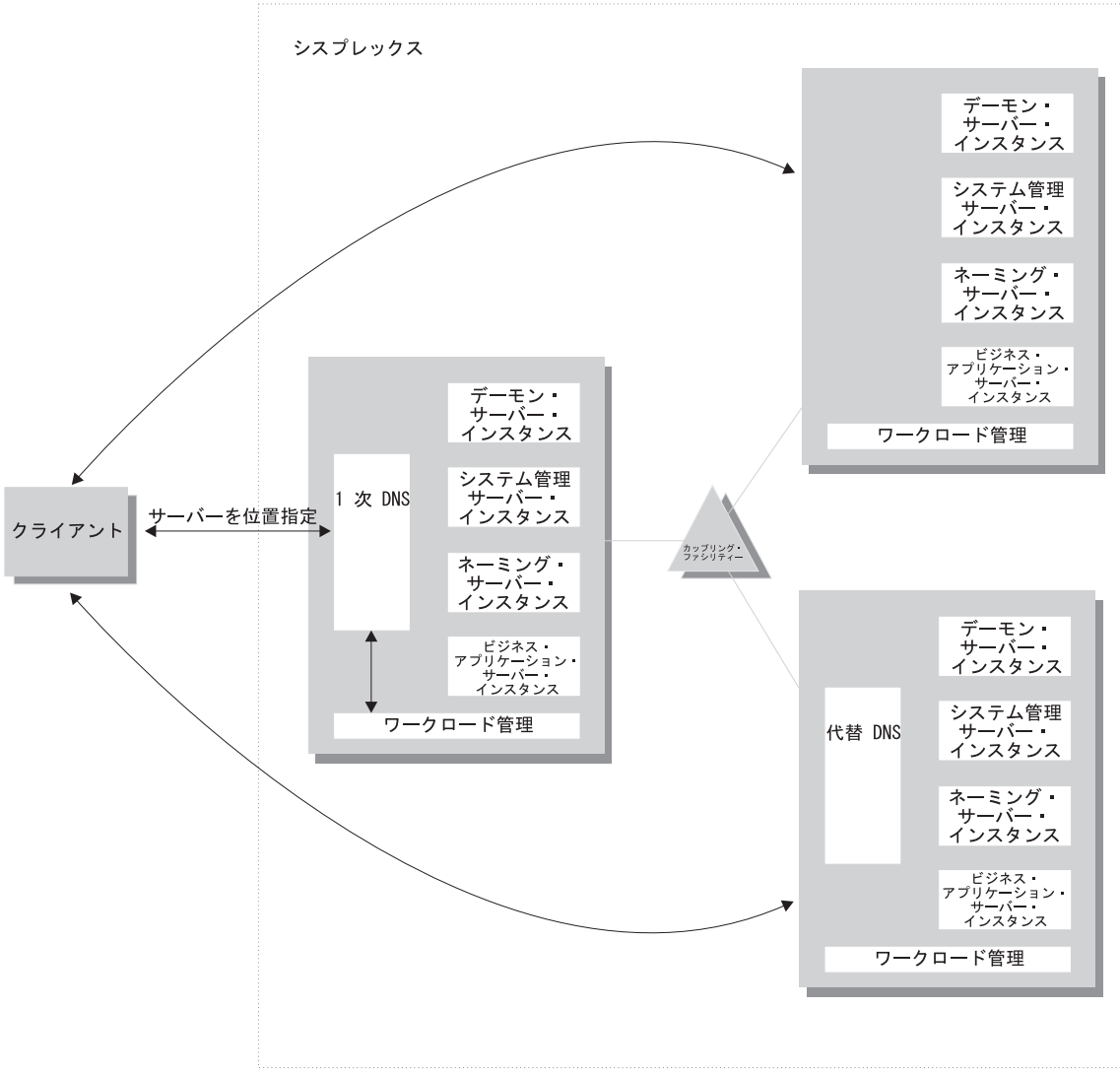


図 14. WebSphere for z/OS、ドメイン・ネーム・サーバー (DNS)、およびワークロード管理

図14 では、シスプレックスの各システムは、WebSphere for z/OS ランタイム (デーモン、システム管理、およびネーミング・サーバー) に加えて、ビジネス・アプリケーション・サーバーも備えています。クライアントは、CORBA General Inter-ORB Protocol (GIOP) を使用して、WebSphere for z/OS の要求を作成します。デーモンは、ロケーション・サービス・エージェントの働きをします。そして、要求のオブジェクト・キーを使用して、位置指定要求を受信します。デーモンはオブジェクト・キーを使用して、そのオブジェクト・キーが表すオブジェクトをサポートするサーバーを位置指定し、次に、そのサーバー

名をワークロード管理に渡します。ワークロード管理は、シスプレックスで、その要求を処理するのに最適なサーバー・インスタンスを選択します。デーモンは、選択されたサーバー・インスタンスに関連した特定の IOR 情報を、オリジナルの IOR に保管されているオブジェクト・キー情報とマージします。このマージの結果、直接 IOR がクライアントに戻されます。クライアント ORB は、この戻された参照を使用して、当該オブジェクトを保持するサーバー・インスタンスに対する IOR 接続を確立します。

WebSphere for z/OS が使用するトランスポート機構は、クライアントがローカルであるかリモートであるかによって異なります。クライアントがリモートの場合 (つまり、同じ OS/390 または z/OS システムで稼働していない場合)、トランスポートは TCP/IP です。クライアントがローカルの場合は、トランスポートはプログラム呼び出しを介するものになります。ローカル・トランスポートが高速なのは、物理的にネットワーク内を移動する必要がなく、データ変換が不要で、要求のマーシャルを単純化し、セキュリティーのために、Kerberos や SSL を起動する必要がなく、最適化された RACF 機能を使用するためです。

作業要求のアドレス・スペース管理: WebSphere for z/OS は、ワークロード管理 (WLM) のエンクレーブを使用することにより、作業要求のパフォーマンス・コンテキストを伝えています。個々のトランザクションは、それぞれ独自のエンクレーブを保有し、そのサービス・クラスに従って管理されます。356ページの図15 で示されているように、サーバー・インスタンスの制御領域 (ワークロード管理は、これをキュー・マネージャーと見なします) は、クライアント要求に関連したエンクレーブを使用して、作業の優先順位を管理します。作業の優先順位が高ければ、ワークロード管理はその作業を、サーバー・インスタンスの高優先順位サーバー領域に送信することができます。作業の優先順位が低ければ、ワークロード管理はその作業を、低優先順位サーバー領域に送信することができます。同じサーバー・インスタンス内で、優先順位によって作業を区分するという効果があります。

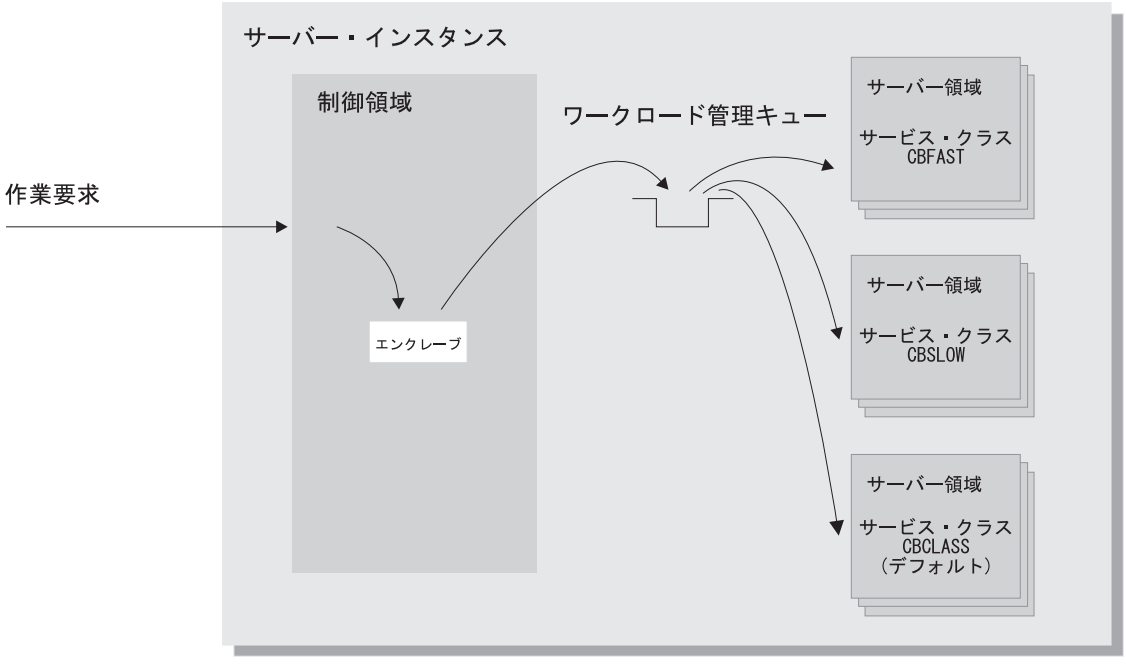


図 15. 作業の優先順位を管理するエンクレーブの使用

エンクレーブは次のいくつかの方法で作成することができます。

- WebSphere for z/OS は独自の規則セットを使用して、ネットワークからのクライアント要求のためのエンクレーブを作成します。
- 一部のサブシステム (Web サーバーなど) は、エンクレーブを作成してそれを WebSphere for z/OS に渡し、それがまた次のエンクレーブに渡されます。
- WebSphere for z/OS は、バッチ・ジョブをリモート・クライアントのように扱います。

ワークロード管理にパフォーマンス・コンテキストを伝達するには、次の作業修飾子に従って、システム内のワークロードを分類する必要があります。

表 40. WLM 作業修飾子とそれに対応する WebSphere for z/OS エンティティー

作業修飾子の省略形	作業修飾子	対応する WebSphere for z/OS エンティティー
CN	集合名	サーバー名
UI	ユーザー ID	作業が実行されているユーザー ID

分類の規則とワークロード修飾子に関する詳細は、*z/OS MVS 計画 : ワークロード管理*, SA88-8574 を参照してください。

クライアントのワークロードに加えて、WebSphere for z/OS ランタイム・サーバー、およびビジネス・アプリケーション・サーバーのパフォーマンスも考慮しなければなりません。一般に、サーバー制御領域は作業ルーターの役目を果たすので、その優先順位は高くなければなりません。ワークロード管理は、サーバー領域を動的に開始および停止するので、迅速に初期化するためには、サーバー領域にも高優先順位を与える必要があります。ただしいったん初期化されれば、サーバー領域は、クライアント・エンクレーブの優先順位に従って作業を実行するので、ユーザーが割り当てるサーバー領域の優先順位は、初期化の後は重要ではありません。

個々のクラスのパフォーマンス上の目標を設定するには、次の表を使用してください。

表 41. ワークロード管理の規則

分類の対象	割り当て先	理由
デーモン	SYSSTC	システムはこれを開始済みタスクとして扱うので、迅速に作業要求の経路を定める必要がある。
OS/390 Component Broker ランタイム・サーバーの**制御**領域	SYSSTC	制御領域は迅速に作業の経路を定めなければならない。
OS/390 Component Broker ランタイム・サーバーの**サーバー**領域	SYSSTC	サーバー領域は迅速に初期化される必要があるが、いったん初期化されると、クライアント・エンクレーブの優先順位に従って作業を実行する。
ユーザーのビジネス・アプリケーションの**制御**領域	領域内で実行される作業と少なくとも同程度の重要性を持つクラス	制御領域は迅速に作業の経路を定めなければならないが、ユーザーのビジネス・アプリケーション・サーバーと、システム内の他の作業とのバランスをとる必要がある。

表 41. ワークロード管理の規則 (続き)

分類の対象	割り当て先	理由
ユーザーのビジネス・アプリケーションの**サーバー**領域	SYSSTC	サーバー領域は迅速に初期化される必要があるが、いったん初期化されると、クライアント・エンクレーブの優先順位に従って作業を実行する。
クライアントのワークロード	システム内の他の作業に対応した重要性を持つクラス	WebSphere for z/OS とワークロード管理は、ユーザーが設定する目標に従って作業を実行する。

分類規則の例

WebSphere for z/OS 用に定義された次の 3 つのワークロード管理サービス・クラス (サブシステム・タイプ CB) があるとします。

1. CBFAST － 高速応答時間を必要とするトランザクション用に設計
2. CBSLOW － 高速応答時間を必要としない長時間実行アプリケーション用に設計
3. CBCLASS － 上記以外の作業要求用に設計

ユーザーは、高速応答時間を必要とするクライアントのワークロード、BBOASR1 を設計します。また、ユーザーの上司のユーザー ID (DBOOZ) で実行する作業の応答時間を、それよりも遅くします。最後に、残りの作業要求はすべて、デフォルトのサービス・クラス、CBCLASS の下で実行するようにします。

表 42. 分類規則の例

タイプの列	名前の列	サービスの列	目標
CN	BBOASR1	CBFAST	2 秒で 90% を完了
UI	DBOOZ	CBSLOW	速さ 50、重要度 = 3
(デフォルト)	(ブランク)	CBCLASS	任意

IWMARIN0 を使用すると、次のようなパフォーマンス上の目標を設定することができます。

1. IWMARIN0 を発行して、オプション 4 を選択する。

```
  File  Utilities  Notes  Options  Help
-------------------------------------------------------------------------------
Functionality LEVEL003         Definition Menu         WLM Appl LEVEL004
Command ===> ____________________________________________________________

Definition data set  . . : 'CB.MYCB.WLM'

Definition name  . . . . . CB390      (Required)
Description  . . . . . . . WLM Setup for WebSphere for z/OS
Select one of the
following options. . . . . 4__  1.  Policies
                               2.  Workloads
                               3.  Resource Groups
                               4.  Service Classes
                               5.  Classification Groups
                               6.  Classification Rules
                               7.  Report Classes
                               8.  Service Coefficients/Options
                               9.  Application Environments
                              10.  Scheduling Environments
```

2. サービス・クラス CBFAST を作成し、2 秒でその 90% を完了するように指定する。

   注: この例では、ONLINE というワークロードを定義したと想定しています。

```
  Service-Class  Notes  Options  Help
-------------------------------------------------------------------------------
                          Create a Service Class              Row 1 to 2 of 2
Command ===> ____________________________________________________________

Service Class Name . . . . . . CBFAST    (Required)
Description  . . . . . . . . . Quick CB transactions
Workload Name  . . . . . . . . ONLINE    (name or ?)
Base Resource Group  . . . . . ________  (name or ?)

Specify BASE GOAL information.  Action Codes: I=Insert new period,
E=Edit period, D=Delete period.

        ---Period---  ----------------------Goal---------------------
Action  #  Duration   Imp.  Description

  __
  __    1              1    90% complete within 00:00:02.000
****************************** Bottom of data ********************************


  .-------------------------------------------------------------------------.
  | Press EXIT to save your changes or CANCEL to discard them. (IWMAM970) |
  '-------------------------------------------------------------------------'
```

3. サービス・クラスを保存する。次のように表示されます。

```
  Service-Class  View  Notes  Options  Help
------------------------------------------------------------------------------
                        Service Class Selection List          Row 1 to 14 of 21
Command ===> ____________________________________________________________

Action Codes: 1=Create, 2=Copy, 3=Modify, 4=Browse, 5=Print, 6=Delete,
              /=Menu Bar


Action  Class     Description                      Workload
   __     CBFAST    Quick CB Transactions            ONLINE
****************************** Bottom of data ********************************
```

4. CBSLOW サービス・クラスについても上記のステップを繰り返す。
5. 新規サービス・クラスを使用して分類規則を作成する。メイン画面のオプション 6 を選択してください。

```
  File  Utilities  Notes  Options  Help
------------------------------------------------------------------------------
Functionality LEVEL003         Definition Menu         WLM Appl LEVEL004
Command ===> ____________________________________________________________

Definition data set  . . : 'CB.MYCB.WLM'

Definition name  . . . . . CB390      (Required)
Description  . . . . . . . WLM Setup for OS/390 Component Broker

Select one of the
following options. . . . . 6__  1.  Policies
                               2.  Workloads
                               3.  Resource Groups
                               4.  Service Classes
                               5.  Classification Groups
                               6.  Classification Rules
                               7.  Report Classes
                               8.  Service Coefficients/Options
                               9.  Application Environments
                              10.  Scheduling Environments
```

6. サービス・クラス用の規則セットを作成する。

```
  Subsystem-Type  Xref  Notes  Options  Help
------------------------------------------------------------------------------
                Create Rules for the Subsystem Type        Row 1 to 2 of 2
Command ===> _____________________________________________ SCROLL ===> PAGE

Subsystem Type . . . . . . . . . CB    (Required)
Description  . . . . . . . . . . CB Series classification
Fold qualifier names?  . . . . Y  (Y or N)

Action codes:  A=After    C=Copy         M=Move     I=Insert rule
               B=Before   D=Delete row   R=Repeat   IS=Insert Sub-rule
          -------Qualifier-------------             -------Class--------
Action    Type       Name     Start                 Service     Report
                                                DEFAULTS: CBCLAS      ________
 ____  1  CN         BBOASR1  ___                   CBFAST      ________
 ____  1  UI         DBOOZ    ___                   CBSLOW      ________
****************************** BOTTOM OF DATA ******************************
```

この例で、BBOASR1 用の作業は、ユーザー ID DBOOZ の下で実行される作業以外はすべて、CBFAST に分類されます。DBOOZ のための作業は、CBSLOW に分類されます。その他の作業 (シスプレックスの外側のクライアントから来る作業、WebSphere for z/OS ランタイム・サーバーのための作業など) はすべて、CBCLASS に分類されます。

IMS-OTMA 手続き型アプリケーション・アダプター

IMS-OTMA 手続き型アプリケーション・アダプターは、IMS の Open Transaction Manager Access (OTMA) プロトコルを使用します。そのため、従わなければならないガイドラインや要件があります。

- IMS、Java for OS/390 または z/OS、および WebSphere for z/OS は、シスプレックスの同一システム上になければなりません。このような制限があるのは、OTMA インターフェース (これによって、RRS はトランザクションの整合ができるようになります) では、クライアント (WebSphere for z/OS) と IMS サーバーが同一システム上なければならないためです。
- IMS を、WebSphere for z/OS および DB2 for OS/390 と同じ再始動グループに組み込んでください。295ページの『自動再始動管理のセットアップ』を参照してください。
- WebSphere for z/OS アプリケーション・サーバー・インスタンスは、IMS-OTMA クライアントの役目を果たします。つまり、IMS-OTMA と通信するためには、同じ XCF グループにいなければならないということです。

  IMS-OTMA XCF グループ名は、ユーザーが管理アプリケーションを使用して、IMS-OTMA PAA 論理リソース・マッピング (LRM) を定義するときに必要なパラメーターの 1 つです。もう 1 つは XCF パートナー名で、これは、サーバーが通信する特定の IMS を識別します。XCF パートナー名は、

初期化に使用される IMS DFSPBxxx proclib メンバーで、OTMANM パラメーターが指定する名前です。OTMANM パラメーターが定義されていない場合は、IMS DFSPBxxx メンバーの APPLID1 パラメーターが指定する名前が、デフォルトの XCF パートナー名として使用されます。

- アプリケーション・サーバー・インスタンスの制御領域ユーザー ID に、RACF FACILITY クラスの IMSXCF.OTMACI リソースに対する読み取り権限を与えなければなりません。詳細は、*IMS/ESA Open Transaction Manager Access Guide*, SC26-8743 を参照してください。
- IMS 並列スケジューリング限界を 0 (任意の数のトランザクションを、スケジューリングすることができる) に設定してください。
- WebSphere for z/OS アプリケーションの 1 つのトランザクションが、IMS では複数のトランザクションになる場合があります。たとえば、WebSphere for z/OS アプリケーションのトランザクションの有効範囲内で、プログラムが、1 つの findByPrimaryKey、3 つの setter、および 3 つの getter を実行したとします。その結果、3 つの個別の IMS トランザクションが生じます。トランザクションに関するこの乗算効果は、IMS に必要なメッセージ処理領域の数に影響を与えます。DFSMPR ジョブで、メッセージ処理領域の数が、WebSphere for z/OS トランザクションから生じる可能性のあるトランザクションの数と等しくなるように、指定しなければなりません。たとえば、WebSphere for z/OS トランザクションが、5 つの IMS トランザクションを生じる可能性がある場合は、メッセージ処理領域の数を 5 に設定します。

  WebSphere for z/OS アプリケーションを追加したために、同じデータベース上で、さらに IMS トランザクションが発生する場合は、メッセージ処理領域の数を、すべてのアプリケーションから生じる可能性のあるトランザクションの最大数に合わせて設定してください。
- IMS のターゲット・トランザクション・プログラムを介して通信する場合は、SendReceive 要求しか使用できません。IMS トランザクション・プログラムを介して、送信専用処理または受信専用処理を行う要求は、サポートしていません。
- OTMA に関する詳細は、*IMS/ESA Open Transaction Manager Access Guide*, SC26-8743 を参照してください。
- 以下は、IMS-OTMA 手続き型アプリケーション・アダプターを使用する、ビジネス・アプリケーション・サーバーのための計画の要件およびガイドラインです。IMS を使用する WebSphere for z/OS アプリケーションのコーディングに関する詳細は、サーバーのセットアップも含めて、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 に記載されています。

– サーバーの論理リソース・マネージャーを定義する場合は、IMS_OTMA_PAA を論理リソース・マネージャーのサブシステム・タイプとして選択し、論理リソース・マネージャー・インスタンスの接続データとして、以下を識別する必要があります。

XCF グループ名
IMS の初期化に使用される DFSPBxxx proclib メンバーの、GRNAME パラメーターで指定される名前を入力します。

XCF パートナー名
IMS の初期化に使用される DFSPBxxx proclib メンバーの、OTMANM パラメーターで指定される名前を入力します。そうでない場合は、DFSPBxxx メンバーの APPLID1 パラメーターが指定する名前を使用します。このパラメーターは、OTMANM パラメーターが定義されていない場合には、デフォルトの XCF パートナー名となります。

セッション数
1 を指定します。

TPIPE 接頭部
システムが、この LRM に必要なすべてのトランザクション・パイプに使用できるように、接頭部を指定します。接頭部は 4 文字以下でなければなりません。この LRM のトランザクション・パイプを作成する際に、システムは、この接頭部を使用し、セッション関連情報を表す 4 文字を付加することにより、固有のトランザクション・パイプ名を生成します。

規則: 任意のサーバー・インスタンスに対して構成される、同一の XCF グループ名を持つ論理リソース・マネージャー・インスタンスを、複数保有することはできません。

特定のサーバー・インスタンスでは、WebSphere for z/OS は、論理リソース・マネージャー・インスタンスが指定する IMS XCF グループ内では、単一の IMS メンバーに一度だけしか接続しません。IMS メンバー名が異なる同じ XCF グループ名、TPIPE 名、またはセッション数をもつ、別の論理リソース・マネージャー・インスタンスを介して、サーバー・インスタンスの構成を行った場合は、その論理リソース・マネージャー・インスタンスの初期化は、同じ IMS XCF グループに接続しようとすると、失敗します。これは、最初の接続の結果、サーバー・インスタンスがすでに IMS グループのメンバーになっているからです。

– XCF データ・セット定義内に必要なメンバーすべてを指定していることを確認してください。IMS-OTMA 手続き型アプリケーション・アダプターを使用して、各サーバーごとに、XCF データ・セット・メンバーを指定しなければなりません。

CICS-EXCI 手続き型アプリケーション・アダプターのセットアップ

CICS 手続き型アプリケーション・アダプターは、CICS-EXCI インターフェースを使用します。この節では、WebSphere for z/OS の CICS-EXCI インターフェースをセットアップする際に従うべきステップについて、説明します。

CICS-EXCI 手続き型アプリケーション・アダプターをセットアップするためのステップ

この作業を始める前に: Java for OS/390 または z/OS、WebSphere for z/OS、および同じ OS/390 または z/OS イメージ上で接続する CICS サブシステムがなければなりません。このような制限があるのは、EXCI インターフェース (これによって、RRS はトランザクションの整合ができるようになります) では、クライアントと CICS サーバーが同一システム上になければならないからです。

CICS-EXCI 手続き型アプリケーション・アダプターをセットアップするには、次のステップに従ってください。

1. CICS *hlq*.SYSIN(*member*) データ・セットで、RRMS=YES と指定して、RRS コンテキストに CICS を参加させる。

   ---

2. CICS を、WebSphere for z/OS および DB2 for OS/390 と同じ再始動グループに組み込む。295ページの『自動再始動管理のセットアップ』を参照してください。

   ---

3. ユーザーのアプリケーション用に CICS 領域をセットアップする。サンプル・ジョブ BBOADEFS が提供され、アプリケーション (ここでは BCASHAC プログラム) 用の CICS 領域がセットアップされます。

   ---

4. CICS 手続き型アプリケーション・アダプターを使用する、以下のビジネス・アプリケーション・サーバーの要件およびガイドラインに従う。
   - WebSphere for z/OS サーバー名と同じ NETNAME を使用して、CICS リソース定義で、特定の タイプ接続を定義しなければなりません。

- サーバーの論理リソース・マネージャーを定義する場合は、CICS_EXCI_PAA を論理リソース・マネージャーのサブシステム・タイプとして選択し、論理リソース・マネージャー・インスタンスの接続データとして、以下を識別する必要があります。

  CICS applid
  CICS アプリケーション ID

  CICS を使用する WebSphere for z/OS アプリケーションのコーディングに関する詳細は、サーバーのセットアップも含めて、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル* に記載されています。

構成ステップに関してはこれで終了です。ビジネス・アプリケーションのテスト機能を使用して、CICS-EXCI のセットアップをテストする必要があります。

IMS-APPC 手続き型アプリケーション・アダプター

IMS-APPC 手続き型アプリケーション・アダプターを使用すると、WebSphere for z/OS が、APPC/MVS を介してリモートまたはローカル・システム上の IMS と通信できるようになります。APPC/MVS は、WebSphere for z/OS が、ピアツーピア・ベースでアプリケーション・プログラムと通信する際に活用する、プログラミング・インターフェース (LU 6.2 アーキテクチャー) を提供します。WebSphere for z/OS の設定を通じて、ユーザーは、APPC 会話を保護するかどうかを決定することができます。次の 3 つが可能です。

- ユーザーは保護会話を要求することができます。保護会話 (論理リソース・マネージャー・インスタンスで指定される `syncpt`) を使用して、APPC/MVS は通信リソース・マネージャーになり、WebSphere for z/OS トランザクションの結果に関心があることを表明して、WebSphere for z/OS と同じトランザクション有効範囲の別のシステムで稼働している、IMS トランザクションを駆動します。分散アプリケーションに代わって実行されるすべての処理は、アトミック操作、または単一の操作として扱われます。つまり、APPC/MVS、WebSphere for z/OS、および IMS は、すべてのアプリケーションが更新される (コミット) か、更新されない (ロールバック) かのいずれかであるように、その処理を調整します。この調整は、データ保全性に大きく依存しているアプリケーションには、非常に有益です。

  このトランザクション管理は、ユーザーが、IMS-APPC 手続き型アプリケーション・アダプターまたは保護会話を使用して、サーバーを作成すると、自

動的に発生します。これを、「会話に同期点機能がある」と言います。つまり、アプリケーションのデータと、IMS データベースのデータとの同期が保たれているということです。

- ユーザーは無保護会話を許可することができます。アプリケーションが保護会話の使用を必要としていない場合は、IMS-APPC 手続き型アプリケーション・アダプターを、同期点機能をオフにして (論理リソース・マネージャー・インスタンスで `none` を指定) 使用して、サーバーを作成することができます。同期点機能がなければ、IMS データベースのデータがクライアント・アプリケーションのデータと同期する保証はありません。更新が行われた場合、IMS のデータを再検査するのは、クライアント・アプリケーションの責任になります。データの同期はとれませんが、次のようなメリットがあります。
  - アプリケーションは、分散トランザクションに関連したパフォーマンスの影響を受けなくなります。
  - IMS メッセージ処理領域 (MPR) が使用中であることが、少なくなります。トランザクションでは、簡単な読み取り / 書き込み操作でも、2 つのメッセージ処理領域が、トランザクション・コミットメントが発生するまで使用中のままになっている必要があります。同期点機能を使用しない場合は、1 つのメッセージ処理領域がデータ要求を処理し、その後ただちに別の要求を受け入れることができます。
- APPC 会話が割り振られるときに保護されるかどうかを、WebSphere for z/OS が決定できるようにすることができます (論理リソース・マネージャー・インスタンスで、`autotran` を指定します)。WebSphere for z/OS は、コンテナー・トランザクション・ポリシーおよび、現在の実行スレッドが動作しているトランザクションのタイプに基づいて、決定を行います。

  コンテナー・トランザクション・ポリシーは、実行スレッドが動作するトランザクションのタイプを制御します。コンテナーは、グローバル・トランザクション (TX_REQUIRED) を要求するか、あるいは、アプリケーションが開始するローカル・トランザクションのバリエーション (これらのバリエーションは、集合的に HYBRID_GLOBAL ポリシーと呼ばれます) を許可することができます。WebSphere for z/OS が APPC 会話を割り振ろうとしているときに `autotran` が設定されていれば、WebSphere for z/OS は次のような動作を行います。
  - 実行スレッドがグローバル・トランザクションの下で動作している (コンテナー・ポリシーが、グローバル・トランザクションを要求する) 場合は、保護会話を割り振ります。

– 実行スレッドがローカル・トランザクションの下で動作している (コンテナー・ポリシーが、ローカル・トランザクションを許可する) 場合は、無保護会話を割り振ります。

APPC 接続をセットアップする前に、アプリケーションのトランザクション特性を決定し、適切なコンテナー・トランザクション・ポリシーを知っていなければなりません。トランザクション・ポリシーに関する詳細は、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 に記載されています。これらのことを知る必要があるのは、それによって、同期点機能を介して APPC 接続を定義する必要があるかどうかが決まるためです。論理リソース・マネージャー・インスタンスで、設定値 `syncpt` または `autotran` を使用する場合は、APPC 接続で、同期点機能を定義しなければなりません。論理リソース・マネージャー・インスタンスで、設定値 `none` を使用する場合は、APPC 接続で、同期点機能を定義する必要はありません。

IMS-APPC 手続き型アプリケーション・アダプターを使用するサーバーのセットアップ

IMS-APPC 手続き型アプリケーション・アダプターを介してサーバーをセットアップするには、通信パスの両側の構成を調整し、次に、管理アプリケーションを介して、WebSphere for z/OS サーバーへの接続を定義しなければなりません。

- WebSphere for z/OS サイド (ローカル・システムとして指定) では、構成を VTAM および APPC 用に調整しなければなりません。
- IMS サイド (パートナー・システムとして指定) では、構成を VTAM、APPC、および IMS 用に調整しなければなりません。
- 最後に、管理アプリケーションを介して、WebSphere for z/OS のための接続を定義しなければなりません。

次の表は、IMS-APPC 手続き型アプリケーション・アダプターを使用するサーバーをセットアップするための、サブタスクおよび関連手順を示したものです。

サブタスク	関連手順 (参照項目)
WebSphere for z/OS (ローカル) サイドをセットアップする	368ページの『WebSphere for z/OS (ローカル) サイドをセットアップするためのステップ』
IMS (パートナー) サイドをセットアップする	369ページの『IMS (パートナー) サイドをセットアップするためのステップ』

サブタスク	関連手順 (参照項目)
WebSphere for z/OS サーバーへの接続を定義する	372ページの『WebSphere for z/OS サーバーへの接続を定義するためのステップ』

APPC/MVS の構成に関する詳細は、*z/OS MVS 計画: APPC/MVS 管理*, SA88-8571 を参照してください。

WebSphere for z/OS (ローカル) サイドをセットアップするためのステップ

この作業を始める前に: VTAM および APPC を、WebSphere for z/OS システムにインストールしておかなければなりません。また、アプリケーションに同期点機能が必要かどうかを決定する必要もあります。

WebSphere for z/OS (ローカル) サイドをセットアップするには、次のステップを実行してください。

1. VTAM に対する論理装置 (LU) を、その APPL 定義で定義する。
   - LU の同期点機能を使用可能にするには、VTAM APPL 定義を、SYNCLVL=SYNCPT および ATNLOSS=ALL を使用してコード化しなければなりません。また、RRS を構成して、それを活動化することも必要です。
   - 同期点機能なしで実行する場合は、SYNCLVL キーワードも ATNLOSS キーワードも指定する必要はありません。

   推奨: LU の方が簡単に管理できるので、特に WebSphere for z/OS の場合は、LU を作成してください。1 つの LU だけを定義すれば、すべての WebSphere for z/OS 開始の会話にそれを渡します。LU 定義の例については、SYS1.SAMPLIB(ATBAPPL) のサンプルを参照してください。

---

2. APPC TP プロファイル・データ・セットを少なくとも 1 つ作成する。APPC TP プロファイル・データ・セットを作成するジョブの例については、SYS1.SAMPLIB(ATBTPVSM) を参照してください。

---

3. VTAM 用に定義した LU と一致する、APPC LU を定義する。TPDATA キーワードで、2 のステップで作成した、APPC TP プロファイル・データ・セットを指定してください。

ヒント: この LU は、おそらく、アウトバウンド会話のみをサポートするので、ユーザーは、LU で NOSCHED を指定することにより、トランザクション・スケジューラーを始動して、リソース・オーバーヘッドの増加を回避することができます。

LU 名は、SYS1.PARMLIB の APPCPMxx メンバーで定義されます。メンバーの例については、SYS1.SAMPLIB(APPCPMxx) を参照してください。

---

4. 同期点機能をインプリメントするには、システム・ロガーに対して、ATBAPPC.LU.LOGNAMES ログ・ストリームを定義する。

   注: WebSphere for z/OS と IMS が同一シスプレックスの異なるシステム上にある場合は、ログ・ストリームにはカップリング・ファシリティーを使用する必要があります。APPC/MVS は、単一システム環境でのみ、DASD のみのログ・ストリームをサポートします。

---

5. IMS システムに対する VTAM 接続が可能であることを確認する。TCP/IP ネットワーク構成では、VTAM サブエリア、VTAM APPN、または SNA を使用することができます。

---

6. VTAM APPL を使用可能にして、VTAM 構成を作成する。

---

7. 新規の WebSphere for z/OS LU 定義を使用して APPC を開始するか、あるいは新規の WebSphere for z/OS LU を動的に活動化して、APPC 構成を作成する。ローカル LU が活動状態であることを確認するには、次のコマンドを発行します。同期点機能が必要な場合は、Protected=YES となっていることを確かめてください。

   ```
   DISPLAY APPC,LU,ALL
   ```

ローカル LU が活動状態になっていて、さらに同期点機能が必要な場合は、Protected=YES が表示されれば、このステップは終了したことになります。

IMS (パートナー) サイドをセットアップするためのステップ

この作業を始める前に: VTAM および APPC を、IMS システムにインストールしておかなければなりません。また、アプリケーションに同期点機能が必要かどうかを決定する必要もあります。

IMS (パートナー) サイドをセットアップするには、次のステップを実行してください。

1. IMS に関連付けられた VTAM に対して、論理装置 (LU) を定義する。この LU を使用して、WebSphere for z/OS は、会話を割り振って IMS との通信を確立します。
   - LU の同期点機能を使用可能にするには、VTAM APPL 定義を、SYNCLVL=SYNCPT および ATNLOSS=ALL を使用してコード化しなければなりません。また、RRS を構成して、それを活動化することも必要です。 LU 定義の例については、SYS1.SAMPLIB(ATBAPPL) を参照してください。
   - 同期点機能なしで実行する場合は、SYNCLVL キーワードも ATNLOSS キーワードも指定する必要はありません。

   規則: このパートナー LU は、通信が開始されると、パスワードのないユーザー ID を受諾できなければなりません (WebSphere for z/OS が、すでにパスワードを検証しています)。このセットアップは、VTAM APPL 定義によって可能になります。そこでは、パラメーター SECACPT=ALREADYV を指定します。その代わりに、APPCLU プロファイルをセットアップすることもできます。この場合は、CONVSEC(ALREADYV) を指定してください。APPC セキュリティーに関する詳細は、*z/OS MVS 計画: APPC/MVS 管理*, SA88-8571 の、セキュリティーに関する章に記載されています。

   ---

2. APPC TP プロファイル・データ・セットを少なくとも 1 つ作成する。APPC TP プロファイル・データ・セットを作成するジョブの例については、SYS1.SAMPLIB(ATBTPVSM) を参照してください。

   ---

3. VTAM で定義したパートナー LU と一致する、APPC LU を定義する。TPDATA キーワードで、2 のステップで作成した、APPC TP プロファイル・データ・セットを指定してください。SCHED キーワードを、LU 定義上の IMS システム ID の値で指定してください。

   LU 名は、SYS1.PARMLIB の APPCPMxx メンバーで定義されます。メンバーの例については、SYS1.SAMPLIB(APPCPMxx) を参照してください。

   ---

4. 同期点機能をインプリメントするには、IMS サイドで、ログ・ストリームを APPC 用に定義したことを確認する。

- IMS が WebSphere for z/OS と同じシステム上で動作している場合は、APPC には、DASD のみまたはカップリング・ファシリティー・ログ・ストリーム (ATBAPPC.LU.LOGNAMES) が必要です。
- IMS が、シスプレックス内の WebSphere for z/OS 以外のシステム上で動作している場合は、APPC には、カップリング・ファシリティーを使用するように定義されているログ・ストリーム (ATBAPPC.LU.LOGNAMES) が必要です。APPC/MVS が、単一システム環境でのみ、DASD のみのログ・ストリームをサポートするためです。
- IMS が、リモート・システム (WebSphere for z/OS と同じシステムでも、シスプレックスでもない) 上で動作している場合は、そのリモート・システム上に、ログ・ストリーム (ATBAPPC.LU.LOGNAMES) が必要です。ログ・ストリームは、DASD のみの構成またはカップリング・ファシリティー構成の、いずれを使用してもかまいません。

---

5. IMS 並列スケジューリング限界を 0 (任意の数のトランザクションを、スケジューリングすることができる) に設定する。

---

6. IMS が保有する必要のあるメッセージ処理の数を決定する。処理数は、同期点機能を使用するかどうかによって決まります。
   - 同期点機能を使用する場合。WebSphere for z/OS アプリケーションの 1 つのトランザクションが、IMS では複数のトランザクションになる場合があります。たとえば、WebSphere for z/OS アプリケーションのトランザクションの有効範囲内で、プログラムが、1 つの findByPrimaryKey、3 つの setter、および 3 つの getter を実行したとします。その結果、3 つの個別の IMS トランザクションが生じます。トランザクションに関するこの乗算効果は、IMS に必要なメッセージ処理領域の数に影響を与えます。DFSMPR ジョブで、メッセージ処理領域の数が、WebSphere for z/OS トランザクションから生じる可能性のあるトランザクションの数と等しくなるように、指定しなければなりません。たとえば、WebSphere for z/OS トランザクションが、5 つの IMS トランザクションを生じる可能性がある場合は、メッセージ処理領域の数を 5 に設定します。
   - 同期点機能を使用しない場合。IMS に処理させようとする同時操作の数に応じて、メッセージ処理領域の数を指定します。

   WebSphere for z/OS アプリケーションを追加したために、同じデータベース上で、さらに IMS トランザクションが発生する場合は、メッセージ処

理領域の数を、すべてのアプリケーションから生じる可能性のあるトランザクションの最大数に合わせて設定してください。

---

7. VTAM APPL を使用可能にして、VTAM 構成を作成する。

---

8. 新規の IMS LU 定義を使用して APPC を開始するか、あるいは新規の IMS LU を動的に活動化して、APPC 構成を作成する。

---

9. APPC-IMS LU を使用可能にするために、MVS または IMS コンソールから、次の IMS コマンドを発行する。

   ```
   /START APPC
   ```

---

10. 次のコマンドを発行して、ローカル LU が活動状態であることを確認する。

    ```
    DISPLAY APPC,LU,ALL
    ```

APPC が正常に開始されれば、このステップは終了したことになります。同期点機能が必要な場合は、Protected=YES となっていることを確かめてください。

WebSphere for z/OS サーバーへの接続を定義するためのステップ

この作業を始める前に: WebSphere for z/OS が、管理アプリケーションも含めてインストールされていなければなりません。

WebSphere for z/OS サーバーへの接続を定義するには、次のステップを実行してください。

⇔ 管理アプリケーションを使用して、そのサーバーの論理リソース・マネージャー (LRM) を定義します。IMS_APPC_PAA を LRM サブシステム・タイプとして選択し、論理リソース・マネージャー・インスタンスの接続データとして、以下を識別してください。

ローカル LU 名
WebSphere for z/OS に関連のある論理装置 (LU) を入力します。このローカル LU 名は、WebSphere for z/OS が動作するシステムの、APPCPMxx parmlib メンバーの LUADD ステートメントで定義されます。

WebSphere for z/OS に関連した LU で、LUADD ステートメントを検索してください。ACBNAME パラメーターで指定された値を、**ローカル** LU 名として使用します。

規則: ACBNAME パラメーターで指定された値だけを使用してください。それが、ネットワーク LU 名です。ローカル LU のネットワーク修飾 (または完全修飾) 名を指定すると、ローカル LU 名が無効であることを指摘するエラー・メッセージ、BBOU0106E が表示されます。

パートナー LU 名

WebSphere for z/OS サーバーが APPC 会話を開始する LU の名前を入力します。このパートナー LU は、IMS が動作するシステムの、APPCPMxx parmlib メンバーの LUADD ステートメントで定義されます。IMS サブシステムは、WebSphere for z/OS サーバーが稼働するシステム以外のシステムに配置することができます。Web Sphere for 2 /oz サーバーと同じシステムに配置してもかまいません。

IMS に関連した LU で、LUADD ステートメントを検索してください (IMS に関連した LU には、LUADD ステートメントの SCHED パラメーターで指定される IMS サブシステム名があります)。ACBNAME パラメーターで指定された値を、**パートナー** LU 名として使用します。

ヒント: パートナー LU 名を指定する場合は、次の形式のいずれか 1 つを使用することができます。

- ACBNAME パラメーターで指定された値のみ (つまり、ネットワーク LU 名)
- ネットワーク修飾名 (形式は、*networkID*.*networkLUname*)

  networkID は、VTAM 開始オプション NETID で指定される値です。*networkLUname* は、ACBNAME パラメーターで指定される値です。
- インストールが汎用リソースを使用するように構成されている場合は、VTAM 汎用リソース名。

VTAM ログモード名

このローカル LU とそのパートナー LU との間の、APPC 会話に関連するネットワーク特性を指定する、VTAM ログモードの名前を入力します。ログモード名は、VTAM ログオン・モード・テーブルに表示されます。このテーブルは、インストールされた VTAMLIB データ・セットにあります。

APPC 会話のタイムアウト値

WebSphere for z/OS サーバーが、その IMS との会話の間に、割り振り呼

び出しおよびそれ以降の任意の呼び出しに対する応答を待機する時間の長さを、分で指定します。有効なタイムアウト値の範囲は、0 〜 1440 (すなわち 24 時間) です。

OTS_DEFAULT_TIMEOUT 環境変数で設定される値より小さい値を指定しても、APPC 会話のタイムアウト値は効果を発揮しません。アプリケーション・サーバーの制御およびサーバー領域で使用する、OTS_DEFAULT_TIMEOUT 環境変数の設定値を検索してください。

APPC 同期レベル

次の表にリストされている値のいずれか 1 つを入力します。この値は、WebSphere for z/OS サーバーが IMS との通信に使用する APPC/MVS 会話のタイプを制御します。このサーバー構成のコンテナーのために選択するトランザクション・ポリシー、およびこのサーバーに配置されるアプリケーションの特性に基づいて、選択を行ってください。

推奨: サーバーが現在処理している要求の、トランザクション・コンテキストと一致する同期レベル値を使用してください。同期レベルとコンテキストを一致させる最も簡単な方法は、**Autotran** を選択して、一致する同期レベルをシステムに判断させることです。

この LRM の接続先	その場合に指定される同期レベル値	注
すべてが TX 必須トランザクション・ポリシーを使用する、1 つまたは複数のコンテナー	**Syncpt** (場合によっては、**None** も許容されます)	このトランザクション・ポリシーは、グローバル・トランザクションの使用を強制するので、APPC 同期レベルの最も論理的な値は、**Syncpt** です。**Syncpt** を使用して、サーバーは保護会話を割り振ります。保護会話は、サーバーと IMS サブシステムの間の対話のために、グローバル・トランザクション・コンテキストを保存し、会話のエラーまたは障害が発生しても、システムがリソースを回復できるようにします。 しかし場合によっては、アプリケーションの処理が、処理中のこの時点でリソースを回復する機能に依存しないなら、**None** の使用を考えてもよいでしょう。**None** を使用すると、APPC/MVS、WebSphere for z/OS、および IMS は、分散アプリケーションに代わって実行された任意の処理を調整しません。調整のオーバーヘッドがなければ、アプリケーションのパフォーマンスは向上します。 **推奨:** • サーバー・アプリケーションが、IMS サブシステムが稼働しているのと同じ z/OS または OS/390 システムで、常に動作することが保証できない場合は、**Syncpt** を使用してください。 • **None** は、慎重に使用してください。この場合に会話のエラーまたは障害が発生したら、アプリケーションが使用するリソースは不整合状態にあることになります。
TX 必須以外のトランザクション・ポリシーを使用する、1 つまたは複数のコンテナー	**Autotran**	これらのポリシーとともに **Autotran** を使用します。システムは、Syncpt または None のどちらの会話タイプが、現行の実行スレッドに関連したトランザクション・コンテキストに適しているかを決定することができます。つまり、現行スレッドがローカル・トランザクション・コンテキストを備えている場合は、サーバーは同期レベル None を使用します。グローバル・トランザクション・コンテキストの場合は、サーバーは Syncpt を使用します。

コンテナーのトランザクション・ポリシーに関する追加情報が必要な場合は、*WebSphere Application Server V4.0 for z/OS and OS/390: J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

論理リソース・マネージャーを保存し、システムが論理リソース・マネージャーを追加したというメッセージを受け取ったら、このステップは終了したことになります。

リカバリーのためのガイドライン

自動再始動管理についておよび、システムに障害が起こり、WebSphere for z/OS がシスプレックスの 2 番目のシステムで復元されるとどうなるかについて、考えてみましょう。RRS が、障害が発生したシステムで動作しているのでない限り、障害が発生したシステムと同じ名前および属性を持つ LU があれば、復元されたシステム上でトランザクションを完了することができます。しかし、障害に備えて、シスプレックスに同じ名前と属性を持つ LU を、2 つセットアップすることはできません。VTAM が、それを許可しないためです (それは、2 つの場所で同じ電話番号を持つようなものです)。ただし、最初のシステムで障害が発生した後に、復元されたシステムで WebSphere for z/OS LU を手動で再活動化することはできます (ちょうど、電話番号を新しい住所に移すようなものです)。

WebSphere for z/OS の機能レベルのマイグレーション

IBM は、WebSphere for z/OS をある機能レベルから別の機能レベルにマイグレーションする必要がある場合に、できるだけ混乱せずにマイグレーションできるような機能と方式を提供しています。これらの機能と方式には、次のようなものがあります。

- マイグレーション・パスのタイプを詳細に記述する。
- WebSphere for z/OS の構成データをオフロードし、後にそのデータを、新規または既存の構成に再ロードする機能を提供する。
- システム管理データベースの環境変数を中央設置場所で管理して、権限のある構成データの検索場所について混乱が起きないようにする。
- WebSphere for z/OS ランタイムの、ある機能レベルから別の機能レベルへの順序に従ってマイグレーションを実行している間は、同じネットワーク内、または同じ OS/390 または z/OS シスプレックス内の、別の機能レベルの WebSphere for z/OS をサポートする。この場合、マイグレーション期間が比較的短い (おそらく数週間) ことが前提となります。

- 異なる機能レベルの WebSphere for z/OS が、長期間 (たとえば、旧リリースの WebSphere for z/OS がまだサポート対象になっている期間) にわたり、同じネットワーク内、または同じ OS/390 または z/OS シスプレックス内で動作できるようにする。

この資料では、WebSphere for z/OS の各リリースおよび機能レベルをマイグレーションする際の、計画情報を提供しています。マイグレーションのパスおよび概念について、ユーザーが計画を決定するのに役立つように説明しています。従うべき実際の手順については、*WebSphere Application Server V4.0 for z/OS and OS/390: 操作および管理*, SA88-8653 を参照してください。

注: このトピックでは、マイグレーションの一般的な概念について説明します。特定のリリースのマイグレーションについては、205ページの『第4章 WebSphere for z/OS の新規リリースへのマイグレーション』を参照してください。

マイグレーション・パスのバックグラウンド情報

WebSphere for z/OS をある機能レベルから別の機能レベルにマイグレーションするには、いくつかの方式があります。方式は、WebSphere for z/OS に加える変更の種類と、ユーザーがデーモン・サーバーを始動する方法によって分類されます。

コールド・スタート

コールド・スタートは、次の場合に使用される方式です。

- WebSphere for z/OS を最初にインストールする場合。WebSphere for z/OS を最初にインストールしてカスタマイズするときのために、デフォルトのシステム構成が提供されます。それらの手順については、55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』で説明しています。
- WebSphere for z/OS の新規機能レベルが WebSphere for z/OS データベースの変更を必要とする際に、既存の構成を、その新規機能レベルに復元する場合。WebSphere for z/OS をある機能レベルから別の機能レベルに移す方式として、このマイグレーション・パスは、最も混乱が起きやすいと言えます。なぜならば、移行の間、WebSphere for z/OS システム (または、シスプレックスで実行している場合はホスト・クラスター全体) をシャットダウンしなければならないからです。
- 災害時回復の場合。災害時回復では、コールド・スタートは、WebSphere for z/OS 構成をオフロードして後の復元に備えるための方式を提供します。

注: WebSphere for z/OS システムのパーシスタント・データをすべてバックアップしたい場合は、次の構成データについて、オフロードだけでなくバックアップも行わなければなりません。

- システム管理データベース
- ネーミング・スペースおよびインターフェース・リポジトリーを含む、LDAP データベース・テーブル
- サーバーが使用する環境変数を含む、HFS のファイル
- WebSphere for z/OS proclib
- WebSphere for z/OS loadlib

詳しくは、285ページの『WebSphere for z/OS システムのバックアップのためのガイドライン』を参照してください。

WebSphere for z/OS をコールド・スタートする際に実行しなければならないタスクは、主に次の 2 つです。

1. コールド・スタートのためのシステムを作成し、既存の構成をオフロード・ファイルにオフロードする。
2. WebSphere for z/OS (または、WebSphere for z/OS がシスプレックスで動作している場合は、ホスト・クラスター全体) をシャットダウンし、機能変更をインストールして、コールド・スタート・オプションでデーモンを再始動する。

コールド・スタート・プロセス: 次の表は、コールド・スタート・プロセスの作業方法について述べたものです。

ステージ	説明
コールド・スタートの準備をする	システム・プログラマーが、管理アプリケーションから、「コールド・スタートの準備 (Prepare for Cold Start)」を実行します。WebSphere for z/OS はすべてのアプリケーション・サーバーを停止します。システムは、構成データを XML 形式で HFS に保管します。また、サーバーの環境変数データも、HFS のファイルに保管します。
WebSphere for z/OS (または、シスプレックスで動作している場合は、ホスト・クラスター全体) をシャットダウンする	WebSphere for z/OS またはホスト・クラスター全体を、シャットダウンしなければなりません。

ステージ	説明
基本コンポーネントを変更する	WebSphere for z/OS の新規機能レベルをインストールします。
システム管理データベースおよび LDAP テーブルを再作成する	システム管理データベースを除去し、WebSphere for z/OS の新規機能レベルに添付されている BBOMCRDB ジョブを実行して、それを再作成します。ネーミングおよびインターフェース・リポジトリー・データが入っている、LDAP テーブルを除去し、それを再作成します。
コールド・スタート・オプション (-ORBCBI COLD) を使用してデーモンを始動する	システムは XML オフロード・ファイルと環境ファイルを読み取り、構成および環境変数のデータを復元します。 システムが、クリーンアップする必要のあるリポジトリーを判別します。たとえば、デーモン IP 名が変更された場合は、システムは、ネーミング・スペースの IOR を無効にします。システム管理データベースは、初期状態にリセットされます。
ネーミングおよびインターフェース・リポジトリー・ブートストラップ・プログラムを実行する	このステージで、新しいホスト名ツリーとインターフェース・リポジトリーが構成されます。
WebSphere for z/OS ブートストラップのフェーズ 2 を実行する	このステージで、WebSphere for z/OS ランタイムの初期構成が完了します。
アプリケーション初期化ルーチンを再実行する	このステージで、アプリケーションのネーミング・コンテキストまたはパーシスタント・データが作成されます。
インターフェース・リポジトリー・ルーチンを再実行する	このステージで、アプリケーションのインターフェース・リポジトリー項目が再作成されます。

このプロセスは、初期インストールおよびカスタマイズとほぼ同じです (55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』を参照)。

コールド・スタートのバックアウト・プラン: 以前の WebSphere for z/OS 機能レベルに復元する必要が生じた場合も、同じコールド・スタート・プロセスを使用しますが、コールド・スタートの準備をして WebSphere for z/OS をシャットダウンしてから、以前の機能レベルの WebSphere for z/OS を復元してください。コールド・スタートの準備中に生成された新規構成データは、以前のレベルでは無視されます。

ホット・スタート

ホット・スタートは、WebSphere for z/OS データベースを変更する必要がなく、クライアントに対する WebSphere for z/OS サービスを中断させることもなく、WebSphere for z/OS の機能レベルを、変更できるようにする方式です。構成内の個々のクラスター・ホスト・インスタンスは、一度に 1 つずつシャットダウンされ、コードの変更が適用されてから、クラスター・ホスト・インスタンスが再始動されます。1 つがシャットダウンされても、他のクラスター・ホスト・インスタンスが動作しているため、クライアントは WebSphere for z/OS からのサービスを受けることができます。

ホット・スタート・プロセス: 次の表は、ホット・スタート・プロセスの作業方法について述べたものです。

ステージ	説明
1 つのクラスター・ホスト・インスタンスにある、すべてのアプリケーション・サーバーを停止する	オペレーターまたはシステム・プログラマーが、すべてのアプリケーション・サーバーを停止します。
クラスター・ホスト・インスタンスをシャットダウンする	クラスター・ホスト・インスタンスは 1 つだけシャットダウンしなければなりません。
必要なコードを更新する	このステージで、新規の WebSphere for z/OS コードをインストールします。
WebSphere for z/OS クラスター・ホスト・インスタンスおよびアプリケーション・サーバーを再始動する	デーモン・サーバー・インスタンスを再始動します。
さらにそれぞれのクラスター・ホスト・インスタンスに対し、このプロセスを繰り返す (一度に 1 つずつ)	

クィック・スタート

クィック・スタートは、WebSphere for z/OS データベースは変更する必要がなく、単一サーバーの再始動だけが必要である場合に使用する方式です。この場合、クラスター・ホスト・インスタンスの単一サーバー・インスタンスが停止され、コードがインストールされた後、そのサーバー・インスタンスは再始動されます。このプロセスは、各サーバー・インスタンスに対し、一度に 1 つずつ繰り返されます。他のサーバー・インスタンスが稼働しているため、そのサーバーは、クライアント要求に応えることができます。

クィック・スタート・プロセス: 次の表は、クィック・スタート・プロセスの作業方法について述べたものです。

ステージ	説明
最初のクラスター・ホスト・インスタンス上のサーバー・インスタンスを停止する	オペレーターまたはシステム・プログラマーが、1 つのサーバー・インスタンスだけを停止します。
必要なコードを更新する	このステージで、新規の WebSphere for z/OS コードをインストールします。
サーバー・インスタンスを再始動する	サーバー・インスタンスが再始動し、クライアントへのサービスができるようになります。
さらにそれぞれのサーバー・インスタンスに対し、このプロセスを繰り返す (一度に 1 つずつ)	

付録A. 環境ファイル

この付録には、環境ファイルと環境変数の参照情報が記載されています。

環境ファイルおよび環境変数

この節では、以下について説明します。

- WebSphere for z/OS による環境変数および環境ファイルの管理方法
- ランタイム・サーバー開始プロシージャーによる環境ファイルを指す方法
- OS/390 または z/OS クライアント用の環境変数
- ランタイム環境変数の構文および意味

注: 追加の環境変数の、アプリケーション開発環境内への設定が必要になる場合があります。*J2EE アプリケーションのアセンブル*, SA88-8654 を参照してください。

WebSphere for z/OS によるサーバー環境変数および環境ファイルの管理方法

インストール中のブートストラップ・プロセスの後、WebSphere for z/OS は、管理アプリケーションを経由して環境データを管理し、その環境データをシステム管理データベースに書き込みます。環境変数データを追加または変更するには、環境データのペア (環境変数名およびその値) をシスプレックス、サーバー、またはサーバー・インスタンスのプロパティー・フォームに入力しなければなりません。会話を活動化にする、またはコールド・スタートを準備する場合、環境変数データは HFS ファイルに書き込まれます。WebSphere for z/OS は、環境ファイルに最も適した値を判別します。たとえば、サーバー・インスタンスの設定は、そのサーバーの同一の変数の設定に優先し、サーバーの設定は、そのシスプレックスの同一の変数の設定に優先します。

環境ファイルを管理アプリケーションを経由せずに直接変更する場合、会話を活動化する、またはコールド・スタートを準備すると、いずれの変更も上書きされます。

会話を活動化する、またはコールド・スタートを準備すると、WebSphere for z/OS は、環境データを各サーバー・インスタンスの HFS ファイルに書き込みます。各環境ファイルのパスおよび名前は、以下のとおりです。

CBCONFIG/controlinfo/envfile/*SYSPLEX*/*SRVNAME*/current.env

ここで、

CBCONFIG
インストール時に、WebSphere for z/OS が構成データおよび環境ファイルを書き込むディレクトリーとして指定する読み取り / 書き込みディレクトリーです。デフォルトは /WebSphere390/CB390 です。

推奨: システム管理サーバー領域のユーザー ID (BBOCBRAC の例では CBSYMSR1) は、/WebSphere390/CB390 ディレクトリーの所有者でなければなりません。システム管理サーバー領域は、このディレクトリーにファイルを書き込みます。他のサーバー領域のユーザー ID に、このディレクトリーへの読み取りアクセスを与えるために、許可ビットを 775 にしてください。

SYSPLEX
シスプレックスの名前です。WebSphere for z/OS は、定義済みの &SYSPLEX JCL 変数からこの名前を派生させます。

SRVNAME
サーバー・インスタンスの名前です。

WebSphere for z/OS の初期インストールを除いて、管理アプリケーションを経由して環境変数を管理しなければなりません。初期インストールでは、初期環境ファイルを変更しなければなりません。これは、ブートストラップ・ジョブが使用しています。環境ファイルを直接変更するのは、このときだけです。

したがって、サーバー用の環境データを定義する 2 つの異なる状態があります。これらの状態を突き合わせることが、環境データを作成する 2 つの異なる方法です。

1. ブートストラップ・プロセスに先行して、環境変数をコーディングすることによって、環境データを定義します。この状態の場合、提供されているサンプルを変更します。ブートストラップ・ジョブは、ファイルを読み取り、環境データをシステム管理データベースに書き込みます。HFS 内の環境ファイルを直接変更するのは、このときだけです。

   環境変数の構文については、386ページの『環境変数の構文』を参照してください。
2. 管理アプリケーションを経由して環境データを定義および管理します。この状態の場合、管理アプリケーション内のパネルを経由して環境データ (環境名およびその値「=」は使用しません) を入力します。

ランタイム・サーバー開始プロシージャーによる環境ファイルを指す方法

WebSphere for z/OS ランタイム・サーバー開始プロシージャーは、構成情報の環境ファイルを指していなければなりません。開始プロシージャーは、HFS フ

ファイルを指す PATH パラメーターのある BBOENV DD ステートメントを使用します。BBOENV DD ステートメントは、以下のとおりです。

```
//BBOENV    DD   PATH='&CBCONFIG/&RELPATH/&SYSPLEX/&SRVNAME/current.env'
```

ここで

&CBCONFIG
開始プロシージャー内に設定する変数です。これは、インストール時に、WebSphere for z/OS が構成データおよび環境ファイルを書き込むディレクトリーとして指定する読み取り / 書き込みディレクトリーと一致しなければなりません。デフォルトは `WebSphere390/CB390` です。

&RELPATH
サブディレクトリー (`controlinfo/envfile`) です。この値を変更してはなりません。

&SYSPLEX
シスプレックスの名前です。これは 定義済み JCL 変数なので、開始プロシージャーで設定する必要はありません。

&SRVNAME
サーバー・インスタンスの名前です。プロシージャーの開始時にサーバー・インスタンスを指定することによって、同じ開始プロシージャーを他のサーバー・インスタンスに使用することができます。

例: サーバー・インスタンス名 BBOASRIA をその開始プロシージャーに渡すには、以下のように指定します。

```
s bboasr1.bboasr1a,srvname='BBOASR1A'
```

同じ開始プロシージャーをサーバー・インスタンス BBOASR1B に使用するには、以下のように指定します。

```
s bboasr1.bboasr1b,srvname='BBOASR1B'
```

OS/390 または z/OS クライアント用の環境変数

管理アプリケーションは、OS/390 または z/OS クライアント用の環境変数の管理は行いません。ユーザーは、OS/390 または z/OS クライアント環境ファイルの作成および管理を行い、クライアント・プログラムからこれらのファイルを指す必要があります。388ページの表43 に、OS/390 または z/OS クライアントに必須の、またはオプションの環境変数が記載されています。

置換変数の使用にあたっての注意

環境ステートメント内では、変数置換 ($ 変数) を使用することはできません。UNIX シェル環境で使用される変数置換は、言語環境プログラム (LE) に

はインプリメントされていません。WebSphere for z/OS は、言語環境プログラム内で環境変数を処理するため、PATH 環境変数内の $PATH などの変数は、失敗します。

例:

UNIX シェル環境では、多くの場合、以下のように、既存のパスに新しいパスを追加することによってパスを設定します。

```
PATH=yourdir
PATH=$PATH/mydir
```

$PATH 変数の置換後、結果のパスは、PATH=yourdir/mydir となります。ただし、WebSphere for z/OS が、変数の割り当てが行われない言語環境プログラム内で環境変数を処理するため、結果のパスは、PATH=$PATH/mydir となります。

環境変数の構文

ブートストラップ・プロセス前の初期環境ファイルの定義時にのみ、この構文に従わなければなりません。

規則: 構文規則は次のとおりです。

- 環境変数の構文は、次のパターンに従います。

  ```
  VARIABLE=VALUE
  ```

  ここで、

  VARIABLE
  環境変数です。

  VALUE
  変数の設定です。この記述は、各変数に対する可能な値を定義しています。

- 変数と値のどちらの場合も、先行および後書きの空白 (ブランクまたはタブ) は無視されます。**例:** 次の 2 行は同じ結果になります。

  ```
  VARIABLE1=VALUE1
  ```

  および

  ```
  VARIABLE1      =      VALUE1
  ```

- 値は空にすることはできず、英字で始めなければなりません。
- 『=』は必須です。

- 値を空にすることは**できません**。必ず、空白文字以外の文字を 1 つ以上指定する必要があります。そうにしなかった場合、その環境変数は無視されます。
- ブランク行は無視されます。
- 大文字と小文字をここに示すとおりにコード化してください。
- 環境変数をコメント化するには、'#' などの文字を変数に追加するだけです。たとえば、TRACEALL=0 を #TRACEALL=0 に変更できます。システムは、変数が英字で始まっていないので、このようなコーディングを無視します。

環境変数の使用

すべての環境変数を各サーバーおよびクライアント用に使用する必要はありません。388ページの表43 に、特定の環境変数を使用する場所について記載されています。ここでは、各列に表示されることがらについての意味を記載します。

- 「R」は、必須の環境変数を意味します。
- 「O」は、オプションを意味します。
- 「F」は、今後のリリースで必須になることを意味します。
- デフォルト列のブランクは、変数が設定されていないことを意味します。
- 他の列のブランクは、変数が使用されないことを意味します。

表の最後に、注が示されています。

注: デフォルト設定および例では、標準の _CEE_ENVFILE 構文を使用します。管理アプリケーション内で環境データを定義する場合には、この構文は使用しません。

表 43. 環境変数を使用する場所

環境変数 =<デフォルト>	デーモン・サーバー・インスタンス	システム管理サーバー・インスタンス		ネーミング・サーバー・インスタンス		インターフェース・リポジトリー・インスタンス		ビジネス・アプリケーション・サーバー・インスタンス		OS/390 または z/OS クライアント
	制御領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	
BBOLANG=ENUS	O	O	O	O	O	O	O	O	O	O
CBCONFIG= /WebSphere390/CB390	R	R	R	R	R	R	R	R	R	
CLASSPATH=			O		O		O		O[1]	
CLIENT_DCE_QOP= NO_PROTECTION										O
CLIENT_HOSTNAME=										O
CLIENTLOGSTREAMNAME=										O
CLIENT_RESOLVE_IPNAME= <RESOLVE_IPNAME の値>			O		O		O		O	O
CLIENT_TIMEOUT=										
com.ibm.ws.naming.ldap.containerdn= ibm-wsnTree=t1,o=WASNaming,c=us				O	O					
com.ibm.ws.naming.ldap. domainname=*sysplex*				O	O					
com.ibm.ws.naming.ldap.masterurl= ldap://<localhost>:1389				O	O					
DAEMON_IPNAME=	R	O								
DAEMON_PORT=5555	O[2]	O[2]								
DATA.CTRLHOST=										O
DATA.CTRLPORT=5000										O
DEFAULT_CLIENT_XML_PATH=										O[3]
DM_GENERIC_SERVER_NAME= CBDAEMON	O[2]	O[2]								
DM_SPECIFIC_SERVER_NAME= DAEMON01	O[4]	O[4]		O[4]		O[4]		O[4]		
HOME=										O
IBM_OMGSSL=0								O	O	
ICU_DATA= /usr/lpp/WebSphere/bin/		R	R							
IR_GENERIC_SERVER_NAME= CBINTFRP		O								

表 43. 環境変数を使用する場所 (続き)

環境変数 =<デフォルト>	デーモン・サーバー・インスタンス	システム管理サーバー・インスタンス		ネーミング・サーバー・インスタンス		インターフェース・リポジトリー・インスタンス		ビジネス・アプリケーション・サーバー・インスタンス		OS/390 または z/OS クライアント
	制御領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	
IR_SPECIFIC_SERVER_NAME= INTFRP01	O[4]	O[4]		O[4]		O[4]		O[4]		
IRPROC=BBOIR	O	O								
IVB_DEBUG_ENABLED=									O	O
IVB_DRIVER_PATH= /usr/lpp/WebSphere		R	R							
IVB_HOME=									O	O
java.naming.factory.initial= com.ibm.ws.naming.ldap. WsnLdapInitialContextFactory				O	O					
java.naming.security.credentials= secret				O	O					
java.naming.security.principal= cn=WASAdmin,o=WASNaming,c=us				O	O					
JAVA_COMPILER=									O	O
JAVA_IEEE754=										O[11]
JVM_DEBUG=			O		O		O		O	
JVM_HEAPSIZE=256									O	
JVM_LOGFILE=									O	O
LDAPBINDPW=		F			R[5]					
LDAPCONF=		F			R[5]					
LDAPHOSTNAME=		F			R[5]					
LDAPIRBINDPW=		F					R[6]			
LDAPIRCONF=		F					R[6]			
LDAPIRHOSTNAME=		F					R[6]			
LDAPIRNAME=		F					R[6]			
LDAPIRROOT=		F					R			
LDAPNAME=		F			R[5]					

表 43. 環境変数を使用する場所 (続き)

環境変数 =<デフォルト>	デーモン・サーバー・インスタンス	システム管理サーバー・インスタンス		ネーミング・サーバー・インスタンス		インターフェース・リポジトリー・インスタンス		ビジネス・アプリケーション・サーバー・インスタンス		OS/390 または z/OS クライアント
	制御領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	
LDAPROOT=		F			R					
LIBPATH=			O		O		O		O[1]	
LOGSTREAMNAME=	O	O								
MIN_SRS=[0 for MOFW の場合 0、J2EE の場合 1]								O		
NM_GENERIC_SERVER_NAME= CBNAMING		O								
NM_SPECIFIC_SERVER_NAME= NAMING01	O[4]	O[4]		O[4]		O[4]		O[4]		
NMPROC=BBONM	O	O								
OTS_DEFAULT_TIMEOUT=30	O	O	O	O	O	O	O	O	O	
OTS_MAXIMUM_TIMEOUT=60	O	O	O	O	O	O	O	O	O	
PATH=									O	O
RAS_MINORCODEDEFAULT= NODIAGNOSTICDATA										
REM_DCEPASSWORD=										O
REM_DCEPRINCIPAL=										O
REM_PASSWORD=		O[7]		O[7]		O[7]		O[7]		O
REM_USERID=		O[7]		O[7]		O[7]		O[7]		O
RESOLVE_IPNAME=		O[8]	O[9]	O[9]	O[9]	O[9]	O[9]	O[9]	O[9]	R[10]
RESOLVE_PORT=900		O	O	O	O	O	O	O	O	O
SM_DEFAULT_ADMIN= CBADMIN		O								
SM_GENERIC_SERVER_NAME= CBSYSMGT		O								
SM_SPECIFIC_SERVER_NAME= SYSMGT01	O[4]	O[4]		O[4]		O[4]		O[4]		
SMPROC=BBOSMS	O	O								
SOMOOSQL=									O	
SRVIPADDR=	O	O		O		O		O		

表 43. 環境変数を使用する場所 (続き)

環境変数 =<デフォルト>	デーモン・サーバー・インスタンス	システム管理サーバー・インスタンス		ネーミング・サーバー・インスタンス		インターフェース・リポジトリー・インスタンス		ビジネス・アプリケーション・サーバー・インスタンス		OS/390 または z/OS クライアント
	制御領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	制御領域	サーバー領域	
SSL_KEYRING=										O
SYS_DB2_SUB_SYSTEM_NAME=DB2	R	R		R		R		R		
TRACEALL=1	O	O	O	O	O	O	O	O	O	O
TRACEBASIC=	O	O	O	O	O	O	O	O	O	O
TRACEBUFFCOUNT=4	O	O	O	O	O	O	O	O	O	
TRACEBUFFLOC=(サーバー: BUFFER クライアント: SYSPRINT)	O	O	O	O	O	O	O	O	O	O
TRACEBUFFSIZE=1M	O	O	O	O	O	O	O	O	O	
TRACEDETAIL=	O	O	O	O	O	O	O	O	O	O
TRACEMINORCODE=										
TRACEPARM=00	O									

注:

1. IMS PAA および CICS PAA を含む、Java を使用するサーバー領域には必須。
2. デーモン・サーバーに値を設定する場合は、システム管理サーバーの制御領域と同じ値を指定しなければなりません。
3. クライアントがシステム管理スクリプト API を使用する場合は必須。
4. シスプレックス内の 2 番目および後続のシステムには、これを指定しなければなりません。
5. LDAPCONF は、LDAPBINDPW、LDAPHOSTNAME、および LDAPNAME と相互に排他的です。LDAPCONF が必須か、あるいは LDAPBINDPW、LDAPHOSTNAME、および LDAPNAME が必須のいずれかです。
6. LDAPIRCONF は、LDAPIRBINDPW、LDAPIRHOSTNAME、および LDAPIRNAME と相互に排他的です。LDAPIRCONF が必須か、あるいは LDAPIRBINDPW、LDAPIRHOSTNAME、および LDAPIRNAME が必須のいずれかです。
7. サーバーが、別のサーバーのリモート・クライアントになる場合に使用されます。
8. ブートストラップ中、デフォルトは、DAEMON_IPNAME の値です。
9. デフォルトは、ローカル・システム IP 名です。通常、コード化は行いません。
10. デーモン・サーバーがクライアントと同一のシステム上にある場合は、オプションです。この場合、デフォルトはローカル・システム IP 名です。
11. OS/390 または z/OS 上で稼働する Java クライアントには必須。

環境変数の説明

BBOLANG=*LANGUAGE*

使用される WebSphere for z/OS メッセージ・カタログの名前です。デフォルトは ENUS です。

CBCONFIG=*path*

会話が活動状態になっている場合に WebSphere for z/OS が構成および環境ファイルを書き込む HFS 内の読み取り / 書き込みディレクトリーを指定します。制御領域およびサーバー領域開始プロシージャー内の &CBCONFIG 変数は、この値と一致しなければなりません。この場合、WebSphere for z/OS は、これらの開始プロシージャーの実行時に、サーバー用の適切な環境ファイルを検出することができます。デフォルトは /WebSphere390/CB390 です。

例: `CBCONFIG=/WebSphere390/CB390`

CLASSPATH=*path1*:*[path2]*:...

サーバー領域内の Java ビジネス・オブジェクトが使用する Java クラス・ファイル (.jar ファイルおよび classes.zip ファイル) を指定します。Java ビジネス・オブジェクトを使用する場合は、その Java ビジネス・オブジェクトの .jar ファイルを指定します。CLASSPATH ステートメントは、全体が 1 行になければなりません。

例:

```
CLASSPATH=/usr/lpp/WebSphere/lib/xerces.jar:...
```

CLIENT_DCE_QOP=*value*

現在のトランザクション・フローに適用する、ローカル OS/390 または z/OS クライアントが使用する DCE メッセージ保護のレベルです。通常は、リモート・システム上のサーバーにアクセスする OS/390 または z/OS クライアント用の DCE セキュリティーを設定します。サーバー用の DCE レベルは、管理アプリケーションを経由して設定されるので、注意してください。

DCE 認証がクライアントおよびサーバー上で使用可能になると、DCE の第三者認証方式を使用したハンドシェーク・メッセージ交換が行われ、それによって、双方の正当性がそれぞれ証明されます。この交換を 1 度行うと、この環境変数の値である、3 つのレベルの保護のうちの 1 つにメッセージを割り当てることができます。

NO_PROTECTION

DCE は、メッセージおよびその応答が正規の送信者からであることのみを保証します。これがデフォルトです。

INTEGRITY
DCE は、そのメッセージが、正規の送信者からであること、および送信者が送信してからいかなる方法でも変更されていないことを保証します。

CONFIDENTIALITY
DCE は、正規の受信者以外は読めないようにメッセージを暗号化します。

CLIENT_HOSTNAME=
OS/390 または z/OS クライアントが、同じシステム上で稼働しているデーモンが存在しなければ、そのクライアントのホスト IP 名を決定できるようにします。クライアント・プログラムで CBSeriesGlobal::hostName() メソッドを発行すると、システムは最初に CLIENT_HOSTNAME 環境変数を検査し、この変数が設定されていれば、その値を戻します。値が設定されていない場合、そのシステム上でデーモンが実行されていれば、システムはデーモンの IP 名を戻します。デフォルト値はヌルです。

例: `CLIENT_HOSTNAME=MYSYS.SYS.COM`

CLIENTLOGSTREAMNAME=*LOG_STREAM_NAME*
OS/390 または z/OS クライアントがエラー情報を書き込む WebSphere for z/OS エラー・ログ・ストリームです。

例: `CLIENTLOGSTREAMNAME=MY.CLIENT.ERROR.LOG`

CLIENT_RESOLVE_IPNAME=*IP_NAME*
OS/390 または z/OS クライアント、またはクライアントとして動作しているサーバー領域がブートストラップ・サーバーにアクセスする場合 (つまり、クライアントまたはサーバー領域が resolve_initial_references メソッドを起動する場合) に使用するインターネット・プロトコル名です。デフォルトは、RESOLVE_IPNAME 環境変数によって指定された値で、システム管理サーバー (デフォルトのブートストラップ・サーバー) に関連付けられたインターネット・プロトコルです。RESOLVE_IPNAME が設定されていない場合、値は、クライアントまたはサーバー領域が稼働しているシステムとなります。

CLIENT_RESOLVE_IPNAME 環境変数を使用すると、リモート・システム上で稼働しているブートストラップ・サーバーを指定できるようになります。一方、他のクライアントは、RESOLVE_IPNAME 環境変数によって定義されたローカル・ブートストラップ・サーバーを使用します。

注: CLIENT_RESOLVE_IPNAME の TCP/IP ポート番号は、RESOLVE_PORT 環境変数によって定義されます。

CLIENT_RESOLVE_IPNAME の値は、255 文字まで可能です。

例: CLIENT_RESOLVE_IPNAME=REMHOST

CLIENT_TIMEOUT=*n*

クライアントのメソッド呼び出しからの応答のタイムアウト値を設定します。これらの値は、整数で、10 分の 1 秒単位の時間を表しています (したがって、値 10 は 1 秒です)。デフォルト値は 0 です。これは、タイムアウト値が設定されていないことを意味します。

例: CLIENT_TIMEOUT=20

com.ibm.ws.naming.ldap.containerdn=*dn*

WsnName ツリーの開始点です。この環境変数は、ネーミング・サーバーだけが使用します。デフォルトは、次のとおりです。

```
ibm-wsnTree=t1,o=WASNaming,c=us
```

この値は、LDAP 初期設定ファイル (弊社のサンプルは bboldif.cb) の中で指定されている値と一致する必要があります。LDAP では大文字と小文字は問題になりませんが、環境変数については問題になる点に注意してください。また、″o=,c=″ の部分も、接尾部として bboslapd.conf の中で指定する必要があります。たとえば次のようになります。

```
suffix   "o=WASNaming,c=US"
```

ヒント: suffix ステートメントは、次のようになります。

```
suffix         "<ws_rdn>"
```

弊社が出荷するサンプルの bboslapd.conf の中でも、このように指定されています。

例:

```
com.ibm.ws.naming.ldap.containerdn=ibm-wsnTree=t1,o=WASNaming,c=us
```

com.ibm.ws.naming.ldap.domainname=*sysplex*

ホスト・ルートを一意的に識別し、JNDI グローバル・ネーム・スペースの区分化の基礎となります。この環境変数は、ネーミング・サーバーだけが使用します。デフォルトはシスプレックス名です。

例:

```
com.ibm.ws.naming.ldap.domainname=plex1
```

com.ibm.ws.naming.ldap.masterurl=ldap://*IP_name*:*port*

LDAP サーバー IP 名とポート番号です。この環境変数は、ネーミング・サーバーだけが使用します。デフォルトは、ldap://<localhost>:1389 です。

例:

```
com.ibm.ws.naming.ldap.masterurl=ldap://wsldap:1389
```

DAEMON_IPNAME=*IP_NAME*

デーモン・サーバーがドメイン・ネーム・サービス (DNS) で登録するインターネット・プロトコル名です。CORBA クライアントの WebSphere for z/OS との通信は、いずれも、この IP 名を必要とします。

デーモン・ブートストラップ・プロセスを開始する前に、インストール時に DAEMON_IPNAME 環境変数を定義しなければなりません。定義しない場合、WebSphere for z/OS はエラー・メッセージを発行し、デーモンを終了します。

ブートストラップ・プロセスは、他のことがらと共に、システム管理データベース内のデーモン IP 名を設定します。ブートストラップ後、WebSphere for z/OS は、システム管理データベース内の値を使用します。ブートストラップの後で、DAEMON_IPNAME 環境変数の値がシステム管理データベース内にある値とは別の値に変わることは、あり得ます。このようなことが起こった場合は、エラー・メッセージが発行されますが、デーモンは、システム管理データベースからのデーモン IP 名で初期化します。

デーモン・サーバー・インスタンスを同一のホスト・クラスター内に配置するには、各サーバー・インスタンスと同一の DAEMON_IPNAME 値をコード化しなければなりません。

規則:

- DAEMON_IPNAME の値は、完全修飾の長い名前でなければなりません。
- 第 1 レベルの修飾子は、1 ～ 18 文字まで可能です。
- デーモンのポートおよび IP 名は、一度選択したら、変更すべきではありません。これは、すべてのオブジェクト参照にこのポートおよび IP 名が含まれているからです。これらを変更すると、既存のオブジェクトにはアクセスできなくなります。

例: `DAEMON_IPNAME=CBQ091.PDL.POK.IBM.COM`

DAEMON_PORT=*n*

デーモン・サーバーが要求を listen するポート番号です。デフォルトは 5555 です。値を設定する場合は、システム管理サーバーの制御領域と同じ値を指定しなければなりません。

例: `DAEMON_PORT=5555`

DATA.CTRLHOST=*IP_ADDRESS*

オブジェクト・レベル・トレースのクライアント・コントローラーが稼働するワークステーション IP アドレスを指定します。IBM 分散デバッガーでクライアントおよびサーバーのコンポーネントをデバッグしている場合に、これを使用します。

例: `DATA.CTRLHOST=MYHOST.IBM.COM`

DATA.CTRLPORT=*n*

オブジェクト・レベル・トレースのクライアント・コントローラーが listen しているポートを指定します。IBM 分散デバッガーでクライアントおよびサーバーのコンポーネントをデバッグしている場合に、これを使用します。デフォルトは 5000 です。

例: `DATA.CTRLPORT=5000`

DEFAULT_CLIENT_XML_PATH=*path*

システム管理スクリプト API で使用されるデフォルトのパラメーター・リストを保持している一連の XML ファイルの位置を指定します。システム管理スクリプト API を使用するクライアントには、この環境変数を設定しなければなりません。

IBM では、デフォルトのパラメーター・リストが入った一連のサンプル XML ファイルを提供しています。インストールの後、それらのサンプルは `/usr/lpp/WebSphere/samples/smapi` に常駐します。XML ファイルとパラメーター・リストについては、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理スクリプト API*, SA88-8657 を参照してください。

システム管理スクリプト API のデフォルト動作は、次の 2 つの方法で上書きできます。

1. システム管理スクリプト API を呼び出す REXX スクリプトの中で明示的にパラメーターを指定します。パラメーターを明示的に指定することにより、IBM が提供する XML サンプルを修正せずに済みます。クライアント環境ファイルの中で、単に、

   ```
   DEFAULT_CLIENT_XML_PATH=/usr/lpp/WebSphere/samples/smapi
   ```

   とコード化します。

2. XML ファイルを別のディレクトリーにコピーし (IBM が提供するサンプルは読み取り専用です)、パラメーター・リストに修正を加えてから、その新しいディレクトリーを指すように DEFAULT_CLIENT_XML_PATH を変更します。これらの変更を加える必要があるのは、システム管理スクリプト API のデフォルト動作を永続的に上書きしたい場合だけです。

例: `DEFAULT_CLIENT_XML_PATH=/usr/lpp/WebSphere/samples/smapi`

DM_GENERIC_SERVER_NAME=*SERVER_NAME*

デーモン・サーバーのサーバー名です。デフォルトは CBDAEMON です。値を設定する場合は、システム管理サーバーの制御領域と同じ値を指定しなければなりません。

例: `DM_GENERIC_SERVER_NAME=CBDAEMON`

DM_SPECIFIC_SERVER_NAME=*SERVER_INSTANCE_NAME*

デーモン・サーバーのサーバー・インスタンス名です。デフォルトは DAEMON01 です。この環境変数は、シスプレックス内の 2 番目以降のシステムにあるすべてのサーバー・インスタンスについて指定する必要があります。

例: `DM_SPECIFIC_SERVER_NAME=DAEMON01`

IBM_OMGSSL=[0 | 1]

CORBA 準拠セキュリティー・タグだけがサーバーによってエクスポートされるのかどうかを指定します。値 1 は、CORBA 準拠タグだけがエクスポートされることを意味します。値 0 (デフォルト値) は、CORBA 準拠タグと非準拠タグがエクスポートされることを意味します。

サーバーがセキュリティーに SSL 基本認証だけを使用し、クライアント (CICS またはその他の OEM ORB) が CORBA 準拠タグを使用するときは、値 1 を使用します。これは、サーバーが SSL 基本認証を使用する場合に限ってのことです。サーバーが SSL クライアント証明書もサポートしている場合は、この変数を設定する必要はありません。

サーバーが SSL 基本認証を使用し、分散プラットフォームまたは WebSphere Application Server エンタープライズ版 for OS/390 V3.02 上の WebSphere クライアントと相互協調処理を行う場合は、値 0 (またはデフォルト値) を使用します。

例: `IBM_OMGSSL=1`

HOME=*path*

ホーム・ディレクトリーを指定します。この変数は、ユーザーが UNIX シェルにログインすると、セキュリティー製品のユーザー・プロファイルか

ら自動的に設定されます。OS/390 または z/OS 上で稼働している C++ または Java クライアントの場合は、IBM 分散デバッガーでビジネス・オブジェクトをデバッグする際に、この変数を /tmp に設定します。

例: HOME=/tmp

ICU_DATA=*path*

XML パーサーが必要とするバイナリー・ファイルへのパスで、この XML パーサーは、ブートストラップおよびインポート・サーバー処理の間にシステム管理サーバーによって使用されます。WebSphere for z/OS コードをデフォルト・ディレクトリーにインストールした場合は、このパスを変更する必要はありません。デフォルトのパスは /usr/lpp/WebSphere/bin/ です。

例: ICU_DATA=/usr/lpp/WebSphere/bin/

IR_GENERIC_SERVER_NAME=*SERVER_NAME*

インターフェース・リポジトリー・サーバーのサーバー名です。デフォルトは CBINTFRP です。インターフェース・リポジトリー・サーバーのサーバー領域が動作するためには、この名前を使用してワークロード管理 (WLM) アプリケーション環境を定義しなければなりません。

IR_SPECIFIC_SERVER_NAME=*SERVER_INSTANCE_NAME*

インターフェース・リポジトリー・サーバーのサーバー・インスタンス名です。デフォルトは INTFRP01 です。この環境変数は、シスプレックス内の 2 番目以降のシステムにあるすべてのサーバー・インスタンスについて指定する必要があります。

IRPROC=*PROC_NAME*

デーモン・サーバーが使用する、インターフェース・リポジトリー・サーバーを開始するための開始プロシージャーです。デフォルトは BBOIR です。独自の開始プロシージャーの名前を提供することができます。その場合、デフォルトの開始プロシージャーからの情報を新しい開始プロシージャーにコピーしてください。

例: IRPROC=BBOIR

IVB_DEBUG_ENABLED=1

この OS/390 または z/OS クライアントがオブジェクト・レベル・トレースのランタイムをロードして、オブジェクト・レベル・トレースを使用することを指定します。値 1 は、IBM 分散デバッガーでビジネス・オブジェクトをデバッグする際に、アプリケーション・サーバーと、OS/390 または z/OS 上で稼働している C++ クライアントおよび Java クライアントの両方に必須です。

IVB_DRIVER_PATH=*path*

SMP/E インストール後に WebSphere for z/OS のファイルが常駐するディレクトリーの名前です。デフォルトは /usr/lpp/WebSphere です。

例: IVB_DRIVER_PATH=/usr/lpp/WebSphere

IVB_HOME=*path*

IBM 分散デバッガーがアプリケーション・ソース・コードを検出できる位置を指定します。この環境変数は、オプションです。

JAVA_COMPILER=

Just-In-JIT (Time) コンパイラーの使用を指定します。

この環境変数を使用する場合、ヌル値を指定 (JAVA_COMPILER=) すると、JIT コンパイラーがオンになります。これ以外の値を指定すると、JIT コンパイラーがオフになります。

デフォルトでは、OS/390 または z/OS 上で稼働している Java 仮想マシン (JVM) は、JIT コンパイラーを使用します。そのため、この環境変数を明示的に設定する必要はありません。ただし、Java ビジネス・オブジェクトをデバッグしている場合は、ヌル以外の値を指定して JIT コンパイラーをオフにしてください。

例: JAVA_COMPILER=

JAVA_IEEE754=EMULATION

OS/390 または z/OS 上の Java クライアントを実行する Java 仮想マシン (JVM) 用にシステムがロードする正しい実行可能コードを指定します。この環境変数の設定は、OS/390 または z/OS 上で実行される Java クライアントに対してのみ必須です。

java.naming.factory.initial=*context*

クライアントが使用する初期ネーミング・ファクトリー・コンテキストです。デフォルト値は
com.ibm.ws.naming.ldap.WsnLdapInitialContextFactory です。
例:

```
java.naming.factory.initial=com.ibm.ws.naming.ldap.WsnLdapInitialContextFactory
```

java.naming.security.credentials=*password*

java.naming.security.principal によって指定された識別名が使用するパスワードです。このパスワードは、システムの初期カスタマイズのときに LDAP 初期設定ファイルによって管理者アクセス ID (デフォルトは WASAdmin) 用に定義されたパスワードに一致しなければなりません。IBM では、

bboldif.cb というサンプル LDIF ファイルの中で WASAdmin アクセス ID を提供しています。デフォルト値は secret です。

例:

```
java.naming.security.credentials=secret
```

推奨: IBM 提供のパスワードを変更してください。

java.naming.security.principal=*distinguished_name*

WsnName ディレクトリーへの書き込みアクセス権を持つよう定義された識別名 (ユーザー ID) です。これを指定するのは、すべての JNDI ユーザーに読み取り / 書き込みアクセスを提供したい場合だけにしてください。この識別名は、システムの初期カスタマイズのときに LDAP LDIF ファイルによって管理者アクセス ID (デフォルトは WASAdmin) 用に定義されたものに一致しなければなりません。IBM では、bboldif.cb というサンプル LDAP 初期設定ファイルの中で WASAdmin アクセス ID を提供しています。デフォルト値は cn=WASAdmin,o=WASNaming,c=us です。

例:

```
java.naming.security.principal=cn=WASAdmin,o=WASNaming,c=us
```

推奨: WASAdmin アクセス ID を保持しておくことをお勧めします。

JVM_DEBUG=1

Java オブジェクトの OLT デバッグ設定をオン / オフにします。値 1 は、IBM 分散デバッガーで Java オブジェクトをデバッグする際に、アプリケーション・サーバーと、OS/390 または z/OS 上で稼働している Java クライアントで必須です。

この変数は、デバッグを行うために JVM メッセージを SYSOUT へ転送する場合にも必要です。JVM_DEBUG=1 を設定して、JVM メッセージングを起動します。

JVM_HEAPSIZE=*n*

JVM ヒープの最大サイズ (メガバイト単位) を設定します。デフォルトは 256 MB です。

例: JVM_HEAPSIZE=256 # specifies a 256 MB heap

JVM_LOGFILE=*filename*

JVM からのメッセージを記録する HFS ファイルを指定します。

推奨: この変数は、単一サーバー環境でのみ使用してください。複数サーバー環境で JVM_LOGFILE を使用すると、すべてのサーバーが同じファイルに書き込む結果、このファイルを診断目的に使用するのが困難になる場合

があります。複数サーバー環境では、JVM_DEBUG=1 を使用して、JVM メッセージを特定のサーバーの SYSOUT へ送信してください。

LDAPBINDPW=*password*
ネーミング・サーバーが LDAP サーバーにバインドするために使用するパスワードです。LDAPNAME に関連して使用されます。

LDAPCONF=*filename*
WebSphere for z/OS が使用する LDAP 構成ファイルです。HFS 内のファイルを指定する場合は、引用符を使用しないでください。MVS データ・セットを指定する場合は、そのデータ・セットを単一引用符で囲んでください。

例: `LDAPCONF='bbo.s21slapd.conf'`

LDAPHOSTNAME=*name:port*
インターフェース・リポジトリー・サーバーがデータ・ストアとして使用する LDAP サーバーのホスト名です。

LDAPIRBINDPW=*password*
インターフェース・リポジトリー・サーバーが LDAP サーバーにバインドする場合に使用するパスワードです。LDAPIRNAME に関連して使用されます。

LDAPIRCONF=*filename*
インターフェース・リポジトリー・サーバーがデータ・ストアとして使用する LDAP サーバーが使用する LDAP 構成ファイルです。HFS 内のファイルを指定する場合は、引用符を使用しないでください。MVS データ・セットを指定する場合は、そのデータ・セットを単一引用符で囲んでください。

LDAPIRHOSTNAME=*name:port*
インターフェース・リポジトリー・サーバーがデータ・ストアとして使用する LDAP サーバーのホスト名です。

LDAPIRNAME
インターフェース・リポジトリー・サーバーがデータ・ストアとして使用する LDAP サーバーに対して自分自身を認証する場合に使用する LDAP の入り口名です。

LDAPIRROOT=*root*
インターフェース・リポジトリー・サーバーがデータをアンカーする LDAP の入り口名です。

例: `LDAPIRROOT=o=BOSS,c=U`

LDAPNAME
ネーミング・サーバーがデータ・ストアとして使用する LDAP サーバーに対して自分自身を認証する場合に使用する LDAP の入り口名です。

LDAPROOT=*root*
ネーミング・サーバーがデータをアンカーする LDAP の入り口名です。

例: `LDAPROOT=o=BOSS,c=US`

LIBPATH=*path1*:*[path2]*:...
階層ファイル・システム (HFS) 内の Java の DLL 検索パスを指定します。システム、WebSphere for z/OS、および Java DLL を指定します。

例:

```
LIBPATH=/db2_install_path/lib:/usr/lpp/java/J1.3/bin:/usr/lpp/java/J1.3/bin/classic:/usr/lpp/WebSphere/lib
```

ここで、*db2_install_path* は DB2 for OS/390 をインストールした HFS です。

LOGSTREAMNAME=*LOG_STREAM_NAME*
デーモンおよびシステム管理サーバーがブートストラップ中に使用する WebSphere for z/OS エラー・ログ・ストリーム名です。ブートストラップ中にデーモンおよびシステム管理サーバーの環境ファイルを指定しない場合は、システムは以下のアルゴリズムを使用して、エラー・ログ・ストリーム名を形成します。

1. デーモン・サーバーの IP 名内の最初の修飾子を取得する。
2. 最初の修飾子が 8 文字以上の場合は、その修飾子を 8 文字の文字ストリングに分割して、ピリオドで区切る。
3. 上位修飾子「BBO」を追加する。

たとえば、デーモン IP 名が MYDAEMONSERVER.IBM.COM の場合、アルゴリズムは、エラー・ログ・ストリーム名 BBO.MYDAEMON.SERVER を生成します。

ブートストラップ後、管理アプリケーションを介して、シスプレックス全体、サーバー、またはサーバー・インスタンスのエラー・ログ・ストリーム名を作成または変更することができます。サーバー・エラー・ログ・ストリームを設定すると、WebSphere for z/OS の一般設定が上書きされます。またサーバー・インスタンスの設定は、サーバーの設定を上書きします。したがって、通常のエラー・ロギングをセットアップすることはできますが、サーバーまたはサーバー・インスタンスのエラー・ロギングを特定のログ・ストリームに送信することはできません。

処理中に、指定したログ・ストリームが検出されない、またはそれにアクセスできない場合は、メッセージが発行され、エラーがサーバーのジョブ・ログに書き込まれます。

例: LOGSTREAMNAME=MY.CB.ERROR.LOG

ヒント: ログ・ストリーム名を引用符で囲まないでください。ログ・ストリーム名は、データ・セット名ではありません。

MIN_SRS=*nn*

初期化した後に稼働したままで保持するサーバー領域の数です。つまり、ワークロード管理はサーバー領域が活動停止中になった場合でも、そのサーバー領域にシャットダウンするように指示しません。この環境変数を使用するのは、ワークロードに対する応答時間を早くするために、いくつかのサーバー領域がいつでも作業を処理できるようにしておく必要がある場合です。

J2EE サーバーのデフォルトは 1 です。MOFW サーバーの場合、デフォルトは 0 です。最大値は 20 です。20 を超える値を指定した場合、この変数は 20 に設定されます。

WebSphere for z/OS のガーベッジ・コレクションによってサーバー領域がリフレッシュされる場合がありますが、サーバー領域の最小数がこの環境変数で指定した値以下になることはありません。

例: MIN_SRS=2

NM_GENERIC_SERVER_NAME=*SERVER_NAME*

ネーミング・サーバーのサーバー名です。デフォルトは CBNAMING です。ネーミング・サーバーのサーバー領域が動作するためには、この名前を使用してワークロード管理 (WLM) アプリケーション環境を定義しなければなりません。

例: NM_GENERIC_SERVER_NAME=CBNAMING

NM_SPECIFIC_SERVER_NAME=*SERVER_INSTANCE_NAME*

ネーミング・サーバーのサーバー・インスタンス名です。デフォルトは NAMING01 です。この環境変数は、シスプレックス内の 2 番目以降のシステムにあるすべてのサーバー・インスタンスについて指定する必要があります。

例: NM_SPECIFIC_SERVER_NAME=NAMING01

NMPROC=*PROC_NAME*

デーモン・サーバーが使用する、ネーミング・サーバーを開始するための開始プロシージャーです。デフォルトは BBONM です。独自の開始プロシ

ージャーの名前を提供することができます。その場合、デフォルトの開始プロシージャーからの情報を新しい開始プロシージャーにコピーしてください。

例: NMPROC=BBONM

OTS_DEFAULT_TIMEOUT=*n*

アプリケーション・トランザクションにデフォルトで指定されている完了までの時間の合計 (秒単位) です。この時間の合計は、current → set_timeout メソッドを通して独自のタイムアウト値を設定しない場合には、アプリケーション・トランザクションに指定されます。

デフォルトは 30 秒で、最大値は 2147483 秒 (24.85 日) です。ヌルまたは 0 値は使用しないでください。

注: 会話が活動化された時点で、システムはシステム管理サーバー・インスタンス**でのみ**特殊処理を行います。

- OTS_DEFAULT_TIMEOUT 変数が設定されていない場合は、それが追加されます。
- OTS_DEFAULT_TIMEOUT の値が 3600 (秒) 未満の場合は、3600 に設定されます。

この特殊処理はシステム管理サーバー・インスタンス用に行われます。これらのサーバー・インスタンスは、長時間を要するトランザクションを実行する場合があるからです。その他のサーバー・インスタンスでは、このように長いトランザクションのデフォルトは必要ありません。

例: OTS_DEFAULT_TIMEOUT=30

OTS_MAXIMUM_TIMEOUT=*n*

アプリケーション・トランザクションに指定されている完了までの最大許容時間の合計 (秒単位) です。アプリケーションが、より大きな合計時間を割り当てると、システムは、その時間を OTS_MAXIMUM_TIMEOUT 値に制限します。

デフォルトは 60 秒で、最大値は 2147483 秒 (24.85 日) です。ヌルまたは 0 値は使用しないでください。

注: 会話が活動化された時点で、システムはシステム管理サーバー・インスタンス**でのみ**特殊処理を行います。

- OTS_MAXIMUM_TIMEOUT 変数が設定されていない場合は、それが追加されます。

- OTS_MAXIMUM_TIMEOUT の値が 3600 (秒) 未満の場合は、3600 に設定されます。

この特殊処理はシステム管理サーバー・インスタンス用に行われます。これらのサーバー・インスタンスは、長時間を要するトランザクションを実行する場合があるからです。その他のサーバー・インスタンスでは、このように長いトランザクションのデフォルトは必要ありません。

例: `OTS_MAXIMUM_TIMEOUT=60`

PATH=*path*

パスを指定します。OS/390 または z/OS 上の Java をトレースおよびデバッグしている場合、アプリケーション・サーバーのみに関して、irmtdbgj と呼ばれる実行可能ファイルへのパスを組み込みます。

RAS_MINORCODEDEFAULT=*value*

システム例外マイナー・コードについての文書を収集するデフォルトの動作を決定します。IBM サービス技術員の指示に従って使用してください。

CEEDUMP

コールバックおよびオフセットを取り込みます。

ヒント: システムが CEEDUMP を取るには時間がかかるので、トランザクション・タイムアウトが発生する場合があります。たとえば、OTS_DEFAULT_TIMEOUT が 30 秒に設定されていても、CEEDUMP を取るのに 30 秒以上かかる場合があるため、アプリケーション・トランザクションはタイムアウトになります。この発生を防ぐには、以下のいずれかを行います。

- トランザクションのタイムアウト値を増加する。
- RAS_MINORCODEDEFAULT=NODIAGNOSTICDATA をコード化する。TRACEMINORCODE が、環境ファイル内に**ない**ことを確認してください。

TRACEBACK

言語環境プログラムおよび OS/390 UNIX トレースバック・データを取り込みます。

SVCDUMP

MVS ダンプを取り込みます (ただし、クライアント内でのダンプの作成は行いません)。

NODIAGNOSTICDATA

デフォルトです。CEEDUMP、TRACEBACK、または SVCDUMP の収集は発生しません。

注: もう 1 つ別の環境変数 TRACEMINORCODE の設定によって、結果が変化することがあります。TRACEMINORCODE=(ヌル値) および RAS_MINORCODEFAULT=TRACEBACK をコード化すると、トレースバックを取得します。しかし、RAS_MINORCODEDEFAULT=NODIAGNOSTICDATA および TRACEMINORCODE=ALL をコード化しても、トレースバックを取得します。したがって、RAS_MINORCODEDEFAULT=NODIAGNOSTICDATA を指定しても TRACEBACK はキャンセルされません。単に TRACEBACK が収集されないようにするだけです。

REM_DCEPASSWORD=*password*

OS/390 または z/OS クライアントがシスプレックス外のシステムへ要求を出し、SSL タイプ 1 認証が使用されている場合の、セキュリティー・コンテキスト内に渡されたリモート DCE プリンシパルのパスワードです。このパスワードは、DCE パスワード要件に準拠していなければなりません。

例: `REM_DCEPASSWORD=mydcePW`

REM_DCEPRINCIPAL=*principal*

クライアントがシスプレックス外のシステムへ要求を出し、SSL タイプ 1 認証が使用されている場合の、セキュリティー・コンテキスト内に渡されたプリンシパルです。このプリンシパルは、ターゲット・サーバー上で定義されなければなりません。この値は、DCE プリンシパル要件に準拠していなければなりません。

例: `REM_DCEPRINCIPAL=myDCEprin`

REM_PASSWORD=*password*

クライアントがリモート OS/390 または z/OS システムに要求を出し、ユーザー ID / パスワードのセキュリティーまたは SSL セキュリティーが使用されている場合の、セキュリティー・コンテキスト内で使用されるパスワードです。

例: `REM_PASSWORD=MYPASSW`

REM_USERID=*USER_ID*

クライアントがリモート OS/390 または z/OS システムに要求を出し、ユーザー ID / パスワードのセキュリティーまたは SSL セキュリティーが使用されている場合の、セキュリティー・コンテキスト内で使用されるユーザー ID です。

例: `REM_USERID=MCOX`

RESOLVE_IPNAME=*IP_NAME*

システム管理サーバーがドメイン・ネーム・サービス (DNS) で登録するインターネット・プロトコル名です。CORBA クライアントの WebSphere for z/OS との通信は、いずれも、この IP 名を必要とします。解決 IP 名が設定されていない場合、この IP 名は、プログラムが稼働しているシステムとなります。

規則: RESOLVE_IPNAME の値は、完全修飾名にする必要がありますが、255 文字を超過することはできません。

例: `RESOLVE_IPNAME=CBQ091.COMPANY.NY.COM`

RESOLVE_PORT=*n*

システム管理サーバーが要求を listen するポート番号です。デフォルトは 900 です。このポートは、オブジェクト・リクエスト・ブローカーのシステムに認識されているポートのため、IBM は、この変数を変更しないようお勧めします。すでにこのポートを使用しているアプリケーションがある場合は、TCP/IP バインド専用のサポートおよび SRVIPADDR 環境変数の使用を検討してください。

例: `RESOLVE_PORT=900`

SM_DEFAULT_ADMIN=*USER_ID*

管理アプリケーションおよび操作アプリケーションを使用する管理者のユーザー ID です。この環境変数は、インストール中にシステム管理ブートストラップが使用します。システム管理ブートストラップの実行後にこの環境変数を設定しても、効果はありません。この環境変数を定義しない場合、デフォルトのユーザー ID は CBADMIN です。このユーザー ID は、OS/390 または z/OS に定義し、適切なセキュリティー許可 (たとえば、RACF 許可や LDAP 許可) を与えなければなりません。

注: システム管理ブートストラップの実行後は、管理アプリケーションを介さなければ、追加の管理者ユーザー ID を定義することはできません。これらのユーザー ID は、SM_DEFAULT_ADMIN で定義されたユーザー ID と置き換えることはできません。

例: `SM_DEFAULT_ADMIN=DUDE`

SM_GENERIC_SERVER_NAME=*SERVER_NAME*

システム管理サーバーのサーバー名です。デフォルトは CBSYSMGT です。システム管理サーバーのサーバー領域が動作するためには、この名前を使用してワークロード管理 (WLM) アプリケーション環境を定義しなければなりません。

例: `SM_GENERIC_SERVER_NAME=CBSYSMGT`

SM_SPECIFIC_SERVER_NAME=*SERVER_INSTANCE_NAME*

システム管理サーバーのサーバー・インスタンス名です。デフォルトは SYSMGT01 です。この環境変数は、シスプレックス内の 2 番目以降のシステムにあるすべてのサーバー・インスタンスについて指定する必要があります。

例: `SM_SPECIFIC_SERVER_NAME=SYSMGT01`

SMPROC=*PROC_NAME*

デーモン・サーバーが使用する、システム管理サーバーを開始するための開始プロシージャーです。デフォルトは BBOSMS です。独自の開始プロシージャーの名前を提供することができます。その場合、デフォルトの開始プロシージャーからの情報を新しい開始プロシージャーにコピーしてください。

例: `SMPROC=BBOSMS`

SOMOOSQL=*value*

オブジェクト指向の SQL 照会を使用するクライアント・アプリケーションのストリング属性に関するパフォーマンスを向上します。SOMOOSQL=1 を使用することによって、ストリング比較はデータベースへプッシュダウンされます。

デフォルト値は (SOMOOSQL=) です。

規則: SOMOOSQL=1 は、データベースおよびサーバー領域のアドレス・スペースが同一のロケール内で稼働すると宣言されている場合にのみ使用することができます。

SRVIPADDR=*IP_ADDRESS*

WebSphere for z/OS サーバーがクライアント接続要求を listen するために使用する、ドット 10 進数形式の IP アドレスです。

この IP アドレスは、TCP/IP へバインドする場合にサーバーが使用します。通常、サーバーは、ローカル TCP/IP スタックに対して構成されたすべての IP アドレスを listen します。ただし、作業を分離したい場合、または複数の異機種のサーバーが同一のポートを listen できるようにしたい場合は、SRVIPADDR を使用することができます。指定した IP アドレスは、WebSphere for z/OS がインバウンド要求を受信する唯一の IP アドレスになります。また、通常、デーモン IP 名、解決 IP 名、または使用しているサーバーのホスト名をこの特定の SRVIPADDR にマップする必要があります。

SSL_KEYRING=*keyring*

OS/390 または z/OS クライアントの、SSL 処理内で使用される鍵リングの名前です。この鍵リングは、RACF 内に常駐しなければなりません。

例: `SSL_KEYRING=IVPRING`

SYS_DB2_SUB_SYSTEM_NAME=*NAME*

データベースに接続する場合にデーモンおよびシステム管理サーバーが使用する DB2 for OS/390 名です。DB2 for OS/390 サブシステム名またはグループ接続名のどちらかを使用します。デフォルトは DB2 です。このデフォルトが、ユーザーのインストールにおいて正しくない場合は、正しい値と一致するよう環境変数を変更します。

例: `SYS_DB2_SUB_SYSTEM_NAME=DB21`

TRACEALL=*n*

WebSphere for z/OS のデフォルト・トレース・レベルを指定します。有効値およびその意味は、以下のとおりです。

0 トレースなし。

1 例外トレース (デフォルト)。

2 基本および例外トレース。

3 詳細トレース (基本および例外トレースを含む)。

この変数を TRACEBASIC および TRACEDETAIL 環境変数に関連して使用し、WebSphere for z/OS サブコンポーネントのトレース・レベルを設定します。IBM サービス技術員の指示なしに、この変数を変更しないでください。

例: `TRACEALL=1`

TRACEBASIC=*n* **|** **(***n***,...)**

特定の WebSphere for z/OS サブコンポーネント用にオーバーライドするトレースを指定します。番号で指定されたサブコンポーネントは、基本および例外トレースを受信します。複数のサブコンポーネントを指定する場合は、括弧を使用し、コンマで番号を区切ります。サブコンポーネントの番号およびその意味については、IBM サービスに問い合わせてください。WebSphere for z/OS の他の部分は、TRACEALL 環境変数上で指定されたとおりにトレースを受信します。IBM サービス技術員の指示なしに、TRACEBASIC を変更しないでください。

例: `TRACEBASIC=3`

TRACEBUFFCOUNT=*n*

割り振るトレース・バッファーを指定します。有効な値は、4 ～ 8 です。デフォルトは 4 です。

TRACEBUFFLOC=SYSPRINT | BUFFER

トレース・レコードの出力先を指定します。sysprint (SYSPRINT) か、または メモリー・バッファー (BUFFER) のいずれかに書き込まれ、その後 CTRACE データ・セットに書き込まれます。デフォルトでは、クライアントの場合は sysprint へ、他のすべての WebSphere for z/OS プロセスの場合はバッファーへ、トレース・レコードが書き込まれます。サーバーの場合は、1 つの値を指定するか、あるいは、両方の値をスペースで区切って指定することができます。クライアントの場合は、TRACEBUFFLOC=SYSPRINT のみ、指定することができます。

例: `TRACEBUFFLOC=SYSPRINT BUFFER`

TRACEBUFFSIZE=*n*

単一トレース・バッファーのサイズをバイト単位で指定します。文字の「K」(キロバイト) または「M」(メガバイト) を使用することができます。有効値は 128K ～ 4M までです。デフォルトは 1M です。

TRACEDETAIL=*n* **| (***n***,...)**

特定の WebSphere for z/OS サブコンポーネント用にオーバーライドするトレースを指定します。番号で指定されたサブコンポーネントが、詳細トレースを受信します。複数のサブコンポーネントを指定する場合は、括弧を使用し、コンマで番号を区切ります。サブコンポーネントの番号およびその意味については、IBM サービスに問い合わせてください。WebSphere for z/OS の他の部分は、TRACEALL 環境変数上で指定されたとおりにトレースを受信します。IBM サービス技術員の指示なしに、TRACEDETAIL を変更しないでください。

例:

```
TRACEDETAIL=3
TRACEDETAIL=(3,4)
```

TRACEMINORCODE=*value*

システム例外マイナー・コードのトレースバックを使用可能にします。IBM サービスの指示がある場合のみ使用します。値は、以下のとおりです。

ALL|all

すべてのシステム例外マイナー・コードのトレースバックを使用可能にします。

minor_code
特定のマイナー・コードのトレースバックを使用可能にします。X'C9C21234' などの 16 進数でコードを指定します。

(ヌル値)
デフォルトです。トレースバックの収集は発生しません。

注: もう 1 つ別の環境変数 RAS_MINORCODEDEFAULT の設定によって、結果が変化することがあります。TRACEMINORCODE=ALL および RAS_MINORCODEDEFAULT=NODIAGNOSTICDATA をコード化すると、トレースバックを取得します。しかし、TRACEMINORCODE=(ヌル値) および RAS_MINORCODEFAULT=TRACEBACK をコード化しても、トレースバックを取得します。したがって、TRACEMINORCODE=(ヌル値) を指定しても TRACEBACK はキャンセルされません。単に TRACEBACK が収集されないようにするだけです。

TRACEPARM=*SUFFIX* | *MEMBER_NAME*
CTRACE PARMLIB メンバーを識別します。この値は、ストリング CTIBBO に追加されて PARMLIB メンバーの名前を形成する 2 文字の接尾部か、または PARMLIB メンバーの完全指定名のいずれかです。たとえば、システムが「CTIBBO01」に対して解決する、接尾部「01」を使用することができます。完全指定名は、CTRACE PARMLIB メンバーの命名要件に準拠していなければなりません。詳細は、*z/OS MVS 診断: ツールと保守援助プログラム*, GA88-8561 を参照してください。

デフォルト値は 00 です。

この環境変数が指定されており、PARMLIB メンバーが検出されない場合は、デフォルトの PARMLIB メンバー、CTIBBO00 が使用されています。指定された PARMLIB メンバーも、デフォルトの PARMLIB メンバーも、どちらも検出されない場合は、トレースは CTRACE に定義されていますが、CTRACE 外部書き出しプログラムへ接続されません。PARMLIB メンバーの詳細および CTRACE 外部書き出しプログラムの使用については、*WebSphere Application Server V4.0 for z/OS and OS/390: メッセージおよび診断*, GA88-8655 を参照してください。

デーモン・サーバーは、この環境変数を認識する唯一のサーバーなので、注意してください。

例: `TRACEPARM=01`

付録B. ネーム・スペースの構成

システムのインストールおよび構成の間に、専用のネーミング構成ファイルを使用してネーム・スペースを構成します。このファイルは、ネーミング・クライアント開始プロシージャー (BBONMC) 内の NCONFIG DD ステートメント上で指定されています。IBM は、SBBOEXEC(BBOCNFG) と呼ばれるサンプルのネーミング構成ファイルを提供しています。ユーザーはこれを変更することができます。このトピックでは、ネーミング構成ファイル用の構文について説明しています。

ネーミング構成ファイルには、以下の情報が入っています。

- 現在存在しているドメイン間ルート (IDR) の位置、またはドメイン間ルートをローカルに作成するよう指示を出しているインディケーター。
- IDR へバインドされるセルを含むホストの名前およびこれらのセルの名前。これによって、すでに構成されている可能性があり、IDR 下で見えるようになっているはずのセル・ネーム・スペース・セグメントを格納している、WebSphere for z/OS ではないホストが識別されます。WebSphere for z/OS は、指定されたホストのローカル・ルート・ネーミング・コンテキストからその 1 次親セルまで横断し、提供された名前を使用して、そのセルをバインドします。
- この WebSphere for z/OS ホスト上に作成されるセルの名前。
- IDR に関連する 1 次および代替セルの名前に加えて、この WebSphere for z/OS ホスト上に作成されるワークグループの名前。
- このホスト上に作成される単一ローカル内のホスト・セグメントの名前。ローカルの 1 次および代替の親ワークグループおよびセルの名前も、IDR と関連して提供されます。

注: 現在、OS/390 または z/OS LDAP は、識別名のサイズとして最高 1000 文字までサポートしています。オブジェクトの名前またはバインドしているコンテキストがこの限界を超えた場合、システムは InvalidName 例外を発行します。指定したものが 1000 バイトよりもかなり短い場合でも、この例外が発生することがあります。これは、名前が著しく長い内部 LDAP 名上にマップされていることが理由です。たとえば、以下のように指定するとします。

```
a/b/c
```

LDAP は、以下の識別名を作成します。

```
TypelessRDN=c,TypelessRDN=b,TypelessRDN=a,TypelessRDN=/,o=BOSS,c=US
TypelessRDN=c,TypelessRDN=b,TypelessRDN=a,TypelessRDN=/,o=WASNaming,c=US
```

ネーミング構成ファイルの構文は、以下のようなスタンザを使用します。

```
[NamingIDR]                       // Cells that currently exist on other
                                  // machines that should be bound under
                                  // the WebSphere for z/OS IDR.

IDRLocation=host:port             // Specifies the location of a remote host
                                  // where the IDR lives or 'local' if we
                                  // create one here.

RemoteHost1=host:port             // Remote host where a cell lives

RemoteCell1=cell                  // Name of that remote cell when bound
                                  // under IDR.

RemoteMemberHost1.1=host:port     // Bind remote host belonging to RemoteCell1
                                  // into the NameSpace
RemoteHost2=host:port

RemoteCell2=cell

⋮


[Cells]                           // Names of new cells to create on this
                                  // machine and bind to IDR.

Cell1=cell
Cell2=cell

⋮


[Workgroups]                      // Names of new workgroups to create on this
                                  // machine and the name of the cells to
                                  // bind them to.

WorkGroup1=workgroup              // Name for this new workgroup.
PrimaryCell1=cell                 // Primary cell bound to this workgroup.
AlternateCell1.1=cell             // Alternate cell bound to this workgroup.

Workgroup2=workgroup
PrimaryCell1=cell
AlternateCell1.1=cell
AlternateCell1.2=cell

⋮


[Hosts]                           // Locals to create on this machine
```

```
                                    // identified by their host name.  Also
                                    // specifies the name of the workgroup
                                    // and cells to bind the host under.

Host1=host|&DAEMON_IPNAME.          // Either the host name or variable for
                                    // the Daemon IP Name

PrimaryCell1=cell
AlternateCell1=cell
PrimaryWorkgroup1=workgroup
AlternateWorkgroup1.1=workgroup
```

最初のスタンザ NamingIDR は、ネーミング構成によって以前からあるセルを IDR に追加できるようにする情報を提供しています。IDR は、WebSphere for z/OS 上でのみサポートされています。したがって、Component Broker for Windows NT 上で作成されたセルは、IDR から見えるようにする場合には、この方法で指定しなければなりません。

NamingIDR スタンザ内の IDR 位置変数は、IDR をローカルに構築するか、または既存の IDR の位置を指定するよう指示します。IDR をローカルに構築する場合は、IDRLocation=local と指定します。既存の IDR を使用する場合は、ホスト名およびポートを指定します。ネーミング構成ユーティリティーは、そのホストにブートストラップし、IDR へナビゲートして、その IDR の参照を取得します。

NamingIDR スタンザ内の RemoteHostn 変数は、IDR 下で 1 次セルを見ることができるホストのホスト名およびポート番号を指定する場合に使用されます。処理中のネーミング構成は、指定したホストへブートストラップし、そのホストのローカル・ルート・ネーミング・コンテキストがセル・ネーミング・コンテキストを取得して、解決します。

複数リモート・ホストを NamingIDR スタンザ内に指定することができます。各ホストは、RemoteHostn 変数上の接尾辞修飾子 *n* によって識別されます。使用される修飾子は、1 から始まり、指定された複数リモート・ホストに順に番号付けされる必要があります。RemoteCelln 変数は、対応するリモート・セルの IDR に関連する名前を提供します。

RemoteMemberHost*n.n* は、RemoteCell に属するリモート・ホストを NameSpace にバインドします。ホストから IDR へのリンクが作成されます (つまり、グローバル IDR コンテキストが "..." という名の下でホストのルート・コンテキストにバインドされ、これによって、ユーザーは、自分のローカル・ホストから直接 IDR 内へナビゲートできるようになり、したがって、統合されたネーム・スペース内へのナビゲートが可能になります)。処理中のセルに属するホストごとに、RemoteMemberHost ステートメントがなければなりません。

Cells スタンザは、このホスト上に作成される新規のセルの IDR に関連する名前を指定します。Celln 変数は、前に説明したような後置表記法を使用して名前を指定します。

Workgroups スタンザは、WorkGroupn 変数を経由してこのホスト上に作成する新規のワークグループの名前を指定します。各新規のワークグループをバインドする 1 次および代替セルも指定しなければなりません。単一の 1 次セルは、*n* によってワークグループの接尾辞を識別される PrimaryCelln 上に指定されます。複数代替セルは、*n* によってワークグループの接尾辞が識別される AlternateCellnz を経由して指定されます。また *z* は、ネーム・スペース構造がワークグループ・スタンザの場合の代替セルです。ただし、新規のワークグループは、その組み立てが正常であると認められるためには、1 次セルと正常にバインドされなければなりません。

Hosts スタンザは、現行システム上のローカル・ネーム・スペース・セグメントの作成の指針に使用されます。単一のローカル・ネーム・スペース・セグメントは、WebSphere for z/OS の現行リリースでは、システムごとに構築されなければなりません。ただし、今後のリリースでは、複数ローカル・セグメントが可能になるかもしれません。新規のローカル・ネーム・スペース・セグメントのホスト部分の名前は、Host*n* 変数を介して指定されます。ここで、現行リリースでは、*n* は 1 でなければなりません (ファイル内により多くのホスト仕様を入れることは可能ですが、それらは単に無視されます)。1 次および代替セルおよびワークグループの名前も、指定しなければなりません。

Host*n* の代わりに、変数 &DAEMON_IPNAME を使用します。変数名は、大文字でなければならず、また、ピリオドで終わらなければなりません。統合されたネーム・スペースをセットアップしている場合、オプションが関係してきます。この場合、関係しているシステムのホスト名は、異なるものでなければなりません。この変数を使用すると、ユーザーは、シスプレックスを通って移動している際に、ファイルを変更せずにファイル内のローカル・ホスト名を変更することが可能になります。

ローカル・ネーム・スペース・セグメントの場合、1 次と代替にはネーム・スペース構造に関して区別があります。1 次セルおよび 1 次ワークグループは、セルおよびワークグループをそれぞれ経由して、ローカル・ルート・ネーム・コンテキストに相対して解決することができます。1 次セルおよびワークグループは、ホストに対して解決することもできます。代替ワークグループおよびセルは、ホストに対するポインターも含んでいます。ホストが代替セルおよびワークグループを指す直接ポインターを含んでいないことで区別します。

ホスト用の 1 次および代替セルは、Workgroup スタンザと同じ方法で、PrimaryCelln および AlternateCellnz 変数上で指定します。1 次および代替ワークグループの名前は、PrimaryWorkgroupn および AlternateWorkgroupnz 変数上の IDR に相対して指定されます。

WebSphere for z/OS の現行リリースでは、異なるネーミング構成ファイルを使用してネーミング構成ユーティリティーを複数回実行し、追加のネーム・スペース・セグメントを構築することが可能です。追加の代替セグメントを追加することもできます。たとえば、ワークグループを追加の代替セルを指すようにすることができます。ただし、ネーム・スペース・セグメントを削除したり、それらの 1 次親を変更することはできません。

ネーミング構成ユーティリティーを続けて実行して、追加のセグメントを構築する場合は、単に既存の構成ファイルを更新しても構いません。既存のセグメントは、いずれも、情報メッセージでフラグが立てられます。

シナリオ

これらのシナリオは、いくつかの可能な構成を示しています。

シナリオ 1

単一のローカル・ワークグループおよびセルを WebSphere for z/OS 上に構築します。1 つまたは複数の Component Broker for Windows NT ホストは、WebSphere for z/OS のネーム・スペース内に代替としてバインドされるローカルを構築します。Component Broker for Windows NT では、1 次ワークグループおよびセルは、Component Broker for Windows NT マシン上になければなりません。WebSphere for z/OS を代替としてバインドすることができます。ステップは、以下のとおりです。

1. アクティビティーは、WebSphere for z/OS で開始しなければなりません。WebSphere for z/OS 構成ファイルが作成されます。NamingIDR スタンザは、この場合、空です。残りのスタンザは、WebSphere for z/OS 内に構築されるネーム・スペースを記述します。WebSphere for z/OS は最初に構成されるホストなので、構築されるネーム・スペース・セグメントの親も、また、この WebSphere for z/OS ホスト上に常駐しなければなりません。さまざまなセグメント間のすべての接続は、必要に応じて追加されます。
2. Component Broker for Windows NT は、ネーム・スペース・セグメント間のリンクの必須の代替メンバーの追加を可能にする管理インターフェースを使用します。管理者は、以下のリンクを定義する必要があります。
   a. ローカルからワークグループへのリンク

b. ローカルからセルへのリンク

c. セルからホストへのリンク

d. ワークグループからホストへのリンク

シナリオ 2

このシナリオでは、ローカル、ワークグループ、およびセルのネーム・スペース・セグメントを Component Broker for Windows NT システム上に作成します。WebSphere for z/OS ローカルが作成され、Component Broker for Windows NT ワークグループおよびセル内にバインドされます。ステップは、以下のとおりです。

1. Component Broker for Windows NT を今日完了したように構成します。
2. WebSphere for z/OS 構成ファイルを作成します。この構成ファイルは、WebSphere for z/OS IDR 下で Component Broker for Windows NT セルをバインドする NamingIDR スタンザ内に項目を持つことになります。WebSphere for z/OS 構成ファイルの Workgroups および Cells スタンザは、空になります。Hosts スタンザは、前述の例と同様に、親ワークグループおよびセルの IDR と相対する名前を指定します。

シナリオ 3

このシナリオでは、ローカル、ワークグループ、およびセル・セグメントが、Component Broker for Windows NT および WebSphere for z/OS ネーム・サーバーの両方に作成されます。ただし、後で戻って、Component Broker for Windows NT セル下に常駐する WebSphere for z/OS へ新規のワークグループを追加します。ステップは、以下のとおりです。

1. WebSphere for z/OS を開始します。417ページの『シナリオ 1』と同様に、WebSphere for z/OS ネーム・スペース・セグメントを構築します。
2. 『シナリオ 2』と同様に、Component Broker for Windows NT ネーム・スペース・セグメントを構築します。
3. 1 つのセルが、Component Broker for Windows NT ホスト上に作成されました。Component Broker for Windows NT には IDR の認識がないため、そのセルは、この段階で IDR にバインドされなければなりません。そうすることで、このセルは、今後の構成アクティビティー中に見ることができるようになります。2 番目の WebSphere for z/OS が作成されます。この構成ファイルには、IDR にバインドされる Component Broker for Windows NT セルを識別する NamingIDR スタンザのみが含まれています。ネーミング構成ユーティリティーは、この後、再び実行され、Component Broker for Windows NT セルを IDR にバインドします。

4. しばらくすると、新規のワークグループが作成され、Component Broker for Windows NT セルにバインドされます。3 番目の WebSphere for z/OS ネーミング構成ファイルが作成され、新規のワークグループの情報を識別する Workgroups スタンザのみを指定します。Component Broker for Windows NT セルは WebSphere for z/OS IDR にバインドされているため、この情報は、通常どおり指定することができます。

付録C. DCE のセットアップ

このトピックでは、WebSphere for z/OS の DCE セキュリティーの使用、このサポートのガイドラインおよび要件、OS/390 または z/OS クライアントおよびサーバー用の DCE セキュリティーのセットアップの指示について説明しています。DCE および Component Broker for Windows NT に関する情報については、*WebSphere Application Server エンタープライズ版 Component Broker システム管理の手引きバージョン 3.0* を参照してください。

WebSphere for z/OS および DCE のバックグラウンド

OS/390 または z/OS の場合、DCE セキュリティー・サーバーは、OS/390 または z/OS セキュリティー・サーバーのコンポーネントで、OS/390 または z/OS のオプション機構です。RACF は、OS/390 または z/OS セキュリティー・サーバー内の別のコンポーネントですが、必ずしもこれを DCE セキュリティー・サーバーで操作する必要はありません。DCE アカウントのプリンシパルを OS/390 または z/OS のユーザー ID に (およびその逆にも) 変換することができ、システム許可機能 (SAF) のインターフェースで操作可能であれば、ユーザーは別のセキュリティー製品を使用しても構いません。RACF について言及している場合は、DCE セキュリティー・サーバーと相互運用する別のセキュリティー製品と置き換えて構いません。

DCE を経由する場合、WebSphere for z/OS はセキュリティーの CORBA 標準をサポートします。作業要求がシステムに来る場合、またはシステムから出る場合 (つまり、作業要求がリモートの場合) は、呼び出し要求があり、かつ DCE アカウントのプリンシパルがその対応する OS/390 または z/OS のユーザー ID に (またはその逆に) マップするならば、WebSphere for z/OS は DCE セキュリティーを使用します。

DCE は、Kerberos セキュリティー・モデルの形式をインプリメントしています。この形式は、クライアントおよびサーバーの両方がセキュリティー・サーバーは信頼していますが、お互いに対しては信頼していません。セキュリティー・サーバーは、第三者オーセンティケーターとして動作します。そのため、クライアントおよびサーバーは、効果的に相互協調処理をするための信頼を確立することができます。

WebSphere for z/OS は、保護のタイプとして、次の 3 つの品質をサポートしています。無保護 (つまり、両方向 (相互) 認証)、メッセージの保全性、およ

びメッセージの機密性 (暗号化) です。壊れたメッセージおよび応答メッセージなしの場合の保護オプションの DCE の品質は、サポートされていません。基本の DCE サポートに加えて、メッセージの機密性には、DCE セキュリティー・サーバーおよび DCE 基本サービス内に Data Encryption Standard (DES) をインプリメントすることが必要となります。

OS/390 または z/OS のクライアントの保護品質は、CLIENT_DCE_QOP 環境変数を経由して使用可能にすることができます (383ページの『付録A. 環境ファイル』を参照してください)。サーバーの保護品質は、管理アプリケーションの属性を設定することによって使用可能にすることができます。

WebSphere for z/OS の DCE サポートの重要な特性は、以下のとおりです。

- サーバーの制御領域、ローカル・クライアント、および DCE セキュリティーに関係しているリモート・クライアントは、同一の DCE セル内に構成されなければなりません。

  注: WebSphere for z/OS のエンティティーが、*非認証* トランザクションを使用しようとしている場合、そのエンティティーは DCE セル内にある必要はなく、あるいは別の DCE セル内にあっても構いませんが、DCE セキュリティーで WebSphere for z/OS を使用することはできません。
- DCE セキュリティーに関係しているシスプレックス内の各 OS/390 または z/OS システムは、同一の DCE セル内で正常に動作している独自の DCE セキュリティー・レプリカ・サーバーを持っている必要があります。この要件は、WebSphere for z/OS が必要としている専用の DCE-WebSphere for z/OS DLL に基づいています。
- 各 OS/390 または z/OS システム HFS 上のキータブ・ファイルのコピーは、そこではサーバーの制御領域がそのファイル内の情報を参照する必要があるため、必ず保守しなければなりません。

WebSphere for z/OS と共に使用するための DCE 構成のガイドラインおよび要件

他の DCE と同様に DCE を WebSphere for z/OS と共にインプリメントしますが、以下のガイドラインおよび要件に従ってください。

- 以下の資料をよくお読みください。
  - *z/OS DCE Planning*
  - *z/OS DCE Configuring and Getting Started*
  - *z/OS DCE Administration Guide*
  - *z/OS DCE Command Reference*
  - *z/OS SecureWay Security Server (RACF) セキュリティー管理者のガイド*

- DCE セキュリティーを使用して、すべての WebSphere for z/OS エンティティー (サーバー制御領域、ローカル・クライアント、およびリモート・クライアント) を同一の DCE セル内に配置します。
- DCE セキュリティー・レプリカ・サーバーを各 OS/390 または z/OS システムの同一の DCE セル内に作成します。
- DCE セキュリティー・サーバー・レプリカは、それぞれの WebSphere for z/OS システムごとに、DCESECD という名前の独自のアドレス・スペース内で稼働していなければなりません。

  注:

  1. DCE セキュリティー・レプリカには、同システム上で動作している DCE 基本サービス環境が必要です。
  2. DCE カーネルのデフォルト設定は、DCE セキュリティー・サーバーがカーネル自体の一部としてではなく、独自のアドレス・スペース内で稼働していることを前提としています。
  3. セル・ディレクトリー・サービスが構成されている場合は、DCECDSD とは別のアドレス・スペースにデフォルト設定されます。
- すべてのセキュリティー・サーバー・レプリカおよびセキュリティー・サーバー・マスターを高可用性を持つプラットフォーム上にセットアップすることを強くお勧めします。DCE リモート・クライアントおよび DCE 管理機能は、セキュリティー・レプリカ・サーバーと共に動作する DCE セル内のシステムが使用可能でない場合、TCP/IP プロトコルのタイムアウトの影響を受けることがあります。長時間使用できないシステムの場合は、セキュリティー・サーバー・レプリカを構成解除して、サーバーの解決処理の遅れを回避してください。環境変数を使用して、作業要求を動作しているサーバーに誘導し、通常のセル・ディレクトリー・サービス・プロセスを上書きすることができますが、この方法は、テスト環境またはエラー・リカバリー・プロセスでのみ使用することをお勧めします。
- DCE セキュリティーを使用しているサーバー (制御領域) を持つそれぞれの OS/390 または z/OS システムごとに、HFS 内のキータブ・ファイルをセットアップおよび保守します。
- 完全構成済みの TCP/IP ドメイン・ネーム・サーバーを DCE にセットアップします。DNS を OS/390 または z/OS 上に置く必要はありません。
- WebSphere for z/OS のメッセージ機密性の保護特性を使用するには、DCE 基本サービスおよびセキュリティー・サーバー・レプリカを DCE の DES 機能と共にインストールします。
- DCE アカウントの設定、管理、および保守に加えて、DCE アカウントと RACF のユーザー ID が一致しなければなりません。RACF は、この情報の

一部を RACF DCE セグメント定義のリソース内に保持しています。このセグメント定義は、RACF DCEUUIDS クラス内の RACF リソースを相互参照します。RACF のユーザー ID と DCE アカウントの相互関連によって、RACF にマップされたユーザー ID 用にセットアップされた特権を使用して、リモート Component Broker クライアントおよびサーバーが安全に動作できるようになります。

- RACF を使用している場合は、DCE と相互協調処理するための RACF のセットアップ方法の情報について、*z/OS DCE Administration Guide* の RACF の相互協調処理に関するトピックを参照してください。適切な RACF 権限をサーバーの制御領域と関連するユーザー ID に付与して、それらのユーザーが DCE アカウント情報を RACF のユーザー ID 特権に変換できるようにします。IRR.RDCERUID プロファイルを RACF ファシリティー・クラス内に定義して、サーバー制御領域のユーザー ID の READ 特権をこのプロファイルに付与します。また、DCEUUIDS クラスを活動化します。

  これらの定義を含む RACF サンプルが同梱されています。84ページの『RACF セキュリティーをセットアップするためのステップ』を参照してください。

  注: DCE を RACF 以外のセキュリティー製品と共に使用する計画がある場合は、そのセキュリティー製品は、DCE プリンシパルをユーザー ID にマップできるものでなければなりません。

サーバーを DCE セキュリティー付きでセットアップするためのステップ

この作業を始める前に: WebSphere for z/OS ランタイム・サーバー・インスタンスおよび管理アプリケーションがインストールされている必要があります。55ページの『第3章 WebSphere for z/OS のインストールおよびカスタマイズ』を参照してください。

422ページの『WebSphere for z/OS と共に使用するための DCE 構成のガイドラインおよび要件』の DCE のセットアップに関するガイドラインおよび要件に従ってください。

注: Windows NT サーバーの場合のセキュリティー情報については、*WebSphere Application Server エンタープライズ版 Component Broker システム管理の手引きバージョン 3.0* を参照してください。

サーバーを DCE セキュリティー付きでセットアップするには、以下のステップを実行してください。

1. 管理アプリケーションとの新規の会話を作成していない場合は、新しく作成してください。会話の開始方法についての情報は、*WebSphere Application Server V4.0 for z/OS and OS/390: システム管理ユーザー・インターフェース*, SA88-8656 を参照してください。

   _____

2. DCE での保護を作成したいサーバーを選択または作成します。

   _____

3. プロパティー・フォームで、「DCE 許可 (DCE allowed)」チェック・ボックスを選択します。他の形式のセキュリティーを希望する場合は、他のチェック・ボックスを選択してください。

   _____

4. プロパティー・フォームで、希望する DCE の保護特性のタイプを選択します。無保護 (つまり、両方向－相互－認証)、メッセージの保全性、およびメッセージの機密性 (暗号化) のタイプがあります。

   _____

5. キータブ・ファイルを入力します。デフォルトは `/krb5/v5srvtab` です。

   _____

6. セキュリティー・プリファレンス・テーブルで、DCE を 1 に設定します。他の形式のセキュリティーを希望する場合は、プリファレンスをそれに対応するように設定します。

   _____

7. 会話内の他の定義を完了して、妥当性検査およびコミットを行い、その会話を活動化します。

   _____

会話が正常に活動化されると、完了したことがわかります。

OS/390 または z/OS クライアントを DCE セキュリティー付きでセットアップするためのステップ

この作業を始める前に: 422ページの『WebSphere for z/OS と共に使用するための DCE 構成のガイドラインおよび要件』の DCE のセットアップに関するガイドラインおよび要件に従ってください。

注: Windows NT クライアントの場合のセキュリティー情報については、*WebSphere Application Server エンタープライズ版 Component Broker システム管理の手引きバージョン 3.0* を参照してください。

OS/390 または z/OS クライアントを DCE セキュリティー付きでセットアップするには、以下のステップを実行してください。

1. クライアントに関連する DCE プリンシパルを OS/390 または z/OS のユーザー ID にマップします。

   ---

2. 環境ファイルで、環境変数 CLIENT_DCE_QOP を設定します。設定しない場合、デフォルトは NO_PROTECTION です。383ページの『付録A. 環境ファイル』内のこの環境変数の説明を参照してください。

   ---

3. 環境ファイルで、環境変数 RESOLVE_IPNAME を OS/390 または z/OS クライアントが通信するホスト・システムに設定します。

   ---

4. 環境ファイルを保存します。

OS/390 または z/OS クライアントが DCE セキュリティーを使用して正常に接続すると、完了したことがわかります。

付録D. 特記事項

本書において、日本では発表されていない IBM 製品 (機械およびプログラム)、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのような IBM 製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で IBM ライセンス・プログラムまたは他の IBM 製品に言及している部分があっても、このことは当該プログラムまたは製品のみが使用可能であることを意味するものではありません。IBM 製品、プログラム、またはサービスに代えて、IBM の有効な知的所有権またはその他の法的に保護された権利を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM によって明示的に指定されたものを除き、他社の製品と組み合わせた場合の操作の評価と検査はお客様の責任で行っていただきます。

IBM は、本書で解説されている主題について特許権 (特許出願を含む)、商標権、または著作権を所有している場合があります。本書の提供は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。

〒106-0032 東京都港区六本木 3 丁目 2-31
AP 事業所
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

本書に対して、周期的に変更が行われ、これらの変更は、文書の次版に組み込まれます。IBM は、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。また、IBM 以外の製品に関するパフォーマンスの正確性、互換性、またはその他の要求は確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書で使用している例について

本書で使用している例は、IBM Corporation が作成した単なるサンプルです。これらの例は、いずれかの標準または IBM 製品の一部ではなく、単に、ユーザーのアプリケーションの開発における支援を目的として提供されています。IBM は、これらの例を特定物として現存するままの状態で提供し、これらの例の機能またはパフォーマンスに関して、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。IBM は、これらの例の使用によって生じたいかなる損害に対して、たとえそのような損害の可能性を推奨している場合でも、その責任を負いません。

これらの例は、上記の免責条項をそのまま適用することを条件として、配布し、複製し、改変し、他のソフトウェアに取り込むことができます。

プログラミング・インターフェース情報

本書は、WebSphere for z/OS のプログラミング・インターフェースとしての使用を目的としていない情報を文書化したものです。

商標

以下は、IBM Corporation の米国またはその他の国における商標または登録商標です。

APPN	OS/390
CICS	RACF
DB2DFSMS	RETAIN
ES/3090	RMF
ES/4381	RS/6000
ES/9000	S/390
ESA/390	S/390 Parallel Enterprise Server
IBM	SecureWay
IMS	System/390
IMS/ESA	VisualAge
Language Environment	VTAM
Multiprise	WebSphere
Open Class	z/OS

本書内で使用されている CORBA という用語は、Object Management Group, Inc によって発表された Common Object Request Broker Architecture 標準のことです。

Microsoft、Windows、Windows NT、および Windows ロゴは Microsoft Corporation の米国およびその他の国における商標です。

UNIX は、The Open Group がライセンスしている米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

他の会社名、製品名またはサービス名等は、それぞれ各社の商標または登録商標です。

用語集

本資料で使用されている用語について、詳しくは、以下を参照してください。

- *WebSphere Application Server エンタープライズ版 Component Broker 用語集* (SD88-7380)。以下のインターネット・アドレスからご覧になれます。

  `http://www.ibm.com/jp/software/websphere/appserv/`

- Sun Microsystems Glossary of Java Technology-Related Terms。この用語集は、以下のインターネット・アドレスからご覧になれます。

  `http://java.sun.com/docs/glossary.html`

お探しの用語が見つからない場合は、*IBM Glossary of Computing Terms* を参照してください。以下のインターネット・アドレスからご覧になれます。

`http://www.ibm.com/ibm/terminology/`

または、以下の Sun の Web サイトもご覧ください。

`http://www.sun.com/`

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

［ナ行］

［ハ行］

［マ行］

［ヤ行］

［ラ行］

[ワ行]

A

C

D

H

I

J

L

M

P

R

S

T

W

プログラム番号: 5655-F31

Printed in Japan

GA88-8652-00

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12