

WebSphere Process Server for z/OS



## アプリケーションとその環境の保護

バージョン 7.0.0

本書は、WebSphere Process Server for z/OS バージョン 7、リリース 0、モディフィケーション 0 (製品番号 5655-N53)、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

本書についてのご意見は、doc-comments@us.ibm.com へ E メールでお寄せください。皆様の率直なご意見をお待ちしています。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

**原典：** WebSphere Process Server for z/OS  
Securing Applications and Their Environments  
Version 7.0.0

**発行：** 日本アイ・ビー・エム株式会社

**担当：** トランスレーション・サービス・センター

第2刷 2012.5

© Copyright IBM Corporation 2006, 2010.

# 目次

## WebSphere Process Server およびアプリケーションの保護

リケーションの保護	1
セキュリティの概要	1
セキュリティの概要	2
WebSphere Process Server のインストール: セキュリ ティの考慮事項	3
インストール時に入力する認証情報	4
スタンドアロン・サーバー用の WebSphere Process Server セキュリティーの構成	5
スタンドアロン WebSphere Process Server インス トール済み環境の保護	5
セキュリティの有効化	6
ユーザー・アカウント・リポジトリの構成	8
サーバーの始動と停止	16
管理セキュリティ・ロール	17
デプロイメント環境サーバー用 WebSphere Process Server セキュリティーの構成	19
WebSphere Process Server のデプロイメント環境 の保護	19
セキュリティの有効化	20
ユーザー・アカウント・リポジトリの構成	22

サーバーの始動と停止	30
管理セキュリティ・ロール	31
WebSphere Process Server におけるアプリケーション の保護	33
アプリケーション・セキュリティの要素	33
セキュア・アプリケーションのデプロイ (インス トール)	42
セキュリティ・ロール・ウィジェット	46
アダプターの保護	50
Business Space のセキュリティのセットアップ	51
Business Space のアプリケーション・セキュリテ ィの設定	53
システム REST サービスのセキュリティのセッ トアップ	57
Business Space ウィジェットのセキュリティ上 の考慮事項	58
Business Space を操作できるように Tivoli Access Manager WebSEAL を構成する	59
Business Space のスーパーユーザー・ロールの割 り当て	67
エンドツーエンド・セキュリティの作成	70



---

## WebSphere Process Server およびアプリケーションの保護

WebSphere® Process Server およびアプリケーションのセキュリティは、ランタイム環境の保護とアプリケーションの保護に依存します。

WebSphere Process Server ランタイム環境のセキュリティを確保するには、管理セキュリティを使用可能にする、アプリケーション・セキュリティを使用可能にする、セキュリティが確保されたプロファイルを作成する、重要な機能へのアクセスを特定のユーザーに制限するなどの作業が必要です。

アプリケーションのセキュリティを確保するには、ユーザーを認証する、操作およびリソースのアクセス制御を実装する、データ保全性およびプライバシーを提供するなどの作業を行います。

WebSphere Process Server のセキュリティのベースとなるのは、WebSphere Application Server バージョン 7.0 のセキュリティです。これらの文書は、WebSphere Application Server インフォメーション・センターにある中心的なセキュリティ文書 (特に『アプリケーションとその環境の保護』のトピック) を補足するものです。

---

### セキュリティの概要

WebSphere Process Server のセキュリティのベースとなるのは、WebSphere Application Server バージョン 7.0 のセキュリティです。

セキュリティについて詳しくは、WebSphere Application Server Network Deployment インフォメーション・センターを参照してください。

セキュリティ関連の操作は、WebSphere Process Server 環境内のセキュリティの管理に関連する操作と WebSphere Process Server で実行されているアプリケーションに関連する操作に大きく分類することができます。サーバー環境のセキュリティはアプリケーション・セキュリティの中心となるものであるため、この 2 つの面は別々に検討しないでください。

環境の保護には、管理セキュリティの使用可能化、アプリケーション・セキュリティの使用可能可、セキュリティを適用したプロファイルの作成、選択したユーザーの重要な機能へのアクセスの制限などがあります。

アプリケーションの保護には、いくつかの局面があります。例えば、以下のものがあります。

- ユーザーの認証 - アプリケーションを起動するユーザーまたはプロセスを認証する必要があります。シングル・サインオンにより、ユーザーは認証データを 1 回入力するだけでよく、この認証情報は下流のコンポーネントに渡されます。
- アクセス制御 - 認証済みユーザーがその操作を実行する権限を持っているかどうかを調べます。

- データ保全性およびプライバシー - アプリケーションがアクセスするデータをセキュリティーで保護して、許可されていない関係者が表示または変更できないようにする必要があります。

このセクションの残りの部分では、WebSphere Process Server のさまざまな操作段階におけるセキュリティーの考慮事項について詳しく説明します。

## WebSphere Process Server に固有のセキュリティー上の考慮事項

WebSphere Process Server のセキュリティーの基盤となるのは、WebSphere Application Server 7.0 のセキュリティーです。WebSphere Process Server に固有の考慮事項を以下に示します。

- 管理コンソールの「ビジネス・インテグレーション・セキュリティー」ページは、WebSphere Process Server に固有の機能です。そのページを表示するには、「セキュリティー」を展開し、「ビジネス・インテグレーション・セキュリティー」をクリックします。

ユーザーは、このページを使用して、自分のユーザー・レジストリーから特定の ID を重要なビジネス・インテグレーション認証別名へ割り当てることができます。さらに、このページでは、Business Process Choreographer セキュリティー設定も管理できます。

- WebSphere Process Server では、デフォルトでアプリケーション・セキュリティーが有効になります。これは WebSphere Application Server の場合とは異なります。
- WebSphere Process Server には、コンポーネント固有の一連のセキュリティー・ロールがあります。

---

## セキュリティーの概要

WebSphere Process Server のインストールの計画、アプリケーションの開発およびデプロイ、およびプロセス・サーバーの日常の稼働において、セキュリティーは不可欠な考慮事項です。

以下のリストは、WebSphere Process Server を保護するときに実行するタスクの概要を記載したものです。

1. WebSphere Process Server のインストール時のセキュリティーについて考慮します。
  - a. インストール前にご使用の環境を保護します。
  - b. WebSphere Process Server をインストールするためにオペレーティング・システムの準備を行います。
  - c. インストール後、ご使用の環境を準備します。
2. インストール済みのスタンドアロン環境またはデプロイメント環境のセキュリティーが有効になっていることを確認します。
  - a. 管理セキュリティーが有効になっていることを確認します。
  - b. アプリケーション・セキュリティーが有効になっていることを確認します。
  - c. 必要に応じて、Java 2 セキュリティーを有効にします。

- d. 管理コンソールのセキュリティー構成ウィザードで、セキュリティー・オプションを構成します。
  - e. セキュリティーで保護された認証メカニズムとユーザー・アカウント・リポジトリをセットアップします。
  - f. 重要なビジネス・インテグレーション認証別名にユーザー名とパスワードを割り当てます。
  - g. 各ユーザーを適切な管理セキュリティー・ロールに割り当てます。
3. 特定の WebSphere Process Server コンポーネントのセキュリティーをセットアップします。例えば、セキュリティー・ロール・ウィジェットを使用して、ビジネス・カレンダー・ウィジェットのタイムテーブルに対するロール・ベースのアクセス制御をセットアップします。
  4. プロセス・サーバー環境にデプロイするアプリケーションを保護します。
    - a. すべての適切なセキュリティー機能を使用して、WebSphere Integration Developer においてアプリケーションを開発します。
    - b. ご使用の WebSphere Process Server 環境にアプリケーションをデプロイします。
    - c. 新規にデプロイされたアプリケーションへのアクセスを制御するため、適切なセキュリティー・ロールにユーザーまたはグループを割り当てます。
  5. ご使用の WebSphere Process Server 環境のセキュリティーを維持管理します。

---

## WebSphere Process Server のインストール: セキュリティーの考慮事項

WebSphere Process Server のインストール前、インストール中、およびインストール後のセキュリティーの実装方法について検討します。

### 手順

#### 手順

1. インストール前にご使用の環境を保護します。

適切なセキュリティーを確保した WebSphere Process Server のインストールに必要なコマンドは、ご使用のオペレーティング・システムによって異なります。インストール前に実行する手順について詳しくは、トピック『**インストール時のセキュリティーの準備**』(WebSphere Application Server インフォメーション・センター) を参照してください。

2. WebSphere Process Server をインストールするためにオペレーティング・システムの準備を行います。

このステップには、WebSphere Process Server をインストールする場合に、各種オペレーティング・システムを準備する方法についての情報が含まれます。現在のオペレーティング・システムをインストール用に準備する方法については、トピック『**Preparing the base z/OS operating system for product installation**』( WebSphere Application Server インフォメーション・センター) を参照してください。

3. インストール後、ご使用の環境を保護します。

この作業では、WebSphere Process Server のインストール後にパスワード情報を保護する方法についての情報を提供します。インストール後のご使用の環境の保護について詳しくは、トピック『インストール後の環境の保護』(WebSphere Application Server インフォメーション・センター) を参照してください。

## 次のタスク

インストールの完了後は、管理コンソールからセキュリティを管理できます。

## インストール時に入力する認証情報

インストール時、すべてのコンポーネントに対して、管理者が提供する 1 次管理資格情報がデフォルトで設定されます。これらのデフォルト値によって、基本的なセキュリティが実現します。しかし、インストール済み環境のセキュリティを強化するためには、それぞれのコンポーネントに適切なセキュリティ ID を提供できるように、WebSphere Process Server のコンポーネントを構成してください。

WebSphere Process Server を構成する場合は、デフォルトのプロファイルを拡張します。このプロファイル拡張プロセスには、応答ファイルのさまざまな部分にユーザー名とパスワードを指定することが含まれます。入力するユーザー名とパスワードは、このプロファイル用に選択されたユーザー・レジストリーの ID と一致している必要があります。入力するユーザー名とパスワードは、管理セキュリティを使用可能にする際に必要になります。デフォルトのローカル・オペレーティング・システムのユーザー・レジストリーまたは Lightweight Directory Access Protocol (LDAP) のいずれかを使用することができます。

WebSphere Process Server の数種類のコンポーネントが認証別名を使用します。これらの別名は、データベースとメッセージング・エンジンへのアクセスのためのランタイム・コンポーネントの認証に使用されます。プロファイル拡張プロセスにより、これらの別名の作成に使用される有効なユーザー名とパスワードが収集されます。

## セキュリティを適用した WebSphere Process Server プロファイルの拡張

WebSphere Application Server for z/OS のデフォルト・プロファイルを WebSphere Process Server セキュリティ・プロファイル・データで拡張するとき、環境を保護するための手順を実行することができます。あるいは、プロファイルを拡張した後に、管理コンソールで同じ情報を入力することもできます。

## このタスクについて

WebSphere Process Server の構成時には、各コンポーネントを表す応答ファイルのいくつかのプロパティがあり、このプロパティに、セキュリティ上の目的でユーザー名とパスワードを入力することができます。これらのユーザー名とパスワードの入力を許可する WebSphere Process Server の 3 つのコンポーネントは、Service Component Architecture (SCA)、Business Process Choreographer、および Common Event Infrastructure (CEI) です。

これらのユーザー名とパスワードは認証別名を作成するために使用され、セキュリティを使用可能にする際に必要になります。 WebSphere Process Server の構成時



にユーザー名とパスワードを入力しなかった場合は、WebSphere Process Server を構成した後に管理コンソールを使用して同じ情報を入力することができます。

ユーザー名とパスワードはプレーン・テキストで保管されるため、編集した応答ファイルは安全な場所に保持する必要があります。

## 手順

### 手順

1. 応答ファイルの Service Component Architecture 部分に、コンポーネントをセキュア・モードでサービス統合バスに接続するために使用される ID を指定します。
  - a. Service Component Architecture のプロパティ値が true に設定されていること (`configureScaSecurity=true`) を確認します。
  - b. 該当するプロパティ・フィールド (「`scaSecurityUserid`」および「`scaSecurityPassword`」) の値として、有効なユーザー名とパスワードを入力します。
2. 応答ファイルの Common Event Infrastructure 部分に、WebSphere Messaging キュー・マネージャーによる認証に使用される ID を指定します。

該当するフィールド (「`ceiSampleJmsUser`」および「`ceiSampleJmsPwd`」) に有効なユーザー名とパスワードを入力します。

3. 応答ファイルの Business Process Choreographer 部分に、セキュア・モードでサービス統合バスに接続するためのサンプルの Business Process Choreographer 構成用の ID を指定します。

`bpcmUser` および `bpcmPwd` フィールドに有効なユーザー名とパスワードを入力します。

## 次のタスク

認証別名の管理については、後続のトピックを参照してください。

---

## スタンドアロン・サーバー用の WebSphere Process Server セキュリティーの構成

WebSphere Process Server のスタンドアロン・インストールのセキュリティーを構成する場合、管理セキュリティーの有効化や、ユーザー・アカウント・レジストリーの構成などを実行します。

## スタンドアロン WebSphere Process Server インストール済み環境の保護

ご使用の WebSphere Process Server 環境でのセキュリティーは、管理コンソールからコントロールします。十分な特権を持っているユーザーは、管理コンソールからすべてのアプリケーション・セキュリティーのオン/オフを行うことができます。このため保護されたアプリケーションをデプロイする前に、環境を保護することが重要です。

## このタスクについて

セキュリティーを有効化するための作業のロードマップを以下のステップに示します。これらの作業の詳細については、後述のトピックで説明します。

### 手順

#### 手順

1. 管理セキュリティーが有効であることを確認します。『セキュリティーの有効化』
2. アプリケーション・セキュリティーが有効であることを確認します。『セキュリティーの有効化』
3. 使用するユーザー・アカウント・リポジトリを選択します。 8 ページの『ユーザー・アカウント・リポジトリの構成』

「**現行として設定 (Set as current)**」を使用して、選択したレジストリーを必ず現在のレジストリーとして設定してください。

4. ユーザーまたはグループを管理ロールに追加します。
5. 必要な場合は、サーバーを停止して再始動します。 16 ページの『サーバーの始動と停止』
6. インストールされたコンポーネントの認証別名、アクセス制御、およびその他のセキュリティー・メカニズムをセットアップします。 33 ページの『WebSphere Process Server におけるアプリケーションの保護』

## セキュリティーの有効化

WebSphere Application Server バージョン 7.0 では、管理セキュリティーは、デフォルトで有効になっています。管理セキュリティーが無効になっている場合は、以下の説明に従って使用可能にしてください。

### 始める前に

これらの操作を開始する前に、WebSphere Process Server をインストールして、インストール済み環境を検証してください。

保護するプロファイルに対して管理コンソールを開きます。任意のユーザー ID を使用して、コンソールにログインします。すべてのユーザー名が、プロファイルが保護されるまで受け入れられます。

### このタスクについて

管理コンソールを使用して、管理セキュリティー、アプリケーション・セキュリティー、および Java 2 セキュリティーを有効にすることができます。

- 管理セキュリティー では、セキュリティーの使用の有無や、認証を実行する基準となるレジストリーのタイプなどの値を決定します。ここで指定する値の多くは、デフォルトとして機能します。管理セキュリティーの設定が不適切な場合は、管理コンソールにアクセスできなくなったり、サーバーが異常終了したりする可能性があるため、適切な計画が必要です。

管理セキュリティは、WebSphere Process Server のさまざまなセキュリティ設定をアクティブにするための「大きなスイッチ」であると考えられます。これらの設定の値を指定しても、管理セキュリティをアクティブにするまでは有効になりません。設定には、ユーザーの認証、Secure Sockets Layer (SSL) の使用、ユーザー・アカウント・リポジトリの選択などが含まれます。具体的にいうと、認証や役割ベースの許可を含むアプリケーション・セキュリティも、管理セキュリティをアクティブにするまでは適用されません。管理セキュリティは、デフォルトで使用可能になっています。

管理セキュリティ構成は、セキュリティ・ドメイン内のすべてのサーバーに適用されます。

- アプリケーション・セキュリティ は、環境内のアプリケーションに対するセキュリティを使用可能にします。このタイプのセキュリティは、各アプリケーションを個別に管理して、アプリケーション・ユーザーの認証を要求します。

WebSphere Process Server の管理セキュリティはデフォルトで有効になっています。アプリケーション・セキュリティも、デフォルトで使用可能になっています。アプリケーション・セキュリティは、管理セキュリティが使用可能である場合にのみ有効になります。

- Java 2 セキュリティ は、保護された特定のシステム・リソースへのアクセスを許可する前にアクセス権限を検査することにより、総合的なシステム安全性を向上する、ポリシー・ベースのきめ細かいアクセス制御メカニズムを提供します。Java 2 セキュリティは、ファイル入出力、ソケット、プロパティなどのシステム・リソースへのアクセスを保護します。また、サーブレット、JavaServer Pages (JSP) ファイル、Enterprise JavaBeans (EJB) メソッドなどの Web リソースへのアクセスも保護します。

Java 2 セキュリティは比較的新しいテクノロジーであるため、既存または新規の多くのアプリケーションは、Java 2 セキュリティが提供する非常に細分化されたアクセス制御プログラミング・モデルに対応していない可能性があります。管理者は、アプリケーションが Java 2 セキュリティに対応していない場合に、Java 2 セキュリティを使用可能にするるとどのような結果となる可能性があるかを認識しておく必要があります。Java 2 セキュリティを導入すると、アプリケーション開発者および管理者は、新規の要件にも従う必要があります。

**重要:** Software Development Kit (SDK) に対する更新が含まれるフィックスパックによって、制限されていないポリシー・ファイルが上書きされる可能性があります。フィックスパックを適用する前に、制限されていないポリシー・ファイルをバックアップし、フィックスパックを適用してから、バックアップしたポリシー・ファイルを再び適用してください。

## 手順

### 手順

1. 管理コンソールで「管理セキュリティ」ページを開きます。

「セキュリティ」を展開して、「グローバル・セキュリティ」をクリックします。

2. 管理セキュリティを使用可能にします。

「管理セキュリティーを使用可能にする」を選択します。

3. アプリケーション・セキュリティーを使用可能にします。

「アプリケーション・セキュリティーを使用可能にする」を選択します。

4. オプション: 必要な場合は、Java 2 セキュリティーを強制します。

「Java 2 セキュリティーを使用してアプリケーションのアクセスをローカル・リソースに制限する」を選択して、Java 2 セキュリティー権限検査を強制します。

Java 2 セキュリティーを使用可能にすると、デフォルト・ポリシーで付与されているよりも多くの Java 2 セキュリティー権限を必要とするアプリケーションは、必要なアクセス権がアプリケーションの `app.policy` ファイルまたは `was.policy` ファイルのいずれかで付与されるまで正常に実行できないことがあります。アクセス制御例外は、必要なすべての権限が与えられていないアプリケーションによって生成されます。Java 2 セキュリティーについて詳しくは、WebSphere Application Server インフォメーション・センターの『Java 2 セキュリティー・ポリシー・ファイルの構成』のトピックを参照してください。

注: `app.policy` ファイルへの更新は、その `app.policy` ファイルが属しているノード上のエンタープライズ・アプリケーションにのみ適用されます。

- a. オプション: 「アプリケーションがカスタム許可を認可されたときに警告する」を選択します。 `filter.policy` ファイルには、J2EE 1.4 仕様によりアプリケーションに対して与えてはならないと規定されている許可のリストが格納されています。このオプションを使用可能にすると、インストールされたアプリケーションに対してこのポリシー・ファイル内で指定された許可が認可されている場合は、警告が発行されます。デフォルトは使用可能です。
  - b. オプション: 「リソース認証データに対するアクセスの制限」を選択します。Java コネクタ・アーキテクチャー (JCA) マッピングの機密認証データに対するアプリケーションのアクセスを制限する必要がある場合は、このオプションを使用可能にします。
5. 以上の変更内容を適用します。

ページの下部の「適用」ボタンをクリックします。

6. ローカル構成へ変更内容を保管します。

メッセージ・ペインの「保管」をクリックします。

7. 必要な場合は、サーバーを停止して再始動します。

サーバーが再始動される必要がある場合は、その旨のメッセージが管理コンソールに表示されます。

## 次のタスク

作成したプロファイルごとに、管理セキュリティーを有効にする必要があります。

## ユーザー・アカウント・リポジトリの構成

登録済みユーザーのユーザー名とパスワードは、ユーザー・アカウント・リポジトリに保管されます。ローカルのオペレーティング・システムのユーザー・アカウ

ント・リポジトリ (デフォルト)、Lightweight Directory Access Protocol (LDAP)、統合リポジトリ、またはカスタム・アカウント・リポジトリのいずれかを使用することができます。

## このタスクについて

ユーザー・アカウント・リポジトリとは、認証メカニズムが認証を実行する際に照会するユーザーおよびグループのレジストリーのことです。管理コンソールでユーザー・アカウント・リポジトリを選択します。

**注:** Network Deployment 環境の場合、LDAP または現在のローカル・オペレーティング・システムのいずれかをユーザー・レジストリーとして使用することができます。

### 手順

#### 手順

1. 管理コンソールの「管理、アプリケーション、インフラストラクチャーの保護」パネルにナビゲートします。「**セキュリティ**」を展開して、「**グローバル・セキュリティ**」をクリックします。
2. 使用するユーザー・レジストリーを選択します。

次の表に、ユーザー・レジストリーの選択およびユーザー・レジストリーの選択と構成に必要なアクションを示します。

ユーザー・レジストリー	アクション
統合リポジトリ	<p>この設定は、1 つのレルムの下で複数のリポジトリ内のプロファイルを管理するために指定します。レルムには、以下のリポジトリ内の ID を含めることができます。</p> <ul style="list-style-type: none"> <li>• システムに組み込まれているファイル・ベース・リポジトリ</li> <li>• 1 つ以上の外部リポジトリ</li> <li>• 組み込まれたファイル・ベース・リポジトリと 1 つ以上の外部リポジトリの両方</li> </ul> <p><b>注:</b> 統合リポジトリ構成を表示できるのは、管理者特権を持つユーザーのみです。詳しくは、フェデレーテッド・リポジトリ構成におけるレルムの管理を参照してください。</p>
ローカル・オペレーティング・システム	<p>これはデフォルトのユーザー・レジストリーです。</p> <p>10 ページの『ローカルのオペレーティング・システムまたはスタンドアロンのカスタム・ユーザー・アカウント・リポジトリの構成』の手順を実行します。</p>

ユーザー・レジストリー	アクション
Lightweight Directory Access Protocol (LDAP)	12 ページの『ユーザー・レジストリーとしての Lightweight Directory Access Protocol (LDAP) の構成』の説明に従って、ユーザー・レジストリーとして LDAP を構成してください。
カスタム・ユーザー・レジストリー	『ローカルのオペレーティング・システムまたはスタンドアロンのカスタム・ユーザー・アカウント・リポジトリーの構成』の説明に従い、カスタム・アカウント・リポジトリーを選択して、各自のニーズに応じて構成します。
Tivoli® Access Manager	注: このオプションは、管理コンソールからは使用できません。wsadmin コマンドを使用して構成する必要があります。

## ローカルのオペレーティング・システムまたはスタンドアロンのカスタム・ユーザー・アカウント・リポジトリーの構成

管理コンソールを使用して、ユーザー・アカウント・リポジトリーを構成できます。ローカルのオペレーティング・システムを構成する手順 (デフォルト) と、スタンドアロンのカスタム・ユーザー・アカウント・レジストリーを構成する手順は似ています。

### このタスクについて

WebSphere Process Server にサーバー・ユーザー ID を自動的に生成させることができます。使用しているユーザー・アカウント・リポジトリーからユーザー ID を指定することもできます。後者を選択すると、管理アクションをより正確に監査できるようになります。

WebSphere Process Server for z/OS® のユーザー・レジストリーとして LDAP を使用する場合、管理コンソールを使用してセキュリティーを管理します。ユーザー・レジストリーにオペレーティング・システムを使用する場合は、System Authorization Facility を使用してセキュリティーを許可します。

### 手順

#### 手順

1. 管理コンソールで、ユーザー・レジストリーの構成ページを開きます。

「セキュリティー」を展開して「グローバル・セキュリティー」をクリックし、「使用可能なレルム定義」メニューで、使用しているユーザー・レジストリーを選択します。「構成」をクリックします。

2. オプション: 「1 次管理ユーザー名」フィールドに有効なユーザー名を入力します。

この値は、管理特権を持ち、レジストリー内で定義されているユーザーの名前です。このユーザー名は、管理コンソールへのアクセスに使用されます。また、wsadmin コマンドでも使用されます。



3. 「自動的に生成されたサーバー ID」または「リポジトリに保管されたサーバー ID」のいずれかのオプションを選択します。

- 「自動的に生成されたサーバー ID (Automatically generated server identity)」を選択すると、内部プロセス通信に使用されるサーバー ID がアプリケーション・サーバーによって生成されます。

このサーバー ID は、「認証メカニズムと有効期限」ページで変更することができます。「認証メカニズムと有効期限」ページにアクセスするには、「セキュリティ」 > 「グローバル・セキュリティ」 > 「認証メカニズムと有効期限」をクリックします。「内部サーバー ID」フィールドの値を変更します。

- 「リポジトリに保管されたサーバー ID」オプションを選択する場合は、以下の情報を入力します。
    - 「バージョン 7.0 ノード上のサーバー・ユーザー ID または管理ユーザー (Server user ID or administrative user on a Version 7.0 node)」に、セキュリティ目的でアプリケーション・サーバーの実行に使用されるユーザー ID を指定します。
    - 「パスワード」に、このユーザーに関連付けるパスワードを指定します。
4. オプション: スタンドアロン・カスタム・レジストリーの場合は、以下の手順を実行します。
- a. 「カスタム・レジストリー・クラス名 (Custom registry class name)」の値が正しいことを確認し、必要に応じて変更します。
  - b. 「認証で大/小文字を無視する (Ignore case for authentication)」のチェック・マークを外します。

このオプションを選択すると、許可検査で大文字と小文字が区別されなくなります。

5. 「適用」をクリックします。
6. ページの下部の「現行として設定 (Set as current)」をクリックします。
7. 「OK」をクリックして、「適用」または「保管」をクリックします。

## 次のタスク

更新が有効になるよう、すべてのサーバーを保管して停止してから再起動します。

サーバーが問題なく始動する場合は、正しくセットアップされています。

## Tivoli Access Manager をユーザー・アカウント・リポジトリとして使用するための WebSphere Process Server の構成

Tivoli Access Manager をユーザー・アカウント・リポジトリとして使用できますが、管理コンソールではなく **wsadmin** コマンドを使用して構成する必要があります。

## このタスクについて

Tivoli Access Manager をユーザー・アカウント・リポジトリとして使用できません。管理コンソールでは構成できないため、**wsadmin** コマンドを使用する必要があります。WebSphere Application Server インフォメーション・センターのトピック

『JACC プロバイダーへのインストール済みアプリケーションのセキュリティー・ポリシーの wsadmin スクリプトを使用した伝搬』を参照してください。

## ユーザー・レジストリーとしての Lightweight Directory Access Protocol (LDAP) の構成

デフォルトのユーザー・レジストリーは、ローカル・オペレーティング・システムのレジストリーです。外部の Lightweight Directory Access Protocol (LDAP) も、ユーザー・レジストリーとして使用することができます。

### 始める前に

このタスクは、管理 セキュリティーがオンになっていることを前提としています。

LDAP を使用してユーザー・レジストリーにアクセスするには、有効なユーザー名 (ID) とパスワード、レジストリー・サーバーのサーバー・ホストとポート、基本識別名 (DN)、必要に応じてバインド DN とバインド・パスワードが必要です。

検索可能なユーザー・レジストリーから、任意の有効なユーザーを選択することができます。管理ロールを持つ任意のユーザー ID を使用してログオンできます。

**重要:** 複数の LDAP サーバーを使用するように WebSphere Process Server を構成した場合、管理コンソールの「グローバル・セキュリティー」 > 「スタンドアロン LDAP レジストリー」ページに示される値は、使用されている LDAP サーバーを反映していない可能性があります。

### 手順

#### 手順

1. 管理コンソールを始動します。
  - セキュリティーが現在無効になっている場合は、ユーザー ID の入力画面が表示されます。入力画面が表示されたら、任意のユーザー ID を入力してログインします。
  - セキュリティーが現在有効になっている場合は、ユーザー ID とパスワードの入力画面が表示されます。入力画面が表示されたら、事前に定義された管理ユーザー ID とパスワードを入力してログインします。
2. 「セキュリティー」を展開して、「グローバル・セキュリティー」をクリックします。
3. 「管理、アプリケーション、およびインフラストラクチャーの保護 (Secure administration, applications, and infrastructure)」ページで、以下の手順を実行します。
  - a. 「管理セキュリティーを使用可能にする」が選択されていることを確認します。
  - b. 「使用可能なレルム定義 (Available realm Definitions)」リストから、「スタンドアロン LDAP レジストリー」を選択します。
  - c. 「構成」をクリックします。
4. 「スタンドアロン LDAP レジストリー」ページの「構成」タブで、以下の手順を実行します。
  - a. 「1 次管理ユーザー名」フィールドに有効なユーザー名を入力します。



この値は、管理特権を持ち、レジストリー内で定義されているユーザーの名前です。このユーザー名は、管理コンソールへのアクセスに使用されます。また、**wsadmin** コマンドでも使用されます。

「拡張 LDAP 設定」ページのユーザー・フィルターで定義されているとおり、ユーザーの完全な識別名 (DN) またはユーザーの短縮名を入力します。

- b. オプション: 「自動的に生成されたサーバー ID」または「リポジトリに保管されたサーバー ID」のいずれかのオプションを選択します。
- 「自動的に生成されたサーバー ID (Automatically generated server identity)」を選択すると、内部プロセス通信に使用されるサーバー ID がアプリケーション・サーバーによって生成されます。

このサーバー ID は、「認証メカニズムと有効期限」ページで変更することができます。「認証メカニズムと有効期限」ページにアクセスするには、「セキュリティ」 > 「グローバル・セキュリティ」 > 「認証メカニズムと有効期限」をクリックします。「内部サーバー ID」フィールドの値を変更します。

- 「リポジトリに保管されたサーバー ID」オプションを選択する場合は、以下の情報を入力します。
  - 「バージョン 7.0 ノード上のサーバー・ユーザー ID または管理ユーザー (Server user ID or administrative user on a Version 7.0 node)」に、セキュリティ目的でアプリケーション・サーバーの実行に使用されるユーザー ID を指定します。
  - 「パスワード」に、このユーザーに関連付けるパスワードを指定します。

この ID は LDAP 管理者ユーザー ID ではありませんが、この項目は LDAP に存在している必要があります。

- c. オプション: 「LDAP サーバーのタイプ (Type of LDAP server)」リストから、LDAP サーバーを選択します。

LDAP サーバーのタイプにより、WebSphere Process Server で使用されるデフォルト・フィルターが決まります。これらのデフォルト・フィルターにより、「LDAP サーバーのタイプ (Type of LDAP server)」フィールドが「カスタム」に変更されます。これは、カスタム・フィールドが使用されるという意味です。このアクションは、「拡張 LDAP 設定」ページで「OK」または「適用」をクリックすると発生します。他の LDAP サーバーを使用するには、リストから「カスタム」タイプを選択し、必要に応じてユーザー・フィルターとグループ・フィルターを変更します。

IBM Tivoli Directory Server ユーザーの場合、ディレクトリー・タイプとして **IBM Tivoli Directory Server** を選択することができます。IBM Tivoli Directory Server ディレクトリー・タイプを使用すると、パフォーマンスが向上します。

- d. 「ホスト」フィールドに、LDAP が常駐するコンピューターの完全修飾名を入力します。

IP アドレスまたはドメイン・ネーム・システム (DNS) 名のいずれかを入力します。

- e. オプション: 「ポート」フィールドに、LDAP サーバーが listen するポート番号を入力します。

ホスト名とポート番号は、WebSphere Process Server セル内の LDAP サーバーのレلمを表します。そのため、異なるセルに存在するサーバーが Lightweight Third Party Authentication (LTPA) トークンを使用して相互に通信する場合は、これらのレلمはすべてのセルで正確に一致している必要があります。

デフォルト値は 389 です。

複数の WebSphere Process Server がインストールされ、同一のシングル・サインオン・ドメインで実行するように構成されている場合、または WebSphere Process Server を WebSphere Process Server の旧バージョンと相互運用する場合は、ポート番号がすべての構成で一致していることを確認してください。

- f. オプション: 「基本識別名 (DN)」フィールドに基本識別名を入力します。

基本識別名は、この LDAP ディレクトリー・サーバーにおける LDAP 検索の開始点を示します。例えば、DN に cn=John Doe, ou=Rochester, o=IBM, c=US が設定されているユーザーの場合、基本 DN を以下のいずれかのオプションとして指定します (サフィックス c=us を想定): ou=Rochester、o=IBM、c=us、あるいは o=IBM c=us または c=us。

許可検査用に、このフィールドでは大文字と小文字が区別されます。そのため、別のセルや Lotus Domino<sup>®</sup> サーバーなどからトークンを受け取った場合に、サーバー内の基本識別名 (DN) が別のセルまたは Lotus Domino サーバーの基本 DN と正確に一致する必要があります。許可検査の際に大文字と小文字を区別する必要がない場合は、「許可検査で大/小文字を区別しない」を有効にしてください。

WebSphere Process Server の場合、識別名は Lightweight Directory Access Protocol (LDAP) 仕様に従って正規化されます。正規化は、基本識別名のコマおよび等号の前後のスペースを取り除くことによって行われます。o = ibm, c = us や o=ibm, c=us は、正規化されていない識別名の例です。o=ibm,c=us は、正規化された識別名の例です。

このフィールドは、(このフィールドがオプションになっている) Lotus Domino Directory の場合を除き、すべての LDAP ディレクトリーで必須です。

- g. オプション: 「バインド識別名 (Bind distinguished name)」フィールドにバインド DN 名を入力します。

ユーザー情報とグループ情報を取得する際に LDAP サーバー上で匿名バインドが使用できない場合は、バインド DN が必要です。

匿名バインドを使用するように LDAP サーバーがセットアップされている場合、このフィールドには何も入力しないでください。名前を指定しない場

合、アプリケーション・サーバーは匿名でバインドを行います。識別名の例については、「基本識別名」フィールドの説明を参照してください。

- h. オプション: 「バインド・パスワード」フィールドに、バインド DN に対応するパスワードを入力します。
- i. オプション: 「**検索タイムアウト (Search time out)**」の値を変更します。

このタイムアウト値は、LDAP サーバーが応答を製品クライアントに送信する際に待機する最大時間です。この時間を超えると、要求が停止されます。デフォルトは 120 秒です。

- j. 「**接続の再利用**」が選択されていることを確認します。

このオプションにより、サーバーが LDAP 接続を再利用するかどうかを指定します。このオプションをクリアするのは、ルーターを使用して要求を複数の LDAP サーバーに送信する場合に、そのルーターがアフィニティーをサポートしていない場合 (ほとんどありません) だけです。それ以外の場合は、このオプションを選択したままにしておきます。

- k. オプション: 「**許可検査で大/小文字を区別しない**」が有効になっていることを確認します。

このオプションを有効にすると、許可検査で大文字と小文字が区別されなくなります。

通常、許可検査には、ユーザーの完全な DN (LDAP サーバー内で固有であり、大文字と小文字が区別される) の検査も含まれます。ただし、IBM Directory Server または Sun ONE (以前の iPlanet) Directory Server LDAP サーバーを使用する場合は、LDAP サーバーから取得されるグループ情報に大文字と小文字の不整合があるため、このオプションを有効にする必要があります。この不整合の影響を受けるのは、許可検査だけです。それ以外の場合、このフィールドは任意で指定します。大文字と小文字を区別する許可検査が必要な場合は、有効に設定します。

例えば、証明書を使用する際に、証明書の内容が LDAP サーバー項目の大文字/小文字と一致しない場合に、このオプションを選択します。製品と Lotus Domino 間でシングル・サインオン (SSO) を使用する場合も、「許可検査で大/小文字を区別しない」を有効にします。

デフォルトは使用可能です。

- l. オプション: LDAP サーバーで Secure Sockets Layer (SSL) 通信を使用する場合は、「**SSL 使用可能**」を選択します。

「**SSL 使用可能**」オプションを選択すると、「**中央管理対象**」または「**特定の SSL 別名を使用する (Use specific SSL alias)**」を選択できます。

- **中央管理対象**

このオプションを使用すると、特定のスコープ (1 つのロケーションのセル、ノード、サーバー、またはクラスターなど) に SSL 構成を指定することができます。「**中央管理対象**」オプションを使用するには、エンドポイントの特定のセットに SSL 構成を指定する必要があります。

「エンドポイント・セキュリティー構成の管理」ページには、SSL プロトコルを使用するすべてのインバウンド・エンドポイントとアウトバウンド・エンドポイントが表示されます。

「エンドポイント・セキュリティー構成の管理」ページの「**インバウンド (Inbound)**」セクションまたは「**アウトバウンド (Outbound)**」セクションを展開してノードの名前をクリックし、そのノード上のすべてのエンドポイントに使用される SSL 構成を指定します。LDAP レジストリーの場合、LDAP の SSL 構成を指定することにより、継承された SSL 構成をオーバーライドすることができます。

- **特定の SSL 別名を使用する**

このオプションは、オプションの下にあるリスト内のいずれかの SSL 構成を選択する場合に使用されます。

この構成が使用されるのは、LDAP で SSL が有効になっている場合だけです。デフォルトは **NodeDefaultSSLSettings** です。

- m. 「**OK**」をクリックし、「**適用**」または「**保管**」をクリックして、「管理、アプリケーション、およびインフラストラクチャーの保護 (Secure administration, applications, and infrastructure)」ページに戻ります。
5. 「管理、アプリケーション、およびインフラストラクチャーの保護 (Secure administration, applications, and infrastructure)」ページで、「**現行として設定 (Set as current)**」をクリックします。
  6. 「**OK**」をクリックして、「**適用**」または「**保管**」をクリックします。

### 次のタスク

更新が有効になるよう、すべてのサーバーを保管して停止してから再起動します。

サーバーが問題なく始動する場合は、正しくセットアップされています。

## サーバーの始動と停止

管理セキュリティーが有効な場合、サーバーをシャットダウンするには、適切なユーザー名とパスワードを入力する必要があります。サーバーは認証なしで始動されますが、管理コンソールにアクセスするためには、認証が必要です。

### 始める前に

管理セキュリティーが有効である必要があります。

**問題の回避:** **Vista** **Windows 7** ユーザー・アカウント制御 (UAC) がいくつかのレベルで有効になっている場合、コマンド・プロンプトからアプリケーション・サーバーを始動するときには、管理者権限を使用する必要があります。以下の操作を実行してコマンド・プロンプト・ウィンドウを起動して、アプリケーション・サーバーを始動します。

- コマンド・プロンプトのショートカットを右クリックします。
- 「**管理者として実行 (Run As Administrator)**」をクリックします。

- コマンド・プロンプト・ウィンドウを管理者として開くと、続行するかどうかをたずねるオペレーティング・システム・ダイアログが表示されます。「続行」をクリックして、操作を続行します。

## 手順

### 手順

1. サーバーを始動します。 コマンド・プロンプトの `/AppServer/bin` ディレクトリで、次のテキストをコマンド行から入力します。 **startServer.sh**  
`servername`

**注:** サーバーを始動するために、ユーザー名とパスワードを入力する必要はありません。ただし、管理コンソールの起動またはその他の管理操作を実行するには、認証を受ける必要があります。

サーバーが始動するか、エラー・メッセージが返されます。

2. サーバーを停止します。 コマンド・プロンプトの `/AppServer/bin` ディレクトリで、次のテキストを入力します。 **stopServer.sh** `servername -username username -password password`

**注:** サーバーを停止するには、ユーザー名とパスワードを入力する必要があります。

入力したユーザー名とパスワードがオペレーター・ロールまたは管理者ロールのメンバーの場合は、サーバーが停止します。

3. サーバーが正常に停止したことを確認します。

入力した要求の結果は、要求を入力したコマンド・ウィンドウに表示されます。

## 管理セキュリティ・ロール

いくつかの管理セキュリティ・ロールが、WebSphere Process Server インストール済み環境の一部として提供されます。

管理コンソールの一部として 8 つのロールが提供されます。これらのロールは、管理コンソール上の機能の範囲にアクセス権を付与します。管理セキュリティが使用可能になっている場合、ユーザーは管理コンソールにアクセスするためにこれらのロールの 1 つにマップされる必要があります。

インストール後にサーバーに最初にログインするユーザーは、管理者ロールに追加されます。

表 1. 管理セキュリティ・ロール

管理セキュリティ・ロール	説明
モニター	モニター・ロールのメンバーは、WebSphere Process Server 構成およびサーバーの現在の状態を表示することができます。
コンフィギュレーター	コンフィギュレーター・ロールのメンバーは、WebSphere Process Server 構成を編集することができます。
オペレーター	オペレーター・ロールのメンバーは、モニター特権に加えてランタイム状態の変更 (つまりサーバーの始動および停止) の権限を持ちます。

表 1. 管理セキュリティ・ロール (続き)

管理セキュリティ・ロール	説明
管理者	<p>管理者ロールに限り、コンフィギュレーター・ロールとオペレーター・ロールの組み合わせに加えて、追加の特権が付与されます。例えば、これらの特権には以下のものがあります。</p> <ul style="list-style-type: none"> <li>• サーバーのユーザー ID とパスワードの変更</li> <li>• ユーザーとグループの管理者ロールへのマッピング</li> </ul> <p>管理者には、以下のような機密情報へのアクセスに必要な権限もあります。</p> <ul style="list-style-type: none"> <li>• Lightweight Third Party Authentication (LTPA) のパスワード</li> <li>• キー</li> </ul>
ISC 管理	<p>このロールを使用できるのは管理コンソールのユーザーのみであり、<b>wsadmin</b> ユーザーは対象外です。このロールを付与されたユーザーは、統合リポジトリ内でユーザーおよびグループを管理するための管理者特権を持ちます。例えば、ISC 管理 (ISC Admins) ロールのユーザーは、以下のタスクを実行できます。</p> <ul style="list-style-type: none"> <li>• フェデレーテッド・リポジトリ構成でのユーザーの作成、更新、または削除</li> <li>• フェデレーテッド・リポジトリ構成でのグループの作成、更新、または削除</li> </ul>
デプロイヤー	<p>このロールを付与されたユーザーが、アプリケーションに対して構成アクションとランタイム操作の両方を実行できます。</p>
セキュリティ・マネージャーの管理	<p>このロールを付与されたユーザーのみが、ユーザーを管理の役割にマップできます。また、細分化された管理セキュリティを使用している場合は、このロールを付与されたユーザーのみが、許可グループを管理できます。</p>
監査員	<p>このロールを与えられたユーザーは、セキュリティ監査サブシステムの構成設定を表示および変更できます。  <b>注:</b> 監査員ロールには、モニター・ロールが含まれていません。このため、監査員は残りのセキュリティ構成を表示できますが、変更することはできません。</p>

詳しくは、WebSphere Application Server インフォメーション・センターの管理ロールを参照してください。

管理セキュリティを使用可能にした際に指定されたサーバーの ID は自動的に管理者ロールにマップされます。ユーザーまたはグループは、WebSphere Process Server の管理コンソールを使用して、随時管理の役割に追加したり、管理の役割から除去したりすることができます。ただし、これらの変更を有効にするには、サーバーの再始動が必要です。

**ヒント:** 管理の役割に特定のユーザーではなく、1 つのグループまたは複数のグループをマップします。これは、管理がより柔軟で容易になるためです。1 つのグループを管理の役割にマップすることによって、ユーザーのグループへの追加また



はグループからの除去が、WebSphere Process Server の外部で実行されるため、変更を有効にするためのサーバーの再始動は不要になります。

失敗したイベント・マネージャーは、管理者またはオペレーターの役割のいずれかが付与されているあらゆるユーザーが操作できます。

セレクターは、管理者またはコンフィギュレーターの役割のいずれかが付与されているあらゆるユーザーが構成できます。

ユーザーまたはグループのマッピングに加えて、特別対象も管理の役割にマップすることができます。特別対象とは、特定クラスのユーザーを一般化したものです。

- 全認証者特別対象とは、管理の役割のアクセス検査によって、要求を出しているユーザーが少なくとも認証されることを意味します。
- 全員特別対象とは、認証されているか否かに関係なく、セキュリティが使用可能になっていない場合と同様に、すべてのユーザーがアクションを実行できることを意味します。

---

## デプロイメント環境サーバー用 WebSphere Process Server セキュリティーの構成

WebSphere Process Server のデプロイメント環境インストールのセキュリティを構成する場合、管理セキュリティの有効化や、ユーザー・アカウント・レジストリーの構成などのタスクを実行します。

### WebSphere Process Server のデプロイメント環境の保護

ご使用の WebSphere Process Server 環境でのセキュリティは、管理コンソールからコントロールします。十分な特権を持っているユーザーは、管理コンソールからすべてのアプリケーション・セキュリティのオン/オフを行うことができます。このため保護されたアプリケーションをデプロイする前に、環境を保護することが重要です。

#### このタスクについて

セキュリティを有効化するための作業のロードマップを以下のステップに示します。これらの作業の詳細については、後述のトピックで説明します。

#### 手順

#### 手順

1. 管理セキュリティが有効であることを確認します。 6 ページの『セキュリティの有効化』
2. アプリケーション・セキュリティが有効であることを確認します。 6 ページの『セキュリティの有効化』
3. 使用するユーザー・アカウント・リポジトリを選択します。 8 ページの『ユーザー・アカウント・リポジトリの構成』

「現行として設定 (Set as current)」を使用して、選択したレジストリーを必ず現在のレジストリーとして設定してください。

4. ユーザーまたはグループを管理ロールに追加します。
5. 必要な場合は、サーバーを停止して再始動します。 16 ページの『サーバーの始動と停止』
6. インストールされたコンポーネントの認証別名、アクセス制御、およびその他のセキュリティー・メカニズムをセットアップします。 33 ページの『WebSphere Process Server におけるアプリケーションの保護』

## セキュリティーの有効化

WebSphere Application Server バージョン 7.0 では、管理セキュリティーは、デフォルトで有効になっています。管理セキュリティーが無効になっている場合は、以下の説明に従って使用可能にしてください。

### 始める前に

これらの操作を開始する前に、WebSphere Process Server をインストールして、インストール済み環境を検証してください。

保護するプロファイルに対して管理コンソールを開きます。任意のユーザー ID を使用して、コンソールにログインします。すべてのユーザー名が、プロファイルが保護されるまで受け入れられます。

### このタスクについて

管理コンソールを使用して、管理セキュリティー、アプリケーション・セキュリティー、および Java 2 セキュリティーを有効にすることができます。

- 管理セキュリティー では、セキュリティーの使用の有無や、認証を実行する基準となるレジストリーのタイプなどの値を決定します。ここで指定する値の多くは、デフォルトとして機能します。管理セキュリティーの設定が不適切な場合は、管理コンソールにアクセスできなくなったり、サーバーが異常終了したりする可能性があるため、適切な計画が必要です。

管理セキュリティーは、WebSphere Process Server のさまざまなセキュリティー設定をアクティブにするための「大きなスイッチ」であると考えられます。これらの設定の値を指定しても、管理セキュリティーをアクティブにするまでは有効になりません。設定には、ユーザーの認証、Secure Sockets Layer (SSL) の使用、ユーザー・アカウント・リポジトリの選択などが含まれます。具体的にいうと、認証や役割ベースの許可を含むアプリケーション・セキュリティーも、管理セキュリティーをアクティブにするまでは適用されません。管理セキュリティーは、デフォルトで使用可能になっています。

管理セキュリティー構成は、セキュリティー・ドメイン内のすべてのサーバーに適用されます。

- アプリケーション・セキュリティー は、環境内のアプリケーションに対するセキュリティーを使用可能にします。このタイプのセキュリティーは、各アプリケーションを個別に管理して、アプリケーション・ユーザーの認証を要求します。



WebSphere Process Server の管理セキュリティーはデフォルトで有効になっています。アプリケーション・セキュリティーも、デフォルトで使用可能になっています。アプリケーション・セキュリティーは、管理セキュリティーが使用可能である場合にのみ有効になります。

- **Java 2 セキュリティー** は、保護された特定のシステム・リソースへのアクセスを許可する前にアクセス権限を検査することにより、総合的なシステム保全性を向上する、ポリシー・ベースのきめ細かいアクセス制御メカニズムを提供します。Java 2 セキュリティーは、ファイル入出力、ソケット、プロパティーなどのシステム・リソースへのアクセスを保護します。また、サーブレット、JavaServer Pages (JSP) ファイル、Enterprise JavaBeans (EJB) メソッドなどの Web リソースへのアクセスも保護します。

Java 2 セキュリティーは比較的新しいテクノロジーであるため、既存または新規の多くのアプリケーションは、Java 2 セキュリティーが提供する非常に細分化されたアクセス制御プログラミング・モデルに対応していない可能性があります。管理者は、アプリケーションが Java 2 セキュリティーに対応していない場合に、Java 2 セキュリティーを使用可能にするるとどのような結果となる可能性があるかを認識しておく必要があります。Java 2 セキュリティーを導入すると、アプリケーション開発者および管理者は、新規の要件にも従う必要があります。

**重要:** Software Development Kit (SDK) に対する更新が含まれるフィックスパックによって、制限されていないポリシー・ファイルが上書きされる可能性があります。フィックスパックを適用する前に、制限されていないポリシー・ファイルをバックアップし、フィックスパックを適用してから、バックアップしたポリシー・ファイルを再び適用してください。

## 手順

### 手順

1. 管理コンソールで「管理セキュリティー」ページを開きます。

「セキュリティー」を展開して、「グローバル・セキュリティー」をクリックします。

2. 管理セキュリティーを使用可能にします。

「管理セキュリティーを使用可能にする」を選択します。

3. アプリケーション・セキュリティーを使用可能にします。

「アプリケーション・セキュリティーを使用可能にする」を選択します。

4. オプション: 必要な場合は、Java 2 セキュリティーを強制します。

「Java 2 セキュリティーを使用してアプリケーションのアクセスをローカル・リソースに制限する」を選択して、Java 2 セキュリティー権限検査を強制します。

Java 2 セキュリティーを使用可能にすると、デフォルト・ポリシーで付与されているよりも多くの Java 2 セキュリティー権限を必要とするアプリケーションは、必要なアクセス権がアプリケーションの `app.policy` ファイルまたは `was.policy` ファイルのいずれかで付与されるまで正常に実行できないことがあります。アクセス制御例外は、必要なすべての権限が与えられていないアプリケ

ーションによって生成されます。Java 2 セキュリティーについて詳しくは、WebSphere Application Server インフォメーション・センターの『Java 2 セキュリティー・ポリシー・ファイルの構成』のトピックを参照してください。

**注:** app.policy ファイルへの更新は、その app.policy ファイルが属しているノード上のエンタープライズ・アプリケーションにのみ適用されます。

- a. オプション: 「**アプリケーションがカスタム許可を認可されたときに警告する**」を選択します。 filter.policy ファイルには、J2EE 1.4 仕様によりアプリケーションに対して与えてはならないと規定されている許可のリストが格納されています。このオプションを使用可能にすると、インストールされたアプリケーションに対してこのポリシー・ファイル内で指定された許可が認可されている場合は、警告が発行されます。デフォルトは使用可能です。
  - b. オプション: 「**リソース認証データに対するアクセスの制限**」を選択します。Java コネクター・アーキテクチャー (JCA) マッピングの機密認証データに対するアプリケーションのアクセスを制限する必要がある場合は、このオプションを使用可能にします。
5. 以上の変更内容を適用します。

ページの下部の「**適用**」ボタンをクリックします。

6. ローカル構成へ変更内容を保管します。

メッセージ・ペインの「**保管**」をクリックします。

7. 必要な場合は、サーバーを停止して再始動します。

サーバーが再始動される必要がある場合は、その旨のメッセージが管理コンソールに表示されます。

## 次のタスク

作成したプロファイルごとに、管理セキュリティを有効にする必要があります。

## ユーザー・アカウント・リポジトリの構成

登録済みユーザーのユーザー名とパスワードは、ユーザー・アカウント・リポジトリに保管されます。ローカルのオペレーティング・システムのユーザー・アカウント・リポジトリ (デフォルト)、Lightweight Directory Access Protocol (LDAP)、統合リポジトリ、またはカスタム・アカウント・リポジトリのいずれかを使用することができます。

### このタスクについて

ユーザー・アカウント・リポジトリとは、認証メカニズムが認証を実行する際に照会するユーザーおよびグループのレジストリーのことです。管理コンソールでユーザー・アカウント・リポジトリを選択します。

**注:** Network Deployment 環境の場合、LDAP または現在のローカル・オペレーティング・システムのいずれかをユーザー・レジストリーとして使用することができます。

### 手順

## 手順

1. 管理コンソールの「管理、アプリケーション、インフラストラクチャーの保護」パネルにナビゲートします。「セキュリティ」を展開して、「グローバル・セキュリティ」をクリックします。
2. 使用するユーザー・レジストリーを選択します。

次の表に、ユーザー・レジストリーの選択およびユーザー・レジストリーの選択と構成に必要なアクションを示します。

ユーザー・レジストリー	アクション
統合リポジトリー	<p>この設定は、1 つのレルムの下で複数のリポジトリー内のプロファイルを管理するために指定します。レルムには、以下のリポジトリー内の ID を含めることができます。</p> <ul style="list-style-type: none"> <li>• システムに組み込まれているファイル・ベース・リポジトリー</li> <li>• 1 つ以上の外部リポジトリー</li> <li>• 組み込まれたファイル・ベース・リポジトリーと 1 つ以上の外部リポジトリーの両方</li> </ul> <p><b>注:</b> 統合リポジトリー構成を表示できるのは、管理者特権を持つユーザーのみです。詳しくは、フェデレーテッド・リポジトリー構成におけるレルムの管理を参照してください。</p>
ローカル・オペレーティング・システム	<p>これはデフォルトのユーザー・レジストリーです。</p> <p>10 ページの『ローカルのオペレーティング・システムまたはスタンドアロンのカスタム・ユーザー・アカウント・リポジトリーの構成』の手順を実行します。</p>
Lightweight Directory Access Protocol (LDAP)	<p>12 ページの『ユーザー・レジストリーとしての Lightweight Directory Access Protocol (LDAP) の構成』の説明に従って、ユーザー・レジストリーとして LDAP を構成してください。</p>
カスタム・ユーザー・レジストリー	<p>10 ページの『ローカルのオペレーティング・システムまたはスタンドアロンのカスタム・ユーザー・アカウント・リポジトリーの構成』の説明に従い、カスタム・アカウント・リポジトリーを選択して、各自のニーズに応じて構成します。</p>
Tivoli Access Manager	<p><b>注:</b> このオプションは、管理コンソールからは使用できません。wsadmin コマンドを使用して構成する必要があります。</p>

## ローカルのオペレーティング・システムまたはスタンドアロンのカスタム・ユーザー・アカウント・リポジトリの構成

管理コンソールを使用して、ユーザー・アカウント・リポジトリを構成できます。ローカルのオペレーティング・システムを構成する手順 (デフォルト) と、スタンドアロンのカスタム・ユーザー・アカウント・レジストリーを構成する手順は似ています。

### このタスクについて

WebSphere Process Server にサーバー・ユーザー ID を自動的に生成させることができます。使用しているユーザー・アカウント・リポジトリからユーザー ID を指定することもできます。後者を選択すると、管理アクションをより正確に監査できるようになります。

WebSphere Process Server for z/OS のユーザー・レジストリーとして LDAP を使用する場合、管理コンソールを使用してセキュリティーを管理します。ユーザー・レジストリーにオペレーティング・システムを使用する場合は、System Authorization Facility を使用してセキュリティーを許可します。

### 手順

#### 手順

1. 管理コンソールで、ユーザー・レジストリーの構成ページを開きます。

「セキュリティー」を展開して「グローバル・セキュリティー」をクリックし、「使用可能なレルム定義」メニューで、使用しているユーザー・レジストリーを選択します。「構成」をクリックします。

2. オプション: 「1 次管理ユーザー名」フィールドに有効なユーザー名を入力します。

この値は、管理特権を持ち、レジストリー内で定義されているユーザーの名前です。このユーザー名は、管理コンソールへのアクセスに使用されます。また、**wsadmin** コマンドでも使用されます。

3. 「自動的に生成されたサーバー ID」または「リポジトリに保管されたサーバー ID」のいずれかのオプションを選択します。

- 「自動的に生成されたサーバー ID (Automatically generated server identity)」を選択すると、内部プロセス通信に使用されるサーバー ID がアプリケーション・サーバーによって生成されます。

このサーバー ID は、「認証メカニズムと有効期限」ページで変更することができます。「認証メカニズムと有効期限」ページにアクセスするには、「セキュリティー」 > 「グローバル・セキュリティー」 > 「認証メカニズムと有効期限」をクリックします。「内部サーバー ID」フィールドの値を変更します。

- 「リポジトリに保管されたサーバー ID」オプションを選択する場合は、以下の情報を入力します。

- 「バージョン 7.0 ノード上のサーバー・ユーザー ID または管理ユーザー (Server user ID or administrative user on a Version 7.0 node)」に、セキュリティ目的でアプリケーション・サーバーの実行に使用されるユーザー ID を指定します。
  - 「パスワード」に、このユーザーに関連付けるパスワードを指定します。
4. オプション: スタンドアロン・カスタム・レジストリーの場合は、以下の手順を実行します。
    - a. 「カスタム・レジストリー・クラス名 (Custom registry class name)」の値が正しいことを確認し、必要に応じて変更します。
    - b. 「認証で大/小文字を無視する (Ignore case for authentication)」のチェック・マークを外します。

このオプションを選択すると、許可検査で大文字と小文字が区別されなくなります。
  5. 「適用」をクリックします。
  6. ページの下部の「現行として設定 (Set as current)」をクリックします。
  7. 「OK」をクリックして、「適用」または「保管」をクリックします。

## 次のタスク

更新が有効になるよう、すべてのサーバーを保管して停止してから再起動します。

サーバーが問題なく始動する場合は、正しくセットアップされています。

## Tivoli Access Manager をユーザー・アカウント・リポジトリーとして使用するための WebSphere Process Server の構成

Tivoli Access Manager をユーザー・アカウント・リポジトリーとして使用できますが、管理コンソールではなく `wsadmin` コマンドを使用して構成する必要があります。

### このタスクについて

Tivoli Access Manager をユーザー・アカウント・リポジトリーとして使用できません。管理コンソールでは構成できないため、`wsadmin` コマンドを使用する必要があります。WebSphere Application Server インフォメーション・センターのトピック『JACC プロバイダーへのインストール済みアプリケーションのセキュリティー・ポリシーの `wsadmin` スクリプトを使用した伝搬』を参照してください。

## ユーザー・レジストリーとしての Lightweight Directory Access Protocol (LDAP) の構成

デフォルトのユーザー・レジストリーは、ローカル・オペレーティング・システムのレジストリーです。外部の Lightweight Directory Access Protocol (LDAP) も、ユーザー・レジストリーとして使用することができます。

### 始める前に

このタスクは、管理 セキュリティーがオンになっていることを前提としています。

LDAP を使用してユーザー・レジストリーにアクセスするには、有効なユーザー名 (ID) とパスワード、レジストリー・サーバーのサーバー・ホストとポート、基本識別名 (DN)、必要に応じてバインド DN とバインド・パスワードが必要です。

検索可能なユーザー・レジストリーから、任意の有効なユーザーを選択することができます。管理ロールを持つ任意のユーザー ID を使用してログオンできます。

**重要:** 複数の LDAP サーバーを使用するように WebSphere Process Server を構成した場合、管理コンソールの「グローバル・セキュリティ」 > 「スタンドアロン LDAP レジストリー」ページに示される値は、使用されている LDAP サーバーを反映していない可能性があります。

## 手順

### 手順

1. 管理コンソールを始動します。
  - セキュリティーが現在無効になっている場合は、ユーザー ID の入力画面が表示されます。入力画面が表示されたら、任意のユーザー ID を入力してログインします。
  - セキュリティーが現在有効になっている場合は、ユーザー ID とパスワードの入力画面が表示されます。入力画面が表示されたら、事前に定義された管理ユーザー ID とパスワードを入力してログインします。
2. 「セキュリティ」を展開して、「グローバル・セキュリティ」をクリックします。
3. 「管理、アプリケーション、およびインフラストラクチャーの保護 (Secure administration, applications, and infrastructure)」ページで、以下の手順を実行します。
  - a. 「管理セキュリティを使用可能にする」が選択されていることを確認します。
  - b. 「使用可能なレルム定義 (Available realm Definitions)」リストから、「スタンドアロン LDAP レジストリー」を選択します。
  - c. 「構成」をクリックします。
4. 「スタンドアロン LDAP レジストリー」ページの「構成」タブで、以下の手順を実行します。
  - a. 「1 次管理ユーザー名」フィールドに有効なユーザー名を入力します。

この値は、管理特権を持ち、レジストリー内で定義されているユーザーの名前です。このユーザー名は、管理コンソールへのアクセスに使用されます。また、`wsadmin` コマンドでも使用されます。

「拡張 LDAP 設定」ページのユーザー・フィルターで定義されているとおり、ユーザーの完全な識別名 (DN) またはユーザーの短縮名を入力します。

- b. オプション: 「自動的に生成されたサーバー ID」または「リポジトリーに保管されたサーバー ID」のいずれかのオプションを選択します。
  - 「自動的に生成されたサーバー ID (Automatically generated server identity)」を選択すると、内部プロセス通信に使用されるサーバー ID がアプリケーション・サーバーによって生成されます。



このサーバー ID は、「認証メカニズムと有効期限」ページで変更することができます。「認証メカニズムと有効期限」ページにアクセスするには、「セキュリティ」 > 「グローバル・セキュリティ」 > 「認証メカニズムと有効期限」をクリックします。「内部サーバー ID」フィールドの値を変更します。

- 「リポジトリに保管されたサーバー ID」オプションを選択する場合は、以下の情報を入力します。
  - 「バージョン 7.0 ノード上のサーバー・ユーザー ID または管理ユーザー (Server user ID or administrative user on a Version 7.0 node)」に、セキュリティ目的でアプリケーション・サーバーの実行に使用されるユーザー ID を指定します。
  - 「パスワード」に、このユーザーに関連付けるパスワードを指定します。

この ID は LDAP 管理者ユーザー ID ではありませんが、この項目は LDAP に存在している必要があります。

- c. オプション: 「LDAP サーバーのタイプ (Type of LDAP server)」リストから、LDAP サーバーを選択します。

LDAP サーバーのタイプにより、WebSphere Process Server で使用されるデフォルト・フィルターが決まります。これらのデフォルト・フィルターにより、「LDAP サーバーのタイプ (Type of LDAP server)」フィールドが「カスタム」に変更されます。これは、カスタム・フィールドが使用されるという意味です。このアクションは、「拡張 LDAP 設定」ページで「OK」または「適用」をクリックすると発生します。他の LDAP サーバーを使用するには、リストから「カスタム」タイプを選択し、必要に応じてユーザー・フィルターとグループ・フィルターを変更します。

IBM Tivoli Directory Server ユーザーの場合、ディレクトリー・タイプとして **IBM Tivoli Directory Server** を選択することができます。IBM Tivoli Directory Server ディレクトリー・タイプを使用すると、パフォーマンスが向上します。

- d. 「ホスト」フィールドに、LDAP が常駐するコンピューターの完全修飾名を入力します。

IP アドレスまたはドメイン・ネーム・システム (DNS) 名のいずれかを入力します。

- e. オプション: 「ポート」フィールドに、LDAP サーバーが listen するポート番号を入力します。

ホスト名とポート番号は、WebSphere Process Server セル内の LDAP サーバーのレルムを表します。そのため、異なるセルに存在するサーバーが Lightweight Third Party Authentication (LTPA) トークンを使用して相互に通信する場合は、これらのレルムはすべてのセルで正確に一致する必要があります。

デフォルト値は 389 です。

複数の WebSphere Process Server がインストールされ、同一のシングル・サインオン・ドメインで実行するように構成されている場合、または WebSphere Process Server を WebSphere Process Server の旧バージョンと相互運用する場合は、ポート番号がすべての構成で一致していることを確認してください。

- f. オプション: 「**基本識別名 (DN)**」フィールドに基本識別名を入力します。

基本識別名は、この LDAP ディレクトリー・サーバーにおける LDAP 検索の開始点を示します。例えば、DN に `cn=John Doe, ou=Rochester, o=IBM, c=US` が設定されているユーザーの場合、基本 DN を以下のいずれかのオプションとして指定します (サフィックス `c=us` を想定): `ou=Rochester, o=IBM, c=us`、あるいは `o=IBM c=us` または `c=us`。

許可検査用に、このフィールドでは大文字と小文字が区別されます。そのため、別のセルや Lotus Domino サーバーなどからトークンを受け取った場合に、サーバー内の基本識別名 (DN) が別のセルまたは Lotus Domino サーバーの基本 DN と正確に一致する必要があります。許可検査の際に大文字と小文字を区別する必要がない場合は、「許可検査で大/小文字を区別しない」を有効にしてください。

WebSphere Process Server の場合、識別名は Lightweight Directory Access Protocol (LDAP) 仕様に従って正規化されます。正規化は、基本識別名のコンマおよび等号の前後のスペースを取り除くことによって行われます。`o = ibm, c = us` や `o=ibm, c=us` は、正規化されていない識別名の例です。`o=ibm,c=us` は、正規化された識別名の例です。

このフィールドは、(このフィールドがオプションになっている) Lotus Domino Directory の場合を除き、すべての LDAP ディレクトリーで必須です。

- g. オプション: 「**バインド識別名 (Bind distinguished name)**」フィールドにバインド DN 名を入力します。

ユーザー情報とグループ情報を取得する際に LDAP サーバー上で匿名バインドが使用できない場合は、バインド DN が必要です。

匿名バインドを使用するように LDAP サーバーがセットアップされている場合、このフィールドには何も入力しないでください。名前を指定しない場合、アプリケーション・サーバーは匿名でバインドを行います。識別名の例については、「基本識別名」フィールドの説明を参照してください。

- h. オプション: 「**バインド・パスワード**」フィールドに、バインド DN に対応するパスワードを入力します。  
i. オプション: 「**検索タイムアウト (Search time out)**」の値を変更します。

このタイムアウト値は、LDAP サーバーが応答を製品クライアントに送信する際に待機する最大時間です。この時間を超えると、要求が停止されます。デフォルトは 120 秒です。

- j. 「**接続の再利用**」が選択されていることを確認します。



このオプションにより、サーバーが LDAP 接続を再利用するかどうかを指定します。このオプションをクリアするのは、ルーターを使用して要求を複数の LDAP サーバーに送信する場合に、そのルーターがアフィニティーをサポートしていない場合 (ほとんどありません) だけです。それ以外の場合は、このオプションを選択したままにしておきます。

- k. オプション: 「許可検査で大/小文字を区別しない」が有効になっていることを確認します。

このオプションを有効にすると、許可検査で大文字と小文字が区別されなくなります。

通常、許可検査には、ユーザーの完全な DN (LDAP サーバー内で固有であり、大文字と小文字が区別される) の検査も含まれます。ただし、IBM Directory Server または Sun ONE (以前の iPlanet) Directory Server LDAP サーバーを使用する場合は、LDAP サーバーから取得されるグループ情報に大文字と小文字の不整合があるため、このオプションを有効にする必要があります。この不整合の影響を受けるのは、許可検査だけです。それ以外の場合、このフィールドは任意で指定します。大文字と小文字を区別する許可検査が必要な場合は、有効に設定します。

例えば、証明書を使用する際に、証明書の内容が LDAP サーバー項目の大文字/小文字と一致しない場合に、このオプションを選択します。製品と Lotus Domino 間でシングル・サインオン (SSO) を使用する場合も、「許可検査で大/小文字を区別しない」を有効にします。

デフォルトは使用可能です。

- l. オプション: LDAP サーバーで Secure Sockets Layer (SSL) 通信を使用する場合は、「SSL 使用可能」を選択します。

「SSL 使用可能」オプションを選択すると、「中央管理対象」または「特定の SSL 別名を使用する (Use specific SSL alias)」を選択できます。

- **中央管理対象**

このオプションを使用すると、特定のスコープ (1 つのロケーションのセル、ノード、サーバー、またはクラスターなど) に SSL 構成を指定することができます。「中央管理対象」オプションを使用するには、エンドポイントの特定のセットに SSL 構成を指定する必要があります。

「エンドポイント・セキュリティー構成の管理」ページには、SSL プロトコルを使用するすべてのインバウンド・エンドポイントとアウトバウンド・エンドポイントが表示されます。

「エンドポイント・セキュリティー構成の管理」ページの「インバウンド (Inbound)」セクションまたは「アウトバウンド (Outbound)」セクションを展開してノードの名前をクリックし、そのノード上のすべてのエンドポイントに使用される SSL 構成を指定します。LDAP レジストリーの場合、LDAP の SSL 構成を指定することにより、継承された SSL 構成をオーバーライドすることができます。

- **特定の SSL 別名を使用する**

このオプションは、オプションの下にあるリスト内のいずれかの SSL 構成を選択する場合に使用されます。

この構成が使用されるのは、LDAP で SSL が有効になっている場合だけです。デフォルトは **NodeDefaultSSLSettings** です。

- m. 「OK」をクリックし、「適用」または「保管」をクリックして、「管理、アプリケーション、およびインフラストラクチャーの保護 (Secure administration, applications, and infrastructure)」ページに戻ります。
5. 「管理、アプリケーション、およびインフラストラクチャーの保護 (Secure administration, applications, and infrastructure)」ページで、「現行として設定 (Set as current)」をクリックします。
6. 「OK」をクリックして、「適用」または「保管」をクリックします。

### 次のタスク

更新が有効になるよう、すべてのサーバーを保管して停止してから再起動します。

サーバーが問題なく始動する場合は、正しくセットアップされています。

## サーバーの始動と停止

管理セキュリティが有効な場合、サーバーをシャットダウンするには、適切なユーザー名とパスワードを入力する必要があります。サーバーは認証なしで始動されますが、管理コンソールにアクセスするためには、認証が必要です。

### 始める前に

管理セキュリティが有効である必要があります。

**問題の回避:** **Vista** **Windows 7** ユーザー・アカウント制御 (UAC) がいくつかのレベルで有効になっている場合、コマンド・プロンプトからアプリケーション・サーバーを始動するときには、管理者権限を使用する必要があります。以下の操作を実行してコマンド・プロンプト・ウィンドウを起動して、アプリケーション・サーバーを始動します。

- コマンド・プロンプトのショートカットを右クリックします。
- 「管理者として実行 (Run As Administrator)」をクリックします。
- コマンド・プロンプト・ウィンドウを管理者として開くと、続行するかどうかをたずねるオペレーティング・システム・ダイアログが表示されます。「続行」をクリックして、操作を続行します。

### 手順

#### 手順

1. サーバーを始動します。 コマンド・プロンプトの `/AppServer/bin` ディレクトリで、次のテキストをコマンド行から入力します。 **startServer.sh**  
`servername`

**注:** サーバーを始動するために、ユーザー名とパスワードを入力する必要はありません。ただし、管理コンソールの起動またはその他の管理操作を実行するに

は、認証を受ける必要があります。  
サーバーが始動するか、エラー・メッセージが返されます。

2. サーバーを停止します。 コマンド・プロンプトの `/AppServer/bin` ディレクトリで、次のテキストを入力します。 **stopServer.sh servername -username username -password password**

**注:** サーバーを停止するには、ユーザー名とパスワードを入力する必要があります。  
入力したユーザー名とパスワードがオペレーター・ロールまたは管理者ロールのメンバーの場合は、サーバーが停止します。

3. サーバーが正常に停止したことを確認します。

入力した要求の結果は、要求を入力したコマンド・ウィンドウに表示されます。

## 管理セキュリティ・ロール

いくつかの管理セキュリティ・ロールが、WebSphere Process Server インストール済み環境の一部として提供されます。

管理コンソールの一部として 8 つのロールが提供されます。これらのロールは、管理コンソール上の機能の範囲にアクセス権を付与します。管理セキュリティが使用可能になっている場合、ユーザーは管理コンソールにアクセスするためにこれらのロールの 1 つにマップされる必要があります。

インストール後にサーバーに最初にログインするユーザーは、管理者ロールに追加されます。

表 2. 管理セキュリティ・ロール

管理セキュリティ・ロール	説明
モニター	モニター・ロールのメンバーは、WebSphere Process Server 構成およびサーバーの現在の状態を表示することができます。
コンフィギュレーター	コンフィギュレーター・ロールのメンバーは、WebSphere Process Server 構成を編集することができます。
オペレーター	オペレーター・ロールのメンバーは、モニター特権に加えてランタイム状態の変更 (つまりサーバーの始動および停止) の権限を持ちます。
管理者	管理者ロールに限り、コンフィギュレーター・ロールとオペレーター・ロールの組み合わせに加えて、追加の特権が付与されます。例えば、これらの特権には以下のものがあります。 <ul style="list-style-type: none"><li>• サーバーのユーザー ID とパスワードの変更</li><li>• ユーザーとグループの管理者ロールへのマッピング</li></ul> 管理者には、以下のような機密情報へのアクセスに必要な権限もあります。 <ul style="list-style-type: none"><li>• Lightweight Third Party Authentication (LTPA) のパスワード</li><li>• キー</li></ul>

表 2. 管理セキュリティ・ロール (続き)

管理セキュリティ・ロール	説明
ISC 管理	このロールを使用できるのは管理コンソールのユーザーのみであり、 <b>wsadmin</b> ユーザーは対象外です。このロールを付与されたユーザーは、統合リポジトリ内でユーザーおよびグループを管理するための管理者特権を持ちます。例えば、ISC 管理 (ISC Admins) ロールのユーザーは、以下のタスクを実行できます。 <ul style="list-style-type: none"> <li>フェデレーテッド・リポジトリ構成でのユーザーの作成、更新、または削除</li> <li>フェデレーテッド・リポジトリ構成でのグループの作成、更新、または削除</li> </ul>
デプロイヤー	このロールを付与されたユーザーが、アプリケーションに対して構成アクションとランタイム操作の両方を実行できます。
セキュリティ・マネージャーの管理	このロールを付与されたユーザーのみが、ユーザーを管理の役割にマップできます。また、細分化された管理セキュリティを使用している場合は、このロールを付与されたユーザーのみが、許可グループを管理できます。
監査員	このロールを与えられたユーザーは、セキュリティ監査サブシステムの構成設定を表示および変更できます。 <b>注:</b> 監査員ロールには、モニター・ロールが含まれていません。このため、監査員は残りのセキュリティ構成を表示できますが、変更することはできません。

詳しくは、WebSphere Application Server インフォメーション・センターの管理ロールを参照してください。

管理セキュリティを使用可能にした際に指定されたサーバーの ID は自動的に管理者ロールにマップされます。ユーザーまたはグループは、WebSphere Process Server の管理コンソールを使用して、随時管理の役割に追加したり、管理の役割から除去したりすることができます。ただし、これらの変更を有効にするには、サーバーの再始動が必要です。

**ヒント:** 管理の役割に特定のユーザーではなく、1 つのグループまたは複数のグループをマップします。これは、管理がより柔軟で容易になるためです。1 つのグループを管理の役割にマップすることによって、ユーザーのグループへの追加またはグループからの除去が、WebSphere Process Server の外部で実行されるため、変更を有効にするためのサーバーの再始動は不要になります。

失敗したイベント・マネージャーは、管理者またはオペレーターの役割のいずれかが付与されているあらゆるユーザーが操作できます。

セレクターは、管理者またはコンフィギュレーターの役割のいずれかが付与されているあらゆるユーザーが構成できます。

ユーザーまたはグループのマッピングに加えて、特別対象も管理の役割にマップすることができます。特別対象とは、特定クラスのユーザーを一般化したものです。

- 全認証者特別対象とは、管理の役割のアクセス検査によって、要求を出しているユーザーが少なくとも認証されることを意味します。
- 全員特別対象とは、認証されているか否かに関係なく、セキュリティーが使用可能になっていない場合と同様に、すべてのユーザーがアクションを実行できることを意味します。

---

## WebSphere Process Server におけるアプリケーションの保護

ご使用の WebSphere Process Server インスタンスにデプロイするアプリケーションは、それらに組み込まれて実行時に適用されるセキュリティーを必要とします。

### このタスクについて

WebSphere Process Server 環境でホストされるアプリケーションは、ビジネスに不可欠なさまざまな機能を実行しますが、これらの機能にはセキュリティーが必要です。一部のアプリケーションは、機密情報 (給与計算情報やクレジット・カードの詳細情報など) へアクセスしたり、これらの情報の転送や変更を行います。また他のアプリケーションでは、請求書作成発行や在庫管理が実行されます。これらのアプリケーションのセキュリティーはきわめて重要です。

以下を実行して、お客様のアプリケーションを保護します。

#### 手順

#### 手順

1. 管理セキュリティーが使用可能であることを確認します。
2. アプリケーション・セキュリティーが使用可能であることを確認します。
  - a. 管理コンソールで「セキュリティー」を展開して、「グローバル・セキュリティー」をクリックします。
  - b. 「アプリケーション・セキュリティーを使用可能にする」を選択すると、WebSphere Process Server は、保護されたアプリケーションにアクセスしようとするユーザーの認証を要求します。
3. すべての適切なセキュリティー機能を使用して、WebSphere Integration Developer においてアプリケーションを開発します。
4. ユーザーまたはグループを適切なセキュリティー・ロールに割り当て、現在の WebSphere Process Server 環境にアプリケーションをデプロイします。
5. ご使用の WebSphere Process Server 環境のセキュリティーを維持管理します。

## アプリケーション・セキュリティーの要素

WebSphere Process Server で実行されるアプリケーションは、認証およびアクセス制御によって保護されます。また、アプリケーションの呼び出し中に転送されるデータは、さまざまなメカニズムによって保護されます。これらのメカニズムにより、転送中のデータの読み取りや変更は不可能になります。セキュリティーの最後の要素は、ユーザーがユーザー名とパスワードを何度も入力する必要がないようにするための、さまざまなシステムを経由するセキュリティー情報の伝搬です。

WebSphere Process Server のセキュリティーは以下の 3 つのグループに大別されます。

- アプリケーション・セキュリティ
- データの保全性とプライバシー
- ID の伝搬

## アプリケーション・セキュリティ

ご使用の WebSphere Process Server アプリケーションのセキュリティは、以下の 2 つの方法で維持されます。

- 認証

アプリケーションを使用するユーザーは、ユーザー・レジストリーのユーザー名とパスワードを入力する必要があります。

- アクセス制御

ユーザーは、アプリケーションを呼び出すためのアクセス権を持っている必要があります。各ロールは、アプリケーションの呼び出しに関連付けられます。認証済みユーザーは適切なロールのメンバーである必要があります、そうでない場合はアプリケーションは実行されません。

## データの保全性とプライバシー

アプリケーションによりアクセスされるデータは、以下のように転送元と転送先において、および転送中に保護されます。

- 保全性

ネットワーク上で送信されるデータを、転送中に変更することはできません。

- プライバシー/機密性

ネットワーク上で送信されるデータを、転送中に傍受したり読み取ることはできません。

## ID の伝搬

セキュリティの最後の要素は ID の伝搬で、これはシングル・サインオンによって実現されます。

クライアント要求が企業内の数種類のシステムを経由する必要がある場合、クライアントは認証データの複数回の入力を強制されません。シングル・サインオン方式は認証情報を下流のシステムに伝搬するために使用され、下流のシステム側ではこの情報を基にアクセス制御を適用できます。

## ユーザーの認証

管理セキュリティがオンになっている場合は、クライアントは認証される必要があります。

クライアントが、認証されていない状態で保護されたアプリケーションにアクセスしようとする、例外が生成されます。



表3 に、WebSphere Process Server コンポーネントを呼び出す一般的なクライアントと、クライアントのタイプごとに利用可能な認証オプションを示します。

表3. さまざまなクライアント用の認証オプション

クライアント	認証オプション	注
Web サービス・クライアント	WS-Security/SOAP 認証を使用できます。	
Web クライアントまたは HTTP クライアント	HTTP 基本認証 (ブラウザがクライアントにユーザー名とパスワードを求めるプロンプトを表示します)。	これらのクライアントは、JSP、 Servlet、 および HTML 文書を参照します。
Java クライアント	JAAS。	
すべてのクライアント	SSL クライアント認証。	

WebSphere Process Server インフラストラクチャーのコンポーネントの中には、データベースおよびメッセージング・エンジンにアクセスする場合のランタイム・コードの認証に使用する、認証別名を持つものがあります。WebSphere Process Server インストーラーは、ユーザー名とパスワードを収集して認証別名を作成します。

一部のランタイム・コンポーネントには、runAs ロールで構成されるメッセージ駆動型 Bean (MDB) が組み込まれています。WebSphere Process Server インストーラーは、runAs ロールのユーザー名とパスワードを収集します。

#### デフォルトの認証別名:

WebSphere Process Server の数種類のコンポーネントは、定義済みの別名を使用してメッセージング・エンジンとデータベースで認証します。該当する応答ファイルのユーザー名とパスワードが、これらの別名に関連付けられます。

#### **Business Process Choreographer の認証別名:**

ビジネス・プロセスには認証別名が事前定義されています。これらの別名は、管理コンソールを使用して変更します。

表4 に示した別名は、呼び出すユーザーの ID に関係なく、コンポーネントを呼び出すために使用されます。

表4. ビジネス・プロセスに関連付けられた認証別名

別名	説明	情報
BPEAuthDataAliasJMS_node_server	メッセージング・エンジンで認証するために使用します。	応答ファイルの該当する Business Process Choreographer プロパティにユーザー名とパスワードを入力します。
BPEAuthDataAliasDbType_node_server	データベースで認証するために使用します。	提供されるスクリプトを使用してデータベースを構成します。

36 ページの表5 は、ビジネス・プロセス用に作成された RunAs ロールについて説明しています。

表 5. ビジネス・プロセスに関連付けられた RunAs ロール

RunAs ロール	説明	情報
JMSAPIUser	bpecontainer.ear の BFM JMS API MDB によって使用されます。	応答ファイルの該当する Business Process Choreographer プロパティにユーザー名とパスワードを入力します。
EscalationUser	task.ear MDB によって使用されます。	応答ファイルの該当する Business Process Choreographer プロパティにユーザー名とパスワードを入力します。

入力したユーザー名は、RunAs ロールに追加されます。

**Common Event Infrastructure 認証別名:**

Common Event Infrastructure には、定義済みの認証別名があります。これらの別名は、管理コンソールを使用して変更します。

表 6 に示した別名は、呼び出すユーザーの ID に関係なく、コンポーネントを呼び出すために使用されます。

表 6. Common Event Infrastructure に関連付けられた認証別名

別名	説明	情報
CommonEventInfrastructure JMSAuthAlias 注: 実際の別名には、この文字スペースは含まれていません。	メッセージング・エンジンで認証するために使用します。	応答ファイルの該当する Common Event Infrastructure 構成プロパティにユーザー名とパスワードの値を入力します。
EventAuthAliasDBType	データベースで認証するために使用します。	応答ファイルの該当する Common Event Infrastructure 構成プロパティにユーザー名とパスワードの値を入力します。

**サービス・コンポーネント・アーキテクチャーの認証別名:**

サービス・コンポーネント・アーキテクチャー (SCA) には、定義済みの認証別名があります。これらの別名は、管理コンソールを使用して変更します。

表 7 の別名は、コンポーネントの起動に使用されます。起動ユーザーの ID には関係ありません。

表 7. SCA コンポーネントに関連付けられた認証別名

別名	説明	情報
SCA_Auth_Alias	メッセージング・エンジンで認証するために使用します。	応答ファイルの該当する SCA 構成プロパティにユーザー名とパスワードの値を入力します。

**認証別名の変更:**

場合によっては、既存の認証別名を変更する必要があります。



## このタスクについて

認証別名は、管理コンソールから次のようにして変更します。

### 手順

#### 手順

1. 「ビジネス・インテグレーション認証別名」 ページにアクセスします。

管理コンソールで「**セキュリティ**」を展開して、「**ビジネス・インテグレーション・セキュリティ**」をクリックします。

**注:** このページには、認証別名情報を必要とするさまざまな管理コンソール・ページからもアクセスできます。  
認証別名構成ページが表示されます。

このページには、認証別名、関連するコンポーネント、その別名に関連付けられているユーザー ID、および別名の説明 (オプション) のリストが表示されます。

2. 「**別名**」列の名前をクリックすることにより、変更する認証別名を選択します。

**注:** 場合によっては、「**別名**」列にリンクが表示されないこともあります。その場合は、編集する認証別名に対応する「**選択**」列のチェック・ボックスを選択し、「**編集**」ボタンをクリックします。

3. 別名のプロパティを変更します。

選択した別名の認証別名構成ページで、別名の名前または別名に関連付けられたユーザー ID とパスワードのいずれかを変更できます。また、認証データ・エントリーの説明も変更することができます。

4. 変更内容を確認します。

「**OK**」または「**適用**」のいずれかをクリックします。「ビジネス・インテグレーション認証別名」ページに戻り、「**適用**」をクリックして変更点をマスター構成に適用します。

**注:** Network Deployment インストール済み環境の場合は、変更を別のノードに伝搬するためのファイル同期操作が実行されることを確認してください。

関連情報については、『*セキュリティを適用した WebSphere Process Server プロファイルの拡張*』を参照してください。

## アクセス制御

一般ユーザーを WebSphere Process Server に対して認証する場合、セキュリティ面で重要なことは、考えられるすべての操作をそのユーザーが実行できるようにしないことです。あるユーザーには特定の操作を行うことを許可し、他のユーザーにはそれらの操作を行うことを認めないようにすることを、**アクセス制御**と言います。

開発するコンポーネントに対し、アクセス制御を手配して、コンポーネントを保護することができます。開発時にサービス・コンポーネント・アーキテクチャー修飾

子を使用することにより、コンポーネントのアクセス制御を提供します。詳しくは、WebSphere Integration Developer インフォメーション・センターを参照してください。

一部の WebSphere Process Server コンポーネントは、エンタープライズ・アーカイブ (EAR) ファイルとしてパッケージされ、そのオペレーションを Java EE ロール・ベース・セキュリティーを使用して保護しています。コンポーネントのオペレーションをセキュリティーで保護するコード・ベースのセキュリティーとは対照的に、ロール・ベースのアクセス制御はリソースをセキュリティーで保護します。例えば、ビジネス・カレンダー・ウィジェットでは、個々のタイムテーブルに対してユーザーが持つアクセス権限のタイプを指定できます。

## セキュリティー・ロール・ウィジェット

Business Space 内のセキュリティー・ロール・ウィジェットを使用して、タイムテーブルごとに、そのタイムテーブルの所有者と、そのタイムテーブルに対する作成者アクセス権限および読者アクセス権限を持つユーザーを指定します。

次の表は、管理ロールとそのデフォルトの許可を示します。

ロール	デフォルトの許可
BPMAdmin	1 次管理ユーザー
BPMRoleManager	すべての認証済みユーザー

## EAR ファイルおよび関連ロール

Business Process Choreographer と Common Event Infrastructure は、WebSphere Process Server の一部としてインストールされます。

表 8. WebSphere Process Server に含まれる EAR ファイルおよび関連ロール

.ear ファイルの名前	ロール	デフォルト
BPEContainer_nodeName_serverName.ear	APIUser	すべての認証済み
または	SystemAdministrator	なし
BPEContainer_clusterName	SystemMonitor	なし
	JMSAPIUser	すべての認証済み
	AdminJobUser	すべての認証済み
	JAXWSAPIUser	全員
BPCExplorer_nodeName_serverName.ear	WebClientUser	すべての認証済み
または		
BPCExplorer_clusterName		
BPCArchiveExplorer_nodeName_serverName.ear	WebClientUser	すべての認証済み
または		
BPCArchiveExplorer_clusterName		
BSpaceEAR_nodeName_server.ear	businessspaceusers	すべての認証済み
BSpaceWebformsEnabler_nodeName_server.ear	WebFormUsers	すべての認証済み

表 8. WebSphere Process Server に含まれる EAR ファイルおよび関連ロール (続き)

.ear ファイルの名前	ロール	デフォルト
BusinessRulesManager.ear	BusinessRuleUsers	すべての認証済み
	NoOne	なし
	AnyOne	全員
BusinessRules_nodeName_server.ear	管理者	すべての認証済み
EventService.ear	eventAdministrator	すべての認証済み
	eventConsumer	すべての認証済み
	eventUpdater	すべての認証済み
	eventCreator	すべての認証済み
	catalogAdministrator	すべての認証済み
	catalogReader	すべての認証済み
mm.was_nodeName_server.ear	すべての認証済み	すべての認証済み
	everyone	全員
REST Services Gateway.ear	RestServicesUser	すべての認証済み
REST Services Gateway Dmgr .ear	RestServicesUser	すべての認証済み
TaskContainer_nodeNameserverName.ear または TaskContainer_clusterName	APIUser	すべての認証済み
	SystemAdministrator	なし
	SystemMonitor	なし
	EscalationUser	すべての認証済み
	AdminJobUser	すべての認証済み
	JAXWSAPIUser	全員
wpsFEMgr_7.0.0 Security	WBIOperator	全員

## Business Process Choreographer の Java EE ロール

以下の表に、Business Process Choreographer の Java EE ロールを示します。

表 9. Business Process Choreographer のロール

コンポーネント	ロール	値
BPEContainer	APIUser	すべての認証済みユーザー
	SystemAdministrator	構成時に入力したユーザー名、グループ名、またはその両方
	SystemMonitor	すべての認証済みユーザー
	JMSAPIUser	構成時に入力したユーザー名
	AdminJobUser	構成時に入力したユーザー名
	JAXWSAPIUser	全員
TaskContainer	APIUser	すべての認証済みユーザー
	SystemAdministrator	SystemAdministrator
	SystemMonitor	SystemMonitor
	EscalationUser	EscalationUser
	AdminJobUser	AdminJobUser
	JAXWSAPIUser	全員

## RunAs ロール

また、securityIdentity ロールまたは RunAs ロールを使用するアプリケーションについては、以下ようになります。

表 10. .ear ファイルおよび関連する RunAs ロール

EAR ファイル	J2EE ロール
BPEContainer_nodeNameserverName.ear	JMSAPIUser AdminJobUser
TaskContainer_nodeNameserverName.ear	EscalationUser AdminJobUser

### ビジネス・プロセスとヒューマン・タスクのアプリケーションにおけるアクセス制御:

WebSphere Process Server インストールの一部としてインストールされる Business Process Choreographer は、ロールを使用して実動システムでのユーザーの能力を判別します。

Business Process Choreographer ロールを表 11 に示します。

表 11. ロールおよびデフォルトの許可

ロール	デフォルトの許可	注
システム管理者	構成時に入力されたユーザー名、グループ名、またはその両方	すべてのビジネス・プロセスとすべての操作にアクセス可能。
システム・モニター	すべての認証済みユーザー	読み取り操作にアクセス可能。
JMSAPIUser	構成時に入力されたユーザー名	この単一ユーザー ID に代わってすべての Business Process Choreographer JMS API が実行されます。
EscalationUser	構成時に入力されたユーザー名	Human Task Manager が非同期 API 呼び出しを処理するために使用します。
AdminJobUser	構成時に入力されたユーザー名 注: 指定されたユーザーは、Business Process Choreographer システム管理者ロールのメンバーでなければなりません。	この単一ユーザー ID に代わって管理ジョブ (例えば、クリーンアップ・サービスやビジネス・プロセス・インスタンス・マイグレーションなど) が実行されます。

注: WebClientUser ロールは、Bpcexplorer.ear ファイルに関連付けられており、Business Process Choreographer Explorer にアクセスすることができます。このロールのデフォルト許可は「すべての認証ユーザー」です。

### データの保全性とプライバシー

WebSphere Process Server の各プロセスが呼び出される際にアクセスされるデータのプライバシーおよび保全性は、セキュリティにとって重要です。

データのプライバシーとデータの保全会性は、密接に関連している概念です。詳しくは、WebSphere Application Server Network Deployment インフォメーション・センターを参照してください。

## プライバシー

プライバシーとは、非認証済みユーザーによるデータのインターセプトと読み取りを可能にすべきではないということを表しています。

## 保全会性

保全会性とは、非認証済みユーザーによるデータの変更を可能にすべきではないということを表しています。

## WebSphere Process Server で提供されるソリューション

WebSphere Process Server では、データのプライバシーおよび保全会性のために一般に広く使用されている以下の 2 つのソリューションをサポートしています。

- **Secure Sockets Layer (SSL) プロトコル。** SSL ではハンドシェイクを使用してエンドポイントを認証し、エンドポイントが暗号化と暗号化解除に用いるセッション鍵の生成に使用される情報を交換します。SSL は、同期プロトコルで Point-to-Point 通信に適しています。SSL では、2 つのエンドポイントは SSL セッションの継続期間中、相互に接続を維持することが必要です。
- **WS-Security。** この標準では、Simple Object Access Protocol (SOAP) メッセージの保護のための SOAP 拡張が定義されています。WS-Security では、単一の SOAP メッセージに対して認証、保全会性、およびプライバシーのサポートが追加されます。SSL とは異なり、セッション鍵を設定するためのハンドシェイクはありません。このため、WS-Security は Java Message Service (JMS) 上の SOAP またはサービス統合バス (SIB) 上の SOAP などの非同期環境でのメッセージの保護に適しています。デプロイメントの前に、アプリケーション内で WS-Security デプロイメント記述子を設定できます。

複数のシステムが相互に対話しているビジネス・インテグレーション環境では、通信の一部が非同期になることがあります。このため、ほとんどの場合 WS-Security の方が優れたソリューションです。

### SSL を使用するための Web サービス・クライアントの構成:

Web サービス・クライアントが Secure Sockets Layer (SSL) を使用して Web サービスを呼び出すように構成することができます。

### このタスクについて

SSL を使用する Web サービス Web クライアントを構成する方法について詳しくは、この WebSphere Application Server 技術情報を参照してください。Web サービスの保護の一般的な説明については、WebSphere Application Server のトピック『トランスポート・レベルでの Web サービス・アプリケーションの保護』を参照してください。

## シングル・サインオン

クライアントは、ユーザー名とパスワード情報を一度だけ入力するように要求されます。入力された ID はシステム全体に伝搬されます。

クライアント要求が企業内の複数のシステムを経由する場合、クライアントは一度だけ認証される必要があります。この ID の伝搬という概念は、シングル・サインオン方式を採用することで解決されます。

認証済みコンテキストはダウンストリームの各システムに伝搬され、このコンテキストに基づき各システムはアクセス制御を適用できます。

WebSphere Process Server の各リソースへのアクセス管理およびシングル・サインオン機能を提供するためのリバース・プロキシ・サーバーとして、Tivoli Access Manager WebSEAL または Tivoli Access Manager plug-in for Web サーバーのいずれかを使用することができます。これらのツールの構成方法の詳細は、WebSphere Application Server の資料に記載されています。

## セキュア・アプリケーションのデプロイ (インストール)

セキュリティー制約 (保護されたアプリケーション) を持つアプリケーションのデプロイは、セキュリティー制約なしのアプリケーションのデプロイとほぼ同じです。唯一の違いは、ユーザーとグループを保護されたアプリケーションのロールに割り当てる必要がある場合もあるという点です。なお、この保護されたアプリケーションでは、正しいアクティブ・ユーザー・レジストリーが必要になります。保護されたアプリケーションをインストールする場合は、ロールをアプリケーション内に事前に定義します。代行がアプリケーションで必要な場合は、RunAs ロールも定義し、有効なユーザー名とパスワードを指定する必要があります。

### 始める前に

この作業を実行する前に、アプリケーションが、すべての関連するセキュリティー構成を使用して設計、開発、およびアセンブルされていることを確認します。これらのタスクについて詳しくは、WebSphere Integration Developer インフォメーション・センターを参照してください。以上のような意味では、アプリケーションのデプロイとインストールは同じ作業であるとみなすことができます。

### このタスクについて

保護されたアプリケーションのデプロイに必要なステップの 1 つとして、アプリケーションを構成した際に定義した役割へのユーザーとグループの割り当てがあります。この作業は、「ユーザーまたはグループへのセキュリティー役割のマップ」というステップの一部として完了させます。アセンブリー・ツールを使用した場合、この割り当ては事前に完了している場合があります。その場合、このステップを完了してマッピングを確認することができます。このステップで、新規のユーザーとグループを追加したり、既存の情報を変更したりすることができます。

RunAs ロールがアプリケーションで定義されている場合は、アプリケーションはデプロイメント中に ID セットアップを使用してメソッドを呼び出します。RunAs ロールを使用して、ダウンストリームの呼び出しを実行する ID を指定します。例えば、RunAs ロールがユーザー「bob」に割り当てられ、クライアント「alice」が (代



行設定を使用して) サブレットを呼び出し、このサブレットがエンタープライズ Bean を呼び出す場合は、このエンタープライズ Bean 上のメソッドは ID「bob」を使用して呼び出されます。

デプロイメント・プロセスの一部として、ユーザーの RunAs ロールへの割り当てや変更を行うステップがあります。このステップは「ユーザーへの RunAs ロールのマップ」といいます。代行ポリシーが SpecifiedIdentity に設定されている場合は、このステップを使用して新規ユーザーを RunAs ロールに割り当てるか、または既存のユーザーをこのロールに変更します。

以下に説明するステップは、アプリケーションのインストールおよび既存のアプリケーションの変更の両方に共通です。アプリケーションにロールが含まれている場合は、アプリケーションのインストール中と管理中に、「追加プロパティ」セクションのリンクとして「ユーザーまたはグループへのセキュリティー役割のマップ」リンクが表示されます。

## 手順

### 手順

1. 管理コンソールで「アプリケーション」を展開し、「新規アプリケーションのインストール」をクリックします。

アプリケーションのインストールに必要なステップを、「ユーザーまたはグループへのセキュリティー・ロールのマップ」というステップの前に完了させておきます。

2. ユーザーとグループをロールに割り当てます。
3. RunAs ロールがアプリケーションに存在している場合は、ユーザーを RunAs ロールにマップします。
4. 必要な場合は、「システム ID の正しい使用」をクリックして、RunAs ロールを指定します。

アプリケーションで代行がシステム ID を使用するよう設定されている場合は、このアクションを完了させます。なお、この設定は、エンタープライズ Bean にのみ適用されます。システム ID は、WebSphere Process Server セキュリティー・サーバー ID を使用してダウンストリームのメソッドを呼び出します。この ID は、WebSphere Process Server 内部メソッドへのアクセスにおいて、他の ID よりも多くの特権を持っているため、使用する場合には注意が必要です。この操作は、ページ内にリストされたメソッドが代行にシステム ID をセットアップしていることをデプロイヤーが認識していることを確認し、必要に応じてそれらを訂正するために実行されるものです。変更が必要ない場合は、この操作をスキップしてください。

5. セキュリティー以外の残りの関連ステップを完了させて、アプリケーションのインストールとデプロイを終了します。

## 次のタスク

保護されたアプリケーションをデプロイした後、正しい資格情報を使用してアプリケーション内のリソースにアクセスできることを確認します。例えば、アプリケーションに保護された Web モジュールが含まれている場合は、ロールに割り当てた



ユーザーのみがこのアプリケーションを使用できることを確認します。

## ユーザーのロールへの割り当て

保護されたアプリケーションでは、セキュリティー修飾子の `securityPermission` と `securityIdentity` のいずれかまたは両方が使用されます。これらの修飾子が存在する場合は、アプリケーションとそのセキュリティー機能が正しく動作するようにデプロイメント時に実行する追加のステップがあります。

## 始める前に

この作業は、保護されたアプリケーションを EAR ファイルとして WebSphere Process Server にデプロイする準備ができていることを想定しています。

## このタスクについて

アプリケーションは、メソッドを持つインターフェースを実装します。Service Component Architecture (SCA) 修飾子の `securityPermission` を使用してインターフェース、つまりメソッドを保護することができます。この修飾子を呼び出す場合は、保護されたメソッドを呼び出すアクセス権を持っているロール（「スーパーバイザー」など）を指定します。アプリケーションをデプロイする際、ユーザーを特定のロールに割り当てる機会があります。

`securityIdentity` 修飾子は、WebSphere Application Server の代行に使用される `RunAs` ロールと同じです。この修飾子に関連付けられている値はロールです。このロールは、デプロイメント中に ID にマップされます。`securityIdentity` で保護されたコンポーネントの呼び出しは、アプリケーションを呼び出しているユーザーの ID に関係なく、指定された ID を使用します。

## 手順

### 手順

1. アプリケーションを WebSphere Process Server にデプロイするための指示に従います。詳しくは、モジュールのデプロイを参照してください。
2. 正しいユーザーをロールに関連付けます。

セキュリティー修飾子	実行するアクション
セキュリティー権限	<p>1 ユーザーまたは複数のユーザーを指定されたロールに割り当てます。以下の 4 つの選択項目があります。</p> <ul style="list-style-type: none"> <li>• 全員 - セキュリティーなしと同等です。</li> <li>• 全認証者 - すべての認証済みユーザーがこのロールのメンバーです。</li> <li>• マップされたユーザー - 個々のユーザーがこのロールに追加されます。</li> <li>• マップされたグループ - ユーザーのグループがこのロールに追加されます。</li> </ul> <p>「マップされたグループ」は、ユーザーがグループに追加されると、その結果サーバーを再始動することなくアプリケーションへのアクセス権を取得できるため、最も柔軟な選択項目です。</p>
セキュリティー ID	<p>ロールがマップされる ID の有効なユーザー名とパスワードを指定します。</p>

## ロールとユーザーの割り当てを実装するためのコマンド (System Authorization Facility 指示)

System Authorization Facility (SAF) は、RACF などの外部セキュリティー・マネージャーと通信するときにプログラムが使用できる z/OS インターフェースです。RACF コマンドを使用して、ロールおよびユーザー割り当てを実装できます。

以下の例を使用して、ロールとユーザーの割り当てを実装するために必要な RACF コマンドを構成できます。

```

RDEFINE EJBROLE (optionalSecurityDomain).WebClientUser UACC(READ)
RDEFINE EJBROLE (optionalSecurityDomain).BPEAPIUser UACC(READ)
RDEFINE EJBROLE (optionalSecurityDomain).BPESystemAdministrator UACC(NONE)
PERMIT (optionalSecurityDomain).BPESystemAdministrator CLASS(EJBROLE) ID(WSCFG1) ACCESS(READ)
RDEFINE EJBROLE (optionalSecurityDomain).BPESystemMonitor UACC(NONE)
PERMIT (optionalSecurityDomain).BPESystemMonitor CLASS(EJBROLE) ID(WSCFG1) ACCESS(READ)
RDEFINE EJBROLE (optionalSecurityDomain).JMSAPIUser UACC(READ) APPLDATA(RACFUserIdentity)

RDEFINE EJBROLE (optionalSecurityDomain).AdminJobUser UACC(READ) APPLDATA(RACFUserIdentity)
RDEFINE EJBROLE (optionalSecurityDomain).JAXWSAPIUser UACC(READ)
PERMIT (optionalSecurityDomain).JAXWSAPIUser CLASS(EJBROLE) ID(WSGUEST) ACCESS(READ)

RDEFINE EJBROLE (optionalSecurityDomain).businessspaceusers UACC(READ)

RDEFINE EJBROLE (optionalSecurityDomain).WebFormUsers UACC(READ)

RDEFINE EJBROLE (optionalSecurityDomain).BusinessRuleUsers UACC(READ)
RDEFINE EJBROLE (optionalSecurityDomain).NoOne UACC(NONE)
RDEFINE EJBROLE (optionalSecurityDomain).AnyOne UACC(READ)
PERMIT (optionalSecurityDomain).AnyOne CLASS(EJBROLE) ID(WSGUEST) ACCESS(READ)

RDEFINE EJBROLE (optionalSecurityDomain).Administrator UACC(READ)
RDEFINE EJBROLE (optionalSecurityDomain).RestServicesUser UACC(READ)

RDEFINE EJBROLE (optionalSecurityDomain).TaskAPIUser UACC(READ)
RDEFINE EJBROLE (optionalSecurityDomain).TaskSystemAdministrator UACC(NONE)
PERMIT (optionalSecurityDomain).TaskSystemAdministrator CLASS(EJBROLE) ID(WSCFG1) ACCESS(READ)
RDEFINE EJBROLE (optionalSecurityDomain).TaskSystemMonitor UACC(NONE)
PERMIT (optionalSecurityDomain).TaskSystemMonitor CLASS(EJBROLE) ID(WSCFG1) ACCESS(READ)
RDEFINE EJBROLE (optionalSecurityDomain).EscalationUser UACC(READ) APPLDATA(RACFUserIdentity)

```

```
RDEFINE EJBROLE (optionalSecurityDomain).Allauthenticated UACC(READ)
RDEFINE EJBROLE (optionalSecurityDomain).everyone UACC(READ)
PERMIT (optionalSecurityDomain).everyone CLASS(EJBROLE) ID(WSGUEST) ACCESS(READ)

RDEFINE EJBROLE (optionalSecurityDomain).WBIOperator UACC(READ)
PERMIT (optionalSecurityDomain).WBIOperator CLASS(EJBROLE) ID(WSGUEST) ACCESS(READ)
```

これらのロールによって保護されているアプリケーションを利用するユーザーは、ロールに対する Read アクセス権限を付与されている必要があります。注意すべき重要な点は、無保護のアプリケーションが WebSphere Application Server 非認証ユーザー ID (デフォルトでは WSGUEST) の下で実行されることです。このユーザー ID は通常、RESTRICTED オプション付きで定義されるので、無保護のアプリケーションが、上記の Java EE ロールによって保護されたアプリケーション機能を使用する場合、WSGUEST には、ロールの EVERYONE ユーザー・マッピングに相当するものを実装する関連プロファイルに対する読み取りアクセス権限が与えられていなければなりません。

**注:** SAF ベースの許可を使用する場合、ロールへのユーザーの割り当てには微妙な点があります。EVERYONE アクセスをエミュレートするには、読み取りの UACC 付きで EJBROLE プロファイルを定義する必要があり、WebSphere Application Server 非認証ユーザー ID (デフォルト WSGUEST) に Read アクセス権限が付与されていなければなりません。all 認証アクセスをエミュレートするには、Read の UACC 付きで EJBROLE プロファイルが定義されていなければなりません。詳細については、WebSphere Application Server インフォメーション・センター: System Authorization Facility (SAF) のオペレーティング・システムおよびアプリケーション・レベルに関する考慮事項を参照してください。

securityIdentity ロールまたは RunAs ロールを使用するアプリケーションも、SAF セキュリティー製品用の特別な構成を必要とします。RACF では、これは EJBROLE APPLDATA パラメーターを使用して RACF ユーザー ID (上記の例では RACFUserIdentity) をロールに割り当てることによって行われます。詳細については、WebSphere Application Server インフォメーション・センター: System Authorization Facility (SAF) 代行を参照してください。

## セキュリティー・ロール・ウィジェット

セキュリティー・ロール・ウィジェットでは、ビジネス・カレンダー・ウィジェット内の個々のタイムテーブルへのアクセスを保護する機能が提供されています。セキュリティー・ロール・ウィジェットを使用して、ロールを組織のメンバーに割り当てます。これらのロールによって、タイムテーブルへのアクセス・レベルが決まります。

セキュリティー・ロール・ウィジェットは、ビジネス・カレンダー・ウィジェットのロール・ベースのアクセス制御を管理するために使用しますが、WebSphere によって提供される Business Space に配置されています。

このロール・ベースのアクセス権限は、オープン・スタンダードである XACML (eXtensible Access Control Markup Language) に基づいています。

ビジネス・カレンダー・ウィジェットでセキュリティー・ロール・ウィジェットのロール・ベースのアクセス制御を使用する利点は何でしょうか。

- タイムテーブルの特定のインスタンスへのアクセスを制御できます。

例えば、あるユーザーがそのユーザー自身のタイムテーブルに対してのみアクセスでき、他のユーザーのタイムテーブルを見たり変更したりできないように指定することができます。

- アクセスの制御は、個々のユーザー・レベルではなく、ロール・レベルで行われます。

メンバーをロールにマップします。メンバーがリソースの特定のインスタンスに対して持つアクセス権は、ロールが定義します。

## タイムテーブルに関連付けられたロール

タイムテーブルがインストールされると、そのタイムテーブルに対して所有者、作成者、および読者という 3 つのロールが作成されます。これらのロールは、コンポーネント固有のロールとして知られています。

それらのロールはどのように使用されるのでしょうか。ある組織で使用される休日タイムテーブルの事例を考えてみます。そのタイムテーブルにはすべての従業員がアクセスできる一方、そのタイムテーブルを更新できる従業員の数は制限したいとします。

休日タイムテーブルがインストールされた時点で、以下のロールが作成されます。

- **HolidayOwner**

このロールに割り当てられたメンバーは、休日タイムテーブルを読むことができ、それに書き込むこともできます。例えば、会社が特別な休暇を追加する場合、HolidayOwner ロールを持つメンバーは変更を加えることができます。

このロールのメンバーは、メンバーを HolidayWriter ロールおよび HolidayReader ロールに割り当てることもできます。例えば、HolidayOwner は、ある上級管理者を HolidayWriter ロールに追加する決定を下すことができます。

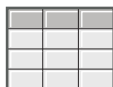
- **HolidayWriter**

このロールに割り当てられたメンバーは、休日タイムテーブルを読むことができ、それに書き込むこともできます。HolidayOwner の事例のように、HolidayWriter ロールのメンバーは休日を追加できます。

- **HolidayReader**

このロールに割り当てられたメンバーは、休日タイムテーブルを読むことができますが、それに書き込むことはできません。

次の図で示すように、HolidayOwner ロールを Human Resources manager に、HolidayWriter ロールを Human Resources Specialists group に、HolidayReader ロールを employee group に割り当てることができます。



休日タイムテーブル



休日の表示および更新が可能。  
休日のライターおよびリーダーの  
ロールを割り当て可能。

Holiday.Owner=Human Resources manager



休日の表示および更新が可能。

Holiday.Writer=Human Resources specialists group



休日の表示が可能。

Holiday.Reader=Employees group

図1. タイムテーブルに割り当てられたロールの例

タイムテーブルをデプロイすると、所有者、作成者、および読者という3つのロールが作成されます。すべてロールのアクセス権は、初期には「すべての認証済み」に設定されます。必ず、この指定を変更し、組織のメンバーを正しいロールに割り当ててください。

**注:** ロールのメンバーシップは変更できます (例えば、読者ロールからメンバーを除去できます) が、ロールの名前の変更、ロールの追加または削除、ロールに関連付けられているアクセス権の変更はできません。アクセス権は、以下のように設定されます。

- 所有者ロールのメンバーはタイムテーブルの読み取りと書き込みができ、他のメンバーを作成者ロールおよび読者ロールに割り当てることができます。
- 作成者ロールのメンバーは、タイムテーブルの読み取りと書き込みができます。
- 読者ロールのメンバーは、タイムテーブルを読み取ることができます。

セキュリティー・ロール・ウィジェットでは、これらのタイムテーブルに関連したロールは、モジュール・ロール としても知られています。

### セキュリティー・ロール・ウィジェットのシステム・ロール

BPMAAdmin および BPMRoleManager ロールは、WebSphere Process Server のインストール後 (または WebSphere Process Server 7.0 へのアップグレード後) に、セキュリティーを使用可能にすると、自動的に作成されます。

- **BPMAdmin**

BPMAdmin は、BPMRoleManager ロールのメンバーを追加または除去する権限を持ちます。例えば、BPMRoleManager ロールを実行している人が組織を去った場合、そのロールに別のメンバーに割り当てることができるのは、BPMAdmin だけです。

BPMAdmin は、初期には 1 人のメンバー (1 次管理ユーザー) に割り当てられます。この割り当ては、インストールまたはアップグレード後にサーバーを再始動してから、直ちに別のメンバーに変更してください。

- **BPMRoleManager**

BPMRoleManager は、タイムテーブルに関連する 3 つのロールである、所有者、作成者、および読者のロールに対して、メンバーを追加または除去する権限を持ちます。例えば、Holiday タイムテーブルが作成されると、BPMRoleManager はメンバーを HolidayOwner ロール、HolidayWriter ロール、および HolidayReader ロールに割り当てます。

BPMRoleManager は、初期には 1 人のメンバー (1 次管理ユーザー) に割り当てられます。この割り当ては、インストールまたはアップグレード後にサーバーを再始動してから、直ちに別のメンバーに変更してください。

## **セキュリティー・ロール・ウィジェットでのロールの管理**

セキュリティー・ロール・ウィジェットを使用して、ユーザーまたはグループをシステム・ロールに割り当てることができます。タイムテーブルに関連付けられたコンポーネント・ロールにユーザーまたはグループを割り当てすることもできます。

### **コンポーネント・ロールの割り当て**

ビジネス・カレンダー・ウィジェットの各タイムテーブルには 3 つのコンポーネント・ロール (所有者、作成者、読者) が関連付けられています。セキュリティー・ロール・ウィジェットを使用して、これらのロールにユーザーまたはグループを割り当てます。

### **始める前に**

セキュリティー・ロール・ウィジェットが表示されることを確認します。

### **このタスクについて**

BPMRoleManager は、ユーザーまたはグループをコンポーネント・ロールに割り当てることができます。

タイムテーブルの所有者も、ユーザーまたはグループをそのタイムテーブルの所有者、作成者、または読者ロールに割り当てることができます。

### **手順**

#### **手順**

1. 個別のメンバーをモジュール・ロールに割り当てするには、以下のステップを実行します。
  - a. 「モジュール」リストから、タイムテーブルを選択します。



- b. ロール (例えばタイムテーブルの作成者ロール) に対して、ロールの名前をクリックします。
  - c. ページの右側で、「追加」をクリックします。
  - d. 「検索対象のユーザーまたはグループ」フィールドに名前 (または名前の一部) を入力します。
  - e. 検索基準に基づいて返されるユーザーまたはグループの数を制限するには、「結果の最大数」フィールドの値を変更します。この値を 0 に設定すると、結果セット全体が返されます。
  - f. 「検索」をクリックします。
  - g. 表示されるリストから、1 人以上のユーザーまたはグループを選択し、「OK」をクリックします。
  - h. すべてのメンバーを割り当てたら、「保管」をクリックします。
2. すべてのメンバーをモジュール・ロールに割り当てるには、以下のステップを実行します。
    - a. 「モジュール」リストから、タイムテーブルを選択します。
    - b. ロール (例えばタイムテーブルの読者ロール) に対して、ロールの名前をクリックします。
    - c. 「すべての認証済み」を選択します。
    - d. 「保存」をクリックします。

---

## アダプターの保護

WebSphere Process Server では、WebSphere Business Integration Adapters と WebSphere Adapters という 2 つのタイプのアダプターがサポートされています。ここでは、両タイプのアダプターのセキュリティーについて説明します。

### このタスクについて

アダプターは、アプリケーションがエンタープライズ情報システム (EIS) と通信するために使用するメカニズムです。アプリケーションと EIS 間で交換される情報は、高い機密性を必要とする可能性があります。そのため、この情報のトランザクションにおけるセキュリティーを確保することは重要です。

WebSphere Business Integration Adapters は、一連のソフトウェア、アプリケーション・プログラム・インターフェース (API)、およびツールから構成され、アプリケーションによる統合ブローカー経由のビジネス・データの交換を可能にしています。WebSphere Business Integration Adapters は JMS メッセージングに依存するため、JMS はセキュリティー・コンテキストの伝搬をサポートしていません。

WebSphere Adapters は、EIS と WebSphere Process Server によってサポートされる Java EE コンポーネントの間の管理された双方向接続を使用可能にします。

この両方のタイプのアダプターから WebSphere Process Server へのインバウンド通信には、認証メカニズムがありません。WebSphere Business Integration Adapters の場合は JMS メッセージングに依存しているため、セキュリティー・コンテキスト

を伝搬することはできません。また、JCA もインバウンド・セキュリティーをサポートしないため、WebSphere Adapter にもインバウンド通信用の認証メカニズムはありません。

アダプターから WebSphere Process Server への入力では、必ず Service Component Architecture (SCA) エクスポートが使用されます。SCA エクスポートは、メディアエーション、ビジネス・プロセス、SCA Java コンポーネント、セレクターなどの SCA コンポーネントに関連付ける必要があります。

セキュリティーの解決策としては、WebSphere Adapter エクスポートのターゲットになっているコンポーネントで runAs ロールを定義することです。これを行うには、開発時に SCA 修飾子 SecurityIdentity を使用します (詳しくは、WebSphere Integration Developer インフォメーション・センター を参照してください)。コンポーネントの実行は、runAs ロールで定義されている ID で行われます。

SecurityIdentity の値は、ユーザーではなくロールです。EAR ファイルを WebSphere Process Server にデプロイするときに、使用する ID のユーザー名とパスワードを指定する必要があります。SecurityIdentity の使用により、ダウンストリームのコンポーネントが保護されていて、クライアントに認証済み ID が必要な場合に、例外の throw が防止されます。

注: SecurityIdentity を使用しても、アダプターと EIS 間の通信は保護されません。

WebSphere Business Integration Adapters は、データをサービス統合バスを介した JMS メッセージとして、WebSphere Process Server に送信します。

WebSphere Adapters は、WebSphere Process Server の JVM に常駐します。このため、保護する必要があるのは、アダプターとターゲットの EIS 間の通信のみです。アダプターと EIS 間のプロトコルは EIS に固有のもので、EIS の資料には、このリンクの保護方法に関する情報が記載されています。

---

## Business Space のセキュリティーのセットアップ

ご使用の環境で WebSphere が提供する Business Space を利用しようとする場合は、Business Space の成果物をチームがどのように処理するかについてのセキュリティー・オプションを検討する必要があります。Business Space のセキュリティーをオンにする場合は、アプリケーション・セキュリティーをセットアップし、ユーザー・リポジトリを指定します。Business Space 管理者を定義するには、スーパーユーザー・ロールを割り当てます。

### このタスクについて

最善の結果を得るため、Business Space を構成する前にセキュリティーを有効にします。管理コンソールの「グローバル・セキュリティー」管理ページで、管理セキュリティーとアプリケーション・セキュリティーの両方を有効にします。また、ユーザー・アカウント・リポジトリも指定します。詳しくは、『セキュリティーのセットアップおよび使用可能化』を参照してください。

ユーザー・アカウント・レジストリーを Business Space と共に使用する場合の考慮事項:

- 使用している LDAP 構成のタイプに応じて、設定が、Business Space に正しくアクセスできる能力に影響を及ぼすことがあります。ユーザー・フィルター、グループ・フィルター、およびマッピング設定が適切に構成されていることを確認してください。詳しくは、WebSphere Application Server 資料の『Lightweight Directory Access Protocol 検索フィルターの構成』を参照してください。
- 使用しているフェデレーテッド・リポジトリ構成のタイプに応じて、設定が、Business Space に正しくアクセスできる能力に影響を及ぼすことがあります。レルムが適切に構成されていることを確認してください。詳しくは、WebSphere Application Server 資料の『フェデレーテッド・リポジトリ構成におけるレルムの管理』を参照してください。
- Business Space での検索にログイン・プロパティ uid (ユーザー ID) を使用するように LDAP セキュリティーがデフォルトでセットアップされます。ログイン・プロパティに、mail (E メール・アドレス) など、別の固有の LDAP フィールドを使用するように LDAP セキュリティーを変更する場合は、Business Space で検索が機能するようにするため、ConfigServices.properties ファイルの `userIdKey` プロパティを変更する必要があります。  
ConfigServices.properties ファイルは、スタンドアロン・サーバーの場合は `profile_root%BusinessSpace% node_name%server_name %mm.runtime.prof%config %ConfigService.properties` に、クラスターの場合は `deployment_manager_profile_root %BusinessSpace%cluster_name %mm.runtime.prof %config%ConfigService.properties` に格納されています。LDAP セキュリティーのログイン・プロパティに合わせて、`userIdKey` 属性を `uid` から、例えば、`mail` に変更します。以下のパラメーターを指定して、`wsadmin` スクリプト・クライアントを使用して `updatePropertyConfig` コマンドを実行します。 `-serverName` および `-nodeName` (スタンドアロン・サーバーの場合) または `-clusterName` (クラスターの場合)、 `-propertyName` (値は ConfigServices.properties ファイルのパス)、ならびに `-prefix` (値は `Mashups_`)。
- Microsoft SQL Server データベースおよび Standalone LDAP レジストリーを使用する場合は、必ずユーザー識別名 (ユーザー DN) を 131 文字より少ないようにしてください。いずれかのユーザー DN エントリーが 131 文字以上の場合には、ユーザー・アカウント・リポジトリに「フェデレーテッド・リポジトリ」オプションを指定する必要があります。フェデレーテッド・リポジトリと他のレジストリーとの切り替えを行うと、すべての既存のスペースおよびページは Business Space でアクセスできなくなるので、再作成する必要があります。
- 「フェデレーテッド・リポジトリ」を使用すると、拡張検索機能などの、ウィジェットおよびフレームワークの機能が追加されます。スペースおよびページを共用するためにユーザーを検索をするときは、検索有効範囲に E メール、ユーザーのフルネーム、およびユーザー ID が含まれます。

**重要:** デフォルトでは、Business Space ウィジェットで使用される Ajax プロキシ構成はどの IP アドレスへのアクセスも制限しません。Business Space 環境のセキュリティを向上させるには、選択したサイトのコンテンツのみを表示するか、選択したサイトのコンテンツをブロックするよう、Ajax プロキシを構成します。詳しくは、『Business Space Ajax プロキシを使用した IP アドレスのブロック化』を参照してください。

IBM® Tivoli Access Manager WebSEAL を使用しており、それを Business Space 環境と共に使用したい場合は、追加の構成ステップを実行する必要があります。外部 Java Authorization Contract for Containers (JACC) プロバイダーと一緒に Tivoli Access Manager のセキュリティーを構成し、Tivoli Access Manager で WebSEAL を構成し、製品アプリケーション・サーバーで WebSEAL を構成し、ご使用の環境のホスト・ジャンクションを構成します。詳しくは、サブトピック『Business Space を操作できるように Tivoli Access Manager WebSEAL を構成する』を参照してください。

Business Space 環境で管理者になるユーザーをセットアップするために、`createSuperUser.py` スクリプトを実行して、Business Space のスーパーユーザー・ロールを割り当てます。詳しくは、サブトピック『Business Space のスーパーユーザー・ロールの割り当て』を参照してください。

## Business Space のアプリケーション・セキュリティーの設定

Business Space のセキュリティーをオンにするには、アプリケーション・セキュリティーと管理セキュリティーの両方を使用可能にする必要があります。

### 始める前に

このタスクを完了する前に、以下のタスクを完了しておく必要があります。

- 製品のユーザー・レジストリーにユーザー ID が登録されていることの確認。

保護された環境を使用することを予定している場合は、必ず、Business Space を構成する前にセキュリティーを有効にしてください。Business Space の構成後にセキュリティーを有効化または除去する場合は、`ConfigServices.properties` ファイルの `MashupAdminFor00Bspace` プロパティーと `noSecurityAdminInternalUserOnly` プロパティーの両方を変更し、有効な管理者 ID として正しいユーザー ID を設定する必要があります。`ConfigServices.properties` ファイルは、スタンドアロン・サーバーの場合は `profile_root%BusinessSpace%node_name%server_name%mm.runtime.prof %config%ConfigService.properties` に、クラスターの場合は `deployment_manager_profile_root%BusinessSpace% cluster_name%mm.runtime.prof% config%ConfigService.properties` に格納されています。変更後のファイルを、システム上の空のフォルダーにコピーします。次に、`wsadmin` スクリプト・クライアントを使用し、以下のパラメーターを指定して `updatePropertyConfig` コマンドを実行します。

- `-serverName` および `-nodeName` (スタンドアロン・サーバーの場合) または `-clusterName` (クラスターの場合)
- `-propertyName` (値は `ConfigServices.properties` ファイルのパス)
- `-prefix` には値 `Mashups_` を指定します

### このタスクについて

Business Space は、アクセスの認証と許可を確実に行うように事前に構成されます。Business Space URL へのアクセス時には、ユーザーに認証のプロンプトが出されます。認証されないユーザーは、ログイン・ページにリダイレクトされます。Business Space には、HTTP または HTTPS のいずれかでアクセスできます。SSL 保護がないためにパスワードの暗号漏えいの懸念がある場合は、WebSphere Application Server を使用して HTTP アクセスを使用不可にすることを検討してく

ださい。詳しくは、WebSphere Application Server インフォメーション・センターを参照してください。そのため、IBM HTTP Server などの Web サーバーを使用する場合は、HTTPS をサポートするようにその Web サーバーを構成する必要があります。

Business Space のスペースおよびページ内容への権限は、スペース管理の一部として Business Space 内で処理されます。

Business Space への認証済みアクセスを使用可能にするには、ユーザー・レジストリーを構成して、アプリケーション・セキュリティーを使用可能にする必要があります。

## 手順

### 手順

1. セキュリティーの詳細な説明については、製品のセキュリティー・ドキュメンテーションを参照してください。
2. Business Space アプリケーションの場合は、「グローバル・セキュリティー」管理コンソール・ページで、「管理セキュリティーを使用可能にする」および「アプリケーション・セキュリティーを使用可能にする」の両方を選択します。
3. 同じ管理コンソール・ページ上の「ユーザー・アカウント・リポジトリー」で、「フェデレーテッド・リポジトリー」、「ローカル・オペレーティング・システム」、「スタンドアロン LDAP レジストリー」、または「スタンドアロン・カスタム・レジストリー」のいずれかを指定します。『Business Space のセキュリティーのセットアップ』で、ユーザー・レジストリーの選択に関する考慮事項を確認してください。
4. 製品を実行している場所とは別の場所に Business Space が存在し、Business Space を実行しているノードと製品を実行しているノードが異なるセル内に存在する場合は、手動でシングル・サインオン (SSO) を有効にする必要があります。例えば、複数の製品 (WebSphere Business Compass、WebSphere Business Monitor、WebSphere Enterprise Service Bus、または WebSphere Process Server) を使用し、サーバーをそれぞれ異なるノードに配置し、さらにそれらすべてが Business Space サーバーと連携できるようにする場合は、手動で SSO を構成する必要があります。SSO を有効にするには、以下のステップを実行します。
  - a. 各サーバーの管理コンソールで、「セキュリティー」 > 「グローバル・セキュリティー」をクリックして、「グローバル・セキュリティー」ページを開きます。「Web および SIP セキュリティー」を展開し、「シングル・サインオン (SSO)」をクリックして、「使用可能」チェック・ボックスが選択されていることを確認します。
  - b. すべてのノードが同じ「ユーザー・アカウント・リポジトリー」の情報 (ステップ 3 を参照) を使用することを確認します。
  - c. 最初のノードの管理コンソールで、「グローバル・セキュリティー」ページを開きます。「認証」の下にある「LTPA」をクリックします。
  - d. 「クロス・セル・シングル・サインオン」の下に、鍵ファイルのパスワード、および完全修飾鍵ファイル名 (つまり、鍵ファイルをエクスポートするロケーションとファイル名) を入力します。完全修飾鍵ファイル名は、サーバーが稼働しているシステム上での絶対パスです。



- e. 「**鍵のエクスポート**」をクリックします。鍵ファイルは、サーバーが稼働しているシステムに保管されます。
  - f. 2つのノードが同じシステム上にない場合は、鍵ファイルを物理的に他のシステムにコピーします。
  - g. 同じ鍵ファイルを使用するその他すべてのノードに鍵ファイルをインポートするには、他のノードの管理コンソールにログオンして、「グローバル・セキュリティ」>「LTPA」ページに移動します。「**クロス・セル・シングル・サインオン**」の下に、鍵ファイルのパスワード、および完全修飾鍵ファイル名（コピーしたエクスポート済み鍵ファイルと同じパスワードを使用）を入力し、「**鍵のインポート**」をクリックします。
  - h. 各システムに鍵をインポートした後、サーバーを再始動します。
5. エンドポイント・ファイルで **HTTPS** を使用していて、エンドポイントのロケーションが **Business Space** とは異なるノード上にあり、**Secure Sockets Layer (SSL)** 証明書が自己署名 **SSL** 証明書である場合には、その **SSL** 証明書をインポートする必要があります。
- a. **Business Space** が含まれているサーバーの管理コンソールにログオンし、製品を実行しているリモート・ノードが使用する **SSL** 証明書をインポートします。
    - 1) 「セキュリティ」の下にある「**SSL 証明書と鍵の管理**」をクリックします。
    - 2) 「**SSL 証明書と鍵の管理**」ページの「関連項目」で、「**鍵ストアおよび証明書**」をクリックします。
    - 3) 「**鍵ストアおよび証明書**」ページで、「**NodeDefaultTrustStore**」をクリックして **truststore** タイプを変更します。
    - 4) 「**NodeDefaultTrustStore**」ページの「追加プロパティ」の下で、「**署名者証明書**」をクリックします。
    - 5) **NodeDefaultTrustStore** の「署名者証明書」ページで、「**ポートから取得**」ボタンをクリックします。
    - 6) 「ポートから取得」ページの「一般プロパティ」に、製品を実行している場所でのホスト、ポート、および別名を入力します。「**署名者情報の取得**」ボタンをクリックして、「**OK**」をクリックします。
    - 7) 両方のサーバーを再始動します。
  - b. 製品ノードの管理コンソールにログオンし、**Business Space** を実行しているノードが使用する **SSL** 証明書をインポートします。
    - 1) ステップ a. の 1) から 5) を繰り返します。
    - 2) 「ポートから取得」ページの「一般プロパティ」に、**Business Space** を実行している場所でのホストおよびポートを入力します。「**署名者情報の取得**」ボタンをクリックして、「**OK**」をクリックします。
    - 3) 両方のサーバーを再始動します。
- SSO** および **SSL** については詳しくは、**WebSphere Application Server** インフォメーション・センターを参照してください。



## 次のタスク

- 管理セキュリティーおよびアプリケーション・セキュリティーをオンにした後は、Business Space にログオンすると、ユーザー ID およびパスワードを求めるプロンプトが表示されます。ログオンするためには、選択したユーザー・レジストリーから有効なユーザー ID およびパスワードを使用する必要があります。管理セキュリティーをオンにした後は、管理コンソールに戻るたびに管理権限を持つユーザー ID でログオンする必要があります。
- ユーザーおよびグループのサブセットに対して、Business Spaceへのログインを制限したい場合は、Business Space J2EE ロールのマッピングを変更することができます。エンタープライズ・アプリケーション **BSpaceEAR\_node\_server** と **mm.was\_node\_server** に対して、ユーザー/グループ・マッピングを更新する必要があります。「アプリケーション」 > 「アプリケーション・タイプ」 > 「WebSphere エンタープライズ・アプリケーション」をクリックして、上の 2 つのアプリケーションを選択します。右のパネルの、「詳細プロパティ」の下の、「ユーザー/グループ・マッピングへのセキュリティー役割」を選択します。最初に特別な対象を削除してから、2 つのアプリケーションの **businessspaceusers** ロールと **Allauthenticated** ロールを再マップします。「特別な対象のマップ」をクリックし、「なし」を選択します。次に、「ユーザーのマップ」または「グループのマップ」をクリックし、選択したユーザーまたはグループに各ロールを割り当てます。J2EE ロール・マッピングを変更しても、Business Space 上でのユーザーやグループの検索機能には影響しません。
- Business Space のページおよびスペースに対する権限を設定するには、Business Space のページおよびスペースを作成するときに権限を管理することができます。

### 注:

SystemOut.log ファイルで次のエラーを見つけた場合は、処理できない余分な属性がユーザー・レジストリーに含まれている可能性があります。

```
00000046 SystemErr R Caused by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
The value of the property secretary is not valid for entity uid=xxx,c=us,ou=yyy,o=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.Ldap.LdapAdapter.setPropertyValue(LdapAdapter.java:3338)
```

これらの属性をバイパスするには、ConfigServices.properties ファイルで以下の属性を設定します。

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

ConfigServices.properties ファイルは、スタンドアロン・サーバーの場合は

```
profile_root%BusinessSpace%node_name %server_name%mm.runtime.prof
%config%ConfigService.properties に、クラスターの場合は
```

```
deployment_manager_profile_root%BusinessSpace% cluster_name
```

```
%mm.runtime.prof% config%ConfigService.properties に格納されています。
```

ConfigServices.properties ファイルに変更を加えた後、以下のパラメーターを指定して、wsadmin スクリプト・クライアントを使用して **updatePropertyConfig** コマンドを実行します。 **-serverName** および **-nodeName** (スタンドアロン・サーバーの場合) または **-clusterName** (クラスターの場合)、**-propertyName** (値は ConfigServices.properties ファイルのパス)、ならびに **-prefix** (値は Mashups\_)。

注:

クラスター環境で Java 2 セキュリティーを有効にした場合は、Business Space ヘルプのロケーションに適用されるサーバー・ポリシーの入力設定を制限することをお勧めします。

Business Space のヘルプのロケーション・ポリシーは次のようになっています。

```
grant codeBase      "file:${was.install.root}/profiles/profile_name/temp/
node_name/-" {

    permission java.security.AllPermission;

};
```

このポリシーを次のように変更して強化します。

```
grant codeBase      "file:${was.install.root}/profiles/profile_name/temp/
node_name/server_name/BusinessSpaceHelpEAR_node_name_server_name/
BusinessSpaceHelp.war/-" {

    permission java.security.AllPermission;

};
```

## システム REST サービスのセキュリティーのセットアップ

ユーザーおよびグループに基づいてウィジェット内のデータのセキュリティーをセットアップするには、REST サービス・ゲートウェイ・アプリケーションにマップされているユーザーを変更する必要があります。

### このタスクについて

REST サービス・プロバイダー・アプリケーションへのユーザーのマップ状況は、プロバイダーに対するすべてのサービスに影響します。

影響を受けるサービスを確認するには、「サービス」 > 「REST サービス」 > 「REST サービス・プロバイダー」を選択し、プロバイダーのリストで一致するプロバイダー・アプリケーションを選択します。

### 手順

#### 手順

1. 管理コンソールで、以下のオプションのいずれか 1 つを選択します。
  - サーバー環境の場合、「アプリケーション」 > 「アプリケーション・タイプ」 > **WebSphere エンタープライズ・アプリケーション** > 「REST サービス・ゲートウェイ」を選択します。
  - さらに、Network Deployment 環境の場合、「アプリケーション」 > 「アプリケーション・タイプ」 > **WebSphere エンタープライズ・アプリケーション** > 「REST サービス・ゲートウェイ Dmgr」を選択します。
2. 右のパネルの、「詳細プロパティ」の下、「ユーザー/グループ・マッピングへのセキュリティー役割」を選択します。

- すべての REST サービス・ウィジェットのデータへのアクセスを制御するには、ユーザーおよびグループを「RestServicesUser」ロールに追加します。

## Business Space ウィジェットのセキュリティ上の考慮事項

Business Process Management 製品と共に Business Space で使用するウィジェットによっては、ウィジェット内のデータへのアクセスを制御するために管理ユーザー・グループ・ロールを割り当てるか、ウィジェットを対象としたロール・ベースのアクセスの追加層を割り当てる必要がある場合があります。

### 管理グループ・ロールおよびウィジェット

ウィジェット内のデータへのアクセスは、管理グループ・ロールと、管理グループ・ロールに割り当てられたユーザーによって制御されます。これらのロールに割り当てられたユーザーを確認するには、管理コンソールを開き、「ユーザーおよびグループ」 > 「管理グループ・ロール」を選択して、グループを選択します。「ロール」リストが表示されます。

ビジネス・ルール・ウィジェットとビジネス変数ウィジェットの 2 つは、管理グループ・ロールを変更する必要がある可能性のあるウィジェット例です。

システム正常性ウィジェットの場合、以下の管理ロールはすべてモニター権限を持ち、管理コンソールへのアクセスが可能であるため、これらのロールに割り当てられたユーザーはシステム正常性ウィジェットのデータにアクセスできます。

- モニター
- コンフィギュレーター
- オペレーター
- 管理者
- Adminsecuritymanager
- デプロイヤー
- iscadmins

これらの管理グループ・ロールにマップされたユーザーは、システム正常性ウィジェットのデータにアクセスできます。これらのロールにマップされていないユーザーは、システム正常性ウィジェットのデータにアクセスできません。

### ウィジェットのロール・ベースのアクセス

一部のウィジェットは、ビジネス・ユーザーが作成した成果物に対し、ロール・ベースのアクセスを使用します。セキュリティ・ロール・ウィジェットでは、ビジネス・カレンダー・ウィジェットのタイムテーブルに対してメンバーが持つアクセス権限のレベルを決定するシステム・ロールまたはモジュール・ロールにユーザーおよびグループを割り当てることができます。セキュリティ・ロール・ウィジェットについて詳しくは、WebSphere Process Server for Multiplatforms の資料に記述されているセキュリティ・ロール・ウィジェットを参照してください。

WebSphere Business Compass の場合、アクセス制御のレビュー・ウィジェットを使用して、レビューを実行してレビューにコメントを入力できるユーザーのアクセス権限を管理できます。詳しくは、対象ウィジェットのオンライン・ヘルプを参照してください。

## Business Space を操作できるように Tivoli Access Manager WebSEAL を構成する

Tivoli Access Manager WebSEAL を保有しており、それを Business Space と共に使用したい場合は、いくつかの追加構成ステップを実行する必要があります。

### このタスクについて

**トピックの対象範囲:** このトピックは、以下の製品を対象としています。

- WebSphere Business Monitor
- WebSphere Enterprise Service Bus
- WebSphere Process Server

Tivoli Access Manager WebSEAL を Business Space と共に使用する場合は、外部 Java Authorization Contract for Containers (JACC) プロバイダーと一緒に Tivoli Access Manager のセキュリティーを構成し、Tivoli Access Manager で WebSEAL を構成し、製品アプリケーション・サーバーで WebSEAL を構成し、ご使用の環境のホスト・ジャンクションを構成します。

### 手順

#### 手順

1. Tivoli Access Manager を JACC と一緒に構成します。
  - a. 管理コンソールと wsadmin コマンドのどちらを使用するかに応じて、以下のいずれかのステップを実行します。
    - 管理コンソールを使用して Tivoli Access Manager を JACC と一緒に構成する場合は、以下のステップを実行します。
      - 1) グローバル・セキュリティーを有効にします。
        - a) 「セキュリティー」 > 「グローバル・セキュリティー」を選択します。
        - b) Tivoli Access Manager と一緒に構成する LDAP サーバーの「管理セキュリティー」、「アプリケーション・セキュリティー」、および「Java 2 セキュリティー」を有効にします。
        - c) 「グローバル・セキュリティー」 > 「LDAP」を選択し、以下の情報を入力して「OK」をクリックします。

名前	説明
サーバー・ユーザー ID	Tivoli Access Manager の設定で管理者 DN に入力したのと同じユーザー ID を入力します。例: user1
サーバー・ユーザー・パスワード	puser1
ホスト	Tivoli Access Manager Access Manager と一緒に構成する LDAP
ポート	例: 389
基本識別名	例: o=ibm, c=us
バインド識別名	例: cn=SecurityMaster,secAuthority=Default

名前	説明
バインド・パスワード	SecurityMaster ユーザーのパスワード

- d) 構成を保存して、サーバーを再始動します。
- 2) Tivoli Access Manager および JACC の外部許可を有効にします。
- 「セキュリティ」 > 「グローバル・セキュリティ」 > 「外部許可プロバイダー」を選択します。
  - 「許可プロバイダー」リストで、「外部 JACC プロバイダー」を選択し、「構成」をクリックします。Tivoli Access Manager のデフォルトのプロパティは正しく設定されているので、デフォルトの値は変更しないでください。
  - 「追加プロパティ」の下の「Tivoli Access Manager プロパティ」を選択します。「組み込み Tivoli Access Manager を使用可能にする」を選択し、以下の情報を入力して「OK」をクリックします。

名前	値
クライアント listen ポートの設定	デフォルト設定は 8900 から 8999 です。別のポートを使用する場合にのみ、変更してください。
ポリシー・サーバー (name:port)	該当する <i>policyserver:port</i> を指定します。例: windomain3.rtp.raleigh.ibm.com:7135
許可サーバーと優先順位 (name:port:priority)	該当する <i>authorizationserver:port:priority</i> を指定します。例: windomain3.rtp.raleigh.ibm.com:7136:1
管理者ユーザー名	Tivoli Access Manager サーバーで別の管理者名を使用する場合を除き、ユーザー名は「sec_master」(デフォルト)のままにしてください。
管理者ユーザー・パスワード	domino123
ユーザー・レジストリー識別名の接尾部	アプリケーション・サーバーに使用する名前を入力します。例: o=ibm,c=us
セキュリティ・ドメイン	セキュリティ・ドメインの設定はデフォルトのままにします。Tivoli Access Manager サーバーでデフォルトのドメインを使用しない場合は、この設定を変更します。Tivoli Access Manager サーバーで複数のドメインを作成し、デフォルト以外のドメインに接続する場合またはそのようなドメインを使用する場合は、この設定を変更します。
管理者ユーザーの識別名	ユーザーの完全修飾名を入力します。例: cn=user1,o=ibm,c=us 注: このユーザーは、LDAP ユーザー・レジストリー・パネルで構成された「サーバー・ユーザー ID」と同じです。

このサーバーは、Tivoli Access Manager サーバーに接続して、いくつかのプロパティ・ファイルをアプリケーション・サーバーの下に作成します。このプロセスには数分かかることがあります。エラーが発生した場合は、system Out を調べて、問題を修正してください。

- wsadmin ユーティリティを使用して Tivoli Access Manager を JACC と一緒に構成する場合は、以下のステップを実行します。以下の手順は、デプロイメント・マネージャー・サーバーで 1 回だけ実行します。同期化が実行されると、構成パラメーターが管理対象サーバー (ノード・エージェントを含む) に転送されます。構成の変更を有効にするには、管理対象サーバー自体を再始動する必要があります。
  - 1) すべての管理対象サーバー (ノード・エージェントを含む) が始動されたことを確認します。
  - 2) サーバーを始動します。
  - 3) `install_root/bin` ディレクトリーから `wsadmin` コマンドを実行して、コマンド行ユーティリティを開始します。
  - 4) `wsadmin` のプロンプトで、以下の表内の該当する情報を指定して、`configureTAM` コマンドを実行します。

Jacl の例:

```
$AdminTask configureTAM -interactive
```

Jython の例:

`AdminTask.configureTAM('-interactive')` 続けて、以下の情報を入力します。

名前	値
製品サーバーのノード名	ノードを 1 つだけ指定するか、アスタリスク (*) を入力してすべてのノードを選択します。
Tivoli Access Manager ポリシー・サーバー	Tivoli Access Manager ポリシー・サーバーの名前、および接続ポートを入力します。 <code>policy_server:port</code> という形式を使用します。 ポリシー・サーバーの通信ポートは Tivoli Access Manager の構成時に設定されます。デフォルトのポートは 7135 です。



名前	値
Tivoli Access Manager 許可サーバー	Tivoli Access Manager 許可サーバーの名前を入力します。 <code>auth_server:port:priority</code> という形式を使用します。許可サーバーの通信ポートは Tivoli Access Manager の構成時に設定されます。デフォルトのポートは 7136 です。エントリーをコンマで区切ることにより、複数の許可サーバーを指定することができます。複数の許可サーバーを構成しておくことは、フェイルオーバーおよびパフォーマンスの観点で有効です。優先順位の値は許可サーバーの使用順序です。例えば、 <code>auth_server1:7136:1,auth_server2:7137:2</code> です。優先順位 1 は、許可サーバーを 1 つだけ構成する場合でも指定する必要があります。
製品サーバーの管理者の識別名	製品サーバーのセキュリティー管理者 ID の完全識別名を入力します。例えば、 <code>cn=wasadmin,o=organization,c=country</code> です。詳細については、関連リンクを参照してください。
Tivoli Access Manager ユーザー・レジストリーの識別名サフィックス	例: <code>o=organization, c=country</code>
Tivoli Access Manager 管理者のユーザー名	Tivoli Access Manager の構成時に作成される Tivoli Access Manager 管理者のユーザー ID を入力します。通常、この ID は <code>sec_master</code> です。
Tivoli Access Manager 管理者のユーザー・パスワード	Tivoli Access Manager 管理者のパスワードを入力します。
Tivoli Access Manager セキュリティー・ドメイン	ユーザーおよびグループを保管するために使用する Tivoli Access Manager セキュリティー・ドメインの名前を入力します。Tivoli Access Manager の構成時にセキュリティー・ドメインを確立していない場合は、「戻る」をクリックしてデフォルトを受け入れます。
Embedded Tivoli Access Manager リスニング・ポート・セット	製品サーバーは、ポリシー・サーバーからの許可データベース・アップデートを TCP/IP ポートで <code>listen</code> します。特定のノードおよびマシンで複数のプロセスが実行されることがあるので、それらのプロセスのため、ポートのリストが必要です。Tivoli Access Manager クライアントがリスニング・ポートとして使用するポートを、コンマで区切って指定します。ポートの範囲を指定する場合は、最小値と最大値をコロンで区切って指定します。例えば、 <code>7999, 9990:9999</code> です。

名前	値
据え置き	このオプションを yes に設定すると、次の再始動時まで、管理サーバーの構成が据え置かれます。no に設定すると、管理サーバーの構成が即座に有効になります。管理対象サーバーは次の再始動時に構成されます。

- 5) 必要な情報をすべて入力したら、「F」を選択して構成プロパティを保存します。または、「C」を選択して構成プロセスを取り消し、入力した情報を破棄します。

#### SVTM TAM60 サーバーの場合の例:

```
wsadmin>$AdminTask configureTAM -interactive
組み込み Tivoli Access Manager の構成

このコマンドは、指定された 1 つまたは複数の WebSphere
Application Server ノードで組み込みの Tivoli Access Manager を
構成します。

WebSphere Application Server ノード名 (nodeName): *
*Tivoli Access Manager Policy Server (policySvr):
  windomain3.rtp.raleigh.ibm.com:7135
*Tivoli Access Manager Authorization Server (authSvrs):
  windomain3.rtp.raleigh.ibm.com:7136:1
*WebSphere Application Server 管理者の識別名 (wasAdminDN):
  cn=was61admin,o=ibm,c=us
*Tivoli Access Manager ユーザー・レジストリー識別名の接尾部 (dnSuffix):
  o=ibm,c=us
Tivoli Access Manager 管理者のユーザー名 (adminUid):
  [sec_master]
*Tivoli Access Manager 管理者のユーザー・パスワード (adminPasswd):
  domino123
Tivoli Access Manager セキュリティー・ドメイン (secDomain): [Default]
Embedded Tivoli Access Manager listen ポート・セット (portSet):
  [9900:9999]
据え置き (defer): [no]

組み込み Tivoli Access Manager の構成

F (完了)
C (キャンセル)

選択 [F, C]: [F] F
WASX7278I: 生成されたコマンド行: $AdminTask configureTAM {-policySvr
  windomain3.rtp.raleigh.ibm.com:7135 -authSvrs
  windomain3.rtp.raleigh.ibm.com:7136:1 -wasAdminDN cn=wa
  組み込み Tivoli Access Manager 構成処置パラメーターが正常に
  保存されました。
  ターゲット・ノード上で実行されているすべての
  WebSphere Application Server インスタンスを再始動します。
wsadmin>
```

- 6) 管理コンソールで、「セキュリティ」 > 「グローバル・セキュリティ」 > 「外部許可プロバイダー」を選択します。次に、「JACC プロバイダーを使用する外部許可」を選択して「OK」をクリックします。
- 7) メイン・セキュリティ画面に移動して、「OK」をクリックします。変更を保存して、同期化します。
- 8) セル内のすべてのプロセスを再始動します。
- b. Tivoli Access Manager を有効にする前にアプリケーションをインストールした場合 (例えば、LDAP セキュリティーを有効にして、保護されたアプリケーションをいくつかインストールし、ユーザーおよびグループをセキュリティ・ロールにマップした場合など) は、セキュリティ・ロール・マッピング情報をデプロイメント記述子から Tivoli Access Manager ポリシー・サーバーに伝搬させます。管理コンソールと wsadmin コマンドのどちらを使用するかに応じて、以下のいずれかのステップを実行します。

- wsadmin コマンド **propagatePolicyToJACCProvider** を使用する場合は、『JACC プロバイダーへのインストール済みアプリケーションのセキュリティー・ポリシーの wsadmin スクリプトを使用した伝搬』を参照してください。
- 管理コンソールを使用する場合は、『前にデプロイ済みのアプリケーションに対するセキュリティー・ポリシーとロールの伝搬』を参照してください。

2. Tivoli Access Manager で WebSEAL を構成します。

- WebSEAL がインストールされて適切に構成されていることを確認します。
- TAI++ の場合は **-c iv\_creds** オプションを使用して、TAI の場合は **-c iv\_user** オプションを使用して、WebSEAL と製品アプリケーション・サーバーの間のジャンクションを作成します。ご使用の環境に応じた変数を使用して、以下のいずれかのコマンドを 1 行に入力します。

TAI++ の場合

```
server task webseald-server create -t tcp -b supply -c iv_creds

-h host_name -p websphere_app_port_number junction_name
```

- (TAI の構成に使用できるように) トラストッド・ユーザー・アカウントを Tivoli Access Manager で作成するには、以下のコマンドを発行します。

```
pdadmin -a sec_master -p domino123
```

```
pdadmin sec_master> user create -gsouser -no-password-policy taiuser
"cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser
```

```
pdadmin sec_master> user modify taiuser password-valid yes
```

```
pdadmin sec_master> user modify taiuser account-valid yes
```

- WebSEAL 構成ファイル *webseal\_install\_directory/etc/webseald-default.conf* で、以下のパラメーターを設定します。

```
basicauth-dummy-passwd=webseal_userid_passwd
```

例えば、Tivoli Access Manager で taiuser または ptaiuser を設定する場合は、次のパラメーターを設定します。basicauth-dummy-passwd = ptaiuser

フォーム・ベースの認証を使用する場合は、以下のパラメーターを設定します。

```
forms-auth=both
```

```
ba-auth=none
```

- 製品アプリケーション・サーバー上で TAI++ インターセプターを有効にして、そのサーバーで WebSEAL を構成します。
  - 管理コンソールで、「グローバル・セキュリティー」 > 「認証メカニズムと有効期限」を選択します。

- b. 「Web および SIP セキュリティー」を展開し、「トラスト・アソシエーション」を選択します。チェック・ボックスを選択して、「適用」をクリックします。
- c. 「インターセプター」 > 「TAMTrustAssociationInterceptorPlus」 > 「カスタム・プロパティー」を選択して、以下のプロパティーを追加します。

名前	値
com.ibm.websphere.security.webseal.configURL	\${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties
com.ibm.websphere.security.webseal.id	iv-creds
com.ibm.websphere.security.webseal.loginId	taiuser (ユーザー taiuser または ptaiuser を Tivoli Access Manager で作成してある場合)

- d. セルを再始動します。
  - e. クライアントにアクセスするため、`https://webseal_server_name:webseal_port/junction_name/web_uri_for_client` に移動します。
4. Business Space ウィジェットが表示されるように、ご使用の環境のホスト・ジャンクションを構成します。仮想ホスト・ジャンクションとトランスペアレント・ホスト・ジャンクションのどちらを使用するかに応じて、以下のいずれかのステップを実行します。
- 仮想ホスト・ジャンクションを使用する場合は、それを作成します。仮想ホスト・ジャンクションを使用することにより、個別にジャンクションを作成しなくても済むようになります。
    - a. 仮想ホストが構成されていることを確認します。仮想ホスト・ジャンクションは、ホスト名、ポート番号、および転送アドレスをターゲット・ホストのものと突き合わせます。URL フィルタリングは一切実行されず、該当するすべての要求がターゲット・ホストに転送されます。
    - b. 同じ仮想ホストに対して以下のアプリケーションが有効になっていることを確認します。Business Space で使用している製品に応じて、これらのアプリケーションの一部を使用している場合と、全部を使用している場合が考えられます。
      - BPMAdministrationWidgets\_nodename\_servername (WebSphere Enterprise Service Bus および WebSphere Process Server の場合)
      - BusinessSpaceHelpEAR\_nodename\_servername (すべての製品の場合)
      - BSpaceEAR\_nodename\_servername (すべての製品の場合)
      - BSpaceWebformsEnabler\_nodename\_servername (すべての製品の場合)
      - HumanTaskManagementWidgets\_nodename\_servername (WebSphere Process Server および WebSphere Business Monitor の場合)
      - REST サービス・ゲートウェイ (すべての製品の場合)
      - REST サービス・ゲートウェイ Dmgr (WebSphere Enterprise Service Bus および WebSphere Process Server の場合)
      - mm.was\_nodename\_servername (すべての製品の場合)
      - WBMDashboardWeb\_nodename\_servername (WebSphere Business Monitor の場合)
      - wesbWidgets\_nodename\_servername (WebSphere Enterprise Service Bus の場合)

- `widgets_busleader_nodename_servername` (WebSphere Business Compass の場合)
- `widgets_pubserver_nodename_servername` (WebSphere Business Compass の場合)
- `widgets_fabric_nodename_servername` (WebSphere Business Services Fabric の場合)

注: このアプリケーション・リストに含まれているのは、Business Space に必要なアプリケーションのみです。状況によっては、Tivoli Access Manager WebSEAL を使用するが Business Space を使用しないシナリオ用に、他のアプリケーションをリストに追加することが必要な場合もあります。

- c. `pdadmin` を使用して、以下のコマンドを実行します。
 

```
server task webseal
server virtualhost create -t transport -h target_host [-p port] [-v
virtual_host_name] virtual_host_label
```

次の情報を使用します。

- `webseal server` は、仮想ホスト・エントリーを作成する WebSEAL サーバーの名前です。
- `transport` はトランスポートのタイプです。有効なエントリーは、`tcp`、`ssl`、`tcpproxy`、および `sslproxy` です。
- `target_host` は、必要なアプリケーションのホストです。
- `virtual_host_name` は、仮想ホスト・ジャンクションに対する HTTP 要求の突き合わせに使用されます。何も値を入力しない場合は、デフォルトで、ターゲット・ホストとポートを組み合わせて値が設定されます。例えば、`virtual_host_name` を `myvirthost.ibm.com:80` に設定した場合、WebSEAL は `myvirthost.ibm.com:80` を含んでいる URL を、`pdadmin` コマンドで指定されているホストと突き合わせて経路指定します。
- `virtual_host_label` は、WebSEAL のエントリーを識別するためのラベルであり、固有のものでなければなりません。

期待したとおりに Business Space が実行されるようにするため、トランスポートのタイプとして `ssl` と `tcp` の両方のエントリーを作成する必要があります。Secure Sockets Layer (SSL) と伝送制御プロトコル (TCP) の両方を同じ仮想ホスト・ジャンクションでサポートする必要がある場合は、`-g vhost_label` オプションを使用する必要があります。`vhost_label` は構成を共有するためのオリジナルの仮想ホストのラベルです。このオプションを指定することにより、事前に作成されている仮想ホスト・ジャンクション (事前に作成された仮想ホスト・ジャンクションであり、`virtual_host_label` が `-g` オプションで指定されるラベルと一致するもの) が検出され、その構成が共有されるようになります。2 番目のエントリーについても、やはり、固有の `virtual_host_label` が必要ですが、ターゲット・ホスト、ポート、およびその他の値を共有することができます。この `-g` オプションを指定しない場合、WebSEAL がターゲット・ホストおよびポートが前に作成されたジャンクションのものと同じであるとみなし (そのような仮想ホストを作成することは許可されない) で、2 番目の仮想ホストは作成されません。

- トランスペアレント・ホスト・ジャンクションを使用する場合は、それぞれの製品のウィジェット用の一連のトランスペアレント・パス・ジャンクションを作成します。
  - a. `pdadmin` を使用して、以下のコマンドを実行します。 `server task webseal server create -t transport type (ssl) or (tcp) -x -h hostname path`  
  
例えば、次のように入力します。 `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`
  - b. ご使用の製品用に以下のコンテキスト・ルートを作成します (『リバース・プロキシ・サーバーの Business Space URL のマッピング』を参照)。
- 5. ブラウザーの Cookie および仮想ホストに関する問題を解決するため、追加構成ステップを実行します。
  - a. Business Space の Cookie の名前変更を解決するため、以下の内容を WebSEAL 構成ファイルに追加します。  
  
[preserve-cookie-names]  
  
name = com.ibm.bspace.UserName  
  
name = com.ibm.wbimonitor.UserName
  - b. オプション: デフォルト以外の仮想ホストをコンテキスト・ルートと一緒に使用する場合は、Business Space ページに関する問題が発生することがあります。その場合は、`-j` オプションをコンテキスト・ルートに追加して、Business Space ページの JavaScript がジャンクションで上書きされないようにすることが必要です。次のコマンドを実行します。 `server task default-webseald create -f -h hostname -p portnumber -t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/root context`

## Business Space のスーパーユーザー・ロールの割り当て

Business Space では、スーパーユーザー (または Business Space 管理者) となるユーザーを割り当てることができます。スーパーユーザーは、すべてのスペースとページの表示、編集、削除のほか、テンプレートの管理と作成を行うことができます。また、所有者 ID を変更することでスペースの所有権を変更することもできます。

### 始める前に

Business Space を構成するときに管理セキュリティーを有効にする場合は、グループおよびスーパーユーザーに関する以下の情報について考慮してください。

- 特別なユーザー・グループ **administrators** に属するユーザーは、デフォルトでスーパーユーザー・ロールを持ちます。結果として、スーパーユーザー・ロールの割り当てはユーザー・グループのメンバーシップによって処理されます。
- シングル・サーバー環境の場合、Business Space サーバーはデフォルトのユーザー・レジストリーに **administrators** ユーザー・グループを作成します。構成中に指定された管理者 ID は、自動的にこのグループのメンバーとして追加されません。



- Network Deployment 環境の場合、自動的に **administrators** ユーザー・グループが作成されることはありません。createSuperUser.py スクリプトを使用してユーザー・グループを作成し、デフォルトのユーザー・レジストリーでそのグループにメンバーを追加してください。
- デフォルトのユーザー・レジストリーではなく別のユーザー・レジストリー (例えば、LDAP など) を使用する場合、またはデフォルトのユーザー・レジストリーを使用するが **administrators** ユーザー・グループを使用したくない場合は、Business Space のスーパーユーザーに使用するユーザー・グループを特定する必要があります。必ず、ユーザー・レジストリーで認識される値を指定してください。例えば、LDAP の場合は、cn=administrators,dc=company,dc=com というように名前を指定します。このユーザー・グループを特定する方法については、「次の作業」で管理者グループの変更手順を参照してください。
- WebSphere Portal のBusiness Space の場合は、デフォルト・グループ **wpsadmins** もスーパーユーザー・ロールに使用されます。このグループのメンバーには、Business Space に対するスーパーユーザー・ロールが付与されます。

注: WebSphere Portal で Business Space を使用する場合は、セキュリティを有効にする必要があります。

Business Space の構成時に管理セキュリティを有効にしない場合、特別なユーザー ID **BPMAdministrator** のみに Business Space のスーパーユーザー・ロールが付与されます。

Network Deployment 環境を使用している場合は、createSuperUser.py スクリプトを実行してスーパーユーザー・ロールを割り当てる (ユーザー・グループを作成してメンバーを追加する) 必要があります。このスクリプトを実行する前に、以下のステップを実行します。

- デフォルトの **administrators** グループ名が変更されていないことを確認します。
- デフォルト・リポジトリをユーザー・レジストリーに使用します。
- Business Space がインストールされているプロファイルについて、Business Space 環境用のサーバーまたはデプロイメント・マネージャーを始動します。

## 手順

### 手順

1. ユーザーにスーパーユーザー・ロールを割り当てるためのスクリプト `install_root%BusinessSpace%scripts%createSuperUser.py` を見つけます。
2. コマンド・プロンプトを開いてディレクトリー `profile_root%bin` に移動します。この `profile_root` は、Business Space がインストールされているプロファイルのディレクトリーを表します。
3. 以下のコマンドを入力します。wsadmin -lang jython -f `install_root%BusinessSpace%scripts%createSuperUser.py user_short_name password` ここで、`user_short_name` は Virtual Member Manager (VMM) のユーザーの固有 ID、`password` はそのユーザーの VMM パスワードです。そのユーザーが VMM に存在する場合、そのユーザーが管理者グループに追加されます。

注: パスにスペースが含まれる場合 (例えば、*install\_root* が My install dir である場合)、パス名を引用符で囲む必要があります。例えば、以下のコマンドを入力します。  
`wsadmin -lang jython -f "%My install dir%BusinessSpace%scripts%createSuperUser.py" user_short_name_in_VMM`

## 次のタスク

Business Space を開くには、以下の URL を使用します。 `http://host:port/BusinessSpace` この *host* はサーバーが稼働しているホスト名で、*port* はサーバーのポート番号です。

デフォルトの特別なユーザー・グループ **administrators** は変更できます。現在のグループ名を確認したり別の名前に変更したりするには、以下の手順を実行します。

以下の構成ファイルで、測定基準 `com.ibm.mashups.adminGroupName` の値を検査します。

- スタンドアロン・サーバーの場合: `profile_root%BusinessSpace%node_name%server_name%mm.runtime.prof%config%ConfigService.properties`
- クラスターの場合: `deployment_manager_profile_root%BusinessSpace%cluster_name%mm.runtime.prof%config%ConfigService.properties`

スタンドアロン・サーバー上で管理グループを変更する場合、以下のステップを実行します。

1. 構成ファイル `profile_root%BusinessSpace%node_name%server_name%mm.runtime.prof%config%ConfigService.properties` の測定基準 `com.ibm.mashups.adminGroupName` を変更します。
2. プロファイルの `wsadmin` 環境で `updatePropertyConfig` コマンド `$AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name -propertyFileName "profile_root%BusinessSpace%node_name%server_name%mm.runtime.prof%config%ConfigService.properties" -prefix "Mashups_"}` を実行してから、`$AdminConfig save` を実行します。
3. サーバーを再始動します。

クラスター上で管理グループを変更する場合、以下のステップを実行します。

1. ユーザー・リポジトリにグループが存在することを確認します。
2. 構成ファイル `deployment_manager_profile_root%BusinessSpace%cluster_name%mm.runtime.prof%config%ConfigService.properties` の測定基準 `com.ibm.mashups.adminGroupName` を変更します。
3. デプロイメント環境プロファイルの `wsadmin` 環境で `updatePropertyConfig` コマンド `$AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName "deployment_manager_profile_root%BusinessSpace%cluster_name%mm.runtime.prof%config%ConfigService.properties" -prefix "Mashups_"}` を実行してから、`$AdminConfig save` を実行します。
4. デプロイメント・マネージャーを再始動します。

スタンドアロン・サーバー上で、セキュリティーが有効でないときにスーパーユーザーを変更する場合、以下のステップを使用します。

1. ユーザー・リポジトリにグループが存在することを確認します。
2. 構成ファイル `profile_root¥BusinessSpace¥node_name¥server_name¥mm.runtime.prof¥config¥ConfigService.properties` の測定基準 `noSecurityAdminInternalUserOnly` を変更します。
3. プロファイルの `wsadmin` 環境で `updatePropertyConfig` コマンド `$AdminTask updatePropertyConfig {-serverName server_name -nodeName node_name -propertyFileName "profile_root¥BusinessSpace¥node_name¥server_name¥mm.runtime.prof¥config¥ConfigService.properties" -prefix "Mashups_"}` を実行してから、`$AdminConfig save` を実行します。
4. サーバーを再始動します。

クラスター上で、セキュリティーが有効でないときにスーパーユーザーを変更する場合、以下のステップを使用します。

1. 構成ファイル `deployment_manager_profile_root¥BusinessSpace¥cluster_name¥mm.runtime.prof¥config¥ConfigService.properties` の測定基準 `noSecurityAdminInternalUserOnly` を変更します。
2. デプロイメント環境プロファイルの `wsadmin` 環境で `updatePropertyConfig` コマンド `$AdminTask updatePropertyConfig {-clusterName cluster_name -propertyFileName "deployment_manager_profile_root¥BusinessSpace¥cluster_name¥mm.runtime.prof¥config¥ConfigService.properties" -prefix "Mashups_"}` を実行してから、`$AdminConfig save` を実行します。
3. デプロイメント・マネージャーを再始動します。

---

## エンドツーエンド・セキュリティーの作成

構築可能なさまざまなエンドツーエンド・セキュリティーのシナリオがあります。これらの各シナリオでは、異なるセキュリティーの手順が必要になる可能性があります。ここでは、必要なセキュリティー・オプションを持つ数種類の標準的なシナリオを提供します。

### 始める前に

これらのシナリオはすべて、管理セキュリティーが実行されていることを前提としています。

#### 手順

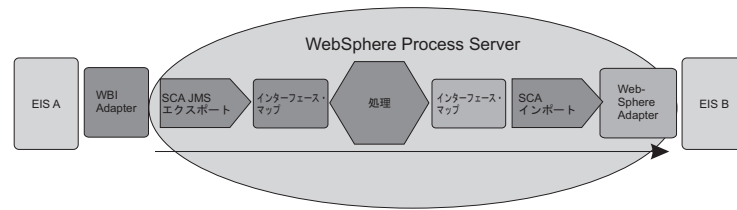
#### 手順

1. このセクションで提供されているどの例が、お客様のセキュリティーのニーズに最も合致しているかを判断します。場合によっては、お客様のニーズに対して複数のシナリオの情報が関連する可能性があります。
2. 関連のシナリオのセキュリティー情報を参照して、それらをお客様のセキュリティーのニーズに適用してください。

## 例

### 標準的な統合シナリオ - インバウンド・アダプターおよびアウトバウンド・アダプター

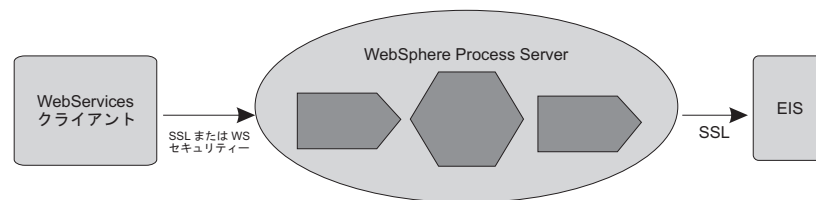
インバウンド要求は、WebSphere Business Integration Adapter で受信します。Service Component Architecture (SCA) は、SCA エクスポートに基づいてインターフェース・マップを呼び出します。この要求は、処理コンポーネント、2 番目のインターフェース・マップを経由した後、WebSphere Adapter を介して 2 番目の EIS (B) に渡されます。これらは、あるコンポーネントが次のコンポーネントのメソッドを呼び出していく SCA 呼び出しです。



インバウンド・アダプターのための認証メカニズムはありません。最初のコンポーネント (この場合、最初のインターフェース・マップ・コンポーネント) 上で SecurityIdentity 修飾子を定義して、セキュリティー・コンテキストを設定することができます。このポイントから、SCA はセキュリティー・コンテキストを各コンポーネントから次のコンポーネントへと伝搬します。コンポーネントごとのアクセス制御は、SecurityPermission 修飾子を使用して定義されます。

### インバウンド Web サービス要求

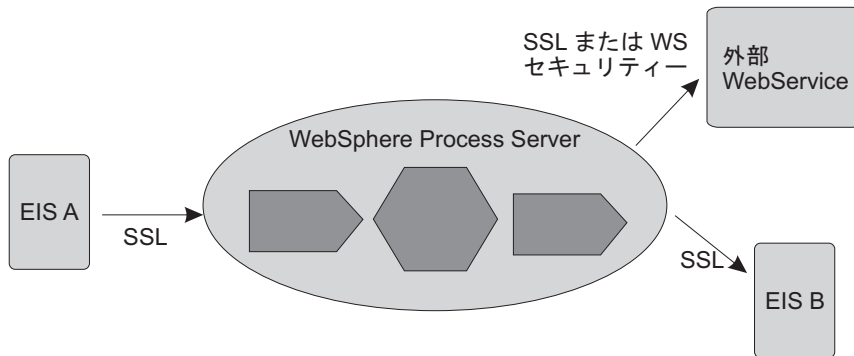
このシナリオでは、Web サービス・クライアントが、WebSphere Process Server のコンポーネントを呼び出します。要求は、WebSphere Process Server 環境内で数種類のコンポーネントを経由した後、アダプターによって EIS に渡されます。



HTTP 基本認証または WS-Security 認証を使用して、SSL クライアントとして Web サービス・クライアントを認証することができます。クライアントが認証される際、アクセス制御が SecurityPermission 修飾子に基づいて適用されます。クライアントと WebSphere Process Server インスタンスの間で、SSL または WS-Security を使用してデータ保全性およびプライバシーを保護することができます。SSL はパイプ全体を保護しますが、WS-Security を使用すると、SOAP メッセージの各部分を暗号化またはデジタル署名することができます。Web サービスの場合、WS-Security が好ましい標準です。

### アウトバウンド Web サービス要求

このシナリオでは、インバウンド要求はアダプター、Web サービス・クライアント、または HTTP クライアントから受信することができます。WebSphere Process Server のコンポーネント (BPEL コンポーネントなど) は、外部の Web サービスを呼び出します。



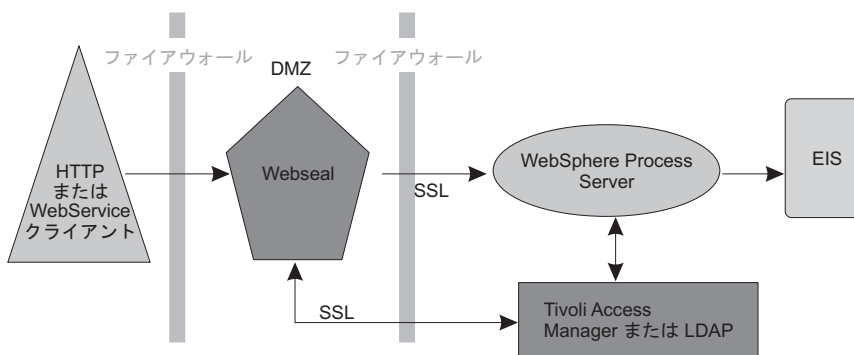
インバウンド Web サービス要求の場合、HTTP 基本認証または WS-Security 認証を使用して、SSL クライアントとして外部の Web サービスを認証することができます。LTPACallbackHandler をコールバック・メカニズムとして使用して、現在の RunAs サブジェクトから usernameToken を抽出します。WebSphere Process Server とターゲットの Web サービスとの間で、WS-Security を使用してデータのプライバシーおよび保全性を確保することができます。

### Web アプリケーション - WebSphere Process Server への HTTP インバウンド要求

WebSphere Process Server では、HTTP 用に以下の 3 種類の認証をサポートしています。

- HTTP 基本認証
- HTTP フォーム・ベースの認証
- HTTPS SSL ベースのクライアント認証

また、侵入者からご使用のイントラネットを保護するために、Web サーバーを非武装地帯 (DMZ) に、WebSphere Process Server を内部ファイアウォールの内側に配置することができます。以下の例では、WebSeal がリバース・プロキシとして使用され、認証を実行します。WebSeal は、ファイアウォールの背後の WebSphere Process Server とトラスト・アソシエーションを持っているため、認証済み要求を転送できます。









Printed in Japan