WebSphere Process Server for Multiplatforms

バージョン 6.2.0

アプリケーションとその環境の保護

WebSphere Process Server for Multiplatforms

バージョン 6.2.0

アプリケーションとその環境の保護

お願い

本書に記載されている情報をご使用になる前に、本書末尾の特記事項セクションに記載されている情報をお読みください。

新しい版で明記されるまで、WebSphere Process Server for Multiplatforms バージョン 6、リリース 2、モディフィケーション 0 (製品番号 5724-L01) 以降のすべてのリリースとモディフィケーションが本書の対象となります。

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 Multiplatforms
Version 6.2.0
Securing Applications and Their Environments

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1刷 2009.1

PDF ブックおよびインフォメーション・センター

PDF ブックは、印刷およびオフラインでの参照用に提供されています。最新情報は、オンラインのインフォメーション・センターを参照してください。

セットとして、PDF ブックには、インフォメーション・センターと同一の内容が含まれます。

PDF 資料は、バージョン 6.0 またはバージョン 6.1 など、インフォメーション・センターのメジャー・リリースの後の四半期以内にご利用いただけます。

PDF 資料の更新頻度は、インフォメーション・センターより低いですが、Redbooks® よりも頻繁に更新されます。通常、PDF ブックはブックに十分な変更が累積されたときに更新されます。

PDF ブックの外部にあるトピックへのリンクを選択すると、Web 上のインフォメーション・センターに移動します。PDF ブックの外部にあるターゲットへのリンクには、そのターゲットが PDF ブックと Web ページのどちらなのかを示すアイコンによるマークが付いています。

表 1. 本書の外部にあるトピックへのリンクのプレフィックスとなるアイコン

アイコン	説明

	インフォメーション・センターのページを含む、Web ページへのリンク。
	
	インフォメーション・センターへのリンクは、ターゲット・トピックが新しい場所に移動した場合でもその機能を保つように、間接参照ルーティング・サービスを経由します。
	
	ローカルのインフォメーション・センターでリンク先ページを見つけたい場合は、リンクのタイトルを検索することができます。あるいは、トピック ID を検索することもできます。検索の結果、タイプが異なる製品についてのトピックがいくつか見つかった場合は、検索結果の「**グループ別 (Group by)**」コントロールを使用して、表示するトピック・インスタンスを識別できます。以下に例を示します。
	1. リンク URL をコピーします。例えば、リンクを右クリックして「リンク先をコピーする (Copy link location)」を選択します。例: `http://www14.software.ibm.com/webapp/wsbroker/redirect?version=wbpm620&product=wesb-dist&topic=tins_apply_service`
	2. `&topic=` の後のトピック ID をコピーします。例: `tins_apply_service`
	3. ローカル・インフォメーション・センターの検索フィールドに、トピック ID を貼り付けます。文書機能がローカルにインストールされている場合は、検索結果にそのトピックが表示されます。以下に例を示します。
	`1 result(s) found for`
	`Group by: None | Platform | Version | Product`
	`Show Summary`
	`Update Installer を使用したフィックスパックおよびリフレッシュ・パックのインストール`
	4. 検索結果のリンクをクリックしてトピックを表示します。

	PDF ブックへのリンク。

目次

アプリケーションとその環境の保護

WebSphere® Process Server 環境のセキュリティーを確保するには、管理セキュリティーを使用可能にする、アプリケーション・セキュリティーを使用可能にする、セキュリティー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。

WebSphere Process Server のセキュリティーのベースとなるのは、WebSphere Application Server バージョン 6.1 のセキュリティーです。これらの資料は、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ー文書、特に WebSphere Application Server セキュリティー資料の「アプリケーションとその環境の保護」を補足するものです。

関連情報

PDF 資料
WebSphere Process Server 資料 (PDF 形式)

情報ロードマップ
IBM developerWorks が提供する Business Process Management 情報ロードマップには、WebSphere Process Server、WebSphere ESB、およびその他の製品に関する情報がポートフォリオに編成されています。

IBM Education Assistant
IBM Education Assistant により提供される WebSphere Process Server に関するマルチメディア教育モジュール。

技術情報
WebSphere Process Server サポート > 6.2 用セキュリティー・カテゴリー資料の技術情報検索。文書タイプ、製品カテゴリー、検索語フィールドを使用して、必要な情報を検索します。

概要
製品ライブラリー Web ページの「概要」タブ。このページを使用して、WebSphere ESB に関連した発表、データ・シート、およびその他の一般ライブラリー資料にアクセスします。

セキュリティーの概要

WebSphere Process Server のセキュリティーのベースとなるのは、WebSphere Application Server バージョン 6.1 のセキュリティーです。

セキュリティーについて詳しくは、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。

セキュリティー関連の操作は、WebSphere Process Server 環境内のセキュリティー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ーはアプリケーション・セキュリティー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、管理セキュリティーの使用可能化、アプリケーション・セキュリティーの使用可能可、セキュリティー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。

関連概念

53 ページの『ユーザーの認証』
管理セキュリティー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。

55 ページの『アクセス制御』
アクセス制御とは、認証済みユーザーがリソースにアクセスしたり、特定の操作を実行したりするために必要な許可 (アクセス権) を確実に得るようにすることです。

56 ページの『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、セキュリティーにとって重要です。

57 ページの『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。

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 6.1 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」パネルは、WebSphere Process Server に固有の機能です。そのパネルを表示するには、「**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、このパネルを使用して、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、このパネルでは、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。
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・リポジトリー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・マネージャーを使用して、Business Calendar Manager 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。

関連タスク

5 ページの『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。

11 ページの『セキュリティーの有効化』
ご使用の WebSphere Process Server 環境およびご使用のアプリケーションを保護するための最初のステップは、管理セキュリティーを有効にすることです。

15 ページの『ユーザー・アカウント・リポジトリーの構成』
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・リポジトリーに保管されます。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・リポジトリー (デフォルト)、Lightweight Directory Access Protocol (LDAP)、統合リポジトリー、またはカスタム・アカウント・リポジトリーのいずれかを使用することができます。

 セキュア・コンポーネントの開発
開発するコンポーネントを保護します。コンポーネントは、メソッドを持つインターフェースをインプリメントします。Service Component Architecture (SCA) 修飾子 SecurityPermission を使用して、インターフェースまたはメソッドを保護します。

58 ページの『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ことが必要な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。

59 ページの『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 securityIdenitity 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。

61 ページの『Business Calendar Manager のセキュリティー』
セキュリティー・マネージャーでは、Business Calendar Manager 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・マネージャーを使用して、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。

関連情報

7 ページの『スタンドアロン・サーバー用 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。

29 ページの『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のタスクを実行します。

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

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。インストールの前に実行する手順について詳しくは、WebSphere Application Server インフォメーション・センターのトピック『**インストール前の環境の保護**』を参照してください。

   i5/OS 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。インストールの前に実行する手順について詳しくは、関連タスクのトピック『**インストールのための i5/OS システムの準備**』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。インストールのためのご使用のオペレーティング・システムの準備について詳しくは、WebSphere Application Server インフォメーション・センターのトピック『**製品インストールのためのオペレーティング・システムの準備**』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、WebSphere Application Server インフォメーション・センターのトピック『**インストール後の環境の保護**』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ーを管理できます。

関連概念

3 ページの『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。

関連情報

インストール前の環境の保護

製品インストールのためのオペレーティング・システムの準備

インストール後の環境の保護

インストールのための i5/OS システムの準備

インストール時に入力する認証情報

WebSphere Process Server 環境を即時に保護するために、インストール中にセキュリティー情報を入力するためのプロンプトが表示されます。

以前のリリースの WebSphere Process Server では、インストール時に各種の認証情報の入力を要求するプロンプトが表示されていました。今回のリリースでは、管理者が提供する 1 次管理資格情報がすべてのコンポーネントのデフォルトとして設定されます。これらのデフォルト値によって、基本的なセキュリティーが実現します。しかし、インストール済み環境のセキュリティー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ー ID を提供できるように、管理コンソールを使用して WebSphere Process Server のコンポーネントを構成してください。

WebSphere Process Server のプロファイルを作成する場合、「**管理セキュリティーを使用可能にする**」を選択したままにすると、ユーザー名の入力を要求するプロンプトが表示されます。 この ID は、基盤となるすべてのコンポーネントのデフォルトとして使用されます。セキュリティーをさらに強化するためには、プロファイルの作成後にこれらの ID を構成することをお勧めします。

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。これらの別名は、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」パネル上で変更できます。

セキュリティーを適用した WebSphere Process Server プロファイルの作成

WebSphere Process Server プロファイルの作成には、セキュリティー資格情報のデフォルト値が使用されます。プロファイルの作成後に、管理コンソールでこれらのセキュリティー設定を構成する必要があります。

このタスクについて

WebSphere Process Server プロファイルを作成する際に、管理者ユーザー ID をデフォルトとして取り込む WebSphere Process Server コンポーネントは 3 つあります。

該当するコンポーネントは、以下のとおりです。

- Service Component Architecture (SCA)
- Business Process Choreographer

- Common Event Infrastructure (CEI)

これらのコンポーネントに関連付けられている ID は、セキュリティーが有効な場合に必要となる認証別名の作成時に使用されます。これらの ID を、ユーザー・アカウント・リポジトリーからの適切なユーザーに変更することが重要です。

手順

1. 管理コンソールで、「ビジネス・インテグレーション・セキュリティー」パネルを表示します。 「**セキュリティー**」を展開して、「**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。
2. Service Component Architecture、Business Process Choreographer、および Common Event Infrastructure の認証別名ごとに、認証別名として使用する適切なユーザー名とパスワードを指定します。
   a. 「**別名**」列の名前をクリックすることにより、変更する別名を選択します。

      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。
   b. 次のパネルで、このコンポーネントの認証別名として使用するユーザー名とパスワードを指定します。

      注: 指定する資格情報は、使用しているユーザー・アカウント・リポジトリー内に存在する必要があります。
   c. 「**OK**」をクリックします。

関連タスク

54 ページの『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生じます。

スタンドアロン・サーバー用 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。

関連概念

3 ページの『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。

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。

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確認してください。

このタスクについて

ご使用の WebSphere Process Server 環境は、プロファイル内で定義されています。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。

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

1. 管理セキュリティーが有効であることを確認します。 11 ページの『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。 51 ページの『WebSphere Process Server におけるアプリケーションの保護』
3. ユーザーまたはグループを管理ロールに追加します。 管理権限は、個別ユーザーまたはユーザー・グループに対して付与できます。設定するには、「**管理ユーザーのロール (Administrative User Roles)**」または「**管理グループのロール (Administrative Group Roles)**」のいずれかを選択します。
4. 使用するユーザー・アカウント・リポジ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	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。 • 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 • 1 つ以上の外部リポジトリー • 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 **注:** 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。

ユーザー・レジストリー	アクション
ローカル・オペレーティング・システム	デフォルトのユーザー・レジストリーです。ユーザー・アカウント・レジストリーの構成方法について詳しくは、 17 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』を参照してください。
スタンドアロン LDAP レジストリー	『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・アカウント・レジストリーとして LDAP を構成してください。
スタンドアロン・カスタム・レジストリー	ユーザー・アカウント・レジストリーの構成方法について詳しくは、 17 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』を参照してください。

5. 選択したレジストリーが現在のレジストリーとして設定されていることを確認します。

   設定されていない場合は、「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)」ページの下部にある「**現行として設定 (Set as current)**」をクリックします。
6. ユーザー・レジストリーの選択後、変更が適用されていることを確認します。

   適用されていない場合は、「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)」ページの下部にある「**適用**」をクリックします。
7. 「ビジネス・インテグレーション・セキュリティー」パネルに進みます。 「**セキュリティー**」を展開して、「**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。
8. リストされた認証別名に対して適切なユーザー ID を指定します。 指定する資格情報は、使用しているユーザー・アカウント・リポジトリー内に存在する必要があります。
9. 同じパネル上で、Business Process Choreographer のセキュリティーを構成できます。

   Business Flow Manager および Human Task Manager 用の Business Process Choreographer ユーザー・ロール・マッピングを設定します。

   - **管理者**: ビジネス・フローおよびヒューマン・タスク管理者ロールのユーザー名またはグループ名 (あるいはその両方)。このロールに割り当てられるユーザーにはすべての特権があります。
   - **モニター**: ビジネス・フローおよびヒューマン・タスク・モニター・ロールのユーザー名またはグループ名 (あるいはその両方)。このロールを割り当て

られたユーザーは、すべてのビジネス・プロセスとタスク・オブジェクトのプロパティーを表示することができます。

Business Process Choreographer 認証別名は、Business Process Choreographer のインストール先である各デプロイメント・ターゲットに対して構成できます。以下の認証別名がリストされています。

- **JMS API 認証**: 非同期 API 呼び出しを処理するための Business Flow Manager メッセージ駆動型 Bean の認証。
- **エスカレーション・ユーザー認証**: 非同期 API 呼び出しを処理するための Human Task Manager メッセージ駆動型 Bean の認証。

10. 以上の変更内容を適用します。

    パネルの下部の「**適用**」ボタンをクリックします。

11. 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。

12. 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。

タスクの結果

管理コンソールに次にログインする際には、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。

次のタスク

作成する各プロファイルは、以上のような方法で保護される必要があります。システム管理者のユーザー ID は、環境のインストールと構成を実行中に複数の場所で使用されることがあります。コア・セキュリティー機能以外のすべての機能で、この ID をユーザー・アカウント・リポジトリーからの適切なユーザー資格情報に置き換えることをお勧めします。これらの ID および別名を管理するには、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**」パネルを使用します。

関連タスク

11 ページの『セキュリティーの有効化』
ご使用の WebSphere Process Server 環境およびご使用のアプリケーションを保護するための最初のステップは、管理セキュリティーを有効にすることです。

51 ページの『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。

関連情報

WebSphere Process Server でのインストール検査ツールの使用 (Using the installation verification tools with WebSphere Process Server)

セキュリティーの有効化

ご使用の WebSphere Process Server 環境およびご使用のアプリケーションを保護するための最初のステップは、管理セキュリティーを有効にすることです。

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 のセキュリティーについて詳しくは、「**サブトピック (Subtopics)**」の下にリストされている情報を参照してください。

手順

1. 管理コンソールで「管理セキュリティー」パネルを開きます。

   「**セキュリティー**」を展開し、「**管理、アプリケーション、インフラストラクチャーの保護**」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、アプリケーションに対して認可すべきでないと J2EE 1.3 仕様で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。

   パネルの下部の「**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。

関連概念

3 ページの『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。

関連タスク

51 ページの『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。

関連情報

Java 2 セキュリティー・ポリシー・ファイルの構成

管理セキュリティー

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」であると考えることができます。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・リポジトリーの選択などが含まれます。具体的にいうと、

認証やロール・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は、セキュリティー・ドメイン全体で有効なセキュリティー構成に相当します。各セキュリティー・ドメインは、同じユーザー・レジストリー・レルム名を使用して構成されたすべてのサーバーから成り立っています。レルムは、ローカル・オペレーティング・システム・レジストリーのマシン名である場合があります。この場合には、すべてのアプリケーション・サーバーが同じ物理マシン上に存在する必要があります。レルムは、スタンドアロン Lightweight Directory Access Protocol (LDAP) レジストリーのマシン名である場合もあります。

LDAP プロトコルをサポートするユーザー・レジストリーにリモート側からアクセスできるので、複数ノード構成がサポートされます。したがって、どこからでも認証を使用可能にできます。

セキュリティー・ドメインの基本要件は、セキュリティー・ドメイン内の 1 つのサーバーからレジストリーまたはリポジトリーによって戻されるアクセス ID が、同じセキュリティー・ドメイン内の他のすべてのサーバー上のレジストリーまたはリポジトリーから戻されるアクセス ID と同じであることです。アクセス ID は、ユーザーを一意的に識別するための情報であり、リソースへのアクセスが許可されているかどうかを判別するために使用されます。

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。

管理セキュリティーを有効にする理由

管理セキュリティーを有効にすると、サーバーを無許可ユーザーから保護するための設定がアクティブになります。管理セキュリティーは、プロファイルの作成中にデフォルトで使用可能になっています。開発システムのような環境では、セキュリティーが不要な場合もあります。このようなシステム上では、管理セキュリティーを使用不可に設定できます。しかし、通常の環境では、管理コンソールやビジネス・アプリケーションに無許可ユーザーがアクセスできないようにすることをお勧めします。アクセスを制限するには、管理セキュリティーを使用可能にする必要があります。

管理セキュリティーで保護される対象

セキュリティー・ドメインに対する管理セキュリティーの構成には、以下のテクノロジーの構成が含まれます。

- HTTP クライアントの認証
- IIOP クライアントの認証
- 管理コンソール・セキュリティー
- ネーミング・セキュリティー
- SSL トランスポートの使用
- サーブレット、エンタープライズ Bean、および MBean のロール・ベースの許可検査
- ID の伝搬 (RunAs)

- 共通ユーザー・レジストリー
- 認証メカニズム

セキュリティー・ドメインの動作を定義するその他のセキュリティー情報:

- 認証プロトコル (Remote Method Invocation over the Internet Inter-ORB Protocol (RMI/IIOP) セキュリティー)
- その他の各種属性

アプリケーション・セキュリティー

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 の以前のリリースでは、ユーザーがグローバル・セキュリティーを使用可能にすると、管理セキュリティーとアプリケーション・セキュリティーが両方とも使用可能になっていました。今回のリリースでは、グローバル・セキュリティーという概念が管理セキュリティーとアプリケーション・セキュリティーに分割されたので、それぞれを個別に使用可能に設定できます。

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

Java 2 セキュリティーは、ポリシー・ベースの細分化されたアクセス制御メカニズムを提供します。これにより、保護されている特定のシステム・リソースへのアクセスを許可する前に権限が検査されるため、システムの全体的な保全性が向上します。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。Java 2 Platform, Enterprise Edition (J2EE) セキュリティーは、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を保護します。

WebSphere Process Server セキュリティーには、以下のテクノロジーが含まれます。

- Java 2 セキュリティー・マネージャー
- Java 認証・承認サービス (JAAS)
- Java 2 コネクター認証データ入力
- J2EE ロール・ベースの許可
- Secure Sockets Layer (SSL) 構成

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とどのような結果が起こ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。

Java 2 セキュリティーについて詳しくは、関連情報を参照してください。

関連情報

Java 2 セキュリティー

ユーザー・アカウント・リポジトリーの構成

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・リポジトリーに保管されます。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・リポジトリー (デフォルト)、Lightweight Directory Access Protocol (LDAP)、統合リポジトリー、またはカスタム・アカウント・リポジトリー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・リポジトリーとは、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・リポジトリーを選択します。

注: Windows Linux UNIX i5/OS Network Deployment 環境の場合、LDAP をユーザー・レジストリーとして使用する必要があります。

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。 「**セキュリティー**」を展開し、「**管理、アプリケーション、インフラストラクチャーの保護**」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	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。 • 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 • 1 つ以上の外部リポジトリー • 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 **注:** 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。
ローカル・オペレーティング・システム	これはデフォルトのユーザー・レジストリーです。 17 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。 **注:** Network Deployment 環境では、ローカル・オペレーティング・システムをユーザー・レジストリーとして使用しないでください。
Lightweight Directory Access Protocol (LDAP)	『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	17 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。
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。

関連概念

3 ページの『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。

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。

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、「**管理、アプリケーション、インフラストラクチャーの保護**」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、「**セキュリティー**」 → 「**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)**」 → 「**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。
   - 「**リポジトリー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 6.0.x 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 6.0.x node)**」に、セキュリティー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. 「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。

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す。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。

Network Deployment 環境では、LDAP を使用する必要があります。

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。

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、「**管理、アプリケーション、インフラストラクチャーの保護**」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、「**セキュリティー**」 → 「**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)**」 → 「**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。
      - 「**リポジトリー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 6.0.x 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 6.0.x node)**」に、セキュリティー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® 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

管理セキュリティーが使用可能になっている場合、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、この認証が必要です。

始める前に

管理セキュリティーが使用可能になっている必要があります。

手順

1. サーバーを始動します。

   次の表に、サーバーを始動するためのオプションを示します。

サーバーの始動	詳細
ファースト・ステップのユーザー・インターフェースから	「サーバーの起動」をクリックします。
コマンド行から	以下のコマンドを入力します。 • Windows **Windows® プラットフォームの場合:** startserver *servername* • Linux UNIX **Linux® および UNIX® プラットフォームの場合:** startserver.sh *servername* • i5/OS **System i® の場合 (QShell コマンド行から):** コマンド・プロンプトで *install_dir*/bin ディレクトリーから startserver *servername*。

   注: サーバーを始動するには、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他の管理操作の実行には、認証を受ける必要があります。
   サーバーが始動するか、またはエラー・メッセージが戻されます。
2. サーバーを停止します。

次の表に、サーバーを停止するためのオプションを示します。

サーバーの停止	詳細
ファースト・ステップのユーザー・インターフェースから	「サーバーの停止」をクリックし、プロンプトが表示されたら有効なユーザー名とパスワードを入力します。入力するユーザー名は、オペレーター・ロールまたは管理者ロールのいずれかである必要があります。
コマンド行から	以下のコマンドを入力します。 • Windows **Windows プラットフォームの場合:** stopserver *servername* -profileName *ProfileName* -username *username* -password *password* • Linux UNIX **Linux および UNIX プラットフォームの場合:** stopserver.sh *servername* -profileName *ProfileName* -username *username* -password *password* • i5/OS **System i の場合 (QShell コマンド行から):** コマンド・プロンプトで *install_dir*/bin ディレクトリーから stopserver *servername* -profileName *ProfileName* -username *username* -password *password*。入力するユーザー名は、オペレーター・ロールまたは管理者ロールのメンバーである必要があります。

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、サーバーは停止します。

3. サーバーが正常に停止したことを確認します。

次の表に、サーバーが正常に停止したことを確認するためのオプションを示します。

サーバーが正常に停止したことを確認します。	詳細
ユーザー・インターフェースから	ファースト・ステップ出力ウィンドウに、入力した要求の結果の詳細が表示されます。
コマンド行から	入力した要求の結果は、要求が入力されたコマンド・ウィンドウに表示されます。

管理セキュリティー・ロール

いくつかの管理セキュリティー・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 7 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。管理セキュリティー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 7 つのロールの 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. 管理セキュリティー・ロール

管理セキュリティー・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。 • サーバーのユーザー ID とパスワードの変更 • ユーザーとグループの管理者ロールへのマッピング 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。 • LTPA パスワード • 鍵
Adminsecuritymanager	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ー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。詳しくは、『管理の役割 (Administrative roles)』を参照してください。
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。

表 2. 管理セキュリティー・ロール (続き)

管理セキュリティー・ロール	説明
iscadmins	このロールは、管理コンソール・ユーザーのみが使用でき、wsadmin ユーザーは使用できません。このロールを付与されたユーザーは、統合リポジトリー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、iscadmins ロールのユーザーは、以下のタスクを実行できます。 • フェデレーテッド・リポジトリー構成でのユーザーの作成、更新、または削除 • フェデレーテッド・リポジトリー構成でのグループの作成、更新、または削除

管理セキュリティー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。ベスト・プラクティスとしては、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することです。これは、管理がより柔軟で容易なためです。 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。

インストール済みコンポーネントのデフォルトのセキュリティー

WebSphere Process Server の数種類の重要なコンポーネントには、デフォルトのセキュリティー情報が保持されています。これらの情報には、デフォルトのユーザーがマップされる別名やこれらのコンポーネントを呼び出すためにアクセスをユーザーに付与する必要があるセキュリティー・ロールが含まれています。

WebSphere Process Server の、Business Process Choreographer、Common Event Infrastructure、および Service Component Architecture の各コンポーネントは、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を認証します。プ

ロファイルの作成中には、これらの認証別名にはメイン管理者のユーザー ID とパスワードがデフォルト値として指定されます。これらの別名は、ユーザー・アカウント・リポジトリー内の他のユーザーに対応するように構成してください。

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 3 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 3. 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。	ユーザー名とパスワードは、プロファイル管理ツールの「Business Process Choreographer の構成」パネルから入力します。
BPEAuthDataAlias*DbType_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。

表 4 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 4. 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。	ユーザー名とパスワードは、プロファイル管理ツールの「Business Process Choreographer の構成」パネルから入力します。
EscalationUser	task.ear MDB によって使用されます。	ユーザー名とパスワードは、プロファイル管理ツールの「Business Process Choreographer の構成」パネルから入力します。

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。

28 ページの表 5 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 5. 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。	プロファイル管理ツールの Common Event Infrastructure 構成パネルで、ユーザー名とパスワードを入力します。
EventAuthAlias*DBType*	データベースで認証するために使用します。	プロファイル管理ツールの Common Event Infrastructure 構成パネルで、ユーザー名とパスワードを入力します。

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 6 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 6. 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。	プロファイル管理ツールの SCA 構成パネルで、ユーザー名とパスワードを入力します。

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

Business Process Choreographer は、WebSphere Process Server インストールの一部としてインストールされます。このインストール中に、(アクセス制御用の) ロールが関連付けられたエンタープライズ・アーカイブ (EAR) ファイルがインストールされます。Human Task Manager 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。

EAR ファイルおよび関連したロールを表 7 に示します。

表 7. EAR ファイルのロールおよびデフォルトの許可

EAR ファイル	ロール	デフォルトの許可	注
bpecontainer.ear	BPESystemAdministrator	インストール時に入力されるグループ名。	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。
bpecontainer.ear	BPESystemMonitor	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。
task.ear	TaskSystemAdministrator	インストール時に入力されるグループ名。	すべてのヒューマン・タスクにアクセス可能。

表 7. EAR ファイルのロールおよびデフォルトの許可 (続き)

EAR ファイル	ロール	デフォルトの許可	注
task.ear	TaskSystemMonitor	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。
Bpcexplorer.ear	WebClientUser	すべての認証済みユーザー。	Business Process Choreographer Explorer にアクセス可能。

Common Event Infrastructure アプリケーションにおけるアクセス制御

Common Event Infrastructure は、WebSphere Process Server インストールの一部としてインストールされます。インストール中に、アクセス制御用に関連付けられたロールを持つ EventServer.ear ファイルがインストールされます。

以下のロールが、EventServer.ear ファイルに関連付けられています。

ロール	デフォルトの許可
eventAdministrator	すべての認証済みユーザー。
eventConsumer	すべての認証済みユーザー。
eventUpdater	すべての認証済みユーザー。
eventCreator	すべての認証済みユーザー。
catalogAdministrator	すべての認証済みユーザー。
catalogReader	すべての認証済みユーザー。

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のタスクを実行します。

関連概念

3 ページの『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。

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。

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確認してください。

このタスクについて

ご使用の WebSphere Process Server 環境は、プロファイル内で定義されています。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。

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

1. 管理セキュリティーが有効であることを確認します。 11 ページの『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。 51 ページの『WebSphere Process Server におけるアプリケーションの保護』
3. ユーザーまたはグループを管理ロールに追加します。 管理権限は、個別ユーザーまたはユーザー・グループに対して付与できます。設定するには、「**管理ユーザーのロール (Administrative User Roles)**」または「**管理グループのロール (Administrative Group Roles)**」のいずれかを選択します。
4. 使用するユーザー・アカウント・リポジ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	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。 • 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 • 1 つ以上の外部リポジトリー • 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 **注:** 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。

ユーザー・レジストリー	アクション
ローカル・オペレーティング・システム	デフォルトのユーザー・レジストリーです。ユーザー・アカウント・レジストリーの構成方法について詳しくは、 17 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』を参照してください。
スタンドアロン LDAP レジストリー	『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。
スタンドアロン・カスタム・レジストリー	ユーザー・アカウント・レジストリーの構成方法について詳しくは、 17 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』を参照してください。

5. 選択したレジストリーが現在のレジストリーとして設定されていることを確認します。

   設定されていない場合は、「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)」ページの下部にある「**現行として設定 (Set as current)**」をクリックします。
6. ユーザー・レジストリーの選択後、変更が適用されていることを確認します。

   適用されていない場合は、「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)」ページの下部にある「**適用**」をクリックします。
7. 「ビジネス・インテグレーション・セキュリティー」パネルに進みます。 「**セキュリティー**」を展開して、「**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。
8. リストされた認証別名に対して適切なユーザー ID を指定します。 指定する資格情報は、使用しているユーザー・アカウント・リポジトリー内に存在する必要があります。システムのセキュリティーを維持するためには、認証別名として機能する適切なユーザー ID を選択することが重要です。
9. 同じパネル上で、Business Process Choreographer のセキュリティーを構成できます。

   Business Flow Manager および Human Task Manager 用の Business Process Choreographer ユーザー・ロール・マッピングを設定します。

   - **管理者**: ビジネス・フローおよびヒューマン・タスク管理者ロールのユーザー名またはグループ名 (あるいはその両方)。このロールに割り当てられるユーザーにはすべての特権があります。
   - **モニター**: ビジネス・フローおよびヒューマン・タスク・モニター・ロールのユーザー名またはグループ名 (あるいはその両方)。このロールを割り当て

られたユーザーは、すべてのビジネス・プロセスおよびタスク・オブジェクトのプロパティーを表示することができます。

Business Process Choreographer 認証別名は、Business Process Choreographer のインストール先である各デプロイメント・ターゲットに対して構成できます。以下の認証別名がリストされています。

- **JMS API 認証**: 非同期 API 呼び出しを処理するための Business Flow Manager メッセージ駆動型 Bean の認証。
- **エスカレーション・ユーザー認証**: 非同期 API 呼び出しを処理するための Human Task Manager メッセージ駆動型 Bean の認証。

10. 以上の変更内容を適用します。

    パネルの下部の「**適用**」ボタンをクリックします。

11. 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。

12. セキュリティー情報がセルのノードに確実に伝搬されるようにします。

    管理コンソールの「**システム管理**」を展開し、「**ノード**」をクリックします。「**完全再同期**」をクリックします。

13. 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。

タスクの結果

管理コンソールに次にログインする際には、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。

次のタスク

作成する各プロファイルは、以上のような方法で保護される必要があります。 システム管理者のユーザー ID は、環境のインストールと構成を実行中に複数の場所で使用されることがあります。コア・セキュリティー機能以外のすべての機能で、この ID をユーザー・アカウント・リポジトリーからの適切なユーザー資格情報に置き換えることをお勧めします。これらの ID および別名を管理するには、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**」パネルを使用します。

関連タスク

11 ページの『セキュリティーの有効化』
ご使用の WebSphere Process Server 環境およびご使用のアプリケーションを保護するための最初のステップは、管理セキュリティーを有効にすることです。

51 ページの『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。

関連情報

 WebSphere Process Server でのインストール検査ツールの使用 (Using the installation verification tools with WebSphere Process Server)

セキュリティーの有効化

ご使用の WebSphere Process Server 環境およびご使用のアプリケーションを保護するための最初のステップは、管理セキュリティーを有効にすることです。

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 のセキュリティーについて詳しくは、「**サブトピック (Subtopics)**」の下にリストされている情報を参照してください。

手順

1. 管理コンソールで「管理セキュリティー」パネルを開きます。

   「**セキュリティー**」を展開し、「**管理、アプリケーション、インフラストラクチャーの保護**」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、アプリケーションに対して認可すべきでないと J2EE 1.3 仕様で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。

   パネルの下部の「**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。

関連概念

3 ページの『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。

関連タスク

51 ページの『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。

関連情報

Java 2 セキュリティー・ポリシー・ファイルの構成

管理セキュリティー

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」であると考えることができます。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・リポジトリーの選択などが含まれます。具体的にいうと、認証やロール・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は、セキュリティー・ドメイン全体で有効なセキュリティー構成に相当します。各セキュリティー・ドメインは、同じユーザー・レジストリー・レルム名を使用して構成されたすべてのサーバーから成り立っています。レルムは、ローカル・オペレーティング・システム・レジストリーのマシン名である場合があります。この場合には、すべてのアプリケーション・サーバーが同じ物理マシン上に存在する必要があります。レルムは、スタンドアロン Lightweight Directory Access Protocol (LDAP) レジストリーのマシン名である場合もあります。

LDAP プロトコルをサポートするユーザー・レジストリーにリモート側からアクセスできるので、複数ノード構成がサポートされます。したがって、どこからでも認証を使用可能にできます。

セキュリティー・ドメインの基本要件は、セキュリティー・ドメイン内の 1 つのサーバーからレジストリーまたはリポジトリーによって戻されるアクセス ID が、同じセキュリティー・ドメイン内の他のすべてのサーバー上のレジストリーまたはリポジトリーから戻されるアクセス ID と同じであることです。アクセス ID は、ユーザーを一意的に識別するための情報であり、リソースへのアクセスが許可されているかどうかを判別するために使用されます。

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。

管理セキュリティーを有効にする理由

管理セキュリティーを有効にすると、サーバーを無許可ユーザーから保護するための設定がアクティブになります。管理セキュリティーは、プロファイルの作成中にデフォルトで使用可能になっています。開発システムのような環境では、セキュリティーが不要な場合もあります。このようなシステム上では、管理セキュリティーを使用不可に設定できます。しかし、通常の環境では、管理コンソールやビジネス・アプリケーションに無許可ユーザーがアクセスできないようにすることをお勧めします。アクセスを制限するには、管理セキュリティーを使用可能にする必要があります。

管理セキュリティーで保護される対象

セキュリティー・ドメインに対する管理セキュリティーの構成には、以下のテクノロジーの構成が含まれます。

- HTTP クライアントの認証
- IIOP クライアントの認証
- 管理コンソール・セキュリティー
- ネーミング・セキュリティー
- SSL トランスポートの使用

- サーブレット、エンタープライズ Bean、および MBean のロール・ベースの許可検査
- ID の伝搬 (RunAs)
- 共通ユーザー・レジストリー
- 認証メカニズム

セキュリティー・ドメインの動作を定義するその他のセキュリティー情報:

- 認証プロトコル (Remote Method Invocation over the Internet Inter-ORB Protocol (RMI/IIOP) セキュリティー)
- その他の各種属性

アプリケーション・セキュリティー

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 の以前のリリースでは、ユーザーがグローバル・セキュリティーを使用可能にすると、管理セキュリティーとアプリケーション・セキュリティーが両方とも使用可能になっていました。今回のリリースでは、グローバル・セキュリティーという概念が管理セキュリティーとアプリケーション・セキュリティーに分割されたので、それぞれを個別に使用可能に設定できます。

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

Java 2 セキュリティーは、ポリシー・ベースの細分化されたアクセス制御メカニズムを提供します。これにより、保護されている特定のシステム・リソースへのアクセスを許可する前に権限が検査されるため、システムの全体的な保全性が向上します。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。Java 2 Platform, Enterprise Edition (J2EE) セキュリティーは、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を保護します。

WebSphere Process Server セキュリティーには、以下のテクノロジーが含まれます。

- Java 2 セキュリティー・マネージャー
- Java 認証・承認サービス (JAAS)
- Java 2 コネクター認証データ入力
- J2EE ロール・ベースの許可
- Secure Sockets Layer (SSL) 構成

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とどのような結果が起こ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。

Java 2 セキュリティーについて詳しくは、関連情報を参照してください。

関連情報

Java 2 セキュリティー

ユーザー・アカウント・リポジトリーの構成

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・リポジトリーに保管されます。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・リポジトリー (デフォルト)、Lightweight Directory Access Protocol (LDAP)、統合リポジトリー、またはカスタム・アカウント・リポジトリー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・リポジトリーとは、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・リポジトリーを選択します。

注: Windows Linux UNIX i5/OS Network Deployment 環境の場合、LDAP をユーザー・レジストリーとして使用する必要があります。

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。 「**セキュリティー**」を展開し、「**管理、アプリケーション、インフラストラクチャーの保護**」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	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。 • 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 • 1 つ以上の外部リポジトリー • 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 **注:** 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。
ローカル・オペレーティング・システム	これはデフォルトのユーザー・レジストリーです。 17 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。 **注:** Network Deployment 環境では、ローカル・オペレーティング・システムをユーザー・レジストリーとして使用しないでください。
Lightweight Directory Access Protocol (LDAP)	『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	17 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。
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。

関連概念

3 ページの『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。

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。

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、「**管理、アプリケーション、インフラストラクチャーの保護**」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、「**セキュリティー**」 → 「**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)**」 → 「**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。
   - 「**リポジトリー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 6.0.x 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 6.0.x node)**」に、セキュリティー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. 「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。

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す。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。

Network Deployment 環境では、LDAP を使用する必要があります。

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。

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、「**管理、アプリケーション、インフラストラクチャーの保護**」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、「**セキュリティー**」 → 「**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)**」 → 「**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。
      - 「**リポジトリー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 6.0.x 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 6.0.x node)**」に、セキュリティー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 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

管理セキュリティーが使用可能になっている場合、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、この認証が必要です。

始める前に

管理セキュリティーが使用可能になっている必要があります。

手順

1. サーバーを始動します。

   次の表に、サーバーを始動するためのオプションを示します。

サーバーの始動	詳細
ファースト・ステップのユーザー・インターフェースから	「サーバーの起動」をクリックします。
コマンド行から	以下のコマンドを入力します。 • Windows **Windows プラットフォームの場合:** startserver *servername* • Linux UNIX **Linux および UNIX プラットフォームの場合:** startserver.sh *servername* • i5/OS **System i の場合 (QShell コマンド行から):** コマンド・プロンプトで *install_dir*/bin ディレクトリーから startserver *servername*。

   注: サーバーを始動するには、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他の管理操作の実行には、認証を受ける必要があります。
   サーバーが始動するか、またはエラー・メッセージが戻されます。
2. サーバーを停止します。

次の表に、サーバーを停止するためのオプションを示します。

サーバーの停止	詳細
ファースト・ステップのユーザー・インターフェースから	「サーバーの停止」をクリックし、プロンプトが表示されたら有効なユーザー名とパスワードを入力します。入力するユーザー名は、オペレーター・ロールまたは管理者ロールのいずれかである必要があります。
コマンド行から	以下のコマンドを入力します。 • Windows **Windows プラットフォームの場合:** stopserver *servername* -profileName *ProfileName* -username *username* -password *password* • Linux UNIX **Linux および UNIX プラットフォームの場合:** stopserver.sh *servername* -profileName *ProfileName* -username *username* -password *password* • i5/OS **System i の場合 (QShell コマンド行から):** コマンド・プロンプトで *install_dir*/bin ディレクトリーから stopserver *servername* -profileName *ProfileName* -username *username* -password *password*。入力するユーザー名は、オペレーター・ロールまたは管理者ロールのメンバーである必要があります。

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、サーバーは停止します。

3. サーバーが正常に停止したことを確認します。

次の表に、サーバーが正常に停止したことを確認するためのオプションを示します。

サーバーが正常に停止したことを確認します。	詳細
ユーザー・インターフェースから	ファースト・ステップ出力ウィンドウに、入力した要求の結果の詳細が表示されます。
コマンド行から	入力した要求の結果は、要求が入力されたコマンド・ウィンドウに表示されます。

管理セキュリティー・ロール

いくつかの管理セキュリティー・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 7 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。管理セキュリティー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 7 つのロールの 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 8. 管理セキュリティー・ロール

管理セキュリティー・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。 • サーバーのユーザー ID とパスワードの変更 • ユーザーとグループの管理者ロールへのマッピング 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。 • LTPA パスワード • 鍵
Adminsecuritymanager	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ー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。詳しくは、『管理の役割 (Administrative roles)』を参照してください。
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。

表 8. 管理セキュリティー・ロール (続き)

管理セキュリティー・ロール	説明
iscadmins	このロールは、管理コンソール・ユーザーのみが使用でき、wsadmin ユーザーは使用できません。このロールを付与されたユーザーは、統合リポジトリー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、iscadmins ロールのユーザーは、以下のタスクを実行できます。 • フェデレーテッド・リポジトリー構成でのユーザーの作成、更新、または削除 • フェデレーテッド・リポジトリー構成でのグループの作成、更新、または削除

管理セキュリティー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。ベスト・プラクティスとしては、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することです。これは、管理がより柔軟で容易なためです。 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。

インストール済みコンポーネントのデフォルトのセキュリティー

WebSphere Process Server の数種類の重要なコンポーネントには、デフォルトのセキュリティー情報が保持されています。これらの情報には、デフォルトのユーザーがマップされる別名やこれらのコンポーネントを呼び出すためにアクセスをユーザーに付与する必要があるセキュリティー・ロールが含まれています。

WebSphere Process Server の、Business Process Choreographer、Common Event Infrastructure、および Service Component Architecture の各コンポーネントは、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を認証します。プ

ロファイルの作成中には、これらの認証別名にはメイン管理者のユーザー ID とパスワードがデフォルト値として指定されます。これらの別名は、ユーザー・アカウント・リポジトリー内の他のユーザーに対応するように構成してください。

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。

27 ページの表 3 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 9. 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。	ユーザー名とパスワードは、プロファイル管理ツールの「Business Process Choreographer の構成」パネルから入力します。
BPEAuthDataAlias*DbType_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。

27 ページの表 4 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 10. 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。	ユーザー名とパスワードは、プロファイル管理ツールの「Business Process Choreographer の構成」パネルから入力します。
EscalationUser	task.ear MDB によって使用されます。	ユーザー名とパスワードは、プロファイル管理ツールの「Business Process Choreographer の構成」パネルから入力します。

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。

28 ページの表 5 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 11. 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。	プロファイル管理ツールの Common Event Infrastructure 構成パネルで、ユーザー名とパスワードを入力します。
EventAuthAlias*DBType*	データベースで認証するために使用します。	プロファイル管理ツールの Common Event Infrastructure 構成パネルで、ユーザー名とパスワードを入力します。

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。

28 ページの表 6 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 12. 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。	プロファイル管理ツールの SCA 構成パネルで、ユーザー名とパスワードを入力します。

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

Business Process Choreographer は、WebSphere Process Server インストールの一部としてインストールされます。このインストール中に、(アクセス制御用の) ロールが関連付けられたエンタープライズ・アーカイブ (EAR) ファイルがインストールされます。Human Task Manager 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。

EAR ファイルおよび関連したロールを 28 ページの表 7 に示します。

表 13. EAR ファイルのロールおよびデフォルトの許可

EAR ファイル	ロール	デフォルトの許可	注
bpecontainer.ear	BPESystemAdministrator	インストール時に入力されるグループ名。	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。
bpecontainer.ear	BPESystemMonitor	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。
task.ear	TaskSystemAdministrator	インストール時に入力されるグループ名。	すべてのヒューマン・タスクにアクセス可能。

表 13. EAR ファイルのロールおよびデフォルトの許可 (続き)

EAR ファイル	ロール	デフォルトの許可	注
task.ear	TaskSystemMonitor	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。
Bpcexplorer.ear	WebClientUser	すべての認証済みユーザー。	Business Process Choreographer Explorer にアクセス可能。

Common Event Infrastructure アプリケーションにおけるアクセス制御

Common Event Infrastructure は、WebSphere Process Server インストールの一部としてインストールされます。インストール中に、アクセス制御用に関連付けられたロールを持つ EventServer.ear ファイルがインストールされます。

以下のロールが、EventServer.ear ファイルに関連付けられています。

ロール	デフォルトの許可
eventAdministrator	すべての認証済みユーザー。
eventConsumer	すべての認証済みユーザー。
eventUpdater	すべての認証済みユーザー。
eventCreator	すべての認証済みユーザー。
catalogAdministrator	すべての認証済みユーザー。
catalogReader	すべての認証済みユーザー。

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。

以下の作業を実行して、お客様のアプリケーションを保護します。

手順

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、「**管理、アプリケーション、インフラストラクチャーの保護**」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。

関連タスク

11 ページの『セキュリティーの有効化』
ご使用の WebSphere Process Server 環境およびご使用のアプリケーションを保護するための最初のステップは、管理セキュリティーを有効にすることです。

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・セキュリティー
- 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・セキュリティー

ご使用の WebSphere Process Server アプリケーションのセキュリティーは、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、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

セキュリティーの最後の要素は 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

管理セキュリティー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と、例外が生成されます。

表 14 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 14. 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 (ブラウザー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。これらの Business Process Choreographer および Common Event Infrastructure の認証別名については、後続のトピックで説明します。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。

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生じます。

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

1. 「ビジネス・インテグレーション認証別名」パネルにアクセスします。

   管理コンソールで「**セキュリティー**」を展開して、「**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。

   注: このパネルには、認証別名情報を必要とするさまざまな管理コンソール・パネルからもアクセスできます。
   認証別名構成パネルが表示されます。

   このパネルには、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. 別名のプロパティーを変更します。

   選択した別名の認証別名構成パネルで、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」パネルに戻り、「**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、『セキュリティーを適用した *WebSphere Process Server* プロファイルの拡張』を参照してください。

   関連タスク

   6 ページの『セキュリティーを適用した WebSphere Process Server プロファイルの作成』
   WebSphere Process Server プロファイルの作成には、セキュリティー資格情報のデフォルト値が使用されます。プロファイルの作成後に、管理コンソールでこれらのセキュリティー設定を構成する必要があります。

アクセス制御

アクセス制御とは、認証済みユーザーがリソースにアクセスしたり、特定の操作を実行したりするために必要な許可 (アクセス権) を確実に得るようにすることです。

一般ユーザーを WebSphere Process Server に対して認証する場合、セキュリティー面で重要なことは、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はしないことです。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。

アクセス制御は、お客様が開発するコンポーネントを保護するために、調整可能です。この調整を行うには、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、その操作を J2EE 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。ここでは、これらのコンポーネントの詳細について説明します。

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 J2EE のロール・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、Business Calendar Manager 内では、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。ビジネス・スペース内のセキュリティー・マネージャーを使用して、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ライター・アクセス権限およびリーダー・アクセス権限を持つユーザーを指定します。

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。これらのコンポーネントに関連付けられたロール・ベース・セキュリティーの詳細を後続のトピックで説明します。

これらのコンポーネントの詳細について、以下で説明します。

表 15. .ear ファイルおよび関連する J2EE ロール

EAR ファイル	**J2EE ロール**	**ユーザー割り当て**
BPCExplorer_<node>_<server>	CleanupUser	すべての認証済み
BPCObserver_<node>_<server>	ObserverUser	すべての認証済み
BPEContainer_<node>_<server>	BPEAPIUser	すべての認証済み
	BPESystemAdministrator	wsadmin
	BPESystemMonitor	wsadmin
	CleanupUser	すべての認証済み
	JMSAPIUser	すべての認証済み
REST サービス・ゲートウェイ	RestServicesUser	すべての認証済み
TaskContainer_<node>_<server>	TaskAPIUser	すべての認証済み
	TaskSystemAdministrator	wsadmin
	TaskSystemMonitor	wsadmin

表 15. .ear ファイルおよび関連する J2EE ロール (続き)

EAR ファイル	J2EE ロール	ユーザー割り当て
	EscalationUser	すべての認証済み
	CleanupUser	すべての認証済み
wpsFEMgr_6.2.0	WBIOperator	全員
EventService (*)	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

(*) EventService はシステム・アプリケーションであり、管理コンソールでは「エンタープライズ・アプリケーション」の下にリストされません。

関連タスク

61 ページの『Business Calendar Manager のセキュリティー』
セキュリティー・マネージャーでは、Business Calendar Manager 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・マネージャーを使用して、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。

関連情報

WebSphere Integration Developer インフォメーション・センター

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、セキュリティーにとって重要です。

データのプライバシーとデータの保全性は、密接に関連している概念です。詳しくは、関連情報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。

保全性

保全性とは、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 ではハンドシェー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ークはありません。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。詳しくは、関連情報を参照してください。

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。

関連情報

セキュリティー計画の概要

モジュール・デプロイメント・プロパティーの編集

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・プロキシー・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。

関連情報

 Tivoli Access Manager または WebSEAL を使用したシングル・サインオン機能の構成

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ことが必要な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。これらの作業について詳しくは、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ロール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、「セキュリティー役割をユーザー/グループにマップ」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) サーブレットを呼び出し、このサー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「RunAs ロールをユーザーにマップ」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、「追加プロパティー」セク

ションのリンクとして「**セキュリティー役割をユーザー/グループにマップ**」リンクが表示されます。

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、「セキュリティー役割をユーザー/グループにマップ」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 を使用するように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 の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、パネル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提供されています。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. 残りのセキュリティー以外の関連の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、正しいクリデンシャル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。

関連概念

3 ページの『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。

関連情報

役割へのユーザーおよびグループの割り当て

RunAs ロールへのユーザーの割り当て

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 securityIdenitity 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

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、『実動サーバーへのモジュールのインストール』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	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。 • 全員 - セキュリティーなしと同等です。 • 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。 • 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。 • 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。 「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。
セキュリティー ID	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。

関連概念

3 ページの『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。

関連情報

代行

Business Calendar Manager のセキュリティー

セキュリティー・マネージャーでは、Business Calendar Manager 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・マネージャーを使用して、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。

Business Calendar Manager 内の各タイムテーブルに対して、所有者、ライター、またはリーダーの 3 つのロールのいずれか 1 つにメンバーを割り当てることができます。

セキュリティー・マネージャーは、Business Calendar Manager 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ビジネス・スペースに配置されています。

この Business Calendar Manager に対するロール・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。

セキュリティー・マネージャーを使用する利点

セキュリティー・マネージャーを使用して、Business Calendar Manager でのロール・ベースのアクセス制御を行う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、ライター、およびリーダーという 3 つのロールが作成されます。

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、実際に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。

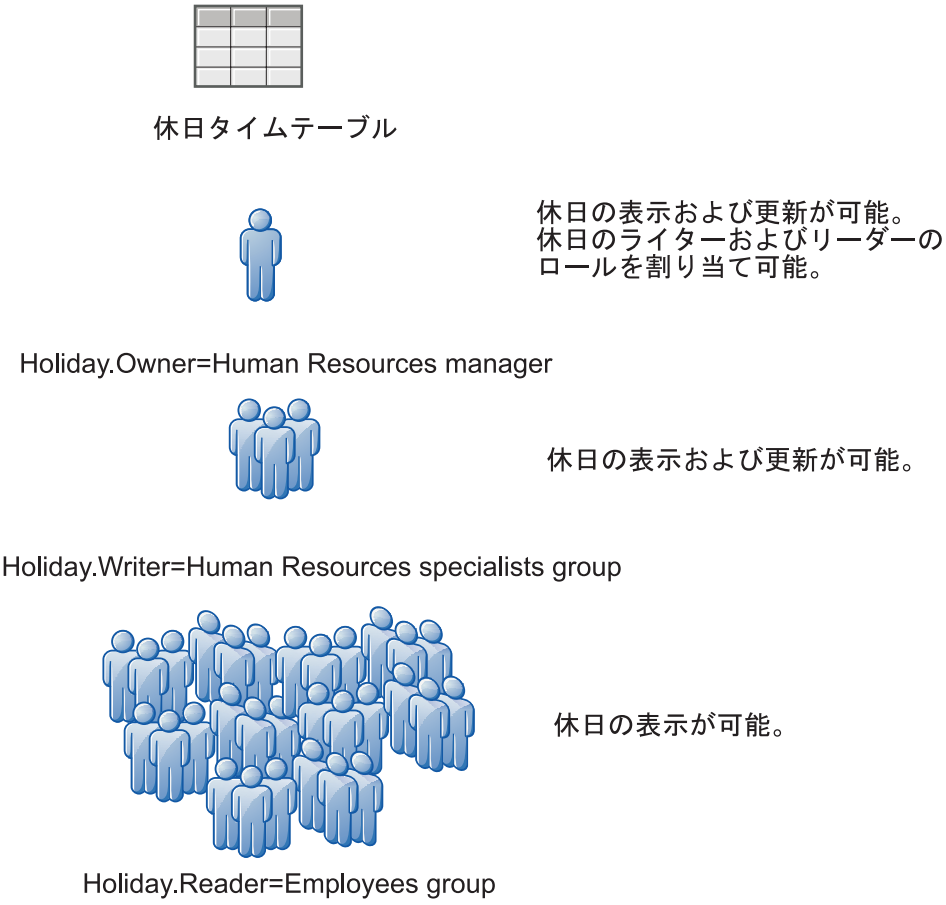


図 1. タイムテーブルに割り当てられたロールの例

タイムテーブルをデプロイすると、所有者、ライター、およびリーダーという 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、リーダー・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、他のメンバーをライター・ロールおよびリーダー・ロールに割り当てることができます。
- ライター・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。
- リーダー・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・マネージャーでは、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・マネージャーの管理ロール

WebSphere Process Server をインストール (または WebSphere Process Server 6.2 にアップグレード) した後、サーバーを再始動すると、以下のロールが作成されます。

- 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、ライター、およびリーダーのロールに対して、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。

注: セキュリティー・マネージャーでは、これらのロールはシステム・ロールとしても知られています。

ロールのセットアップ

WebSphere Process Server をインストールした後、セキュリティー・マネージャーで以下のタスクを実行してください。

1. BPMAdmin が BPMRoleManager ロールの再割り当てを行います。
2. BPMRoleManager は、3 つのタイムテーブル関連のロールのどれか 1 つにメンバーを割り当てます。

これらのタスクの実行方法については、セキュリティー・マネージャーのヘルプ・トピックを参照してください。

関連概念

3 ページの『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。

55 ページの『アクセス制御』
アクセス制御とは、認証済みユーザーがリソースにアクセスしたり、特定の操作を実行したりするために必要な許可 (アクセス権) を確実に得るようにすることです。

 WebSphere が提供するビジネス・スペース
WebSphere Process Server WebSphere が提供するビジネス・スペース が含まれています。これは IBM® WebSphere Business Process Management ポートフォリオ横断の Web インターフェースを作成、管理および統合するための共通インターフェースをアプリケーション・ユーザーに提供します。

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) と通信するためのメカニズムです。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、アプリケーションが統合ブローカーを介してビジネス・データを交換できるようにする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) とツールで構成されています。WebSphere Business Integration Adapters は、JMS メッセージングに依存していますが、JMS はセキュリティー・コンテキスト伝搬をサポートしていません。

WebSphere Adapters は、WebSphere Process Server によってサポートされる J2EE コンポーネントと EIS の間の管理された双方向接続を可能にします。

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するため、セキュリティー・コンテキストの伝搬はできません。また、J2C もインバウンド・セキュリティーはサポートしていないため、WebSphere Adapters にもインバウンド通信の認証メカニズムはありません。

アダプターから WebSphere Process Server への入力には、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、メディエーション、ビジネス・プロセス、SCA Java コンポーネント、またはセレクターなどの SCA コンポーネントにワイヤーする必要があります。

セキュリティーの解決策は、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、例外のスローが防止されます。

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 に固有のものです。このリンクを保護する方法について詳しくは、EIS の資料を参照してください。

関連概念

サービス統合バスのセキュリティー上の考慮事項

ヒューマン・タスクとビジネス・プロセスにおけるセキュリティー

ヒューマン・タスクとビジネス・プロセスに関連付けられたロールは数多く存在します。このトピックでは、選択可能なロールについて説明します。

ヒューマン・タスクは、その名のとおり、完了するために人間の介入を必要とします。一部のビジネス・プロセスも、人間の介入を必要とする場合があります。これらのヒューマン・タスクおよびビジネス・プロセスは、WebSphere Integration Developer を使用して開発され、Business Process Choreographer を使用して呼び出されます。タスクまたはプロセスを開発する場合は、ヒューマン・タスクおよびビジネス・プロセスに関係するユーザーまたはグループにロールを割り当てる必要があります。ロールの割り当て、または特定のロールに関連付けられたロールの照会について詳しくは、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。

Human Task Manager 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。

ヒューマン・タスクおよびビジネス・プロセスに関連付けられたロール

重要: こうしたロールは、Business Process Choreographer のビジネス・コンテナーとヒューマン・タスク・コンテナーで実行されているタスクとプロセスに固有のものです。

WebSphere Process Server は、タスクとプロセスに関する次のロールをサポートしています。

管理者 このロールに属するユーザーは、タスクとプロセスをモニター、終了、または削除し、タスクとプロセスについての情報を表示することもできます。

リーダー
このロールに属するユーザーは、タスクとプロセスの表示のみを行うことができます。

スターター
このロールに属するユーザーは、タスクとプロセスを開始または表示することができます。

タスクには次に示す追加のロールもあります。

所有者 このロールに属するユーザーは、すでに要求済みのタスクを保管、取り消し、完了、または表示することができます。

潜在的な所有者
このロールに属するユーザーは、タスクを要求および表示できます。

関連概念

プロセスのための許可および担当者割り当て

関連情報

許可および担当者割り当て

ビジネス・スペースのセキュリティーのセットアップ

製品のWebSphere が提供するビジネス・スペースのインストールおよび構成を行ったら、ビジネス・スペース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。アプリケーション・セキュリティーをセットアップできますが、その場合は、アプリケーションに管理セキュリティーも必要になります。さらに、Jython スクリプトを実行して、スーパーユーザー・ロールをビジネス・スペースに割り当てる必要もあります。

ビジネス・スペースのアプリケーション・セキュリティーの設定

ビジネス・スペースのセキュリティーをオンにするには、アプリケーション・セキュリティーおよび管理セキュリティーの両方を有効にする必要があります。

始める前に

このタスクの前に、以下のタスクを完了しておく必要があります。

- プロファイルの構成、およびそのプロファイルでのビジネス・スペースの構成。
- データベース表の構成 (リモート・データベースまたはデプロイメント環境を使用する場合)。
- ビジネス・スペースで使用するウィジェットの REST サービス・エンドポイントの構成。
- 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。

このタスクについて

アクセスの認証と権限を確実にするためにビジネス・スペースのエンタープライズ・アーカイブ (EAR) ファイルが事前構成済みである。ビジネス・スペースは、すべての認証ユーザーにマップされているデフォルトの J2EE ロールを使用し、これ

により、ビジネス・スペース URL にアクセスするときにユーザーに認証のプロンプトが表示されます。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。

ビジネス・スペース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ビジネス・スペース内で処理されます。

ビジネス・スペースへの認証アクセス (J2EE ロール・ベースの許可) を有効にするには、ユーザー・レジストリーを構成してアプリケーション・セキュリティーを有効にする必要があります。

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. ビジネス・スペース・アプリケーションの場合、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の管理コンソール・ページ上で、「**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**」の下で、「**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**」、 「**Lightweight Directory Access Protocol (LDAP)**」、または「**カスタム・ユーザー・レジストリー**」のいずれかを指定することができます。 ただし、ビジネス・スペースに対して「**フェデレーテッド・リポジトリー**」を選択すると、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の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とユーザー ID が含まれます。

次のタスク

- 管理およびアプリケーションのセキュリティーをオンにした後は、 ビジネス・スペースにログオンすると、ユーザー ID およびパスワードの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、ビジネス・スペースへのログインを制限したい場合は、ビジネス・スペース J2EE ロールのマッピングを変更することができます。「**アプリケーション**」 → 「**エンタープライズ・アプリケーション**」 → **アプリケーション名**をクリックします。右のパネルの、「詳細プロパティー」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・ロール**」を選択します。
- ビジネス・スペースのページおよびスペースへの権限を設定するには、ページおよびスペースを作成するときにビジネス・スペースでこれを管理することができます。
- 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・アプリケーションへのユーザーのマッピングを変更する必要があります。REST サービス・ゲートウェイ・アプリケーションを選択し、右のパネルの、「詳細プロパティー」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・ロール**」を選択します。RestServicesUser ロールの場合、ユーザーおよびグループを追加して、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ことができます。

- ユーザー・グループ・ロールに基づいてウィジェットのデータへのアクセスを制限したい場合は、管理グループ・ロールに割り当てたユーザーを変更することを検討してください。管理コンソールを開いて、「**セキュリティー**」 → 「**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**」 → 「**管理グループ・ロール**」 をクリックし、グループを選択することにより、ロール・リストを表示してこれらのロールに割り当てられているユーザーを確認することができます。

  ビジネス・ルールやビジネス変数などの、ウィジェットの管理グループ・ロールに割り当てられたユーザーを変更することを検討したい場合があります。

  例えば、ヘルス・モニター・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ヘルス・モニター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

  それらの管理グループ・ロールにマップされたユーザーは、ヘルス・モニターのデータへのアクセス権限を持ちます。それらのロールにマップされていないユーザーは、ヘルス・モニターのデータにアクセスできません。
- さらに、ウィジェットの中には、ビジネス・ユーザーが作成した成果物へのロール・ベースのアクセスの追加層を持つものもあります。ソリューション管理の場合、セキュリティー・マネージャー・ウィジェットを使用すると、Business Calendar Manager 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ユーザーおよびグループのシステム・ロールまたはモジュール・ロールを割り当てることができます。レビューの場合、Publishing Server Access Control ウィジェットは、レビューを行いコメントを入力できるユーザーのアクセス権限を管理します。詳しくは、ご使用のウィジェットのオンライン・ヘルプを参照してください。

ビジネス・スペースのスーパーユーザー・ロールの割り当て

ビジネス・スペースでは、スーパーユーザー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、ビジネス・スペース内のすべてのスペースとページの表示、編集、削除を行うことができ、また、どのスペースをテンプレートにするかを指定することができます。ユーザー ID に対して、ビジネス・スペースのスーパーユーザー・ロールを割り当てるスクリプトを実行したり、wsadmin スクリプト・クライアントを使用して、ビジネス・スペースのスーパーユーザーを有効にするスクリプトを作成することができます。

始める前に

製品のユーザー・レジストリーにユーザー ID が登録されている必要があります。

手順

1. スーパーユーザー・ロールをユーザーに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、ビジネス・スペース 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 -wsadmin_classpath install_root¥plugins¥com.ibm.bspace.plugin_6.2.0.jar -f createSuperUser.py user_short_name_in_VMM`

次のタスク

ユーザー名にスーパーユーザー・ロールが含まれているか照会する場合、またはスーパーユーザー・ロールを除去する場合は、他に 2 つのスクリプトが用意されています。両方とも、*install_root*/BusinessSpace/scripts/ ディレクトリーにあります。

- isSuperUser.py はユーザー名にスーパーユーザー・ロールが含まれているか照会します。
- removeSuperUserAccess.py は、ユーザーからスーパーユーザー・ロールを除去します。

提供されている 3 つのスクリプトに基づいて、追加スクリプトを作成することができます。スクリプト中の MBean 呼び出しを以下のいずれかのメソッドで置き換えて、スーパーユーザー・ロールを処理することができます。

```
public boolean assignSuperUserRole(String userId);
public boolean removeSuperUserRole(String userId);
public List getAllSuperUsers();
public boolean isSuperUser(String userId);
public boolean removeAllSuperUsers();
```

MBean 記述子ファイル BSpaceSecurityAdminMBean.xml を参照してください。このファイルは *install_root*/BusinessSpace/scripts に格納されています。

ビジネス・スペースを開くには、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。

エンドツーエンド・セキュリティーの構築

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。

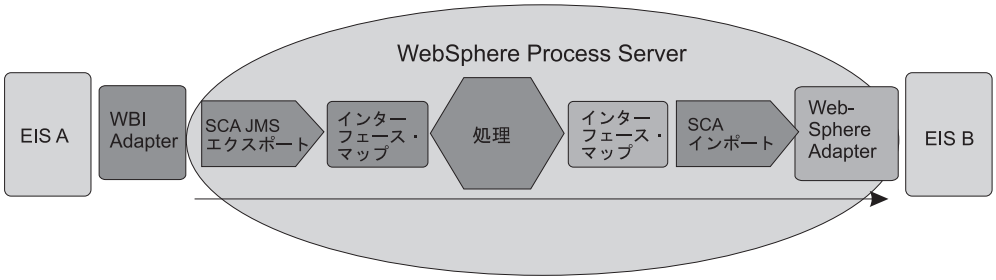
手順

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

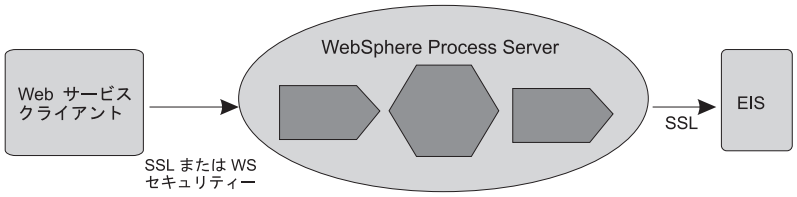
インバウンド要求は、WebSphere Business Integration Adapter で受信します。 Service Component Architecture (SCA) は、SCA エクスポートに基づいてインターフェース・マップを呼び出します。この要求は、処理コンポーネントおよび 2 番目のインターフェース・マップを経由した後、WebSphere Adapter を経由して 2 番目の EIS (B) に渡されます。これらは、あるコンポーネントが次のコンポーネントのメソッドを呼び出していく SCA 呼び出しです。



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 (この場合は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

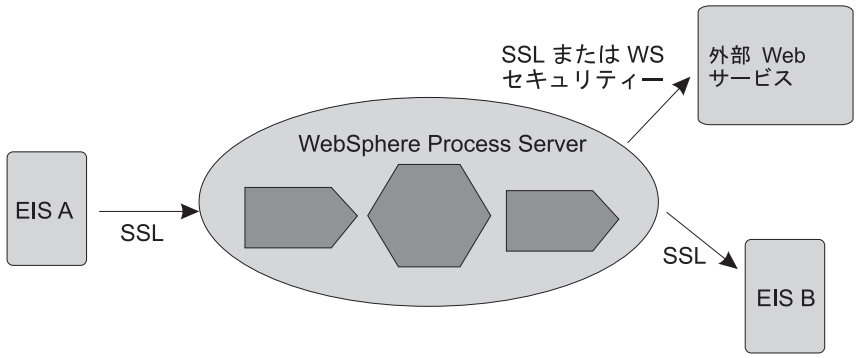
このシナリオでは、Web サービス・クライアントが WebSphere Process Server のコンポーネントを呼び出します。要求は、アダプターによって EIS に渡される前に WebSphere Process Server 環境内で数種類のコンポーネントを経由します。



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 (例えば、BPEL コンポーネント) は、外部 Web サービスを呼び出します。



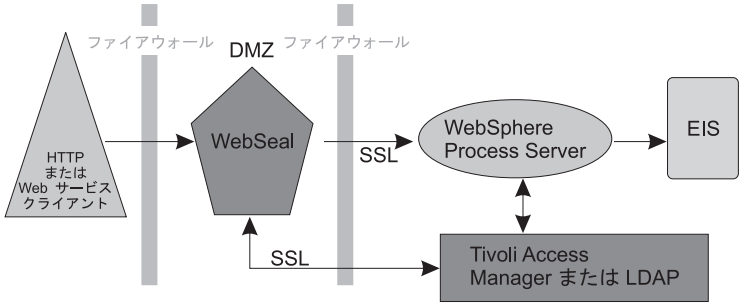
インバウンド Web サービス要求の場合、HTTP 基本認証または WS-Security 認証を使用して、SSL クライアントとして外部の Web サービスを認証することができます。LTPACallBackHandler をコールバック・メカニズムとして使用して、現在の RunAs サブジェクトから usernameToken を抽出します。WebSphere Process Server とターゲットの Web サービスとの間で、WS-Security を使用してデータのプライバシーおよび保全性を確保することができます。

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・プロキシーとして使用され、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。



関連概念

サービス統合バスのセキュリティー上の考慮事項

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-8711
東京都港区六本木 3-2-12
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
1001 Hillsdale Blvd., Suite 400
Foster City, CA 94404
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。(c) (お客様の会社名) (西暦年)。このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 (C) Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

プログラミング・インターフェース情報がある場合、それらはこのプログラムを使用してアプリケーション・ソフトウェアを作成する際に役立つよう提供されています。

一般使用プログラミング・インターフェースにより、お客様はこのプログラム・ツール・サービスを含むアプリケーション・ソフトウェアを書くことができます。

ただし、この情報には、診断、修正、および調整情報が含まれている場合があります。診断、修正、調整情報は、お客様のアプリケーション・ソフトウェアのデバッグ支援のために提供されています。

警告: 診断、修正、調整情報は、変更される場合がありますので、プログラミング・インターフェースとしては使用しないでください。

商標

IBM、IBM ロゴ、および ibm.com は、International Business Machines Corporation の米国およびその他の国における商標または登録商標です。これらおよび他の IBM 商標に、この情報の最初に現れる個所で商標表示 (® または ™) が付されている場合、これらの表示は、この情報が公開された時点で、米国において、IBM が所有する登録商標またはコモン・ロー上の商標であることを示しています。このような商標は、その他の国においても登録商標またはコモン・ロー上の商標である可能性があります。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」をご覧ください。

Windows は、Microsoft Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Java および JavaBeans は、Sun Microsystems, Inc. の米国およびその他の国における商標です。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

この製品には、Eclipse Project (http://www.eclipse.org) により開発されたソフトウェアが含まれています。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12