WebSphere. WebSphere Process Server for z/OS

バージョン 6.1.0

アプリケーションと環境の保護

WebSphere WebSphere Process Server for z/OS

バージョン 6.1.0

アプリケーションと環境の保護

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。

本書は、WebSphere Process Server for z/OS (製品番号 5655-N53) バージョン 6、リリース 1、モディフィケーション 0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

IBM 発行のマニュアルに関する情報のページ

`http://www.ibm.com/jp/manuals/`

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。

(URL は、変更になる場合があります)

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 z/OS
Version 6.1.0
Securing Applications and Their Environments

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2008.2

目次

アプリケーションとその環境の保護

WebSphere® Process Server 環境およびお客様のアプリケーションのセキュリティーは、非常に重要です。

1. ここに示す情報は、Adobe® PDF 形式で、WebSphere Process Server の資料 (PDF 形式) から入手できます。
2. IBM® developerWorks® の Business Process Management 情報のロードマップには、WebSphere Process Server およびポートフォリオのその他の製品に関する情報がまとめられています。

これらの資料は、WebSphere Application Server インフォメーション・センター、具体的には WebSphere Application Server セキュリティー資料にある中核的なセキュリティー資料を補足するものです。

データおよびプロセスのセキュリティーは重要です。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。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・センターを参照してください。

概説

データおよびプロセスのセキュリティーは重要です。

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。セキュリティーについて詳しくは、WebSphere Application Server Network Deployment バージョン 6 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 環境でのセキュリティーの管理に操作と 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。以下のような局面があります。

- **38 ページの『認証』**: アプリケーションを呼び出すユーザーまたはプロセスを認証する必要があります。
- **40 ページの『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確認します。

- **40 ページの『データの保全性とプライバシー』**: アプリケーションがアクセスするデータを保護して、無許可ユーザーがデータを一切表示または変更できないようにする必要があります。
- **42 ページの『シングル・サインオン』**: シングル・サインオンを使用すると、ユーザーが認証データを指定するのは 1 回のみでよく、この認証情報がダウンストリームのコンポーネントへ渡されます。

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

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

WebSphere Process Server のセキュリティーの基盤となるのは、WebSphere Application Server 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。

WebSphere Process Server のセキュリティー機能

- 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。使用するには、「**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。
- コンポーネント固有のセキュリティー・ロールのセットがあります。

セキュリティーの概要

WebSphere Process Server のインストールを計画するときでも、アプリケーションを開発およびデプロイするときでも、プロセス・サーバーを日常的に運用するときでも、セキュリティーについての考慮は不可欠です。

このタスクについて

機密データのセキュリティーを維持するには、プロセス・サーバー環境およびその環境にデプロイするアプリケーションの両方を保護する必要があります。

プロシージャー

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。 3 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』を参照してください。
2. ご使用のスタンドアロン・インストール済み環境またはデプロイメント環境に対するセキュリティーが有効であることを確認します。

a. 10 ページの『管理セキュリティー』が有効であることを確認します。 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。
b. 11 ページの『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。 アプリケーション・セキュリティーは、デフォルトで有効になっています。
c. 必要な場合は、 11 ページの『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を使用して、セキュリティー・オプションを構成します。
e. セキュアな認証メカニズムおよびユーザー・アカウント・リポジトリーをセットアップします。
f. ユーザー名およびパスワードを重要な ビジネス・インテグレーション認証別名に割り当てます。
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. 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. 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て、新しくデプロイしたアプリケーションへのアクセスを制御します。
   d. ご使用の WebSphere Process Server 環境のセキュリティーを維持管理します。

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

WebSphere Process Server のインストール前、インストール中、およびインストール後にこれらのタスクを実行し、セキュリティーをインプリメントします。

このタスクについて

以下の作業を WebSphere Process Server のインストール時に実行してください。

プロシージャー

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 for z/OS インフォメーション・センターのトピック『**インストール時のセキュリティーの準備**』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。

   インストールのためのご使用の z/OS® オペレーティング・システムの準備については、 WebSphere Application Server インフォメーション・センターのトピック『基本オペレーティング・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 for z/OS のインストールと構成を行った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。インストールおよび構成の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**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

インストール時に入力する認証情報

WebSphere Process Server の以前のリリースでは、インストール中にさまざまな認証情報の入力が求められていました。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することをお勧めします。

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

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

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

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

このタスクについて

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

これらのユーザー名とパスワードは認証別名を作成するために使用され、セキュリティーを使用可能にする際に必要になります。 WebSphere Process Server の構成時にユーザー名とパスワードを入力しなかった場合は、 WebSphere Process Server を構成した後に管理コンソールを使用して同じ情報を入力することができます。

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

プロシージャー

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

   該当するフィールド (「**ceiSampleJmsUser**」および「**ceiSampleJmsPwd**」) に有効なユーザー名とパスワードを入力します。
3. 応答ファイルの Business Process Choreographer 部分に、セキュア・モードでサービス統合バスに接続するためのサンプルの Business Process Choreographer 構成用の ID を指定します。

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

次のタスク

認証別名の管理について詳しくは、後続のトピックを参照してください。

関連タスク

39 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・インストール済み環境のセキュリティーの構成方法については、以下のリンクを参照してください。

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。

プロシージャー

1. 管理セキュリティーが有効であることを確認します。 8 ページの『管理セキュリティーの使用可能化』を参照してください。
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。 37 ページの『WebSphere Process Server におけるアプリケーションの保護』を参照してください。
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 • 組み込みファイル・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	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、13 ページの『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 LDAP を構成するには、『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、13 ページの『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. 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. 「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。
7. 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。
8. 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)。このロールに割り当てられるユーザーは、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。

9. 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。

10. 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。

11. 必要な場合は、サーバーを停止した後再始動します。

    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。

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。

作成する各ノードは、以上のような方法で保護される必要があります。環境のインストールおよび構成中に、システム管理者ユーザー ID が複数の場所で使用されている可能性があります。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。

管理セキュリティーの使用可能化

WebSphere Application Server バージョン 6.1 の場合、デフォルトで管理セキュリティーが使用可能になっています。管理セキュリティーを使用不可にした場合は、以下の説明に従って、もう一度使用可能にしてください。

始める前に

これらの操作を開始する前に、WebSphere Process Server をインストールして、インストール済み環境を確認します。

このタスクについて

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。

プロシージャー

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. 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。必要な権限をすべては持っていないアプリケーションは、AccessControl 例外を生成します。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。
4. 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。
5. 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。
6. 必要な場合は、サーバーを停止した後再始動します。

   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、認証や役割ベースの許可を含むアプリケーション・セキュリティーも、管理セキュリティーをアクティブにするまでは適用されません。管理セキュリティーは、デフォルトで使用可能になっています。

管理セキュリティーは、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 の役割ベースの許可検査
- ID の伝搬 (RunAs)
- CBIND 検査
- 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。

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。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 役割ベースの許可
- 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・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: Network Deployment 環境では、LDAP またはご使用のローカル・オペレーティング・システムのいずれかをユーザー・レジストリーとして使用することができます。

プロシージャー

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 • 組み込みファイル・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	デフォルトのユーザー・レジストリーです。「**使用可能なレルム定義**」で、「**ローカル・オペレーティング・システム**」を選択し、「**構成**」をクリックします。「ローカル OS ユーザー・レジストリー」ページで、ユーザー名とパスワードを入力します。このユーザー名はサーバーの ID として使用されます。ユーザーは**管理者**ロールに自動的に追加されます。 **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	カスタム・アカウント・リポジトリーを選択し、必要に応じて構成します。
Tivoli® Access Manager	**注:** このオプションは、管理コンソールでは使用できないため、wsadmin コマンドを使用して構成する必要があります。

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。サーバー・ユーザー ID を選択できます。サーバー ID を自動的に生成させることもできます。

このタスクについて

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

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

プロシージャー

1. 管理コンソールから、ご使用のユーザー・レジストリーの「**ユーザー・アカウント・リポジトリー (User account repository)**」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**」を入力します。 管理特権を持ち、ローカル・オペレーティング・システム内で定義されているユーザーの名前を指定します。ユーザー名は、管理セキュリティーが使用可能である場合に、管理コンソールにログオンするために使用されます。
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。

   「**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。
   - サーバー・ユーザー ID または管理ユーザー
   - このユーザーに関連付けられたパスワード

   この ID は、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。

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

このタスクについて

このタスクでは、グローバル・セキュリティーがオンになっていることを想定しています。

プロシージャー

1. WebSphere Process Server を開始します。
2. 管理コンソールを起動します。
3. LDAP 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「**LDAP**」を選択します。「**構成**」をクリックします。
4. 「**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時および wsadmin コマンドの実行時に使用されます。
5. 「**適用**」をクリックします。
6. 「**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。

   「**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。
   - サーバー・ユーザー ID または管理ユーザー
   - このユーザーに関連付けられたパスワード

   この ID は LDAP 管理者ユーザー ID ではありませんが、この ID のエントリーが LDAP に存在している必要があります。
7. 使用する LDAP のタイプを選択します。

   「**タイプ**」リストから、ユーザー・レジストリーとして使用する特定の LDAP を選択します。
8. LDAP が常駐するコンピューターの名前を入力します。

   「**ホスト**」フィールドに、LDAP が常駐するサーバーの名前を入力します。
9. LDAP が listen するポート番号を入力します。

   「**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。
10. 「**基本識別名**」を入力します。

この値には、ディレクトリー・サービスの基本識別名を指定します。これは、ディレクトリー・サービスの LDAP 検索の開始点を表します。

許可を目的として、このフィールドでは大/小文字の区別が行われます。この指定は、(例えば、別のセルまたは Lotus Domino® サーバーから) 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 サーバーから受け取った基本 DN と正確に一致する必要があることを意味しています。許可の際に大/小文字の区別を考慮しない場合は、「**大/小文字を区別しない**」フィールドを使用可能にしてください。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。

11. その他のパラメーターはデフォルト値のまま残し、変更内容を確認します。

    「**OK**」をクリックします。

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。

プロシージャー

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

   注: サーバーを始動するには、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。 コマンド・プロンプトの *install_dir*/bin ディレクトリーで、次のテキストを入力します。stopServer.sh *servername* -username *username* -password *password*

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

   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 4 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 1. 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 機密情報へのアクセスに必要な以下のような権限もあります。 • 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 1. 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。 • 統合リポジトリー構成内のユーザーの作成、更新、または削除。 • 統合リポジトリー構成内のグループの作成、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。

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。

目的

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

Business Process Choreographer の認証別名

ビジネス・プロセスには、次に示す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 2 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 2. ビジネス・プロセスに関連付けられた認証別名

別名	説明	情報
BPEAuthDataAliasJMS_*node_server*	メッセージング・エンジンで認証するために使用します。	応答ファイルの該当する Business Process Choreographer プロパティーにユーザー名とパスワードの値を入力します。
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 3 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 3. ビジネス・プロセスに関連付けられた RunAs ロール

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

入力したユーザー名は、RunAs ロールに追加されます。

Common Event Infrastructure 認証別名

Common Event Infrastructure には、次に示す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。

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

表 4. Common Event Infrastructure に関連付けられた認証別名

別名	説明	情報
CommonEventInfrastructure JMSAuthAlias 1 つの文字スペースが、テーブルのセルにうまく収まるようにこのエントリーに追加されています。実際の別名には、この文字スペースは含まれていません。	メッセージング・エンジンで認証するために使用します。	応答ファイルの該当する Common Event Infrastructure 構成プロパティーにユーザー名とパスワードの値を入力します。
EventAuthAlias*DBType*	データベースで認証するために使用します。	応答ファイルの該当する Common Event Infrastructure 構成プロパティーにユーザー名とパスワードの値を入力します。

Service Component Architecture の認証別名

Service Component Architecture (SCA) には、次に示す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 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. SCA コンポーネントに関連付けられた認証別名

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

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

次に示すエンタープライズ・アーカイブ (EAR) ファイルは、Business Process Choreographer インストールの一部として、アクセス制御と共にインストールされます。 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。 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	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。

EAR ファイル	ロール	デフォルトの許可	注®
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。
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

次に示すエンタープライズ・アーカイブ (EAR) ファイルは、Common Event Infrastructure インストールの一部として、アクセス制御と共にインストールされます。 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。

EventServer.ear ファイルは、Common Event Infrastructure インストールの一部としてインストールされる唯一の EAR ファイルです。

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・インストール済み環境のセキュリティーの構成方法については、以下のリンクを参照してください。

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。

プロシージャー

1. 管理セキュリティーが有効であることを確認します。 8 ページの『管理セキュリティーの使用可能化』を参照してください。
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。 37 ページの『WebSphere Process Server におけるアプリケーションの保護』を参照してください。
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 • 組み込みファイル・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	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、 13 ページの『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。

ユーザー・レジストリー	アクション
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、 13 ページの『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. 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. 「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。
7. 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。
8. 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)。このロールに割り当てられるユーザーは、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。
9. 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。
10. 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。
11. 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。
12. 必要な場合は、サーバーを停止した後再始動します。

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。

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。

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。 環境のインストールおよび構成中に、システム管理者ユーザー ID が複数の場所で使用されている可能性があります。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。

管理セキュリティーの使用可能化

WebSphere Application Server バージョン 6.1 の場合、デフォルトで管理セキュリティーが使用可能になっています。管理セキュリティーを使用不可にした場合は、以下の説明に従って、もう一度使用可能にしてください。

始める前に

これらの操作を開始する前に、WebSphere Process Server をインストールして、インストール済み環境を確認します。

このタスクについて

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。

プロシージャー

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. 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。必要な権限をすべては持っていないアプリケーションは、AccessControl 例外を生成します。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。

4. 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。

5. 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。

6. 必要な場合は、サーバーを停止した後再始動します。

   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、

認証や役割ベースの許可を含むアプリケーション・セキュリティーも、管理セキュリティーをアクティブにするまでは適用されません。管理セキュリティーは、デフォルトで使用可能になっています。

管理セキュリティーは、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 の役割ベースの許可検査
- ID の伝搬 (RunAs)
- CBIND 検査

- 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。

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。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 役割ベースの許可
- 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・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: Network Deployment 環境では、LDAP またはご使用のローカル・オペレーティング・システムのいずれかをユーザー・レジストリーとして使用することができます。

プロシージャー

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 • 組み込みファイル・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。「**使用可能なレルム定義**」で、「**ローカル・オペレーティング・システム**」を選択し、「**構成**」をクリックします。「ローカル OS ユーザー・レジストリー」ページで、ユーザー名とパスワードを入力します。このユーザー名はサーバーの ID として使用されます。ユーザーは**管理者**ロールに自動的に追加されます。 **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	カスタム・アカウント・リポジトリーを選択し、必要に応じて構成します。
Tivoli Access Manager	**注:** このオプションは、管理コンソールでは使用できないため、wsadmin コマンドを使用して構成する必要があります。

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。サーバー・ユーザー ID を選択できます。サーバー ID を自動的に生成させることもできます。

このタスクについて

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

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

プロシージャー

1. 管理コンソールから、ご使用のユーザー・レジストリーの「**ユーザー・アカウント・リポジトリー (User account repository)**」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**」を入力します。 管理特権を持ち、ローカル・オペレーティング・システム内で定義されているユーザーの名前を指定します。ユーザー名は、管理セキュリティーが使用可能である場合に、管理コンソールにログオンするために使用されます。
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。

   「**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。
   - サーバー・ユーザー ID または管理ユーザー
   - このユーザーに関連付けられたパスワード

   この ID は、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。

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

このタスクについて

このタスクでは、グローバル・セキュリティーがオンになっていることを想定しています。

プロシージャー

1. WebSphere Process Server を開始します。
2. 管理コンソールを起動します。
3. LDAP 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「**LDAP**」を選択します。「**構成**」をクリックします。

4. 「**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時および wsadmin コマンドの実行時に使用されます。
5. 「**適用**」をクリックします。
6. 「**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。

   「**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。
   - サーバー・ユーザー ID または管理ユーザー
   - このユーザーに関連付けられたパスワード

   この ID は LDAP 管理者ユーザー ID ではありませんが、この ID のエントリーが LDAP に存在している必要があります。
7. 使用する LDAP のタイプを選択します。

   「**タイプ**」リストから、ユーザー・レジストリーとして使用する特定の LDAP を選択します。
8. LDAP が常駐するコンピューターの名前を入力します。

   「**ホスト**」フィールドに、LDAP が常駐するサーバーの名前を入力します。
9. LDAP が listen するポート番号を入力します。

   「**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。
10. 「**基本識別名**」を入力します。

    この値には、ディレクトリー・サービスの基本識別名を指定します。これは、ディレクトリー・サービスの LDAP 検索の開始点を表します。

    許可を目的として、このフィールドでは大/小文字の区別が行われます。この指定は、(例えば、別のセルまたは Lotus Domino サーバーから) 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 サーバーから受け取った基本 DN と正確に一致する必要があることを意味しています。許可の際に大/小文字の区別を考慮しない場合は、「**大/小文字を区別しない**」フィールドを使用可能にしてください。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。
11. その他のパラメーターはデフォルト値のまま残し、変更内容を確認します。

    「**OK**」をクリックします。

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。

プロシージャー

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

   注: サーバーを始動するには、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。 コマンド・プロンプトの *install_dir*/bin ディレクトリーで、次のテキストを入力します。stopServer.sh *servername* -username *username* -password *password*

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

   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 4 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 6. 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。

表 6. 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
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 機密情報へのアクセスに必要な以下のような権限もあります。 • 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。
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。 • 統合リポジトリー構成内のユーザーの作成、更新、または削除。 • 統合リポジトリー構成内のグループの作成、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。

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。

目的

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

Business Process Choreographer の認証別名

ビジネス・プロセスには、次に示す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。

19 ページの表 2 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 7. ビジネス・プロセスに関連付けられた認証別名

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

19 ページの表 3 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 8. ビジネス・プロセスに関連付けられた RunAs ロール

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

表 8. ビジネス・プロセスに関連付けられた RunAs ロール (続き)

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

入力したユーザー名は、RunAs ロールに追加されます。

Common Event Infrastructure 認証別名

Common Event Infrastructure には、次に示す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。

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

表 9. Common Event Infrastructure に関連付けられた認証別名

別名	説明	情報
CommonEventInfrastructure JMSAuthAlias 1 つの文字スペースが、テーブルのセルにうまく収まるようにこのエントリーに追加されています。実際の別名には、この文字スペースは含まれていません。	メッセージング・エンジンで認証するために使用します。	応答ファイルの該当する Common Event Infrastructure 構成プロパティーにユーザー名とパスワードの値を入力します。
EventAuthAlias*DBType*	データベースで認証するために使用します。	応答ファイルの該当する Common Event Infrastructure 構成プロパティーにユーザー名とパスワードの値を入力します。

Service Component Architecture の認証別名

Service Component Architecture (SCA) には、次に示す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。

20 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 10. SCA コンポーネントに関連付けられた認証別名

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

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

次に示すエンタープライズ・アーカイブ (EAR) ファイルは、Business Process Choreographer インストールの一部として、アクセス制御と共にインストールされます。 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。 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	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。
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

次に示すエンタープライズ・アーカイブ (EAR) ファイルは、Common Event Infrastructure インストールの一部として、アクセス制御と共にインストールされます。 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。

EventServer.ear ファイルは、Common Event Infrastructure インストールの一部としてインストールされる唯一の EAR ファイルです。

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。

始める前に

アプリケーションの保護では、管理セキュリティーが使用可能になっていることを想定しています。

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 (例えば、給与計算情報やクレジット・カードの詳細情報) へアクセスしたり、これらの情報の転送や変更を実行したりします。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。当然のことながら、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。

プロシージャー

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。 詳しくは、 8 ページの『管理セキュリティーの使用可能化』を参照してください。
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。 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。「**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へのアクセスを試行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 Process Server 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・ロールに割り当てて、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。
5. ご使用の WebSphere Process Server 環境のセキュリティーを維持管理します。

アプリケーション・セキュリティーの要素

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

WebSphere Process Server におけるセキュリティーは、以下の 3 つのグループに大別することができます。

- 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のセキュリティーは、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は、転送中に変更することは不可能です。
- **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は、転送中のインターセプトや読み取りは不可能です。

ID の伝搬

セキュリティーの最後の要素は、以下の ID の伝搬のものです。

- **シングル・サインオン** 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、認証情報をダウンストリームのシステムに伝搬するために使用され、この情報を基にダウンストリームのシステム側では次にアクセス制御を適用できます。

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 11 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、および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 11. 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。

表 11. さまざまなクライアント用の認証オプション (続き)

クライアント	認証オプション	注
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。

プロシージャー

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認証別名**」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。
2. 変更する認証別名を選択します。

   「ビジネス・インテグレーション認証別名」パネルには、認証別名、関連コンポーネント、その別名に関連付けられたユーザー ID、および別名の説明 (オプション) を示したリストが表示されます。変更する認証別名をクリックします。代わりに、編集する認証別名に対応する「**選択**」列のチェック・ボックスを選択してから、「**編集**」ボタンをクリックすることもできます。 認証別名構成パネルが表示されます。
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 (Augmenting WebSphere Process Server profiles with security)*』を参照してください。

関連タスク

4 ページの『セキュリティーを適用した WebSphere Process Server プロファイルの拡張』

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

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 Process Server で一般ユーザーを認証する場合、そのユーザーが実行できる操作を制限することがセキュリティー上重要になります。一部のユーザーには特定の作業の実行を許可しつつ、他のユーザーにはその実行を拒否することを、アクセス制御といいます。

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。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。

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

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_plan.html

http://publib.boulder.ibm.com/infocenter/dmndhelp/v6r1mx/topic/com.ibm.wbit.610.help.runtime.doc/topics/tusergoal.html

SSL を使用する Web サービス Web クライアントの構成:

Secure Sockets Layer (SSL) を使用する Web サービスを呼び出すように、Web サービス・クライアントを構成できます。

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 (Securing Web services applications at the transport level)』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必要がある場合、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

Configuring single sign-on capability with Tivoli Access Manager or WebSEAL

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。

始める前に

保護されたアプリケーションを WebSphere Integration Developer で開発します。アプリケーションをエンタープライズ・アーカイブ (EAR) ファイルとしてエクスポートし、WebSphere Process Server にデプロイします。

WebSphere Process Server for z/OS のコンポーネントを開発するときは、プラットフォーム固有の機能 (System Authorization Facility など) を使用してセキュリティーを管理できることに留意してください。

このタスクについて

次のステップに従い、保護されたアプリケーションを WebSphere Process Server にインポートします。

プロシージャー

1. アプリケーション EAR ファイルをインストールします。

   管理コンソールで「**アプリケーション**」を展開し、「**エンタープライズ・アプリケーション**」をクリックします。「**インストール**」をクリックし、新規アプリケーションの詳細情報を入力します。
2. 新規アプリケーションにセキュリティー・ロールを割り当てます。

「**セキュリティー・ロールをユーザーおよびグループにマップ**」をクリックします。アプリケーションのロールは、4 つの項目の中から選択します。

オプション	説明
全員	これは、セキュリティーなしと同等です。
全認証者	正当なユーザー名とパスワードで認証するユーザーは、だれでも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のメンバーとしてリストされます。
マップされたグループ	グループは、ユーザーを追加するために最も便利な方法です。指定されたグループのメンバーすべてがこのロールのメンバーになります。

「**ユーザーの検索 (Look up users)**」および「**グループの検索 (Look up groups)**」を使用して、このロールにマップ可能なユーザーとグループをリストします。

次のサンプル SCDL では、**onewayinvoke** メソッドへのアクセスが、**manager** ロールのメンバー・ユーザーに制限されています。

```
<?xml version="1.0" encoding="UTF-8"?>
<scdl:component xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:java="http://www.ibm.com/xmlns/prod/websphere/scdl/java/6.0.0"
xmlns:ns1="http://sample.recovery.security/Itarget"
xmlns:scdl="http://www.ibm.com/xmlns/prod/websphere/scdl/6.0.0"
xmlns:wsdl="http://www.ibm.com/xmlns/prod/websphere/scdl/wsdl/6.0.0"
displayName="secure" name="Component1">
  <interfaces>
    <interface xsi:type="wsdl:WSDLPortType" portType="ns1:Itarget">
      <method name="onewayinvoke">
       <scdl:interfaceQualifier xsi:type="scdl:SecurityPermission"
role="manager"/>
      </method>
      </interface>
  </interfaces>
  <references/>
  <implementation xsi:type="java:JavaImplementation"
class="sca.component.java.impl.Component1Impl1">
 </implementation>
</scdl:component>
```

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は、この割り当ては事前に完了されている場合があります。その場合は、このステップを完了させて、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、ステップの 1 つで、ユーザーを RunAs ロールに割り当てまたは変更します。このステップは「RunAs 役割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。

プロシージャー

1. 管理コンソールで、「アプリケーション」を展開して、「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、注意して使用してください。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。

関連情報

役割へのユーザーおよびグループの割り当て

RunAs 役割へのユーザーの割り当て (Assigning users to RunAs roles)

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 および securityIdenitity の 1 つまたは両方が使用されます。これらの修飾子が存在している場合は、アプリケーションおよび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必要があ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 を持つインターフェースまたは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 (例えば「スーパーバイザー」) 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。

プロシージャー

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。

関連情報

代行

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

WebSphere Business Integration Adapters は、複数のソフトウェア、アプリケーション・プログラム・インターフェース (API)、およびツールの集合で構成され、アプリケーションが統合ブローカーを通してビジネス・データを交換できるようにします。WebSphere Business Integration Adapters は JMS メッセージングに依存しており、JMS はセキュリティー・コンテキストの伝搬をサポートしません。

WebSphere Adapters は、エンタープライズ情報システム (EIS) と、WebSphere Process Server によってサポートされる J2EE コンポーネントの間の管理された双方向接続を使用可能にします。

この両方のタイプのアダプターから WebSphere Process Server へのインバウンド通信には、認証メカニズムがありません。WebSphere Business Integration Adapters の場合は、JMS メッセージングに依存しているので、セキュリティー・コンテキストの伝搬は不可能です。また、J2C でもインバウンド・セキュリティーはサポートしないため、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 への入力では、必ず Service Component Architecture (SCA) エクスポートが使用されます。SCA エクスポートは、メディエーション、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 コンポーネントに関連付けられる必要があります。

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。ただし、EAR ファイルが WebSphere Process Server にデプロイされる際に、使用される ID のユーザー名とパスワードを入力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。 EIS の資料には、このリンクの保護方法に関する情報が記載されています。

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

チュートリアル

チュートリアルは、いくつかの重要なセキュリティー・シナリオの内容を紹介するために提供されています。

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、グローバル・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。

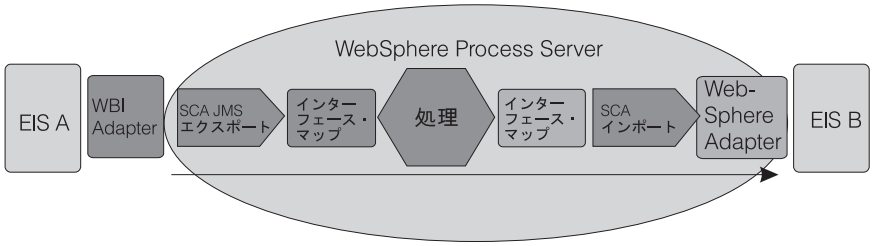
このタスクについて

プロシージャー

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。 特定の状況では、お客様のシナリオとして複数の例の情報を組み合わせることが必要になる場合もあります。
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。

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

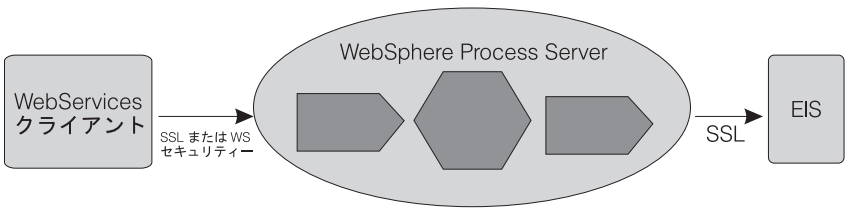
インバウンド要求は、WebSphere Business Integration Adapter で受信します。Service Component Architecture (SCA) は、SCA エクスポートに基づいてインターフェース・マップを呼び出します。この要求は、処理コンポーネント、2 番目のインターフェース・マップを経由した後、 WebSphere Adapter を介して 2 番目の EIS (B) に渡されます。これらは、あるコンポーネントが次のコンポーネントのメソッドを呼び出していく SCA 呼び出しです。



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

WebSphere Process Server へのインバウンド 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。

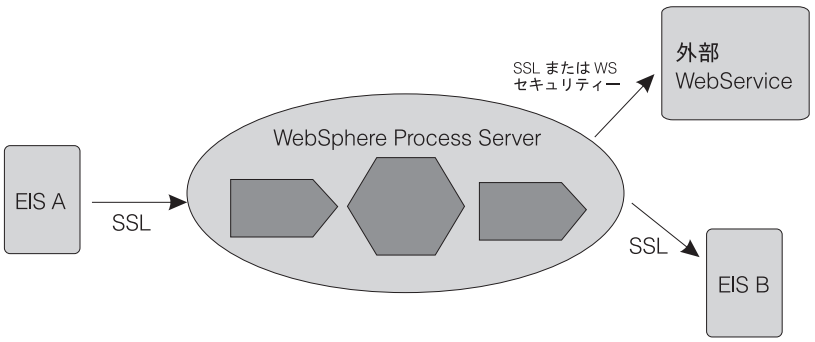


HTTP 基本認証または WS-Security 認証を使用して、SSL クライアントとして Web サービス・クライアントを認証することができます。クライアントが認証される際、アクセス制御が SecurityPermission 修飾子に基づいて適用されます。クライアン

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。

WebSphere Process Server からのアウトバウンド 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、外部の Web サービスを呼び出します。



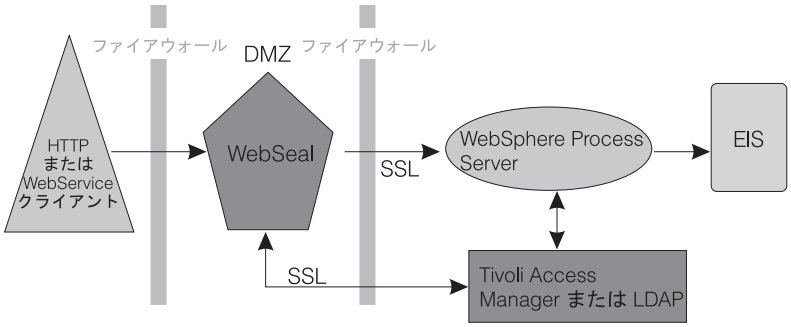
インバウンド Web サービス要求の場合、HTTP 基本認証または WS-Security 認証を使用して、SSL クライアントとして外部の Web サービスを認証することができます。LTPACallBackHandler をコールバック・メカニズムとして使用して、現在の RunAs サブジェクトから usernameToken を抽出します。WebSphere Process Server とターゲットの Web サービスとの間で、WS-Security を使用してデータのプライバシーおよび保全性を確保することができます。

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

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

- HTTP 基本認証
- HTTP フォーム・ベース認証
- 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

チュートリアル: セキュリティー・ロールをリストする jacl スクリプトの記述

このチュートリアルでは、JMX MBean を利用および管理できる単純な jacl スクリプトの記述と実行方法について説明します。このスクリプトは、グローバル・セキュリティーが使用可能な場合にロールを呼び出すことと関係しています。このスクリプトを使用して、リレーションシップ内のロールごとにロール名をプリントすることができます。

このチュートリアルの目的

このチュートリアルを終了すると、次の操作ができるようになります。

- すべてのリレーションシップのリストを要求する JMX MBean を呼び出す jacl スクリプトを記述する。

スクリプトの記述について詳しくは、の『スクリプトの使用 (wsadmin)』を参照してください。

このチュートリアルを完了するのに必要な時間

このチュートリアルは、完了するのにおよそ 15 分から 30 分の時間を要します。

前提条件

このチュートリアルでは、JMX セキュリティー・サンプルに組み込まれているスクリプトを使用します。このサンプルでは、ロール・リレーションシップのリストをプリントする MBean 機能を実例で示します。

注: このスクリプトを使用するには、WebSphere Process Server のインストール時に、コード・サンプルをインストールするオプションを選択する必要があります。

サンプル Jacl スクリプトは、 および にあります。スクリプトの名前は、`RelServicesAdmin.jacl` です。

スクリプトを実行するには、次のように入力します。または、次のように入力します。

このスクリプトは、ご使用の環境にあるリレーションシップを 10 件まで呼び出し、それぞれのリレーションシップごとのロールを 10 個までコンソールにプリントします。

演習: jacl スクリプトの記述

このタスクについて

このスクリプトの基本概念を使用して、システム内の MBean のどれとでも通信できます。必要なものは、MBean の名前とタイプ、および MBean で使用可能なメソッドと属性のみです。getAttribute コマンドと setAttribute コマンドは、属性に対して使用します。invoke コマンドはメソッドに対して使用します。JMX セキュリティー MBean を管理する `.jacl` スクリプトを作成するには、次のステップを実行します。

注: 各ステップのコードの前には、コードの動作を説明した記述があります。

プロシージャー

1. **nodename** を決定する。

   以下に示すスクリプトの最初の部分では、nodename を決定しています。
   `nodeName` が正しく指定されない場合は、正しい構文がプリントされ、スクリプトが終了します。

   ```
   # read and validate arguments

       if {{$argc == 1 } && { [lindex $argv $i] == "-nodeName" } {
               set nodeName [lindex $argv $i]
   ```

2. **MBean** を識別する。

   MBean は、タイプと名前によって識別されます。

   注: この場合、使用する特定の MBean がわかっているので、名前とタイプはハードコーディングされています。
   スクリプトの後半では、MBean を識別します。

   ```
   # these two variables, mbeanName and mbeanType are used
     to uniquely identify the mbean.
          # for this sample, the mbean that access relationship
            services will be used.

          set mbeanName"RelService"
          set mbeanType"WBIRelServices"
   ```

3. MBean を位置指定して、**参照**を設定する。

   ここに示されるコードを使用して、MBean の参照を設定します。

   ```
   # locate the mbean and set a reference to it in "relSvcsMBean" variable

          set relSvcsMBean [$AdminControl queryNames
              name=$mbeanName,node=$nodeName,type=$mbeanType,*]
   ```

4. getAttribute コマンドを使用して**リレーションシップ**を呼び出す。

   この特定の MBean のドキュメンテーションでは、`allRelationshipNames` という名前の属性が定義されています。 getAttribute コマンドを使用して、その属性について MBean に問い合わせます。属性値は、そのコマンドを呼び出す次のステップでステップスルーするリストになります。

```
# request the list of relationships from the mbean

      set relationships
       [$AdminControl getAttribute $relSvcsMBean allRelationshipNames]
```

5. 各リレーションシップ名の**コマンド**を呼び出し、その名前をプリントして、MBean に戻って追加情報を入手します。

   この例では、特定のリレーションシップ名の単一パラメーターを持つ getAllRoleNames というメソッドを、MBean によって定義しています。invoke コマンドを使用してこのメソッドを呼び出すと、メソッドは現在のリレーションシップ名を渡します。リレーションシップ内のロールごとに、ロール名がプリントされます。

```
# loop through the list of role names and print name

        foreach roleName $roles {
          puts "    Role: $roleName"
        }
      }
    } else {
        # arguments were not correct, print correct syntax
           puts "Usage: wsadmin -f RelServicesAdmin.jacl -nodeName nodeName"
    }
```

結果

これで、リレーションシップを呼び出すスクリプトの記述が終了しました。

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
577 Airport Blvd., Suite 800
Burlingame, CA 94010
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 logo、Lotus Domino、Tivoli、WebSphere、および z/OS は、International Business Machines Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標です。

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

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

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

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。

IBM WebSphere Process Server for z/OS バージョン 6.1.0

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