IBM WebSphere Commerce

セキュリティー・ガイド

バージョン 5.5

IBM WebSphere Commerce

セキュリティー・ガイド

バージョン 5.5

ご注意!

本書および本書で紹介する製品をご使用になる前に、 245 ページの『特記事項』をお読みください。

本書は、IBM WebSphere Commerce バージョン 5.5 (プロダクト番号 5724-A18) 、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。製品のレベルにあった版を使用していることをご確認ください。

資料のご注文方法については、http://www.ibm.com/jp/manuals の「ご注文について」をご覧ください。 (URL は、変更になる場合があります)

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

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

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

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

(URL は、変更になる場合があります)

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： IBM WebSphere Commerce
Security Guide
Version 5.5

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 2003.7

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

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

目次

本書について

本書は、WebSphere Commerce のセキュリティー・フィーチャーについて、およびそのフィーチャーの構成方法について説明します。

本書は、認証、許可、およびアクセス制御ポリシーなどの、 WebSphere Commerce のセキュリティー上の懸案事項を詳述しています。本書の目的は、それぞれのサイトのセキュリティー担当者 (システム管理者や WebSphere Commerce サイト管理者も含まれると想定されます) によって、 WebSphere Commerce の実動サイトを確実にセキュアにするのに役に立つ包括的な資料として用いられることにあります。

本書の対象読者は、WebSphere Commerce サイトのセキュリティー担当責任者またはセキュリティー管理者です。

重要

本書では、e-commerce サイトの配置に関連した WebSphere Commerce のセキュリティー上の案件のみを取り上げています。オペレーティング・システムの弱点に関する内容は述べていません。オペレーティング・システムをセキュアにするために講じる必要のある対策を確かめるには、オペレーティング・システムのベンダーに問い合わせてください。

変更の要約

この「セキュリティー・ガイド」と将来の改訂版は、WebSphere® Commerce の技術ライブラリーの Web ページから入手できます。 WebSphere Commerce の各エディションに関する追加情報は、それぞれの概要ページを参照してください。

- Business Edition (`http://www.ibm.com/software/webservers/commerce/wc_be/`)
- Professional Edition (`http://www.ibm.com/software/commerce/wscom/support/wc_pe/`)

その他のサポート情報については、 WebSphere Commerce のサポート・ページ (`http://www.ibm.com/software/commerce/support/`) を参照してください。

この製品の最終的な変更については、やはり上記の Web サイトから入手できる改訂版の README ファイルを参照してください。

本書の改訂部分については、この後に要約を示します。

本書の編成

本書は次のような内容に分かれています。

- 1 ページの『第 1 部 WebSphere Commerce のセキュリティー概念』は、WebSphere Commerce セキュリティー・モデルを取り上げ、 WebSphere Commerce のセキュリティーの概念について概略しています。第 1 部は、

WebSphere Commerce セキュリティーの一般概要を知りたい人や、 WebSphere Commerce サイトのセキュリティーを計画する人すべてにとって必読の項です。

- 53 ページの『第 2 部 セキュリティー認証の管理』は、サイト・セキュリティーにまつわる種々の WebSphere Commerce 管理タスクを解説しています。第 2 部は、サイト・セキュリティーに関連した管理タスクを担うすべての人を対象に説明しています。
- 99 ページの『第 3 部 セキュリティー許可の管理』は、 WebSphere Commerce のアクセス制御にかかわる許可タスクを解説しています。第 3 部は、 WebSphere Commerce のアクセス制御にかかわるシステム許可タスクを実行するすべての人を対象に説明しています。
- 191 ページの『第 4 部 Payments のセキュリティー』は、 WebSphere Commerce Payments のセキュリティーにかかわる WebSphere Commerce の管理タスクを解説しています。第 4 部は、 WebSphere Commerce Payments を管理するすべての人を対象に説明しています。
- 197 ページの『第 5 部 その他のセキュリティー・トピック』は、 WebSphere Application Server のセキュリティー機能強化など、 WebSphere Commerce のその他の管理タスクを解説しています。第 5 部は、セキュリティーを担当するシステム管理者を対象に説明しています。

本書の表記規則

本書では以下の強調表示規則を使用します。

太文字	コマンドまたは、フィールド名、アイコン、メニュー選択などのグラフィカル・ユーザー・インターフェース (GUI) コントロールを示します。
モノスペース (Monospace)	示されたとおり正確に入力する必要のあるテキストです (ファイル名、ディレクトリー・パスと名前)。
イタリック	語句の強調に使用します。イタリックは、ご使用のシステムの該当する値に置換しなければならない名前も示します。
host_name	WebSphere Commerce Web サーバーの完全修飾ホスト名 (たとえば、 server.mydomain.ibm.com は完全修飾名です)。
instance_name	作業対象の WebSphere Commerce インスタンスの名前。
Windows *drive*	この製品またはコンポーネントがインストールされているドライブを表す文字。 (たとえば、C:)

このアイコンは、ヒント (作業を完了するために役立つ追加情報) を表すマークです。

重要

これらのセクションは、特に重要な情報を強調しています。

注意

これらのセクションは、データを保護するための情報を強調しています。

Business は、WebSphere Commerce Business Edition に固有の情報を示します。

Professional は、WebSphere Commerce Professional Edition に固有の情報を示します。

AIX は、WebSphere Commerce for AIX® に固有の情報を示します。

400 は、 WebSphere Commerce for the IBM® @server iSeries™ 400® (以前の AS/400®) に固有の情報を示します。

Linux は、 WebSphere Commerce for Linux に固有の情報を示します。

Solaris は、WebSphere Commerce for Solaris オペレーティング環境ソフトウェアに固有の情報を示します。

Windows は、WebSphere Commerce for Windows® 2000 に固有の情報を示します。

パス変数

本書では、ディレクトリー・パスを表すために以下の変数を使用します。

DB2_installdir

この変数は、マシン上の DB2 Universal Database の実際のインストール・ディレクトリーを表します。 DB2 Universal Database のデフォルトのインストール・ディレクトリーは、それぞれのオペレーティング・システムで次のようになります。

AIX `/usr/lpp/db2_08_01`

400 不適用 (オペレーティング・システムの一部としてインストールされる)

Linux `/opt/IBM/db2/V8.1`

Solaris `/opt/IBM/db2/V8.1`

Windows `C:¥Program Files¥WebSphere¥sqllib`

HTTPServer_installdir

この変数は、マシン上の IBM HTTP Server の実際のインストール・ディレクトリーを表します。 IBM HTTP Server のデフォルトのインストール・ディレクトリーは、それぞれのオペレーティング・システムで次のようになります。

AIX `/usr/IBMHttpServer`

400 不適用 (オペレーティング・システムの一部としてインストールされる)

Linux /opt/IBMHttpServer

Solaris /opt/IBMHttpServer

Windows C:¥Program Files¥WebSphere¥IBMHTTPServer

Oracle_installdir

この変数は、マシン上の Oracle の実際のインストール・ディレクトリーを表します。 Oracle のデフォルトのインストール・ディレクトリーは、それぞれのオペレーティング・システムで次のようになります。

AIX /oracle/u01/app/oracle/product/9.2.0

400 OS/400® には適用しません。

Linux Linux には適用しません。

Solaris /opt/oracle/u01/app/oracle/product/9.2.0

Windows C:¥oracle¥ora91

WAS_installdir

この変数は、マシン上の WebSphere Application Server の実際のインストール・ディレクトリーを表します。 WebSphere Application Server のデフォルトのインストール・ディレクトリーは、それぞれのオペレーティング・システムで次のようになります。

AIX /usr/WebSphere/AppServer

400 /QIBM/ProdData/WebAS5/Base

Linux /opt/WebSphere/AppServer

Solaris /opt/WebSphere/AppServer

Windows C:¥Program Files¥WebSphere¥AppServer

WAS_userdir

400 この変数は、 iSeries マシン上の WebSphere Application Server が使用するすべてのデータ (ユーザーが変更できるデータ、またはユーザーが構成しなければならないデータ) のディレクトリーを表します。このディレクトリーのデフォルトは、次のとおりです。

400 /QIBM/UserData/WebAS5/Base/*WAS_instance_name*

WC_installdir

この変数は、マシン上の WebSphere Commerce の実際のインストール・ディレクトリーを表します。 WebSphere Commerce のデフォルトのインストール・ディレクトリーは、それぞれのオペレーティング・システムで次のようになります。

AIX /usr/WebSphere/CommerceServer55

400 /QIBM/ProdData/CommerceServer55

Linux /opt/WebSphere/CommerceServer55

Solaris /opt/WebSphere/CommerceServer55

Windows C:¥Program Files¥WebSphere¥CommerceServer55

WC_userdir

400 この変数は、iSeries マシン上の WebSphere Commerce が使用するすべてのデータ (ユーザーが変更できるデータ、またはユーザーが構成しなければならないデータ) のディレクトリーを表します。このディレクトリーのデフォルトは、次のとおりです。

400 /QIBM/UserData/CommerceServer55

第 1 部 WebSphere Commerce のセキュリティー概念

第 1 部では、WebSphere Commerce のセキュリティー概念の概略を示します。

第 1 章 WebSphere Commerce セキュリティー・モデルの概要

この章は、WebSphere Commerce セキュリティー・モデルならびに WebSphere Commerce のさまざまなセキュリティー概念を説明しています。

概要

本書では、次のような認証、許可、ポリシー、および機密性の概念が説明されています。

認証とは

認証とは、ユーザーまたはアプリケーションが自称どおりのものかどうかを確認するためのプロセスのことです。 WebSphere Commerce システムでは、ゲスト・ユーザーを除き、システムにアクセスするすべてのユーザーとアプリケーションに認証が必要です。ユーザー認証プロセスは常に SSL のもとで実行されます。そのため、第三者はネットワークの不正使用プログラムを使っても、ユーザーからのパスワードの送信時にネットワークでスヌープ できなくなります。通常のセキュリティー措置の場合と同様、認証プロセス中にパスワードが暗号化解除されることはありません。すべてのユーザー・パスワードは、マーチャント鍵 と呼ばれる 128 ビット鍵を使って一方向ハッシュされ、暗号化されます。マーチャント鍵は、WebSphere Commerce システムのインストールおよび構成時に指定します。

WebSphere Commerce システムには管理用の独自のパスワードがあります。そのパスワードは、WebSphere Commerce サイト全体のセキュリティー・ポリシーの一環として定期的に変更する必要があります。 WebSphere Commerce システムのパスワードの変更方法の詳細は、83 ページの『第 6 章 パスワードの設定と変更』を参照してください。

許可とは

許可とは、ユーザーがリソースに対して特定の操作を実行できるかどうかを決定するプロセスのことです。許可は、WebSphere Commerce リソースを管理するアクセス制御ポリシーから決定されます。 WebSphere Commerce システムでは以下の 2 つの領域でアクセス制御が必要です。

- 無許可アクセスが起きないように WebSphere Commerce Enterprise JavaBeans™ (EJB Beans) を保護するため。このプロセスについては、199 ページの『第 16 章 WebSphere Application Server のセキュリティーの使用可能化』に説明されています。
- 許可を受けた関係者のみが、さまざまな WebSphere Commerce コマンド・グループを実行できるようにするため。このプロセスについては、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」の『アクセス制御』に関する項で説明されています。

アクセス制御ポリシーとは

e-commerce サイトに参加する組織とユーザーの定義が完了したと仮定すると、その後一連のポリシーを通してそれらの人々のアクティビティーを管理することができます。このプロセスを*アクセス制御* と呼びます。

アクセス制御ポリシーは、サイト上で特定のアクティビティーの実行を許可されている、ユーザーのグループを記述する規則のことです。これらのアクティビティーには、登録から、オークションの管理、商品カタログの更新、およびオーダーにおける承認、その他 e-commerce サイトで操作し、保守する必要のあるたくさんのアクティビティーが含まれます。

ポリシーとは、ユーザーがサイトにアクセスすることを認可する手段です。担当作業を実行する許可を 1 つ以上のアクセス制御ポリシーを通して受けない限り、ユーザーはサイトのどの機能にもアクセスできません。

WebSphere Commerce の許可モデルは、アクセス制御ポリシーの規定内容に基づきます。アクセス制御ポリシーは、アクセス制御ポリシー・マネージャーによって規定されます。一般的に、保護される可能性のあるリソースにユーザーがアクセスしようとすると、アクセス制御ポリシー・マネージャーはまず、そのユーザーに対してどのアクセス制御ポリシーを適用できるかを判別してから、適用可能なそのアクセス制御ポリシーに基づいて、そのユーザーが要求した操作を特定のリソースで実行してもよいかどうかを決定します。

監査記録とは

コンピューターでは、*監査記録* とはコンピューターのアクティビティーを追跡記録するのに使われる電子または書面ログを言う語です。たとえば、企業の社員は売掛管理などの一部の社内ネットワークにアクセスできても、給与計算などの他のシステム部分へのアクセスは許可されないことがあります。その社員がパスワードを入力して無許可セクションへのアクセスを試みた場合、その不適切なアクティビティーは監査記録に記録されます。

e-commerce システムでは、監査記録は顧客アクティビティーを記録するのに使われます。システムに対する顧客の最初のコンタクトや、商品またはサービスの決済や納品などのその後のアクションが監査記録に記録されます。企業はこの監査記録を使って、すべての照会または苦情に対処することができます。また、監査記録を使って、アカウントの調整、今後の計画と予算設定に関する分析と履歴情報の提供、および税務監査の場合の販売記録の提供を行うことも可能です。

さらに監査記録を使えば、サイバースペースやインターネットを介したコンピューター犯罪を調査することもできます。システムに対して不純な意図をもって不正行為を働いた人物が残した監査記録をたどって調査すれば、犯人を特定することができます。コンピューター犯罪の実行者は、インターネット・サービス・プロバイダーでのアクティビティーのログや、チャット・ルームのログを介して、うかつにも監査記録を残していることがあるからです。

機密性とは

機密性とは、指定外の宛先によって機密情報が暗号解読されないように保護するためのプロセスのことです。 WebSphere Commerce システムで機密性が必要になるの

は、機密情報が、ユーザーのブラウザーから WebSphere Commerce サーバーに送られるときと、 WebSphere Commerce サーバーから元のユーザーのブラウザーへ返送されるときです。 213 ページの『第 17 章 IBM HTTP Server での実動のための SSL の使用可能化』に説明されているとおり、 SSL (Secure Sockets Layer) を使うことによって、このシナリオの機密性が実現されます。

機密性は、セッション管理の分野においても重大な要件です。 HTTP (Hypertext Transfer Protocol) はステートレスであるため、 WebSphere Commerce サーバーに対して継続的にユーザーを識別するために通常は *cookie* が使用されます。この cookie が傍受されると、ユーザー・アカウントに不祥事が起きる可能性があります。通常はこれをセッション・ハイジャック と呼んでいます。 WebSphere Commerce では、 75 ページの『第 5 章 セッション管理』に説明されているとおり、 cookie を指定するための独自のフィーチャーを介してセッション・ハイジャックが防止されています。

セキュリティーに関する一般的な考慮事項

継続的セキュリティー評価

WebSphere Commerce 製品ラインに関しては、IBM セキュリティーの専門家から成る独立グループが実施するセキュリティー分析が通常は行われています。そのような専門家は、ブラウザーを使って WebSphere Commerce にアクセスするだけのユーザーから、 WebSphere Commerce サーバーが稼働するのと同じシステム上にアカウントを有するもっと高い特権のユーザーにいたるまでの観点でセキュリティー分析を行っています。このセキュリティー専門家の分析によるフィードバックが、WebSphere Commerce のセキュリティーを高めるために継続的に使用されています。

WebSphere Commerce 5.5 でのセキュリティーの向上

WebSphere Commerce 5.5 では、ポリシー・グループの加入を、アクセス制御インフラストラクチャーに追加しています。

WebSphere Commerce 5.4 では、ポリシーは、ポリシー所有者の子孫によって所有されるリソースに適用されました。同じ組織階層のさまざまな組織が、さまざまなレベルのアクセス制御を必要とした場合でも、異なるレベルを実現することは困難な場合がありました。さらに、組織階層が非常に深い場合、階層の下の方に近い組織に適用されるすべてのポリシーを理解することには、混乱が生じることもありました。

WebSphere Commerce 5.5 では、さらに簡略化してより明示的にするために、ポリシーをまずビジネスおよびアクセス制御要件に基づいて、ポリシー・グループ別にグループ化します。たとえば、1 つのポリシー・グループは、契約をサポートするために必要なポリシーを持ち、別のポリシー・グループは、登録済みのユーザーだけがショッピングをすることを許可します。次いで、組織のビジネスおよびアクセス制御要件に応じて、組織は明示的に適切なポリシー・グループに加入します。組織がポリシー・グループに加入する場合、そのポリシー・グループ内のポリシーだけが、その組織のリソースに適用されます。その祖先の組織のポリシーは適用され

ません。ただし、組織が明示的にポリシー・グループに加入していない場合は、加入している最も近い祖先のポリシー加入を継承します。

ポリシー・グループの概要については、 19 ページの『第 3 章 許可の概念』の「ポリシー・グループ」に関する項を参照してください。

WebSphere Commerce 5.4 でのセキュリティーの向上

以下の項では、 WebSphere Commerce Suite 5.1 から見て WebSphere Commerce 5.4 において強化され、 WebSphere Commerce 5.5 でも保持されたセキュリティーの内容を一覧で示しています。この強化内容の大半は、WebSphere Commerce Business Edition 5.1 リリースで行われたものです。この機能強化は概して以下の担当者を対象とします。

- WebSphere Commerce サイト管理者
- システム管理者
- WebSphere Commerce 開発者

場合によっては上記の担当は入れ替わる可能性があることに注意してください。

サイト管理者を対象とした機能強化

概してシステム管理者を対象とする WebSphere Commerce のセキュリティーの機能強化は次のとおりです。

アクセス制御

- **アクセス制御フレームワーク** — 主要な機能強化は、新規のアクセス制御フレームワークが WebSphere Commerce 5.4 でインプリメントされ、(WebSphere Commerce 5.5 での新規ポリシー・グループの機能強化と共に) WebSphere Commerce 5.5 でも保持された点にあります。この新規のフレームワークは、アクセス制御ポリシーを使用して、特定のユーザーが特定のリソースで特定のアクションを実行することを許可されているかどうかを判別します。この新規のアクセス制御フレームワークは、詳細なアクセス制御を提供します。これは、WebSphere Application Server に備わったアクセス制御と共同で稼働しますが、それに代わるものではありません。この新規のアクセス制御フレームワークについては、 99 ページの『第 3 部 セキュリティー許可の管理』に詳しく説明されています。

  この新規のアクセス制御フレームワークは、これまでのアクセス制御を次のように強化しています。

  多様性の実現...
  多種多様なアクセス・ポリシーの目標が取り込まれています。このフレームワークは汎用であるため、広範囲にわたるユーザー・グループ、リソース・グループ、アクション・グループ、および関係グループを扱うことができます。

  階層化...
  アクセス制御ポリシーは、ポリシー・グループに属しています。1 つの組織に対して設定されているポリシー・グループは、その組織の下部組織にも暗黙的に適用されます。

  カスタマイズ可能...
  アクセス制御ポリシーは、アプリケーション・コードの外部に置

くことができるので、コードを再コンパイルすることなく、ポリシーに変更を加えることができます。

コンパクト...

新規のフレームワークは簡単に縮尺できます。アクセス制御ポリシーの数は、オブジェクトの数の増加によってではなく、ビジネス・プロセス数の増加によって増加します。グループ設定用のフレームワークの多くは暗黙条件をベースにするので、条件が満足されている限り同じポリシーが適用されるからです。

- **サイト間スクリプト記述** — WebSphere Commerce 構成マネージャーの「サイト間スクリプト保護」ノードを使って、不許可と指定された属性や文字を使用しているユーザー要求を拒否します。これについては、55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。

認証

- **「パスワード・ストレージ (Password storage)」** — WebSphere Commerce は、パスワードそのものを保管するのではなく、 WebSphere Commerce データベース内に SHA-1 ハッシュ体系を使ってパスワードの一方向ハッシュを暗号化して保管します。それによってユーザー・パスワードは、サイト管理者やシステム管理者も含め誰にも解読できないようになります。
- **「パスワード無効化」** — ユーザーが初めてシステムにログインしたときに、 WebSphere Commerce 構成マネージャーの「パスワード無効化」ノードを使って各自のパスワードを変更することを義務付けます。これについては、55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。
- **「アカウント・ポリシー」** — WebSphere Commerce 管理コンソールの「アカウント・ポリシー」ページを使って、使用中のアカウント関連のポリシーを定義するために、ユーザーのサイト用のアカウント・ポリシーをセットアップします。これについては、55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。
- **「パスワード・ポリシー」** — WebSphere Commerce 管理コンソールの「パスワード・ポリシー」ページを使って、ユーザーのパスワード選択特性を制御するために、ユーザーのサイト用のパスワード・ポリシーをセットアップします。これについては、55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。
- **「アカウント・ロックアウト・ポリシー」** — WebSphere Commerce 管理コンソールの「アカウント・ロックアウト・ポリシー」ページを使って、ユーザー・アカウントに不祥事が起きる可能性を減少するために、ユーザーのサイト用のアカウント・ロックアウト・ポリシーをセットアップします。これについては、55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。

許可

「パスワード保護されたコマンド」 — WebSphere Commerce 構成マネージャーの「パスワード保護されたコマンド」ノードを使って、指定コマンドを実行する要求を実行する場合はパスワードを入力することをユーザーに義務付けます。これについては、55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。

データの暗号化

「データベース更新ツール」 — WebSphere Commerce 構成マネージャーの「データベース更新ツール」ノードを使って、パスワードやクレジット・カードの情報などの暗号化データならびに WebSphere Commerce データベース内のマーチャント鍵を更新します。これについては、 55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。

セッション管理

「ログイン・タイムアウト」 — 「ログイン・タイムアウト」ノードを使って、一定期間を超えて非アクティブになっているユーザーをログオフさせ、もう一度システムにログオンし直すよう要求します。この強化機能は、WebSphere Commerce 構成マネージャーを使って起動します。これについては、 55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。

ロギング

「アクセス・ロギング (Access logging)」 — アクセス・ロギングの使用可能化によって、 WebSphere Commerce に対するセキュリティー上の脅威をすべて速やかに特定します。この強化機能は、WebSphere Commerce 構成マネージャーを使って起動します。これについては、 55 ページの『第 4 章 サイト・セキュリティーの機能強化』に詳述されています。

システム管理者を対象とした機能強化

サイト管理者を主な対象として WebSphere Commerce 5.4 で追加され、 WebSphere Commerce 5.5 でも保持されたセキュリティーの機能強化は次のとおりです。

- セキュリティーの重要な機能強化の 1 つは、非標準のポート番号 (たとえば、ポート 443 に対してポート 8000) で実行するように WebSphere Commerce 管理ツールを構成することができるようになったことがあります。このポートへのアクセスを制限することにより、ローカル・ネットワークまたはイントラネットだけが管理ツールにアクセスできるよう制限を設けることができます。
- WebSphere Commerce 管理コンソールから「セキュリティー検査の立ち上げ (Launch security check)」ページを使って、機密漏れの可能性があると思われる一時 WebSphere Commerce ファイルの検査と削除を行うためのセキュリティー・プログラムを立ち上げます。

WebSphere Commerce プログラマーを対象とした機能強化

主要な機能強化は、新規のアクセス制御フレームワークが WebSphere Commerce 5.4 でインプリメントされ、 WebSphere Commerce 5.5 でも保持された点にあります。このフレームワークは、アクセス制御ポリシーを使用して、特定のユーザーが特定のリソースで特定のアクションを実行することを許可されているかどうかを判別します。この新規のアクセス制御フレームワークは、詳細なアクセス制御を提供します。これは、WebSphere Application Server に備わったアクセス制御と共同で稼働しますが、それに代わるものではありません。この新規のアクセス制御フレームワークについては、 99 ページの『第 3 部 セキュリティー許可の管理』に詳しく説明されています。

この新規のアクセス制御フレームワークは、これまでのアクセス制御を次のように強化しています。

多様性の実現...

多種多様なアクセス・ポリシーの目標が取り込まれています。このフレームワークは汎用であるため、広範囲にわたるユーザー・グループ、リソース・グループ、アクション・グループ、および関係グループを扱うことができます。

階層化...

ある組織が所有するアクセス制御ポリシーを、その下位組織にも適用されます。

カスタマイズ可能...

アクセス制御ポリシーは、アプリケーション・コードの外部に置くことができるので、コードを再コンパイルすることなく、ポリシーに変更を加えることができます。

コンパクト...

新規のフレームワークは簡単に縮尺できます。アクセス制御ポリシーの数は、オブジェクトの数の増加によってではなく、ビジネス・プロセス数の増加によって増加します。グループ設定用のフレームワークの多くは暗黙条件をベースにするので、条件が満足されている限り同じポリシーが適用されるからです。

プログラマーを対象としたセキュリティー考慮事項についての詳細は、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」を参照してください。

WebSphere Commerce Suite 5.1 Pro Edition におけるセキュリティー上の向上

Commerce Suite 5.1 は新規の e-commerce アーキテクチャーを具現化したものであり、 C++ ベースの Commerce Suite 4.1 の全面的書き直しであった一方で、それ以前のバージョンの WebSphere Commerce Suite のすべてのセキュリティー・フィーチャーに加え、セキュリティー上の新規の改善点も盛り込まれていました。これらの改善点は、WebSphere Commerce 5.5 でも引き継がれています。

Commerce Suite 5.1 では引き続き以下のようにして、旧リリースで備えられた WebSphere Commerce Suite 管理者およびショッパー・リソースへの無許可アクセスに対する保護が行われていました。

- 認証を受けた WebSphere Commerce Suite ユーザーであるか、または SSL モードになっていることを確認してから機密情報へのアクセスやその送信を行えるようにするためのアクセス制御フィーチャーのサポートの継続。
- Commerce Suite 4.1 と同じモデルに準じて、サイト管理者またはストア・レベルの管理者のみが特定のコマンドを実行できるようにするための、グループに対する WebSphere Commerce Suite コマンドの割り当て。

セキュリティーの一般的な機能強化

Commerce Suite 5.1 を Java™ で書き直したことによって、 C++ で書かれたソフトウェアでは免れえないセキュリティー上の問題が取り除かれました。 Java はポインターを使用しないので、 C++ ベースのほとんどのソフトウェアのセキュリティー上の短所であるバッファーのオーバーフローがなくなりました。業界標準の J2EE 仕

様に準拠している WebSphere Commerce は、厳格な型検査を行って、悪意のある人物によって指定された妨害ステートメントをサーバーが実行することのないようにしています。

業界標準の Triple-DES (Data Encryption Standard) アルゴリズムを使って WebSphere Commerce システムの機密情報が保護されました。 Triple-DES アルゴリズムを収めたパッケージは、改ざんされた場合は WebSphere Commerce サーバーが始動しないようにディジタル署名されています。これらの機能強化は、WebSphere Commerce 5.5 にも引き継がれています。

セッション管理

cookie を盗まれないようにするための独自の技法を使って WebSphere Commerce セッション管理は全面的に書き換えられ、最大限のセキュリティーが実現されました。このように書き換えられたセッション管理は、SSL (secure sockets layer) のみを経由し、しかも暗号化タイム・スタンプで構成された認証 cookie を使用することによって、セッションのハイジャック対策を講じています。

認証

実行時に WebSphere Commerce サーバーで必要なシステムおよびアプリケーションのパスワードは、マーチャント指定の 128 ビット鍵を使って確実に暗号化され、WebSphere Commerce 構成ファイルに保管されます。ユーザーの URL エントリー・ボックスに表示される機密情報は、無許可の開示からショッパーを保護するために暗号化されます。

ロギング

WebSphere Commerce ログ・システムは、セキュリティーを最重要課題として設計されているので、ショッパーのパスワードやクレジット・カード情報などの機密情報は、デフォルトで WebSphere Commerce ログ・ファイルに記録されません。

第 2 章 認証

WebSphere Commerce では認証は、ユーザーまたはアプリケーションが自称どおりであるかどうかを検査するプロセスと見なされます。この項では、WebSphere Commerce の認証のいくつかの側面を詳しく説明します。

WebSphere Commerce 認証モデル

WebSphere Commerce の認証モデルは、次のような概念に基づいています。

- チャレンジ機構
- 認証機構
- ユーザー・レジストリー

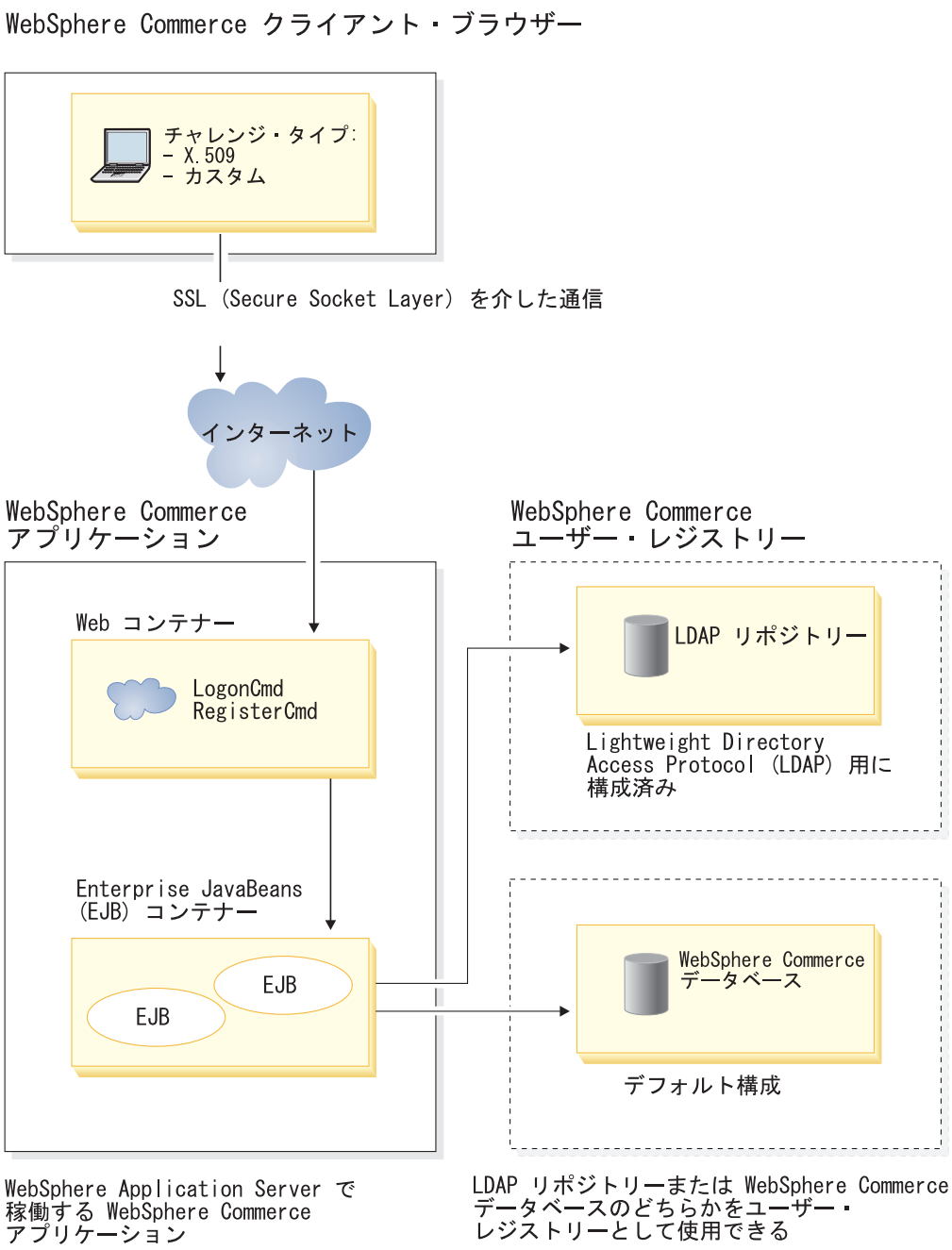


図 1. WebSphere Commerce セキュリティー・モデル

チャレンジ機構

チャレンジ機構は、サーバーがユーザーの認証データをどのように確認し取り出すかを指定します。 WebSphere Commerce は、以下の認証方式またはチャレンジ機構をサポートしています。

フォーム・ベース認証またはカスタム認証

この認証機構では、HTML ページまたは JSP フォームを介したサイトまたはストア独自のログインが許可されます。

証明書ベースの認証 (X.509 証明書)

証明書チャレンジ機構は、 SSL を通して相互認証を実行するよう Web サーバーが構成されているという意味を含みます。接続を確立しようとするクライアントは、証明書の提示を要求されます。この証明書は次に、ユーザー・レジストリーにマップされる認証情報になります。

認証機構

認証機構 は、ユーザーに関連付けられたユーザー・レジストリーに照らして認証データを検証してユーザーを認証します。認証プロセスが完了した後は WebSphere Commerce は、要求があるたびにユーザーに関連付けられた認証トークンを発行します。そのトークンは、ユーザーがブラウザーをログオフまたはクローズすると終了します。

証明書の妥当性検査

これは、X.509 クライアント証明書が Web サーバーによって信頼されていて、しかもその Web サーバーの証明書ポリシーに準拠していることを検証するプロセスです。また WebSphere Commerce は、WebSphere Commerce データベースにも照らし合わせて X.509 証明書を検証します。 Web サーバーは証明書を概括的にアクセス制御するのに対して、 WebSphere Commerce は証明書をち密にアクセス制御します。

LDAP バインド

これは、LDAP バインド操作の実行によってユーザーを認証することで、入力されたチャレンジ情報が正しいことを検証するプロセスです。

データベースのバインド

これは、認証プロセス中に入力されたユーザー ID とパスワードが、 WebSphere Commerce データベースに保管されている認証情報と比較して正しいことを検証するプロセスです。

ユーザー・レジストリー

ユーザー・レジストリーとは、ユーザー情報と、ユーザーの認証情報 (パスワードなど) の入ったリポジトリーのことです。プリンシパル (つまり、実際のユーザーまたはユーザー・レジストリー内のシステム・エンティティーを表します) によって入力された認証情報は、このユーザー・レジストリーに突き合わせて検証または検査することができます。

WebSphere Commerce は、 LDAP ユーザー・レジストリーと WebSphere Commerce データベースの 2 つのユーザー・ドメインを基盤としてユーザー・レジストリーをサポートします。

WebSphere Commerce は以下の LDAP プロバイダーをサポートします。

- AIX 400 Linux Solaris Windows IBM SecureWay® Directory
- AIX Solaris Windows Netscape Directory Server
- 2000 Windows 2000 Active Directory

認証情報

WebSphere Commerce サーバーは、証明書、トークン、またはユーザー ID とパスワードなどの認証情報の検証に基づいた認証機構をサポートします。認証情報は、そのような体系をサポートするユーザー・レジストリーに照らし合わせて検証されます。

WebSphere Commerce トークン

WebSphere Commerce は、セキュア認証 cookie を使って認証データを管理します。認証 cookie は SSL を通してのみやりとりされ、しかもセキュリティーの最大化のためにタイム・スタンプが押されます。たとえば、ユーザーのクレジット・カード番号を尋ねる `DoPaymentCmd` といった機密性の高いコマンドが実行されるたびに、ユーザーを認証するのにこの cookie が使用されます。この cookie が盗まれて無許可のユーザーによって使用される危険性は最小化されています。

SSL または非 SSL のどちらの接続の場合にもブラウザーとサーバーとの間でやりとりされるさらに別の cookie がありますが、これは、非 SSL 接続を介するユーザーを検証するのに使われます。

WebSphere Application Server LTPA トークン

LTPA トークンとは、ユーザーから要求されたリソースに対するアクセス許可を確認するのに必要なユーザー情報の入ったデータのことです。これには、認証データならびに WebSphere Application Server LTPA サーバーのディジタル・シグニチャーが入っています。

WebSphere Application Server の LTPA (Lightweight Third Party Authentication) 機構の場合、ユーザーに関する情報の入った LDAP ディレクトリーが、認証の実行対象のユーザー・レジストリーになります。リソース・サーバーは、WebSphere Application Server セキュリティー・サーバーに連絡をとって、認証機構として LTPA を指定します。また、その要求に関連した認証データも提供します。次に WebSphere Application Server セキュリティー・サーバーは LTPA サーバーに対して認証データを検証し、 LTPA トークンを戻します。

単一サインオン

さまざまな Web アプリケーションに一貫してユーザー認証を保持するというのが、 HTTP 単一サインオンの背後にある考え方です。その目標は、以下を含め、特定の信頼されたドメイン内でセキュリティー認証情報を何回もユーザーに尋ねなくて済むようにすることにあります。

- 共同で稼働する異種の WebSphere Application Server Web サーバー同士
- LDAP サーバー (IBM SecureWay Directory Server など) のような、共同作業を担うアプリケーション

単一サインオン (SSO) のシナリオでは、種々の Web サーバーにユーザーの認証情報を伝搬して、新規のクライアント・サーバー・セッションで、そのつどユーザーが認証情報を入力しなくて済む (基本認証を前提として) ようにするために HTTP cookie が使われます。

WebSphere Commerce での単一サインオンのインプリメントの詳細は、 91 ページの『第 7 章 単一サインオン』を参照してください。

認証ポリシー

認証ポリシーとは一連の規則のことですが、それらの規則は、認証プロセスに対してと、WebSphere Commerce での認証データの検証に対して適用されます。この後の項に説明されているとおり、WebSphere Commerce は、アカウント・ポリシー、他の認証関連のポリシー、およびセッション・ポリシーをサポートします。

アカウント・ポリシー

以下の項では、WebSphere Commerce で利用できるアカウント・ポリシーについて説明します。

アカウント・ポリシー

WebSphere Commerce 管理コンソールの「アカウント・ポリシー」ページで、アカウント・ポリシーをセットアップすることができます。アカウント・ポリシーは、パスワード・ポリシーやアカウント・ロックアウト・ポリシーなどのアカウントに関連するポリシーを定義します。

アカウント・ポリシーを作成したら、ユーザーにそのポリシーを割り当てることができます。そのアカウント・ポリシーが使用中の場合 (つまり、ユーザーがそのアカウント・ポリシーに割り当てられている場合) は、そのポリシーを削除することはできません。

アカウント・ポリシーの詳細は、 67 ページの『アカウント・ポリシーのセットアップ』を参照してください。

「WebSphere Commerce オンライン・ヘルプ」の『デフォルト認証ポリシー』も参照してください。

アカウント・ロックアウト・ポリシー

WebSphere Commerce 管理コンソールの「アカウント・ロックアウト・ポリシー」ページで、WebSphere Commerce 内のさまざまなユーザー役割用のアカウント・ロックアウト・ポリシーをセットアップすることができます。アカウント・ロックアウト・ポリシーは、ユーザー・アカウントに対して不正アクションがとられた場合にそのアカウントを使用禁止にすることで、そのようなアクションによってアカウントが被害を受ける機会を減らします。

アカウント・ロックアウト・ポリシーは次のようなアイテムを統制します。

- アカウント・ロックアウトのしきい値。無効なログオンの試行回数がこの値に達すると、アカウントが使用不可になります。
- ログインの連続失敗による遅延。これは、ユーザーがログインに 2 回失敗した場合にその後ログインできなくなる期間を指します。ログインの失敗が続くと、この遅延はそのつど構成済みの時間遅延値 (たとえば 10 秒) ずつ増加されます。

アカウント・ロックアウト・ポリシーの作成の詳細は、 69 ページの『アカウント・ロックアウト・ポリシーのセットアップ』を参照してください。

パスワード・ポリシー

WebSphere Commerce 管理コンソールの「パスワード・ポリシー」ページでは、ユーザーのパスワード選択を制御して、サイトのセキュリティー・ポリシーが順守されるようにユーザーのパスワードの特性を定義することができます。

このフィーチャーは、パスワードが守らなければならない属性を定義します。パスワード・ポリシーで、以下の条件を決定します。

- ユーザー ID とパスワードが同じでよいか
- 連続する最大文字数
- 文字の最大インスタンス
- パスワードの最長存続期間
- 英字の最小文字数
- 数字の最小文字数
- パスワードの最低限の長さ
- ユーザーの以前のパスワードを再利用できるか

パスワード・ポリシーの詳細は、 68 ページの『パスワード・ポリシーのセットアップ』を参照してください。

「WebSphere Commerce オンライン・ヘルプ」の『デフォルト認証ポリシー』も参照してください。

その他の認証関連のポリシー

以下の項では、WebSphere Commerce で利用できるその他の認証関連のポリシーについて説明します。

パスワード無効化

パスワード無効化フィーチャーを使用可能または使用不可にするには、構成マネージャーの「パスワード無効化」ノードを使用します。このフィーチャーを使用可能にした場合に WebSphere Commerce ユーザーのパスワードの有効期限が切れると、そのユーザーはパスワードの変更を要求されます。その場合、ユーザーは、パスワードの変更を要求されるページにリダイレクトされます。ユーザーは、パスワードの変更を完了するまで、そのサイトのどのセキュア・ページにもアクセスすることができません。

「パスワード無効化」ノードの使用の詳細は、 60 ページの『パスワード無効化の活動化』を参照してください。

パスワード保護されたコマンド

「パスワード保護されたコマンド」フィーチャーを使用可能または使用不可にするには、「構成マネージャー」の「パスワード保護されたコマンド」ノードを使用します。このフィーチャーを使用可能にすると、WebSphere Commerce は、WebSphere Commerce にログオンした登録済みユーザーに、まずパスワードを入力してから、指定した WebSphere Commerce コマンドの実行要求を続行するよう求めます。

注意: パスワード保護されたコマンドを構成する場合、コマンド選択リストに表示されるコマンドには、一般ユーザーまたはゲスト・ユーザーが実行できるコマンドもあることに注意してください。そのようなコマンドを、パスワードで保護して構

成すると、一般ユーザーおよびゲスト・ユーザーはそのコマンドを実行できなくなります。したがって、コマンドを構成してパスワードで保護する場合は注意を払う必要があります。

注: WebSphere Commerce では、**認証済み (authenticated)** と指定されているコマンドか、または URLREG 表で https フラグが設定されているコマンドのみが使用可能コマンド・リストに表示されます。

「パスワード保護されたコマンド」ノードの使用の詳細は、 61 ページの『パスワード保護されたコマンドの使用可能化』を参照してください。

セッション・ポリシー

WebSphere Commerce ではセッション・ポリシーは、ログイン・タイムアウト・ポリシーとして具体化されています。

ログイン・タイムアウト・ポリシーの使用時には WebSphere Commerce は「ログイン・タイムアウト」ノードを使って、期間を超えて非アクティブになっているユーザーをログオフさせ、再度、システムにログオンするよう要求します。この強化機能は、WebSphere Commerce 構成マネージャーを使って起動します。これについては、 59 ページの『ログイン・タイムアウトの使用可能化』に詳述されています。

第 3 章 許可の概念

WebSphere Commerce は、アクセス制御または許可を、ユーザーまたはアプリケーションがリソースにアクセスする権限を持っていることを検査するプロセスと見なします。このセクションでは、WebSphere Commerce のアクセス制御のいくつかの面の詳細を説明します。

WebSphere Commerce での許可またはアクセス制御は、アクセス制御ポリシーを使用して行われます。アクセス制御ポリシーとは、一連のリソースに対して一連のアクションを実行できるユーザーのグループを記述する規則のことです。 WebSphere Commerce には、デフォルトのアクセス制御ポリシーのセットが用意されています。これらのデフォルト・アクセス制御ポリシーは、XML 形式で指定されており、e-commerce サイトが必要とする一般的なアクセス制御要件のほとんどを解決するように設計されています。

ビジネス・モデル

WebSphere Commerce 5.4 では、インスタンスの作成後に、サイト管理者が以下の点を決定する必要がありました。

1. サイトに適した組織構造
2. 各組織に割り当てる役割
3. 必要なアクセス制御ポリシー

これらの点に関する決定が済んだ時点で、該当する組織に対してストアを公開できるようになりました。

WebSphere Commerce 5.5 では、ビジネス・モデルの作成によってこのプロセスが簡略化されています。ビジネス・モデルは、特定の e-commerce ソリューションを対象とした組織構造、役割、アクセス制御ポリシー、事前定義ストアを提供します。開発ステージでは、ビジネス・モデルを 1 つの基盤として活用し、その基盤に対してコンテンツの追加や削除や変更を行えるようになっています。

WebSphere Commerce 5.5 には、以下のビジネス・モデルが用意されています。

- 消費者向け
- B2B 向け
- デマンド・チェーン
- ホスティング
- サプライ・チェーン

ビジネス・モデルと WebSphere Commerce のアクセス制御コンポーネントを理解するには、まず e-commerce サイトの一般的な組織的階層について理解する必要があります。

注: ビジネス・モデルについての詳細は、「*WebSphere Commerce 基本*」を参照してください。

組織的な階層

WebSphere Commerce メンバー・サブシステム内のユーザーおよび組織エンティティーは、階層的に編成されています。この階層は典型的な組織的階層をエミュレートしており、組織および組織単位ごとにエントリーがあり、リーフ・ノードのユーザーごとにエントリーがあります。この階層には、最上部に*ルート組織* と呼ばれる人工的な組織エンティティーが置かれます。他のすべての組織単位およびユーザーは、このルート組織の子孫になります。ルート組織の下に、1 つのセラー組織といくつかのバイヤー組織が置かれます。これらの組織すべてには、その下に 1 つ以上のサブ組織が置かれます。バイヤーまたはセラー管理者は、その組織の責任者であり、その組織を保守する責任があります。セラー組織サイドでは、各サブ組織内に 1 つ以上のストアが置かれます。ストア管理者がそのストアを保守する責任者です。次の図は、企業間取引 e-commerce サイトの組織階層を示しています。

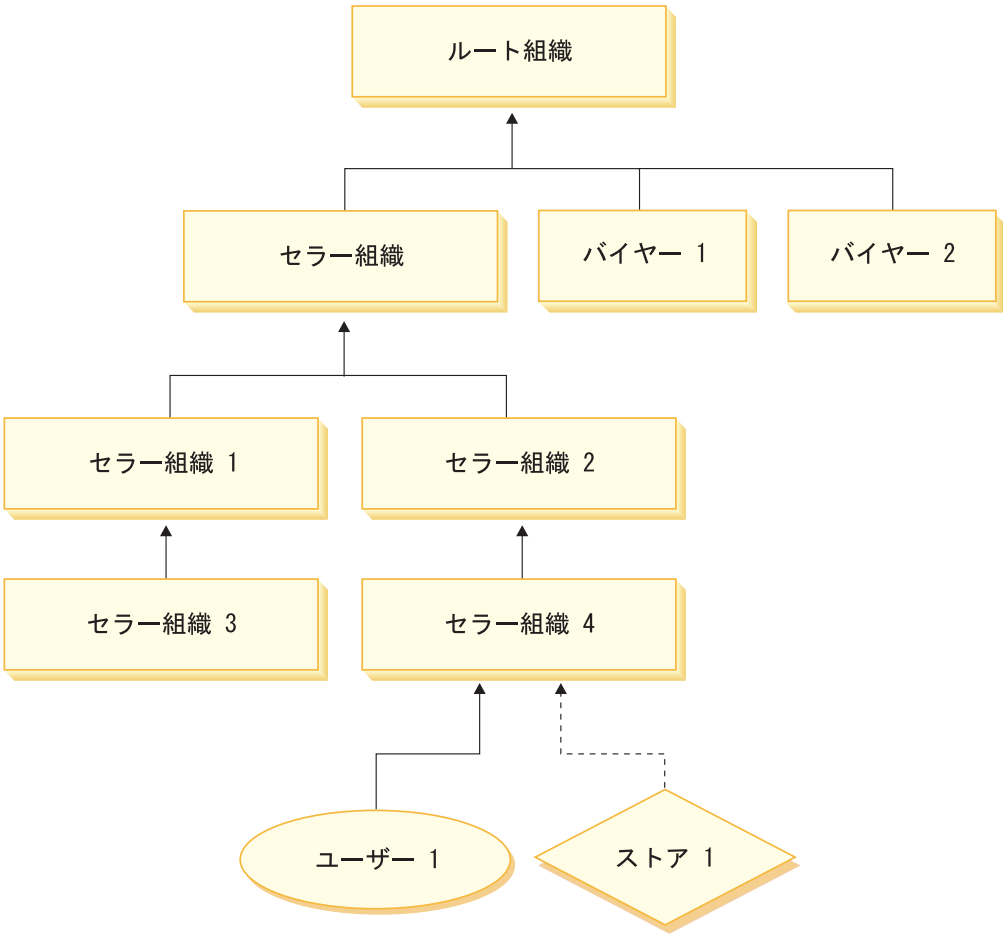


図 2. 企業間取引サイトの組織階層

ルート組織

ルート組織は、組織階層の最上部に位置します。サイト管理者は、WebSphere Commerce 内でどの操作でも実行できるスーパーユーザー・アクセスを持っています。サイト管理者は、WebSphere Commerce および関連ソフトウェアやハードウェ

アのインストール、構成、および保守を行います。この役割では、通常、アクセスおよび許可を制御 (つまり、メンバーを作成して適切な役割に割り当てる) して、Web サイトを管理します。 サイト管理者は、ユーザーに役割を割り当て、そのユーザーが役割を果たす特定の組織を指定することができます。許可を受けた関係者しか機密情報にアクセスできないようにするために、サイト管理者は、各管理者にパスワードを割り当てなければなりません。このようにすることで、カタログの更新または RFQ の承認などに関して重要な責任を制御することができます。

注: ユーザーは、親組織以外の組織で役割を果たすことができます。

WebSphere Commerce サイトには、1 つのセラー組織があります。企業間取引サイトでは、1 つ以上のバイヤー組織もあります。サイト管理者はセラー組織 (ストアを組織する) のアクセス制御ポリシーと、そのストアから購入する各組織のアクセス制御ポリシーの両方を定義します。企業対顧客のサイトでは、バイヤー組織はありません。企業対顧客の顧客は、デフォルト組織のメンバーとしてモデル化されています。

組織 (セラー)

企業間取引および企業対顧客取引の両方で、サイト管理者は最上位のセラーを 1 つ作成します。このセラー組織の下に、他のサブ組織または組織単位を作成できます。これら販売サイドの組織エンティティーは 1 つ以上のストアを所有できます。そしてサイト管理者は、セラー組織に特別なアクセス制御ポリシーを定義し、その組織を管理するためにセラー管理者を割り当てます。セラー管理者はユーザーを登録し、その組織に関係するアクセス制御ポリシーに従って、その組織のビジネス・ニーズに合うようにユーザーに異なる役割を割り当てます。

セラー管理者の責任は以下のように要約できます。

- ストアを所有できるサブ組織を作成します。オプションで、組織の中のどのプロセスに承認が必要であるかを定義します。このステップは、企業間取引のサイトにのみ必要です。
- サブ組織に役割を割り当てます。
- ユーザーを作成します。
- ユーザーに役割を割り当てます。

組織 (バイヤー)

企業間取引サイトでは、サイト管理者はビジネスの必要に応じて、 1 つまたは複数のバイヤー組織を作成します。そしてサイト管理者は、バイヤー組織に特別なアクセス制御ポリシーを定義し、バイヤー組織を管理するためにバイヤー管理者を割り当てます。バイヤー管理者はユーザーを登録し、その組織に関係するアクセス制御ポリシーに従って、その組織のビジネス・ニーズに合うようにユーザーに異なる役割を割り当てます。

バイヤー管理者の責任は以下のように要約できます。

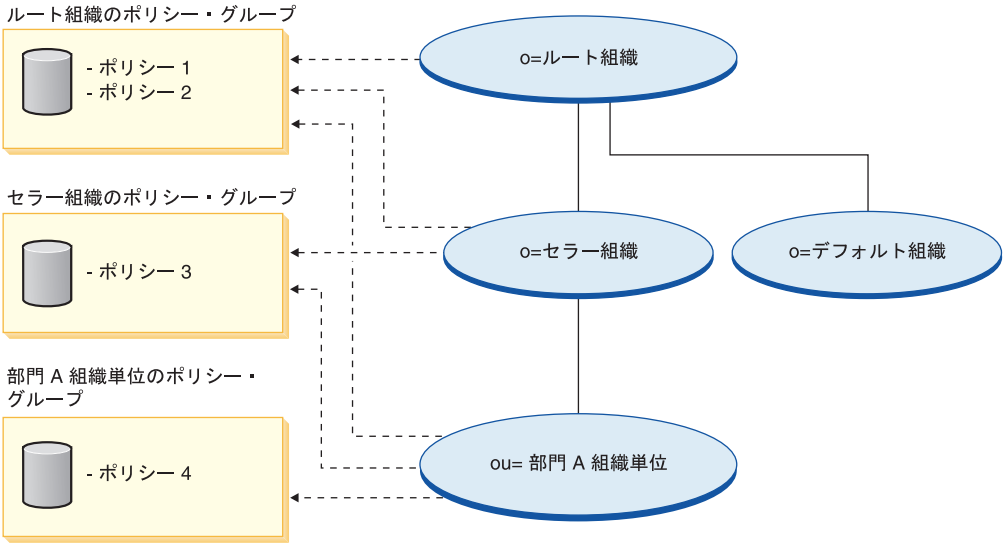
- バイヤー組織の中にサブ組織を作成して管理します。オプションで、組織の中のどのプロセスに承認が必要であるかを定義します。このステップは、企業間取引のサイトにのみ必要です。
- サブ組織に役割を割り当てます。

- ユーザーを作成します。
- ユーザーに役割を割り当てます。

注: サイト管理者は、必要に応じて、バイヤー組織のアクセス制御ポリシーを変更および管理できます。サイト管理者の作業の詳細については、「WebSphere Commerce オンライン・ヘルプ」を参照してください。

ポリシー・グループ

WebSphere Commerce 5.5 は各種のビジネス・モデルをサポートしており、各ビジネス・モデルには独自のアクセス制御ポリシー・セットがあります。それぞれのモデルの中でポリシー・セットをグループ化するために、ポリシー・グループを作成します。ポリシーが該当するポリシー・グループに明示的に割り当てられた時点から、各組織は 1 つ以上のポリシー・グループに加入できるようになります。たとえば、以下の図では、セラー組織はセラー組織ポリシー・グループと、ルート組織ポリシー・グループに加入しています。

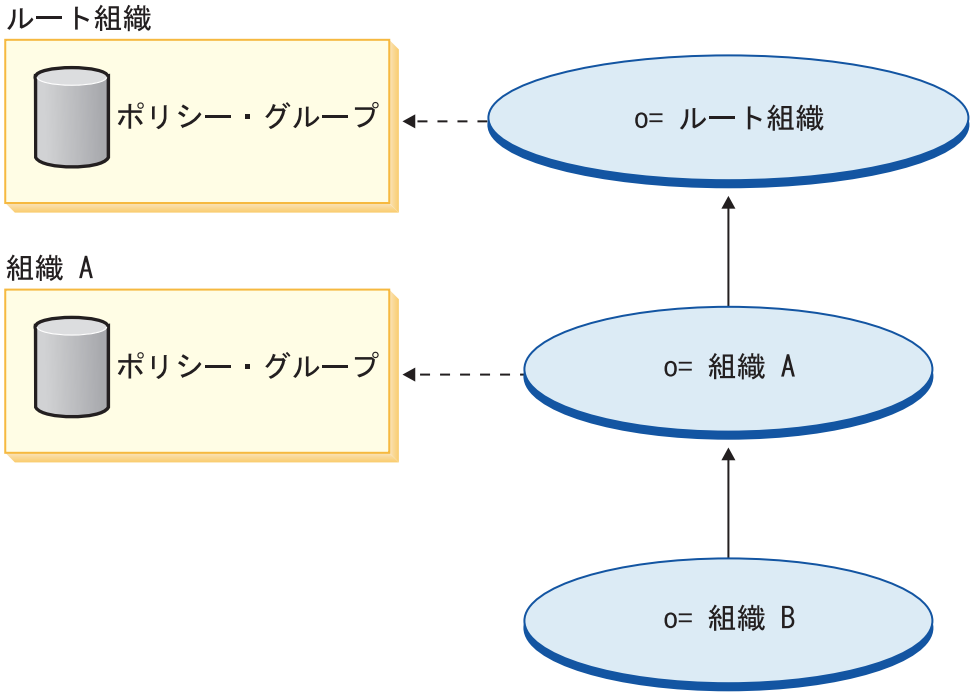


ポリシーは、ポリシー・グループに割り当てられます。たとえば、前の図では、ポリシー 1 とポリシー 2 はルート組織ポリシー・グループに割り当てられ、ポリシー 3 はセラー組織ポリシー・グループに割り当てられ、ポリシー 4 は部門 A 組織単位ポリシー・グループに割り当てられます。

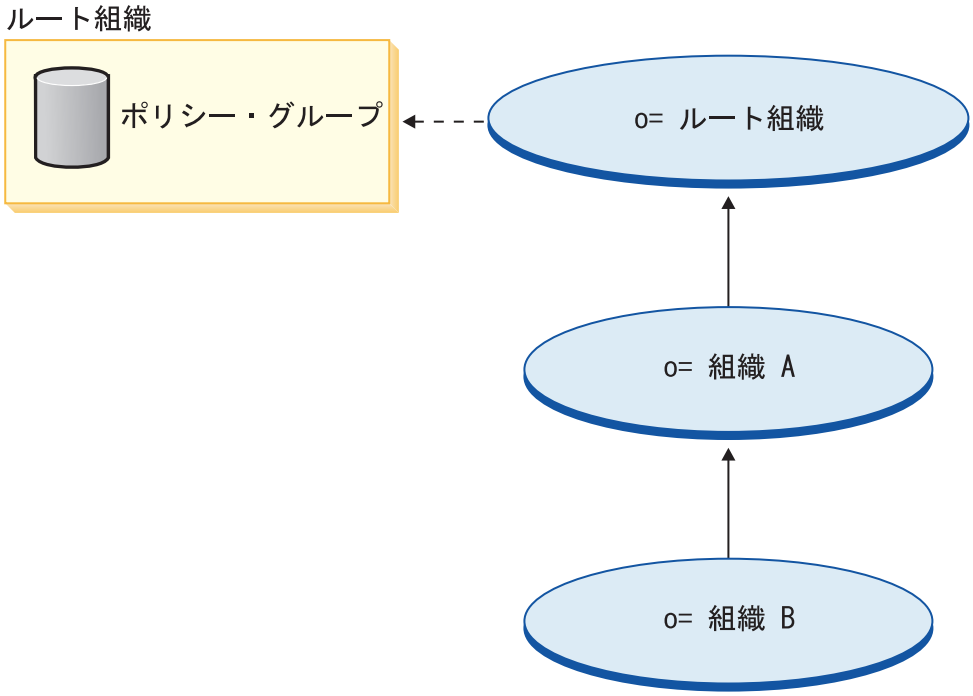
ポリシー・グループの加入

旧バージョンの WebSphere Commerce では、ポリシーは、ポリシー所有者組織の子孫が所有するすべてのリソースに適用されました。たとえば、組織 A に 1 つのポリシーがあり、その組織 A が組織 B の親になっている場合、組織 B にもそのポリシーが暗黙的に適用されることになります。 WebSphere Commerce 5.5 では、各組織がポリシー・グループに加入できるようになりました。 WebSphere Commerce 5.5 では、たとえば、組織 B がどのポリシー・グループにも加入していないと、アクセス制御フレームワークは、組織階層の上位に向かって検索を開始し、少なくとも 1 つのポリシー・グループに加入している組織を検出しようとします。組織 B の直接の親に当たる組織 A がいずれかのポリシー・グループに加入していれば、検索はそこでストップし、そのポリシー・グループのポリシーが組織 A と B に適用

されます。このことが、以下の図に示されています。

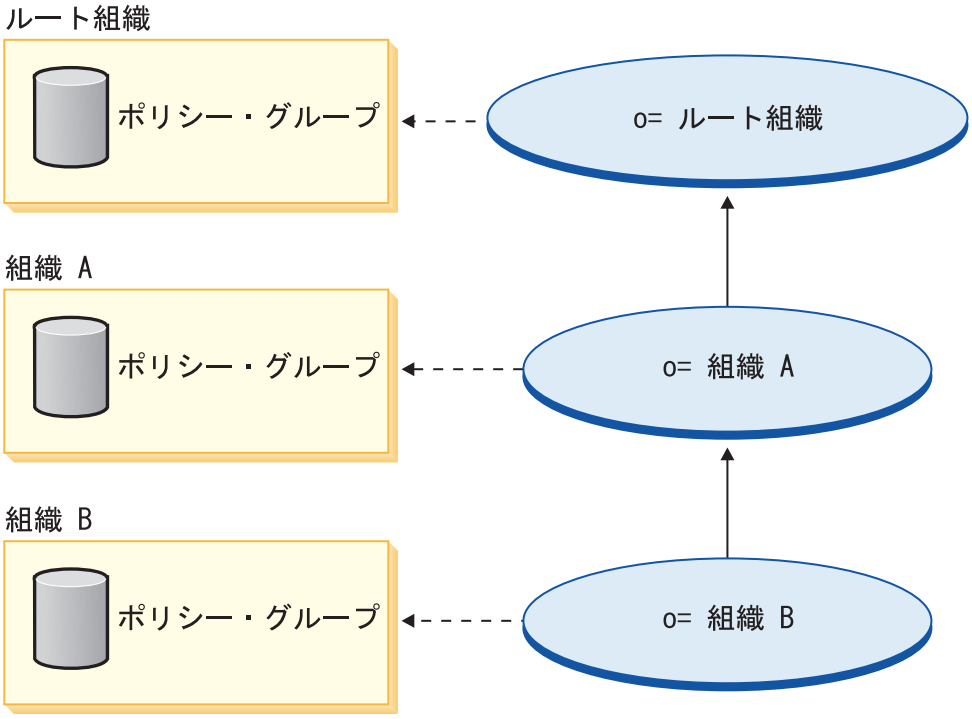


組織 A がいずれのポリシー・グループにも加入していない場合は、検索処理が組織階層をさらに上っていき、ポリシー・グループに加入している組織を検出するまで検索を続けます。このことは、ルート組織がポリシー・グループに加入している、以下の図に示されています。そのグループのポリシーは、組織 B と組織 A に適用されます。



組織 B がいずれかのポリシー・グループに加入している場合は、検索は組織 B でストップします。そのため、組織 B ポリシー・グループのポリシーだけが、組織

B に適用されます。



アクセス制御ポリシー

アクセス制御ポリシーは、ユーザーのグループが、WebSphere Commerce 内の一連のリソースに対して一連のアクションを実行することを許可します。 1 つ以上のアクセス制御ポリシーによって許可されない限り、ユーザーはシステムのどの機能にもアクセスすることができません。アクセス制御ポリシーを理解するためには、ユーザー、アクション、リソース、および関係の 4 つの概念を理解することが必要です。ユーザーは、システムを使用する人間です。リソースは、保護される必要のあるシステム内のオブジェクトです。アクションは、ユーザーがリソースに対して実行できるアクティビティーです。 関係は、ユーザーとリソースの間に存在するオプションの条件です。

アクセス制御ポリシーのエレメント

アクセス制御ポリシーは、4 つのエレメントで構成されています。

アクセス・グループ
ポリシーが適用されるユーザーのグループ。

アクション・グループ
ユーザーがリソースに対して実行するアクションのグループ。

リソース・グループ
ポリシーが制御するリソース。リソース・グループには、`contract` や `order` などのビジネス・オブジェクト、あるいは特定の役割を持つユーザーが実行できるすべてのコマンドなど、関連するコマンドのセットが含まれることがあります。

関係 (オプション)

各リソース・クラスには、関係のセットを関連付けることができます。各リソースは、それぞれの関係を実行する一連のユーザーを指定できます。 たとえば、ポリシーは、オーダーの作成者だけがオーダーを変更できると指定できます。この場合、関係は creator で、この関係はユーザーとオーダー・リソースの間に存在することになります。

アクセス制御ポリシーの概念

アクセス制御ポリシーは、サイトに対するユーザーのアクセスを認可します。担当作業を実行する許可を 1 つ以上のアクセス制御ポリシーを通して受けない限り、ユーザーはサイトのどの機能にもアクセスできません。

アクセス制御ポリシーはそれぞれ以下の形式をとります。

```
AccessControlPolicy [AccessGroup,ActionGroup,ResourceGroup,Relationship]
```

アクセス制御ポリシー内に含まれるエレメントは、ある特定のアクセス・グループに属するユーザーに対して、特定のリソース・グループに属するリソース上で指定されるアクション・グループのアクションを実行する許可が与えられているということを指定します。ただし、ユーザーがそのリソースに関して特定の関係を満たしているということを前提とします。 関係は必要な場合にのみ指定します。たとえば、[AllUsers, UpdateDoc, doc, creator] は、文書の作成者であれば、すべてのユーザーが文書を更新できることを指定します。

次のセクションでは、アクセス制御に関連する、概念的な情報と用語を説明します。

メンバー・グループ

WebSphere Commerce のメンバー・サブシステムを使用して、メンバー・グループを作成することが可能です。メンバー・グループとは、さまざまなビジネスの要件に合わせて分類されたユーザー・グループのことです。アクセス制御や承認といった目的のほかにも、マーケティング (割引や価格の計算や商品の表示) などを目的としてグループ分けを使用できます。アクセス・グループ (-2) タイプのメンバー・グループはアクセス制御の目的、ユーザー・グループ (-1) タイプのメンバー・グループは一般的な使用目的で使用されます。メンバー・グループは、MBRGRPUSG 表内でメンバー・グループ・タイプと関連付けられます。

アクセス・グループ: アクセス・グループ (-2) タイプのメンバー・グループは、アクセス制御を目的としてユーザーをグループ化するためのものです。アクセス・グループは、アクセス制御ポリシーの 1 つのエレメントです。通常、アクセス・グループでのメンバーシップの基準は、役割、ユーザーが所属する組織、またはユーザーの登録情報に基づいています。たとえば、Buyer Administrators というアクセス・グループは、バイヤー管理者の役割を果たすユーザーのグループです。

WebSphere Commerce には、多数のデフォルトの役割が組み込まれています。また、各役割には、暗黙的にその役割を参照する対応したデフォルトのアクセス・グループがあります。役割は、ユーザーがサイトで実行するアクティビティーのタイプに基づいて、アクセス・グループにユーザーを追加する際の属性として使用されます。たとえば、デフォルトでセラー管理者と呼ばれる役割があり、それに対応する Seller Administrators という名前のアクセス・グループがあります。サイト管

理者は、WebSphere Commerce 管理コンソールを使ってサイトのアクセス・グループを作成、保守、および削除します。サイト管理者、バイヤー管理者、セラー管理者、またはチャネル・マネージャーは、 WebSphere Commerce 組織管理コンソールを使用して、ユーザーに役割を割り当てたり、ユーザーを明示的にアクセス・グループに割り当てたりします。

暗黙アクセス・グループ: 暗黙アクセス・グループは、一連の基準によって定義されます。基準を満たす人はすべてこのグループのメンバーです。 基準は、通常はユーザーの役割、親組織、または登録状況を基にしています。マーケット・グループにメンバーシップを定義する暗黙的な条件は、 MBRGRPCOND 表の CONDITIONS 列に指定します。 ユーザーの属性を指定する暗黙アクセス・グループを使用すると、個々のユーザーを明示的に割り当てたり割り当てを解除したりする必要がないので、同様のユーザーへのアクセスを許可することが簡単になります。また、ユーザーの属性が変化するときに、グループのメンバーを更新する必要もなくなります。さらに、複数のアクセス・グループは、同じユーザー属性を参照できるので、属性をユーザーに割り当てると、そのユーザーを複数のアクセス・グループに暗黙に組み込むことができます。アクセス・グループの単純な基準は、ユーザーがどの組織のその役割を果たすかどうかに関係なく、特定の役割に割り当てられているすべての人を含めます。さらに複雑な基準を使用して、特定の組織の考えられる一連の役割のうちの 1 つを果たすユーザーだけがアクセス・グループに所属することを指定します。

明示アクセス・グループ: ユーザーを明示的にメンバー・グループに追加したり、メンバー・グループから除去することができます。これら明示的な操作はどちらも MBRGRPMBR 表を使用して行われます。明示アクセス・グループには、明示的に割り当てられたユーザーが含まれており、これらのユーザーは共通属性を共用している場合もあれば、共用していない場合もあります。また、 暗黙的に定義されたグループに入るための条件を満たしているユーザーのうち、除外したい個々のユーザーを除外することもできます。

ユーザー・グループ: ユーザー・グループ (-1) タイプのメンバー・グループは、マーチャントによって定義される共通の関心を持つユーザーの集合です。ユーザー・グループは、常連の顧客または優良な顧客に対して、大きなストアが提供するクラブに似ています。このユーザー・グループに加わると、顧客は割引や製品購入に関係する他の特典を受けることができます。たとえば、市場調査の結果、年齢層の高い顧客が旅行用の書籍とバッグを頻繁に購入することが分かった場合、これらの顧客を Seniors' Travel Club というグループのメンバーに割り当てることができます。同様に、ビジネスの目的で常連の顧客に特典を与えるためにユーザー・グループを作成することもできます。

アクション

一般に、アクションとはリソースに対して実行する操作のことです。コントローラー・コマンドの役割ベースのポリシーでは、アクションは Execute であり、リソースは実行されるコマンドです。ビューの役割ベースのポリシーでは、アクションはビューの名前であり、リソースは com.ibm.commerce.commands.ViewCommand です。リソース・レベルのアクセス制御の場合、アクションは通常は WebSphere Commerce コマンドにマップされ、リソースは一般に保護されている EJB (Enterprise Java Bean) のリモート・インターフェースになります。たとえば、コントローラー・コマンド com.ibm.commerce.order.commands.OrderCancelCmd は、

com.ibm.commerce.order.objects.Order リソース上で操作を行います。最後に、Data Bean ポリシーでは、Display アクションは Data Bean リソースをアクティブにするために使用されます。

サイト管理者は、既存のアクションをアクション・グループに関連付けるために WebSphere Commerce 管理コンソールを使用することはできますが、新しいアクションを作成するためにこれを使用することはできません。新しいアクションは、XML ファイルで定義し、データベースにロードすることによって作成できます。アクションは ACACTION 表に格納されます。

アクション・グループ

アクション・グループは、関連するアクションのグループのことです。アクション・グループの例としては、以下のコマンドを含む AccountManage グループがあります。

- com.ibm.commerce.account.commands.AccountDeleteCmd
- com.ibm.commerce.account.commands.AccountSaveCmd

アクション・グループを作成、更新、および削除できるのはサイト管理者のみです。 これは、 WebSphere Commerce 管理コンソールを使用したり、XML を介して行うことができます。アクション・グループは、ACACTGRP 表に格納されます。 アクションは、ACACTACTGP 表内でアクション・グループと関連付けられます。

リソース・カテゴリー

リソース・カテゴリーとは、アクセス制御によって保護する必要のあるリソースのクラスのことです。 リソースには、保護可能インターフェース情報をインプリメントする必要があります。また、リソース・カテゴリーは、オーダー、RFQ、オークションなどの Java クラスです。リソースとは、これらのクラスのインスタンスです。たとえば、オークション管理者 A によって作成された Auction1 は 1 つのリソースであり、オークション管理者 B によって作成された Auction2 はまた別のリソースです。これら 2 つのリソースは、リソース・カテゴリー「オークション」に属します。

注: 保護可能インターフェースについての詳細は、「*IBM WebSphere Commerce プログラマーズ・ガイド*」を参照してください。

リソース・カテゴリーは、ACRESCGRY 表で定義され、便宜上、リソースと呼ばれることがあります。 サイト管理者は、 WebSphere Commerce 管理コンソールを使用して、既存のリソース・カテゴリーをリソース・グループに関連付けることができます。新しいリソース・カテゴリーは、XML を使用して作成することができます。

リソース

リソースとは、システム内の保護する必要があるオブジェクトのことです。たとえば、WebSphere Commerce において保護する必要のあるリソースの一部として、RFQ、オークション、オーダーなどがあります。リソースごとに所有者がいます。リソースの所有権を使用して、どのアクセス制御ポリシーを適用するかが判別されます。アクセス制御ポリシーには所有者がおり、この所有者は組織上のエンティティーです。ある組織エンティティーが所有しているポリシーは、そのポリシーを含む、そのポリシー・グループに加入している組織エンティティーが所有しているリ

ソースだけに適用されます。ポリシー・グループに加入していないリソースを所有する組織の場合、最も近い子孫の組織が加入しているポリシー・グループ内のポリシーが適用されます。

コントローラー・コマンド・リソース: コントローラー・コマンドの役割ベースのアクセス制御の場合、ポリシーは、コントローラー・コマンド・リソース上で `Execute` アクションが実行されるように構成されています。これらのポリシーの目的は、コントローラー・コマンドの実行対象を、指定された役割のユーザーだけに限定することにあります。普通は、これらのポリシーのアクセス・グループには 1 つの役割があります。たとえば、プロダクト・マネージャーにはプロダクト・マネージャー役割があります。したがって、リソース・グループは、プロダクト・マネージャーが実行できるコントローラー・コマンドの集合になります。

コントローラー・コマンドで役割ベースのアクセス制御を強制する間に、このコマンドの所有者を判別する必要があります。これは、コマンドで `getOwner()` メソッドを呼び出すことによって行います (このメソッドがインプリメントされている場合)。 通常はこのメソッドはインプリメントされていないので、 WebSphere Commerce Runtime は以下のいずれかを行ってコマンドの所有者を評価します。

- 現在コマンド・コンテキストにあるストアを所有する組織を使用する。
- コマンド・コンテキストにストアがない場合は、ルート組織を所有者として使用する。

Data Bean リソース: Data Bean の中には保護する必要がないものもあります。既存の WebSphere Commerce アプリケーション内では、保護する必要のある Data Bean は、必要なアクセス制御をすでにインプリメントしています。何を保護すべきかという問題は、新しい Data Bean を作成するときに発生します。どのリソースを保護するかは、アプリケーションに応じて決定します。表示する情報が、 Data Bean を含む JSP (Java Server Page) に関連する、ビューが役割ベースのアクセス制御によって十分に保護されていない場合は、 Data Bean を保護する (直接的にまたは間接的に) 必要があります。

Data Bean を保護する必要がある場合で、Data Bean が単独で存在できる場合は、これを直接保護する必要があります。 Data Bean の存在が別の Data Bean の存在に依存する場合は、他の Data Bean に保護を代行させるべきです。直接保護される Data Bean の例としては、`Order` Data Bean があります。間接的に保護される Data Bean の例としては、`OrderItem` Data Bean があり、これは `Order` Data Bean がある場合に限り存在します。 Data Bean リソースを保護する方法の詳細については、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」を参照してください。

データ・リソース: データ・リソースは、オークション、オーダー、RFQ、ユーザーなどの、操作できるビジネス・オブジェクトを指します。通常、これらは、Enterprise Bean レベルで保護されますが、保護可能インターフェースがインプリメントされている限り、どのクラスを保護することも可能です。データ・リソースは、リソース・レベルのアクセス制御検査を使用して保護されます。これを行う一般的な方法は、コントローラー・コマンドまたはタスク・コマンドの `getResources()` メソッドでデータ・リソースを戻すという方法です。詳細については、「*WebSphere Commerce 5.4 プログラマーズ・ガイド*」を参照してください。

リソース・グループ

リソース・グループは、関連したリソースのセットを指します。リソース・グループには、契約または関連コマンドのセットなどのビジネス・オブジェクトを含めることができます。アクセス制御では、リソース・グループは、アクセス制御ポリシーがアクセス権を与えるリソースを指定します。

リソース・グループは、ACRESGRP 表で定義されています。 サイト管理者は、WebSphere Commerce 管理コンソールまたは XML を使用して、リソース・グループを管理したり、リソースをリソース・グループに関連付けることができます。

暗黙的なリソース・グループ: 暗黙的なリソース・グループは、特定の属性に合うリソースを定義します。これらの属性の 1 つは、 Java クラス名でなければなりません。他の属性には、状況、ストア ID、価格などを含めることができます。たとえば、保留状況 (ORDERS.STATUS=P) のオーダーをすべて組み込む暗黙的なリソース・グループを作成できます。通常、暗黙的なリソース・グループは、リソースが Java クラス名を超えて共通属性を共有する場合に、リソース・レベルのポリシーで使用されるリソースをグループ化するために使用されます。

暗黙的なリソース・グループは、 ACRESGRP 表の CONDITIONS 列で定義されています。 簡単な暗黙的リソース・グループは、 WebSphere Commerce 管理コンソールを使用して作成できます。より複雑なグループは、XML を使用して作成できます。

明示的なリソース・グループ: 明示的なリソース・グループは、 1 つ以上のリソース・カテゴリーをリソース・グループに関連づけることによって指定します。この関連づけは、ACRESGPRES 表で行います。 Java クラス名をリストすることによって、明示的にリソース・カテゴリーをグループに追加すると、共通の属性を共用する必要のない個々のリソースをグループ化することになります。

関係

各リソースでは、何らかの関係をそのリソース自体に関連させていたり、各関係を満たすメンバーのセットを関連させている場合があります。たとえば、すべてのリソースには、*所有者* の関係があり、その関係はリソースの所有者によって実現されます。他の関係には、文書の宛先やオーダーの作成者を含めることができます。これらのリソース関係は、リソースの特定のインスタンスでの特定のアクションを実行する人を決定する上で重要です。たとえば、文書の作成者は、文書を削除することができないかもしれませんが、監査者はおそらく削除できます。同様に、校閲者は文書を読み、承認することしかできず、文書を転送したり他の操作を実行したりすることはできないかもしれません。

関係は ACRELATION 表に保管され、 ACPOLICY 表の ACRELATION_ID 列を使ってアクセス制御ポリシー・オプションで指定されます。ユーザーとリソースの間の関係を満たす必要のあるポリシーを評価する際には、リソースに対しての fulfills(Long Member, String relationship) メソッドが呼び出されて、評価が行われます。これらの関係のことを、関係グループと比較して、単純関係と呼ぶことがあります。

関係グループ: アクセス制御ポリシーは、アクセス対象のリソースに対してユーザーが特定の関係を満たさなければならないよう指定したり、関係グループ名の中に指定されている条件をユーザーが満たさなければならないように指定したりできます。ほとんどの場合 1 つの関係だけで十分です。しかしながら、もっと複雑な関係が必要な場合は、代わりに関係グループを使用できます。関係グループを使用する

と、複数の関係や、関係のチェーンを指定できます。どちらの場合も、関係チェーン構成を使用して指定します。関係チェーンでは、単純関係 (ユーザーとリソースの間の直接の関係) も表せますが、ユーザーとリソースの間の一連の関係も表すことができます。たとえば、リソースと関係 (所有者関係以外) のある組織内のユーザーに役割がなければならないことを表すには、関係グループを使用しなければなりません。この例では、ユーザーと組織の間の役割関係と、組織とリソースの間の関係が存在します。

関係と関係グループの比較: 概念上はほとんどの関係はユーザーとリソースの間の直接の関係なので、ほとんどの場合 1 つの関係を使用すれば、ユーザー・アプリケーションのアクセス制御要件を満たせるはずです。たとえば、ユーザーがリソースの作成者でなければならないことをポリシーに指定する場合が該当します。しかしながら、複数の関係を指定する必要がある場合は、関係グループを使用する必要があります。たとえば、ユーザーがリソースの作成者または送信者でなければならないことをポリシーに指定する場合が該当します。

関係グループは、ユーザーとリソースの間の関係のチェーンを表す場合にも必要になります。関係のチェーンでは、ユーザーとリソースの間の直接の関係はありません。たとえば、オーダーに指定されている購買組織にユーザーが所属していている場合が該当します。この場合、ユーザーと組織との間に子関係があり、組織とオーダーの間に購買関係があります。

関係チェーン: 各関係グループは、andListCondition または orListCondition エレメントによってグループ化された 1 つ以上の RELATIONSHIP_CHAIN オープン条件で構成されます。関係チェーンとは、1 つ以上の一連の関係のことです。関係チェーンの長さは、その関係チェーンを構成している関係の数によって決まります。長さを判別するには、関係チェーンの XML 表記内の <parameter name= "X" value="Y"/> エントリーの数を調べます。以下は、長さが 1 の関係チェーンの例です。

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

長さ 1 の関係チェーンの場合、<parameter name="Relationship" value="something"> エレメントは、ユーザーとリソースの間の直接の関係を指定します。 value 属性は、ユーザーとリソースの間の関係を表すストリングです。 value 属性は、保護可能リソース上の fulfills() メソッドの関係パラメーターにも対応していなければなりません。

関係チェーンの長さが 2 の場合は、2 つの一連の関係です。 1 つ目の <parameter name= "X" value="Y"/> エレメントは、ユーザーと組織エンティティーとの間に関するものです。 2 つ目の <parmeter name= "X" value="Y"/> エレメントは、組織エンティティーとリソースとの間に関するものです。以下は、長さが 2 の関係チェーンの例です。

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

aValue1 の有効値は HIERARCHY および ROLE です。 HIERARCHY は、メンバーシップ階層内のユーザーと組織エンティティーとの間に階層関係があることを示しています。 ROLE は、ユーザーが組織エンティティーでの役割を果たしていることを示しています。

aValue1 の値が HIERARCHY である場合、可能な値には child が含まれます。これは、ユーザーがメンバー階層内で直接の子となっている組織エンティティーを戻します。 aValue1 の値が ROLE である場合、可能な値には ROLE 表の NAME 列にある有効なエンティティーが含まれます。これは、現行ユーザーがこの役割を果たしているすべての組織エンティティーが含まれます。

aValue3 エントリーは、 1 つ目のパラメーターの評価結果として取り出された 1 つ以上の組織エンティティーとリソースとの間の関係を表すストリングです。この値は、保護可能リソース上の fulfills() メソッドの関係パラメーターに対応します。パラメーター aValue1 を評価することによって複数の組織エンティティーが戻される場合、RELATIONSHIP_CHAIN のこの部分は、これらの組織エンティティーの 1 つ以上がパラメーター aValue2 によって指定される関係を満たす場合に満たされます。

注: 関係グループが 1 つの関係チェーンだけで構成され、その関係チェーンにパラメーター・エレメントが 1 つだけある場合は、単純関係と機能的に同等です。この場合、ポリシー内で関係グループの代わりに関係を使用する方が簡単です。関係グループを定義する方法についての詳細は、 171 ページの『関係グループの定義』を参照してください。

アクセス制御ポリシーのタイプ

アクセス制御ポリシーには、次の 2 つのタイプがあります。

- グループ化可能標準ポリシー (ポリシー・タイプ -2)
- グループ化可能テンプレート・ポリシー (ポリシー・タイプ -3)

グループ化可能テンプレート・ポリシーとグループ化可能標準ポリシーはどちらも、システム内で適用するためには、特定のポリシー・グループに属している必要があります。グループ化可能標準ポリシーは、ポリシーを含むポリシー・グループに加入する組織で一度適用されます。

グループ化可能テンプレート・ポリシーには、システムの実行中に、リソースを所有する組織に範囲指定されるアクセス・グループを持つという点で、動的な性質があります。たとえば、このタイプのポリシーが、組織 XYZ に所有されるリソースに適用される場合、ユーザーが、組織 XYZ またはその上位組織のためにいずれかの指定された役割を果たしたかどうかを検査します。

特殊なデフォルトのアクセス制御ポリシー

以下のポリシーは、いくらかの付加的な説明が必要です。

- SiteAdministratorsCanDoEverything (サイト管理者は実行制限なし)
- BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup (顧客に代わりユーザー顧客サービス・グループがユーザー・コマンドを実行)

SiteAdministratorsCanDoEverything ポリシーは、サイト管理者役割を持つ管理者にスーパーユーザー・アクセスを付与する特別なデフォルト・ポリシーです。このポリ

シーでは、サイト管理者は、たとえアクションやリソースが定義されていない場合であっても、どのリソースに対してもすべてのアクションを実行できます。この役割をユーザーに割り当てる場合は、この点に注意してください。

BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup ポリシーは特殊なポリシーで、これによって特定の管理ユーザーは、他のユーザーに代わって指定のコマンドを実行できます。このポリシーは、たとえば顧客が顧客サービス担当者に、自分に代わってオーダーを作成することを求めるような場合に必要になります。この場合、顧客サービス担当者は、顧客自身がそうしているかのようにコマンドを実行することができます。

役割

上記のとおり、WebSphere Commerce にはデフォルトの役割のセットが用意されています。サイト管理者は、ユーザーをこれらの特定の役割に割り当てる前にこの役割をすべての組織に割り当てる必要があります。 組織が担うことのできる役割は、親組織に割り当てられている役割だけです。

WebSphere Commerce では、すべての役割の有効範囲は 1 つの組織に設定されています。たとえば、あるユーザーが組織 X のプロダクト・マネージャーの役割を果たす場合、組織 X はプロダクト・マネージャーの役割をサポートする必要があります。一般に、ある役割を組織がサポートしなければ、ユーザーはその組織に対してその役割を割り当てることはできません。その場合、このユーザーが組織 X とその下部組織でのみ商品管理を実行できるようにアクセス制御ポリシーをセットアップできます。

注: ユーザーと組織への役割の割り当ては、MBRROLE 表で行います。

WebSphere Commerce に付属のデフォルトの役割は、以下のカテゴリーにグループ分けできます。

- 技術操作の役割
- マーケティングの役割
- 運用の役割
- 顧客サービスの役割
- 企業間関係の役割
- 商品管理と取引管理の役割

WebSphere Commerce 5.5 では、各役割が 1 つ以上のビジネス・モデルと関連付けられています。役割は各モデルの中で、Commerce アクセラレーター、管理コンソール、組織管理コンソールといったツールを使って、一定数のタスクを実行できます。ビジネス・モデルの詳細は、「*WebSphere Commerce 基本*」を参照してください。

以下の図表は、各役割が各ツールに対して持っているアクセス権限をまとめたものです。ユーザーに役割を割り当てる前に、それぞれの役割に適用されるアクセス制限を正しく把握しておいてください。

すべてのストア・サンプルで WebSphere Commerce ツールにマップされている役割

表 1. WebSphere Commerce ツールにマップされている役割

役割	サンプル	ツール
アカウント担当者	• B2B 向け: ToolTech	• アクセラレーター
バイヤー管理者	• B2B 向け: ToolTech	• 組織管理コンソール
バイヤー承認者	• B2B 向け: ToolTech	• 組織管理コンソール
バイヤー (販売サイド)	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター
バイヤー (購買サイド)	• B2B 向け: ToolTech • ホスティング: ホストされるストア • サプライ・チェーン: サプライヤーによってホストされるストア	この役割はサンプルでは使用可能ですが、特定のツールへのアクセス権はありません。
カテゴリー・マネージャー	• 消費者向け: FashionFlow • B2B 向け: ToolTech • デマンド・チェーン: ホストされるストア、カタログ資産ストア • ホスティング: ホストされるストア、カタログ資産ストア • サプライ・チェーン: カタログ資産ストア、サプライヤーによってホストされるストア	• アクセラレーター
チャネル・マネージャー	• デマンド・チェーン: チャネル・ハブ • ホスティング: ホスティング・ハブ • サプライ・チェーン: ストア・ディレクトリー	• アクセラレーター • 組織管理コンソール
顧客サービス担当者	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター
顧客サービス・スーパーバイザー	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター

表 1. WebSphere Commerce ツールにマップされている役割 (続き)

役割	サンプル	ツール
物流管理マネージャー	• B2B 向け: ToolTech • サプライ・チェーン: サプライヤーによってホストされるストア	• アクセラレーター
マーケティング・マネージャー	• 消費者向け: Fashion Flow • B2B 向け: ToolTech • デマンド・チェーン: チャネル・ハブ、ホストされるストア、販売店ストアフロント資産ストア • ホスティング: ホストされるストア、ホストされるストアフロント資産ストア	• アクセラレーター
オペレーション・マネージャー	• 消費者向け: Fashion Flow • デマンド・チェーン: ホストされるストア • ホスティング: ホストされるストア	• アクセラレーター
梱包担当者	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター
調達バイヤー	• B2B 向け: ToolTech • サプライ・チェーン: サプライヤーによってホストされるストア	この役割はサンプルでは使用可能ですが、特定のツールへのアクセス権はありません。
調達バイヤー管理者	• B2B 向け: ToolTech • サプライ・チェーン: サプライヤーによってホストされるストア	この役割はサンプルでは使用可能ですが、特定のツールへのアクセス権はありません。
プロダクト・マネージャー	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター
受取人	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター

表 1. WebSphere Commerce ツールにマップされている役割 (続き)

役割	サンプル	ツール
登録済み顧客	• 消費者向け: Fashion Flow • B2B 向け: ToolTech • デマンド・チェーン: チャネル・ハブ、ホストされるストア • ホスティング: ホスティング・ハブ、ホストされるストア • サプライ・チェーン: ストア・ディレクトリー、サプライヤーによってホストされるストア	この役割はサンプルでは使用可能ですが、特定のツールへのアクセス権はありません。
返品管理者	• 消費者向け: Fashion Flow • B2B 向け: ToolTech	• アクセラレーター
セールス・マネージャー	• B2B 向け: ToolTech • サプライ・チェーン: サプライヤーによってホストされるストア	• アクセラレーター
セラー	• 消費者向け: Fashion Flow • B2B 向け: ToolTech • デマンド・チェーン: ホストされるストア • ホスティング: ホストされるストア • サプライ・チェーン: サプライヤーによってホストされるストア	• アクセラレーター
セラー管理者	• 消費者向け: Fashion Flow • B2B 向け: ToolTech • デマンド・チェーン: チャネル・ハブ、ホストされるストア • ホスティング: ホスティング・ハブ、ホストされるストア • サプライ・チェーン: ストア・ディレクトリー、サプライヤーによってホストされるストア	• 組織管理コンソール

表 1. WebSphere Commerce ツールにマップされている役割 (続き)

役割	サンプル	ツール
サイト管理者 (ルート組織)	• 消費者向け: Fashion Flow • B2B 向け: ToolTech • デマンド・チェーン: チャネル・ハブ、ホストされるストア、カタログ資産ストア、販売店ストアフロント資産ストア • ホスティング: ホスティング・ハブ、ホストされるストア、カタログ資産ストア、ホストされるストアフロント資産ストア • サプライ・チェーン: ストア・ディレクトリー、サプライヤーによりホストされるストア、カタログ資産ストア、サプライヤー資産ストア	• アクセラレーター • 組織管理コンソール • 管理コンソール

注:

1. サイト管理者は、管理コンソールにアクセスできる唯一の役割です。
2. それぞれの役割と、それぞれの役割からアクセスできる各ツールのメニューについての詳細は、「WebSphere Commerce Production オンライン・ヘルプ」の「役割」ファイルを参照してください。
3. 各サンプル・ストアの詳細は、「WebSphere Commerce Production and Development オンライン・ヘルプ」の『ストア』を参照してください。

アクセス制御が無許可のアクションを回避する方法

このセクションでは、ユーザーが許可されたアクションだけを実行できることを保証するために、ポリシー・ベースのアクセス制御がどのように作動するかを説明します。

ユーザー主導のアクションを実行する前の許可の検査

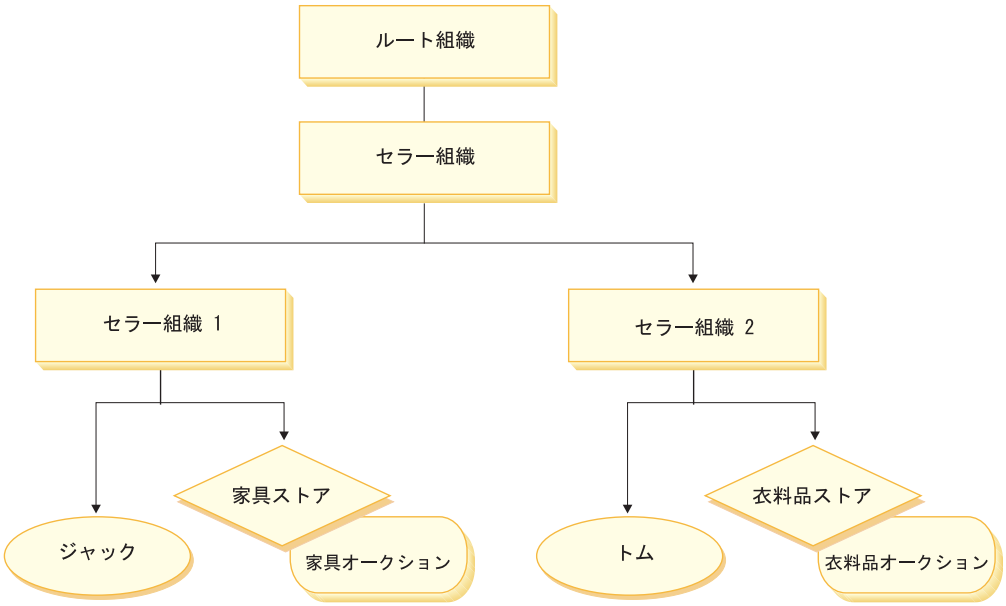
ポリシー・マネージャー は、現行ユーザーが指定されたリソースで指定されたアクションを実行することを許可されているかどうかを判別する、アクセス制御コンポーネントです。アクセス制御ポリシーは XML 形式で指定されます。インスタンスの作成時に、デフォルト・ポリシーおよびポリシー・グループが適切なデータベース表にロードされます。 WebSphere Commerce Application Server の始動時に、アクセス制御情報はメモリー内のキャッシュに入れられるので、ユーザーの許可を検査するために Policy Manager が呼び出されたときに、迅速にその検査を行うことができます。 WebSphere Commerce 管理コンソールを使用したり、 XML ポリシー・データをロードしたりして、データベース内のアクセス制御情報に変更を加える場合には、アクセス制御キャッシュを更新する必要があります。これは、WebSphere

Commerce 管理コンソール内で適切なレジストリーを更新することによって実行できます。ポリシー・データが変更されている場合、 「アクセス制御ポリシー (Access Control Policies)」レジストリーを更新する必要があります。ポリシー・グループ・データが変更されている場合、「アクセス制御ポリシー・グループ (Access Control Policy Groups)」レジストリーを更新する必要があります。 WebSphere Commerce を再始動しても、キャッシュが更新されます。

ユーザーが保護されたリソースに対してアクションを実行しようとすると、アクセス制御検査が行われ、そのユーザーが許可されているかどうかが確認されます。 Policy Manager は、リソースを所有する組織に適用されるすべてのアクセス制御ポリシーを検索します。それから、これらのポリシーを検査して、ユーザーが宛先リソースに対するアクションを実行するよう許可されているかどうかを評価します。そのようなポリシーが少なくとも 1 つあれば、 Policy Manager はアクセス権を付与しますが、なければアクセスが拒否されます。

アクセス制御のレベル

WebSphere Commerce では、2 つの幅広いレベルのアクセス制御があり、それらはコマンド・レベル (役割ベースとも呼ばれる) およびリソース・レベル (インスタンス・レベルとも呼ばれる) です。



コマンド・レベルまたは役割ベースのアクセス制御

コマンド・レベルまたは役割ベースのアクセス制御は、大ざっぱなアクセス制御です。それは「誰が何をできるか」を定義します。役割ベースのアクセス制御によって、特定の役割をもつすべてのユーザーが、特定のコマンドを実行できるように指定できます。「セラーはセラー・コマンドを実行できる」というアクセス制御ポリシーについて検討してみましょう。このポリシー内で、セラー・コマンドの 1 つに `ModifyAuction` コマンドがあります。上記の図で、ジャックとトムはどちらもセラーなので、どちらもオークションに変更を加えることができます。

役割ベースのアクセス制御は、コントローラー・コマンドやビューの場合に使用します。このタイプのアクセス制御は、コマンドが影響を及ぼすデータ・リソースのことを考慮しません。単に、ユーザーが特定のコントローラー・コマンドやビューを実行できるかどうかを判別するだけです。このレベルのアクセス制御は必須であり、ランタイムによって強制されます。

コントローラー・コマンド用のコマンド・レベル・アクセス制御: コントローラー・コマンドを実行するときはいつでも、ユーザーには、コマンド・リソースに対して Execute アクションの実行を認可するアクセス制御ポリシーがなければなりません。リソースはコントローラー・コマンドのインターフェース名です。アクセス・グループは普通、単一の役割に適合します。たとえば、アカウント担当者の役割をもつユーザーが、AccountRepresentativesCmdResourceGroup リソース・グループで任意のコマンドを実行できるように指定できます。

ビュー用のコマンド・レベル・アクセス制御: ビューが URL から直接呼び出されるか、コマンドからのリダイレクトの結果である場合には、アクセス制御ポリシーが必要です。そのようなポリシーには、 ACACTION 表内でアクションとして指定された viewname が必要です。次いでこのアクションは、 ACACTACTGP 表を使ってアクション・グループに関連付けられる必要があります。そしてこのアクション・グループは、 ACPOLICY 表内の適切なコマンド・レベル・ポリシーで参照される必要があります。

インスタンス・レベルまたはリソース・レベルのアクセス制御

インスタンス・レベルまたはリソース・レベルのアクセス制御ポリシーは、 「誰がどんなコマンドをどんなリソースで実行できるか」を決定するきめ細かいアクセス制御を提供します。前述の、セラーがオークションに変更を加えることができる役割ベースのアクセス制御ポリシーの例で、セラーが、役割が自分に割り当てられている組織が所有しているオークションに変更を加えられるように微調整することによって、リソース・レベルのアクセス制御にすることができます。 37 ページで、ジャックはセラー組織 1 に関してセラーの役割を果たします。トムはセラー組織 2 に関してセラーの役割を果たします。ジャックは家具のストアで家具のオークションを作成します。トムは衣料品ストアで衣料品のオークションを作成します。ジャックは家具のオークションに変更を加えられますが、衣料品のオークションには変更を加えられません。トムは衣料品のオークションに変更を加えられますが、家具のオークションには変更を加えられません。

要約すると、最初にシステムはコマンド・レベルのアクセス検査を行います。ユーザーがコマンドの実行を許可されている場合、ユーザーが問題のリソースにアクセスできるかどうかを判別するために、続いてリソース・レベルのアクセス制御ポリシーが適用されます。

リソース・レベルのアクセス制御は、コマンドと Data Bean に適用されます。

コマンドに対するリソース・レベルのアクセス制御: コマンド・レベルのアクセス制御検査が完了した後に、アクセス権が付与されていた場合、次の 2 つのケースのいずれかではリソース・レベルの検査が行われます。

- コマンドが getResources() をインプリメントする場合 — このメソッドは、現行アクションに対して検査の必要なリソースのインスタンスを指定します。なお、コマンドは、ここではアクションです。 WebSphere Commerce Runtime は、getResources() によって指定されるすべてのリソースへのアクセス権を、現行ユ

ーザーが持つように強制します。デフォルトでは getResources() はヌルを戻します。つまり、それはリソース・レベルの検査を何も行わないということです。

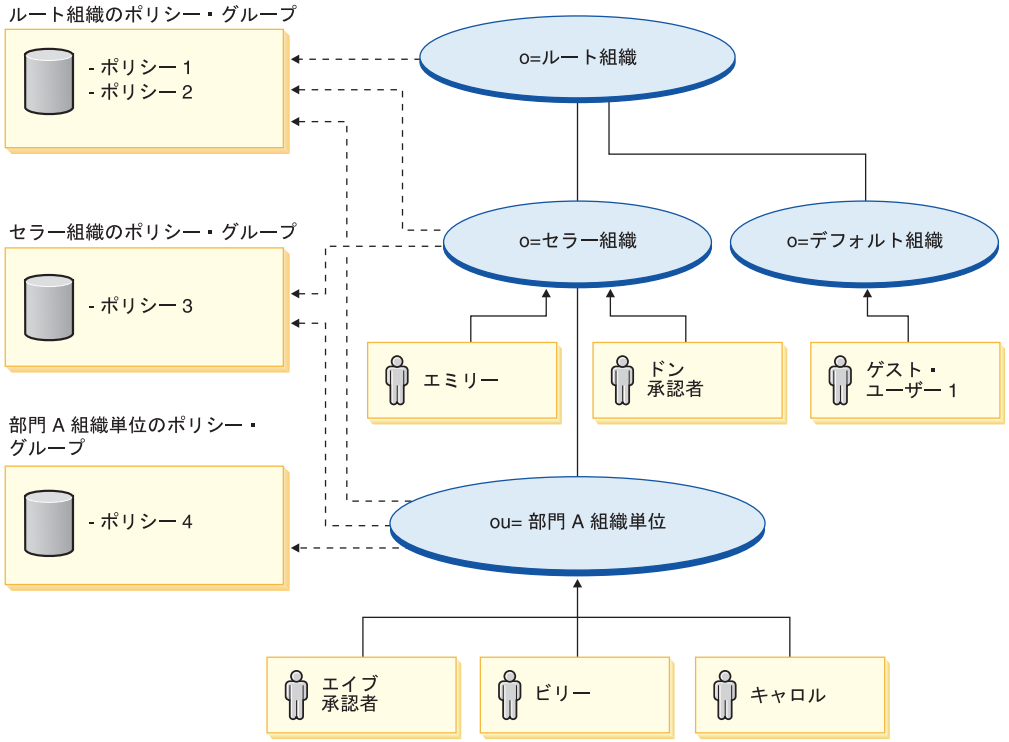
- コマンドが checkIsAllowed(Object Resource, String Action) を呼び出す場合 — これは、getResources() が Runtime により呼び出される時点でどのリソースが検査を必要としているかをコマンド・ライターが知らない場合です。コマンドは必要に応じてこの checkIsAllowed() メソッドを呼び出して、現行のアクションとリソースの対が許可されているかどうかを判別することができます。普通アクションは現行コマンドのインターフェース名です。このメソッドが呼び出されたときにアクセスが拒否された場合には、次の例外が投じられます。
  ECApplicationException(ECMessage._ERR_USER_AUTHORITY, ..)

Data Bean に対するリソース・レベルのアクセス制御: 前述のように、ビューはコマンド・レベル・ポリシーによって保護され、通常は役割に基づいています。たとえば、コマンド・レベル・ポリシーは、セラー管理者が特定のビューに対してアクセス権があることを指定します。多くの場合、JSP 上の Data Bean がすべて、ユーザーがセラー管理者役割を担っている組織に関連していることをさらに保証することが必要です。そのためには、保護 (直接または間接) の必要なすべての Data Bean に Delegator インターフェースをインプリメントさせます。これらの Data Bean は、基本 (独立) Data Bean (保護可能インターフェースをインプリメントしている) を代行します。基本 Data Bean は自己代行するので、両方のインターフェースがインプリメントされることになります。これで、Data Bean 管理者の activate() メソッドを使って Data Bean が呼び出されるたびに、現在のユーザーが 1 次 Data Bean リソースで Display アクションを実行する権限を認可するポリシーがあるかどうかが WebSphere Commerce ランタイムによって確認されます。

アクセス制御ポリシーの評価

アクセス制御ポリシーの評価に関する手引きを以下に示します。このセクションでは、シナリオを示し、グループ化が可能な標準およびテンプレートのアクセス制御ポリシーを評価する方法に関する例を使って説明します。それぞれの項では、まず関連したポリシーの説明があり、次に個々のポリシーを使用したシナリオが説明されています。グループ化可能な標準ポリシーとグループ化可能なテンプレート・ポリシーについての詳細は、 31 ページの『アクセス制御ポリシーのタイプ』を参照してください。

以下の図は、このシナリオを図示したものです。



組織的な階層

この図から、以下の組織がサイトにあることが分かります。

- ルート組織
- セラー組織
- デフォルト組織
- 部門 A 組織単位

図の中の実線は所有を示し、点線は加入を示します。図示されているように、ルート組織はセラー組織とデフォルト組織の親です。セラー組織は部門 A 組織単位の親です。

ユーザー

この図では、ドンとエミリーがセラー組織に登録されています。エイブ、ビリー、およびキャロルは部門 A 組織単位に登録されています。ゲスト・ユーザー 1 は登録されていませんが、アクセス制御の目的で、暗黙的にデフォルト組織に所属しています。

役割

ドンはセラー組織に関して承認者の役割を果たします。エイブは部門 A 組織単位に関して承認者の役割を果たします。

アクセス・グループ

このシナリオでは、以下のアクセス・グループが使用されます。

- Registered users (登録済みユーザー): このグループには、サイト内の少なくとも 1 つの組織に登録されているすべてのユーザーが暗黙的に含まれます。
- Approvers for Seller (セラーの承認者): このグループには、セラー組織に関する承認者の役割を果たすすべてのユーザーが暗黙的に含まれます。
- Approvers for Division A (部門 A の承認者): このグループには、部門 A 組織単位に関する承認者の役割を果たすすべてのユーザーが暗黙的に含まれます。

文書

文書オブジェクトは、保護リソースです。文書の作成場所の組織がその文書の所有者になるよう定義されます。

文書を更新する場合のアクセス制御要件

文書を更新する場合のアクセス制御要件を以下に示します。

1. 登録済みユーザーは、自分が作成した文書を更新できます。
2. 部門 A の承認者は、部門 A が所有する文書を更新できますが、セラーが所有する文書は更新できません。セラー組織の承認者は、部門 A およびセラーの両方が所有する文書を更新できます。

グループ化が可能な標準ポリシーの評価

以下に、グループ化が可能な標準ポリシーとそれらを評価するシナリオをひととおり示します。

文書の更新に関連したアクセス制御ポリシー

文書の更新に関連したポリシーの形式とアクセス制御ポリシーについて、以下に示します。

ポリシーの形式: `[Access Group, Action Group, Resource Group, Relationship]`

ポリシー 1:

```
[Registered Users, Execute Command Action Group,  Update Document
Resource Group, - ]
```

これは、グループ化が可能な役割ベースの標準ポリシーであり、ルート組織が加入するルート組織ポリシー・グループの一部になっています。このポリシーでは、登録済みユーザーが `Update Document` コマンドを実行できます。

ポリシー 2:

```
[Registered Users, Update Document Action Group, document, creator ]
```

これは、グループ化が可能なリソース・レベルの標準ポリシーであり、ルート組織が加入するルート組織ポリシー・グループの一部になっています。このポリシーでは、登録済みユーザーが文書の作成者である場合にその文書を更新できます。

ポリシー 3:

```
[Approvers for Seller, Update Document Action Group, document, - ]
```

これは、グループ化が可能なリソース・レベルの標準ポリシーであり、セラー組織と部門 A 組織単位が加入するセラー組織ポリシー・グループの一部になっています。このポリシーでは、セラーの承認者が、セラーによって所有される文書を更新できます。

ポリシー 4:

```
[Approvers for Division A, Update Document Action Group, document, - ]
```

これは、グループ化が可能なリソース・レベルの標準ポリシーであり、部門 A 組織単位が加入する部門 A 組織単位ポリシー・グループの一部になっています。このポリシーでは、部門 A の承認者が、部門 A によって所有される文書を更新できます。

シナリオ

シナリオ 1 : ビリーが自分の文書を更新しようとする: このシナリオのアクセス制御の評価を以下に示します。

コマンド・レベルの検査:

1. ストア ID が指定されていないので、コマンドの所有者はルート組織に設定されます。したがって、ユーザーにコマンド・レベルのアクセス権があるかどうかを評価するには、ルート組織が加入するポリシー・グループに属するポリシーだけが使用されます。ポリシー 1 および 2 は、ルート組織が加入するポリシー・グループの一部になっています。
2. ビリーは「登録済みユーザー」アクセス・グループのメンバーで、 `Update Document` コマンド・リソースに対して `Execute` アクションを実行しようとしているので、ポリシー 1 によりアクセス権が付与されます。

リソース・レベルの検査:

1. `Update Document` コマンドは、文書リソースを保護するよう指定します。ビリーの文書は部門 A によって所有されています。部門 A はポリシー・グループに加入しているので、そのポリシー・グループに属するすべてのポリシー、つまりポリシー 1、2、3、4 が適用されます。
2. ビリーは「登録済みユーザー」アクセス・グループのメンバーで、文書リソースに対して `Update Document` コマンド・アクションを実行しようとしており、文書との間に作成者関係があるので、ポリシー 2 によりアクセス権が付与されます。

ビリーはコマンド・レベルとリソース・レベルの両方のアクセス制御検査に合格したので、自分の文書を更新できます。

シナリオ 2: ドンがキャロルの文書を更新しようとする: このシナリオのアクセス制御の評価を以下に示します。

コマンド・レベルの検査:

1. ストア ID が指定されていないので、コマンドの所有者はルート組織に設定されます。したがって、ユーザーにコマンド・レベルのアクセス権があるかどうかを評価するには、ルート組織が加入するポリシー・グループに属するポリシーだけが使用されます。ポリシー 1 および 2 は、ルート組織によって所有されています。

2. ドンは「登録済みユーザー」アクセス・グループのメンバーで、 Update Document コマンド・リソースに対して Execute アクションを実行しようとしているので、ポリシー 1 によりアクセス権が付与されます。

リソース・レベルの検査:

1. Update Document コマンドは、文書リソースを保護するよう指定します。キャロルの文書は部門 A によって所有されています。部門 A はポリシー・グループに加入しているので、そのポリシー・グループに属するすべてのポリシー、つまりポリシー 1、2、3、4 が適用されます。
2. ドンは「セラーの承認者」アクセス・グループのメンバーで、文書リソースに対して Update Document コマンド・アクションを実行しようとしているので、ポリシー 3 によりアクセス権が付与されます。

ドンはコマンド・レベルとリソース・レベルの両方のアクセス制御検査に合格したので、キャロルの文書を更新できます。

シナリオ 3: エイブがエミリーの文書を更新しようとする: このシナリオのアクセス制御の評価を以下に示します。

コマンド・レベルの検査:

1. ストア ID が指定されていないので、コマンドの所有者はルート組織に設定されます。したがって、ユーザーにコマンド・レベルのアクセス権があるかどうかを評価するには、ルート組織が加入するポリシー・グループに属するポリシーだけが使用されます。ポリシー 1 および 2 は、ルート組織によって所有されています。
2. エイブは「登録済みユーザー」アクセス・グループのメンバーで、 Update Document コマンド・リソースに対して Execute アクションを実行しようとしているので、ポリシー 1 によりアクセス権が付与されます。

リソース・レベルの検査:

1. Update Document コマンドは、文書リソースを保護するよう指定します。エミリーの文書はセラーによって所有されています。セラー組織はポリシー・グループに加入しているので、そのポリシー・グループに属するすべてのポリシー、つまりポリシー 1、2、3 が適用されます。
2. エイブは「セラーの承認者」アクセス・グループのメンバーではないので、ポリシー 3 によるアクセス権は付与されません。

エイブはコマンド・レベル検査に合格しましたが、リソース・レベルのアクセス制御検査に失格したので、エミリーの文書を更新できません。

シナリオ 4 : ゲスト・ユーザー 1 が自分の文書を更新しようとする: このシナリオのアクセス制御の評価を以下に示します。

コマンド・レベルの検査:

1. ストア ID が指定されていないので、コマンドの所有者はルート組織に設定されます。したがって、ユーザーにコマンド・レベルのアクセス権があるかどうかを評価するには、ルート組織が加入するポリシー・グループに属するポリシーだけが使用されます。ポリシー 1 および 2 は、ルート組織によって所有されています。

2. ゲスト・ユーザー 1 は 「登録済みユーザー」 アクセス・グループのメンバーではないので、ポリシー 1 によるアクセス権は付与されません。

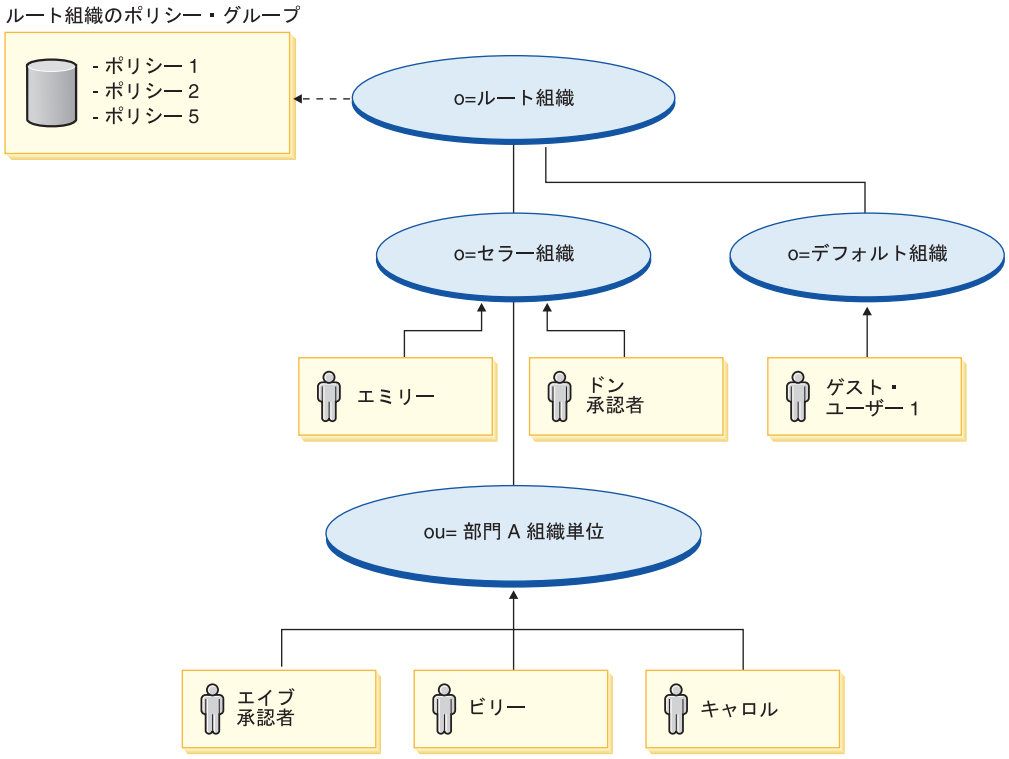
リソース・レベルの検査:

1. コマンド・レベルの検査に失格したので、リソース・レベルの検査は行われません。

ゲスト 1 はコマンド・レベルの検査に失格したので、 自分の文書を更新できません。

グループ化が可能なテンプレート・ポリシーの評価

このセクションは、以下の図に示す構成に基づいています。



文書の更新に関連したアクセス制御ポリシー

この構成では、アクセス制御ポリシー 1 および 2 が依然として適用されますが、グループ化が可能な標準ポリシー 3 および 4 は、グループ化が可能なテンプレート・ポリシー 5 に置き換えられています。ポリシー 1 および 2 についての詳細は、 41 ページの『グループ化が可能な標準ポリシーの評価』を参照してください。

ポリシー 5:

```
[Approvers for Organization, Update Document Action Group, document, - ]
```

このポリシーは、グループ化が可能なリソース・レベルのテンプレート・ポリシーです。これは、ルート組織が加入するルート組織ポリシー・グループの一部です。グループ化が可能なテンプレート・ポリシーは、実行時にリソースを所有する組織に動的に適用されます。これらのポリシーは通常、パラメーター化アクセス・グループを使用します。この場合は、以下のパラメーター化アクセス・グループが使用されます。

- Approvers for Organization (組織の承認者): このグループには、この文書リソースを所有する組織、またはその先祖に当たる組織で承認者の役割を担うすべてのユーザーが暗黙的に含まれます。

シナリオ

以下のシナリオは、前の図で示した 1 つのポリシー・グループだけを持つ構成に基づくものです。「ルート組織」ポリシー・グループには、ポリシー 1、2、および 5 が組み込まれています。

シナリオ 1: ドンがキャロルの文書を更新しようとする: このシナリオのアクセス制御の評価を以下に示します。

コマンド・レベルの検査:

1. ストア ID が指定されていないので、コマンドの所有者はルート組織に設定されます。したがって、ユーザーにコマンド・レベルのアクセス権があるかどうかを評価するには、ルート組織が加入するポリシー・グループに属するポリシー、つまりポリシー 1、2、5 だけが使用されます。
2. ドンは「登録済みユーザー」アクセス・グループのメンバーで、 `Update Document` コマンド・リソースに対して `Execute` アクションを実行しようとしているので、ポリシー 1 によりアクセス権が付与されます。

リソース・レベルの検査:

1. `Update Document` コマンドは、文書リソースを保護するよう指定します。キャロルの文書は部門 A によって所有されています。部門 A はどのポリシー・グループにも加入していないので、アクセス制御フレームワークは、組織階層の検索を開始し、少なくとも 1 つのポリシー・グループに加入している組織を検出しようとします。部門 A の直接の親に当たるセラー組織もポリシー・グループに加入していません。組織階層をさらに上っていくと、ルート組織に行き当たります。この組織はポリシー・グループに加入しているため、そのポリシー・グループ内のポリシー、つまりポリシー 1、2、5 を適用できます。
2. グループ化が可能なテンプレート・ポリシー 5 は、そのリソースを所有する組織、つまり部門 A に適用されます。パラメーター化アクセス・グループ、つまり組織の承認者は、現在のリソース・コンテキストに有効範囲を動的に絞り込み、ユーザーがそのリソースを所有している組織、またはその先祖に当たる組織のアクセス・グループ条件を満たしているかどうかを検査します。この場合、ドンはセラー組織 (部門 A の先祖) の承認者なので、そのアクセス・グループ条件を満たしています。ドンはこの文書リソースに対して Update Document コマンド・アクションを実行するので、ポリシー 5 のその他のエレメントも満たされることになり、リソース・レベルのポリシー検査に合格します。

ドンはコマンド・レベルとリソース・レベルの両方のアクセス制御検査に合格したので、キャロルの文書を更新できます。

シナリオ 2: エイブがエミリーの文書を更新しようとする: このシナリオのアクセス制御の評価を以下に示します。

コマンド・レベルの検査:

1. ストア ID が指定されていないので、コマンドの所有者はルート組織に設定されます。したがって、ユーザーにコマンド・レベルのアクセス権があるかどうかを

評価するには、ルート組織が加入するポリシー・グループに属するポリシー、つまりポリシー 1、2、5 だけが使用されます。

2. エイブは「登録済みユーザー」アクセス・グループのメンバーで、 Update Document コマンド・リソースに対して Execute アクションを実行しようとしているので、ポリシー 1 によりアクセス権が付与されます。

リソース・レベルの検査:

1. Update Document コマンドは、文書リソースを保護するよう指定します。エミリーの文書はセラーによって所有されています。セラー組織はどのポリシー・グループにも加入していないので、アクセス制御フレームワークは、組織階層の検索を開始し、少なくとも 1 つのポリシー・グループに加入している組織を検出しようとします。組織階層をさらに上っていくと、ルート組織に行き当たります。この組織はポリシー・グループに加入しているため、そのポリシー・グループ内のポリシー、つまりポリシー 1、2、5 を適用できます。
2. グループ化が可能なテンプレート・ポリシー 5 は、そのリソースを所有する組織、つまりセラー組織に適用されます。パラメーター化アクセス・グループ、つまり組織の承認者は、現在のリソース・コンテキストに有効範囲を動的に絞り込み、ユーザーがそのリソースを所有している組織、またはその先祖に当たる組織のアクセス・グループ条件を満たしているかどうかを検査します。この場合、エイブは部門 A 組織単位 (セラー組織の子孫) の承認者なので、そのアクセス・グループ条件を満たしていません。

エイブはコマンド・レベル検査に合格しましたが、リソース・レベルのアクセス制御検査に失格したので、エミリーの文書を更新できません。

ポリシーの詳細

これまで、アクセス制御ポリシーの基本構造とポリシーのタイプを理解してきたので、次に一連のさまざまな例を使って、デフォルト・ポリシーの 1 つを詳しく調べます。これから調べるのは、次のポリシーです。

```
AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
```

注: このポリシーはリソース・レベルのポリシーです。このポリシー・タイプは、グループ化が可能なテンプレートです。

最初の例では、WebSphere Commerce 組織管理コンソールを使用したポリシーの読み取り、その各部分の識別、およびポリシーの意味の理解について学びます。 2 番目の例では、ポリシーを XML 形式で見て、同じ情報がコードではどのように表示されるかを理解します。

さらに 3 番目の例は、あるポリシーが他のポリシーとどのように関連するかを理解するステップです。ポリシー間の依存関係を理解することは、アクセス制御ポリシーに変更を加えたり、新しいアクセス制御ポリシーを作成するにあたり、重要な前提条件です。

例 1: ポリシーの読み取り

この例では、WebSphere Commerce 組織管理コンソールを使ってポリシーを調べ、ポリシーを定義する部分を識別します。また、これらの部分を使って、ポリシーの一般的な記述を形成します。

組織管理コンソールでポリシーを調べる

1. WebSphere Commerce 組織管理コンソールにログインします。「アクセス管理」メニューから、**「ポリシー」**を選択します。
2. ルート組織が大半のデフォルトのアクセス制御ポリシーを所有しているので、「ルート組織」をリスト・ボックスから選択します。
3. 「ポリシー」ページで、ポリシーのリスト全体をスクロールし、次のポリシーを探します。

   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

   ポリシーのリストは、スクロール・バーを使っても、**「最初 (First)」**、**「前へ」**、**「次へ」** および **「最終 (Last)」** リンクを使ってもスクロールできることに注目してください。

ポリシーの部分の表示

1. ポリシーの隣のボックスをクリックしてそのポリシーを選択し、**「アクション・グループの表示 (Show Action Group)」**をクリックします。
2. 「アクション・グループ (Action Group)」ページに、アクション・グループ AuctionManage が表示されます。これが、ポリシーと関連したアクション・グループです。 AuctionManage を選択し、**「アクションの表示 (Show Actions)」**をクリックします。
3. 次のページで、AuctionManage アクション・グループに、アクションつまりコマンドの次のリストが表示されます。
   - com.ibm.commerce.negotiation.commands.CloseBiddingCmd
   - com.ibm.commerce.negotiation.commands.DeleteAuctionCmd
   - com.ibm.commerce.negotiation.commands.ModifyAuctionCmd

   ここで、AuctionManage にはオークションの終了 (CloseBiddingCmd)、オークションの削除 (DeleteAuctionCmd)、およびオークションの変更 (ModifyAuctionCmd) が含まれています。コマンドに関する詳細については、オンライン・ヘルプ文書の関連セクションを参照してください。

   また、「ポリシー」ページから**「アクションの表示 (Show Actions)」**をクリックすることによって、同じアクションのリストにアクセスできることにも注目してください。
4. 「ポリシー」ページに戻るには、いずれかのアクションを選択し、**「ポリシーの表示 (Show Policies)」**をクリックします。
5. ポリシーを再度選択しますが、ここでは**「メンバー・グループの表示 (Show Member Group)」**をクリックして、このポリシーで使用されるメンバー (アクセス) グループを表示します。
6. メンバー (アクセス) グループ名に注目します。この場合、メンバー (アクセス) グループは AuctionAdministratorsForOrg です。
7. 「アクセス管理」メニューから、**「アクセス・グループ」**を選択します。

8. AuctionAdministratorsForOrg を見つけます。見つけたらクリックし、**「変更」**をクリックします。
9. **「基準」**をクリックします。「基準」ページで、選択済みの役割と組織の下を調べます。次の役割が表示されているはずです。
   - Seller-For organization
   - Product Manager-For organization
   - Buyer (sell-side)-For organization
   - Category Manager-For organization

   オークション・リソースを所有する組織に関するこれらの役割の 1 つに割り当てられるユーザーは AuctionAdministratorsForOrg アクセス・グループに属します。
10. 何も変更を加えずに「基準」ページから移動します。「アクセス管理」メニューから、再び**「ポリシー」**を選択します。以下のポリシーを見つけます。

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
11. ポリシーを選択し、**「リソースの表示 (Show Resources)」**をクリックします。「リソース (Resources)」ページに、com.ibm.commerce.negotiation.objects.Auction リソースが表示されます。これは、アクション・グループにリストされるアクションが作動するリソースです。この場合、リソースはオークション (Auction) です。「ポリシー」ページから**「リソース・グループの表示 (Show Resource Group)」**をクリックして、個々のリソースにドリルダウンすることによって、この同じリストにアクセスできることに注目してください。
12. ここで、「アクセス管理」メニューから**「ポリシー」**を選択し、以下のポリシーを見つけます。

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
13. ポリシーを選択し、**「変更」**をクリックします。「ポリシーの変更 (Change Policy)」ページで、**「関係」**の下のドロップダウン・メニューを調べます。関係が何に対しても設定されていないことに注目してください。これは、ポリシーに関係が設定されていないということです。
14. ダイアログ・ボックスで、**「キャンセル」**および**「OK」**をクリックします。

ポリシーの意味の理解

ここまでで、このポリシーの個々の部分を識別したので、ポリシーが何を実行するか理解するために、それらの部分をまとめて考慮することにします。まず、ポリシーが、AuctionAdministratorsForOrg グループに所属するすべてのユーザーに適用されるということが分かっています。これは、**「メンバー・グループの表示 (Show Member Group)」**をクリックすることによって分かりました。そこから、「アクセス管理」メニューを使って「アクセス・グループ」ページに移動し、アクセス・グループには次の役割、つまり**セラー**、**商品管理者**、**バイヤー (販売サイド)**、および**カテゴリー管理者**があることを確認しました。まとめて、これら 4 つの役割のいずれかを持つユーザーは、オークション管理者と呼ばれることがあります。

また、アクション・グループにはオークションの変更、撤回、クローズが含まれること、リソース・グループには管理されるオークション・リソースだけが含まれることも理解しました。これも、「ポリシー」ページから**「アクションの表示 (Show**

Actions)」および**「リソースの表示 (Show Resources)」**をクリックして、詳細レベルまで降りることによって分かります。最後に、そのポリシーに、アクセス・グループとリソース間の関係が含まれないことも理解しました。

これらすべてを総合すると、このポリシーによって、オークションを所有する組織に関する役割を果たしている場合にオークション管理者は、オークションの変更、撤回およびクローズなど、オークション・リソース上のオークションの管理に関連したすべてのアクティビティーを実行できるという結論に達します。

ポリシーの名前を見れば、それば何を意味するか予想することができます。この例では、ポリシーは、ユーザーの指定されたグループの名前、 AuctionAdministratorForOrg で始まります。 ForOrg という表記は、これがグループ化が可能なテンプレート・ポリシーであることを示しています。AuctionManageCommands はアクション・グループの説明で、 AuctionResource はリソース・グループの説明です。

例 2: XML 形式でポリシーを読み取る

デフォルトのアクセス制御ポリシーは、インスタンスの作成時にデータベースにロードされた XML ファイルに保管されています。 WebSphere Commerce 管理コンソールでポリシーを表示する場合、データベースに保管された情報を表示および変更するためのインターフェースを使用します。データベース内の情報は、 Policy Manager でアクセス制御を評価するのに使用されます。データベースの情報が XML ファイルより新しい場合は、Extractor ツールを使用して、アクセス制御ポリシーの情報をデータベースから XML ファイル内に抽出できます。

これは XML ファイル内でのポリシーの外観を示しています。

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="groupable Template">
</Policy>
```

ここで、ポリシーは次のように定義されます。

Name: ポリシーの名前。

OwnerID: ポリシーが適用される組織。

UserGroup: アクセス・グループ。

ActionGroupName: アクション・グループ。

ResourceGroupName: リソース・グループ。

PolicyType: ポリシーのタイプ。グループ化が可能な標準や、グループ化が可能なテンプレートなど。

デフォルトのアクセス制御ポリシーすべてを含むファイルの名前は、defaultAccessControlPolicies.xml で、以下のディレクトリーにあります。

X:¥*installation_directory*¥xml¥policies¥xml

注: デフォルトの各アクセス制御ファイルの記述は、同じディレクトリーにある defaultAccessControlPolicies_*locale*.xml ファイルにあります。デフォルトのアクセス制御ファイル内にある、デフォルトのアクセス制御ポリシーに変更を加える場合、 defaultAccessControlPolicies_en_US.xml の対応する記述を更新する必要があります。 XML ファイルに加える変更は、高度なユーザーだけが行うよう強くお勧めします。

例 3: 自分のポリシーと関連した他のポリシーを識別する

この最後の例では、アクセス制御ポリシーが、他のポリシーにどのように依存するかを調べます。

ユーザーのグループ (アクセス・グループ) がリソースに対して実行できるコマンド (アクション) を定義するポリシーは、リソース・レベル・ポリシーと呼ばれます。たとえば、今まで詳細を見てきたポリシー

AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource は、リソース・レベル・ポリシーの一例です。

しかし、リソース・レベル・ポリシーに許可されるアクションも、ポリシーのアクセス・グループに所属する各役割ごとに許可されるアクションに依存しています。特定の役割に許可されるアクションを説明するポリシーを、役割ベースのポリシーと呼びます。

リソース・レベル・ポリシーに関連した役割ベースのポリシーを識別するには、次のようにします。

ポリシーに関連した役割を調べる

1. WebSphere Commerce 管理コンソールにログインし、「ポリシー」ページでリソース・レベル・ポリシーを探します。同じ例を使っているので、今探しているポリシーが、以下のポリシーであることが分かります。

   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
2. ポリシーに関連したアクセス・グループを識別します。この場合、アクセス・グループが AuctionAdministratorsForOrg であることはすでに分かっています。
3. アクセス・グループに関連した役割を調べます。 AuctionAdministratorsForOrg の場合、前の例から、役割がバイヤー (販売サイド)、カテゴリー管理者、商品管理者、およびセラーであることが分かっています。

各役割ごとの役割ベースのポリシーを調べる

1. このマニュアルの最後にある付録を開き、「役割ベースのポリシー」という見出しのセクションを見つけてください。この付録は、役割に関連した各役割ベースのポリシーを見つけるのに使用します。

2. Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup ポリシーを見つけます。このポリシーは、**バイヤー (販売サイド)** 役割に関連しています。これは、ポリシーの接頭部が Buyers(sell-side) であることから分かります。
3. 接頭部を見て正しいポリシーを識別し、 **バイヤー (販売サイド)**、**カテゴリー管理者**、**商品管理者**、および**セラー**役割に関連する役割ベースのポリシーの残りを見つけます。次のリストが表示されるはずです。
   - Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
   - Buyers(sell-side)ExecuteBuyers(sell-side)Views
   - CategoryManagersExecuteCategoryManagersCmdResourceGroup
   - CategoryManagersExecuteCategoryManagersViews
   - ProductManagersExecuteProductManagersCmdResourceGroup
   - ProductManagersExecuteProductManagersViews
   - SellersExecuteSellersCmdResourceGroup
   - SellersExecuteSellersViews
4. 各役割ベースのポリシーは、その役割を持つユーザーに、特定のコントローラー・コマンドやビューを実行する許可を与えます。役割ベースのポリシーに関連するアクションを理解するには、例 1 と同じ手順を使って WebSphere Commerce 組織管理コンソールから「ポリシー」ページのポリシーを調べます。

ポリシー間の依存関係の識別が重要である理由

リソース・レベル・ポリシーに関連する役割ベースのポリシーを理解することは、大抵の場合、ポリシーのカスタマイズ、および新しいポリシーの作成の前提条件です。

99 ページの『第 3 部 セキュリティー許可の管理』では、リソース・レベルと役割ベースのポリシーについて、その認識方法、それらの違いの理解、および相互の関連などをより詳しく調べます。

第 2 部 セキュリティー認証の管理

第 2 部では、WebSphere Commerce サイト管理者が通常実行できるセキュリティー認証タスクについて説明します。

第 4 章 サイト・セキュリティーの機能強化

以下の WebSphere Commerce 構成マネージャーのフィーチャーのいずれかを使用可能にして、WebSphere Commerce サイトのセキュリティーを強化することができます。

- 「ログイン・タイムアウト」ノードを使って、一定期間を超えて非アクティブになっているユーザーをログオフさせ、システムに再度ログオンするよう要求します。詳細は、 59 ページの『ログイン・タイムアウトの使用可能化』を参照してください。
- 「パスワード無効化」ノードを使ってユーザーが初めてシステムにログインしたときに、各自のパスワードを変更することを義務付けます。詳細は、 60 ページの『パスワード無効化の活動化』を参照してください。
- 「パスワード保護されたコマンド」ノードを使って、指定コマンドを実行する要求を実行する場合はパスワードを入力することをユーザーに義務付けます。詳細は、 61 ページの『パスワード保護されたコマンドの使用可能化』を参照してください。
- 構成マネージャーの「データベース更新ツール」ノードを使って、パスワードやクレジット・カードの情報などの暗号化データならびに WebSphere Commerce データベース内のマーチャント鍵を更新します。詳細は、 62 ページの『暗号化データの更新』を参照してください。
- 「サイト間スクリプト保護」ノードを使って、不許可と指定された属性や文字を使用しているユーザー要求を拒否します。詳細は、 63 ページの『サイト間スクリプト保護の使用可能化』を参照してください。
- アクセス・ロギングの使用可能化によって、WebSphere Commerce に対するセキュリティー上の脅威をすべて早急に特定します。詳細は、 65 ページの『アクセス・ロギングの使用可能化』を参照してください。

それ以外に、WebSphere Commerce の管理コンソールの「セキュリティー」ドロップダウンから、次のようなフィーチャーを使用可能にすることができます。

- 「アカウント・ポリシー」ページを使って、使用中のアカウント関連のポリシーを定義するためのサイト用のアカウント・ポリシーをセットアップします。詳細は、 67 ページの『アカウント・ポリシーのセットアップ』を参照してください。
- 「パスワード・ポリシー」ページを使って、ユーザーのパスワード選択特性を制御するためのサイト用のパスワード・ポリシーをセットアップします (ユーザーが WebSphere Commerce データベースに対する認証を受けている場合のみ)。詳細は、 68 ページの『パスワード・ポリシーのセットアップ』を参照してください。
- 「アカウント・ロックアウト・ポリシー」ページを使って、ユーザー・アカウントに不祥事が起きる可能性を減少するためにサイト用のアカウント・ロックアウト・ポリシーをセットアップします (ユーザーが WebSphere Commerce データベースに対する認証を受けている場合のみ)。詳細は、 69 ページの『アカウント・ロックアウト・ポリシーのセットアップ』を参照してください。

- 「セキュリティー検査の立ち上げ」ページを使って、機密漏れの可能性があると思われる一時 WebSphere Commerce ファイルの検査と削除を行うためのセキュリティー・プログラムを立ち上げます。詳細は、70 ページの『セキュリティー検査の立ち上げ』を参照してください。

関連概念の詳細は、以下の WebSphere Commerce オンライン・ヘルプの中のトピックを参照してください。

- 構成マネージャー
- WebSphere Commerce 構成ファイル
- 管理コンソール
- セキュリティー

関連タスクの詳細は、以下の WebSphere Commerce オンライン・ヘルプの中のトピックを参照してください。

- 構成マネージャーの立ち上げ
- 管理コンソールのオープン

Internet Information Services (IIS) Web サーバーのセキュリティー考慮事項

注意

WebSphere Commerce で IIS Web サーバーを使用している場合、以下のセキュリティー考慮事項に留意し、推奨アクションを実行して、WebSphere Commerce データの機密漏れを最小限にする必要があります。

問題: IIS Web サーバーの場合、 仮想ディレクトリーに対する読み取り許可によって、 JSP ファイルのソース・コードに対するアクセスが提供されます。 JSP ソース・コードのダウンロードを避けるために、 IIS Web サーバーを使用する場合は、Web ページの静的内容を動的内容から物理的に分離する必要があります。この理由は、IIS セキュリティーが、ファイル・タイプよりもディレクトリーの位置に基づくものであるからです。デフォルトの IIS 構成の下では、イメージ・ファイルおよび JSP ファイルは、単一の別名の下に置かれます。デフォルトの構成はテスト目的にのみ使用すべきです。

ソリューション: すべての Web 資産を保護するには、*動的コンテンツには、実行専用 (読み取りはなし) 許可で、必ず仮想ディレクトリーを使用してアクセスし、静的コンテンツは、読み取り専用許可で別の仮想ディレクトリーに移動させる必要があります。*仮想ディレクトリーに許可を設定する詳細な方法については、IIS ヘルプ情報の手順を参照してください。 Microsoft® Corporation のセキュリティー・パッチおよび構成ポリシーに関する現行の資料を参照することもお勧めします。

セキュリティー用のビュー

WebSphere Commerce のいずれかのセキュリティー・フィーチャーを使用したい場合に、そのフィーチャーを使用可能にするには、ストア関連のビューを事前に定義する必要があります。この後の項では、次のような機能用にビューを定義する方法を説明しています。

- ログイン・タイムアウト (『ログイン・タイムアウト』を参照)
- パスワード無効化 (58 ページの『パスワード無効化』を参照)
- パスワード保護されたコマンド (58 ページの『パスワード保護されたコマンド』を参照)
- サイト間スクリプト保護 (59 ページの『サイト間スクリプト保護』を参照)

ビューの作成とストアフロントの開発に関する一般情報は、「*WebSphere Commerce ストア開発ガイド*」を参照してください。

ログイン・タイムアウト

ログイン・タイムアウトのセキュリティー・フィーチャーを使用するには、ストアに関して LoginTimeoutErrorView と ReLogonFormView ビューを定義する必要があります。

LoginTimeoutErrorView

ログイン・タイムアウト情報が誤っていると、WebSphere Commerce はこのビューをユーザーにリダイレクトします。ビューがリダイレクトされた場合、その原因は誰かが cookie を悪用したためと考えられます。

表 2. LoginTimeoutErrorView の属性

ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE	**1** 有効期限が誤った値に設定されています。 **2** ログオン時刻が誤った値に設定されています。 **3** 有効期限またはログオン時刻が誤った値に設定されています。

ReLogonFormView

このビューは、セッションの期限が切れた後でユーザーに対して表示されます。このビューでは、ユーザーのログオン ID とパスワードを入力するためのフォームが表示されなければなりません。送信ボタンを使うと、ログオン・コマンドが起動されます。また、たいていはストアフロント・ページなどの別のページにユーザーをリダイレクトするための「取り消し」ボタンもなければなりません。

ReLogonFormView には属性はありません。

表 3. ReLogonFormView フォームの属性

ECUserConstants.EC_UREG_LOGONID	ユーザーのログオン ID。
ECUserConstants.EC_UREG_LOGONPASSWORD	ユーザーのログオン・パスワード。
ECUserConstants.EC_RELOGIN_URL	入力した認証情報が無効の場合に表示される URL。たいていの場合、それはこのビューの名前です。
ECConstants.EC_STORE_ID	ストア ID。
ECConstants.EC_URL	入力した認証情報が別のユーザーのものである場合に表示される URL。たいていの場合それはストアのホーム・ページであるか、またはログオン・ページで使用されているのと同じ URL です。

パスワード無効化

パスワード無効化のセキュリティー・フィーチャーを使用するには、ストアに関して ChangePassword ビューを定義する必要があります。

ChangePassword

このビューが表示されるのは、ユーザーのパスワードの期限が切れた場合です。このビューでは、現行 (期限の切れた) パスワードと新規パスワードを入力するためのフォームが表示されなければなりません。「送信」ボタンを使うと、ResetPassword コマンドが起動されます。また、たいていはストアフロント・ページなどの別のページにユーザーをリダイレクトするための「取り消し」ボタンもなければなりません。

表 4. ChangePassword の属性

ECConstants.EC_PASSWORD_EXPIRED_FLAG	**1** ユーザーのパスワードの有効期限は切れています。この属性が必要なのは、同じパスワード変更のフィーチャーとして使用するようなビューとこのビューを区別するためです。パスワード変更のビューは、ユーザーによって起動されますが、このビューに割り当てられる JSP はどちらの場合も同じでなければなりません。 JSP はこの属性を見つけ出して、何を表示すればよいかを決める必要があります。 **ヌル** 属性は URL 上にありません。これは、パスワード変更時の通常の動作です。
ECUserConstants.EC_UREG_LOGONID	現行ユーザーのログオン ID。
ECConstants.EC_LOGIN_RETURN_URL	パスワード変更が正常に完了した後でブラウザーがリダイレクトされる先の URL。この URL は、ECConstants.EC_URL という名前でアクション・コマンドに渡されます。

表 5. ChangePassword フォームの属性

ECUserConstants.EC_UREG_LOGONID	ユーザーのログオン ID。現在のログオン ID は、ビューに渡されています。
ECUserConstants.EC_UREG_LOGONPASSWORDOLD	旧パスワード。
ECUserConstants.EC_UREG_LOGONPASSWORD	新規パスワード。
ECUserConstants.EC_UREG_LOGONPASSWORDVERIFY	新規パスワードの検査。
ECConstants.EC_URL	パスワード変更の正常完了後にユーザーがリダイレクトされる先の URL。値は、ビューに渡されました。
ECUserConstants.EC_RELOGIN_URL	パスワード変更が失敗した場合にブラウザーがリダイレクトされる先の URL。

パスワード保護されたコマンド

パスワード保護されたコマンドのセキュリティー・フィーチャーを使用するには、ストア用の PasswordReEnterErrorView および PasswordReEnterFormView ビューを定義する必要があります。

PasswordReEnterErrorView

このビューは、以下のシナリオで使用されています。

- ユーザーが正しいパスワードを入力しなかった場合、ログオフします。
- 認証が失敗しました。

どちらの場合も、ユーザーは現行ページ上のリンクを使って別のページに進むための手段を講じる必要があります。

表 6. PasswordReEnterErrorView の属性

ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	**0** ユーザーを認証しようとしたときに問題が起きました。 **ヌル** 属性は URL 上にありません。ユーザーは、パスワードを入力しなかったのでログオフします。

PasswordReEnterFormView

このビューが表示されるのは、ユーザーがパスワード保護されたコマンドを実行しようとした場合です。パスワードを入力するためのフォームをユーザーに提示しなければなりません。パスワード用の入力フィールドが 2 つなければなりません。

表 7. PasswordReEnterFormView の属性

ECConstants.EC_PASSWORD_REREQUEST_URL	URL は、このフォームの「送信」ボタンを使って実行されます。
ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	ユーザーに対して示されるメッセージを指定するメッセージ・コードは次のとおりです。 **1** 入力したパスワードは一致しません。 **2** パスワードが入力されていません。 **3** 誤ったパスワードを入力しました。

アクション: 以下を指定したパラメーターとして URL が渡されます。

表 8. PasswordReEnterFormView フォームの属性

ECConstants.EC_PASSWORD_REREQUEST_PASSWORD1	最初のパスワード。
ECConstants.EC_PASSWORD_REREQUEST_PASSWORD2	2 番目のパスワード。

サイト間スクリプト保護

サイト間スクリプトのセキュリティー・フィーチャーを使用するには、ストア用の ProhibitedAttrsErrorView、ProhibitedCharacterErrorView、および ProhibCharEncodingErrorView ビューを定義する必要があります。

ProhibitedAttrsErrorView

このビューがユーザーに対して示されるのは、禁止属性が要求内で使われているためにその要求を処理できないときです。

ProhibitedCharacterErrorView

このビューがユーザーに対して示されるのは、禁止文字が要求内で使われているためにその要求を処理できないときです。

ProhibCharEncodingErrorView

これは、上記の ProhibitedCharacterErrorView と同じです。

ログイン・タイムアウトの使用可能化

注: ログイン・タイムアウトのセキュリティー・フィーチャーをストアで使用するには、 57 ページの『ログイン・タイムアウト』に説明されているとおりに、ストア用の LoginTimeoutErrorView と ReLogonFormView ビューを定義する必要があります。

ログイン・タイムアウト・フィーチャーを使用可能または使用不可にするには、構成マネージャーの「ログイン・タイムアウト」ノードを使用します。このフィーチャーを使用可能にすると、一定期間を超えて非アクティブになっている WebSphere Commerce ユーザーは、システムからログオフされ、ログオンし直すように要求さ

れます。その後ユーザーが正常にログオンすると、 WebSphere Commerce は、そのユーザーが出していた元の要求を実行します。ユーザーのログオンが失敗した場合は、元の要求は廃棄され、そのユーザーはシステムからログオフされたままになります。

WebSphere Commerce ツール (管理コンソール、WebSphere Commerce アクセラレーターなど) の場合、ログイン・タイムアウトではユーザーに対して再ログイン・ページは表示されないことに注意してください。そのような場合、ブラウザー・ウィンドウはクローズされ、ツールに再ログオンするかどうかはユーザーにゆだねられます。したがって、ツールの場合は、ユーザーが送信していた元の要求は処理されません。

このフィーチャーを使用可能にするには、以下のようにします。

1. 構成マネージャーを立ち上げて、次のようにして該当するインスタンスの「ログイン・タイムアウト」ノードまでたどっていきます。**「WebSphere Commerce」>「***host_name***」>「インスタンス・リスト (Instance List)」>「***instance_name***」>「インスタンス・プロパティー」>「ログイン・タイムアウト」**となります。
2. ログイン・タイムアウト・フィーチャーをアクティブにするには、**「使用可能」**チェック・ボックスをクリックします。
3. 「値」フィールドに、ログイン・タイムアウト値を秒単位で入力します。
4. 変更内容を構成マネージャーに適用するには、**「適用」**をクリックします。
5. インスタンスの構成が正常に更新されると、更新が正常に行われたことを示すメッセージが表示されます。
6. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

ログイン・タイムアウトの値は *instance*.xml ファイルにミリ秒数で保管されるのに対して、構成マネージャーには秒数で入ることに注意してください。

パスワード無効化の活動化

注: パスワード無効化のセキュリティー・フィーチャーを使用するには、 58 ページの『パスワード無効化』に説明されているとおりに、ストア用の ChangePassword ビューを定義する必要があります。

パスワード無効化フィーチャーを使用可能または使用不可にするには、構成マネージャーの「パスワード無効化」ノードを使用します。パスワード無効化を使用可能にした場合に WebSphere Commerce ユーザーのパスワードの有効期限が切れると、そのユーザーはパスワードの変更を要求されます。その場合、ユーザーは、パスワードを要求するページにリダイレクトされます。ユーザーは、パスワードの変更を完了するまで、そのサイトのどのセキュア・ページにもアクセスすることができません。このフィーチャーを使用可能にするには、以下のようにします。

1. 構成マネージャーを立ち上げて、次のようにして該当するインスタンスの「パスワード無効化」ノードまでたどっていきます。**「WebSphere**

Commerce」>「*host_name***」>「インスタンス・リスト (Instance List)」>「***instance_name***」>「インスタンス・プロパティー」>「パスワード無効化」**となります。

2. パスワード無効化フィーチャーをアクティブにするには、**「使用可能」**チェック・ボックスをクリックします。
3. 変更内容を構成マネージャーに適用するには、**「適用」**をクリックします。
4. インスタンスの構成が正常に更新されると、更新が正常に行われたことを示すメッセージが表示されます。
5. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

パスワード保護されたコマンドの使用可能化

注: パスワード保護されたコマンドのセキュリティー・フィーチャーを使用するには、 58 ページの『パスワード保護されたコマンド』に説明されているとおりに、ストア用の PasswordReEnterErrorView および PasswordReEnterFormView ビューを定義する必要があります。

「パスワード保護されたコマンド」フィーチャーを使用可能または使用不可にするには、「構成マネージャー」の「パスワード保護されたコマンド」ノードを使用します。このフィーチャーを使用可能にすると、WebSphere Commerce は、WebSphere Commerce にログオンした登録済みユーザーに、まずパスワードを入力してから、指定した WebSphere Commerce コマンドの実行要求を続行するよう求めます。

注意: パスワード保護されたコマンドを構成する場合、コマンド選択リストに示されているコマンドの中には、一般ユーザーまたはゲスト・ユーザーが実行できるコマンドもあることに注意してください。そのようなコマンドを、パスワードで保護して構成すると、一般ユーザーおよびゲスト・ユーザーはそのコマンドを実行できなくなります。したがって、コマンドを構成してパスワードで保護する場合は注意を払う必要があります。

このフィーチャーを使用可能にするには、以下のようにします。

1. 構成マネージャーを立ち上げて、次のようにして該当するインスタンスの「パスワード保護されたコマンド」ノードまでたどっていきます。**「WebSphere Commerce」>「***host_name***」>「インスタンス・リスト (Instance List)」>「***instance_name***」>「インスタンス・プロパティー」>「パスワード保護されたコマンド」**となります。
2. 「一般」タブで、以下のようにします。
   a. 「パスワード保護されたコマンド」フィーチャーをアクティブにするには、**「使用可能」**をクリックします。
   b. 「再試行」フィールドに再試行の回数を入力します。 (デフォルトの再試行回数は 3 です。)
3. 「拡張」タブで、以下のようにします。
   a. 保護したい WebSphere Commerce コマンドを「パスワード保護されたコマンドのリスト (Password Protected Command List)」ウィンドウのリストから選

択して、**「追加」**をクリックします。選択したコマンドが「現行のパスワード保護されたコマンドのリスト (Current Password Protected List)」ウィンドウにリストされます。

b. いずれかの WebSphere Commerce コマンドのパスワード保護を使用不可にしたい場合は、「現行のパスワード保護されたコマンドのリスト (Current Password Protected Command list)」ウィンドウにあるコマンドを選択して、**「除去」**をクリックします。

4. 変更内容を構成マネージャーに適用するには、**「適用」**をクリックします。
5. インスタンスの構成が正常に更新されると、更新が正常に行われたことを示すメッセージが表示されます。
6. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

注: WebSphere Commerce では、**認証済み (authenticated)** と指定されているコマンドか、または URLREG 表で https フラグが設定されているコマンドのみが使用可能コマンド・リストに表示されます。

暗号化データの更新

構成マネージャーのデータベース・ノードからデータベース更新ツールを使って、特定インスタンスの 1 つ以上の WebSphere Commerce データベースのマーチャント鍵を変更し、すべての暗号化データ (パスワードやクレジット・カード番号など) を更新することができます。このツールを使用するには、次のようにします。

1. 構成マネージャーを立ち上げて、次のようにして個々のデータベース・エントリーまでたどっていきます。**「WebSphere Commerce」>「***host_name***」>「インスタンス・リスト (Instance List)」 >「***instance_name***」>「インスタンス・プロパティー」>「データベース」>「***database_name***」** を選びます。
2. *database_name* を右マウス・ボタンでクリックし、**「データベース更新ツールの実行」**を選択します。
   - すべてのデータベース用に選択したインスタンスの暗号化データをマイグレーションするには、**「このインスタンスの全データベースの更新」**を選択します。

     400 iSeries は単一データベース構成をサポートするので、このオプションは iSeries には該当しません。
   - ドロップダウン・リストでデータベースを選択して個々のデータベースごとに暗号化データをマイグレーションするには、**「選択したデータベースの更新」**を選択します (デフォルト)。
3. 実行したいアクションを「アクション・アイテム」ボックスで選択し、次のような必要な情報を「パラメーター」フィールドに入力します。

アクション	パラメーター	必要なアクション

マーチャント鍵の変更	古いマーチャント鍵	現在の WebSphere Commerce インスタンスの作成時に使った既存のマーチャント鍵を入力します。
	新しいマーチャント鍵	新しいマーチャント鍵を入力します。これは、構成マネージャーが現在暗号化されているデータを再暗号化するための 16 桁の 16 進数です。マーチャント鍵には 1 つ以上の英数字 (a ～ f) と 1 つ以上の数字 (0 ～ 9) がなければなりません。英数字は小文字で入力しなければならず、 1 行に 5 回以上同じ文字を入力することはできません。

4. **「OK」**をクリックして、選択した WebSphere Commerce データベースだけ、またはすべての WebSphere Commerce データベース用にデータベース更新ツールを実行します。
5. インスタンスの構成が正常に更新されると、更新が正常に行われたことを示すメッセージが表示されます。
6. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

サイト間スクリプト保護の使用可能化

注: サイト間スクリプトのセキュリティー・フィーチャーをストアで使用するには、 59 ページの『サイト間スクリプト保護』に説明されているとおりに、ストア用に `ProhibitedAttrsErrorView`、 `ProhibitedCharacterErrorView`、および `ProhibCharEncodingErrorView` ビューを定義する必要があります。

インスタンスのサイト間スクリプト保護機能を使用可能または使用不可にするには、「構成マネージャー」の「サイト間スクリプト保護」ノードを使用します。サイト間スクリプト保護を使用可能にすると、許可不能と指定されている属性またはストリングを使っているユーザー要求はすべて拒否されます。構成マネージャーのこのノードで、許可しない属性とストリングを指定することができます。また、サイト間スクリプト保護からコマンドを除外することもできます。それには、該当するコマンドに指定される属性の値の中で禁止ストリングを使用できるようにします。サイト間スクリプト保護は、デフォルトでは使用不可になっています。

警告: サイト間スクリプト保護フィーチャーは、構成に基づいてコマンドの実行を制限するという点で制約的なフィーチャーです。このフィーチャーは、どの属性またはストリングが禁止と定義されているかを検査しないので、その構成時には、禁止属性がコマンドで使われる属性でないことを確認してください。また、禁止ストリングが、いつもコマンドに渡される値でないことも確認してください。このフィーチャーを構成するときは、特別な注意が必要です。

このフィーチャーを使用可能にするには、以下のようにします。

1. 構成マネージャーを立ち上げて、次のようにして該当するインスタンスの「サイト間スクリプト保護」ノードまでたどっていきます。**「WebSphere**

Commerce」>「*host_name***」>「インスタンス・リスト (Instance List)」>「***instance_name***」>「インスタンス・プロパティー」 >「サイト間スクリプト保護」**を選びます。

2. サイト間スクリプト保護フィーチャーをアクティブにするには、次のように「一般」タブを使用します。
   a. **「使用可能」**をクリックします。
   b. WebSphere Commerce コマンドでの使用を許可しない属性を追加するには、「禁止属性」テーブルをマウスの右ボタンでクリックして、**「行の追加」**を選択します。使用を禁止したい属性を入力します。 1 行に 1 つの属性しか指定できません。
   c. 「禁止属性」テーブルから属性を除去するには、テーブル内でその属性が示されている行を強調表示してから、マウスの右ボタンでクリックして**「行の削除」**を選択します。
   d. WebSphere Commerce コマンドでの使用を許可しないストリングを追加するには、「禁止文字」テーブルをマウスの右ボタンでクリックしてから、**「行の追加」**を選択します。使用を禁止したいストリングを追加します。 1 行に 1 つのストリングしか指定できません。
   e. 「禁止文字」テーブルから文字を除去するには、テーブル内でその文字が示されている行を強調表示してから、マウスの右ボタンでクリックして**「行の削除」**を選択します。

   注: 以下のストリングは、デフォルトで「禁止文字」フィールドに指定されています。これらのストリングは、サイト・スクリプト記述に対して危害を加えようとする攻撃でのタグのスクリプト記述として最も多く使われます。
   - `<SCRIPT`
   - `<SCRIPT`
   - `<%` および `<%`
3. 「拡張」タブを使って、サイト間スクリプト保護から除外したい WebSphere Commerce コマンドを指定することができます。そのためには、次のようにして、該当するコマンドの指定の属性値の中で禁止ストリングを使用できるようにします。
   a. 「コマンド・リスト」ボックスからコマンドを選択します。
   b. 「例外属性のリスト」ウィンドウに、禁止文字を許可する属性をコンマで区切ったリストを入力します。**「追加」**をクリックします。
   c. その属性を持つコマンドを除去するには、「例外コマンドのリスト」ウィンドウからそのコマンドを選択して、**「除去」**をクリックします。

   属性を選択して**「除去」**をクリックして、コマンドから特定の属性を除去することもできます。
4. 変更内容を構成マネージャーに適用するには、**「適用」**をクリックします。
5. インスタンスの構成が正常に更新されると、更新が正常に行われたことを示すメッセージが表示されます。
6. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

注:

1. サイト間スクリプト保護からコマンドを除外すると、指定した属性の値は、HTML エンコード方式の記号でエンコードされます。たとえば、cmd1?user=<Thomas> というコマンドは、ascmd1?user=<Thomas> とエンコードされます。
2. 「禁止文字」フィールドにストリングを指定する場合、以下の点に注意してください。
   - 文字をある特定の並びにすると、 URL エンコード標準に準じてストリングが 1 つの文字に変換される可能性があります。たとえば、ストリング <%bb はストリング <*X* に変換されます。つまり *X* は、 16 進数 'bb' (10 進数の 187) という 16 進数で表される単一文字です。この場合、ストリング <%bb は、URL で渡されると、サイト間スクリプト保護ではキャッチされません。
   - 特定の並びになった文字の場合に、 URL エンコード標準に準じていないと、ストリングの変換が失敗する可能性があります。たとえば、ストリング <%gg は変換が失敗する原因になるかもしれません。16 進の 'gg' は、有効な 16 進値表現ではないからです。この場合、ストリング <%gg は例外の原因になるので、サイト間スクリプト保護が使用可能になっていてもいなくても、このストリングを使用する URL 要求に対しては応答が行われません。

例: 以下の例について考えてみます。

- 禁止ストリング: <SCRIPT, <%

  禁止属性: mycomment, description

コマンド	状況
cmd1?description=Available...	拒否
cmd2?userid=Thomas...	受諾
cmd3?mycomment=<SCRIPT>...	拒否
cmd4?password=<%...%>...	拒否

- cmd1 コマンドの属性 text 内で禁止ストリング (<SCRIPT, <%) の使用を許可し、たとえば属性 txt などの他の属性の場合は許可しないようにするには、 cmd1 を除外し、例外属性として text を指定します。

コマンド	状況
cmd1?text=<SCRIPT>...	受諾
cmd1?text=<%...%>...	受諾
cmd1?txt=<SCRIPT>...	拒否
cmd1?txt=<%..%>...	拒否

アクセス・ロギングの使用可能化

アクセス・ロギング・フィーチャーを使用可能にすることにより、 WebSphere Commerce サーバーへの着信要求がすべて記録されるか、あるいはアクセス違反を起こした要求だけが記録されます。アクセス違反の例としては、認証失敗、コマンド実行に不十分な権限、あるいはサイトのパスワード規則に違反するパスワードの

リセットがあります。アクセス・ロギングを使用可能にすると、WebSphere Commerce 管理者は WebSphere Commerce システムに対するセキュリティー上の脅威を速やかに確認できます。

認証障害や許可障害のイベントが発生すると、次のような情報がアクセス・ログ・ファイル・データベース表 ACCLOGMAIN および ACCLOGSUB にログ記録されます。

- クライアントのホスト名
- コマンドを実行するスレッドの ID
- クライアントのユーザー ID
- イベントが発生した時刻
- 実行されたコマンド
- コマンドの実行対象であったストア
- オペレーションが実行されたリソース
- アクセス制御検査の結果

アクセス・ロギングを使用可能にするには、次のようにします。

1. 構成マネージャーを立ち上げます。
2. **「ホスト名」**>**「インスタンス」** > **「Instance_List」**を選択してから、**「コンポーネント」**フォルダーをオープンします。
3. **AccessLoggingEventListener** を選択します。
4. 「一般」パネルで**「コンポーネント使用可能」**チェック・ボックスをアクティブにします。
5. 「拡張」パネルを選択し、**「開始」**を使用可能にします。
6. **「適用」**をクリックします。
7. 構成マネージャーを終了します。
8. WebSphere Application Server を再始動します。

ログ・ファイルのサイズを変更したり、すべての要求をログ記録するかどうかを指定したりするには、次のようにして、 WebSphere Commerce インスタンス・サブディレクトリーに置かれている WebSphere Commerce インスタンスの *instance*.xml ファイルを手動で編集する必要があります。

1. インスタンスの *instance*.xml ファイルをエディターでオープンします。
2. <LogSystem>/<activitylog> ノードに置かれている次のようなノードを見つけ出します。

   ```
   <accessLogging cacheSize="aa" logAllRequests="bbbbb" />
   ```

   ここで、

   - *aa* は、データベースへのエントリーの書き込みの前にメモリーにログ記録されるエントリーの最大数を指定する整数値です。一般的に、この数値が大きいほど、アクセス・ロギングに関するパフォーマンスは向上します。デフォルト値は 32 です。
   - *bbbbb* は true または false です。 true の値は、すべての着信要求をログ記録することを意味します。 false の値は、アクセス違反のみをログ記録することを意味します。過多または不要なログ記録を行わないようにするには、

false をお勧めします。 true を使用するのは、サイトにおいて認証上の問題やセキュリティー違反の恐れがある場合のみです。デフォルト値は false です。

3. 更新が完了したら、WebSphere Commerce インスタンスの *instance*.xml ファイルを保管します。
4. WebSphere Application Server を再始動します。

以下に示す例ではアクセス・ロギングを使って、データベース表へのエントリーのログ記録の前に、 3 つのエントリーをメモリー内に保存します。さらに、すべての着信要求を WebSphere Commerce サーバーにログ記録します。

```
<accessLogging cacheSize="3" logAllRequests="true" />
```

アカウント・ポリシーのセットアップ

WebSphere Commerce 管理コンソールの「アカウント・ポリシー」ページで、アカウント・ポリシーをセットアップすることができます。このページには、既存のアカウント・ポリシーがすべてリストされます。その中には、デフォルトで WebSphere Commerce に付属している、事前定義されたあらゆるアカウント・ポリシーも含まれます。アカウント・ポリシーは、パスワード・ポリシーやアカウント・ロックアウト・ポリシーなどのアカウントに関連するポリシーを定義します。このページでは以下を行うことができます。

- **「新規」**をクリックすれば、新しいアカウント・ポリシーを作成することができます。
- リストで既存のアカウント・ポリシーを選択してから**「変更」**をクリックすれば、そのポリシーを変更することができます。
- リストで既存のアカウント・ポリシーを選択してから**「削除」**をクリックすれば、そのポリシーを削除することができます。

新規アカウント・ポリシーを作成するには、次のようにします。

1. WebSphere Commerce 管理コンソールをオープンします。
2. 管理コンソールの「セキュリティー」ドロップダウン・メニューで**「アカウント・ポリシー」**をクリックします。
3. 「アカウント・ポリシー」ページで**「新規」**をクリックして、新しいアカウント・ポリシーを作成します。
4. アカウント・ポリシーの名前を「名前」フィールドに入力します (たとえば、my_account_policy など)。
5. 「パスワード・ポリシー」メニューで、既存のパスワード・ポリシーを選択します。
6. 「アカウント・ロックアウト・ポリシー」メニューで、既存の存在するアカウント・ロックアウト・ポリシーを選択します。
7. **「OK」**をクリックします。

アカウント・ポリシーを作成したら、ユーザーにそのポリシーを割り当てることができます。アカウント・ポリシーが使用中の (つまり、ユーザーにアカウント・ポリシーが割り当てられている) 場合は、そのポリシーを削除することはできません。

追加情報については、 71 ページの『デフォルト認証ポリシー』も参照してください。

パスワード・ポリシーのセットアップ

WebSphere Commerce 管理コンソールの「パスワード・ポリシー」ページでは、ユーザーのパスワード選択を制御して、サイトのセキュリティー・ポリシーが順守されるようにユーザーのパスワードの特性を定義することができます。このページには、既存のパスワード・ポリシーがすべてリストされます。その中には、デフォルトで WebSphere Commerce に付属している、事前定義されたあらゆるパスワード・ポリシーも含まれます。

パスワード・ポリシーは、パスワードが守らなければならない属性を定義します。パスワード・ポリシーで、以下の条件を決定します。

- ユーザー ID とパスワードが同じでよいか
- 連続する最大文字数
- 文字の最大インスタンス
- パスワードの最長存続期間
- 英字の最小文字数
- 数字の最小文字数
- パスワードの最低限の長さ
- ユーザーの以前のパスワードを再利用できるか
- **「新規」**をクリックすれば、新しいパスワード・ポリシーを作成することができます。
- リストで既存のパスワード・ポリシーを選択してから**「変更」**をクリックすれば、そのポリシーを変更することができます。
- リストで既存のパスワード・ポリシーを選択してから**「削除」**をクリックすれば、そのポリシーを削除することができます。

新規のパスワード・ポリシーを作成するには、次のようにします。

1. WebSphere Commerce 管理コンソールをオープンします。
2. 管理コンソールの「セキュリティー」ドロップダウン・メニューで**「パスワード・ポリシー」**をクリックします。
3. 「パスワード・ポリシー」ページで**「新規」**をクリックして、新しいアカウント・ポリシーを作成します。
4. パスワード・ポリシーの名前を「名前」フィールドに入力します (たとえば、`my_password_policy` など)。
5. 必要があれば以下を更新し、ショッパー用のデフォルト値を任意の値に変更します。
   - **ユーザー ID とパスワードは一致していてもかまいませんか？** ユーザー ID とパスワードが同じでもよいかどうかを定義します。リストで「はい」または「いいえ」を選択します。
   - **最大連続文字タイプ**。パスワード内での連続文字の最大出現回数を定義します。連続文字の最小値は 2 回です。たとえば 2 の値の場合、ユーザーは `aaabc` のような値を入力することはできません。

- **文字の最大インスタンス**。パスワード内に同一文字が出現してもかまわない最大回数を定義します。最小値は 1 つの文字インスタンスです。たとえば 2 の値の場合、ユーザーは abcaabc のような値を入力することはできません。
- **パスワードの最長存続時間**。パスワードが存続できる最大期間を日数で定義します。最小値は 1 日です。その期間を過ぎると、ユーザーはパスワードを変更するようプロンプトで指示されます。
- **英字の最小文字数**。パスワード内で使用しなければならない英字の最小数を定義します。最小値は 0 個の英字です。
- **数字の最小文字数**。パスワード内で使用しなければならない数字の最小数を定義します。最小値は 0 個の数字です。
- **パスワードの最低限の長さ**。パスワードの最短長を文字数で定義します。最小値は 1 文字です。
- **パスワードは再使用できますか ?** ユーザーの旧パスワードを再利用できるかどうかを定義します。リストで「はい」または「いいえ」を選択します。

6. **「OK」**をクリックします。

注:

1. パスワード・ポリシーが使用中の (つまり、ユーザーがそのパスワード・ポリシーを割り当てられている) 場合は、そのポリシーを削除することはできません。
2. パスワード・ポリシーが有効化されるのは、ユーザーが WebSphere Commerce データベースに対して認証されている場合のみです。

追加情報については、 71 ページの『デフォルト認証ポリシー』も参照してください。

アカウント・ロックアウト・ポリシーのセットアップ

WebSphere Commerce 管理コンソールの「アカウント・ロックアウト・ポリシー」ページで、WebSphere Commerce 内のさまざまなユーザー役割用のアカウント・ロックアウト・ポリシーをセットアップすることができます。このページには、既存のアカウント・ロックアウト・ポリシーがすべてリストされます。その中には、デフォルトで WebSphere Commerce に付属している、事前定義されたあらゆるアカウント・ポリシーも含まれます。アカウント・ロックアウト・ポリシーは、ユーザー・アカウントに対して不正アクションがとられた場合にそのアカウントを使用禁止にすることで、そのようなアクションによってアカウントが被害を受ける機会を減らします。

アカウント・ロックアウト・ポリシーは次のようなアイテムを統制します。

- アカウント・ロックアウトのしきい値。無効なログオンの試行回数がこの値に達すると、アカウントが使用不可になります。
- ログインの連続失敗による遅延。これは、ユーザーがログインに 2 回失敗した場合にその後ログインできなくなる期間を指します。ログインの失敗が続くと、この遅延はそのつど構成済みの時間遅延値 (たとえば 10 秒) ずつ増加されます。

アカウント・ロックアウト・ポリシーを設定するには、次のようにします。

1. WebSphere Commerce 管理コンソールをオープンします。

2. 管理コンソールの「セキュリティー」ドロップダウン・メニューで**「アカウント・ロックアウト・ポリシー」**をクリックします。
3. 既存のすべてのアカウント・ロックアウト・ポリシーが「アカウント・ロックアウト・ポリシー」ページに示されます。 このページでは以下を行うことができます。
   - **「新規」**をクリックすれば、新しいポリシーを作成することができます。
   - リストでポリシーを選択してから**「変更」**をクリックすれば、既存のポリシーを変更することができます。
   - リストでポリシーを選択してから**「削除」**をクリックすれば、既存のポリシーを削除することができます。

新規のアカウント・ロックアウト・ポリシーの場合、「アカウント・ロックアウト・ポリシー」ページで次のようにします。

1. アカウント・ロックアウト・ポリシーの名前を「名前」フィールドに入力します (たとえば、`my_policy` など)。
2. 「アカウント・ロックアウトしきい値」フィールドにそのしきい値を入力します。たとえば 6 (6 回の試行) と入力します。
3. ログインの連続失敗による遅延を秒数で「待ち時間 (Wait time)」フィールドに入力します。たとえば 10 (10 秒の場合) と入力します。
4. **「OK」**をクリックします。

注:

1. アカウント・ロックアウト・ポリシーが使用中の (つまり、ユーザーがそのアカウント・ロック・ポリシーを割り当てられている) 場合は、そのポリシーを削除することはできません。
2. アカウント・ロックアウト・ポリシーが実効化されるのは、ユーザーが WebSphere Commerce データベースに対して認証されている場合のみです。

セキュリティー検査の立ち上げ

400 このフィーチャーは、 WebSphere Commerce for iSeries では使用できません。

WebSphere Commerce 管理コンソールの「セキュリティー検査の立ち上げ (Launch security check)」ページを使って、機密漏れの可能性があると思われる一時 WebSphere Commerce ファイルの検査と削除を行うためのセキュリティー・プログラムを手動で立ち上げることができます。通常、セキュリティー検査プログラムは定期的なジョブとして実行され、デフォルトでは月に一度実行するように設定されています。

セキュリティー検査プログラムを起動するには、次のようにします。

1. WebSphere Commerce 管理コンソールをオープンします。
2. 管理コンソールの「セキュリティー」ドロップダウン・メニューで**「セキュリティー・チェッカー」**をクリックします。
3. 「セキュリティー検査の立ち上げ」ページで、**「立ち上げ」**をクリックします。

プログラムによってとられたすべてのアクションを含め、セキュリティー検査の結果が「セキュリティー検査」ウィンドウと、次のような logs サブディレクトリー内の sec_check.log ファイルに書き込まれます。

AIX Linux Solaris WC_installdir/instances/*instance_name*/logs

Windows WC_installdir¥instances¥*instance_name*¥logs

Windows Windows 以外のプラットフォームでは、無許可のユーザーが機密ファイルにアクセスできないようにするため、ファイル許可は WebSphere Commerce で自動的に設定されます。 Windows プラットフォームでは、次のようにして、許可を手動で設定する必要があります。この手順を行えば、機密ファイルに対して管理者グループのみが**読み取り/書き込み/実行**の権限を持つようにすることができます。

1. Windows のエクスプローラーで *drive*:¥WebSphere フォルダーを右マウス・ボタンでクリックします。
2. **「プロパティ」**をクリックし、次に**「セキュリティ」**をクリックします。デフォルトでは、「Everyone」グループが、このフォルダーに対する**すべての**許可を受けています。
3. **「追加」**をクリックします。
4. (「ユーザー、コンピューターの選択 (Select users, computers...)」) ウィンドウが表示されます。 このウィンドウで、**「Administrators」**グループを選択します。

   注: この場合、これは若干まぎらわしいかもしれません。Administrator をユーザーと見なすことができますが、 Administrator ユーザーではなく、Administrator グループを追加する必要があるからです。

   「追加」をクリックしてから、**「OK」**をクリックします。
5. 「セキュリティ」タブに Administrators グループが追加されました。「Everyone」を除去する必要があります。**「全員 (Everyone)」**を選択してから、「継承可能なアクセス許可を...」と書かれているボックスのチェックを取り除きます。
6. 表示される「セキュリティ」ウィンドウの**「削除」**をクリックします。

構成マネージャーの PDI 暗号化フィールド

WebSphere Commerce インスタンスを構成するときは、「PDI 暗号化 (PDI Encrypt)」チェック・ボックスを選択するようお勧めします。「PDI 暗号化 (PDI Encrypt)」フィールドを使用可能にすると、 ORDPAYINFO と ORDPAYMTHD 表に指定された情報が暗号化されます。このチェック・ボックスを選択すると、決済情報が WebSphere Commerce データベースに暗号化された形式で保管されます。

デフォルト認証ポリシー

WebSphere Commerce には、 2 つのデフォルト認証ポリシーが組み込まれています。

- 72 ページの『ショッパー』
- 72 ページの『管理者』

ショッパー

ショッパー用のデフォルト・アカウント・ポリシーには、ショッパー用のデフォルト・アカウント・ロックアウト・ポリシーとデフォルト・パスワード・ポリシーが含まれています。

ショッパー用のデフォルト・アカウント・ロックアウト・ポリシーには、以下のデフォルト属性が含まれています。

属性	デフォルト値
アカウント・ロックアウトのしきい値	6 回の試行
ログインの連続失敗による遅延	10 秒

ショッパー用のデフォルト・パスワード・ポリシーには、 以下のデフォルト属性が含まれています。

属性	デフォルト値
ユーザー ID とパスワードが同じでよいか	N (同じではいけない)
連続する最大文字数	3 文字
文字の最大インスタンス	4 インスタンス
パスワードの最長存続時間	180 日
英字の最小文字数	1 英字
数字の最小文字数	1 数字
パスワードの最低限の長さ	6 文字
ユーザーの以前のパスワードを再利用できるか	N (再利用できない)

自己登録を実行するショッパーには、ショッパー用のデフォルト認証ポリシー (Shoppers) が割り当てられます。

管理者

管理者用のデフォルト・アカウント・ポリシーには、管理者用のデフォルト・アカウント・ロックアウト・ポリシーとデフォルト・パスワード・ポリシーが含まれています。

管理者用のデフォルト・アカウント・ロックアウト・ポリシーには、以下のデフォルト属性が含まれています。

属性	デフォルト値
アカウント・ロックアウトのしきい値	3 回の試行
ログインの連続失敗による遅延	20 秒

ショッパー用のデフォルト・パスワード・ポリシーには、 以下のデフォルト属性が含まれています。

属性	デフォルト値
ユーザー ID とパスワードが同じでよいか	N (同じではいけない)

属性	デフォルト値
連続する最大文字数	3 文字
文字の最大インスタンス	4 インスタンス
パスワードの最長存続時間	90 日
英字の最小文字数	1 英字
数字の最小文字数	1 数字
パスワードの最低限の長さ	8 文字
ユーザーの以前のパスワードを再利用できるか	N (再利用できない)

WebSphere Commerce の出荷時のデフォルト `wcsadmin` 管理者ユーザーには、管理者用のデフォルト認証ポリシー (`Administrators`) が割り当てられます。

第 5 章 セッション管理

Web ブラウザーと e-commerce サイトは、HTTP を使って通信します。 HTTP はステートレス・プロトコル (つまり、どのコマンドも、前に発行されたコマンドを関知せずに独立して実行されます) であるため、ブラウザー・サイドとサーバー・サイドどうしのセッションを管理する手段が必要です。

WebSphere Commerce は、cookie ベースおよび URL 再書き込みの 2 つのタイプのセッション管理をサポートします。管理者は、cookie ベースのセッション管理だけのサポート、または cookie ベースと URL 再書き込みの両方のセッション管理のサポートを選択することができます。 WebSphere Commerce が cookie ベースのみをサポートする場合、ショッパーのブラウザーは cookie を受け入れ可能になっていなければなりません。 cookie ベースと URL 再書き込みの両方を選択すると、WebSphere Commerce はまず cookie を使ってセッション管理を試みます。ショッパーのブラウザーが cookie を受け入れないように設定されている場合に、 URL 再書き込みが使われます。

cookie ベースのセッション管理

cookie ベースのセッション管理を使用すると、ユーザー情報の入ったメッセージ (cookie) が Web サーバーからブラウザーに送られます。この cookie は、ユーザーが特定のページにアクセスしようとしたときにサーバーに返送されます。サーバーは、cookie の返送によってユーザーを識別することができ、セッション・データベースからそのユーザーのセッションを取り出します。それによって、ユーザーのセッションが保守されます。 cookie ベースのセッションは、ユーザーがログオフまたはブラウザーをクローズすると終了します。 cookie ベースのセッション管理は安全であり、しかもパフォーマンス上の利点があります。 cookie ベースのセッション管理が安全なのは、 SSL を通してのみやりとりされる識別タグを使用するからです。cookie ベースのセッション管理は、パフォーマンスの点から見るとかなり有利です。 WebSphere Commerce のキャッシング機構は cookie ベースのセッションだけをサポートし、 URL 再書き込みをサポートしないからです。 cookie ベースのセッション管理は、ショッパー・セッションの場合にお勧めします。

URL の再書き込みを使用していない場合に、ユーザーがブラウザー上で cookie を使用可能にしているかどうかを確認したければ、構成マネージャーの「セッション管理」ページの**「cookie 受け入れテスト」**にチェックしてください。これで、ショッパーのブラウザーが cookie をサポートしていない場合や、cookie がオフになっている場合に、 WebSphere Commerce サイトをブラウズするには cookie をサポートしているブラウザーが必要であることがショッパーに知らされます。

セキュリティー上の理由から、cookie ベースのセッション管理では次の 2 種類の cookie が使われます。

- 非セキュア・セッション cookie

  セッション・データを管理するのに使われます。セッション ID、ネゴシエーションされた言語、現在のストア、およびショッパーの希望通貨 (cookie の構成時の

もの) が入っています。この cookie は、SSL または非 SSL のどちらの接続でもブラウザーとサーバーとでやり取りすることができます。次の 2 タイプの非セキュア・セッション cookie があります。

– WebSphere Application Server セッションの cookie は、サーブレット HTTP セッション標準をベースとします。 WebSphere Application Server の cookie は、メモリー、または複数のノードに配置されたデータベースに存在しています。詳細については、「WebSphere Application Server Information Center」(http://www.ibm.com/software/webservers/appserv/infocenter.html) で「session management (セッション管理)」を検索してください。

– WebSphere Commerce セッションの cookie は WebSphere Commerce から見て内部的であり、データベースには存在していません。

どのタイプの cookie を使用するかを選択するには、構成マネージャーの「セッション管理 (Session Management)」ページの **「cookie セッション・マネージャー (Cookie Session Manager)」**パラメーターで WCS または WAS を選択します。

- セキュア認証 cookie

  認証データの管理に使用されます。認証 cookie は SSL を通してやりとりされ、セキュリティーの最大化のためにタイム・スタンプを押されます。これは、たとえばユーザーのクレジット・カード番号をたずねる DoPaymentCmd といった機密性の高いコマンドが実行されるたびに、ユーザーを認証するのに使用される cookie です。この cookie が盗まれて無許可のユーザーによって使用される危険性は最小化されています。 cookie ベースのセッション管理を使用する場合は、常に認証コード cookie が WebSphere Commerce によって生成されます。

セキュア・ページを表示するには、セッション cookie と認証コード cookie の両方が必要です。

以下の場合に cookie エラーが起きると、CookieErrorView が呼び出されます。

- ユーザーが同じログオン ID を使って別のロケーションからログインした場合。
- cookie が壊れたかまたは改ざんされた (またはこの両方) 場合。
- cookie の受け入れが「true」に設定されているのに、ユーザーのブラウザーが cookie をサポートしていない場合。

セッション管理での cookie の使用

WebSphere Commerce で cookie を使用するには、以下のようにします。

1. 構成マネージャーをオープンします。
2. **「インスタンス」**を選択してから、**「セッション管理」**フォルダーをオープンします。
3. 該当するセッション値を選択します。
   - cookie 受け入れテスト

     顧客のブラウザーが、 cookie のみをサポートしているサイトの cookie を受け入れるかどうか調べるには、このチェック・ボックスを選択します。
   - cookie セッション・マネージャー

     cookie の管理に WebSphere Commerce を使用するのか、 WebSphere Application Server を使用するのかを選択します。デフォルトは WebSphere Commerce です。

– WebSphere Application Server セッションの cookie は、サーブレット HTTP セッション標準をベースとします。 WebSphere Application Server の cookie は、メモリー、または複数のノードに配置されたデータベースに存在しています。詳細については、「WebSphere Application Server Information Center」 (http://www.ibm.com/software/webservers/appserv/infocenter.html) で「session management (セッション管理)」を検索してください。

– WebSphere Commerce セッションの cookie は WebSphere Commerce から見て内部的であり、データベースには存在していません。

4. **「拡張」**タブをクリックします。該当するセッション値を選択します。
   - Cookie パス

     cookie のパスを指定します。これは cookie の送信先の URL のサブセットです。通常、このフィールドを変更してはなりません。

     cookie のパスについての詳細は、 Netscape の cookie 仕様と RFC 2109 を参照してください。
   - Cookie ドメイン

     ドメインの制限パターンを指定します。通常、このフィールドを変更してはなりません。

     ドメインは cookie を受け取るサーバーを指定します。デフォルトでは、cookie はその発信元の WebSphere Commerce Server にだけ返送されます。またデフォルトでは cookie は、保管先のホストにのみ返送されます。ドメイン・ネーム・パターンを指定すると、それがオーバーライドされます。そのパターンは、ピリオドで始まっていて、少なくとも 2 つのピリオドが使われていなければなりません。パターンは、最初のピリオドの後は 1 つのエントリーにしか一致しません。たとえば、「.ibm.com」は有効であり、「a.ibm.com」と「b.ibm.com」に一致しますが、「www.a.ibm.com」には一致しません。ドメイン・パターンの詳細は、Netscape の cookie の仕様と RFC 2109 を参照してください。
5. **「適用」**をクリックします。
6. 構成マネージャーをクローズします。
7. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

URL 再書き込み

URL 再書き込みを使った場合、ブラウザーに戻ってくるか、またはリダイレクトされたすべてのリンクには、セッション ID が付けられます。ユーザーがそのようなリンクをクリックすると、書き換えられたフォームの URL が、クライアント要求の一部としてサーバーに送信されます。サーブレット・エンジンは、URL 内のセッション ID を認識し、そのユーザーの正しいオブジェクトを取得するために保管します。 URL の再書き込みを使用するには、リンクに HTML ファイル (.html または .htm の拡張子の付いたファイル) は使用できません。 URL の再書き込みを使用するには、JSP ファイルを表示用に使用する必要があります。 URL の再書き込みを使用するセッションは、ショッパーがログオフすると期限が切れます。

注: WebSphere Commerce の動的キャッシングと URL の再書き込みの操作は両立しません。 URL 再書き込みをオンにする場合、WebSphere Commerce 動的キャッシングを使用不可にする必要があります。詳しくは、「*WebSphere Commerce 管理ガイド*」の動的キャッシングについての章を参照してください。

URL 再書き込みセッション管理の使用

セッションを管理する方法を指定するには、次のようにします。

1. 構成マネージャーをオープンします。
2. **「インスタンス」**を選択してから、**「セッション管理」**フォルダーをオープンします。
3. 該当するセッション値を選択します。

   「URL 再書き込み」を使用可能にします。セッション管理に URL 再書き込みを使用する場合は、このチェック・ボックスを選択します。

   「cookie セッション・マネージャー。」 WebSphere Application Server を選択します。
4. **「適用」**をクリックします。
5. 構成マネージャーをクローズします。
6. WebSphere Application Server 管理コンソールから、 WebSphere Commerce サーバー・インスタンスをいったん停止してから再始動します。

URL 再書き込み用の JSP テンプレートの作成

セッション状態の保守に URL 再書き込みを使用したい場合、 Web アプリケーションのパーツへのリンクをプレーン・テキストの HTML ファイルに組み込まないでください。この制約事項が必要なのは、プレーン・テキストの HTML ファイル内で URL エンコードを使用できないからです。 URL 再書き込みを使って状態を保守するには、セッション中のユーザー要求では、 Java インタープリターが理解できるコードを使用する必要があります。そのようなプレーン・テキストの HTML ファイルや、ユーザーがセッション中にアクセスする可能性のあるサイト部分が Web アプリケーションに含まれている場合、それを JSP ファイルに変換してください。これによってアプリケーションの作成が影響を受けることになります。
cookie を使ってセッションを保守するのと違って、URL 再書き込みでセッションを保守するには、アプリケーション内の各 JSP テンプレートの中で `<A>` タグの各 `HREF` 属性ごとに URL エンコードを使用する必要があるからです。アプリケーション内の 1 つ以上の JSP テンプレートが `encodeURL(String url)` を呼び出さなかったり、 `RedirectURL(String url)` メソッドをエンコードしたりすると、セッションは消失します。

リンクの作成

URL 再書き込みでは、ブラウザーに戻ってくるか、またはリダイレクトされるすべてのリンクには、セッション ID が付けられている必要があります。たとえば、Web ページ内に次のようなリンクがあるとします。

```
<a href="store/catalog">
```

上記は次のように書きます。

```
<a href="store/catalog;$jsessionid$DA32242SSGE2">
```

ユーザーがこのリンクをクリックすると、書き換えられたフォームの URL が、クライアント要求の一部としてサーバーに送信されます。サーブレット・エンジンは、;$jsessionid$DA32242SSGE2 をセッション ID として認識し、このユーザーの正しい HttpSession オブジェクトを取得するために保管します。

以下の例は、 JSP ファイル内に Java コードを組み入れる方法を示しています。

```
<%
 response.encodeURL ("/store/catalog");
%>
```

ブラウザーに送り返される URL を再書き込みするには、 JSP テンプレート内で encodeURL() メソッドを呼び出してから、その URL を出力ストリームに送信します。たとえば、次のような、URL 再書き込みを使用しない JSP テンプレートがあるとします。

```
out.println("<a href=¥"/store/catalog¥">catalog</a>")"
```

上記を次のように書き換えます。

```
out.println("<a href=¥"");
out.println(response.encodeURL ("/store/catalog"));
out.println("¥">catalog</a>");
```

リダイレクトしようとする URL を再書き込みするには、 encodeRedirctURL() メソッドを呼び出します。たとえば、次のような JSP テンプレートがあるとします。

```
response.sendRedirect (response.encodeRedirectURL ("http://myhost/store/catalog"));
```

encodeURL() と encodeRedirectURL() メソッドは、 HttpServletResponse オブジェクトの一部を成します。どちらの場合も、URL のエンコードの前に URL が再書き込みされるよう構成されているかどうかが、それらの呼び出しによって検査されて確かめられます。そのように構成されていないと、元の URL が返送されます。

フォームの作成: 送信用のフォームを作成するには、フォーム・テンプレートの ACTION タグ上の response.encodeURL("Logon"); を呼び出します。以下に例を示します。

```
String strLoginPost = response.encodeURL("Logon");
<FORM NAME="Logon" METHOD="post" ACTION= <%= strLoginPost %> >
...
</FORM>
```

先頭ページの作成: 通常はホーム・ページである導入ページでは、フレームを使用することはできません。ストア内でフレームを使用したい場合、そのストアへのリンクをもつ非フレーム・ページをストアの導入ページとして機能させることができます。ただし、ストアがフレームを使用し、顧客がまず導入ページを経由せずにフレームを備えたこれらのページにアクセスしようとすると、そのセッションは消失することがあります。また顧客が、**「戻る」**ボタン (フレームにのみ装備) を使って導入ページに戻って、導入ページを最新表示にしようとした場合も、セッションが消失する可能性があります。導入ページを最新表示にすると、新規のセッション ID が発行されるからです。この種のセッションの消失を防止するには、**「戻る」**ボタンの代わりに、導入ページに戻るためのリンクが必要です。

ストア・レベルのセッション管理

以下の図は、 WebSphere Commerce のストア・レベルの登録インフラストラクチャーをまとめたものです。ストア・レベルの登録では、アクセス制御の役割を使用してショッパーとストアを関連付けます。

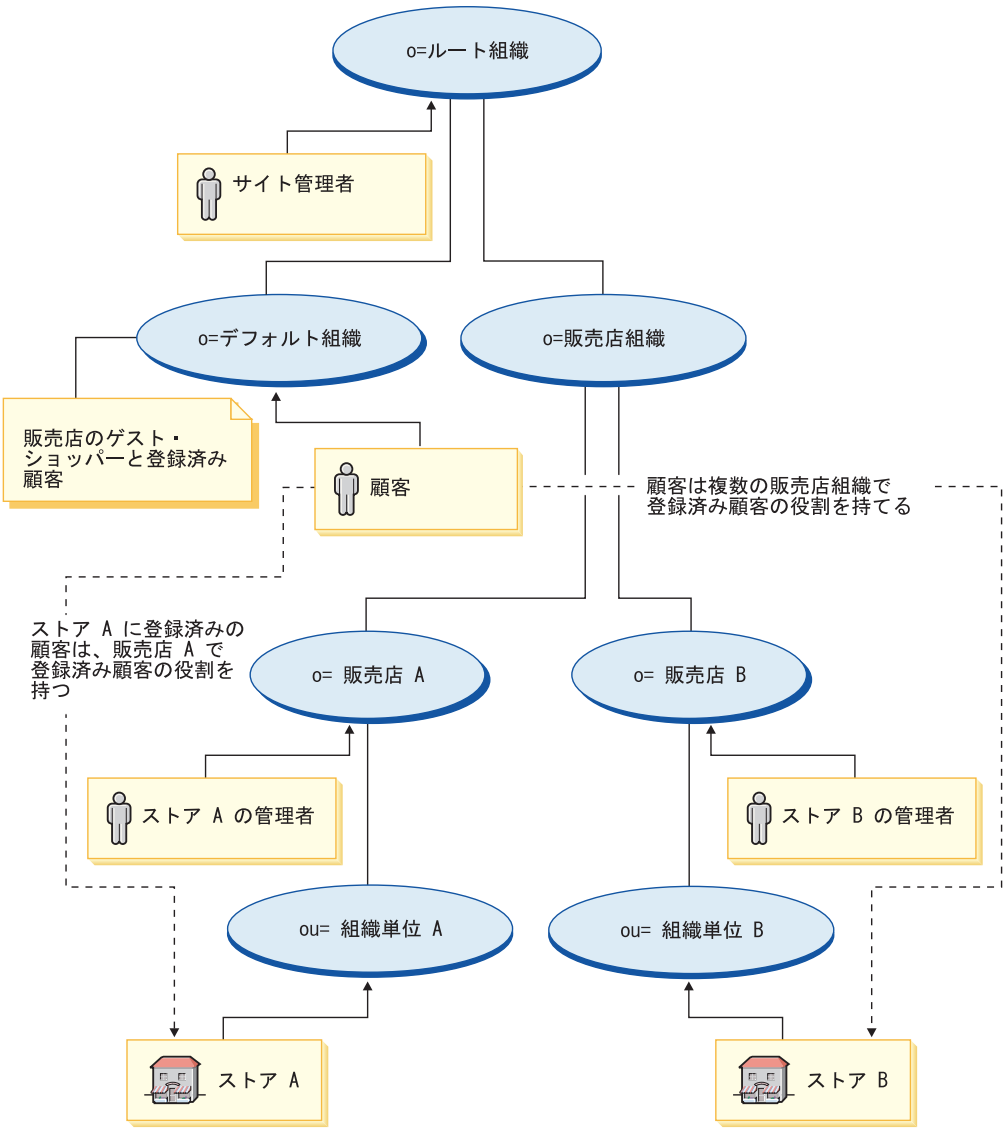


図 3. ストア・レベルの登録

ストアでショッピングをするユーザーは、そのストアの組織のメンバーである必要はありませんが、その組織内でショッピングの役割 (つまり登録済みの顧客という役割) を演じる必要があります。一方、組織内で管理の役割を演じるユーザーは、組織との親子関係によって組織と関連付けられるのが普通です。

たとえば、上の図のようにストア A というストアがあるとしましょう。また、スーはストア A でショッピングをしますが、ジョーはストア A の運営の管理業務を担当する、ストア A の従業員であるとします。このシナリオを組織の観点からモデル化すると、ジョーはストア A という組織の下に配置されますが、スーはそうではあ

りません。スーはストア A の社員ではなく、ストア A という組織内でショッピングの役割を演じるという意味で、ストア A との関係を持っているにすぎません。

ストアが登録済みのすべてのショッパーを判別するには、ストアの組織内でショッピングの役割を演じるすべてのユーザーを抽出することになります。それができた時点で、ストアのユーザー管理者は、ストア内のすべての登録済みユーザーに対するキャンペーンの実施など、ストア全体にまたがる操作や、ストアに登録されている 1 人のユーザーのパスワードのリセットなど、個別の事例に関するアクションを実行できるようになります。

80 ページの図 3 を参照しながら、以下のシナリオについて検討してみましょう。

- デフォルト組織のメンバーであるスーは、販売店 A の組織内でショッピングの役割を持っています。販売店 A の親組織は販売店組織です。
- 販売店 A はストア A を所有しています。
- スーは販売店 B の組織内で組織的な役割を持っていません。
- 販売店 B はストア B を所有しています。

スーはストア A にログインして、いつものとおりにショッピングをします。スーがストア B にアクセスすると、スーはストア B のゲスト・ユーザーとして新しいセッション ID を割り当てられます。スーがストア A にもう 1 度アクセスすると、WebSphere Commerce は、スーがストア A で持っていた以前のセッション ID の情報を使用して、スーのセッションを管理します。

ストア A のセッション ID は、以下の場合にストア B で再利用されます。

- ストア A とストア B が同じ組織に属している場合。
- スーが販売店 A の組織と販売店 B の組織の両方で定義されている役割を持っている場合。

第 6 章 パスワードの設定と変更

WebSphere Commerce のコンポーネントの大半は、オペレーティング・システムによって検証されるユーザー ID とパスワードを利用します。これらのパスワードの変更の詳細は、オペレーティング・システムの資料を参照してください。この章では、オペレーティング・システムを介してユーザー ID とパスワードを検証しない WebSphere Commerce コンポーネント用のパスワードの設定と変更の方法について述べます。

ユーザー ID、パスワード、および Web アドレスの早見表

WebSphere Commerce 環境での管理には、さまざまなユーザー ID が必要です。それらのユーザー ID と、それに必要な権限のリストを、次の表に示します。各 WebSphere Commerce ユーザー ID ごとにデフォルトのパスワードが示されています。

400 **iSeries ユーザー・プロファイル**

WebSphere Commerce をインストールして構成するときは、以下の 2 つの iSeries ユーザー・プロファイルを頻繁に使用および参照します。

- WebSphere Commerce をインストールしたり構成マネージャーを開始するために作成して使用するユーザー・プロファイル。 WebSphere Commerce をインストールして構成するには、USRCLS(*SECOFR) の iSeries ユーザー・プロファイルを使用するか、または QSECOFR ユーザー・プロファイルを使用しなければなりません。ユーザー・プロファイルを作成する必要がある場合、iSeries 用の「*WebSphere Commerce インストール・ガイド*」を参照してください。
- WebSphere Commerce インスタンスの作成時に構成マネージャーによって作成されるユーザー・プロファイル。このユーザー・プロファイルは、*インスタンス・ユーザー・プロファイル* とも呼ばれます。 USRCLS(*USER) のユーザー・プロファイルは、WebSphere Commerce インスタンスを作成するごとに構成マネージャーによって作成されます。ユーザー・プロファイルを作成する必要がある場合、iSeries 用の「*WebSphere Commerce インストール・ガイド*」を参照してください。

構成マネージャーのユーザー ID

構成マネージャー・ツールのグラフィカル・インターフェースを使用すれば、 WebSphere Commerce の構成方法を変更できます。構成マネージャーのデフォルト・ユーザー ID およびパスワードは、 webadmin および webibm です。

AIX Linux Solaris Windows 構成マネージャーには、 WebSphere Commerce マシンからか、または WebSphere Commerce と同じネットワーク上の任意のマシンからアクセスできます。

400 iSeries の場合、構成マネージャーには、 iSeries サーバーと同じネットワーク上にある任意の Windows マシンからアクセスすることができます。

IBM HTTP Server のユーザー ID

AIX Linux Solaris Windows IBM HTTP Server を使用している場合、Web ブラウザーをオープンして、以下の Web アドレスを入力すれば Web サーバーのホーム・ページにアクセスできます。

```
http://host_name
```

Web サーバーをカスタマイズした場合、ホスト名の後に Web サーバーのフロントページの名前を入力する必要があります。

WebSphere Commerce インスタンス管理者

インスタンス管理者のユーザー ID とパスワードは、以下の WebSphere Commerce ツールに適用されます。

- WebSphere Commerce アクセラレーター. Windows オペレーティング・システムが実行されているリモート・マシンから WebSphere Commerce アクセラレーターにアクセスするには、 Internet Explorer Web ブラウザーをオープンしてから、以下の Web アドレスを入力します。

  ```
  https://host_name:8000/accelerator
  ```

- WebSphere Commerce 管理コンソール. Windows オペレーティング・システムが実行されているリモート・マシンから WebSphere Commerce 管理コンソールにアクセスするには、 Internet Explorer Web ブラウザーをオープンしてから、以下の Web アドレスを入力します。

  ```
  https://host_name:8002/adminconsole
  ```

- WebSphere Commerce 組織管理コンソール. Windows オペレーティング・システムが実行されているリモート・マシンから WebSphere Commerce 組織管理コンソールにアクセスするには、 Internet Explorer Web ブラウザーをオープンしてから、以下の Web アドレスを入力します。

  ```
  https://host_name:8004/orgadminconsole
  ```

前述のツールで、WebSphere Commerce インスタンスを作成したときに入力した管理者のユーザー ID とパスワードを入力します。

注: サイト管理者のユーザー ID は、決して削除しないようにしてください。また、そのユーザー ID にはインスタンス管理者の権限を常に与えておく必要があります。

WebSphere Commerce では、ユーザー ID とパスワードに関して次の規則に従う必要があります。

- パスワードの長さは、少なくとも 8 文字なければなりません。
- パスワード内では、少なくとも 1 字の数字を使用しなければなりません。
- パスワード内では、1 つの文字が 4 回を超えて出現してはなりません。
- パスワード内では、同じ文字を 3 回を超えて繰り返し使用してはなりません。

WebSphere Commerce Payments 管理者

WebSphere Commerce Payments をインストールすると、 WebSphere Commerce サイト管理者 ID に Payments 管理者役割が自動的に割り当てられます。 Payments のレルム・クラスをまだ WCSRealm に切り替えていない場合は、「*WebSphere Commerce インストール・ガイド*」の指示に従って切り替えてください。

Payments 管理者役割を使えば、ユーザー ID で WebSphere Commerce Payments の制御と管理ができます。

400 **注:**

- 各インスタンス用に作成したサイト管理者のユーザー ID の削除や名前変更はしないでください。また、事前に割り当てられている WebSphere Commerce Payments の役割の変更もしないでください。もし変更すると、 WebSphere Commerce Payments の統合に関連した WebSphere Commerce の機能が動作しなくなります。

Windows **Windows ユーザー ID**

Windows ユーザー ID は管理者権限をもっている必要があります。 DB2® を使用する場合、ユーザー ID とパスワードに関して次の規則に従う必要があります。

- 長さが 8 文字を超えてはなりません。
- 使用できる文字は A～Z、a～z、0～9、@、#、$、および _ だけです。
- 下線 (_) で始めることはできません。
- USERS、ADMINS、GUESTS、PUBLIC、LOCAL は、大文字小文字の別に関係なく、ユーザー ID として使用できません。
- IBM、SQL、SYS は、大文字小文字の別に関係なく、ユーザー ID の先頭の 3 文字として使用できません。
- Windows サービス名と同じユーザー ID は使用できません。
- ユーザー ID はローカル・マシン上で定義されていなければならず、ローカル管理者のグループに属していなければなりません。
- ユーザー ID には、拡張ユーザー権限として *オペレーティング・システムの一部として機能* が付与されていなければなりません。

オペレーティング・システムの一部として機能 拡張ユーザー権限を持っていなくてもインストールは実行できますが、 DB2 セットアップ・プログラムは、管理サーバーに指定したアカウントの妥当性検査を行うことができません。DB2 のインストールに使用するユーザー・アカウントはすべて、この拡張ユーザー権限を持つことをお勧めします。

重要

使用している Windows のユーザー ID に管理者権限がない 場合、ユーザー ID の長さが 8 文字を超える場合、またはローカル・マシン上で定義されていない場合には、その問題についての通知が出され、インストールを続行することはできません。

DB2 を使用している場合は、後でこのユーザー ID を DB2 データベース・ユーザー名 (データベース・ユーザーのログオン ID) として使用します。

上述の基準を満たすユーザー ID を作成する必要がある場合、 Windows オンライン・ヘルプで Windows ユーザー ID の作成に関する情報を見つけることができます。

構成マネージャー・パスワードの変更

構成マネージャー・パスワードを変更するには、構成マネージャーを立ち上げてから、ユーザー ID とパスワードを入力するウィンドウで**「変更」**をクリックします。

または、構成マネージャーのユーザー ID またはパスワードを変更するために、WebSphere Commerce のインストール・パスの下の bin サブディレクトリーに切り替えてから、コマンド・ウィンドウに以下のコマンドを入力します。

1. WebSphere Commerce bin サブディレクトリーに移動します。

   ```
   cd WC55_installdir/bin
   ```

2. 以下のように wcs_encrypt スクリプトを実行して、暗号化されたバージョンのパスワードを入手します。

   AIX 400 Linux Solaris

   ```
   ./wcs_encrypt.sh new_password
   ```

   Windows

   ```
   wcs_encrypt new_password
   ```

3. *WC55_installdir*/instances ディレクトリーで PwdMgr.xml ファイルを開き、LoginPassword を、ステップ 2 で暗号化した暗号化パスワードを使って変更します。

IBM HTTP Server 管理者パスワードの設定

AIX Linux Solaris Windows IBM HTTP Server 管理者のパスワードを設定するには、次のようにします。

1. マシン上の *HTTPServer_installdir*/bin ディレクトリーに切り替えます。
2. 以下のコマンドを入力します。

   AIX Linux Solaris `./htpasswd -b ../conf/admin.passwd user password`

   Windows `htpasswd -b conf¥admin.passwd user password` ここで、*user* および *password* は、IBM HTTP Server への管理権限を付与するユーザー ID およびパスワードです。

これで、IBM HTTP Server 管理パスワードを正しく設定できました。

注: 管理者パスワードが存在しない場合、htpassword に -c オプションを指定して実行し、まずパスワードを作成する必要があります。

SSL 鍵ファイル・パスワードの変更

AIX Linux Solaris Windows IBM HTTP Server を使用している場合、SSL 鍵ファイル・パスワードを変更するには、以下の手順を実行します。

1. Windows **「スタート」メニュー → 「プログラム」 → 「IBM HTTP Server」 → 「鍵管理ユーティリティーの開始 (Start Key Management Utility)」**をクリックします。
2. **「鍵データベース・ファイル (Key Database File)」**メニューから、**「オープン」**を選択します。
3. IBM HTTP Server インストール・パスの下の ssl サブディレクトリーに切り替えます。鍵ファイル (ファイル拡張子 .kdb) は、このフォルダーに入っていなければなりません。入っていない場合は、213 ページの『第 17 章 IBM HTTP Server での実動のための SSL の使用可能化』で示されている指示に従って新しい鍵ファイルを作成します。
4. **「鍵データベース・ファイル (Key Database File)」**メニューから、**「パスワード変更」**を選択します。「パスワード変更」ウィンドウが表示されます。
5. 新しいパスワードを入力し、**「パスワードをファイルに隠す (Stash the password to a file)」**を使用可能にします。
6. **「OK」**をクリックします。パスワードが変更されます。

これで、SSL 鍵ファイルの管理パスワードを正しく変更できました。

WebSphere Commerce 暗号化パスワードの生成

ユーザーのパスワードを手動でリセットするために、コマンド行から、暗号化されたパスワードを生成できます。同じタスクを実行する別のツール (ResetPassword コマンドなど) が存在します。パスワードを手動でリセットするために、管理者は以下のユーティリティーで出力される暗号化されたパスワードを使用して、 USERREG 表の LOGONPASSWORD フィールドを更新します。さらに管理者は、選択した salt で USERREG 表の SALT フィールドを更新します。

AIX Linux Solaris Windows WebSphere Commerce では、暗号化パスワードを生成できます。暗号化パスワードを生成するには、以下のようにします。

1. WebSphere Commerce インストール・ディレクトリーの下の bin サブディレクトリーに進みます。
2. コマンド行から以下のスクリプトを実行します。

   Windows `wcs_password.bat` *`password SALT merchant_key`*

   AIX Linux Solaris `./wcs_password.sh` *`password SALT merchant_key`*

   ここで、

   - *password* はプレーン・テキストのパスワードです。

- *SALT* は、パスワードの生成で使われるランダム・ストリングです。これは、パスワードを更新している特定ユーザーの USERREG データベース表の SALT 列にあります。
- *merchant_key* はインスタンスの作成中に入力したマーチャント鍵

400 iSeries の場合、ショッパー用の暗号化パスワードを変更するには、chgwcspwd.sh コマンドを使用します。

1. iSeries システム上で QShell セッションを開始します。
2. *WC_installdir*/bin ディレクトリーに移動します。
3. コマンド行から chgwcspwd.sh スクリプトを実行します (使用法パラメーターが表示されます)。
4. 適切なパラメーターを指定してコマンドを実行します。

このコマンドの実行の詳細については、「WebSphere Commerce Production and Development オンライン・ヘルプ」を参照してください。

WebSphere Commerce Payments 暗号化パスワードの生成

WebSphere Commerce を使用して、WebSphere Commerce Payments の暗号化パスワードを生成できます。暗号化パスワードを生成するには、以下のようにします。

1. WebSphere Commerce インストール・ディレクトリーの下の bin サブディレクトリーに進みます。
2. コマンド行から以下のスクリプトを実行します。

   Windows `wcs_pmpassword.bat password SALT`

   AIX 400 Linux Solaris `./wcs_pmpassword.sh password SALT`

   ここで、

   - *password* はプレーン・テキストのパスワードです。
   - *SALT* は、パスワードの生成で使われるランダム・ストリングです。これは、パスワードを更新している特定ユーザーの USERREG データベース表の SALT 列にあります。

管理者アカウントのリセット

WebSphere Commerce アカウントが何かの理由でロック状態または使用不可状態になった場合は、次のようにしてアンロックするか、使用可能にします。

アカウントがサイト管理者のアカウントでない 場合:

1. 管理コンソールをオープンします。
2. **「アクセス管理」** > **「ユーザー」**をクリックします。
3. ユーザー・アカウントをダブルクリックするか、リストからユーザー・アカウントを選択して、**「変更」**をクリックします。
4. アカウント状況のフィールドで**「使用可能」**を選択します。
5. **「OK」**をクリックします。

アカウントがサイト管理者のアカウントまたは他のユーザー・アカウントである 場合は、 DB2 コマンド・ウィンドウまたは SQLPlus プロンプト (Oracle データベースの場合) から次の SQL ステートメントを実行します。

```
CONNECT TO db_name [USER user_id USING password]
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='logonId'
```

ここで、

db_name
ご使用の WebSphere Commerce データベース名 (MALL など) です。

user_id そのデータベースのデータベース管理者のユーザー ID です。

password
そのデータベース管理者のユーザー ID のパスワードです。

logonId
リセットしたいアカウントのユーザー ID (wcsadmin など) です。

たとえば、データベース管理者のユーザー ID でシステムにログオンしている場合、 wcsadmin アカウントをリセットするには、以下の SQL ステートメントを実行できます。

```
CONNECT TO mall
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='wcsadmin'
```

400 iSeries プラットフォームで SQL ステートメントを入力するには、DB2/400 Query Manager および SQL Development Kit を使用するか、または iSeries Navigator を使用することができます。 IBM iSeries Access を使用してデータベース照会を実行する場合は、以下のようにします。

1. インストール先の PC から iSeries Navigator を開始します。
2. iSeries システムを展開します。データベースを展開し、「リレーショナル・データベース (Relational Database)」を右マウス・ボタン・クリックし、**「SQL スクリプトの実行 (Run SQL Scripts)」**を選択します。「SQL スクリプトの実行 (Run SQL Scripts)」ウィンドウがオープンします。
3. 「接続 (Connection)」メニューから、**「JDBC セットアップ (JDBC Setup)」**を選択します。**「サーバー (Server)」**タブをクリックします。
4. デフォルト・ライブラリーのフィールドで、既存の値を消去して、現在のインスタンスのデータベース・スキーマの名前を入力します。デフォルトでは、スキーマ名がインスタンス名になっています。**「OK」**をクリックして、変更内容を保管します。
5. ウィンドウで上記の SQL ステートメントを入力します。

第 7 章 単一サインオン

この章では、WebSphere Commerce 用に単一サインオンをセットアップする方法の概要を述べます。

前提条件

単一サインオンを使用可能にするには、以下の要件を満たす必要があります。

- すでに LDAP サーバーがインストールおよび構成済みになっていなければなりません。 LDAP サーバーの構成方法については、「*WebSphere Commerce 追加ソフトウェア・ガイド*」を参照してください。
- WebSphere Commerce がインストールされていて、LDAP を使用するように構成済みでなければなりません。
- WebSphere Application Server 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。 WebSphere Application Server セキュリティーを使用可能にする方法の詳細は、199 ページの『第 16 章 WebSphere Application Server のセキュリティーの使用可能化』を参照してください。

単一サインオンの使用可能化

注意

単一サインオンを WebSphere Commerce で使用する場合、次のようないくつかの主な制限事項があります。そのような制限事項を以下に示します。

- LTPA cookie は、さまざまな Web サーバー・ポート間でやりとりされる可能性があります。
- `ldapentry.xml` ファイルを変更し、オブジェクト・クラス `ePerson` を追加する必要があるかもしれません。それは、`ldapocs` エレメントの属性として追加します。
- `instance.xml` を変更し、`MigrateUsersFromWCSdb` フラグを必ず `ON` に設定する必要があります。
- 単一サインオン構成に属する各マシンは、それぞれのシステム・クロックを同期させる必要があります。
- 単一サインオンがサポートされるのは、 WebSphere Application Server LTPA (Lightweight Third Party Authentication) トークンの読み取りと発行を行えるアプリケーションどうしの場合のみです。

単一サインオンを使用可能にするには、以下を行う必要があります。

1. WebSphere Application Server 内で単一サインオンを使用可能にします。詳細については、「WebSphere Application Server Information Center」(`http://www.ibm.com/software/webservers/appserv/infocenter.html`) で「single sign-on (単一サインオン)」を検索してください。**「Single Sign-On:**

WebSphere Application Server (単一サインオン: WebSphere Application Server)」を選択してから、以下の項の説明どおりにします。

- **WebSphere Application Server 用の SSO の構成。**
  - **WebSphere Application Server のセキュリティー設定の変更。**

    注: LDAP フィールドへの入力方法について詳述したステップは、省いても問題はありません。
  - **ファイルへの LTPA 鍵のエクスポート。**

2. WebSphere Commerce マシンで WebSphere Commerce 構成マネージャーを開始します。
3. **「メンバー・サブシステム」**ノードを構成するには、次のようにします。
   a. **WebSphere Commerce** の下から、「*host_name*」→**「インスタンス・リスト」**→「*instance_name*」→**「インスタンス・プロパティー」**→**「メンバー・サブシステム」**の順に展開します。
   b. **「認証モード」**ドロップダウン・メニューで **LDAP** を選択します。
   c. **「単一サインオン」**チェック・ボックスを使用可能にします。
   d. **「ホスト」**フィールドに LDAP サーバーの完全修飾ホスト名を入力します。
   e. 管理者の識別名を**「管理者識別名」**フィールドに入力します。これは、LDAP サーバーで使用したものと同じ名前でなければなりません。
   f. **「管理者のパスワード」**フィールドに管理者のパスワードを入力します。これは、LDAP サーバーで使用したものと同じパスワードでなければなりません。**「確認パスワード」**フィールドのパスワードを確認します。
   g. 残りのフィールドをすべて完了します。
   h. **「適用」**をクリックしてから、**「OK」**をクリックします。
4. シングル・サインオン (SSO) でシステムにアクセスするユーザーに割り当てる役割を構成します。ユーザーが SSO WebSphere Commerce でシステムに接続するたびに、登録タイプが ″SSO″ の `MemberRegistrationAttributes.xml` ファイルから役割の割り当てが試行されます。 MRA.xml を説明する新規セクションにリンクします。
5. WebSphere Application Server を再始動します。

SSO ユーザーの役割の構成

WebSphere Commerce 5.5 セキュリティー役割は、登録プロセスの一部として割り当てられます。シングル・サインオンでは、顧客はコラボレーティング・システムに正常に認証されていれば、サイトへの登録ステップをバイパスすることができます。 WebSphere Commerce 5.5 のサイトに暗黙的に認証される機能は、ユーザーがたとえばストアでのショッピングを行いたい場合に、その機能へのアクセスが拒否されて終了してしまう場合はほとんど価値がありません。

したがって、ユーザー登録と共に実行される自動役割割り当ての同じ機能は、セッション管理コードでも実行されます。この場合、SSO ショッパーの役割は、'SSO' 登録タイプを使用して構成します。このようにして、顧客がシステムで認証される場合、 WebSphere Commerce 5.5 はそのサイトが必要とするすべての役割を自動的に提供します。 SSO 役割割り当てはサイト・レベルで実行され、ストア・レベル

ではないことに注意してください (一般的なユーザー登録の場合)。したがって、指定されている storeAncestor 属性が、実際にサイトの祖先 (ストア 0) であることを確認する必要があります。

例:

```
<User registrationType="SSO" memberAncestor="o=Default Organization,o=Root Organization" storeAncestor="o=Root Organization"><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="o=Reseller Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="o=Seller Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="o=Supplier Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="ou=Supplier Hub Organization,o=Business Indirect Supplier Organization,
          o=Root Organization"/><BR>
  </User>
```

この例は、SSO によってシステムにアクセスするショッパーに 4 つの役割を付与します。

第 8 章 X.509 証明書の管理

WebSphere Commerce は、サイトと顧客の両方を保護するためのセキュリティー機構として、クライアント証明書ログオンをサポートしています。 X.509 証明書は、サイトに入る顧客の基本認証を補足する役目を果たします。この証明書を持っている顧客は、クライアント証明書認証に対応しているセキュアな WebSphere Commerce サイトにアクセスできます。

WebSphere Commerce インスタンスの作成時に、認証モードを選択します。認証モードには、基本と X.509 があります。デフォルトは、基本認証 (ログオン ID とパスワードを使ったログオン認証) です。 X.509 証明書を使ったログオン認証をアクティブにするには、 X.509 認証を選択します。

X.509 証明書を使用するには、 X.509 証明書の電子認証を扱う外部の認証局との信頼関係をまず確立する必要があります。 Web サーバーとして Netscape Enterprise を使用している場合は、Web サーバー上で X.509 証明書を使用可能にするためにさらに追加の手順を実行する必要があります。詳しい説明については、 Netscape Enterprise Server の資料を参照してください。

X.509 ユーザーには、 WebSphere Commerce アクセラレーターによってアクセスできます。管理者は X.509 証明書を使用可能にする前に、サーバー証明書によって認識され、ブラウザー上にインストールされているクライアント証明書が存在することを確認しなければなりません。そうでなければ、管理者はログオンできません。管理者が WebSphere Commerce 管理コンソールのログイン・ウィンドウに初めてアクセスすると、証明書ショッパー・レコードが作成され、ショッパー cookie が発行されます。これはちょうど、通常のショッパーがセキュアな URL にアクセスするときと同じです。管理者が正しい ID とパスワードを使って WebSphere Commerce 管理コンソールにログオンすると、管理者の cookie が発行され、ショッパーの cookie に取って代わります。その時点で管理者は、管理者ユーザー用と前のショッパー・ユーザー用の 2 つのユーザー・レコードを持つことになります。

次のような場合には、エラー・メッセージが表示されます。

- ユーザーの X.509 証明書がサイトで失効している場合
- ショッパーが WebSphere Commerce 内で固有の存在であることを保証するための必要情報がクライアント証明書に含まれていない場合

X.509 エラー・ビュー・タスクは、 `VIEWREG` データベース表に `X509 ErrorView` として登録されています。

X.509 証明書の使用可能化

WebSphere Commerce の作成時に、構成マネージャーを使って基本認証と X.509 認証のいずれかを選択します。デフォルトは、基本認証 (ログオン ID とパスワードを使った認証) です。

X.509 証明書を使った認証を使用可能にするには、以下のようにします。

1. 自分用の IBM HTTP Web サーバー SSL 証明書をセットアップします。 SSL サーバー証明書には、信頼関係を構築するためのクライアント認証局のリストが含まれています。場合によっては、クライアント認証局を追加する必要があります。
2. WebSphere Commerce 構成マネージャーを開始します。
3. **「インスタンス・プロパティー」 -> 「WebServer」**を選択します。
4. 認証モードの**「X.509」**ボックスにチェックマークを付けます。**「適用」**をクリックします。これで、X.509 クライアント証明書ユーザーが受け入れられるようになります。 X.509 認証モードを選択すると、 IBM HTTP Server の証明書サポートが自動的に有効になります。
5. WebSphere Commerce サーバーをいったん停止してから、再始動します。サーバーを再始動するまで、 WebSphere Commerce は X.509 ユーザーを `CERT_X509` 表に登録しません。

注: IBM HTTP Server では、 X.509 証明書をオプションにするか必須にするかを設定できます。

1. 構成ファイル `httpd.conf` をオープンして、 `SSLClientAuth` ディレクティブを見つけます。そのディレクティブを 1 (オプション) または 2 (必須) に設定します。推奨パラメーターは、*必須* です。
2. WebSphere Commerce Payments クライアントは SSL クライアント認証をサポートしていないので、 WebSphere Commerce Payments クライアントと Web サーバーとの間の SSL を使用不可にする必要があります。
   a. テキスト・エディターで、 `PaymentServlet.properties` ファイルをオープンします。このファイルは、 WebSphere Commerce Payments のインストール・ディレクトリーに入っています。
      - `UseNonSSLWCSClient` プロパティーを見つけます。このプロパティーを 1 に設定します。
      - このファイル内に `UseNonSSLWCSClient` プロパティーが存在しない場合は、以下の行を追加します。

        ```
        UseNonSSLWCSClient=1
        ```

   b. このファイルを保管し、エディターを終了します。
3. WebSphere Commerce Payments が WebSphere Commerce と同じマシンにインストールされている場合:
   a. 構成マネージャーを開始します。
   b. インスタンスを選択してから、**「Payments」**を選択します。
   c. **「非 SSL Payments クライアントを使用 (Use non-SSL Payments Client」**にチェックマークを付けます。これで、WebSphere Commerce Server クライアントは、 SSL を使用しないで WebSphere Commerce Payments と通信できるようになります。
   d. **「適用」**をクリックします。
   e. 構成マネージャーをクローズします。
4. WebSphere 管理コンソールから WebSphere Commerce Payments アプリケーション・サーバーを再始動します。

5. WebSphere 管理コンソールから WebSphere Commerce アプリケーション・サーバーを再始動します。

この点の詳細や、制限を設定するためのその他のオプションや、証明書用のフィルター・パラメーターについては、 IBM HTTP Server の資料を参照してください。

X.509 証明書ユーザーの状況の更新

サイト管理者は WebSphere Commerce アクセラレーターを使用して、 X.509 証明書ユーザーの状況を以下の 3 つの値のいずれかに更新できます。

有効 ユーザーは自分の証明書でセキュアな WebSphere Commerce サイトにアクセスできます。

失効 ユーザーは WebSphere Commerce サイトにアクセスできません。失効した証明書のユーザーがログオンしようとすると、 X.509 証明書エラー・ページが表示されます。

期限切れ
ユーザーは WebSphere Commerce サイトにアクセスできません。 期限切れの証明書のユーザーがログオンしようとすると、 X.509 証明書エラー・ページが表示されます。

X.509 証明書を管理するときに、証明書の所有者について制限やフィルター・パラメーターを設定したいと思うことがあります。たとえば、 `httpd.conf` 構成ファイルを変更して、セキュアなサイトにアクセスできる証明書所有者のタイプを制限するといったことが考えられます。

詳しい説明については、ご使用の Web サーバーの資料を参照してください。

標準的な認証シナリオ

X.509 証明書の標準的な認証シナリオは、次のような手順になります。

1. ショッパーによるアクセス:
   - `http://` 経由で非セキュアな URL にアクセスする場合

     認証は実行されません。
   - `https://` 経由でセキュアな URL にアクセスする場合

     ショッパーに対して、クライアント証明書を選択するための画面が表示されます。
   - URL コマンドのアクセス・モードが原因で、 URL コマンドが `https://` に転送される場合

     ショッパーに対して、クライアント証明書を選択するための画面が表示されます。
2. WebSphere Commerce サーバーはクライアント証明書の情報に基づいて、ショッパーが WebSphere Commerce の `SHOPPER` 表にすでに存在するかどうかを確認します。
   - ショッパーが存在しており、証明書状況が有効になっている場合、そのショッパーは認証され、ショッピング・フローが再開します。
   - ショッパーが存在しない場合:

– そのショッパーは WebSphere Commerce データベースに自動的に登録され、ショッピング・フローが再開します。

注: 証明書から取られるのは、 CERT_X509 表の情報だけです。ただし、ショッパーの住所情報があれば、その情報が X.509 クライアント証明書から取られることもあります。

第 3 部 セキュリティー許可の管理

第 3 部では、WebSphere Commerce サイト管理者が実行できるセキュリティー許可タスクについて説明します。

第 9 章 アクセス制御の概要

e-commerce の果たす役割により、会社がビジネスを行う方法が変わっただけでなく、会社が期待する会社と顧客との関係および会社とビジネス・パートナーとの関係の種類も大幅に増えました。 Web は、より一層の価値を既存の顧客に提供したり、インターネットの能力と改善された効率から益を受けることを強く望んでいる新しい顧客のために道を開く点で、重要な要因となっています。ビジネスを Web 上で行うことの明らかな利点や顧客ベースを増加させる途方もない可能性はありますが、同時に、高度にセキュアな環境を保守したり、適切なトランザクションを許可したり、作業プロセスを合理化する際に、ビジネス・フローおよび取引パートナーを管理しなければならないという課題も生じます。

アクセス制御の顕著な特徴は、これらの作業プロセスを監視する機能です。これは、ユーザーのアクティビティーや、ユーザーと会社の製品およびサービスとのビジネス相互関係に基づいて、ユーザーがシステムに参加する方法を管理することによって行われます。たとえば、ストアに登録済みの顧客だけが、ストアのオークション用の商品を表示したり、その商品に入札できるようにしたい場合もあるでしょう。同様に、グラフィック設計担当者には、ストア・ページのカスタマイズを許可する一方で、商品カタログの実際の内容の管理については制限することもできます。

WebSphere Commerce には、インスタンス作成時にシステムにロードされる 200 を超えるデフォルトのアクセス制御ポリシーが組み込まれており、アクセス管理用の適切なツールが用意されています。これらのポリシーは、ビジネスで必要な典型的なアクセス制御要件の多くに対処できるように設計されており、独自の e-commerce ソリューションに適するようにカスタマイズすることもできます。

電子マーケットでのアクティビティーへのアクセスを管理することは、会社の金融資産およびリソースを保護する際に不可欠であり、サイトの承認済みメンバー間のセキュアな商取引を保証したり、オンライン操作の適法性を検証することを目的としています。アクセス制御は e-commerce との関連において特に重要であり、e-commerce では、ビジネスに参加できるかどうかは、 Web 上で始まる顧客関係に大きく依存しています。

アクセス制御の意味

アクセス制御によって、ビジネス・ワークフローを管理し、ユーザーがその役割と責任に適したアクティビティーだけを実行するようにできます。 WebSphere Commerce は、「箱から出してすぐに」使用できるデフォルト・ポリシーを提供するだけではなく、ポリシーをビジネスの必要に合わせてカスタマイズするためのツールや能力も提供しています。

次の表は、単純な変更によって、ビジネス環境に合わせてアクセスをカスタマイズする方法をいくつか概説しています。

ユーザーがデフォルトで実行できること	ユーザーがカスタマイズ後に実行できること
顧客は自己登録できます。	セラー管理者だけが新しい顧客を登録できます。
バイヤーは自分が作成した RFQ を表示できます。	RFQ の結果が契約である場合、セラーだけが RFQ を表示できます。
オーダーが保留状態である場合、顧客だけが作成したオーダーをキャンセルできます。	商品価格の合計が 1000 ドル未満の場合、顧客サービス担当者も保留状態のオーダーをキャンセルできます。
オーダーは、そのオーダーを作成した人によって変更できます。	**購入者**の役割を持つバイヤー組織のユーザーだけが、作成されたオーダーを変更できます。
アカウント担当者はすべてのアカウントを表示できます。	アカウント担当者はアクティブ・アカウントだけを表示できます。
物流管理者役割を持つ従業員は、配送センターを作成および変更できます。	物流管理者役割を持つ従業員は、配送センターを作成できますが変更できません。

次の章では、組織とユーザーの作成方法、およびアクセス制御ポリシーの詳細を説明します。

第 10 章 始めに

前の章では、アクセス制御が e-commerce で果たす重要な役割、および Web を使ったビジネスの実行の効率と信頼性を改善する上でのかぎとなる利点について学びました。

この章では、WebSphere Commerce のアクセス管理の基本、たとえば組織とユーザーの定義、および組織およびユーザーがシステムを使って実行するアクティビティーを管理するために、アクセス制御ポリシーが使用される方法などを説明します。組織とユーザーをセットアップするために実行するステップを概説した後、アクセス制御ポリシーと、WebSphere Commerce でのその役割を詳しく見ていきます。

この章は、以下のセクションに分かれています。

- 組織およびユーザーの定義
- アクセス制御の理解
- アクセス制御の使用を開始する方法

組織およびユーザーの定義

サイト管理者の場合、WebSphere Commerce のインストールおよび構成後の最初のタスクの 1 つは、 e-commerce サイトへのアクセスをセットアップし、管理することです。これには、サイトに参加する組織の作成に加え、それらの組織のメンバーになるユーザーの定義が含まれます。 WebSphere Commerce 5.5 では、ビジネス・モデルが導入されています。インスタンスを作成したら、管理者が公開できるサンプル・ビジネス・モデルができます。これにより、組織の構造を設定します。ビジネス・モデルの詳細は、 19 ページの『ビジネス・モデル』を参照してください。

場合によっては、サイトに参加する組織はバイヤー組織であったり、その他の組織であったりするので、企業との間で企業対消費者の関係で契約している顧客を、サイトに登録することができます。企業間取引サイトまたは企業対消費者取引サイトのどちらを管理しているかに関係なく、サイトの組織構造を定義することは、メンバーからシステムへのアクセスのタイプを管理する上で重要です。

このセクションでは、サイトの構造を定義するために実行する必要のある、高レベルのステップを提供します。提供されるサンプル・ビジネス・モデルを使用する場合、次のアクセス制御のセクションに進むことができます。独自の組織構造を定義する場合、以下のステップを続けます。

組織、ユーザー、および役割の作成の詳細については、「Technical Library」ページにある次のオンライン・ヘルプを参照してください。

Business

```
http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html
```

Professional

```
http://www.ibm.com/software/webservers/commerce/wc_pe/lit-tech-general.html
```

さらに、「*WebSphere Commerce 基本*」を参照されることもお勧めします。ビジネス・モデル全体の概観は、それぞれ「*WebSphere Commerce ストア開発ガイド*」、および「*WebSphere Commerce サンプル・ストア・ガイド*」を参照してください。

セラー組織の定義

通常、セラー組織は WebSphere Commerce サイトに 1 つ以上のストアを所有します。セラー組織は、サブ組織または部門を持つことができ、それらは 1 つ以上のストアを所有できます。たとえば、ファッション用品を販売するサンプル・ストア InFashion には、レディース部門とメンズ部門があり、それぞれが個別のオンライン・ストアを持っているかもしれません。

これから、サブ組織を何ももっていないセラー組織をセットアップすると仮定します。セラー組織をセットアップするために、実行する必要のある事項を以下に概説します。

1. 新規の組織を作成します。新規の組織を作成する場合、その組織のプロファイルを作成します。プロファイルには、組織名、説明、住所、連絡先、および組織のタイプを含めます。
2. (オプション) セラー組織内で承認の必要なタスク、たとえばオーダー処理、またはユーザー登録などを定義します。このステップは、企業間取引サイトにのみ必要です。承認の詳細については、製品のオンライン・ヘルプを参照してください。
3. 新規の組織に役割を割り当てます。 組織が担うことのできる役割は、親組織に割り当てられている役割だけです。ルート組織は他のすべての組織の上位組織なので、ルート組織にはすべての役割を割り当てる必要があります。 WebSphere Commerce は、すぐに使用して開始できるデフォルトの役割のセットを提供しています。セラー組織を作成しているので、割り当てられる典型的な役割には、セラー管理者、セラーなどが含まれます。デフォルトの役割のリストについては、32 ページの『役割』を参照してください。
4. ユーザーを作成します。組織と同様、ユーザー名、連絡先情報、およびそのユーザーに割り当てられる役割を含む、各ユーザーのプロファイルを作成します。割り当てるとき、前のステップで組織に割り当てた役割のリストから役割を選択することができます。
5. 顧客が組織で管理しているストアでショッピングできるように、ポリシー・グループを新しい組織に割り当てます。必要になる代表的なポリシー・グループは、管理ポリシー・グループ、共通ショッピング・ポリシー・グループ、 B2C ポリシー・グループ、または B2B ポリシー・グループです。ポリシー・グループの詳細は、 229 ページの『デフォルトのアクセス制御ポリシーおよびグループ』を参照してください。

上記で概説したすべてのステップは、サイト管理者が、組織管理コンソールの「アクセス管理」メニューから実行できます。

注: WebSphere Commerce Professional Edition では、組織を作成できません。セラー組織はすでに作成されて用意されています。

バイヤー組織の定義

企業間取引サイトを実行している場合、そのサイトに 1 つ以上のバイヤー組織が所属できます。 (企業対消費者取引サイトを実行している場合は、個々のバイヤーをデフォルトの組織に登録します。) サイトでの購入関係に参加する企業を確立した後に、各企業ごとにバイヤー組織を作成する必要があります。必要に応じていくつでもバイヤー組織を作成することができます。

バイヤー組織は、構造的にセラー組織と似ています。セラー組織と同じように、バイヤー組織も、組織のための異なる購入アクティビティーを代表する、サブ組織または部門を持つことができます。

この例では、バイヤー組織にサブ組織がないものと仮定します。バイヤー組織をセットアップするために実行する必要のある事項を以下に概説します。

1. セラー組織を作成した場合と同じように、新しい組織を作成し、必要なら適切なタスクを定義します。適切なタスクの定義が必要なのは、企業間取引サイトだけです。
2. 新規のバイヤー組織に役割を割り当てます。今はバイヤー組織を作成しているので、割り当てられる典型的な役割には、バイヤー管理者、バイヤー (購買サイド)、バイヤー承認者などが含まれます。
3. ユーザーを作成し、ユーザーに役割を割り当てます。割り当てるとき、前のステップでバイヤー組織に割り当てた役割のリストから役割を選択することができます。
4. サイトに追加したいバイヤー組織ごとに手順全体を繰り返します。

注: 通常の環境では、バイヤー組織は、ルート組織が加入しているポリシー・グループを継承するので、ポリシー・グループに加入する必要はありません。

バイヤー組織についても、上記で概説したすべてのステップを、組織管理コンソールの「アクセス管理」メニューから実行します。

注: WebSphere Commerce Professional Edition では、すべての顧客はデフォルト組織に所属します。

アクセス制御の理解

e-commerce サイトに参加する組織とユーザーを定義すると、ポリシーのセット、つまり*アクセス制御* と呼ばれるプロセスを使って、そのアクティビティーを管理することができます。次のセクションでは、アクセス制御ポリシーとその基本構造を見ていきます。

アクセス制御ポリシーとは

アクセス制御ポリシーは、サイト上で特定のアクティビティーの実行を許可されている、ユーザーのグループを記述する規則のことです。これらのアクティビティーには、登録から、オークションの管理、商品カタログの更新、およびオーダーにおける承認、その他 e-commerce サイトで操作し、保守する必要のあるたくさんのアクティビティーが含まれます。

ポリシーとは、サイトに対するユーザーのアクセスを認可するものです。担当作業を実行する許可を 1 つ以上のアクセス制御ポリシーを通して受けない限り、ユーザーはサイトのどの機能にもアクセスできません。

アクセス制御ポリシーの作動方法

アクセス制御ポリシーは、アクセス・グループ、アクション・グループ、リソース・グループ、およびオプションの関係の 4 つの部分から構成されています。

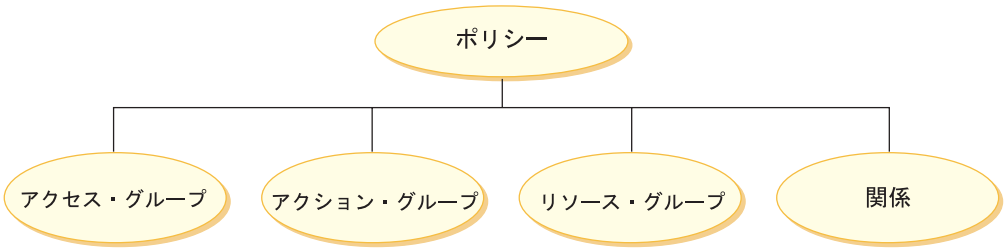
アクセス・グループ は、サイト上の機能のセットへの共通のアクセスを共用するユーザーのグループです。通常、アクセス・グループには、同じ役割、部門、またはスキル・セットなど、共通の属性を共用するユーザーが含まれます。

アクション・グループ とは、同じリソース上で動作できるアクションのグループのことです。一般的には、アクション・グループには、共通ビジネス・エリアと関連するアクション、またはサイト上の関連アクティビティーのセットが含まれます。

リソース・グループ には、ポリシーに制御されるリソースが含まれます。リソース・グループには、契約などのビジネス・オブジェクトや関連するコマンドのセットが含まれることがあります。

場合によっては、リソースは、そのリソースに*関係* のあるユーザーによってのみ動作することがあります。たとえば、契約を作成したユーザーだけが、その契約を変更することを許可される場合があります。

図 4. アクセス制御ポリシーの 4 つの部分



これらの 4 つの部分すべてが組み合わさって、ユーザー、ユーザーが取るアクション、そのアクションが実行されるビジネス・オブジェクトまたはコマンドのセット、およびオプションで、ユーザーのリソース・グループに対する関係を指定することにより、 WebSphere Commerce 内のポリシーを定義します。

アクセス・グループ、アクション・グループ、リソース・グループ、および関係の詳細については、 19 ページの『第 3 章 許可の概念』を参照してください。

アクセス制御の使用を開始する方法

場合によっては、何もする必要はありません。ビジネス・モデルを導入することにより、システム内に基本的なアクセス制御構造も用意されました。 WebSphere Commerce のデフォルト・ポリシーは、システム内の典型的なユーザーに基づくアクセス制御の基本構造と、組織内のユーザーの役割に関連する、ユーザーが実行するアクティビティーを提供するように設計されています。ポリシーは、メンバーシップ、オーダーの作成と処理、作業の流れの承認、オークションなどの取引、割り当て量や契約の要求を含む、共通のビジネス・アクティビティーを広範囲に渡って扱います。組織およびユーザーの定義後、デフォルト・ポリシーを提供された状態のままで使用するか、または個々の企業の必要に応じてカスタマイズして使用することができます。

しかし、デフォルト・ポリシーを使用するかカスタマイズするかを決定する前に、それらのポリシーが WebSphere Commerce でどのような構成になるかを理解することは重要です。デフォルト・ポリシーの詳細については、 46 ページの『ポリシーの詳細』を参照してください。

第 11 章 デフォルトのアクセス制御ポリシーのカスタマイズ

WebSphere Commerce が提供するデフォルトのアクセス制御ポリシーは、ユーザーに使用可能なアクションと情報を規制するために組織が持つ基本要件を対象にしています。多くの場合、デフォルト・ポリシーだけでサイトの必要を十分満たすかもしれません。同時に、デフォルト・ポリシーは非常にカスタマイズしやすいので、自分の要件に合わせて調整することができます。

SiteAdministratorsCanDoEverything ポリシーは、サイト管理者役割を持つ管理者にスーパーユーザー・アクセスを付与する特別なデフォルト・ポリシーです。このポリシーでは、サイト管理者は、たとえアクションやリソースが定義されていない場合であっても、どのリソースに対してもすべてのアクションを実行できます。この役割をユーザーに割り当てる場合は、この点に注意してください。

この章では、WebSphere Commerce に含まれるデフォルトのアクセス制御ポリシーに、基本的な変更を加えるための情報が提供されています。まず、理解する必要がある概念と関係を紹介します。

注: 分からない用語や概念が出てきたら、 19 ページの『第 3 章 許可の概念』を参照してください。

変更によって影響されるポリシーの識別

19 ページの『第 3 章 許可の概念』 では、ポリシーは通常、他のポリシーと関連していることを学びました。また、リソース・レベル・ポリシーを開始する方法と、それに関連する役割ベースのポリシーを識別する方法も理解しました。このセクションでは、ポリシーの相互関係、既存のポリシーの変更または新規のポリシーの作成前にその関係を理解する必要がある理由を、さらに詳しく説明します。多くの場合、変更を適切にインプリメントするには、いくつかのポリシーを変更する必要があります。

役割ベースのポリシーとリソース・レベル・ポリシー間の関係の理解

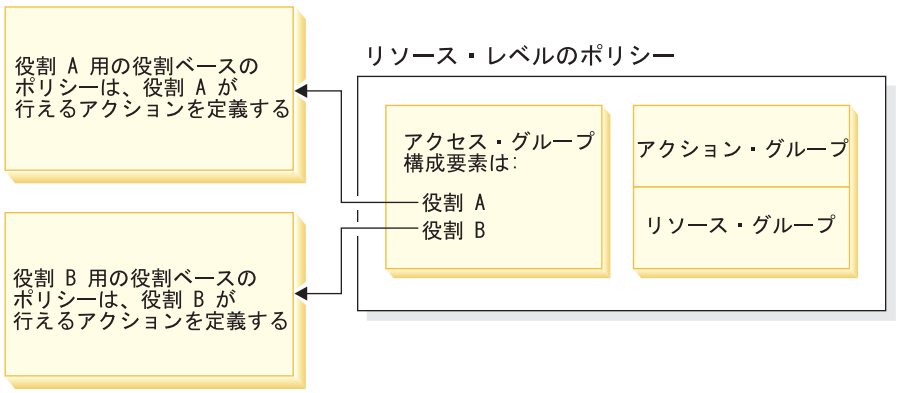
WebSphere Commerce では、ユーザーが行える各アクションは、次のように役割ベースのポリシーを使って 1 つ以上の役割に割り当てられます。

- 各デフォルト役割には、対応するアクセス・グループがあります。たとえば、役割「セラー」のアクセス・グループは Sellers です。
- 各「役割ベース」のアクセス・グループには、一般的には 2 つの関連する役割ベースのポリシーがあります。
  - 役割が実行する権限を持つコントローラー・コマンドを定義するポリシー。
  - 役割が実行する権限を持つ表示アクションを定義するポリシー。表示アクションは、VIEWREG テーブル内のビューにマップされます。たとえば、OperationalReportsHomeRHSView は、 セラーがアクセスする運用レポートがある Web ページを表示します。

一部のコマンドは、役割ベースのポリシーだけを持ち、リソース・レベル・ポリシーを持ちません。コマンドが保護可能リソースに対するものでない場合に、このようになります。たとえば、コマンド SetCurrencyPreferenceCmd は、このコマンドを実行しているユーザーの通貨設定を変更するだけなので、リソース・レベル・ポリシーは不要です。このコマンドが別のユーザーの通貨設定も変更できるとすれば、ユーザー・オブジェクトを保護する必要があり、リソース・レベル・ポリシーが必要となります。

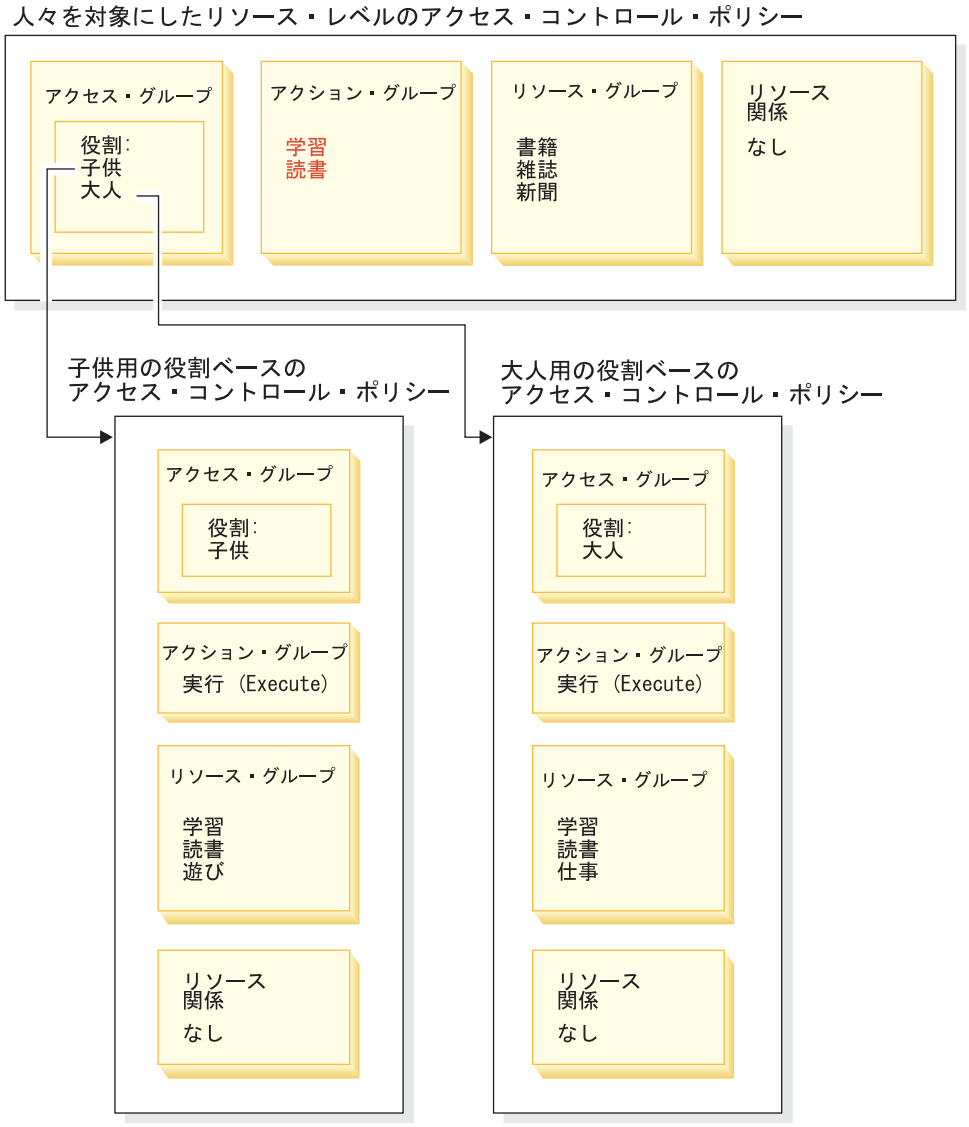
コントローラー・コマンドのリソース・レベル・ポリシーは、コントローラー・コマンドの特定の役割ベース・ポリシーに直接関連付けられています。リソース・レベル・ポリシーでは、コントローラー・コマンドはアクション・グループの一部ですが、役割ベースのポリシーでは、コントローラー・コマンドはリソース・グループの一部です。下の図は、この関係を例示しています。リソース・レベル・ポリシーには、そのアクセス・グループに役割 A と B が含まれており、これによって役割 A と B の役割ベースのポリシーが活動化します。リソース・レベル・ポリシーが役割 A または B を持つユーザーに、リソースの特定のセットでの特定のアクションを実行する権限を付与する一方、関連する役割ベースのポリシーは、役割 A および B を持つユーザーに、これらのアクションを一般的に実行する権限を提供します。

図 5. リソース・レベル・ポリシーと、それに関連した役割ベースのポリシー



次の図は、People アクセス・グループのユーザーに、特定のリソース、つまり書籍、雑誌、および新聞を読んだり学習したりする権限を与えるリソース・レベル・ポリシーのサンプルを示しています。役割が子供および大人の役割ベースのポリシーも、ユーザーに書籍、雑誌、および新聞を読んだり学習したりする権限を与えているので、このポリシーは正しく構成されていると言えます。

図 6. リソース・レベル・ポリシーと、それに影響する役割ベースのポリシー



コントローラー・コマンドの役割ベースのポリシーに関して、次のことに注目してください。

- アクション・グループには、Execute という 1 つのアクションしかありません。
- リソース・グループには、実行できるコントローラー・コマンドが含まれます。

同様に、ビューの役割ベースのポリシーに関しては次のことが言えます。

- アクション・グループには、実行できるビューが含まれます。
- リソース・グループには、com.ibm.commerce.command.ViewCommand という 1 つのリソースが含まれます。

一方、リソース・レベル・ポリシーに関しては次のことが言えます。

- アクション・グループには、リソース・グループのリソースで実行できる、アクションのセットがあります。
- リソース・グループには、実際のビジネス・リソースのリストがあり、そのリストで作業することができます。

リソース・レベル・ポリシーができるのは、対応する役割ベースのポリシーにより、すでに権限を与えられているアクションを実行する権限を、特定の役割のユーザーに与えることだけです。たとえば、上記の例では、役割**子供**は次のアクションを実行する権限があります。

- 学習
- 読書
- 遊び

リソース・レベル・ポリシーが、**仕事**という新しいアクションを含むように変更されたと仮定します。役割**大人**を持つユーザーは、アクション**仕事**を実行できるようになります。しかし、役割**子供**はそのアクションを実行できません。この理由は、2つの役割で役割ベースのポリシーを調べると明らかになります。 **大人**のポリシーは、リソース・グループにアクション**仕事**がリストされています。 **子供**のポリシーはリストされていません。 **子供**と**大人**の両方がリソース・レベル・ポリシーによって適切に権限を与えられていても、**子供**の役割ベースのポリシーがアクション**仕事**の権限を持っていません。

リソース・レベル・ポリシーが役割ベースのポリシーに結び付けられる方法のため、特定の変更の影響を受けるすべてのポリシーを追跡する最善の方法は、リソース・レベル・ポリシーから逆方向に作業することです。最初のステップとして、リソース・レベル・ポリシーのアクセス・グループを調査し、何らかの役割を持っているかどうかを判別します。組織管理コンソールから、「アクセス管理」>「役割」を選択すると、デフォルト役割の完全なリストを表示できます。

リソース・レベル・ポリシーのアクセス・グループに役割が含まれる場合、その役割ベースのポリシーを確認して、変更の必要があるかどうか調べてください。リソース・レベル・ポリシーのアクション・グループにアクションを追加している場合、関連する役割ベースのポリシーも、新しいアクションを許可していることを確認する必要があります。リソース・レベル・ポリシーからアクションを削除している場合で、このアクションを参照している他のリソース・レベル・ポリシーがない場合は、関連した役割ベースのポリシーから対応するリソースを削除するのが最善です。

ポリシー・モデルの理解

ユーザーがアクションを実行するためには、許可するためのポリシーが存在していなければなりません。しかし WebSphere Commerce では、必要な許可を与える**何らかの**ポリシーがあれば、ユーザーはアクションを実行できます。そのため、デフォルトよりも制限の厳しいポリシーを新規に定義した場合、より緩やかなデフォルト・ポリシーを削除または変更して、それが新規のポリシーをオーバーライドすることがないようにしなければなりません。

たとえば、デフォルト・ポリシー A は、すべての登録済みユーザーにオークションの入札を送信する許可を与えると想定します。このポリシーを変更して、オークションの入札をバイヤーの役割を持つユーザーだけに限定したい場合を考えます。バイヤーにオークションの作成を許可する新規のポリシーを定義するだけでは、その新規のポリシーには効果がありません。デフォルト・ポリシー A が、まだすべての登録済みユーザーに入札を許可しているからです。新規のポリシーを有効にするには、より緩やかなデフォルト・ポリシーを削除する必要があります。

以下の表は、リソース・レベルのポリシーを作成、削除、または変更するときに必要な追加の変更を要約しています。

表 9. 役割を使用するリソース・レベルのポリシーを変更する場合に必要な追加の変更

リソース・レベルのポリシーに移動します。	**リソース・レベルのアクセス・グループが役割を使用しているときは、変更が必要です。**
アクションをポリシーのアクション・グループに追加します。	該当する役割ベースのポリシーがそのリソース・グループにアクションを含んでいることを確認します。
アクションをポリシーのアクション・グループから除去します。	追加の変更は必要ありません。 整合性を保つために、関連した役割ベースのポリシー内の対応するリソース・グループからこのアクションを除去する方がよいでしょう。これは、このアクションを参照している他のアクション・グループがない場合にのみ行うべきです。他のアクション・グループがこのアクションを参照している場合は、このアクションをリソース・グループ内に持っていなければならない役割ベースのポリシーが存在する可能性があります。
異なるアクション・グループを使用します。	該当する役割ベースのポリシーがそのリソース・グループに新規のアクション・グループのアクションを含んでいることを確認します。
役割をポリシーのアクセス・グループに追加します。	新規の役割に対応する役割ベースのポリシーが、リソース・レベル・ポリシーで指定されたアクションを含むリソース・グループを参照するようにしてください。
役割をポリシーのアクセス・グループから除去します。	追加の変更は必要ありません。 整合性を保つために、対応する役割ベースのポリシーがリソース・グループ内でこれらのアクションを参照することがないように、対応する役割ベースのポリシーを変更する方がよいでしょう。
異なるアクセス・グループを使用します。	該当する役割ベースのポリシーがそのリソース・グループ内に、リソース・レベルのポリシーのアクション・グループ内のアクションを含んでいることを確認します。
新規のポリシーを作成します。	同じアクションを許可する既存のポリシーが存在するかどうかを調べます。必要であれば、それを削除します。
そのポリシーを削除します。	ユーザーがそのポリシーのアクションを実行しないようにするため、同じアクションを許可する他のポリシーをすべて削除します。

ポリシーが役割ベースかリソース・レベルかの判断

役割ベースのポリシーは、コマンドのセットを実行するための特定の役割をユーザーに許可するので、コマンド・レベルのポリシーとしても知られています。リソース・レベルのポリシーは、特定のセットのリソースに対してコマンドのセットを実行する許可をユーザーのグループに与えます。たとえば、役割ベースのポリシーは子供たちに食べる許可を与えます。それに対して、リソース・レベルのポリシーは子供たちに米を食べる許可を与えます。

通常はポリシーの名前から、それが役割ベースのポリシーかリソース・レベルのポリシーかを判別できます。

役割ベースのポリシー

役割が実行できるコントローラー・コマンドを定義するポリシーは、以下の命名規則に従います。

<AccessGroupforRoleXYZ> Execute <XYZCmdResourceGroup>

たとえば、ProductManagersExecuteProductManagersCmdResourceGroup となります。

コントローラー・コマンド用の役割ベースのポリシーでは、アクション・グループに Execute と呼ばれる単一の項目が含まれ、リソース・グループにその役割を持つユーザーが実行できる WebSphere Commerce コマンドのリストが含まれます。

役割が実行できるビューを定義するポリシーは、以下の命名規則に従います。

<AccessGroupforRoleXYZ> Execute <XYZViews>

たとえば、SalesManagersExecuteSalesManagersViews となります。

リソース・グループには、com.ibm.commerce.command.ViewCommand という 1 つのリソースが含まれます。

リソース・レベルのポリシー

データ・リソース (作成または操作が可能なビジネス・オブジェクト) に対してアクションを実行できるユーザーを定義するポリシーは、以下の命名規則に従います。

<AccessGroupXYZ> Execute <XYZCommands> On <XYZResource>

たとえば、AllUsersExecuteOrderProcessOnOrderResource となります。

リソース・レベルのポリシーでは、アクション・グループには WebSphere Commerce コマンドが含まれ、リソース・グループは適用対象とすることができる特定のビジネス・リソースを識別します。

1 つの例外は、オーダー、入札、または RFQ などのエンティティーの作成を許可するポリシーです。これらのポリシーは、エンティティー自体がまだ作成されていないので、そのエンティティーに適用されることはありません。代わりに、これらのポリシーは包含するエンティティーに対して適用されます。たとえば、オークションがストアのコンテキスト内に作成される場合、ユーザーは組織のコンテキスト内に作成されます。ほとんどのリソースはストアのコンテキスト内に作成されます。そのため、ポリシーには以下のような名前があります。

<AccessGroupXYZs> Execute <XYZCommands> On <StoreEntityResource>

たとえば:

AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource

Data Bean リソース (Data Bean には、通常は JSP で使用される入札やオーダーなどのデータ・リソースに関する情報が含まれています) を表示できるユーザーを定義するポリシーは、以下の命名規則に従っています。

<AccessGroupXYZs> Display <XYZDatabeanResourceGroup>

たとえば、MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup となります。

デフォルト・ポリシーを変更するためのヒント

デフォルト・ポリシーを変更する場合は、以下の事柄に注意してください。

- ほとんどのアクセス・グループは、バイヤーやプロダクト・マネージャーなどのユーザー役割によって定義されます。これらの役割について、およびそれらが実行できるアクションについてさらに知るためには、 32 ページの『役割』を参照してください。
- 異なるアクセス・グループを使用できるようにポリシーを変更する前に、そのアクセス・グループの定義を再検討して、それが必要にかなっていることを確認してください。これを行うには、組織管理コンソールから**「アクセス管理」>「アクセス・グループ」**を選択します。
- 「ビュー」で選択した値に応じて、「ポリシー」ページには、選択した組織によって所有されるポリシーがリストされます。これは、サイト・レベルのポリシーと、特定の組織に固有のポリシーとを区別しません。
- 変更するデフォルト・ポリシーを名前変更して、ポリシー名がポリシーの動作を反映して、変更済みデフォルト・ポリシーを識別できるようにします。カスタマイズしたポリシーが命名規則をインプリメントすることを検討してください。適切であれば、ポリシーの説明とその表示名も変更します。

注: 「アクセス制御ポリシー」メニューは、組織管理コンソールに移動しています。組織管理コンソールでは、アクセス制御ポリシー定義とアクセス・グループ定義に対する簡単な変更しか行えません。より強力なソリューションとして、XML ファイルを使用してデータを更新する方法があります。以下の操作は、XML によってしか行えません。

1. 新しいアクション、リソース、属性、関係、関係グループの定義。
2. 複合暗黙リソース・グループと、複合暗黙アクセス・グループの定義。
3. 新規ポリシーのポリシー・グループへの割り当て。

ポリシーの変更後に

新規ポリシーは、作成後にポリシー・グループに割り当ててから有効になります。新規ポリシーは、そのポリシーの目的に適したグループに割り当てる必要があります。ポリシー・グループ名の詳細については、 229 ページの『デフォルトのアクセス制御ポリシーおよびグループ』を参照してください。

アクセス制御ポリシーを作成または変更するたびに、特定のテストを実行してポリシーが適正に作動していることを確認する必要があります。現在データベース内にある新規のポリシーおよび変更されたポリシーすべてをテストした後、その情報を抽出して XML ファイルに入れる方がよいでしょう。 これらのファイルの形式は、初期アクセス制御ポリシーに関連したファイル (defaultAccessControlPolices.xml、defaultAccessControlPolicies_locale.xml、および ACUserGroup_locale.xml) の形式と同じです。このステップが必要なのは、管理コンソールからの変更はデータ

ベースに保管されているポリシー情報だけに影響を与えるためです。 インスタンス作成中にデフォルトのアクセス制御ポリシーとそのコンポーネントをロードするために使用された XML ファイルが、自動的に更新されることはありません。

以下に示すいくつかの理由により、XML ファイルとデータベース内のアクセス制御情報との間の整合性を保つ必要があります。

- WebSphere Commerce のインスタンスを作成するとき、ポリシーおよびアクセス・グループ定義は XML ファイルからロードされます。
- XML ファイルはポリシーとそのコンポーネント・パーツを直接表示して編集するための便利な手段となるので、それらのファイルを最新の状態に保守することは大切です。

ポリシー変更のテスト

ポリシーごとに、以下の点を確認してください。

- ポリシーのアクセス・グループに属するユーザーが、指定のリソースに対して指定のアクションを実行できること。アクションを実行する許可を除去した場合、ユーザーがアクションを実行できなくなっていることもテストする必要があります。
- ポリシーのアクセス・グループに属していないユーザーは、指定のリソース上で指定のアクションを実行できないこと。

たとえば、第 5 章のオークション・カスタマイズ・シナリオ 1 をインプリメントして、オークション管理者からオークション入札をクローズする権限を除去したと想定します。この変更が正常に機能しているかどうかをテストするには、 **オークション管理者**アクセス・グループに属するユーザーとしてログインしてから、以下のアクションを実行します。

- オークションの変更
- オークションの削除

さらに、オークション管理者が入札をクローズできないことも確認する必要があります。

その後、**オークション管理者**アクセス・グループに属さないユーザーとしてログインしてから、同じアクションの実行を試行します。ポリシーが正常に機能していれば、その試行は失敗するはずです。

ポリシーの変更を XML ファイルに抽出する

ポリシーの変更を完了してテストした後、 XML ファイルを更新してデータベース内のポリシー情報と同期させてください。アクセス制御ポリシーとアクセス・グループに関連した別の XML ファイルについては、 151 ページの『第 13 章 XML を使用したアクセス制御ポリシーのカスタマイズ』を参照してください。これには、ポリシーの変更をデータベースから抽出して XML ファイルに入れる方法と、ポリシー情報を XML ファイルから取り出してデータベースにロードする方法についての説明もあります。

第 12 章 GUI を使用したアクセス制御ポリシーのカスタマイズ

これまでアクセス制御ポリシーについて学習した事柄を応用しながら、以下に示すシナリオに沿って、 GUI からデフォルト・ポリシーにさまざまな基本変更を行ってみましょう。高度な変更を加えたい場合は、XML を使用する必要があります。151 ページの『第 13 章 XML を使用したアクセス制御ポリシーのカスタマイズ』を参照してください。

これらのすべてのシナリオでは、サイト管理者がルート組織のポリシーを変更すると想定しています。いくつかのシナリオを体験することにより、同じ方法を使用して、ここでは特に取り上げられていない変更を行うことが可能になります。

以下のシナリオはビジネス領域に応じて編成されています。それぞれのビジネス領域では、次第に複雑になるような順序でシナリオが示されています。

表 10. シナリオの目次

ビジネス領域	開始ページ
オークション	118 ページの『オークション・シナリオ 1: オークション管理者からオークション入札をクローズする権限を除去する』
契約	122 ページの『契約シナリオ 1: 契約マネージャーから契約に付加項目を追加または削除する権限を除去する』
オーダー	125 ページの『オーダー・シナリオ 1: バイヤーだけにオーダーの作成を許可する』
メンバーシップ	132 ページの『メンバーシップ・シナリオ 1: ユーザーが自己登録できないようにする』
クーポン	137 ページの『クーポン・シナリオ 1: バイヤーだけがクーポンを使用できるようにする』
調達	141 ページの『調達シナリオ 1: 調達ショッピング・カート管理者が、組織によって作成されるオーダー用の調達ショッピング・カートを管理できるようにする』
在庫	145 ページの『在庫シナリオ 1: 配送センター管理者が配送センターを更新できるが削除できないようにする』
ビジネス・インテリジェンス	147 ページの『ビジネス・インテリジェンス・シナリオ 1: 監査者がビジネス・インテリジェンス・レポートを参照できるようにする』

特定の種類の変更を例示するシナリオを探している場合、例示されるカスタマイズのタイプに応じてシナリオを相互参照している 118 ページの表 11 を参照してください。

表 11. カスタマイズのタイプに応じて編成されたカスタマイズ・シナリオ

カスタマイズ	参照ページ
役割をポリシーのアクセス・グループに追加する	139
ポリシーのアクション・グループを変更する	142,145
ポリシーのリソース関係を変更する	127,141
異なるアクセス・グループを使用するようにポリシーを変更する	120,125,127,133,137,139
新規のアクセス・グループを作成してポリシー内で使用する	130,134
新規のアクション・グループを作成してポリシー内で使用する	134,142
新規のリソース・レベルのポリシーを作成する	123,143
新規の役割ベースのポリシーを作成する	134,147
新規の役割を作成してリソース・レベルのポリシー内で使用する	134,147
ポリシーを削除する	119,132
アクションをポリシーのアクション・グループから除去する	3,122

オークション・シナリオ 1: オークション管理者からオークション入札をクローズする権限を除去する

デフォルトでは、ストアのオークション管理者はストアのオークションを変更または削除すること、および入札をクローズすることができます。場合によっては、入札をクローズするアクションを他の人が行うようにするため、またはストアでそのアクションが必要ないために、オークション管理者に入札をクローズする権限を付与したくないことがあります。

このシナリオでは、オークション管理者から入札をクローズする権限を除去します。この変更を実現するために、以下のようにします。

1. 付録を参照して、オークション管理者が実行できるアクションを定義するリソース・レベルのポリシーを見つけます。
2. そのポリシーのアクション・グループの名前を判別します。
3. ポリシーのアクション・グループから、オークション入札をクローズするアクションを削除します。

実行するステップ

アクション・グループを変更しなければならないポリシーを識別する

1. 付録の『オークション』を参照して、変更するリソース・レベルのポリシーを識別します。そのポリシーは以下のとおりです。

   ```
   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。

3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。
5. ポリシーのアクション・グループの名前 AuctionManage を書き留めます。これが、入札をクローズするアクションを除去するために変更しなければならないアクション・グループです。

ポリシーのアクション・グループから、入札をクローズするアクションを除去する

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**AuctionManage** を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。
4. 「選択したアクション」リストから、**「com.ibm.commerce.negotiation.commands.CloseBiddingCmd」** を選択します。
5. **「除去」**をクリックします。
6. **「OK」**をクリックします。

ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

オークション・シナリオ 2: オークション・マネージャーから入札を撤回する権限を除去する

デフォルトでは、ストアのオークション・マネージャーはオークションで送信された入札を撤回することができます。場合によっては、この権限を誰にも付与したくないことがあります。この変更を行うには、誰が入札を撤回して削除できるかを定義するリソース・レベルのポリシーを見つける必要があります。

オークション・シナリオ 1 では、入札のクローズというアクションが、ポリシーに含まれるいくつかのアクションの 1 つでした。したがって、必要なのはそのアクションをポリシーのアクション・グループから除去することだけです。しかしこのシナリオでは、ポリシー全体が入札の撤回を制御しています。そのため、アクションだけでなくポリシーを削除する必要があります。

ポリシーを削除するには、以下を行う必要があります。

- 付録を参照して、オークション・マネージャーによるオークション入札の撤回を範囲に含むリソース・レベルのポリシーを見つけます。
- そのポリシーを削除します。

注: ポリシーを削除する前に、その名前、アクセス・グループ名、リソース・グループ名、およびアクション・グループ名を書き留めて、次回のシナリオでこのポリシーを再作成できるようにしてください。

実行するステップ

1. 付録の『オークション』を参照して、変更するリソース・レベルのポリシーを識別します。そのポリシーは以下のとおりです。

   AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、以下を選択します。

   AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. **「削除」**をクリックします。

ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。
5. **「アクセス制御ポリシー・グループ・レジストリー (Access Control Policy Groups Registry)」**で、ステップ 3 と 4 を繰り返します。

オークション・シナリオ 3: オークションの入札をバイヤーに制限する

デフォルトでは、すべての登録済みユーザーが組織内での地位に関係なくストアでオークション中の商品に対して入札することができます。場合によっては、入札を WebSphere Commerce でバイヤー役割に割り当てられたユーザーなど特定のグループのユーザーに制限したいことがあります。

このシナリオでは、リソース・レベルのポリシーおよび関連した役割ベースのポリシーを変更します。入札をバイヤー役割のある購買組織のメンバーに制限するには、以下のようにする必要があります。

- 付録を参照して、オークション入札を誰が作成できるかを指定するリソース・レベルのポリシーを見つけます。
- ポリシーのアクセス・グループを、登録されているすべてのユーザーから、バイヤー役割を持つユーザーに変更します。
- ポリシー、説明、および表示名を名前変更します。
- 入札を作成するコマンドを識別します。
- 付録を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見つけます。このポリシーは、バイヤー (購買サイド) の役割を持つユーザーが実行できるコマンドを定義します。入札を作成するコマンドの実行をバイヤーに許可するためには、このポリシーのリソース・グループを更新しなければなりません。
- この役割ベースのポリシーのリソース・グループを更新して、入札を作成するコマンドを含むようにします。

実行するステップ

リソース・レベルのポリシーを識別する

1. 付録の『オークション』を参照して、変更するリソース・レベルのポリシーを識別します。ポリシーは、RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource です。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、**「RegisteredApprovedUsersExecuteBidCreateCommandsOnAuction Resource」** を選択します。
5. ポリシーのアクション・グループの名前 BidCreate を書き留めます。これが、入札を作成するコマンドの名前を見つけるために表示しなければならないアクション・グループです。

ポリシーのアクセス・グループを変更する

1. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。
2. 「ユーザー・グループ」で、**「検索」**をクリックして**「バイヤー (購買サイド)」**を選択します。
3. **「OK」**をクリックします。
4. ポリシー、表示名、およびポリシーの説明のテキストを編集して名前変更します。
5. **「OK」**をクリックします。

入札を作成するコマンドの識別

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**BidCreate** を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。入札を作成するコマンド名 com.ibm.commerce.negotiation.commands.BidSubmitCmd を書き留めます。このコマンドを、バイヤーが実行できるコマンドのリストを含むリソース・グループに追加しなければなりません。

バイヤー (購買サイド) 役割の役割ベースのポリシーおよびリソース・グループを識別する

1. 付録の『役割ベースのポリシー』を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見つけます。そのポリシーは以下のとおりです。

   Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
2. **「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. リソース・グループの名前 Buyers(buy-side)CommandsResourceGroup を書き留めます。これで、更新する必要のあるリソース・グループの名前が判明しました。

役割ベース・ポリシーのリソース・グループを更新して、入札を作成するコマンドを組み込む

1. **「アクセス管理」>「リソース・グループ」**をクリックします。
2. **「Buyers(buy-side)CommandsResourceGroup」**を選択します。
3. **「変更」**をクリックして、「リソース・グループの変更」ページを表示します。
4. **「次へ」**をクリックして、「詳細情報」ページを表示します。
5. 「使用可能なリソース」リストから、**「com.ibm.commerce.negotiation.commands.BidSubmitCmd」** を選択します。これが入札を作成するコマンドです。
6. **「追加」**をクリックして、コマンドをリソース・グループに追加します。
7. **「終了」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

契約シナリオ 1: 契約マネージャーから契約に付加項目を追加または削除する権限を除去する

デフォルトでは、ストアの契約マネージャーは管理する契約に付加項目を追加または削除することができます。場合によっては、この権限を契約マネージャーに付与したくないことがあります。

このシナリオでは、契約マネージャーが実行できるアクションを定義するリソース・レベルのポリシーを変更します。契約に付加項目を追加または削除する契約マネージャーの権限を除去するには、以下のようにする必要があります。

- 付録を参照して、契約マネージャーが実行できるアクションを定義するリソース・レベルのポリシーを見つけます。
- そのポリシーのアクション・グループの名前を判別します。
- ポリシーのアクション・グループ内にあるアクションのリストから、付加項目を追加するアクションおよび付加項目を削除するアクションを削除します。

実行するステップ

リソース・レベルのポリシーおよびアクション・グループを識別する

1. 付録の『契約』を参照して、変更するリソース・レベルのポリシーを識別します。そのポリシーは以下のとおりです。

   ```
   ContractManagersForOrgExecuteContractManageCommandsOnContractResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。

5. ポリシーのアクション・グループの名前 — ContractManage を書き留めます。これが、付加項目を追加および削除するアクションを除去するために変更しなければならないアクション・グループです。

ポリシーのアクション・グループから付加項目を追加または削除するアクションを除去する

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**ContractManage** を選択します。
3. **「変更」**をクリックして、「リソース・グループの変更」ページを表示します。
4. 「選択したアクション」リストから、以下のアクションを選択します。
   「com.ibm.commerce.contract.commands.ContractAttachmentAddCmd」
   「com.ibm.commerce.contract.commands.ContractAttachmentDeleteCmd」
5. **「除去」**をクリックします。
6. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

契約シナリオ 2: 契約オペレーターと契約管理者の両方に契約をデプロイすることを許可する

デフォルトでは、ストアの契約オペレーターが契約をデプロイすることができます。場合によっては、この権限を契約管理者にも付与したいことがあります。

アクセス制御ポリシーの設計が柔軟であるため、この変更をいくつかの方法で実現することができます。

- 契約オペレーターおよび契約管理者の両方を含む新規のアクセス・グループを作成して、誰が契約をデプロイできるかを定義するポリシーにその新規のアクセス・グループを割り当てることができます。
- 契約のデプロイ (deploy contract) アクションを、契約管理者が実行できるアクションを指定するポリシーに追加することができます。
- 契約管理者に契約のデプロイを許可する新規のポリシーを作成することができます。

このシナリオは、3 番目のアプローチを例示しています。これは、契約管理者に契約のデプロイを許可する新規のリソース・レベルのポリシーを作成する方法を示しています。

ポリシーを作成するには、以下のようにする必要があります。

- 付録を参照して、契約オペレーターに契約のデプロイを許可するリソース・レベルのポリシーを見つけます。
- このポリシーのアクション・グループの名前を書き留めます。

- このポリシーのリソース・グループの名前を書き留めます。
- 契約オペレーターに契約のデプロイを許可するポリシーからアクション・グループおよびリソース・グループを指定して、 契約管理者アクセス・グループのポリシーを新規に定義します。

実行するステップ

新規のポリシー内で使用するアクション・グループおよびリソース・グループを識別する

1. 付録の『契約』を参照して、契約オペレーターに契約のデプロイを許可するリソース・レベルのポリシーを見つけます。ポリシーは、ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource です。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。
5. ポリシーのアクション・グループの名前 — ContractDeploy を書き留めます。これが、新規のポリシーを定義するために使用しなければならないアクション・グループです。
6. リソース・グループの名前 —ContractDataResourceGroup を書き留めます。これが、新規のポリシーを定義するために使用しなければならないリソース・グループです。

新しいポリシーの定義

1. **「新規」**をクリックして、「新規のポリシー」ページを表示します。
2. 「名前」には、以下を指定します。

   ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource
3. 「表示名」に、ポリシーの簡単な説明をご使用の言語で指定します。
4. 「説明」に、ポリシーの詳しい説明をご使用の言語で入力します。
5. 「ユーザー・グループ」では、**「検索」**をクリックして、**「ContractAdministratorForOrg」** を選択します。
6. **「OK」**をクリックします。
7. 「リソース・グループ」では、**「ContractDataResourceGroup」** を選択します。
8. 「アクション・グループ」では、**「ContractDeploy」** を選択します。
9. 「ポリシーのタイプ」で、**「グループ可能化テンプレート・ポリシー (Groupable Template Policy)」**を選択して、ポリシーをテンプレート・ポリシーとして指定します。
10. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。

3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

注: この新規ポリシーは、ポリシー・グループに割り当てられてから有効になります。ポリシーの割り当ては、XML を使用して実行する必要があります。

オーダー・シナリオ 1: バイヤーだけにオーダーの作成を許可する

デフォルトでは、組織内の地位に関係なくすべてのユーザーが商品のオーダーを作成することを許可されています。場合によっては、オーダーを作成する許可を、購買組織の従業員などの限定されたグループのユーザーに制限することもできます。通常、これらの従業員には、購買組織のバイヤー (購買サイド) の役割が割り当てられます。

オーダーの作成を**バイヤー**の役割を持つユーザーに限定するには、以下のようにする必要があります。

- 付録を参照して、オーダーを作成できる人を指定しているリソース・レベル・ポリシーを見つけます。
- ポリシーのアクセス・グループを、すべてのユーザーから**バイヤー**の役割のユーザーに変更します。
- ポリシーの名前、表示名、および説明を更新します。
- オーダー作成用のコマンドを識別します。
- 付録を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見つけます。このポリシーは、バイヤー (購買サイド) の役割を持つユーザーが実行できるコマンドを定義します。バイヤーがオーダー作成用のコマンドを実行することを許可するには、このポリシーのリソース・グループを更新しなければなりません。
- この役割ベースのポリシーのリソース・グループを更新して、オーダー作成用のコマンドを組み込みます。

実行するステップ

リソース・レベルのポリシーを識別する

1. 付録の『オーダー』を参照して、変更するリソース・レベル・ポリシーを識別します。ポリシーは `AllUsersExecuteOrderCreateCommandsOnStoreResource` です。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、**「AllUsersExecuteOrderCreateCommandsOnStoreResource」**を選択します。 ポリシーのアクション・グループ `OrderCreateCommands` の名前を記録します。このアクション・グループは、オーダー作成用のコマンドの名前を検索する際に表示する必要があります。

アクセス・グループを変更する

1. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。

2. 「ユーザー・グループ」で、**「検索」**をクリックして**「バイヤー (購買サイド)」**を選択します。
3. **「OK」**をクリックします。
4. アクセス・グループの変更を反映するように、ポリシーの名前、表示名、および説明を更新します。
5. **「OK」**をクリックします。

オーダー作成用のコマンドの識別

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**「OrderCreateCommands」**を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。オーダー作成用のコマンドの名前を記録します。

   ```
   com.ibm.commerce.order.commands.OrderCopyCmd
   com.ibm.commerce.order.commands.OrderScheduleCmd
   com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
   com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
   com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
   ```

   これらのコマンドを、バイヤーが実行できるコマンドのリストを含むリソース・グループに追加しなければなりません。

   注: コマンド
   `com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd` は必要ありません。

バイヤー (購買サイド) の役割ベースのポリシーを識別する

1. 付録の『役割ベースのポリシー』を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見つけます。ポリシーは `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup` です。
2. **「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. リストからポリシーを探します。
5. リソース・グループの名前 —`Buyers(buy-side)CommandsResourceGroup` を書き留めます。 これは、更新の必要なリソース・グループです。

役割ベースのポリシー内のリソース・グループを更新して、オーダー作成用コマンドを組み込む

1. **「アクセス管理」>「リソース・グループ」**をクリックします。
2. リソース・グループのリストから、**「Buyers(buy-side)CommandsResourceGroup」**を選択します。
3. **「変更」**をクリックして、「リソース・グループの変更」ページを表示します。
4. **「次へ」**をクリックして、「詳細情報」ページを表示します。

5. 「使用可能なリソース」リストから、以下のコマンドをオーダー作成用コマンドとして選択します。

```
com.ibm.commerce.order.commands.OrderCopyCmd
com.ibm.commerce.order.commands.OrderScheduleCmd
com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
com.ibm.commerce.orderitems.commands.OrderItemAddCmd
com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
```

6. **「追加」**をクリックします。
7. **「終了」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

オーダー・シナリオ 2: バイヤー管理者だけがオーダーを変更できるようにする

注: このシナリオは、WebSphere Commerce Professional Edition には適用されません。

デフォルトでは、組織内の地位に関係なくすべてのユーザーが、作成済みのオーダーを変更することを許可されています。場合によっては、オーダーを変更する許可を、組織のバイヤー管理者だけに制限することもできます。

このシナリオでは、リソース・レベル・ポリシーと役割ベースのポリシーを変更します。バイヤー管理者だけがバイヤー組織のメンバーに属するオーダーを変更できるようにするには、以下のようにする必要があります。

- 付録を参照して、オーダーを変更できる人を指定しているリソース・レベル・ポリシーを見つけます。
- ポリシーのアクセス・グループを、すべてのユーザーから `buyer administrator` の役割のユーザーに変更します。
- リソース関係の指定を除去して、バイヤー管理者が他のユーザーに属するオーダーを変更することを許可します。
- ポリシーの名前、表示名、および説明を更新します。
- オーダー変更用のコマンドを識別します。
- 付録を参照して、バイヤー管理者の役割ベースのポリシーを見つけます。このポリシーは、バイヤー管理者の役割のユーザーが実行できるコマンドを定義します。バイヤー管理者がオーダー変更用のコマンドを実行することを許可するには、このポリシーのリソース・グループを更新しなければなりません。
- 役割ベースのポリシーのリソース・グループを更新して、オーダー変更用のコマンドを組み込みます。

実行するステップ

リソース・レベルのポリシーを識別する

1. 付録の『オーダー』を参照して、変更するリソース・レベル・ポリシーを識別します。ポリシーは AllUsersExecuteOrderWriteCommandsOnOrderResource です。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、**「AllUsersExecuteOrderWriteCommandsOnOrderResource」**を選択します。
5. ポリシーのアクション・グループ OrderWriteCommands の名前を記録します。このアクション・グループは、オーダー作成用コマンドの名前を検索する際に表示する必要があります。

アクセス・グループを変更する

1. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。
2. 「ユーザー・グループ」で、**「検索」**をクリックして、**「バイヤー管理者 (Buyer Administrators)」**を選択します。
3. **「OK」**をクリックします。
4. 「関係」で**「なし」**を選択します。
5. アクセス・グループの変更を反映するように、ポリシーの名前、表示名、および説明を更新します。
6. **「OK」**をクリックします。

オーダー変更用のコマンドの識別

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**「OrderWriteCommands」**を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。オーダー変更用のコマンドの名前を記録します。

```
com.ibm.commerce.order.commands.OrderCancelCmd
com.ibm.commerce.order.commands.OrderCopyCmd-Write
com.ibm.commerce.order.commands.OrderUnlockCmd
com.ibm.commerce.orderitems.commands.OrderItemAddCmd
com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd
```

これらのコマンドを、バイヤーが実行できるコマンドのリストを含むリソース・グループに追加しなければなりません。

注: コマンド com.ibm.commerce.order.commands.OrderCopyCmd-Write をリソース・グループに追加すると、「使用可能なリソース」の下に com.ibm.commerce.order.commands.OrderCopyCmd と表示されます。

バイヤー管理者役割の役割ベースのポリシーの識別

1. 付録の『役割ベースのポリシー』を参照して、バイヤー管理者の役割ベースのポリシーを見つけます。ポリシーは
   BuyerAdministratorsExecuteBuyersAdministratorsCommands です。
2. **「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. リストからポリシーを探します。
5. リソース・グループ BuyersAdministratorsCommmandsResourceGroup の名前を記録します。
   このリソース・グループの名前を更新する必要があります。

役割ベースのポリシー内のリソース・グループを更新して、オーダー変更用コマンドを組み込む

1. **「アクセス管理」>「リソース・グループ」**をクリックします。
2. **「BuyersAdministratorsCommandsResourceGroup」** を選択します。
3. **「変更」**をクリックして、「リソース・グループの変更」ページを表示します。
4. **「次へ」**をクリックして、「詳細情報」ページを表示します。
5. 「使用可能なリソース」リストから、オーダー変更用コマンドを選択します。

```
com.ibm.commerce.order.commands.OrderCancelCmd
com.ibm.commerce.order.commands.OrderCopyCmd
com.ibm.commerce.order.commands.OrderUnlockCmd
com.ibm.commerce.orderitems.commands.OrderItemAddCmd
com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd
```

6. **「追加」**をクリックして、コマンドをリソース・グループに追加します。
7. **「終了」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

オーダー・シナリオ 3: RMA 承認者がすべての RMA を承認できるようにする

デフォルトでは、ストアに関する返品商品取引権限 (RMA) の承認者は、自分のストアの RMA だけを承認します。場合によっては、RMA 承認者がすべてのストアの RMA を承認することもできます。同一の組織が複数のストアを所有している場合や、同一人物が複数のストアに関する RMA 承認を処理している場合は、この方が望ましいことがあります。

このシナリオでは、新しいアクセス・グループを作成し、新しいリソース・レベル・ポリシー内でこのアクセス・グループを使用します。 RMA 承認者がすべてのストアに対して RMA を承認できるようにするには、以下のようにする必要があります。

- 付録を参照して、組織の RMA 承認者が自分の組織の RMA を承認することを認可するためのリソース・レベル・ポリシーを見つけます。
- ポリシーで使用されているリソース・グループとアクション・グループの名前を記録します。
- ポリシーのアクセス・グループ RMAApproversForOrg を表示して、組み込まれている役割を記録します。アクセス・グループは、選択基準として組織と役割を使用して定義されます。複数の組織にまたがってアクションを実行する権限をユーザーに付与するには、組織の基準を使用せずにアクセス・グループを定義しなければなりません。
- 新しいアクセス・グループ RMAApprovers を作成します。このアクセス・グループは、同じ役割を使用しますが、組織の基準は組み込まれていません。
- 以下のものを使用して新しいポリシーを作成します。
  - 新しいアクセス・グループ RMAApprovers
  - 既存のポリシーからのアクション・グループ
  - 既存のポリシーからのリソース・グループ

実行するステップ

新しいポリシーの定義内で使用するアクション・グループとリソース・グループを識別する

1. 付録の『オーダー』を参照して、 RMAApproversForOrg が自分のストアの RMA を承認することを認可しているリソース・レベル・ポリシーを見つけます。ポリシーは RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource です。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。
5. ポリシーのアクション・グループ RMAApproveCommands の名前を記録します。このアクション・グループは、新しいポリシーを定義するときに使用することになります。
6. リソース・グループ RMADataResourceGroup の名前を記録します。このリソース・グループは、新しいポリシーを定義する際に使用することになります。
7. アクセス・グループ RMAApproversForOrg の名前を記録します。このアクセス・グループを表示して、新しいアクセス・グループに組み込む役割を参照します。

新しいアクセス・グループ内で使用する役割を識別する

1. **「アクセス管理」>「アクセス・グループ」**をクリックします。
2. アクセス・グループのリストから、**「RMAApproversForOrg」**を選択します。
3. **「変更」**をクリックします。
4. **「基準」**を選択して、「基準」ページを表示します。

5. 「選択した役割」および「組織」の下で、アクセス・グループ内で使用されている役割を記録します。
   - 顧客サービス・スーパーバイザー (Customer Service Supervisor)
   - セラー (Seller)
   - セールス・マネージャー (Sales Manager)
   - オペレーション・マネージャー (Operations Manager)
6. **「キャンセル」**をクリックして、アクセス・グループのリストに戻ります。

新しいアクセス・グループの定義

1. **「新規」**をクリックして、新しいアクセス・グループに関する「詳細情報」ページを表示します。
2. 「名前」に、RMAApprovers を指定します。
3. 「説明」に、アクセス・グループの説明を指定します。
4. 「親組織」に、「ルート組織」を選択します。
5. **「次へ」**をクリックして、新しいアクセス・グループの「基準」ページを表示します。
6. **「組織および役割別の基準 (Criteria based on organizations and roles)」**をクリックします。
7. 役割のリストから、以下の役割を選択します。
   - **顧客サービス・スーパーバイザー (Customer Service Supervisor)**
   - **セラー (Seller)**
   - **セールス・マネージャー (Sales Manager)**
   - **オペレーション・マネージャー (Operations Manager)**
8. **「終了」**をクリックします。

新しいポリシーの定義

1. **「アクセス管理」>「ポリシー」**をクリックします。
2. **「新規」**をクリックして、「新規のポリシー」ページを表示します。
3. 「名前」で、RMAApproversExecuteRMAApproveCommandsOnRMAResource を指定します。
4. 「表示名」に、ポリシーの簡単な説明をご使用の言語で指定します。
5. 「説明」に、ポリシーの詳しい説明をご使用の言語で入力します。
6. 「ユーザー・グループ」で、**「検索」**をクリックして、**「RMAApprovers」**を選択します。
7. **「OK」**をクリックします。
8. 「リソース・グループ」で、**「RMADataResourceGroup」**を選択します。
9. 「アクション・グループ」で、**「RMAApproveCommands」**を選択します。
10. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。

3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

メンバーシップ・シナリオ 1: ユーザーが自己登録できないようにする

デフォルトでは、ユーザーが登録済みの組織に属している場合、そのユーザーは自己登録することを許可されています。メンバーシップ管理者も、自分の組織に属するユーザーの登録を許可されています。厳密にアクセス制御する必要があるサイトの場合、自己登録の許可を除去して、メンバーシップ管理者でなければユーザーを登録できないようにする必要が生じることがあります。

注: WebSphere Commerce Professional Edition では、ルート組織、デフォルトの組織、およびセラー組織の 3 つの組織だけが存在します。

このシナリオでは、ユーザーの自己登録を許可しているリソース・レベル・ポリシーを除去しますが、メンバーシップ管理者が自分の組織内のユーザーを登録することを許可するポリシーは除去しません。

ユーザーの自己登録を許可しているリソース・レベル・ポリシーを削除するには、以下のようにします。

- 付録を参照して、ユーザーの自己登録を許可しているリソース・レベル・ポリシーを見つけます。
- そのポリシーを削除します。

実行するステップ

ポリシーを削除する

1. 付録の『メンバーシップ』を参照して、ユーザーが自己登録することを許可しているリソース・レベル・ポリシーを見つけます。ポリシーは `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource` です。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、**「GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource」**を選択します。
5. **「削除」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。
5. **「アクセス制御ポリシー・グループ・レジストリー (Access Control Policy Groups Registry)」**で、ステップ 3 と 4 を繰り返します。

メンバーシップ・シナリオ 2: 登録されて承認されたユーザーだけが自分の住所情報を変更できるようにする

デフォルトでは、ユーザーの登録が承認されているか承認保留されている場合に、そのユーザーは自分の住所情報を変更できます。場合によっては、登録され、承認されたユーザーだけが自分の住所を管理できるようにすることもできます。

このシナリオでは、以下のようにして、ユーザーが自分の住所情報を管理することを許可しているリソース・レベル・ポリシーのアクセス・グループを変更します。

- 付録を参照して、ユーザーが自分の住所情報を管理することを許可しているリソース・レベル・ポリシーを見つけます。
- そのポリシーのアクセス・グループを変更します。

  アクセス・グループ `RegisteredApprovedUsers` には役割が含まれていないので、この変更を加える際に役割ベースのポリシーを更新する必要はありません。

実行するステップ

リソース・レベル・ポリシーのアクセス・グループの変更

1. 付録の『メンバーシップ』を参照して、ユーザーが自分の住所情報を管理することを許可しているリソース・レベル・ポリシーを見つけます。ポリシーは `NonRejectedUsersExecuteAddressManageCommandsOnUserResource` です。

   注: 非拒否ユーザー (Non-rejected users) とは、登録が拒否されていないユーザーのことです。この種のユーザーの登録は承認済みか承認保留のどちらかです。
2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、**「NonRejectedUsersExecuteAddressManageCommandsOnUserResource」**を選択します。
5. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。
6. 「ユーザー・グループ」で、**「検索」**をクリックして、**「RegisteredApprovedUsers」**を選択します。
7. **「OK」**をクリックします。
8. アクセス・グループの変更を反映するように、ポリシーの名前、表示名、および説明を更新します。
9. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

メンバーシップ・シナリオ 3: メンバーシップ登録者がユーザーを登録できるようにする

デフォルトでは、組織のメンバーシップ管理者が、自分の組織のメンバーを登録することを許可されています。アクセス・グループ MemberAdministratorsForOrg には、バイヤー管理者やセラー管理者などの複数の役割が組み込まれており、これらの役割はさまざまな管理用タスクを実行することが許可されています。場合によっては、組織のメンバーを登録することだけを許可されている役割を別個に作成することができます。

関係するステップの概要を以下に示します。

- 新しい役割を作成し、その役割の新しいアクセス・グループ、新しいリソース・グループ、新しい役割ベースのポリシーを作成します。
- 既存のリソース・レベル・ポリシーを変更して、新しい役割を使用します。

このシナリオでは、以下を行います。

- Member Registrar という新しい役割を定義します。
- MemberRegistrars という新しいアクセス・グループを定義し、メンバー登録者の役割を組み込みます。
- 付録を参照して、メンバーシップ管理者がメンバーを登録することを許可するリソース・レベル・ポリシーを見つけます。
- アクション・グループ内のアクションの名前を記録します。このアクションの入った新しいリソース・グループを作成して、その新しい役割の役割ベースのポリシーでそのグループを使用する必要があります。アクションの役割ベースのポリシーでは、アクション・グループには 1 つのアクション実行しか入れることができないことに注意してください。リソース・グループには、実行可能なアクション (コマンド) が入れられます。
- UserAdminRegistrationCommands という新しいリソース・グループを定義して、メンバー登録用のコマンドを組み込みます。メンバー登録者の役割の役割ベース・ポリシー内で、このリソース・グループを使用することになります。
- メンバー登録者の役割ベースのポリシーを定義します。このポリシーは、MemberRegistrars アクセス・グループと MemberRegistrationCommands リソース・グループを使用します。
- メンバーを登録できる人を定義しているリソース・レベル・ポリシーに変更を加え、そのポリシーのアクセス・グループを MembershipAdministrators から MemberRegistrars に変更します。

実行するステップ

新しい役割の定義

1. 組織管理コンソールから、**「アクセス管理」>「役割」**をクリックします。
2. 「役割」ページで、**「新規」**をクリックします。
3. 「名前」で、「メンバー登録者 (Member Registrar)」を指定します。
4. 「説明」で、メンバー登録者の役割に関する説明をご使用の言語で指定します。
5. **「OK」**をクリックします。

メンバー登録者の役割を含む新しいアクセス・グループを定義する

1. **「アクセス管理」>「アクセス・グループ」**をクリックします。
2. 「アクセス・グループ」ページで、**「新規」**をクリックして、新しいアクセス・グループに関する「詳細情報」ページを表示します。
3. 「名前」に、「MemberRegistrars」を指定します。
4. 「親組織」に、**「ルート組織」**を選択します。
5. 「説明」に、アクセス・グループの説明をご使用の言語で指定します。
6. **「次へ」**をクリックして、新しいアクセス・グループの「基準」ページを表示します。
7. **「組織および役割別」**をクリックします。
8. 「役割」リストから、**「メンバー登録者 (Member Registrar)」**を選択します。
9. **「組織 (For Organization)」**をクリックして、この役割がユーザーの組織内またはその上位組織内で果たされなければならないことを指定します。
10. **「終了」**をクリックします。

メンバー登録者役割ベースのポリシーのためにリソース・グループで使用するアクションを識別する

1. 付録の『メンバーシップ』を参照して、メンバーシップ管理者にユーザーの登録を許可するポリシーを見つけます。そのポリシーは以下のとおりです。

   ```
   CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOn
   OrganizationResource
   ```

2. **「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. リストからポリシーを探します。
5. ポリシーのアクション・グループの名前 —`UserAdminRegistration` を記録します。これは、メンバーを登録するアクションを見分けるために表示する必要のあるアクション・グループです。
6. **「アクセス管理」>「アクション・グループ」**をクリックします。
7. アクション・グループのリストから、**「UserAdminRegistration」** を選択します。
8. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。
9. メンバーを登録するコマンドの名前 `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd` を記録します。

メンバー登録者のための役割ベース・ポリシーで使用される新しいリソース・グループを定義する

1. **「アクセス管理」>「リソース・グループ**」をクリックして、「リソース・グループ」ページを表示します。
2. **「新規」**をクリックして、新しいリソース・グループの「一般」ページを表示します。

3. 「名前」に、「UserAdminRegistrationCommands」を指定します。
4. 「表示名」に、リソース・グループの説明をご使用の言語で入力します。
5. 「説明」に、リソース・グループの詳しい説明をご使用の言語で入力します。
6. 「タイプ」に、**「明示的なリソース・グループ」**を選択します。
7. **「次へ」**をクリックします。
8. **「次へ」**をクリックして、新しいリソース・グループの「詳細情報」ページを表示します。
9. 「使用可能なリソース」リストから、以下を選択します。

   com.ibm.commerce.usermanagement.commands.
   UserRegistrationAdminAddCmd
10. **「追加」**をクリックします。
11. **「終了」**をクリックします。

メンバー登録者役割のための役割ベース・ポリシーを定義する

1. **「アクセス管理」**>**「ポリシー」**をクリックします。
2. 「ポリシー」ページで、**「新規」**をクリックします。
3. 「名前」に、**「MemberRegistrarsExecuteUserAdminRegistrationCommands」**を指定します。
4. 「表示名」に、ポリシーの説明をご使用の言語で入力します。
5. 「説明」に、ポリシーの詳しい説明をご使用の言語で入力します。
6. 「ユーザー・グループ」で、**「検索」**をクリックして**「MemberRegistrars」**を選択します。
7. **「OK」**をクリックします。
8. 「リソース・グループ」で、**「UserAdminRegistrationCommands」**を選択します。
9. 「アクション・グループ」で、**「ExecuteCommandActionGroup」**を選択します。
10. **「OK」**をクリックします。

注: この新規ポリシーは、作成後にポリシー・グループに割り当てられてから有効になります。これは XML を使用して実行する必要があります。詳しくは、151 ページの『第 13 章 XML を使用したアクセス制御ポリシーのカスタマイズ』 を参照してください。

新しいアクセス・グループを使用するために、リソース・レベルのポリシーを変更する

リソース・レベルのポリシーを変更した後に、リソースと同じ組織でメンバー登録役割を果たすユーザーだけが、ユーザーを登録することができます。他の組織で役割を果たすユーザーは、これを実行することはできません。

1. ポリシーのリストから、以下を選択します。

   CSAMembershipAdministratorsForOrgExecuteUserAdmin
   RegistrationCommandsOnOrganizationResource

   .

2. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。
3. アクセス・グループの変更を反映するように、ポリシーの名前、表示名、および説明を更新します。
4. 「ユーザー・グループ」で、**「検索」**をクリックして**「MemberRegistrars」**を選択します。
5. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

クーポン・シナリオ 1: バイヤーだけがクーポンを使用できるようにする

デフォルトでは、すべてのユーザーがクーポンを使用できます。しかし、クーポンの使用を WebSphere Commerce でバイヤーの役割を持つユーザーだけに限定したい場合があるかもしれません。

このシナリオでは、リソース・レベルのポリシーおよび関連した役割ベースのポリシーを変更します。クーポンの使用をバイヤーの役割を持つユーザーに限定するには、以下のようにする必要があります。

- 付録を参照して、クーポンを使用できるユーザーを指定するリソース・レベル・ポリシーを見つけます。
- ポリシーのアクセス・グループを、すべてのユーザーからバイヤーの役割のユーザーに変更します。
- クーポンを使用するためのコマンドを識別します。
- 付録を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見つけます。このポリシーは、バイヤー (購買サイド) の役割を持つユーザーが実行できるコマンドを定義します。バイヤーがクーポン使用のコマンドを実行できるように、このポリシーのリソース・グループを更新する必要があります。
- この役割ベースのポリシーのリソース・グループを更新して、クーポン使用のコマンドを組み込みます。

実行するステップ

リソース・レベルのポリシーとそのアクション・グループを識別する

1. 付録の『クーポン』を参照して、変更するリソース・レベルのポリシーを識別します。そのポリシーは以下のとおりです。

   ```
   AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、以下を選択します。

AllUsersExecuteCouponRedemptionCommandsOnCoupon WalletResource

5. ポリシーのアクション・グループの名前 — CouponRedemption を記録します。これが、クーポン使用のコマンドの名前を探すために表示する必要のあるアクセス・グループです。

アクセス・グループを変更する

1. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。
2. 「ユーザー・グループ」で、**「検索」**をクリックして**「バイヤー (購買サイド)」**を選択します。
3. **「OK」**をクリックします。
4. アクセス・グループの変更を反映するように、ポリシーの名前、表示名、および説明を更新します。
5. **「OK」**をクリックします。

クーポンを使用するためのコマンドを識別する

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**「CouponRedemption」**を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。入札を作成するコマンドの名前 (以下のとおり) を記録します。

```
com.ibm.commerce.couponredemption.commands.CouponDSSCmd
com.ibm.commerce.couponredemption.commands.UseCouponIdCmd
```

これらのコマンドを、バイヤーが実行できるコマンドのリストを含むリソース・グループに追加しなければなりません。

バイヤー (購買サイド) の役割ベースのポリシーを識別する

1. 付録の『役割ベースのポリシー』を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見つけます。そのポリシーは以下のとおりです。

```
Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
```

2. **「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。
5. リソース・グループの名前 Buyers(buy-side)CommandsResourceGroup を書き留めます。 このリソース・グループの名前を更新する必要があります。

役割ベース・ポリシーのリソース・グループを更新して、入札を作成するコマンドを組み込む

1. **「アクセス管理」>「リソース・グループ」**をクリックします。
2. **「Buyers(buy-side)CommandsResourceGroup」**を選択します。
3. **「変更」**をクリックして、「リソース・グループの変更」ページを表示します。
4. **「次へ」**をクリックして、「詳細情報」ページを表示します。
5. 「使用可能なリソース」リストから、以下を選択します。
   「com.ibm.commerce.couponredemption.commands.CouponDSSCmd」

「com.ibm.commerce.couponredemption.commands.UseCouponIdCmd」
これらは、クーポンを使用するためのコマンドです。

6. **「追加」**をクリックして、これらのコマンドをリソース・グループに追加します。
7. **「終了」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

クーポン・シナリオ 2: クーポン管理者とオペレーション・マネージャーの両方が電子クーポン販売促進を作成できるようにする

デフォルトでは、ストアのクーポン管理者は自身のストアでの電子クーポン販売促進を作成できます。場合によっては、この権限をオペレーション・マネージャーにも付与したいことがあります。

アクセス制御ポリシーの設計が柔軟であるため、この変更をいくつかの方法で実現することができます。

- 電子クーポン販売促進を作成できるユーザーを指定するポリシーのアクセス・グループに、オペレーション・マネージャー役割を追加できます。
- オペレーション・マネージャーが電子クーポン販売促進を作成できるようにする新しいポリシーを作成できます。

このシナリオでは、前者の方法を紹介します。それで、クーポン管理者にクーポン作成を許可しているリソース・レベル・ポリシーに、オペレーション・マネージャーの役割を追加する方法を示します。

この変更を行うには、以下のようにする必要があります。

- 付録を参照して、電子クーポンを作成できるユーザーを指定するリソース・レベル・ポリシーを見つけます。
- ポリシーのアクセス・グループを変更して、 オペレーション・マネージャー役割を持つユーザーを組み込みます。
- リソース・レベル・ポリシーのアクション・グループを表示して、電子クーポン販売促進を作成するためのコマンドを確認します。
- 付録を参照して、オペレーション・マネージャーの役割ベース・ポリシーを見つけます。このポリシーは、オペレーション・マネージャー役割を持つユーザーが実行できるコマンドを定義します。ストア管理者が電子クーポン販売促進作成のコマンドを実行できるように、このポリシーのリソース・グループを更新する必要があります。
- この役割ベースのポリシーのリソース・グループを更新して、電子クーポン作成のコマンドを組み込みます。

実行するステップ

リソース・レベル・ポリシーのアクション・グループとアクセス・グループを識別する

1. 付録の『オークション』を参照して、変更するリソース・レベルのポリシーを識別します。そのポリシーは以下のとおりです。

   CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands OnStoreEntityResource

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。
5. ポリシーのアクション・グループの名前 —CouponPromotionCreate を記録します。これが、電子クーポン作成のコマンドの名前を探すために表示する必要のあるアクセス・グループです。
6. ポリシーのアクセス・グループの名前 —CouponAdministratorsForOrg を記録します。これが、ストア管理者役割を組み込むように更新する必要のあるアクセス・グループです。

アクセス・グループを変更する

1. **「アクセス管理」>「アクセス・グループ」**をクリックします。
2. アクセス・グループのリストから、**「CouponAdministratorsForOrg」**を選択します。
3. **「変更」**をクリックして、「詳細情報」ページを表示します。
4. **「基準」**をクリックして、「基準」ページを表示します。
5. 「役割」リストから**「オペレーション・マネージャー」**を選択します。
6. **「組織 (For Organization)」**をクリックして、この役割がリソースの組織またはその上位組織で果たされなければならないことを指定します。
7. **「追加」**をクリックします。
8. **「OK」**をクリックします。

電子クーポン販売促進作成のコマンドを識別する

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**「CouponPromotionCreate」**を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。電子クーポン販売促進作成のコマンドの名前 —com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd を記録します。オペレーション・マネージャーが実行できるコマンドのリストが入ったリソース・グループに、このコマンドを追加する必要があります。

オペレーション・マネージャーの役割ベース・ポリシーを識別する

1. 付録の『役割ベースのポリシー』を参照して、オペレーション・マネージャーの役割ベースのポリシーを見つけます。ポリシーは OperationsManagersExecuteOperations ManagersCmdResourceGroup です。

2. **「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. リストからポリシーを探します。
5. そのリソース・グループの名前 —OperationsManagersCmdResourceGroup を記録します。 このリソース・グループの名前を更新する必要があります。

役割ベースのポリシーのリソース・グループを更新して、電子クーポン販売促進のコマンドを組み込む

1. **「アクセス管理」>「リソース・グループ」**をクリックします。
2. **「OperationsManagersCmdResourceGroup」**を選択します。
3. **「変更」**をクリックして、「リソース・グループの変更」ページを表示します。
4. **「次へ」**をクリックして、「詳細情報」ページを表示します。
5. 「使用可能なリソース」リストから、com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd を選択します。これは、電子クーポン販売促進を作成するコマンドです。
6. **「追加」**をクリックします。
7. **「終了」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

調達シナリオ 1: 調達ショッピング・カート管理者が、組織によって作成されるオーダー用の調達ショッピング・カートを管理できるようにする

注: このシナリオは、WebSphere Commerce Professional Edition には適用されません。

デフォルトでは、調達ショッピング・カート管理者は、自分でオーダーを作成した場合に調達ショッピング・カートを管理できます。しかし、調達ショッピング・カート管理者の権限を拡張して、自分たちの組織のメンバーによって作成されたオーダーに関しても、調達カートを管理できるようにしたい場合があるかもしれません。

この変更を行うには、以下のようにする必要があります。

- 付録を参照して、調達ショッピング・カート管理者が調達ショッピング・カートを管理できるようにするリソース・レベル・ポリシーを見つけます。
- このポリシーのリソース関係を 作成者から作成者と同じ組織エンティティーに変更します。

実行するステップ

リソース・レベル・ポリシーのリソース関係を変更する

1. 付録の『調達』を参照して、調達ショッピング・カート管理者にオーダーの調達ショッピング・カートを管理する権限を与えるリソース・レベル・ポリシーを見つけます。そのポリシーは以下のとおりです。

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   CartManageOnOrderResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. ポリシーのリストから、以下を選択します。

   ProcurementShoppingCartManagersExecuteProcurementShopping CartManageOnOrderResource

5. **「変更」**をクリックして、「ポリシーの変更」ページを表示します。
6. 「関係」で、**「sameOrganizationalEntityAsCreator」**を選択します。
7. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

調達シナリオ 2: 調達バイヤー管理者が、組織によって作成されるオーダー用の調達ショッピング・カートを送信できるようにする

注: このシナリオは、WebSphere Commerce Professional Edition には適用されません。

デフォルトでは、調達ショッピング・カート管理者は、自分でオーダーを作成した場合に調達ショッピング・カートを保管または送信できます。しかし、これらのタスクの責任を分担したい場合があるかもしれません。調達ショッピング・カート管理者が、自分で作成したオーダーの入った調達ショッピング・カートを保管することはできますが、さらにオーダー作成者と同じ組織内の調達バイヤー管理者に、調達ショッピング・カートを送信する権限を与えることもできます。これは、調達バイヤー管理者が、計画された購入を送信前に確認できるようにしたい場合に役立ちます。

この変更を行うには、以下のようにする必要があります。

- 付録を参照して、調達ショッピング・カート管理者が管理者を集中させて配送センターを管理できるようにするリソース・レベル・ポリシーを見つけます。
- ポリシーのアクション・グループから、調達ショッピング・カートを送信するアクションを除去します。

- 調達ショッピング・カートを送信するコマンドの入った新しいアクション・グループを定義します。このアクション・グループを使用して、調達バイヤー管理者がオーダーの作成者と同じ組織に属している場合、管理者が調達ショッピング・カートを送信できるようにする新しいリソース・レベル・ポリシーを定義します。
- 調達バイヤー管理者がオーダーの作成者と同じ組織に属している場合、管理者が調達ショッピング・カートを送信できるようにする新しいリソース・レベル・ポリシーを作成します。

実行するステップ

リソース・レベル・ポリシーのアクション・グループとリソース・グループを識別する

1. 付録の『調達』を参照して、調達ショッピング・カート管理者にオーダーの調達ショッピング・カートを管理する権限を与えるリソース・レベル・ポリシーを見つけます。そのポリシーは以下のとおりです。

   ```
   ProcurementShoppingCartManagersExecuteProcurement
   ShoppingCartManageOnOrderResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. ポリシーのリストからポリシーを探します。
4. アクション・グループの名前 — `ProcurementShoppingCartManage` を記録します。このアクション・グループを更新して、調達ショッピング・カートを送信するアクションを除去します。
5. リソース・グループの名前 — `OrderDataResourceGroup` を記録します。このリソース・グループを使用して、新しいリソース・レベル・ポリシーを定義します。

リソース・レベル・ポリシーのアクション・グループを更新する

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. アクション・グループのリストから、**「ProcurementShoppingCartManage」**を選択します。
3. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。
4. 「選択したアクション」リストから、**「com.ibm.commerce.me.commands.SubmitShoppingCartCmd」**を選択します。 後で、このアクションの入った新しいアクション・グループを作成して、新しいリソース・レベル・ポリシーでこのアクション・グループを使用します。
5. **「除去」**をクリックします。
6. **「OK」**をクリックします。

新しいアクション・グループを定義する

1. **「アクセス管理」>「アクション・グループ」**をクリックします。
2. **「新規」**をクリックして、「新規のアクション・グループ」ページを表示します。
3. 「名前」に、`ProcurementShoppingCartSubmit` を指定します。

4. 「表示名」に、アクション・グループの簡単な説明をご使用の言語で指定します。
5. 「説明」に、アクション・グループの詳しい説明をご使用の言語で入力します。
6. 「使用可能なアクション」リストから、**「com.ibm.commerce.me.commands.SubmitShoppingCartCmd」**を選択します。
7. **「追加」**をクリックします。
8. **「OK」**をクリックします。

新しいポリシーの定義

1. **「アクセス管理」>「ポリシー」**をクリックします。
2. 「ビュー」から、**「ルート組織」**をクリックして、所有するポリシーを表示します。
3. **「新規」**をクリックして、「新規のポリシー」ページを表示します。
4. 「名前」には、以下を指定します。

   ```
   ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommands
   OnOrderResource
   ```

5. 「表示名」に、ポリシーの簡単な説明をご使用の言語で指定します。
6. 「説明」に、ポリシーの詳しい説明をご使用の言語で入力します。
7. 「ユーザー・グループ」で、**「検索」**をクリックして、**「ProcurementBuyerAdministrators」**を選択します。
8. **「OK」**をクリックします。
9. 「リソース・グループ」で、**「OrderDataResourceGroup」**を選択します。
10. 「アクション・グループ」で、**「ProcurementShoppingCartSubmit」**を選択します。
11. 「関係」で、**「sameOrganizationalEntityAsCreator」**を選択します。
12. 「ポリシーのタイプ」で、**「グループ可能化テンプレート・ポリシー (Groupable Template Policy)」**を選択して、ポリシーをテンプレート・ポリシーとして指定します。
13. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

注: 新規ポリシーは、作成後にポリシー・グループに割り当てられてから有効になります。これは XML を使用して実行します。詳しくは、151 ページの『第 13 章 XML を使用したアクセス制御ポリシーのカスタマイズ』を参照してください。

在庫シナリオ 1: 配送センター管理者が配送センターを更新できるが削除できないようにする

デフォルトでは、配送センター管理者に、それぞれのストアに関連づけられた配送センターを更新または削除する権限が与えられています。しかし、配送センター管理者が配送センターを更新することはできても、削除することはできないようにしたい場合があるかもしれません。

この変更を行うには、以下のようにする必要があります。

- 付録を参照して、配送センター管理者に配送センターを管理する権限を与えるリソース・レベル・ポリシーを見つけます。
- そのポリシーのアクション・グループから、配送センターを削除するアクションを除去します。

実行するステップ

配送センターを削除するアクションを除去する

1. 付録の『調達』を参照して、調達ショッピング・カート管理者にオーダーの調達ショッピング・カートを管理する権限を与えるリソース・レベル・ポリシーを見つけます。そのポリシーは以下のとおりです。

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
   ManageCommandsOnFulfillmentResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. ポリシーのリストからポリシーを探します。
4. そのアクション・グループの名前 —FulfillmentCenterManage を記録します。このアクション・グループを更新して、配送センターを削除するアクションを除去します。
5. **「アクセス管理」>「アクション・グループ」**をクリックします。
6. アクション・グループのリストから、**「FulfillmentCenterManage」**を選択します。
7. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。
8. 「選択したアクション」リストから、**「com.ibm.commerce.inventory.commands.FulfillmentCenterDeleteCmd」**を選択します。
9. **「除去」**をクリックします。
10. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

在庫シナリオ 2: 物流管理マネージャー、オペレーション・マネージャー、およびアカウント担当者だけが配送センターを作成、更新、削除できるようにする

デフォルトでは、配送センター管理者には、それぞれのストアに関連した配送センターの作成、更新、または削除を行う権限が与えられています。配送センターのアクセス・グループには、セラー、物流管理マネージャー、オペレーション・マネージャー、およびアカウント担当者の役割が含まれます。しかし、セラーには配送センター管理者の権限を与えたくない場合があるかもしれません。

この変更を行うには、以下のようにする必要があります。

- 付録を参照して、配送センター管理者に配送センターを管理する権限を与えるリソース・レベル・ポリシーを見つけます。
- `fulfillment center managers` アクセス・グループの定義から、セラー役割を除去します。

実行するステップ

アクセス・グループからセラー役割を除去する

1. 付録の『調達』を参照して、調達ショッピング・カート管理者にオーダーの調達ショッピング・カートを管理する権限を与えるリソース・レベル・ポリシーを見つけます。そのポリシーは以下のとおりです。

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「アクセス・グループ」**をクリックします。
3. アクセス・グループのリストから、**「FulfillmentCenterManagersForOrg」**を選択します。
4. **「変更」**をクリックして、「アクセス・グループの変更」ページを表示します。
5. **「アクセス管理」>「アクセス・グループ」**をクリックします。
6. **「変更」**をクリックして、「詳細情報」ページを表示します。
7. **「基準」**をクリックして、「基準」ページを表示します。
8. 「役割」リストから**「セラー」**を選択します。
9. **「除去」**をクリックします。
10. **「OK」**をクリックします。

アクセス制御ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。
3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

ビジネス・インテリジェンス・シナリオ 1: 監査者がビジネス・インテリジェンス・レポートを参照できるようにする

デフォルトでは、インテリジェンス・レポートの参照権限を持つユーザーは、ストアのビジネス・インテリジェンス・レポートを参照することができます。しかし、auditor (監査者) という新しい役割を作成して、この役割を持つユーザーがストアのビジネス・インテリジェンス・レポートを参照できるようにしたい場合があるかもしれません。

関係するステップの概要を以下に示します。

- Auditor (監査者) という新しい役割を作成し、その役割の新しいアクセス・グループ Auditors、新しいリソース・グループ、新しい役割ベースのポリシーを作成します。
- 新しい役割をリソース・レベルのポリシーのアクセス・グループに追加します。
- ストアのビジネス・インテリジェンス・レポートを参照できるユーザーを定義する、リソース・レベルのポリシーのアクセス・グループに、**監査者**役割を追加します。

このシナリオでは、以下を行います。

- 付録を参照して、ビジネス・インテリジェンス・レポートを参照できるユーザーに、そのリポートの参照を許可しているリソース・レベル・ポリシーを見つけます。
- アクション・グループ内のアクションの名前を記録します。このアクションの入った新しいリソース・グループを作成して、その新しい役割の役割ベースのポリシーでそのグループを使用する必要があります。アクションの役割ベースのポリシーでは、アクション・グループには 1 つのアクション実行しか入れることができないことに注意してください。リソース・グループには、実行可能なアクション (コマンド) が入れられます。
- AuditorCommands という新しいリソース・グループを定義します。このグループには、ビジネス・インテリジェンス・レポートを参照するコマンドが入れられます。監査者役割に関する役割ベースのポリシーでこのリソース・グループを使用します。
- 監査者に関する新しい役割ベースのポリシーを定義します。このポリシーは、Auditors アクセス・グループおよび AuditorCommands リソース・グループを使用します。
- ストアのビジネス・インテリジェンス・レポートを参照できるユーザーを定義する、リソース・レベル・ポリシーのアクセス・グループに、監査者役割を追加します。

実行するステップ

新しい Auditor (監査者) 役割を定義する

1. 組織管理コンソールから、**「アクセス管理」>「役割」**をクリックします。
2. 「役割」ページで、**「新規」**をクリックします。
3. 「名前」に、「Auditor」を指定します。
4. 「説明」に、auditor (監査者) 役割に関する説明をご使用の言語で入力します。

5. **「OK」**をクリックします。

Auditor (監査者) 役割の新しいアクセス・グループを定義する

1. **「アクセス管理」>「アクセス・グループ」**をクリックします。
2. 「アクセス・グループ」ページで、**「新規」**をクリックして、新しいアクセス・グループに関する「詳細情報」ページを表示します。
3. 「名前」に、「Auditors」を指定します。
4. 「説明」に、アクセス・グループの説明をご使用の言語で指定します。
5. 「親組織」に、**「ルート組織」**を選択します。
6. **「次へ」**をクリックして、新しいアクセス・グループの「基準」ページを表示します。
7. **「組織および役割別」**をクリックします。
8. 「役割」リストから、**「Auditor」**を選択します。
9. **「追加」**をクリックします。
10. **「終了」**をクリックします。

Auditor (監査者) 役割の役割ベースのポリシーのリソース・グループで使用するアクションを識別する

1. 付録の『ビジネス・インテリジェンス』を参照して、インテリジェンス・レポートを参照できるユーザーにビジネス・インテリジェンス・レポートの参照の権限を与えるポリシーを見つけます。そのポリシーは以下のとおりです。

   ```
   IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport
   CommandsOnStoreEntityResource
   ```

2. 組織管理コンソールから、**「アクセス管理」>「ポリシー」**をクリックします。
3. 「ビュー」から、**「ルート組織」**を選択して、所有するポリシーを表示します。
4. リストからポリシーを探します。
5. ポリシーのアクション・グループの名前 `ViewBusinessIntelligenceReport` を記録します。これは、メンバーを登録するアクションを見分けるために表示する必要のあるアクション・グループです。
6. **「アクセス管理」>「アクション・グループ」**をクリックします。
7. アクション・グループのリストから、**「ViewBusinessIntelligenceReport」**を選択します。
8. **「変更」**をクリックして、「アクション・グループの変更」ページを表示します。
9. ビジネス・インテリジェンス・レポートを参照するコマンドの名前 `com.ibm.commerce.bi.commands.BIShowReportCmd` を記録します。

Auditor (監査者) 役割の役割ベース・ポリシーで使用される新しいリソース・グループを定義する

1. **「アクセス管理」>「リソース・グループ」**をクリックして、「リソース・グループ」ページを表示します。
2. **「新規」**をクリックして、新しいリソース・グループの「一般」ページを表示します。
3. **「名前」**に、「AuditorCommands」を指定します。

4. **「表示名」**に、リソース・グループの説明をご使用の言語で入力します。
5. **「説明」**に、リソース・グループの詳しい説明をご使用の言語で入力します。
6. **「次へ」**をクリックします。
7. 「タイプ」に、**「明示的なリソース・グループ」**を選択します。
8. **「次へ」**をクリックして、新しいリソース・グループの「詳細情報」ページを表示します。
9. 「使用可能なリソース」リストから、**「com.ibm.commerce.bi.commands.BIShowReportCmd」**を選択します。
10. **「追加」**をクリックします。
11. **「終了」**をクリックします。

Auditor (監査者) 役割の役割ベース・ポリシーを定義する

1. **「アクセス管理」>「ポリシー」**をクリックします。
2. 「ポリシー」ページで、**「新規」**をクリックします。
3. 「名前」に、**「AuditorsExecuteAuditorCommands」**を指定します。
4. 「表示名」に、ポリシーの説明をご使用の言語で入力します。
5. 「説明」に、ポリシーの詳しい説明をご使用の言語で入力します。
6. 「ユーザー・グループ」で、**「検索」**をクリックして、**「Auditors」**を選択します。
7. **「OK」**をクリックします。
8. 「リソース・グループ」で、**「AuditorCommands」**を選択します。
9. 「アクション・グループ」で、**「ExecuteCommandActionGroup」**を選択します。
10. **「OK」**をクリックします。

リソース・レベル・ポリシーのアクセス・グループに Auditor (監査者) 役割を追加する

1. **「アクセス管理」>「アクセス・グループ」**をクリックします。
2. アクセス・グループのリストから、**「IntelligenceReportViewersForOrg」**を選択します。
3. **「変更」**をクリックして、「アクセス・グループの変更」ページを表示します。
4. **「基準」**をクリックして、そのアクセス・グループの「基準」ページを表示します。
5. 「役割」リストから、**「Auditor」**を選択します。
6. **「組織 (For Organization)」**をクリックして、この役割がリソースの組織内またはその上位組織内で果たされなければならないことを指定します。
7. **「追加」**をクリックします。
8. **「OK」**をクリックします。

ポリシー・レジストリーに変更を適用して更新する

1. 管理コンソールにログオンします。
2. **「構成」>「レジストリー」**をクリックします。

3. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
4. **「更新」**をクリックします。

第 13 章 XML を使用したアクセス制御ポリシーのカスタマイズ

WebSphere Commerce 管理コンソールを使用して、アクセス制御ポリシーおよびその一部に簡単な変更を行うことができます。より複雑な変更を行うためには、XML ファイルを直接編集し、次いでそれらをデータベースにロードする必要があります。

アクセス制御について XML ファイルを変更する前に、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」でアクセス制御についての章をお読みください。この章では、アクセス制御についての技術的な概要を示し、アクセス制御ポリシーによって保護されるカスタマイズされたコマンド、 Entity Bean、および JSP テンプレートを作成する方法について説明します。

「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」に示された手順に従ってコードのカスタマイズを完了した後、アクセス制御の XML ファイルを編集して必要な保護を確立することができます。

XML ファイルを編集およびロードすることによってのみ行える変更

以下の変更は XML ファイルを変更してロードすることによってのみ行えます。

- アクションの作成または変更
- 関係の作成または変更
- 関係グループの作成または変更
- リソースの作成または変更
- 属性の作成または変更
- 複雑な基準を使用するアクセス・グループの作成または変更
- 複雑な基準を使用するリソース・グループの作成または変更
- ビューに対する役割ベース・ポリシーの作成
- ビューに対する役割ベース・ポリシーでのアクション・グループの変更
- ポリシー・グループの作成または変更
- ポリシーとポリシー・グループとの関連付け

アクセス制御用の XML ファイルについて

WebSphere Commerce の XML ファイル、DTD ファイル、および XML トランスフォーマーの XSL ファイルの名前および説明が、以下の表に示されています。

表 12. アクセス制御用の WebSphere Commerce XML ファイル

ファイル名	説明
ACUserGroups_de_DE.xml ACUserGroups_en_US.xml ACUserGroups_es_ES.xml ACUserGroups_fr_FR.xml ACUserGroups_it_IT.xml ACUserGroups_ja_JP.xml ACUserGroups_ko_KR.xml ACUserGroups_pt_BR.xml ACUserGroups_zh_CN.xml ACUserGroups_zh_TW.xml	サポートされている各言語での、アクセス・グループの定義および説明。
defaultAccessControlPolicies.xml	デフォルトのアクセス制御ポリシー、アクション・グループ、リソース・グループ、関係、関係グループ、アクション、リソース・カテゴリー、および属性の定義を含むメイン・ファイル。
defaultAccessControlPolicies_de_DE.xml defaultAccessControlPolicies_en_US.xml defaultAccessControlPolicies_es_ES.xml defaultAccessControlPolicies_fr_FR.xml defaultAccessControlPolicies_it_IT.xml defaultAccessControlPolicies_ja_JP.xml defaultAccessControlPolicies_ko_KR.xml defaultAccessControlPolicies_pt_BR.xml defaultAccessControlPolicies_zh_CN.xml defaultAccessControlPolicies_zh_TW.xml	デフォルトのアクセス制御ポリシー、アクション・グループ、アクション、リソース・グループ、リソース・カテゴリー、関係、および属性について、サポートされている各言語での表示名および説明を含むファイル。
ACPoliciesfilter.xml	すべてのアクセス制御情報をデータベースから抽出するために使用されるフィルター・ファイル。
OrganizationPoliciesFilter.xml	特定の組織が所有するポリシーに関連したすべてのアクセス制御情報を抽出するために使用されるフィルター・ファイル。

表 12. アクセス制御用の WebSphere Commerce XML ファイル (続き)

ファイル名	説明
ACUserGroupsFilter.xml	すべてのアクセス・グループ情報を抽出するために使用されるフィルター・ファイル。
accesscontrolpolicies.dtd	アクセス制御ポリシー XML ファイルは、この DTD に準拠していなければなりません。
accesscontrolpoliciesnls.dtd	アクセス制御ポリシー NLS (各国語に特定の) XML ファイル (表示名と説明のみ) は、この DTD に準拠していなければなりません。
ACUserGroups_en_US.dtd	アクセス制御ユーザー・グループ XML ファイルは、この DTD に準拠していなければなりません。
accesscontrol.xsl	アクセス制御ポリシー XML ファイルの XSL トランスフォーム・ルール・ファイル。
accesscontrolnls.xsl	アクセス制御ポリシー NLS XML ファイル (表示名と説明のみ) の XSL トランスフォーム・ルール・ファイル。
ACUserGroup.xsl	アクセス・グループ XML ファイルの XSL トランスフォーム・ルール・ファイル。
wcstoacpolicies.xsl	アクセス制御ポリシー XML ファイルを作成するための、抽出後の ExtractedACPolicies.xml ファイルの XSL トランスフォーム・ルール・ファイル。
wcstoacpoliciesnls.xsl	アクセス制御ポリシー NLS XML ファイルを作成するための、抽出後の ExtractedACPolicies.xml の XSL トランスフォーム・ルール・ファイル。
wcstoacusergroup.xsl	アクセス・グループ XML ファイルを作成するための、抽出後の ExtractedACPolicies.xml ファイルの XSL トランスフォーム・ルール・ファイル。

XML ファイルの変更

XML ファイルを操作して、以下の許可タスクを実行できます。

- ビューの保護
- コントローラー・コマンドの保護
- リソース・レベルのアクセス制御のインプリメント

- Data Bean の保護
- リソースの属性別のグループ化
- 関係の定義
- 関係グループの定義

ビューの保護

URL から直接呼び出されるビュー、または他のコマンドからのリダイレクトされて立ち上げられるビューは、表示されるための役割ベースのアクセス制御ポリシーを必要とします。以下の例では、ビュー用の役割ベースのポリシーが表示されます。

```
<Policy Name="ProductManagersExecuteProductManagersViews"
   OwnerID="RootOrganization"
UserGroup="ProductMangers"
ActionGroupName="ProductMangersViews"
ResourceGroupName="ViewCommandResourceGroup"
PolicyType="groupableStandard">
</Policy>
```

ResourceGroup 名の ViewCommandResourceGroup は、これがビューの役割ベースのポリシーであることを示しています。このポリシーは、ProductManagers ユーザー・グループ内のユーザーが ProductMangersViews アクション・グループ内のビューを表示できることを示しています。同様に、たいていの役割の場合、役割がアクセスできるビューをグループ化する、対応するアクション・グループがあります。これはたとえば Seller 役割 -> Sellers アクセス・グループ -> SellersViews アクション・グループなどです。

以下は、ProductMangersViews アクション・グループの例です。

```
<ActionGroup Name="ProductManagersViews"
 OwnerID="RootOrganization">

<ActionGroupAction Name="ProductImageView"/>
<ActionGroupAction Name="ProductManufacturerView"/>
<ActionGroupAction Name="ProductSalesTaxView"/>

 </ActionGoup>
```

上記の例では、ProductManagerViews アクション・グループ内で実行可能な 3 つのアクション、 ProductImageView、ProductManufacturerView、および ProductSalesTaxView がリストされます。

以下は、ProductImageView アクション定義の例です。

```
<Action Name="ProductImageView"
CommandName="ProductImageView">
</Action>
```

Name 属性 ProductImageView は、アクションとアクション・グループとを関連付けるときなど、 XML 内の他の場所でこのアクションを参照するためのタグとして使用されます。

注: VIEWREG 表の VIEWNAME 列に保管されているこのビューの名前は、アクション定義の CommandName と一致しなければなりません。 CommandName の値は、ACACTION 表の ACTION 列に保管されています。 Name と CommandName 属性とは同じである必要はありません。

既存のポリシーを使用する新規のビューを追加する

既存の役割ベースのビュー・ポリシーからアクセス可能な新規のビューを追加するには、示されているものと類似の XML ファイルを作成し、次いで以下のようにします。

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

 <Action Name="MyNewView"
         CommandName="MyNewView">
 </Action>

  <ActionGroup Name="ProductManagersViews" OwnerID="RootOrganization">
             <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>

 </Policies>
```

1. ビュー名が *MyNewView* の新規のアクション定義を XML ファイル内に作成します。この名前は自由に変更してかまいません。

   ```
   <Action Name="MyNewView"
      CommandName="MyNewView">
   </Action>
   ```

2. どの役割にこのビューへのアクセスがあるかを判別し、新規のアクションと XML ファイル内の対応するアクション・グループとを関連付けます。たとえば、次のようになります。

   ```
   <ActionGroup Name="ProductManagersViews"
       OwnerID="RootOrganization">

     <ActionGroupAction Name="MyNewView"/>

    </ActionGroup>
   ```

   このアクション・グループも含まれている、役割ベースのポリシー ProductManagersExecuteProductManagersViews は既に存在しているので、新しいポリシーを作成する必要はありません。さらに、デフォルトの役割ベース・ポリシーは ManagementAndAdministrationPolicyGroup ポリシー・グループに属し、これは、すべてではありませんがサイト内の大半の組織に適用されるので、それ以上のポリシー・グループの加入を必要としません。

3. XML の変更をデータベースにロードします。 XML の変更をロードする方法についての詳細は、 186 ページの『変更をデータベースにロードする』を参照してください。

4. 管理コンソール内でアクセス制御ポリシー・レジストリーを更新します。その手順は、以下のとおりです。

   a. サイト管理者として管理コンソールにログオンします。

   b. **「構成」**>**「レジストリー」**をクリックします。

   c. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。

   d. **「更新」**をクリックします。

新規のポリシーを使用する新規のビューを追加する

既存の役割ベースのポリシーを持たない新規の役割からアクセス可能な新規のビューを追加するには、示されているものと類似の XML ファイルを作成し、次いで以下のようにします。

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

 <Action Name="MyNewView"
         CommandName="MyNewView">
 </Action>

  <ActionGroup Name="XYZViews" OwnerID="RootOrganization">
             <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>

 <Policy Name="XYZExecuteXYZViews"
   OwnerID="RootOrganization"
   UserGroup="XYZ"
   ActionGroupName="XYZViews"
   ResourceGroupName="ViewCommandResourceGroup"
   PolicyType="groupableStandard">
  </Policy>

 <PolicyGroup Name="ManagementAndAdministrationPolicyGroup" OwnerID="RootOrganization">
  <PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization" />
 </PolicyGroup>

 </Policies>
```

1. ビュー名が *MyNewView* の新規のアクション定義を XML ファイル内に作成します。この名前は自由に変更してかまいません。

   ```
   <Action Name="MyNewView
   CommandName="MyNewView">
   </Action>
   ```

2. 新規の役割に関連付ける新規のアクション・グループを作成します。

   ```
   <ActionGroupName="XYZViews"
   OwnerID="RootOrganization">
       </ActionGroup>
   ```

   ここで、 *XYZViews* はアクション・グループの名前です。アクション・グループの OwnerID は必ず RootOrganization にします。

3. 新規のアクションを新規のアクション・グループに関連付けます。

   ```
   < ActionGroupName="XYZViews"
   OwnerID="RootOrganization">

    <ActionGroupAction Name="MyNewView"/>

       </ActionGroup>
   ```

   ここで、 *XYZViews* はアクション・グループの名前、 *MyNewView* は自分で作成したアクションです。

4. 新規のアクション・グループを参照するポリシーを作成します。

   ```
   <Policy Name="XYZExecuteXYZViews"
      OwnerID="RootOrganization"
   UserGroup="XYZ"
   ActionGroupName="XYZViews"
   ResourceGroupName="ViewCommandResourceGroup"
   PolicyType="groupableStandard">
   </Policy>
   ```

ここで、 *XYZExecuteXYZViews* はポリシー名、 *XYZViews* はアクション・グループです。 WebSphere Commerce 5.5 では、ポリシー加入モデルであるため、ポリシーを適用するリソースを判別するのに、グループ化可能な標準ポリシーおよびグループ化可能なテンプレート・ポリシーの OwnerID は使用されません。 OwnerID の値は、今のところ、ポリシーを表示するために、組織 (所有者) が管理コンソールで使用するだけです。ポリシーを複数の組織に適用する場合、 OwnerID を、ルート組織のような共通の上位組織に設定するようお勧めします。ポリシーを特定の組織にだけ適用する場合、OwnerID を、その組織の `orgentity_id` に設定するようお勧めします。

5. 新しいポリシーを適切なポリシー・グループに組み込みます。デフォルトでは、ほとんどの役割ベースのポリシーは、すべての組織に適用する必要のある、ManagementAndAdministrationPolicyGroup に入れられます。

```
<PolicyGroupName="ManagementAndAdministrationPolicyGroup"
OwnerID="RootOrganization">
<PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization"/>
</PolicyGroup>
```

   ここで `PolicyOwnerId` 値は、ポリシー定義で使用した `OwnerID` 値と同じでなければなりません。

6. XML の変更をデータベースにロードします。 XML の変更をロードする方法についての詳細は、 186 ページの『変更をデータベースにロードする』を参照してください。
7. 管理コンソール内でアクセス制御ポリシー・レジストリーを更新します。その手順は、以下のとおりです。
   a. サイト管理者として管理コンソールにログオンします。
   b. **「構成」**>**「レジストリー」**をクリックします。
   c. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
   d. **「更新」**をクリックします。

これでビューが使用可能となります。

コントローラー・コマンドの保護

すべてのコントローラー・コマンドは、実行するために役割ベースのアクセス制御ポリシーを必要とします。コントローラーまたはタスク・コマンドには、そのコマンドがリソース・レベルの検査を行う場合、リソース・レベルのポリシーも必要となります。詳細については、 164 ページの『リソースの保護』を参照してください。以下の例では、コントローラー・コマンド用の役割ベースのポリシーが表示されます。

```
<Policy Name="SellersExecuteSellersCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="Sellers"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="SellersCmdResourceGroup"
PolicyType="groupableStandard">
    </Policy>
```

ActionGroupName の `ExecuteCommandActionGroup` は、これがコントローラー・コマンドの役割ベースのポリシーであることを示しています。このポリシーは、`Sellers`

アクセス・グループ内のユーザーが SellersCmdResourceGroup リソース・グループ内のコマンドを実行できることを示しています。

以下は、SellersCmdResourceGroup リソース・グループ定義の例です。

```
<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CancelCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CreateCmdResourceCategory"/>
</ResourceGroup>
```

上記の例は、コントローラー・コマンドに対応するリソース・グループ内の、次の 3 つのリソースを示しています。

- com.ibm.contract.commands.ContractCancelCmdResourceCategory
- com.ibm.contract.commands.ContractCloseCmdResourceCategory
- com.ibm.contract.commands.ContractCreateCmdResourceCategory

以下は、リソースのサンプル定義です。

```
<ResourceCategory Name="com.ibm.commerce.contract.commands.Contract
CloseCmdResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.commands.ContractCloseCmd">

<ResourceAction Name="ExecuteCommand"/>

</ResourceCategory>
```

Name 属性、
com.ibm.commerce.contract.commands.ContractCloseCmdResourceCategory は、XML ファイル内のリソースを参照するためのタグとして使用されます。
ResourceAction Name の ExecuteCommand は、リソース上で操作可能なアクションを指定するために使用されます。この情報は、アクセス制御ポリシーを使用して特定のリソースに対応する「アクション」選択ボックスに値を取り込むとき、管理コンソールで使用されます。この場合、アクション Execute が指定されます。
Execute アクションは以下のように定義されます。

```
<Action Name="ExcecuteCommand
CommandName="Execute">
</Action>
```

注: コントローラー・コマンドのインターフェース名は、リソース定義内の ResourceBeanClass と一致していなければなりません。 ResourceBeanClass の値は、ACRESCGRY 表の RESCLASSNAME 列に保管されます。これらのコマンドは ControllerCommand インターフェースを拡張し、それは AccCommand インターフェースを拡張して、さらにそれは保護可能インターフェースを拡張するので、リソースとして使用できます。これらのインターフェースについては、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」を参照してください。

既存のポリシーを使用する新規のコントローラー・コマンドを追加する

既存の役割ベースのポリシーを持つ新規の役割からアクセス可能な新規のコントローラー・コマンドを追加するには、以下のような XML ファイルを作成します。後で個別のステップをリストします。

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

  < ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
    ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">

     <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
    ResourceGroupResource Name="com.xyz.commands.MyNewControllerCmdResource
    Category"/>
 </ResourceGroup>

 </Policies>
```

1. コントローラー・コマンドのインターフェース名に対応する新規のリソース定義を、 XML ファイル内に作成します。

   ```
   <ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
      ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">

     <ResourceAction Name="ExecuteCommand"/>
    </ResourceCategory>
   ```

2. どの役割にこのコマンドへのアクセスがあるかを判別し、新規のリソースと XML ファイル内の対応するリソース・グループとを関連付けます。たとえば、次のようになります。

   ```
    <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
       <ResourceGroupResource Name="com.xyz.commands.
   MyNewControllerCmdResourceCategory"/>

    </ResourceGroup>
   ```

   使用する役割に応じて、リソース・グループを変更できます。役割ベースのポリシーについての詳細は、 230 ページの『役割ベースのポリシー』を参照してください。

3. XML の変更をデータベースにロードします。 XML の変更をロードする方法についての詳細は、 186 ページの『変更をデータベースにロードする』を参照してください。
4. 管理コンソール内でアクセス制御ポリシー・レジストリーを更新します。その手順は、以下のとおりです。
   a. サイト管理者として管理コンソールにログオンします。
   b. **「構成」**>**「レジストリー」**をクリックします。
   c. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
   d. **「更新」**をクリックします。

このリソース・グループを含む役割ベースのポリシーがすでに存在するため、それがリソース・レベルの検査を行っていなければ、これで新規のコントローラー・コマンドを使用できるようになりました。リソース・レベルの検査とコマンドについての詳細は、 162 ページの『既存のポリシーのリソース・レベル・アクセス制御の変更』を参照してください。

新規のポリシーを使用する新規のコントローラー・コマンドを追加する

既存の役割ベースのポリシーを持たない新規の役割からアクセス可能な新規のコントローラー・コマンドを追加するには、以下のような XML ファイルを作成します。後で個別のステップをリストします。

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies>

  < ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
    <ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">

     <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

        <ResourceGroup Name="XYZCmdResourceGroup"  OwnerID="RootOrganization"
    <ResourceGroupResource Name="com.xyz.commands.MyNewController
    CmdResourceCategory"/>
 </ResourceGroup>

    <Policy Name="XYZExecuteXYZsCmdResourceGroup"
   OwnerID="RootOrganization"
    UserGroup="XYZ"
   ActionGroupName="ExecuteCommandActionGroup"
    ResourceGroupName="XYZCmdResourceGroup"
   PolicyType="groupableStandard">
  </Policy>

  <PolicyGroup Name="ManagementAndAdministrationPolicyGroup"
   OwnerID="RootOrganization">
  <PolicyGroupPolicy  Name="XYZExecuteXYZsCmdResourceGroup"
   PolicyOwnerId="RootOrganization" />
 </PolicyGroup>

 </Policies>
```

1. コントローラー・コマンドのインターフェース名に対応する新規のリソース定義を、 XML ファイル内に作成します。例については、 159 ページの『既存のポリシーを使用する新規のコントローラー・コマンドを追加する』を参照してください。
2. 新規の役割に関連付ける新規のリソース・グループを作成します。

   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   </ResourceGroup>
   ```
3. 新規のリソースを新規のリソース・グループに関連付けます。

   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   <ResourceGroupResource Name="com.xyz.commands.MyNewControllerResourceCategory"/>
   </ResourceGroup>
   ```
4. 新規のリソース・グループを参照するポリシーを作成します。

```
<Policy Name="XYZExecuteXYZsCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="XYZ"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="XYZCmdResourceGroup">
   PolicyType="groupableStandard">
</Policy>
```

5. XML の変更をデータベースにロードします。 XML の変更をロードする方法についての詳細は、 186 ページの『変更をデータベースにロードする』を参照してください。
6. 管理コンソール内でアクセス制御ポリシー・レジストリーを更新します。その手順は、以下のとおりです。
   a. サイト管理者として管理コンソールにログオンします。
   b. **「構成」**>**「レジストリー」**をクリックします。
   c. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
   d. **「更新」**をクリックします。

それがリソース・レベルの検査を行っていなければ、これで新規のコントローラー・コマンドを使用できるようになりました。リソース・レベルの検査とコマンドについての詳細は、 162 ページの『既存のポリシーのリソース・レベル・アクセス制御の変更』を参照してください。

コントローラー・コマンドのコマンド・レベル・アクセス制御の変更

デフォルトのアクセス制御ポリシーに基づき、マーケティング・マネージャー役割しか持たないユーザーは、 UserRegistrationAdminAddCmd コマンドを実行できません。以下のシナリオでは、そのようなユーザーがこのコマンドを実行できるよう、既存のポリシーを変更するのに必要な手順を示します。このシナリオの手順をそれぞれの要件に合わせてカスタマイズしてください。

すべてのコントローラー・コマンドには、 ActionGroupName = ExecuteCommandActionGroup という指定を含んだコマンド・レベル・アクセス制御ポリシーが必要です。また、このポリシーには、コントローラー・コマンドのインターフェース名を含んだリソース・グループの指定も必要です。さらに、この種のポリシーは、MarketingManagersExecuteMarketingManagerCmdResourceGroup などの役割を参照するのが普通です。

```
<Policy Name="MarketingManagersExecuteMarketingManagerCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="MarketingManagers"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="MarketingManagerCmdResourceGroup"
   PolicyType="groupableStandard">

</Policy>
```

注: 上記のポリシーは、インスタンス作成時にデータベースへロードされるデフォルト・ポリシーの 1 つです。デフォルト・ポリシーについての詳細は、 229 ページの『デフォルトのアクセス制御ポリシーおよびグループ』を参照してください。

この場合、マーケティング・マネージャー役割を持ったユーザーに UserRegistrationAdminAddCmd の実行権限を与えるには、独自の XML ファイルを

作成することによって、このポリシーで使用している既存のリソース・グループにこのコマンドを追加してから、次のようにする必要があります。

1. ExecuteCommand アクションを再定義します。
2. com.ibm.commerce.usermanagement.commands.UserRegistrationAddCmd をリソース・カテゴリーとして再定義します。
3. そのリソース・カテゴリーを必要なリソース・グループ (この場合は、MarketingManagerCmdResourceGroup) に関連付けます。
4. この XML ファイルを *WC_installdir*/xml/policies/xml にコピーします。以下は、そのような XML の例です。

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>


<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies>

 <Action Name="ExecuteCommand"
   CommandName="Execute">

 </Action>

 <ResourceCategory
      Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdmin
AddCmdResourceCategory"
   ResourceBeanClass="com.ibm.commerce.usermanagement.commands.
UserRegistrationAdminAddCmd">
  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

 <ResourceGroup Name="MarketingManagerCmdResourceGroup"
   OwnerID="RootOrganization"
  ResourceGroupResource
      Name="com.ibm.commerce.usermanagement.commands.
UserRegistrationAdminAddCmdResourceCategory"/>
 </ResourceGroup>

 </Policies>
```

5. *WC_installdir*/bin/acpload スクリプトを使用して、その XML ファイルをデータベースにロードします。 XML ファイルのロードについての詳細は、 186 ページの『変更をデータベースにロードする』を参照してください。
6. WebSphere Commerce 管理コンソール内でアクセス制御ポリシー・レジストリーを更新します。その手順は、以下のとおりです。
   a. サイト管理者として管理コンソールにログオンします。
   b. **「構成」**>**「レジストリー」**をクリックします。
   c. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。
   d. **「更新」**をクリックします。

それがリソース・レベルの検査を行っていなければ、これで新規のコントローラー・コマンドを使用できるようになりました。リソース・レベルの検査を行っている場合については、 『既存のポリシーのリソース・レベル・アクセス制御の変更』を参照してください。

既存のポリシーのリソース・レベル・アクセス制御の変更: リソース・レベルのアクセス制御を必要とするコマンドでは、各コマンドの getResources() メソッドによって、アクセス対象の保護リソースが戻されます。この時点から、WebSphere Commerce アクセス制御フレームワークによるリソース・レベルのアクセス制御検査が始まります。 WebSphere Commerce は、現在のコマンド (この例では、com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd) に等

しいアクションを含む「アクション・グループ」を使用して、システム内のアクセス制御ポリシーを検索します。ポリシーの「リソース・グループ」には、getResources() メソッドで戻されたリソースも含まれている必要があります。その場合、UserRegistrationAdminAddCmd コマンドは、 getResources() メソッドをインプリメントし、そのメソッドは、新規のユーザーの登録先になる組織を戻します。

初期設定では、defaultAccessControlPolicies.xml に、com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd がすでにアクションとして定義されています。

```
<Action Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"
   CommandName="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd">
 </Action>
```

defaultAccessControlPolicies.xml XML ファイルで以下のように定義した、アクション・グループにも含まれます。

```
<ActionGroup Name="UserAdminRegistration"
    OwnerID="RootOrganization">

  <ActionGroupAction
        Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"/>
 </ActionGroup>
```

このアクション・グループは、既存のブートストラップ・ポリシーですでに使用されています。

```
<Policy
   Name="MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource"
   OwnerID="RootOrganization"
   UserGroup="MembershipAdministratorsForOrg"
   ActionGroupName="UserAdminRegistration"
   ResourceGroupName="OrganizationDataResourceGroup"
   PolicyType="groupableTemplate">

</Policy>
```

注: 多くのポリシーはデフォルト・ポリシーであり、インスタンス作成時にデータベースにロードされます。デフォルト・ポリシーについての詳細は、 229 ページの『デフォルトのアクセス制御ポリシーおよびグループ』を参照してください。

UserRegistrationAdminAddCmd に、必要な役割を追加するには、以下のようにします。

1. このポリシーが使用するアクセス・グループに必要な役割を追加します。この例では、MembershipAdministratorsForOrg です。

   このアクセス・グループは、*WC_installdir*/xml/policies/xml/ACUserGroup_en_US.xml で次のように定義されています。

   ```
   <UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
      Description="Administrators of membership for the organization" MemberGroupID="-97"

   <UserCondition><![ CDATA [
        <profile>
    <orListCondition>
         <simpleCondition>
           <variable name="role"/>
           <operator name="="/>
           <value data="Buyer Administrator"/>
        <qualifier name="org" data="?"/>
         </simpleCondition>
         <simpleCondition>
           <variable name="role"/>
           <operator name="="/>
   ```

```
        <value data="Seller Administrator"/>
      <qualifier name="org" data="?"/>
       </simpleCondition>
    </orListCondition>
</profile>
 ]]></UserCondition>
</UserGroup>
```

上記の XML には、getResources() によって戻されたリソース (組織) の所有者の祖先に当たる組織の Buyer Administrator (バイヤー管理者) または Seller Administrator (セラー管理者) という役割のいずれか 1 つを持っているユーザーが組み込まれています。 マーケティング・マネージャー役割を追加する場合は、その新規の役割も組み込むような形で機能を拡張する必要があります。

2. この XML ファイルを *WC_installdir*/xml/policies/xml にコピーします。以下は、そのような XML の例です。

```
?xml version="1.0" encoding="UTF-8"?
<!DOCTYPE UserGroups SYSTEM "../dtd/ACUserGroups_en_US.dtd">

<UserGroups>

<UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
    Description="Administrators of membership for the organization" MemberGroupID="-97">

  <UserCondition><![CDATA[
<profile>
    <orListConditio>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Buyer Administrator"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Seller Administrator"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Marketing Manager"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
   </orListCondition>
</profile>
 ]]></UserCondition>
</UserGroup>

</UserGroups>
```

3. *WC_installdir*/bin/acpload スクリプトを使用して、その XML ファイルをデータベースにロードします。 XML ファイルのロードについての詳細は、 186 ページの『変更をデータベースにロードする』を参照してください。

4. WebSphere Commerce 管理コンソール内でアクセス制御ポリシー・レジストリーを更新します。その手順は、以下のとおりです。

   a. サイト管理者として管理コンソールにログオンします。

   b. **「構成」**>**「レジストリー」**をクリックします。

   c. レジストリーのリストから、**「アクセス制御ポリシー (Access Control Policies)」**を選択します。

   d. **「更新」**をクリックします。

リソースの保護

リソース・レベルのアクセス制御をコントローラーまたはタスク・コマンドに追加することができます。リソース・レベルの検査は WebSphere Commerce ランタイム

で、コマンドの getResources() メソッドによって戻されるデータに基づいて行われます。リソース・レベルの検査は、コマンドの performExcecute() 部分を実行中に、メソッド void checkIsAllowed(Object resource, String action) throws ECException を使用してアクセス制御ポリシー・マネージャーを直接呼び出すことによっても行うことができます。現行ユーザーに指定のソース上での指定のアクションを実行する許可がない場合、このメソッドは ECApplicationException をスローします。

注: デフォルトでは、getResources() メソッドはヌルを戻し、リソース・レベルの検査は行われません。

以下の場合に、新規のコマンドのリソース・レベル・ポリシーを作成しなければなりません。

- この新規コマンドは、リソース・レベルの検査を行う基本的な WebSphere Commerce コマンドから拡張され、リソース・レベルのポリシーを持ち、基本コマンドとは異なるインターフェースをインプリメントします。
- 新規のコマンド自体がリソース・レベルのアクセス制御検査を行う場合。

以下は、リソース・レベル・ポリシーの例です。

```
<Policy Name="ContractMangersForOrgExecuteContractManageCommandsOnContractResource"
  OwnerID="RootOrganization"
  UserGroup="ContractManagersForOrg"
  ActionGroupName="ContractManage"
  ResourceGroupName="ContractDataResourceGroup"
  PolicyType="groupableTemplate">
</Policy>
```

ここで、

Name: ポリシーの名前。

PolicyType: ポリシーのタイプ。これはグループ化可能なテンプレート・ポリシーであり、リソースを所有する編成されたエンティティーとその祖先に動的に適用されます。

OwnerID: ポリシーを所有するメンバー。

UserGroup: ポリシーはこのグループのユーザーに適用されます。役割がリソースを所有する組織に動的に範囲指定されるアクセス・グループの命名規則は、 ForOrg をグループ名に追加することです。

ActionGroupName: リソースに対して実行するアクションを含むアクション・グループの名前。

ResourceGroupName: 実行の対象となるリソースを含むリソース・グループの名前。

上の例では、アクション・グループ ContractManage は ContractDataResourceGroup に対して実行されるコマンドのセットを含むアクション・グループです。上記のリソース・レベル・ポリシーで使用されるアクション・グループの例を以下に示します。

```
<ActionGroupName="ContractManage" OwnerID="RootOrganization">
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
    </ActionGroup>
```

役割ベースのポリシーのリソースとして以前に定義されていたコマンドは、新しくアクションとして定義されます。上記の ContractManage グループの一部であるアクションのサンプル定義を、以下に示します。

```
<Action Name="com.ibm.commerce.contract.commands.ContractCloseCmd"
CommandName="com.ibm.commerce.contract.commands.ContractCloseCmd">
</Action>
```

注: CommandName の値は、リソース・レベルの検査を行うコマンドのインターフェース名に対応する必要があります。

ほとんどのコマンドは、Enterprise Bean と共に実行されます。これらの Bean は通常、リソース・レベルのポリシーが保護しているリソースです。上記のリソース・ポリシーで使用されるリソース・グループの例を以下に示します。

```
<ResourceGroup Name="ContractDataResourceGroup" OwnerId="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.contract.
objects.ContractResourceCategory"/>
</ResourceGroup>
```

この例で、ContractDataResourceGroup は定義済みであり、 1 つのリソースから構成されています。そのリソースは以下のように定義されています。

```
<ResourceCategory Name="com.ibm.commerce.contract.objects.ContractResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.objects.Contract"
 <ResourceAction Name="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
 <ResourceAction Name="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
 <ResourceAction Name="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
</ResourceCategory>
```

ここで、

Name: XML ファイル内の他の場所からこのリソースを参照するためのタグ。

ResourceBeanClass: 保護するリソースを表すクラス。このクラスは、保護可能インターフェースをインプリメントする必要があります。リソースが Enterprise Bean である場合、そのリモート・インターフェースは保護可能インターフェースを拡張する必要があります。

ResourceAction: このリソース上で操作されるアクションを指定します。この情報は特定のリソースに関して有効なアクションを判別するために、管理コンソールによって使用されます。

注: 保護可能インターフェースの詳細は、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」を参照してください。

Data Bean の保護

Data Bean にはビジネス・オブジェクトに関する情報が含まれていて、 Web ページ上にオブジェクト情報を表示するために使用されます。動的 Web ページは、通常 WebSphere Commerce 内のビューにマップされ、それらのビューは役割ベースの

ポリシーによって保護されます。 Data Bean が存在する場合、それを保護することによって Web ページのコンテンツをさらに保護することが必要になる場合があります。

DataBeanManager.activate(..) メソッドを使用して Data Bean に値が取り込まれたとき、Data Bean 管理者はそれらに対するアクセス制御を強制します。 Data Bean は Delegator インターフェースを使用して直接または間接に保護することができます。直接に保護される Data Bean は、保護可能インターフェースもインプリメントします。間接に保護される Data Bean が Delegator インターフェースをインプリメントしない場合、または getDelegate() メソッドに対して NULL 値を戻す場合、それは保護されていないので誰でも表示できます。

注: 保護可能インターフェースについての詳細は、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」を参照してください。

以下は、Data Bean のリソース・レベル・ポリシーの例です。

```
<Policy Name="AllUsersDisplayOrderDataBeanResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="DisplayDataBeanActionGroup"
   ResourceGroupName="OrderDataBeanResourceGroup"
   RelationName="creator"
   PolicyType="groupableStandard">
  </Policy>
```

ActionGroupName の DisplayDataBeanActionGroup は、ポリシーが Data Bean のポリシーであることを示しています。このアクション・グループには、 1 つの Display アクションが含まれます。

ここで、

Name: このポリシーの名前。

UserGroup: ポリシーが適用されるユーザーを含むアクセス・グループ。この場合、すべてのユーザーが含まれます。

ActionGroupName: 値 DisplayDataBeanActionGroup は、それが Data Bean のリソース・レベルのポリシーであることを示しています。

ResourceGroupName: 保護される Data Bean を含むリソース・グループの名前。

RelationName: ユーザーとリソースとの間で満たされなければならない関係。この場合、ユーザーはビジネス Order リソースの作成者でなければなりません。

OrderDataBeanResourceGroup は、以下のように定義されます。

```
<ResourceGroup Name="OrderDataBeanResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.order.beans.
OrderListDataBeanResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.order.beans
.OrderDataBeanResourceCategory"/>
</ResourceGroup>
```

OrderDataBeanResourceGroup は、2 つのリソースから成ります。以下は、Data Bean のリソース定義のサンプルです。

```
<ResourceCategory Name="com.ibm.commerce.order.beans.OrderDataBeanResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.beans.OrderDataBean">
<ResourceAction Name="DisplayDataBean"/>
</ResourceCategory>
```

ここで、

Name: XML ファイル内でこのリソースを参照するためのタグ。

ResourceBeanClass: 直接に保護されている Data Bean のクラス名。このクラスは、保護可能インターフェースをインプリメントする必要があります。

ResourceAction: 管理コンソールでポリシーを編集するために必要なエレメント。この場合、このエレメントは Display がこのリソースに対して実行される有効なアクションであることを示しています。

リソースの属性別のグループ化

リソース・グループは ACRESGRP 表の CONDITIONS 列を使用して、直接に定義することができます。 CONDITIONS 列には、リソースのグループ化に使用される制約と属性値のペアを含む XML 文書が保管されます。このタイプのリソース・グループは暗黙的リソース・グループと呼ばれ、通常はリソースのクラス名が不十分であるときに使用されます。たとえば、アクセス制御ポリシーが、状況が P (保留) または E (顧客サービス担当者による編集中) である Order リソースに適用される場合、それに対してリソース・グループを定義できます。

注: リソースをクラス名ではなく属性ごとにグループ化するには、そのリソースが Groupable インターフェースをインプリメントしていなければなりません。グループ化可能なインターフェースの詳細は、「*WebSphere Commerce プログラミング・ガイドとチュートリアル*」を参照してください。

以下は、Order リソース・グループの例です。

```
<ResourceGroup  Name="OrderResourceGroupwithPEStatus"
      OwnerID="RootOrganization">
  <ResourceCondition>
   <![CDATA[
    <profile>
     <andListCondition>
   <orListCondition>
        <simpleCondition>
         <variable name="Status"/>
         <operator name="="/>
         <value data="P"/>
        </simpleCondition>
        <simpleCondition>
         <variable name="Status"/>
         <operator name="="/>
         <value data="E"/>
        </simpleCondition>
    </orListCondition>
        <simpleCondition>
         <variable name="classname"/>
         <operator name="="/>
         <value data="com.ibm.commerce.order.objects.Order"/>
        </simpleCondition>
      </andListCondition>
     </profile>
```

```
   ]]>
  </ResourceCondition>

 </ResourceGroup>
```

ここで、

Name: ACRESGRP 表の GRPNAME 列に保管されているリソース・グループの名前。

OwnerID: リソース・グループの所有者。これはルート組織でなければなりません。

<ResourceCondition>: リソース・グループを定義するために ACRESGRP 表の CONDITIONS 列にロードされるデータを指定します。

<![CDATA[...]]>: 入力されたままの状態で使用される文字データのセクション。

<profile>: すべてのリソース条件に必要なパラメーター。

リソース・グループ定義の重要なコンポーネントは、 name="classname" を持つ <simpleCondition> エレメントです。このエレメントは、グループが適用されるリソースの Java クラスを識別します。 Java クラス com.ibm.commerce.order.objects.Order は、以下の例に示されています。

```
<simpleCondition>
   <variable name="classname"/>
   <operator name="="/>
   <value data="com.ibm.commerce.order.objects.Order"/>
   </simpleCondition>
```

以下の例は、状況が P でなければならないという、com.ibm.commerce.objects.order.objects.Order リソースの条件を指定します。

```
<simpleCondition>
 <variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
   </simpleCondition>
```

上記の例で、 <variable name="*value*"/> はリソースに対して getGroupingAttributeValue (String attributeName, GroupContext context)() メソッドによって認識される属性名を表しています。このメソッドは、Groupable インターフェースの一部です。 WebSphere Commerce 管理コンソール内で暗黙的リソース・グループを管理するために、その属性は ACATTR 表内でも定義して、ACRESATREL 表内のリソースと関連付ける必要があります。指定のリソースとアクションのために適切なポリシーを検索するときになると、getGroupingAttributeValue(..) メソッドが呼び出されて、この条件が検査されます。この場合、これは Status 内で attributeName パラメーターとして渡されます。

<orListCondition> は、このブロック内の条件をブール OR を使用して適用する必要があることを示しています。この場合、状況は P または E のいずれかです。<andListConditon> は、このブロック内の条件をブール AND を使用して適用する必要があることを示しています。この場合、(Classname = com.ibm.commerce.order.objects.Order) AND (Status = P OR Status=E) となります。

ACATTR 表に値を取り込むための属性定義のサンプルを、以下に示します。

```
<Attribute Name="Status" Type="String">
</Attribute>
```

Name エレメントは属性を識別する用語であり、 Type エレメントは属性のデータ・タイプを識別します。属性の値としては、以下が可能です。

- String
- Integer
- Double
- Currency
- Decimal
- URL
- Image
- Date

属性のリソースへの関連付けは、リソース定義内で指定されます。たとえば、以下の例で Status 属性は OrderResourceCategory に関連付けられています。

```
<ResourceCategory Name="com.ibm.commerce.order.objects.OrderResourceCategory"
     ResourceBeanClass="com.ibm.commerce.order.objects.Order" >

  <ResourceAttributes Name="Status"
   AttributeTableName="ORDERS"
   AttributeColumnName="STATUS"
   ResourceKeyColumnName="ORDERS_ID"/>
</ResourceCategory>
```

ここで、

<ResourceAttributes>: 属性をリソースに関連付けるコードのブロック。

AttributeTableName: リソースのデータベース表の名前。

AttributeColumnName: リソース表内で属性を保管する列の名前。

ResourceKeyColumnName: リソース表内で主キーを保管する列の名前。

関係の定義

アクセス制御ポリシーには、オプションの関係エレメントがあります。この関係は、XML ポリシーを以下に示す関係定義と共にロードすることによってのみ作成されます。

```
  <Relation Name="value">
   </Relation>
```

Name エントリーは、任意のポリシーで使用される関係の名前で、 ACRELATION 表に追加されるものです。 Name は、保護可能リソース上の fulfills() メソッドの関係パラメーターに対応します。

以下の例は、creator と呼ばれる関係の定義を表示します。

```
<Relation Name="creator">
</Relation>
```

関係グループの定義

関係グループは、関係グループに属するための条件であるオープン条件を含んでいます。関係グループを定義する必要がある場合、関係グループ情報を XML ファイル内に定義するか、または以下のように defaultAccessControlPolicies.xml ファイルを変更することによって行う必要があります。

```
<RelationGroup
  Name="aValue"
  OwnerID="Root Organization">
  <RelationCondition><![CDATA[
   <profile>
    Relationship Chain Open Condition XML
   </profile>
  ]]></RelationCondition>
 </RelationGroup>
```

関係チェーン

各関係グループは、andListCondition または orListCondition エレメントによってグループ化された 1 つ以上の RELATIONSHIP_CHAIN オープン条件で構成されます。関係チェーンとは、1 つ以上の一連の関係のことです。関係チェーンの長さは、その関係チェーンを構成している関係の数によって決まります。これは、関係チェーンの XML 表記内にある <parmeter name= "X" value="Y"> エントリーの数を調べることによって判別できます。以下は、長さが 1 の関係チェーンの例です。

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

ここで、

aValue: ユーザーとリソースの間の関係を表すストリングです。このストリングは、リソースの fulfills メソッドで検査されるいずれかの関係でなければなりません。

関係チェーンの長さが 2 以上であるとき、それは 2 つの関係の系列となります。最初の <parmeter name= "X" value="Y"> エントリーは、ユーザーと組織エンティティーとの間の関係です。最後の <parmeter name= "X" value="Y"> エンティティーは、組織エンティティーとリソースとの間の関係です。チェーン内にある中間の <parmeter name= "X" value="Y"> エントリーは、組織間の関係です。以下は、長さが 2 の関係チェーンの例です。

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

ここで、

aValue1 : 可能な値には、HIERARCHY および ROLE があります。 HIERARCHY は、メンバーシップ階層内のユーザーと組織エンティティーとの間に階層関係があることを示しています。 ROLE は、ユーザーが組織エンティティーでの役割を果たしていることを示しています。 aValue1 の値が HIERARCHY である場合、aValue2 の可能な値には child が含まれます。これは、ユーザーがメンバー階層内で直接の子となっている組織エンティティーを戻します。 aValue1 の値が ROLE である場合、

aValue2 の可能な値には ROLE 表の NAME 列にある有効なエンティティーが含まれます。これは、現行ユーザーがこの役割を果たしているすべての組織エンティティーを戻します。

aValue3: 最初のパラメーターとリソースを評価することによって検索される、 1 つ以上の組織エンティティーの間の関係を表すストリング。この値は、保護可能リソース上の fulfills() メソッドの関係パラメーターに対応します。パラメーター aValue1 を評価することによって複数の組織エンティティーが戻される場合、RELATIONSHIP_CHAIN のこの部分は、これらの組織エンティティーの 1 つ以上がパラメーター aValue2 によって指定される関係を満たす場合に満たされます。

注: 関係グループを定義する方法についての詳細は、 171 ページの『関係グループの定義』を参照してください。

単一チェーン関係グループの定義

アクセス制御ポリシーの一部としてユーザーが組織エンティティー (リソースの BuyingOrganizationalEntity など) に属することを強制する必要がある場合、長さが 2 の関係チェーン 1 つから成る関係グループを作成しなければなりません。以下に、この例を示します。

```
<RelationGroup Name="MemberOf->BuyerOrganizationEntity"
OwnerID="RootOrganization
<RelationCondition><![CDATA[
<profile>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="HIERARCHY" value="child"/>
<parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
</profile>
]]><RelationCondition>
<RelationGroup>
```

2 つの異なる関係から成るために、関係チェーンの長さは 2 です。最初の関係は、ユーザーとその親である組織エンティティーとの間の関係です。ユーザーは、その関係の子です。 2 番目の関係では、アクセス制御ポリシー管理者が親である組織エンティティーがリソースとの BuyingOrganizationalEntity 関係を満たしているかどうかを検査します。つまり、それがリソースの購買組織エンティティーである場合、true が戻されます。

注: openCondition タグについての詳細は、「 *WebSphere Commerce アクセラレーター カスタマイズ・ガイド*」を参照してください。

別の例としては、ユーザーがリソースの購買組織エンティティーである組織エンティティーのアカウント担当者の役割を持つように強制する必要がある場合です。この場合にも、長さが 2 の関係チェーン 1 つから成る関係グループが使用されます。チェーンの最初の部分は、ユーザーがアカウント担当者の役割を持つ組織エンティティーをすべて検索します。その後、組織エンティティーのセットについて、アクセス制御ポリシー管理者がそれらの 1 つ以上がリソースとの BuyingOrganizationalEntity 関係を満たしているかどうかを検査します。満たしている場合、値の true が戻されます。

以下の例は、このタイプの関係グループを定義する方法について示しています。

```
<RelationGroup Name="AccountRep->BuyerOrganizationalEntity"
OwnerID="RootOrganization">
<RelationCondition><![CDATA[
<profile>
 <openCondition name="RELATIONSHIP_CHAIN">
 <parameter name="ROLE" value="Account Representative"/>
 <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
 </profile>
]]><RelationCondition>
<RelationGroup>
```

複数チェーン関係グループの定義

複数チェーンの関係から成る関係グループを作成する必要がある場合、ユーザーがすべての関係チェーンを満たす必要があるか (AND シナリオであるか)、またはユーザーが関係チェーンの 1 つ以上を満たす必要があるのか (OR シナリオであるか) を指定しなければなりません。

以下の例では、ユーザーはリソースの作成者で、リソース内で指定された BuyingOrganizationalEntity に属していなければなりません。ユーザーがリソースの作成者でなければならないことを指定する最初のチェーンは、長さが 1 です。ユーザーがリソースで指定された BuyingOrganizationalEntity に属していなければならないことを示す 2 番目のチェーンは、長さが 2 です。

```
<RelationshipGroup Name="Creator_And_MemberOf->BuyerOrganizationalEntity"
 OwnerID="RootOrganization">
<RelationCondition><![CDATA[
<profile>
<andListCondition>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP" value="creator" />
</openCondition>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="HIERARCHY" value="child"/>
<parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
</andListCondition>
</profile>
]]></RelationCondition>
</RelationGroup>
```

注: ユーザーが 2 つの関係チェーンのいずれかを満たさなければならないことにする場合、 <andListConditon> タグを <orListConditon> タグに変更してください。

アクセス・グループ

WebSphere Commerce の一部であるデフォルトのアクセス・グループは、*WC_installdir*/xml/policies/xml/ACUserGroups_locale.xml などの言語に特定の XML ファイル内にあります。このファイルは、*WC_installdir*/xml/policies/dtd/ACUserGroups_en_US.dtd によって指定される DTD の直後にあります。

以下は、アクセス・グループ・エレメントの形式です。

```
<UserGroup Name="value"
   OwnerID="value"
   Description="value"

   <UserCondition>
```

```
      <![CDATA[
        <profile>
         Condition XML
        </profile>
      ]]>
    </UserCondition>
</UserGroup>
```

ここで、

Name: MBRGRP 表の MBRGRPNAME 列に保管されたアクセス・グループの名前。

OwnerID: このアクセス・グループを所有する Member ID。 Name と OwnerID との組み合わせは、固有でなければなりません。使用可能な特殊値としては、RootOrganization (-2001) や DefaultOrganization (-2000) があります。

Description (オプション): アクセス・グループの説明に使用されるオプションの属性。

UserCondition (オプション): このアクセス・グループ内のメンバーシップの暗黙条件を指定するオプションのエレメント。この基準は、MBRGRPCOND 表の CONDITIONS 列に保管されています。

Condition XML: 条件フレームワークを使用する、orListCondition、andListCondition、simpleCondition、および trueConditionCondition エレメントの有効な組み合わせ。

以下の SimpleCondition 名が、UserCondition エレメントのためにサポートされています。

表 13. サポートされている単純条件名

変数名	説明	サポートされている演算子	サポートされている値	修飾子	修飾子の値
role	ユーザーがこの役割を MBRROLE 表内に持っていなければならないことを指定します。	= !=	ROLE 表内の NAME 列の任意の値。	org (指定されない場合、ユーザーは MBRROLE 表内の組織に対する役割を持っていなければなりません。)	• OrgEntityID : ユーザーが役割を持っていなければならない場所。 • OrgAndAncestorOrgs: それがグループ化可能なテンプレート・ポリシー内で使用される時。これにより、ユーザーが、リソースを所有する組織またはその上位組織で、指定した役割を持っているかどうかを検査します。
registration status	ユーザーにこの登録状況がなければならないことを指定します。	= !=	USERS 表内の REGISTER-TYPE 列の任意の値。ゲストを表す G や、登録済みを表す R など。	none	適用外

表 13. サポートされている単純条件名 (続き)

変数名	説明	サポートされている演算子	サポートされている値	修飾子	修飾子の値
status	ユーザーにこのメンバー状態がなければならないことを指定します。これは通常、登録承認の状況に関して使用されます。	= !=	MEMBER 表内の STATE 列の任意の値。登録承認が保留中であることを表す 0 、登録が承認されたことを表す 1、登録が拒否されたことを表す 2 など。	none	適用外
org	ユーザーが、指定した組織の子であることを指定します。この情報は、MBRREL 表に保管されたデータに基づきます。	= !=	• ORGENTITY 表内の ORGENTITY_ID の任意の値。 • ?: これがグループ化可能なテンプレート・ポリシーの場合。これにより、ユーザーがリソースを所有する組織の子であるかどうかを検査します。さらに、ユーザーがリソース所有者の先祖 (ポリシー・グループに加入している、一番近い先祖まで) の子であるかどうかも検査します。	none	適用外

アクセス・グループの simpleCondition の例

role:

修飾子なしの role: 以下の例は、役割ベースのポリシーで最も普通に使用される、修飾子のない role simpleCondition を表示します。この例では、ユーザーは組織エンティティーに対するセラー管理役割を持っていなければなりません。

```
<UserConditon>
  <![CDATA[
  <profile>
   <simpleCondition>
    <variable name="role"/>
    <operator name="="/>
    <value data="Seller Administrator"/>
```

```
   </simpleCondition>
  </profile>
]]>
</UserCondition>
```

修飾子のある role: 以下の例は、組織レベルのポリシーで最も普通に使用される、修飾子のある role simpleCondition を表示します。この例では、ユーザーは ORGENTITY_ID = 100 を指定した組織エンティティーに対するセラー役割を持っていなければなりません。

```
<UserCondition>
   <!CDATA[
  <profile>
    <simpleCondition>
    <variable name="role"/>
    <operator name="="/>
    <value data="Seller"/>
     <qualifier name="org" data="100"/>
    <simpleCondition>
  </profile>
]]>
</UserCondition>
```

修飾子とパラメーターのある role: 以下の例は、修飾子のある役割 simpleCondition と特殊データ値 OrgAndAncestorOrgs を表示します。この修飾データ値 OrgAndAncestorOrgs は、グループ化可能なテンプレート・ポリシーだけで有効です。この例では、ユーザーはリソースを所有する組織、またはその組織の上位組織内でセールス・マネージャー、アカウンティング・マネージャー、またはセラーの役割を持っていなければなりません。

```
<UserCondition><!CDATA[
  <profile>
   <orListCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Sales Manager"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Account Representative"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Seller"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
   </orListCondition>
  </profile/>
]]></UserCondition>
```

registrationStatus: 以下の例では、registrationStatus simpleCondition が表示されます。この例では、ユーザーは登録済み (USERS.REGISTERTYPE = R) であることが必要です。

```
<UserCondition><!CDATA[
  <profile>
  <simpleCondition>
   <variable name="registrationStatus"/>
```

```
   <operator name="="/>
   <value data="R"/>
  </simpleCondition>
  </profile>
]]></UserCondition>
```

status: 以下の例では、status simpleCondition が表示されます。この例では、ユーザーは登録が承認されていることが必要です。 (MEMBER.STATUS = 1)

```
<UserCondition><![CDATA[
  <profile>
    <simpleCondition>
     <variable name="status"/>
     <operator name="="/>
     <value data="1"/>
     </simpleCondition>
  </profile>
]]></UserCondition>
```

org: 以下の例では、org simpleCondition が表示されます。この例では、ユーザーは組織エンティティー 100 に登録されていることが必要です。 MBRREL 表では、ユーザーが ANCESTOR_ID = 100 および SEQUENCE = 1 を持つ組織の子孫になっているレコードが必要です。

```
<UserCondition><![CDATA[
  <profile>
   <simpleCondition>
    <variable name="org"/>
    <operator name="="/>
    <value data="100"/>
   </simpleCondition>
  </profile>
]]>
</UserCondition>
```

ポリシー

WC_installdir/xml/policies/xml/defaultAccessControlPolicies.xml ファイルは、組み込まれずに出荷されるデフォルトのアクセス制御ポリシーを定義します。これは *WC_installdir*/xml/policies/dtd/accesscontrolpolicies.dtd によって定義される DTD の後に続きます。

以下は、ポリシー・エレメントのテンプレートです。

```
<Policy Name="value"
  OwnerId="value"
  UserGroup="value"
  UserGroupOwner="value"
  ActionGroupName="value"
  ResourceGroupName="value"
  PolicyType="value"
  RelationName="value"
  RelationGroupName="value"
  RelationGroupOwner="value"
</Policy>
```

ここで、

Name: ポリシーの名前。これは ACPOLICY 表の POLICYNAME 列にロードされます。Name と OwnerID は、共に固有でなければなりません。

OwnerID: ポリシーを所有する組織エンティティーのメンバー ID。これは ACPOLICY 表の member_id 列にロードされます。 OwnerID と Name は、共に固有でなければなりません。トランスフォーマー・ツールによって認識される 2 つの特殊値があります。それらは、RootOrganization: -2001 および DefaultOrganization: -2000 です。

UserGroup: MBRGRP 表の MBRGRPNAME 列で指定されたアクセス・グループの名前。これは ACPOLICY 表の mbrgrp_id 列にロードされます。デフォルトのアクセス・グループは、 *WC_installdir*/xml/policies/xml/ACUserGroups_language.xml ファイルに定義されています。

UserGroupOwner: アクセス・グループを所有するメンバーのメンバー ID。これは、アクセス・グループがポリシー所有者以外のメンバーによって所有されている場合に必要です。これが指定されていない場合、アクセス・グループは OwnerID 属性が指定するメンバーによって所有されていると想定されます。

ActionGroupName: ACACTGRP 表の GROUPNAME 列で指定されているアクション・グループの名前。これを使用して、ACPOLICY 表に格納される対応するアクション・グループ ID (ACACTGRP_ID) を取得します。コントローラー・コマンド用の役割ベースのポリシーでは、 ActionGroupName が ExecuteCommandActionGroup に設定されています。 Data Bean のポリシーでは、 ActionGroupName が DisplayDatabeanActionGroup に設定されています。

ResourceGroupName: ACRESGRP 表の GRPNAME 列で指定されているリソース・グループの名前。これを使用して、ACPOLICY 表に格納される対応するリソース・グループ ID (ACRESGRP_ID) を取得します。ビューに対する役割ベースのポリシーでは、ResoureGroupName が ViewCommandResourceGroup に設定されています。

PolicyType: ポリシーのタイプ。有効値は groupableStandard および groupableTemplate です。後方互換性のために、standard と template の値もサポートされます。新規ポリシーのロード時にこの属性が指定されていない場合、ヌルの値が使用されます。既存ポリシーの更新時にこの属性が指定されていない場合、値は変更されません。以下の表は、ストリング値と ACPOLICY 表の POLICYTYPE 列に格納されたデータベース値との対応を示しています。

表 14. ストリング値とデータベース値の対応

String	ACPOLICY.POLICYTYPE
groupableTemplate	3
groupableStandard	2
template	1
standard	0 またはヌル

ポリシーのタイプについての詳細は、 19 ページの『第 3 章 許可の概念』を参照してください。

RelationName (オプション): ACRELATION 表の RELATIONNAME 列に指定されている、関係の名前。指定されている場合、これを使用して、ACPOLICY 表に格納される対応する関係 ID (ACRELATION_ID) を取得します。

RelationGroupName (オプション): ACRELGRP 表の GRPNAME 列に指定されている、関係グループの名前。この属性が指定されている場合、関係グループが優先されるため、RelationName は指定しないでください。

RelationGroupOwner: 関係グループを所有するメンバー ID。この属性が必要なのは、RelationGroupName 属性が指定されていて、 OwnerID 属性の値が RootOrganization ではないときだけです。その場合、RelationGroupOwner に RootOrganization (-2001) を指定しなければなりません。

ポリシーの例

役割ベースのポリシー:

コントローラー・コマンドの場合: この例では、AllUsers アクセス・グループに属するユーザーが AllUserCmdResourceGroup リソース・グループに属するコントローラー・コマンドを実行できます。

```
<Policy Name="AllUsersExceuteAllUserCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="AllUserCmdResourceGroup"
   PolicyType="groupableStandard">
</Policy>
```

ビューの場合: この例では、 MarketingManagers アクセス・グループに属するユーザーが MarketingManagersViews アクション・グループに属するビューを実行できます。

```
<Policy Name="MarketingManagersExecuteMarketingManagersViews"
   OwnerID="RootOrganization"
   UserGroup="MarketingManagers"
   ActionGroupName="MarketingManagersViews"
   ResourceGroupName="ViewCommandResourceGroup"
   PolicyType="groupableStandard">
</Policy>
```

リソース・レベルのポリシー:

コマンドの場合: この例では、AllUsers アクセス・グループに属するユーザーは、ユーザーがリソースに関する creator 関係を満たしている限り、CouponWalletResourceGroup によって指定されたリソースに対して CouponRedemption アクション・グループによって指定されたアクションを実行できます。

```
<Policy Name="AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="CouponRedemption"
   ResourceGroupName="CouponWalletResourceGroup"
   RelationName="creator"
   PolicyType="groupableStandard">
</Policy>
```

Data Bean の場合: この例では、AllUsers アクセス・グループに属するユーザーは、そのユーザーがリソースに関する owner 関係を満たしている限り、UserDatabeanResourceGroup リソース・グループによって指定される Data Bean を表示できます。

```
<Policy Name="AllUsersDisplayUserDatabeanResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="DisplayDatabeanActionGroup"
   ResourceGroupName="UserDatabeanResourceGroup"
   RelationName="owner"
   PolicyType="groupableStandard">
</Policy>
```

グループ化が可能なテンプレート・ポリシー: この例では、

```
OrgAdminConsoleMembershipAdministratorsForOrg
```

アクセス・グループに属するユーザーは、OrganizationDataResourceGroup によって指定されたリソースに対して ApproveGroupUpdate アクション・グループによって指定されたアクションを実行できます。

```
<Policy Name="OrgAdminConsoleMembershipAdministratorsForOrgExecuteApprove
GroupUpdateCommandsOnOrganizationResource"
   OwnerID="RootOrganization"
   UserGroup="OrgAdminConsoleMembershipAdministratorsForOrg"
   ActionGroupName="ApproveGroupUpdate"
   ResourceGroupName="OrganizationDataResourceGroup"
   PolicyType="groupableTemplate">
</Policy>
```

OrgAdminConsoleMembershipAdministratorsForOrg アクセス・グループの定義を調べると、メンバーについての以下の条件が明らかになります。

```
<UserCondition>

 <profile>
    <orListCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Buyer Administrator"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Seller Administrator"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Channel Manager"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
    </orListCondition>
   </profile>
  UserCondition>
```

注: role の simpleCondition は、 org = **OrgAndAncestorOrgs** によって修飾されます。 OrgAndAncestorOrgs は、グループ化が可能なテンプレート・ポリシーでのみ使用可能なキーワードです。これは、役割を、現在のリソースの所有者のコンテキストに動的に範囲指定します。この例では、ユーザーはリソースを所有する組織、またはその組織の上位組織内で、いずれかの指定した役割を持っていなければなりません。

ポリシー・グループの定義

ポリシー・グループは、ビジネスおよびアクセス制御要件に基づき、ポリシーをグループ分けするときに作成されます。いくつかのデフォルト・ポリシー・グループは、最初から作成されています。詳細は、 229 ページの『デフォルトのアクセス制御ポリシーおよびグループ』を参照してください。他のポリシー・グループは、ストアまたはビジネス・モデルの公開中に必要に応じて作成されます。ほとんどの場合、作成する新しいポリシーを、既存のポリシー・グループへ追加するだけで構いません。新しいポリシー・グループを作成する必要がある場合、defaultAccessControlPolicies.xml のような XML ファイルでそれを定義してから、データベースにロードする必要があります。サンプル定義は、以下のとおりです。

```
<PolicyGroup Name="aValue" OwnerID="aValue">
 </PolicyGroup>
```

ここで、

Name: ポリシー・グループの名前。

OwnerID: ポリシー・グループを所有する組織エンティティーのメンバー ID。これは ACPOLGRP 表の member_id 列にロードされます。 OwnerID と Name は、共に固有でなければなりません。トランスフォーマー・ツールによって認識される 2 つの特殊値があります。それらは、RootOrganization: -2001 および DefaultOrganization: -2000 です。

ポリシーとポリシー・グループとの関連付け

ポリシーは、複数のポリシー・グループに属することも可能です。しかし、ポリシーの管理を簡単にするため、ポリシーは 1 つのポリシー・グループだけに属させるようお勧めします。この関連付けは、defaultAccessControlPolicies.xml のような XML ファイルで定義してから、データベースへロードするようにします。サンプル定義は、以下のとおりです。

```
<PolicyGroup Name="aValue" OwnerID="aValue">
  <PolicyGroupPolicy  Name="aValue" PolicyOwnerID="aValue" />
</PolicyGroup>
```

ここで、

PolicyGroupPolicy Name: 指定したポリシー・グループに関連付けるものとして以前に定義したポリシーの名前。このポリシーは、groupableStandard または groupableTemplate のいずれかのポリシー・タイプでなければなりません。

PolicyGroupPolicy PolicyOwnerID (オプション): 指定したポリシーを所有する組織エンティティーのメンバー ID。このパラメーターを指定しない場合、デフォルト値はポリシー・グループの OwnerID です。トランスフォーマー・ツールによって認識される 2 つの特殊値があります。それらは、RootOrganization: -2001 および DefaultOrganization: -2000 です。

ポリシー・グループへの加入

組織のリソースは、その組織が加入するポリシー・グループのポリシーに保護されます。その組織がポリシー・グループに加入していない場合、その組織の一番近い上位組織が加入しているポリシー・グループが適用されます。組織が加入する必要

のあるポリシー・グループの詳細は、 229 ページの『デフォルトのアクセス制御ポリシーおよびグループ』を参照してください。

ポリシー・グループの加入は、組織管理コンソールで行えますが、defaultAccessControlPolicies.xml のような XML ファイルで定義してから、データベースにロードすることもできます。サンプル定義は、以下のとおりです。

```
<PolicyGroup Name="aValue" OwnerID="aValue">
  <PolicyGroupSubscription OrganizationID="aValue"/>
 </PolicyGroup>
```

ここで、

OrganizationID: このポリシー・グループに加入している組織エンティティーのメンバー ID。トランスフォーマー・ツールによって認識される 2 つの特殊値があります。それらは、RootOrganization: -2001 および DefaultOrganization: -2000 です。

変換可能なポリシー・データ

以下は、変換可能なポリシー・データを定義するのに使用できる、カスタマイズ済みポリシー・ファイルのテンプレートです。

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
 <!--The following TRANSLATABLE access control elements should
 be defined in this file:
 <Attribute_nls>
 <Action_nls>
 <Relation_nls>
 <ResourceCategory_nls>
 <ActionGroup_nls>
 <ResourceGroup_nls>
 <Policy_nls>
 <PolicyGroup_nls>-->
<!DOCTYPE PoliciesNLS SYSTEM "../dtd/accesscontrolpoliciesnls.dtd">

<PoliciesNLS LanguageID="value">


 <!--Insert access control element definitions here -->
 </PoliciesNLS>
```

LanguageID 属性は、言語特有のデータに対応するストリングです。 LanguageID の値としては、以下が有効です。

- en_US
- fr_FR
- de_DE
- it_IT
- es_ES
- pt_BR
- zh_CN
- zh_TW
- ko_KR
- ja_JP

変換できないポリシー・データ

以下は、変換できないデータを含むカスタマイズ済みポリシー・ファイルのテンプレートです。

```
   <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>

<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

 <!--The following NON-TRANSLATABLE access control elements
 should be defined in this file:

 <Attribute>
 <Action>
 <ResourceCategory>
 <Relation>
 <RelationGroup>
 <ActionGroup>
 <ResourceGroup>
 <Policy>
 <PolicyGroup>-->
<Policies>

 <!--Insert access control element definitions here-->
 </Policies>
```

言語特有のデータ

以下に示すオプションの言語特有のデータをロードして、変換不可の XML ファイルに定義済みのアクセス制御エレメントに記述を追加することができます。デフォルトの言語特有のデータは、以下のアドレスにあります。

WC_installdir¥xml¥policies¥xml¥
defaultAccessControlPolicies_*locale*.xml

たとえば、defaultAccessControlPolicies_en_US.xml です。

属性: 以下の例は、追加の属性エレメント情報を定義します。

```
<Atrribute_nls AttributeName="Status"
DisplayName_nls="Status attribute"
Description_nls="Resource status attribute"
/>
```

ここで、

AttributeName: 属性の名前。この値は ACATTR 表の ATTRNAME 列に保管されます。

DisplayName_nls: 属性の表示名。この値は ACATTRDESC 表の DISPLAYNAME 列に保管されます。

Description_nls: 属性のオプションの記述。この値は ACATTRDESC 表の DESCRIPTION 列に保管されます。

アクション: 以下の例は、追加のアクション・エレメント情報を定義します。

```
<Action_nls ActionName="OrderAdjustmentButton"
DisplayName_nls="Order Adjustment Button View"
Description_nls="The view for loading buttons in the order adjustment page
 when placing an order from Commerce Acclerator"
/>
```

ここで、

ActionName: アクションの名前。この値は ACACTION 表の ACTION 列に保管されます。

DisplayName_nls: アクションの表示名。この値は ACACTDESC 表の DISPLAYNAME 列に保管されます。

Description_nls: アクションのオプションの記述。この値は ACACTDESC 表の DESCRIPTION 列に保管されます。

関係: 以下の例は、追加の関係エレメント情報を定義します。

```
<Relation_nls RelationName="creator"
DisplayName_nls="creator"
Description_nls="creator"
/>
```

ここで、

RelationName: 関係の名前。この値は ACRELATION 表の RELATIONNAME 列に保管されます。

DisplayName_nls: 関係の表示名。この値は ACRELDESC 表の DISPLAYNAME 列に保管されます。

Description_nls: 関係のオプションの記述。この値は ACRELDESC 表の DESCRIPTION 列に保管されます。

リソース・カテゴリー: 以下の例は、追加のリソース・カテゴリー情報を定義します。

```
<ResourceCategory_nls ResourceCategoryName="com.ibm.commerce.
catalog.objects."InterestItemList"
DisplayName_nls="Interest Item List"
Description_nls="Interest Item List command"
/>
```

ここで、

ResourceCategoryName: リソース・カテゴリーの名前。この値は ACRESCGRY 表の RESCLASSNAME 列に保管されます。

DisplayName_nls: リソース・カテゴリーの表示名。この値は ACRSCGDES 表の DISPLAYNAME 列に保管されます。

Description_nls: リソース・カテゴリーのオプションの記述。この値は ACRSCGDES 表の DESCRIPTION 列に保管されます。

アクション・グループ: 以下の例は、追加のアクション・グループ情報を定義します。

```
<ActionGroup_nls ActionGroupName="DoEverything"
DisplayName_nls="Do Everything"
Description_nls="Permits access to all Actions"
/>
```

ここで、

ActionGroupName: アクション・グループの名前。この値は ACACTGRP 表の GROUPNAME 列に保管されます。

DisplayName_nls: アクション・グループの表示名。この値は ACACGPDESC 表の DISPLAYNAME 列に保管されます。

Description_nls: アクション・グループのオプションの記述。この値は ACACGPDESC 表の DESCRIPTION 列に保管されます。

リソース・グループ: 以下の例は、追加のリソース・グループ情報を定義します。

```
<ResourceGroup_nls ResourceGroupName="AllResourceGroup"
DisplayName_nls="All Resources Group"
Description_nls="All Resources"
/>
```

ここで、

ResourceGroupName: リソース・グループの名前。この値は ACRESGRP 表の GRPNAME 列に保管されます。

DisplayName_nls: リソース・グループの表示名。この値は ACRESGPDES 表の DISPLAYNAME 列に保管されます。

Description_nls: リソース・グループのオプションの記述。この値は ACRESGPDES 表の DESCRIPTION 列に保管されます。

ポリシー: 以下の例は、追加のポリシー情報を定義します。

```
<Policy_nls PolicyName="SiteAdministratorsCanDoEverything"
   OwnerID="RootOrganization"
DisplayName_nls="Site Administrators Can Do Everything"
Description_nls="Policy that allows Site Administrators to do everything"
/>
```

ここで、

PolicyName: アクセス制御ポリシーの名前。この値は ACPOLICY 表の POLICYNAME 列に保管されます。

OwnerID: このポリシーを所有する組織エンティティーのメンバー ID。

DisplayName_nls: ポリシーの表示名。この値は ACPOLDESC 表の DISPLAYNAME 列に保管されます。

Description_nls: ポリシーのオプションの記述。この値は ACPOLDESC 表の DESCRIPTION 列に保管されます。

ポリシー・グループ: 以下の例は、追加のポリシー・グループ情報を定義します。

```
<PolicyGroup_nls PolicyGroupName="B2CPolicyGroup" OwnerID="RootOrganization"
  DisplayName_nls="B2C Policy Group"
  Description_nls="This policy group contains all the B2C specific policies."
 />
```

ここで、

PolicyGroupName: 追加情報が追加されるアクセス制御ポリシー・グループの名前。この値は、ACPOLGRP 表の NAME 列にあります。

OwnerID: このポリシー・グループを所有する組織エンティティーのメンバー ID。

DisplayName_nls: ポリシー・グループの表示名。この値は ACPLGPDESC 表の DISPLAYNAME 列に保管されます。

Description_nls: ポリシー・グループのオプションの記述。この値は ACPLGPDESC 表の DESCRIPTION 列に保管されます。

XML ファイルを変更した後に

変更をテストする

変更を検査する方法についての詳細は、115 ページの『ポリシーの変更後に』を参照してください。

変更をデータベースにロードする

XML ファイルを直接作業してポリシーを変更した場合、変更された XML ファイルをロードしてデータベースに戻さなければなりません。以下に示すいくつかの理由により、 XML ファイルとデータベース内のアクセス制御情報との間の整合性を保つことは重要です。

- WebSphere Commerce のインスタンスを作成するとき、ポリシーおよびアクセス・グループ定義は XML ファイルからロードされます。
- WebSphere Commerce の 2 番目のインスタンスで同じアクセス制御ポリシーをインプリメントしたい場合、 2 番目のインスタンスを作成する前に XML ファイルを適切なディレクトリーにコピーすることができます。
- XML ファイルはポリシーとそのコンポーネント・パーツを直接表示して編集するための便利な手段となるので、それらのファイルを最新の状態に保守することは大切です。

XML の変更をデータベースにロードする

ロード処理は、アクセス制御ポリシー情報およびアクセス・グループ定義を含む XML ファイルを読み取り、それらを適切なデータベースにロードします。 XML ファイルに含まれるポリシーおよびアクセス・グループ情報はインストール時にロードされます。しかし、それらのファイルに変更を加えた場合、再ロードしなければなりません。

注:

1. カスタマイズされた XML ファイルを作成する場合、それらを *<WC_installdir>*/xml/policies/xml ディレクトリーにコピーして、データベースにロードできるようにしてください。
2. ロードするスクリプトには、ID を解決してデータをデータベースにロードするときに、 "-maxerror 100000" というパラメーター設定を指定する設定があります。これは、データのロード中の外部キー違反が 100000 までであれば、打ち切

られずに無視されるということです。この値は、必要に応じて増やすことも減らすこともできます。たとえば、そのようなエラーが 1 つ生じても停止する場合は、値を 1 に変更します。

400 では：カスタマイズされた XML ファイルを作成する場合、ファイル内の DTD への絶対パスを使用しなければなりません。アクセス制御ポリシー DTD は、 *WC_installdir*/xml/policies/dtd にあります。

アクセス・グループおよびアクセス制御ポリシーをロードするには、以下のコマンドを実行します。

2000 では：

1. ディレクトリー <*WC_installdir*>¥bin から、必要に応じてここにリストされた順序で以下のコマンド・ファイルを実行します。
   - ユーザー (アクセス) グループ定義をロードするには、 **acugload** コマンド・ファイルを実行します。**構文**: acugload.cmd <*database name*> <*database user*> <*database user password*> <*UserGroups xml file*>[*schema name*] **例**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml
   - メイン・アクセス制御ポリシー・ファイルをロードするには、 **acpload** コマンド・ファイルを実行します。 **構文:**acpload.cmd <*database name*> <*database user*> <*database user password*> <*Policies xml file*>[*schema name*] **例**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
   - 表示名および説明ファイルをロードするには、 **acpnlsload** コマンド・ファイルを実行します。 **構文:** acpnlsload.cmd <*database name*> <*database user*> <*database user password*> <*NLS Policies xml file*>[*schema name*] **例**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml
2. <*WC_installdir*>¥logs にあるログ・ファイル **acugload.log**、 **acpload.log**、および **acpnlsload.log** にエラーがないかどうかを調べます。

400 AIX Solaris Linux では:

データベース・ユーザー ID には、以下の手順を進めるために、次の許可が必要です。

- *WC_installdir*/xml/policies および *WC_installdir*/logs のディレクトリー、サブディレクトリー、およびファイルに対する、読み取り/書き込み/実行権限。
- *WC_installdir*/bin ディレクトリーおよびそのファイルに対する読み取り/実行権限。

データベース・ユーザー ID に上記の必須権限がない場合、 chmod コマンドを使用して、この権限を付与する必要があります。

1. データベースのユーザー ID としてログインします。
2. ディレクトリー <*WC_installdir*>/bin から、ここにリストされた順序で必要に応じて以下のシェル・スクリプトを実行します。

1. ユーザー (アクセス) グループ定義をロードするには、 **acugload** シェル・スクリプトを実行します。**構文:** acugload.sh <*database name*> <*database user*> <*database user password*> <*UserGroups xml filename*>[*schema name*] **例**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml

2. メイン・アクセス制御ポリシー・ファイルをロードするには、 **acpload** シェル・スクリプトを実行します。 **構文:**acpload.sh *<database name> <database user> <database user password> <Policies xml filename>*[*schema name*] **例**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
3. 表示名および説明ファイルをロードするには、 acpnlsload シェル・スクリプトを実行します。**構文:** acpnlsload.sh *<database name> <database user> <database user password> <NLS Policies xml filename>*[*schema name*] **例**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml

<WC_installdir>/logs にあるログ・ファイル acugload.log、 acpload.log、および acpnlsload.log にエラーがないかどうかを調べます。

注: これらのスクリプトの実行中に生じる可能性のあるエラーはコマンド行に表示されないので、これらのスクリプトを実行した後にログ・ファイルを調べる必要があります。

400 では :

注: 400 では、ログ・ファイルは *WC_userdir*/instances にあります。

ポリシーおよびアクセス・グループ定義をデータベースから XML ファイルに抽出する

抽出プロセスは、アクセス制御データベース内のポリシーおよびアクセス・グループ情報を読み取り、その情報を XML 形式で取り込んだファイルを生成します。抽出ユーティリティーでは、入力フィルター XML ファイルを使用して、データベースから抽出するデータを指定します。以下のフィルター・ファイルが用意されています。

- ACPoliciesfilter.xml: すべてのアクセス・グループおよびポリシー・データを抽出するのに使用します。
- ACUserGroupsFilter.xml: すべてのアクセス・グループ・データを抽出するのに使用します。
- OrganizationPoliciesFilter.xml: 特定組織のすべてのアクセス・グループおよびポリシー・データを抽出するのに使用します。このファイルを使用する前に、編集して必要な組織 ID を指定する必要があります。この組織 ID に所有されるポリシー・データが抽出されます。

NT 2000 では :

1. *<WC_installdir>*¥bin ディレクトリーから、以下の acpextract コマンドを実行します。

   ```
   acpextract.cmd <database name> <database user> <database user password>
   <input xml filter file> [schema name]
   ```

   以下に例を示します。

   ```
   acpextract.cmd mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   以下のファイルが生成されます。

- ExtractedACPolicies.xml: このファイルには、 Extract コマンドによって抽出された指定のフィルター基準を満たすデータが含まれます。
- ExtractedACPolicies.dtd: ExtractedACPolicies.xml ファイルの DTD。
- AccessControlUserGroups.xml: アクセス・グループ定義を含むファイル。
- AccessControlPolicies.xml: 言語に依存しないアクセス制御ポリシー情報を含むファイル。
- AccessControlPolicies_LOCALE.xml: 表示名および記述を含む、言語に依存したアクセス制御ポリシー・ファイル。

2. ログ・ファイル *<WC_installdir>*¥logs¥acpextract.log を調べて、生じた可能性のある処理エラーを探してください。

400 AIX Solaris Linux では:

1. データベースのユーザー ID としてログインします。
2. *<WC_install_dir>*¥bin ディレクトリーから、以下の acpextract シェル・スクリプトを実行します。

   ```
   acpextract.sh <database name> <database user>
   <database user password> <input xml filter file> [schema name]
   ```

   以下に例を示します。

   ```
   acpextract.sh mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   以下のファイルが生成されます。

   - ExtractedACPolicies.xml: このファイルには、 Extract コマンドによって抽出された指定のフィルター基準を満たすデータが含まれます。
   - ExtractedACPolicies.dtd: ExtractedACPolicies.xml ファイルの DTD。
   - AccessControlUserGroups.xml: アクセス・グループ定義を含むファイル。
   - AccessControlPolicies.xml: 言語に依存しないアクセス制御ポリシー情報を含むファイル。
   - AccessControlPolicies_LOCALE.xml: 表示名および記述を含む、言語に依存したアクセス制御ポリシー・ファイル。

3. ログ・ファイル *<WC_installdir>*¥logs¥acpextract.log を調べて、生じた可能性のある処理エラーを探してください。

400 では :

1. 以下のファイルが、OUTDIR パラメーターを使用して、*WC_installdir*/xml/policies/xml ディレクトリーに作成されます。
   - ExtractedACPolicies.xml: このファイルには、 Extract コマンドによって抽出された指定のフィルター基準を満たすデータが含まれます。
   - ExtractedACPolicies.dtd: ExtractedACPolicies.xml ファイルの DTD。
   - AccessControlUserGroups.xml: アクセス・グループ定義を含むファイル。
   - AccessControlPolicies.xml: 言語に依存しないアクセス制御ポリシー情報を含むファイル。
   - AccessControlPolicies_LOCALE.xml: 表示名および記述を含む、言語に依存したアクセス制御ポリシー・ファイル。

第 4 部 Payments のセキュリティー

第 4 部では、Payments のセキュリティー管理タスクについて説明します。

第 14 章 WebSphere Commerce Payments のアクセス

WebSphere Commerce Payments は、レルムを利用してユーザーを認証します。レルムとは、基本的にはユーザーのレジストリーのことですが、ユーザー認証の 1 つの方法 (ユーザー名とパスワードなど) が関連付けられています。 WebSphere Commerce Payments の各システムでは、複数のレルムを同時に使用できません。レルムのタイプとしては、 LDAP レルムやオペレーティング・システム・レルムなどがあります。ユーザーにリソースへのアクセス権限を与えるには、まずユーザーをレルム内で定義する必要があります。したがって、有効な WebSphere Commerce Payments ユーザーになるには、次の 2 つの条件を両方とも満たしていなければなりません。

- レルム内に入っていること
- WebSphere Commerce Payments で役割を割り当てられていること

WebSphere Commerce Payments は、役割ベースのアクセス制御方式を採用しており、 WebSphere Commerce Payments で定義されている役割は以下の 4 つです。

1. Payments 管理者
2. マーチャント管理者
3. スーパーバイザー
4. クラーク

Payments 管理者は、 WebSphere Commerce Payments ユーザー・インターフェースの「ユーザー」ウィンドウを使用して、レルム内に定義されているユーザーに役割ベースのアクセス権限を割り当てることができます。 WCSRealm は WebSphere Commerce Payments に付属しています。システムには、WCSRealm クラスが自動的に構成されます。このレルムを使用すれば、WebSphere Commerce Payments Servlet は、WebSphere Commerce ユーザー・テーブルにすでに登録されている管理者情報を使用することになります。 Payments 管理者用としてこの管理者情報を使用すれば、 WebSphere Commerce Payments ユーザー・インターフェースを使用するために、別の管理者 ID セットを定義する必要がなくなります。

第 15 章 WebSphere Commerce Payments のセキュリティー保守

WebSphere Commerce Payments のセキュリティーは、いくつかの重要なセキュリティー・エレメントに基づいています。これらのエレメントを組み合わせることによって、 Web 上でセキュアにサービスをデプロイするための環境を構築できます。

注: IBM WebSphere Commerce Payments (以降 WebSphere Commerce Payments と記す) は、以前は Payment Manager という名称になっていました。バージョン 3.1.3 以降、この決済アプリケーションは WebSphere Commerce Payments と改称され、本書でこの製品に言及した箇所も改訂されました。

WebSphere Commerce Payments の保護

WebSphere Commerce Payments の心臓部に位置しているのが Payment Servlet です。その周辺を固める製品として、WebSphere Application Server、データベース、ユーザー・インターフェースなどで構成された Web サーバーがあり、そのすべてを考慮に入れて初めて WebSphere Commerce Payments の全体像を把握できます。この章では、 WebSphere Commerce Payments の各種コンポーネントのセキュリティーを確保するための方法を取り上げます。

機密データの保護

それぞれの照会コマンドについて、このフレームワークはユーザーの役割を機密データ用の最低限の役割に照らして確認し、クレジット・カード番号や請求先住所などの機密データをすべて見える形で戻すべきか、それとも隠すべきかを示すインディケーターを QueryRequest オブジェクトに設定します。 WebSphere Commerce Payments フレームワークは、照会コマンドによって戻すことのできる機密データを保守しません。しかし、カセット・ライターに用意されている新しいメソッドによって、そのインディケーターの値を検査し、標準化した方法で機密データを隠すことができるようになっています。各カセットは、格納データの中から機密データを識別する必要があります。基本的には、カセットが WebSphere Commerce Payments データベースへの格納前に暗号化したデータが、機密データと言えます。

ユーザーが機密データにアクセスするために最低限必要とする役割は、 JVM システム・パラメーター `wpm.MinSensitiveAccessRole={clerk|supervisor|madmin|psadmin|none}` で指定します。この値については、大文字小文字の区別があります。このプロパティーを指定しない場合は、 clerk という値が想定され、すべてのユーザーが機密データを見ることができるようになります。無効な値を指定すると、Payment Servlet の初期化が失敗します。

このパラメーターは、Payments のインスタンス作成時に設定でき、 WebSphere Commerce 構成マネージャーを使用していつでも更新できることに注意してください。構成マネージャーでのパラメーターの名前は、Payments インスタンス・パネルの「最小アクセス役割」です。構成マネージャーのパネルの詳細は、それぞれのプ

ラットフォームの「*WebSphere Commerce インストール・ガイド*」か、構成マネージャー使用中に Payments インスタンス・パネルのオンライン・ヘルプを参照してください。

以下の表は、サポートされている値をまとめたものです。下に行くに従って権限が大きくなります。

表 15. Payments のユーザー役割の権限

ユーザー	説明
clerk	クラーク以上の役割を持ったユーザーが機密データを参照できます。
supervisor	スーパーバイザー以上の役割を持ったユーザーが機密データを参照できます。
madmin	マーチャント管理者以上の役割を持ったユーザーが機密データを参照できます。
psadmin	Payments 管理者だけが機密データを参照できます。
なし	だれも機密データを参照できません。

この `wpm.MinSensitiveAccessRole` パラメーターは、WebSphere Commerce の構成マネージャーで指定できます。

データベースの保護

WebSphere Commerce Payments データベースには機密データが格納されるので、無許可の読み取りや書き込みからの保護が必要です。 WebSphere Commerce Payments は、データベースに格納されているパスワードやカード所有者情報などの機密データの暗号化をサポートしています。

トランザクション・データ

ここでは、トランザクション・データの扱いに関する指針を示します。

- 機密性の高いトランザクション情報は、インスタンス・ライブラリー内のデータベース表に格納されます。このライブラリーは、 Payments インスタンス作成ウィザードでインスタンス・スキーマ名として指定したものです。
- バックアップもセキュアに保管する必要があります。
- インスタンス・ライブラリー内のデータベース表は、構成やトランザクションに関する重要データを格納しているので、システム・バックアップ・ストラテジーに組み込む必要があります。以下のバックアップも作成する必要があります。
  - `/QIBM/UserData/CommercePayments/V55/instance` ディレクトリー内のファイル (instance は WebSphere Commerce Payments インスタンスの名前)。
  - WebSphere Commerce Payments 用に構成した HTTP サーバー・インスタンス。この HTTP サーバーは、 Payments インスタンス作成ウィザードで Web サーバーとして指定したものです。
  - ローカル・マシンのインスタンス・ライブラリー内のオブジェクト。リモートのデータベース・ストレージを使用している場合は、リモート・マシンのデータベース・コレクション内のオブジェクトもバックアップする必要があります。

第 5 部 その他のセキュリティー・トピック

第 5 部では、WebSphere Commerce システム管理者が実行できるその他のセキュリティー・タスクについて説明します。

第 16 章 WebSphere Application Server のセキュリティーの使用可能化

この章では、WebSphere Application Server のセキュリティーを使用可能にする方法について説明します。 WebSphere Application Server のセキュリティーを使用可能にすると、部外者からのリモート呼び出しによってすべての Enterprise JavaBeans コンポーネントが開示されないようにすることができます。

注:

1. Windows WebSphere Application Server グローバル・セキュリティーが、この章のステップで概説されているとおりに使用可能になっている場合、 WebSphere Application Server サーバー (たとえば server1) を、Windows 2000 の「サービス」パネルから適切に停止させることはできません。セキュリティーが使用可能になっている場合にサービスを停止するには、コマンド・プロンプトで WAS_*installdir*¥bin ディレクトリーから stopserver コマンドを以下のように使用します。

   ```
   stopserver server -username user_id -password password
   ```

   ここで、*server* は停止したい WebSphere Application Server 構成ディレクトリーの名前 (たとえば server1)、 *user_id* はサーバーでセキュリティーが使用可能になっている場合の認証用のユーザー名、および *password* はサーバーでセキュリティーが使用可能になっている場合の認証用のパスワードです。

   「サービス」パネルからサーバーを停止したい場合、プロパティーが上記のようであるのでユーザー ID とパスワードは組み込まれません。グローバル・セキュリティーを使用可能にすると、サーバーの停止時に、ユーザー ID とパスワードが認証用に要求されます。 (「サービス」パネルでは停止したと示されますが) サービスは続行します。「サービス」パネルからサービスを開始するためには、ユーザー ID とパスワードは必要とされないことに注意してください。

2. WebSphere Application Server セキュリティーが使用可能になっているときにアプリケーション・サーバーを停止する必要がある場合、コマンド・プロンプトで WAS_*installdir*/bin ディレクトリーから stopserver コマンドを使用します。

   AIX Linux Solaris

   ```
   stopserver server -username user_id -password password
   ```

   ここで *server* は停止したい WebSphere Application Server アプリケーション・サーバーの名前 (たとえば、server1)、 *user_id* は認証用のユーザー名、*password* は認証用のパスワードです。

   400

   ```
   stopserver -instance WAS_instancename server -username user_id
      -password password
   ```

ここで *WAS_instancename* は WebSphere Application Server インスタンスの名前、 *server* は停止したい WebSphere Application Server アプリケーション・サーバーの名前 (たとえば、 `server1`)、*user_id* は認証用のユーザー名、 *password* は認証用のパスワードです。

3. AIX Linux Solaris Windows WebSphere Application Server セキュリティーを使用可能にする場合には、ご使用のマシンで以下の要件を満たすよう強くお勧めします。
   - 1 GB 以上のマシン・メモリー
   - WebSphere Commerce アプリケーション用に、384 MB 以上のヒープ・サイズ

はじめに

セキュリティーを使用可能にする前に、セキュリティーを使用可能にする WebSphere Application Server がユーザー ID の妥当性を検査する方法を知る必要があります。 WebSphere Application Server は LDAP またはオペレーティング・システムのユーザー・レジストリーを WebSphere Application Server ユーザー・レジストリーとして使用できます。

LDAP ユーザー・レジストリーを使用するセキュリティーの使用可能化

AIX Solaris Linux LDAP を WebSphere Application Server ユーザー・レジストリーとして使用しているときに WebSphere Application Server セキュリティーを使用可能にするには、 `wasuser` ID としてシステムにログインし、次のようなステップを行います。

400 LDAP を WebSphere Application Server ユーザー・レジストリーとして使用しているときに WebSphere Application Server セキュリティーを使用可能にするには、システムにログインして次のようなステップを行います。

Windows LDAP を WebSphere Application Server ユーザー・レジストリーとして使用しているときに WebSphere Application Server セキュリティーを使用可能にするには、管理権限をもったユーザーとしてシステムにログインし、次のようなステップを行います。

1. WebSphere Application Server を開始し、 WebSphere Application Server 管理コンソールをオープンします。
2. 管理コンソールで、以下のようにグローバル・セキュリティー設定値を変更します。
   a. **「セキュリティー」**の下の**「ユーザー・レジストリー (User Registries)」**を展開して、**「LDAP」**をクリックします。ご使用のディレクトリー・サーバーのタイプに応じて、**「構成」**タブの各フィールドを次のように設定します。

表 16. *IBM Directory Server* のユーザー： AIX 400 Linux Solaris Windows

フィールド名	定義	サンプル値	備考
サーバー・ユーザー ID (Server User ID)	ユーザー ID	*user_ID*	• これは LDAP 管理者にすることはできません。 • cn=xxx として指定されているユーザーは使用しないでください。 • このユーザーのオブジェクト・クラスが、「LDAP 拡張プロパティー (LDAP Advanced Properties)」ウィンドウの「ユーザー・フィルター (User Filter)」フィールドに指定されたオブジェクト・クラスと互換性があることを確認します。
サーバー・ユーザー・パスワード (Server User Password)	ユーザー・パスワード	*password*	
タイプ (Type)	LDAP サーバーのタイプ	SecureWay	
ホスト (Host)	LDAP サーバーのホスト名	*hostname.domain.com*	
ポート (Port)	LDAP サーバーが使用しているポート		このフィールドは不要です。
基本識別名 (Base Distinguished Name)	検索に使用される識別名	o=ibm,c=us	
バインド識別名 (Bind Distinguished Name)	検索時にディレクトリーにバインドするための識別名		このフィールドは不要です。
バインド・パスワード (Bind Password)	バインド識別名のパスワード		このフィールドは不要です。

表 17. *Netscape* ユーザー： Windows

フィールド名	定義	サンプル値	備考
サーバー・ユーザー ID (Server User ID)	ユーザー ID	*user_ID*	• これは LDAP 管理者にすることはできません。 • cn=xxx として指定されているユーザーは使用しないでください。 • このユーザーのオブジェクト・クラスが、「LDAP 拡張プロパティー (LDAP Advanced Properties)」ウィンドウの「ユーザー・フィルター (User Filter)」フィールドに指定されたオブジェクト・クラスと互換性があることを確認します。
サーバー・ユーザー・パスワード (Server User Password)	ユーザー・パスワード	*password*	
タイプ (Type)	LDAP サーバーのタイプ	Netscape	
ホスト (Host)	LDAP サーバーのホスト名	*hostname.domain.com*	
ポート (Port)	LDAP サーバーが使用しているポート		このフィールドは不要です。
基本識別名 (Base Distinguished Name)	検索に使用される識別名	o=ibm	
バインド識別名 (Bind Distinguished Name)	検索時にディレクトリーにバインドするための識別名		このフィールドは不要です。
バインド・パスワード (Bind Password)	バインド識別名のパスワード		このフィールドは不要です。

表 18. *Domino™* ユーザー： Windows

フィールド名	定義	サンプル値	備考
サーバー・ユーザー ID (Server User ID)	ショート・ネーム / ユーザー ID	*user_ID*	このユーザーのオブジェクト・クラスが、「LDAP 拡張プロパティー (LDAP Advanced Properties)」ウィンドウの「ユーザー・フィルター (User Filter)」フィールドに指定されたオブジェクト・クラスと互換性があることを確認します。
サーバー・ユーザー・パスワード (Server User Password)	ユーザー・パスワード	*password*	
タイプ (Type)	LDAP サーバーのタイプ	Domino 5.0	
ホスト (Host)	LDAP サーバーのホスト名	*hostname.domain.com*	
ポート (Port)	LDAP サーバーが使用しているポート		このフィールドは不要です。
基本識別名 (Base Distinguished Name)	検索に使用される識別名		このフィールドは不要です。
バインド識別名 (Bind Distinguished Name)	検索時にディレクトリーにバインドするための識別名		このフィールドは不要です。
バインド・パスワード (Bind Password)	バインド識別名のパスワード		このフィールドは不要です。

表 19. アクティブ・ディレクトリー・ユーザー： Windows

フィールド名	定義	サンプル値	備考
サーバー・ユーザー ID (Server User ID)	sAMAccountName	*user_ID*	• 任意の通常ユーザーのユーザー・ログオン名。 • cn=xxx として指定されているユーザーは使用しないでください。 • このユーザーのオブジェクト・クラスが、「LDAP 拡張プロパティー (LDAP Advanced Properties)」ウィンドウの「ユーザー・フィルター (User Filter)」フィールドに指定されたオブジェクト・クラスと互換性があることを確認します。
サーバー・ユーザー・パスワード (Server User Password)	ユーザー・パスワード	*password*	
タイプ (Type)	LDAP サーバーのタイプ	アクティブ・ディレクトリー	
ホスト (Host)	LDAP サーバーのホスト名	*hostname.domain.com*	
ポート (Port)	LDAP サーバーが使用しているポート		このフィールドは不要です。
基本識別名 (Base Distinguished Name)	検索に使用される識別名	CN=users, DC=domain1, DC=domain2, DC=com	
バインド識別名 (Bind Distinguished Name)	検索時にディレクトリーにバインドするための識別名	CN=*user_ID*, CN=users, DC=domain1, DC=domain2, DC=com	*user_ID* 値は表示名です。これはユーザー・ログオン名と同じでなくてもかまいません。
バインド・パスワード (Bind Password)	バインド識別名のパスワード	*bind_password*	これはセキュリティー・サーバー・パスワードと同じでなければなりません。

「適用」をクリックしてから、**「保管」**をクリックします。

b. 管理コンソールで、**「セキュリティー」**を展開し、**「グローバル・セキュリティー (Global Security)」**をクリックします。
   1) 「グローバル・セキュリティー構成 (Global Security Configuration)」タブで、**「使用可能」**を選択し、**「Java 2 セキュリティーの実施 (Enforce Java 2 Security)」**のチェックマークを外します。

      注: WebSphere Commerce 5.5 は、Java 2 セキュリティーをサポートしません。
   2) 「アクティブ認証機構 (Active Authentication Mechanism)」フィールドで、**「Lightweight Third Party Authentication (LTPA)」**を選択します。
   3) 「アクティブ・ユーザー・レジストリー (Active User Registry)」フィールドで、**「LDAP」**を選択します。
   4) **「適用」**をクリックしてから、**「保管」**をクリックします。

c. 管理コンソールで、**「セキュリティー」**を展開してから、**「認証機構 (Authentication Mechanisms)」**を展開し、**「LTPA」**をクリックします。
   1) 「LPTA 構成 (LPTA Configuration)」タブで、必要に応じて LTPA 設定値を入力します。
   2) 「追加プロパティー (Additional Properties)」で、**「単一サインオン (SSO)」**をクリックし、この機能を使用したくない場合は、**「使用可能」**チェック・ボックスのチェックマークを外します。
   3) **「適用」**をクリックしてから、**「保管」**をクリックします。

d. 管理コンソールで、**「アプリケーション (Applications)」**を展開してから、**「エンタープライズ・アプリケーション (Enterprise Applications)」**をクリックします。
   1) 「エンタープライズ・アプリケーション (Enterprise Applications)」ウィンドウで、 **WC**_*instance_name* という形式で表示されているご使用の Commerce アプリケーション (`WC_demo` など) をクリックします。
   2) 「追加プロパティー (Additional Properties)」で、**「セキュリティー役割をユーザー/グループにマップする (Map security roles to users/groups)」**をクリックします。
   3) **「ユーザーの検索 (Lookup users)」**をクリックして、役割をマップしたいユーザーを検索します。
   4) そのユーザーについて、**「WCSecurityRole」**を選択し、**「OK」**をクリックします。

3. 管理コンソールをクローズして、WebSphere Application Server 管理コンソールを停止してから、再始動します。この後は、WebSphere Application Server 管理コンソールをオープンするとき、セキュリティー・サーバー ID とパスワードの入力を求めるプロンプトが出されます。
4. WebSphere Commerce 構成マネージャーをオープンして、**「Instances (インスタンス)」>**「*instance_name*」**>「インスタンス・プロパティー」>「セキュリティー」**を選択し、**「使用可能」**チェック・ボックスをクリックします。ステップ 2b で入力したユーザー名とパスワードを入力するよう促されます。**「適用」**をクリックして、構成マネージャーを終了します。
5. WebSphere Application Server 管理コンソールを停止してから、再始動します。

オペレーティング・システム・ユーザー・レジストリーを使用したセキュリティーの使用可能化

AIX Linux Solaris 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するには、 WebSphere Application Server を root ID として実行する必要があります。 WebSphere Application Server を root として実行し、次のようなステップを行います。

400 Windows オペレーティング・システムのユーザー妥当性検査を WebSphere Application Server ユーザー・レジストリーとして使用しているときに WebSphere Application Server セキュリティーを使用可能にするには、管理権限をもったユーザーとしてシステムにログインし、次のようなステップを行います。

1. AIX Linux Solaris root としてログインします。
2. AIX Linux Solaris root としてログインしている間に、 WebSphere Application Server を開始して、WebSphere Application Server 管理コンソールを立ち上げます。サーバーを始動するには、以下のようにします。

   ```
   cd WAS_installdir/bin
   ./startServer server
   ```

   ここで *server* は WebSphere Application Server アプリケーション・サーバーの名前です (たとえば、server1)。
3. WebSphere Application Server 管理コンソールで、以下のようにグローバル・セキュリティー設定値を変更します。
   a. 管理コンソールで、**「セキュリティー」**を展開し、**「ユーザー・レジストリー (User Registries)」**を展開し、**「ローカル OS (Local OS)」**をクリックします。ご使用のセキュリティー・レジストリー・サーバーに応じて、**「構成」**タブの各フィールドを次のように設定します。

フィールド名	サンプル値	備考
サーバー・ユーザー ID (Server User ID)	*wcsuser*	400 iSeries でのユーザー ID は、 *SECOFR 権限をもっていなければなりません。 AIX Solaris Linux root または root 権限をもつユーザー ID。 Windows ログインしたオペレーティング・システム管理権限のあるユーザー ID。マシンがドメインに属する場合、完全修飾ユーザー ID を使用してください (たとえば、*DomainXYZ¥user_id*)。このアカウントがドメイン・サーバーに属していて、管理者のグループのメンバーであることを確認してください。
セキュリティー・サーバー・パスワード (Security Server Password)	*password*	これはログインの際に使用した、オペレーティング・システム管理権限のあるユーザーのパスワードです。

「適用」をクリックしてから、**「保管」**をクリックします。

b. 管理コンソールで、**「セキュリティー」**を展開し、**「グローバル・セキュリティー (Global Security)」**をクリックします。

1) 「グローバル・セキュリティー構成 (Global Security Configuration)」タブで、**「使用可能」**を選択し、**「Java 2 セキュリティーの実施 (Enforce Java 2 Security)」**のチェックマークを外します。

2) 「アクティブ認証機構 (Active Authentication Mechanism)」フィールドで、**「SWAM (Simple WebSphere Authentication Mechanism」**を選択します。

3) 「アクティブ・ユーザー・レジストリー (Active User Registry)」フィールドで、**「ローカル OS (Local OS)」**を選択します。

4) **「適用」**をクリックしてから、**「保管」**をクリックします。

4. 管理コンソールで、**「アプリケーション (Applications)」**を展開してから、**「エンタープライズ・アプリケーション (Enterprise Applications)」**をクリックします。

a. 「エンタープライズ・アプリケーション (Enterprise Applications)」ウィンドウで、 **WC**_*instance_name* という形式で表示されているご使用の Commerce アプリケーション (`WC_demo` など) をクリックします。

b. 「追加プロパティー (Additional Properties)」で、**「セキュリティー役割をユーザー/グループにマップする (Map security roles to users/groups)」**をクリックします。

c. **「ユーザーの検索 (Lookup users)」**をクリックして、役割をマップしたいユーザーを検索します。

d. そのユーザーについて、**「WCSecurityRole」**を選択し、**「OK」**をクリックします。

5. WebSphere Commerce 構成マネージャーをオープンし、**「インスタンス・リスト (Instances List)」→** *「instance_name」* **→「インスタンス・プロパティー」→「セキュリティー」**を選択し、**「セキュリティーを使用可能にする (Enable Security)」**チェック・ボックスを選択します。認証モードの**「オペレーティング・システム・ユーザー・レジストリー」**を選択し、ステップ 3a (206 ページ) で入力したユーザー名とパスワードを入力します。**「適用」**をクリックして、構成マネージャーを終了します。

6. WebSphere Application Server 管理サーバーを停止してから、再始動します。この後は、WebSphere Application Server 管理コンソールをオープンするとき、セキュリティー・サーバー ID とパスワードの入力を求めるプロンプトが出されます。

WebSphere Commerce EJB セキュリティーの使用禁止

WebSphere Commerce Business Edition を使用して、 EJB セキュリティーを使用不可にすることができます。 WebSphere Commerce EJB セキュリティーを使用不可にするには、以下のようにします。

1. WebSphere Application Server 管理コンソールを開始します。
2. 管理コンソールで、**「セキュリティー」**を展開し、**「グローバル・セキュリティー (Global Security)」**をクリックします。「グローバル・セキュリティー構成 (Global Security Configuration)」タブで、**「使用可能」**チェック・ボックスのチェックマークを外します。
3. WebSphere Commerce 構成マネージャーをオープンして、**「インスタンス (Instances)」→** *「instance_name」* **→「インスタンス・プロパティー」→「セキュリティー」**を選択し、**「セキュリティーを使用可能にする (Enable Security)」**チェック・ボックスをクリアします。
4. WebSphere Application Server 管理コンソールを終了します。
5. WebSphere Application Server 管理サーバーを停止してから、再始動します。

WebSphere Commerce セキュリティー・デプロイメント・オプション

WebSphere Commerce は、さまざまなセキュリティー・デプロイメント構成をサポートしています。以下の表には、使用できるセキュリティー・デプロイメント・オプションが示されています。

表 20. 単一マシンのセキュリティーのシナリオ

WebSphere Application Server セキュリティーが使用可能。	• オペレーティング・システムを WebSphere Application Server レジストリーとして使用する。 • データベースを WebSphere Commerce レジストリーとして使用する。
	• LDAP を WebSphere Application Server レジストリーとして使用する。 • LDAP を WebSphere Commerce レジストリーとして使用する。
	• LDAP を WebSphere Application Server レジストリーとして使用する。
WebSphere Application Server セキュリティーが使用不可、および WebSphere Commerce サイトがファイアウォールに守られている。	• WebSphere Application Server レジストリーは不要。 • データベースを WebSphere Commerce レジストリーとして使用する。
	• WebSphere Application Server レジストリーは不要。 • LDAP を WebSphere Commerce レジストリーとして使用する。

表 21. 複数マシンのセキュリティーのシナリオ

WebSphere Application Server セキュリティーが使用可能。 LDAP が常にデプロイされている。	• LDAP を WebSphere Application Server レジストリーとして使用する。 • LDAP を WebSphere Commerce レジストリーとして使用する。
	• LDAP を WebSphere Application Server レジストリーとして使用する。 • データベースを WebSphere Commerce レジストリーとして使用する。 • LDAP をセットアップし、 LDAP レジストリー内に 1 つの管理エントリーを組み込む必要がある。

表 21. 複数マシンのセキュリティーのシナリオ (続き)

WebSphere Application Server セキュリティーが使用不可、および WebSphere Commerce サイトがファイアウォールに守られている。	• データベースを WebSphere Commerce レジストリーとして使用する。 • WebSphere Application Server レジストリーは不要。 • 単一サインオンはサポートされない。
	• LDAP を WebSphere Application Server レジストリーとして使用する。 • WebSphere Application Server レジストリーは不要。

注: ファイアウォールの内部で WebSphere Commerce サイトを操作する場合は、WebSphere Application Server セキュリティーを使用不可にすることができます。WebSphere Application Server セキュリティーを使用不可にするのは、ファイアウォールの内部で有害なアプリケーションが稼働していないことが確認されている場合に限る必要があります。

動的キャッシュ・モニターのセキュリティー構成

WebSphere Application Server 動的キャッシュ・モニターを使用してモニターしている場合で、モニターしているアプリケーションが、デプロイメント記述子でセキュリティー役割を定義している場合、以下を実行する必要があります。

WebSphere Application Server 管理コンソールの「ステップ: セキュリティー役割をユーザー/グループにマップする (Step: Map security roles to users/groups)」パネルに移動するには、**「アプリケーション (Applications)」**—>**「新規アプリケーションのインストール (Install New Application)」**をクリックし、 (セキュリティー関連ではない) 必要な手順を完了してください。 (詳細は、「WebSphere Application Server Information Center」
(`http://www.ibm.com/software/webservers/appserv/infocenter.html`) の、『Deploying secured applications』および『Assigning users and groups to roles』トピックを参照してください。) 「ステップ: セキュリティー役割をユーザー/グループにマップする (Step: Map security roles to users/groups)」パネルで、以下を実行します。

1. 各セキュリティー役割にマップされるユーザーおよびグループを指定します。
2. 必要に応じて**「役割 (Role)」**の隣のチェック・ボックスをチェックし、すべての役割を選択するか、個々の役割を選択します。役割ごとに、Everyone や All Authenticated ユーザーなどの事前定義されたユーザーを役割にマップするかどうか指定できます。ユーザー・レジストリーから特定のユーザーまたはグループを選択するには、以下のようにします。
   a. 役割を選択して、**「ユーザーの検索 (Lookup users)」**または**「グループの検索 (Lookup groups)」**をクリックします。
   b. 表示される**「ユーザーの検索 (Lookup users)」**または**「グループの検索 (Lookup groups)」**パネルで、検索基準を入力して、ユーザー・レジストリーからユーザーまたはグループのリストを取り出します。
   c. 表示される結果から、個々のユーザーまたはグループを選択します。

d. 「**OK**」をクリックして、選択したユーザーまたはグループを、「ステップ: セキュリティー役割をユーザー/グループにマップする (Step: Map security roles to users/groups)」パネルで選択した役割にマップします。

現在は、すべてのキャッシュ・モニター機能へアクセスできるようにする 1 つの役割が定義されています。つまり、このページを使用して、動的キャッシュ・モニターへアクセスできるユーザーを指定できるということです。

構成マネージャーを使用した WebSphere Commerce インスタンスの管理

WebSphere Application Server グローバル・セキュリティーが使用可能な場合、構成マネージャーを使用して、WebSphere Commerce または WebSphere Commerce Payments インスタンスを正しく停止、開始、作成、または削除するために、以下の手順を実行する必要があります。

1. *WAS_installdir*/properties ディレクトリーで、以下のファイルおよびプロパティーを、以下の値に更新します。
   - sas.client.props

     com.ibm.CORBA.securityEnabled=true

     com.ibm.CORBA.loginSource=properties

     com.ibm.CORBA.LoginUserid=validUser

     com.ibm.CORBA.LoginPassword=validPassword
   - soap.client.props

     com.ibm.SOAP.loginUserid=validUser

     com.ibm.SOAP.loginPassword=validPassword

     com.ibm.SOAP.secrityEnabled=true
2. *WAS_installdir*/bin ディレクトリーで、PropFilePasswordEncoder コマンドを (1 行で) 実行し、パスワードを sas.client.props および soap.client.props ファイルにエンコードします。

   AIX Linux Solaris

   ```
   PropFilePasswordEncoder.sh WAS_installdir/properties/
      sas.client.props com.ibm.CORBA.LoginPassword

   PropFilePasswordEncoder.sh WAS_installdir/properties/
      soap.client.props com.ibm.SOAP.loginPassword
   ```

   400

   ```
   PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
      sas.client.props com.ibm.CORBA.LoginPassword

   PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
      soap.client.props com.ibm.SOAP.loginPassword
   ```

   Windows

   ```
   PropFilePasswordEncoder.bat WAS_installdir¥properties¥
      sas.client.props com.ibm.CORBA.LoginPassword

   PropFilePasswordEncoder.bat WAS_installdir¥properties¥
      soap.client.props com.ibm.SOAP.loginPassword
   ```
3. config_client スクリプトを更新します。

AIX 400 Linux Solaris $CLIENTSOAP $CLIENTSAS を、 Java 引き数リストに追加します。たとえば、以下のようにします。

```
${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
-Djava.security.policy="config.policy" -Djava.version="1.3"
-Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
-Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME" $CLIENTSOAP $CLIENTSAS
$PM_ARGS -Xmx128m com.ibm.commerce.config.client.CMClient "$@"
```

Windows %CLIENTSOAP% %CLIENTSAS% を、 Java 引き数リストに追加します。たとえば、以下のようにします。

```
"%JAVA_HOME%¥bin¥java" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS% "
-Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"
-Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
-Djava.security.policy="config.policy"
com.ibm.commerce.config.client.CMClient %*
```

4. config_server スクリプトを更新します。

AIX 400 Linux Solaris $CLIENTSOAP $CLIENTSAS を、 Java 引き数リストに追加します。たとえば、以下のようにします。

```
${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
-Djava.security.policy="config.policy"
-Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
-Dws.ext.dirs="$WAS_EXT_DIRS" -Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME"
$CLIENTSOAP $CLIENTSAS $PM_ARGS $MAX_HEAP
com.ibm.commerce.config.server.CMServerImpl "$@"
```

Windows %CLIENTSOAP% %CLIENTSAS% を、 Java 引き数リストに追加します。たとえば、以下のようにします。

```
"%JAVA_HOME%¥bin¥java.exe" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS%
"-Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"
"-Dws.ext.dirs=%WAS_EXT_DIRS%" -Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
-Djava.security.policy="config.policy"
com.ibm.commerce.config.server.CMServerImpl %*
```

第 17 章 IBM HTTP Server での実動のための SSL の使用可能化

400 この項は、 iSeries プラットフォームには当てはまりません。 iSeries に関する詳細は、 220 ページの『IBM HTTP サーバーでの SSL の使用可能化 (iSeries)』を参照してください。

IBM HTTP Server で WebSphere Commerce インスタンスを作成し終えると、SSL (Secure Sockets Layer) を使ってテストすることができます。サイトをショッパーに対してオープンする前に、この章の以下のステップを実行して、SSL を実動用に使用可能にしなければなりません。

セキュリティーについて

IBM HTTP Server は暗号化テクノロジーを使用して、商取引のための機密保護機能のある環境を提供します。暗号化とは、インターネット上の情報トランザクションをスクランブルし、受信側がスクランブル解除するまで判読不能にすることです。送信側はアルゴリズム・パターンつまり鍵を使用してトランザクションをスクランブル (暗号化) し、受信側は復号鍵を使用します。これらの鍵は、Secure Sockets Layer (SSL) プロトコルで使用されます。

Web サーバーは認証プロセスを使用して、ビジネス上の取引をしている個人の識別を検証します (つまり、当人が呼称されるとおりの人物であることを確認します)。これには、認証局 (CA) と呼ばれる信頼のおける第三者機関によって署名された証明書を取得することが含まれます。 IBM HTTP Server ユーザーの場合、CA は Equifax® や VeriSign® Inc. などです。他の CA も同様に使用可能です。

実動鍵ファイルを作成するには、以下のステップを完了します。

1. 実動用のセキュリティー鍵ファイルを構成します。
2. 認証局からセキュアな証明書を要求します。
3. 実動鍵ファイルを現行鍵ファイルとして設定します。
4. 証明書を受け取り、実動鍵ファイルをテストします。

これらのステップについて、以下に詳細に説明します。

注:

1. 認証局が署名した実動鍵ファイルをすでに使用している場合、これらのステップを省略することもできます。この章を読んで決定してください。
2. これらのステップを実行する際に、ブラウザーにセキュリティー・メッセージが表示されることがあります。それぞれのメッセージに示された情報を注意深く確認して、続行する方法を判別してください。

実動用のセキュリティー鍵ファイルの構成

実動用のセキュリティー鍵ファイルを構成するには、 Web サーバー・マシンで以下のようにします。

1. IBM HTTP Server を停止します。
2. マシン上の IBM HTTP Server インストール・ディレクトリーの下の conf サブディレクトリーに移動します。
3. httpd.conf のバックアップ・コピーを作成し、そのバックアップ・コピーの名前を httpd.conf.backup に変更します。
4. httpd.conf をテキスト・エディターでオープンします。
5. ポート 443 について、以下の行のコメントを解除します (つまり、行の先頭の『#』 を削除します)。
   - Windows
     a. LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     b. Listen 443
     c. <VirtualHost *host.some_domain.*com:443> (さらに、この行内の完全修飾ホスト名を置き換える必要もあります。)
     d. SSLEnable
     e. </VirtualHost>
     f. Keyfile "*HTTPServer_installdir*/ssl/keyfile.kdb"
   - AIX Linux Solaris
     a. LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
     b. AddModule mod_ibm_ssl.c
     c. Listen 443
     d. <VirtualHost *host.some_domain.*com:443> (さらに、この行内の完全修飾ホスト名を置き換える必要もあります。)
     e. SSLEnable
     f. </VirtualHost>
     g. SSLDisable
     h. Keyfile "*HTTPServer_installdir*/ssl/keyfile.kdb"
     i. SSLV2Timeout 100
     j. SSLV3Timeout 1000
6. 以下の行のコメントを解除します (つまり、行の先頭の 『#』 を削除します)。
   a. WebSphere Commerce の管理用ツールについては、ポート 8000、8002、8004 が必要です。

   ```
   Listen 8000
   Listen 8002
   Listen 8004
   ```

   WebSphere Commerce Payments を使用している場合は、ポート 5432、5433 も必要です。

   ```
   Listen 5432
   Listen 5433
   ```

b. 上記のポートの仮想ホスト・セクションのコメントも解除します (つまり、行の先頭に 『#』 が付いていればそれを削除します)。これらのセクション内の完全修飾ホスト名を正しい名前に置き換える必要があります。以下の例のデフォルト・パス名変数のリストについては、 ix ページの『パス変数』を参照してください。

以下の例は、Windows システムの httpd.conf ファイルから、コメントを解除した仮想ホスト・セクションを抽出したものです。他のオペレーティング・システムの場合も、同じような記述になっています。

```
########## IBM WebSphere Payments (Do not edit this section) #################
Listen 5432
Listen 5433
########## End of IBM WebSphere Payments (Do not edit this section) ##########

...

########## IBM WebSphere Commerce (Do not edit this section) #################
Listen 8000
Listen 8002
Listen 8004
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
```

図 7. httpd.conf ファイルの "Listen" セクションの例

```
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
## VirtualHost: Allows the daemon to respond to requests for more than one
## server address, if your server machine is configured to accept IP packets
## for multiple addresses. This can be accomplished with the ifconfig
## alias flag, or through kernel patches like VIF.
#
## Any httpd.conf or srm.conf directive may go into a VirtualHost command.
## See also the BindAddress entry.
#
#<VirtualHost host.some_domain.com:443>
```

図 8. httpd.conf ファイルの仮想ホスト・ヘッダー・セクションの例

```
########## IBM WebSphere Payments (Do not edit this section) #################
<VirtualHost host.some_domain.com:5433>
SSLEnable
SSLClientAuth 0
ServerName wordsworth.torolab.ibm.com
DocumentRoot "HTTPServer_installdir¥htdocs¥en_US"
</VirtualHost>
########## End of IBM WebSphere Payments (Do not edit this section) ##########
```

図 9. httpd.conf ファイルの Payments 用の仮想ホスト・セクションの例

```
########## IBM WebSphere Commerce (Do not edit this section) #################
#Instance name : instance_name
<VirtualHost host.some_domain.com:80>
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wcsstore  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/Stores.war"
Alias /wcs   "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

図 10. httpd.conf ファイルの WebSphere Commerce ポート 80 用の仮想ホスト・セクションの例: (非セキュア・ポート)

```
<VirtualHost host.some_domain.com:443>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wcsstore  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/Stores.war"
Alias /wcs   "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

図 11. httpd.conf ファイルの WebSphere Commerce ポート 443 用の仮想ホスト・セクションの例: (セキュア・ポート)

```
<VirtualHost host.some_domain.com:8000>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

図 12. httpd.conf ファイルの WebSphere Commerce ポート 8000 用の仮想ホスト・セクションの例: (WebSphere Commerce アクセラレーター)

```
<VirtualHost host.some_domain.com:8002>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

図 13. httpd.conf ファイルの WebSphere Commerce ポート 8002 用の仮想ホスト・セクションの例： WebSphere Commerce 管理コンソール

```
<VirtualHost host.some_domain.com:8004>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir¥installedApps¥host¥WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
```

図 14. httpd.conf ファイルの WebSphere Commerce ポート 8004 用の仮想ホスト・セクションの例： WebSphere Commerce 組織管理コンソール

注: WebSphere Commerce ツール用に構成したポート (デフォルトではポート 8000、8002、および 8004) への外部アクセスをファイアウォール・ソフトウェアで阻止することをお勧めします。その方法に関する詳細は、サイトでご使用のファイアウォール・ソフトウェアの資料を調べてください。

7. 変更を保管します。
8. `httpd.conf` ファイルに構文エラーがないことを確認するには、次のようにします。

   AIX Linux Solaris ご使用のマシンの IBM HTTP Server インストール・ディレクトリーの下にある `bin` サブディレクトリーに移動し、 `./httpd -t` コマンドを実行します。

   Windows マシン上の IBM HTTP Server インストール・ディレクトリーに移動し、次のコマンドを実行します。

   ```
   apache -t
   ```

9. IBM HTTP Server を開始します。

認証局に対するセキュアな証明書の要求

前のステップで作成したセキュリティー鍵を妥当性検査するには、 Equifax や VeriSign などの認証局 (CA) が発行した証明書が必要です。証明書には、サーバーの公開鍵、サーバーの証明書に関連した識別名、および証明書のシリアル番号と有効期限が含まれています。

他の CA を使用する場合、実行する手順については、直接その CA に問い合わせてください。

Equifax ユーザー

Equifax からセキュア・サーバー証明書を要求するには、以下の Web アドレスを参照して、示される指示に従ってください。

`http://www.equifax.com`

Equifax からの証明書は E メールで 2 ～ 4 日以内に送られてきます。

VeriSign ユーザー

VeriSign からセキュア・サーバー証明書を要求するには、以下の URL を参照して、示される指示に従ってください。

`http://www.verisign.com`

AIX IBM HTTP Server 用の手順を使用していても、 **Internet Connection Secure Server** (ICSS) のリンクをたどります。示される指示に従ってください。実動鍵ファイルをまだ作成していないならば、証明書ファイルを受け取ったときに、前の項で説明した方法によってそれを作成してください。

Solaris IBM HTTP Server 用の手順を使用していても、 **Internet Connection Secure Server** (ICSS) のリンクをたどります。後続のページには、その手順は OS/2® および AIX プラットフォームに適用されることが示されています。これらの指示は Solaris ソフトウェアにも適用されます。

示される指示に従ってください。要求を送信すると、証明書は 3 ～ 5 日以内に送られてきます。実動鍵ファイルをまだ作成していないならば、証明書ファイルを受け取ったときに、前の項で説明した方法によってそれを作成してください。

実動鍵ファイルの受け取りと現行鍵ファイルとしての設定

CA からの証明書が到着した後、Web サーバーが実動鍵ファイルを使用するように設定する必要があります。以下のステップを完了します。

1. 認証局から受け取った *certificatename*.kdb、 *certificatename*.rdb、および *certificatename*.sth ファイルを、マシン上の IBM HTTP Server インストール・パスの下の `ssl` サブディレクトリーにコピーします。 *certificatename* は認証要求で指定した証明書名です。
2. IBM HTTP Server を停止します。
3. AIX Solaris 以下のコマンドを実行して、 `JAVA_HOME` をエクスポートします。

```
DISPLAY=host_name:0.0
export DISPLAY
JAVA_HOME=java_home
export JAVA_HOME
```

ここで、 *host_name* は、 *java_home* が存在する現在使用中のマシンの完全修飾ホスト名です。

- AIX `/usr/java130`
- Solaris `/opt/WebSphere/AppServer/java131`

4. 鍵管理ユーティリティー (ikeyman) をオープンします。
5. *certificatename*.kdb ファイルをオープンして、プロンプトが出たらパスワードを入力します。
6. **「個人用証明書 (Personal Certificates)」**を選択して、**「受け取り」**をクリックします。
7. **「参照」**をクリックします。
8. 認証局から受け取ったファイルを格納しているフォルダーを選択します。*certificatename*.txt ファイルを選択して、**「OK」**をクリックします。
9. これで**「個人用証明書 (Personal Certificates)」**リスト・ボックスには、VeriSign *certificatename* 証明書または Equifax *certificatename* 証明書がリストされます。
10. 鍵管理ユーティリティーを終了します。
11. マシン上の IBM HTTP Server インストール・パスの下の conf サブディレクトリーに移動します。
12. httpd.conf のバックアップ・コピーを作成します。
13. httpd.conf をテキスト・エディターでオープンします。
14. ステップ 5 (214 ページ) でリストされた行がコメント化されていないことを確認します。
15. Keyfile "*keyfile_path_name*/keyfile.kdb" ディレクティブを検索して、上記のステップで作成されたファイルを指し示すようにパス名を変更します。
16. IBM HTTP Server を再始動します。

実動鍵ファイルのテスト

実動鍵をテストするには、以下のようにします。

1. ブラウザーを使用して以下の URL を表示します。

   `https://host_name`

   注:

   a. Web サーバーをカスタマイズしている場合、ホスト名の後に Web サーバーのフロントページの名前を入力しなければならないことがあります。

   b. http *ではなく* https と入力します。

   鍵が正しく定義されていれば、新規の証明書に関するいくつかのメッセージが表示されます。

2. **「新規のサイト証明書 (New Site Certificate)」**パネルで、この証明書を受け入れたい場合、**「この証明書を永続的に (有効期限が切れるまで) 受け入れる (Accept this certificate forever (until it expires))」** ラジオ・ボタンを選択します。
3. Web ブラウザーから、キャッシングおよびプロキシー (または Socks) サーバーの設定値を初期値に戻します。

これで、サーバー上で SSL が使用可能になりました。

WebSphere Commerce Payments の場合の SSL に関する考慮事項

デフォルトでは、WebSphere Commerce と WebSphere Commerce Payments の間の通信は SSL を経由します。ただし、次のようにして WebSphere Commerce Payments ユーザー・インターフェースを立ち上げた場合は、非 SSL 通信によって WebSphere Commerce Payments を呼び出すことになります。

http://*host_name*:*port_number*/webapp/PaymentManager

ここで、*host_name* はご使用の Payments Server マシン名で、*port_number* は 5432 です (デフォルト)。

必ず SSL 経由の通信にするには、以下の URL にアクセスします。

https://*host_name*:*port_number*/webapp/PaymentManager

ここで、*host_name* はご使用の Payments Server マシン名で、*port_number* は 5433 です (デフォルト)。

機密性の機能強化

WebSphere Commerce が URL 要求を受け取ると、Web コントローラーが、その要求されたコントローラー・コマンドのインターフェース名を取り込み、そのインターフェース名に基づいて、CMDREG 表からインプリメンテーション・クラス名を検索します。また、URLREG 表の HTTPS 列を検査して、その URL 要求に HTTPS (セキュア) プロトコルが必要かどうかも判別します。

機密情報を表示するコマンドについては、URLREG 表で HTTPS 値を 『1』 に設定しておく必要があります。たとえば、顧客注文の詳細情報を表示する OrderProcessView という表示コマンドは、必ず HTTPS プロトコル経由で実行しなければならないので、 URLREG 表の OrderProcessView エントリーの HTTPS 列には 『1』 を設定しておきます。

IBM HTTP サーバーでの SSL の使用可能化 (iSeries)

400 この項では、 iSeries プラットフォームに関連した説明を述べます。

SSL は、セキュリティー・プロトコルです。 SSL を使うと、クライアントとサーバーがやりとりするデータをプライベート・データのままに保つことができます。それによって、クライアントはサーバーの ID を認証し、サーバーはクライアントの ID を認証することができます。

ディジタル証明書とは、インターネット上のセキュア・トランザクションに関与するサーバーとクライアントを認証するための電子文書のことです。ディジタル証明書の発行者を認証局 (CA) と呼びます。 iSeries システムは、イントラネット環境においてサーバーおよびクライアントの証明書を発行する CA の役割を果たすことで、 iSeries CA または VeriSign のようなインターネット CA から発行されるサーバー証明書を持った認証済みサーバーとして稼働することができます。 IBM HTTP Server for iSeries が Web サーバーの場合、 SSL 対応のクライアントの認証用のクライアント証明書を要求するようこのサーバーを構成することもできます。

IBM HTTP Server for iSeries 上で SSL を使用可能にする方法の詳細は、「iSeries Information Center」(http://publib.boulder.ibm.com/html/as400/infocenter.html) を参照してください。このサイトにアクセスしたら、該当するオペレーティング・システムのバージョンと言語を選択して、**「Go」**をクリックします。 『SSL によるアプリケーションの保護』というトピックを検索して、SSL を使用可能にする方法を調べてください。

WebSphere Commerce Payments での SSL の使用

WebSphere Commerce インスタンスを作成した後でシステム証明書ストアを作成する場合、 WebSphere Commerce Payments と WebSphere Commerce インスタンスの両方に対して、そのシステム証明書ストアへのアクセスを認可する必要があります。たとえば、以下のコマンドは、 V5R1 システムで必要なアクセス権を WebSphere Commerce Payments インスタンスに認可します。

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QPYMSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QPYMSVR) DTAAUT(*R)
```

また、以下のコマンドは、 V5R1 システムで必要なアクセス権を WebSphere Commerce インスタンスに認可します。

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QEJBSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QEJBSVR) DTAAUT(*R)
```

リモート WebSphere Commerce Payments インスタンスを使用することにした場合、ディジタル証明書を発行するリモート認証局を信頼するように、 WebSphere Commerce インスタンスと WebSphere Commerce Payments インスタンスの両方を構成する必要があります。この 2 つのリモート・アプリケーションの間に信頼関係を確立したい場合は、以下の高レベルの手順を参照してください。

1. WebSphere Commerce マシンで、ディジタル証明書マネージャーを使ってサーバーの認証局をエクスポートします。
2. 証明書ファイルを WebSphere Commerce Payments マシンに転送します。
3. WebSphere Commerce Payments マシンで、ディジタル証明書マネージャーを使って WebSphere Commerce サーバーの認証局をインポートします。
4. インポートした WebSphere Commerce サーバーの認証局を信頼するように WebSphere Commerce Payments アプリケーション・サーバーを構成します。
5. WebSphere Commerce Payments マシンで、ディジタル証明書マネージャーを使ってサーバーの認証局をエクスポートします。
6. 証明書ファイルを WebSphere Commerce マシンに転送します。
7. WebSphere Commerce マシンで、ディジタル証明書マネージャーを使って WebSphere Commerce Payments サーバーの認証局をインポートします。

8. インポートした WebSphere Commerce Payments サーバーの認証局を信頼するように WebSphere Commerce アプリケーション・サーバーを構成します。

詳細は、 WebSphere Commerce の技術ライブラリーの Web ページ (http://www.software.ibm.com/software/commerce/wscom/library/lit-tech.html) で、**「Hints and Tips (ヒント)」**の項を参照してください。

第 18 章 IBM Directory Server (LDAP) での SSL の使用可能化

以下に、IBM Directory Server と WebSphere Commerce 用の SSL セキュリティーを構成するステップを示します。

IBM Directory Server のセットアップ

400 この項は、 iSeries プラットフォームには当てはまりません。 iSeries に関する詳細は、 224 ページの『iSeries プラットフォーム上での IBM OS/400 Directory Services のセットアップ』を参照してください。

IBM Directory Server をセットアップするには、以下のようにします。

1. IBM Directory Server 製品のインストール手順に従って IBM Directory Server をインストールします。必ず GSKit コンポーネントをインストールしてください。
2. インストールが完了したら、gsk5ikm 実行可能ファイルを実行して IBM Key Manager を呼び出します。
3. 新規の CMS 鍵データベース・ファイルを作成します。**「ファイルへのパスワードの stash (Stash the password to file)」**が選択されていることを確かめます (たとえば `ldap_key.kdb`)。
4. 自己署名証明書を、X509 V3 のバージョンおよび鍵サイズ 1024 で作成します。 (証明書には、自分の名前など、分かりやすいラベルを割り当てることができます。)
5. `Base64-encoded ASCII data` データ・タイプを使用して、証明書を証明書ファイル (たとえば、`cert.arm`) から取り出します。
6. ブラウザーをオープンして、アドレス `http://`*`host_name`*`/ldap` にアクセスします。ここで *host_name* は、ご使用の LDAP サーバー・マシン名です。
7. **「セキュリティー」→「SSL」→「設定」**をクリックし、次のような変更を加えます。
   - SSL 状況: SSL をオンまたは SSL のみ
   - 認証方法: サーバー認証
   - セキュア・ポート: 636
   - 鍵データベース・パスおよびファイル名:

     AIX Linux Solaris `/Keys/ldap_key.kdb`

     Windows *drive*`:¥Keys¥ldap_key.kdb`
   - 鍵ラベル: *your_label* (証明書のラベル)
   - 鍵パスワード: *xxxxx* (CMS 鍵データベース・ファイルのパスワード。**「ファイルへのパスワードの stash (Stash the password to file)」**を選択している場合は、パスワードを入力する必要はありません。)
8. **「更新」**をクリックし、SecureWay を再始動します。

iSeries プラットフォーム上での IBM OS/400 Directory Services のセットアップ

400 IBM OS/400 Directory Services を iSeries 上でセットアップするには、以下のようにします。

1. IBM iSeries Access for Windows をインストールします。
2. iSeries Navigator を Windows マシン上で、**「スタート」**—>**「プログラム」**—>**「IBM iSeries Access for Windows」**—>**「iSeries Navigator」**と進んで選択します。
3. ターゲットの iSeries マシンへの接続がない場合は、接続を作成します。
4. 左方のパネルでターゲット・マシンを展開し、次いで左方のパネルで**「ネットワーク」** —>**「サーバー」**を展開します。
5. 左方のパネルで**「TCP/IP」**をクリックします。
6. 右方のパネルで**「ディレクトリ」**を右マウス・ボタン・クリックし、ポップアップ・メニューから**「プロパティ」**を選択します。
7. 「ディレクトリのプロパティ (Directory Properties)」ウィンドウから、**「ネットワーク」**タブをクリックします。
8. **「ディジタル証明書マネージャ (Digital Certificate Manager)」**をクリックして、ディジタル証明書マネージャを起動し、証明書をアプリケーションの ″Directory Services server″ に割り当てます。
9. 証明書をディレクトリー・サービス・サーバーに割り当てた後に、**「OK」**をクリックして「ディレクトリのプロパティ (Directory Properties)」ウィンドウを閉じます。
10. 「ディレクトリのプロパティ (Directory Properties)」ウィンドウを再オープンすると、 SSL (Secure Socket Layer) が使用可能になっています。デフォルトの設定値を受け入れることができます。
    - SSL 状況:
    - 認証方法: サーバー認証
    - セキュア・ポート: 636
11. ディレクトリー・サービス・サーバーを再始動します。

WebSphere Application Server への自己署名証明書のインポート

400 SSL 証明書が VeriSign または Thwate などの認証局 (CA) によって発行されていない場合、 iSeries マシンからローカル CA をエクスポートして、それを WebSphere Commerce マシン上のデフォルトのトラスト鍵ストアにインポートする必要があります。 SSL を iSeries のローカル証明書で使用可能にし、ローカル CA を iSeries マシンからエクスポートするには、以下のようにします。

1. `HTTP *Admin` サーバーが稼働していることを確認します。稼働していない場合は、以下を実行します。

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. ブラウザーを起動してアドレス `http://host name:2001/` にアクセスし、iSeries タスク・ページをオープンします。

3. **「Digital Certificate Manager (ディジタル証明書マネージャ)」**を選択します。
4. **「証明書ストアの選択 (Select a Certificate Store)」**をクリックします。
5. 証明書ストアから、**「*System」**を選択します。
6. **「PC へのローカル CA 証明書のインストール (Install Local CA Certificate on Your PC)」**リンクが表示されない場合は、以下のようにしてローカル CA を作成する必要があります。
   a. 「認証局 (CA) の作成 (Create a Certificate Authority (CA))」をクリックします。
   b. iSeries 上で *Admin HTTP Server を再始動します。
   c. 新規の証明書をクライアントまたはサーバーのいずれかのタイプとして作成します。
   d. 新規に作成したローカル認証局を選択します。
   e. この証明書をディレクトリー・サービス・サーバーに割り当てます。
7. **「ローカル CA 証明書のインストール (Install Local CA Certificate)」**を PC 上でクリックします。
8. 「証明書のインストール (Install Certificate)」をクリックします。次いで、証明書 (.cer ファイル) を一時フォルダーに保管します。
9. 認証局 (.cer file) を Microsoft Internet Explorer にインポートし、次いで認証局を再び一時ディレクトリーの .cer ファイル (バイナリー 64 エンコード) にエクスポートします。
10. 証明書 (バイナリー 64 エンコード) を、WebSphere Application Server トラスト鍵ストアにインポートします。たとえば、以下のようにします。

```
keytool -import -alias nck -file /temp_dir/nck.cer
        -keystore /qibm/proddata/java400/jdk13/lib/security/cacerts
```

WebSphere Application Server

WebSphere Application Server の場合:

1. WebSphere Application Server が提供する IKeyMan (IBM Key Manager) を起動します。 (これは WebSphere Application Server メニューから見つけるか、またはコマンド・ウィンドウに ikeyman と直接入力することができます。)

   注: この IBM Key Manager は、 SecureWay が提供するものとは異なっています。

   デフォルトのパスワードは 'changeit' です。
2. WebSphere Application Server carcerts 鍵ストアをオープンします (たとえば、Windows 上では *WAS_installdir*¥AppServer¥java¥jre¥lib¥security¥cacerts)。
3. **「署名者証明書 (Signer Certificates)」**を検索し、次いで**「追加」**をクリックします。**「基本 64 エンコード ASCII データ (Base64-encoded ASCII data)」**データ・タイプを使用し、ステップ 5 (223 ページ) で作成した証明書ファイルを選択します。
4. 証明書の名前を入力します。
5. IKeyMan をクローズします。

WebSphere Commerce

SecureWay を扱えるように WebSphere Commerce をセットアップするには、次のように *instance*.xml ファイルを変更する必要があります。

1. 以下のようにして新規の JNDI 環境変数を追加します。

   ```
   java.naming.security.protocol = ssl
   ```

2. 以下のようにして LdapPort を '636' に変更します。

   ```
   LdapPort = 636
   ```

3. WebSphere Commerce を再始動します。

以下に例を示します。

```
<MemberSubSystem name="Member SubSystem"
          AuthenticationMode="LDAP"
          ProfileDataStorage="LDAP"  >

  <Directory LdapAdminDN="cn=root"
                LdapAuthenticationMode="SIMPLE"
                LdapTimeOut="0"
                LdapVersion="3"
                EntryFileName="E:/WebSphere/WPS/xml/ldap/attributeMap.xml"
                LdapPort="636"
                LdapAdminPW="<adminpassword>"
                LdapHost="<hostname>"
                MigrateUsersFromWCSdb="OFF"
                JNDIEnvPropName1="java.naming.security.protocol"
                JNDIEnvPropValue1="ssl"
                display="false"
                LdapType="SECUREWAY"

   . . . .

  />


</MemberSubSystem>
```

第 6 部 付録

付録. デフォルトのアクセス制御ポリシーおよびグループ

付録では、WebSphere Commerce に付属のデフォルト・ポリシーおよびグループをリストします。

デフォルトのアクセス制御ポリシー

デフォルトのアクセス制御ポリシーは、以下のカテゴリー別に編成されています。

- **役割ベースのポリシー:** それぞれのデフォルト役割ごとの役割ベースのポリシーです。それらのポリシーは、だれがそれぞれのコマンドを実行できるかを定義しているので、コマンド・レベル・ポリシーとも呼ばれます。
- **リソース・レベルのポリシー:** ビジネス分野別のリソース・レベルのポリシーです。これらのポリシーは、特定のリソースに対してユーザーのグループが実行できるアクションを定義します。各ビジネス分野の下で、ポリシーが規定するリソースのタイプ別にポリシーが編成されています。
  - **データ・リソース** - オーダーや入札など、操作できるビジネス・オブジェクトです。
  - **Data Bean リソース** - ビジネス・オブジェクトに関する情報が入っています。 Data Bean はオブジェクト情報を Web ページに表示するために使用されます。

表 22. ポリシーの情報の入手先

ポリシー	開始ページ
役割ベースのポリシー	230 ページの『役割ベースのポリシー』
ビジネス分野別のリソース・レベルのポリシー	233 ページの『ビジネス分野別のリソース・レベルのポリシー』
オーダー	233 ページの『オーダー』
取引 (契約)	235 ページの『取引 (契約)』
承認	235 ページの『承認』
オークション	235 ページの『オークション』
ビジネス・インテリジェンス	236 ページの『ビジネス・インテリジェンス』
メンバーシップ	236 ページの『メンバーシップ』
マーケティング	237 ページの『マーケティング』
カタログ	237 ページの『カタログ』
接続および通知	238 ページの『接続および通知』
調達	238 ページの『調達』
クーポン	238 ページの『クーポン』
顧客プロファイル作成	238 ページの『顧客プロファイル作成』
割引	239 ページの『割引』
スケジュール済み在庫	
在庫管理	
オーダー管理	240 ページの『オーダー管理』
決済	240 ページの『決済』
ポリシー・エディター	240 ページの『ポリシー・エディター』
商品アドバイザー	241 ページの『商品アドバイザー』

表 22. ポリシーの情報の入手先 (続き)

ポリシー	開始ページ
RFQ	241 ページの『RFQ』
ルール	241 ページの『ルール』
スケジューラー	241 ページの『スケジューラー』
Commerce アクセラレーター	241 ページの『Commerce アクセラレーター』
配送	242 ページの『配送』
税	242 ページの『税』
ライブ・ヘルプ/コラボレイティブ・ワークスペース/カスタマー・ケア	242 ページの『ライブ・ヘルプ/コラボレイティブ・ワークスペース/カスタマー・ケア』
ストアの状態	242 ページの『ストアの状態』
ストア管理	

役割ベースのポリシー

- SiteAdministratorsCanDoEverything
- BuyerAdministratorsExecuteBuyersAdministratorsCommands
- BuyerApproversExecuteBuyerApproversCmdResourceGroup
- GuestsExecuteGuestUsersCmdResourceGroup
- BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
- MarketingManagersExecuteMarketingManagerCmdResourceGroup
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
- AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
- SalesManagersExecuteSalesManagersCmdResourceGroup
- ProductManagersExecuteProductManagersCmdResourceGroup
- SellerAdministratorsExecuteSellerAdministratorsCommands
- SellersExecuteSellersCmdResourceGroup
- CategoryManagersExecuteCategoryManagersCmdResourceGroup
- Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
- Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
- PickPackersExecutePickPackersCmdResourceGroup
- ReceiversExecuteReceiversCmdResourceGroup
- ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
- OperationsManagersExecuteOperationsManagersCmdResourceGroup
- LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
- ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeViews
- BuyerAdministratorsExecuteBuyerAdministratorsViews
- BuyerApproversExecuteBuyerApproversViews
- MarketingManagersExecuteMarketingManagersViews

- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
- SalesManagersExecuteSalesManagersViews
- AccountRepresentativesExecuteAccountRepresentativesViews
- Buyers(buy-side)ExecuteBuyers(buy-side)Views
- Buyers(sell-side)ExecuteBuyers(sell-side)Views
- CategoryManagersExecuteCategoryManagersViews
- CustomersExecuteCustomersViews
- ProductManagersExecuteProductManagersViews
- PickPackersExecutePickPackersViews
- ReceiversExecuteReceiversViews
- ReturnsAdministratorsExecuteReturnsAdministratorsViews
- OperationsManagersExecuteOperationsManagersViews
- LogisticsManagersExecuteLogisticsManagersViews
- SellerAdministratorsExecuteSellerAdministratorsViews
- SellersExecuteSellersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersViews
- NonRejectedUsersExecuteNonRejectedUsersViews
- GuestUsersExecuteGuestUsersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersCommandsResourceGroup
- ChannelManagersExecuteChannelManagersCommands
- AllUsersExecuteAllSiteUserCmdResourceGroup
- AllUsersExecuteAllSiteUsersViews
- RegisteredCustomersForOrgExecuteRegisteredUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredUserViews
- ChannelManagersExecuteChannelManagersViews
- AllUsersExecuteResellerUserCmdResourceGroup
- AllUsersExecuteResellerUserViews
- RegisteredCustomersForOrgExecuteRegisteredResellerUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredResellerUserViews

以下の表は、役割ベースのポリシーを、役割、アクセス・グループ、リソース・グループ、そしてビュー別に示しています。

注:

1. 表の**役割**列以外のほとんどの項目は、長さの関係により各セルの中で改行されています。
2. 下記のすべての役割が、WebSphere Commerce での定義された役割というわけではありません。定義された WebSphere Commerce 役割の詳細は、 32 ページの『役割』を参照してください。

表 23. 役割、アクセス・グループ、リソース・グループ、そしてビュー別に示した役割ベースのポリシー

役割	役割ベースのポリシーで使用されるアクセス・グループ	コントローラー・コマンドの役割ベースのポリシーで使用されるリソース・グループ	ビューの役割ベースのポリシーで使用されるアクション・グループ
サイト管理者	SiteAdministrators	n/a	n/a
バイヤー管理者	BuyerAdministrators	BuyerAdministrators CommandsResource Group	BuyerAdministrators Views
バイヤー承認者	BuyerApprovers	BuyerApproversCmd ResourceGroup	BuyerApproversViews
ゲスト[1]	Guests	GuestUsersCmd ResourceGroup	GuestUsersViews
顧客サービス担当者	CustomerService Representatives	CustomerService RepCmdResourceGroup	CustomerService Representative Views
マーケティング・マネージャー	MarketingManagers	MarketingManager CmdResourceGroup	MarketingManagersViews
顧客サービス・スーパーバイザー	CustomerService Supervisors	CustomerService Supervisor CmdResourceGroup	CustomerService SupervisorViews
アカウント担当者	Account Representatives	AccountRepresentativesCmd ResourceGroup	AccountRepresentatives Views
セールス・マネージャー	SalesManagers	SalesManagersCmd ResourceGroup	SalesManagersViews
プロダクト・マネージャー	ProductManagers	ProductManagers CmdResourceGroup	ProductManagersViews
セラー管理者	Seller Administrators	SellerAdministrators CommandsResourceGroup	SellerAdministrators Views
セラー	Sellers	SellersCmdResourceGroup	SellersViews
カテゴリー・マネージャー	CategoryManagers	CategoryManagers CmdResourceGroup	CategoryManagersViews
バイヤー (購買サイド)	Buyers(buy-side)	Buyers(buy-side) CommandsResourceGroup	Buyers(buy-side)Views
バイヤー (販売サイド)	Buyers(sell-side)	Buyers(sell-side) CommandsResourceGroup	Buyers (sell-side)Views
梱包担当者	PickPackers	PickPackersCmd ResourceGroup	PickPackersViews
受取人	Receivers	ReceiversCmdResourceGroup	ReceiversViews
返品管理者	ReturnsAdministrators	ReturnsAdministratorsCmd ResourceGroup	ReturnsAdministrators Views
オペレーション・マネージャー	OperationsManagers	OperationsManagersCmd ResourceGroup	OperationsManagersViews
物流管理マネージャー	LogisticsManagers	LogisticsManagersCmd ResourceGroup	LogisticsManagersViews
調達バイヤー	ProcurementBuyers	ProcurementBuyersCmd ResourceGroup	n/a

表 23. 役割、アクセス・グループ、リソース・グループ、そしてビュー別に示した役割ベースのポリシー (続き)

役割	役割ベースのポリシーで使用されるアクセス・グループ	コントローラー・コマンドの役割ベースのポリシーで使用されるリソース・グループ	ビューの役割ベースのポリシーで使用されるアクション・グループ
登録済み承認ユーザー[2]	RegisteredApprovedUsers	RegisteredApprovedUsersCommandsResourceGroup	RegisteredApprovedUsersViews
拒否されないユーザー[3]	NonRejectedUsers	NonRejectedUserCommandsResourceGroup	NonRejectedUsersViews
チャネル・マネージャー	ChannelManagers	ChannelManagersCmdResourceGroup	ChannelManagersViews
すべてのユーザー[4]	AllUsers	ResellerUserCmdResourceGroup[5]	ResellerUserViews[5]
		AllSiteUserCmdResourceGroup[6]	AllSiteUsersViews[6]
登録済み顧客 (OrgandAncestorOrgs 役割修飾子付き)	RegisteredCustomersForOrg	RegisteredUserCmdResourceGroup	RegisteredUserViews
		RegisteredResellerUserCmdResourceGroup	RegisteredResellerUserViews

注:

1. 「ゲスト」は本当の役割ではありません。登録状況を 『G』 に設定する (USER.REGISTERTYPE 列を 『G』 に設定する) ユーザーは、暗黙的に Guests アクセス・グループに属することになります。
2. 「登録済み承認ユーザー」は本当の役割ではありません。登録状況を 『R』 に設定し (USER.REGISTERTYPE 列を 『R』 に設定する)、状況が承認済みである (MEMBER.STATE 列が 1 に設定される) ユーザーは、暗黙的に RegisteredApprovedUsers アクセス・グループに属することになります。
3. 「拒否されないユーザー」は本当の役割ではありません。登録状況が「拒否されない」である (MEMBER.STATE 列が 2 に設定される) ユーザーは、暗黙的に NonRejectedUsers アクセス・グループに属することになります。
4. 「すべてのユーザー」は本当の役割ではありません。システムのすべてのユーザーは、暗黙的に AllUsers アクセス・グループに属することになります。
5. これらのアクション・グループとリソース・グループは、 B2CPolicyGroup の一部であるポリシーに属します。このポリシー・グループは、B2C ビジネス・モデルに従う組織だけに適用される可能性が高くなります。
6. これらのアクション・グループとリソース・グループは、 ManagementAndAdministrationPolicyGroup の一部であるポリシーに属します。このポリシー・グループは、すべての組織に適用される可能性が高くなります。

ビジネス分野別のリソース・レベルのポリシー

オーダー

データ・リソース: オーダー:

- AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
- AllUsersExecuteOrderCreateCommandsOnStoreResource
- AllUsersExecuteOrderReadCommandsOnOrderResource
- AllUsersExecuteOrderPrepareCommandsOnOrderResource
- AllUsersExecuteOrderWriteCommandsOnOrderResource
- AllUsersExecuteScheduledOrderCancelOnOrderResource
- AllUsersExecuteReturnAgainstOrderOnOrderResource

- AllUsersExecuteOrderProcessOnOrderResource
- OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
- CustomerOrderManagersForOrgExecuteOrderProcessOnOrderResource
- ResellerAdministratorsForOrgExecuteOrderReadCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderPrepareCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderWriteCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteScheduledOrderCancelOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderProcessOnOrderDataResourceGroup
- EmailOrderNotificationManagersForOrgExecuteCustomerServiceEmailOrderOnOrderResource

データ・リソース: リクィジション・リスト:

- AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
- AllUsersExecuteRequisitionListSharedReadCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveReadCommandsOnPrivateRequisitionListResource
- AllUsersExecuteRequisitionListWriteCommandsOnRequisitionListResource
- AllUsersExecuteRequisitionListSharedProcessCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveProcessCommandsOnPrivateRequisitionListResource

データ・リソース: 興味のあるアイテム:

- AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
- AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource

データ・リソース: RMA:

- AllUsersExecuteRMACreateCommandsOnStoreResource
- AllUsersExecuteRMAReadCommandsOnRMAResource
- AllUsersExecuteRMAPrepareOnRMAResource
- AllUsersExecuteRMAWriteCommandsOnRMAResource
- AllUsersExecuteRMAProcessCommandsOnRMAResource
- RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
- RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
- RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
- RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
- StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource

Data Bean: オーダー:

- AllUsersDisplayOrderDatabeanResourceGroup
- AllUsersDisplayApprovalsOrderDataBeansResourceGroup
- AccountRepresentativesForOrgDisplayOrderDatabeanOnlyResourceGroup

Data Bean: リクィジション・リスト:

AllUsersDisplaySharedRequisitionListDataBeansIfSameOrganizationalEntityAsCreator

Data Bean: 興味のあるアイテム: AllUsersDisplayInterestItemDatabeanResourceGroup

Data Bean: RMA: AllUsersDisplayRMADatabeanResourceGroup

取引 (契約)

データ・リソース: 契約:

- ContractCreatorsForOrgExecuteContractCreateCommandsOnMemberResource
- ContractManagersForOrgExecuteContractManageCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource
- ContractViewersExecuteContractDisplayCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractSubmitCommandsOnContractResource
- ContractManagersForOrgExecuteContractAccountManageCommandsOnAccountResource

データ・リソース: ビジネス・ポリシー:

- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyCreateCommandsOnStoreResource
- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyManageCommandsOnBusinessPolicyResource

データ・リソース: ストア作成: StoreCreatorsForOrgExecuteStoreCreationCommandsOnOrganizationResource

Data Bean: AccountHandlersForOrgDisplayTradingDatabeanResourceGroup

承認

データ・リソース:

- AllUsersExecuteApproveCommandsOnApprovalResource
- FlowAdministratorExecutesFlowAdminCreateCommandsOnStoreEntityResource
- FlowAdministratorExecutesFlowadminDeleteCommandsOnFlowadminResource

Data Bean: FlowAdministratorsForOrgDisplayFlowadminDatabean

オークション

データ・リソース:

- AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
- AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
- AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionStyleManageCommandsOnAuctionStyleResource
- AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteBidControlRuleManageCommandsOnBidControlRuleResource
- RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteBidManageCommandsOnBidResources
- RegisteredApprovedUsersExecuteAutoBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteAutoBidManageCommandsOnAutoBidResources

Data Bean: AuctionDatabeanOwnersDisplayAuctionDatabeans

ビジネス・インテリジェンス

データ・リソース:

- BusinessAnalystsForOrgExecuteViewContextListCommandsOnStoreEntityResource
- IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReportCommands OnStoreEntityResource

メンバーシップ

データ・リソース: ユーザー:

- MembershipAdministratorsForOrgExecuteUserAdminUpdateCommandsOnUserResource
- GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteUserSelfRegistrationContinuationCommandsOnUserResource
- NonRejectedUsersExecuteNonRejectedUserCommands
- AllUsersDisplayUserDatabeanResourceGroup
- NonRejectedDisplayUserDatabeanResourceGroup

データ・リソース: 組織:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrgEntityPolicySubscription UpdateCommandsOnOrganizationResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrganizationManageActions OnOrganiztionResource
- CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommands OnOrganizationResource
- CSAMembershipAdministratorsExecuteUserAdminRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityUpdateCommandsOnOrganizationResource GuestsExecuteResellerSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteResellerSelfRegistrationContinuationCommandsOnOrganizationResource
- ChannelManagersExecuteOrgEntityLockCommandsOnOrgResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteApproveGroupUpdateCommands OnOrganizationResource

データ・リソース: メンバー・グループ:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnUserResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnMemberGroupResource
- MemberGroupAdministratorsForOrgExecuteMemberGroupCreateCommandsOnMemberResource
- MemberGroupManagersForOrgExecuteMemberGroupManageCommandsOnMemberGroupResource

データ・リソース: 住所:

- NonRejectedUsersExecuteAddressManageCommandsOnUserResource
- MembershipAdministratorsForOrgExecuteAddressManageCommandsOnMemberResource

データ・リソース: 役割:

- MembershipAdministratorsForOrgExecuteRoleUnassignCommandsOnUserResource
- OrganizationRoleAdministratorsExecuteRoleManageCommandsOnOrganizationResource

- MembershipAdministratorsForOrgExecuteUserRoleAssignCommandsOnOrganizationResource

データ・リソース: メンバー属性:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberAttributeCommands OnOrgResource
- AllUsersExecuteMemberAttributeCommandsOnUserResource

Data Bean:

- MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayOrganizationDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayUserDatabeanResourceGroup
- EmployeesDisplayOrganizationSpecificDatabeanResourceGroup

マーケティング

データ・リソース: キャンペーン:

- CampaignManagersForOrgExecuteCampaignRelatedCreateCommandsOnStoreEntityResource
- CampaignManagersForOrgExecuteCampaignUpdateCommandsOnCampaignResource
- CampaignManagersForOrgExecuteInitiativeUpdateCommandsOnInitiativeResource
- CampaignManagersForOrgExecuteEMarketingSpotUpdateCommandsOnEMarketingSpotResource
- CampaignManagersForOrgExecuteCollateralUpdateCommandsOnCollateralResource

データ・リソース: E メール・アクティビティー:

- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnEmailActivity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivityDeleteCommandsOnEmailActivity DataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivityConfigurationSaveCommands OnEmailActivityDataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroupAllUsersExecuteEmailOptOutDataResourceGroup

Data Bean: キャンペーン: CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

Data Bean: E メール・アクティビティー:

- EmailUserReceiveDataBeanPolicy
- EmailActivityDataBeanPolicy
- EmailConfigurationDataBeanPolicy

Data Bean: e-販売促進: EpromotionDisplayDataBeanPolicy

カタログ

データ・リソース:

- CatalogManagersForOrgExecuteStoreCategoryManageCommandsOnCatalogResource
- CatalogManagersForOrgExecuteCatalogManageCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteCatalogGroupManageCommandsOnCatalogGroupResource
- CatalogEntryManagersForOrgExecuteStoreCatalogEntryManageCommandsOnStoreEntityResource

- CatalogGroupManagersForOrgExecuteProductSetAddCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteProductSetManageCommandsOnProductSetResource
- CatalogEntryManagersForOrgExecuteCatalogEntryManageCommandsOnCatalogEntryResource
- CatalogEntryManagersForOrgExecuteCatalogEntryRelationManageCommandsOnCatalogResource
- CatalogEntryManagersForOrgExecuteCatalogStoreManageCommandsOnStoreEntityResource

Data Bean:

- ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup
- CatalogGroupViewersForOrgDisplayCatalogGroupDataBeansResourceGroup
- CatalogListViewersForOrgDisplayCatalogListDataBeansResourceGroup

接続および通知

データ・リソース:

- BackendOrderAdministratorsForOrgExecuteBackendOrderStatusCreateCommandsOnOrderDataResource
- BackendPickPackersForOrgExecuteBackendPickPackListCommandsOnFulfillmentCenterDataResource
- MessagingUpdateAdministratorsForOrgExecuteMessagingUpdateCommandsOnStoreEntityResource

調達

データ・リソース:

- ProcurementAdministratorsForOrgExecuteProcurementAuthenticationAndRegistration OnOrganizationResource
- ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource

クーポン

データ・リソース:

- CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource
- CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommandsOnCouponPromotionResource
- AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
- AllUsersExecuteCouponDeleteCommandsOnCouponWalletResource
- CouponAdministratorsForOrgExecuteCouponPromotionUpdateCommandsOnStoreEntityResource
- AllUsersExecuteCouponSaveCommandsOnCouponWalletResource

Data Bean: CouponAdministratorsForOrgDisplayECouponPromotionBeans

顧客プロファイル作成

データ・リソース: CustomerProfileEditorsForOrgExecuteSegmentManageCommandsOnStoreEntityResource

Data Bean: CustomerProfileEditorsForOrgDisplaySegmentationDatabeansResourceGroup

割引

データ・リソース:

- DiscountAdministratorsForOrgExecuteDiscountCreateCommandsOnStoreEntityResource
- DiscountAdministratorsForOrgExecuteDiscountDeployCommandsOnCalculationCodeResource
- DiscountAdministratorsForOrgExecuteDiscountAssociateCommandsOnCalculationCodeResource

Data Bean: DiscountViewersForOrgDisplayDiscountDatabeans

在庫管理

データ・リソース:

- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterCreateCommandsOn OrganizationResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommandsOn FulfillmentCenterResource
- PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommandsOn FulfillmentCenterResource
- VendorInventoryManagersForOrgExecuteVendorManageCommandsOnVendorResource
- VendorInventoryManagersForOrgExecuteVendorCreateCommandsOnStoreEntityResource
- ExpectedInventoryManagersForOrgExecuteInventoryManageCommandsOnStoreEntityResource
- PickPackGeneratorsForOrgExecutePickPackGenerateCommandsOnFulfillmentCenterResource
- InventoryAdjustersForOrgExecuteInventoryAdjustCommandsOnStoreEntityResource
- ReturnReasonsManagersForOrgExecuteReturnReasonsCommandsOnStoreEntityResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterReleaseOnFulfillmentCenter ReleaseDataResourceGroup
- SharedFulfillmentCenterPickBatchInventoryManagersExecuteReleaseReadyShipCommands OnFulfillmentCenterDataResource
- SharedFulfillmentCenterPickPackGeneratorsExecutePickPackGenerateCommands OnFulfillmentCenterResource
- SharedFulfillmentCenterManagersExecuteFulfillmentCenterReleaseCommandsOnFulfillment CenterReleaseDataResourceGroup

Data Bean:

- ReturnReasonsManagersForOrgDisplayReturnReasonsOrderManagementDataBeansResourceGroup
- ExpectedInventoryManagersForOrgDisplayExpectedInventoryDataBeansResourceGroup
- VendorInventoryManagersForOrgDisplayVendorInventoryDataBeansResourceGroup
- ProductFindInventoryManagersForOrgDisplayProductFindInventoryDataBeansResourceGroup
- FulfillmentCenterManagersForOrgDisplayFulfillmentCenterDataBeansResourceGroup
- PickBatchInventoryManagersForOrgDisplayPickBatchInventoryDataBeansResourceGroup
- ReceiverOrderManagersForOrgDisplayReceiverOrderManagementDataBeansResourceGroup
- ReturnsAdminOrderManagersForOrgDisplayReturnsAdminOrderManagementDataBeans ResourceGroup
- SuperUserOrderManagersForOrgDisplaySuperUserOrderManagementDataBeans ResourceGroupFulfillmentManagersForOrgDisplayReleaseOrderItemsDatabeanResourceGroup

オーダー管理

データ・リソース:

- CustomerOrderManagersForOrgExecuteCustomerServiceOrderWriteCommands OnOrderResource
- CustomerOrderManagersForOrgExecuteCustomerServiceOrderCreateCommands OnStoreEntityResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnWriteCommands OnRMAResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnCreateCommands OnStoreEntityResource
- CustomerOrderManagersExecuteCustomerWriteCommandsOnUserResource
- CustomerOrderManagersForDefaultOrgExecuteCustomerServiceCustomerWriteCommandsOn UserDataResourceGroupwithGuestRegisterType

Data Bean:

- CustomerOrderManagersForOrgDisplayCustomerOrderManagementDatabeans
- MemberOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- MemberOrderManagersDisplayOrganizationSpecificDatabeans
- MemberOrderManagersDisplayUserDatabeanResourceGroup
- UserOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- UserOrderManagersDisplayOrganizationSpecificDatabeans
- UserOrderManagersDisplayUserDatabeanResourceGroup
- LogisticsManagersForOrgDisplayOrdersAndReturnsListsDatabeans
- ReturnsManagersForOrgDisplayReturnsListsDatabeans

決済

データ・リソース:

- AccountManagersForOrgExecuteAccountCreateCommandsOnOrganizationResource
- AccountAdministratorsForOrgExecuteAccountManageCommandsOnAccountResource
- AccountViewersForOrgExecutePaymentSummaryGenerateCommandsOnAccountResource
- AccountViewersForOrgExecuteStorePaymentAdminCommandsOnStoreEntityResource
- AllUsersExecutePaymentOrderWriteCommandsOnOrderResource

ポリシー・エディター

データ・リソース:

- StoreAdministratorsForOrgExecuteACPolicyCreateCommandsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACPolicyEditCommandsOnACPolicyResource
- StoreAdministratorsForOrgExecuteACViewPoliciesForUpdateActionsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACViewApplicablePoliciesActionsOnOrganizationResource
- DescendantStoreAdministratorsExecuteACViewPoliciesForOrgActionsOnOrganizationResource

Data Bean: StoreAdministratorsForOrgExecuteUserGroupSearchViews

商品アドバイザー

Data Bean:

- ProductAdvisorStatisticiansForOrgDisplayProductAdvisorStatisticsDatabeans
- SalesAssistantStatisticiansForOrgDisplaySalesAssistantStatisticsDatabeans
- ProductAdvisorManagersDisplayPAWCBEDatabeanResourceGroup
- GuidedSellManagersDisplayGSWCBEDatabeanResourceGroup

RFQ

データ・リソース:

- RFQBuyersExecuteRFQCreateCommandsOnStoreEntityDataResourceGroup
- RFQBuyersManageRFQResourcesTheyOwn
- RFQBuyersManageRFQResponsesForRFQsTheyOwn
- RFQAdministratorsAdministerRFQs
- RFQAdministratorsManageRFQResponses
- RFQSalesManagersForOrgCreateRFQResponse
- RFQSalesManagersExecuteRFQResponseManageCommandsOnRFQResponseResource
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQWithPublicAccess TypeResourceGroup
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQResourceGroup

Data Bean:

- RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
- RFQBuyersDisplayRFQResponseDataBeansViewabletoRFQOwnerResourceGroup
- RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup
- RFQSalesViewersDisplayRFQDataBeanWithPublicAccessTypeResourceGroup
- RFQSalesViewersDisplayRFQDataBeanResourceGroup

ルール

データ・リソース: StoreAdministratorsForOrgExecutePersonalizationRuleServiceAdministrationCommands OnStoreEntityResource

Data Bean: StoreAdministratorsForOrgDisplayPersonalizationRuleServiceAdministrationDataBeanResourceGroup

スケジューラー

データ・リソース:

- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnStoreEntityResource
- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnUserResource

Data Bean: StoreAdministratorsForOrgDisplaySchedulerDataBeansResourceGroup

Commerce アクセラレーター

データ・リソース:

- B2CCSAViewUsersForOrgExecuteB2CCSAViewActionsOnStoreEntityResource

- B2BCSAViewUsersForOrgExecuteB2BCSAViewActionsOnStoreEntityResource
- CHSCSAViewUsersForOrgExecuteCHSCSAViewActionsOnStoreEntityResource
- RHSCSAViewUsersForOrgExecuteRHSCSAViewActionsOnStoreEntityResource
- CPSCSAViewUsersForOrgExecuteCPSCSAViewActionsOnStoreEntityResource
- RPSCSAViewUsersForOrgExecuteRPSCSAViewActionsOnStoreEntityResource
- HCPCSAViewUsersForOrgExecuteHCPCSAViewActionsOnStoreEntityResource
- MHSCSAViewUsersForOrgExecuteMHSCSAViewActionsOnStoreEntityResource
- MPSCSAViewUsersForOrgExecuteMPSCSAViewActionsOnStoreEntityResource
- SCPCSAViewUsersForOrgExecuteSCPCSAViewActionsOnStoreEntityResource
- SHSCSAViewUsersForOrgExecuteSHSCSAViewActionsOnStoreEntityResource
- SPSCSAViewUsersForOrgExecuteSPSCSAViewActionsOnStoreEntityResource

配送

データ・リソース: ShippingMembershipAdministratorsForOrgExecuteShippingManageCommandsOnStore DataResourceGroup

Data Bean: ShippingMembershipAdministratorsForOrgDisplayShippingDatabeanResourceGroup

税

データ・リソース: TaxationAdministratorsForOrgExecuteTaxationManageCommandsOnStoreDataResourceGroup

Data Bean: TaxationAdministratorsForOrgDisplayTaxationDatabeanResourceGroup

ライブ・ヘルプ/コラボレイティブ・ワークスペース/カスタマー・ケア

データ・リソース: ライブ・ヘルプ:

- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnUserDataResources
- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnOrderDataResources

データ・リソース: カスタマー・ケア:
CustomerCareAdministratorsForOrgExecuteCustomerCareQueueManageCommandsOnStoreResource

Data Bean: ライブ・ヘルプ: LiveHelpAgentsForOrgDisplayCustomerCareDatabeanResourceGroup

Data Bean: コラボレイティブ・ワークスペース:
CollaborativeWorkspaceAdministratorsForOrgDisplayCollaborativeWorkspaceDatabeanResourceGroup

ストアの状態

データ・リソース:

- ChannelManagersExecuteStoreStateChangeCommandsOnStoreResource
- AdministrativeRolesForOrgExecuteStoreStateChangeCommandsOnStoreResource
- AdministratorsForOrgAccessStoreWithCloseOrSuspendStateResourceGroup
- AllUsersAccessStoreWithOpenStateResourceGroup

ストア管理

データ・リソース: レポート送付:

ReportDeliveryManagersForOrgExecuteSetupReportDeliveryCommandsOnStoreDataResourceGroup

データ・リソース: ストア:

- StoreFrontManagersForOrgExecuteStoreFrontRelatedUpdateOnStoreEntityResource
- StoreProfileManagersForOrgExecuteStoreProfileRelatedUpdateOnStoreEntityResource

デフォルトのアクセス制御ポリシー・グループ

WebSphere Commerce に付属するデフォルトのアクセス制御ポリシー・グループは、以下のとおりです。

- Management and Administration Policy Group: このポリシー・グループには、すべてのメンバー管理およびストア管理ポリシーが含まれています。
- Guest Shopper Management Policy Group: このポリシー・グループには、ゲスト・ショッパー管理に関連したポリシーすべてが含まれています。
- Common Shopping Policy Group: このポリシー・グループには、消費者向けと B2B シナリオの両方に共通するショッピング関連ポリシーすべてが含まれています。
- B2C Policy Group: このポリシー・グループには、消費者向け固有のショッピング・ポリシーすべてが含まれています。
- B2B Policy Group: このポリシー・グループには、 B2B 固有のショッピング・ポリシーすべてが含まれています。

注: Management and Administration Policy Group は、一般的にすべての組織に適用される、中核となるポリシー・グループです。組織が何らかのポリシー・グループに加入している場合、このポリシー・グループにも加入しているはずです。ストアを所有する組織の場合、Management and Administration Policy Group に加えて、ストアのタイプに応じて、Common Shopping Policy Group、B2C Policy Group、 B2B Policy Group にも加入しているはずです。 Guest Shopper Management Policy Group には、ゲスト・ショッパーを所有する組織だけが加入します。共通シナリオでは、デフォルト組織がそれに相当します。

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あり、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。

本文書中において IBM プログラム・プロダクトについて言及している場合、当該 IBM プログラム・プロダクトのみが使用可能であることを意味するものではありません。 IBM 製品、プログラムまたはサービスに代えて、 IBM の知的所有権を侵害することのない機能的に同等のプログラムまたは製品を使用することができます。ただし、IBM によって明示的に指定されたものを除き、他社の製品と組み合わせた場合の動作の評価と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。使用許諾については、下記の宛先に書面にてご照会ください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

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

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 Canada Ltd.
Office of the Lab Director
8200 Warden Avenue
Markham, Ontario
L6G 1C7
Canada

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。

この製品で使用されているクレジット・カードのイメージ、商標、商号は、そのクレジット・カードを利用して支払うことを、それら商標等の所有者によって許可された人のみが、使用することができます。

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。お客様は、IBM 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。

商標

以下は、IBM Corporation の商標です。

AIX	AS/400	DB2
@server	IBM	iSeries
OS/2	OS/400	SecureWay
WebSphere	Domino	

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

Microsoft および Windows は、Microsoft Corporation 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。

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