IBM® WebSphere® Commerse

アクセス・コントロール・ガイド

バージョン 5.4

IBM® WebSphere® Commerse

アクセス・コントロール・ガイド

バージョン 5.4

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、『特記事項』に記載されている情報をお読みください。

本書は以下の製品に適用されます。

IBM WebSphere Commerce Business Edition for Windows NT and Windows 2000 バージョン 5.4

IBM WebSphere Commerce Business Edition for AIX バージョン 5.4

IBM WebSphere Commerce Business Edition for Solaris Operating Environment Software バージョン 5.4

IBM WebSphere Commerce Studio, Business Developer Edition for Windows NT and Windows 2000 バージョン 5.4

IBM WebSphere Commerce Professional Edition for Windows NT and Windows 2000 バージョン 5.4

IBM WebSphere Commerce Professional Edition for AIX バージョン 5.4

IBM WebSphere Commerce Professional Edition for Solaris Operating Environment Software バージョン 5.4

IBM WebSphere Commerce Studio, Professional Developer Edition for Windows NT and Windows 2000 バージョン 5.4

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。

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

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

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは `http://www.ibm.com/jp/manuals/` の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

原 典:	IBM WebSphere Commerce Access Control Guide Version 5.4
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 2002.4

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

情報の入手場所

WebSphere Commerce™ には、オンラインとハードコピーの資料が付属しており、e-commerce ソリューション全体の情報を説明します。さらに、WebSphere Commerce にバンドルされているソフトウェア製品では、そのソフトウェアの特定の特徴や機能を説明した情報が提供されています。このセクションでは、多様な種類の情報の入手場所を一覧にしています。

WebSphere Commerce の資料

- *IBM WebSphere Commerce 基本、バージョン 5.4*
- *IBM WebSphere Commerce プログラマーズ・ガイド、バージョン 5.4*
- *IBM WebSphere Commerce for Windows NT and Windows 2000 クィック・スタート、バージョン 5.4*
- *IBM WebSphere Commerce Studio Business Developer Edition for Windows NT and Windows 2000 インストール・ガイド、バージョン 5.4*
- *IBM WebSphere Commerce マイグレーション・ガイド、バージョン 5.4*

これらの資料の更新情報については、
`http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`
の Web アドレスを参照してください。

WebSphere Commerce の「オンライン・ヘルプ」

WebSphere Commerce の「オンライン・ヘルプ」は、 Web ブラウザーを使って表示できるオンライン情報で構成されています。また、取り出されたオンライン情報は、関連するサブジェクト・エリア PDF (Portable Document Format) 文書にも編集されています。

「オンライン・ヘルプ」については、 Internet Explorer バージョン 5.5 またはそれ以降で実行する Web ブラウザーを使用して、

`http://`*`host_name`*`/wchelp/` でアクセスできます (*`host_name`* は、使用する WebSphere Commerce マシンの名前)。

さらに、Windows では、次のようにして「スタート」メニューからヘルプにアクセスできます。

「スタート」- > 「プログラム」- > 「IBM® WebSphere Commerce」- > 「文書」

Web 上で提供される情報

サポート

ニュースグループ、FAQ、技術情報、トラブルシューティング情報、およびダウンロードなどのサポート情報を入手するには、次の Web アドレスにアクセスしてください。

Business

http://www.ibm.com/software/webservers/commerce/wc_be/support.html

Professional

http://www.ibm.com/software/webservers/commerce/wc_pe/support.html

ソフトウェア・パートナー

多くのソフトウェア・パートナーが WebSphere Commerce を強化するための製品やサービスを提供しています。これらのパートナーの情報については、http://www.ibm.com/software/webservers/commerce/community の Web アドレスにアクセスし、「Software Developers」リンクをクリックします。

レッドブック

さらに高度な技術情報を入手するには、Redbooks の Web サイトに移動してください。 http://www.ibm.com/redbooks から WebSphere Commerce を探します。

始める前に

IBM WebSphere Commerce、バージョン 5.4 アクセス・コントロール・ガイド は、WebSphere Commerce サイトへのアクセスを管理したいサイト管理者を対象としています。本書では、アクセス・コントロールの概要を説明し、組織およびユーザー、アクセス・コントロール・ポリシー、アクセス・コントロールの階層と関係、および製品に付属のデフォルト・ポリシーについても概説します。さらに、本書には、変更されたポリシーをテストするためのガイドラインや、パフォーマンスについて考慮する場合のガイドラインに加えて、既存のポリシーに対して基本的なカスタマイズを行いたいサイト管理者に役立つシナリオも用意されています。

本書は、以下のように構成されています。

第 1 章: 概要 WebSphere Commerce のアクセス・コントロール・システムの重要な機能についての概説。 WebSphere Commerce の旧リリースからの変更点についても説明しています。

第 2 章: 始めに アクセス・コントロールの概要。組織およびユーザーを定義する方法、組織およびユーザーをアクセス・コントロール・ポリシーに関連付ける方法、アクセス・コントロール・ポリシーの基本構造、管理コンソールおよび XML を使用してポリシーの重要な部分を読み取って識別する方法についても取り上げます。

第 3 章: アクセス・コントロール・ポリシーのカスタマイズ リソース・レベルのポリシーおよび役割ベースのポリシー、それらの関係、および階層についての詳細な説明。

第 4 章: アクセス・コントロールのシナリオ WebSphere Commerce に付属のデフォルトのアクセス・コントロール・ポリシーに対して基本的な変更を行う方法を示すさまざまなシナリオ。

第 5 章: 概念 組織および下部組織の構造についての概念、システムへのアクセスをユーザーに付与する方法、デフォルトの役割の説明、および関連用語。

付録 A: デフォルトのアクセス・コントロール・ポリシーの表 インストール時にシステムにロードされるすべてのデフォルトのアクセス・コントロール・ポリシーの完全なリスト。

付録 B: ポリシー情報の抽出とロード アクセス・コントロール・ポリシーのポリシー情報を XML ファイルに抽出したり、 XML ファイルのポリシー情報をアクセス・コントロール・データベースに抽出するための段階的な手順。アクセス・コントロール用の XML ファイルのリストも示されています。

前提事項

本書は、IBM WebSphere Commerce、バージョン 5.4 がサイトに正常にインストールおよび構成されていること、また読者が管理コンソール・ツールに対するサイト管理者アクセス権を持っていることを前提としています。

さらに、システムが、WebSphere Commerce を実行するためのソフトウェア要件およびハードウェア要件のすべてを満たしていることも前提としています。前提条件を含めた WebSphere Commerce のインストール方法の詳細については、 *IBM WebSphere Commerce*、*バージョン 5.4 インストール・ガイド* を参照してください。

本書の表記規則

本書では、以下のような規則を使用しています。

太文字は、フィールド名、ボタン名、または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) を示します。

モノスペース (Monospace) は、ディレクトリー・パスのほか、指示された通りに入力する必要があるテキストの例です。

イタリック は、強調のため、また独自の値に置き換えることができる変数を表すために使用されます。


は、作業を完了するために役立つ追加情報を示します。

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

2000 は、WebSphere Commerce for Windows ® 2000 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。

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。

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

400 は、 WebSphere Commerce for the IBM eServer iSeries 400 ® (以前の AS/400 ®) 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。

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

目次

第 1 章 アクセス・コントロールの概要

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、会社が期待でき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・コントロールの顕著な特徴は、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、グラフィックス設計担当者には、ストア・ページのカスタマイズを許可する一方、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、インストール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・コントロール・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・コントロール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目的としています。アクセス・コントロールは 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。

WebSphere Commerce バージョン 5.4 の新機能

WebSphere Commerce に追加されたその他の新機能と拡張のリストについては、*IBM WebSphere Commerce*、*バージョン 5.4 新着情報* を参照してください。

拡張されたユーザー・インターフェース

管理コンソールの「アクセス管理」メニューからアクセスできるポリシー編集に加えて、 WebSphere Commerce ではポリシー、およびそれに関連するアクション・グループ、アクセス・グループ、およびリソース・グループを表示するための、ビューアー・ページを追加しました。ポリシー表示ページは、管理コンソールのユーザ

ー・インターフェースにシームレスに統合され、既存のポリシー編集ページに追加されたボタンを使用してアクセスできます。

精密な制御

WebSphere Commerce Suite の旧バージョンが提供するアクセス・コントロールは、「粗い」アクセス・コントロールで、誰が、システム中のどの機能を呼び出せるかを定義できるものでした。たとえば、WebSphere Commerce Suite の旧リリースでは、 **オーダーのキャンセル** 機能を呼び出すことによって、バイヤーにオーダーのキャンセルを許可するための粗いアクセス・コントロールを使用していたかもしれません。

WebSphere Commerce の新バージョンでは、誰が、どの機能を、どのビジネス・オブジェクト・インスタンス (**リソース**とも呼ばれる) に対して呼び出すかを定義することによって、「精密」なアクセス・コントロール機能が提供されています。いくつかの例では、バイヤーにオーダーのキャンセルを許可するだけでなく、他のユーザーのオーダーではなく、自分のオーダーに対してのみ、オーダーのキャンセル機能を呼び出すようにバイヤーを制限することもできます。

精密なアクセス・コントロールが、粗いアクセス・コントロールに追加されたことによって、アクセス管理の範囲が大幅に広がり、ユーザーがサイト上で許可されるアクティビティーを、微調整することができるようになりました。

個別に管理されるコンポーネント

WebSphere Commerce Suite の旧リリースでは、精密なアクセス・コントロールがシステム・コードに組み入れられていたため、リソース・レベルでポリシーのカスタマイズを実施するためにはコードに変更を加える必要がありました。

新しい WebSphere Commerce では、アクセス・コントロール・ポリシーを XML ファイルにコード化することによって、粗いアクセス・コントロールと精密なアクセス・コントロールを外部化しました。アクセス・コントロール・ポリシーは、管理コンソールのツールに含まれるポリシー・ビューアー・インターフェースを使って、または標準テキスト・エディターを使って、変更を加えることができます。

粗いアクセス・コントロール・ポリシーと精密なアクセス・コントロール・ポリシーが製品コードとは別個に使用できるので、アクセス管理を自分の業務に適応させるには、製品コードではなく XML ファイルに含まれる情報に変更を加える必要があります。

新しいビジネス・プロセスへの適応

日々変化している現在の市場では、競争に勝ち残り、市場の変更に合わせて調整し、新しいビジネス・プロセスに適応していく上で、ビジネス環境をすばやくカスタマイズする能力が重要な役割を果たします。粗いポリシーと精密なポリシーの両方を外部化することによって、コードをカスタマイズするのではなくポリシーを変更すれば、システムへのアクセスのレベルに加える変更を迅速かつ容易に行うことができます。さらに重要なこととして、以前は契約サービス・チームにしか利用できなかった精密ポリシーを公開することによって、自分のポリシーへの基本的な変更の多くを自分の組織で実行でき、 WebSphere Commerce を Web サイトに合わせてカスタマイズする余分のコストを削減することができます。

拡張容易性

時間とともに組織が変化し成長していくにつれ、システムへのアクセスはこれらの変更にも適合していかなければなりません。新しい従業員が増えるにつれて、役割と責任分担、そのアクセスのレベルを変更し、それらの雇用者が必要な業務を実行できるようにする必要があります。それでも個々のユーザーの活動を追跡するタスクは、時間がかかりますし、困難で、実行不可能な場合さえあります。

しかし、WebSphere Commerce を使うと、メンバーシップが ID ではなく*属性* の共用セットにより定義されるアクセス・グループを使用して、暗黙的にシステムへのアクセス権限付与を管理できます。ユーザーは役割を割り当てられ、その役割に合わせてアクセスを付与されます。たとえば、ユーザー A、B、および C に**バイヤー**役割が割り当てられると、すべてのユーザーに、適切なアクセス・コントロール・ポリシーを使ってまだ出荷されていないオーダーをキャンセルする能力が付与されます。ユーザー A が組織から出た場合、ユーザー A のメンバーシップ情報は削除でき、その一方でユーザー B と C のために、バイヤー役割をオーダーのキャンセルに関連付けるアクセス・コントロール・ポリシーはそのまま残ります。

システムへのアクセス権限を暗黙的にユーザーに付与する機能は、アクティビティーの管理のための強力な手段になり、時間も労力もかなり少なくてすみます。さらに、アクセス・コントロールを管理するのに必要な労力は、システムのサイズ、組織に所属するユーザーの数、または扱うビジネス・アクティビティーのレベルではなく、変更するポリシーの数に左右されます。システムで実行するアクセス・コントロール・ポリシーは、小規模な組織でも、大規模な組織でも適用できます。その結果、WebSphere Commerce で実行するアクセス・コントロール・ポリシーの拡張容易性によって、操作の構造や効率性に悪影響を与えることなく、会社が変化し成長し続けることができます。

アクセス・コントロールの意味

アクセス・コントロールによって、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。	バイヤー組織は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からのユーザーだけが、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、変更はできません。

次の章では、組織とユーザーの作成方法、およびアクセス・コントロール・ポリシーの詳細を説明します。

第 2 章 始めに

前の章では、アクセス・コントロールが 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・コントロール・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・コントロール・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・コントロールの理解
- アクセス・コントロールを使用開始する方法
- ポリシーの詳細: 例

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。

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、ビジネスとの間に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。企業間取り引きサイトまたは企業対消費者取り引き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。すでに組織とユーザーをセットアップしてある場合、次のアクセス・コントロールのセクションに進むことができます。そうでない場合は、このセクションをガイドラインとして、この先の計画を立ててください。

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

IBM WebSphere Commerce 基本、バージョン 5.4 を参照することもお勧めします。

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する組織です。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。ほとんどの場合、サイト管理者はセラー組織に所属します。

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、および組織の名前を含めます。
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。 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、ストア管理者、ストア開発者、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、第 5 章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。

上記で概説したすべてのステップは、WebSphere Commerce が提供するツールの 1 つ、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、存在できるセラー組織は 1 つだけです。

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、個々のバイヤーをサイトに登録します。) サイトで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、企業間取り引きサイトだけです。
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、ストア管理者、ストア開発者、バイヤーなどが含まれます。
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。

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、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・コントロールの理解

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・コントロール* 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・コントロール・ポリシーとその基本構造を見ていきます。

注: WebSphere Commerce Professional Edition には、ルート組織、デフォルト組織、およびセラー組織の 3 つがあるだけで、これらの組織はすでに定義済みです。

アクセス・コントロール・ポリシーとは

アクセス・コントロール・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までが含まれます。

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。 1 つ以上のアクセス・コントロール・ポリシーで、その責任を実行する権限を付与されない限り、ユーザーはどのサイトの機能にもアクセスできません。

アクセス・コントロール・ポリシーの作動方法

アクセス・コントロール・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、同じ部門、スキル・セット、または役割など、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、契約や関連するコマンドのセットなどのビジネス・オブジェク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、契約を作成するユーザーだけが、その契約を変更することを許可される場合があります。

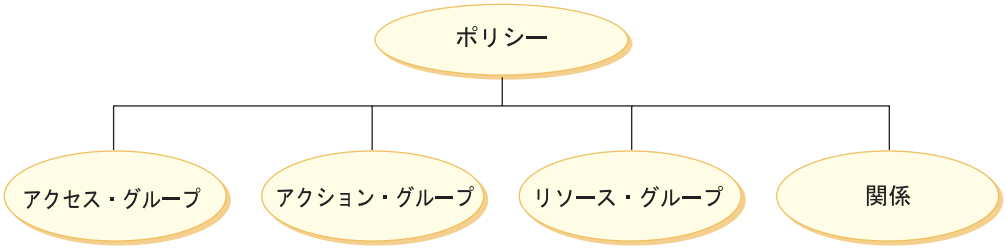

図 1 アクセス・コントロール・ポリシーの 4 つの部分

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、第 5 章「アクセス・コントロールの概念」を参照してください。

ポリシー・タイプ

アクセス・コントロール・ポリシーは、サイト・レベル・ポリシー、テンプレート・ポリシー、および組織レベル・ポリシーの 3 つのカテゴリー、つまりポリシー・タイプ に分けられます。ポリシー・タイプは、アクセス・コントロール・ポリシーに加えられる変更に影響を受ける人、およびその変更が行われる場所を判別します。

WebSphere Commerce は、インストール時にシステムにロードされる、 200 以上のデフォルト・アクセス・コントロール・ポリシーをサイト管理者に提供します。デフォルト・ポリシーには、サイト・レベル・ポリシーとテンプレート・ポリシーの両方が含まれます。

サイト・レベル・ポリシー

サイト・レベル・ポリシーは、サイト全体およびそのメンバー組織に適用するポリシーです。通常は、サイト・レベル・ポリシーは、すべての組織に影響する統括ア

クティビティー、つまりサイト登録やメンバーシップ機能などに使用されます。サイト・レベル・ポリシーは、異なる組織にまたがるプロセスを標準化するのに使用されます。たとえば、サイト管理者は、すべての組織がオーダーを扱う際に、承認プロセスに従うように求める場合があります。

サイト・レベル・ポリシーを、個々の組織が変更することはできません。

テンプレート・ポリシー

テンプレート・ポリシーは、サイト・レベルで定義されるポリシーですが、個々の組織で変更することが可能です。テンプレート・ポリシーは、個々の組織が必要に応じて変更できる、デフォルトつまり「ひな型」ポリシーと考えることができます。テンプレート・ポリシーは、組織の必要に従って、WebSphere Commerce 機能へのアクセスを管理するために使用されます。たとえば、オークションの管理、RFQ 要求の処理、および組織レベルで発生する、その他の取引上または管理上のアクティビティーがあります。

サイト管理者は、いつでもテンプレート・ポリシーを変更することができます。テンプレート・ポリシーがサイト管理者によってルート・レベルで変更されると、その変更はすべての組織に適用されます。たとえば、サイト管理者は、すべてのバイヤー組織がそのユーザーを登録するように要求するかもしれません。図 2 を参照してください。

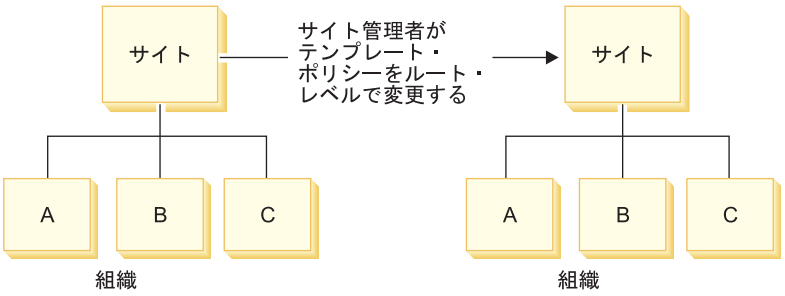

図 2 サイト管理者がルート・レベルでテンプレート・ポリシーを変更すると、その変更はすべての組織に適用される

一方、サイト管理者がある組織のテンプレート・ポリシーに変更を加えると、その変更はその組織だけに適用されます。図 3 を参照してください。

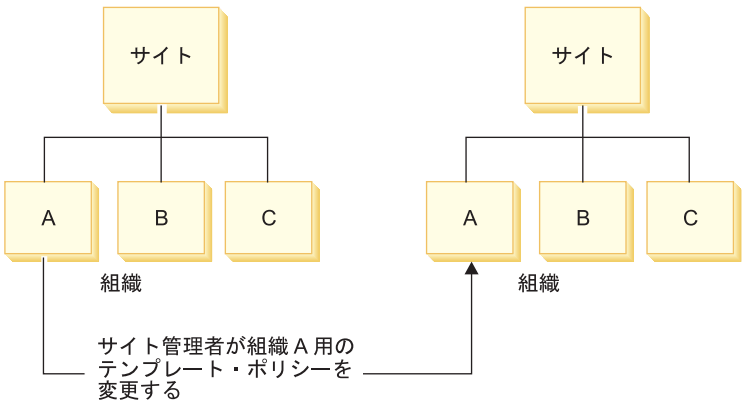

図 3 サイト管理者が組織 A のテンプレート・ポリシーを変更すると、変更は組織 A だけに適用される

たとえば、サイト管理者は、オーダーをキャンセルする権限を、1 つの組織だけに制限したいと考えるかもしれません。

組織レベル・ポリシー

サイト管理者がテンプレート・ポリシーを変更するか、または個々の組織に新しいポリシーを作成すると、そのポリシーはその特定の組織だけに適用されるので、ポリシーは*組織レベル・ポリシー*と呼ばれるようになります。そのような組織レベル・ポリシーは、元のテンプレート・ポリシーにさらに変更が加えられても、影響されることはありません。

役割ベースのポリシーおよびリソース・レベル・ポリシー

アクセス・コントロール・ポリシーは、さらに、コマンド・レベルおよびリソース・レベル・ポリシーに分類することができます。コマンド・レベル・ポリシーは通常、特定の役割がコマンドのグループを実行することを許可し、リソース・レベル・ポリシーは特定のリソースへのアクセスを制御するのに使用されます。コマンド・レベル・ポリシーは、通常、役割 (ジョブ機能) に対応し、*役割ベースのポリシー* とも呼ばれます。

役割ベースのポリシーとリソース・レベル・ポリシーの違いを理解することは、アクセス・ポリシー自体がどのように作動するか、および既存のポリシーのカスタマイズ、または新規ポリシーの作成に何が必要かを理解するために不可欠です。次のセクションでは、デフォルトのアクセス・コントロール・ポリシーの 1 つを詳しく学びながら、その違いを理解していきます。

役割ベースのポリシーとリソース・レベル・ポリシーの違いに関する詳細は、第 4 章を参照してください。

アクセス・コントロールの使用開始方法

場合によっては、何もする必要はありません。これは、WebSphere Commerce のデフォルト・ポリシーが、システム内の典型的なユーザーに基づくアクセス・コントロールの基本構造と、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るためです。ポリシーは、メンバーシップ、オーダー作成と処理、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。次のセクションでは、デフォルト・ポリシーの詳細を調べます。

ポリシーの詳細: 例

これまで、アクセス・コントロール・ポリシーの基本構造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

最初の例では、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・コントロール・ポリシーに変更を加えたり、新しいアクセス・コントロール・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、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。

管理コンソールでポリシーを調べる

1. 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. 「View (表示)」ドロップダウン・メニューが自分の組織に設定されていることを確認します。
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、**「First (最初)」**、**「前へ」**、**「次へ」** および **「Last (最終)」** 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、**「Show Action Group (アクション・グループの表示)」**をクリックします。
2. 「Action Group (アクション・グループ)」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、**「Show Actions (アクションの表示)」**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、**「Show Actions (アクションの表示)」**をクリックすることによって、「ポリシー」ページから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. ポリシーのページに戻るには、いずれかのアクションを選択し、**「Show Policies (ポリシーの表示)」**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**「Show Member Group (メンバー・グループの表示)」**をクリックして、このポリシーの適用先のメンバー (アクセス・グループ) を表示します。
6. メンバー (アクセス)・グループ名の注釈を作成します。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

   これらの役割の 1 つに割り当てられるユーザーがいれば、そのユーザーは AuctionAdministratorsForOrg アクセス・グループの一部です。
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。

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

    ポリシーを見つけます。
11. ポリシーを選択し、**「Show Resources (リソースの表示)」**をクリックします。「Resources (リソース)」ページに、次のリソースのリストが表示されます。
    - com.ibm.commerce.common.objects.StoreEntity
    - com.ibm.commerce.negotiation.objects.Auction
    - com.ibm.commerce.negotiation.objects.AuctionStyle
    - com.ibm.commerce.negotiation.objects.ControlRule

    これらは、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、リソースはストア・エンティティー、オークション、オークション・スタイル、および入札ルール・オブジェクトです。**「Show Resource Group (リソース・グループの表示)」**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、「ポリシー」ページから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、

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

    を見つけます。
13. ポリシーを選択し、**「変更」**をクリックします。「Change Policy (ポリシーの変更)」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するということが分かっています。これは、**「Show Member Group (メンバー・グループの表示)」**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・グループが役割 **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**を含むことを確認しました。集合的に、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、リソースにはオークションが行われるストア、オークション、そのオークションが使用するオークション・スタイルまたは入札ルール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**「Show Actions (アクションの表示)」**および**「Show Resources (リソースの表示)」**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管理者が、オークションの変更、撤回およびクローズ、オークションが作成されたストアによって部分的にオークションが定義される位置、さらにそのオークション・スタイルと入札ルールなど、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、 AuctionAdministrator で始まります。 ForOrg は、ポリシーが組織に適用されることを示します。 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。デフォルト・ポリシーの命名規則の詳細については、第 3 章を参照してください。

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・コントロール・ポリシーは、インストール時にシステムにロードされた XML ファイルに保管されています。管理コンソールでポリシーを表示する場合、 XML ファイル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ていることになります。

ほとんどの場合、ポリシーを管理するには管理コンソールのユーザー・インターフェースを使用します。しかし、ポリシーを XML で表示したい場合や、高度な変更を加えたい場合には、 XML ファイルのポリシーは次のようになります。

```
!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="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。サイト・レベル、テンプレート、組織など

デフォルトのアクセス・コントロール・ポリシーすべてを含むファイルの名前は、defaultAccessControlPolicies.xml で、次のディレクトリーにあります。

X:¥wcs_directory¥xml¥policies¥xml

注: デフォルトの各アクセス・コントロール・ファイルの記述は、同じディレクトリーにある default_AccessControlPolicies_en_US.xml ファイルにあります。defaultAccessControlPolicies.xml にある、デフォルトのアクセス・コントロール・ポリシーに変更を加える場合、defaultAccessControlPolicies_en_US.xml の対応する記述も同様に更新する必要があります。しかし、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・コントロール・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) がリソースで実行できる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. 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、AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource であることが分かります。
2. ポリシーに関連したアクション・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 A 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。付録 A 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、特定のアクション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。

次の章では、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 3 章 デフォルトのアクセス・コントロール・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・コントロール・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。

この章では、WebSphere Commerce に含まれるデフォルトのアクセス・コントロール・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。次に、デフォルト・ポリシーに加えられる可能性のある、共通度の高い変更をいくつか例示する、一連のシナリオを提供します。シナリオはコンポーネントによって配置されており、加えるべき変更を説明する簡潔な概説、続いてタスクを完了するための手順ごとの簡単な指示のリストが含まれます。シナリオは単純な変更からより複雑な変更まで広範囲に適用することができ、ご使用のシステムで同様のタイプのポリシー変更を行う場合にガイドラインとして使用することができます。シナリオで説明されるすべてのポリシーは、付録 A にリストされています。この付録にはデフォルトのアクセス・コントロール・ポリシーの完全なリストが掲載されています。

注: 分からない用語や概念が出てきたら、第 4 章「アクセス・コントロールの概念」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

前の章では、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「ストア管理者」のアクセス・グループは `StoreAdministrators` 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マンド (アクション) を定義するポリシー。役割ベースのポリシーは、特定のコマンドを実行できる人を定義するため、コマンド・レベル・ポリシーとも呼ばれます。

– 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、実行時にビューを表示するコマンドです。たとえば、StoreListView はシステム内のストアのリストを持つ Web ページを表示します。

いくつかの役割は、役割ベースのポリシーを持っているだけで、どのリソース・レベル・ポリシーでも使用されていません。この状態は、役割に権限が付与されるアクションを特定のリソースに制限する必要がない場合、またはアクションの性質上、そこで動作するリソースがない場合に発生します。

たとえば、役割ベースのポリシー SiteAdministratorsCanDoEverything は、サイト管理者が実行できるアクションを定義します。このポリシーにより、サイト管理者はすべてのコマンドを実行できます。サイト管理者がアクションを実行するための特定のリソースを定義する、リソース・レベル・ポリシーはありません。

リソース・レベル・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特定のアクションを定義するポリシーで、役割がポリシーのアクセス・グループを定義するのに使用される場合、役割ベースのポリシーに直接結び付けられます。図 4 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。この図は、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の例です。

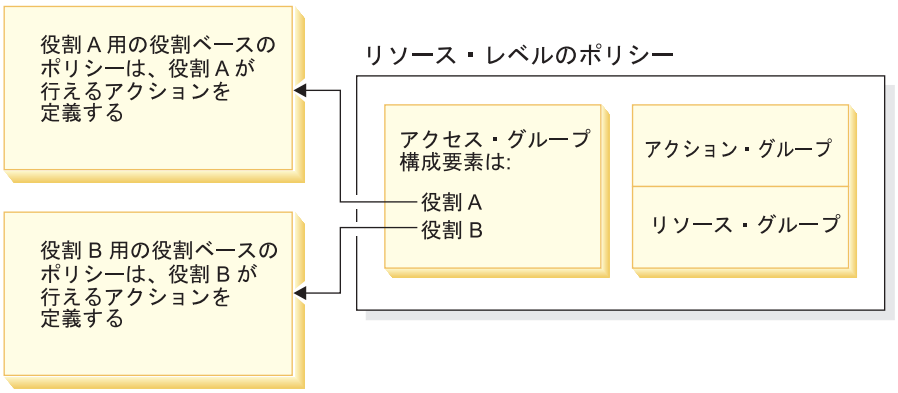

図 4: リソース・レベル・ポリシーと、それに関連した役割ベースのポリシー

図 5 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です。役割 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。

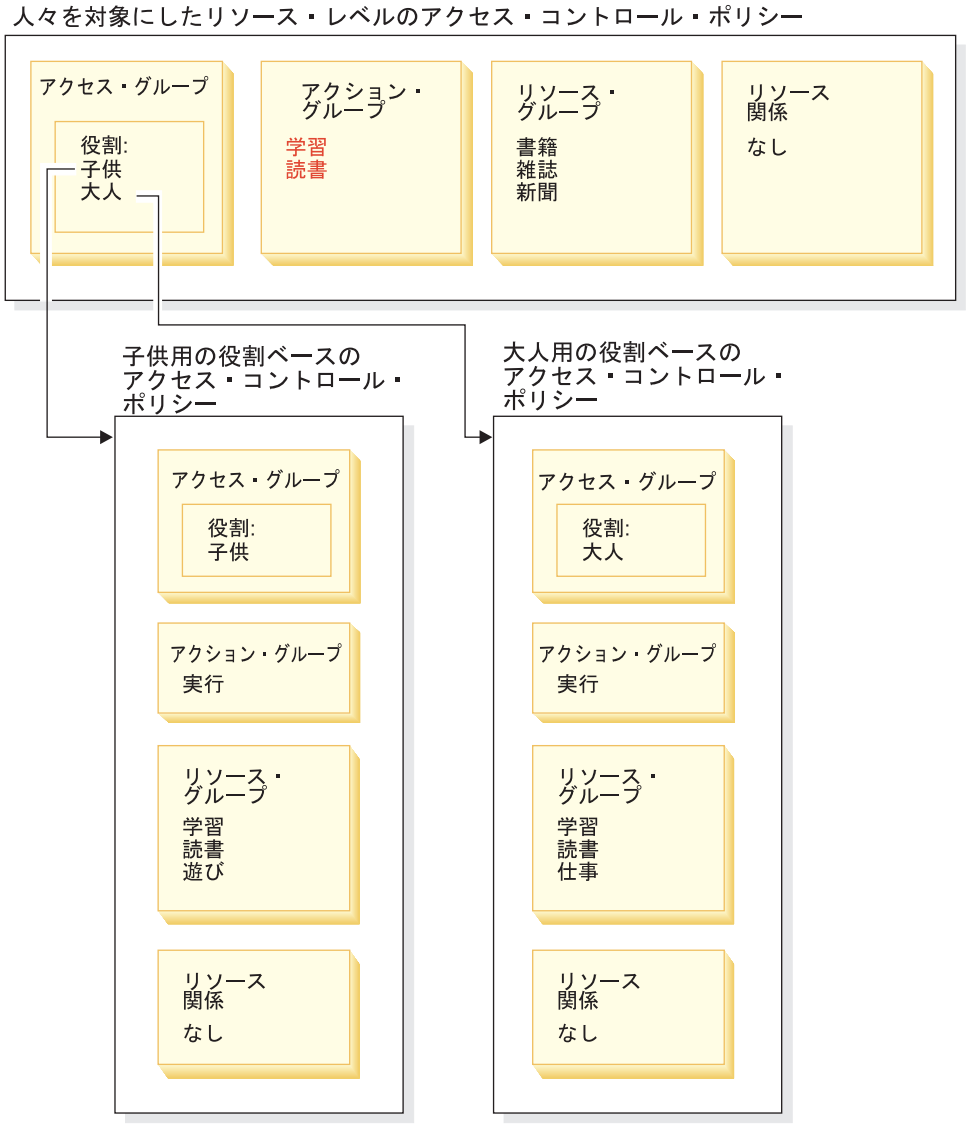

図 5: リソース・レベル・ポリシーと、それに影響する役割ベースのポリシー

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、実行 (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、実行可能なコマンドまたは表示アクションがあります。

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** をリストしています。 **子供** のポリシーはリストしていません。 **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。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ない場合、そのポリシーには役割ベースのポリシーとの関連がありません。

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。

しかし、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、関連した役割ベースのポリシーからアクションを削除する必要はありません。役割ベースのポリシーは、役割に、現在リソース・レベル・ポリシーで指定されていないアクションを実行する権限を与えることができます。この状態では、アクションは役割に対して使用可能と見なされますが、現時点では権限がありません。

ポリシー階層について

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。

表 1 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。

リソース・レベルのポリシーに以下の変更を行う場合 :	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には、以下の変更も行う必要があります :
アクションをポリシーのアクション・グループに追加する。	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・グループから除去する。	追加の変更は必要ありません。
異なるアクション・グループを使用する。	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・グループに追加する。	役割ベースのポリシーのリソース・グループが、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。
役割をポリシーのアクセス・グループから除去する。	追加の変更は必要ありません。
異なるアクセス・グループを使用する。	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する。	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。
ポリシーを削除する。	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。

表 1: 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。

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、SalesManagersExecuteSalesManagerViews となります。

ビュー用の役割ベースのポリシーでは、アクション・グループにその役割を持つユーザーが実行できるビューのリストが含まれます。

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、
AuctionAdministorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource
となります。

databean リソース (DataBean には、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、第 4 章で役割についてのトピック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、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」に選択した値に応じて、「ポリシー」ページにはサイト・レベルのポリシーまたは特定の組織に特定のポリシーのいずれかが表示されます。
  - 「ビュー」フィールドに**「ルートの組織」**を選択した場合、サイト・レベルのポリシーおよびテンプレート・ポリシーのマスター・バージョンが表示されます。
  - 「ビュー」フィールドに組織の名前を設定した場合、その組織のためだけに指定されたポリシー、および組織が変更できるテンプレート・ポリシーが表示されます。
- 役割ベースのポリシーでは、アクション・グループに単一のアクション execute (実行) だけが含まれます。リソース・グループには、実行可能なコマンドまたは表示アクションが含まれています。そのため、役割ベースのポリシーからアクションを削除するには、そのリソース・グループを更新しなければなりません。
- 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、変更したデフォルト・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用の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。

ポリシーの変更後に

アクセス・コントロール・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。

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、最後のステップとして変更を抽出してそれを XML ファイルに適用します。このステップが必要なのは、管理コンソールからの変更が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。ポリシー、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、および関係を定義する XML ファイルは、自動的には更新されません。

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・コントロール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。
- WebSphere Commerce の 2 番目のインスタンスで同じアクセス・コントロール・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。

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、指定のリソース上で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、オークション・シナリオ 1 をインプリメントして、オークション管理者が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る場合、その試行は失敗するはずです。

ポリシーの変更を抽出して XML ファイルに適用する

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するようにします。付録 B では、ポリシー、アクセス・グループ、リソース・グループ、およびアクション・グループ定義に関連した異なる XML ファイルについて説明します。さらに、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も説明します。

第 4 章 カスタマイズのシナリオ

以下に示すカスタマイズのシナリオによって、アクセス・コントロール・ポリシーについて学習した事柄を適用してデフォルト・ポリシーにさまざまな基本変更を行うことができます。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 1.

ビジネス領域	開始ページ
オークション	26 ページの『オークション・シナリオ 1: オークション管理者がオークション入札をクローズする権限を除去する』
契約	31 ページの『契約シナリオ 1: 契約管理者が契約に付加項目を追加または削除する権限を除去する』
RFQ	34 ページの『RFQ シナリオ 1: RFQ 管理者が RFQ を管理できるようにする』
オーダー	35 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	42 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	47 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	52 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	55 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	57 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』

表 2: シナリオの目次

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下記の表を参照してください。

表 2.

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	49
ポリシーのアクション・グループを変更する	53,55
ポリシーのリソース関係を変更する	38,52
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	29,35,38,43,47,50
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	40,44
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	45,53
新規のリソース・レベルのポリシーを作成する	33,34,53
新規の役割ベースのポリシーを作成する	44,57
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	44,57
ポリシーを削除する	28,28,43
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	3,31

表 3: 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

オークション・シナリオ 1: オークション管理者が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が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. 付録を使用して、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検索します。
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 A でオークションの項を調べて、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、AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource です。
2. 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、**「ルートの組織」**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 — 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、「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、**「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. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

オークション・シナリオ 2: オークション管理者が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管理者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付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 A を使用して、オークション管理者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付けます。
- 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 A でオークションの項を調べて、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、

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`

   です。
2. 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、**「ルートの組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. ポリシーのリストから、**「AuctionAdministratorsForOrgExecuteAdmin RetractBidCommandsOnAuctionResource」** を選択します。
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. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

オークション・シナリオ 3: 1 つの組織内でオークション管理者が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管理者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、サイト管理者として、特定の組織についてこのポリシーを変更したいことがあります。この変更を行うには、この組織についてこのアクションを許可するテンプレート・ポリシーを削除しなければなりません。

注: WebSphere Commerce Professional Edition では、ルートの組織、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。

ポリシーを削除した後、その組織のオークション管理者は入札を撤回できなくなります。他の組織のオークション管理者は、この変更の影響を受けません。

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 A を使用して、オークション入札の撤回を許可するリソース・レベルのポリシーを見付けます。

- 組織のポリシーのリストから、そのポリシーを見付けます。
- 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 A でオークションの項を調べて、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、

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`

   です。
2. 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」では、ポリシーを削除したい組織を選択します。 **「ルートの組織」**ではなく特定の組織を選択した場合、ポリシーの変更はサイト内のすべての組織にではなく、その組織にだけ適用されます。
4. ポリシーのリストから、**「AuctionAdministratorsForOrgExecuteAdmin RetractBidCommandsOnAuctionResource」** を選択します。
5. **「削除」**をクリックします。

アクセス・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

オークション・シナリオ 4: 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 A を使用して、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付けます。
- 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 A を使用して、バイヤー (購買サイド) の役割ベースのポリシーを見付けます。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 A でオークションの項を調べて、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. 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、**「ルートの組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. ポリシーのリストから、**「RegisteredApprovedUsersExecuteBidCreate CommandsOnAuctionResource」** 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付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を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、**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 A で役割ベースのポリシーに関する項を参照して、バイヤー (購買サイド) の役割ベースのポリシーを見付けます。そのポリシーは以下のとおりです。

   Buyers(buy-side)ExecuteBuyers(buyside)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、**「ルートの組織」**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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

契約シナリオ 1: 契約管理者が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、ストアの契約管理者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、この権限を契約管理者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変更します。契約に付加項目を追加または削除する契約管理者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 A を使用して、契約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検索します。
- 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 A で契約の項を調べて、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、

   ```
   ContractAdministratorsForOrgExecuteContractManageCommandsOnContractResource
   ```

   です。
2. 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、**「ルートの組織」**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 — `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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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・コントロール・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。

- deploy contract (契約のデプロイ) 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 A を使用して、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検索します。
- 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 A で契約の項を調べて、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付けます。ポリシーは、ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource です。
2. 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、**「ルートの組織」**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 — 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、

   ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource

   を指定します。
3. 「表示名」には、ポリシーに関する簡略説明をローカル言語で指定します。

4. 「説明」には、ポリシーの機能に関する詳細説明をローカル言語で指定します。
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、**「Template Policy (テンプレート・ポリシー)」**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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

RFQ シナリオ 1: RFQ 管理者が RFQ を管理できるようにする

注: WebSphere Commerce Professional Edition では、RFQ 機能は使用できません。

デフォルトでは、RFQ バイヤーが自分の RFQ を管理できます。場合によっては、RFQ 管理者に管理権限を付与して、管理者 RFQ と同様に管理してもらうこともできます。

この変更を加えるには、以下のようにしなければなりません。

- 付録 A を使用して、 RFQ バイヤーが自分の RFQ を管理することを認可しているリソース・レベル・ポリシーを検索する。
- このポリシーのアクション・グループとリソース・グループの名前を記録する。
- RFQ バイヤーが自分の RFQ を管理することを認可しているポリシーのアクション・グループとリソース・グループの名前を指定して、 `RFQ administrator` アクセス・グループの新しいリソース・レベル・ポリシーを定義する。 RFQ 管理者がすべての RFQ を管理できるようにするには、リソース関係の指定を省略します。

実行するステップ

新しいポリシーの定義中に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 A 中の『RFQ』を検索して、 RFQ バイヤーが自分の RFQ を管理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 `RFQBuyersManageRFQResourcesTheyOwn` です。
2. 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、**「ルートの組織」**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 RFQManage 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 RFQResourceGroup 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ときに使用します。

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」で、RFQAdministratorsManageRFQResources を指定します。
3. 「表示名」で、ポリシーの簡略説明をご使用の言語で指定します。
4. 「説明」で、ポリシーの実行内容に関する詳細説明をご使用の言語で指定します。
5. 「ユーザー・グループ」で、**「検索」**をクリックして、**「RFQAdministrators」**を選択します。
6. 「リソース・グループ」で、**「RFQResourceGroup」**を選択します。
7. 「アクション・グループ」で、**「RFQManage」**を選択します。
8. 「ポリシーのタイプ」で、**「Template Policy (テンプレート・ポリシー)」**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。
9. **「OK」**をクリックします。

アクセス・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

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。WebSphere Commerce では、通常これらの従業員は **バイヤー** の役割を割り当てられます。

購買組織内の **バイヤー** の役割のメンバーに、オーダーの作成を限定するには、以下のようにします。

- 付録 A を使用して、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・ポリシーを検索する。
- 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する。
- ポリシーの名前、表示名、および説明を更新する。

- オーダー作成用のコマンドを識別する。
- 付録 A を使用して、バイヤー (購買サイド) の役割ベースのポリシーを検索する。このポリシーは、バイヤー (購買サイド) 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む。

実行するステップ

リソース・レベル・ポリシーの識別

1. 付録 A の『オーダー』を検索して、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. 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、**「ルートの組織」**を選択して、サイト・レベル・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・グループの変更

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
```

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の識別

1. 付録 A 中の『役割ベースのポリシー』を検索して、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(buyside)ExecuteBuyers(buyside)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、**「ルートの組織」**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 Buyers(buyside)CommandsResourceGroup の名前を記録します。 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中のリソース・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(buyside)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
```

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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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 A を使用して、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・ポリシーを検索する。
- 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する。
- 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する。
- ポリシーの名前、表示名、および説明を更新する。
- オーダー変更用のコマンドを識別する。
- 付録 A を使用して、バイヤー管理者の役割ベースのポリシーを検索する。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む。

実行するステップ

リソース・レベル・ポリシーの識別

1. 付録 A の『オーダー』を検索して、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. 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、**「ルートの組織」**を選択して、サイト・レベル・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・グループの変更

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、**「Buyer Administrators (バイヤー管理者)」**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
```

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:

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

b. 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 A 中の『役割ベースのポリシー』を検索して、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、**「ルートの組織」**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中のリソース・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
```

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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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・ポリシー中でこのアクセス・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 A を使用して、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しているリソース・レベル・ポリシーを検索する。
- 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する。
- 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する。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` を作成する。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する。
  - 新しいアクセス・グループ `RMAApprovers`
  - 既存のポリシー中のアクション・グループ
  - 既存のポリシー中のリソース・グループ

実行するステップ

新しいポリシーの定義中に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 A 中の『オーダー』を検索して、 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. 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、**「ルートの組織」**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 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. アクション・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・グループ中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・グループ中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」で、RMAApprovers を指定します。
3. 「説明」で、アクセス・グループの説明を指定します。
4. **「次へ」**をクリックして、新しいアクセス・グループに関する「基準」ページを表示します。
5. **「Criteria based on organizations and roles (組織および役割別の基準)」**をクリックします。

6. 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)**
7. **「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」で、ポリシーの簡略説明をご使用の言語で指定します。
5. 「説明」で、ポリシーの実行内容に関する詳細説明をご使用の言語で指定します。
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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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・コントロール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、ルートの組織、デフォルトの組織およびセラー組織の 3 つだけ組織があります。

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中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 A を使用して、ユーザーの自己登録を許可しているリソース・レベル・ポリシーを検索する。
- ポリシーを削除する。

実行するステップ

ポリシーの削除

1. 付録 A 中の『メンバーシップ』を検索して、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. 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、**「ルートの組織」**を選択して、サイト・レベル・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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

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 A を使用して、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・ポリシーを検索する。
- そのポリシーのアクセス・グループを変更する。

  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 A 中の『メンバーシップ』を検索して、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. 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、**「ルートの組織」**を選択して、サイト・レベル・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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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する。
- 既存のリソース・レベル・ポリシーを変更して、新しい役割を使用する。

このシナリオでは、以下を実行します。

- Member Registrar という新しい役割を定義する。
- 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む。
- 付録 A を使用して、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・ポリシーを検索する。
- アクション・グループ中のアクションの名前を記録する。このアクションを指定して新しいリソース・グループを作成し、新しい役割の役割ベースのポリシー中で使用しなければなりません。アクションの役割ベースのポリシー中で、アクション・グループには実行アクションが 1 つしか含まれないことに注意してください。リソース・グループには、実行できる複数のアクション (コマンド) が含まれます。
- MemberRegistrationCommands 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む。メンバー登録者の役割の役割ベース・ポリシー中で、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する。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 に変更する。

実行するステップ

新しい役割の定義

1. 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、「Member Registrar (メンバー登録者)」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」で、「MemberRegistrars」を指定します。
4. 「説明」で、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. **「次へ」**をクリックして、新しいアクセス・グループに関する「基準」ページを表示します。
6. **「組織および役割別」**をクリックします。
7. 「役割」リストから、**「Member Registrar (メンバー登録者)」**を選択します。
8. **「For Organization (組織の)」**をクリックして、この役割がユーザーの組織内になければならないことを指定します。
9. **「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 A の『メンバーシップ』のセクションで、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探します。そのポリシーは、MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource 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、**「ルートの組織」**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. **「次へ」**をクリックします。
7. **「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。
8. 「使用可能なリソース」リストから、**「com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd」**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。

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。

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

1. ポリシーのリストから、「MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource」を選択します。
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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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、登録されている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・レベルのポリシーとともに、関連する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 A 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・ポリシーを探します。

- 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。
- クーポンを使用するためのコマンドを識別します。
- 付録 A 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探します。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 A の『クーポン』のセクションを参照して、変更すべきリソース・レベル・ポリシーを識別します。そのポリシーは、

   ```
   RegisteredApprovedUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
   ```

   です。
2. 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、**「ルートの組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. ポリシーのリストから、**「RegisteredApprovedUsersExecuteCouponRedemptionCommandsOnCouponWalletResource」**を選択します。
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 A の『役割ベースのポリシー』のセクションを参照して、バイヤー (購買サイド) の役割ベースのポリシーを探します。そのポリシーは以下のものです。

   `Buyers(buy-side)ExecuteBuyers(buyside)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、**「ルートの組織」**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(buyside)CommandsResourceGroup` 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・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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

クーポン・シナリオ 2: クーポン管理者とストア管理者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。しかし、この権限をストア管理者に付与したい場合もあります。

アクセス・コントロール・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、ストア管理者役割を追加できます。
- ストア管理者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、ストア管理者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 A 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・ポリシーを探します。
- ポリシーのアクセス・グループを変更して、 **ストア管理者**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 A を参照して、**ストア管理者**の役割ベース・ポリシーを探します。このポリシーは、**ストア管理者**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 A の『オークション』のセクションを参照して、変更すべきリソース・レベル・ポリシーを識別します。そのポリシーは、`CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource` です。
2. 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、**「ルートの組織」**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 —`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. アクション・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、**「ストア管理者」**を選択します。
6. **「For Organization (組織の)」**をクリックして、この役割がユーザーの組織内に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。ストア管理者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。

ストア管理者の役割ベース・ポリシーを識別する

1. 付録 A の『役割ベースのポリシー』のセクションを参照して、ストア管理者の役割ベースのポリシーを探します。そのポリシーは、StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup 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、**「ルートの組織」**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 —StoreAdministratorsCmdResourceGroup 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. **「StoreAdministratorsCmdResourceGroup」**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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。

2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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する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 A 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・ポリシーを探します。
- 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 A の『調達』のセクションを参照して、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・ポリシーを探します。そのポリシーは、`ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource` です。
2. 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、**「ルートの組織」**を選択して、サイト・レベル・ポリシーを表示します。
4. ポリシーのリストから、**「ProcurementShoppingCartManagersExecute ProcurementShoppingCartManageOnOrderResource」**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. 「関係」では、**「sameOrganizationalEntityAsCreator」**を選択します。
7. **「OK」**をクリックします。

アクセス・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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する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 A 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・ポリシーを探します。
- 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 A の『調達』のセクションを参照して、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・ポリシーを探します。そのポリシーは、`ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource` です。
2. 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」に、**「ルートの組織」**をクリックして、サイト・レベルの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、「ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommandsOnOrderResource」 を指定します。
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、**「Template Policy (テンプレート・ポリシー)」**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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

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 A 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・ポリシーを探します。
- 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 A の『調達』のセクションを参照して、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・ポリシーを探します。そのポリシーは、`FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommands OnFulfillmentResource` です。
2. 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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

在庫シナリオ 2: ロジスティクス・マネージャーとオペレーション・マネージャー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、ロジスティクス・マネージャー、オペレーション・マネージャー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 A 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・ポリシーを探します。
- `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 A の『調達』のセクションを参照して、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・ポリシーを探します。そのポリシーは、`FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommandsOnFulfillmentResource` です。
2. 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・コントロール・ポリシー・レジストリーに変更を適用して更新する

1. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「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。

- 新しい役割を作成して、その役割に関して、新しいアクセス・グループ、新しいリソース・グループ、および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。
- Auditor という新しい役割を定義します。
- auditor (監査者) 役割を含んだ Auditors という名前の新しいアクセス・グループを定義します。
- 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 A 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・ポリシーを探します。
- そのアクション・グループのアクション名を記録します。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. 管理コンソールから、**「アクセス管理」>「役割」**を選択します。
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入力します。
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 (Based on organizations and roles)」**をクリックします。
7. 「役割」リストから、**「Auditor」**を選択します。
8. **「追加」**をクリックします。
9. **「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 A で『ビジネス・インテリジェンス』のセクションを参照して、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探します。そのポリシーは `IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport CommandsOnStoreEntityResource` です。
2. 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、**「ルートの組織」**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 `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. **「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。
8. 「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。
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・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. **「For Organization (組織)」**をクリックして、ユーザーの組織に含める必要のある役割を指定します。
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. **「構成」>「レジストリー」**をクリックします。
2. レジストリーのリストから、**「Access Control Policies Registry (アクセス・コントロール・ポリシー・レジストリー)」**を選択します。
3. **「更新」**をクリックします。

第 5 章 与信 (アクセス・コントロール)

WebSphere Commerce は、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して与信を表示します。このセクションでは、WebSphere Commerce の与信つまりアクセス・コントロールのいくつかの点の詳細を説明します。

WebSphere Commerce での与信つまりアクセス・コントロールは、アクセス・コントロール・ポリシーを使用して行われます。アクセス・コントロール・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・コントロール・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・コントロール・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・コントロール要件のほとんどを解決するように設計されています。 WebSphere Commerce のアクセス・コントロール・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。

組織的な階層

WebSphere Commerce メンバー・サブシステム内のユーザーまたは組織エンティティーは、階層的に編成されています。一般に、この階層は普通の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。組織管理者は、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、各セラー組織内に 1 つ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。以下の図は、企業間取り引き e-commerce サイトの組織階層を示しています。

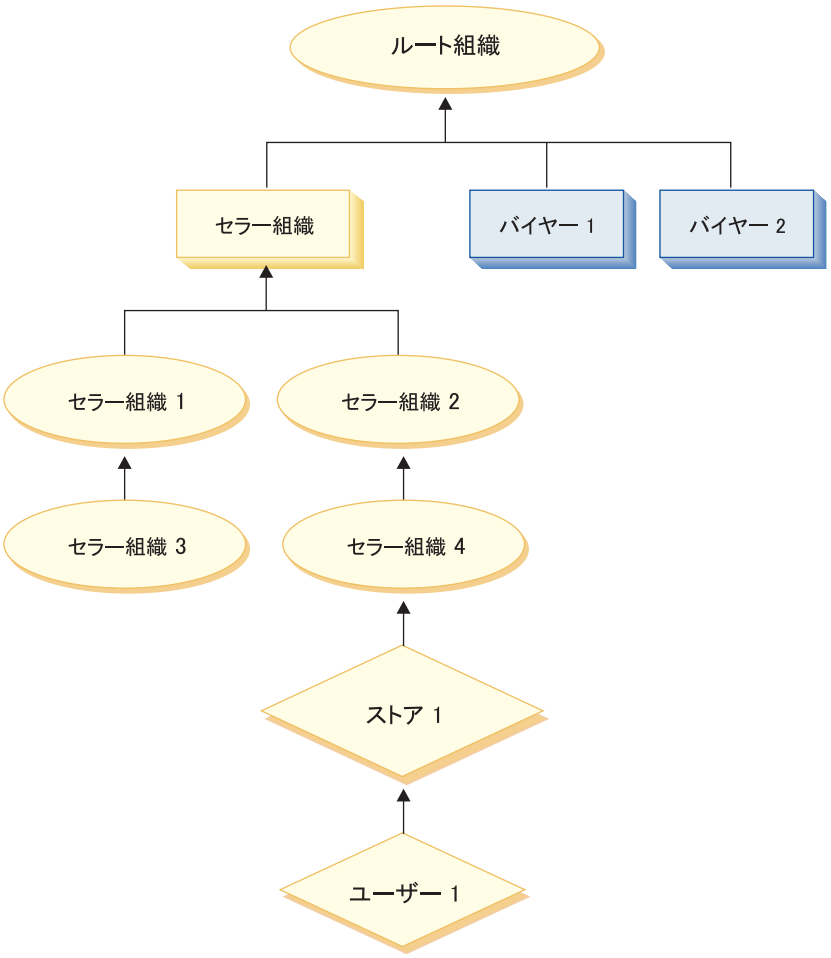

図 1. 企業間取り引きサイトの組織階層

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* 役割を持つユーザーが、ルート組織を管理する責任者です。サイト管理者は WebSphere Commerce と関連するソフトウェアおよびハードウェアをインストールし、構成し、保守します。この役割では、通常、アクセスおよび与信を制御 (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、ストア管理者と他のすべての管理者、さらにその管理者がアクセスする組織を設計できます。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。

WebSphere Commerce サイトには、1 つのセラー組織があります。企業間取り引きサイトでは、1 つ以上のバイヤー組織も入っています。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・コントロール・ポリシーと、そのストアから購入する各組織のアクセス・コントロール・ポリシーの両方を定義します。ビジネス対顧客のサイトでは、バイヤー組織はありません。ビジネス対顧客の顧客は、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 (バイヤー)

企業間取り引きサイトでは、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・コントロール・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・コントロール・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を異なる役割に割り当てます。

サイト管理者は、必要な場合、バイヤー組織のアクセス・コントロール・ポリシーを変更および管理できることに注意してください。

組織 (セラー)

企業間取り引きおよび企業対顧客取り引きの両方で、サイト管理者は 1 つの最上位のセラーを作成します。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・コントロール・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・コントロール・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を異なる役割に割り当てます。

セラー管理者の責任は以下のように要約できます。

- ストアを所有する組織を作成します。オプションで、組織の中のどの処理に承認が必要であるかを定義します。このステップは、企業間取り引きのサイトにのみ必要です。
- 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。

メンバー・グループ: ユーザー・グループおよびアクセス・グループ

WebSphere Commerce のメンバー・サブシステムでは、メンバー・グループを作成することも可能です。メンバー・グループとは、さまざまなビジネスの理由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・コントロール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) の目的としてグループ分けを使用できます。 **ユーザー・グループ**は一般的な使用目的、 **アクセス・グループ**はアクセス・コントロールの目的で使用されます。

ユーザー・グループ・タイプのメンバー・グループは、共通の関心を持つユーザーの集合として、マーチャントによって定義されます。ユーザー・グループは、常連の顧客または優良な顧客に関して、大きなストアから提供されるクラブに似ています。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カバン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・グループを作成できます。

アクセス・グループ・タイプのメンバー・グループは、アクセス・コントロールを目的としたユーザーのグループ化です。アクセス・グループは、アクセス・コントロール・ポリシーの 1 つのエレメントです。アクセス・グループでのメンバーシップは、通常暗黙的に定義されます。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、 MBRGRP テーブルの CONDITIONS 列に指定します。ユーザーを明示的にメンバー・グループに追加することもできます。同様に、ユーザーを明示的にメンバー・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 テーブルを使用して行われます。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、またはユーザー登録情報に基づいています。たとえば、Seller Administrators というアクセス・グループは、セラ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、デフォルトでいくつかの役割と、それに対応するメンバー・グループが組み込まれています。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、それに対応してセラー管理者という名前のメンバー・グループがあります。

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、特定の役割をすべての組織に割り当てる必要があります。役割は、絶対的または範囲限定のどちらかになります。絶対的役割では、ユーザーに役割が割り当てられますが、ユーザーは自分が属する組織でその役割を必ずしも果たすわけではありません。絶対的役割の例として、「公認会計士 (CPA)」があります。ユーザーは CPA になることができますが、自分が属する組織の会計士ではない場合もあり、他の組織の会計士である場合もあります。 CPA は絶対的役割ですが、経理担当者は範囲限定つまり相対組織役割です。 WebSphere Commerce 内のほとんどの役割は範囲限定です。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とします。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・コントロール・ポリシーをセットアップできます。

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。

- サイトの運用
- サイトおよびコンテンツの作成
- 技術的な運用
- マーケティングの管理
- 商品の管理
- ビジネス関係管理
- ロジスティクスおよび運用の管理
- 組織の管理

サイトの運用

WebSphere Commerce では、以下の技術的な運用の役割がサポートされています。

- サイト管理者

- ストア管理者

サイト管理者

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。管理者は、システムの警告、アラート、エラーに対して応答し、システムの問題を診断して解決します。この役割では、通常、アクセスおよび許可の制御 (メンバーを作成して適切な役割に割り当てる)、Web サイトの管理、パフォーマンスのモニター、および負荷均衡化タスクの管理を行います。管理者には、様々な開発段階 (テスト、ステージング、実動など) のいくつかのサーバー構成を設定して保守する責任もあります。またこの役割は、重要なシステムのバックアップを処理したり、パフォーマンス上の問題を解決したりします。

ストア管理者

ストア管理者は、ストア資産を管理し、税、配送、およびストア情報の変更を更新して公開します。ストア管理者は、組織のアクセス・コントロール・ポリシーを管理することもできます。ストア管理者 (通常はストア開発チームのリーダー) は、ストア開発チームではストア・アーカイブを公開する権限のある唯一の役割です (サイト管理者も、ストア・アーカイブを公開できます)。通常、ストア管理者は、Web を十分に理解しており、ストアのビジネス手順における広範囲な知識を持っています。

サイトおよびコンテンツの作成

WebSphere Commerce は、ストア開発者のサイトとコンテンツ開発の役割をサポートしています。

ストア開発者

ストア開発者は、Java Server Pages ファイルおよび必要とされるすべてのカスタマイズ・コードを作成します。また、WebSphere Commerce に組み込まれている標準機能のすべてを修正することができます。ストア・アーカイブが作成されると、ストア開発者はそれを手動で変更したり、またはストア・プロファイル・ノートブック、税ノートブック、および配送ノートブックを使って変更する許可を持っています。しかし、ストア・アーカイブを WebSphere Commerce Server に公開する許可はありません。

ロジスティクスおよび運用

WebSphere Commerce は、以下のロジスティクスおよび運用管理の役割をサポートしています。

- ロジスティクス・マネージャー
- オペレーション・マネージャー
- 受取人
- 返品担当者
- 梱包担当者

B2C — ロジスティクス・マネージャー

ロジスティクス・マネージャー (配送マネージャーと呼ばれることもある) は、大量貨物輸送や、運送会社から倉庫さらに個々の顧客への配送を管理および交渉しま

す。この役割には、会社の戦略にかなうように、会社が料金の最も安い最良の配送者を使用するようにする責任があります。配送は顧客サービスの重要な面であり、オンライン・ビジネスの成功のかぎとなる要因である場合があります。

B2B — オペレーション・マネージャー

この役割は、オーダーが適切に実行されていること、支払いを受け取ったこと、オーダーが配送されたことを確認して、オーダー処理を管理します。オペレーション・マネージャーは、顧客オーダーの検索、詳細情報の表示、オーダー情報の管理、および返品の編集を実行できます。

梱包担当者

梱包担当者は、配送センターから商品を選択し、その商品を梱包し、顧客に配送します。梱包担当者は、オーダー・フルフィルメントにおいて商品の配送を確認するために使用されるピッキング・チケットとパッキング・スリップも管理します。

受取人

受取人は、配送センターで在庫を受け取ったり、オーダー済み商品の予測在庫レコードと随時受け取りを追跡したり、顧客から返品された返品商品を受け取ったりします。

返品担当者

返品担当者は、返品された商品の処分を以下のように管理します。

- 返品のリスト
- 返品された商品をリストする
- 返品された商品を処分する

商品の管理

WebSphere Commerce では、以下の商品管理の役割がサポートされています。

- バイヤー (セラー・サイド)
- カテゴリー・マネージャー
- プロダクト・マネージャーまたは取引管理マネージャー

バイヤー (セラー・サイド)

バイヤーは、売り物の商品を購入します。バイヤーは、取引先またはサプライヤーとの関係を処理し、配送および支払いオプションなどについて有利な条件で希望する商品を調達できるように交渉します。バイヤーは、価格を設定する場合があります。購買する数量を決定したり、在庫の補充を適切に行うようにするために、在庫はバイヤーによって管理されます。

カテゴリー・マネージャー

カテゴリー・マネージャーは、カテゴリーを作成、変更、および削除することによってカテゴリー階層を管理します。カテゴリー階層は、ストアが提供する商品やサービスを編成します。カテゴリー・マネージャーは、商品、予測在庫レコード、取引先情報、および返品理由も管理します。

プロダクト・マネージャー

マーチャンダイジング・マネージャーまたはプロダクト・マネージャーは、顧客の購入履歴をトレースし、割引を提案し、オンライン・ストアにおける商品の最良の表示方法、価格設定方法、および販売方法を決定します。

- カテゴリー・マネージャーのすべてのタスクを実行します
- マーケティング・マネージャーのすべてのタスクを実行します

セールスの管理

WebSphere Commerce では、以下のビジネス関係管理の役割がサポートされています。

- セールス・マネージャー
- アカウント担当者
- 顧客サービス・スーパーバイザー
- 顧客サービス担当者

セールス・マネージャー

セールス・マネージャーは、顧客の獲得と維持に努め、販売予測に対応し、顧客のビジネスが拡張するような刺激を与えます。さらに、管理を担当し、価格を設定し、プロダクト・マネージャーと協働して在庫予測を立てたり、マーケティング・マネージャーと協働して販売促進を企画したりします。

アカウント担当者

アカウント担当者は、個々のアカウントを処理して、関係を確立し、顧客サービスを管理します。アカウント担当者は、契約価格の変更、契約の交渉、プロファイル作成、およびアカウント・カテゴリー別に収益性を分析する権限が与えられています。

顧客サービス・スーパーバイザー

この役割には、すべての顧客サービス・タスクへのアクセス権が与えられています。顧客サービス・スーパーバイザーは、顧客からの問い合わせ (顧客登録、オーダー、返品、オークションなど) を管理します。また、システムが拒否した返品レコードを承認することや支払い例外 (クレジット・カードの与信失敗など) に関連して顧客に連絡することなど、顧客サービス担当者ではアクセスできないアクションを完了する権限を持ちます。

顧客サービス担当者

オンライン・ビジネスが、顧客がセルフサービス機能を使用できるように優れた設計がされていても、普段は Web を利用する顧客が個人的に連絡をとることを必要とする場合もあります。ほとんどのオンライン・ビジネスでは、顧客のダイレクト・サービスのために E メール、ファクシミリ、または電話窓口を用意しています。顧客からのすべての問い合わせを扱うのは、顧客サービス担当者の責任です。

マーケティングの管理

WebSphere Commerce は、マーケティング・マネージャーのマーケティング管理役割をサポートします。

マーケティング・マネージャー

マーケティング・マネージャーは、マーケット戦略およびブランド・メッセージを顧客に伝達します。この役割は、顧客の振る舞いをモニターしたり、分析したり、また把握したりします。さらに、マーケティング・マネージャーは目標とする販売のための顧客プロファイルを作成または変更します。また、キャンペーンおよび販売促進の作成と管理を行います。キャンペーン・イベントの計画は、マーチャント、マーケティング・マネージャー、およびマーチャンダイジング・マネージャーで構成されるチームによって処理されます。

組織の管理

WebSphere Commerce は、以下の組織管理の役割をサポートしています。

- セラー管理者
- バイヤー管理者
- バイヤー承認者
- バイヤー (購買サイド)

セラー管理者

セラー管理者は、販売組織に関する情報を管理します。セラー管理者は、販売組織の中にサブ組織を作成して管理します。また、適切なビジネス役割の割り当てを含め、さまざまなユーザーの管理を行います。

バイヤー管理者

セラー管理者は、購買組織に関する情報を管理します。セラー管理者は、購買組織の中にサブ組織を作成して管理し、ユーザーをバイヤーとして承認することを含め、さまざまなユーザーの管理を行います。その他の購買サイドの役割 (バイヤー承認者およびバイヤー組織の管理者など) を作成して、管理できます。

バイヤー承認者

バイヤー承認者は、購買組織の中の担当者の一人であり、バイヤーによって作成されたオーダーがセラーによる購入のために送信される前に、そのオーダーの承認を行います。

バイヤー (購買サイド)

バイヤーは、バイヤーまたはバイヤー組織を代表して、セラーからの購入を行う担当者です。通常、購入はセラーと交渉して 1 つ以上の条件の下に行われます。バイヤーはセラーの Web サイトとやり取りして、購入を行います。

リソース・カテゴリー

リソース・カテゴリーとはリソースのクラスのことです。それで、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。

リソース・カテゴリーは、ACRESCGRY テーブルで定義されています。

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・コントロールでは、リソース・グループは、アクセス・コントロール・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 テーブルで定義されています。

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。たとえば、リソースの Java クラス名をリソース・グループにすることができます。属性を指定することによって、グループにリソースを暗黙的に追加すると、各リソースを指定せずに、大量のリソースへのアクセス権を簡単に設定できます。リソースに変更が加えられる場合に、リソースを追加または削除する必要もありません。

暗黙的なリソース・グループは、 ACRESGRP テーブルの CONDITIONS 列で定義されています。

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 テーブルで行います。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。

リソースの関係

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、文書の宛先やカタログ・エントリーの供給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 テーブルに保管され、アクセス・コントロール・ポリシーで、ACPOLICY テーブルの ACRELATION_ID 列を使ってオプションで指定されます。

アクセス・コントロール・ポリシー

アクセス・コントロール・ポリシーは、WebSphere Commerce のリソース上で、ユーザーまたはユーザー・グループが特定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・コントロール・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・コントロール・ポリシーを理解するためには、ユーザー、アクション、およびリソースの 3 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で実行できるアクティビティーです。

アクセス・コントロール・ポリシーのエレメント

アクセス・コントロール・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
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、「契約」や「オーダー」などのビジネス・オブジェクト、あるいはユーザーが実行できるオークション関連のコマンドなど、関連するコマンドのセットが含まれることがあります。

リソース関係 (オプション)
各リソース・タイプには、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。ある特定のアクセス・グループに属するユーザーが、指定されたリソース・グループに属するリソース上のアクション・グループの中で指定されている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。たとえば、オーダーに対して「所有者」関係を持つストアで作業するストア管理者によって、オーダーが削除されることを許可するポリシーを作成できます。

アクセス・コントロール・ポリシーの概念

アクセス・コントロール・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。 1 つ以上のアクセス・コントロール・ポリシーで、その責任を実行する権限を付与されない限り、ユーザーはどのサイトの機能にもアクセスできません。

アクセス・コントロール・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・コントロール・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。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・コントロールに関連する、概念的な情報と用語を説明します。

アクセス・グループ

アクセス・グループは、アクセス・コントロールの目的で特に定義されたユーザーのグループです。サイト管理者は、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。バイヤー管理者またはセラー管理者は、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。アクセス・グループでは、ユーザーは大抵その役割、組織、および登録状況に基づいてグループに分けられます。

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。

アクセス・グループは、暗黙的か、明示的か、あるいはその両方です。

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。基準を満たす人がグループのメンバーです。属性を指定することによって、アクセス・グループを暗黙的に追加すると、それぞれの名前を指定しなくても、簡単にたくさんのユーザーにアクセスを許可することができます。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。アクセス・グループの単純な基準は、ユーザーがその組織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。さらに複雑な基準は、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: 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。明示的にアクセス・グループを追加すると、共通属性を共用していない可能性がある個々のユーザーをグループ化できます。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。

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・コントロールの場合、アクションは通常は WebSphere Commerce コマンドにマップし、リソースは普通は保護されている EJB 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。最後の点として、Display アクションはデータ Bean リソースをアクティブにするのに使用されます。アクションは ACACTION テーブルに格納されます。

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。この処理は、管理コンソールから行います。アクション・グループは、ACACTGRP テーブルに格納されます。

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・コントロール・ポリシーを適用するかが判別されます。アクセス・コントロール・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、その同じ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。上位の組織エンティティーによって所有されているポリシーも、そのリソースに適用されます。

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・コントロールの場合、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。

データ Bean リソース: データ 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データ Bean は、必要なアクセス・コントロールをすでに実装しています。何を保護すべきかという問題は、新しいデータ 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。

データ Bean オブジェクトが自分だけで存在できる場合は、直接保護される必要があります。データ Bean の存在が別のデータ Bean の存在に依存する場合は、他のデータ Bean に保護を代行させるべきです。直接保護されるデータ Bean の例としては、Order データ Bean があります。間接的に保護されるデータ Bean の例としては、OrderItem データ Bean があり、これは Order データ Bean がある場合に限り存在します。データ Bean リソースを保護する方法については、*WebSphere Commerce 5.4 プログラマーズ・ガイド* を参照してください。

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。これらのリソースは保護されます。

リソースとポリシーの所有権

すべてのポリシーは、組織上のエンティティーによって所有されます。すべてのアクセス・コントロール・リソースにも所有者がおり、この所有者は普通は組織上のエンティティーです。たとえば、オーダーはストアを所有する組織によって所有されます。ユーザーもリソースを所有できます。たとえば、登録済みのユーザーは自分の登録情報を所有します。リソースとアクセス・コントロール・ポリシーの所有権は、特定のリソースに適用するポリシーを判別する際に重要になります。あるリ

ソースを所有している組織エンティティーに属するポリシーと、その所有者の上位の組織エンティティーに属するポリシーが、そのリソースに適用されます。

アクセス・コントロール・ポリシーのタイプ

アクセス・コントロール・ポリシーには、次の 2 つのタイプがあります。

- 正規ポリシー
- テンプレート・ポリシー

正規ポリシー

正規ポリシーの所有者は固定されています。たとえば、正規ポリシーがセラー組織によって所有される場合、そのポリシーはセラー組織によって所有されるリソースおよびその子孫となる組織エンティティー (存在する場合) によって所有されるリソースにのみ適用されます。ルートの組織は WebSphere Commerce 内にある他のすべての組織の先祖となる組織なので、ルートの組織 (メンバー ID = -2001) によって所有されるすべてのポリシーは、その定義によりサイト内のすべてのリソースに適用されます。したがって、ルートの組織によって所有される正規ポリシーは、サイト・レベルのポリシーと呼ばれることもあります。

ルートの組織によって所有されない正規ポリシーは、サイト全体に適用されるのではなくポリシー所有者またはその子孫となる組織エンティティーが所有するリソースに対してのみ適用されるので、組織レベルのポリシーと呼ばれます。ストア管理者は、自己の組織エンティティーおよびその子孫となる組織エンティティーのポリシーだけを管理できます。サイト管理者は、すべてのポリシーを変更できます。

テンプレート・ポリシー

テンプレート・ポリシーの所有者は動的です。テンプレート・ポリシーは、リソースを所有する組織エンティティーおよびその先祖となる組織エンティティーに対して動的に適用されます。たとえば、ルートの組織の下に 10 の組織があり、それぞれの組織は、役割に対応する組織が所有するリソースだけをストア管理者が変更できるようにしたいと願っていると想定します。これを実現する方法は次の 2 つです。

1. アクセスされているリソースに応じて 10 の組織のいずれかに動的に適用される、 1 つのテンプレート・ポリシーを持ちます。テンプレート・ポリシー内のアクセス・グループの基準も、動的にすることができます。たとえば、ユーザーが組織 X3 によって所有されるリソースにアクセスしようと試行している場合、テンプレート・ポリシーは組織 X3 に動的に変更されて、アクセス・グループも動的に組織 X3 を範囲とします。つまり、ユーザーは組織 X3 に関してストア管理者の役割を果たさなければならないということです。
2. 10 のポリシーを持ち、それぞれが 10 の組織のいずれかによって所有されるようにする。組織 X1 のアクセス・グループは、ユーザーが組織 X1 に関してストア管理者の役割を果たさなければならないことを指定します。組織 X2 のアクセス・グループは、ユーザーが組織 X2 に関してストア管理者の役割を果たさなければならないことを指定し、以下同様となります。

最初のソリューションの利点は、ポリシーの物理コピーは 1 つでも、10 の論理コピーが存在することです。テンプレート・ポリシーはサイト管理者が管理することができます。

テンプレート・ポリシーをオーバーライドする: テンプレート・ポリシーのもう 1 つの特徴は、指定の組織エンティティーについてそれらをオーバーライドできるということです。上記の例に戻ると、11 番目の組織エンティティーが WebSphere Commerce サイトに追加されて、この新規の組織エンティティーが上記のテンプレート・ポリシーの適用を受けたい場合、これを指定する方法があります。テンプレート・ポリシーのポリシー ID および 11 番目の組織の組織エンティティー ID を指定して、エントリーを ACORGPOL テーブルに追加しなければなりません。ストア管理者が特定の組織のコンテキストでテンプレート・ポリシーを削除または作成したとき、管理コンソールによってこれを実現することもできます。

アクセス・コントロールのレベル

WebSphere Commerce では、2 つの幅広いレベルのアクセス・コントロールがあり、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・ベースとも呼ばれる) です。

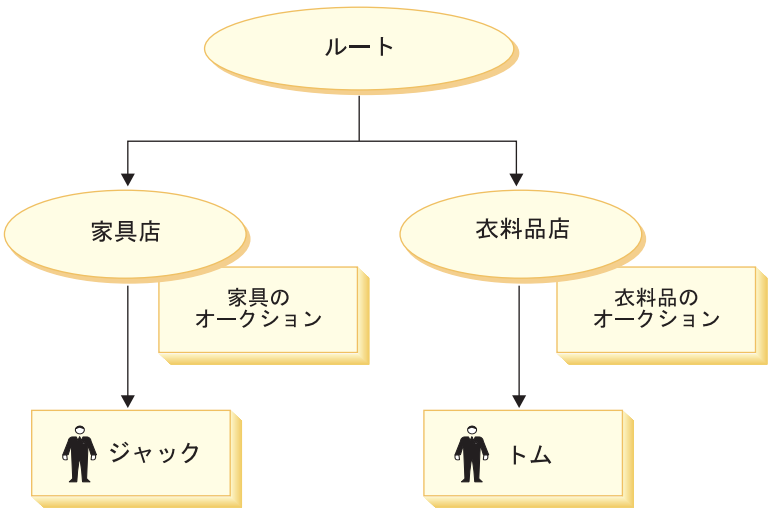

図 2. ポリシー・レベル

コマンド・レベルまたは役割ベースのアクセス・コントロール

コマンド・レベルまたは役割ベースのアクセス・コントロールは、大ざっぱなアクセス・コントロールです。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・コントロールによって、特定の役割をもつすべてのユーザーが、あるタイプのコマンドを実行できるように指定できます。 「セラーはオークションの変更を行える」というアクセス・コントロール・ポリシーについて検討してみましょう。 図 2 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を開始できます。

コマンド・レベルまたは役割ベースのアクセス・コントロールは、コントローラーおよびビュー・コマンドに使用できます。このタイプのアクセス・コントロールは、コマンドが影響を及ぼすリソースのことを考えません。単に、ユーザーが特定のコマンド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・コントロールは必須であり、Runtime によって強制されます。すべてのコントローラー・コマンドは、コマンド・レベルのアクセス・コントロールによって保護されなければなりません。さらに、直接呼び出せるビュー、または別のコマンドからリダイレクトに起動できるビューはすべて (ビューへの転送によって起動される場合とは対照的に)、コマンド・レベルのアクセス・コントロールによって保護されなければなりません。

コントローラー・コマンド用のコマンド・レベル・アクセス・コントロール: コントローラー・コマンドを実行するときはいつでも、ユーザーがコマンド・リソース上で ″Execute″ アクションを実行するのを認可するアクセス・コントロール・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・グループのスコープは普通、単一の役割になります。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・コントロール: 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・コントロール・ポリシーが必要です。そのようなポリシーには、 ACACTION テーブル内でアクションとして指定されたビュー名が必要です。次いでこのアクションは、 ACACTACTGP テーブル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 テーブル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・ベースまたはリソース・レベルのアクセス・コントロール

インスタンス・レベルまたはリソース・レベルのアクセス・コントロール・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・コントロールを提供します。役割ベースのアクセス・コントロールの例である「セラーはオークションで変更を行える」は、リソース・レベルのアクセス・コントロールに精練して、 「セラーは自分が作成したオークションで変更を行える」とすることができます。 74 ページの図 2では、ジャックは家具店のセラーです。トムは衣料品店のセラーです。ジャックは家具店で家具のオークションを作成します。トムは衣料品店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、後続のリソース・レベルのアクセス・コントロール・ポリシーが適用されます。

リソース・レベルのアクセス・コントロールは、コマンドと databean 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・コントロール: コマンド・レベルのアクセス・コントロール検査が完了した後に、アクセス権が付与された場合、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与信済みかどうかを判別することができます。アクションのデフォルトは、現行コマンドのインターフェース名になります。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, ..)

データベースに対するリソース・レベルのアクセス・コントロール: 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 databean 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。このことは、プライマリー (独立) databean を Protectable (保護可能) リソースとして指定することによって行います。そうすれば、Databean Manager の activate() メソッドを使って databean が起動されるときはいつでも、 WebSphere Commerce Runtime は、databean リソースで ″表示″ アクションを実行するための権限を現行ユーザーに付与するポリシーが必ずあることを保証します。

アクセス・コントロール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、ユーザーが与信済みの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・コントロール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与信の検査

Policy Manager 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・コントロール・コンポーネントです。アクセス・コントロール・ポリシーは XML 形式で指定されます。インストール時に、デフォルト・ポリシーは適切なデータベース・テーブルに自動的にロードされます。実行時に、Policy Manager は SQL 照会を使用して、データベース・テーブル内の情報を読み取ります。アクセス・コントロール情報はキャッシュに入れられるので、ユーザーの与信を検査するように Policy Manager が呼び出されたときに迅速にそうすることができます。アクセス・コントロール・ポリシーは、 UI ユーザーがアクセス権を与えられているアクションおよび情報だけを見られるようにするためにも使用されます。

ユーザーが特定のアクションを実行しようとすると、生成されたイベントがアクセス検査を起動し、そのユーザーが与信済みかどうかを確認します。 Policy Manager は、ターゲット・リソースに対してユーザーがアクションを実行するのを許可する

アクセス・コントロール・ポリシーをシステム内で探します。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、なければアクセスを拒否します。

第 6 章 XML ファイルを使用してアクセス・コントロール・ポリシーをカスタマイズする

管理コンソールを使用して、アクセス・コントロール・ポリシーおよびそのパーツ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する必要があります。

アクセス・コントロールのために XML ファイルを変更する前に、 *IBM WebSphere Commerce プログラマーズ・ガイド* でアクセス・コントロールについての章をお読みください。この章では、アクセス・コントロールについての技術的な概要を示し、アクセス・コントロール・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、エンティティー 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。

プログラマーズ・ガイド 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・コントロールの 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 ファイルを直接変更することによってのみ行えます。

- 新規のコマンドまたはビューの保護
- リソース関係の作成または変更
- リソース関係グループの作成または変更
- 新規のリソースの保護
- リソース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

アクセス・コントロール用の XML ファイルについて

WebSphere Commerce の XML 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 3. *WebSphere Commerce の XML ファイル*

ファイル名	説明
ACUserGroups_de_DE.xmll 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、ユーザー (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・コントロール・ポリシー、アクション・グループ、リソース・グループ、およびリソース関係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・コントロール・ポリシー、アクション・グループ、およびリソース・グループについて、サポートされている各言語でのビュー名および説明を含むファイル。
ACPoliciesfilter.xml	変更されたアクセス・コントロール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。

アクセス・コントロール用の XML タグの概要

カスタマイズのシナリオ

ビューの使用

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として立ち上げられるビューは、表示されるために役割ベースのアクセス・コントロール・ポリシーを必要とします。役割ベースのポリシーの形式は以下のとおりです。

```
<Policy Name="ProductManagersExecuteProductManagersViews"
OwnerID="RootOrganization"
UserGroup="ProductMangers"
ActionGroupName="ProductMangersViews"
ResourceGroupName="ViewCommandResourceGroup">
</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。

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・グループ内の 3 つのアクション、 ProductImageView、ProductManufacturerView、および ProductSalesTaxView が表示されます。

以下は、ProductImageView アクション定義の例です。

```
<Action Name="ProductImageView"
CommandName="ProductImageView">
</Action>
```

アクション名 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 テーブルの 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 テーブルの Action 列に保管されています。 Action Name と CommandName とは同じである必要はありません。

既存のポリシーを持つビューを追加する

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、以下のようにします。

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。

```
<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。

```
<ActionGroup Name="ProductManagersViews"
OwnerID="RootOrganization">

<ActionGroupAction Name="ProductImageView"/>
<ActionGroupAction Name="ProductManufacturerView"/>
<ActionGroupAction Name="ProductSalesTaxView"/>

</ActionGoup>
```

このアクション・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、これでビューを使用できるようになりました。

既存のポリシーを持たないビューを追加する

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、以下のようにします。

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。

```
<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>
```

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>
```

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">
</Policy>
```

これでビューが使用可能となり、それはアクションに関連付けられています。

コントローラー・コマンドを使用する

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・コントロール・ポリシーを必要とします。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">
</Policy>
```

ActionGroupName の ExecuteCommandActionGroup は、これが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 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.ContractCancelCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.ContractCloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.ContractCreateCmdResourceCategory"/>
</ResourceGroup>
```

上記の例は、コントローラー・コマンドに応答するリソース・グループ内の 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.ContractCloseCmdResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.commands.ContractCloseCmd">

<ResourceAction Name="ExecuteCommand"/>

</ResourceCategory>
```

名前 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・コントロール・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 テーブルの 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 Protectable インターフェースを拡張するので、リソースとして使用されます。これらの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。

既存のポリシーを持つコントローラー・コマンドを追加する

既存の役割ベースのコントローラー・コマンド・ポリシーを持つ役割によって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、以下を行います。

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">
   </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。

   ```
   <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
   <ResourceGroupResource Name="com.ibm.commerce.contract.commands.ContractCancelCmdResourceCategory"/>
   <ResourceGroupResource Name="com.ibm.commerce.contract.commands.ContractCloseCmdResourceCategory"/>
   <ResourceGroupResource Name="com.ibm.commerce.contract.commands.ContractCreateCmdResourceCategory"/>
   <ResourceGroupResource Name="com.xyz.commerce.contract.commands.MyNewControllerCmdResourceCategory"/
   </ResourceGroup>
   ```

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、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。

既存のポリシーを持たないコントローラー・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、以下のようにします。

- インターフェース名に対応する新規のアクション定義を、XML ファイル内に作成します。例については、1を参照してください。
- 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。

  ```
  <ActionGroup Name="XYZsCmdResourceGroup" OwnerID="RootOrganization">
  </ActionGroup>
  ```

- 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。

  ```
  <ActionGroup Name="XYZsCommands" OwnerID="RootOrganization">
  <ActionGroupAction Name="com.xyz.commands.MyNewControllerResourceCategory"/>
  </ActionGroup>
  ```

- 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="XYZsExecuteXYZsCmdResourceGroup"
  OwnerID="RootOrganization"
  UserGroup="XYZs"
  ActionGroupName="ExecuteCommandActionGroup"
  ResourceGroupName="XYZsCmdResourceGroup">
  </Policy>
  ```

これでコントローラー・コマンドが使用可能となり、それはアクションに関連付けられています。

リソース・レベルのアクセス・コントロールを使用する

リソース・レベルのアクセス・コントロール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、 `checkIsAllowed(Object resource, String action)` メソッドを使用してアクセス・コントロール・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。

注: デフォルトでは、getResources() メソッドはヌルを戻し、リソース検査は行われません。

以下の場合に、コマンドのリソース・ポリシーを作成する必要があります。

- コマンドが、リソース・レベルの検査を実行中の他のコマンドから拡張されている。
- コマンド自体がリソース・レベルのアクセス・コントロール検査を行う。

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="template">
</Policy>
```

パラメーター :

Name— ポリシーの名前。

PolicyType— ポリシーのタイプ。これはテンプレート・ポリシーであり、編成されたエンティティーとその祖先を所有するリソースに動的に適用されます。

OwnerID—ポリシーを所有するメンバー。これはテンプレート・ポリシーであり、ポリシーが Access Control Policy Manager によって適用されるにつれて、編成されたエンティティーとその祖先を所有するリソースに動的に変更されます。

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、23 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・コントロール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・コントロール・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・プロセスは、アクセス・コントロール・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。

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 <*wcs_home*>/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されるようにします。

400 では：カスタマイズされた XML ファイルを作成する場合、ファイル内で DTD への絶対パスを使用しなければなりません。アクセス・コントロール・ポリシー DTD は、 **/QIBM/ProdData/WebCommerce/xml/policies/dtd** にあります。

アクセス・グループおよびアクセス・コントロール・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。

NT 2000 では：

1. ディレクトリー<*wcs_home*>¥bin から、ここにリストされた順序で必要に応じて以下のコマンド・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*> **例**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml
   - メイン・アクセス・コントロール・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*> **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*> **例**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml
2. <*wcs_home*>¥schema 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。

AIX Solaris では：

データベースのユーザー ID は、ディレクトリー <*wcs_home*>/xml/policies、<*wcs_home*>/bin、および <*wcs_home*>/properties/utilities、さらにそのサブディレクトリーおよびファイルに対して、読み取り / 書き込み / 実行の権限を持っていなければなりません。

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<*wcs_home*>/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。

- 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*> **例**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml

- メイン・アクセス・コントロール・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*> **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 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*> **例**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_en_US.xml

1. <*wcs_home*>/schema 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 では :

コマンド行から、以下のコマンドを指定された順序で必要に応じて実行します。

- ユーザー (アクセス) グループ定義をロードするには、**LODWCSUG** コマンドを実行します。 **構文**: LODWCSUG DATABASE(<*database name*>) SCHEMA(<*schema_name*>) PASSWD(<*instance_password*>) INSTROOT(<*instance_root*>) INFILE(<*full path for XML file*>)
- メイン・アクセス・コントロール・ポリシー・ファイルをロードするには、**LODWCSAC** コマンドを実行します。 **構文**: LODWCSAC DATABASE (<database name>) SCHEMA (<schema_name>) PASSWD (<instance_password>) INSTROOT (<instance_root>) INFILE (<*full path for XML file*>)
- 表示名および説明ファイルをロードするには、**LODWCSACD** コマンドを実行します。 **構文**: LODWCSACD DATABASE(<*database name*>) SCHEMA(<*schema_name*>) PASSWD (<*instance_password*>) INSTROOT(<*instance_root*>) INFILE(<*full path to XML file*>)

付録. デフォルトのアクセス・コントロール・ポリシー

付録 A では、WebSphere Commerce に付属のデフォルト・ポリシーをリストします。それらは、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。
  - **DataBean 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。DataBean 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 4.

ポリシー	開始ページ
役割ベースのポリシー	90 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 :	91 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	91 ページの『オーダー』
取り引き (契約)	92 ページの『取り引き (契約)』
承認	93 ページの『承認』
オークション	93 ページの『オークション』
ビジネス・インテリジェンス	94 ページの『ビジネス・インテリジェンス』
メンバーシップ	94 ページの『メンバーシップ』
バイヤー管理コンソール	95 ページの『バイヤー管理コンソール』
キャンペーン	95 ページの『キャンペーン』
カタログ	95 ページの『カタログ』
接続および通知	96 ページの『接続および通知』
調達	96 ページの『調達』
クーポン	96 ページの『クーポン』
顧客プロファイル作成	97 ページの『顧客プロファイル作成』
割引	97 ページの『割引』
在庫	97 ページの『在庫管理』
スケジュール済み在庫	98 ページの『スケジュール済み在庫』
在庫管理	98 ページの『在庫管理』
オーダー管理	99 ページの『オーダー管理』
決済	99 ページの『決済』

表 4. (続き)

ポリシー、アクセス・グループ、リソース・グループ、およびアクション・グループを編集するための管理コンソール・ページ	100 ページの『ポリシー、アクセス・グループ、リソース・グループ、およびアクション・グループを編集するための管理コンソール・ページ』
商品アドバイザー	100 ページの『商品アドバイザー』
RFQ	100 ページの『RFQ』
ルール	101 ページの『ルール』
スケジューラー	101 ページの『スケジューラー』

役割ベースのポリシー

表 5.

AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
AccountRepresentativesExecuteAccountRepresentativesViews
AllUsersExecuteAllUserCmdResourceGroup
AllUsersExecuteAllUsersViews
BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
BuyerAdministratorsExecuteBuyerAdminstratorsViews
BuyerAdministratorsExecuteBuyerAdminstratorsCommands
BuyerApproversExecuteBuyerApproversCmdResourceGroup
BuyerApproversExecuteBuyerApproversViews
Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
Buyers(buy-side)ExecuteBuyers(buy-side)Views
Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
Buyers(sell-side)ExecuteBuyers(sell-side)Views
CategoryManagersExecuteCategoryManagersCmdResourceGroup
CategoryManagersExecuteCategoryManagersView
CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeView
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
CustomersExecuteCustomersViews
GuestsExecuteGuestUsersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersViews
MarketingManagersExecuteMarketingManagerCmdResourceGroup
MarketingManagersExecuteMarketingManagersViews
OperationsManagersExecuteOperationsManagersCmdResourceGroup
OperationsManagersExecuteOperationsManagersView
PickPackersExecutePickPackersCmdResourceGroup
PickPackersExecutePickPackersViews

表 5. (続き)

ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
ProductManagersExecuteProductManagersCmdResourceGroup
ProductManagersExecuteProductManagersViews
ReceiversExecuteReceiversCmdResourceGroup
ReceiversExecuteReceiversViews
ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
ReturnsAdministratorsExecuteReturnsAdministratorsViews
SalesManagersExecuteSalesManagersCmdResourceGroup
SalesManagersExecuteSalesManagersViews
SellerAdministratorsExecuteSellerAdministratorsCommands
SellerAdministratorsExecuteSellerAdministratorsViews
SellersExecuteSellersCmdResourceGroup
SellersExecuteSellersView
SiteAdministratorsCanDoEverything
StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup
StoreAdministratorsExecuteStoreAdministratorViews

ビジネス分野別のリソース・レベルのポリシー

オーダー

表 6.

データ・リソース	
オーダー	AllUsersExecuteOrderCreateCommandsOnStoreResource
	AllUsersExecuteOrderPrepareCommandsOnOrderResource
	AllUsersExecuteOrderProcessOnOrderResource
	AllUsersExecuteOrderReadCommandsOnOrderResource
	AllUsersExecuteOrderWriteCommandsOnOrderResource
	AllUsersExecuteReturnAgainstOrderOnOrderResource
	AllUsersExecuteScheduledOrderCancelOnOrderResource
	OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
リクィジション・リスト	AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
	AllUsersExecuteRequisitionListExclusiveProcessCommands OnPrivateRequisitionListResource
	AllUsersExecuteRequisitionListExclusiveReadCommandsOn PrivateRequisitionListResource
	AllUsersExecuteRequisitionListSharedProcessCommandsOn SharedRequisitionListResource

表 6. (続き)

	AllUsersExecuteRequisitionListSharedReadCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListWriteCommandsOn RequisitionListResource
買い物候補アイテム	AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
	AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource
RMA (返品取引許可)	AllUsersExecuteRMACreateCommandsOnStoreResource
	AllUsersExecuteRMAProcessCommandsOnRMAResource
	AllUsersExecuteRMAReadCommandsOnRMAResource
	AllUsersExecuteRMAWriteCommandsOnRMAResource
	RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
	RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
	RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
	RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
	StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource
DataBean	
オーダー	AllUsersDisplayApprovalsOrderDataBeansResourceGroup
	AllUsersDisplayOrderDatabeanResourceGroup
リクィジション・リスト	AllUsersDisplaySharedRequisitionListDataBeansIfSame OrganizationalEntityAsCreator
買い物候補アイテム	AllUsersDisplayInterestItemDatabeanResourceGroup
RMA	AllUsersDisplayRMADatabeanResourceGroup

取り引き (契約)

表 7.

データ・リソース	
契約	ContractAdministratorsForOrgExecuteContractCreateCommandsOn MemberResource
	ContractAdministratorsForOrgExecuteContractManageCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractDeployCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractSubmitCommandsOn ContractResource
	ContractViewersExecuteContractDisplayCommandsOnContractResource

表 7. (続き)

ビジネス・ポリシー	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy CreateCommandsOnStoreResoure
	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy ManageCommandsOnBusinessPolicyResourcee
DataBean	AccountHandlersDisplayTradingDatabeanResourceGroup

承認

表 8.

データ・リソース	
	AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
	AllUsersExecuteApproveCommandsOnApprovalResource
	AllUsersExecuteCancelApproveCommandsOnApprovalResource

オークション

表 9.

データ・リソース	
オークション	AuctionAdministratorsForOrgExecuteAdminRetractBidCommands OnAuctionResource
	AuctionAdministratorsForOrgExecuteAuctionCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionManageCommands OnAuctionResource
オークション・スタイル	AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionStyleManageCommands OnAuctionStyleResource
入札制御ルール	AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteBidControlRuleManageCommands OnBidControlRuleResource
入札	RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
	RegisteredApprovedUsersExecuteBidManageCommands OnBidResourcesTheyOwn
自動入札	RegisteredApprovedUsersExecuteAutoBidCreateCommands OnAuctionResource
	RegisteredApprovedUsersExecuteAutoBidManageCommands OnAutoBidResourcesTheyOwn
DataBean	AuctionDatabeanOwnersDisplayAuctionDatabeans

ビジネス・インテリジェンス

表 10.

データ・リソース	
	BusinessAnalystsForOrgExecuteViewContext ListCommandsOnStoreEntityResource
	IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport CommandsOnStoreEntityResource

メンバーシップ

表 11.

データ・リソース	
ユーザー	GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource
	MembershipAdministratorsForOrg ExecuteUserAdminUpdateCommandsOnUserResource
	NonRejectedUsersExecuteUserSelfRegistration ContinuationCommandsOnUserResource
組織	MembershipAdministratorsForOrgExecute OrgEntityRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteOrg EntityUpdateCommandsOnOrganizationResource
住所	MembershipAdministratorsForOrg ExecuteAddressManageCommandsOnMemberResource
	NonRejectedUsersExecuteAddressManageCommandsOn UserResource
役割	MembershipAdministratorsForOrgExecute RoleManageCommandsOnUserResource
	OrganizationRoleAdministratorsExecute RoleManageCommandsOnOrganizationResource
メンバー・グループ	MemberGroupAdministratorsForOrgExecute MemberGroupCreateCommandsOnMemberResource
	MemberGroupManagersForOrgExecute MemberGroupManageCommandsOnMemberGroupResource
DataBean	MembershipAdministratorsForOrgDisplay OrganizationDatabeanResourceGroup
	MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup

バイヤー管理コンソール

表 12.

データ・リソース	
承認グループ	MembershipAdministratorsForOrgExecute ApproveGroupUpdateCommandsOnOrganizationResource
メンバー・グループ	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnMemberGroupResource
	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnUserResource

キャンペーン

表 13.

データ・リソース	
	CampaignManagersForOrgExecute CampaignRelatedCreateCommandsOnStoreEntityResource
	CampaignManagersForOrgExecute CampaignUpdateCommandsOnCampaignResource
	CampaignManagersForOrgExecute CollateralUpdateCommandsOnCollateralResource
	CampaignManagersForOrgExecute EMarketingSpotUpdateCommandsOnEMarketingSpotResource
	CampaignManagersForOrgExecute InitiativeUpdateCommandsOnInitiativeResource
DataBean	CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

カタログ

表 14.

データ・リソース	
	CatalogEntryManagersForOrgExecute CatalogEntryManageCommandsOnCatalogEntryResource
	CatalogEntryManagersForOrgExecute CatalogEntryRelationManageCommandsOnCatalogResource
	CatalogEntryManagersForOrgExecute StoreCatalogEntryManageCommandsOnStoreEntityResource
	CatalogGroupManagersForOrgExecute CatalogGroupManageCommandsOnCatalogGroupResource
	CatalogGroupManagersForOrgExecute ProductSetAddCommandsOnCatalogResource
	CatalogGroupManagersForOrgExecute ProductSetManageCommandsOnProductSetResource

表 14. (続き)

	CatalogManagersForOrgExecute CatalogManageCommandsOnCatalogResource
	CatalogManagersForOrgExecute StoreCategoryManageCommandsOnCatalogResource
DataBean	CatalogGroupManagersForOrgDisplay CatalogGroupDataBeansResourceGroup
	ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup

接続および通知

表 15.

データ・リソース	
	BackendOrderAdministratorsForOrgExecute BackendOrderStatusCreateCommandsOnOrderDataResource
	BackendPickPackersForOrgExecute BackendPickPackListCommandsOnFulfillmentCenterDataResource
	StoreAdministratorsForOrgExecute MessagingAdminCommandsOnStoreEntityResource
DataBean	StoreAdministratorsForOrgDisplayMessagingDataBeans

調達

表 16.

データ・リソース	
	ProcurementAdministratorsForOrgExecute ProcurementAuthenticationAndRegistrationOnOrderDataResource
	ProcurementShoppingCartManagersExecute ProcurementShoppingCartManageOnOrderResource

クーポン

表 17.

データ・リソース	
	CouponAdministratorsForOrgExecute CouponPromotionCreateCommandsOnStoreEntityResource
	CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommands OnCouponPromotionResource
	RegisteredApprovedUsersExecute CouponDeleteCommandsOnCouponWalletResource
	RegisteredApprovedUsersExecute CouponRedemptionCommandsOnCouponWalletResource

表 17. (続き)

	StoreAdministratorsForOrgExecute ScheduledCouponCmdsOnStoreResource
DataBean	CouponAdministratorsForOrgDisplayECouponPromotionListBeans

顧客プロファイル作成

表 18.

データ・リソース	
	CustomerProfileEditorsForOrgExecute SegmentManageCommandsOnStoreEntityResource
DataBean	CustomerProfileEditorsForOrgDisplay SegmentationDatabeansResourceGroup

割引

表 19.

データ・リソース	
	DiscountAdministratorsForOrgExecute DiscountAssociateCommandsOnCalculationCodeResource
	DiscountAdministratorsForOrgExecute DiscountCreateCommandsOnStoreEntityResource
	DiscountAdministratorsForOrgExecute DiscountDeployCommandsOnCalculationCodeResource
DataBean	DiscountViewersForOrgDisplayDiscountDatabeans

在庫管理

表 20.

データ・リソース	
	ExpectedInventoryManagersForOrgExecute InventoryManageCommandsOnStoreEntityResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterCreateCommandsOnOrganizationResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterManageCommandsOnFulfillmentResource
	InventoryAdjustersForOrgExecute InventoryAdjustCommandsOnStoreEntityResource
	PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommands OnFulfillmentCenterResource
	PickPackGeneratorsForOrgExecute PickPackGenerateCommandsOnFulfillmentCenterResource

表 20. (続き)

	ReturnReasonsManagersForOrgExecute ReturnReasonsCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorCreateCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorManageCommandsOnVendorResource
DataBean	StoreAdministratorsForOrgDisplay OrderFulfillmentStatusDataBeansResourceGroup

スケジュール済み在庫

表 21.

データ・リソース	
	StoreAdministratorsForOrgExecute InventoryScheduledCommandsOnStoreEntityResource

在庫管理

表 22.

DataBean	
	ExpectedInventoryManagersForOrgDisplay ExpectedInventoryDataBeansResourceGroup
	FulfillmentCenterManagersForOrgDisplay FulfillmentCenterDataBeansResourceGroup
	PickBatchInventoryManagersForOrgDisplay PickBatchInventoryDataBeansResourceGroup
	ProductFindInventoryManagersForOrgDisplay ProductFindInventoryDataBeansResourceGroup
	ReceiverOrderManagersForOrgDisplay ReceiverOrderManagementDataBeansResourceGroup
	ReturnReasonsManagersForOrgDisplay ReturnReasonsOrderManagementDataBeansResourceGroup
	ReturnsAdminOrderManagersForOrgDisplay ReturnsAdminOrderManagementDataBeansResource
	SuperUserOrderManagersForOrgDisplay SuperUserOrderManagementDataBeansResourceGroup
	VendorInventoryManagersForOrgDisplay VendorInventoryDataBeansResourceGroup

オーダー管理

表 23.

データ・リソース	
	CustomerOrderManagersExecute CustomerServiceCustomerWriteCommandsOnUserResource
	CustomerOrderManagersForDefaultOrgExecute CustomerServiceCustomerWriteCommandsOnUse
	CustomerOrderManagersForOrgExecute CustomerServiceOrderCreateCommandsOnStoreEntityResource
	CustomerOrderManagersForOrgExecute CustomerServiceOrderWriteCommandsOnOrderResource
	CustomerOrderManagersForOrgExecute CustomerServiceReturnCreateCommandsOnStoreEntity
	CustomerOrderManagersForOrgExecute CustomerServiceReturnWriteCommandsOnRMAResource
DataBean	CustomerOrderManagersDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForDefaultOrgDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForOrgDisplay CustomerOrderManagementDatabeans
	LogisticsManagersForOrgDisplay OrdersAndReturnsListsDatabeans
	ReturnsManagersForOrgDisplayReturnsListsDatabean
	UserOrderManagersDisplayUserDatabeans
	UserOrderManagersForDefaultOrgDisplayUserDatabeans

決済

表 24.

データ・リソース	
	AccountAdministratorsForOrgExecute AccountManageCommandsOnAccountResource
	AccountManagersForOrgExecute AccountCreateCommandsOnOrganizationResource
	AccountViewersForOrgExecute PaymentSummaryGenerateCommandsOnAccountResource
	AccountViewersForOrgExecute StorePaymentAdminCommandsOnStoreEntityResource
	AllUsersExecutePaymentOrderWrite CommandsOnOrderResource

ポリシー、アクセス・グループ、リソース・グループ、およびアクション・グループを編集するための管理コンソール・ページ

表 25.

データ・リソース	
	DescendantStoreAdministratorsExecute ACViewPoliciesForOrgActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyCreateCommandsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyEditCommandsOnACPolicyResource
	StoreAdministratorsForOrgExecute ACViewApplicablePoliciesActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACViewPoliciesForUpdateActionsOnOrganizationResource
DataBean	StoreAdministratorsForOrgExecute UserGroupSearchViews

商品アドバイザー

表 26.

DataBean	
	ProductAdvisorStatisticiansForOrgDisplay ProductAdvisorStatisticsDatabeans
	SalesAssistantStatisticiansForOrgDisplay SalesAssistantStatisticsDatabeans

RFQ

表 27.

データ・リソース	
	RFQAdministratorsAdministerRFQs
	RFQAdministratorsManageRFQResponses
	RFQBuyersEvaluateRFQResponsesForRFQsTheyOwn
	RFQBuyersForOrgExecuteRFQCreate CommandsOnStoreEntityDataResourceGroup
	RFQBuyersManageRFQResourcesTheyOwn
	RFQBuyersManageRFQResponsesForRFQsTheyOwn
	RFQSalesManagersExecuteRFQResponse ManageCommandsOnRFQResponseResource
	RFQSalesManagersForOrgCreateRFQResponse
DataBean	RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn

表 27. (続き)

	RFQBuyersDisplayRFQResponseDataBeans ViewabletoRFQOwnerResourceGroup
	RFQSalesViewersDisplayRFQDataBeanResourceGroup
	RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup

ルール

表 28.

データ・リソース	
	StoreAdministratorsForOrgExecutePersonalization RuleServiceAdministrationCommandsOnStoreEntityResource
DataBean	StoreAdministratorsForOrgDisplay PersonalizationRuleServiceAdministrationDataBeanResource

スケジューラー

表 29.

データ・リソース	
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnStoreEntityResource
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnUserResource
DataBean	StoreAdministratorsForOrgDisplay SchedulerDataBeansResourceGroup

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、米国以外の国においては本書で述べる製品、サービス、またはプログラムを提供し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、プログラムまたはサービスの操作性の評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。 実施権の許諾については、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 丁目 2-31
IBM World Trade Asia Corporation
Intellectual Property Law & Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

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

本書は定期的に見直され、必要な変更 (たとえば、技術的に不適切な表現や誤植など) 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。

Manager, e-Commerce Product Development IBM 17 Skyline Drive Hawthorne, NY 10532 U.S.A.

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

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

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。

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。

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。

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。 したがって 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。

DB2 DB2 Universal Database

IBM WebSphere

Lotus、Domino、および Go Webserver は、Lotus Development Corporation の商標です。

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

Action Media、LANDesk、MMX、Pentium および ProShare は、Intel 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などはそれぞれ各社の商標または登録商標です。

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。

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