Oracle® Universal Content Management

セキュリティおよびユーザー・アクセスの管理

10*g* リリース 3（10.1.3.3.1）

部品番号 : E05627-01

2007 年 10 月

ORACLE®

Oracle Universal Content Management セキュリティおよびユーザー・アクセスの管理 , 10*g* リリース 3（10.1.3.3.1）

部品番号 : E05627-01

原本名 : Oracle Universal Content Management Managing Security and User Access, 10*g* Release 3 (10.1.3.3.1)

原本部品番号 : A00025-01

原本協力者 : Karen Johnson, Peter Walters, Samuel White

目次

第 1 章： 概要

第 2 章： セキュリティ・モデルの設計

第 3 章 : 内部セキュリティ : セキュリティ・グループ、ロールおよび権限

第 4 章： 内部セキュリティ：アカウントの使用

第 5 章： 内部セキュリティ：ユーザー・ログインおよび別名の割当て

第 6 章： 外部セキュリティ：Active Directory

第 7 章： 外部セキュリティ：LDAP

第 8 章 : プロキシ接続

付録 A: サード・パーティ・ライセンス

索引

1

概要

概要

この項の内容は次のとおりです。

このガイドについて

このガイドでは、セキュリティ・モデルの計画や実装、ユーザーの追加や削除およびアカウントの実装など、ユーザー管理に関連するタスクを説明します。また、外部ユーザー・ベースと Content Server の統合方法も説明します。2 つの最も一般的なセキュリティ統合である Active Directory および LDAP についても詳細に説明しています。

新機能

次に、Content Server 10*g* リリース 3 の新機能を示します。

- **類似ユーザーの作成 :** ユーザー管理アプレットには、新しい「Create Similar」ボタンがあります。このボタンを使用すると、既存のユーザーに割り当てられたロールやアカウントに基づいてユーザー・ログインを作成できます。詳細は、3-11 ページの「「Create Similar Users」へのロールの割当て」を参照してください。

- **プロキシ接続 :** プロキシ接続を使用すると、次の機能により、Content Server のセキュリティ・レベルが向上します。
  - あるコンテンツ・サーバーから別のコンテンツ・サーバーへのセキュリティ資格証明マッピング
  - コンテンツ・サーバーへのセキュアな名前付きパスワード接続（パスワードで保護されたプロバイダ接続）
  - コンテンツ・サーバー間の HTTP プロトコルによる通信（HTTP ベースのプロキシ・サーバー）

  詳細は、第 8 章「プロキシ接続」を参照してください。

- **無効または破損した HTML 構成データのフィルタ処理 :** encodeHtml Idoc スクリプト機能により、無効または破損した HTML 構成データをフィルタ処理できます。これは、WCM 環境では特に便利です。詳細は、2-7 ページの「データ入力フィルタ」を参照してください。

- **異なる Web サーバー・フロントエンド（HTTP/HTTPS）からのログイン :** BrowserUrlPath コンポーネントが組み込まれました。ユーザーが異なる Web サーバー・フロントエンド（1 つは HTTPS でもう 1 つは HTTP）を使用して Content Server にアクセスできるようにする場合は、BrowserUrlPath コンポーネントをお薦めします。この機能を使用するには、このコンポーネントを有効化する必要があります。

- **Cookie ベースのログアウト :** バージョン 10*g* リリース 3 には、ログアウト機能を簡単に追加できる構成エントリの設定を可能にする ExtranetLook コンポーネントが同梱されています。付属の機能を使用するには、このコンポーネントを有効化する必要があります。詳細は、2-5 ページの「ログイン / ログアウトのカスタマイズ」を参照してください。

対象読者

このガイドは、ネットワーク・セキュリティおよび Content Server のコンテンツ・セキュリティの管理を担当する管理者を対象としています。

その他の管理者ガイド

管理者は、Content Server のユーザー、コンテンツおよびシステム構成を設定、維持および管理します。管理者の一般的なタスクには、ファイルを管理および索引付けするためのシステム構成、情報のアーカイブおよびレプリケート、コンテンツ・サーバーのセキュリティに関する作業、システム・プロパティの調整、ログ・ファイルの確認などがあります。

次に、Content Server ソフトウェアの管理者および副管理者向けのガイドを示します。

- 『Getting Started』（PDF および HTML）
  このガイドでは、製品の Oracle スイートの概要、およびそれらの設定や実装に関する一般的なガイドラインを説明します。
- 『セキュリティおよびユーザー・アクセスの管理』（PDF および HTML）
  このガイドでは、セキュリティ・モデルの計画や実装、ユーザーの追加や削除およびアカウントの実装など、ユーザー管理に関連するタスクを説明します。また、外部ユーザー・ベースと Content Server の統合方法も説明します。最も一般的なセキュリティ統合である Active Directory および LDAP についても詳細に説明しています。
- 『Managing Repository Content』（PDF および HTML）
  このガイドでは、カスタマイズされたコンテンツ・タイプの作成、スキーマの使用、Web サイトの構築、またはワークフローを介したコンテンツの移動など、コンテンツの表示や処理方法に影響するタスクを説明します。
- 『Managing System Settings and Processes Guide』（PDF および HTML）
  このガイドでは、リビジョンや索引付けの管理、プロバイダの構成、システム・プロパティに関する作業など、継続的にシステム構成に影響を与えるタスクを説明します。
- 『Administration Tutorials』（PDF および HTML）
  このガイドには、Content Server ベースのコンテンツ管理ソリューション（の一部）を管理する必要があるユーザー向けの管理チュートリアルが含まれています。
- 『Enterprise Search Administration and User Guide』（PDF および HTML）
  このガイドでは、エンタープライズ検索の管理情報を提供します。これにより、複数のコンテンツ・サーバー・インスタンスを単一のインスタンスであるかのように検索できます。
- 『Troubleshooting Guide』（PDF および HTML）
  このガイドには、Content Server 環境のトラブルシューティングに関する一般的な情報や問題の診断方法が含まれており、特定領域のトラブルシューティングに関するより詳細な情報が提供されています。

- ❖ リリース・ノート（印刷および PDF）
  Content Server ソフトウェアにはリリース・ノートが同梱されています。リリース・ノートには、各ソフトウェアの新規リリースの新機能および拡張機能が記載されており、ソフトウェアのインストールおよび使用方法に関する固有の最新の注意事項も説明されています。リリース・ノートは重要なドキュメントです。Content Server ソフトウェアのインストールまたは更新前には、必ずリリース・ノートを読んでください。

注意 : Content Server へのオプションのアドオンには、通常独自の管理ガイドがあり、一般的にはアドオン配布メディアの /documentation ディレクトリに PDF ファイルとして含まれています。

CONTENT SERVER の概要

この項の内容は次のとおりです。

目的

Content Server は、低コストのアクセス・ポイントとして Web サイトを使用し、ビジネス情報を共有、管理および配布するために使用されます。

Web 用に設計されたこのソフトウェアは、中規模から大規模の企業が、コンテンツのチェックイン、チェックアウト、リビジョンの管理および Web 対応形式での自動公開が可能なセキュアなビジネス・ライブラリを構築する際の、他に類のないソリューションであると考えられています。認可されたユーザーは、時間や場所を選ばずに最新の情報を参照できます。手紙、レポート、製品図面、スプレッドシート、マニュアル、販売文献などあらゆるタイプのファイルを、ナレッジ配布の強力な 1 つのシステムに実質的にリンクできます。

ユーザー

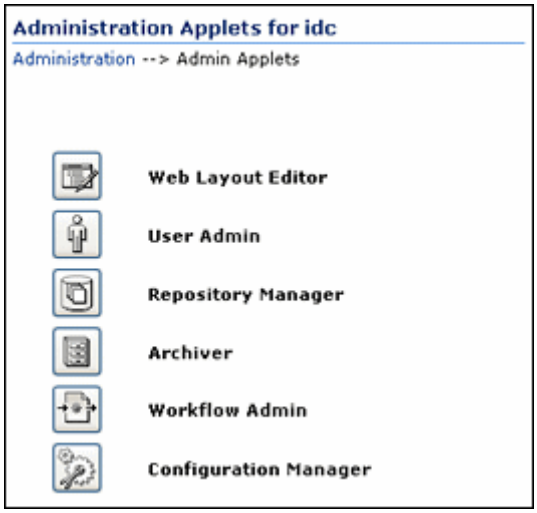
Content Server は、2 つのタイプのユーザーおよび管理者向けに設計されています。

- **コンシューマ :** ファイルの検索、表示および印刷のみを必要とするユーザー
- **コントリビュータ :** ファイルを作成および変更する必要があるユーザー
- **管理者 :** インスタンス全体を監視する管理者
- **副管理者 :** インスタンスのサブセットを監視する管理者

一般的なシステムでは、大部分のユーザーはコンシューマです。ファイルがセキュリティで保護されている場合を除き、これらのユーザーには、コンテンツ・サーバー・システムへのアクセスにユーザー名やパスワードは必要ありません。ファイルの整合性を保護するため、コントリビュータがシステムのファイルをチェックインおよびチェックアウトするには、ユーザー名とパスワードが必要です。

通常、大部分の管理者は副管理者です。システム管理者によって割り当てられた権限に対応するソフトウェアの一部を管理します。

「ADMINISTRATION」ページ



このページから、管理アプレットおよび構成ツールにアクセスできます。このページにアクセスするには、管理者または副管理者としてログインし、ポータル・ナビゲーション・バーにある「Administration」トレイをクリックします。次に、「Admin Applet」リンクをクリックします。

注意 : Sun 社の JDK 1.3/1.4 Java プラグインを使用するブラウザから Java アプレット（Content Server の管理アプレットまたは複数ファイルのアップロード・アプレットなど）を起動すると、問題が発生する場合があります。これらの問題は、初めてアプレットを起動する場合の認証や、親ウィンドウが変更された場合のアプレットの終了に関連します。

アプリケーションの起動

次の方法で Content Server の管理アプリケーションを起動できます。

- アプレットとしてのアプリケーションの起動（1-6 ページ）
- スタンドアロン・モードでのアプリケーションの実行（1-7 ページ）

アプレットとしてのアプリケーションの起動

コンテンツ・サーバーにアクセスできる任意のブラウザから、Content Server の複数の管理アプリケーションをアプレットとして実行できます。アプレットは、リモート管理に便利です。

バッチ・ローダ、コンポーネント・ウィザード、システム・プロパティおよび Content Server アナライザ・ユーティリティは、セキュリティの理由から、コンテンツ・サーバーがインストールされているコンピュータからスタンドアロン・モードで実行する必要があるため、アプレットとして実行できません。詳細は、1-7 ページの「スタンドアロン・モードでのアプリケーションの実行」を参照してください。

アプリケーションのスタンドアロン・バージョンで使用可能ないくつかの機能は、アプレット・バージョンでは使用できません。詳細は、各アプリケーションのマニュアルを参照してください。

管理アプリケーションを Java 対応ブラウザ内の Java アプレットとして実行するには、次のようにします。

1. ブラウザ・ウィンドウを開きます。
2. 管理者としてコンテンツ・サーバーにログインします。
3. ポータル・ナビゲーション・バーの「Administration」トレイ・リンクをクリックします。
4. 「Admin Applets」リンクをクリックします。

スタンドアロン・モードでのアプリケーションの実行

Content Server がインストールされているコンピュータから、Content Server の多数の管理アプリケーションをスタンドアロン・モードで実行できます。これらのプログラムの起動に必要な方法は、Windows と UNIX インストールで多少異なります。

アプリケーションのスタンドアロン・バージョンを実行した場合、セキュリティはブラウザ・アプレットより強力で、Web やネットワークから捕捉またはコピーせずにパスワードを送信できます。

Windows システムの場合

Windows オペレーティング・システムでスタンドアロンの管理アプリケーションを実行するには、次のようにします。

1. Windows の「スタート」メニューからアプリケーションを選択します。
   - 「**スタート**」→「**プログラム**」→「**Content Server**」→「***instance***」→「**Applications**」→「***application***」を選択します。
   - 管理ユーティリティの 1 つを実行するには、「**スタート**」→「**プログラム**」→「**Content Server**」→「***instance***」→「**Utilities**」→「***utility***」を選択します。

   コンポーネント・ウィザードおよびシステム・プロパティ以外のすべてのアプリケーションでは、ログイン画面が表示されます。コンポーネント・ウィザードおよびシステム・プロパティでは、アプリケーションのメイン画面が表示されます。

技術ヒント : ログイン画面またはアプリケーション画面が表示されるまでに数秒かかり、画面が別のウィンドウに隠れている場合があります。

2. 管理者ログイン名およびパスワードを入力します。
3. 「**OK**」をクリックします。

   アプリケーションのメイン画面が表示されます。

UNIX システムの場合

UNIX オペレーティング・システムでスタンドアロンの管理アプリケーションを実行するには、次のようにします。

1. <*Install_Dir*>/bin/ ディレクトリに移動します。
2. 実行可能なアプリケーションが表示されます。***/application_name*** を入力します。ここで、*application_name* は 1 つの実行可能ファイルの名前です。アプリケーションが表示されていない場合は、次の例のように、IntradocApp アプリケーションへのパラメータとして入力できます。

   ```
   %<Install_Dir>%/bin/intradocApp workflow
   ```

3. コンポーネント・ウィザードおよびシステム・プロパティ以外のすべてのアプリケーションでは、ログイン画面が表示されます。コンポーネント・ウィザードおよびシステム・プロパティでは、アプリケーションのメイン画面が表示されます。
4. 管理者ログイン名およびパスワードを入力します。
5. 「**OK**」をクリックします。

   アプリケーションのメイン画面が表示されます。

表記規則

このガイドでは、次の表記規則が使用されています。

- *<Install_Dir>/* という表記は、コンテンツ・サーバー・インスタンスがインストールされているシステム上の場所の参照に使用されます。
- スラッシュ（/）は、パス名のディレクトリ・レベルを区切るために使用されます。スラッシュは、ディレクトリ名の最後に表示されます。
- 注意、技術ヒント、重要な通知および警告には、次の表記が使用されます。

記号	説明
	これは注意書きです。特に注意が必要な情報に使用されます。
	これは技術ヒントです。作業を簡単にするために使用できる情報を示す場合に使用されます。
	これは重要な通知です。必要な手順または情報を示す場合に使用されます。
	これは警告です。データ損失や深刻なシステムの問題の原因となる可能性のある情報を示す場合に使用されます。

2

セキュリティ・モデルの設計

概要

この項の内容は次のとおりです。

セキュリティのレベル

Oracle Content Server のコンテンツ・セキュリティのレベルには、セキュリティ・グループ（必須）およびアカウント（オプション）の 2 つがあります。各コンテンツ・アイテムはセキュリティ・グループに割り当てられ、アカウントを有効化している場合は、アカウントにも割り当てられます。ユーザーには、各セキュリティ・グループおよびアカウントに対するあるレベルの権限（読取り、書込み、削除または管理）が割り当てられます。これにより、ユーザーは、アイテムのセキュリティ・グループおよびアカウントに対して持っている権限の範囲内でコンテンツ・アイテムを使用できます。

セキュリティ・オプション

Content Server には、次のセキュリティ・オプションがあります。

- 内部セキュリティ（2-2 ページ）
- 外部セキュリティ（2-3 ページ）
- 追加のセキュリティ・オプション（2-4 ページ）

内部セキュリティ

ユーザー管理アプリケーションを使用して、Content Server 内のユーザー・セキュリティを設定できます。各ユーザーを 1 つ以上のロールに割り当てると、セキュリティ・グループに対する特定の権限が割り当てられます。アカウントを有効化している場合は、特定のアカウントに対する特定の権限をユーザーごとに割り当てられます。これにより、割り当てられたロールを介して付与される可能性のある権限を制限できます。

次のコンポーネントを使用して、追加の内部セキュリティを提供することもできます。

- ExtranetLook コンポーネントを使用して、ユーザー・アクセスのセキュリティをカスタマイズできます。このコンポーネントは、Content Server のインストール時にインストールおよび有効化できます。詳細は、2-5 ページの「ログイン / ログアウトのカスタマイズ」を参照してください。
- Need to Know コンポーネントを使用して、ユーザー・アクセスおよび検索結果のセキュリティをカスタマイズできます。このコンポーネントを使用すると、ユーザー・アクセス制限の追加構成、検索結果の表示の変更、検索動作の変更、およびヒット・リスト・ロールの設定を実行できます。

注意 : MS Internet Explorer 7 では、安全な接続を使用しない Basic 認証でログインしているユーザーに対して、「警告 : このサーバーは、ユーザー名とパスワードを安全ではない方法で送信することを要求しています。」というメッセージが表示されます。これは新しいメッセージです。この動作（ユーザー名とパスワードのテキストでの送信）は Basic 認証では新しいことではなく、問題は発生しません。

関連項目

– 第 3 章「内部セキュリティ : セキュリティ・グループ、ロールおよび権限」

外部セキュリティ

ユーザー・ログイン、パスワードおよび権限は、次の外部ユーザー・ベースのいずれか 1 つから導出されます。

- **Active Directory:** ユーザー情報は、Microsoft Active Directory のユーザー・ベースに格納されます。詳細は、第 6 章「外部セキュリティ : Active Directory」を参照してください。
- **LDAP:** ユーザー情報は、iPlanet などの LDAP 準拠のユーザー・ベースに格納されます。詳細は、第 7 章「外部セキュリティ : LDAP」を参照してください。
- **Active Directory と LDAP の併用 :** ユーザー情報は、Microsoft Active Directory のユーザー・ベースに格納されます。Content Server は LDAP プロバイダを使用してこのユーザー・ベースにアクセスします。このタイプのセキュリティ統合には、カスタムの Active Directory LDAP コンポーネントが必要です。このコンポーネントのインストールおよび構成の詳細は、『Active Directory LDAP Component Administration Guide』を参照してください。

外部ユーザー

外部セキュリティ（Active Directory または LDAP）を介して認証されているユーザーは、Content Server の外部ユーザーとみなされます。外部ユーザーが初めてログインすると、データベースに追加され、管理者はリポジトリ・マネージャを使用して外部ユーザー情報を表示できます。ただし、外部ユーザーは、「content Check In」ページの「Author」フィールドなどのユーザー・リストには含まれません。

注意 : ユーザーの「User Profile」ページで「Override」チェック・ボックスが選択されている場合、外部ユーザー・ベースから導出されたユーザー情報は、Content Server データベースに定義されているユーザー情報で上書きされます。

デフォルトでは、限られたユーザー情報（ユーザー名、パスワード、ロールおよびアカウント）のみが、外部セキュリティ統合により外部ユーザー・ベースからコンテンツ・サーバーにマッピングされます。Active Directory または LDAP 統合を使用している場合には、電子メール・アドレスやユーザー・ロケールなどの追加のユーザー情報を、Content Server の管理ページからマッピングできます。プロキシ接続を使用すると、特定のアカウント名へのドメイン接頭辞のマッピングなど、より複雑なマッピング技術が提供されます。ある Content Server から別の Content Server への資格証明のマッピング方法の詳細は、第 8 章「プロキシ接続」を参照してください。

Microsoft ログイン

Active Directory セキュリティを Content Server と統合すると、ユーザーはユーザー名とパスワードを再入力せずに、ポータル・ナビゲーション・バーの「**Microsoft Login**」ボタンを使用して Content Server にログインできるようになります。標準の「Login」ボタンをクリックすると、ユーザー名とパスワードを要求されます。

関連項目

– 外部セキュリティ : Active Directory（第 6 章）

追加のセキュリティ・オプション

コンテンツ管理システムでは、認証方式を組み合せることができます。たとえば、Content Server に複数のローカル・ユーザーを定義し、一部のユーザーには Microsoft のドメイン ID を使用したログインを許可し、その他のユーザーには Active Directory または LDAP 資格証明に基づいて Content Server のアクセス権を付与できます。次のオプションを使用して、追加のセキュリティを提供できます。

- 無効または破損したHTML構成のデータ入力をフィルタ処理するようContent Serverをカスタマイズできます。詳細は、2-7 ページの「データ入力フィルタ」を参照してください。
- セキュリティ統合がマスター・コンテンツ・サーバーとは異なるプロキシ・コンテンツ・サーバーを使用できます。たとえば、マスター投稿サーバーには内部ユーザーのみを定義し、プロキシ消費サーバーには LDAP セキュリティ統合を設定できます。また、プロキシ接続を使用することで、資格証明マッピングやマスター・サーバーとプロキシ・サーバー間の HTTP プロトコル通信を設定し、複数のコンテンツ・サーバー上のエンタープライズ検索をサポートできます。詳細は、第 8 章「プロキシ接続」を参照してください。
- ユーザーが異なる Web サーバー・フロントエンド（一方のサーバー・フロントエンドは HTTPS でもう一方は HTTP）を使用して Content Server にアクセスできるようにする場合は、BrowserUrlPath コンポーネントを使用して構成をカスタマイズできます。このコンポーネントは、Content Server のインストール時にインストールおよび有効化できます。このコンポーネントは、HTTPS を使用する Web サーバー・フロントエンド、および HTTP ホスト・ヘッダーとして転送されるロード・バランサをサポートします。1 つのアクセス方法のみ（HTTPS のみまたは HTTP のみ）を使用する場合や、ブラウザからのホスト・パラメータをブロックするロード・バランサを使用していない場合は、このコンポーネントは不要です。詳細は、2-9 ページの「ブラウザ URL のカスタマイズ」を参照してください。
- セキュリティ・プロバイダ・コンポーネントを使用して、Web 通信の暗号化や認証をサポートするようにセキュリティをカスタマイズできます。このコンポーネントを使用すると、ソケットまたはサーバーの認証に証明書を使用するように構成できる Secure Socket Layer（SSL）プロバイダが有効化されます。

注意 : Content Server への接続に SSL および HTTPS を使用していて、WebDAV を介して接続できない場合は、WebDAV 接続文字列に使用したのと同じ URL を使用してブラウザからコンテンツ・サーバーへの接続を試行してください。これにより、通信の暗号化に使用する証明書に問題があるかどうかが確認できます。証明書の問題が記載されたダイアログ・ボックスが表示された場合は、問題を解決して、WebDAV を介した接続を再試行します。

技術ヒント : どのような環境においても、セキュリティ統合を成功させるには、組織のセキュリティのニーズを包括的に理解し、綿密に計画することが非常に重要です。コンテンツ・サーバーのセキュリティの詳細は、『Planning and Implementation Guide』および『Getting Started Guide』を参照してください。また、セキュリティ・モデルの計画および実装時にさらにサポートが必要な場合には、コンサルティング・サービスに連絡することをお薦めします。

ログイン / ログアウトのカスタマイズ

注意 : この機能は、Content Server のインストール時に ExtranetLook コンポーネントをインストールおよび有効化した場合にのみ使用できます。

Content Server で使用可能な ExtranetLook コンポーネントは、2 つの方法でユーザー・アクセスをカスタマイズするために使用できます。Cookie ベースのログイン・フォームやページを有効化する方法、および Content Server に認証されていないユーザー用のインタフェースを Web サーバーにより発行されるエラー・ページやチャレンジ・ページを使用して抑止する方法です。この項では、Cookie ベースの認証およびログアウトの設定について説明します。インタフェースの変更の詳細は、『Modifying the Content Server Interface』を参照してください。

デフォルトのユーザー認証では、カスタマイズまたはログアウト機能は許可されていません。Content Server セッションを終了するには、ブラウザ・セッションを終了する必要があります。組込みの Web サーバー・プラグイン `CookieLoginPlugin.dll` で、リクエストを監視し、リクエストが Cookie の設定に基づいて認証されているかどうかを判断できます。ユーザー認証が Cookie ベースの場合、ログアウト機能は、ブラウザ・セッションを終了せずに実装できます。

Cookie ベースの認証を有効化するには、*<Install_Dir>*/config/config.cfg ファイルに次の構成変数を設定します。

- `CookieProxyPassword`: ユーザーが Cookie ベースの認証を使用して Web サイトにログインした場合に、パスワードの暗号化に使用されます。任意の値に変更できます。
- `CookieAuthTimeoutInDays`: 正の値に設定されている場合、Cookie はその日数の間タイムアウトしません。ゼロ（0）以下の値は、Cookie がブラウザ・セッションの間

のみ存続することを指定します。値が正の値に設定されている場合は、ログアウト・オプションで Cookie を消去する必要があります。

タイムアウトを短くする必要がある場合は、構成変数 `CookieAuthTimeoutInMins` を使用して分単位で時間を指定できます。この変数は、Web サーバー・プラグイン `CookieLoginPlugin.dll` のリリース 10.1.3.3.0 以降でのみ使用可能です。ただし、旧リリースの Content Server でも使用できます。

- `IsWebServerPagesOnly`: カスタマイズまたはログアウト機能を使用できないBasic認証の設定に使用されます。`IsWebServrePagesOnly` を `TRUE` に設定することで、Web サーバー・プラグインの機能を削減できます。

プラグイン `CookieLoginPlugin.dll` の名前を変更する場合は、`iapFileNameRoot` エントリである `CookieLoginPlugin` を新しい名前に変更する必要があります。`iapFileNameRoot` エントリは、拡張子またはディレクトリ・パスのない `.dll`、`.so` または `.sl` ファイルの名前です。拡張子およびディレクトリの両方が、ネイティブのオペレーティング・システムの機能に基づいて、Web サーバー・フィルタによって計算されます。`iapFileNameRoot` エントリは、*<Install_Dir>*/custom/ExtranetLook/resources ディレクトリの extranetlook_resource.hda ファイルに配置されています。

ログイン / ログアウト構成のカスタマイズには、次のファイルを使用できます。

- access_denied.htm
- login_page.htm
- prompt_login.htm
- redirect_after_url.htm
- report_error.htm

これらのファイルには、`<!--$ParameterName-->` という書式のパラメータがあり、HTTP ヘッダー、フィルタ内の計算済の変数、構成パラメータの参照を可能にします。

注意 : これらのファイルで使用できるのは、置換および単純な IF 条件文のみです。条件文でテストできるのは 1 つの変数のみで、ELSE または ELSEIF 構成はサポートされていません。プラグイン・フィルタでは、Cookie ベースのログインに対してその他の Idoc スクリプト機能はサポートされていません。具体的には、INCLUDE は**サポートされていません。**

注意 : Cookie ベースの認証は、特定の状況では十分に機能しません。たとえば、Cookie ベースの認証を使用して sysadmin としてログインし、コンテンツ・サーバーにインストールするコンポーネントのアップロードを試行した場合、管理サーバーではコンポーネントのアップロードに、ログイン時に使用したホスト・アドレスとは異なるホスト・アドレスが使用されるため、アップロードが実行されません。

変数およびコンポーネントの有効化の詳細は、『Idoc Script Reference Guide』および使用しているオペレーティング・システム向けの Content Server のインストレーション・ガイドを参照してください。Content Server インタフェースのルック・アンド・フィールの変更の詳細は、『Modifying the Content Server Interface』を参照してください。

データ入力フィルタ

`encodeHtml` Idoc スクリプト機能およびフィルタ・フックを使用することで危険な HTML 構成のすべての入力データを自動的に修正し、無効または破損した HTML 構成のデータ入力をフィルタ処理するように Content Server をカスタマイズできます。`encodeHtml` 関数は特定の文字列に適用できます。`HtmlDataInputFilterLevel` 構成変数は、あるレベルのエンコーディングを適用して、Content Server へのすべてのデータ入力をフィルタ処理するために使用できます。

次の項を参照してください。

- encodeHtml 関数（2-7 ページ）
- HtmlDataInputFilterLevel 構成変数（2-8 ページ）

encodeHtml 関数

`encodeHtml` Idoc 関数は、無効または破損した HTML 構成のデータ入力をフィルタ処理するために使用できます。出力はエンコードされた文字列です。`encodeHtml` 関数は、スレッド・ディスカッション・コンポーネントのディスカッションにデフォルトで適用されます。

`HtmlDataInputFilterLevel` 構成変数は `unsafe` としてエンコードされているため、`encodeHtml` 関数は、一般的に `exceptsafe` 以上のレベルのエンコーディングで使用されます（デフォルト構成が使用されている場合）。

`encodeHtml` 関数の定義は次のとおりです。

`encodeHtml` (*string, rule, wordbreakrules*)

- **string:** エンコードする文字列。
- **rule:** HTML 構成をエンコードする際に適用するルールです。次の値を使用できます。
  - `none`: HTML 構成は変換されません。
  - `unsafe`: 既知の安全ではないスクリプト・タグのみがエンコードされます。リストに含まれているのは、script、applet、object、html、body、head、form、input、select、option、textarea です。
  - `exceptsafe`: 既知の安全なスクリプト・タグのみがエンコードされません。リストに含まれているのは、font、span、strong、p、b、i、br、a、img、hr、center、link、blockquote、bq、fn、note、tab、code、credit、del、dfn、em、h1、h2、h3、h4、h5、blink、s、small、sub、sup、tt、u、ins、kbd、q、

person、samp、var、ul、li、math、over、left、right、text、above、below、bar、dot、ddot、hat、tilde、vec、sqrt、root、of、array、row、item です。

- `lfexceptsafe:` （ユーザーにより拡張コメントが入力され、コメントで元のテキストのライン・フィードによる改行を保持する必要がある場合にお薦めします。）`exceptsafe` に似ていますが、ライン・フィード（ASCII 10）文字が HTML の改行タグ（br）に変換されます。HTML タグ内のライン・フィードは、改行タグに変換されません。`exceptsafe` で安全とみなされる br、p、ul、li のスクリプト・タグは、`lfexceptsafe` では安全とみなされません。

rule の `none` を除き、すべてのルールには独特の HTML コメントの処理方法があります。具体的には、すべての HTML コメントはフィルタを介して許可されます。ただし、HTML コメント内の < （より小さい）および > （より大きい）の記号はすべてエンコードされます。これは、HTML の終了記号（-->）には適用されません。また、終了していないコメントがある場合、エンコード機能により、HTML のコメントの終了記号（-->）が追加されます。

また、rule の `none` 以外、タグ内に配置された属性値では、カッコは `%28`（左カッコ）または `%29`（右カッコ）にエンコードされます。それ以外の場合、エスケープされている文字は、XML（`&xxxx;`）タイプ・エンコーディングを使用してエスケープされます。

wordbreakrules: 空白文字のない長い文字列を改行するかどうか、および適用する最大ワード・サイズを指定するオプションのパラメータです。文字列 `wordbreak` または `nowordbreak` を指定できます。このパラメータは、`encodeHtml` の任意のルールとともに使用できます。デフォルトでは、rule に `lfexceptsafe` が指定されている場合は `wordbreak` が有効化され、`maxlinelength` の 120 文字が使用されます。

追加のパラメータ `maxlinelength=`*xxx* は、`wordbreak` パラメータとともに使用して、必要な最大の行の長さを指定できます。次に例を示します。

```
encodeHtml ("exceptsafe", "<bad> text", "wordbreak, maxlinelength=80")
```

`encodeHtml` 関数は表示用に使用され、データが保存される前には適用されないため、`wordbreak` 機能はこの関数でのみ使用可能です。

Idoc スクリプトの詳細は、『Idoc Script Reference Guide』を参照してください。

HtmlDataInputFilterLevel 構成変数

`HtmlDataInputFilterLevel` 構成変数は、あるレベルのエンコーディングを適用して、不正な HTML 構成に関する Content Server へのすべての入力データをフィルタ処理するために使用できます。std_resources.htm ファイルの HtmlDataInputEncodingRulesForSpecialFields 表は、特別な場合のエンコーディング・ルールに使用され、特定のパラメータのこの構成エントリを上書きする場合があります。

注意 : `HtmlDataInputFilterLevel` 値を変更した場合は、Content Server を再起動する必要があります。

`HtmlDataInputFilterLevel` 変数を使用しても、Idoc スクリプトの `encodeHtml` 関数の動作に影響はありません。

`HtmlDataInputFilterLevel` 構成変数は次の値に設定できます。

- `none:` （非推奨。）すべてのフィルタ処理が無効化されます。
- `unsafe:` （デフォルト。推奨。）不正な HTML 構成から保護されます。不正な構成の例は、script、applet、object、html、body、head、form、input、select、option、textarea です。
- `exceptsafe:` （非推奨。）フィルタを介して既知の安全な構成のみが許可されます。`exceptsafe` を選択すると、GET スタイル・リクエストを使用したリクエストに `unsafe` オプションが適用されます。GET リクエストにこれより高いレベルのエンコーディングを実行すると、<$...$> およびその他のタグがパラメータ・データまたは URL の一部として定期的に渡されるため、Content Server の操作が分断されます。より高レベルのフィルタ処理は、スクリプト化できないサービス（通常 POST を使用してコールされるサービス）にのみ適用されます。

  既知の安全な構成の例は、font、span、strong、p、b、i、br、a、img、hr、center、link、blockquote、bq、fn、note、tab、code、credit、del、dfn、em、h1、h2、h3、h4、h5、blink、s、small、sub、sup、tt、u、ins、kbd、q、person、samp、var、ul、li、math、over、left、right、text、above、below、bar、dot、ddot、hat、tilde、vec、sqrt、root、of、array、row、item です。

HTML コメントの処理に関する情報は、encodeHtml 関数（2-7 ページ）の rule の説明を参照してください。この説明は、`HtmlDataInputFilterLevel` 構成変数にも当てはまります。

注意 : `HtmlDataInputFilterLevel` 構成変数では、値 `lfexceptsafe` はサポートされていません。encodeHtml 関数でのみサポートされています。

ブラウザ URL のカスタマイズ

注意 : この機能は、Content Server のインストール時に BrowserUrlPath コンポーネントをインストールおよび有効化した場合にのみ使用できます。

BrowserUrlPath コンポーネントは、Oracle Content Server および Web サーバーの特定の構成で使用される URL パスの特定をサポートします。

この項の内容は次のとおりです。

BrowserUrlPath のカスタマイズについて

このコンポーネントにより、特定の Idoc スクリプト変数および関数の上書き、特定の変数に対する計算の追加、および URL パスを判断するための追加の構成エントリの提供が行われます。

- 異なる Web サーバー・フロントエンドを使用してシステムを構成できます。一方のフロントエンドには HTTP を使用し、もう一方には HTTPS を使用できるため、HTTP および HTTPS を使用して複数の Web サイトから同時に Content Server にアクセスできます。BrowserUrlPath コンポーネントを適用して、Content Server でどちらのタイプのアクセスも処理できるようにする必要があります。
- HTTP ホスト・ヘッダーとして転送されるロード・バランサを使用している場合は、BrowserUrlPath コンポーネントを適用する必要があります。

BrowserUrlPath 構成変数は、*<instance>*/custom/components/browserurlpath/config.cfg ファイルにあります。

警告 : BrowserUrlPath コンポーネントには、変数を使用した拡張構成が必要です。変数を変更する前に構成をバックアップすることをお薦めします。

注意 : BrowserUrlPath コンポーネントは、Content Server ユーザー・インタフェースの「Trays」および「Top Menu」レイアウトでのみサポートされています。「Classic」レイアウトではサポートされていません。

一般的なシナリオでは、Web サーバーにより、2 つの重要な情報が Content Server に転送されます。

- HTTP_HOST: ブラウザにより送信されるホスト・ヘッダー。ブラウザのアドレス・バーに表示される際にホストを識別します。
- SERVER_PORT: Content Server への接続時にブラウザにより使用されるポート。

2 つの重要な機能には、ブラウザ・ベースの完全なアドレスが使用されます。

1. Content Server の「Trays」レイアウトの左フレームにおける URL の自動作成。特に、左フレームのミニ検索では、相対 URL ではなく完全な URL を予測する必要があります。
2. PDF ドキュメントを強調表示する 2 番目の URL（PDF の URL に続く #xml-http... の部分）。

BrowserUrlPath コンポーネントにより、追加の構成なしで特定の変数の機能が強化され、SERVER_PORT の値が 433 の場合、コンポーネントではプロトコルは HTTP ではなく HTTPS であると推測されます。同様に、SERVER_PORT の値が 433 ではない場合、コンポーネントでは、ブラウザが HTTPS ではなく HTTP を使用してリクエストを発行したと推測されます。この拡張により、SSL（HTTPS）および非 SSL の WEB サーバー（HTTP）の両方から、同じ Content Server にアクセスできます。

このコンポーネントには、WebDAV アクセスに関する特別な機能もあります。構成エントリ WebDavBaseUrl が追加されたため、動的に使用されます（ホストおよびプロトコルが絶対パス・ルールを使用して変更されます）。

警告 : WebDAV アクセスの機能により、一部の Content Server のページにおける CHECKOUT と OPEN 関数の動作、および Site Studio クライアントの一部の動作が変更されます。

影響を受ける Idoc スクリプト変数および関数

BrowserUrlPath コンポーネントは、次の Idoc スクリプト変数および関数の計算を上書きします。

- HttpBrowserFullCgiPath
- HttpWebRoot
- HttpCgiPath
- HttpEnterpriseWebRoot
- HttpEnterpriseCgiPath
- HttpAdminCgiPath
- HttpImagesRoot
- proxiedCgiWebUrl
- proxiedBrowserFullCgiWebUrl

BrowserUrlPath コンポーネントにより、次の変数に計算が追加されます。

- `HttpBrowserFullWebRoot`: ユーザーが現在使用しているブラウザのアドレス・バーから提供される値を使用して、現在の Content Server の Web ルートへの完全な URL パスを定義します。この変数は、Web ルート用であることを除き `HttpBrowserFullCgiPath` に似ています。
- `HttpAbsoluteWebRoot`: 現在のContent ServerのWebルートへの汎用の完全なURLパスを定義します。`HttpBrowerFullWebRoot` のパスとは異なるプロトコルまたはホスト名を使用できます。たとえば、ユーザーがホスト名の IP アドレスを指定した場合、`HttpBrowserFullWebRoot` 変数ではその IP アドレスが使用されますが、`HttpAbsoluteWebRoot` 変数では無視され、内部的に構成された適切なホスト名が使用されます。
- `HttpAbsoluteCgiPath`: 現在のContent Serverの汎用の完全な動的ルートURLを定義します。これは、Content Server の動的コンテンツをコールする Web サーバーでプラグイン・コードを実行するパスです。`HttpBrowserFullCgiPath` のパスとは異なるプロトコルまたはホスト名を使用できます。たとえば、ユーザーがホスト名の IP アドレスを指定した場合、`HttpBrowserFullCgiPath` 変数ではその IP アドレスが使用されますが、`HttpAbsoluteCgiPath` 変数では無視され、内部的に構成された適切なホスト名が使用されます。
- `HttpAbsoluteEnterpriseWebRoot`: プロトコル、ホスト名およびオプションでポート番号のみを含む汎用の完全な URL パスを定義します。`HttpEnterpriseWebRoot` のパスとは異なるプロトコルまたはホスト名を使用できます。たとえば、ユーザーがホスト名の IP アドレスを指定した場合、`HttpEnterpriseWebRoot` 変数ではその IP アドレスが使用されますが、`HttpAbsoluteEnterpriseWebRoot` 変数では無視され、内部的に構成された適切なホスト名が使用されます。

ブラウザ・パス変数 `HttpBrowserFullCgiPath` および `HttpBrowserFullWebRoot` の場合、ユーザーが現在使用しているブラウザのプロトコル（HTTP と HTTPS）、ポート番号およびホスト名は実装コードにより判断されます。この判断は、Web サーバーがリクエストで何を受信するかに基づいています。

URL パスの判断

BrowserUrlPath コンポーネントでは、ブラウザが URL パスを判断する際にそれを推測するための次の構成エントリがサポートされています。

- `HttpIgnoreWebServerInternalPortNumber`: true に設定すると、SERVER_PORT パラメータを使用できなくなります。このエントリは、SERVER_PORT がブラウザで使用されるポートではなく、Web サーバーと通信するためにロード・バランサで使用されるポートであるロード・バランシングのシナリオに便利です。このエントリを有効化すると、Content Server は（BrowserUrlPath コンポーネントなしでは）ブラウザが Web サーバーへのアクセスに使用したポートを判断できなくなります。追加の BrowserUrlPath 構成がない場合、この変数が原因で、同じ Content Server への

SSL および非 SSL アドレスの両方をサポートできなくなります。この変数を使用すると、ロード・バランシング・サーバーで、内部 Web サーバーが実際にリクエストへのレスポンスの配信に使用しているものとは異なるポート番号が使用されるというロード・バランシング構成の問題を防ぐことができます。

- `HttpIgnoreServerNameForHostName`: true に設定すると、HTTP_HOST パラメータが欠落している場合に、Content Server はパラメータ SERVER_NAME（Web サーバーの自己識別）を検索するというフォールバック・ロジックが無効化されます。
- `HttpBrowserSSLPort`: この構成エントリは、SERVER_PORT エントリが Content Server と通信する Web サーバーに転送される場合にのみ使用します。このエントリは、SERVER_PORT パラメータと比較することで、リクエストが HTTPS と HTTP のいずれであるかを判断する際に使用されます。デフォルトの SERVER_PORT の値は 443 です。HTTPS を使用するが 443 以外のポートを使用する場合は、使用する HTTPS のポート番号をこのエントリを使用して設定する必要があります。
- `HttpBrowserUseIsSslCookie`: SSL を使用するかどうかが特定されていることを確認するために Cookie を調査する必要がある場合は、このエントリを true に設定します。
- `HttpBrowserIsSslCookieName`: このエントリは、`HttpBrowserUseIsSslCookie` エントリが有効化されている場合にのみ使用します。ブラウザで SSL が使用されているかどうかをサーバーが判断するために使用される Cookie の名前にこのエントリを設定します。デフォルトは Cookie 名 `UseSSL` です。Cookie の値は 1 または 0（ゼロ）です。この名前の Cookie が存在する場合には、SSL を使用するかどうかを判断するためのその他のルールより優先されます。
- `HttpBrowserUseHostAddressCookie`: true に設定すると、ブラウザの完全なホスト名（プロトコルおよび相対 Web アドレスの間の部分）の判断に Cookie を使用することが指定されます。
- `HttpBrowserHostAddressCookieName`: このエントリは、`HttpBrowserUseHostAddressCookie` が有効化されている場合にのみ有効化されます。このエントリは、サーバーがブラウザの現在のホスト名であると判断した内容の確認に使用される Cookie 名の指定に使用します。プロトコルのホスト名の部分には、ポート番号が含まれる場合があります。たとえば、`HttpbrowserHostAddressCookieName=myhost:81` では、Web ポート `81` を使用するホスト `myhost` が指定されています。この Cookie を使用する場合、`myhost:433` を使用すると `https://myhost/%rest-of-url%` に変換されるため、`HttpBrowserUseIsSslCookie` を有効化する必要はありません。

絶対フルパスの計算の変更

BrowserUrlPath コンポーネントでは、絶対フルパスの計算方法を変更するための次の構成エントリがサポートされています。ブラウザで別の URL が示されていても、固有のホスト名とプロトコルを使用する方がよい電子メールに便利です。このパスは、絶対または汎用パスとみなされます。

- `HttpBrowserAbsoluteUrlHasRelativeSSL`: true に設定すると、Content Server がユーザーのブラウザで現在使用されていると判断した内容に応じ、HTTP から HTTPS（config.cfg ファイルで `UseSSL` が有効化されている場合は HTTPS から HTTP）に変更するために、「Content Info」ページで URL を計算できるようになります。HTTP と HTTPS を変更すると、複数の電子メール宛先リンクに対して電子メール本体を作成するための URL の計算も変更されます。この構成は、自動的に生成される電子メールには影響しません。
- `HttpBrowserAlternateWebAddress`: 代替の絶対ホスト Web アドレス（ホスト名およびオプションでポート番号）を指定します。
  `HttpBrowserAlternateWebAddresss=<host_name>:447` などです。この Web アドレスは、現在の SSL の選択が Content Server のデフォルトと異なる場合に、絶対パスの計算に使用されます。この構成は、自動的に生成される電子メールには影響しません。
- `HttpBrowserAbsoluteUrlUsesBrowser Path`: true に設定すると、ブラウザ・パス情報が計算される場合、絶対パスにブラウザ・パスが使用されます。これにより、基本的に、バックグラウンド・アクティビティ（通知電子メールの送信など）を除く絶対パスが無効化されます。

管理パスの計算の変更

BrowserUrlPath コンポーネントでは、「Administration」トレイまたは上部のメニュー・リンクのパスの計算方法を変更するための次の構成エントリがサポートされています。たとえば、管理パスは、管理サーバーの CGI を管理サーバーへの相対 URL として取得する変数 `HttpAdminCgiPath` により計算されます。

- `HttpBrowserAdminUsesAbsolutePath`: true に設定すると、構成変数 `HttpBrowserUseAdminSSL` により決定されるプロトコルを除き、ブラウザ・ベースのパス（BrowserUrlPath コンポーネントのデフォルト）を使用するかわりに、管理パスの計算のベースとして絶対パスが使用されます。
- `HttpBrowserUseAdminSSL`: この構成エントリは、`HttpBrowserAdminUsesAbsolutePath` 変数が設定されている場合にのみ関連します。true に設定すると、`HttpBrowserAbsoluteUrlHasRelativeSSL` が設定されている場合でも、この変数により管理パスのプロトコル（HTTP または HTTPS）が決定されます。
  `HttpBrowserUseAdminSSL` のデフォルト値は、`UseSSL` の反対の値です。これにより、管理パスは、その他すべてのパスに対するデフォルトの URL 構成の標準ではなくなります。変数 `HttpBrowserAlternateWebAddress` が設定されている場合には、

`HttpBrowserUseAdminSSL` が `UseSSL` の反対の値に設定されている際に、この変数を使用して管理パスに別の Web アドレスを指定できます。

変数および BrowserUrlPath コンポーネントの有効化の詳細は、『Idoc Script Reference Guide』および使用しているオペレーティング・システム向けの Content Server のインストレーション・ガイドを参照してください。

セキュリティの推奨事項

Content Server インスタンスの全体的なセキュリティを向上させるための推奨事項を示します。Content Server を完全に保護するために、4 つのタイプのセキュリティを使用することをお薦めします。

❖ **ディレクトリ構造へのアクセス :** アクセスが必要なオペレーティング・システム・アカウントにのみアクセスを許可するために、ファイル・システムを保護します。

- 読取り権限 : ログ・ファイルを確認するシステム管理者、および通常のバックアップや定期的な障害リカバリ・バックアップを実行する必要のあるユーザーに読取り権限を指定します。

  また、コンテンツ・サーバーにアクセスし、コンテンツ・サーバーの Web サイトからユーザーのブラウザにファイルを配信する Web サーバーを実行するアカウントにも読取り権限を設定します。Web サイトには、weblayout ディレクトリ、data ディレクトリおよび idcplg ディレクトリにファイルが保存されています。Netscape Enterprise Server または MS ネットワーク・セキュリティ統合を使用せずに稼働している IIS の場合は、単一のオペレーティング・システム・アカウントです。Content Server が MS ネットワーク・セキュリティ統合で実行されている場合は、IIS によりシステムにアクセス中のユーザーのアカウントが想定されます。Web サーバーには、その他のディレクトリへのアクセス権は必要ありません。

- 書込み権限 : システム管理者に、新しいソフトウェアをインストールしてカスタマイズを実行するための書込み権限を指定します。Content Server およびオプションで Inbound Refinery への書込み権限を設定します（すべて同一のアカウント）。

その他のアカウントに Content Server ディレクトリ構造へのアクセス権を付与する必要はありません（データに直接アクセスするその他のプロセスを実行している場合を除く）。

- **ネットワーク・アクセス :** Content Server ディレクトリ構造への、Content Server アプリケーションによるアクセスのみを許可するようにネットワークを構成します。別のコンピュータ上のオプションの Inbound Refinery が Content Server ディレクトリにアクセスできるようファイルを共有する必要がある場合には、Inbound Refinery のみがそのディレクトリにアクセスできるように共有の設定を行う必要があります。

  data ディレクトリおよび config ディレクトリには、ユーザー名とパスワードが保存されています。これらのディレクトリは、ネットワーク上で共有しないでください。

  さらにセキュリティを強化するために、Web サーバーとの伝送は、Secure Socket Layer（SSL）を使用して暗号化する必要があります。

- **データベース・アクセス :** Content Server では、データベースに格納されたデータへのアクセスに単一のデータベース・アカウントが使用されます。解読されにくいデータベース・ユーザー名およびパスワードにして、定期的に更新する必要があります。

- **物理アクセス :** Content Server が実行されているサーバーは、鍵のかかる部屋に保管してください。

ユーザーのタイプ

ユーザーは、様々な方法で Content Server インスタンスにアクセスするよう設定できます。具体的には、次の 3 つのユーザー・ログイン・タイプを使用します。

- ローカル・ユーザー（2-16 ページ）
- グローバル・ユーザー（2-18 ページ）
- 外部ユーザー（2-18 ページ）

ローカル・ユーザー

ローカル・ユーザーは、管理者または副管理者によって Content Server システム内に定義されます。管理者はこれらのユーザーに 1 つ以上のロールを割り当てます。これにより、ユーザーにセキュリティ・グループへのアクセス権が付与されます。未定義のユーザーにはゲスト・ロールが割り当てられます。次の章では、ローカル・ユーザーを説明します。

- 第 3 章「内部セキュリティ : セキュリティ・グループ、ロールおよび権限」
- 第 4 章「内部セキュリティ : アカウントの使用」
- 第 5 章「内部セキュリティ : ユーザー・ログインおよび別名の割当て」

次に、ローカル・ユーザーの一般的な特性を示します。

- **ログイン作成者 :** 管理者 / 副管理者によって、Content Server インスタンス内に作成されます。資格証明は、複数の Content Server インスタンスに適用されます。
- **アクセスの指定 :** Content Server ロールによって、セキュリティ・グループへのアクセス権が付与されます。
- **ユーザー・ログイン :** ユーザーが管理サーバーにログインする際に、Content Server が実行されている必要はありません。ユーザーは、サーバーの相対 URL を使用してプロキシ・サーバーにログインできます。次に例を示します。

  username<proxied_server>/<local_user_on_proxied_server>
- **ユーザー・パスワード :** ユーザーはパスワードを変更できます。
- **インタフェースについて :** コンテンツのチェックイン・リストにユーザー名が表示されます。ユーザーは、フルネーム、電子メール・アドレスおよびユーザー・タイプを変更するかどうかを指定できます。
- **推奨 :** ユーザー数が 1000 以下の場合。

注意 : パフォーマンス上の問題から、1000 を超えるローカル・ユーザーを構成しないでください。

コンテンツ・サーバーでは約 1000 のローカル・ユーザーを処理できますが、それを超えるとパフォーマンスの問題が発生する可能性があります。大規模なエンタープライズ・ユーザー・ベースでは、検証が常に動的に実行されるグローバル・タイプのユーザーが作成されます。グローバル・ユーザーの資格証明は Web サーバーのセキュリティ・フィルタにはパブリッシュされないため、データベース表に問い合せることによってマスター・サーバーは資格証明を常に検証します。このため、グローバル・ユーザーとしてログインするには、マスター・サーバーが設定されている必要があります。

ローカル・ユーザーを設定するには、次の手順を実行します。

1. セキュリティ・グループを設定します。詳細は、3-5 ページの「セキュリティ・グループの追加」を参照してください。
2. ロールを設定します。詳細は、3-10 ページの「ロールの作成」を参照してください。
3. 権限を割り当てます。詳細は、3-12 ページの「権限の追加および編集」を参照してください。
4. ユーザー・ログインを割り当てます。詳細は、5-4 ページの「ユーザー・ログインの追加」を参照してください。
5. アカウントを使用します（オプション）。詳細は、4-7 ページの「アカウントの有効化」を参照してください。

グローバル・ユーザー

グローバル・ユーザーは簡単に管理できるユーザーで、その資格証明は複数のコンテンツ・サーバーに適用されます。グローバル・ユーザーの情報は、マスター・コンテンツ・サーバーにのみ保存されます。

グローバル・ユーザーの概念は、ローカル・ユーザーのスケーラビリティの問題に対応するために作成されました。ユーザー数が 500 を超える場合、「Author」オプション・リストが長くなりすぎて効率的に名前を選択できなくなります。そのため、ユーザーのリストをフィルタ処理する方法が必要になります。これは、「Organization Path」フィールドを使用して行います。このフィールドには、ユーザーに割り当てられている追加の情報を含めることが可能なため、その情報でフィルタ処理できます。「Organization Path」の詳細は、5-13 ページの「「Add User」/「Edit User」画面 :「Info」タブ（グローバル・ユーザー）」を参照してください。

次に、グローバル・ユーザーの一般的な特性を示します。

- **ログインの定義 :** 複数のコンテンツ・サーバーに適用される資格証明によって定義されます。自動登録されたユーザーはグローバル・ユーザーです。
- **アクセスの指定 :** マスター・インスタンスに設定された Content Server ロールによって、複数のインスタンスにまたがるセキュリティ・グループへのアクセス権が付与されます。
- **ユーザー・ログイン :** ユーザーがログインするにはマスター・コンテンツ・サーバーが実行されている必要があります。
- **インタフェースについて :** ユーザー名は、コンテンツのチェックイン・リストに表示されません。ユーザーは、フルネーム、電子メール・アドレスおよびユーザー・タイプを変更する場所を指定できます。
- **推奨 :** ユーザー数が 1000 を超えるエンタープライズ、または自動登録が実装されている場合。

グローバル・ユーザーを設定するには、次のようにします。

1. マスター・サーバーおよびプロキシ・サーバー構成を設定します。詳細は、第 8 章「プロキシ接続」を参照してください。
2. マスター・サーバー・ログインを使用して、ユーザーをシステムにログインさせます。

外部ユーザー

外部ユーザーは Content Server システム外に定義され、外部セキュリティを介して認証されます。システムに自動的に登録され、管理者が手動で設定していない外部ユーザーは、Microsoft ログインまたはその他のタイプのプロバイダ・ログイン（LDAP など）を使用します。

一般的に、これらは信頼できるドメインに存在するユーザーで、アクセス権を付与し、Content Server を使用しないで管理します。これらのユーザーのパスワードは、Microsoft ネットワーク・ドメインまたはその他のタイプのプロバイダにより所有されます。ローカル・ユーザーとは異なり、未定義の外部ユーザーにはゲスト・ロールは割り当てられません。

次に、外部ユーザーの一般的な特性を示します。

- **ログインの定義 :** 次に示す外部ユーザー・データベースへの追加により定義されます。
  - 信頼できるドメイン /Microsoft
  - LDAP
  - その他のデータベース
- **アクセスの指定 :** 信頼できるドメインまたはその他のユーザー・ベース（LDAP など）からの資格証明によって決定されます。
- **ユーザー・ログイン :** ユーザーがログインするには Content Server が実行されている必要があります。
- **ユーザー・パスワード :** ユーザーはパスワードを変更できません。
- **インタフェースについて :** ユーザー名は、コンテンツのチェックイン・リストに表示されません。ただし、ユーザーはワークフローに参加できます。
- **推奨 :** 外部ユーザー・ベースと統合する場合。次に例を示します。
  - 信頼できるドメイン /Microsoft ログイン
  - Active Directory Server
  - LDAP
  - その他のユーザー・データベース

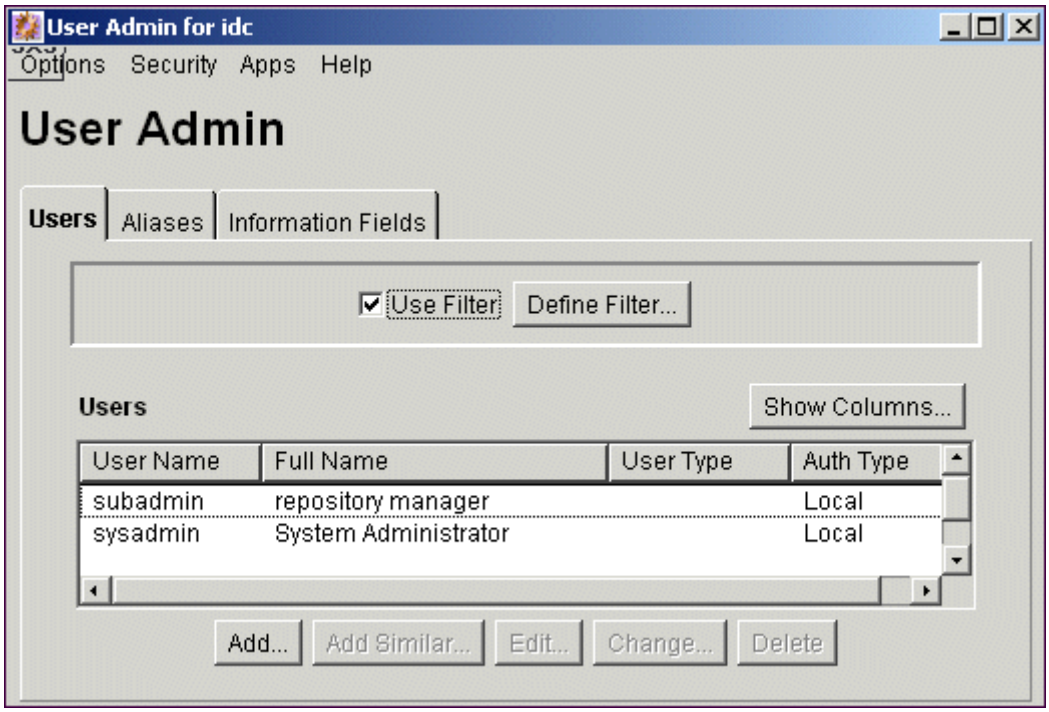
外部ユーザーの追加の詳細は、第 6 章「外部セキュリティ : Active Directory」および第 7 章「外部セキュリティ : LDAP」を参照してください。

セキュリティ管理インタフェース

次に、セキュリティを管理する際に使用するメイン画面を示します。

- ユーザー管理アプリケーション（2-20 ページ）
- 「Define Filter」画面（2-22 ページ）
- 「Show Columns」画面（2-24 ページ）

ユーザー管理アプリケーション



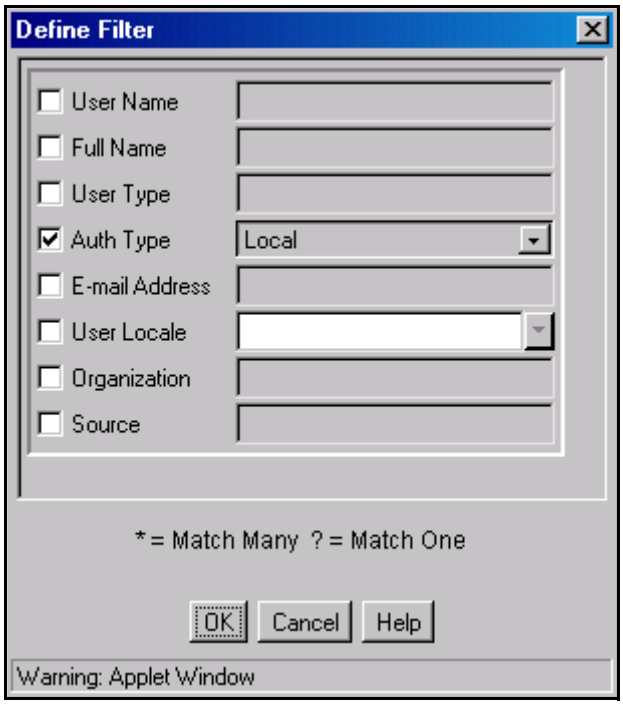
ユーザー管理アプリケーションは、ユーザー、セキュリティ・グループ、アカウントの設定および管理に使用する管理アプリケーションです。このアプリケーションは、「Administration」ページから、またはスタンドアロン・モードでアクセスして実行できます。詳細は、1-6 ページの「アプレットとしてのアプリケーションの起動」または 1-7 ページの「スタンドアロン・モードでのアプリケーションの実行」を参照してください。

注意 : スタンドアロン・モードでアクセスしてユーザー管理アプリケーションを実行すると、ADSI 認証済ユーザーが資格証明を失う場合があります。

機能	説明
「Options」メニュー	**Tracing:** 「Tracing Configuration」画面が表示されます。この画面では、システム全体のトレースに関する機能を実行できます。 **Exit:** ユーザー管理アプリケーションを終了します。

機能	説明
「Security」メニュー	次の内容を設定するオプションが表示されます。 **Permissions by Group:** 「Permissions By Group」画面（3-13 ページ）が表示されます。 **Permissions by Role:** 「Permissions By Role」画面（3-15 ページ）が表示されます。 **Predefined Accounts:** 「Predefined Accounts」画面（4-11 ページ）が表示されます。このオプションは、アカウントが有効化されている場合にのみ使用できます。詳細は、4-7 ページの「アカウントの有効化」を参照してください。
「Apps」メニュー	その他の管理アプリケーションの起動に使用します。その他のアプリケーションは、現在のアプリケーションと同じモード（アプレットまたはスタンドアロン）で起動されます。
「Help」メニュー	**Contents:** Content Server のオンライン・ヘルプが表示されます。 **About Content Server:** Content Server のバージョン、ビルドおよびコピーライト情報が表示されます。
「Users」タブ	ユーザー・ログインの追加、編集および削除に使用します。詳細は、5-8 ページの「「User Admin」画面：「Users」タブ」を参照してください。
「Aliases」タブ	ユーザー別名の追加、編集および削除に使用します。詳細は、5-19 ページの「「User Admin」画面：「Aliases」タブ」を参照してください。
「Information Fields」タブ	ユーザー情報フィールドの追加、編集および削除に使用します。詳細は、5-32 ページの「「User Admin」画面：「Information Fields」タブ」を参照してください。

「Define Filter」画面

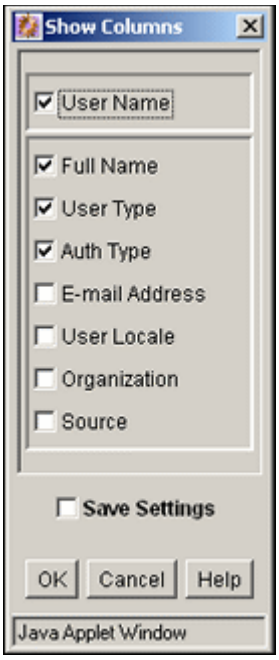


「Define Filter」画面は、いくつかの管理アプリケーション画面に表示される情報のリストを絞り込むために使用します。「Define Filter」画面には、管理アプリケーション画面に適用可能な一連のフィールドが表示されます。フィールドの隣にあるボックスを選択して、そのフィールドをフィルタとしてアクティブ化します。

この画面には、その他の様々な管理画面からアクセスできます。たとえば、「Define Filter」ボタンは、「User Admin」画面の一部である「Users」タブに表示されます。

機能	説明
チェック・ボックス	1 つ以上のチェック・ボックスを選択して、フィルタ・フィールドをアクティブ化します。
フィールド	入力した基準に基づいて、元の画面の「Users」リストがフィルタ処理されます。これらのフィールドでは、次のワイルドカードを使用できます。 • MS Access または MSDE の場合 : *: 1 つ以上の文字 ?: 単一の文字 • その他すべてのデータベースの場合 : %: 1 つ以上の文字 _: 単一の文字
「User Name」フィールド	ユーザー・ログイン。
「Full Name」フィールド	ユーザー・ログインに対応するフルネーム。
「User Type」フィールド	ユーザーの分類方法としてシステム管理者により定義される属性。
「Auth Type」フィールド	「Local」、「Global」または「External」のいずれかのユーザー認証タイプ。
「E-Mail Address」フィールド	ユーザーに関連付けられた電子メール・アドレス。ワークフローおよびサブスクリプションの通知に使用されます。
「User Locale」フィールド	ユーザーのロケール。これにより、ユーザー・インタフェースの言語および日付 / 時間の書式が指定されます。
「Organization」フィールド	ユーザーの組織パスの値。この値は、グローバル・ユーザーの分類方法としてシステム管理者により定義されます。
「Source」フィールド	ユーザー情報の取得に使用される LDAP ユーザー・プロバイダ。また、このフィールドでは、値が MSN の NTLM または ADSI 統合からユーザーを受け入れるかどうかを指定します。
「Custom」フィールド	任意のカスタム・ユーザー情報フィールドを、フィルタ・フィールドとして使用できます。

「Show Columns」画面



「Show Columns」画面は、いくつかの管理アプリケーション画面に表示する列の指定に使用します。「Show Columns」画面には、管理アプリケーション画面に適用可能な一連のフィールドが表示されます。フィールドの隣にあるボックスを選択すると、そのフィールドが管理画面の列として表示されます。

この画面には、その他の様々な管理画面からアクセスできます。たとえば、「Show Columns」ボタンは、「User Admin」画面の一部である「Users」タブに表示されます。

機能	説明
チェック・ボックス	**選択 :** フィールドが元の画面の「Users」リストに表示されます。 **選択解除 :** フィールドは「Users」リストに表示されません。 **注意 :** フィールドの説明は、2-22 ページの「「Define Filter」画面」を参照してください。
「Save Settings」チェック・ボックス	**選択 :** 元の画面が表示されるたびに、列設定が適用されます。 **選択解除 :** 列設定は、元の画面を閉じるまで適用されます。

セキュリティのアーキテクチャ

Content Server セキュリティの設定時には、システム・アーキテクチャの複数の側面を考慮する必要があります。Web サーバー、Web サーバー・フィルタおよびフィルタ・プラグインの詳細は、『Managing System Settings and Processes』を参照してください。

3

内部セキュリティ：セキュリティ・グループ、ロールおよび権限

概要

この項の内容は次のとおりです。

概念

タスク

- ユーザーへのロールの割当て（3-11 ページ）
- 権限の追加および編集（3-12 ページ）

インタフェース

- 「Permissions By Group」画面（3-13 ページ）
- 「Add New Group」画面（3-14 ページ）
- 「Edit Permissions」画面（3-16 ページ）
- 「Permissions By Role」画面（3-15 ページ）
- 「Add New Role」画面（3-16 ページ）

セキュリティ・グループについて

セキュリティ・グループは、一意の名前でグループ化された一連のファイルです。コンテンツ・サーバー・リポジトリ内の各ファイルはセキュリティ・グループに属します。セキュリティ・グループへのアクセスは、ユーザーに割り当てられるロールに割り当てられた権限によって制御されます。

セキュリティ・グループを使用すると、コンテンツ・ファイルを特定のユーザーのみがアクセス可能な個別のグループに編成できます。たとえば、人事指定のドキュメントを表す HRDocs という名前のセキュリティ・グループにファイルを割り当て、このグループには人事部で働く従業員のみがアクセスするようにできます。事前定義済のセキュリティ・グループが 2 つあります。

パブリック	デフォルトでは、すべてのユーザーがログインせずに、パブリック・グループのドキュメントを表示できます。
セキュア	システム・ファイルはセキュア・グループに格納され、システム管理者のみが使用できます。

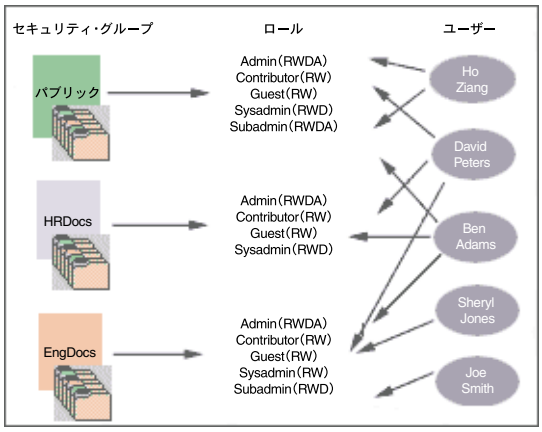
セキュリティ・グループの使用に関するヒント

セキュリティ・グループを定義する際は、次の考慮事項に注意してください。

重要 : セキュリティ・グループは、保護する必要のあるファイルがチェックインされる**前**に定義してください。

- 検索およびユーザー管理の効率を最適化するために、セキュリティ・グループの数は最低限に維持する必要があります。セキュリティ・モデルに 50 を超えるセキュリティ分類が必要な場合は、アカウントを有効化し、それらを使用してユーザー権限を制御する必要があります。数は、検索効率（3-4 ページ）およびユーザー管理効率（3-4 ページ）により異なります。
- 同じアクセスを共有するすべてのファイルを 1 つのセキュリティ・グループに含めます。
- セキュリティ・グループに論理ネーミング規則を設定します。たとえば、イントラネットを設定している場合は部門名を使用し、エクストラネットを設定している場合はセキュリティ・レベル（内部や分類済など）を使用します。

図 3-1　セキュリティ・グループの定義例



パフォーマンスの問題

セキュリティ・グループおよびロールに関するユーザー・アクセス設定は、システム効率の次の内容に影響する可能性があります。

- 検索効率（3-4 ページ）
- ユーザー管理効率（3-4 ページ）

検索効率

検索効率は、ユーザーがアクセス権を持つセキュリティ・グループの数に影響されます。ユーザーが表示権限を持つコンテンツのみを戻すには、データベースの WHERE 句にセキュリティ・グループのリストを含めます。WHERE 句には、ユーザーがアクセス権を持っているすべてのセキュリティ・グループ、またはアクセス権を持っていないすべてのセキュリティ・グループを含めます。どちらの方法にするかは、ユーザーの持っている権限が、定義されているセキュリティ・グループの 50% を超えているかまたは 50% に満たないかにより異なります。

たとえば、100 のセキュリティ・グループが定義されていて、ユーザーが 10 のセキュリティ・グループの権限を持っている場合は、WHERE 句に 10 のセキュリティ・グループを含めます。反対に、ユーザーが 90 のセキュリティ・グループへのアクセス権を持っている場合は、そのユーザーがアクセス権を持っていない 10 のセキュリティ・グループを WHERE 句に含めます。

そのため、ユーザーが 50% に近いセキュリティ・グループに対する権限を持っている場合、検索効率は低下します。ユーザーがすべてのセキュリティ・グループに対する権限を持っている場合、またはどのセキュリティ・グループに対する権限も持っていない場合は、検索効率が向上します。

ユーザー管理効率

セキュリティ・グループの合計数にロールの合計数を掛けた数が、RoleDefinition データベース表の行数になります。この数は、ユーザー管理アプリケーションのローカル・ユーザーに関連する作業効率に影響します。ユーザー管理アプリケーションにおける、セキュリティ・グループの追加やロールの権限の変更などの操作の実行に必要な概算の時間を判断するには、次の式を使用します。

（セキュリティ・グループ数）X（ロール数）/ 1000 = 秒単位の操作時間

たとえば、400MHz プロセッサ搭載で RAM が 128MB の PC を使用すると、RoleDefinition 表に 10,000 行ある場合、ユーザー管理アプリケーションを使用したセキュリティ・グループまたはロール（あるいはその両方）の追加には約 10 秒かかります。

セキュリティ・グループの数が増加すると、コンシューマの検索効率よりも管理効率が影響を受けます。

グループの管理

次のタスクは、セキュリティ・グループの管理に使用されます。

❖ セキュリティ・グループの追加（3-5 ページ）

❖ セキュリティ・グループの削除（3-5 ページ）

セキュリティ・グループの追加

セキュリティ・グループを作成して権限を割り当てるには、次のようにします。

1. ユーザー管理アプリケーション（2-20 ページ）で、「**Security**」→「**Permissions by Group**」を選択します。

   「Permissions By Group」画面（3-13 ページ）が表示されます。

2. 「**Add Group**」をクリックして、「Add New Group」画面（3-14 ページ）を表示します。
3. グループ名および説明を入力します。
4. 「**OK**」をクリックします。
5. セキュリティ・グループに権限を設定します。
   a. セキュリティ・グループを選択します。
   b. 編集するロールを選択します。
   c. 「**Edit Permissions**」をクリックします。
   d. グループのロールに必要な権限を有効化したら、「**OK**」をクリックして「Permissions by Group」画面を閉じます。

セキュリティ・グループの削除

セキュリティ・グループを削除するには、次のようにします。

1. 削除するセキュリティ・グループにコンテンツ・アイテムが割り当てられていないことを確認します。セキュリティ・グループにコンテンツが存在する場合は、そのセキュリティ・グループを削除できません。
2. ユーザー管理アプリケーション（2-20 ページ）で、「**Security**」→「**Permissions by Group**」を選択します。

   「Permissions By Group」画面（3-13 ページ）が表示されます。

3. 削除するグループを選択します。
4. 「**Delete Group**」をクリックします。

   確認画面が表示されます。

5. 「**Yes**」をクリックします。

   セキュリティ・グループが削除されます。

6. セキュリティ・グループを削除したら、「**OK**」をクリックして「Permissions by Group」画面を閉じます。

ロールおよび権限について

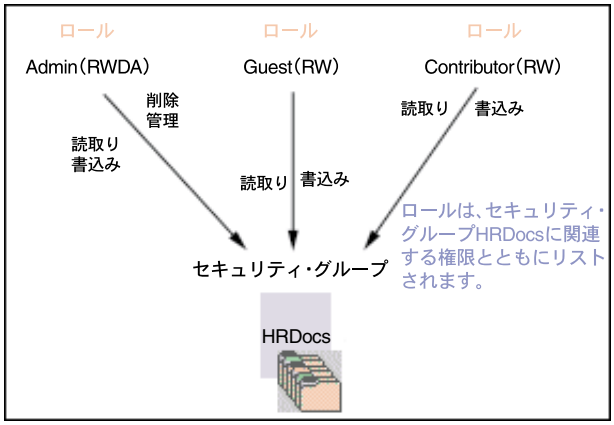
ロールは、各セキュリティ・グループに対する一連の権限（読取り、書込み、削除、管理）です。ロールはユーザーのジョブと考えられます。ユーザーは、様々なセキュリティ・グループに対して異なるジョブを持っています。ユーザーは、ユーザーが参加する異なるチームを識別するために、異なるジョブを持つこともできます。次のことが可能です。

- ❖ 1 人のユーザーに複数のロールを割り当てられます。
- ❖ 複数のユーザーで 1 つのロールを共有するよう設定できます。
- ❖ ロールの権限を複数のセキュリティ・グループに設定できます。

注意 : 権限の編集の詳細は、5-27 ページの「副管理者の設定」を参照してください。

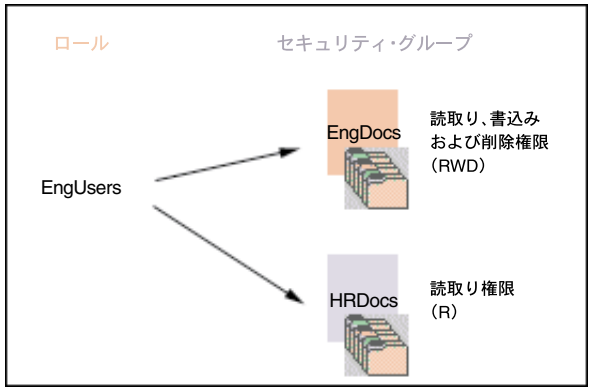
たとえば、図 3-2 では、3 つのロールと、それらのロールが同じセキュリティ・グループに対して持つ権限を示しています。

図 3-2 ロールおよびその権限の例



セキュリティ・グループにアクセスできるように、システム管理者はロールに 1 人以上のユーザーを割り当てます。図 3-3 に、HRDocs セキュリティ・グループに対して読取り権限のみを持つ EngUsers ロールを示します。ただし、このロールは、EngDocs セキュリティ・グループに対して読取り、書込みおよび削除権限を持っています。これにより、セキュリティが強化され、特定のドキュメントにアクセスする必要のあるユーザーのみがそれらのドキュメントを変更できるようになります。

図 3-3　ロールおよびセキュリティ・グループのアクセスの例



事前定義済ロール

次のロールは事前に定義されています。

ロール	説明
admin	admin ロールは、システム管理者に割り当てられます。デフォルトでは、このロールには、すべてのセキュリティ・グループとアカウントに対する管理権限、およびすべての管理ツールに対する権限があります。
contributor	contributor ロールには、パブリック・セキュリティ・グループに対する読取りおよび書込み権限があり、ユーザーはコンテンツを検索、表示、チェックインおよびチェックアウトできます。
guest	guest ロールには、パブリック・セキュリティ・グループに対する読取り権限があり、ユーザーはコンテンツを検索および表示できます。
sysmanager	sysmanager ロールには、管理サーバーへのアクセス権があります。

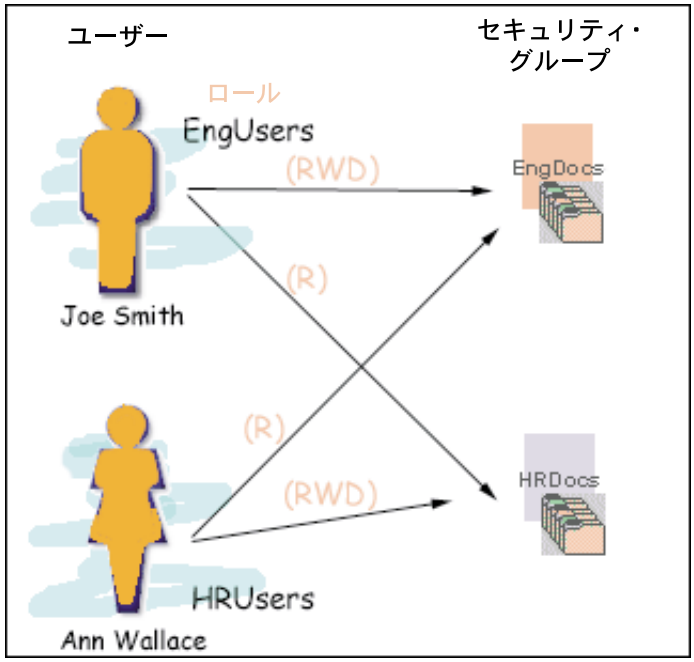
権限について

各ロールには、各セキュリティ・グループに対する読取り（R）、書込み（W）、削除（D）または管理（A）権限が許可されています。セキュリティ・グループのファイルにアクセスするためにユーザーが持つ権限は、**任意のユーザーのロールにより定義される最高の権限です**。つまり、ユーザーに guest および contributor ロールがあり、guest にはパブリック・セキュリティ・グループに対する読取り権限が、contributor には書込み権限が付与されている場合、そのユーザーがパブリック・セキュリティ・グループのコンテンツに対して持つのは書込み権限です。

次の図では、Joe Smith および Ann Wallace が 2 つのセキュリティ・グループに対する権限を持っています。

- Joe Smith は、EngDocs セキュリティ・グループに対して読取り、書込みおよび削除権限を持っていますが、HRDocs セキュリティ・グループに対しては読取り権限のみを持っています。EngUsers ロールのメンバーとして、エンジニアリング・ドキュメントには読取り、書込みおよび削除アクセス権が付与されていますが、人事ドキュメントには読取りアクセス権のみが付与されています。
- Ann Wallace は、HRDocs セキュリティ・グループに対して読取り、書込みおよび削除権限を持っていますが、EngDocs セキュリティ・グループに対しては読取り権限のみを持っています。HRUsers ロールのメンバーとして、人事ドキュメントには読取り、書込みおよび削除アクセス権が付与されていますが、エンジニアリング・ドキュメントには読取りアクセス権のみが付与されています。

図 3-4　割当て済権限の例



事前定義済権限

各ロールでは、各セキュリティ・グループに次の権限を割り当てることができます。

権限	説明
読取り	セキュリティ・グループのファイルを表示できます。
書込み	セキュリティ・グループのドキュメントの表示、チェックイン、チェックアウトおよびコピーの取得を実行できます。新しいセキュリティ・グループの書込み権限を持っている作成者がいない場合、作成者はドキュメントのセキュリティ・グループの設定を変更できます。
削除	セキュリティ・グループのファイルの表示、チェックイン、チェックアウト、削除およびコピーの取得を実行できます。構成設定 `AuthorDelete=true` により、作成者が書込み権限を持っているすべてのセキュリティ・グループに対する削除権限が追加されます。
管理	セキュリティ・グループのファイルの表示、チェックイン、チェックアウト、削除およびコピーの取得を実行できます。ユーザーにワークフロー権限がある場合は、セキュリティ・グループのワークフローを開始または編集できます。 また、別のユーザーが作成者として指定されているセキュリティ・グループにもドキュメントをチェックインできます。新しいセキュリティ・グループの書込み権限を持っている作成者がいない場合、作成者はドキュメントのセキュリティ・グループの設定を変更できません。

ロールおよび権限の管理

次のタスクは、ユーザー・ロールの管理に使用されます。

- ロールの作成（3-10 ページ）
- ロールの削除（3-10 ページ）
- ユーザーへのロールの割当て（3-11 ページ）
- 「Create Similar Users」へのロールの割当て（3-11 ページ）
- 権限の追加および編集（3-12 ページ）

ロールの作成

ロールを作成して権限を構成するには、次のようにします。

1. ユーザー管理アプリケーション（2-20 ページ）で、**「Security」**→**「Permissions by Role」**を選択します。

   「Permissions By Role」画面（3-15 ページ）が表示されます。

2. **「Add New Role」**をクリックします。

   「Add New Role」画面（3-16 ページ）が表示されます。

3. ロール名を入力します。
4. ロールに権限を設定します。
   a. ロールを選択します。
   b. 編集するセキュリティ・グループを選択します。
   c. **「Edit Permissions」**をクリックします。
   d. 権限を編集します。
   e. **「OK」**をクリックして、「Permissions By Role」画面（3-15 ページ）を閉じます。

ロールの削除

ロールを削除するには、次のようにします。

1. 削除するロールにユーザーが割り当てられていないことを確認します。（ユーザーが割り当てられている場合は、そのロールを削除できません。）
2. ユーザー管理アプリケーション（2-20 ページ）で、**「Security」**→**「Permissions by Role」**を選択します。

   「Permissions By Role」画面（3-15 ページ）が表示されます。

3. 削除するロールを選択します。
4. **「Delete Role」**をクリックします。

   確認画面が表示されます。

5. **「Yes」**をクリックします。

ユーザーへのロールの割当て

ユーザーにロールを割り当てるには、次のようにします。

1. ユーザー管理アプリケーション（2-20 ページ）で、ユーザーを選択します。
2. **「Edit」**ボタンをクリックします。

   「Add User」/「Edit User」画面（5-10 ページ）が表示されます。
3. 「Roles」タブをクリックします。

   「Add User」/「Edit User」画面：「Roles」タブ（5-15 ページ）が表示されます。
4. **「Add Role」**をクリックします。

   「Add New Role」画面（3-16 ページ）が表示されます。
5. 「Role Name」リストからロールを選択します。
6. **「OK」**をクリックします。

   ロールが「Roles」リストに追加されます。

「Create Similar Users」へのロールの割当て

別のユーザー・ログインと類似のアクセス権を持つユーザー・ログインを作成するには、次のタスクを実行します。

1. ユーザー管理アプリケーション（2-20 ページ）で、ユーザーを選択します。
2. **「Add Similar」**ボタンをクリックします。

   「Add User」/「Edit User」画面（5-10 ページ）が表示されます。
3. 「Roles」タブをクリックします。

   「Add User」/「Edit User」画面：「Roles」タブ（5-15 ページ）が表示されます。「Roles」タブは、選択したユーザーに割り当てられているロールおよびアカウントに基づいて移入されることに注意してください。
4. 「Info」タブに新しいユーザー固有のデータを入力します。
5. **「Add Role」**をクリックします。

権限の追加および編集

ロールへの権限の追加または既存の権限の編集を実行するには、次のようにします。

1. ユーザー管理アプリケーション（2-20 ページ）で、**「Security」**→**「Permissions by Role」**を選択します。

   「Permissions By Role」画面（3-15 ページ）が表示されます。

2. 既存のロールを選択するか、新しいロールを追加します。

   セキュリティ・グループに関連付けられた権限が表示されます。

3. 「Groups/Rights」列でアイテムを選択します。
4. **「Edit Permissions」**をクリックします。

   「Edit Permissions」画面（3-16 ページ）が表示されます。

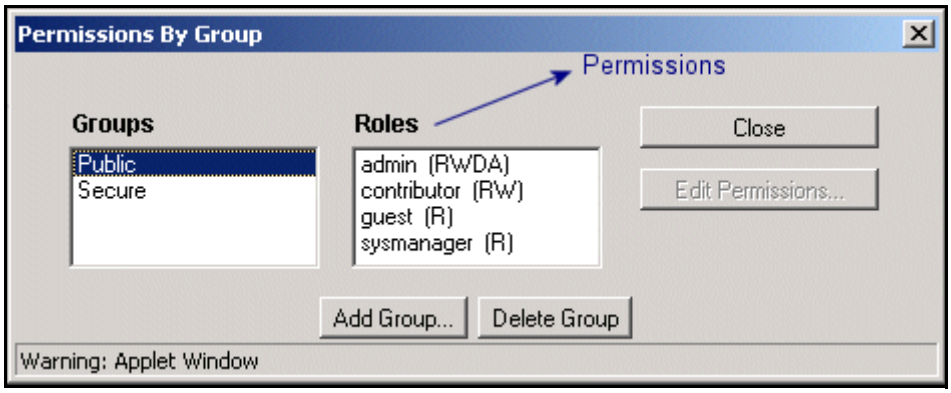
5. ロールおよびセキュリティ・グループに関連付ける権限を指定します。詳細は、3-9 ページの「事前定義済権限」を参照してください。
6. **「OK」**をクリックします。

グループ、ロールおよび権限のインタフェース画面

次の画面は、グループやロールの作成および権限の設定に使用します。

- ❖ 「Permissions By Group」画面（3-13 ページ）
- ❖ 「Add New Group」画面（3-14 ページ）
- ❖ 「Permissions By Role」画面（3-15 ページ）
- ❖ 「Add New Role」画面（3-16 ページ）
- ❖ 「Edit Permissions」画面（3-16 ページ）

「Permissions By Group」画面

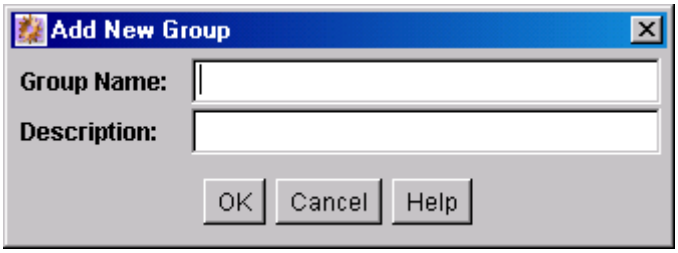


「Permissions By Group」画面は、セキュリティ・グループの追加や削除、既存のセキュリティ・グループに関連付けられた権限の編集に使用します。この画面にアクセスするには、ユーザー管理アプリケーション（2-20 ページ）で、「**Security**」→「**Permissions by Group**」を選択します。

警告 : セキュリティ・グループ名には、大カッコを使用できません。これは、検索エンジン・テクノロジの制限によるものです。

機能	説明
「Groups」リスト	既存のセキュリティ・グループが表示されます。
「Roles」リスト	既存のセキュリティ・グループに関連付けられたロールが表示されます。
「Edit Permissions」ボタン	セキュリティ・グループの権限を編集できます。
「Add Group」ボタン	「Add New Group」画面（3-14 ページ）が表示されます。
「Delete Group」ボタン	既存のセキュリティ・グループを削除できます。（セキュリティ・グループにコンテンツが存在する場合は、そのセキュリティ・グループを削除できません。）

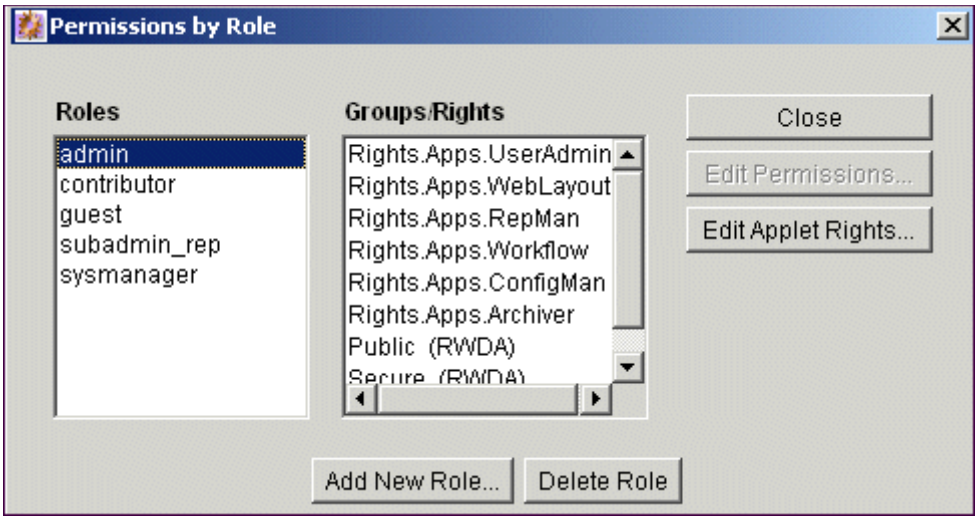
「Add New Group」画面



「Add New Group」画面は、新しいセキュリティ・グループの名前および説明の定義に使用します。この画面にアクセスするには、「Permissions By Group」画面（3-13 ページ）で**「Add Group」**をクリックします。

機能	説明
「Group Name」フィールド	• グループ名は 30 文字に制限されています。 • 空白、タブ、ライン・フィード、キャリッジ・リターン、;、:、^、?、&、+、"、#、%、<、*、~、| は使用できません。 • アクセント記号付きの大文字は使用できませんが、アクセント記号付きの小文字は使用できます。（たとえば、*Älvdalsån* は使用できませんが *älvdalsån* は可能です。）
「Description」フィールド	セキュリティ・グループの簡単な説明。 • 説明は 80 文字に制限されています。 • このフィールドはユーザー管理アプリケーションにのみ表示されます。

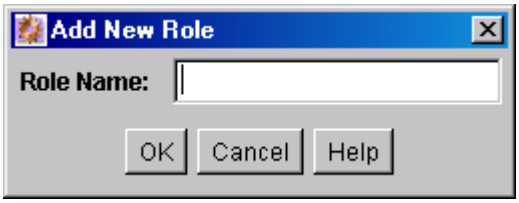
「Permissions By Role」画面



「Permissions By Role」画面は、ロールの追加や削除、権限やロールに関連付けられた権限の編集に使用します。この画面にアクセスするには、ユーザー管理アプリケーション（2-20 ページ）で、**「Security」**→**「Permissions by Role」**を選択します。

機能	説明
「Roles」リスト	既存のロールが表示されます。
「Groups/Rights」リスト	選択したロールに関連付けられているセキュリティ・グループおよび権限が表示されます。
「Edit Permissions」ボタン	セキュリティ・グループおよびロールの権限を編集できます。このボタンは、ロールおよびグループ / 権限を選択した場合に使用できます。
「Edit Applet Rights」ボタン	ロールの権限を編集できます。このボタンは、ロールを選択した場合に使用できます。
「Add New Role」ボタン	「Add New Role」画面（3-16 ページ）が表示されます。この画面では、ユーザーに新しいロールを設定できます。ロール名を追加して**「OK」**をクリックします。
「Delete Role」ボタン	選択したロールを削除できます。（ロールにユーザーが割り当てられている場合は、そのロールを削除できません。）

「Add New Role」画面



「Add New Role」画面は、新しいロールの名前の定義に使用します。この画面にアクセスするには、「Permissions By Role」画面（3-15 ページ）で「**Add New Role**」をクリックします。

機能	説明
「Role Name」フィールド	• ロール名は 30 文字に制限されています。 • 空白、タブ、ライン・フィード、キャリッジ・リターン、;、:、^、?、&、+、"、#、%、<、*、~、| は使用できません。 • 最初、ロールには、パブリック・セキュリティ・グループに対する読取り（R）権限が割り当てられていて、その他のセキュリティ・グループに対する権限はありません。

「Edit Permissions」画面

「Edit Permission」画面は、特定のロールの特定のセキュリティ・グループに対する権限の変更に使用します。この画面にアクセスするには、次のいずれかを実行します。

❖ 「Permissions By Group」画面（3-13 ページ）でセキュリティ・グループとロールを選択し、「**Edit Permissions**」をクリックします。

❖ 「Permissions By Role」画面（3-15 ページ）でロールとセキュリティ・グループを選択し、「**Edit Permissions**」をクリックします。

機能	説明
「Read」チェック・ボックス	ユーザーによるファイルの表示を可能にします。
「Write」チェック・ボックス	ユーザーによるファイルの表示、チェックイン、チェックアウトおよびコピーの取得を可能にします。
「Delete」チェック・ボックス	ユーザーによるファイルの表示、チェックイン、チェックアウト、コピーの取得および削除を可能にします。
「Admin」チェック・ボックス	ユーザーによるファイルの表示、チェックイン、チェックアウト、コピーの取得、削除および別のユーザーに対するファイルのチェックインを可能にします。また、ユーザーにワークフロー権限がある場合は、ワークフローを開始または編集できます。

4

内部セキュリティ：アカウントの使用

概要

この項の内容は次のとおりです。

概念

タスク

インタフェース

- 「Predefined Accounts」画面（4-11 ページ）
- 「Add New Predefined Account」画面（4-12 ページ）
- アカウント権限の追加 / 編集画面（4-12 ページ）

例

- アカウントの事例（4-13 ページ）

アカウントについて

アカウントを使用すると、セキュリティ・グループのみの場合よりも、セキュリティ構造の柔軟性と精度が向上します。アカウント権限は、ユーザー管理ツールを使用して、ロール権限の割当てと同じような方法でユーザーに割り当てられます。アカウントは、各コンテンツ・アイテムに割り当てることもできます。アカウントが割り当てられたコンテンツ・アイテムにアクセスするには、そのアカウントに対する適切な権限を持っている必要があります。

アカウントの作成方法は 3 つあります。

- システム管理者による、ユーザー管理ツールを使用した事前定義済アカウントの作成。詳細は、4-7 ページの「事前定義済アカウントの作成」を参照してください。
- システム管理者による、ユーザーへのアカウントの割当て中におけるアカウントの作成（ユーザー管理ツールを使用）。詳細は、4-8 ページの「ユーザー管理中のアカウントの作成」を参照してください。
- ユーザー管理者による、コンテンツのチェックイン時におけるアカウントの作成。詳細は、4-8 ページの「コンテンツのチェックイン中のアカウントの作成」を参照してください。

注意 : アカウントを使用するには、アカウントを有効化する必要があります。詳細は、4-7 ページの「アカウントの有効化」を参照してください。

アカウントおよびセキュリティ・グループ

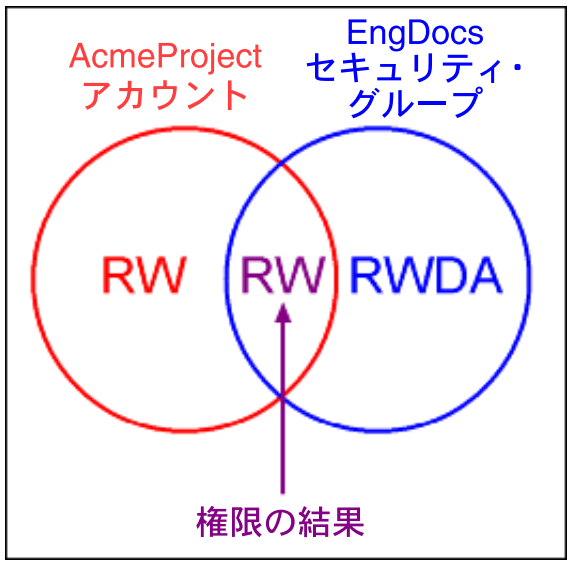
アカウントを使用する場合、**アカウントが、セキュリティ・グループ権限より優先されるプライマリ権限になります。**。特定のドキュメントへのユーザーのアクセスを、アカウント権限とセキュリティ・グループ権限の間の共通部分と考えることもできます。

たとえば、EngAdmin ロールには、EngDocs セキュリティ・グループのすべてのコンテンツに対する読取り、書込み、削除および管理権限があります。ユーザーは EngAdmin

ロールに割り当てられ、AcmeProject アカウントに対する読取りおよび書込み権限も割り当てられます。その結果、ユーザーは、EngDocs セキュリティ・グループおよび AcmeProject アカウントに属するコンテンツ・アイテムに対する読取りおよび書込み権限のみを持ちます。

図 4-1 に、AcmeProject アカウント権限と EngDocs セキュリティ・グループ権限の共通部分を示します。

図 4-1　セキュリティ・グループ権限の例

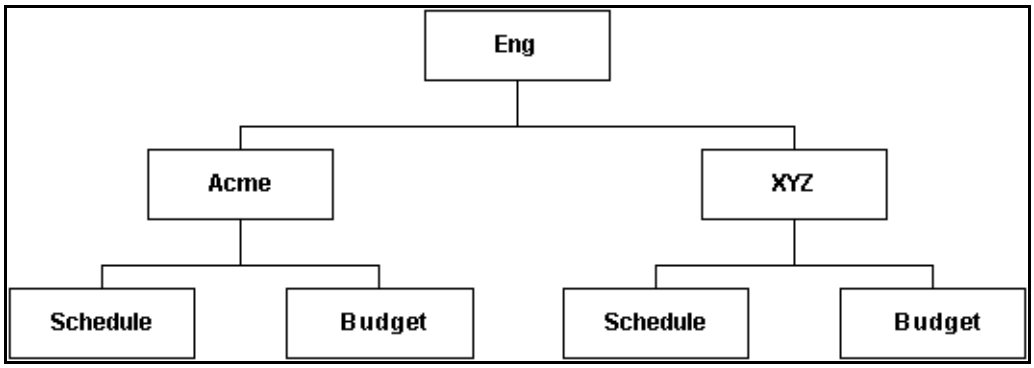


注意 : アカウントで任意のコンテンツへのアクセスが許可されていない場合、セキュリティ・グループ権限は無視されます。アカウントは、ユーザーのロールによって定義された権限より優先されるフィルタとして機能します。

階層アカウント

アカウントは階層構造に設定できます。これにより、一部のユーザーには構造のブランチ全体に対するアクセス権を付与する一方で、構造の下位レベルのアカウントを割り当てることによりその他のユーザーの権限を制限できます。図 4-2 に、典型的な階層アカウント構造を示します。

図 4-2　階層アカウント構造の例



重要 : アカウント名は、コンテンツ・アイテムの URL のディレクトリ・パスの一部を形成するため、30 文字を超えることはできません。

- ❖ アカウント名のレベルを区切るためにスラッシュを使用すると（Eng/Acme/Budget など）、Content Server によりアカウント構造に応じて weblayout ディレクトリ構造が作成されます。（ただし、実際の各ディレクトリは、チェックイン・プロセス中にコンテンツ・アイテムがアカウントに割り当てられるまで作成されません。）アカウント名の各下位レベルは、そのディレクトリがアカウント・レベルであることを示す @ 記号接頭辞付きの上位レベルのサブディレクトリになります。
- ❖ ユーザーが特定の接頭辞のアカウントに対する権限を持っている場合、その接頭辞の付くすべてのアカウントへのアクセス権があります。たとえば、Eng/XYZ アカウントを割り当てられている場合、Eng/XYZ アカウントおよび Eng/XYZ 接頭辞で始まる任意のアカウント（Eng/XYZ/Schedule および Eng/XYZ/Budget など）へのアクセス権があります。

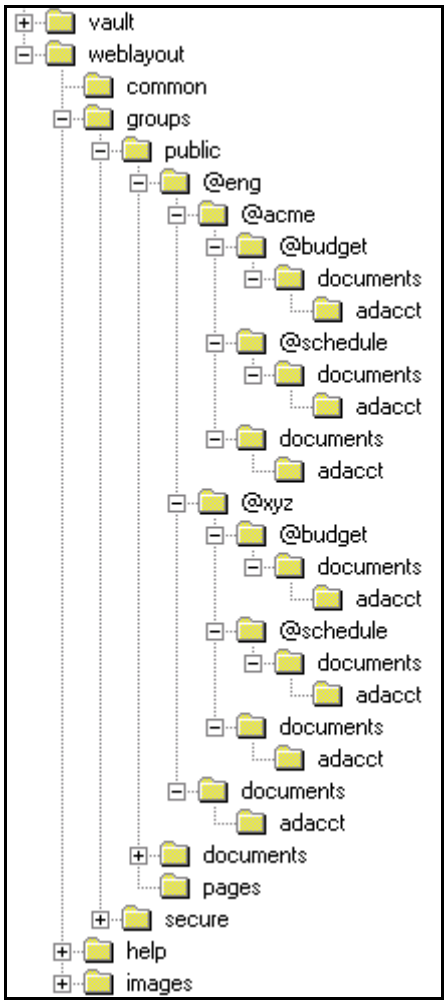
重要 : アカウント接頭辞にスラッシュを含める必要はありません。たとえば、abc、abc_docs および abcdefg というアカウントがある場合、abc アカウントへのアクセス権を持つすべてのユーザーには、その他 2 つのアカウントに対するアクセス権もあります。

前述のセキュリティ構造に対応するには、次のアカウントを作成します。

- Eng
- Eng/Acme
- Eng/XYZ
- Eng/Acme/Schedule
- Eng/Acme/Budget
- Eng/XYZ/Schedule
- Eng/XYZ/Budget

図 4-3 に、Content Server により、<*Install_Dir*>/weblayout/ ディレクトリに作成されるファイル構造を示します。

図 4-3　セキュリティ・ファイル構造の例



作業効率に関する考慮事項

セキュリティ・モデルでアカウントを使用する際には、次の作業効率の問題を考慮してください。

- 理論上、コンテンツ・サーバーのパフォーマンスに影響を与えずに無制限にアカウントを作成できます。100,000 を超えるコンテンツが存在するシステムでは、1 人当たり 200 アカウントの場合に管理効率上の限られた問題があります。ただし、1 人当たり 100 を超えるアカウントがあると、検索効率に重大な影響があります。（これらは、階層アカウント接頭辞を介して暗黙的にユーザーに関連付けられたアカウントではなく、明示的なアカウントであることに注意してください。ユーザーは、単一の接頭辞を介して多数の暗黙的アカウントに対する権限を持つことができます。）
- アカウントを有効化する場合は、作業効率上の理由から、使用するセキュリティ・グループが 50 を超えないようにしてください。
- セキュリティ・グループおよびアカウントには、比較的短い名前を付けるようにしてください。

外部ディレクトリ・サーバーの考慮事項

アカウントは、コンテンツ・サーバーが外部ディレクトリ・サーバー（ADSI または LDAP など）と統合されているかどうかに関係なく使用できます。外部ディレクトリを使用するアカウントを使用する場合は、次の追加のガイドラインに従ってください。

- 適切なユーザーを含むグローバル・グループをアカウントに一致するように設定します。
- マッピング接頭辞を構成して、グループ名をロールまたはアカウントにマッピングします。

アカウントの管理

アカウントの管理には、次のタスクが関連します。

アカウントの有効化

警告：アカウントを有効化して使用する場合は、データを損失せずにアカウントを無効化することはできません。確実に使用する必要がある場合以外は、アカウントを有効化しないでください。

アカウントを有効化するには、次のようにします。

1. 「Administration」ページ（1-5 ページ）で、「**Admin Server** 」リンクをクリックします。
2. 「*<name_of_instance>*」ボタンをクリックします。
3. 左側のナビゲーション・バーで、「**General Configuration**」を選択します。
4. *<Install_Dir>*/config/config.cfg ファイルのコンテンツを示す、「Additional Configuration Variables」フィールドに次の行を追加します。

   ```
   UseAccounts=true
   ```

5. 変更内容を保存します。
6. コンテンツ・サーバーを停止して再起動します。

事前定義済アカウントの作成

事前定義済アカウントを作成するには、次のようにします。

1. 「User Admin」画面で、「**Security**」→「**Predefined Accounts**」を選択します。

   「Predefined Accounts」画面（4-11 ページ）が表示されます。

2. 「**Add**」をクリックします。

   アカウントの有効化（4-7 ページ）が表示されます。

3. 新規アカウントの名前を追加します。短くて一貫性のある名前を付けます。たとえば、場所または部門による 3 文字の略語（MSP または NYC など）を使用してすべてのアカウントを設定します。アカウント名は 30 文字以内にする必要があり、空白、タブ、ライン・フィード、キャリッジ・リターン、および ;、^、?、:、&、+、"、#、%、<、>、*、~ の記号は使用できません。
4. 「**OK**」をクリックします。
5. すでにコンテンツ・サーバーにコンテンツがチェックインされていて、Verity、FAST または全文索引付けのデータベースを使用している場合は、検索索引を再作成します。

   メタデータ・データベースの検索インデクサ・エンジンのみを使用している場合は、検索索引を再作成する必要はありません。

関連項目

– ユーザー管理中のアカウントの作成（4-8 ページ）
– コンテンツのチェックイン中のアカウントの作成（4-8 ページ）

ユーザー管理中のアカウントの作成

技術ヒント : 一般的に、ユーザー定義中にアカウントを作成するのではなく、事前定義済アカウントを作成する必要があります。詳細は、4-7 ページの「事前定義済アカウントの作成」を参照してください。

ユーザーへのアカウントの割当て中にアカウントを作成するには、sysadmin としてログインして次のタスクを実行します。

1. アカウントを作成するユーザーの「Add User」/「Edit User」画面（5-10 ページ）を表示します。
2. 「Accounts」タブをクリックします。
3. **「Add」**をクリックします。
4. 新しいアカウント名を入力します。
5. チェック・ボックスを選択または選択解除して、アカウント権限を指定します。
6. **「OK」**をクリックします。

   ユーザーに新規アカウントが割り当てられます。

関連項目

– 事前定義済アカウントの作成（4-7 ページ）
– コンテンツのチェックイン中のアカウントの作成（4-8 ページ）

コンテンツのチェックイン中のアカウントの作成

技術ヒント : 一般的に、コンテンツのチェックイン・プロセス中にアカウントを作成するのではなく、事前定義済アカウントを作成する必要があります。詳細は、4-7 ページの「事前定義済アカウントの作成」を参照してください。

コンテンツ・アイテムのチェックイン時にアカウントを作成するには、ユーザー管理権限を持っている必要があります。次のタスクを実行します。

1. 「Content Check In Form」ページを表示します。
2. 必須およびオプションの情報をすべて入力します。
3. 「Account」フィールドにアカウント名を入力します。
4. **「Check In」**をクリックします。

   コンテンツ・アイテムに新規アカウントが割り当てられます。

関連項目

– 事前定義済アカウントの作成（4-7 ページ）
– ユーザー管理中のアカウントの作成（4-8 ページ）

事前定義済アカウントの削除

事前定義済アカウントを削除するには、次のようにします。

1. **「Security」→「Predefined Accounts」**を選択します。

   「Predefined Accounts」画面（4-11 ページ）が表示されます。
2. 削除するアカウントを選択します。
3. **「Delete」**をクリックします。

   アカウントが即時に削除されます。

注意 : アカウントのコンテンツが存在していても、そのアカウントを削除できます。アカウントの値はコンテンツ・アイテムに割り当てられたままですが、ユーザー定義のアカウントとみなされます。

ユーザーへのアカウントの割当て

ユーザーにアカウントを割り当てるには、次のようにします。

1. 「User Admin」画面で、ユーザーを選択します。
2. **「Edit」**ボタンをクリックします。

   「Add User」/「Edit User」画面（5-10 ページ）が表示されます。
3. 「Accounts」タブをクリックします。

   「Add User」/「Edit User」画面 :「Accounts」タブ（5-16 ページ）が表示されます。

4. 「**Add**」をクリックします。

   アカウント権限の追加 / 編集画面（4-12 ページ）が表示されます。

5. 「**Account**」リストからアカウントを選択します。
6. チェック・ボックスを選択または選択解除して、アカウント権限を指定します。
7. 「**OK**」をクリックします。
8. 必要な場合には、デフォルトのアカウントを指定します。これは、「Content Check In Form」ページにデフォルトで表示されるアカウントです。
9. 「**OK**」をクリックします。

アカウントのインタフェース画面

アカウントを追加する際には、次の画面を使用します。

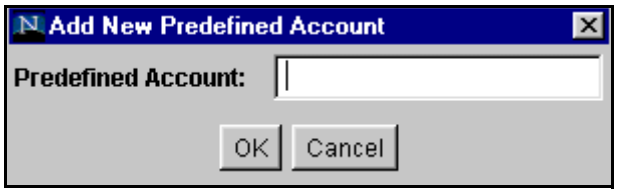
- ❖ 「Predefined Accounts」画面（4-11 ページ）
- ❖ 「Add New Predefined Account」画面（4-12 ページ）
- ❖ アカウント権限の追加 / 編集画面（4-12 ページ）

「Predefined Accounts」画面

「Predefined Accounts」画面は、事前定義済アカウントの追加および削除に使用します。この画面にアクセスするには、ユーザー管理アプリケーション（2-20 ページ）で、**「Security」→「Predefined Accounts」**を選択します。

機能	説明
「Predefined Accounts」リスト	事前定義済アカウントが表示されます。
「Add」ボタン	アカウントの有効化（4-7 ページ）が表示されます。
「Delete」ボタン	選択したアカウントを削除します。 **注意：**アカウントのコンテンツが存在していても、そのアカウントを削除できます。アカウントの値はコンテンツ・アイテムに割り当てられたままですが、ユーザー定義のアカウントとみなされます。

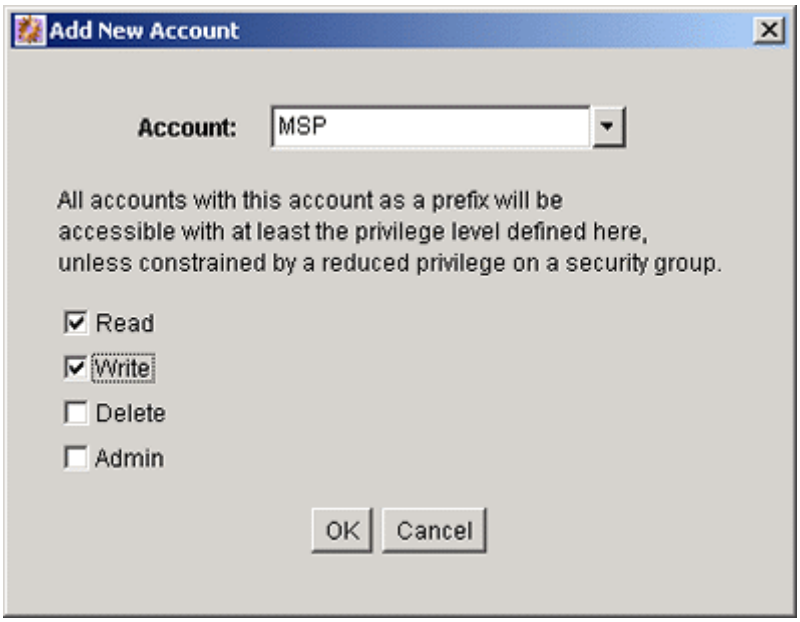
「Add New Predefined Account」画面



「Add New Predefined Account」画面は、新しい事前定義済アカウントに名前を付ける際に使用します。この画面にアクセスするには、「Predefined Accounts」画面（4-11 ページ）で「**Add**」をクリックします。

機能	説明
「Predefined Account」フィールド	追加するアカウントの名前を入力します。短くて一貫性のある名前を付けます。たとえば、場所または部門による 3 文字の略語（MSP または NYC など）を使用してすべてのアカウントを設定します。アカウント名は 30 文字以内にする必要があり、空白、タブ、ライン・フィード、キャリッジ・リターン、および ;、^、?、:、&、+、"、#、%、<、>、*、~ の記号は使用できません。

アカウント権限の追加 / 編集画面



「Add New Account」/「Edit Permissions for Account」画面は、ユーザーにアカウント権限を割り当てる際に使用します。この画面にアクセスするには、「Add User」/「Edit User」画面 :「Accounts」タブ（5-16 ページ）で**「Add」**または**「Edit」**クリックします。

機能	説明
「Account」リスト	リストから事前定義済アカウントを選択するか、ユーザー定義のアカウントを入力します。
「Permissions」チェック・ボックス	ユーザーがアカウントに対して持つ事前定義済権限（3-9 ページ）を設定します。

アカウントの事例

この例において、Xalco はロンドン、ニューヨークおよびパリに支社のある世界的なソフトウェア企業です。コンテンツ・サーバーはロンドン支社でホストされていて、企業 WAN 経由でその他の支社からのアクセスがあります。また、Xalco は、パブリック Web サイトに一部のファイルをレプリケートしています。まず、各地の営業部および経理部で、ファイルを公開するためにそれらのインスタンスを使用する必要があります。ニューヨーク支社は小規模で、営業部がありません。

次の項では、Xalco の事例に関するサンプル情報を示します。

- Xalco のセキュリティ（4-13 ページ）
- Xalco 社のアカウント（4-14 ページ）
- Xalco 社のロール（4-15 ページ）
- ロールおよび権限の表（4-15 ページ）
- ロールおよびユーザーの表（4-16 ページ）
- アカウントおよびユーザーの表（4-16 ページ）

Xalco のセキュリティ

- Xalco の従業員およびセキュリティ・レベル :
  - **ロンドン :** David Smith（社全体の CFO）および Jim McGuire（イギリスの営業部長）
  - **ニューヨーク :** Catherine Godfrey（ニューヨークの経理部長）
  - **パリ :** Helene Chirac（ヨーロッパの財務係）

❖ Xalco 社のコンテンツのセキュリティ検査（セキュリティ・グループ）のレベル :

- **パブリック :** パブリックのメンバーに公開できるファイル（パブリック・コンテンツは Xalco 社の Web サイトにレプリケートされます。）
- **内部 :** 内部ではアクセスの制限はないが、パブリックには公開できないファイル
- **機密 :** 業務上機密性が要求され、中間管理職以上に制限されているファイル
- **極秘 :** 機密性が高く、役員にのみ公開されるファイル

❖ Xalco 社の従業員のアクセス権 :

- **David Smith:** Xalco 社全体の CFO として、インスタンスに保持されているすべてのファイルへの完全なアクセス権が必要です。
- **Jim McGuire:** イギリスの営業部長として、ロンドンの営業ファイルに対してフルコントロールのアクセス権を持ち、パリの営業活動を把握できる必要があります。部長として、機密レベルの許可があります。
- **Helene Chirac:** パリ支社を本拠地としていて、ヨーロッパの経理に関するファイルのみを参照する必要があり、内部レベルの許可のみがあります。
- **Catherine Godfrey:** ニューヨークを本拠地とする地区の経理部長として、ニューヨークの経理ファイルの投稿、およびその他すべての経理ドキュメントの参照を実行できる必要があります。部長として、機密レベルの許可があります。

Xalco 社のアカウント

アクセス権は場所や職務権限により異なるため、アカウント構造に反映されています。

❖ ロンドンには経理部と営業部があるため、2 つのアカウントが必要です。

- London/Finance
- London/Sales

❖ ニューヨークには経理部のみがあります。

- NewYork/Finance

❖ パリには、経理部と営業部の両方があります。

- Paris/Finance
- Paris/Sales

このため、最上位レベルのアカウントは 3 つ（London、NewYork、Paris）で、下位レベルのアカウントは 5 つになります。

Xalco 社のロール

各セキュリティ・グループに 2 つのロール（1 つはコンシューマ用でもう 1 つはコントリビュータ用）を作成する必要があります。

- PublicConsumer
- PublicContributor
- InternalConsumer
- InternalContributor
- SensitiveConsumer
- SensitiveContributor
- ClassifiedConsumer
- ClassifiedContributor

ロールおよび権限の表

ロール	パブリック	内部	機密	極秘
PublicConsumer	R			
PublicContributor	RWD			
InternalConsumer		R		
InternalContributor		RWD		
SensitiveConsumer			R	
SensitiveContributor			RWD	
ClassifiedConsumer				R
ClassifiedContributor				RWD

注意 : 特定のユーザーにワークフローを開始する権限を付与するには、コントリビュータ・ロールに管理権限とワークフロー権限を追加する必要があります。

ロールおよびユーザーの表

ロール	David Smith	Helene Chirac	Jim McGuire	Catherine Godfrey
PublicConsumer		X		
PublicContributor	X		X	X
InternalConsumer		X		
InternalContributor	X		X	X
SensitiveConsumer				
SensitiveContributor	X		X	X
ClassifiedConsumer				
ClassifiedContributor	X		X	X

アカウントおよびユーザーの表

アカウント	David Smith	Helene Chirac	Jim McGuire	Catherine Godfrey
London/Finance	RWDA	R		R
London/Sales	RWDA		RWDA	
NewYork/Finance	RWDA			RW
Paris/Finance	RWDA			R
Paris/Sales	RWDA		R	

注意 : David Smith にはロンドン、ニューヨークおよびパリのアカウントの RWDA 権限を付与する必要があります。

5

内部セキュリティ：ユーザー・ログインおよび別名の割当て

概要

この章の内容は次のとおりです。

概念

タスク

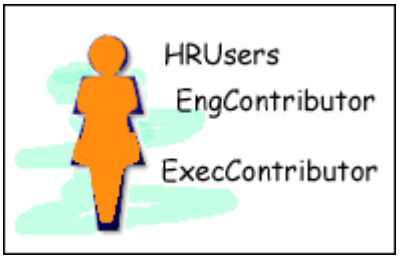
インタフェース

ユーザー・ログインおよび別名について

ユーザー・ログインは、コンテンツ・サーバーにアクセスするユーザーに関連付けられた名前です。システム管理者または副管理者により、各ユーザーに 1 つ以上のロールが割り当てられます。ロールにより、セキュリティ・グループ内のファイルに対するアクセス権がユーザーに付与されます。未定義のユーザーには guest ロールが割り当てられます。このロールには、デフォルトで、パブリック・セキュリティ・グループのドキュメントのみの表示が許可されています。

ワークフロー、サブスクリプションおよびプロジェクトに、単一の名前または別名で参照できるユーザーのグループを作成することもできます。たとえば、user1、user2、user3 などを追加するより、Support という別名をワークフローに追加する方が簡単です。

図 5-1 ロールを持つユーザーの例



重要 : ユーザー・ログインでは、大 / 小文字が区別されます。

技術ヒント : 異なるログイン方法（標準ログイン、Microsoft ログインまたは自動登録ログインなど）で同じコンピュータ上の複数のブラウザ・ウィンドウにログインすると、それぞれのウィンドウにどのユーザーがログインしているかに関してコンテンツ・サーバーが混乱する可能性があります。異なるログイン方法のテスト中は、開いているブラウザ・ウィンドウを閉じてください。

事前定義済のユーザー・ログイン

次のユーザー・ログインは事前定義されています。変更または削除しないでください。

ユーザー・ログイン	説明
sysadmin	このログインはシステム管理者で、デフォルトで admin および sysmanager ロールが割り当てられています。デフォルトのパスワードは idc です。このログインは、ローカル・ユーザーです。
user1	このログインには contributor ロールが割り当てられています。デフォルトのパスワードは idc です。このログインは、ローカル・ユーザーです。

重要 : セキュリティ上の理由から、sysadmin ユーザーのデフォルトのパスワードを変更する必要があります。

ログインおよび別名の管理

この項では、ユーザー・ログインの管理に関連するタスクを説明します。

ユーザー・ログインの追加

ユーザー・ログインを追加するには、次のようにします。

1. 「User Admin」画面 :「Users」タブ（5-8 ページ）で、**「Add」**をクリックします。
   - コンテンツ・サーバーがマスター・サーバーの場合は、「Choose the Authorization Type」画面（5-9 ページ）が表示されます。
   - コンテンツ・サーバーがプロキシ・サーバーの場合は、手順 4 に進みます。
2. ドロップダウン・リストから認可タイプを設定します。詳細は、ユーザーのタイプ（2-16 ページ）を参照してください。
3. **「OK」**をクリックします。

   「Add User」/「Edit User」画面（5-10 ページ）が表示されます。
4. ユーザーに関する情報を入力します。
   - パスワードを入力した場合、「Confirm Password」フィールドに同じパスワードを再入力する必要があります。
   - ユーザー名とパスワードでは、大 / 小文字が区別されます。
5. ユーザーにロールを割り当てます。詳細は、3-11 ページの「ユーザーへのロールの割当て」を参照してください。
6. アカウントが有効化されている場合は、ユーザーにアカウントを割り当てます。詳細は、4-9 ページの「ユーザーへのアカウントの割当て」を参照してください。
7. **「OK」**をクリックします。

ユーザー・ログインの編集

ユーザー・ログインを編集するには、次のようにします。

1. ユーザー管理アプリケーション（2-20 ページ）の「Users」タブで、ユーザー名をダブルクリックするか、ユーザー名を選択して「**Edit**」をクリックします。

   「Add User」/「Edit User」画面（5-10 ページ）または「Add User」/「Edit User」画面 :「Info」タブ（グローバル・ユーザー）（5-13 ページ）が表示されます。

2. 必要に応じてユーザー・ログインを編集します。

注意 : sysmanager ロールを持つユーザーのユーザー・ロケールを変更した場合は、ユーザーのロケール言語で表示されるように、管理サーバー・インタフェースの管理サーバー・サービスを再起動する必要があります。

ユーザー・ログインの削除

ユーザー・ログインを削除するには、次のようにします。

1. ユーザー管理アプリケーション（2-20 ページ）の「Users」タブで、ユーザー名を選択します。
2. 「**Delete**」をクリックします。

   確認画面が表示されます。

3. 「**Yes**」をクリックします。

注意 : ワークフローに関連するユーザーを削除した場合は、削除を確認するよう要求されます。ワークフローを調整し、ワークフロー・レビューアのリストからそのユーザーを削除する必要があります。

別名の作成

別名を定義するには、次のようにします。

1. 「User Admin」画面 :「Aliases」タブ（5-19 ページ）を表示します。
2. 「**Add**」をクリックします。

   「Add New Alias」/「Edit Alias」画面（5-20 ページ）が表示されます。

3. 「**Alias Name**」フィールドで、ユーザーのグループを識別する名前を入力します。
4. 「**Description**」フィールドで、別名の詳細な説明を入力します。
5. 「**Add**」をクリックします。

   「Select Users」画面（5-22 ページ）が表示されます。

6. リストからユーザー名を選択します。
   - 「Select Users」画面のユーザーのリストを絞り込むには、**「Use Filter」**チェック・ボックスを選択して**「Define Filter」**をクリックし、フィルタ基準を選択して**「OK」**をクリックします。
   - 一連のユーザーを選択するには、ユーザー・ログインを 1 つクリックし、[Shift] キーを押しながら別のユーザー・ログインをクリックします。
   - ユーザーを個別に選択するには、[Ctrl] キーを押しながら各ユーザー・ログインをクリックします。
7. **「OK」**をクリックします。
8. 「User Admin」画面を閉じます。

別名の編集

別名を編集するには、次のようにします。

1. 「User Admin」画面 :「Aliases」タブ（5-19 ページ）を表示します。
2. 別名を選択して**「Edit」**をクリックします。

   「Add New Alias」/「Edit Alias」画面（5-20 ページ）が表示されます。
3. 必要に応じて情報を変更します。
4. **「Description」**フィールドで、別名の詳細な説明を入力します。
5. **「OK」**をクリックします。
6. 「User Admin」画面を閉じます。

別名の削除

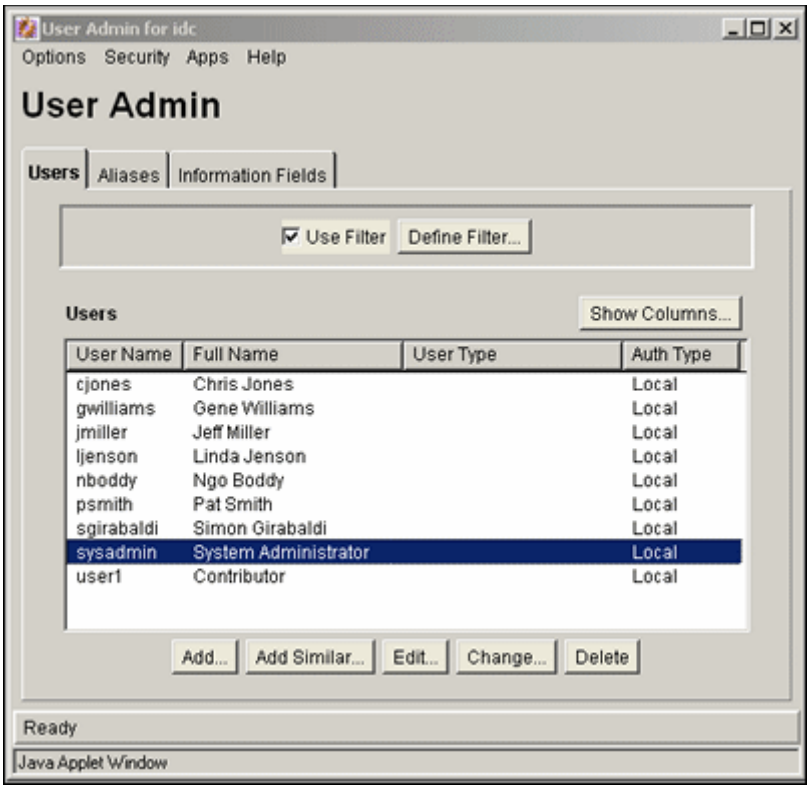
1. 「User Admin」画面 :「Aliases」タブ（5-19 ページ）を表示します。
2. 削除する別名を選択して**「Delete」**をクリックします。

   画面が表示され、削除を確認するよう要求されます。**「Yes」**をクリックしてエントリを削除するか、**「No」**をクリックしてそのままにします。
3. 「User Admin」画面を閉じます。

ユーザー・ログインおよび別名のインタフェース画面

次の画面は、ユーザー・ログインおよび別名の作成に使用します。

「User Admin」画面：「Users」タブ

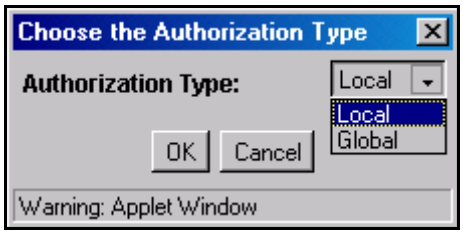


「User Admin」画面の「Users」タブは、ユーザー・ログインの追加、編集および削除に使用します。このタブにアクセスするには、ユーザー管理アプリケーション（2-20 ページ）を表示します。

機能	説明
「Use Filter」チェック・ボックス	このチェック・ボックスは、「Define Filter」画面（2-22 ページ）で定義された「Users」リストを絞り込む場合に選択します。
「Define Filter」ボタン	「Define Filter」画面（2-22 ページ）が表示されます。
「Show Columns」ボタン	「Show Columns」画面（2-24 ページ）が表示されます。
「Users」リスト	フィルタ設定に一致するユーザーが表示されます。ユーザーをダブルクリックすると、そのユーザーの「Add User」/「Edit User」画面（5-10 ページ）が表示されます。

機能	説明
「Add」ボタン	「Choose the Authorization Type」画面（5-9 ページ）が表示されます。
「Add Similar」ボタン	ユーザーを選択して**「Add Similar」**をクリックすると、システムにより、一部のフィールドがすでに移入された「Add User」/「Edit User」画面（5-10 ページ）が表示されます。
「Edit」ボタン	選択したユーザーの「Add User」/「Edit User」画面（5-10 ページ）が表示されます。
「Delete」ボタン	ユーザー・ログインを削除できます。

「Choose the Authorization Type」画面



「Choose the Authorization Type」画面は、新規ユーザーを追加する際に、ユーザー認可タイプの指定に使用します。この画面にアクセスするには、「User Admin」画面 : 「Users」タブ（5-8 ページ）で**「Add」**をクリックします。

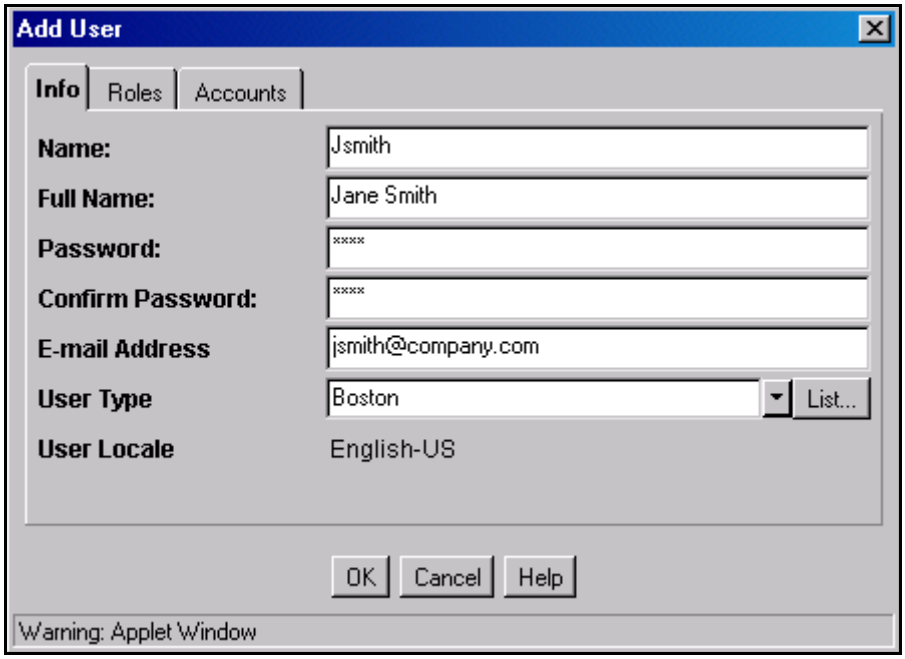
注意 : グローバル・ユーザーはマスター・コンテンツ・サーバーにのみ作成できるため、この画面はプロキシ・コンテンツ・サーバーからは使用できません。詳細は、2-16 ページの「ユーザーのタイプ」を参照してください。

機能	説明
「Authorization Type」リスト	ユーザーのタイプ。 **Local:** 管理者または副管理者によって Content Server システム内に定義されたユーザー。管理者はこれらのユーザーに 1 つ以上のロールを割り当てます。これにより、ユーザーにセキュリティ・グループへのアクセス権が付与されます。未定義のユーザーには、guest ロールが割り当てられます。このガイドでは冒頭の多くのページで、ローカル・ユーザーを詳細に説明しています。 **Global:** 簡単に管理できるユーザー。ローカルおよびグローバル・ユーザーの両方の資格証明は、複数のコンテンツ・サーバーに拡張されます。

機能	説明
「OK」ボタン	どちらの認可タイプが選択されているかに応じて、「Add User」/「Edit User」画面 :「Info」タブ（ローカル・ユーザー）（5-11 ページ）または「Add User」/「Edit User」画面 :「Info」タブ（グローバル・ユーザー）（5-13 ページ）が表示されます。

注意 : 外部ユーザーは、外部ユーザー・リポジトリを使用してコンテンツ・サーバーへのアクセス権が付与される際に自動的に作成されます。

「Add User」/「Edit User」画面



「Add User」/「Edit User」画面は、ユーザー情報の定義、ロールの割当て、ユーザーへのアカウント権限の割当てに使用します。この画面にアクセスするには、次のいずれかを実行します。

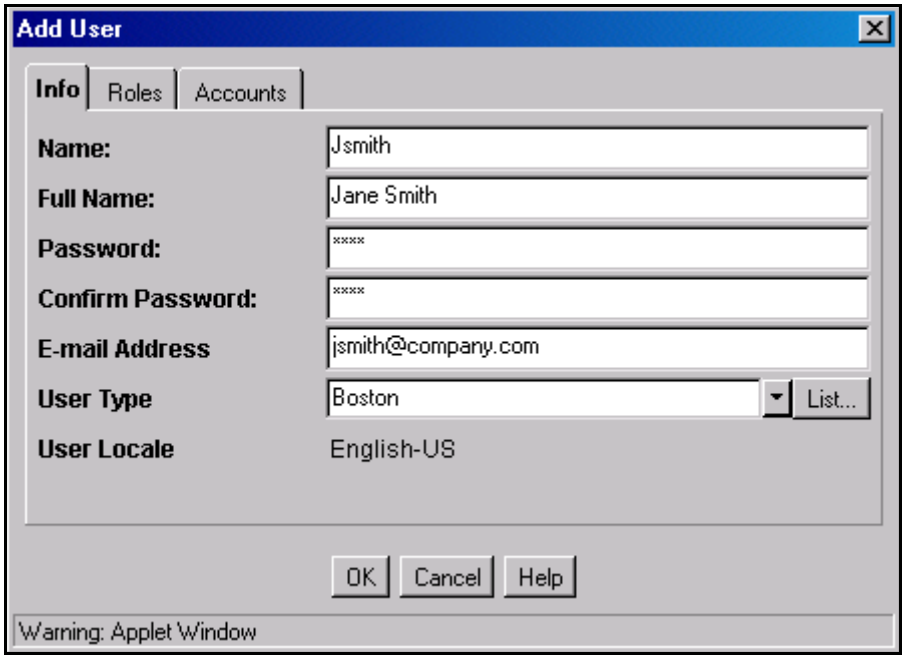
- ユーザー・タイプを選択し、「Choose the Authorization Type」画面（5-9 ページ）で**「OK」**をクリックします。「Add User」画面が表示されます。
- ユーザーを選択し、「User Admin」画面 :「Users」タブ（5-8 ページ）で**「Edit」**をクリックします。「Edit User」画面が表示されます。

カスタムのメタデータ・フィールドが追加されている場合、この画面に表示される情報は、ユーザーのシステムの情報と異なる場合があります。この画面ショットに表示されているフィールドは、Content Server とともにインストールされたデフォルトです。カスタム・フィールドの設定の詳細は、5-30 ページの「ユーザー情報フィールドの管理」を参照してください。

この画面のタブは、選択されたユーザーのタイプおよびアカウントが有効化されているかどうかによって異なります。

- 「Add User」/「Edit User」画面：「Info」タブ（ローカル・ユーザー）（5-11 ページ）
- 「Add User」/「Edit User」画面：「Info」タブ（グローバル・ユーザー）（5-13 ページ）
- 「Add User」/「Edit User」画面：「Roles」タブ（5-15 ページ）
- 「Add User」/「Edit User」画面：「Accounts」タブ（5-16 ページ）

「Add User」/「Edit User」画面：「Info」タブ（ローカル・ユーザー）



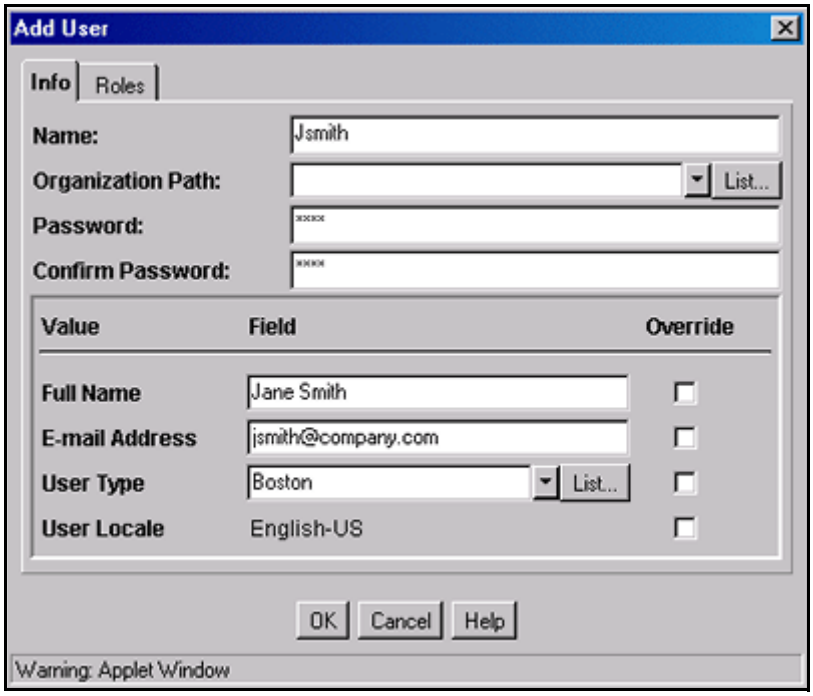
「Add User」/「Edit User」画面の「Info」タブは、ユーザーの追加に使用します。ローカル・ユーザーのこのタブにアクセスするには、次のいずれかを実行します。

- **「Local」**を選択し、「Choose the Authorization Type」画面（5-9 ページ）で**「OK」**をクリックします。

❖ ローカル・ユーザーを選択し、「User Admin」画面 : 「Users」タブ（5-8 ページ）で「**Edit**」をクリックします。

機能	説明
「Name」フィールド	新規ユーザーの名前。 • このフィールドには 50 文字の制限があります。 • ユーザー名では、大 / 小文字が区別されます。
「Full Name」フィールド	新規ユーザーの完全な名前。このフィールドには 50 文字の制限があります。
「Password」フィールド	新規ユーザー・ログインのパスワード。 • このフィールドには 50 文字の制限があります。 • パスワードでは、大 / 小文字が区別されます。
「Confirm Password」フィールド	スペルを確認するために、前のフィールドのパスワードを再入力します。
「E-Mail Address」フィールド	ユーザーに関連付けられた電子メール・アドレス。ワークフローおよびサブスクリプションの通知に使用されます。
「User Type」リスト	ユーザーの分類方法としてシステム管理者により定義される属性のリスト。
「List」ボタン	「Option List」画面（5-18 ページ）が表示されます。
「User Locale」フィールド	ユーザーのロケール。これにより、ユーザー・インタフェースの言語および日付 / 時間の書式が指定されます。ロケール・オプションは、システム管理者が有効化する必要があります。 詳細は、『Using Content Server in International Environments』を参照してください。 **注意 :** sysmanager ロールを持つユーザーのユーザー・ロケールを変更した場合は、ユーザーのロケール言語で表示されるように、管理サーバー・インタフェースの管理サーバー・サービスを再起動する必要があります。

「Add User」/「Edit User」画面：「Info」タブ（グローバル・ユーザー）



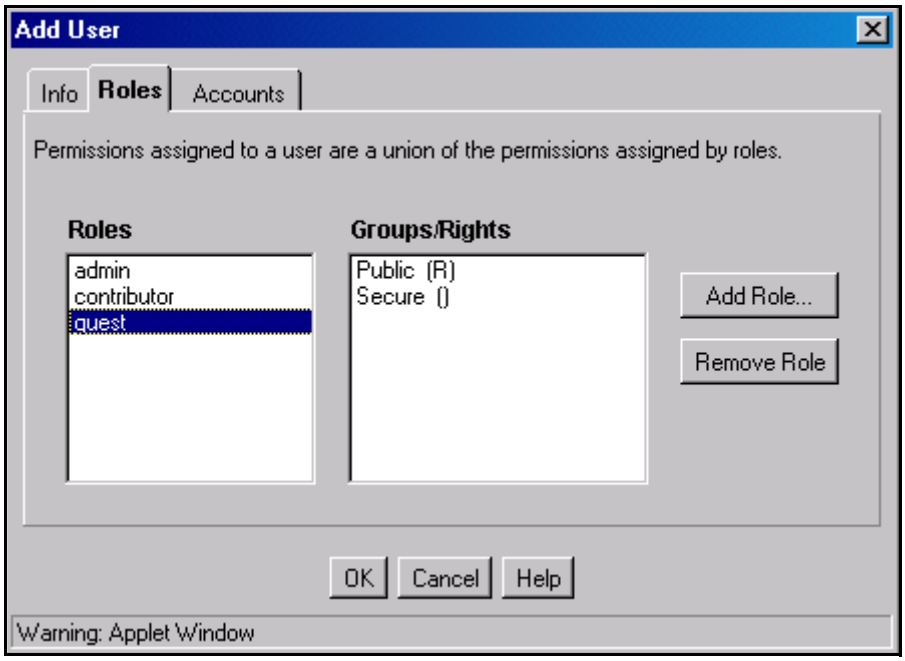
「Add User」/「Edit User」画面の「Info」タブは、ユーザーの追加に使用します。グローバル・ユーザーのこのタブにアクセスするには、次のいずれかを実行します。

- ❖ **「Global」**を選択し、「Choose the Authorization Type」画面（5-9 ページ）で**「OK」**をクリックします。
- ❖ グローバル・ユーザーを選択し、「User Admin」画面：「Users」タブ（5-8 ページ）で**「Edit」**をクリックします。

機能	説明
「Name」フィールド	新規ユーザーの名前。このフィールドには 50 文字の制限があります。
「Organization Path」リスト	ユーザーの分類方法としてシステム管理者により定義されるリスト。
「List」ボタン	「Option List」画面（5-18 ページ）が表示されます。
「Password」フィールド	新規ユーザー・ログインのパスワード。このフィールドには 50 文字の制限があります。

機能	説明
「Confirm Password」フィールド	スペルを確認するために、前のフィールドのパスワードを再入力します。同様の制限が適用されます。
「Full Name」フィールド	新規ユーザーの完全な名前。このフィールドには 50 文字の制限があります。
「E-Mail Address」フィールド	ユーザーに関連付けられた電子メール・アドレス。ワークフローおよびサブスクリプションに使用されます。
「User Type」フィールド	ユーザーの分類方法としてシステム管理者により定義される属性のリスト。
「User Locale」フィールド	ユーザーのロケール。これにより、ユーザー・インタフェースの言語および日付 / 時間の書式が指定されます。ロケール・オプションは、システム管理者が有効化する必要があります。 詳細は、『Using Content Server in International Environments』を参照してください。 **注意 :** sysmanager ロールを持つユーザーのユーザー・ロケールを変更した場合は、ユーザーのロケール言語で表示されるように、管理サーバー・インタフェースの管理サーバー・サービスを再起動する必要があります。
「Override」チェック・ボックス	これらの設定は、ユーザーがグローバル・ユーザーから外部ユーザーに変更された場合、またはユーザー情報がコンテンツ・サーバーへのカスタム・プラグインにより自動的に割り当てられた場合にのみ適用されます。 **選択 :** 外部（LDAP サーバーからのユーザー属性など）から割り当てられたユーザー情報が、「Add User」/「Edit User」画面に割り当てられたユーザー情報で上書きされます。 **選択解除 :** コンテンツ・サーバーに割り当てられたユーザー情報が、外部から割り当てられたユーザー情報で上書きされます。

「Add User」/「Edit User」画面：「Roles」タブ



「Add User」/「Edit User」画面の「Roles」タブは、ユーザーへのロールの割当てに使用します。このタブにアクセスするには、「Add User」/「Edit User」画面（5-10 ページ）で**「Roles」**をクリックします。

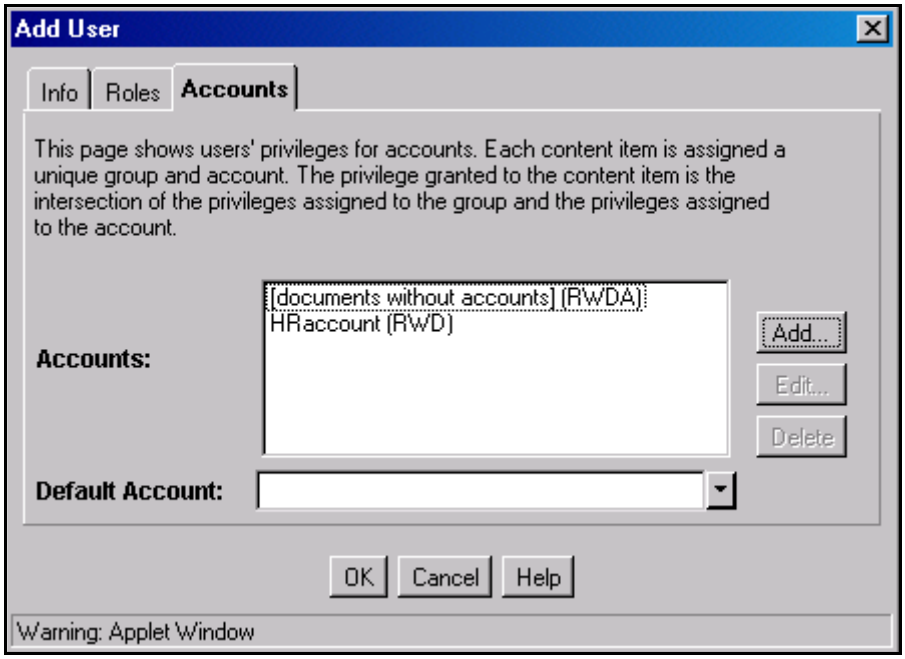
機能	説明
「Roles」リスト	これらのロールは「Roles」フィールドに表示されます。
「Groups/Rights」リスト	選択したロールに関連付けられているセキュリティ・グループ権限が表示されます。
「Add Role」ボタン	「Add Role」画面（5-16 ページ）が表示されます。この画面では、ドロップダウン・リストからロールを選択できます。
「Remove Role」ボタン	選択したロールをユーザー・ログインから削除します。

「Add Role」画面

「Add Role」画面は、ユーザーへのロールの割当てに使用します。この画面にアクセスするには、「Add User」/「Edit User」画面 :「Roles」タブ（5-15 ページ）で「**Add Role**」をクリックします。

機能	説明
「Role Name」フィールド	ユーザーに割り当てるロールを選択します。

「Add User」/「Edit User」画面 :「Accounts」タブ

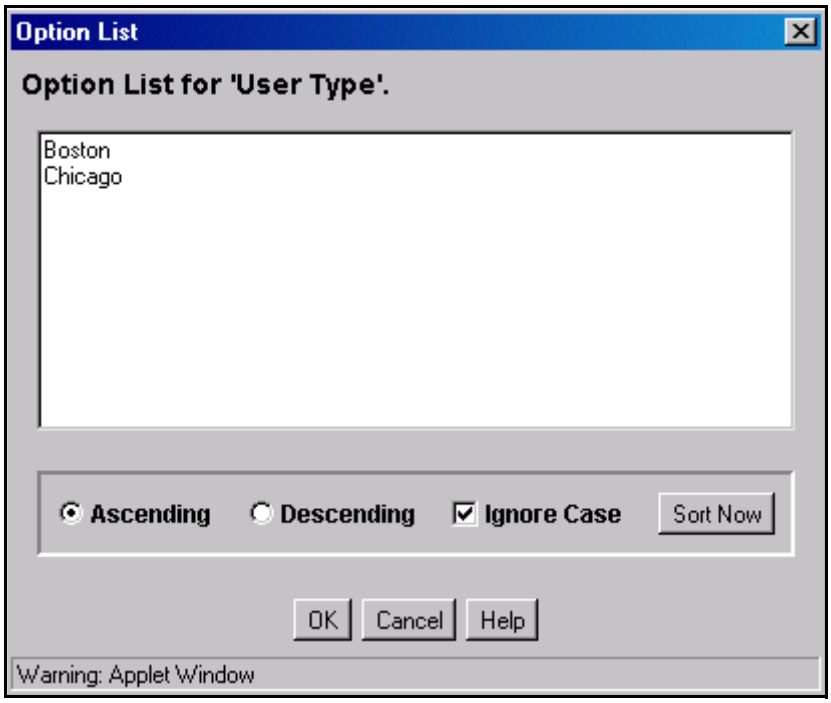


「Add User」/「Edit User」画面の「Accounts」タブは、ユーザーへのアカウントの割当てに使用します。このタブにアクセスするには、「Add User」/「Edit User」画面（5-10 ページ）で「**Accounts**」をクリックします。

注意 : このタブは、アカウントが有効化されている場合にのみ使用できます。詳細は、第 4 章「内部セキュリティ : アカウントの使用」を参照してください。

機能	説明
「Accounts」リスト	このユーザー・ログインに割り当てられているアカウントがリストされます。デフォルトで、すべての新規ユーザーには、アカウントにはないドキュメントの読取り、書込み、削除および管理権限が割り当てられています。
「Add」ボタン	アカウント権限の追加 / 編集画面（4-12 ページ）が表示されます。
「Edit」ボタン	アカウントの事例（4-13 ページ）が表示されます。
「Delete」ボタン	新規アカウントを削除できます。
「Default Account」リスト	このユーザーの「Content Check In Form」ページに、デフォルト値として入力されるアカウントを選択します。ユーザーが少なくとも RW 権限を持っているすべてのアカウントがリストされます。

「Option List」画面



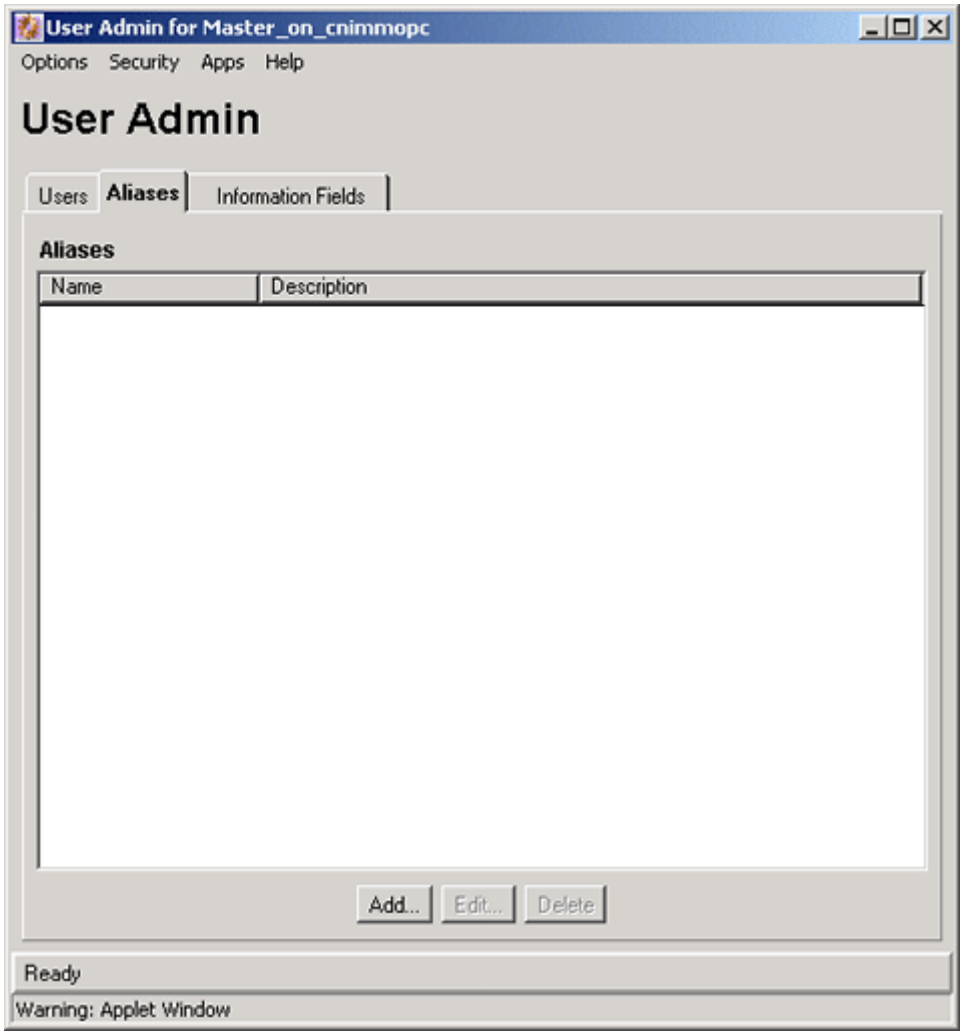
「Option List」画面は、ユーザーのグループ化に使用できるオプションのリストの作成に使用します。この画面には、インタフェースの複数の場所からアクセスできます。この画面には、「Add User」/「Edit User」画面 :「Info」タブ（ローカル・ユーザー）（5-11 ページ）および「Add User」/「Edit User」画面 :「Info」タブ（グローバル・ユーザー）（5-13 ページ）の「User Type」のプルダウン・メニューを使用してアクセスします。

注意 : これらのオプション・リストにはコンテンツ・サーバーのセキュリティ機能がありません。単に、ユーザーをグループ化するための手段です。

機能	説明
「Option」リスト	「User Type」または「Organization Path」に対して選択可能な値を入力します。各値は、値の間にキャリッジ・リターンを入力して、別々の行に指定する必要があります。
「Ascending」オプション	リストがアルファベット順にソートされます。
「Descending」オプション	リストがアルファベットの逆の順序でソートされます。

機能	説明
「Ignore Case」チェック・ボックス	**選択 :** 大 / 小文字に関係なく、リストがアルファベット順にソートされます。 **選択解除 :** 大文字で始まる値が、小文字で始まる値とは別にグループ化されます。
「Sort Now」ボタン	「Ascending」、「Descending」および「Ignore Case」オプションで指定された方法で、リストがソートされます。

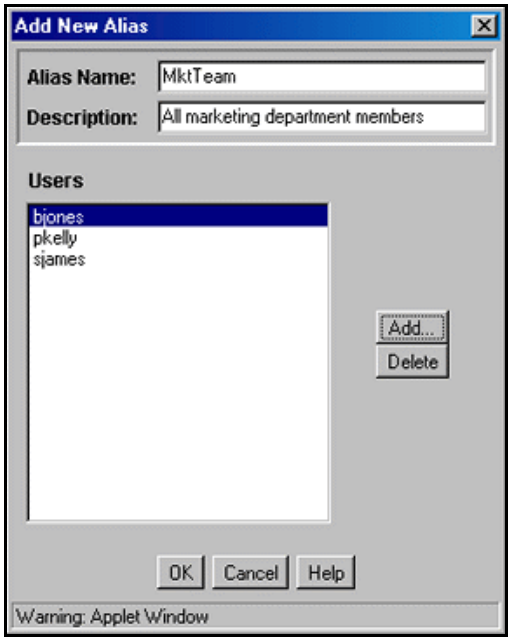
「User Admin」画面 : 「Aliases」タブ



「User Admin」画面の「Aliases」タブは、別名の追加、編集および削除に使用します。このタブにアクセスするには、ユーザー管理アプリケーション（2-20 ページ）を表示して**「Aliases」**をクリックします。

機能	説明
「Name」列	別名が表示されます。
「Description」列	各別名の説明。
「Add」ボタン	「Add New Alias」/「Edit Alias」画面（5-20 ページ）が表示されます。
「Edit」ボタン	「Add New Alias」/「Edit Alias」画面（5-20 ページ）が表示されます。
「Delete」ボタン	選択した別名を削除できます。

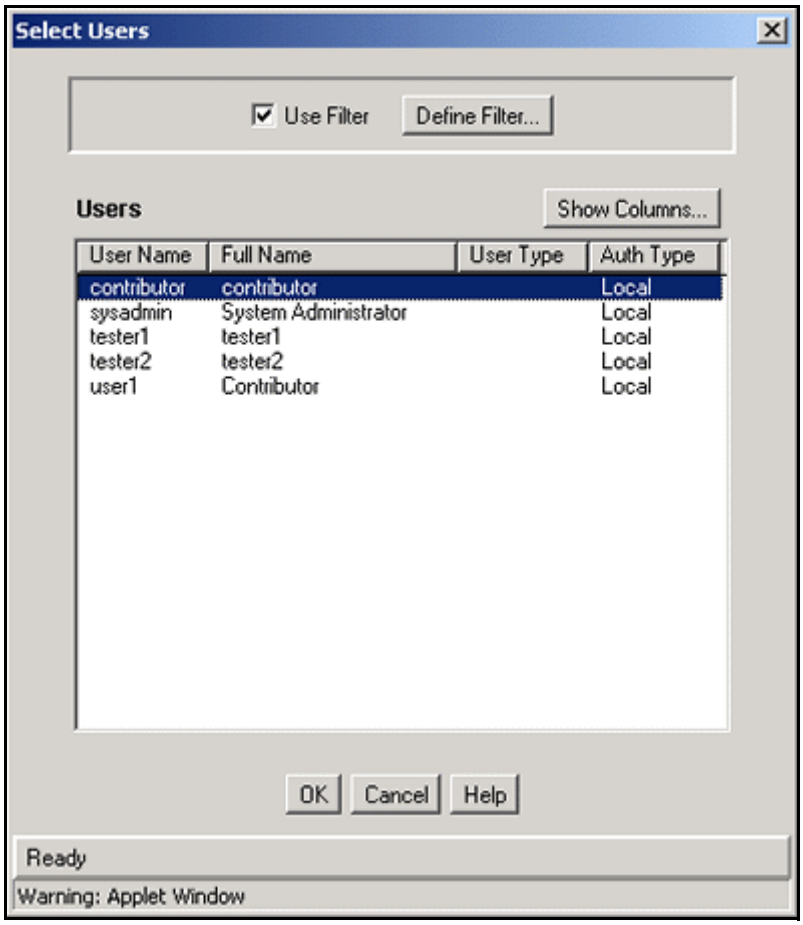
「Add New Alias」/「Edit Alias」画面



「Add New Alias」/「Edit Alias」画面は、別名のユーザー・ログインの追加、編集および削除に使用します。この画面にアクセスするには、「User Admin」画面：「Aliases」タブ（5-19 ページ）で**「Add」**または**「Edit」**をクリックします。

機能	説明
「Alias Name」フィールド	別名は 30 文字に制限されています。空白、タブ、ライン・フィード、キャリッジ・リターン、;、:、^、?、@、&、+、"、#、%、<、*、~、| は使用できません。
「Description」フィールド	最大 80 文字。
「Users」リスト	別名に含まれているユーザー・ログインが表示されます。
「Add」ボタン	「Select Users」画面（5-22 ページ）が表示されます。
「Delete」ボタン	選択したユーザー・ログインを別名から削除します。

「Select Users」画面



「Select Users」画面は、別名へのユーザー・ログインの追加に使用します。この画面にアクセスするには、「Add New Alias」/「Edit Alias」画面（5-20 ページ）で**「Add」**をクリックします。

機能	説明
「Use Filter」チェック・ボックス	このチェック・ボックスは、「Choose the Authorization Type」画面（5-9 ページ）で定義された「Users」リストを絞り込む場合に選択します。
「Define Filter」ボタン	「Choose the Authorization Type」画面（5-9 ページ）が表示されます。
「Show Columns」ボタン	「Show Columns」画面（2-24 ページ）が表示されます。

機能	説明
「Users」リスト	フィルタ設定に一致するユーザーが表示されます。列の説明は、「Choose the Authorization Type」画面（5-9 ページ）を参照してください。

副管理者

この項の内容は次のとおりです。

概念

❖ 副管理者について（5-23 ページ）

タスク

❖ 副管理者の設定（5-27 ページ）

インタフェース

❖ 副管理者のインタフェース：「Edit Rights」画面（5-28 ページ）

副管理者について

副管理者は、システム管理者によって 1 つ以上の管理ツール（ユーザー管理、Web レイアウト・エディタ、リポジトリ・マネージャおよびワークフロー管理）に対して特定の権限を割り当てられたユーザーで、それらの権限に対応するソフトウェアの一部を管理します。admin ロールを持つユーザーのみが、構成マネージャおよびアーカイバ・ツールにアクセスできます。

副管理者は、管理タスクを実行できるよう、少なくとも 1 つのセキュリティ・グループの管理権限を持っている必要があります。一般的に、副管理者は、特定のセキュリティ・グループまたはアカウントの管理者に割り当てられます。

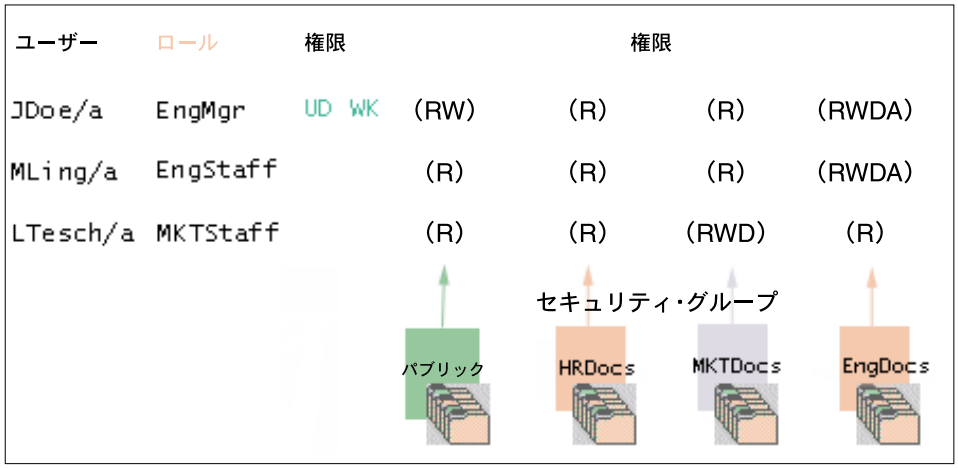
次の表に、副管理者が実行できる機能を説明します。

権限	説明
UserAdmin	ロールおよびアカウントが、副管理者のロールおよびアカウントのサブセットであるユーザーを追加、編集および削除できます。

権限	説明
WebLayout	副管理者が、対応するセキュリティ・グループおよびアカウントの管理権限を持っている「Library」ページを追加、編集および削除できます。
RepMan	ドキュメントの表示、および副管理者が管理権限を持っているドキュメントに対するリポジトリ・マネージャ機能（更新、承認、削除など）の実行を行うことができます。
Workflow	副管理者が管理権限を持っているセキュリティ・グループ内のワークフローを追加、編集または削除できます。

図 5-2 に示されている JDoe の副管理者権限と対応する説明について考察します。

図 5-2　副管理者権限の例



- **UserAdmin:** ユーザー MLing のロールおよびアカウントは JDoe のロールおよびアカウントのサブセットであるため、JDoe にはユーザー MLing を追加、編集および削除する権限があります。ただし、MKTDocs セキュリティ・グループに対するユーザー LTesch の権限は JDoe より多いため、JDoe は LTesch を追加、編集または削除できません。
- **WebLayout:** JDoe には WebLayout 権限がないため、Web レイアウト・エディタの管理タスクは実行できません。
- **RepMan:** JDoe は、アカウント a の EngDocs セキュリティ・グループに存在するドキュメント、または EngDocs セキュリティ・グループに存在し、アカウントが割り当てられていないドキュメントに対して、リポジトリ・マネージャ機能を実行できます。ただし、JDoe は、アカウント b や c の EngDocs セキュリティ・グループに存在するドキュメント、またはその他のセキュリティ・グループのドキュメントに

対する管理権限を持っていないため、これらのドキュメントに対してリポジトリ・マネージャ機能を実行することはできません。

- **Workflow:** JDoe は、EngDocs セキュリティ・グループのワークフローを追加、編集および削除できます。

UserAdmin 権限

UserAdmin 権限を持っているユーザーは、次のタスクを実行できます。

- 新規ユーザーを追加できます。ただし、割り当てられるのは、副管理者が属するロールおよび副管理者が権限を持っているアカウントのみです。

  たとえば、副管理者が EngAdmin、EngContributor および EngUser というロールに属しているとします。この副管理者が新規ユーザーに割り当てられるのは、これら 3 つのロールのみです。この副管理者は contributor というロールは割り当てられません。

- 副管理者が属するロールのサブセット、および副管理者が権限を持っているアカウントのサブセットを所有するユーザーを編集および削除できます。

  たとえば、副管理者が HTAdmin、HTContributor および HTUser というロールに属しているとします。副管理者は、副管理者のロールのサブセットであるロールに属するユーザーのみを編集または削除できます。ユーザーが MKTUser というロールに属する場合、この副管理者はこのユーザーを編集または削除できません。

UserAdmin 権限を持っているユーザーは、次のタスクを実行できません。

- 副管理者より多くの権限を持つ新規ユーザーの作成
- ロールの追加、編集または削除
- セキュリティ・グループの追加、編集または削除
- 別名の作成

WebLayout 権限

WebLayout 権限を持っているユーザーは、次のタスクを実行できます。

- グループおよびアカウントの権限を持っている場合は、それらのディレクトリ・ページを作成できます。

注意 : レポートとしてのローカル・ページを作成できるのは、管理者のみです。適切な権限を持っている管理者または副管理者は、ディレクトリとしてのローカル・ページを作成できます。

- 副管理者には、「Options」メニューの「Query Result Pages」の機能、および権限のないアプリケーションへのアクセス権はありません。また、前後の項で説明されているように、副管理者の表示、編集および削除権限は制限されています。
- 副管理者が「weblayout」ペインのページを参照するには、その親を表示できる必要があります。副管理者がページを削除するには、そのページがディレクトリ・ページで、副管理者がそのページとそのすべての子に対するアクセス権を持っている必要があります。
- 副管理者がページのコンテンツを参照するには、そのページおよびそのすべての親に対する読取りアクセス権を持っている必要があります。これにより、「Library」リンクを介して表示できないページを、副管理者が参照するのを防ぐことができます。
- 問合せ結果ページの追加、編集および削除のタスクを実行できるのは、WebLayout 権限を持つ副管理者ではなく管理者のみです。

RepMan 権限

RepMan 権限を持っているユーザーは、次のタスクを実行できます。

- RepMan 権限を持っている管理者および副管理者は、リポジトリ・マネージャでコンテンツ・アイテムのリビジョンのリストを表示できます。管理者はすべてのコンテンツ・アイテムを表示できますが、RepMan 権限を持つ副管理者が表示できるのは、セキュリティ・グループおよびアカウントに対する管理権限を持っているコンテンツ・アイテムのみ（該当する場合）です。メタデータ・フィールドとリビジョン・ステータスをフィルタ基準として指定することで、リビジョン・リストを検索できます。

❖ 管理者（副管理者ではない）は、「Repository Manager」画面の「Indexer」タブを使用して次のことを実行できます。

- **検索索引の更新：**索引データベースを徐々に更新できます。索引は、サーバーにより約 5 分ごとに自動的に更新されるため、通常は必要ありません。
- **コレクションの再作成：**検索索引が全体的に再作成され、古い索引コレクションが新しい索引コレクションに置き換えられます。

Workflow 権限

Workflow 権限を持っているユーザーは、次のタスクを実行できます。

❖ 副管理者が管理権限を持っているセキュリティ・グループ内のワークフローを追加、編集または削除できます。

副管理者の設定

副管理者を設定する際には、管理タスクの実行に使用するセキュリティ・グループおよび副管理者ロールに管理権限を付与してください。副管理者の権限は、管理権限が少なくとも 1 つのセキュリティ・グループに関連付けられていないと使用できません。

また、副管理者がユーザーを追加する際、ユーザーに割り当てられるのは副管理者のロールのみであるため、副管理者に UserAdmin 権限がある場合は複数のロールを割り当ててください。副管理者に subadmin ロールのみを割り当てた場合、管理するユーザーに割り当てることができるのはこのロールのみです。

副管理者を設定するには、次のようにします。

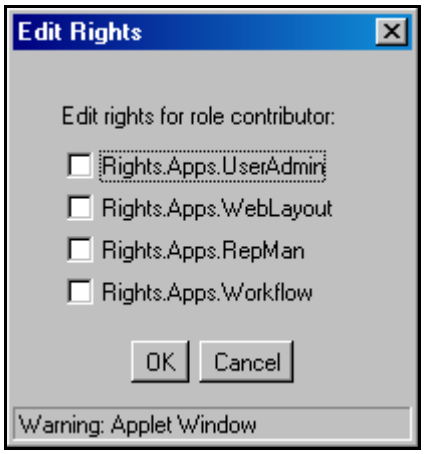
1. HRsubadmin などの副管理者ロールを追加します。詳細は、3-10 ページの「ロールの作成」を参照してください。
2. 「Permissions By Role」画面（3-15 ページ）で、副管理者に権限を割り当てます。
   a. 副管理者ロールを選択します。
   b. **「Edit Permissions」**をクリックします。
      「Edit Permissions」画面（3-16 ページ）が表示されます。
   c. 副管理者が管理タスクを実行するセキュリティ・グループを選択します。
   d. **「Admin」**権限を選択します。
   e. **「OK」**をクリックします。
   f. **「Edit Rights」**をクリックします。
      副管理者のインタフェース：「Edit Rights」画面（5-28 ページ）が表示されます。

g. 副管理者に 1 つ以上の権限を選択します。

h. 「**OK**」をクリックします。

3. 副管理者ロールをユーザーに割り当てます。詳細は、5-29 ページの「ユーザー情報フィールド」を参照してください。

副管理者のインタフェース：「Edit Rights」画面



「Edit Rights」画面は、ロールへの副管理者権限の割当てに使用します。この画面にアクセスするには、「Permissions By Role」画面（3-15 ページ）でロールを選択し、「**Edit Rights**」をクリックします。

機能	説明
「Rights.Apps.UserAdmin」チェック・ボックス	ユーザー管理アプリケーションに副管理者権限を割り当てます。詳細は、5-25 ページの「UserAdmin 権限」を参照してください。
「Rights.Apps.WebLayout」チェック・ボックス	Web レイアウト・エディタ・アプリケーションに副管理者権限を割り当てます。詳細は、5-25 ページの「WebLayout 権限」を参照してください。
「Rights.Apps.RepMan」チェック・ボックス	リポジトリ・マネージャ・アプリケーションに副管理者権限を割り当てます。詳細は、5-26 ページの「RepMan 権限」を参照してください。
「Rights.Apps.Workflow」チェック・ボックス	ワークフロー管理アプリケーションに副管理者権限を割り当てます。詳細は、5-27 ページの「Workflow 権限」を参照してください。

ユーザー情報フィールド

この項の内容は次のとおりです。

概念

タスク

インタフェース

ユーザー情報フィールドについて

ユーザー情報では、フルネーム、パスワードおよび電子メール・アドレスなど、ユーザーの一意の属性を定義します。ユーザー情報フィールドでは、メタデータ・フィールドでコンテンツ・アイテムを説明するのと同様にユーザーを説明します。ユーザー情報はコンテンツ・サーバー・データベースに格納され、ユーザーのソート、コンテンツ・サーバーの Web ページでのユーザー情報の表示、またはユーザー属性に基づいた Web ページの表示のカスタマイズに使用できます。

次のユーザー情報フィールドは、システムで事前定義されています。これらのフィールドの削除、およびフィールド名やタイプの変更はできません。

Name	Type	Caption	Is Option List
dFullName	Long Text	Full Name	False
dEmail	Long Text	E-mail Address	False

Name	Type	Caption	Is Option List
dUserType	Text	User Type	True
dUserLocale	Text	User Locale	True

ユーザー情報フィールドの管理

この項では、ユーザー情報フィールドの管理に関連するタスクを説明します。

- 新しいユーザー情報フィールドの追加（5-30 ページ）
- オプション・リストの編集（5-30 ページ）
- ユーザー情報フィールドの編集（5-31 ページ）

新しいユーザー情報フィールドの追加

新しいユーザー情報フィールドを追加するには、次のようにします。

1. 「User Admin」画面 :「Information Fields」タブ（5-32 ページ）で、**「Add」**をクリックします。

   「Add Metadata Name Field」画面（5-34 ページ）が表示されます。

2. 新しいフィールド名を入力します。重複した名前は使用できません。最大フィールド長は 29 文字です。空白、タブ、ライン・フィード、キャリッジ・リターン、;、^、?、:、@、&、+、"、#、%、<、*、~、| は使用できません。

3. **「OK」**をクリックします。

   「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）が表示されます。

4. フィールドのプロパティを構成して、**「OK」**をクリックします。

5. **「Update Database Design」**をクリックします。

オプション・リストの編集

オプション・リスト・キーを編集するには、次のようにします。

1. 「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）で、「Enable Option List」チェック・ボックスを選択します。

2. **「Edit」**をクリックします。

   「Option List」画面（5-37 ページ）が表示されます。

3. オプションの値を追加、編集または削除します。
   - 各値は、別々の行に表示される必要があります。
   - 空白の行は、オプション・リストで空白の値になります。
4. リストをソートするには、ソート・オプションを選択して「**Sort Now**」をクリックします。
5. 「**OK**」をクリックします。

ユーザー情報フィールドの編集

ユーザー情報フィールドを編集するには、次のようにします。

1. フィールドをダブルクリックするか、フィールドを選択して「**Edit**」をクリックします。

   「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）が表示されます。
2. オプションの値を追加、編集または削除します。
3. 「**OK**」をクリックします。

情報フィールドのインタフェース画面

情報フィールドを定義する際には、次の画面を使用します。

❖ 「User Admin」画面：「Information Fields」タブ（5-32 ページ）

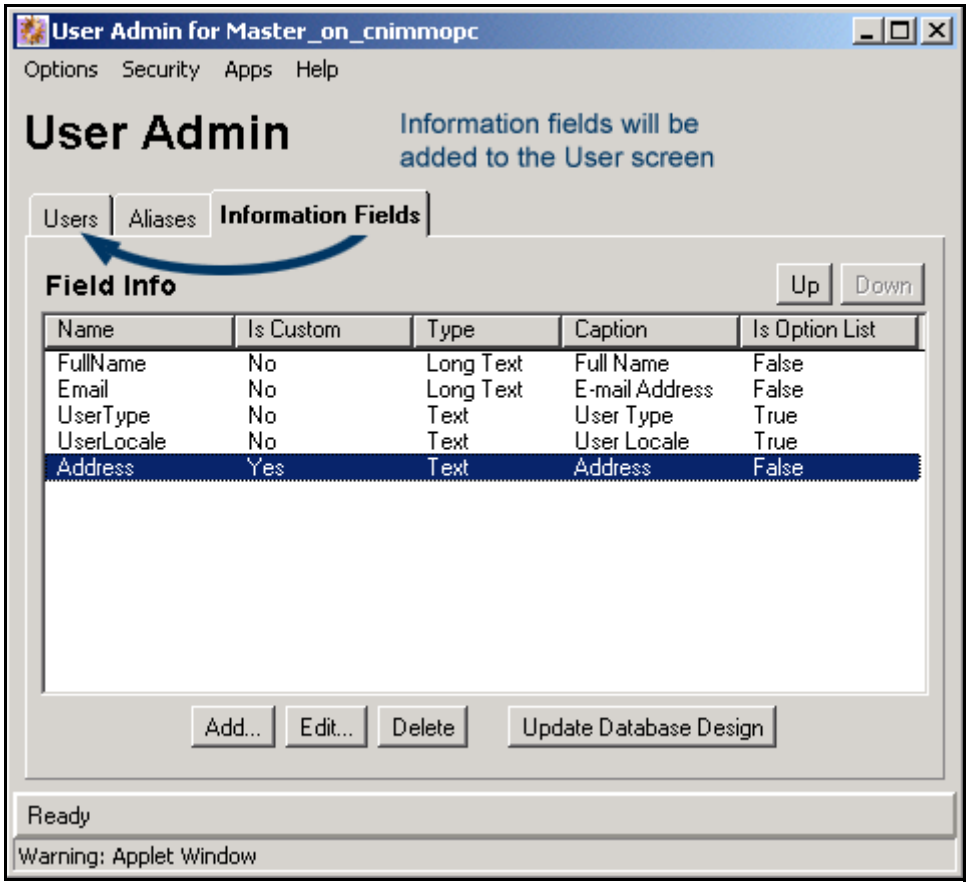
❖ 「Add Metadata Name Field」画面（5-34 ページ）

❖ 「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）

❖ 「Option List」画面（5-37 ページ）

❖ 「Update Database Design」画面（5-38 ページ）

「User Admin」画面 :「Information Fields」タブ



「User Admin」画面の「Information Fields」タブは、ユーザー情報フィールドの追加、編集および削除に使用します。このタブにアクセスするには、ユーザー管理アプリケーション（2-20 ページ）を表示して「**Information Fields**」をクリックします。

- 「Information Fields」タブにフィールドが追加されると、「Users」タブのユーザー情報にも追加されます。
- 新規ユーザー・フィールドの追加後に、検索索引を再作成する必要はありません。

機能	説明
「Up」ボタン	選択したユーザー情報フィールドが、リストの上に移動されます。
「Down」ボタン	選択したユーザー情報フィールドが、リストの下に移動されます。

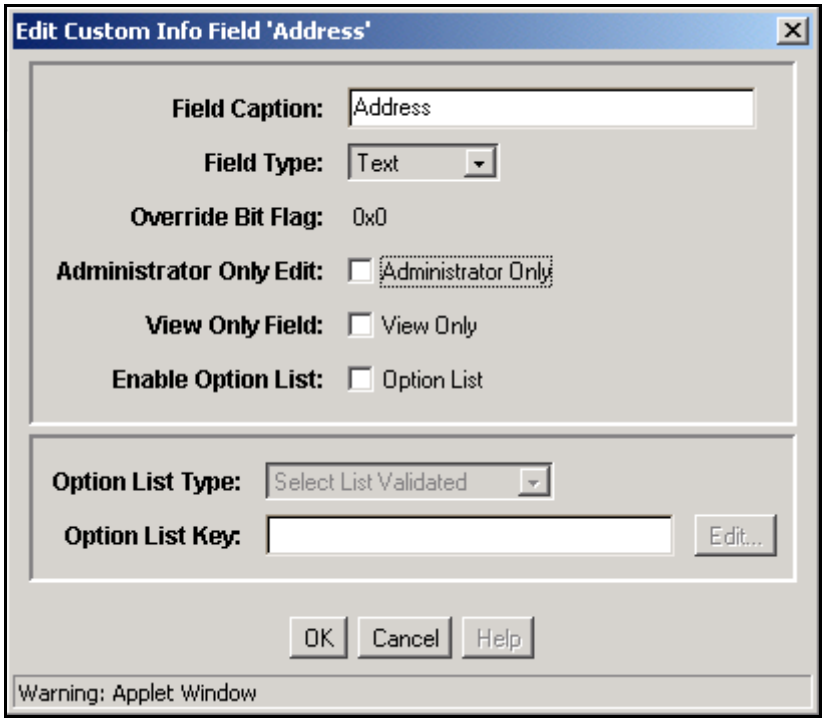
機能	説明
「Name」列	ユーザー情報フィールドの名前。
「Is Custom」列	**No:** システム（事前定義済）のユーザー情報フィールドであることを示します。 **Yes:** カスタムのユーザー情報フィールドであることを示します。
「Type」列	フィールドのタイプ。 **Text:** 30 文字。 **Long Text:** 100 文字。 **Date:** 日付書式（英語（米国）ロケールの場合、dd/mm/yyyy または dd/mm/yy など）。 **Memo:** 255 文字。 **Integer:** -231 ～ 231（-20 億～ +20 億）。定義により、整数は自然数であるため、小数およびカンマは許可されていません。
「Caption」列	コンテンツ・サーバーのページに表示されるフィールドのラベル。
「Is Option List」列	**False:** ユーザー情報フィールドに、オプション・リストはありません。 **True:** ユーザー情報フィールドにオプション・リストがあります。
「Add」ボタン	「Add Metadata Name Field」画面（5-34 ページ）が表示されます。この画面では、新しいフィールド名を追加できます。
「Edit」ボタン	「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）が表示されます。
「Delete」ボタン	選択したカスタムのユーザー情報フィールドを削除します。（システムのユーザー情報フィールドは削除できません。）
「Update Database Design」ボタン	「Update Database Design」画面（5-38 ページ）が表示されます。

「Add Metadata Name Field」画面

「Add Custom Info Field」画面は、カスタムのユーザー情報フィールドの名前の定義に使用します。この画面にアクセスするには、「User Admin」画面 : 「Information Fields」タブ（5-32 ページ）で「**Add**」をクリックします。

機能	説明
「Field Name」フィールド	重複した名前は使用できません。最大フィールド長は 29 文字です。空白、タブ、ライン・フィード、キャリッジ・リターン、;、^、?、:、@、&、+、"、#、%、<、*、~、| は使用できません。 **注意 :** カスタムのユーザー情報フィールドを追加すると、予約済の名前と競合しない一意の名前になるように、システムにより自動的に u という接頭辞が付けられます。ただし、データベース内の予約済の名前と競合する可能性があるため、ユーザー・ログイン表内の列に制限されている名前を誤って使用しないよう注意する必要があります。 たとえば、新しいカスタムのユーザー情報フィールドに ID という名前を付けると、システムにより接頭辞が追加され、結果は UID になります。この場合、UID は予約済のデータベース名であるためエラーが発生します。 同様に、カスタムのメタデータ・フィールドを定義すると、予約済の名前と競合しない一意の名前になるように、システムにより自動的に x という接頭辞が付けられます。カスタムのメタデータ・フィールドの追加の詳細は、5-34 ページの「「Add Metadata Name Field」画面」を参照してください。
「OK」ボタン	「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）が表示されます。

「Add Custom Info Field」/「Edit Custom Info Field」画面



「Add Custom Info Field」/「Edit Custom Info Field」画面は、ユーザー情報フィールドの定義に使用します。この画面にアクセスするには、次のいずれかを実行します。

- ❖ フィールド名を入力し、「Add Metadata Name Field」画面（5-34 ページ）で「**OK**」をクリックします。
- ❖ ユーザー情報フィールドを選択し、「User Admin」画面：「Information Fields」タブ（5-32 ページ）で「**Edit**」をクリックします。

機能	説明
「Field Caption」フィールド	コンテンツ・サーバーのページに表示されるフィールドのラベル。
Field Type	**Text:** 30 文字。 **Long Text:** 100 文字。 **Date:** 日付書式（英語（米国）ロケールの場合、dd/mm/yyyy または dd/mm/yy など）。 **Memo:** 255 文字。 **Integer:** -231 ～ 231（-20 億～ +20 億）。定義により、整数は自然数であるため、小数およびカンマは許可されていません。
Override Bit Flag	内部使用向けです。
Administrator Only Edit	**選択 :** フィールドは「User Profile」ページに表示されません。ただし、ユーザー管理アプレットを使用している管理ユーザーには、このフィールドが表示されます。 **選択解除 :** フィールドは「User Profile」ページに表示されます。
View Only Field	**選択 :** フィールドは「User Profile」ページに表示されますが、ユーザーは編集できません。 **選択解除 :** 「Administrator Only Edit」チェック・ボックスが選択解除されている場合、ユーザーは「User Profile」ページでこのフィールドを編集できます。
Enable Option List	このフィールドには、「Option List Type」および「Option List Key」で定義されたオプション・リストがあります。

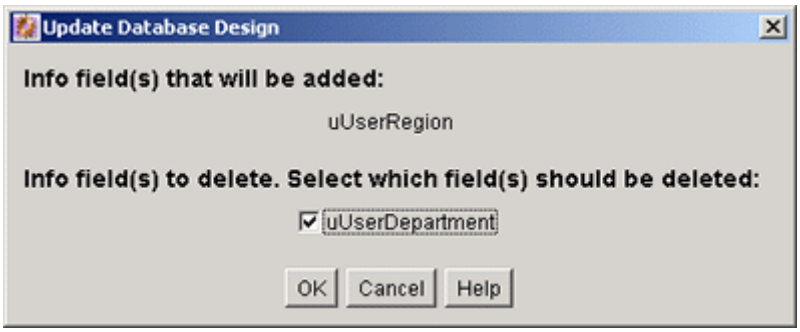
機能	説明
Option List Type	オプション・リストのタイプを指定します。 • **Select List Validated:** バッチ・ロードおよびアーカイバの場合は、このオプションを使用すると、指定されている値が該当フィールドの現在のオプションになっているユーザーのみがインポートされます。 • **Select List Not Validated:** バッチ・ロードおよびアーカイバの場合は、このオプションを使用すると、指定されている値が該当フィールドの現在のオプションになっていないユーザーがロードされます。 • **Edit and Select List:** テキスト・フィールドとコンボ・ボックスの両方が提供されます。ユーザーは、オプション・リストにない値を入力できます。 • **Edit and Multiselect List:** テキスト・フィールドとコンボ・ボックスの両方が提供されます。ユーザーは、オプション・リストにない値を入力できます。また、複数の値を選択または入力できます。
Option List Key	オプション・リストに表示される特定の値リストのフィールド・キャプションから生成される指定。このリストは、オプション・リスト・キーを使用する複数のフィールドで再利用できます。

「Option List」画面

「Option List」画面は、カスタムのユーザー情報フィールドのオプション・リストの作成に使用します。この画面にアクセスするには、「Enable Option List」チェック・ボックスを選択し、「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）で「**Edit**」をクリックします。

詳細は、5-18 ページの「「Option List」画面」を参照してください。

「Update Database Design」画面



「Update Database Design」画面は、コンテンツ・サーバー・データベースのユーザー情報フィールドの追加または削除に使用します。この画面にアクセスするには、ユーザー情報フィールドを追加または削除し、「Add Custom Info Field」/「Edit Custom Info Field」画面（5-35 ページ）で**「Update Database Design」**をクリックします。

機能	説明
Info field(s) that will be added	最後にデータベースが更新されてから追加されたユーザー情報フィールドが表示されます。
「Info field(s) to delete」チェック・ボックス	最後にデータベースが更新されてから削除されたユーザー情報フィールドが表示されます。 **選択 :** ユーザー情報フィールドがデータベースから削除されます。 **選択解除 :** ユーザー情報フィールドはデータベースから削除されません。このフィールドは、「User Admin」画面および「User Profile」ページでは表示されないままですが、データベースには存在します。

自動登録

この項の内容は次のとおりです。

概念

❖ 自動登録について（5-39 ページ）

タスク

❖ 自動登録の設定（5-39 ページ）

自動登録について

自動登録を使用すると、ユーザーが自身のコンテンツ・サーバー・ログイン（ユーザー名およびパスワード）を作成できるようになります。

- 自動登録されたユーザーは、グローバル・ユーザーとして作成されます（2-16 ページの「ユーザーのタイプ」を参照）。
- 自動登録をその他のユーザー・ログイン方法と組み合せることができます（ローカル・ユーザーは標準の「Login」ボタンを使用し、外部ユーザーは統合された Windows ログインを使用するなど）。
- 自動登録機能を有効化すると、ポータル・ナビゲーション・バーに「Self-Registration」リンクが追加されます。
- 自動登録方法の詳細は、『Oracle Content Server ユーザー・ガイド』を参照してください。

自動登録の設定

自動登録を設定して有効化するには、次のようにします。

1. 管理サーバーの「General Configuration」ページにある「Additional Configuration Variables」フィールド、または *<Install_Dir>*/config/config.cfg ファイルに、次の行を追加します。

```
UseSelfRegistration=true
SelfRegisteredRoles=contributor,guest
```

注意 : SelfRegisteredRoles 設定により、すべての自動登録ユーザーに割り当てられるロールが定義されます。値は、ロールのカンマ区切りのリストである必要があります。

2. アカウントが有効化されている場合は、「Additional Configuration Variables」フィールド、または config.cfg ファイルに次の行を追加します。

```
SelfRegisteredAccounts=Acme(RW),#none(RWDA),<$NewUser$>(RWDA)
```

注意 : SelfRegisteredAccounts 設定により、すべての自動登録ユーザーに割り当てられるアカウントが定義されます。値は、アカウントのカンマ区切りのリストで、各アカウントの後ろのカッコ内にアカウント権限が指定されている必要があります。次の特別なアカウントを指定できます。

- **#none** では、アカウントが指定されていないコンテンツ・アイテムに権限が割り当てられます。
- **#all** では、すべてのアカウントに権限が割り当てられます。
- **<$NewUser$>** では、ユーザー名（pkelly など）と同じアカウントが作成されます。

3. 「Admin Server 」で「**Save**」をクリックするか、config.cfg ファイルを保存して閉じます。
4. コンテンツ・サーバーを再起動します。
5. ポータル・ページを更新します。

重要 : ポータル・ページを更新するまで、ポータル・ナビゲーション・バーに「Self-Registration」リンクは表示されません。

6

外部セキュリティ：ACTIVE DIRECTORY

概要

この項の内容は次のとおりです。

概念

タスク

インタフェース

❖ 「Active Directory Configuration」ページ（6-17 ページ）

ACTIVE DIRECTORY の概要

この項の内容は次のとおりです。

Active Directory について

Microsoft Active Directory は、Windows 2000 Server 以降のバージョンに同梱されているディレクトリ・サービスです。特に、Windows ネットワーク環境で運用するために設計されています。Active Directory にはネットワーク上のオブジェクトの情報が格納され、この情報はアプリケーション、ユーザーおよびネットワーク管理者が使用できるようになります。Active Directory を使用すると、認可済のネットワーク・ユーザーは、1 回のログイン・プロセスでネットワーク上の任意の場所にあるリソースにアクセスできます。Active Directory には、ネットワークのリソースを管理するために、LDAP（Lightweight Directory Access Protocol）と同じ高レベルの機能が提供されています。

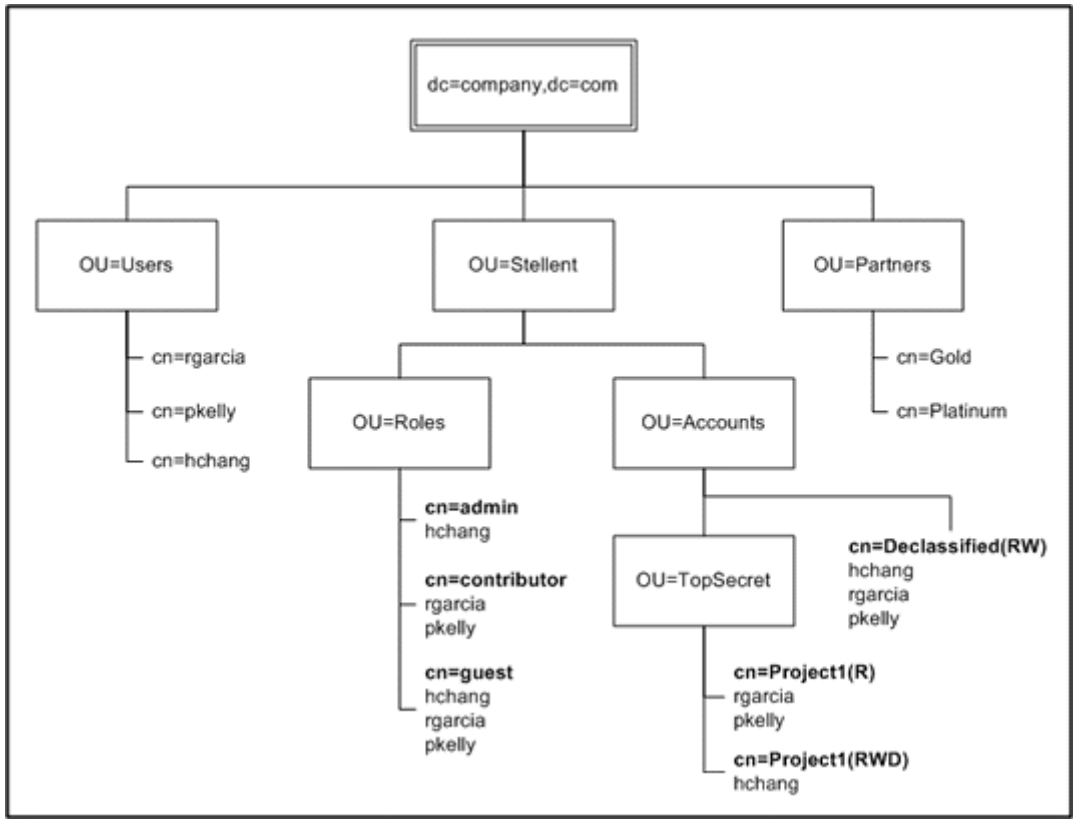
注意 : Active Directory セキュリティは、Windows のドメイン・ルールおよび制限事項の対象です。詳細は、6-4 ページの「ドメイン」および 6-7 ページの「ドメインおよび Oracle Content Server」を参照してください。

注意 : このガイドで説明されている直接統合ではなく、LDAP プロバイダを使用して Active Directory サーバーに対してユーザーを認証する場合は、カスタムの Active Directory LDAP コンポーネントをインストールおよび構成する必要があります。このコンポーネントの使用方法の詳細は、『Active Directory LDAP Component Administration Guide』を参照してください。

Active Directory 構造

Active Directory は、ディレクトリ・ツリーと呼ばれる LDAP 形式の階層構造でネットワーク・オブジェクトを編成します。図 6-1 のツリーの図で、典型的な Active Directory 構造を示します。

図 6-1 Active Directory 構造の例



この場合、ユーザーは次の DN（識別名）を持つグループに割り当てられます。

```
cn=Project1,OU=TopSecret,OU=Accounts,OU=Stellent,dc=company,dc=com
```

ここで、グループ DN は、次の LDAP 表記規則に準拠しています。

LDAP での略語	LDAP での意味	説明
dc	ドメイン・コンポーネント	ネーミング・コンテキストを指定する最上位レベルのユニット。
OU	編成ユニット	通常は、課、部門またはその他の個々のビジネス・グループを表します。Oracle 統合では、ロールやアカウントは一般的に OU として指定されます。
cn	共通名	一般的に、DN の最下位レベルの属性で、一意の名前を識別します。ユーザーの場合は、ユーザー ID の単位である uid でもかまいません。

ドメイン

Windows ネットワークにおいて、ドメインは、共通のドメイン名およびセキュリティ情報を共有するコンピュータのグループです。ドメインのセキュリティを管理するために、プライマリ・ドメイン・コントローラとして Windows Server マシンが 1 つ選択されます。ユーザーは、ユーザーのローカル・コンピュータにセキュリティ情報が定義されているローカル・ユーザーか、セキュリティがプライマリ・コントローラに管理されているグローバル（ドメイン）ユーザーのいずれかです。グローバル・ユーザーがドメインにログインすると、ユーザーのセキュリティ資格証明を取得するようプライマリ・コントローラに問合せが行われます。

技術ヒント : プライマリ・ドメイン・コントローラ・マシンに、最新の Windows Service Pack がインストールされていることを確認してください。Microsoft Windows 2000 Service Pack 1 または Service Pack 適用なしで稼働しているネットワーク環境では、Content Server セキュリティ統合はサポートされていません。

セキュリティに影響を及ぼし、ネットワーク・ユーザーが Content Server インスタンスにアクセスできるかどうかを決定する Windows ネットワーク・コンポーネントが 3 つあります。

- 通常は、グローバル（またはドメイン）グループ、ローカル・グループを使用することで、ネイティブ・モード・ドメインの場合はユニバーサル・グループを使用することで、ドメイン・セキュリティが確立されます。（ユニバーサル・グループは、複合モード・ドメインでは使用できません。）
- 各グローバルまたはローカル・グループには、配布グループまたはセキュリティ・グループとして定義するスコープがあります。Content Server と統合する場合、Content Server のロールおよびアカウントにマッピングできるのは、Windows セ

キュリティ・グループのみです。配布グループでは、ユーザー資格証明の認証に十分な情報が提供されません。

- 各ドメインは、複合モード・ドメイン、または Windows 2000 Server のみを含むことができるネイティブ・モード・ドメインとして設定されます。

グループのタイプおよびドメインのモードによっては、グループをネストさせることができます。たとえば、ユーザーをグローバル・グループに割り当て、そのグローバル・グループを、ローカル・コンピュータのリソースへのアクセス権を持つローカル・グループに割り当てられます。

次の表に、Windows セキュリティ・グループがどのようにネストできるかを示します。

グループ・タイプ	ドメイン・モード	ローカル・グループのネスト	グローバル・グループのネスト	ユニバーサル・グループのネスト
ローカル	複合モード	X	○	使用不可
	ネイティブ・モード	○	○	○
グローバル	複合モード	X	X	使用不可
	ネイティブ・モード	X	○	X
ユニバーサル（Active Directory）	複合モード	使用不可	使用不可	使用不可
	ネイティブ・モード	X	○	○

信頼できるドメイン

小規模な組織では、ユーザー・アカウントおよびリソースを単一のドメインに格納できますが、大規模な組織では、通常複数のドメインを確立します。たとえば、ユーザー・アカウントはあるドメインに格納し、リソースは別のドメインに格納します。Windows Server を使用すると、複数のドメインのセキュリティが信頼関係で統合されます。信頼関係は、2 つのドメインを、両方のドメインのリソースへのアクセスを認証できる 1 つの管理単位に結合するリンクです。

信頼関係には 2 つのタイプがあります。

- **一方向の信頼関係 :** 一方のドメインが、もう一方のドメインのユーザーによるリソースの使用を信頼します。より具体的には、一方のドメインが、もう一方のドメインのドメイン・コントローラによる、そのドメイン内のユーザー・アカウントの検証を信頼します。

- **双方向の信頼関係 :** 一方向の信頼が 2 つ設定されるため、それぞれのドメインがもう一方のドメインのユーザーを信頼します。ユーザーはどちらのドメインのコンピュータからもログインでき、どちらのドメインのリソースも使用できます。どちらのドメインのグローバル・グループも、両方のドメインのリソースに権限を付与できます。

関連項目

– ドメインおよび Oracle Content Server（6-7 ページ）

ACTIVE DIRECTORY セキュリティの統合

この項の内容は次のとおりです。

Microsoft ログイン

Active Directory セキュリティを Content Server と統合すると、ユーザー・ログイン、パスワードおよび権限は Active Directory 情報から導出されます。ポータル・ナビゲーション・バーの「Microsoft Login」ボタンを使用すると、ユーザーは、ユーザー名およびパスワードを再入力せずに Content Server にログインできます。標準の「Login」ボタンをクリックすると、ユーザー名とパスワードを要求されます。

注意 : ユーザーの「User Profile」ページで「Override」チェック・ボックスが選択されている場合、Active Directory 資格証明から導出されたユーザー情報は、Content Server データベースに定義されているユーザー情報で上書きされます。

技術ヒント : 次のような場合に、ブラウザで Active Directory 認証が使用されます。

- 「Microsoft Login」ボタンがクリックされると、Content Server データベースではなく Active Directory からユーザー情報が取得されます。
- ユーザーの資格証明が最初にContent Serverに送信された際にCookieがインストールされているため、Active Directory セキュリティが有効化されている場合に、ユーザーがログインせずにセキュアな Content Server リソースをリクエストすると、ブラウザでは Active Directory 認証が使用されます。

技術ヒント : テスト目的で別の Content Server ユーザーとしてログインする場合、次のようにして、Internet Explorer の「Microsoft Login」ボタンからログインを強制できます。

1. Internet Explorer で、**「ツール」→「インターネット オプション」**を選択します。
2. 「セキュリティ」タブをクリックします。
3. 「インターネット」ゾーン（または Content Server が含まれるゾーン）をクリックします。
4. **「レベルのカスタマイズ」**をクリックします。
5. **「ユーザー認証」**の**「ログオン」**で、**「ユーザー名とパスワードを入力してログオンする」**を選択します。
6. **「OK」**を 2 回クリックします。

Active Directory セキュリティの制限事項

次に、Active Directory セキュリティの制限事項を示します。

- **Web サーバー :** IIS 5.0 以上を使用する必要があります。
- **ユーザー :** Content Server にセキュアにアクセスするには、ユーザーは、Windows ドメインのグローバルまたはローカル・グループに属している必要があります。（ドメイン・ユーザーは、ドメイン・グループに属さなくてもゲスト・アクセス権を付与されます。）

注意 : Active Directory セキュリティは、Windows のドメイン・ルールおよび制限事項の対象です。詳細は、6-4 ページの「ドメイン」および 6-7 ページの「ドメインおよび Oracle Content Server」を参照してください。

ドメインおよび Oracle Content Server

Content Server インスタンスを Windows ネットワーク・ドメインと統合する際には、考慮事項がいくつかあります。

- ローカル・ユーザーには、Content Server のロールおよびアカウントへのアクセス権を付与できません。Content Server アクセスはグループ名によって決定されるため、Content Server ユーザーはグローバル・グループまたはローカル・グループに割り当てられている必要があります。
- ドメイン・ユーザーは、ユーザー名に追加された DOMAINNAME¥ 接頭辞で識別されます。
  - プライマリ・ドメイン・コントローラのドメインは推測されるため、Content Server と同じドメインのグローバル・グループのユーザーは、Content Server へのログイン時に DOMAINNAME¥ 接頭辞を含める必要はありません。

- ローカル・グループのユーザーは、ユーザー名を認識するために、Content Server へのログイン時に DOMAINNAME¥ 接頭辞を含める必要があります。
- Content Server とは異なるドメインのグループのユーザーは、ユーザー名を認識するために、Content Server へのログイン時に DOMAINNAME¥ 接頭辞を含める必要があります。

❖ Content Server ユーザーが Content Server ドメインとは異なるドメインのグローバル・グループのメンバーである場合は、それらのドメイン間に双方向の信頼関係を作成する必要があります。

❖ あるドメインのユーザーを別のドメインにある Content Server のロールにマップする場合は、ロール名にドメイン名を含める必要があります。次に例を示します。

- Content Server が corporate ドメインに存在するとします。
- ユーザーは、HR ドメインの HRStaff グループに属するとします。
- ユーザーには、HR¥HRStaff という名前の Content Server ロールに対する権限が付与されます。HRStaff という名前のロールに対する権限は付与されません。

関連項目

– ドメイン（6-4 ページ）

Active Directory の認証プロセス

Active Directory セキュリティが Content Server と統合されている場合は、IIS と Web サーバー・フィルタが連携し、次のようにしてユーザーの資格証明を認証します。

1. クライアントにより、IIS Web サーバーへのリクエストが行われます。
2. Web サーバー・フィルタでリクエストされたリソースの資格証明が要求される場合には、Web サーバー・フィルタにより、ユーザーが Content Server の内部ユーザーとして定義されているかどうかが確認されます。
   - ユーザーがローカルまたはグローバルの Content Server ユーザーとして定義されている場合は、Content Server でこのユーザーに定義されているロール、アカウントおよびユーザー属性が使用されます。
   - ユーザーが定義されていない場合、または Content Server の外部ユーザーとしてのみ定義されている場合は、Web サーバー・フィルタでチャレンジ / レスポンス・シーケンスが開始されます。
     a. Web サーバーにより、Active Directory サーバーにユーザー・パスワードの問合せが行われます。
     b. Web サーバー・フィルタにより、ユーザー・パスワードが検証されます。
     c. チャレンジ / レスポンス・シーケンスが正常に完了すると、Web サーバー・フィルタにより、Active Directory サーバーからユーザーが属するグループが取得されます。

d. ユーザーの Active Directory グループが Content Server のロールおよびアカウントにマッピングされます。（詳細は、6-9 ページの「ロールおよびアカウントのマッピング」を参照してください。）

e. 「Active Directory Configuration」ページ（6-17 ページ）に指定されている場合は、Web サーバー・フィルタにより、Active Directory サーバーから電子メールやユーザー・タイプなどのユーザー情報が取得されます。

3. リクエストが CGI URL の場合、そのリクエストは、ユーザーのロールおよびアカウントとともに Content Server に転送されます。

4. リクエストが静的 URL の場合、ユーザーがリクエストされたリソースにアクセスするための十分な権限を持っていることを確認するために、Web サーバー・フィルタによりユーザーのロールおよびアカウントが確認されます。
   - ユーザーに十分な資格証明がない場合は、エラー・ページが取得されます。
   - ユーザーに十分な資格証明がある場合は、そのリクエストは、ユーザーのロールおよびアカウントとともに Content Server に転送されます。

ロールおよびアカウントのマッピング

Active Directory セキュリティが Content Server と統合されている場合、ユーザーが属する Active Directory グループは、次のようにして Content Server のロールおよびアカウントにマッピングされます。

- ❖ グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）（6-10 ページ）および完全なグループ名（6-11 ページ）の設定は、ユーザーのロールおよびアカウントを判断するためのグループ名の解析に使用されます。
- ❖ グループ名をロールとして解析し、Content Server ロールの名前に一致した場合、ユーザーはそのロールに基づいて権限を付与されます。
- ❖ グループ名をカウントとして解析すると、ユーザーはそのアカウントを割り当てられます。この方法で、Active Directory グループから新しいアカウントを作成できます。
- ❖ Content Server ロールまたはアカウント接頭辞に一致しない解析済のグループ名は無視されます。
- ❖ アカウント権限は、グループ名自体またはデフォルトの権限設定から判断されます。詳細は、6-13 ページの「アカウント権限」を参照してください。

グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）

グループのフィルタ処理は、Active Directory のグループ名のどの部分を Content Server のロールまたはアカウントにマッピングするかの指定に使用されます。

- 「Active Directory Configuration」ページ（6-17 ページ）でグループのフィルタ処理が有効化されている場合、「Role Prefix」および「Account Prefix」フィールドは、各ユーザーのグループ名のフィルタ処理に使用されます。ロール接頭辞およびアカウント接頭辞は無制限に指定できます。これらの接頭辞は、Active Directory の各グループ名と比較されるサブストリングです。グループ名に接頭辞サブストリングがある場合は、その接頭辞より後ろのその他のグループ名（ディレクトリ・ツリーの下位レベル）は、ロールまたはアカウントとして解析されます。結果のロールおよびアカウントのマッピングは、完全なグループ名（6-11 ページ）の設定が有効化されているかどうかによって異なります。
- グループのフィルタ処理が無効化されている場合、すべてのグループ名は完全なグループ名（6-11 ページ）の設定に基づいて、Content Server のロールとして解析されます。
- 各ロール接頭辞およびアカウント接頭辞には深さ（6-12 ページ）パラメータがあり、有効なロールまたはアカウントとみなされるために、接頭辞とそのグループのグループ名の最後のユニットの間に存在可能な最大のレベル数を指定できます。
- 特定の接頭辞の深さパラメータにアスタリスク（*）を指定すると、接頭辞を使用してマッピングされた任意のグループの短縮名が使用されます。たとえば、CN=TestApp,OU=Apps,OU=Roles,[LdapSuffix] という DN のグループの場合は、次のようになります。

```
Role Prefix -> Role Name
OU=Roles[4] -> Apps/TestApp
OU=Roles[*4] -> TestApp
```

次に、子 OU の名前が Roles および Accounts で、Stellent という名前の OU が含まれるディレクトリ・ツリーの一般的なロール接頭辞およびアカウント接頭辞を示します。

ロール接頭辞 : `OU=Roles,OU=Stellent`

アカウント接頭辞 : `OU=Accounts,OU=Stellent`

注意 : 接頭辞のユニットを区切るカンマの前後に空白を含めないでください。また、階層アカウント構造を作成するため、Content Server により % はスラッシュに変換されます。たとえば、グループ名 FOO%BOO%BASH は、アカウント FOO/BOO/BASH にマッピングされます。

完全なグループ名

完全なグループ名は、Active Directory のグループ名のツリー構造全体を、Content Server のロール名またはアカウント名に含めるために使用されます。この設定は、Oracle Content Server で階層アカウント構造を使用するセキュリティ・モデルに特に便利です。

- 「Active Directory Configuration」ページ（6-17 ページ）で完全なグループ名が有効化されている場合、ネーミング・コンテキスト（dc=company,dc=com など）を除くディレクトリ・ツリーのすべてのユニットが、ロール名またはアカウント名に含まれます。

注意 : 特定の接頭辞の深さパラメータにアスタリスク（*）を指定すると、接頭辞を使用してマッピングされた任意のグループの短縮名が使用されます。

- 完全なグループ名が無効化されている場合、ディレクトリ・ツリーの最後のユニットのみが、ロール名またはアカウント名としてマッピングされます。
- ロールおよびアカウントのマッピングも、グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）（6-10 ページ）の設定が有効化されているかどうかによって異なります。
- 次の例では、完全なグループ名の設定を有効化または無効化した結果を示します。

  グループ : `CN=admin,OU=Mgr,OU=Dept,OU=Roles,OU=Stellent,dc=company,dc=com`

  アカウント名（完全なグループ名を無効化）: `admin`

  アカウント名（完全なグループ名を有効化）: `Dept/Mgr/admin`

マッピングの例

この項では、グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）（6-10 ページ）および完全なグループ名（6-11 ページ）の設定の可能な組合せをいくつか示します。

ロール・マッピングの例

グループ : `CN=admin,OU=Mgr,OU=Dept,OU=Roles,OU=Stellent,dc=company,dc=com`

ロール接頭辞 : `OU=Roles,OU=Stellent[2]`

グループのフィルタ処理	完全なグループ名	結果
有効化	有効化	**ロール** = Dept/Mgr/admin
有効化	無効化	**ロール** = admin
無効化	有効化	**ロール** = Stellent/Roles/Dept/Mgr/admin

グループの フィルタ処理	完全なグループ名	結果
無効化	無効化	**ロール** = admin

アカウント・マッピングの例

グループ : `CN=admin,OU=Mgr,OU=Dept,OU=Accounts,OU=Stellent,dc=company,dc=com`

ロール接頭辞 : `OU=Accounts,OU=Stellent[2]`

グループの フィルタ処理	完全なグループ名	結果
有効化	有効化	**アカウント** = Dept/Mgr/admin
有効化	無効化	**アカウント** = admin
無効化	有効化	**ロール** = Stellent/Accounts/Dept/Mgr/admin
無効化	無効化	**ロール** = admin

深さ

ロール接頭辞またはアカウント接頭辞の深さパラメータでは、有効なロールまたはアカウントとみなされるために、接頭辞とそのグループのグループ名の最後のユニットの間に存在可能な最大のレベル数を指定できます。深さパラメータは、ディレクトリ・ツリーの下位のグループに、誤って権限を付与するのを防ぐのに役立ちます。

注意 : 特定の接頭辞の深さパラメータにアスタリスク（*）を指定すると、接頭辞を使用してマッピングされた任意のグループの短縮名が使用されます。

- 深さは、接頭辞の定義の後ろの大カッコ **[ ]** 内に指定された数です。たとえば、`OU=Roles,OU=Stellent[1]` のようになります。
- 接頭辞と最後のユニットの間のレベル数が深さの設定以下の場合に、グループはロールまたはアカウントにマッピングされます。グループ名で、接頭辞と最後のユニットの間のレベルが深さパラメータで指定された数より多い場合は、グループはロールまたはアカウントにマッピングされません。

  次に例を示します。

  ロール接頭辞 : `OU=Roles,OU=Stellent[1]`

  グループ 1: `CN=admin,OU=Roles,OU=Stellent,dc=company,dc=com`

  グループ 2: `CN=admin,OU=Mgr,OU=Roles,OU=Stellent,dc=company,dc=com`

グループ 3: `CN=admin,OU=Mgr,OU=Dept,OU=Roles,OU=Stellent,dc=company,dc=com`

この場合、結果は次のようになります。

- 接頭辞と最後のユニットの間のレベルが 1 より少ないため、グループ 1 は有効なロールとみなされます。
- 接頭辞と最後のユニットの間のレベルが 1 であるため、グループ 2 は有効なロールとみなされます。
- 接頭辞と最後のユニットの間のレベルが 1 より多いため、グループ 3 は有効なロールとみなされません。

❖ 接頭辞に深さが指定されていない場合、深さのデフォルトは 0 に設定されます。つまり、グループ名の最下位レベルが接頭辞の直後にある必要があります。

次に例を示します。

ロール接頭辞 : `OU=Roles,OU=Stellent`

グループ 1: `CN=admin,OU=Roles,OU=Stellent,dc=company,dc=com`

グループ 2: `CN=admin,OU=Mgr,OU=Roles,OU=Stellent,dc=company,dc=com`

この場合、結果は次のようになります。

- 接頭辞と最後のユニットの間にレベルがないため、グループ 1 は有効なロールとみなされます。
- 接頭辞と最後のユニットの間にレベルが 1 つあるため、グループ 2 は有効なロールとみなされません。

アカウント権限

アカウント権限は、次の方法で指定できます。

❖ 「Active Directory Configuration」ページの「Account Permissions Delimiter」フィールド（6-21 ページ）に指定されている文字が先頭に付いた、Active Directory のグループ名自体から指定できます。

❖ 「Active Directory Configuration」ページの「Default Network Accounts」フィールド（6-23 ページ）に指定されているデフォルトのアカウント設定から指定できます。デフォルトの設定は #none(RWDA) で、Active Directory ユーザーは、アカウントが割り当てられていないすべてのコンテンツ・アイテムに対する管理権限を持っていることを意味します。

注意 : デフォルトのアカウント権限は、Active Directory グループによって定義された権限に追加されます。たとえば、デフォルトが #none(RW),Project(R) で、ユーザーのグループが Project(RWD) 権限にマッピングされている場合、ユーザーの権限は #none(RW),Project(RWD) です。

ACTIVE DIRECTORY セキュリティの設定

この項の内容は次のとおりです。

Content Server の Active Directory 向けの設定

Active Directory セキュリティを Oracle Content Server と統合するには、Content Server を次のように設定する必要があります。

1. IIS Web サーバーが外部セキュリティ統合用に構成されていることを確認します。
2. Active Directory セキュリティを有効化します。詳細は、6-14 ページの「Active Directory セキュリティの有効化」を参照してください。
3. Active Directory 設定に一致するように構成エントリを設定します。詳細は、6-15 ページの「Active Directory セキュリティの構成」を参照してください。

注意 : このガイドで説明されている直接統合ではなく、LDAP プロバイダを使用して Active Directory サーバーに対してユーザーを認証する場合は、カスタムの Active Directory LDAP コンポーネントをインストールおよび構成する必要があります。

Active Directory セキュリティの有効化

Content Server で Active Directory セキュリティを有効化するには、次のいずれかの手順を実行します。

- インストール中

  インストール中に、「Security」画面で「Active Directory Security」オプションを選択します。これにより、Active Directory セキュリティが有効化され、ポータル・ナビゲーション・バーの「Microsoft Login」ボタンが表示されます。

- システム・プロパティの使用

  1. Content Server インスタンスの**システム・プロパティ**にアクセスします。
  2. 「Internet」タブをクリックします。
  3. 「Use Microsoft Security」チェック・ボックスを選択します。
  4. 「Active Directory Security (ADSI)」オプションを選択します。
  5. **「OK」**をクリックします。
  6. Content Server を再起動します。

7. IIS サービスを再開します。
8. Content Server の「Home」ページまたは「Administration」ページに移動し、ポータル・ナビゲーション・バーに「Microsoft Login」ボタンが表示されていることを確認します。

❖ 管理サーバーの使用

1. Content Server にシステム管理者としてログインします。
2. ポータル・ナビゲーション・バーの「**Administration**」をクリックします。
3. 「**Admin Server**」をクリックします。
4. 「**Master_on_*instance***」をクリックします。
5. ポータル・ナビゲーション・バーの「**Internet Configuration**」をクリックします。
6. 「Use Microsoft Security」で、「Active Directory Security」オプションを選択します。
7. 「**Save**」をクリックします。
8. Content Server を再起動します。
9. IIS サービスを再開します。
10. Content Server の「Home」ページまたは「Administration」ページに移動し、ポータル・ナビゲーション・バーに「Microsoft Login」ボタンが表示されていることを確認します。

Active Directory セキュリティの構成

Active Directory セキュリティを構成するには、次のようにします。

1. Active Directory セキュリティを有効化します。詳細は、6-14 ページの「Active Directory セキュリティの有効化」を参照してください。
2. Content Server にシステム管理者としてログインします。
3. ポータル・ナビゲーション・バーの「Administration」リンクをクリックします。
4. 「**Filter Administration**」をクリックします。

   「Configure Web Server Filter」ページが表示されます。
5. 「Special Integrations」で「**Configure**」をクリックします。

   「Active Directory Configuration」ページ（6-17 ページ）が表示されます。

6. ロール接頭辞またはアカウント接頭辞（あるいはその両方）を指定するには、次のようにします。
   a. 「Group Filtering」チェック・ボックスを選択します。
   b. 適切な接頭辞フィールドに、ロールまたはアカウント接頭辞を入力します。
   c. 「Depth」フィールドに数値を入力します。（数を指定しない場合、デフォルトは 0 です。）
   d. **「Add」**をクリックします。

      対応するテキスト・ボックスに、ロールまたはアカウント接頭辞が追加されます。
   e. 必要な場合には、テキスト・ボックスの接頭辞を直接編集します。

注意 : 詳細は、6-9 ページの「ロールおよびアカウントのマッピング」を参照してください。

7. ユーザー属性マップを指定するには、次のようにします。
   a. 「Attribute Map」セクションで、「LDAP Attribute」フィールドに Active Directory のユーザー属性を入力します。
   b. 「User Attribute」リストから Content Server のユーザー情報フィールドを選択します。
   c. **「Add」**をクリックします。

      テキスト・ボックスに属性マップが追加されます。
   d. 必要な場合には、テキスト・ボックスの属性マップを直接編集します。
8. 必要に応じて、その他の構成設定を変更します。
9. **「Update」**をクリックします。
10. 変更内容が反映されていない場合は、IIS サービスを再開します。

「ACTIVE DIRECTORY CONFIGURATION」ページ

Active Directory Configuration

Authorization Method UseTokenGroups

This value determines which method the Active Directory plugin will use to retrieve group and user information for a user.
ADSI - This method uses the legacy ADSI calls.
ADSI with nested groups - This method uses the legacy ADSI calls, but will also retrieve all nested group information for the user.
User Tokens - This method reads the group information from the user token that is created when IIS authenticates the user. This includes the users nested group information. This is also the fastest of the above methods and the recommended method.

Use Group Filtering

Enabling this will add the ability to use a filter to select the groups that will be mapped into the Content Server. The filtering works by specifying a set of LDAP-style prefixes for both roles and accounts. These prefixes are LDAP-style strings which specify an area of the tree that roles and/or accounts are located. Each group the user belongs to is checked to see if the group contains one of these prefixes as a substring. If so, the group is considered a role or account depending on what type of prefix it was. Along with each prefix is a depth value listed in '[]' after the prefix. This value dictates how 'far away' a group can be from the prefix to be considered valid. For example, if we have the setup:

Role Prefix: "OU=Roles, OU=Stellent"
Depth: 1
"CN=testRole, OU=subOrg2, OU=org1, OU=Roles, OU=Stellent, dc=mydomain, dc=com"

The above group matches the Role Prefix, and the remainder of the group name after the Role Prefix is "CN=testRole, OU=subOrg2, OU=org1" . This group (testRole) is two organizational units (OU) away from the Role Prefix, which translates into a depth of 2. Since the depth is 1 the group does not become a role. If the depth were 2 or higher, the group would have become a role. The notion of depth is introduced to prevent groups deep in the LDAP tree from inadvertently granting privileges such as 'admin' to users. If no depth is specified for a prefix, the depth defaults to 0, which means the group must be contained directly with in the prefix. For example if the Role Prefix is "OU=Roles, OU=Stellent" and the depth defaults to 0, "CN=roleA, OU=Roles, OU=Stellent" would be a valid role, but "CN=roleB, OU=subOrg, OU=Roles, OU=Stellent" would not.

Role Prefix	Depth	
OU=Roles,OU=Stellent	1	Add

Account Prefix	Depth	
OU=Accounts,OU=Stellent	1	Add

Account Permissions Delimiter _

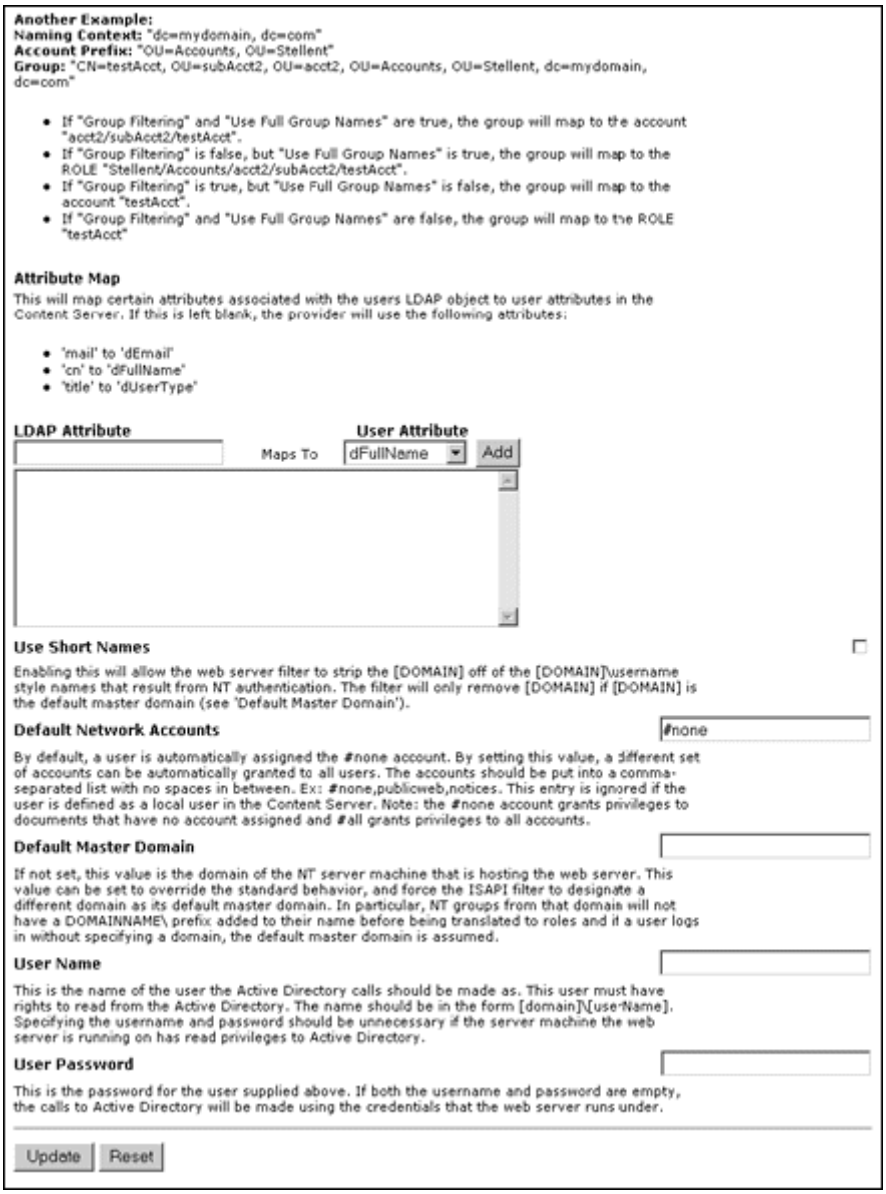
If this value is found in a group name that is being treated as an account, the group name will be split on this value and the left part of the string will become the account name and the right side of the string becomes the permissions for that account. For example, if the group name is 'acct1_rw' and the Account Permissions Delimiter is '_', the group will become the account 'acct1' with read and write privileges. If the delimiter is set to anything but '_', the group will map to the account 'acct1_rw' with default privileges.

Use Full Group Names

By checking this value, groups retrieved from the directory will preserve their hierarchy. The groups will have the naming context removed, along with the matching Role or Account Prefix. Take the following example:

Naming Context: "dc=mydomain, dc=com"
Role Prefix: "OU=Roles, OU=Stellent"
Group: "CN=group1, OU=subDept1, OU=dept2, OU=Roles, OU=Stellent, dc=mydomain, dc=com"

- If "Group Filtering" and "Use Full Group Names" are true, the group will map to the role "dept2/subDept1/group1".
- If "Group Filtering" is false, but "Use Full Group Names" is true, the group will map to the role "Stellent/Roles/dept2/subDept1/group1".
- If "Group Filtering" is true, but "Use Full Group Names" is false, the group will map to the role "group1".
- If "Group Filtering" and "Use Full Group Names" are false, the group will map to the role "group1"



「Active Directory Configuration」ページは、Active Directory セキュリティとともに Content Server 統合を構成する際に使用します。このページにアクセスするには、Active Directory セキュリティを有効化（6-14 ページの「Active Directory セキュリティの有効化」を参照）して、「Configure Web Server Filter」ページの「**Configure**」をクリックします。

次の表において、1 列目のカッコ内の文字列は、<*Install_Dir*>/data/users/config/filter.hda ファイルの対応する構成設定です。

機能	説明
「Authorization Method」セクション	
「Authorization Method」フィールド	オプション・リストから認証方法を選択します。 • UseTokenGroups • UseNestedGroups • UseBasicGroups この値は、ユーザーのグループおよびユーザー情報を取得するために、Active Directory プラグインによって使用されます。 **User Tokens:** このメソッドでは、IIS によるユーザーの認証時に作成されるユーザー・トークンから、ユーザーのネストしたグループ情報も含むグループ情報が取得されます。これは最も高速で、推奨のメソッドです。 **ADSI with nested groups:** このメソッドではレガシー ADSI コールが使用されますが、ユーザーのすべてのネストしたグループ情報も取得されます。 **ADSI:** この基本メソッドでは、レガシー ADSI コールが使用されます。
「Use Group Filtering」セクション 詳細は、6-9 ページの「ロールおよびアカウントのマッピング」を参照してください。	
「Group Filtering」チェック・ボックス (UseGroupFilter)	**選択 :** Content Server のロールおよびアカウントにマッピングされる Active Directory グループの選択に、ロール接頭辞およびアカウント接頭辞の定義が使用されます。 **選択解除 :** すべての Active Directory グループが Content Server のロールおよびアカウントにマッピングされます。これがデフォルトです。
「Role Prefix」フィールド	Active Directory のグループ名のどの部分からが Content Server のロール名に一致するかを指定する文字列。
「Role Prefix」の「Depth」フィールド	有効なロールであるとみなされるために、Active Directory のグループ名で、グループ名のロール接頭辞の後に含むことのできるレベル数を指定する数値。
「Role Prefix」の「Add」ボタン	「Role Prefix」ボックスに、ロール接頭辞文字列および深さが句として追加されます。

機能	説明
「Role Prefix」ボックス (RolePrefix)	「Group Filtering」チェック・ボックスが選択されている場合、Active Directory グループの選択に使用されるロール接頭辞句がリストされます。このボックスは直接編集できます。 **注意 :** 接頭辞のユニットを区切るカンマの前後に空白を含めないでください。
「Account Prefix」フィールド	Active Directory のグループ名のどの部分からが Content Server のアカウント名に一致するかを指定する文字列。 このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Account Prefix」の「Depth」フィールド	有効なアカウントであるとみなされるために、Active Directory のグループ名で、グループ名のアカウント接頭辞の後に含むことのできるレベル数を指定する数値。 このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Account Prefix」の「Add」ボタン	「Account Prefix」ボックスに、アカウント接頭辞文字列および深さが句として追加されます。 このボタンは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Account Prefix」ボックス (AcctPrefix)	「Group Filtering」チェック・ボックスが選択されている場合、Active Directory グループの選択に使用されるアカウント接頭辞句がリストされます。このボックスは直接編集できます。 **注意 :** 接頭辞のユニットを区切るカンマの前後に空白を含めないでください。 このボックスは、Content Server でアカウントが有効化されている場合にのみ表示されます。

機能	説明
「Account Permissions Delimiter」セクション 詳細は、6-9 ページの「ロールおよびアカウントのマッピング」を参照してください。	
「Account Permissions Delimiter」フィールド (AcctPermDelim)	Active Directory のグループ名のアカウント権限とアカウント名を区切る文字列。 • Active Directory のグループ名がアカウントにマッピングされていて、このサブストリングが含まれている場合、このサブストリングの左側の文字列がアカウント名で、右側の文字列がアカウント権限です。 • たとえば、デリミタが + (プラス記号) に定義されている場合、グループ名 Acct1+rw は、読取りおよび書込み権限のある Acct1 という名前のアカウントにマッピングされます。デリミタが _ (アンダースコア) に定義されている場合、Acct1+rw グループ名は、デフォルトで RWDA 権限のある Acct1+rw という名前のアカウントにマッピングされます。 • デフォルトは _ (アンダースコア) です。 • このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Use Full Group Names」セクション 詳細は、6-9 ページの「ロールおよびアカウントのマッピング」を参照してください。	
「Use Full Group Names」チェック・ボックス (UseFullGroupName)	**選択 :** Active Directory グループの階層全体 (指定された接頭辞またはネーミング・コンテキストまで) が、Content Server のロールまたはアカウントへのマッピングに含まれます。 **選択解除 :** Active Directory グループの最下位レベルのユニットのみが Content Server のロールまたはアカウントにマッピングされます。これがデフォルトです。
「Attribute Map」セクション	
「LDAP Attribute」フィールド	Content Server のユーザー情報フィールドにマッピングされる Active Directory のユーザー属性を入力します。

機能	説明
「User Attribute」フィールド	「LDAP Attribute」フィールドからマッピングされる Content Server のユーザー情報フィールドを選択します。 • 値を変更できるすべての Content Server のユーザー情報フィールドがリストされます。 • 標準のユーザー情報フィールドは d から始まります。 • カスタムのユーザー情報フィールドは u から始まります。
「Add」ボタン	「Attribute Map」ボックスに、LDAP 属性およびユーザー属性がコロン区切りの句として追加されます。

「Attribute Map」ボックス
（AttributeMap）
	Active Directory のユーザー属性を Content Server の情報フィールドにマッピングするために使用される属性マップ句がリストされます。
	• このボックスは直接編集できます。
	• このフィールドを空にした場合、デフォルトは次のとおりです。
	`mail:dEmail`
	`cn:dFullName`
	`title:dUserType`

「Use Short Names」セクション	
「Use Short Names」チェック・ボックス （UseShortNamesAlways）	**選択 :** Web サーバー・フィルタにより、Active Directory のすべてのユーザー名から DOMAINNAME¥ 接頭辞が削除されます。 **選択解除 :** デフォルトのマスター・ドメインを除き、DOMAINNAME¥ 接頭辞が、Active Directory のすべてのユーザー名に含まれます。これがデフォルトです。

機能	説明
「Default Network Accounts」セクション	
「Default Network Accounts」フィールド (DefaultNetworkAccounts)	Active Directory 資格証明を使用して Content Server にログインするユーザーのデフォルトのアカウント権限を定義します。 • アカウントのカンマ区切りのリストである必要があります。 **注意 :** アカウントを区切るカンマの前後に空白を含めないでください。 • 各アカウントの権限は、account(RWDA) のように、アカウント名の後ろのカッコ内に指定できます。権限が指定されていない場合は、デフォルトで RWDA 権限が付与されます。 • #none エントリの場合は、アカウントが割り当てられていないドキュメントに対する権限が付与されます。 • #all エントリの場合は、すべてのアカウントに対する権限が付与されます。 • デフォルトは #none(RWDA) です。 • この設定は、匿名ユーザーには適用されません。 • この設定により最低限のアカウント権限が定義されます。外部ユーザー・ベースにより定義されたアカウント権限は、これらの権限に追加されます。たとえば、デフォルトが #none(RW),Project(R) で、ユーザーのグループが Project(RWD) 権限にマッピングされている場合、ユーザーの権限は #none(RW),Project(RWD) です。 • このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。

機能	説明
「Default Master Domain」セクション	
「Default Master Domain」フィールド (DefaultMasterDomain)	Web サーバー・フィルタのデフォルトのマスター・ドメインである Windows ドメイン。 • 指定したドメインの Active Directory ユーザーの場合、グループがロールおよびアカウントに変換される前には、DOMAINNAME¥ 接頭辞はユーザー名に追加されません。 • ユーザーがドメイン接頭辞を指定せずにログインした場合は、このデフォルトのマスター・ドメインが推測されます。 • デフォルトは、Web サーバーをホストしている Windows Server マシンのドメインです。
「User Name」セクション	
「User Name」フィールド (AdsUserName)	Web サーバーが、Active Directory に対する読取り権限を持たない Windows Server 上で稼働している場合は、Active Directory の読取り権限を持っているユーザー名を入力します。 • ユーザー名は、*DOMAIN_NAME¥username* という書式である必要があります。 • この設定およびユーザー・パスワード設定が指定されていない場合、デフォルトは Web サーバーを稼働するユーザー名です。
「User Password」セクション	
「User Password」フィールド (AdsUserPassword)	Web サーバーが、Active Directory に対する読取り権限を持たない Windows Server 上で稼働している場合は、ユーザー名のパスワードを入力します。 • この設定およびユーザー名設定が指定されていない場合、デフォルトは Web サーバーを稼働するユーザー名です。

7

外部セキュリティ：LDAP

概要

この項の内容は次のとおりです。

概念

タスク

インタフェース

LDAP の概要

この項の内容は次のとおりです。

LDAP について

LDAP（Lightweight Directory Access Protocol）は、iPlanet Directory Server や Novell eDirectory などの LDAP ディレクトリに格納された情報へのアクセスに TCP/IP を使用するプロトコルです。LDAP ディレクトリにはネットワーク上のオブジェクトの情報が格納され、アプリケーション、ユーザーおよびネットワーク管理者がこの情報を使用できるようになります。LDAP を使用すると、認可済のネットワーク・ユーザーは、1 回のログイン・プロセスでネットワーク上の任意の場所にあるリソースにアクセスできます。

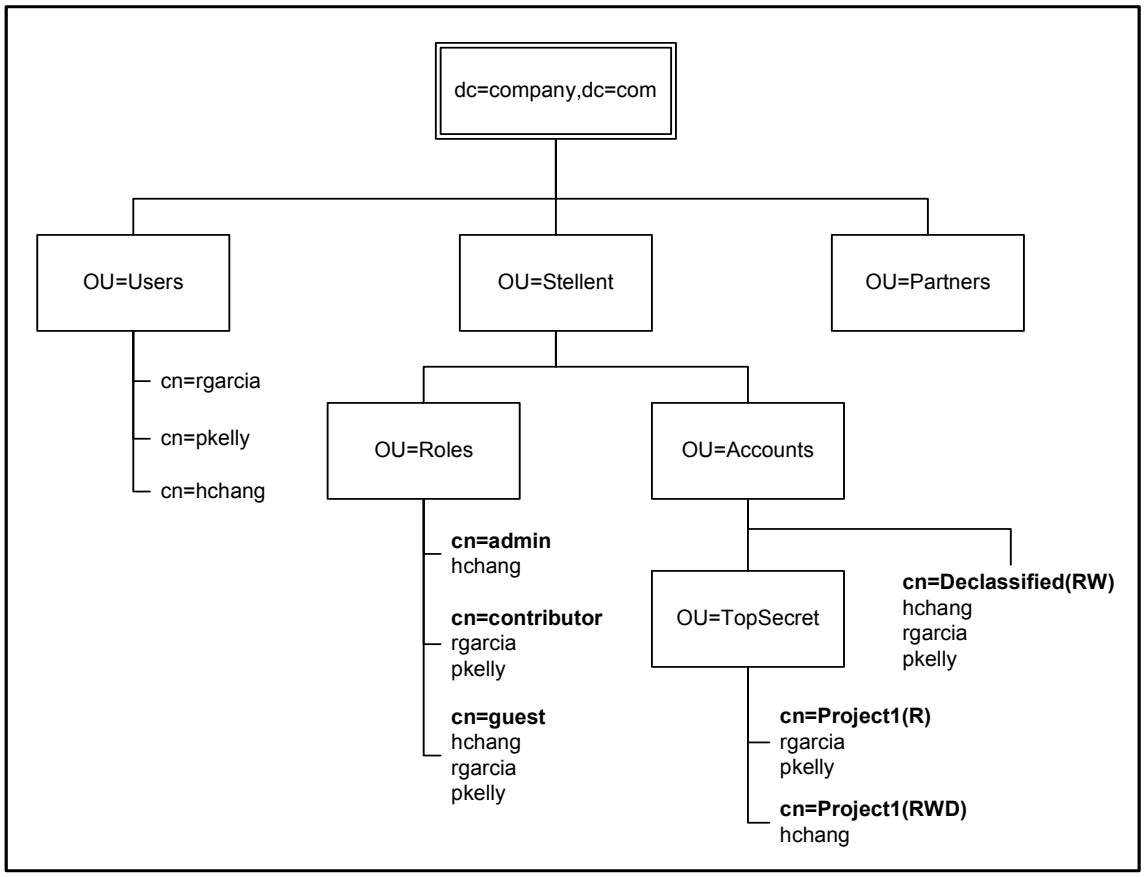
注意 : 必須ではありませんが、LDAP セキュリティ・モデルの作成時および LDAP 統合のデプロイ時には、コンサルティング・サービスのサポートを受けることをお薦めします。

注意 : このガイドで説明されている直接統合ではなく、LDAP プロバイダを使用して Active Directory サーバーに対してユーザーを認証する場合は、カスタムの Active Directory LDAP コンポーネントをインストールおよび構成する必要があります。

LDAP のディレクトリ構造

LDAP は、ディレクトリ・ツリーと呼ばれる階層構造でネットワーク・オブジェクトを編成します。図 7-1 のツリーの図で、典型的な LDAP のディレクトリ構造を示します。

図 7-1 LDAP のディレクトリ構造の例



この場合、ユーザーは次の DN（識別名）を持つグループに割り当てられます。

```
cn=Project1,OU=TopSecret,OU=Accounts,OU=Stellent,dc=company,dc=com
```

ここで、グループ DN は、次の LDAP 表記規則に準拠しています。

LDAP での略語	LDAP での意味	説明
dc	ドメイン・コンポーネント	ネーミング・コンテキストを指定する最上位レベルのユニット。o=company.com のように、結合して 1 つの組織指定にすることもできます。
OU	編成ユニット	通常は、課、部門またはその他の個々のビジネス・グループを表します。Content Server 統合では、ロールやアカウントは一般的に OU として指定されます。
cn	共通名	一般的に、DN の最下位レベルの属性で、一意の名前を識別します。ユーザーの場合は、ユーザー ID の単位である uid でもかまいません。

LDAP セキュリティの統合

この項の内容は次のとおりです。

LDAP ログイン

LDAP セキュリティを Content Server と統合すると、ユーザー・ログイン、パスワードおよび権限は LDAP サーバーの情報から導出されます。ユーザーは、ポータル・ナビゲーション・バーの「Login」ボタンを使用して Content Server にログインします。

Content Server と LDAP サーバーの両方にユーザー名が定義されている場合は、接頭辞としてドメイン名が含まれていないかぎり（*DOMAINNAME¥user_name* など）、Content Server のユーザー・パスワードが優先されます。

LDAP の認証プロセス

LDAP セキュリティが Content Server と統合されると、ユーザーの資格証明は次のようにして認証されます。

1. クライアント・ブラウザにより、Content Server に対してセキュアなリソースのリクエストが発行されます。リクエストは Web サーバーにより受信されます。
2. Web サーバー・フィルタにより、ユーザーに、ユーザー名およびパスワードの入力を要求するチャレンジが送信されます。
3. ユーザー資格証明とともに、リクエストが再度 Web サーバーに送信されます。
4. Web サーバー・フィルタにより、Content Server にリクエストが転送されます。
5. ユーザー名が内部ユーザーとして認識されない場合、資格証明は LDAP プロバイダにより LDAP ディレクトリに渡されて認証されます。
6. LDAP ディレクトリによりユーザーが認証され、ユーザーの LDAP グループおよび属性情報が Content Server に送信されます。
7. Content Server により、ユーザーのグループが Content Server のロールおよびアカウントにマッピングされ、ユーザー属性（フルネームおよび電子メール・アドレス）は Content Server のユーザー情報フィールドにマッピングされます。
8. ユーザーがリクエストされたセキュアなリソースへのアクセス権を持っている場合は、Content Server によりレスポンスがクライアント・ブラウザに送信されます。

ロールおよびアカウントのマッピング

LDAP セキュリティが Content Server と統合されている場合、ユーザーが属する LDAP グループは、次のようにして Content Server のロールおよびアカウントにマッピングされます。

- グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）（7-6 ページ）および完全なグループ名（7-7 ページ）の設定は、ユーザーのロールおよびアカウントを判断するためのグループ名の解析に使用されます。
- グループ名をロールとして解析し、Content Server ロールの名前に一致した場合、ユーザーはそのロールを割り当てられます。
- グループ名をアカウントとして解析すると、ユーザーはそのアカウントを割り当てられます。この方法で、LDAP グループから新しいアカウントを作成できます。
- Content Server ロールまたはアカウント接頭辞に一致しない解析済のグループ名は無視されます。
- アカウント権限は、グループ名自体またはデフォルトの権限設定から判断されます。詳細は、7-9 ページの「アカウント権限」を参照してください。

❖ ロールが定義されていない LDAP ユーザーには、guest または anonymous ロールは自動的に割り当てられません。LDAP ユーザーが Content Server のロールに一致するロールを持っていない場合、そのユーザーがコンテンツ・サーバーに接続するとエラーが発生します。

これを避けるために、次の 3 つのいずれかを実行できます。

- サーバー・ディレクトリまたはグループで、ユーザーにロールを定義します。
- SystemFilters.hda ファイルに構成エントリ FORCE_WEBSERVER_CREDENTIALS=1 を追加して、Web サーバー・フィルタにより、デフォルトでユーザーに guest ロールが割り当てられるようにします。
- LDAP の設定時に、定義済のネットワーク・ロールを指定します。

グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）

グループのフィルタ処理は、LDAP のグループ名のどの部分を Content Server のロールまたはアカウントにマッピングするかの指定に使用されます。

❖ 「LDAP Provider」ページ（7-15 ページ）でグループのフィルタ処理が有効化されている場合、「Role Prefix」および「Account Prefix」フィールドは、各ユーザーのグループ名のフィルタ処理に使用されます。ロール接頭辞およびアカウント接頭辞は無制限に指定できます。これらの接頭辞は、LDAP の各グループ名と比較されるサブストリングです。グループ名に接頭辞サブストリングがある場合は、その接頭辞より後ろのその他のグループ名（ディレクトリ・ツリーの下位レベル）は、ロールまたはアカウントとして解析されます。結果のロールおよびアカウントのマッピングは、完全なグループ名（7-7 ページ）の設定が有効化されているかどうかによって異なります。

❖ グループのフィルタ処理が無効化されている場合、すべてのグループ名は完全なグループ名（7-7 ページ）の設定に基づいて、Content Server のロールとして解析されます。

❖ 各ロール接頭辞およびアカウント接頭辞には深さ（7-8 ページ）パラメータがあり、有効なロールまたはアカウントとみなされるために、接頭辞とそのグループのグループ名の最後のユニットの間に存在可能な最大のレベル数を指定できます。

❖ 次に、子 OU の名前が Roles および Accounts で、Stellent という名前の OU が含まれるディレクトリ・ツリーの一般的なロール接頭辞およびアカウント接頭辞を示します。

ロール接頭辞 : `OU=Roles,OU=Stellent`

アカウント接頭辞 : `OU=Accounts,OU=Stellent`

注意 : 接頭辞のユニットを区切るカンマの前後に空白を含めないでください。

完全なグループ名

完全なグループ名は、LDAP のグループ名のツリー構造全体を、Content Server のロール名またはアカウント名に含めるために使用されます。この設定は、Content Server で階層アカウント構造を使用するセキュリティ・モデルに特に便利です。

- 「LDAP Provider」ページ（7-15 ページ）で完全なグループ名が有効化されている場合、ネーミング・コンテキスト（dc=company,dc=com など）を除くディレクトリ・ツリーのすべてのユニットが、ロール名またはアカウント名に含まれます。
- 完全なグループ名が無効化されている場合、ディレクトリ・ツリーの最後のユニットのみが、ロール名またはアカウント名としてマッピングされます。
- ロールおよびアカウントのマッピングも、グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）（7-6 ページ）の設定が有効化されているかどうかによって異なります。
- 次の例では、完全なグループ名の設定を有効化または無効化した結果を示します。

  グループ : `CN=admin,OU=Mgr,OU=Dept,OU=Roles,OU=Stellent,dc=company,dc=com`

  アカウント名（完全なグループ名を無効化）: `admin`

  アカウント名（完全なグループ名を有効化）: `Dept/Mgr/admin`

マッピングの例

この項では、グループのフィルタ処理（ロール接頭辞およびアカウント接頭辞）（7-6 ページ）および完全なグループ名（7-7 ページ）の設定の可能な組合せをいくつか示します。

ロール・マッピングの例

グループ : `CN=admin,OU=Mgr,OU=Dept,OU=Roles,OU=Stellent,dc=company,dc=com`

ロール接頭辞 : `OU=Roles,OU=Stellent[2]`

グループのフィルタ処理	完全なグループ名	結果
有効化	有効化	ロール = Dept/Mgr/admin
有効化	無効化	ロール = admin
無効化	有効化	ロール = Stellent/Roles/Dept/Mgr/admin
無効化	無効化	ロール = admin

アカウント・マッピングの例

グループ : `CN=admin,OU=Mgr,OU=Dept,OU=Accounts,OU=Stellent,dc=company,dc=com`

ロール接頭辞 : `OU=Accounts,OU=Stellent[2]`

グループの フィルタ処理	完全なグループ名	結果
有効化	有効化	**アカウント** = Dept/Mgr/admin
有効化	無効化	**アカウント** = admin
無効化	有効化	**ロール** = Stellent/Accounts/Dept/Mgr/admin
無効化	無効化	**ロール** = admin

深さ

ロール接頭辞またはアカウント接頭辞の深さパラメータでは、有効なロールまたはアカウントとみなされるために、接頭辞とそのグループのグループ名の最後のユニットの間に存在可能な最大のレベル数を指定できます。深さパラメータは、ディレクトリ・ツリーの下位のグループに、誤って権限を付与するのを防ぐのに役立ちます。

❖ 深さは、接頭辞の定義の後ろの大カッコ [ ] 内に指定された数です。たとえば、`OU=Roles,OU=Stellent[1]` のようになります。

❖ 接頭辞と最後のユニットの間のレベル数が深さの設定以下の場合に、グループはロールまたはアカウントにマッピングされます。グループ名で、接頭辞と最後のユニットの間のレベルが深さパラメータで指定された数より多い場合は、グループはロールまたはアカウントにマッピングされません。

次に例を示します。

ロール接頭辞 : `OU=Roles,OU=Stellent[1]`

グループ 1: `CN=admin,OU=Roles,OU=Stellent,dc=company,dc=com`

グループ 2: `CN=admin,OU=Mgr,OU=Roles,OU=Stellent,dc=company,dc=com`

グループ 3: `CN=admin,OU=Mgr,OU=Dept,OU=Roles,OU=Stellent,dc=company,dc=com`

この場合、結果は次のようになります。

- 接頭辞と最後のユニットの間のレベルが 1 より少ないため、グループ 1 は有効なロールとみなされます。
- 接頭辞と最後のユニットの間のレベルが 1 であるため、グループ 2 は有効なロールとみなされます。
- 接頭辞と最後のユニットの間のレベルが 1 より多いため、グループ 3 は有効なロールとみなされません。

❖ 接頭辞に深さが指定されていない場合、深さのデフォルトは 0 に設定されます。つまり、グループ名の最下位レベルが接頭辞の直後にある必要があります。

次に例を示します。

ロール接頭辞 : `OU=Roles,OU=Stellent`

グループ 1: `CN=admin,OU=Roles,OU=Stellent,dc=company,dc=com`

グループ 2: `CN=admin,OU=Mgr,OU=Roles,OU=Stellent,dc=company,dc=com`

この場合、結果は次のようになります。

- 接頭辞と最後のユニットの間にレベルがないため、グループ 1 は有効なロールとみなされます。
- 接頭辞と最後のユニットの間にレベルが 1 つあるため、グループ 2 は有効なロールとみなされません。

アカウント権限

アカウント権限は、次の方法で指定できます。

❖ 「LDAP Provider」ページの「Account Permissions Delimiter」フィールドに指定されている文字が先頭に付いた、LDAP のグループ名自体から指定できます。

❖ 「LDAP Provider」ページの「Default Network Accounts」フィールドに指定されているデフォルトのアカウント設定から指定できます。デフォルトの設定は #none(RWDA) で、LDAP ユーザーは、アカウントが割り当てられていないすべてのコンテンツ・アイテムに対する管理権限を持っていることを意味します。

LDAP セキュリティの設定

この項の内容は次のとおりです。

LDAP セキュリティ向けの Content Server の設定

LDAP セキュリティを Content Server と統合するには、Content Server を次のように設定する必要があります。

1. Web サーバーが外部セキュリティ統合用に構成されていることを確認します。
2. LDAP プロバイダを作成します。詳細は、7-10 ページの「LDAP プロバイダの作成」を参照してください。
3. LDAP 設定に一致するように構成エントリを設定します。詳細は、7-12 ページの「LDAP セキュリティの構成」を参照してください。

注意 : 第 6 章「外部セキュリティ : Active Directory」で説明されている直接統合ではなく、LDAP プロバイダを使用して Active Directory サーバーに対してユーザーを認証する場合は、カスタムの Active Directory LDAP コンポーネントをインストールおよび構成する必要があります。

LDAP プロバイダの作成

LDAP プロバイダを追加するには、次のようにします。

1. Content Server に sysadmin としてログインします。
2. 左側のナビゲーション・バーの「Administration」リンクをクリックします。
3. 「Providers」リンクをクリックします。

   「Providers」ページが表示されます。
4. 「Create a New Provider」表で、ldapuser プロバイダ・タイプの「Action」列の**「Add」**をクリックします。

   「LDAP Provider」ページ（7-15 ページ）が表示されます。
5. 次のフィールドに入力します。

   必須フィールド

   - Provider Name
   - Provider Description
   - Provider Class（事前定義済）
   - Source Path
   - LDAP Server
   - LDAP Suffix
   - LDAP Port（デフォルトは 389。SSL を使用している場合は 636。）

オプションのフィールド

- Connection（事前定義済）
- Configuration Class
- Number of connections（事前定義済）
- Connection timeout（事前定義済）

6. Content Server インスタンスに複数の LDAP プロバイダがある場合は、「Priority」フィールドに数値を入力します。この数値は、新規ユーザーが Content Server の資格証明をリクエストした場合に、プロバイダが確認される順序を示します。各 LDAP プロバイダには、一意の優先度番号が必要です。（詳細は、7-14 ページの「追加の LDAP プロバイダの設定」を参照してください。）
7. 「Use Netscape SDK」チェック・ボックスを選択します（パフォーマンスを向上させる場合にお薦めします）。
8. LDAP サーバーおよびコンテンツ・サーバー間の通信を保護するには、「Use SSL」チェック・ボックスを選択します。（LDAP サーバーに適切な資格証明がインストールされている必要があります。）

注意 : SSL を使用する場合は、「LDAP Port」フィールドを **636** に設定します。

9. 必要な場合には、アカウント権限デリミタを変更します。
10. 必要な場合には、デフォルトのネットワーク・ロールを追加します。
11. 必要な場合には、デフォルトのネットワーク・アカウントを変更または追加します。
12. ロール接頭辞またはアカウント接頭辞（あるいはその両方）を指定するには、次のようにします。
    a. 「Use Group Filtering」チェック・ボックスを選択します。
    b. 適切な接頭辞フィールドに、ロールまたはアカウント接頭辞を入力します。
    c. 「Depth」フィールドに数値を入力します。（数を指定しない場合、デフォルトは 0 です。）
    d. **「Add」**をクリックします。

       対応するテキスト・ボックスに、ロールまたはアカウント接頭辞が追加されます。
    e. 必要な場合には、テキスト・ボックスの接頭辞を直接編集します。

注意 : 詳細は、7-5 ページの「ロールおよびアカウントのマッピング」を参照してください。

13. ユーザー属性マップを指定するには、次のようにします。
    a. 「Attribute Map」セクションで、「LDAP Attribute」フィールドに LDAP のユーザー属性を入力します。
    b. 「User Attribute」リストから Content Server のユーザー情報フィールドを選択します。
    c. **「Add」**をクリックします。

       テキスト・ボックスに属性マップが追加されます。
    d. 必要な場合には、テキスト・ボックスの属性マップを直接編集します。
14. Content Server による LDAP サーバーのコール時に使用されるユーザー名およびパスワードを入力します。
    - このユーザーには、LDAP サーバーに対する読取り権限がある必要があります。
    - ユーザー名を空にすると、プロバイダは LDAP サーバーに匿名で接続します。
    - プロバイダが Active Directory と通信する場合は、ユーザー名とパスワードが必要で、*DOMAIN¥username* という書式の有効なドメイン・ユーザーである必要があります。
15. **「Add」**をクリックします。

    「Providers」表に新しいプロバイダが追加された状態で「Providers」ページが表示されます。
16. Content Server を再起動します。
17. Web サーバーを再起動します。

LDAP セキュリティの構成

LDAP セキュリティを構成するには、次のようにします。

1. LDAP プロバイダを作成します。詳細は、7-10 ページの「LDAP プロバイダの作成」を参照してください。
2. Content Server に sysadmin としてログインします。
3. 左側のナビゲーション・バーの「Administration」リンクをクリックします。
4. 「Providers」リンクをクリックします。

   「Providers」ページが表示されます。
5. 「Providers」表で、LDAP プロバイダの「Action」列の「Info」リンクをクリックします。

   「LDAP Provider Information」ページが表示されます。

6. **「Edit」**をクリックします。

   「LDAP Provider」ページ（7-15 ページ）が表示されます。

7. ロール接頭辞またはアカウント接頭辞（あるいはその両方）を指定するには、次のようにします。
   a. 「Group Filtering」チェック・ボックスを選択します。
   b. 適切な接頭辞フィールドに、ロールまたはアカウント接頭辞を入力します。
   c. 「Depth」フィールドに数値を入力します。（数を指定しない場合、デフォルトは 0 です。）
   d. **「Add」**をクリックします。

      対応するテキスト・ボックスに、ロールまたはアカウント接頭辞が追加されます。
   e. 必要な場合には、テキスト・ボックスの接頭辞を直接編集します。

注意 : 詳細は、7-5 ページの「ロールおよびアカウントのマッピング」を参照してください。

8. ユーザー属性マップを指定するには、次のようにします。
   a. 「Attribute Map」セクションで、「LDAP Attribute」フィールドに LDAP のユーザー属性を入力します。
   b. 「User Attribute」リストから Content Server のユーザー情報フィールドを選択します。
   c. **「Add」**をクリックします。

      テキスト・ボックスに属性マップが追加されます。
   d. 必要な場合には、テキスト・ボックスの属性マップを直接編集します。
9. 必要な場合には、「LDAP Admin DN」フィールドに、LDAP サーバーをコールするユーザー名を指定します。
10. LDAP サーバーへのコールにユーザー名が指定されている場合は、「LDAP Admin Password」フィールドにそのユーザーのパスワードを指定します。
11. **「Update」**をクリックします。
12. Content Server を再起動します。
13. Web サーバーを再起動します。

追加の LDAP プロバイダの設定

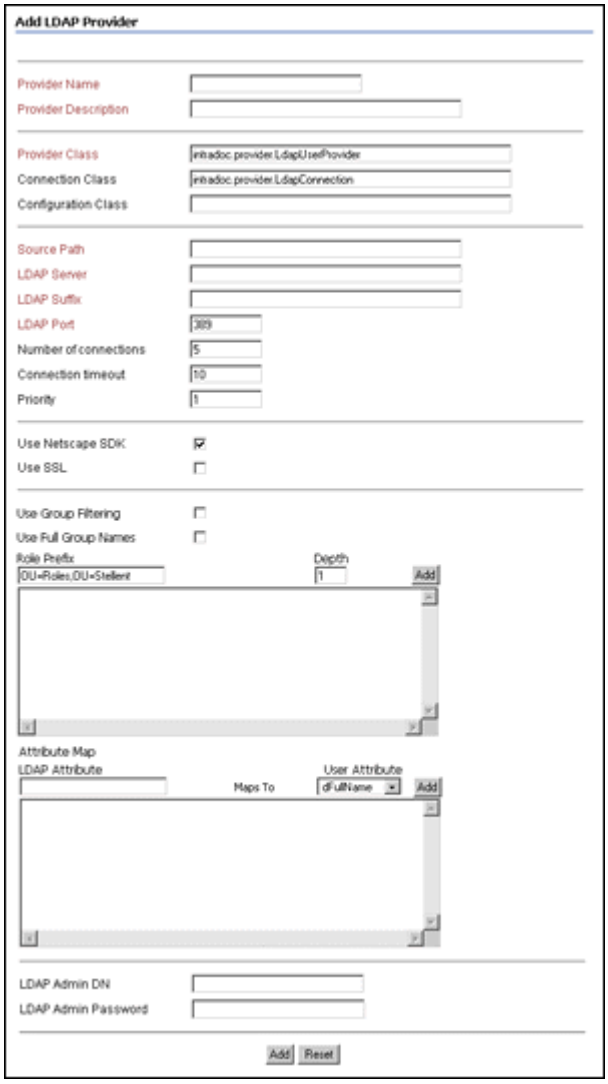
Content Server を使用すると、別の LDAP プロバイダのフェイルオーバーとして使用する追加の LDAP プロバイダを作成できます。これは、メインの LDAP サーバーが停止し、ユーザーが Content Server にログインできない場合に便利です。

追加の LDAP プロバイダを設定するには、LDAP プロバイダの作成（7-10 ページ）の指示に従い、プロバイダ定義で指定可能な「Priority」フィールドを使用します。「Priority」フィールドの設定を使用して、ユーザー情報の検出中に LDAP プロバイダに接続する順序を Content Server に指示します。最上位の LDAP プロバイダが停止するか、ユーザーが検出されない場合、Content Server は（優先度のランクに応じて）次の LDAP プロバイダに接続します。

複数の LDAP プロバイダを使用している場合は、プライマリ LDAP サーバーが停止すると、次のようなことが起こります。

- LDAP プロバイダへの接続が失敗すると、最初のユーザーの一部がわずかな遅延に気付きます。
- Content Server が、バックアップの LDAP プロバイダを使用しているユーザーを検出すると、ユーザーがバックアップの LDAP プロバイダ経由で接続していることが記憶され、プライマリ LDAP プロバイダがオンラインになった場合や、Content Server の再起動後でも、次にユーザー情報が必要な場合にはバックアップの LDAP プロバイダに接続します。この動作により、Content Server は、ユーザー情報が必要になるたびにプロバイダのリスト全体を確認する必要がなくなります。かわりに、Content Server は最後に正常に情報を取得した LDAP プロバイダを記憶し、そのプロバイダを使用します。ただし、バックアップの LDAP プロバイダが停止した場合、Content Server はユーザー情報を取得するためにプライマリ LDAP プロバイダを確認します。検出すると、その後はプライマリ LDAP プロバイダに接続するようになります。

「LDAP PROVIDER」ページ



「LDAP Provider」ページは、LDAP プロバイダの作成および LDAP セキュリティを使用した Content Server 統合の構成に使用します。このページにアクセスするには、「Providers」ページで ldapuser プロバイダ・タイプの「**Add**」または「**Edit**」をクリックします。

次の表において、1 列目のカッコ内の文字列は、<*Install_Dir*>/data/providers/*provider_name*/provider.hda ファイルの対応する構成設定です。

機能	説明
「Provider Name」フィールド *	プロバイダの名前。*<Install_Dir>*/data/providers/ ディレクトリのサブディレクトリになります。
「Provider Description」フィールド *	わかりやすいプロバイダの説明。
「Provider Class」フィールド * (ProviderClass)	プロバイダを実装する Java クラスの名前。 • デフォルトは intradoc.provider.LdapUserProvider です。 • プロバイダが Active Directory と通信している場合、このクラスは intradoc.ActiveDirectoryLdapProvider である必要があります。
「Connection Class」フィールド (ProviderConnection)	LDAP サーバーへの接続を実装する Java クラスの名前。デフォルトは intradoc.provider.LdapConnection です。
「Configuration Class」フィールド (ProviderConfig)	いくつかの追加の構成を実行する Java クラスの名前。このクラスは、接続クラスがすでにプロバイダであるデータベース・プロバイダに便利です。
「Source Path」フィールド * (SourcePath)	LDAP プロバイダを識別する一意の文字列。ユーザーが初めてプロバイダを介して資格証明をリクエストすると、この文字列はユーザー情報とともに格納されるため、次にそのユーザーが資格証明を要求した際にそのユーザーとプロバイダの照合に使用されます。ソース・パスとして、プロバイダ名を使用することをお薦めします。
「Ldap Server」フィールド * (LdapServer)	LDAP サーバーのホスト名。プロバイダが Active Directory と通信している場合は、プライマリ・ドメイン・コントローラのホスト名である必要があります。
「Ldap Suffix」フィールド * (LdapSuffix)	すべての LDAP 操作に使用するルート接尾辞（ネーミング・コンテキスト。o=company.com または dc=company,dc=com など）。Content Server のロールおよびアカウントへの LDAP グループのすべてのマッピングは、このルートから始まります。 **注意 :** カンマの前後に空白を含めないでください。
「Ldap Port」フィールド * (LdapPort)	LDAP サーバーがリスニングするポート。デフォルトは 389 です。SSL を使用する場合は、636 に設定する必要があります。

機能	説明
「Number of connections」フィールド （NumConnections）	プロバイダが維持する LDAP サーバー接続の数。
「Connection timeout」フィールド	プロバイダ接続が閉じられて再度開かれるまでに、LDAP サーバーへのプロバイダ接続が開かれている時間（分単位）。 **注意 :** 最良の結果を実現するには、時間を 15 分未満に設定します。時間が 15 分以上の場合、開いている接続を保持していない JNDI 層で問題が発生する可能性があります。
「Priority」フィールド （Priority）	ユーザー資格証明に関して LDAP プロバイダが確認される順序を指定します。 • このフィールドは、ユーザーがこれまでに Content Server にログインしたことがない場合にのみ使用します。ユーザーが資格証明をリクエストしたことがある場合は、そのユーザー用にソース・パスが保存されているため、そのソース・パスによって指定された LDAP プロバイダが使用されます。 • Content Server インスタンスの各 LDAP プロバイダには、一意の優先度番号が必要です。
「Using Netscape SDK」チェック・ボックス （UseNetscape）	LDAP サーバーへの接続には、Netscape SDK を使用する方法と JNDI を使用する方法の 2 つがあります。このチェック・ボックスは、その 2 つのオプションの切替えの役割を果します。 **選択 :** Netscape SDK を使用 **選択解除 :** JNDI を使用
「Use SSL」チェック・ボックス （UseSecureLdap）	このチェック・ボックスを選択する場合、LDAP サーバーに適切な資格証明がインストールされている必要があります。SSL が起動されると、資格証明により、LDAP サーバーおよびコンテンツ・サーバー間の通信が保護されます。

機能	説明
「Use Group Filtering」セクション 詳細は、7-5 ページの「ロールおよびアカウントのマッピング」を参照してください。	
「Use Group Filtering」チェック・ボックス (UseGroupFilter)	**選択 :** Content Server のロールおよびアカウントにマッピングされる LDAP グループの選択に、ロール接頭辞およびアカウント接頭辞の定義が使用されます。 **選択解除 :** すべての LDAP グループが Content Server のロールおよびアカウントにマッピングされます。これがデフォルトです。
「Use Full Group Names」チェック・ボックス (UseFullGroupName)	**選択 :** LDAP グループの階層全体（指定された接頭辞またはネーミング・コンテキストまで）が、Content Server のロールまたはアカウントへのマッピングに含まれます。 **選択解除 :** LDAP グループの最下位レベルのユニットのみが Content Server のロールまたはアカウントにマッピングされます。これがデフォルトです。
「Account Permissions Delimiter」フィールド (AcctPermDelim)	LDAP のグループ名のアカウント権限とアカウント名を区切る文字列。 • LDAP のグループ名がアカウントにマッピングされていて、このサブストリングが含まれている場合、このサブストリングの左側の文字列がアカウント名で、右側の文字列がアカウント権限です。 • たとえば、デリミタが + （プラス記号）に定義されている場合、グループ名 Acct1+rw は、読取りおよび書込み権限のある Acct1 という名前のアカウントにマッピングされます。デリミタが _（アンダースコア）に定義されている場合、Acct1+rw グループ名は、デフォルトで RWDA 権限のある Acct1+rw という名前のアカウントにマッピングされます。 • デフォルトは _（アンダースコア）です。 • このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Default Network Roles」フィールド	contributor など、このプロバイダを介して接続するユーザーに割り当てられているデフォルトのロール。

機能	説明
「Default Network Accounts」フィールド (DefaultNetworkAccounts)	LDAP 資格証明を使用して Content Server にログインするユーザーのデフォルトのアカウント権限を定義します。 • アカウントのカンマ区切りのリストである必要があります。 **注意 :** アカウントを区切るカンマの前後に空白を含めないでください。 • 各アカウントの権限は、account(RWDA) のように、アカウント名の後ろのカッコ内に指定できます。権限が指定されていない場合は、デフォルトで RWDA 権限が付与されます。 • #none エントリの場合は、アカウントが割り当てられていないドキュメントに対する権限が付与されます。 • #all エントリの場合は、すべてのアカウントに対する権限が付与されます。 • デフォルトは #none(RWDA) です。 • この設定は、匿名ユーザーには適用されません。 • この設定により最低限のアカウント権限が定義されます。外部ユーザー・ベースにより定義されたアカウント権限は、これらの権限に追加されます。たとえば、デフォルトが #none(RW),Project(R) で、ユーザーのグループが Project(RWD) 権限にマッピングされている場合、ユーザーの権限は #none(RW),Project(RWD) です。 • このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Role Prefix」フィールド	LDAP のグループ名のどの部分からが Content Server のロール名に一致するかを指定する文字列。
「Role Prefix」の「Depth」フィールド	有効なロールであるとみなされるため、LDAP のグループ名で、グループ名のロール接頭辞の後に含むことのできるレベル数を指定する数値。特定の接頭辞の深さパラメータにアスタリスク (*) を指定すると、接頭辞を使用してマッピングされた任意のグループの短縮名が使用されます。
「Role Prefix」の「Add」ボタン	「Role Prefix」ボックスに、ロール接頭辞文字列および深さが句として追加されます。

機能	説明
「Role Prefix」ボックス (RolePrefix)	「Group Filtering」チェック・ボックスが選択されている場合、LDAP グループの選択に使用されるロール接頭辞句がリストされます。このボックスは直接編集できます。 **注意 :** 接頭辞のユニットを区切るカンマの前後に空白を含めないでください。
「Account Prefix」フィールド	LDAP のグループ名のどの部分からが Content Server のアカウント名に一致するかを指定する文字列。 このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Account Prefix」の「Depth」フィールド	有効なアカウントであるとみなされるため、LDAP のグループ名で、グループ名のアカウント接頭辞の後に含むことのできるレベル数を指定する数値。 このフィールドは、Content Server でアカウントが有効化されている場合にのみ表示されます。 特定の接頭辞の深さパラメータにアスタリスク（*）を指定すると、接頭辞を使用してマッピングされた任意のグループの短縮名が使用されます。
「Account Prefix」の「Add」ボタン	「Account Prefix」ボックスに、アカウント接頭辞文字列および深さが句として追加されます。 このボタンは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Account Prefix」ボックス (AcctPrefix)	「Group Filtering」チェック・ボックスが選択されている場合、LDAP グループの選択に使用されるアカウント接頭辞句がリストされます。このボックスは直接編集できます。 **注意 :** 接頭辞のユニットを区切るカンマの前後に空白を含めないでください。 このボックスは、Content Server でアカウントが有効化されている場合にのみ表示されます。
「Attribute Map」セクション	
「LDAP Attribute」フィールド	Content Server のユーザー情報フィールドにマッピングされる LDAP のユーザー属性を入力します。

機能	説明
「User Attribute」フィールド	「LDAP Attribute」フィールドからマッピングされる Content Server のユーザー情報フィールドを選択します。 • 値を変更できるすべての Content Server のユーザー情報フィールドがリストされます。 • 標準のユーザー情報フィールドは d から始まります。 • カスタムのユーザー情報フィールドは u から始まります。
「User Attribute」の「Add」ボタン	「Attribute Map」ボックスに、LDAP 属性およびユーザー属性がコロン区切りの句として追加されます。

「Attribute Map」ボックス
(AttributeMap)
	LDAP のユーザー属性を Content Server の情報フィールドにマッピングするために使用される属性マップ句がリストされます。
	• このボックスは直接編集できます。
	• このフィールドを空にした場合、デフォルトは次のとおりです。
	`mail:dEmail`
	`cn:dFullName`
	`title:dUserType`

「Account Permissions Delimiter」セクション 詳細は、7-5 ページの「ロールおよびアカウントのマッピング」を参照してください。	
「Default Network Accounts」セクション	
「LDAP Admin DN」フィールド (LdapAdminDN)	LDAP サーバーに対するコールを行うユーザー名。 • このユーザーには、LDAP サーバーに対する読取り権限がある必要があります。 • ユーザー名を空にすると、プロバイダは LDAP サーバーに匿名で接続します。 • プロバイダが Active Directory と通信する場合は、ユーザー名とパスワードが必要で、*DOMAIN¥username* という書式の有効なドメイン・ユーザーである必要があります。

機能	説明
「Ldap Admin Password」フィールド（LdapAdminPassword）	LDAP サーバーに対するコールを行うユーザーのパスワード。
「Add」/「Update」ボタン	プロバイダ情報を保存します。
「Reset」ボタン	プロバイダ情報を最後に保存された値にリセットします。

8

プロキシ接続

概要

プロキシ接続は、Content Server のインストール時にインストールおよび有効化できるオプションのコンポーネントです。この章の情報は、このコンポーネントをインストールして有効化している場合にのみ関係があります。

この項の内容は次のとおりです。

概念

タスク

- 資格証明マップの作成（8-6 ページ）
- プロキシ接続の作成（8-9 ページ）
- HTTP プロバイダの構成（8-11 ページ）

インタフェース

- 「Credential Maps」画面（8-13 ページ）
- 「Proxied Connections」画面（8-14 ページ）
- 「Edit Outgoing Http Provider」ページ（8-16 ページ）

プロキシ接続について

プロキシ接続を使用すると、次の機能により、Content Server のセキュリティ・レベルが向上します。

- あるコンテンツ・サーバーから別のコンテンツ・サーバーへのセキュリティ資格証明マッピング
- コンテンツ・サーバーへのセキュアな名前付きパスワード接続（パスワードで保護されたプロバイダ接続）
- コンテンツ・サーバー間の HTTP プロトコルによる通信（HTTP ベースのプロキシ・サーバー）

名前付きパスワード接続と HTTP ベースのプロキシ・サーバー通信の両方を使用できますが、多くの場合、どちらかのタイプの接続を使用する方が便利です。どちらのタイプの接続でも、資格証明マッピングによりセキュリティが向上します。

プロキシ接続の一般的な使用方法は次のとおりです。

- コンテンツ・アイテムのアーカイブ・レプリケーションの実行を可能にするため。たとえば、ある企業が別の企業を買収したが、情報を共有するための共通のインフラストラクチャがないとします。どちらの企業も、Secure Sockets Layer（SSL）を使用してインターネットに接続しています。この企業で、2 つのサイト間のコンテンツを共有するとします。プロキシ接続を使用してこの企業のサーバー間にセキュアなインターネット接続を設定できるため、コンテンツには一方のサイトから安全にアクセスでき、もう一方のサイトでレプリケートおよびアーカイブできます。
- ターゲット・マスター・サーバーのプロキシ接続に対して名前付きパスワードを使用することにより、コンテンツ・サーバーへのアクセス制限を向上させるため。たとえば、コンテンツ・サーバーでの認証に Active Directory Service Interfaces（ADSI）を使用している企業が、パートナーのサーバーからその企業のコンテンツ・

サーバーへの接続に追加のセキュリティを適用するとします。名前付きパスワードを使用すると、着信接続によるアクセスを、プロキシ接続および名前付きパスワードが事前に設定されている接続に制限できます。

- エンタープライズ・サーチ機能をサポートするため。たとえば、ある企業で、特定のユーザーが 1 つ以上のコンテンツ・サーバーでエンタープライズ・サーチを実行できるようにするとします。管理者は、特定のユーザー、またはロールやアカウントが指定されたコンテンツ・サーバーへの制御されたアクセスを許可されるよう資格証明マッピングを設定できます。

資格証明マッピング

管理者は、ユーザー、ロールおよびアカウントに複数の資格証明マップを作成できます。資格証明マッピングは、マスターを別のマスターのかわりにするシナリオに便利です。たとえば、あるコンテンツ・サーバーで作成されたユーザー、ロールまたはアカウントの資格証明を、別のコンテンツ・サーバーのユーザー、ロールまたはアカウントにマッピングできるため、ユーザーは、エンタープライズ検索などのタスク用のマスターまたはプロキシ・コンテンツ・サーバーの情報への制御されたアクセスを許可されます。

この項の内容は次のとおりです。

資格証明マッピングについて

資格証明マップを作成する際には、マップの一意の識別子、およびユーザー、ロールやアカウントの固有の資格証明値を入力します。プロキシ接続では、ユーザー資格証明が入力値に一致すると、出力値で指定した資格証明がユーザーに付与されます。ユーザー資格証明は次の順序で評価されます。

1. すべてのロール
2. すべてのアカウント
3. ユーザー名

変換の実行後、ユーザーは入力値から正常にマッピングされた属性値のみを持ちます。

資格証明マップを作成したら、送信プロバイダの構成時に、名前付きパスワード接続とともに資格証明マップを指定できます。ユーザー・プロバイダ（LDAP など）の構成時にも資格証明マップを指定できます。

注意 : LDAP プロバイダのデフォルトの動作では、guest ロールは自動的にユーザーに割り当てられません。ただし、ユーザーがマスター・サーバーの資格証明を使用してプロキシ Content Server にログオンした場合は、ユーザーは自動的に guest ロールを取得します。

注意 : 資格証明マッピングの実装は、Web サーバー・プラグインおよび Content Server で複製されます。最適なパフォーマンスを実現するために設計および実装されているため、マッピングの変更内容はすぐに適用されます。（変更内容がキャッシュされ、最大数分の間コンテンツ・サーバーに反映されない、NT や NT 管理者インタフェースを使用する ADSI ユーザー記憶域のパフォーマンスと比較できます。）

資格証明値

ロールまたはユーザー名の場合、資格証明の入力値は完全一致がある場合に一致します。入力アカウント値は、フィルタの場合を除き、いずれかのユーザー・アカウントに接頭辞がある場合に一致します（8-5 ページの「ロールおよびアカウントの一致」を参照）。たとえば、次の資格証明値により、admin ロールを持つすべてのユーザーが guest ロールを持つユーザーに変更されます。

```
admin, guest
```

次の表に、資格証明値の基本的な構文を示します。

値	接頭辞または順序	例
ユーザー名	&	`&name`
ロール		`admin`
アカウント	@	`@marketing`
空のアカウント	@#none	`@#none`
すべてのアカウント	@#all	`@#all`
値を無視または値をコメント・アウト	#	`#comment`

資格証明マップが割り当てられていない場合は、どの資格証明がデフォルトで適用されているかを表示できます。変更せずにすべてをマッピングする次のマッピングを使用します。このマッピングでは、まずすべてのロールが、次にすべてのアカウントがフィルタ処理されます。マッピング構文の詳細は、8-5 ページの「ロールおよびアカウントの一致」を参照してください。

```
|#all|,%%
@|#all|,@%%
```

警告 : 資格証明マップに、匿名ユーザーがコンテンツ・サーバーの Web サイトに接続する際に付与される最低限の権限も割り当てられていない場合、ログイン済のユーザーが異常な動作を体験する可能性があります。たとえば、アクセスが拒否されたというレスポンスを受信するブラウザでは、一般的に匿名ユーザーに戻ります。特に、ドキュメントにアクセスできる場合やアクセスできない場合に、予期しない動作が発生する可能性があります（その場合に、ブラウザがユーザーの認証資格証明を送信するかしないかによって異なります）。NTLM 認証は定期的に更新する必要があるため、これは特に NTLM 認証に当てはまります。

ロールおよびアカウントの一致

アカウントおよびロールの一致には特別なフィルタを使用できます。たとえば、アカウント・フィルタの構文は、アカウント値を接頭辞 @| で開始し、| で終了することで指定されます（`@|accountname|` など）。パイプ（|）は、フィルタを介して値を処理するコマンド・リダイレクション演算子を表します。プロキシ接続の場合は、空白で区切られたアカウントのリストが指定されます。各アカウントをダッシュ（-）で開始して、負の値を指定することもできます。ダッシュで開始されていない指定した任意のアカウント文字列がユーザー・アカウントの接頭辞である場合や、ダッシュで開始されているすべてのアカウント文字列がそのユーザー・アカウントの接頭辞ではない場合に、フィルタが一致します。

警告 : フィルタでは、アカウント `@#all` はマッピングされません。`all accounts` というアカウント値を明示的にマッピングするには、`@#all, @#all` マッピングを使用する必要があります。

ロールは、フィルタの先頭から @ 記号を削除することで（同じルールを使用して）マッピングできます。たとえば、次の入力値では、接頭辞 `visitor` で開始されるロールを除くすべてのロールが取得されます。`#all` という式では、すべてのロールが一致することに注意してください。

```
|#all -visitor|, %%
```

入力値の参照

出力値の特殊な配列 %% を使用して、入力値を参照できます。たとえば、次のマッピングでは、接頭辞 `financial` で開始されないすべてのアカウントは同じアカウントにマッピングされますが、先頭に接頭辞 `employee/` が追加されます。

```
@|#all -financial|, @employee/%%
```

ユーザーのアカウントが marketing の場合、マッピング後、ユーザーのアカウントは employee/marketing になります。

権限レベル

カッコで囲まれた文字 R、W、D または A を使用したアカウント指定に準拠することで、出力値のアカウントに特定の権限レベル（読取り、書込み、削除、すべて）を付与できます。たとえば、次の構文で、すべてのアカウントのすべての権限レベルを読取り権限に変更できます。

```
@|#all -financial|, @employee/%%(R)
```

置換

置換 %% を適用する前に、接頭辞を削除するのが便利な場合があります。構文 %%[n] を使用して、置換のオフセットを指定できます。ここで、n は、%% 式に入力値をマッピングする前に使用する開始のオフセットです。オフセットはゼロベースであるため、%%[1] では入力値の先頭の文字が削除されます。たとえば、すべてのロールから接頭辞 DOMAIN1¥ を削除するには、次の式を使用します。

```
|domain1¥|, %%[8]
```

この機能の別の使用方法は、接頭辞 marketing/ で開始されるすべてのアカウントを、接頭辞 org1/mkt で置換することです。この式は次のようになります。

```
@|marketing/|, @org1/mkt/%%[10]
```

特殊文字

入力値で指定するのが難しい一般的ではない文字が、ロールに含まれている場合があります。エスケープ・シーケンス %*xx*（ここで *xx* は ASCII の 16 進値）を使用して、入力値に文字を指定できます。たとえば、#,& |@（シャープ、カンマ、アンパサンド、空白、パイプ、アットマーク）で始まるすべてのロールを取得するには、次の式を使用します。

```
|%35%2c%26%20%7c%40|, %%
```

資格証明マップの作成

資格証明マップを作成するには、次の手順を実行します。

1. 新しいブラウザ・ウィンドウを開き、システム管理者として Content Server にログインします。
2. **「Administration」→「Credential Maps」**を選択します。

   「Credential Maps」画面（8-13 ページ）が表示されます。
3. 作成する資格証明マップの一意の識別子を入力します。

重要 : コンテンツ・サーバーへの接続に、複数の名前付きパスワード接続を使用できます。それぞれの名前付きパスワード接続に、異なる資格証明マップを使用できます。

4. 値を 2 列で入力します。列はカンマで区切り、値の各行の間にはキャリッジ・リターンを使用します。1 列目では入力値を指定し、2 列目では出力値を指定します。
5. 「**Update**」をクリックします。

重要 : NT 統合を使用して取得したロールおよびアカウントに資格証明マップを適用するには、Content Server の構成エントリ ExternalCredentialsMap を、適用する資格証明マップの名前に設定します。

CONTENT SERVER へのセキュアな接続

コンテンツ・サーバーへのセキュアな接続は、着信リクエストにパスワードの保護を作成することでサポートできます。パスワードを保護すると、コンテンツ・サーバーは別のコンテンツ・サーバーのプロキシとして機能できます。

この項の内容は次のとおりです。

名前付きパスワード接続について

「Proxied Connections」ページを使用して、名前付きパスワードを作成できます。名前付きパスワードは、特定のプロキシ接続に名前で割り当てるパスワードです。各名前付きパスワードを関連付けられるのは、コンテンツ・サーバーへの直接ソケット通信と、コンテンツ・サーバーの Web サーバー（HTTP フィルタ）を制御することで実行される任意の通信の両方に対するホストおよび IP アドレス・フィルタです。外部エージェント（別のコンテンツ・サーバーの Web サーバーなど）がマスター・コンテンツ・サーバーと通信する必要がある場合には、名前付きパスワード接続を使用できます。名前付きパスワード接続は、資格証明マップにも関連付けられるため、コンテンツ・サーバーにアクセスするユーザーの権限を削減することや変更することが可能です。

プロキシ接続のエントリ・フィールドは、送信ソケット・プロバイダおよび送信 HTTP プロバイダを構成するためのフォームに提供されており、名前付きパスワード接続を指定できます。（インスタンスに選択されているプロバイダを表示するには、「**Administration**」→「**Providers**」を選択します。）

パスワードは、クライアント側の許可されているホストおよび IP アドレスのワイルドカード・フィルタを使用してハッシュされます（SHA1 メッセージ・ダイジェスト）。これは、格納されているパスワードのコピーが露呈した場合、ホストおよび IP アドレス・フィルタの両方を満たすクライアントからのアクセスのみが許可されることを意味します。

警告 : すべてのパスワードは、サーバーに送信される前にタイムアウト値でハッシュされます。これは、サーバーへの通信中にパスワード値が露呈した場合、有効期限（リクエストが発行された後の約 15 分）までの間のみパスワードが使用不可になることを意味します。また、前述した同じソース・ホストおよび IP アドレスからのリプレイ攻撃でのみ、パスワードが使用不可になります。ファイアウォールで保護された内部ホストおよび IP アドレスが使用されていない場合は、その実行した攻撃者が主要な DNS サーバーのいずれかをハイジャックすることで、ホストおよび IP アドレスが偽装される可能性があります（複数件発生しています）。

重要 : パスワードに有効期限を実装する場合は、関連する様々なサーバーの時計がかなり正確（最低数分以内）に同期している必要があります。

プロキシ接続データのガイドライン

「Proxied Connections」ページに入力するデータにより、外部エージェントがコンテンツ・サーバーに接続する際に使用可能な異なるパスワードを定義できます。様々な理由（メッセージ・ダイジェスト・アルゴリズムでクリア・テキスト・パスワードが使用されていないなど）でクライアントに対して使用できない可能性があるため、外部エージェントに各ユーザーのパスワードの入力を要求するのではなく、プロキシ接続を使用します。これにより、ユーザーは単一の名前付き接続パスワードを使用して認証できます。各名前付きパスワード接続をルールにリンクし、マスター・コンテンツ・サーバーに接続できるホストを制限することや、ユーザーに付与される権限を制御することができます。各名前付きパスワード接続は一意に識別されますが、コール側のエージェントはパスワードとともに識別子を指定する必要があります。

ホスト名および IP アドレス・フィルタは、コンテンツ・サーバーへの直接ソケット接続を実行する際に、どのホスト名または IP アドレスで名前付きパスワード接続の使用が許可されているかの判断に使用されます。フィルタの定義ルールは、システム・プロパティ・エディタに定義されているルールと同様です（0 または複数の一致を表す * や、いずれかに一致を表す | のワイルドカード記号を使用して、柔軟なルールを作成できます）。エントリが空の場合には、ターゲット属性の制限はありません（後から示す 2 つのフィールドのどちらが関連するかによって、クライアントのホスト名または IP アドレスのいずれかになります）。

Web サーバーを介して別のコンテンツ・サーバーのかわりをするには、コンテンツ・サーバーに HTTP IP アドレス・フィルタを指定する必要があります。このフィルタはクライアント・サーバーの IP アドレスに適用され、マスター・サーバーが一致する場合に通信を続行できます。

「Providers」ページを介して、次の 2 つのオプションが実装されます。

- 送信プロバイダを追加した場合には、名前付きパスワード接続の使用、および（Web アクセスとセキュリティがリモート・サーバーを介して制御されるように）プロバイダをプロキシ・サーバーにするかどうかの選択のオプションがあります。
- ユーザー・プロバイダ（LDAP など）を追加した場合は、使用可能な資格証明マップの使用を選択できます。

資格証明マップは、「Proxied Connections」ページには定義されていません。資格証明マップの作成の詳細は、8-3 ページの「資格証明マッピング」を参照してください。

プロキシ接続の作成

プロキシ接続を作成するには、次の手順を実行します。

1. 新しいブラウザ・ウィンドウを開き、システム管理者として Content Server にログインします。
2. **「Administration」**をクリックします。
3. **「Connection Passwords」**をクリックします。

   「Proxied Connections」画面（8-14 ページ）が表示されます。
4. 「Proxied Connections」ページのフィールドに情報を入力します。

   資格証明マップが存在する場合は、既存の資格証明マップの使用を選択できます。また、プロキシ接続に使用する資格証明マップを作成することもできます。
5. **「Update」**をクリックします。

HTTP プロトコルを使用する CONTENT SERVER プロキシ

管理者は、HTTP プロトコルを使用してプロキシ・コンテンツ・サーバーを作成できます。たとえば、どちらもそれぞれの機能にアクセスするための Web サーバーを持つ、2 つのコンテンツ・サーバーを作成できます。多くのユーザーがそれらのコンテンツ・サーバーのいずれかにある情報へのアクセスにブラウザを使用する必要があるが、すべてのユーザーがそのサーバーに直接アクセスできるわけではない場合に、この機能は便利です。プロキシ・コンテンツ・サーバーを設定すると、ユーザーはマスター・コンテンツ・サーバーにアクセスでき、それを介してプロキシ・コンテンツ・サーバーの情報にもアクセスできます。

アーカイブの転送には、HTTP プロトコルも便利です。HTTP プロバイダは、Secure Socket Layer（SSL）を使用した HTTPS プロトコルと連携し、2 つのコンテンツ・サーバー間のセキュアな通信を可能にします。

この項の内容は次のとおりです。

Content Server プロキシに対する HTTP プロトコルの使用について

管理者は、「Providers」ページを介して構成可能な httpoutgoing プロバイダを実装できます。このプロバイダにより、ある Content Server（マスター）から別の Content Server（プロキシ）への通信が可能になります。Content Server の <*Weblayout_Dir*>/groups/ に対する静的 URL のすべてのリクエストは、別の Web サーバーに転送され、Content Server レベルのプロキシとともに Web サーバー・レベルにもプロキシが作成されます。

httpoutgoing HTTP プロバイダの追加を選択した場合、次の追加のオプションがあります。

- CGI URL の指定
- 名前付きパスワード接続およびクライアント IP フィルタの指定
- （Web アクセスおよびセキュリティがリモート・サーバーを介して制御されるよう）プロバイダをプロキシ・サーバーにするかどうかの選択

この場合に使用される HTTP プロバイダは、代替する側と代替される側の構成方法や、エンタープライズ検索の構成方法の点で通常の送信プロバイダに非常に似ています。

httpoutgoing HTTP プロバイダの選択を表示するには、Content Server のナビゲーション・パネルから「**Administration**」→「**Providers**」を選択します。

注意 : マスター・コンテンツ・サーバーを別のマスター・コンテンツ・サーバーのかわりにする場合は、IdcRealm（以前の IntradocRealm）に共通の値を選択し、各サーバーの config.cfg ファイルに同じ値を入力します。レルムは、ユーザーがブラウザによりログインを要求される際に、ユーザー名およびパスワードの上位にある値です。IdcRealm に共通の値を設定しない場合、一方のマスター・サーバーにより配信されるコンテンツから、もう一方のマスター・サーバーにより配信されるコンテンツに切り替える際に、ユーザーは再度ログインする必要があります。

警告 : 2 つのコンテンツ・サーバー間にプロキシ関係を作成するには、いくつかの準備が必要です。マスター・サーバーで、weblayout ディレクトリに、プロキシ・サーバーと同じ相対 Web ルートを使用することはできません。プロキシ・サーバーへの追加のナビゲーション・リンクを提供するには、コンポーネント・アーキテクチャを一部変更する必要があります。プロキシ・サーバーの相対 URL が proxied1 の場合、次の例の動的にレンダリングされたホームページ（マスター・サーバーから参照）へのパスは次のようになります。

```
http://<host_name>/idcm1/idcplg/proxied1/pxs?IdcService=GET_DOC_PAGE&
Action=GetTemplatePage&Page=HOME_PAGE
```

/proxied1/pxs 接尾辞構成により、このリクエストがプロキシ・サーバー宛であることが、Web サーバー・フィルタに伝達されます。

注意 : Web サーバーで SSL が使用され、マスター・サーバーのフロントエンドで HTTP が使用されている状態でプロキシ・コンテンツ・サーバーを設定した場合、ユーザーがブラウザでマスター・サーバーの URL を変更してプロキシ・サーバーへのアクセスを試行すると、HTTPS（資格証明が必要）と HTTP の間の差異が原因でエラーが発生します。この問題を解決するには、Content Server とともに入手可能な BrowserUrlPath コンポーネントを使用します。詳細は、使用しているオペレーティング・システム向けの Oracle Content Server のインストレーション・ガイドと、コンポーネントの readme.txt ファイルを参照してください。

HTTP プロバイダの構成

プロキシ HTTP プロバイダを構成するには、次の手順を実行します。

注意 : アーカイブを転送するためにのみプロキシ HTTP プロバイダを設定する場合は、スタブ weblayout ディレクトリを作成する必要はありません。手順 8 から構成を開始してください。

1. マスター・コンテンツ・サーバーで、Content Server インストールの下に http-web-stubs ディレクトリを追加します。たとえば、C:¥stellent¥http-web-stubs のようになります。

2. http-web-stubs ディレクトリの下に、プロキシ・コンテンツ・サーバーの相対 Web ルートと同じ名前を使用してディレクトリを作成します。たとえば、C:¥stellent¥http-web-stubs¥stellent のようになります。
3. プロキシ・サーバーの weblayout ディレクトリ（groups サブディレクトリを除く）をコピーして、マスター・サーバーの C:¥stellent¥http-web-stubs ディレクトリの下に貼り付けます。
4. マスター・サーバーの Web サーバーに、仮想ディレクトリを追加します。仮想ディレクトリの名前は、プロキシ・サーバーの相対 Web ルートと同じである必要があります。仮想ディレクトリを、http-web-stubs ディレクトリの下の weblayout ディレクトリに指定します。

重要 : このコピーされたコンテンツはどこにでも配置でき、Web サーバーがそのディレクトリの適切な相対 URL をマッピングするよう設定されているかぎり、マスター・サーバーの weblayout ディレクトリの下に配置する必要はありません。

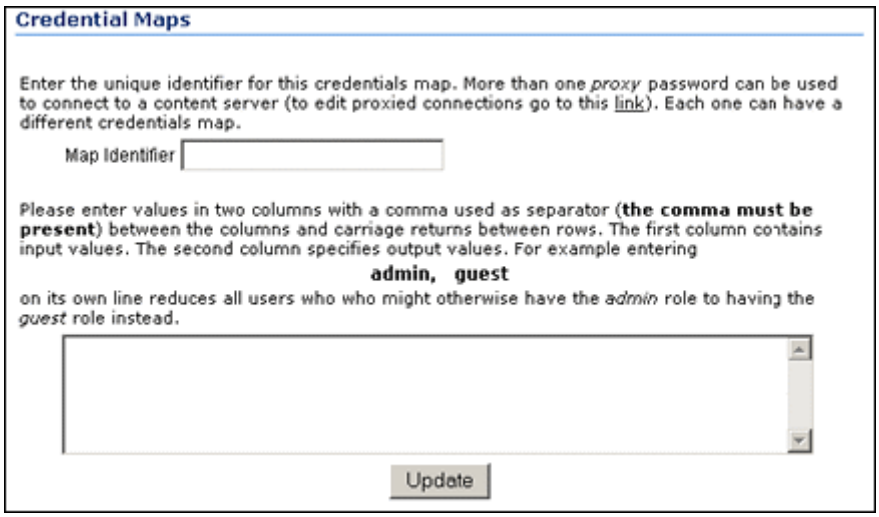
5. マスター Content Server を再起動します。
6. マスター Web サーバーを再起動します。
7. プロキシ・サーバーからマスター・サーバーへのエンタープライズ検索機能が必要な場合は、プロキシ・サーバーに対して手順 1 ～ 6 を繰り返します。
8. マスター Content Server に httpoutgoing プロバイダを追加します。プロキシ・サーバーからマスター・サーバーへのエンタープライズ・サーチ機能が必要な場合は、プロキシ・サーバーに対してこの手順を繰り返します。
   a. ブラウザで、「Administration」ページに移動して「**Providers**」をクリックします。
   b. httpoutgoing プロバイダ・タイプの隣にある「**Add**」をクリックします。
   c. httpoutgoing プロバイダの必要な情報を入力します。詳細は、8-16 ページの「「Edit Outgoing Http Provider」ページ」の表を参照してください。
      - ❖「Server Options」では「**Proxied**」を選択します。
      - ❖ エンタープライズ・サーチの場合は、「**Enterprise Searchable**」を選択します。
9. 前の手順で指定した名前付きパスワード接続および接続パスワードを使用するプロキシ・サーバーにプロキシ接続を作成します。
   a. プロキシ・サーバーで、「**Administration**」→「**Connection Passwords**」を選択します。
   b. プロキシ接続の情報を入力します。IP アドレス・フィルタ・エントリには、マスター・サーバーの IP アドレスが含まれている必要があります。

プロキシ接続のインタフェース画面

プロキシ接続を作成する際には、次の画面を使用します。

- ❖ 「Credential Maps」画面（8-13 ページ）
- ❖ 「Proxied Connections」画面（8-14 ページ）
- ❖ 「Edit Outgoing Http Provider」ページ（8-16 ページ）

「Credential Maps」画面

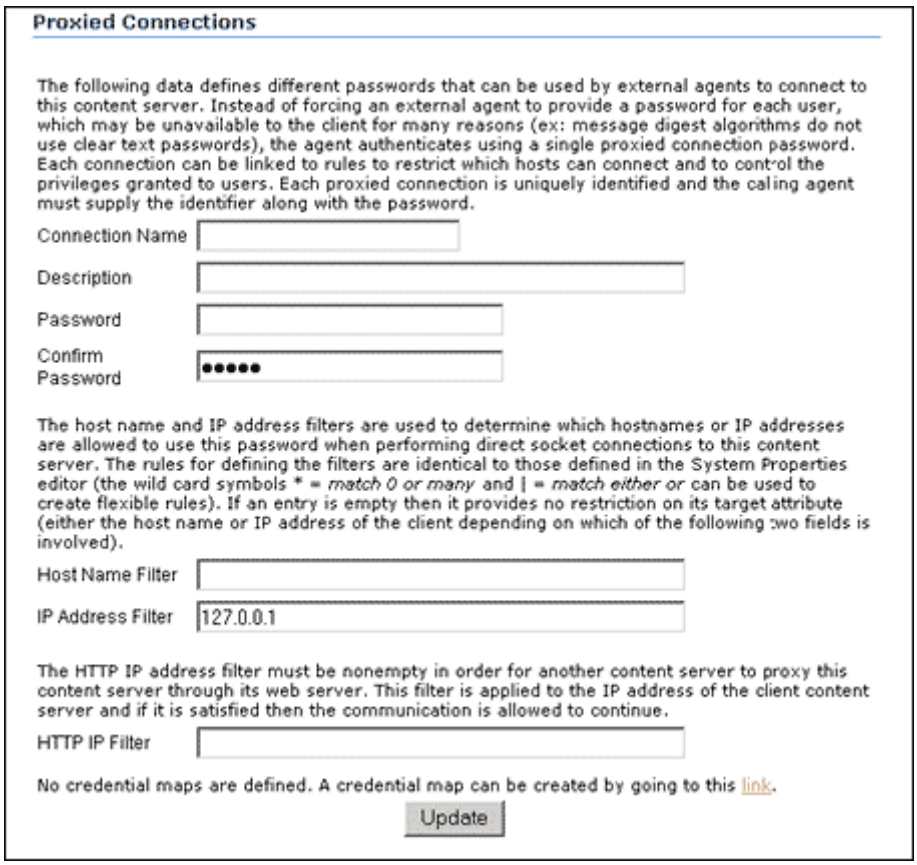


管理者はこの画面を使用して、特定のユーザーの資格証明を作成できます。この資格証明をマッピングして、ユーザーにマスター・コンテンツ・サーバーとプロキシ・コンテンツ・サーバー間の制御されたアクセスを許可できます。このページにアクセスするには、Content Server のナビゲーション・パネルから「**Administration**」→「**Credential Maps**」を選択します。

機能	説明
「Map Identifier」フィールド	資格証明マップの一意の識別子を入力します。
値フィールド	資格証明値を 2 列で入力します。列の間のセパレータとしてカンマを使用し、行の間にはキャリッジ・リターンを入力します。1 列目には入力値を指定します。2 列目には出力値を指定します。

機能	説明
「Update」ボタン	「Credential Maps」ページに指定された資格証明値を入力します。

「Proxied Connections」画面



管理者はこの画面を使用して、名前付きパスワードを作成できます。名前付きパスワードは、特定のプロキシ接続に名前で割り当てるパスワードです。このページにアクセスするには、Content Server のナビゲーション・パネルから「**Administration**」→「**Connection Passwords**」を選択します。

機能	説明
「Connection Name」フィールド	プロキシ接続に付けられた名前。
「Description」フィールド	プロキシ接続の簡単な説明。
「Password」フィールド	プロキシ接続に割り当てられたパスワード。
「Confirm Password」フィールド	プロキシ接続に割り当てられたパスワード。
「Host Name Filter」フィールド	マスター・サーバーへの直接ソケット接続の実行時にパスワードを使用できるホスト名。
「IP Address Filter」フィールド	クライアント・コンテンツ・サーバーの IP アドレス番号。
「HTTP IP Filter」フィールド	クライアント・コンテンツ・サーバーの IP アドレスに適用された HTTP IP アドレス・フィルタ。

「Edit Outgoing Http Provider」ページ

管理者はこの画面を使用して、マスター Content Server に httpoutgoing プロバイダを追加できます。このページにアクセスするには、次の手順を実行します。

1. Content Server のナビゲーション・パネルから「**Administration**」→「**Providers**」を選択します。

   「Providers」ページが表示されます。

2. 「**Create a New Provider**」の下で、httpoutgoing プロバイダの「Action」列の「**Add**」を選択します。

機能	説明
「Provider Name」フィールド *	プロバイダの名前。
「Provider Description」フィールド *	わかりやすいプロバイダの説明。
「Provider Class」フィールド *	プロバイダの Java クラスの名前。proxyconnections.HttpOutgoingProvider などです。
「Connection Class」フィールド	プロバイダ接続を実装する Java クラスの名前。proxyconnections.HttpOutgoingConnection などです。
「Configuration Class」フィールド	いくつかの追加の構成を実行する Java クラスの名前。このフィールドは空のままにします。
「CGI URL」フィールド *	プロキシ・サーバーの URL。
「Instance Name」フィールド *	プロキシ・コンテンツ・サーバーのインスタンス名。
「Relative Web Root」フィールド *	コンテンツ・サーバー・インスタンスの相対 Web ルート。
「Connection Password Name」フィールド	パスワード接続の名前（既存の名前か、プロキシ・サーバーで作成するパスワード接続の名前）。名前は、ターゲット・マスター・サーバーのいずれか 1 つのプロキシ接続を指定している必要があります。ターゲット・サーバーには名前付きパスワードが必要です。
「Connection Password」フィールド	名前付きパスワード接続のパスワード。
「Client IP Filter」フィールド	クライアント IP アドレス、またはターゲット・サーバーにこの接続を使用できるアドレス。
「Proxied」チェック・ボックス	プロバイダが現行インスタンスにより制御されるコンテンツ・サーバーに接続している場合に、このオプションを有効化します。

機能	説明
「Notified Target」チェック・ボックス	プロバイダが制御インスタンスとして機能しているコンテンツ・サーバーに接続していて、ユーザー情報またはコンテンツ・アイテム情報（あるいはその両方）が変更された際に、そのコンテンツ・サーバーからその制御インスタンスに通知する場合に、このオプションを有効化します。
「Users」チェック・ボックス	ユーザー情報が変更された際にコンテンツ・サーバーから制御インスタンスに通知する場合に、このオプションを有効化します。
「Released Documents」チェック・ボックス	コンテンツ・アイテム情報が変更された際にコンテンツ・サーバーから制御インスタンスに通知する場合に、このオプションを有効化します。
「Enterprise Searchable」チェック・ボックス	エンタープライズ検索を有効化し、このコンテンツ・サーバー・インスタンスを検索可能にする場合に、このオプションを有効化します。詳細は、『Stellent Enterprise Search Administration and User Guide』を参照してください。
「Required Roles」フィールド	エンタープライズ・サーチを使用してこのコンテンツ・サーバー・インスタンスを検索する権限があるロールを入力します。ロールを入力しない場合、すべてのユーザーに権限が付与されます。
「Account Filter」フィールド	エンタープライズ検索を使用してこのコンテンツ・サーバー・インスタンスを検索する権限があるアカウントを入力します。アカウントを入力しない場合、すべてのユーザーに権限が付与されます。
「Add」ボタン	プロバイダ情報を保存します。
「Reset」ボタン	プロバイダ情報を最後に保存された値にリセットします。

* 必須メタデータ・フィールド

A

サード・パーティ・ライセンス

概要

この付録には、この製品に付属するすべてのサード・パーティ製品のサード・パーティ・ライセンスの説明が含まれます。

APACHE SOFTWARE LICENSE

```
* Copyright 1999-2004 The Apache Software Foundation.
* Licensed under the Apache License, Version 2.0 (the "License");
* you may not use this file except in compliance with the License.
* You may obtain a copy of the License at
*      http://www.apache.org/licenses/LICENSE-2.0
*
```

```
* Unless required by applicable law or agreed to in writing, software
* distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
```

W3C® SOFTWARE NOTICE AND LICENSE

```
* Copyright © 1994-2000 World Wide Web Consortium,
* (Massachusetts Institute of Technology, Institut National de
* Recherche en Informatique et en Automatique, Keio University).
* All Rights Reserved.  http://www.w3.org/Consortium/Legal/
*
* This W3C work (including software, documents, or other related items) is
* being provided by the copyright holders under the following license.By
* obtaining, using and/or copying this work, you (the licensee) agree that
* you have read, understood, and will comply with the following terms and
* conditions:
*
* Permission to use, copy, modify, and distribute this software and its
* documentation, with or without modification, for any purpose and without
* fee or royalty is hereby granted, provided that you include the following
* on ALL copies of the software and documentation or portions thereof,
* including modifications, that you make:
*
*   1. The full text of this NOTICE in a location viewable to users of the
*      redistributed or derivative work.
*
*   2. Any pre-existing intellectual property disclaimers, notices, or terms
*      and conditions.If none exist, a short notice of the following form
*      (hypertext is preferred, text is permitted) should be used within the
*      body of any redistributed or derivative code: "Copyright ©
*      [$date-of-software] World Wide Web Consortium, (Massachusetts
```

```
*      Institute of Technology, Institut National de Recherche en
*      Informatique et en Automatique, Keio University).All Rights
*      Reserved. http://www.w3.org/Consortium/Legal/"
*
*   3. Notice of any changes or modifications to the W3C files, including the
*      date changes were made.(We recommend you provide URIs to the location
*      from which the code is derived.)
*
* THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS
* MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT
* NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR
* PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE
* ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.
*
* COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR
* CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR
* DOCUMENTATION.
*
* The name and trademarks of copyright holders may NOT be used in advertising
* or publicity pertaining to the software without specific, written prior
* permission.Title to copyright in this software and any associated
* documentation will at all times remain with copyright holders.
*
```

ZLIB LICENSE

```
* zlib.h -- interface of the 'zlib' general purpose compression library
  version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler
This software is provided 'as-is', without any express or implied
  warranty.In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
     claim that you wrote the original software.If you use this software
     in a product, an acknowledgment in the product documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly jloup@gzip.org
  Mark Adler madler@alumni.caltech.edu
```

一般的な BSD ライセンス

一般的な MIT ライセンス

DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNICODE ライセンス

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/ .Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement.BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT.IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2006 Unicode, Inc. All rights reserved.Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS.IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

その他の帰属

索引

記号

A

C

D

N

O

P

R

S

U

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

わ