

Oracle® Access Manager

ID および共通管理ガイド

10g (10.1.4.0.1)

部品番号 : B31468-01

2006 年 11 月

Oracle Access Manager ID および共通管理ガイド, 10g (10.1.4.0.1)

部品番号 : B31468-01

原本名 : Oracle Access Manager Identity and Common Administration Guide, 10g (10.1.4.0.1)

原本部品番号 : B25343-01

原本著者 : Nina Wishbow

原本協力者 : Gail Tiberi

Copyright © 2000, 2006 Oracle. All rights reserved.

制限付権利の説明

このプログラム（ソフトウェアおよびドキュメントを含む）には、オラクル社およびその関連会社に所有権のある情報が含まれています。このプログラムの使用または開示は、オラクル社およびその関連会社との契約に記された制約条件に従うものとします。著作権、特許権およびその他の知的財産権と工業所有権に関する法律により保護されています。

独立して作成された他のソフトウェアとの互換性を得るために必要な場合、もしくは法律によって規定される場合を除き、このプログラムのリバース・エンジニアリング、逆アセンブル、逆コンパイル等は禁止されています。

このドキュメントの情報は、予告なしに変更される場合があります。オラクル社およびその関連会社は、このドキュメントに誤りが無いことの保証は致し兼ねます。これらのプログラムのライセンス契約で許諾されている場合を除き、プログラムを形式、手段（電子的または機械的）、目的に関係なく、複製または転用することはできません。

このプログラムが米国政府機関、もしくは米国政府機関に代わってこのプログラムをライセンスまたは使用する者に提供される場合は、次の注意が適用されます。

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

このプログラムは、核、航空産業、大量輸送、医療あるいはその他の危険が伴うアプリケーションへの用途を目的としておりません。このプログラムをかかるとして使用する際、上述のアプリケーションを安全に使用するために、適切な安全装置、バックアップ、冗長性（redundancy）、その他の対策を講じることは使用者の責任となります。万一かかるとしてプログラムの使用に起因して損害が発生いたしましても、オラクル社およびその関連会社は一切責任を負いかねます。

Oracle、JD Edwards、PeopleSoft、Siebel は米国 Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称は、他社の商標の可能性がります。

このプログラムは、第三者の Web サイトへリンクし、第三者のコンテンツ、製品、サービスへアクセスすることがあります。オラクル社およびその関連会社は第三者の Web サイトで提供されるコンテンツについては、一切の責任を負いかねます。当該コンテンツの利用は、お客様の責任になります。第三者の製品またはサービスを購入する場合は、第三者と直接の取引となります。オラクル社およびその関連会社は、第三者の製品およびサービスの品質、契約の履行（製品またはサービスの提供、保証義務を含む）に関しては責任を負いかねます。また、第三者との取引により損失や損害が発生いたしましても、オラクル社およびその関連会社は一切の責任を負いかねます。

目次

はじめに	xiii
対象読者	xiv
ドキュメントのアクセシビリティについて	xiv
関連ドキュメント	xv
表記規則	xvi
サポートおよびサービス	xvi
Oracle Access Manager の新機能	xvii
製品とコンポーネントの名称変更	xviii
グローバル化	xix
パスワード・ポリシーとロスト・パスワード管理	xx
複数の検索ベースの構成	xx
ワークフローの構成	xx
監査	xx
ロギング	xx
ディレクトリ・サーバーの構成	xxi
Active Directory	xxi
トラブルシューティング	xxi
第 I 部 Oracle Access Manager 管理の概要	
1 管理の準備	
前提条件	1-2
ID システムの構成および管理について	1-2
ID システムのコンポーネント	1-2
ID システムのインストールおよび設定の確認	1-3
ID システムの構成について	1-4
ID システムの管理について	1-5
Oracle Access Manager の使用方法の概要	1-6
ログイン	1-6
ID システムへのログイン	1-7
アクセス・システムへのログイン	1-8
ページ上の機能領域	1-9
ナビゲーション要素	1-9
検索機能	1-10
セレクト	1-11
オンライン・ヘルプ	1-12

「バージョン情報」 ページ・リンク	1-12
ログアウト	1-12
ログアウトの手順	1-12

2 ID システム管理者の指定

ID システム管理者について	2-2
管理者の指定	2-4
管理者の削除	2-4
管理の委任	2-5
管理の委任について	2-5
委任管理モデル	2-6
エクストラネット・モデル	2-6
イントラネット・モデル	2-7
ASP モデル	2-7
委任管理者の追加	2-8
代替管理者の追加	2-10

第 II 部 ID システムの構成

3 ID システムでのスキーマ・データの使用

オブジェクト・クラスの概要	3-2
テンプレート・オブジェクトを使用した外部システムへのデータの送信	3-2
スキーマ・データを構成するためのプロセス	3-3
インストール時に構成されるオブジェクト	3-3
ID システムの構造化オブジェクト・クラスと補助オブジェクト・クラス	3-4
テンプレート・オブジェクト・クラス	3-5
オブジェクト・クラス・タイプ	3-6
オブジェクト・クラスの表示	3-6
オブジェクト・クラスの変更	3-7
クラス属性の選択	3-8
構造化オブジェクト・クラスの変更	3-9
オブジェクト・クラスの追加	3-9
補助クラスの用途	3-10
オブジェクト・クラスの削除	3-10
オブジェクト・クラス属性の概要	3-11
属性構成の概要	3-11
属性のデータ型	3-12
属性のセマンティック型	3-12
システム設定時に定義されるセマンティック型	3-13
プロファイル・ページで使用されるセマンティック型	3-14
Group Manager で使用されるセマンティック型	3-14
「ロケーション座標」セマンティック型	3-15
ロスト・パスワード管理のためのセマンティック型	3-15
その他のセマンティック型	3-15
属性の表示タイプ	3-16
属性の表示	3-18

属性の構成	3-19
ルールとリストの使用法	3-20
ルールの定義	3-20
リストの定義	3-21
属性表示名のローカライズ	3-22
「オブジェクト・セレクタ」表示タイプの検索フィルタ	3-23
「オブジェクト・セレクタ」表示タイプの検索フィルタの作成	3-24
複数のターゲット・オブジェクト・クラスの検索フィルタ	3-25
検索フィルタの削除	3-25
ルールとフィルタの使用法	3-25
静的 LDAP 検索フィルタ	3-25
ワイルド・カードを使用した静的検索	3-25
複数のターゲット・オブジェクト・クラスを使用した静的検索	3-26
置換構文: ログイン・ユーザーの DN に一致するターゲットを戻す方法	3-26
動的 LDAP 検索フィルタの例	3-27
ワイルド・カードを使用した動的検索	3-27
複数值を使用した動的検索	3-27
NOT 演算子の使用法	3-27
その他の表示タイプの構成	3-28
導出属性の構成: 異なる属性間で一致する値	3-28
導出属性の例	3-29
User Manager タブへの導出属性の割当て	3-30
導出属性の権限	3-31
アプリケーション別の属性の構成	3-31

4 User Manager、Group Manager および Organization Manager の構成

User Manager、Group Manager および Organization Manager の概要	4-2
タブの構成	4-2
タブ構成情報の表示と変更	4-3
タブのローカライズ	4-5
Organization Manager へのタブの追加	4-6
タブの検索属性の指定	4-6
検索結果に表示される属性の表示、変更およびローカライズ	4-7
User Manager または Organization Manager タブへの補助オブジェクト・クラスおよび テンプレート・オブジェクト・クラスの追加	4-8
Group Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラス の追加	4-9
Group Manager タブのオプションの構成	4-10
Organization Manager でのタブの削除	4-11
Organization Manager でのタブの並べ替え	4-11
タブのプロファイル・ページおよびパネルの構成	4-11
パネルでの LDAP オブジェクトおよびテンプレート・オブジェクトの使用	4-12
ヘッダー・パネルの構成	4-12
エンド・ユーザー・アプリケーションに構成されているパネルの表示	4-13
パネルの追加、変更、ローカライズおよび削除	4-13
パネルの並べ替え	4-17
グループ・タイプ・パネルの表示	4-17
グループ・タイプ・パネルの追加、変更、ローカライズおよび削除	4-18

パネルに表示される属性の変更とローカライズ	4-20
ユーザーによる LDAP データの表示および変更の許可	4-21
検索ベースの概要	4-22
検索ベースを設定する際のガイドライン	4-22
検索ベースを変更する必要がある場合	4-23
索引付けと検索ベース	4-23
Oracle Internet Directory の索引付け要件	4-23
検索ベースの設定	4-24
グループの検索ベースを設定する場合	4-26
非結合検索ベースの構成と削除	4-26
クエリー・ビルダーを使用した LDAP フィルタの記述	4-27
一致を取得するための方法	4-29
クエリー・ビルダーを使用した拡張 LDAP フィルタの作成	4-30
表示権限と変更権限の概要	4-31
LDAP 属性権限の設定と変更	4-31
複数の属性を選択するためのキー	4-33
LDAP 属性権限の評価	4-34
アプリケーション構成の例	4-35
ユーザー・プロファイルでの写真の表示	4-35
ディレクトリへの写真のインポートと格納	4-35
ファイル・システム内の写真の参照	4-36
デフォルトの写真イメージ	4-37
Organization Manager での「ロケーション」タブの有効化	4-37
Group Manager でグループを作成する権限	4-38
エンド・ユーザーの使用例	4-38
Group Manager でのグループ・メンバーの管理	4-38
グループ・メンバーの検索	4-39
グループ・メンバーの削除	4-40
グループ・メンバーの追加	4-40
グループ・サブスクリプションの管理	4-41
グループへのサブスクライブ	4-42
監査ポリシーの構成	4-43
監査ポリシーの表示	4-43
監査ポリシーの変更	4-44
レポートの生成	4-44
レポートの構成	4-44
レポートの表示、変更、ローカライズおよび削除	4-47
拡張構成	4-48
動的グループの拡張	4-48
検索ベースのデフォルト有効範囲の変更	4-49
グループの簡易属性権限	4-50
簡易権限の実装	4-50
gscacparams.xml ファイルの例	4-50
簡易権限の予約語	4-51
Organization Manager でのコンテナ制限の設定	4-52
コンテナ制限のコピー	4-54
コンテナ制限の変更	4-54

5 ID 機能とワークフローの連携

ワークフローの概要	5-2
ワークフローの開始方法	5-2
典型的なワークフローの例	5-2
拡張ワークフロー・オプション	5-3
ワークフロー・タイプ	5-4
ワークフローの作成	5-4
ID システム・アプリケーションでユーザーがワークフローにアクセスする方法	5-5
ワークフロー・チケットの概要	5-5
ワークフローの使用例	5-6
ワークフローでの LDAP 属性とテンプレート属性の比較	5-7
ワークフローのタイプ、ステップおよびアクション	5-7
ワークフロー・ステップの概要	5-8
ステップ・アクションの概要	5-10
ステップ・アクションの説明	5-13
サブフローの概要	5-15
クイックスタート・ツールの使用方法	5-16
クイックスタート・ツールを使用した自己登録ワークフローの作成	5-18
ワークフロー・アプレットの使用方法	5-19
新規ワークフロー定義の開始	5-20
オブジェクトの作成ワークフローの LDAP ターゲットの定義	5-22
ワークフローの最初のステップの定義	5-24
ステップ属性の定義	5-26
後続のステップの定義	5-30
ワークフロー・ステップのコミット	5-31
ワークフローの有効化	5-31
ワークフローのテスト	5-31
ワークフロー定義の例	5-32
サブフローの定義	5-33
サブフローとワークフローの関連付け	5-33
サブフロー・ステップの承認	5-34
拡張ワークフロー・チケット・ルーティング	5-34
拡張チケット・ルーティングのためのワークフロー・アクションの構成	5-35
新規に割り当てられたステップ参加者への通知	5-36
動的参加者の指定	5-36
ワークフロー参加者の概要	5-36
ワークフロー・チケット・ルーティングの概要	5-37
動的参加者の概要	5-37
静的参加者の概要	5-38
「静的参加者が使用不可」ボタンの概要	5-38
動的参加者の有効化	5-39
サロゲートの指定	5-42
時間ベース・エスカレーションの有効化	5-45
非同期操作の実行	5-49
非同期ワークフローに関する留意事項	5-49
ワークフローの使用方法	5-50
ワークフローの起動	5-50

チケットの検索と処理	5-51
ユーザーの非アクティブ化と再アクティブ化	5-52
非アクティブなユーザーの再アクティブ化	5-53
ワークフローのモニタリング	5-54
リクエストのアーカイブ	5-54
リクエストの削除	5-55
他の管理者がワークフロー・チケットを操作できないようにする方法	5-55
ワークフローの管理	5-55
ワークフロー・サマリーの表示とエクスポート	5-55
ワークフローのコピー	5-57
ワークフローの変更	5-57
ワークフローの削除	5-58
ワークフローのエクスポート	5-58
ワークフロー・パネル設定の表示	5-59
ワークフロー・パネルの外観の変更	5-60
ワークフロー・パネルのローカライズ	5-61
ワークフロー・パフォーマンス	5-62
ID 管理者の変更権限	5-62
拡張ワークフロー・オプション	5-62
事前アクションと事後アクション	5-62
外部アクション	5-63
ワークフローのデータおよびアクションのカスタマイズ	5-63
ワークフローへのロールの追加	5-64
自己登録ワークフローの作成	5-65
ロケーション・ワークフローの作成	5-67

6 外部アプリケーションへの非 LDAP データの送信

非 LDAP データの構成の概要	6-2
ワークフローで非 LDAP データを使用する方法の概要	6-2
テンプレート・オブジェクトの概要	6-3
テンプレート・オブジェクト・データとワークフローの概要	6-4
オブジェクト・テンプレートの構成	6-4
オブジェクト・テンプレート・ファイルの形式	6-5
ID システムでのテンプレート・オブジェクトの表示	6-6
オブジェクト・テンプレート・ファイルの要素	6-7
オブジェクト・テンプレート・ファイルの例	6-9
テンプレート属性用の ID イベント・プラグインの作成	6-10

7 グローバル設定の構成

ID システム・アプリケーションのスタイルの構成	7-2
スタイルの表示	7-3
カスタム・スタイル・ディレクトリの追加	7-3
スタイルの配布	7-6
スタイル名の変更	7-6
スタイルの変更	7-6
スタイルの削除	7-7
デフォルト・スタイルの設定	7-7

Oracle Access Manager での複数の言語の構成	7-7
管理ページ用言語の選択	7-8
エンド・ユーザー・アプリケーションでの言語の評価順序	7-9
Identity Server 設定の構成	7-10
セッション・タイムアウトの構成	7-11
電子メール宛先のカスタマイズ	7-12
メール・サーバーの構成	7-13
キャッシュの管理	7-14
複数言語の管理	7-14
Identity Server の管理	7-15
複数の Identity Server の設定	7-15
Identity Server の追加	7-16
Identity Server パラメータの表示と変更	7-18
Identity Server パラメータの削除	7-19
コマンドラインによる Identity Server サービスの管理	7-19
ディレクトリ・サーバー・プロファイルの管理	7-20
LDAP ディレクトリ・サーバー・プロファイルの概要	7-21
LDAP ディレクトリ・サーバー・プロファイルの作成	7-22
LDAP ディレクトリ・サーバー・プロファイルの表示	7-27
LDAP ディレクトリ・サーバー・プロファイルの変更	7-28
手動によるシステム設定の再実行	7-28
ID システム設定の再実行	7-29
Policy Manager 設定の再実行	7-29
Access Server の再構成	7-30
LDAP ディレクトリ・サーバー・プロファイルへのデータベース・インスタンスの追加	7-30
LDAP 参照	7-31
LDAP ディレクトリ・サーバー・インスタンスの削除	7-33
複数のディレクトリ検索ベースの操作	7-34
RDBMS プロファイルの管理	7-35
RDBMS プロファイルの追加または変更	7-36
RDBMS データベース・インスタンスの追加または変更	7-38
WebPass の構成	7-39
構成済の WebPass の表示	7-40
WebPass の追加または変更	7-40
WebPass の削除	7-42
コマンドラインによる WebPass の変更	7-43
Identity Server と WebPass の関連付けの管理	7-45
WebPass に関連付けられている Identity Server を表示する手順	7-45
WebPass に対する Identity Server の接続を変更する手順	7-45
Identity Server を WebPass に関連付ける手順	7-46
Identity Server と WebPass の関連付けの解除	7-46
パスワード・ポリシーの構成	7-47
パスワード・ポリシーの評価順序	7-48
パスワード・ポリシーの管理	7-48
パスワード・ポリシーの表示	7-49
異なるタイプのパスワード・ポリシーのデフォルトの設定	7-49
特定ドメイン用のパスワード・ポリシーの作成	7-50
パスワード・ポリシーの変更	7-53

パスワード・ポリシーの削除	7-54
ロスト・パスワード管理	7-54
ロスト・パスワード管理 URL の構文	7-56
ユーザーへのチャレンジ・フレーズの表示	7-56
チャレンジおよびレスポンス・ページのその他の要素	7-56
ロスト・パスワード管理でユーザーに複数のチャレンジが表示される場合	7-56
ロスト・パスワード管理ポリシーの表示と構成	7-57
アクセス・システムでのパスワード・ポリシーの実施	7-61
認証スキームを変更してパスワード・ポリシーを含める方法	7-61
パスワードのリダイレクト URL の構成	7-61
パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成	7-62
パスワード期限切れ警告のリダイレクト URL の設定	7-63
アカウント・ロックアウトのリダイレクト URL の設定	7-65
Access Server キャッシュの更新	7-65
ID システムの Access Manager SDK の構成	7-65
コンポーネントのクローニングと同期化	7-67

第 III 部 共通管理タスクの実行

8 トランスポート・セキュリティ・モードの変更

トランスポート・セキュリティ・モードについて	8-2
コンポーネント間のトランスポート・セキュリティ・モード	8-3
CA 証明書について	8-5
ID システムのトランスポート・セキュリティの変更	8-6
ID システムのトランスポート・セキュリティ・モードの変更	8-7
簡易トランスポート・セキュリティ・モードへの変更	8-8
証明書トランスポート・セキュリティ・モードへの変更	8-9
アクセス・システムのトランスポート・セキュリティ・モードの変更	8-11
アクセス・システムのトランスポート・セキュリティ・モードの変更	8-11
オープン・トランスポート・セキュリティ・モードへの変更	8-15
簡易トランスポート・セキュリティ・モードへの変更	8-16
証明書トランスポート・セキュリティ・モードへの変更	8-18
ディレクトリ・サーバーのトランスポート・セキュリティの変更	8-22
トランスポート・セキュリティ・パスワードの変更	8-24
複数の CA 証明書のインポート	8-26
Access Server のセキュリティ・パスワードの変更	8-26

9 レポート

レポートについて	9-2
レポート・タイプ	9-3
データ・ソース	9-3
データ出力	9-4
出力構成	9-4
データの用途	9-4
レポート機能のサマリー	9-5

10 ログ

ロギングおよびログ・レベルについて	10-2
ログ・レベル	10-2
ログ構成ファイルについて	10-3
ログ構成ファイルのパス	10-3
ログ構成ファイル名	10-4
ログ構成ファイルの変更	10-4
埋込みコメントについて	10-4
ログ・ライターについて	10-7
ログ構成ファイルの構造	10-8
XML 要素の順序について	10-9
ロギング・レベルの制御	10-10
ログ・ハンドラの優先順位について	10-10
編集の有効化	10-11
ログ構成パラメータ	10-11
デフォルトのログ設定	10-13
デフォルトのログ構成ファイルの解析	10-14
ID システム・コンソールでのログの構成	10-15

11 監査

監査について	11-2
監査出力の考慮事項	11-2
監査セキュリティの考慮事項	11-2
監査パフォーマンスの考慮事項	11-3
静的監査レポート	11-4
動的監査レポート	11-4
監査出力の制御	11-5
監査オプションについて	11-5
監査要件	11-8
データベースの監査の要件	11-8
データベース監査のための特別なコンポーネント	11-8
サポートされているバージョンおよびプラットフォームへの更新	11-9
データベースの監査のアーキテクチャ	11-9
OCI 設定について	11-11
ODBC データ・ソース定義について	11-11
ODBC ドライバについて	11-13
Windows ODBC ドライバについて	11-13
データベース監査用の RDBMS プロファイルについて	11-13
ODBC 接続タイプを使用するデータベースのプロファイルについて	11-14
OCI 接続タイプを使用するデータベースのプロファイルについて	11-14
監査データベースについて	11-14
Crystal リポジトリについて	11-14
監査レポートについて	11-15
ファイルベース監査の設定	11-16
データベース監査の設定	11-19
データベース監査用のシステムの設定	11-20
監査データベースの設定	11-20

データベース・サーバーのインストール	11-21
監査データベースの作成	11-22
監査スキーマのアップロード	11-23
Access Server と Identity Server の監査データベースへの接続の有効化	11-28
監査の構成	11-35
監査レポートの設定	11-44

12 SNMP モニタリング

前提条件	12-2
Oracle Access Manager SNMP モニタリングおよびエージェントについて	12-2
SNMP エージェント	12-3
Oracle Access Manager MIB およびオブジェクトについて	12-3
MIB 索引フィールド	12-4
Identity Server の MIB オブジェクト	12-5
Access Server の MIB オブジェクト	12-9
SNMP モニタリングの有効化および無効化	12-13
SNMP エージェントおよびトラップの宛先の設定	12-13
SNMP 構成設定の変更	12-15
SNMP のロギング	12-16
SNMP メッセージ	12-16
Netstat 値と SNMP 値の差異	12-21
停止間隔の構成	12-21

第 IV 部 付録

A Active Directory でのデプロイ

ディレクトリ・プロファイルと検索ベースの設定	A-2
他のドメインのディレクトリ・サーバー・プロファイルの定義	A-2
非結合検索ベースの設定	A-3
非結合検索ベースの削除について	A-3
グループ検索読取り操作の構成 (オプション)	A-4
Active Directory での認証および認可	A-4
親子認証	A-5
親子認可	A-6
ObMyGroups アクション属性	A-6
credential_mapping プラグインの構成	A-7
Active Directory で使用するシングル・サインオンの構成	A-8
検索フィルタについて	A-9
SAMAccountName の長さについて	A-9
.NET 機能の構成	A-10
トラブルシューティング	A-10
Microsoft リソース	A-10

B ADSI に対する構成

Oracle Access Manager での ADSI について	B-2
推奨	B-2
ID システムの ADSI 構成	B-3
ADSI 認証を行う純粋な ADSI	B-3

LDAP 認証を行う混在 ADSI	B-4
Identity Server のバインド・メカニズム	B-4
Oracle Access Manager ADSI 構成ファイル	B-5
globalparams について	B-5
adsi_params について	B-5
アクセス・システムの ADSI 構成	B-7
ADSI 認証を行う純粋な ADSI	B-7
アクセス・システム ADSI 構成ファイル	B-8
ID システムに対する ADSI の構成	B-9
デフォルトのディレクトリ・プロファイルに対する ADSI の有効化	B-10
その他のディレクトリ・プロファイルに対する ADSI の有効化	B-10
アクセス・システムに対する ADSI の構成	B-12
pageSize パラメータの変更	B-13
トラブルシューティング	B-13

C LDAP を使用する Active Directory に対する構成

概要	C-2
LDAP に対する Policy Manager の設定	C-3
LDAP に対する Access Server の設定	C-3
LDAP での Active Directory タイムアウトの設定	C-4
ADSI での LDAP 認証の有効化	C-5

D .NET 機能の実装

あいまいな名前の解決	D-2
ANR 属性、検索および結果について	D-2
ANR に対する構成	D-3
構成データの更新	D-3
ID システム・パネルでの ANR の構成	D-4
ANR 属性アクセス制御の検証	D-5
ID システム検索での ANR の使用方法	D-5
動的にリンクされた補助クラスの構成	D-6
属性の動的な追加	D-7
グループの属性の追加	D-8
アクセス・システム認証のファスト・バインドの有効化	D-9
暗号化の有効化	D-10
統合 Windows 認証の設定	D-11
WebGate Web サーバーでの IWA の有効化	D-12
IWA に対する WebGate の構成	D-13
Oracle Access Manager での IWA 認証スキームの作成	D-13
IWA 実装のテスト	D-14
アクセス・システム・パスワード管理の使用法	D-14
管理コードとヘルパー・クラスの使用法	D-15
Authorization Manager サービスとの統合	D-15
スマートカード認証との統合	D-15
Security Connector for ASP.NET との統合	D-16
トラブルシューティング	D-16
Microsoft リソース	D-16

E Oracle Access Manager パラメータ・ファイル

ファイルのカテゴリ	E-2
パラメータ・ファイルの詳細情報	E-2

F Oracle Access Manager のトラブルシューティング

問題と解決策	F-2
ディレクトリ・サーバー・プロファイルの構成後に Identity Server のメモリー使用量が 増える	F-2
問題	F-2
解決策	F-2
ディレクトリ・サーバー・プロファイルを保存できない	F-3
問題	F-3
解決策	F-3
Active Directory: メンバーを追加するとグループ・サイズが縮小する	F-3
ディレクトリ・プロファイルに対して ADSI を有効にできない	F-4
問題	F-4
解決策	F-4
データベースの検証に失敗する	F-4
問題	F-4
解決策	F-4
簡易トランスポート・セキュリティ・モードが1年後に期限切れになる	F-5
問題	F-5
解決策	F-5
スタイルシートの検証に失敗する	F-6
問題	F-6
解決策	F-6
ワークフローを使用しているときに「xenroll.cab が見つかりません」エラーが発生する	F-6
問題	F-6
解決策	F-6
ワークフローを使用しているときに「有効化に失敗しました」エラーが発生する	F-7
問題	F-7
解決策	F-7
JPEG 写真イメージが更新されない	F-7
問題	F-7
解決策	F-7
詳細情報	F-7

索引

はじめに

Oracle Access Manager には2つの管理ガイドがあります。この『Oracle Access Manager ID および共通管理ガイド』では、ディレクトリ内のデータを読み取って利用するための Oracle Access Manager の構成、ディレクトリ・データを表示するための ID アプリケーションの構成、ユーザーへの読取り権限および書込み権限の割当て、自動的に開始する一連のステップに ID アプリケーション機能をリンクするワークフローの定義に関する情報を示します。このガイドでは、アクセス・システムと ID システムの両方に共通する機能についても説明します。共通機能には、ディレクトリ・サーバーおよびパスワード・ポリシーの構成が含まれます。

注意： Oracle Access Manager は、以前は Oblix NetPoint と呼ばれていました。スキーマ・オブジェクト、パスなどの一部の項目では、現在も "oblix" または "NetPoint" という用語を使用している場合があります。

内容は次のとおりです。

- [対象読者](#)
- [ドキュメントのアクセシビリティについて](#)
- [関連ドキュメント](#)
- [表記規則](#)
- [サポートおよびサービス](#)

対象読者

このガイドは、Oracle Access Manager のインストールおよび設定を行う際に割り当てられる管理者、マスター ID 管理者および委任 ID 管理者を対象としています。管理者は、他の管理者およびエンド・ユーザーから使用可能な権利およびタスクを構成します。最上位レベルの管理者であるマスター管理者は、ID システムの設定時に選択されます。この管理者は、このマニュアルで説明するように、他の管理者に職責を委任します。

このマニュアルでは、LDAP ディレクトリと Web サーバーに精通していることを前提とします。

ドキュメントのアクセシビリティについて

オラクル社は、障害のあるお客様にもオラクル社の製品、サービスおよびサポート・ドキュメントを簡単にご利用いただけることを目標としています。オラクル社のドキュメントには、ユーザーが障害支援技術を使用して情報を利用できる機能が組み込まれています。HTML 形式のドキュメントで用意されており、障害のあるお客様が簡単にアクセスできるようにマークアップされています。標準規格は改善されつつあります。オラクル社はドキュメントをすべてのお客様がご利用できるように、市場をリードする他の技術ベンダーと積極的に連携して技術的な問題に対応しています。オラクル社のアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト <http://www.oracle.com/accessibility/> を参照してください。

ドキュメント内のサンプル・コードのアクセシビリティについて

スクリーン・リーダーは、ドキュメント内のサンプル・コードを正確に読めない場合があります。コード表記規則では閉じ括弧だけを行に記述する必要があります。しかし JAWS は括弧だけの行を読まない場合があります。

外部 Web サイトのドキュメントのアクセシビリティについて

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。

Oracle サポート・サービスへの TTY アクセス

アメリカ国内では、Oracle サポート・サービスへ 24 時間年中無休でテキスト電話 (TTY) アクセスが提供されています。TTY サポートについては、(800)446-2398 にお電話ください。

関連ドキュメント

詳細は、Oracle Access Manager リリース 10g (10.1.4.0.1) ドキュメント・セットの次のドキュメントを参照してください。

- 『Oracle Access Manager 概要』: Oracle Access Manager の概要、マニュアルへのロード・マップおよび用語集を提供します。
- Oracle Application Server のリリース・ノート: Oracle Access Manager の最新の更新情報はこのリリース・ノートを参照してください。リリース・ノートは、プラットフォーム固有のマニュアルに付属しています。リリース・ノートの最新バージョンは、<http://www.oracle.com/technology/documentation> の Oracle Technology Network で入手できます。
- 『Oracle Access Manager インストール・ガイド』: Oracle Access Manager コンポーネントのインストールおよび設定方法について説明します。
- 『Oracle Access Manager アップグレード・ガイド』: Oracle Access Manager の旧バージョンを最新バージョンにアップグレードする方法について説明します。
- 『Oracle Access Manager アクセス管理ガイド』: ポリシー・ドメイン、認証スキームおよび認可スキームを定義してリソースを保護する方法、単一および複数ドメインのシングル・サインオンを構成してユーザーが複数のリソースに 1 回のログインでアクセスできるようにする方法およびカスタム・ログイン・フォームを設計する方法を説明します。このマニュアルでは、アクセス・システムの設定および管理方法について説明します。
- 『Oracle Access Manager ID および共通管理ガイド』: ユーザー、グループおよび組織に関する情報を表示するように ID システム・アプリケーションを構成する方法、ID システム・アプリケーションに表示されるデータを表示および変更する権限をユーザーに割り当てる方法、およびユーザーに関する基本情報の追加、ユーザーに関する追加情報の提供、新規ユーザー・エントリの承認などの ID アプリケーション機能を自動的に実行されるステップのチェーンにリンクするワークフローの構成方法について説明します。このマニュアルでは、ディレクトリ・プロファイル構成、パスワード・ポリシー構成、ロギング、監査など、ID システムおよびアクセス・システムに共通の管理機能についても説明します。
- 『Oracle Access Manager デプロイメント・ガイド』: Oracle Access Manager が実行される環境を計画および管理する人々に情報を提供します。このガイドでは、容量計画、システム・チューニング、フェイルオーバー、ロード・バランシング、キャッシングおよび移行計画について説明します。
- 『Oracle Access Manager カスタマイズ・ガイド』: Oracle Access Manager アプリケーションの外観を変更する方法、およびオペレーティング・システム、Web サーバー、ディレクトリ・サーバー、ディレクトリ・コンテンツに変更を加えるか、CGI ファイルまたは JavaScript を Oracle Access Manager 画面に接続することで、動作を制御する方法を説明します。このマニュアルでは、Access Manager API と認証および認可プラグイン API についても説明します。
- 『Oracle Access Manager 開発者ガイド』: IdentityXML と WSDL を使用して ID システム機能にプログラムでアクセスする方法、カスタム WebGate (AccessGate と呼ぶ) を作成する方法およびプラグインを開発する方法を説明します。このガイドは、Oracle Access Manager の CGI ファイルまたは JavaScript の作成時に認識しておく必要のある情報も提供します。
- 『Oracle Access Manager 統合ガイド』: BEA WebLogic、Siebel 7、IBM Websphere などのサード・パーティ製品とともに実行するように Oracle Access Manager を設定する方法を説明します。
- 『Oracle Access Manager スキーマ詳細』: スキーマに関する情報を提供します。
- また、最新の更新情報については、Oracle Application Server のリリース・ノートを参照してください。リリース・ノートは、プラットフォーム固有のマニュアルに付属しています。リリース・ノートの最新バージョンは、Oracle Technology Network (<http://www.oracle.com/technology/documentation>) で入手できます。

表記規則

このマニュアルでは次の表記規則を使用します。

規則	意味
太字	太字は、操作に関連する Graphical User Interface 要素、または本文中で定義されている用語および用語集に記載されている用語を示します。
イタリック体	イタリックは、ユーザーが特定の値を指定するプレースホルダ変数を示します。
固定幅フォント	固定幅フォントは、段落内のコマンド、URL、サンプル内のコード、画面に表示されるテキスト、または入力するテキストを示します。

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

オラクル製品サポートの購入方法、および Oracle サポート・サービスへの連絡方法の詳細は、次の URL を参照してください。

<http://www.oracle.co.jp/support/>

製品マニュアル

製品のマニュアルは、次の URL にあります。

<http://otn.oracle.co.jp/document/>

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

<http://www.oracle.co.jp/education/>

その他の情報

オラクル製品やサービスに関するその他の情報については、次の URL から参照してください。

<http://www.oracle.co.jp>

<http://otn.oracle.co.jp>

注意： ドキュメント内に記載されている URL や参照ドキュメントには、Oracle Corporation が提供する英語の情報も含まれています。日本語版の情報については、前述の URL を参照してください。

Oracle Access Manager の新機能

この項では、Oracle Access Manager 10g (10.1.4.0.1) の新機能について説明し、このマニュアル内の追加情報の参照先を示します。現在のリリースに移行するユーザーに役立つように、旧リリースからの情報も含まれています。

次の各項では、このマニュアルで扱う Oracle Access Manager の新機能について説明します。

- [製品とコンポーネントの名称変更](#)
- [グローバリゼーション](#)
- [パスワード・ポリシーとロスト・パスワード管理](#)
- [複数の検索ベースの構成](#)
- [ワークフローの構成](#)
- [監査](#)
- [ロギング](#)
- [ディレクトリ・サーバーの構成](#)
- [Active Directory](#)
- [トラブルシューティング](#)

注意： Oracle Access Manager 10g (10.1.4.0.1) の新機能の包括的なリスト、および各機能が記載されている場所については、『Oracle Access Manager 概要』の「Oracle Access Manager の新機能」の章を参照してください。

製品とコンポーネントの名称変更

元の製品名である Oblix NetPoint は、Oracle Access Manager に変更されました。ほとんどのコンポーネント名は同じままです。ただし、次の表に示すように、知っておく必要のある重要な変更がいくつかあります。

項目	旧名称	新名称
製品名	Oblix NetPoint Oracle COREid	Oracle Access Manager
製品名	Oblix SHAREid NetPoint SAML サービス	Oracle Identity Federation
製品名	OctetString Virtual Directory Engine (VDE)	Oracle Virtual Directory
製品リリース	Oracle COREid 7.0.4	Oracle Application Server 10g リリース 2 (10.1.2) の一部としても利用可能
ディレクトリ名	COREid Data Anywhere	Data Anywhere
コンポーネント名	COREid Server	Identity Server
コンポーネント名	Access Manager	Policy Manager
コンソール名	COREid システム・コンソール	ID システム・コンソール
ID システム・トランスポート・セキュリティ・プロトコル	NetPoint ID プロトコル	Oracle ID プロトコル
アクセス・システム・トランスポート・プロトコル	NetPoint Access プロトコル	Oracle Access プロトコル
管理者	NetPoint 管理者 COREid 管理者	マスター管理者
ディレクトリ・ツリー	Oblix ツリー	構成ツリー
データ	Oblix データ	構成データ
ソフトウェア開発者キット	Access Server SDK ASDK	Access Manager SDK
API	Access Server API Access API	Access Manager API
API	Access 管理 API Access Manager API	Policy Manager API
デフォルトのポリシー・ドメイン	NetPoint Identity ドメイン COREid Identity ドメイン	Identity ドメイン
デフォルトのポリシー・ドメイン	NetPoint Access Manager COREid Access Manager	Access ドメイン
デフォルトの認証スキーム	NetPoint None 認証 COREid None 認証	匿名認証
デフォルトの認証スキーム	NetPoint Basic Over LDAP COREid Basic Over LDAP	Oracle Access and Identity Basic Over LDAP

項目	旧名称	新名称
デフォルトの認証スキーム	AD Forest 用の NetPoint Basic Over LDAP AD Forest 用の COREid Basic Over LDAP	AD Forest 用の Oracle Access and Identity
アクセス・システム・サービス	AM サービス状態	Policy Manager API サポート・モード

製品またはドキュメントに残っている古い名前の参照は、すべて新しい名前を意味しているものと理解する必要があります。

グローバリゼーション

- グローバリゼーション・サポートの一貫として、一部のファイル形式は固有の .lst 形式から .xml 形式に変更されました。

Oracle Access Manager 10g リリース 3 (10.1.4) ではグローバリゼーション・プロセスが実施され、国際化されたデータおよびメッセージをユーザーの母国語で処理できるようにするマルチバイト・サポートが提供されます。

password.xml、globalparams.xml、obscoreboard、AppDBfailover.xml および AppDB.xml、ConfigDBfailover.xml および ConfigDB.xml、WebResrcDBfailover.xml (現在の WebResrcDB.xml)、snmp_agent_config_info.xml、obscoreboard_params.xml

関連項目： このマニュアルのこれらのファイル名の参照

- 検索結果表の列ヘッダー (姓名など) をクリックすると、Oracle Access Manager では、大 / 小文字を区別しないロケールベースのソート方式が使用されます。

関連項目： 1-10 ページの「[検索機能](#)」

- ID システム・コンソールでは、ブラウザのロケールが表示名に使用されている文字のロケールと異なる場合に、一部の表示名が間違っ表示されます。

関連項目： 3-16 ページの「[属性の表示タイプ](#)」

- ID アプリケーションのレポートを生成する場合は、文字を正しく表示するために、レポート・ファイルを .txt として保存し、再インポートします。

関連項目： 4-47 ページの「[レポートの表示、変更、ローカライズおよび削除](#)」

パスワード・ポリシーとロスト・パスワード管理

- パスワード・ポリシーとロスト・パスワード管理が拡張されました。

ユーザーがパスワードに指定できる最小文字数と最大文字数を構成できます。ロスト・パスワード管理では、複数のチャレンジ・レスポンスのペアの設定、複数のスタイル・シートを作成、およびユーザーのロスト・パスワード管理操作性のその他の側面の構成を行うことができます。パスワードの再設定後に、最初にリクエストされたページにユーザーをリダイレクトすることもできます。

関連項目： 7-48 ページの「[パスワード・ポリシーの管理](#)」および
7-54 ページの「[ロスト・パスワード管理](#)」

複数の検索ベースの構成

- このマニュアルには、非結合ドメインまたはレルムとも呼ばれる複数のディレクトリ検索ベースを使用するための Oracle Access Manager の構成に関する広範な情報が記載されています。

関連項目： 7-34 ページの「[複数のディレクトリ検索ベースの操作](#)」

ワークフローの構成

- このマニュアルには、動的ターゲットのワークフローの構成に関する広範な情報が記載されています。

ユーザーの作成ワークフローでユーザーをターゲットに動的に割り当てることができます。たとえば、ユーザー A が `ou=users` にログインできるようにするユーザーの作成ワークフローを定義し、ワークフローを起動して、エントリがユーザー A と同じ `ou` があると自動的に判断されるユーザー B を作成できます。この機能は、ID システムに常に存在し、ワークフローの章に明示的に記載されています。

- クイックスタート・ツールの項には、マスター管理者のみがクイックスタート・ツールを使用できることが記載されています。

関連項目： 5-20 ページの「[新規ワークフロー定義の開始](#)」、5-22 ページの「[オブジェクトの作成ワークフローの LDAP ターゲットの定義](#)」および
5-16 ページの「[クイックスタート・ツールの使用方法](#)」

監査

- Oracle Database と Microsoft SQL Server を監査できるようになりました。MySQL のサポートは、このリリースでは推奨されません。

Crystal Reports パッケージは、Oracle Access Manager パッケージでは提供されなくなりました。この製品はベンダーから入手する必要があります。

関連項目： 第 11 章「[監査](#)」

ロギング

- ロギング・パラメータに対する変更は、1 分以内に有効になります。変更を行ったサーバーを再起動する必要はありません。

関連項目： 第 10 章「[ロギング](#)」

ディレクトリ・サーバーの構成

- ディレクトリ・サーバーの SSL モードを構成する場合は、サーバー認証のみサポートされます。クライアント証明書はサポートされていません。

関連項目： 8-3 ページの「コンポーネント間のトランスポート・セキュリティ・モード」

- 「最大セッション時間」をデフォルト値の 0（最大時間なし）に設定すると、LDAP キャッシュが非常に大きくなります。推奨値は 600（10 時間）です。

関連項目： 7-22 ページの「LDAP ディレクトリ・サーバー・プロファイルの作成」

Active Directory

- samAccountNameLength パラメータにより、SamAccountName 属性値として許可されている文字数を増やすことができます。ネイティブ・モードで稼働している Active Directory 環境では、このパラメータのデフォルト値を増やすことが必要な場合があります。

関連項目： A-9 ページの「SAMAccountName の長さについて」

トラブルシューティング

- このマニュアル全体に分散していたトラブルシューティングに関する情報は、独立した付録に統合されました。

関連項目： 付録 F「Oracle Access Manager のトラブルシューティング」

- 新しいトラブルシューティング・トピックが追加されました。

関連項目： F-6 ページの「ディレクトリ・サーバー・プロファイルを保存できない」、F-3 ページの「Active Directory: メンバーを追加するとグループ・サイズが縮小する」、F-4 ページの「ディレクトリ・プロファイルに対して ADSI を有効にできない」、F-6 ページの「スタイルシートの検証に失敗する」、F-5 ページの「簡易トランスポート・セキュリティ・モードが 1 年後に期限切れになる」、F-7 ページの「JPEG 写真イメージが更新されない」、F-7 ページの「ワークフローを使用しているときに「有効化に失敗しました」エラーが発生する」、F-6 ページの「ワークフローを使用しているときに「xenroll.cab が見つかりません」エラーが発生する」

第 I 部

Oracle Access Manager 管理の概要

Oracle Access Manager での作業を開始する前に、基本的な Oracle Access Manager 管理の概念を理解することが重要です。

第 I 部では、Oracle Access Manager 管理の概要を示します。次の章があります。

- [第 1 章「管理の準備」](#)
- [第 2 章「ID システム管理者の指定」](#)

管理の準備

Oracle Access Manager を構成および管理する前に、管理者として実行するタスクをプレビューすることが役に立つ場合があります。ID システムとアクセス・システムにログインし、ユーザー・インタフェースを表示することが役に立つ場合もあります。

この章には、次のトピックを含め、Oracle Access Manager の構成および管理を開始する前に必要な情報が記載されています。

- [前提条件](#)
- [ID システムの構成および管理について](#)
- [Oracle Access Manager の使用方法の概要](#)

注意：製品名は Oracle Access Manager に変更されましたが、マニュアルや製品で、NetPoint または Oblix という名前を使用している場合があります。特にファイル名とパス名で使用されています。

前提条件

『Oracle Access Manager インストレーション・ガイド』の説明に従って、Oracle Access Manager をインストールおよび設定してください。他のマニュアルには記載されていない Oracle Access Manager の概要については、『Oracle Access Manager 概要』を参照してください。

このマニュアルでは、ID システム管理の他、一般的な構成と管理タスクに焦点を当てていません。

ID システムの構成および管理について

ID システムおよびディレクトリ・サービスのオブジェクトを使用して、個人、グループ、組織およびその他のオブジェクトに関する ID 情報を管理します。マスター管理者は、権限を他の管理者に委任して、ID システムを数 100 万人のユーザーに拡張できます。

ID システムでは、ID 情報の管理に加えて、特定のユーザー属性、グループのメンバーシップまたは組織との関連に基づいて、ユーザーの読取り、書込みおよび変更権限を管理できます。複数の権限を 1 つのワークフローにリンクできます。

たとえば、ユーザーが自己登録を行ったときに登録リクエストが承認のために適切な人物に転送され、承認されるとユーザーの ID 属性に適したすべてのリソースへのアクセス権がそのユーザーに即時かつ自動的に付与されるように、自己登録ワークフローを設定できます。

最後に、ID システムでは、ユーザー ID、グループ・メンバーシップおよび組織オブジェクトを正確に管理できます。この情報をアクセス・システムで利用して、ユーザー属性、グループ・メンバーシップまたは組織エンティティとの関連に基づいてユーザーのアクセス権限を管理できます。

ID システムのコンポーネント

ID システムは、次のコンポーネントから構成されます。

- Identity Server
- WebPass

Identity Server: ユーザー、グループ、組織などのオブジェクトに関する ID 情報を管理するスタンドアロン・サーバーまたは複数のインスタンス。Identity Server では次のアプリケーションが提供されます。

- **User Manager:** 管理者またはユーザーの場合、ユーザー ID の追加、変更および削除を実行するワークフローに参加していれば、User Manager を使用してこれらの処理を実行できます。User Manager データをアクセス・システムで利用して、ディレクトリ・プロファイルに基づいてユーザーにアクセス権限を付与できます。User Manager にはレポート機能もあります。

通常、User Manager では、エンド・ユーザーが他のユーザーの表示や自身の ID 情報の変更を行うことができます。表示可能なユーザーおよび変更可能な ID 情報は、マスター管理者が付与する権限によって決まります。

- **Group Manager:** 管理者およびユーザーによるグループの作成または削除、およびユーザーによるグループの登録または登録解除を行うことができます。必要な機能を実行するワークフローの参加者になっている必要があります。Group Manager にはレポート機能もあります。

通常、Group Manager では、エンド・ユーザーがグループの表示やグループ内のメンバーシップの登録を行うことができます。表示可能なグループおよび登録権は、マスター管理者によって付与されます。

- **Organization Manager:** 管理者またはユーザーの場合、Organization Manager を使用して、組織や、User Manager または Group Manager に属さない他のオブジェクト（床配置図や資産など）を作成および削除できます。必要な機能を実行するワークフローの参加者になっている必要があります。Organization Manager にはレポート機能もあります。

Organization Manager により、エンド・ユーザーは、床配置図などの組織エンティティを表示できます。表示可能な組織エンティティは、マスター管理者が付与する権限によって決まります。

- **ID システム・コンソール:** ID システムを管理および構成できます。システム・コンソールを使用して、管理者を作成したり、権限を割り当てて管理タスクを委任したりすることもできます。

Identity Server は、ユーザー情報をディレクトリ・サーバーに格納します。Identity Server は、Access Server が正しい情報を取得できるようにディレクトリを最新状態に保ちます。

WebPass: WebPass は、Web サーバーと Identity Server 間で情報を受け渡す Web サーバー・プラグインです。WebPass は複数の Identity Server と通信できます。

次に詳細を示します。

- [ID システムのインストールおよび設定の確認](#)
- [ID システムの構成について](#)
- [ID システムの管理について](#)

ID システムのインストールおよび設定の確認

インストールおよび設定には、次のイベントが含まれます。

- 少なくとも 1 つの Identity Server と 1 つの WebPass がインストールされて、ID システムが設定されます。
- Identity Server と WebPass 間の通信を保護するトランスポート・セキュリティ・モードが選択されます。
- Identity Server が LDAP ディレクトリ・サーバーまたは仮想ディレクトリと通信するように構成されます。

ディレクトリ・サーバー・スキーマの自動設定に関するプロンプトが表示されます。スキーマを自動的に更新しないことを選択した場合は、構成時に手動で行うようにプロンプトが表示されます。ディレクトリ・サーバー・スキーマの手動更新の方法は、このマニュアルで説明しています。

- 必要な各アプリケーションが Identity Server とともにインストールされます。

ID システムにログインしたときに、上部のナビゲーション・バーに、アプリケーションに対応する一連のタブが表示されます。これらのタブから、User Manager アプリケーション、Group Manager アプリケーションおよび Organization Manager アプリケーションの外観と機能を構成できます。

- ユーザーおよびグループ・オブジェクト・クラスの必須属性が設定されます。

その他の属性も構成されます。

- 少なくとも 1 人のマスター管理者が選択されます。

マスター管理者は、最上位レベルの管理者です。Oracle Access Manager での作業を開始するには、少なくとも 1 人の管理者を定義する必要があります。これらの管理者がシステムを構成します。マスター管理者は、マスター ID 管理者と呼ばれる下位レベルの管理者を作成します。

表 1-1 で、ID システムのインストールおよび設定を確認します。

詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

ID システムの構成について

ID システムは、1 つの管理コンソールおよび前に説明した 3 つのエンドユーザー・アプリケーションから構成されます。

- ID システム・コンソール（「User Manager 構成」、「Group Manager 構成」、「Org. Manager 構成」、「共通構成」、「システム構成」など）
- User Manager アプリケーション
- Group Manager アプリケーション
- Organization Manager アプリケーション

個人情報の変更、パスワードの再設定、他のユーザーの追加、組織情報の検索などのタスクには、ID システム・エンドユーザー・アプリケーションを使用します。この ID データは、LDAP ディレクトリにあります。ID システム・アプリケーションを構成するには、表示するディレクトリ内の属性および変更可能にする属性を把握しておく必要があります。

ディレクトリ内のデータと連動するように ID システムを構成した後で、ID システム・アプリケーション・プロファイル・ページを構成します。プロファイル・ページには、ディレクトリ・データが表示されます。たとえば、ユーザーの名前、役職、住所および電話番号を User Manager アプリケーションのプロファイル・ページに表示できます。ID ワークフローを使用して組織の効率を改善することもできます。ID ワークフローにより、ユーザーを作成してそのユーザーに電子メールやその他のアカウントを割り当てるなど、ID システム・アプリケーション関連のアクティビティを自動化できます。

最後に、ID システムを使用して、ID ワークフローを作成します。ID ワークフローは、一連のアクションおよびアクションを完了するために実行する手順の定義です。たとえば、新しい従業員を企業の各種情報システムに追加するためのワークフロー定義を作成できます。

表 1-1 に、ID システムの構成の概要を示します。

表 1-1 ID システム構成の概要

実行するタスク	説明	参照先
Organization Manager の追加の構造化オブジェクト・クラスおよびすべてのアプリケーションの補助オブジェクト・クラスの指定	<p>設定時に、User Manager、Group Manager および Organization Manager にそれぞれ 1 つの構造化オブジェクト・クラスを構成します。</p> <p>Organization Manager に対して追加の構造化オブジェクト・クラスを定義できます。たとえば、Organization Manager で資産を表示できます。</p> <p>補助オブジェクト・クラスを追加して、ID システム・アプリケーションにデータを提供することもできます。</p>	3-2 ページの「オブジェクト・クラスの概要」
属性の構成	<p>User Manager アプリケーション、Group Manager アプリケーションおよび Organization Manager アプリケーションで使用可能な属性を決定できます。</p> <p>ID システム・アプリケーション・プロファイル・ページに属性値を表示する方法に関するルールも構成できます。たとえば、従業員がリストから部門名を選択できるようにすることが必要な場合があります。</p>	3-11 ページの「オブジェクト・クラス属性の概要」
ユーザー、グループおよび組織のアプリケーション・タブの構成	<p>User Manager では、「ID」タブに表示される内容を構成します。</p> <p>Group Manager では、「グループ」タブに表示される内容を構成します。</p> <p>Organization Manager では、「ロケーション」タブに表示される内容と、オプションで追加のタブを構成します。</p>	4-3 ページの「タブ構成情報の表示と変更」

表 1-1 ID システム構成の概要（続き）

実行するタスク	説明	参照先
ユーザー、グループおよび組織のプロファイル・ページの構成	<p>タブには、1 つ以上のプロファイル・ページが含まれます。プロファイル・ページには、一連のパネルが含まれます。パネルは属性の集まりです。</p> <p>たとえば、ユーザーのプロファイル・ページでは、「名前」、「写真」、「役職」などの属性の値を表示するように ID パネルを定義できます。</p>	4-11 ページの「 タブのプロファイル・ページおよびパネルの構成 」
検索ベースの設定	<p>検索ベースは、ディレクトリ・ツリー内の検索のエントリ・ポイントを決定します。</p>	4-22 ページの「 検索ベースの概要 」
属性の表示および変更権限の構成	<p>誰が何を検索ベースのどのポイントでどのフィルタを使用して検索できるかを決定する必要があります。</p> <p>これらの決定は、誰がデータを読み取りまたは書き込みでき、属性が変更されたときに誰が電子メール通知を受け取るかに影響します。</p>	4-21 ページの「 ユーザーによる LDAP データの表示および変更の許可 」
ワークフローの定義	<p>ワークフローは、ID システムの属性を作成、削除および変更するための一連の手順です。</p> <p>たとえば、User Manager では、組織の複数の人物からの新規ユーザーに関する情報の収集を含むユーザー作成のワークフローを定義できます。</p>	第 5 章「 ID 機能とワークフローの連携 」
パスワード・ポリシーの構成	<p>パスワードの長さやパスワード変更の頻度などを決定できます。</p>	7-47 ページの「 パスワード・ポリシーの構成 」
委任管理	<p>インストールを拡張するには、それぞれユーザーのサブセットを監督する複数の管理者が必要です。</p>	第 2 章「 ID システム管理者の指定 」

ID システムの管理について

サーバーを追加し、ID システム管理者のネットワークを拡張することにより、ID システムを拡張できます。監査とログを構成し、その他の管理機能を実行できます。表 1-2 に、ID システムの管理の概要を示します。

表 1-2 ID システムの詳細情報の参照先

実行するタスク	参照先
Identity Server の追加	『Oracle Access Manager インストール・ガイド』。このプロセスを簡単にするために、『Oracle Access Manager インストール・ガイド』の説明に従って、サイレント・インストールまたはクローニングを通じて Identity Server を追加することを選択できます。
WebPass の追加	『Oracle Access Manager インストール・ガイド』。このプロセスを簡単にするために、インストール・マニュアルの説明に従って、サイレント・インストールまたはクローニングを通じて WebPass を追加することを選択できます。
その他の ID システム・コンポーネントの追加	『Oracle Access Manager インストール・ガイド』に、ほとんどのコンポーネントのインストール方法が説明されています。Access Manager SDK のインストール方法は、『Oracle Access Manager 開発者ガイド』に記載されています。
Organization Manager のコンテナ制限の構成	4-52 ページの「 Organization Manager でのコンテナ制限の設定 」。

Oracle Access Manager の使用方法の概要

Oracle Access Manager ユーザー・インタフェースでよく使用される機能は次のとおりです。

- [ログイン](#)
- [ページ上の機能領域](#)
- [セレクト](#)
- [オンライン・ヘルプ](#)
- [「バージョン情報」ページ・リンク](#)
- [ログアウト](#)

ログイン

Oracle Access Manager では、割り当てられているロールに基づいてログインします。[第 2 章「ID システム管理者の指定」](#)で説明するように、ユーザーに対して次のロールを指定できます。

- **エンドユーザー**: エンドユーザーは、個々の属性に設定されているアクセス権限に応じて、検索の実行、プロファイル・データの表示およびプロファイル・データの変更を行うことができます。
- **委任アクセス管理者**: 委任管理者は、エンドユーザーと同じタスクをすべて実行でき、付与されている権限のレベルに応じてユーザー・オブジェクト、グループ・オブジェクトおよび組織オブジェクトを作成できるユーザーです。委任管理者は、リクエストも表示できません。
- **委任 ID 管理者**: 委任 ID 管理者は、User Manager アプリケーション、Group Manager アプリケーションおよび Organization Manager アプリケーションの構成タブを表示する権限を委任されたユーザーです。この人物は、属性アクセス制御の設定やワークフローの定義などを行うことができます。
- **ID 管理者**: ID 管理者は、User Manager アプリケーション、Group Manager アプリケーションおよび Organization Manager アプリケーションを表示でき、ID システム・コンソールの ID システム構成機能を使用できます。

たとえば、ID 管理者としてログインした場合は、すべてのアプリケーションのすべての画面を表示できます。しかし、エンドユーザーとしてログインした場合は、User Manager アプリケーション、Group Manager アプリケーションおよび Organization Manager アプリケーションのサブセットのみ表示でき、ID システム管理機能にはアクセスできません。

デフォルトでは、ID システムとアクセス・システムの間にはシングル・サインオンが構成されません。一方のシステムにログインした場合は、もう一方のシステムへのログインが要求されません。

アクセス・システムを使用して ID システム・アプリケーションを保護する場合は、デフォルトのログイン形式を使用しないで、独自のカスタム形式を実装できます。ポリシー・ドメインでのリソースの保護の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

ID システムへのログイン

ID システムへのログインの手順は、ログイン画面をカスタマイズしたかどうか、Portal Inserts として使用可能にしたかどうか、またはアクセス・システムで保護したかどうかによって決まります。

この項では、ID システムに付属のデフォルトのログイン画面と、デフォルトのユーザー・タイプがログインに与える影響を説明します。カスタマイズの詳細は、『Oracle Access Manager カスタマイズ・ガイド』および『Oracle Access Manager 開発者ガイド』を参照してください。

ユーザーが ID システムにログインする前に、セマンティック型のログインで属性を構成する必要があります。この属性は、インストール時に自動的に構成するか、ID システム・コンソールから手動で構成できます。詳細は、第 3 章「ID システムでのスキーマ・データの使用」を参照してください。

注意： マスター ID 管理者および委任 ID 管理者のみが ID システム・コンソールにアクセスできます。これらの管理者の構成の詳細は、第 2 章「ID システム管理者の指定」を参照してください。

ID システムへのログインの手順

1. ブラウザで、ID システムへのパスを入力し、[Enter] を押します。

例：

```
https://hostname:port/identity/oblix
```

hostname は、WebPass がインストールされているコンピュータの名前で、*port* は、WebPass 用の Web サーバー・ポートです。HTTP または HTTPS プロトコルを使用してログインできます。

製品のメイン・ページが表示されます。このページには、User Manager、Group Manager、Org Manager などの 1 つ以上のアプリケーションへのリンクがあります。

このデフォルトの変更の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

2. 必要なアプリケーションを選択します。
ログイン・ページが表示されます。
3. ユーザー名とパスワードを入力します。

Active Directory ユーザーの場合、「ドメイン」フィールドが表示されたら、ID システムのインストール環境が動作するドメインを選択します。

デフォルトでは、ID システムにログインしたときに、ID システム管理者が使用できる機能がすべて表示されます。たとえば、User Manager では、「ID」、「レポート」などの機能、および検索機能が表示されます。

アクセス・システムへのログイン

デフォルトでは、ユーザーが ID システムにすでにログインしている場合、アクセス・システムにログインする必要はありません。また、アクセス・システムにログインしている場合は、ID システムにログインする必要はありません。セッション情報は、ObTEMC Cookie という Cookie に格納されます。ポリシー・ドメインで ID システム・アプリケーションを保護することを選択でき、その場合は別の認証を使用できます。ポリシー・ドメインでのリソースの保護の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

ユーザーがアクセス・システムにログインする前に、セマンティック型のログインで属性を構成する必要があります。この属性は、インストール時に自動的に構成するか、ID システム・コンソールから手動で構成できます。詳細は、第 3 章「ID システムでのスキーマ・データの使用」を参照してください。

この項では、アクセス・システムに付属のデフォルトのログイン画面について説明します。

注意： マスター管理者およびマスター・アクセス管理者のみがアクセス・システム・コンソールにアクセスできます。マスター・アクセス管理者の構成の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

アクセス・システムへのログインの手順

1. ブラウザで、アクセス・システムへのパスを入力し、[Enter] を押します。

例: `https://hostname:port/access/oblix`

hostname は、Policy Manager がインストールされているコンピュータの名前で、*port* は、Policy Manager 用の Web サーバー・ポートです。HTTP または HTTPS プロトコルを使用してログインできます。

製品のメイン・ページが表示されます。このページには、ID システム、Policy Manager、アクセス・システム・コンソールなどの 1 つ以上のアプリケーションへのリンクがあります。

2. 必要なアプリケーションを選択します。

Policy Manager: 委任アクセス管理者のみがポリシー・ドメインを参照できます。Policy Manager での管理の委任の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

アクセス・システム・コンソール: マスター管理者とマスター・アクセス管理者のみが、その機能にアクセスできます。マスター・アクセス管理者の構成の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

3. ログイン・ページが表示されます。

ページ上の機能領域

次に、ID システム・ページの主要コンポーネントを示します。

ナビゲーション要素

次に、「ID システム・コンソール」ページの一部を示します。このページは、ID システムのランディング・ページにアクセスし、そのページの「ID システム・コンソール」リンクをクリックしてから「User Manager 構成」サブタブをクリックしたときに表示されます。

The screenshot shows the Oracle Identity Administration console interface. At the top, there is a navigation bar with tabs for 'User Manager', 'Group Manager', and 'Org. Manager', and a link for 'Identity System Console'. Below this, a breadcrumb trail indicates the current path: 'システム構成 | User Manager 構成 | Group Manager 構成 | Org Manager 構成 | 共通構成'. The main content area is titled 'User Manager 構成' and contains a table with the following information:

機能	説明
タブの構成	User Managerでユーザー・プロファイル情報の格納および表示に使用される機能区分を変更および管理します。
レポートの構成	レポートを作成、公開、変更および削除します。
監査ポリシーの構成	User Managerの監査ポリシーを指定します。

各機能の詳細は、「ヘルプ」をクリックしてください。

すべてのページには、次の機能領域があります。

- **アプリケーション・タブ**: ID システム・アプリケーション (User Manager、Group Manager、Organization Manager (ユーザー・インターフェースでは Org. と省略) および ID システム・コンソール) を表示する一連のタブです。
- **アプリケーション・サブタブ**: ID システム・アプリケーションの主要機能を表示する一連のタブです。たとえば、ID システム・コンソールには、「システム構成」、「User Manager 構成」、「Group Manager 構成」および「共通構成」のモジュールがあります。
- **「ヘルプ」、「バージョン情報」および「ログアウト」リンク**: これらのリンクは、ページの上部に表示されます。
- **左側のナビゲーション・ペイン**: ID システム・コンソールでは、左側のナビゲーション・ペインを使用します。このペインには、選択されたタブまたはサブタブに適用される機能へのリンクのリストが含まれます。ユーザー・アプリケーションでは、左側のナビゲーション・ペインのかわりにサブタブとパネルを使用します。
- **本体**: 本体には、現在選択している機能または入力するフィールドの説明が表示されます。

検索機能

ユーザー・インタフェースには、ユーザーまたはグループを検索するための検索フィールドがあります。これらの検索フィールドは、ほとんどの ID アプリケーション・ページに表示されます。使用可能なフィールド数および検索できる項目は、管理者が検索機能をどのように構成したかによって決まります。

ユーザーまたはグループを問い合わせるには、検索基準を入力し、「実行」をクリックします。オプションとして、「レポート」タブをクリックし、「レポートの生成」を選択して、問合せの結果を格納できます。検索結果表の列ヘッダー（姓名など）をクリックすると、Oracle Access Manager では、大 / 小文字を区別しないロケールベースのソート方式が使用されます。



検索機能の使用手順

1. 検索基準を入力します。

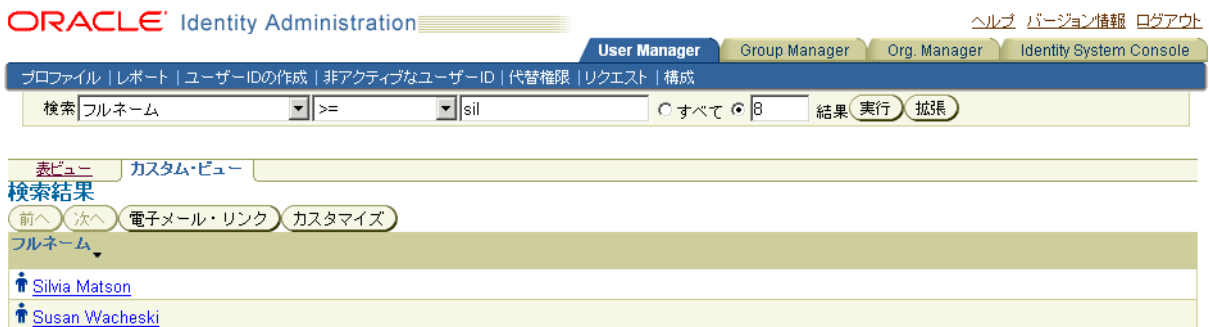
最も単純な検索方法としては、「検索」入力フィールドにテキスト文字列を入力します。

デフォルトでは、最小文字数を入力する必要はありません。ただし、ユーザーが検索基準を絞り込めるように、oblixadminparams.xml で searchStringMinimumLength パラメータを設定して、検索フィールドに入力する必要のある最小文字数を制御できます。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

2. 「実行」をクリックします。

検索基準に一致するユーザーまたはグループが画面に表示されます。

デフォルトでは、1 ページに 8 個の結果が表示されます。これは、セレクタとクエリー・ビルダーの両方に適用されます。検索や問合せの結果が 20 ヒットを超えると、切り捨てられた結果が戻されます。この検索上限の変更方法は、『Oracle Access Manager カスタマイズ・ガイド』の cookieBustLimit パラメータの説明を参照してください。



3. 検索結果で、ユーザーまたはグループのリンクをクリックして選択します。

注意：「完了」をクリックしたときに「不正なリクエスト」メッセージが表示された場合は、検索文字列がブラウザにとって長すぎます。ブラウザは、検索パラメータを URL として扱い、検索が最大 URL 長を超えた場合にエラーを生成します。

4. 検索結果で、列ヘッダーをクリックしてリストをソートします。

注意：Oracle Access Manager では、大 / 小文字を区別しないロケールベースのソート方式が使用されます。

セレクトタ

セレクトタは、検索機能および検索の結果を集計する機能を提供します。たとえば、グループを作成する場合は、「Group Manager」タブをクリックし、「グループの作成」サブタブをクリックすると、選択ボタンのあるページが表示されます。

選択ボタン（この例では「メンバーの選択」）をクリックすると、セレクトタが表示されます。

セレクトタのランディング・ページは、「完了」ボタン、「取消」ボタンおよび空の選択済項目リストが表示された空白の検索ページです。このページで検索機能を使用する場合は、セレクトタを使用して、取得した項目を「選択」リストに移動できます。

名前	フルネーム
追加	Silvia Matson
追加	Skipper McQuaig
追加	Susan Wacheski

オンライン・ヘルプ

「ヘルプ」リンクは、ID システム画面の右上、およびアクセス・システム画面のサイド・ナビゲーション・バーにあります。オンライン・ヘルプにアクセスするには、このリンクをクリックします。

オンライン・ヘルプ・ウィンドウで、次のタスクを実行できます。

- スクロールしてヘルプ・トピック全体を表示します。
- 「目次」をクリックしてトピックのリストを表示します。
- 「戻る」または「進む」をクリックして他のヘルプ・トピックを表示します。
- 「終了」をクリックしてウィンドウを閉じます。

「バージョン情報」ページ・リンク

「バージョン情報」ページへのリンクは、ID システム・ページとアクセス・システム・ページの右上にあります。「バージョン情報」リンクをクリックすると、オラクル社の住所、電話番号およびその他の連絡先情報と、著作権情報が表示されます。

「システム情報の表示」ボタンでは、サーバーのプラットフォームとバージョン、および Oracle に関する連絡先情報が表示されます。

ログアウト

「ログアウト」リンクは、ID システム・ページとアクセス・システム・ページの上部にあります。デフォルトでは、ID システムからログアウトすると、アクセス・システムからも自動的にログアウトします。また、アクセス・システムからログアウトすると、ID システムからも自動的にログアウトします。

Oracle Access Manager の使用が終了したら、権限を持たない人々が情報にアクセスすることを防ぐために、ログアウトしてブラウザを閉じる必要があります。

デフォルトでは、セッションは3時間後に期限切れになります。タイムアウトを変更するには、7-11 ページの「セッション・タイムアウトの構成」で詳細を参照してください。

注意：Firefox では、ログアウト後にブラウザ・ウィンドウを手動で閉じることをユーザーに求めるプロンプトが表示されます。

ログアウトの手順

1. ページの右上隅にある「ログアウト」をクリックします。
2. ブラウザを閉じるよう求めるプロンプトが表示されたら、「OK」をクリックします。

ID システム管理者の指定

この章では、ID システム管理者の指定方法を説明します。

この章の内容は次のとおりです。

- ID システム管理者について
- 管理者の指定
- 管理の委任

ID システム管理者について

『Oracle Access Manager 概要』に説明されているように、ID システムはユーザー、グループおよび組織 ID 情報を管理します。

ID システムの管理には、データの管理、パフォーマンスの向上および ID システム・アプリケーションの外観と機能の制御に役立つように設計された様々なタスクが関係します。これらのタスクの詳細は、[第 7 章「グローバル設定の構成」](#)を参照してください。

ID システムの管理の職責は、マスター管理者とマスター ID 管理者で分担します。

マスター管理者: 製品の設定時に少なくとも 1 人のマスター管理者が指定されます。マスター管理者は、最上位レベルの管理者です。この管理者は、他のマスター管理者およびマスター ID 管理者を指定できます。

マスター ID 管理者: マスター ID 管理者は、委任 ID 管理者と呼ばれる管理者に特定の職責を委任できます。

委任 ID 管理者: 委任 ID 管理者は、マスター ID 管理者によって割り当てられ、User Manager で作成されます。

ID システム管理者のタイプおよびその権限の説明は、[表 2-1](#) を参照してください。

表 2-1 ID システム管理者のタイプ

管理者	管理者の指定	実行するタスク
マスター管理者	Oracle Access Manager のインストール時に割り当てられます。	<ul style="list-style-type: none"> ■ 他のマスター管理者およびマスター ID 管理者の割当て ■ マスター ID 管理者としての自身の割当て ■ ID システム・コンソールのすべてのシステム構成およびシステム管理機能の管理 ■ Identity Server の構成 ■ 管理者の指定 ■ スタイルの構成 ■ ディレクトリ・サーバー・プロファイルの構成 ■ WebPass の構成 ■ パスワード・ポリシーの構成 ■ Identity Server 設定の管理 ■ 写真のインポート ■ ログ・ファイルおよび監査ファイルの管理

表 2-1 ID システム管理者のタイプ (続き)

管理者	管理者の指定	実行するタスク
マスター ID 管理者	マスター管理者によって割り当てられます。	<ul style="list-style-type: none"> ■ 委任 ID 管理者の割当て ■ 3つの ID システム・アプリケーション (User Manager、Group Manager および Organization Manager) すべての管理 ■ ID システム・コンソールの共通構成およびアプリケーション固有の構成の管理 ■ 共通構成タスク： <ul style="list-style-type: none"> オブジェクト・クラスの構成 ワークフロー・パネルの構成 マスター監査ポリシーの構成 ロギングと監査ポリシーの構成 ■ User Manager 構成タスク： <ul style="list-style-type: none"> タブの構成 レポートの構成 ロギングと監査ポリシーの構成 ■ Group Manager 構成タスク： <ul style="list-style-type: none"> タブの構成 レポートの構成 グループ・タイプの構成 Group Manager オプションの構成 ロギングと監査ポリシーの構成 グループ・キャッシュの管理 ■ Organization Manager 構成タスク： <ul style="list-style-type: none"> タブの構成 レポートの構成 ロギングと監査ポリシーの構成
委任 ID 管理者	マスター ID 管理者によって割り当てられます。	<ul style="list-style-type: none"> ■ 他の委任 ID 管理者の割当て ■ 割り当てられたタスクの管理 ■ 管理の委任 ■ 属性アクセス制御の構成 ■ ワークフローの定義 ■ ワークフロー・ステータスのモニター ■ 検索ベースの設定 ■ 動的グループの拡張 ■ コンテナ制限の設定

管理者の指定

ID システム・コンソールを使用して、委任 ID 管理者およびマスター ID 管理者を割り当てます。前に述べたように、このタスクを実行するにはマスター管理者になっている必要があります。

マスター管理者およびマスター ID 管理者を指定する手順

1. ID システムにマスター管理者としてログインし、ID システムのランディング・ページで、「ID システム・コンソール」リンクをクリックします。
すでにログインしている場合は、「ID システム・コンソール」タブをクリックします。
2. 「システム構成」サブタブをクリックします。
「システム構成」ページが表示されます。
3. 左側のナビゲーション・ペインで「管理者」をクリックします。
「管理者の構成」ページが表示され、「マスター ID 管理者」と「マスター管理者」の 2 つのオプションが表示されます。
各タイプの管理者が実行するタスクのリストは、表 2-1 を参照してください。
4. 追加する管理者のカテゴリをクリックします。
「*type_of_administrator* の変更」ページが表示されます。
type_of_administrator は、マスター管理者またはマスター ID 管理者です。
5. 「ユーザーの選択」をクリックして管理者を追加します。
この機能の使用方法は、1-11 ページの「セレクトタ」を参照してください。
6. ユーザーを選択し、「追加」をクリックします。
「セレクトタ」ページで選択した名前が、「*type of administrator* の変更」ページに表示されます。*type of administrator* は、マスター管理者またはマスター ID 管理者です。複数の管理者を指定できます。
7. 「完了」をクリックして「セレクトタ」ページを終了します。
8. 「保存」をクリックして管理者を追加します。

管理者の削除

管理者を削除すると、ユーザーから管理権限が削除されますが、ユーザーが LDAP ディレクトリから削除されたり非アクティブ化されたりすることはありません。

管理者の削除の手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックします。
2. 「管理者」をクリックします。
3. 「管理者の構成」ページで、削除する管理者のタイプのリンクをクリックします。
「*type of administrator* の変更」ページが表示されます。*type of administrator* は、マスター管理者またはマスター ID 管理者です。
「ユーザーの選択」をクリックします。
4. 削除する管理者の横の「削除」ボタンの選択を解除します。
5. 「完了」をクリックして削除を確認します。

管理の委任

権限および職責を他の管理者に委任できます。委任されたタスクは、委任された権限、ターゲットおよびツリー・パスに固有です。

この項の内容は次のとおりです。

- [管理の委任について](#)
- [委任管理モデル](#)
- [委任管理者の追加](#)
- [代替管理者の追加](#)

管理の委任について

管理を委任すると、マスター管理者およびマスター ID 管理者は、よりローカルな他の管理者に職責を委任できます。この機能は、数千人または数百万人のユーザーを管理する必要のある大規模組織で特に役立ちます。

管理を委任する場合は、別のユーザーに付与する権限を決定します。権限には、次の項目を構成する能力が含まれます。

- 属性の読取りアクセス権
- 属性の書込みアクセス権
- 属性変更の電子メールによる通知
- 検索ベースの設定
- リクエストのモニタリング
- ワークフローの定義
- 包含制限

また、自分の代替として行動する人物を指定できます。代替権限を付与されている人々は、自分が代替となる人が実行を許可されている機能を一時的に実行できます。

別のユーザーに権限を委任すると、そのユーザーが委任 ID 管理者になります。管理を委任することにより、誰がどの機能をどのレベルでどのフィルタを使用して構成またはアクセスできるかを決定します。構成またはアクセス権限は、特定のユーザー、ユーザーのグループ、ロールまたはルールに対するものになります。構成またはアクセスできるリソースには、検索ベース、属性アクセス制御、ワークフロー定義などがあります。レベルは開始 DN です。

タスクの概要：管理者の委任

1. 必要なアプリケーションの委任手順を開始します。

注意： ここに示すすべてのアクティビティは、2-8 ページの「[委任管理者の追加](#)」で説明されています。

2. 付与する権限を選択します（読取り、書込みおよび通知権限の場合のみ）。
3. 権限に関連付けられている属性を識別します。
4. 属性のアクセス制御のレベルを指定します。これにより、権限が適用されるディレクトリ・ツリーの有効範囲を設定します。
5. 権限を委任する人を選択します。

たとえば、マスター ID 管理者として、「役職」属性の読取りアクセス制御を設定する能力を 1 人以上のユーザーに付与できます。委任 ID 管理者がアクセス制御を他のユーザーに委任できるようにするかどうかを指定できます。

詳細は、2-8 ページの「委任管理者の追加」を参照してください。

委任管理モデル

ID システムでは、様々なビジネス・モデルを表すディレクトリ・ツリー構造のアクセス制御の設定および管理の委任を行うことができます。これらのモデルには、エクストラネット・モデル、イントラネット・モデルおよび ASP モデルが含まれます。これらのモデルについて、次の各項で説明します。

- [エクストラネット・モデル](#)
- [イントラネット・モデル](#)
- [ASP モデル](#)

エクストラネット・モデル

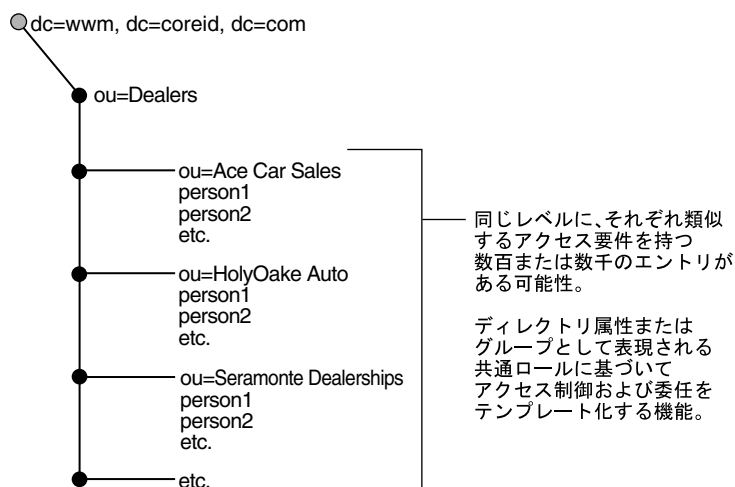
典型的な企業間エクストラネットには、1つのサイトを使用する500以上のエクストラネット組織がある場合があります。これらの組織は、顧客、パートナーおよびサプライヤを表し、それぞれに1～100人のユーザーがいます。

エクストラネット・モデルの目標は、マスター ID 管理者が管理職責を各パートナーに渡すことです。しかし、パートナーの数が非常に多いため、パートナーが参加するたびに新しいロールおよび職責を定義することが負担になります。したがって、ディレクトリ管理者は、既存および新規のすべての顧客に利用できるロールおよび職責の固定セットを定義する必要があります。その後でマスター ID 管理者は、アクセス制御を定義し、すべての組織で対称的な委任管理者ポリシーを作成できます。

各パートナー・サイトの委任 ID 管理者は、通常、ユーザーの作成や属性アクセス権限の変更など、適切に定義されたタスクと権限の固定セットを持つ基幹業務の人物です。委任 ID 管理者は、定義済ロールのセットに人々を追加および削除することで、自身の組織内でのみ管理権限を他の人に付与できます。

たとえば、委任 ID 管理者は、`admin=yes` の属性で新規ユーザーを作成します。図 2-1 に示すように、この新規ユーザーは、属性アクセス制御権限の変更、新規ユーザーの作成およびその他の適切に定義されたタスクを行う能力を継承します。

図 2-1 エクストラネット委任管理の例



イントラネット・モデル

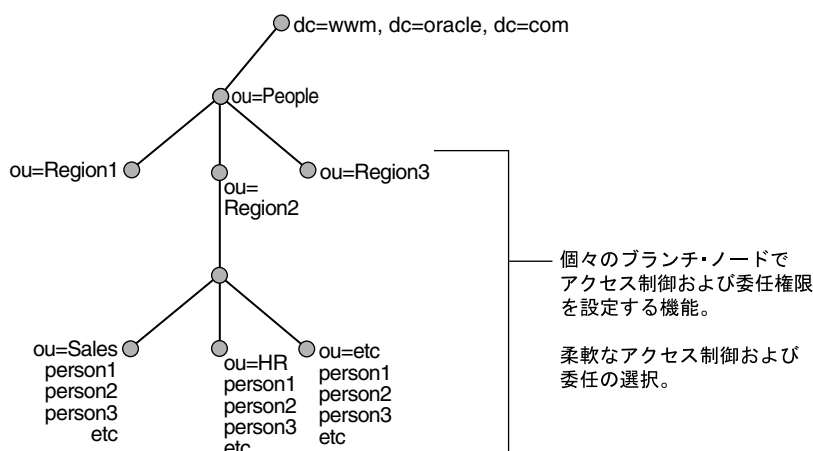
典型的なイントラネット・モデルでは、ディレクトリ・ツリーは一般に地域（北米とヨーロッパ）や職能（マーケティングとエンジニアリング）などのユーザーの論理的な区分に従って編成されます。

ディレクトリは、各 OU に少数のブランチがあるのが特徴ですが、いくつかのレイヤーは深く分岐することがあります。ブランチは、それぞれ非常に異なる場合があります。各ブランチには数千人のユーザーがいる場合があります。特定のノードで、ヨーロッパ・ブランチの販売およびマーケティングに 500 人のユーザーがいて、北米ブランチの東部、中部および西部に 10,000 人のユーザーがいる場合があります。

マスター ID 管理者は、技術的知識およびビジネス・プロセスの知識が存在する場所に応じて、管理を集中的に委任するか OU レベルで委任するかを選択できます。または、マスター ID 管理者は、特定のタスクについて管理を委任することも選択できます。たとえば、電話番号のプロビジョニングのタスクを委任し、アクセス権限の管理または新規ユーザーの作成は委任しないことができます。

図 2-2 に、イントラネット・モデルを示します。

図 2-2 イン트라ネット委任管理モード



ASP モデル

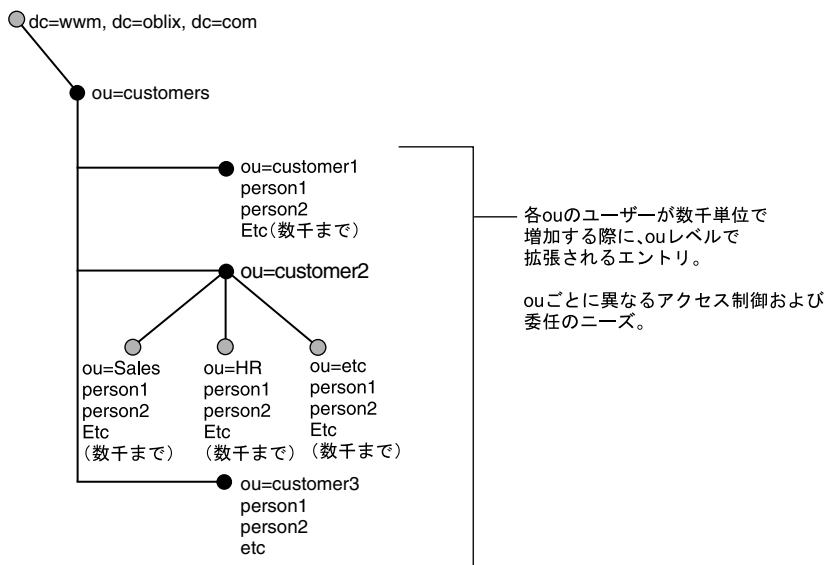
一部の企業間エクストラネット・サイトが従うモデルは、前に説明したエクストラネット・モデルよりもアプリケーション・サービス・プロバイダ（ASP）モデルに近い場合があります。

ASP モデルでは、エクストラネット・パートナーの数は少なくなります。各パートナー・サイトのユーザー数は非常に多くなります。たとえば、パートナーの数は約 50 で、各パートナーに 1,000 人のユーザーがいる場合があります。

ASP は、ホストされたサービスを提供します。異なる顧客が異なるサービス・セットを必要とする場合があります。このため、アクセス権など、管理する必要のあるデータの有効範囲は、OU ごとに異なる場合があります。さらに、各 OU のディレクトリ構造が大幅に異なる場合があります。各 OU では、イントラネット・モデルと同様にイントラネット・ディレクトリの複雑さがすべて存在し、ツリーの構造は顧客 1 の OU と顧客 2 の OU とでまったく異なる場合があります。

ASP モデルには、イントラネット・モデルと同様の柔軟な委任モデルが必要です。ASP サイトのマスター ID 管理者は、検索ベースの設定などの一部の上位レベル構成を実行し、エクストラネット・モデルと同様の初期委任モデルを構成します。ただし、各顧客サイトには、顧客サイトの技術的な委任 ID 管理者または ASP サイトのマスター ID 管理者がカスタマイズした委任管理モデルを作成するための柔軟性が必要です。

図 2-3 ASP 委任管理モデル



委任管理者の追加

管理を委任すると、マスター ID 管理者または委任 ID 管理者は、職責を他のローカルな管理者にさらに委任できます。

管理の委任の手順

1. ID システムにログインし、ランディング・ページで、「User Manager」、「Group Manager」または「Organization Manager」のリンクを選択します。
すでにログインしている場合は、アプリケーションのタブを選択します。
2. 「構成」サブタブをクリックします。
「構成」ページが表示されます。
3. 「委任管理」リンクをクリックします。
一部のブラウザでは、アプリケーションの証明書を信頼するかどうかを尋ねるプロンプトが表示されることがあります。このプロンプトが表示された場合は、「常に信頼」オプションを選択してください。
「管理の委任」ページが表示されます。
4. 「管理ドメイン」ボックスで、この権限が適用される DIT の有効範囲を指定します。
最初は、このフィールドには設定時に定義した検索ベースが表示されます。検索ベースは、通常は最上位（企業全体）レベルで定義されます。委任された権限のレベルに応じて、最下位レベル（個々のユーザー）から中間レベル（部門、課、パートナ）を経て最上位レベル（企業全体）まで、任意のレベルでアクセス制御を指定できます。たとえば、「フルネーム」属性を選択し、販売などの部門を選択した場合は、販売部門に属するすべてのフルネームに適用されるアクセス制御を設定することになります。
選択は、「管理ドメイン」ボックスの下のフィールドに表示されます。
5. オプションで、「フィルタ」フィールドを使用して変数置換または LDAP ルールを指定し、選択した DIT レベルをフィルタ処理できます。
詳細は、3-25 ページの「[ルールとフィルタの使用方法](#)」を参照してください。

6. オプションで、「フィルタの追加」フィールドに別のフィルタを入力し、「保存」をクリックします。
新規フィルタが、前のフィルタの下のフィールドに表示されます。
7. 「権限の付与」リストで、委任管理者に付与する権限を選択します。
 - **読取り**: 選択した属性の読取り（表示）権限の設定が許可されます。
 - **変更**: この属性の変更権限の設定が許可されます。
 - **通知**: ユーザーが属性値の変更をリクエストした場合の通知権限の設定が許可されません。
 - **検索ベースの設定**: 検索ベースの指定が許可されます。
 - **リクエストのモニター**: リクエストのモニターおよび非アクティブなユーザーの管理が許可されます。
 - **ワークフローの定義**: ワークフローの定義が許可されます。
 - **代替権限**: 他の人々を自分の代替として指定できます。
8. 新しい管理者に、この権限を他の管理者にさらに委任する権限を付与するには、「権限の委任」チェック・ボックスを選択します。

注意: 委任を選択しても、権限付与権限は自動的に割り当てられません。委任権限と権限付与権限は別々に定義する必要があります。

9. 「属性」ボックスで、権限に関連付ける属性を選択します。
10. 次の1つ以上の方法で1つ以上の権限を割り当てる受託者を選択します。
 - **ルール**: 「フィルタの作成」をクリックし、クエリー・ビルダーを使用してルールを作成します。詳細は、4-27 ページの「クエリー・ビルダーを使用した LDAP フィルタの記述」を参照してください。
 - **人**: 「ユーザーの選択」をクリックし、セレクトアを使用して1人以上のユーザーを指定します。
 - **グループ**: 「グループの選択」をクリックし、セレクトアを使用して1つ以上のグループを指定します。
「ルール」、「人」、「グループ」の各フィールドにはリレーションシップがあります。これらのフィールドのいずれかで指定されたユーザーに権限が割り当てられます。
11. 「コピー」および「貼付け」ボタンを使用して、ある属性から別の属性にユーザーおよびグループをコピーします。
「コピー」、「リセット」の順にクリックし、別の属性を選択して「貼付け」をクリックします。ユーザーとグループが、対応する個々のボックスに表示されます。
12. 次のいずれかのボタンをクリックします。
 - **保存**: 変更を保存し、実装します。
 - **リセット**: すべての選択を消去します。
 - **削除**: すべてのルール、グループおよびユーザー指定を消去します。
 - **レポート**: すべての属性のレポートおよびドメインでのそれらのアクセス権を生成します。

代替管理者の追加

ID システム管理者として、代替権限を付与した場合は、自身の権限を一時的に取得する他の人を指定できます。代替ユーザーは、ID システムにログインした後で、自分が代替する人の ID を取得できます。代替ユーザーが「ID」ページを表示すると、その人の情報ではなく代替する人物の情報が表示されます。

代替権限を割り当てることで、自分の ID を他の人が一時的に取得することができます。たとえば、自分が委任 ID 管理者であるとします。休暇に入る前に、代替権限を J. Smith に割り当てます。J. Smith は、ログイン時に委任 ID 管理者の ID を取得します。後で J. Smith は、自分の仕事をすると、委任された権限を元に戻します。ID を取得している間は代替ユーザーが委任 ID 管理者のように見えますが、ID システムは代替ユーザーの ID と委任 ID 管理者の ID の両方のアクティビティをすべてログに記録します。すべてのログおよびアラームには、両方の ID を使用して重複エントリが表示されます。

代替の割当てまたは削除の手順

1. ID システムのランディング・ページで、ログインし、「User Manager」のリンクを選択します。
すでにログインしている場合は、「User Manager」タブをクリックします。
2. 「代替権限」リンクをクリックします。
代替権限ページが表示されます。
代替権限を付与されている場合は、このページに「ユーザーの選択」ボタンが表示されません。自分の代替とする人を指定した場合は、指定した人々が「代替」フィールドにリストされます。このページには、自分を代替として指定した人々のリストを表示する代替フィールドもあります。リストに誰も表示されていない場合は、誰からも代替として指定されていません。
3. 代替権限を付与していると想定して、「ユーザーの選択」をクリックします。
「セレクト」ページが表示されます。詳細は、1-11 ページの「セレクト」を参照してください。
4. ユーザーを選択し、「追加」をクリックします。
ユーザーが「選択」リストに追加されます。
5. ユーザーを選択し、「削除」をクリックしてユーザーを削除します。
ユーザーが「選択」リストから削除されます。
6. 「完了」をクリックして「セレクト」ページを終了します。
7. 「保存」をクリックして変更を保存します。

ID を取得する手順

1. ID システムのランディング・ページで、ログインし、「User Manager」のリンクを選択します。
すでにログインしている場合は、「User Manager」タブをクリックします。
2. 「代替権限」をクリックします。
3. このページの「ユーザーの代替」セクションで、権限を取得するユーザーを選択します。
自分がこのユーザーから代替としてすでに割り当てられている必要があります。
4. 「権限の取得」を選択し、「保存」をクリックします。

自身の ID を回復する手順

1. 「User Manager」から、「代替権限」を選択します。
2. 「元に戻す」を選択します。

ID システム・アプリケーションのスタイルの構成、ID システムの複数言語の構成、Identity Server および WebPass の構成と管理、および ID システムのパスワード・ポリシーと Access Manager SDK の構成の詳細は、[第 7 章「グローバル設定の構成」](#)を参照してください。

第 II 部

ID システムの構成

Oracle Access Manager の ID システムを使用すると、ユーザー・データの管理、ID アプリケーション (User Manager、Group Manager および Organization Manager) の構成、ワークフローの定義、および外部アプリケーションへの非 LDAP データの送信を行うことができます。

第 II 部では、ID システムの構成方法について説明します。第 II 部には、次の各章が含まれます。

- 第 3 章「ID システムでのスキーマ・データの使用」
- 第 4 章「User Manager、Group Manager および Organization Manager の構成」
- 第 5 章「ID 機能とワークフローの連携」
- 第 6 章「外部アプリケーションへの非 LDAP データの送信」
- 第 7 章「グローバル設定の構成」

ID システムでのスキーマ・データの使用

ユーザーは、ID システム・アプリケーション (User Manager、Group Manager および Organization Manager) を使用して、自分、他のユーザー、グループ、およびその他のオブジェクトに関するデータを参照および変更できます。ユーザーが ID システム・アプリケーションで参照できる項目は、管理者が ID システム・コンソールで構成した LDAP ディレクトリ属性に基づきます。ID システム・アプリケーションにデータを表示するには、ID システム・コンソールを使用して、アプリケーションで操作するディレクトリ・スキーマのオブジェクトおよび属性を構成します。

ID システム・アプリケーションにより、ユーザーは、データをバックエンド・アプリケーションに送信することもできます。たとえば、ユーザーがワークフローにデータを入力すると、そのデータはユーザーの新規電子メール・アカウントを作成するアプリケーションに送信されます。このような使用方法に対応するよう ID システム・アプリケーションを準備するには、ID システム・コンソールを使用してテンプレート・スキーマのオブジェクトおよび属性を構成します。ID システムには、汎用のスキーマ・ファイルが付属しています。

この章には、次の各項が含まれます。

- オブジェクト・クラスの概要
- オブジェクト・クラスの表示
- オブジェクト・クラスの変更
- オブジェクト・クラスの追加
- オブジェクト・クラスの削除
- オブジェクト・クラス属性の概要
- 属性の表示
- 属性の構成
- 導出属性の構成: 異なる属性間で一致する値
- アプリケーション別の属性の構成

オブジェクト・クラスの概要

ID システム管理者は、ユーザー（および他の管理者）のために 3 つのアプリケーションを構成します。これらのアプリケーションは、User Manager、Group Manager および Organization Manager です。

図 3-1 は、User Manager のプロフィール・ページの一部を示しています。

図 3-1 User Manager のプロフィール・ページの例

The screenshot shows the Oracle Identity Administration console. The top navigation bar includes 'ORACLE Identity Administration', 'ヘルプ', 'バージョン情報', and 'ログアウト'. Below this, there are tabs for 'User Manager', 'Group Manager', 'Org. Manager', and 'Identity System Console'. The main content area is titled 'プロフィール | レポート | ユーザーIDの作成 | 非アクティブなユーザーID | 代替権限 | リクエスト | 構成'. A search bar contains 'フルネーム' and '次を含む'. Below the search bar, there are buttons for 'パネルの表示' and '変更', and a link for 'ユーザー・プロフィール'. The user's details are listed as follows:

役職	Director
フルネーム	Silvia Matson
自動車免許	WKQTW2H
部門番号	20P556

ID システム・アプリケーションでは、表示されるデータの大部分が LDAP ディレクトリのエントリから取得されます。たとえば、User Manager では、個人の名前や電子メールなどが表示される場合があります。このデータは、ディレクトリ内の Person オブジェクトに格納されている属性値から取得されます。これらの属性とその値は、User Manager のプロフィール・ページに表示されます。図 3-1 で、ユーザー・プロフィールに表示されている名前は、ディレクトリ内の Person オブジェクトの名前属性に基づいています。実際に表示される名前は、属性とともに格納されている値です。役職は、Person オブジェクトの役職属性に基づいています。

すべての ID システム・アプリケーション（User Manager、Group Manager および Organization Manager）のプロフィール・ページに、特定のオブジェクトの属性値が表示されます。

テンプレート・オブジェクトを使用した外部システムへのデータの送信

ID システムでは、LDAP ディレクトリのオブジェクトと属性を構成できる以外に、テンプレート・スキーマを定義できます。ID システム・コンソールを使用して、LDAP データを構成する場合と同じようにテンプレート・スキーマのオブジェクトと属性を構成できます。ただし、LDAP データとテンプレート・データの用途は異なります。LDAP データは、ID システム・アプリケーションに移入する目的で構成します。ユーザーは、ID システム・アプリケーションのプロフィール・ページまたはワークフローから LDAP データの値を入力します。LDAP データは、プロフィール・ページに表示されます。一方、テンプレート・データは、ワークフロー・ステップの処理中のみ入力できます。このデータは、プロフィール・ページには表示されません。かわりに、データを必要とするバックエンド・アプリケーションに送信されます。

テンプレート・オブジェクト・データは、LDAP データと異なり、データをバックエンド・システムに送信する場合にのみ使用されます。たとえば、電子メール・システムにより認識可能な属性を含むオブジェクト・テンプレート・スキーマを作成できます。その後、ID システムでそのスキーマの各属性を構成し、それらの属性を使用するワークフローを定義して、ID イベント API の使用によりそのデータをバックエンド・システムに送信できます。

注意：テンプレート・オブジェクト・ファイルの構成方法の詳細は、第 6 章「外部アプリケーションへの非 LDAP データの送信」を参照してください。ID システム・コンソールでテンプレート・オブジェクトを構成するには、第 6 章「外部アプリケーションへの非 LDAP データの送信」の説明に従ってテンプレート・オブジェクト・ファイルを完成する必要があります。

スキーマ・データを構成するためのプロセス

Oracle Access Manager を最初にインストールして設定した段階では、User Manager、Group Manager および Organization Manager の各アプリケーションは空です。これらのアプリケーションは、情報を含むよう構成する必要があります。たとえば、User Manager には、名前、役職、電話番号、電子メールなどのユーザー情報を表示できます。これらのアプリケーションの外観を構成する前に、まず ID システム・コンソールを使用してアプリケーション・プロファイル・ページに表示する LDAP オブジェクトおよび属性を構成する必要があります。また、文字列値、選択リスト、ラジオ・ボタンのどれを使用するかなど、各属性の表示方法も定義する必要があります。ID システム・コンソールでは、主に LDAP ディレクトリ・データを使用して、アプリケーション・プロファイル・ページでユーザーに表示するオブジェクトと属性を指定します。

ID システム・コンソールでオブジェクトと属性を構成したら、ID システム・アプリケーションを構成して各属性とその値を表示できます。ID システム・アプリケーションの構成方法の詳細は、第 4 章「[User Manager、Group Manager および Organization Manager の構成](#)」を参照してください。最後に、それらの属性を表示および変更できるユーザーを指定するために、表示権限と変更権限を割り当てます。

ID システムを外部アプリケーションの入力メカニズムとして使用する場合、ID システム・コンソールを使用してテンプレート・オブジェクトおよび属性を構成します。LDAP データと同様に、プロファイル・ページに各属性をどのように表示するかを定義します。LDAP データとテンプレート・データの主な違いは、ユーザーがテンプレート属性の値を入力できるのはワークフロー・ステップの処理中のみであり、そのデータは ID イベント API を使用してバックエンド・アプリケーションに渡す必要があるということです。

インストール時に構成されるオブジェクト

ID システムのインストールおよび設定時に、次のオブジェクト・クラスを構成します。

- **User Manager:** 必要な Person オブジェクト・クラス
- **Group Manager:** 必要な Group オブジェクト・クラス
- **Organization Manager:** 事前定義された Location オブジェクト・クラス

これらのオブジェクト・クラスは、ID システムの通信先である LDAP ディレクトリから取得されます。

インストール・プロセス中に構成されるオブジェクト・クラスとは別に、LDAP およびテンプレート・ベースの追加のオブジェクトと属性を構成できます。後続の各項では、オブジェクトと属性を構成して ID システム・アプリケーションにデータを提供する方法について説明します。

注意: 属性を構成するだけでは、その属性は ID システム・アプリケーション・ページに表示されません。特定の属性を ID システム・アプリケーション・ページに関連付けて、それらの属性に表示権限と変更権限を割り当てる必要があります。詳細は、第 4 章「[User Manager、Group Manager および Organization Manager の構成](#)」を参照してください。

ID システムの構造化オブジェクト・クラスと補助オブジェクト・クラス

ID システムは、LDAP の構造化オブジェクト・クラスおよび補助オブジェクト・クラスと連携して機能します。ID システムをインストールすると、User Manager、Group Manager および Organization Manager アプリケーションは、それぞれ 1 つの構造化オブジェクト・クラスに関連付けられます。構造化オブジェクト・クラスには、オブジェクトの基本要素に関する記述が含まれます。構造化オブジェクト・クラスの例として、Person や groupOfNames があげられます。Person オブジェクト・クラスには、名前、部門、従業員 ID、電子メール・アドレスなどの属性が含まれます。

User Manager および Group Manager は、常にただ 1 つの構造化オブジェクト・クラスに関連付けられます。

Organization Manager は、汎用または Location オブジェクト・クラス・タイプの任意の数の構造化オブジェクト・クラスに関連付けることが可能です（詳細は、3-6 ページの「[オブジェクト・クラス・タイプ](#)」を参照してください）。インストールおよび設定時に、Location 構造化オブジェクト・クラスが Organization Manager に関連付けられます。Organization Manager では、ページの右上のメニューに各構造化オブジェクト・クラスがオプションとして表示されます。Organization Manager で特定のオブジェクト・クラスの作業領域は、タブと呼ばれます。

図 3-2 Organization Manager のタブ



補助オブジェクト・クラスを使用すると、すでに構造化クラスに属しているエントリに関連属性のセットを追加できます。補助オブジェクト・クラスは、任意の構造化クラスに追加できるミックスイン LDAP オブジェクト・クラスです。請求先住所、チャレンジ・フレーズ、チャレンジ・フレーズに対するレスポンスなどの項目は、補助オブジェクト・クラスでの定義に使用できる可能性があります。

ID システム・コンソールを使用して、管理する各オブジェクト・クラスの属性を構成する必要があります。詳細は、3-11 ページの「[オブジェクト・クラス属性の概要](#)」を参照してください。

注意： 構成した属性の値をユーザーに表示するには、User Manager、Group Manager および Organization Manager タブを設定し、必要に応じてユーザーに表示権限と変更権限を付与する必要があります。詳細は、第 4 章「[User Manager、Group Manager および Organization Manager の構成](#)」を参照してください。

すべてのオブジェクトの継承は、構造化オブジェクト・クラスと補助クラスの両方に共通のスーパー・クラスが存在するという前提に基づきます。それ以外の場合、オブジェクト・クラスの拡張は実行できません。たとえば、eDirectory で継承オブジェクト・クラスとして Top を選択しない場合、NDS では継承オブジェクト・クラスが None に設定されます。ID システムでこのオブジェクト・クラスを補助クラスとして構成すると、初めは問題は表面化しません。ただし、この補助クラスの属性を含むユーザーの作成ワークフローを実行すると、コミットの試行時に「有効化」ステップに失敗します。その理由は、スキーマに互換性がなく、スキーマ違反によりエントリのオブジェクト・クラス属性に補助クラスを追加できないためです。

テンプレート・オブジェクト・クラス

ID システムでは、構造化オブジェクト・クラスおよび補助オブジェクト・クラス以外に、テンプレート・オブジェクト・クラスが認識されます。テンプレート・オブジェクト・クラスは、部分的には補助オブジェクト・クラスと同様に機能します。つまり、これらのクラスは、ID システム・アプリケーション・タブの機能を拡張する場合に使用します。これらのクラスをタブの基盤として使用することはできません。ただし、テンプレート・オブジェクトは、LDAP ディレクトリでは定義しません。また、タブに表示されるプロフィール・ページの構成には使用しません。

テンプレート・オブジェクトは、スキーマ・ファイルに定義します。テンプレート・オブジェクトは、バックエンド・アプリケーションにデータを送信する目的で、ID システム・ワークフローでのみ使用します。テンプレート・オブジェクト・クラスは、次のようないくつかの点で他のオブジェクト・クラスと異なります。

- ユーザーは、テンプレート・オブジェクト・クラス属性とやり取りしてバックエンド・アプリケーションにデータを送信します。
- ユーザーは、ID システム・ワークフローのコンテキスト内でのみテンプレート・オブジェクト・クラス・データ属性とやり取りします。

テンプレート属性の値は、ユーザーがワークフロー・インスタンスを起動してデータを入力する場合にのみ表示されます。データの送信後は、ID システムで再度表示することはできません。詳細は、[第 5 章「ID 機能とワークフローの連携」](#)を参照してください。この動作は、ID システム・アプリケーション・ページに表示されるフィールドやラベルなどの項目の構成に使用される LDAP データとは異なります。

注意：現在のところ、ID システムからバックエンド・システムに向かう一方のデータ・フローのみが存在するため、テンプレート属性の値は表示されません。この制限は、将来のリリースでなくなる予定です。

- テンプレート・オブジェクト・データは、LDAP ディレクトリではなくテンプレート・オブジェクト・ファイルに存在します。

テンプレート・オブジェクトの定義方法と、テンプレート・オブジェクトをバックエンド・アプリケーションと組み合わせて使用する完全なプロセスの詳細は、[第 6 章「外部アプリケーションへの非 LDAP データの送信」](#)を参照してください。

オブジェクト・クラス・タイプ

オブジェクト・クラスを構成する場合、オブジェクト・クラス・タイプを指定するよう求められます。オブジェクト・クラス・タイプという用語は、ID システム内でのオブジェクト・クラスの用途を示しています。表 3-1 に、ID システムでサポートされるオブジェクト・クラス・タイプを示します。

表 3-1 オブジェクト・クラス・タイプ

タイプ	説明
Person	このタイプには、個人に関する情報が含まれます。このタイプの例として、companyOrgPerson や customerOrgPerson があげられます。ID システムをインストールすると、oblixOrgPerson タイプが作成されます。これは、重要な補助オブジェクト・クラスです。このクラスにより、変更が禁止されている obUserAccountControl 属性が提供されます。この属性は、非アクティブ化されるすべてのユーザーのプロファイルに書き込まれます。
Group	このタイプには、グループに関する情報が含まれます。例として、groupOfUniqueNames や mailGroups があげられます。ID システムをインストールすると、oblixGroup および oblixadvancedgroup タイプの補助クラスが作成されます。これらのクラスは、Group Manager で有益な情報を構成する際に役立ちます。
Location	このタイプには、ロケーションに関する情報が含まれます。Organization Manager では、ロケーション情報の格納と表示にこのオブジェクト・クラスが使用されます。
汎用	他のカテゴリに当てはまらない任意のオブジェクト・クラスです。例として、Organization Manager により管理される organizationalUnit オブジェクト・クラスがあげられます。

オブジェクト・クラスの表示

ID システムのインストールおよび設定時に、いくつかのオブジェクト・クラスが構成されています。これらのオブジェクト・クラスは、表示および変更できます。また、追加のオブジェクト・クラスを作成することも可能です。

構成済のオブジェクト・クラスを表示する手順

1. ID システム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
2. 左側のナビゲーション・ペインの「オブジェクト・クラス」リンクをクリックします。
「オブジェクト・クラスの構成」ページに、LDAP ディレクトリおよびオブジェクト・テンプレートに構成されているオブジェクト・クラスが、次の情報とともに表示されます。

列	説明
オブジェクト・クラス	オブジェクト・クラスの名前。
オブジェクト・クラス・タイプ	ID システムでのオブジェクト・クラスの用途。詳細は、3-6 ページの「オブジェクト・クラス・タイプ」を参照してください。
オブジェクト・クラス種別	LDAP オブジェクトを構成している場合、その種別は「構造型」、「補助型」またはその他のオブジェクトのいずれかです。詳細は、3-4 ページの「ID システムの構造化オブジェクト・クラスと補助オブジェクト・クラス」を参照してください。オブジェクト・クラス種別が「その他」の場合、種別が未定義であることを示します。テキストは、「オブジェクト・クラスは考慮不要です」または「不明」のいずれかです。 テンプレート・オブジェクトを構成している場合、その種別は「テンプレート」のみです。詳細は、3-5 ページの「テンプレート・オブジェクト・クラス」を参照してください。

列	説明
オブジェクト・クラス属性	この属性は、属性アクセスのために ID システムで使用されます。また、検索結果をプロファイル・ページにリンクするために ID システムで使用されます。詳細は、3-8 ページの「 クラス属性の選択 」を参照してください。

オブジェクト・クラスの変更

ID システム・コンソールで、クラス属性とオブジェクト・クラス・タイプを変更できます。構造化オブジェクト・クラスにクラス属性を指定することは重要です。

構造化オブジェクト・クラスは変更できます。ただし、変更する必要のないように構成を計画することをお勧めします。

注意：アプリケーション固有の「タブ」機能を使用すると、そのアプリケーション固有の構成タブの属性のみを対象に、オブジェクト・クラス・レベルの構成とは異なる表示名または表示タイプを使用できます。これにより、オブジェクト・クラス・レベルで構成されている属性の情報は上書きされます。詳細は、4-20 ページの「[パネルに表示される属性の変更とローカライズ](#)」を参照してください。

オブジェクト・クラス・タイプを変更する手順

1. ID システム・コンソールで、「共通構成」をクリックします。

「共通構成」ページが表示されます。

2. 左側のナビゲーション・ペインの「オブジェクト・クラス」リンクをクリックします。

3. 変更するオブジェクト・クラスのリンクをクリックします。

「オブジェクト・クラスの表示」ページが表示されます。

4. 「変更」をクリックします。

「オブジェクト・クラスの変更」ページが表示されます。

5. 新規クラス・タイプを選択します。

オブジェクト・クラス・タイプの詳細は、3-6 ページの「[オブジェクト・クラス・タイプ](#)」を参照してください。

6. 変更を保存します。

クラス属性の選択

User Manager、Group Manager および Organization Manager の各タブは、構造化オブジェクト・クラスに関連付けられます。構造化オブジェクト・クラス内で、クラス属性に設定する属性を選択します。クラス属性は、属性アクセスに使用されます。クラス属性に対する読取り権限を持たないユーザーは、エントリ全体にアクセスできません。

注意： テンプレート・オブジェクト・クラスのクラス属性を設定する必要はありません。テンプレート・オブジェクトおよび属性に対するユーザー・アクセスは、ワークフローの構成時に決定します。第5章「ID 機能とワークフローの連携」を参照してください。

ID システムでは、プロフィール・ページに検索結果を表示する場合にもクラス属性が使用されます。ユーザーが検索を実行すると、ID システムにより結果のリストが戻されます。戻される項目ごとに、リンクとして表示される1つの値が含まれます。リンクの値は、戻されるオブジェクトのクラス属性から取得されます。ユーザーがリンクをクリックすると、そのリンクに関連付けられたプロフィールが表示されます。

たとえば、orgPerson オブジェクト・クラスのクラス属性として「ユーザー名」を指定すると、User Manager での検索時に、検索結果のリストにユーザー名がリンクとして表示されます。リンクをクリックすると、そのユーザーのプロフィールが表示されます。

通常、クラス属性は次のように選択されます。

- User Manager では、個人名に対応するクラス属性が使用されます。
- Group Manager では、グループ名に対応するクラス属性が使用されます。
- Organization Manager では、タブごとに1つのクラス属性が使用されます。Location 構造化オブジェクト・クラスの場合、クラス属性はロケーション名となるのが普通です。

クラス属性を選択する手順

1. ID システム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
2. 左側のナビゲーション・ペインの「オブジェクト・クラス」リンクをクリックします。
3. 変更するオブジェクト・クラスのリンクをクリックします。
「オブジェクト・クラスの表示」ページが表示されます。
4. 「変更」をクリックします。
「オブジェクト・クラスの変更」ページが表示されます。
5. 属性のリストからクラス属性を選択します。
ここで選択できるのは、構造化オブジェクト・クラスのクラス属性のみです。
6. 「保存」をクリックします。

構造化オブジェクト・クラスの変更

ユーザーまたはグループの構造化オブジェクト・クラスを変更する場合、ID システム設定を再実行する必要があります。

ユーザーまたはグループの構造化オブジェクト・クラスを変更する手順

1. Identity Server を 1 つだけ残して停止します。
2. `IdentityServer_install_dir/identity/oblix/config/setup.xml` を見つけ、`status` パラメータの値を `done` から `incomplete` に変更します (7-28 ページの「[手動によるシステム設定の再実行](#)」を参照してください)。
3. 変更するアプリケーションに応じて、次のように構造化オブジェクト・クラスの最上位ノードを削除します。

User Manager ノード : `obapp=userservcenter,o=Oblix,o=company,c=us`

Group Manager ノード : `obapp=groupservcenter,o=Oblix,o=company,c=us`

4. Identity Server を再起動して ID システム管理コンソールに移動し、構造化オブジェクト・クラスを再構成する設定プロセスを開始して完了します。

Identity Server を再起動すると、他の Identity Server により、更新されたディレクトリ・ツリーからユーザーまたはグループの新規構造化オブジェクト・クラスが取得されます。

オブジェクト・クラスの追加

ID システム・コンソールでオブジェクト・クラスを追加する場合、次の 2 つの基本的な方法があります。

- 各属性を手動で構成します。
- オブジェクト・クラスの自動構成オプションを選択します。

この方法では、ID システムによる設定を使用してオブジェクト・クラスを構成します。このオプションは、手動構成より高速です。ID システムにより提供される属性は、インポートするまで表示または変更できません。

どちらのオプションの場合も、後からシステム・コンソールを使用して属性を変更できます。3-11 ページの「[オブジェクト・クラス属性の概要](#)」を参照してください。

オブジェクト・クラスを追加する手順

1. ID システム・コンソールで、「共通構成」→「オブジェクト・クラス」をクリックします。
2. 「追加」をクリックします。

「オブジェクト・クラスの追加」ページが表示されます。

デフォルト・スキーマ・ドメインは、LDAP です。テンプレート・オブジェクト・クラスを定義していない場合、LDAP のみを選択できます。追加のテンプレート・オブジェクト・クラスを構成しており、その追加クラスのオブジェクトを構成する場合、「スキーマ・ドメイン」リストからクラスを選択します。

3. 「スキーマ・ドメイン」リストで、使用するスキーマのタイプを選択します (該当する場合)。
4. 「オブジェクト・クラス」リストで、追加するオブジェクト・クラスを選択します。

これにより、ID システムでそのオブジェクト・クラスを管理できます。このリストには、ID システムのインストール前に LDAP ディレクトリに定義されていたオブジェクト・クラスが含まれます。

5. 「クラス・タイプ」フィールドで、このオブジェクト・クラスを管理する ID システム・アプリケーションのタイプを選択します。

詳細は、3-6 ページの「[オブジェクト・クラス・タイプ](#)」を参照してください。

6. 「クラス種別」フィールドで、「構造型」、「補助型」、「テンプレート」または「その他」を選択します。

LDAP ディレクトリに基づいて ID システムでクラス種別を決定できる場合、これらのラジオ・ボタンは非表示になります。

7. ID システムにより提供されるファイルの属性をこのオブジェクト・クラスに移入する場合、「自動構成」オブジェクト・クラスを選択します。

8. 「保存」をクリックします。

テンプレート・オブジェクト・クラスを保存すると、完全修飾形式で保存されます。たとえば、次のようになります。

```
obclass=person,o=oblix,o=company,c=us
```

この形式は、テンプレート・オブジェクト・クラスの定義を含む .tpl ファイルから取得されます。詳細は、第 6 章「外部アプリケーションへの非 LDAP データの送信」を参照してください。

補助クラスの用途

補助オブジェクト・クラスは、構造化オブジェクト・クラスに追加するミックスイン・クラスとして使用できます。このクラスは、User Manager、Group Manager および Organization Manager アプリケーションを構成する場合に役立ちます。自由に使用できるオブジェクト・クラスが増加すれば、各アプリケーションのタブに表示できる項目や、アプリケーション・ユーザーのために構成できる情報も増加します。

補助オブジェクト・クラスに割り当てられたオブジェクトは、構造化クラスに関連付ける必要があります。たとえば、構造化オブジェクト・クラスとして inetOrgPerson を追加し、それを User Manager アプリケーションのタブに関連付けることができます。その後、特定の種類の人々（顧客やパートナなど）に対応する属性を含む補助オブジェクト・クラスを追加できます。

ID システム・アプリケーションのために選択された構造化オブジェクト・クラスに 1 つ以上の補助オブジェクト・クラスを関連付ける方法の詳細は、4-8 ページの「[User Manager または Organization Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加](#)」を参照してください。

オブジェクト・クラスの削除

補助オブジェクト・クラスは削除できます。ユーザーまたはグループのタブに追加されていないテンプレート・オブジェクト・クラスも削除できます。構造化オブジェクト・クラスは削除できません。新しい構造化オブジェクト・クラスで既存の構造化クラスを置換することのみ可能です。詳細は、3-9 ページの「[構造化オブジェクト・クラスの変更](#)」を参照してください。オブジェクト・クラスを削除する場合、そのオブジェクト・クラスに構成されている検索ベースもすべて削除する必要があります。詳細は、4-24 ページの「[検索ベースの設定](#)」を参照してください。

補助オブジェクト・クラスを削除する手順

1. ID システム・コンソールで、「共通構成」→「オブジェクト・クラス」を選択します。
2. オブジェクト・クラスのリンクをクリックします。
オブジェクト・クラスの種別は「補助型」である必要があります。
3. 「オブジェクト・クラスの表示」ページで、「削除」をクリックします。

オブジェクト・クラス属性の概要

ID システムのインストール時に、必要な構造化オブジェクト・クラスとその属性を構成します。ID システム設定の完了後、必要に応じてオブジェクト・クラスの追加、追加属性の構成、および既存の属性の変更を行うことが可能です。オブジェクト・クラスを追加する場合、そのオブジェクト・クラスの属性は ID システムで自動構成できます (3-9 ページの「[オブジェクト・クラスの追加](#)」を参照してください)。「属性の変更」機能を使用して、属性の変更と追加属性の構成を行います。

次の各項で、属性の構成について説明します。

- [属性構成の概要](#)
- [属性のデータ型](#)

注意： Active Directory インストール環境の場合、デフォルトでは一部の属性がスキーマ定義で使用できません。ID システムでの構成用にこれらの属性を表示するには、*IdentityServer_install_dir/identity/oblix/data/common* ディレクトリにある *exclude_attrs_config.xml*、*exclude_attrs-ad.xml* および *ad_exclude_attrs.xml* という 3 つのファイルから属性のエントリを削除する必要があります。変更を反映するには、Identity Server を再起動してください。

属性構成の概要

ID システムでオブジェクトを構成する場合、3-8 ページの「[クラス属性の選択](#)」の手順に従ってクラス属性を選択します。また、ID システムで他のオブジェクト属性をどのように表示し、操作するかを決定する必要があります。たとえば、User Manager で表示する個人に関する項目を決定する必要があります。同時に、データの表示方法も決定する必要があります。

Organization Manager では、プリンタのリストなどを表示できます。または、ユーザーの地理的な場所に基づいて、優先される旅行代理店のリストを表示することも可能です。

ID システムを構成して、LDAP ディレクトリに格納されている任意の属性を使用できます。ID システムでは、適切に構造化された操作用の属性セットを保持することで、管理者が表示を希望するデータを表示することや、ユーザーに詳細なアクセス制御を提供することができます。

属性の構成後、User Manager、Group Manager または Organization Manager のプロファイル・ページに属性を表示するには、追加の手順を実行する必要があります。詳細は、4-11 ページの「[タブのプロファイル・ページおよびパネルの構成](#)」を参照してください。

属性の構成後、表示権限と変更権限を設定し、管理者が表示するよう設定した属性をユーザーが参照できるようにします。ユーザーに読取り権限と変更権限を付与する方法の詳細は、4-21 ページの「[ユーザーによる LDAP データの表示および変更の許可](#)」を参照してください。

属性を構成する前に、属性のデータ型、セマンティック型および検索実行機能の間の関係を理解しておく必要があります。後続の各項では、これらの内容について説明します。

属性のデータ型

3-11 ページの「オブジェクト・クラス属性の概要」のとおり属性を変更する場合、その属性のデータ型が表示されます。データ型は、属性の値の形式です。たとえば、名前属性には、単一行テキストというデータ型を割り当てることができます。すべての LDAP 属性には、関連するデータ型があります。ID システムでは、6 つのデータ型がサポートされます。3-16 ページの「属性の表示タイプ」に記載されているとおり、データ型にはそれぞれ対応する表示タイプがあります。テンプレートまたは LDAP 属性のデータ型は、システム・コンソールでは構成できません。これらのデータ型は、.tpl ファイルまたは LDAP スキーマで構成します。表 3-2 に、サポートされるデータ型を示します。

表 3-2 サポートされるデータ型

データ型	説明	使用可能な表示タイプ
文字列	大 / 小文字を区別しない文字列または区別する文字列。	ブール、チェック・ボックス、日付、電子メール・アドレス、フィルタ・ビルダー、GIF イメージ URL、複数行テキスト、数値文字列、住所、ラジオ・ボタン、選択メニュー、単一行テキスト
識別名	識別名は、エントリの参照方法です。識別名 (DN) は、ファイルのパス名に似ていますが、ディレクトリの最下位からパスを逆順に読み取るところが異なります。	オブジェクト・セクタ、ロケーション (LDAP データのみ)
整数	整数。	なし、ブール、チェック・ボックス、日付、電子メール・アドレス、フィルタ・ビルダー、GIF イメージ URL、複数行テキスト、数値文字列、パスワード、住所、ラジオ・ボタン、選択メニュー、単一行テキスト
電話	電話番号。	任意の表示タイプ
バイナリ	バイナリ・ファイル (GIF ファイルなど)。	GIF イメージ、メディア、パスワード、S/MIME 証明書
住所	これは、デリミタのドル記号 (\$) で連結された 1 ~ 6 個のサブストリングを含む複合文字列です。各サブストリングには、最大 30 文字を割り当てることができます。	住所

属性のセマンティック型

セマンティック型は、ID システム・アプリケーション内の属性の動作を制御するためのオプションの特性です。たとえば、セマンティック型の「写真」に割り当てられた属性の値は、ID システム・アプリケーションのプロファイル・ページのヘッダー領域に表示されます。セマンティック型は、1 つの属性にのみ割り当てることができます。ただし、1 つの属性には、複数のセマンティック型を関連付けることができます。たとえば、「ログイン」および「DN 接頭辞」セマンティック型は、cn 属性に割り当てることができます。

セマンティック型は、一度属性に割り当てたら、その属性との関連付けを解除しないかぎりドメイン内の別の属性に割り当てることができません。たとえば、「パスワード」セマンティック型は、ただ 1 つの LDAP 属性にのみ割り当てることができます。他のスキーマ・ドメインを構成している場合、「パスワード」セマンティック型は、そのドメインのただ 1 つの属性にのみ割り当てることが可能です。詳細は、第 6 章「外部アプリケーションへの非 LDAP データの送信」を参照してください。

属性とセマンティック型との関連付けを解除するには、まずその属性に「なし」セマンティック型を指定し、次に新規セマンティック型を割り当てます。

各セマンティック型は、1 つ以上の表示タイプに関連付けられます (3-16 ページの「属性の表示タイプ」を参照してください)。

システム設定時に定義されるセマンティック型

表 3-3 に、ID システム設定時に必要とされるセマンティック型を示します。

表 3-3 セマンティック型

セマンティック型	説明	使用可能な表示タイプ
フルネーム	Person および Group 構造化オブジェクト・クラスと、Organization Manager のすべての構造化オブジェクト・クラスに必要です。通常は、cn 属性に割り当てられます。cn 属性は、ほとんどのスキーマに必要です。	チェック・ボックス、日付、電子メール・アドレス、複数行テキスト、数値文字列、ラジオ・ボタン、選択メニュー、単一行テキスト
ログイン	Person オブジェクト・クラスに必要です。ログイン時のユーザー資格証明を指定します。	単一行テキスト、電子メール・アドレス
パスワード	Person オブジェクト・クラスのパスワード管理に必要です。また、Active Directory でも必要です。パスワード管理用のユーザー・パスワードを指定します。 注意: Sun 社の iPlanet ディレクトリを使用している場合、パスワードに UTF-8 文字は使用できません。ユーザーが UTF-8 文字を指定すると、iPlanet ディレクトリのデフォルトの 7 ビット・プラグインは操作に失敗します。7 ビット・プラグインのデフォルトでは、UID、メールおよびユーザー・パスワードの各属性値が 7 ビットである必要があります。この問題を解決するには、プラグインを無効化するか、構成からユーザー・パスワード属性を削除します。	パスワード
DN 接頭辞	Person および Group 構造化オブジェクト・クラスと、Organization Manager のすべての構造化オブジェクト・クラスに必要です。オブジェクトの相対識別名 (RDN) を指定します。RDN は、識別名 (DN) の一番左の部分です。DN 接頭辞は、ワークフローを通じてオブジェクトを作成する場合に使用されます。ワークフローの開始ステップには、このセマンティック型の属性が存在する必要があります。	チェック・ボックス、日付、電子メール・アドレス、複数行テキスト、数値文字列、ラジオ・ボタン、選択メニュー、単一行テキスト

プロフィール・ページで使用されるセマンティック型

表 3-4 に、プロフィール・ヘッダー・パネルで使用されるセマンティック型を示します。プロフィール・パネルの詳細は、第 4 章「[User Manager、Group Manager および Organization Manager の構成](#)」を参照してください。

表 3-4 プロフィール・ヘッダー・パネルのセマンティック型

セマンティック型	説明	使用可能な表示タイプ
写真	GIF または JPEG イメージを指定します。「写真」セマンティック型により、プロフィール・ページのヘッダーにイメージが表示されます。	GIF イメージ、GIF イメージ URL
役職	プロフィール・ページのヘッダーに属性値が表示されます。構造化クラスに関連付けられている必要があります。	チェック・ボックス、日付、電子メール・アドレス、複数行テキスト、数値文字列、ラジオ・ボタン、選択メニュー、単一行テキスト
フルネーム	ID システムをパーソナライズするためにプロフィール・ヘッダー・パネルで使用されます。ユーザーは、ID システム・アプリケーションのユーザー・インタフェースで自分の名前を確認できます。	チェック・ボックス、日付、電子メール・アドレス、複数行テキスト、数値文字列、ラジオ・ボタン、選択メニュー、単一行テキスト

Group Manager で使用されるセマンティック型

表 3-5 に、Group Manager で使用されるセマンティック型を示します。

表 3-5 Group Manager で使用されるセマンティック型

セマンティック型	説明	使用可能な表示タイプ
グループの所有者	グループの所有者が格納される属性を指定します。ID システムでは、この情報を主に属性アクセスと委任管理におけるロールとして使用します。また、グループの所有者は、ユーザーによるグループへのサブスクリプションまたはサブスクリプション解除が発生したときに通知を受信できます。	オブジェクト・セレクタ
グループ動的メンバー	グループの動的メンバーシップを定義する動的フィルタが格納される属性を指定します。Group Manager を構成する場合、このセマンティック型を属性に割り当てる必要があります。また、この属性は、Group オブジェクト・クラスに属している必要があります。	オブジェクト・セレクタ
グループ静的メンバー	グループの静的メンバーが格納される属性を指定します。Group Manager を使用する場合、このセマンティック型を属性に割り当てる必要があります。また、この属性は、Group オブジェクト・クラスに属している必要があります。Netscape インストール環境の場合、この属性は uniqueMember です。Active Directory の場合、この属性は Member です。	オブジェクト・セレクタ

「ロケーション座標」セマンティック型

「ロケーション座標」セマンティック型は、ロケーションを追跡するために使用します。このセマンティック型で、ロケーション GIF イメージの位置を指定します。その場合、`obRectangle` 属性と組み合わせて使用します。このセマンティック型は、ID システムで内部的に使用されるため、使用可能な表示タイプはありません。

ロスト・パスワード管理のためのセマンティック型

ロスト・パスワード管理では、2つのセマンティック型が使用されます。ロスト・パスワード機能は、ID システムとアクセス・システムの両方に提供されます。これらのセマンティック型で属性を構成すると、エンド・ユーザーは、後でロスト・パスワードを回復するために使用できるチャレンジおよびレスポンス・フレーズを入力できます。

表 3-6 ロスト・パスワード管理で使用されるセマンティック型

セマンティック型	説明	使用可能な表示タイプ
チャレンジ	エンド・ユーザーがロスト・パスワード管理を起動したときに表示されるチャレンジ・フレーズです。エンド・ユーザーは、正しいレスポンス・フレーズを入力する必要があります。	単一行テキスト
レスポンス	エンド・ユーザーは、ロスト・パスワード管理機能の実装時に、チャレンジ・フレーズに対する正しいレスポンスを入力する必要があります。	パスワード

その他のセマンティック型

表 3-7 に、その他のセマンティック型を示します。

表 3-7 その他のセマンティック型

セマンティック型	説明	使用可能な表示タイプ
優先電子メール・アドレス	電子メール通知の送信に使用されます。	電子メール・アドレス
マップ	このセマンティック型は、 <code>Organization Manager</code> のロケーション機能で使用されます。オブジェクトをロケーションとして構成する場合、バイナリ属性を「マップ」セマンティック型に構成する必要があります。バイナリ属性には、ロケーション機能に対応するマップの GIF または JPEG が格納されます。	GIF イメージ
なし	これは、プレースホルダであり、正式なセマンティック型ではありません。ID システムのビジネス・ルールを属性に関連付けない場合、「なし」を選択します。	該当なし

属性の表示タイプ

表示タイプでは、属性値の表示形式（たとえば、使用可能な値を True/False または電子メール・アドレスのいずれにするかなど）を指定します。表示タイプにより、ユーザーがその属性を使用して検索を実行できるかどうかも決定されます。次の表に示すとおり、「日付」や「複数行テキスト」などの一部の表示タイプのみが検索可能です。

4-11 ページの「[タブのプロファイル・ページおよびパネルの構成](#)」の手順に従って ID システム・アプリケーション・パネルに属性を割り当てた後に、属性の表示タイプまたはセマンティック型を変更する場合、パネルを削除して属性の表示タイプを変更してからそのパネルを再作成する必要があります。

表 3-8 に、属性の表示タイプを示します。

表 3-8 オブジェクトの表示タイプ

表示タイプ	説明	構成可能な特性
なし	ブレースホルダ。	該当なし
ブール	ユーザーが指定する必要がある True または False の選択肢を表示します。この表示タイプは検索できません。	該当なし
チェック・ボックス	チェック・ボックスを表示します。この表示タイプでは、複数值のみサポートされます。また、ルールまたはリストを指定する必要があります。詳細は、3-20 ページの「 ルールとリストの使用方法 」を参照してください。この表示タイプは検索できません。	ルール (LDAP フィルタおよび属性)、リスト (表示名とその他の機能)
日付	ユーザーは、年月日を入力できます。この表示タイプでは、単一値または複数值がサポートされます。この表示タイプは検索可能です。	データ型、データ・セパレータ
電子メール	エンド・ユーザーの電子メール・アドレスへのリンクを表示します。この表示タイプは検索可能です。	該当なし
フィルタ・ビルダー	フィルタ・ビルダーを起動するボタンを作成します。フィルタ・ビルダーにより、ユーザーはカスタム LDAP 問合せを設計できます。この表示タイプは検索できません。	ターゲット・オブジェクト・クラスのリスト
GIF イメージ	ユーザーは、イメージを検索できます。一部の ID システム・アプリケーションでは、JPEG もサポートされます。この表示タイプは検索できません。	写真のスタイル、高さ、幅
GIF イメージ URL	GIF イメージの外部の場所を指定できます。これにより、プロファイル・ページにイメージを表示できます。この表示タイプは検索可能です。	写真のスタイル、高さ、幅
ロケーション	関連するプロファイル・ページに「ロケーション」ページへのリンクを作成します。この表示タイプは、ID システムで内部的に使用されます。	ターゲット・オブジェクト・クラスのリスト
メディア	バイナリ・メディア・ファイルに使用します。この属性には、「バイナリ」データ型を割り当てる必要があります。この表示タイプは検索できません。	説明、MIME タイプ
複数行テキスト	住所などの複数行のテキストです。この表示タイプでは、単一値または複数值がサポートされます。この表示タイプは検索可能です。	該当なし

表 3-8 オブジェクトの表示タイプ (続き)

表示タイプ	説明	構成可能な特性
数値文字列	数値を指定するためのフィールドを表示します。このフィールドには、数値以外の文字は入力できません。この表示タイプは検索可能です。	該当なし
オブジェクト・セレクト	「オブジェクト・セレクト」表示タイプは、セレクトを使用した属性の変更をユーザーに許可する場合に使用します。この表示タイプは、DN 型の属性にのみ有効です。この表示タイプでは、単一値および複数値がサポートされます。検索はできません。「オブジェクト・セレクト」表示タイプの詳細は、3-23 ページの「 「オブジェクト・セレクト」表示タイプの検索フィルタ 」を参照してください。	オブジェクト・クラスのリスト、LDAP フィルタ
パスワード	ユーザーは、パスワードを入力できません。パスワードの文字はアスタリスクで表示されます。また、パスワードは 2 回入力するよう求められます。この表示タイプは検索できません。	テキストのサイズと長さ
住所	ユーザーが住所を指定できる 6 つのデータ入力フィールドです。各フィールドには、最大 30 文字を入力できます。この表示タイプでは、単一値および複数値がサポートされます。	該当なし
ラジオ・ボタン	ラジオ・ボタンのセットを表示します。ユーザーは、ラジオ・ボタンのリストから 1 つの値を選択できます。この表示タイプでは、ルールまたはリストを指定する必要があります。詳細は、3-20 ページの「 ルールとリストの使用方法 」を参照してください。この表示タイプは検索できません。	ルール (LDAP フィルタ、属性)、リスト (表示名、ストレージ名)
選択メニュー	リストを表示します。この表示タイプでは、選択可能な単一値または複数値がサポートされます。この表示タイプでは、ルールまたはリストを指定する必要があります。詳細は、3-20 ページの「 ルールとリストの使用方法 」を参照してください。この表示タイプは検索できません。 「選択メニュー」表示タイプを使用して DN 属性を構成することは避けてください。この表示タイプでは、順序がサポートされません (順序は DN で重要な意味を持つ可能性があります)。たとえば、DN に 2 つの <code>ou</code> が存在する場合、順序が重要になります。	ルール (LDAP フィルタ、属性)、リスト (表示名、ストレージ名)
単一行テキスト	単一行テキストの形式で情報を表示します。このフィールドには、最大文字数がありません。この表示タイプでは、単一値または複数値がサポートされます。この表示タイプは検索可能です。	該当なし
S/MIME 証明書	ディスクではなく構成された属性に証明書データを格納します。この表示タイプは検索できません。	該当なし

注意：ID システム・コンソールでは、表示タイプのリスト（ラジオ・ボタンやチェック・ボックスなど）の項目値として表示される表示名は、Java アプレットおよび国際文字の既知の制限のために破損する可能性があります。ブラウザの JVM では、現在のロケールに含まれる文字のみが表示されます。国際文字は、ブラウザが同じロケールに設定されている場合にのみアプレットで正しく表示されます。

属性の表示

属性は、「属性の変更」ページで参照できます。

システム・コンソールで「属性の変更」ページを表示する手順

1. ID システムのランディング・ページで、ID システム・コンソールのリンクをクリックします。
すでにログインしている場合は、「ID システム・コンソール」タブをクリックします。
2. 「共通構成」サブタブをクリックし、左側のナビゲーション・ペインの「オブジェクト・クラス」をクリックします。
3. オブジェクト・クラスのリンクをクリックします。
選択したクラスの「オブジェクト・クラスの表示」ページが表示されます。
4. 「属性の変更」をクリックします。
「属性の変更」ページが表示されます。

アプリケーション固有の「属性の変更」ページを表示する手順

1. ID システムのランディング・ページで、ID システム・コンソールのリンクをクリックします。
すでにログインしている場合は、「ID システム・コンソール」タブをクリックします。
2. システム・コンソールで、「User Manager 構成」サブタブをクリックします。
「Group Manager 構成」または「Organization Manager 構成」サブタブをクリックすることもできます。
3. 左側のナビゲーション・ペインで、「タブ」をクリックします。
「タブの構成」ページが表示されます。そのタブの構造化オブジェクト・クラスは、「既存のタブ」という見出しの下にリンクとして表示されます。
4. 「既存のタブ」ラベルの下のリンクをクリックします。
「タブの表示」ページが表示されます。
5. 「属性の変更」ボタンをクリックします。
「属性の変更」ページが表示されます。

属性の構成

ID システムのインストール時に、構造化オブジェクト・クラスのすべての必須属性を構成します。インストール後、構成済の属性間の競合を解決する場合や、追加属性を構成する場合に、属性を変更できます。

Active Directory インストール環境の場合、デフォルトでは一部の属性が使用できません。ID システムでの構成用にこれらの属性を使用可能にするには、`IdentityServer_install_dir/identity/oblix/data/common` ディレクトリにある `exclude_attrs_config.xml`、`exclude_attrs-ad.xml` および `ad_exclude_attrs.xml` という 3 つのファイルから属性のエントリを削除して、Identity Server を再起動します。

注意： `oblixadvancedgroup` オブジェクト・クラスでは、`obgroupsubscribenotification` 属性に「チェック・ボックス」および「リスト」サブタイプの表示タイプが含まれます。リストには、次の 2 つの値が含まれます。

- サブスクライブ用の 1 つの値 (`NotifyUponSubscription`)
- サブスクライブ解除用のもう 1 つの値 (`NotifyUponUnsubscription`)

この属性の値を変更する場合、「表示名」フィールドの値のみを変更できます。「ストレージ」フィールドの値は変更しないでください。

属性を構成する手順

1. 3-18 ページの「[属性の表示](#)」の手順に従って「属性の変更」ページを表示します。

注意： アプリケーション固有の「タブ」機能を使用すると、そのアプリケーション固有の構成タブの属性のみを対象に、オブジェクト・クラス・レベルの構成とは異なる表示名または表示タイプを使用できます。これにより、オブジェクト・クラス・レベルで構成されている属性の情報は上書きされます。詳細は、4-20 ページの「[パネルに表示される属性の変更とローカライズ](#)」を参照してください。

2. 「属性」リストで、変更する属性を選択します。

リストの次に属性のデータ型が表示されます。これは読み取り専用フィールドです。

注意： Novell Directory Server (NDS) では、属性名とオブジェクト・クラス名がネイティブ・ディレクトリ・サーバーから NDS の LDAP レイヤーにマップされます。これらの属性またはオブジェクト・クラスの一部には、LDAP レイヤーで複数のマッピング (別名) が割り当てられます。たとえば、ネイティブの NDS オブジェクト・クラスは `Group` ですが、NDS の LDAP レイヤーでは `GroupofNames` および `GroupofUniqueNames` という 2 つの別名がマップされます。ID システムが適切に動作するように、構成時に指定するオブジェクト・クラス名または属性名が、同じオブジェクト・クラスまたは属性の他のマッピングより先に出現していることを確認してください。マッピング順序は、`ConsoleOne` を通じてチェックできます。

3. 「表示名」フィールドに、ユーザーにとってわかりやすいこの属性の表示名を入力します。

表示名は、`User Manager` などの ID システム・アプリケーション・ページに表示されます。たとえば、`departmentNumber` 属性に対して、表示名として「部門番号」と入力できます。

テンプレート・オブジェクト属性では、表示名により使用中のテンプレートを示す必要があります。前述のとおり、ユーザーはこれらの属性のデータ値を参照できません。そのため、データが表示されないことが正常な動作であるとユーザーに知らせる目的で、これらの特殊な形式のフィールドを指定する必要があります。たとえば、ABC アプリケーション

のオブジェクト・テンプレートでは、`assistant.person.abc`などの表示名を使用すると、ABC 関連のすべての属性を識別することが可能になります。

「データ型」フィールドには、属性のデータ型が表示されます (3-12 ページの「属性のデータ型」を参照してください)。これは読取り専用フィールドです。

「バイナリ」、「識別名」または「住所」データ型の属性は、レポート基準または検索属性としては使用できません。

4. オプションで、「セマンティック型」リストから 1 つ以上のセマンティック型を選択できます。セマンティック型の詳細は、3-12 ページの「属性のセマンティック型」を参照してください。
5. 「属性値」フィールドで、属性に単一値と複数値のどちらを割り当てるかを指定します。属性、データ型および表示タイプによっては、このオプションは使用できません。
6. 「表示タイプ」リストで、属性の表示タイプを選択します。

表示タイプに日付属性を選択する場合、ID システム・アプリケーションのプロファイル・ページに日付を表示する方法を指定するため、日付タイプを選択する必要があります。選択後に日付タイプを変更することは避けてください。既存のデータが不適切に表示される可能性があります。

いくつかの表示タイプでは、ルールまたはリストを指定できます。詳細は、3-20 ページの「ルールとリストの使用法」を参照してください。

別の表示タイプでは、写真やテキストを指定できます。これらのフィールドの詳細は、3-28 ページの「その他の表示タイプの構成」を参照してください。

ルールとリストの使用法

「選択メニュー」、「ラジオ・ボタン」および「チェック・ボックス」表示タイプでは、ルールまたはリストを指定する必要があります。たとえば、文字列のデータ型とラジオ・ボタンの表示タイプを「役職」属性に割り当てることができます。User Manager のプロファイル・ページに役職のリストを表示するには、リストを構築する必要があります。

リストは、静的な値のセットです。ルールは、リストの構築前にディレクトリに問い合わせるための LDAP フィルタです。たとえば、TelephoneNumber という属性を持つ `objectClass=dialUpConnection` のすべてのインスタンスを検出するフィルタを作成すると、選択メニューに電話番号のリストが表示されます。

LDAP フィルタの詳細は、3-23 ページの「オブジェクト・セレクタ」表示タイプの検索フィルタを参照してください。また、Internet Engineering Task Force の RFC 2254 には、LDAP 検索フィルタの文字列表現が定義されています。

ルールの定義

ID システム・アプリケーション・ページに表示する静的リストを定義するか、またはルールを定義することが可能です。たとえば、使用可能なプリンタの静的リストを指定するか、ディレクトリ内のプリンタのエントリからこのリストを構築します。ルールを構成する場合、ディレクトリ内のエントリに基づいて動的リストを作成します。ルールは、そのルールで指定する属性に基づくディレクトリ問合せです。問合せにより、ディレクトリからレコードのセットが戻されます。ルールを使用すると、次の操作の実行により、アプリケーション・ページに表示するリストを ID システムで構築できます。

- 特定のオブジェクトまたは属性を対象にディレクトリを問い合わせます。
- 一致した項目のリストを構築します。
- ディレクトリの各一致項目から 1 つの属性を選択します。
- 各属性の値を示すリストを構築します。

リストと比較した場合のルールのメリットは、ルール・フィルタの結果として表示される項目が、ディレクトリの変更に合せて更新されることです。

ルールを定義する手順

1. 3-18 ページの「属性の表示」の手順に従って「属性の変更」ページを表示します。
2. リストから「属性」を選択します。
3. 「表示タイプ」リストで、属性の表示タイプを選択します。

属性のルールを構成する場合、表示タイプは「選択メニュー」、「チェック・ボックス」または「ラジオ・ボタン」である必要があります。

「ルール」ボタン、「フィルタの追加」テキスト・ボックスおよび「属性」フィールドが表示されます。

4. 「ルール」ボタンを選択します。
5. 「フィルタの追加」ボックスに LDAP フィルタを入力します。

ルールは、有効な LDAP フィルタである必要があります。

たとえば、次のようになります。

```
(objectclass=printer)
```

ここでは、「プリンタ」という表示名を持つプリンタ属性の「属性の変更」ページを表示していると仮定します。この手順で説明するルールは、プリンタのリストを表示する場合に適しています。

フィルタの例は、3-23 ページの「[「オブジェクト・セレクタ」表示タイプの検索フィルタ](#)」を参照してください。

6. 「属性」フィールドに、フィルタに関連付ける属性の LDAP 名を入力します。
7. 3-21 ページの「リストの定義」に進みます。

プリンタの例では、PrinterName などを入力します。このルールにより、プリンタ・オブジェクト・クラスに対する LDAP 問合せが実行され、戻された各エントリの PrinterName 属性の値でリストが構築されます。

リストの定義

リストは、ユーザーに表示される静的な値のセットです。

リストを定義する手順

1. 「属性の変更」ページで、「リスト」ボタンをクリックします。
- リストに関連する「表示」フィールドと「ストレージ」フィールドがアクティブになります。
2. 「表示」フィールドにリスト項目の表示名を入力します。
- これは、この属性が User Manager などのアプリケーション・ページに表示されるときにユーザーが参照できる名前です。
3. 「ストレージ」フィールドに属性のストレージ名を入力します。
- この値は、データベースに保存されます。表示名と同じにするか、データベース固有のネーミング規則に準拠することが可能です。
- ストレージ名を省略したまま「追加」をクリックすると、表示名がストレージ名として使用されます。
- ストレージ名を変更する場合は、「ストレージ」フィールドのエントリを削除して、表示名とストレージ名を再入力します。
4. 「追加」をクリックします。
- 情報が「リスト」フィールドに追加されます。

リストの各項目は、このページと同じ表示順序で ID システム・アプリケーション・ページに表示されます。リストの項目を再編成する場合や、項目を削除する場合は、「上へ移動」、「下へ移動」および「削除」ボタンを使用します。

属性表示名のローカライズ

属性表示名をローカライズして、エンド・ユーザーにとって固有の言語で ID システム・アプリケーションに表示できます。複数の言語を管理する方法の詳細は、7-7 ページの「[Oracle Access Manager での複数の言語の構成](#)」を参照してください。

オブジェクト・クラス属性をローカライズするには、インストールされている言語ごとに ID システム・コンソールで属性表示名を手動で入力する必要があります。オブジェクト・クラス属性のローカライズ後、それらの属性を ID システム・コンソールで表示および変更できます。

ローカライズのプロセスは、LDAP オブジェクトとテンプレート・オブジェクトで同じです。

表 3-9 に、各オブジェクト・クラスでローカライズ可能な属性を示します。

表 3-9 ローカライズ可能な項目

項目	翻訳可能な要素
タブに構成されているオブジェクト・クラス	名前 説明 マウスオーバー
パネルに構成されているオブジェクト・クラス	名前 説明 マウスオーバー
属性	表示名
メディア型の表示タイプの属性	表示名
選択型の表示タイプの属性	表示名
ワークフロー定義	ワークフロー名 注意: ワークフロー定義を作成または変更するときに、ワークフロー名の翻訳を指定できます。 第 5 章「ID 機能とワークフローの連携 」を参照してください。

ローカライズされた属性表示名を作成、表示または変更する手順

1. ID システム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
2. 左側のナビゲーション・ペインの「オブジェクト・クラス」リンクをクリックします。
3. 変更するオブジェクト・クラスのリンクをクリックします。
「オブジェクト・クラスの表示」ページが表示されます。
4. 「翻訳」をクリックします。

注意: 「翻訳」ボタンは、2 つ以上の言語がインストールされている場合にのみ表示されます。

「属性表示名のサマリー」ページが表示されます。言語固有の属性表示名は、すべてこのページに表示されます。まだ構成されていない表示名は、「未構成」としてマークされ、青色のテキストで表示されます。

5. 「変更」をクリックして表示名を入力または変更します。
「属性表示名の構成」ページが表示されます。このページには、インストール済言語のリンクと、ローカライズされた属性表示名がリストされます。まだ構成されていない表示名は、左揃えとならずに青色のテキストで表示されます。
6. 属性表示名を変更する言語をクリックします。
7. 「表示名」フィールドに表示名を入力します。
8. 「保存」をクリックして変更を保存します（変更を保存せずにページを終了する場合は、「取消」をクリックします）。

注意：言語に対応する表示名が構成されていない場合、ローカライズされた「未構成」というメッセージが「表示名」フィールドに表示されます。

「オブジェクト・セクタ」表示タイプの検索フィルタ

「オブジェクト・セクタ」表示タイプにより、この表示タイプに割り当てられた LDAP 属性にセクタが関連付けられます。（これは、テンプレート属性には適用されません。）ユーザーは、ユーザーまたはグループを検索するためにセクタを起動します。セクタは、プロフィールまたはワークフローを表示、作成、変更する場合に使用できます。

「オブジェクト・セクタ」表示タイプを使用すると、セクタ用の検索フィルタを作成できます。詳細は、1-11 ページの「[セクタ](#)」を参照してください。検索フィルタを記述することで、ユーザーは、次の操作時に簡単にセクタ検索を実行できます。

- プロファイルの作成
- プロファイルの変更
- ワークフローの変更
- ワークフローの削除

これらのフィルタは、クエリー・ビルダーには適用されません。

ユーザーがセクタを起動すると、ディレクトリ検索が実行されます。セクタ用のフィルタを作成すると、そのフィルタは、ユーザー指定の検索基準と AND 関係で組み合わされて使用されます。

フィルタは、静的フィルタとして使用できます。たとえば、ディレクトリ・プロフィールの組織単位が **Corporate** の人々のみを検索結果に含むようにセクタ検索を制限できます。

フィルタは、動的フィルタとしても使用できます。たとえば、検索の実行された「プロフィールの変更」ページに表示されているユーザーの組織単位に一致する組織単位に含まれる人々のみを戻すようにセクタ検索を制限できます。「プロフィールの変更」ページで動的フィルタを使用する場合、セクタ検索は、表示されているユーザーのディレクトリ・プロフィールに基づいて実行されます。プロフィールを作成する場合、動的フィルタにより、そのタスクを実行するユーザーのログイン・プロフィールに基づいたセクタ検索結果が生成されます。

「オブジェクト・セクタ」表示タイプの検索フィルタの作成

フィルタを使用すると、ユーザーは、検索結果を絞り込むことができます。フィルタにより、検索が実行されるディレクトリ・ツリーの場所が限定されます。

フィルタを作成する手順

1. ID システム・コンソールで、「共通構成」をクリックし、次に「オブジェクト・クラス」をクリックします。
2. フィルタを作成するオブジェクト・クラスのリンクをクリックします。
たとえば、営業担当者用の検索フィルタを作成するには、Person オブジェクト・クラスの「属性の変更」ページに移動します。
3. 「属性の変更」をクリックします。
4. 「属性の変更」ページの「属性」リストで、セクタ検索を定義する属性を選択します。
ここでは、DN 属性を選択する必要があります。たとえば、営業担当者用のセクタ検索を定義する場合、salesPersonDN という DN 属性を選択します。
5. 「表示タイプ」リストで、「オブジェクト・セクタ」を選択します。
前の手順で選択した属性が DN 属性の場合、リストに「オブジェクト・セクタ」オプションが表示されます。また、「ターゲット・オブジェクト・クラス」リストと「フィルタの追加」入力ボックスも表示されます。
6. 「ターゲット・オブジェクト・クラス」リストで、検索フィルタの主キーとして使用するオブジェクト・クラスを選択します。
ターゲット・オブジェクト・クラスにより、「セクタ」検索ページに表示される内容が決定されます。たとえば、ユーザーが営業担当者を検索するのをセクタで支援する場合、ターゲット・オブジェクト・クラスとして「人」を使用します。「属性の変更」ページで複数のターゲット・オブジェクト・クラスを選択すると、セクタ・アプリケーションに各オブジェクト・クラスのタブが割り当てられます。
7. 「フィルタの追加」入力ボックスに有効な LDAP フィルタを入力します。
フィルタにより、セクタの検索結果として表示される内容が決定されます。記述可能な LDAP フィルタ・タイプの例は、3-25 ページの「静的 LDAP 検索フィルタ」および 3-27 ページの「動的 LDAP 検索フィルタの例」を参照してください。
フィルタに使用できるのは、ターゲット・オブジェクト・クラスの定義に含まれている属性のみです。

注意： ID システムでは、空白が文字どおり扱われます。フィルタの末尾に余分な空白や改行が含まれていないことを確認してください。

8. 変更を保存します。
これで、セクタ検索時にユーザーが指定するその他の検索基準と AND 関係で組み合されるフィルタが作成されました。

複数のターゲット・オブジェクト・クラスの検索フィルタ

「属性の変更」ページで複数のターゲット・オブジェクト・クラスを選択すると、セレクト・アプリケーションに各オブジェクト・クラスのタブが割り当てられます。検索フィルタには、OR 演算子 (|) と、選択した各オブジェクト・クラス用の個別の選択基準が含まれる必要があります。このタイプの検索フィルタの例は、3-26 ページの「[複数のターゲット・オブジェクト・クラスを使用した静的検索](#)」を参照してください。

検索フィルタの削除

フィルタを削除するには、「フィルタ」テキスト・ボックスのテキストを削除します。

ルールとフィルタの使用方法

この項には、ルールとフィルタに関連する次の重要な内容が含まれます。

- 基本的な静的フィルタの作成
- 置換構文を使用した動的フィルタの作成
- 検索でのワイルド・カードの使用
- フィルタ記述時における NOT 演算子の適切な使用

静的 LDAP 検索フィルタ

静的検索フィルタの実装では、すべての検索結果が固定値に一致する必要があります。たとえば、ディレクトリ・プロファイルの組織単位が Sales の人々のみを戻すように検索を制限できます。

単純な静的フィルタの例として、seeAlso 属性でセレクト検索を使用する場合を検討します。このフィルタにより、ディレクトリ・プロファイルに businessCategory 値として dealership を含む人々のみが検索結果として戻されます。

静的フィルタを作成する手順

1. 3-18 ページの「[属性の表示](#)」の手順に従って「属性の変更」ページを表示します。
この検索フィルタを起動するオブジェクト・タイプ (Person など) の「属性の変更」ページに移動します。
2. 「属性」リストで seeAlso 属性を選択します。
3. 「表示タイプ」リストで、「オブジェクト・セクタ」を選択します。
4. 「ターゲット・オブジェクト・クラス」で、フィルタの主キーとなるオブジェクト・クラス (Person など) を選択します。
5. 「フィルタ」テキスト・ボックスに次のように検索基準を入力します。

```
(businessCategory=dealership)
```

ワイルド・カードを使用した静的検索

ワイルド・カードを使用する静的フィルタの例として、セクタを使用した検索時に Manager という語を含む役職の人々のみを戻す場合を検討します。Manager という文字列を検索するフィルタを作成できます。

ワイルド・カードを使用した静的検索フィルタを作成する手順

1. セレクタに関連付ける DN 属性を含むオブジェクト・クラス (Person オブジェクト・クラスなど) の「属性の変更」ページに移動します。
2. 「属性」リストで、DN 属性 (Manager 属性など) を選択します。
3. 「表示タイプ」リストで、「オブジェクト・セレクタ」を選択します。
4. 「フィルタ」テキスト・ボックスに次のように検索基準を入力します。

```
(attribute=*value*)
```

たとえば、次のようになります。

```
(title=*manager*)
```

複数のターゲット・オブジェクト・クラスを使用した静的検索

複数のターゲット・オブジェクト・クラスを検索する静的フィルタを作成できます。例として、セレクタを使用した検索で次のいずれかの項目を戻すため、uniqueMember 属性を対象にフィルタを作成する場合を検討します。

- 個人の検索では、検索結果として正社員のみを表示します。
- グループの検索では、検索結果としてメール・グループのみを表示します。

この例の場合、両方の検索目的に対応する LDAP フィルタを作成するには、ディレクトリ・プロファイルで **employee=fulltime** という条件に一致する人々を選択し、さらにディレクトリ・プロファイルでオブジェクト・クラスが **MailGroup** であるグループを選択する必要があります。フィルタの各属性は、適切なオブジェクト・クラスに関連付けます。最後に、次のように OR 演算子 (|) を使用して 2 つの検索基準を結合します。

```
(| (&(objectclass=inetOrgPerson) (employeeType=FullTime))
 (&(objectclass=groupOfUniqueNames) (objectclass=MailGroup)))
```

置換構文: ログイン・ユーザーの DN に一致するターゲットを戻す方法

クエリー・ビルダーの「拡張」ボタンを使用することで、置換構文を入力できます。詳細は、4-27 ページの「クエリー・ビルダーを使用した LDAP フィルタの記述」を参照してください。

置換構文を使用すると、ソース DN (アプリケーションにログインしているユーザー) の変数属性値がルール内で代入され、ターゲット DN (参照または変更しようとしているエントリ) に対して評価されます。

置換構文により、タスクを実行するユーザーに応じて動的にルールを評価できます。構文は次のとおりです。

```
attribute=${attribute$}
```

たとえば、次のようになります。

```
(ou=${ou$})
```

このルールでは、アプリケーションにログインしているユーザーと同じ組織単位に属するすべての人々がフィルタされます。

フィルタには、AND や OR などの演算子を使用できます。たとえば、次のようになります。

```
(| (ou=${ou$}) (ou=people))
```

注意: 選択された検索ベースでは、ユーザーは自分と同じ ou のエントリのみを検索できます。また、ou=people のユーザーは、選択された検索ベース内のエントリを検索できます。

動的 LDAP 検索フィルタの例

従来の LDAP 検索フィルタを指定する以外に、ID システムのフィルタ置換構文を使用して動的フィルタを作成できます。動的フィルタにより、ユーザー・プロファイルに基づいた検索結果を戻すことができます。例として、次の検索基準を含む `orgPerson` 属性用の検索フィルタを作成する場合を検討します。

```
(ou=$ou$)
```

この検索フィルタを使用して個人の「プロフィールの変更」ページでセレクト検索を実行すると、変更対象の個人のプロフィールに含まれる組織単位と一致するディレクトリ・プロフィールを持つ人々のみが検索結果として戻されます。たとえば、`John Smith` の「プロフィールの変更」ページを表示して `John Smith` のマネージャを選択するセレクトを起動した場合、検索結果には `John Smith` の組織単位に属する人々のみが表示されます。

フィルタ置換の使用により、検索ターゲットのプロファイルが代入されます。`(ou=ou)` の例では、`John Smith` の `ou` の値が代入されます。「ワークフローの作成」機能などでターゲットが存在しない場合、検索フィルタでは、ワークフローを作成しているユーザーのログイン・プロファイルの値が代入されます。

例として、ディレクトリ・サーバーでまだ組織単位が定義されていない `Corporate` というグループのワークフローを作成する場合を検討します。この場合、ID システムでは、グループを作成しているログイン参加者の `ou` 値が使用されます。ログイン参加者の `ou` 値は、ディレクトリ・サーバーでこのグループをコミットするまでワークフローで使用されます。コミットの時点で、動的フィルタ `(ou=ou)` の `ou` 値は、グループの `ou` 値に変更されます。

別の例として、ディレクトリ・プロファイルに「秘書」属性を持つユーザーが、自分と同じマネージャを担当する人々のみを含む検索結果を取得する場合を検討します。この場合、「秘書」属性の「属性の構成」ページで次のように指定します。

```
(manager=$manager$)
```

ワイルド・カードを使用した動的検索

動的フィルタにワイルド・カードを使用できます。例として、`organizationalUnit` オブジェクトの `contactPerson` 属性を指定する場合を検討します。`contactPerson` 属性により、`organizationalUnit` オブジェクトと同じ郵便番号の人々を戻す必要があります。`organizationalUnit` プロファイルに `zipCode` という属性が含まれており、`postalAddress` ディレクトリ属性の最後に郵便番号が指定されている場合、フィルタで次のように指定します。

```
(postalAddress=*$zipCode$)
```

複数値を使用した動的検索

動的検索フィルタには複数値も指定できます。例として、ビジネス・オブジェクトの `seeAlso` 属性で `dealership` の `businessCategory` を選択する際に、特に検索ターゲットと同じ都道府県 (`state`) の販売代理店 (`dealership`) を対象とする場合を検討します。この場合、`seeAlso` 属性に次のフィルタを指定します。

```
(&(businessCategory=dealership)(state=$state$))
```

NOT 演算子の使用方法

フィルタを作成する場合、AND (&) 演算子と NOT (!) 演算子を使用できます。たとえば、次のようになります。

- AND 演算子の例: `(&(sn=white)(objectclass=personOC))`
- NOT 演算子の例: `(&(!(sn=white))(objectclass=personOC))`

この NOT フィルタの使用例から、次のフィルタも有効であると思われるかもしれません。

```
(!(sn=white))
```

しかし、NOT 演算子を指定する場合、NOT 演算子は AND 演算子内に組み入れ、`Person` オブジェクト・クラスを指定する必要があります。`(!(sn=white))` などのフィルタは、使用できません。その理由は、フィルタに指定された一部のドメイン・セットを検索対象とする前に、ドメイン全体に対してこのタイプの検索を実行することになるためです。この手順の場合、パ

パフォーマンス上のコストがかかります。ID システムにより使用される最適化されたアルゴリズムでは、検索は一部のドメイン・セットに対して実行されます。NOT 演算子の適切な使用方法は、次のとおりです。

```
(&(! (sn=white)) (objectclass=personOC))
```

最適化されたアルゴリズムを使用する場合、フィルタ `!(sn=white)` では期待した結果は得られません。

その他の表示タイプの構成

その他の表示タイプのための構成オプションがあります。

「GIF イメージ」表示タイプを構成する手順

1. 「属性の変更」 ページで、「写真」属性を選択します。
2. 「表示タイプ」 リストの下のボタンを使用して、写真スタイルを選択します。
 - **正確なサイズ**: GIF を実際のサイズで表示する場合、「正確なサイズ」を選択します。
 - **固定サイズ**: イメージの高さと幅を指定する場合、「固定サイズ」を選択します。

テキスト・ベースの表示タイプを選択する場合、XSL スタイルシートを使用してテキスト用のデフォルトを構成できます。この方法は、列や行の設定にも使用できます。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

ターゲット・オブジェクト・クラスを使用する表示タイプの属性を選択する場合、その属性に関連付ける 1 つ以上のオブジェクトを指定します。この表示タイプでは、単一値または複数値がサポートされます。

- ターゲット・オブジェクト・クラスを設定する場合、「ターゲット・オブジェクト・クラス」リストから 1 つ以上の必要なオブジェクト・クラスを選択します。
- MIME タイプを設定する場合、「MIME タイプ」リストから添付するメディア・ファイルの種類を選択します。

導出属性の構成：異なる属性間で一致する値

導出属性は、仮想 LDAP オブジェクト・クラス属性です。導出属性は、あるオブジェクト・クラスの属性の内容を、同じまたは異なるオブジェクト・クラスの属性と比較することで生成されます。導出属性の主な目的は、逆参照です。

たとえば、誰かのプロフィールに補佐スタッフの名前が含まれることはありますが、補佐スタッフのプロフィールに補佐対象のすべての人々の名前が含まれることはまずありません。導出属性を使用すると、個人プロフィールに補佐スタッフ属性を保持するすべての人々を、補佐スタッフのプロフィールから逆に参照できます。この例では、補佐スタッフの自己属性値を、組織内の他の人々の `AdminAssistant` 属性値と比較します。同様に、`groupOfUniqueNames` オブジェクトは、グループのメンバーへのリンクを備えた `uniqueMember` 属性を含むことができます。ただし、個人のデータを含むオブジェクトから `groupOfUniqueNames` オブジェクトに逆にリンクすることはできない可能性があります。導出属性機能を使用すると、グループ・メンバーは、自分が所属するグループを逆に参照できます。

導出属性を作成するには、比較される値を保持する 2 つの属性を指定します。一致項目は、すべて導出属性に追加されます。

導出属性を使用すると、通常であれば LDAP フィルタ、検索またはレポートを必要とする情報をプロフィールに提供できます。

テンプレート・オブジェクトに関連付けられた属性は、導出属性として構成できません。

注意： 導出属性を使用すると、特に複数の属性がある場合や、属性で複数のオブジェクト・クラスを参照する場合に（Group Manager の導出属性で User Manager の属性に対して参照を実行する場合など）、レスポンス時間が低下する可能性があります。導出属性に関連するパフォーマンス上の問題が発生した場合、対応する属性索引を含めるよう索引ファイルを変更し、そのファイルを再インポートすることをお勧めします。

導出属性の例

ここでは、組織の補佐スタッフが、サポートしているすべてのマネージャを User Manager のユーザー・プロフィールで参照できるよう構成します。これを行うには、各補佐スタッフの属性を取得して、その属性を他のすべての個人プロフィールに含まれる秘書属性の値と比較する導出属性を作成します。補佐スタッフが User Manager でユーザー ID を参照すると、導出属性に一致する人々のみが表示されます。

次に、導出属性を作成する際の手順の概要を示します。

タスクの概要：導出属性の構成

1. ID システム・コンソールで導出属性を追加します。新規属性に「直属の上司」などの説明的な表示名を指定します。
2. 「一致する属性」として「自己」を指定します。

これにより、補佐スタッフの DN が検索基準であることを示します。

3. 補佐スタッフの直属の上司を検索するため、検索対象オブジェクト・クラスとして Person オブジェクト・クラスを指定します。

グループやその他の種類のオブジェクトではなく、必ず個人を検索対象にします。

4. 「参照属性」として「秘書」を指定します。

秘書属性の値が一致するユーザーのユーザー ID を検索します。

5. 新規属性を保存し、その属性を User Manager の「従業員」タブに関連付けます。

これで、補佐スタッフが「ユーザー・プロフィール」ページを表示すると、ID システムにより自己属性（DN）の値が取得され、その属性が他のユーザーの秘書属性の値と比較されます。項目が一致すると、補佐スタッフの「ユーザー・プロフィール」ページの「直属の上司」セクションに、一致したマネージャの名前がリストされます。

注意： プロファイルに表示される属性は、選択済のオブジェクト・クラスのオブジェクト・クラス属性によって決定されます。この値を変更するには、オブジェクト・クラスを変更する必要があります。

導出属性を構成する手順

1. ID システム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
2. 左側のナビゲーション・ペインの「オブジェクト・クラス」リンクをクリックし、次にオブジェクト・クラスの名前の付いたリンクをクリックします。
「オブジェクト・クラスの表示」ページが表示されます。
3. 導出属性を変更するオブジェクト・クラスのリンクをクリックします。
4. 「導出属性の変更」をクリックし、次に「追加」をクリックします。
「導出属性の作成」ページが表示されます。
5. 「属性名」フィールドに、新規導出属性の名前を指定します。

注意: 導出属性は仮想属性のため、属性名はスキーマに含まれません。

6. 「表示名」フィールドに、ID システム・ページに表示する導出属性の名前を入力します。
7. 「一致する属性」フィールドで、現在のオブジェクト・クラスにおいて値を一致させる属性を選択します。
8. 「オブジェクト・クラス」フィールドで、検索するオブジェクト・クラスを選択します。
9. 「参照属性」フィールドで、指定したオブジェクト・クラスにおいて値を比較する属性を選択します。
10. 「保存」をクリックして変更を保存します（保存せずに終了する場合は、「取消」をクリックします）。

User Manager タブへの導出属性の割当て

導出属性を使用する前に、ID システム・アプリケーション・タブに導出属性を割り当てる必要があります。

導出属性をアプリケーション・タブに追加する手順

1. ID システム・コンソールで、「User Manager 構成」（または「Group Manager 構成」あるいは「Organization Manager 構成」）をクリックします。
2. 「タブ」をクリックします。
3. 「既存のタブ」ラベルの下で、変更するアプリケーション・タブのリンクをクリックし、次に「オブジェクト・プロファイルの表示」をクリックします。

表示されるページは、使用中のアプリケーションに応じて異なります。User Manager では、「ユーザー・プロファイルの構成」ページが表示されます。Group Manager では、「グループ・プロファイルの構成」ページが表示されます。Organization Manager では、「オブジェクトの構成」ページが表示されます。

4. 「User Manager 構成」または「Organization Manager 構成」で作業している場合、「パネルの構成」をクリックします。

Group Manager の場合、リンク名は「グループ・プロファイル・パネルの構成」です。

「パネルの構成」（または「グループ・プロファイル・パネルの構成」）ページに、User Manager プロファイルに現在表示するよう構成されているパネルが表示されます。

5. 導出属性を追加するパネルの名前をクリックします。

「パネルの表示」ページが表示されます。

6. 「変更」をクリックします。

「パネルの変更」ページが表示されます。

7. 「属性」メニューで、追加する導出属性を選択します。
8. 関連するテキスト・ボックスに、ID システム・ページに表示する名前を入力します。
9. 追加の「属性」フィールドが必要な場合は、「追加」をクリックします。
10. 「保存」をクリックして変更を保存します（保存せずに終了する場合は、「取消」をクリックします）。

導出属性の権限

導出属性には読取り権限を割り当てることができます。属性に権限を割り当てる方法の詳細は、4-31 ページの「[LDAP 属性権限の設定と変更](#)」を参照してください。

アプリケーション別の属性の構成

この章の説明に従って属性を構成すると、それらの属性は、すべての ID システム・アプリケーションで使用可能になります。つまり、User Manager、Group Manager または Organization Manager 内で属性を使用できます。

ただし、特定のアプリケーションで一部の属性のみを使用することもできます。たとえば、個人の住所に関する属性を User Manager アプリケーションでのみ使用できます。この場合、関連するアプリケーションから、前述の各項に記載されているオブジェクトおよび属性の構成機能にアクセスします。Organization Manager の場合、個々のタブのオブジェクトおよび属性を構成できます。

User Manager、Group Manager および Organization Manager の構成方法の詳細は、[第 4 章「User Manager、Group Manager および Organization Manager の構成」](#)を参照してください。

User Manager、Group Manager および Organization Manager の構成

User Manager、Group Manager および Organization Manager は、エンド・ユーザーが自分、他人、グループ、インベントリ、および管理者が使用を許可したその他の項目に関する情報を参照および変更できる ID システム・アプリケーションです。

第 3 章「ID システムでのスキーマ・データの使用」の章では、ディレクトリやオブジェクト・テンプレート・ファイルのオブジェクトおよび属性を ID システムに認識させる方法と、アプリケーション・ページでの属性の表示形式を構成する方法について説明しました。この章では、属性を特定のアプリケーション・ページに配置する方法と、ユーザーにそれらの属性の参照および変更を許可する方法について説明します。また、各アプリケーションの使用方法についても説明します。

User Manager、Group Manager および Organization Manager アプリケーションを構成するには、マスター ID 管理者または委任 ID 管理者である必要があります。2-5 ページの「[管理の委任](#)」を参照してください。

この章の内容は次のとおりです。

- [User Manager、Group Manager および Organization Manager の概要](#)
- [タブの構成](#)
- [タブのプロファイル・ページおよびパネルの構成](#)
- [ユーザーによる LDAP データの表示および変更の許可](#)
- [アプリケーション構成の例](#)
- [エンド・ユーザーの使用例](#)
- [監査ポリシーの構成](#)
- [レポートの生成](#)
- [拡張構成](#)

User Manager、Group Manager および Organization Manager の概要

User Manager、Group Manager および Organization Manager は、ID システムの主要アプリケーションです。

- ユーザーは、User Manager を使用して、自分の ID 情報の参照、自宅電話番号などの情報の変更、および他のユーザーに関する情報の検索を実行できます。
- ユーザーは、Group Manager を使用して、グループの参照、グループへのサブスクリプト、およびグループ・サブスクリプションの管理を実行できます。
- ユーザーは、Organization Manager を使用してその他のオブジェクトを管理できます。
- Organization Manager の一般的な使用方法として、組織図の参照やインベントリ項目の検索などがあげられます。

管理者は、これらのアプリケーションで誰にどの属性および値を表示するかを制御します。また、ユーザーが検索を実行した際にディレクトリ・ツリーのどの部分へのアクセスを許可することも制御します。管理者は、フィルタを追加して、ユーザー検索の結果がフィルタに指定した基準に準拠するよう設定できます。

ID システムを初めてインストールして設定し、そのオブジェクトと属性を構成した段階では、ID システム・アプリケーション・ページは空です。次の手順に従って、ID システム・アプリケーションで情報を使用できるようにします。

タスクの概要：アプリケーションでの情報の表示

1. ID システム・アプリケーションで使用できるようオブジェクトおよび属性を構成します（第3章「ID システムでのスキーマ・データの使用」を参照してください）。
2. ID システム・アプリケーション・ページ（タブ）を構成します（4-2 ページの「タブの構成」を参照してください）。
3. 属性のグループをパネルに編成して、各タブのプロファイル・ページを構成します（4-11 ページの「タブのプロファイル・ページおよびパネルの構成」を参照してください）。
4. オプションで、LDAP 属性専用の検索にディレクトリ・ツリーのどの部分を含めるかを制御するため、検索ベースを設定します（4-22 ページの「検索ベースの概要」を参照してください）。
5. アプリケーション・タブに表示される属性を参照および変更するためのユーザー権限を設定します（4-31 ページの「表示権限と変更権限の概要」を参照してください）。

タブの構成

ID システム・アプリケーションには、それぞれ1つ以上のタブが含まれます。これらのタブは、次のように構成します。

- ID システム・コンソールの「Group Manager 構成」タブで作業すると、Group Manager アプリケーションの「グループ」タブを構成できます。
- 同様に、ID システム・コンソールの「User Manager 構成」タブを使用すると、User Manager アプリケーションの「ID」タブを構成できます。
- User Manager や Group Manager とは異なり、Organization Manager では複数のタブを構成できます。
- ID システムのインストール時に、デフォルトの構造化オブジェクト・クラスである Location が Organization Manager に定義されます。Organization Manager では、汎用または Location データ型を保持することで ID システムに定義されたオブジェクトを管理できます。詳細は、3-6 ページの「オブジェクト・クラス・タイプ」を参照してください。

User Manager のタブは、Person 構造化オブジェクト・クラスに関連付けられます。Group Manager のタブは、Group 構造化オブジェクト・クラスに関連付けられます。Organization Manager では、複数のタブを保持することが可能であり、各タブはそれぞれ異なるオブジェクト・クラスに関連付けられます。すべてのタブには、補助 LDAP オブジェクト・クラスおよびテンプレート・オブジェクト・クラスを関連付けることができます。

タブ構成情報の表示と変更

User Manager、Group Manager および Organization Manager ページに表示されるタブの特性を参照および変更できます。

タブ構成情報を表示または変更する手順

1. ID システム・コンソールに移動し、「User Manager 構成」、「Group Manager 構成」または「Org. Manager 構成」をクリックします。

「User Manager 構成」、「Group Manager 構成」または「Organization Manager 構成」ページが表示されます。

2. 「タブ」をクリックします。

アプリケーションのタブの名前が含まれる「タブの構成」ページが表示されます。

Organization Manager では、2 つ以上のタブが表示される場合があります。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

システム構成 | **User Manager 構成** | Group Manager 構成 | Org. Manager 構成 | 共通構成 User Manager Group Manager Org. Manager Identity System Console

ログイン・ユーザー: Master Admin

- **タブ**
- レポート
- 監査ポリシー

タブの構成

「タブの構成」には現在構成済のユーザー・タブが表示されます。ユーザー・タブを変更するには、該当タブの名前をクリックします

既存のタブ

Employees	Personクラス・タブ
---------------------------	--------------

3. タブのリンクをクリックします。

User Manager および Group Manager のタブは 1 つのみであるため、ただ 1 つのリンクが表示されます。Organization Manager では、2 つ以上のタブが表示される場合があります。

「タブの表示」ページが表示されます。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

システム構成 | **User Manager 構成** | Group Manager 構成 | Org. Manager 構成 | 共通構成 User Manager Group Manager Org. Manager Identity System Console

ログイン・ユーザー: Master Admin

- **タブ**
- レポート
- 監査ポリシー

タブの表示

「タブの表示」画面には、ユーザー・タブの情報が表示されます。ユーザー・タブの情報を変更するには、「変更」をクリックします。「検索結果属性の表示」をクリックすると、検索結果の一覧表示に現れる属性を見ることができます。このオブジェクトのプロファイル・ページを構成するには、「オブジェクト・プロファイルの表示」をクリックします。User Manager で検索できる属性を選択または選択解除するには、「検索属性の表示」をクリックします。このタブの属性の表示名、セマンティック型、表示型および属性カーディナリティを変更するには、「属性の変更」をクリックします。

タブID	Employees
タブ名	Employees
タブ・イメージ	(イメージなし)
押した状態のタブ・イメージ	(イメージなし)
マウスを置いたときに表示されるメッセージ	
クラス・タイプ	
オブジェクト・クラス	gensiteorgperson OblixOrgPerson
タブ・フィルタ	
タブ検索ベース	

変更 検索結果属性の表示 オブジェクト・プロファイルの表示 検索属性の表示 属性の変更 翻訳 戻る

表 4-1 に、このページに含まれる情報を示します。

表 4-1 タブ情報

フィールド	説明
タブ ID	タブの一意の識別子。
タブ名	アプリケーション・タブに表示される名前。 このフィールドはローカライズできます。
タブ・イメージ	タブの GIF イメージ。GIF は、 <code>WebPass_install_dir/identity/oblix/lang/langTag/style0</code> に格納されている必要があります。ここで、 <code>WebPass_install_dir</code> は WebPass がインストールされているディレクトリであり、 <code>langTag</code> は使用中の特定の言語が含まれるフォルダです。 GIF ファイルの名前のみを入力し、フルパスは入力しないでください。
押した状態のタブ・イメージ	ユーザーがタブ・イメージをクリックしたときに表示される GIF イメージ。
マウスを置いたときに表示されるメッセージ	ユーザーがタブにカーソルを置いたときに表示されるテキスト。 このフィールドはローカライズできます。
クラス・タイプ	このタブの構造化クラスに関連付けられているタイプ。詳細は、3-6 ページの「 オブジェクト・クラス・タイプ 」を参照してください。
オブジェクト・クラス	このタブで使用されている構造化オブジェクト・クラス、補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラス。テンプレート・オブジェクト・クラスは、 <code>miis.person</code> などの完全修飾形式で表示されます。この形式は、クラスの定義されている <code>.tpl</code> ファイルから読み取られます。第 6 章「 外部アプリケーションへの非 LDAP データの送信 」を参照してください。 構造化オブジェクト・クラスは、ID システム・コンソールでは変更できません。補助オブジェクト・クラスは、構造化オブジェクト・クラスに関連付けることができます。4-8 ページの「 User Manager または Organization Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加 」を参照してください。 一部のオブジェクト・クラスはこのページの編集不可能なリストに表示され、他のオブジェクト・クラスはこのページのテキスト・ボックスに表示されます。テキスト・ボックスのオブジェクト・クラスは、まだタブに追加されていません。
タブ・フィルタ	ディレクトリを問い合わせるための LDAP フィルタ。このフィルタにより、限定されたオブジェクトが戻されます。記述可能な LDAP フィルタ・タイプの例は、3-25 ページの「 静的 LDAP 検索フィルタ 」および 3-27 ページの「 動的 LDAP 検索フィルタの例 」を参照してください。 タブ・フィルタでは、フィルタ置換がサポートされません。タブ・フィルタの効果があるのは、タブにおいて検索、プロフィールの表示と変更、およびレポートの作成を行う場合です。フィルタは、検索時に指定された基準と AND 関係で組み合わせられて使用されます。また、レポートの作成時に使用されます。つまり、フィルタと検索の両方の基準が適用されます。表示操作と変更操作では、このフィルタの使用によりターゲット・オブジェクトが限定されます。
タブ検索ベース	ディレクトリ・ツリー (DIT) でのユーザー検索の開始ポイント。詳細は、4-22 ページの「 検索ベースの概要 」を参照してください。

4. 「変更」をクリックします。
5. 必要に応じて変更を加え、「保存」をクリックします。

変更が ID システム・アプリケーションに反映されない場合は、ID システム・コンソールで「システム構成」→「サーバー設定の表示」に移動し、「メモリー・キャッシュを消去」をクリックしてフラッシュ操作を実行し、キャッシュをリロードします。

注意: タブ・イメージや押した状態のタブ・イメージなどを変更すると、これらの要素は即座にユーザーに表示されます。この操作は、パネルに属性を追加する操作（ユーザーが情報を参照するには権限の設定が必要）とは異なります。

タブのローカライズ

複数の言語パックをインストールしている場合、それらの言語で表示するようタブ名をローカライズできます。ローカライズされたタブ名は、管理コンソールで作成、表示および変更します。

複数の言語を管理する方法の詳細は、7-7 ページの「[Oracle Access Manager での複数の言語の構成](#)」を参照してください。

注意: 「翻訳」ボタンは、2つ以上の言語がインストールされている場合にのみ表示されます。

ローカライズされたタブ構成を作成、表示および変更する手順

1. ID システム・コンソールにログインし、「User Manager 構成」（または「Group Manager 構成」あるいは「Org. Manager 構成」）をクリックします。
「User Manager 構成」、「Group Manager 構成」または「Organization Manager 構成」ページが表示されます。
2. 左側のナビゲーション・ペインの「タブ」リンクをクリックします。
アプリケーションの1つ以上のタブ名が含まれる「タブ」ページが表示されます。
3. 既存のタブのリンクをクリックしてその詳細を表示します。
「タブの表示」ページが表示されます。このページには、ID、名前、クラス・タイプ、オブジェクト・クラスなどのタブの詳細が表示されます。
4. 「翻訳」をクリックします。
このボタンがページに表示されない場合は、インストールされている言語が1つのみのため、表示名をローカライズすることはできません。インストールされている単一言語の表示名を変更するには、「変更」をクリックします。
「タブ・ラベル表示名のサマリー」ページが表示されます。次の言語固有のフィールドに対して構成された表示名があれば、その名前がこのページに表示されます。
 - タブ名
 - マウスを置いたときに表示されるメッセージ

特定の言語でまだ構成されていない表示名は、「未構成」としてマークされます。
5. 「変更」をクリックしてタブ表示名を入力するか、既存の表示名を変更します。
タブ・ラベル表示名の構成ページが表示されます。このページには、タブ表示名のフィールドと、すべてのインストール済言語のリンクが含まれます。
6. タブをローカライズする言語をクリックします。
7. 「タブ名」および「マウスを置いたときに表示されるメッセージ」フィールドに表示名を入力します。
8. 「保存」をクリックして変更を保存します。

Organization Manager へのタブの追加

Organization Manager には、2つ以上のタブを含めることができます。

タブを追加する手順

1. ID システム・コンソールで、「Org. Manager 構成」をクリックし、次に「タブ」をクリックします。
「タブの構成」ページが表示されます。
2. 「追加」をクリックします。
「タブの作成」ページが表示されます。
3. 4-3 ページの「[タブ構成情報の表示と変更](#)」の手順に従ってこのページのフィールドを完成します。
4. 「保存」をクリックします。

タブの検索属性の指定

User Manager、Group Manager および Organization Manager のアプリケーション・ページの上部には、検索フィールドがあります。検索フィールドの例は、4-9 ページの「[Group Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加](#)」を参照してください。検索機能リストに表示する属性を指定できます。検索属性は、LDAP ディレクトリからのみ取得できます。テンプレート属性は、検索属性として使用できません。

注意： タブに属性を表示するには、先に属性を構成する必要があります。詳細は、3-11 ページの「[オブジェクト・クラス属性の概要](#)」を参照してください。

検索に使用できる属性を指定する手順

1. ID システム・コンソールで、「User Manager 構成」（または「Group Manager 構成」あるいは「Org. Manager 構成」）をクリックし、次に左側のナビゲーション・ペインの「タブ」リンクをクリックします。
2. タブのリンクをクリックします。
3. 「検索属性の表示」をクリックします。
「検索属性の表示」ページが表示されます。
4. 「変更」ボタンをクリックします。
5. 検索可能にする属性のチェック・ボックスを選択します。
6. 「保存」をクリックします。

検索結果に表示される属性の表示、変更およびローカライズ

検索結果に表示する属性を選択できます。複数の言語をインストールして構成している場合は、検索結果属性をローカライズできます。これにより、複数の言語で検索結果を表示できます。

検索結果属性を表示する手順

1. ID システム・コンソールで、「User Manager 構成」（または「Group Manager 構成」あるいは「Org. Manager 構成」）をクリックします。
2. 左側のナビゲーション・ペインの「タブ」リンクをクリックします。
3. タブのリンクをクリックします。
4. 「検索結果属性の表示」をクリックします。
「検索結果属性の表示」ページが表示されます。

このページには、ユーザーによる検索の結果が戻されるときに表示される属性が含まれます。複数の言語で ID システムを構成している場合、それらの言語がこのページに表示されます。

5. 「変更」をクリックして属性を変更します。
「検索結果属性の変更」ページが表示されます。
最初の属性は、常に「クラス属性」です。
このページでクラス属性の名前を変更することはできません。クラス属性は太字で表示され、このページでは編集できません。クラス属性を変更する方法の詳細は、3-8 ページの「[クラス属性の選択](#)」を参照してください。
6. 属性リストで、変更する検索フィールドごとに新規属性を選択します。
属性の表示名は、属性リストの右側の編集可能なフィールドに表示されます。この名前は、ID システムのユーザー・アプリケーションに表示されます。詳細は、3-11 ページの「[オブジェクト・クラス属性の概要](#)」を参照してください。
7. 追加の属性フィールドが必要な場合は、「追加」をクリックします。
8. 「保存」をクリックします。

検索結果をローカライズする手順

1. ID システム・コンソールで、「User Manager 構成」（または「Group Manager 構成」あるいは「Org. Manager 構成」）を選択します。
2. 左側のナビゲーション・ペインの「タブ」をクリックし、次にリンクをクリックします。
「タブの表示」ページが表示されます。
3. 「検索結果属性の表示」をクリックして「検索結果属性の表示」ページを表示します。
4. 「翻訳」をクリックします。

注意: 「翻訳」ボタンは、2 つ以上の言語がインストールされている場合にのみ表示されます。

「検索結果属性の表示名のサマリー」ページが表示されます。このページには、すべてのローケルの既存の表示名がリストされます。特定の言語でまだ構成されていない表示名は、「未構成」としてマークされます。

5. 「変更」をクリックして任意の言語の表示名を構成します。
「検索結果属性の表示名の構成」ページが表示されます。
6. 表示名を構成する言語をクリックします。
7. 「表示名」フィールドに名前を入力します。

8. 「保存」をクリックして変更を保存します。

User Manager または Organization Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加

補助オブジェクト・クラスは、構造化オブジェクト・クラスに追加するミックスイン・クラスとして使用できます。たとえば、個人用の補助クラスが存在し、そこに個人のバッジ番号の属性が含まれる場合、その補助クラスを構造化オブジェクト・クラスに関連付けることが可能です。User Manager、Group Manager および Organization Manager アプリケーションを構成する場合に、自由に使用できるオブジェクト・クラスが増加すれば、アプリケーション・ユーザーのために構成できる情報も増加します。

第5章「ID 機能とワークフローの連携」の手順に従ってワークフローを作成している場合、補助オブジェクト・クラスをタブに関連付ける際には次のことに留意してください。

- タブによりワークフローと保留中のリクエストが関連付けられている場合、補助オブジェクト・クラスを追加することはできません。
- 追加する補助オブジェクト・クラスに必須属性が含まれる場合、すべての関連ワークフローを編集してそれらの属性を含める必要があります。

テンプレート・オブジェクトもタブに関連付けることができます。テンプレート・オブジェクトを使用するワークフローを構成する予定の場合、この作業は必須です。

注意： User Manager または Organization Manager タブに追加した補助オブジェクト・クラスは削除できません。Group Manager では、「グループ・タイプ」で補助クラスを削除できます。

User Manager または Organization Manager タブに補助オブジェクト・クラスまたはテンプレート・オブジェクト・クラスを追加する手順

1. 追加するオブジェクト・クラスを「共通構成」タブで構成済であることを確認します。
詳細は、3-9 ページの「オブジェクト・クラスの追加」を参照してください。
2. ID システム・コンソールで、「User Manager 構成」(または「Org. Manager 構成」)を選択して「タブ」をクリックします。
「タブ」ページが表示されます。
3. タブのリンクをクリックします。
「タブの表示」ページが表示されます。
4. 「変更」をクリックします。
「タブの変更」ページが表示されます。
5. 「オブジェクト・クラス」ラベルの右端のメニューで、タブに関連付ける1つ以上の補助オブジェクト・クラスまたはテンプレート・オブジェクト・クラスを選択します。
6. 「保存」をクリックします。
変更を保存すると、選択した1つ以上のオブジェクト・クラスが、選択ボックスの左側のリストに追加されます。

Group Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加

補助オブジェクト・クラスを Group Manager に関連付ける場合、グループ・タイプを使用します。Oracle Access Manager では、oblixAdvancedGroup 補助オブジェクト・クラスを提供しており、グループへのメンバーのサブスクライブや、動的グループの作成と拡張を行うための属性を構成できます。

次のページは、「Group Manager」タブをクリックし、次に「グループ」サブタブをクリックすると表示されます。「グループ」は、複数のグループ・タイプ・パネルで構成されます。



グループのメンバー
グループ

newNestedGP1
newAdvGP2

グループ・タイプ・パネルを作成すると、関連付けられたオブジェクト・クラスの属性を Group Manager ユーザー・アプリケーションで使用できます。

Group Manager に補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスを追加する手順

1. 追加する 1 つ以上のオブジェクト・クラスを「共通構成」タブで構成済であることを確認します。

詳細は、3-9 ページの「オブジェクト・クラスの追加」を参照してください。

2. ID システム・コンソールで、「Group Manager 構成」を選択し、次に「グループ・タイプの構成」をクリックします。
3. 「グループ・タイプ・パネルの構成」をクリックし、次に「作成」をクリックします。
4. 一番上のメニューで、追加するオブジェクト・クラスを選択します。
5. 「パネル・ラベル」フィールドに、エンド・ユーザーが Group Manager でこのオブジェクト・クラスの要素を参照したときに表示されるラベルを入力します。
6. 「パネル情報完了」チェック・ボックスを選択します。
7. 「保存」をクリックします。

オブジェクト・クラスが追加されます。この新規オブジェクト・クラスを参照するには、「Group Manager 構成」の左側のナビゲーション・ペインにある「タブ」リンクをクリックします。

Group Manager から補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスを削除する手順

1. ID システム・コンソールで、「Group Manager 構成」を選択し、次に「グループ・タイプの構成」をクリックします。
2. 「グループ・タイプ・パネルの構成」をクリックします。
3. 削除するグループ・タイプのリンクをクリックします。
4. 「削除」ボタンをクリックします。

Group Manager タブのオプションの構成

「Group Manager オプション」機能を使用すると、Group Manager アプリケーションの「グループ」および「メンバー・プロフィールの表示」ページに表示する項目を選択できます。この機能により、コストのかかる操作を無効化できます。この機能は、ID システムのパフォーマンスを向上する必要がある場合に役立ちます。

「グループ」および「メンバー・プロフィールの表示」に表示する項目を選択する手順

1. ID システム・コンソールで、「Group Manager 構成」をクリックし、次に「Group Manager オプション」をクリックします。

「Group Manager オプション」ページが表示されます。

2. 「変更」をクリックして「Group Manager オプションの変更」ページを表示します。

表 4-2 に、各オプションを示します。

表 4-2 Group Manager オプション

オプション	説明
静的グループの表示	個々のメンバーで構成されるグループの表示と非表示を切り替えます。「グループ」ページに適用されます。
ネストされたグループの表示	個々のメンバーおよび他のグループを含むグループの表示と非表示を切り替えます。「グループ」ページに適用されます。
動的グループの表示	フィルタによって決定されるメンバーを含むグループの表示と非表示を切り替えます。「グループ」ページに適用されます。
メンバーとして属するグループを表示	「グループ」ページに「グループのメンバー」属性を表示します。この機能を有効化するには、静的グループの表示、ネストされたグループの表示、および動的グループの表示の各オプションも有効化する必要があります。
所有者であるグループの表示	「グループ」ページで「グループの所有者」属性を使用可能にします。この機能を使用するには、属性を「グループの所有者」セマンティック型に構成する必要があります。
管理者であるグループの表示	「グループ」ページで「グループの管理者」属性を使用可能にします。この機能を使用するには、属性を「グループ管理者」セマンティック型に構成する必要があります。
このグループの静的ユーザー・メンバーの表示	「メンバーの表示」ページに適用されます。静的メンバーシップ機能を使用するには、属性を「グループ静的メンバー」セマンティック型に構成する必要があります。
このグループのネストされたユーザー・メンバーの表示	「メンバーの表示」ページに適用されます。
このグループの動的ユーザー・メンバーの表示	「メンバーの表示」ページに適用されます。動的メンバーシップ機能を使用するには、属性を「グループ動的メンバー」セマンティック型に構成する必要があります。
URL パラメータによるデフォルトのオーバーライドをユーザーに許可	URL パラメータの入力による Group Manager 表示オプションのカスタマイズをユーザーに許可するかどうかを指定します。「メンバーの表示」および「グループ」ページに適用されます。

3. Group Manager に適用する各オプションを選択します。
4. 「保存」をクリックします。

Organization Manager でのタブの削除

Organization Manager に複数のタブが含まれる場合、タブを削除できます。

タブを削除する手順

1. ID システム・コンソールで、「Org. Manager 構成」をクリックし、次に左側のナビゲーション・ペインの「タブ」リンクをクリックします。
2. 削除するタブのリンクをクリックします。
「タブの表示」ページが表示されます。Organization Manager に複数のタブが定義されている場合、このページに「削除」ボタンが表示されます。
3. 「削除」をクリックします。
削除の確認を求められます。
4. 「OK」をクリックすると、タブとそのすべての関連情報が削除されます。

Organization Manager でのタブの並べ替え

Organization Manager に複数のタブがリストされている場合、タブの表示順序を変更できます。

Organization Manager でタブを並べ替える手順

1. ID システム・コンソールで、「Org. Manager 構成」→「タブ」をクリックします。
2. タブのリストの下部にある「タブの順序付け」ボタンをクリックします。
Tab 1、Tab 2 のようにリストされた「タブの順序付け」ページが表示されます。各タブ番号の横に、既存のタブの名前を含むリストがあります。
3. 各タブ番号の横のリストを使用して、希望の順序を指定します。たとえば、次のようになります。
Tab 1: Site
Tab 2: Location
4. 「保存」をクリックします。

タブのプロファイル・ページおよびパネルの構成

プロファイル・ページは、ID システム・アプリケーションのオブジェクトに関する情報が表示される Web ページです。たとえば、User Manager でユーザーに関する情報を検索すると、そのユーザーのプロファイル・ページが表示されます。プロファイル・ページには、ユーザーの次のようなデータが含まれます。

- 名前
- 住所
- 部門
- マネージャ
- 電話番号
- 電子メール

プロファイル・ページの情報は、ID システムの通信先である LDAP ディレクトリのオブジェクトおよび属性に基づきます。または、オブジェクト・テンプレート・ファイルの情報に基づく場合もあります。

プロファイル・ページは、一連のパネルで編成できます。たとえば、個人のプロファイル・ページには、個人、ロケーションおよびプロジェクト情報に関する複数のパネルを含めること

が可能です。プロビジョニング目的でオブジェクト・テンプレート・ファイルを構成している場合、テンプレート・ファイルの各属性を1つの特定のパネルに配置できます。

ユーザーは、次のいずれかの方法でプロファイル・ページを表示できます。

- パネル・ビューでは、プロファイル・ページのデータが複数のパネルに編成されます。
- ページ・ビューでは、プロファイル・ページのデータが1つの長いリストに編成されます。

パネルでの LDAP オブジェクトおよびテンプレート・オブジェクトの使用

パネルで LDAP 属性を構成すると、その属性のラベルと値は、パネルを使用するプロファイル・ページに表示されます。一方で、テンプレート属性は、プロファイル・ページには実際に表示されません。テンプレート属性は、その属性を使用するワークフローを定義している場合にかぎり、「プロファイルの変更」ページにのみ表示されます。


詳細は、第6章「外部アプリケーションへの非 LDAP データの送信」を参照してください。

ヘッダー・パネルの構成

ヘッダー・パネルは、User Manager または Organization Manager のプロファイルの上部に表示されます。ヘッダーには、タブの構造化オブジェクト・クラスから取得された「フルネーム」、「役職」および「写真」セマンティック型の属性が表示されます。ヘッダーは、ユーザー ID プロファイル・ページで表示しないよう無効化できます。

ユーザーのヘッダー・パネルの例は、次のとおりです。

ユーザー・プロファイル

役職	Principal Engineer
フルネーム	Angela Silver
写真	

注意：ヘッダー・パネルで構成できるのは、タブの構造化オブジェクト・クラスの LDAP 属性のみです。

ヘッダー・パネルを構成する手順

1. ID システム・コンソールで、「User Manager 構成」または「Org. Manager 構成」→「タブ」をクリックします。

「タブの構成」ページが表示されます。Organization Manager では、複数のタブが表示される場合があります。

2. タブ・リンクをクリックし、次に「オブジェクト・プロファイルの表示」ボタンをクリックします。
3. ページ上部にリストされているヘッダーをクリックします。

プロファイル・ヘッダーに表示される属性が、「ヘッダー・パネルの構成」ページに表示されます。たとえば、「マップ・イメージ」、「ロケーション名」、「ロケーション・タイトル」などです。

4. 「変更」ボタンをクリックし、ヘッダー・パネルに表示する各属性を選択します。
5. ユーザー・プロファイルにヘッダー・パネルを表示する場合、「User Manager にヘッダー・パネルを表示します。」を選択します。
6. 「保存」をクリックします。

エンド・ユーザー・アプリケーションに構成されているパネルの表示

ID システム・コンソールで構成したパネルは、User Manager、Group Manager および Organization Manager ページで一連の属性としてユーザーに表示されます。

次の表に、ユーザー・プロファイル・パネルのいくつかの例を示します。

表 4-3 ユーザー・プロファイル・パネルの属性

パネル	属性
通信	電話番号
	FAX 番号
	携帯電話番号
ロケーション	部屋
	フロア番号
	建物番号
個人	組織名
	タイプ
	マネージャ

パネルを構成する前に、パネルに配置する属性のオブジェクト・クラスが適切なオブジェクト・クラス・タイプで構成されていることを確認してください。3-6 ページの「[オブジェクト・クラス・タイプ](#)」を参照してください。

エンド・ユーザーの ID システム・アプリケーションでパネルを表示する手順

1. User Manager、Group Manager または Organization Manager で、ユーザー、グループまたは組織オブジェクトの検索を実行します。
2. 検索で戻されたリンクの 1 つをクリックします。
そのオブジェクトのプロファイル・ページが表示されます。
プロファイルがページ・ビューでアプリケーションに表示されている場合は、「パネルの表示」ボタンをクリックします。

パネルの追加、変更、ローカライズおよび削除

パネルは、システム設定時に構成した属性と、[第 3 章「ID システムでのスキーマ・データの使用」](#)に記載されたタスクの実行により構成した属性を使用して作成できます。1 つのパネルで属性を 1 回のみ使用することや、複数のパネルで同じ属性を常時使用することが可能です。

以前のリリースでは、チャレンジ・フレーズ属性とレスポンス属性を「ユーザー・プロファイル」ページの異なるパネルに配置できました。ただし、リリース 10g (10.1.4.0.1) では、チャレンジ・フレーズ属性とレスポンス属性を同じパネルに配置する必要があります。リリース 10g (10.1.4.0.1) の場合、チャレンジ・フレーズとレスポンスは、パネルで交互に構成されていない場合でも、交互に表示されます。

パネルにチャレンジ属性のみが含まれる場合、チャレンジ属性は「ユーザー・プロファイル」ページにレスポンスなしで表示されます。パネルにレスポンスのみが含まれる場合（チャレンジ属性がない場合）、レスポンスは「ユーザー・プロファイル」ページに表示されません。

注意： 1 つ以上の LDAP 属性や、LDAP 属性とテンプレート属性の組合せを 1 つのパネルで構成することも考えられます。テンプレート属性は、ワークフロー実行のコンテキストでのみ表示されるため、テンプレート属性のみで構成されるパネルは空の状態が表示されます。

複数の言語で ID システムを構成している場合、各言語のパネル・フィールドを表示または変更できます。次のパネル・フィールドの表示名をローカライズできます。

- パネル・ラベル
- 説明
- 属性
- マウスを置いたときに表示されるメッセージ

パネルを作成または追加する手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Org. Manager 構成」をクリックし、次に「タブ」をクリックします。
2. タブのリンクをクリックします。
「タブの表示」ページが表示されます。
3. 「オブジェクト・プロファイルの表示」をクリックします。
4. ページ上部の適切なボタンをクリックします。

- User Manager および Organization Manager の場合、「パネルの構成」をクリックします。
- Group Manager の場合、「グループ・プロファイル・パネルの構成」をクリックします。

「パネルの構成」ページが表示されます。現在定義されているパネルが表示されます。

5. 操作を選択します。
 - パネルを追加するには、「作成」をクリックします。
 - パネルを変更するには、パネル・リンクをクリックし、次に「変更」をクリックします。
 - パネルを削除するには、パネル・リンクをクリックし、次に「削除」をクリックします。

「作成」を選択すると、「パネルの作成」ページが表示されます。

6. フィールドを編集します。
「パネルの変更」ページは、「パネルの作成」ページとほぼ同じです。どちらのページでも、次のフィールドを使用できます。

ラベル	説明	ラベル
パネル・ラベル	ユーザー・アプリケーションでのこのパネルの名前。 この名前はローカライズできます。	パネル・ラベル
説明	「パネルの表示」ページに表示されるテキスト。 このテキストはローカライズできます。	説明
属性	リストから選択された属性。追加の属性フィールドが必要な場合は、ページの右側の「追加」をクリックします。テンプレート属性を選択した場合、属性ラベルはこのパネルに表示されません。テンプレート属性は、ワークフローのコンテキストでのみ表示されます。 これらの属性はローカライズできます。	属性

ラベル	説明	ラベル
タイトル・イメージ	<p>ユーザー・プロファイルは、タブで分けられたページとして、または単一のページとして表示できます。タイトル・イメージは、プロファイルを単一のページとして表示したときにパネル・タイトルに使用される GIF イメージです。GIF は、<code>WebPass_install_dir/identity/oblix/lang/langTag/style0</code> に格納されている必要があります（ここで、<code>WebPass_install_dir</code> は WebPass がインストールされているディレクトリであり、<code>langTag</code> は使用中の特定の言語が含まれるフォルダです）。パスなしで GIF ファイルの名前のみを入力します。タイトル・イメージは、7-2 ページの「ID システム・アプリケーションのスタイルの構成」の手順に従って変更できます。</p>	タイトル・イメージ
「タブ・イメージ」と「タブ・イメージ(下)」	<p>ユーザー・プロファイルは、タブで分けられたページとして、または単一のページとして表示できます。タブ・イメージは、タブで分けられたページとしてプロファイルを表示したときに使用される GIF イメージです。タブ・イメージは、通常、パネル・ラベルと一致します。タブ・イメージを定義するまでは、パネル・ラベルがユーザー・プロファイル・ページにリンクとして表示されます。リンクまたはタブ・イメージをクリックすると、パネルが表示されます。「タブ・イメージ(下)」のイメージは、ユーザー・プロファイル・ページの下部に表示されます。</p>	「タブ・イメージ」と「タブ・イメージ(下)」
押した状態のタブ・イメージ	<p>ユーザーがユーザー・プロファイルのパネル・タブをクリックしたときに使用されるイメージ。</p>	押した状態のタブ・イメージ

7. パネルの使用準備が完了したら、ページの下部にある「パネル情報完了」を選択します。
8. 「保存」をクリックします。

注意: 「パネル情報完了」の横のボックスを選択すると、パネル定義が保存されます。ただし、ユーザーがパネルの内容を参照できるかどうかは、読取り権限によって制御されます。これらのオプションの詳細は、4-21 ページの「ユーザーによる LDAP データの表示および変更の許可」を参照してください。

パネルの構成を表示または変更する手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Org. Manager 構成」をクリックします。
2. 左側のナビゲーション・ペインの「タブ」リンクをクリックします。
3. タブのリンクをクリックします。
「タブの表示」ページが表示されます。
4. 「オブジェクト・プロファイルの表示」ボタンをクリックします。
「プロファイル」ページが表示されます。
5. ページ上部の「パネルの構成」をクリックします。
適切な「パネルの構成」ページが表示されます。このページには、構成済の各パネルのリンクが表示されます。
6. パネル・リンクをクリックしてその詳細を表示します。
7. 「変更」をクリックして「パネルの変更」ページを表示します。
8. 必要に応じて情報を変更します。
9. 「保存」をクリックして変更を保存します。

パネルをローカライズする手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Org. Manager 構成」をクリックし、次に左側のナビゲーション・ペインの「タブ」リンクをクリックします。
既存のタブがページに表示されます。
2. タブのリンクをクリックします。
3. 「オブジェクト・プロファイルの表示」ボタンをクリックして「プロファイル」ページを表示します。
4. 「パネルの構成」をクリックして構成済の各パネルのリンクを表示します。
5. リンクをクリックして「パネルの表示」ページを表示します。
6. 「翻訳」をクリックします。
「翻訳」ボタンが表示されない場合は、インストールされている言語が 1 つのみのため、パネルをローカライズすることはできません。インストールされている単一言語のパネル要素の表示名を編集するには、「変更」をクリックします。
「翻訳」をクリックすると、「パネル表示名のサマリー」ページが表示されます。このページには、次のフィールドに対して構成されているすべての言語固有の表示名が表示されます。
 - パネル・ラベル
 - 説明
 - 属性
 - マウスを置いたときに表示されるメッセージまだ構成されていない表示名は、「未構成」としてマークされます。
7. 「変更」をクリックして表示名を作成または変更します。
パネル表示名の構成ページが表示されます。このページには、パネル表示名のフィールドと、すべてのインストール済言語のリンクが含まれます。
8. 任意の言語をクリックします。
9. 適切なフィールドに表示名を入力します。

10. 「保存」をクリックして変更を保存します。

パネルの並べ替え

パネルは、特定の順序でプロファイル・ページに表示されます。Group Manager でのパネルの表示順序は、変更できます。

パネルの表示順序を変更する手順

1. ID システム・コンソールで、「Group Manager 構成」をクリックします。
2. 「グループ・タイプ」をクリックし、次にページ上部の「グループ・タイプ・パネルの順序付け」をクリックします。

注意: 「User Manager 構成」、「Group Manager 構成」または「Organization Manager 構成」を選択し、次に「タブ」→「タブ・リンク」→「オブジェクト・プロファイルの表示」→「パネルの順序付け」の順に選択することも可能です。「Group Manager 構成」では、ページ上部に「グループ・プロファイル・パネルの順序付け」オプションがあります。

「パネルの順序付け」ページが表示されます。

3. 各パネル番号の横のリストを使用して、表示されるパネルの名前を識別します。
4. 「保存」をクリックします。

グループ・タイプ・パネルの表示

グループ・タイプ・パネルにより、「グループ」タブの属性を編成できます。たとえば、構造化オブジェクト・クラスとして `groupOfUniqueNames` を、補助クラスとして `oblixAdvancedGroup` を構成している場合、グループ・タイプ・パネルを作成することで、これらのクラスから「グループ」タブの属性を編成できます。

グループ・タイプ・パネルは、LDAP 属性用に確保されています。テンプレート属性は、グループ・タイプ・パネルで構成できません。

ID システムでグループ・タイプとして識別される各オブジェクト・クラス (3-6 ページの「[オブジェクト・クラス・タイプ](#)」を参照) は、グループ・タイプ・パネルに関連付けることができます。

グループ・タイプ・パネルを表示する手順

1. ID システム・コンソールで、「Group Manager 構成」→「グループ・タイプ」→「グループ・タイプ・パネルの構成」リンクをクリックします。

「パネルの構成」ページに構成済のグループ・タイプ・パネルのリストが表示されます。

2. リンクをクリックしてグループ・タイプの設定を表示します。
 選択したパネルの設定を含む「パネルの表示」ページが表示されます。

ORACLE Identity Administration

ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | **Group Manager構成** | Org Manager構成 | 共通構成

ログイン・ユーザー: Master Admin

グループ・タイプ・パネルの構成 **グループ・タイプ・パネルの順序付け**

グループ・タイプ	グループ・タイプ・パネルの順序付け
パネルの表示	Adv Group
パネルの表示	oblizadvancedgroup
パネル・ラベル	
関連オブジェクト・クラス	
説明	
タイトル・イメージ	(イメージなし)
タブ・イメージ	(イメージなし)
押した状態のタブ・イメージ	(イメージなし)
タブ・イメージ(下)	(イメージなし)
マウスを置いたときに表示されるメッセージ	(イメージなし)

変更 削除 翻訳 戻る

グループ・タイプ・パネルの追加、変更、ローカライズおよび削除

Group オブジェクト・クラスの属性を編成するには、グループ・タイプ・パネルを構成する必要があります。Group 構造化オブジェクト・クラスに対して、少なくとも 1 つのパネルを作成する必要があります。これにより、Group 構造化オブジェクト・クラスの属性のみを含むグループを「グループ」プロファイル・ページで参照できます。

複数の言語をインストールして構成している場合は、次のパネル・フィールドの表示名をローカライズできます。

- パネル・ラベル
- 説明
- マウスを置いたときに表示されるメッセージ

グループ・タイプ・パネルを追加、変更または削除する手順

1. ID システム・コンソールで、「Group Manager 構成」→「グループ・タイプ」をクリックします。
 「グループ・タイプ」ページにグループ・タイプのリストが表示されます。
2. 「グループ・タイプ・パネルの構成」をクリックして「パネルの構成」ページを表示します。
3. 操作を選択します。
 - グループ・タイプ・パネルを追加するには、「作成」をクリックします。
 - 既存のパネルを変更するには、パネル・リンクをクリックし、「パネルの表示」ページで「変更」をクリックします。
 - 既存のパネルを削除するには、パネル・リンクをクリックし、「パネルの表示」ページで「削除」をクリックします。
4. 「グループ・タイプを選択します」というラベル付きのフィールドで、グループ・タイプに関連付けるオブジェクト・クラスを選択します。

注意： Group 構造化オブジェクト・クラスを拡張する補助オブジェクト・クラスか、スキーマで Group 構造化オブジェクト・クラスに関連付けられている補助オブジェクト・クラスのみを選択します。このページで選択できるのは、構成済の補助クラスのみです。詳細は、3-9 ページの「[オブジェクト・クラスの追加](#)」を参照してください。

5. 残りのフィールドに、4-14 ページの「[パネルを作成または追加する手順](#)」に従って値を入力します。
6. 「パネル情報完了」の横のボックスを選択します。
7. 「保存」をクリックします。

注意：「タブ情報完了」を選択すると、パネル定義が保存されますが、ユーザーがパネルの内容を参照できるかどうかは読取り権限によって制御されます。4-21 ページの「[ユーザーによる LDAP データの表示および変更の許可](#)」を参照してください。

パネルの表示名をローカライズする手順

1. ID システム・コンソールで、「Group Manager 構成」をクリックします。
2. 左側のナビゲーション・ペインの「グループ・タイプの構成」をクリックします。
3. 「グループ・タイプ・パネルの構成」をクリックします。
4. 「パネルの構成」ページに構成済のグループ・タイプ・パネルのリストが表示されます。
5. 表示名を構成するパネルをクリックします。
「パネルの表示」ページが表示されます。
6. 「翻訳」をクリックします。

このボタンは、2 つ以上の言語がインストールされている場合にのみ表示されます。1 つの言語のみをインストールしている場合にパネル要素の表示名を構成するには、「変更」をクリックします。

「パネル表示名のサマリー」ページが表示されます。このページには、次のフィールドに対して構成されているすべての表示名がリストされます。

- パネル・ラベル
- 説明
- マウスを置いたときに表示されるメッセージ

特定の言語でまだ構成されていない表示名は、「未構成」としてマークされます。

7. 「変更」をクリックします。
パネル表示名の構成ページが表示されます。
8. 表示名を構成する言語をクリックします。
9. パネル・フィールドの表示名を入力します。
10. 「保存」をクリックして変更を保存します。

パネルに表示される属性の変更とローカライズ

「共通構成」ページで構成した属性は、そのオブジェクト・クラスを利用する各アプリケーションで使用されます。たとえば、共通構成を通じて **cn** 属性の表示名を「フルネーム」に設定できます。この名前は、ユーザー・プロフィール・ページに表示されます。その後、「User Manager 構成」画面で **cn** 属性を「氏名」と表示するよう構成すると、ユーザー・プロフィール・ページにはデフォルトで「氏名」と表示されます。詳細は、第3章「ID システムでのスキーマ・データの使用」を参照してください。

パネルに表示される属性の表示名をローカライズすることも可能です。これにより、ユーザーにとって固有の言語で属性を表示できます。複数の言語を管理する方法の詳細は、7-7 ページの「Oracle Access Manager での複数の言語の構成」を参照してください。

注意： 一度パネルに割り当てた属性の表示タイプまたはセマンティック型を変更するには、そのパネルを削除して再作成する必要があります。

ただし、次に説明するとおり、オブジェクト・クラス・レベルで属性に構成されている情報は上書きできます。

各 ID システム・アプリケーション（User Manager、Group Manager および Organization Manager）には、「タブ」機能を備えたアプリケーション固有の構成タブがあります。アプリケーション固有の「タブ」機能を使用すると、そのアプリケーション固有の構成タブの属性のみを対象に、オブジェクト・クラス・レベルの構成とは異なる表示名または表示タイプを使用できます。たとえば、「User Manager 構成」タブの「説明」属性に異なる表示名を指定できます。

複数の言語をインストールしている環境で適切なローカライズを行うには、タブ・レベルで属性を再構成するときに、インストール済のすべての言語でその属性の表示名を指定する必要があります。例として、2つの言語をインストールしている場合を検討します。たとえば、「User Manager 構成」タブの「説明」属性を2つの言語に翻訳するには、同じタブ・レベルで各インストール済言語の属性の表示名を指定する必要があります。「翻訳」ボタンは、2つ以上の言語がインストールされている場合にのみ表示されます。

次の手順では、タブ・レベルで属性を再構成し、オブジェクト・クラス・レベルで属性に構成されている情報を上書きする方法について説明します。

User Manager、Group Manager または Organization Manager 固有の属性を変更する手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Organization Manager 構成」タブをクリックします。
2. 左側のナビゲーション・ペインの「タブ」リンクをクリックします。
「タブ」ページが表示されます。Organization Manager では、複数のタブが表示される場合があります。
3. タブのリンクをクリックします。
「タブの表示」ページが表示されます。
4. 「属性の変更」をクリックします。
「属性の変更」ページが表示されます。

属性の変更方法の詳細は、3-19 ページの「属性の構成」を参照してください。次の手順を使用すると、属性の表示名をローカライズできます。

属性の表示名をローカライズする手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Organization Manager 構成」をクリックします。
2. 左側のナビゲーション・ペインの「タブ」リンクをクリックします。
「タブの構成」ページが表示されます。Organization Manager では、複数のタブが表示される場合があります。
3. タブのリンクをクリックします。
「タブの表示」ページが表示されます。
4. 「翻訳」をクリックします。

注意: 「翻訳」ボタンは、2 つ以上の言語がインストールされている場合にのみ表示されます。

「属性表示名のサマリー」ページが表示されます。このページには、構成済の属性の表示名がすべての言語でリストされます。まだ構成されていない表示名は、「未構成」としてマークされます。

5. 「変更」をクリックします。
「検索結果属性の表示名の構成」ページが表示されます。このページには、属性の表示名フィールドと、インストール済言語のリンクがリストされます。
6. 表示名を構成する言語をクリックします。
7. 「表示名」フィールドに名前を入力します。
8. 「保存」をクリックして変更を保存します。

ユーザーによる LDAP データの表示および変更の許可

オブジェクトや属性を構成し、アプリケーション・タブのパネルに属性を編成する操作は、ブロックを組み立てることに似ています。基礎となるブロックを配置したら、次にそれらの操作を誰に許可するかを決定できます。

ID システムを設定して、アプリケーション・パネルに構成した LDAP 属性の検索と表示をユーザーに許可する必要があります。これを行うには、次の操作を実行します。

- ユーザーに検索を許可するディレクトリ・ツリーのレベルを決定します。
- ディレクトリ・ツリーの特定の属性に対する表示権限と変更権限を設定します。

注意: 次の項では、表示権限と変更権限を構成する手段として、検索ベースを設定する方法について説明します。検索ベースは、LDAP ディレクトリ・ツリーの検索に関連します。テンプレート属性は、検索ベースの設定とは無関係です。ユーザーにテンプレート属性の値の入力を許可するには、それらのユーザーがテンプレート属性の使用されるワークフローの参加者である必要があります。詳細は、[第 5 章「ID 機能とワークフローの連携」](#)を参照してください。

検索ベースの概要

検索ベースは、ディレクトリ・ツリーのブランチです（または、ツリーの最上位ノードとなることもあります）。インストール時に、デフォルトの検索ベースを選択します。デフォルトの検索ベースは、その下にすべてのユーザー・データが格納されるディレクトリ・ツリー内のノードであり、すべてのユーザー・データを検索できる最上位の基準です。検索ベースにより、検索時にユーザーが使用できるディレクトリ・ツリーの特定部分が決定されます。ユーザーにエントリの参照を許可するには、ID システムに構成された各構造化オブジェクト・クラスに対して検索ベースを設定する必要があります。構造化オブジェクト・クラスごとに複数の検索ベースを設定できます。

検索ベースを設定する場合、誰に何を（ディレクトリ・ツリーの特定レベルのオブジェクト・クラス）検索可能にするかを決定します。このとき、オプションで検索フィルタを使用します。

検索ベースを設定する前に、次のことを決定する必要があります。

- どのオブジェクト・クラス（ユーザーまたはグループ）に検索ベースを設定するか。
- どこに検索の開始ポイントを設定するか。
- 誰に検索を許可するか。

たとえば、ある検索ベースを従業員用として構成し、別の検索ベースを顧客用として構成できます。これにより、顧客側から従業員情報が参照されないことが保証されます。

別の例としては、2つの競合する部品納入サプライヤが存在する場合に、各サプライヤのユーザーが自社に関する部分のみを DIT で参照できるように検索ベースを設定できます。

注意： 検索ベースは、User Manager アプリケーションで設定します。この場合、「User Manager 構成」機能ではなくエンド・ユーザー・アプリケーションを使用します。グループ・クラスのグループ・プロフィール・ページに対する読取り権限も構成する必要があります。

検索ベースを設定する際のガイドライン

検索ベースを設定する場合、ログイン・ユーザーが参照できる検索ベースのブランチを指定するためのフィルタを定義できます。ディレクトリ・ツリーが特にフラットな形状の場合、ノードを選択しても検索ベースをあまり限定できないため、フィルタ機能は検索の絞込みに役立ちます。フィルタは、ディレクトリ・ツリーに大量のブランチがある場合にも役立ちます。たとえば、10,000 の販売代理店がある場合、販売店内で検索を絞り込むことが可能です。

ただし、フィルタにより大量のエントリが生成される場合、パフォーマンスが影響を受ける可能性があります。検索ベース・フィルタを使用するかわりに、クラス属性に対する読取り権限を設定できます（3-8 ページの「[クラス属性の選択](#)」を参照してください）。クラス属性は、属性アクセスと、プロフィール・ページへの検索結果のリンクに使用されます。

たとえば、検索ベースからリソース・フィルタを削除して、「すべてのユーザー」のロールに Person オブジェクト・クラスへのアクセスを許可するとします。検索ベースを設定するかわりに、クラス属性にアクセスできるユーザーを指定するルールを使用して、そのクラス属性に対する読取り権限を定義します。これにより、ID システムで実行されるディレクトリ検索の数を削減できます。詳細は、4-31 ページの「[LDAP 属性権限の設定と変更](#)」を参照してください。

注意： 特定のユーザーがディレクトリ・ツリーの異なる部分にアクセスする必要がある場合、同じユーザーまたはグループに対して複数の検索ベースを設定できます。たとえば、従業員がツリーで従業員と顧客の両方のブランチを検索する場合、従業員用と顧客用の検索ベースを定義して、その両方の表示権限を従業員に付与できます。ただし、特定のオブジェクト・クラスに複数の検索ベースを構成する場合は、その数が多くなりすぎないようにしてください。可能であれば、かわりに属性に対する読取り権限と書込み権限を定義します。同じオブジェクト・クラスに対して複数の検索ベースを設定すると、パフォーマンスが低下する可能性があります。

検索ベースを変更する必要がある場合

ディレクトリ・ツリーの検索対象レベルを変更する場合、または検索属性を変更する場合、検索ベースを直接変更することはできません。直接変更すると、ID システムでは、変更された検索ベースが新しく定義された検索ベースとして扱われます。検索ベースを変更する唯一の方法は、検索ベースを一度削除して新しく作成することです。

注意： この項で説明されている変更以外であれば、検索ベースを変更できません。

索引付けと検索ベース

ディレクトリの検索は、システム・パフォーマンスにおける重要な要因です。索引付けのガイドラインは、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

Oracle Internet Directory の索引付け要件

Oracle Internet Directory では、索引付けされていない属性が検索で使用されると、エラーが戻されます。たとえば、索引付けされていない「一致する属性」を使用して導出属性を定義し、その属性を Oracle Access Manager のプロファイル・ページに追加するとします。ページが表示されると、Oracle Internet Directory によってエラーが戻され、導出属性の値はプロファイル・ページに表示されません。Oracle Access Manager のログ・ファイルには、「操作はサポートされていません。」というエラー・メッセージが記録されます。

検索フィルタで追加属性を使用するには、それらの属性をカタログ・エントリに追加する必要があります。索引付けできるのは、次の条件に対応する属性のみです。

- 等価性一致ルール
- 『Oracle Identity Management ユーザー・リファレンス』の「LDAP 属性の一致ルールについて」にリストされている、Oracle Internet Directory でサポートされる一致ルール
- 128 文字以下の名前

新規属性（つまり、ディレクトリ内にデータが存在しない属性）を索引付けするには、`ldapmodify` ツールを使用します。ディレクトリ内にすでにデータが存在する属性を索引付けするには、カタログ管理ツールを使用します。属性から索引を削除する場合、`ldapmodify` も使用できますが、カタログ管理ツールを使用することをお勧めします。

スキーマに新規属性を定義したら、`ldapmodify` を使用してその属性をカタログ・エントリに追加できます。

ディレクトリ・データが存在しない属性を追加するには、`ldapmodify` を使用して LDIF ファイルをインポートします。たとえば、スキーマに定義されている新規属性 `foo` を追加するには、`ldapmodify` を使用して次の LDIF ファイルを Oracle Internet Directory にインポートします。

```
dn: cn=catalogs
changetype: modify
add: orclindexedattribute
orclindexedattribute: foo
```

この方法は、ディレクトリにデータが存在する属性の索引付けには使用しないでください。ディレクトリにデータが存在する属性を索引付けするには、カタログ管理ツールを使用します。

検索ベースの設定

次の手順では、検索ベースを設定する方法について説明します。

検索ベースを設定する手順

1. User Manager アプリケーションで、「構成」サブタブをクリックします。

「構成」ページが表示されます。

2. 「検索ベースの設定」をクリックします。

一部のブラウザでは、アプリケーションの証明書を信頼するかどうかを尋ねるプロンプトが表示されることがあります。その場合は、「常に信頼」オプションを選択してください。

「検索ベースの設定」ページが表示されます。



検索ベースの設定

特定の組織や人に対して検索ベースを設定します。これによりアクセスが限定され、セキュリティが確保されます。

1) オブジェクト・クラス	<input type="text" value="gensiteorgperson"/>
2) 検索ベース ドメイン	<input type="text" value="o=company,c=us"/>
フィルタ	<input type="text" value="o=company,c=us"/>
フィルタの追加	<input type="text" value="(ou=\$ou\$)"/>
<hr/>	
3) ターゲット ドメイン	<input type="text" value="o=company,c=us"/>
ロール	<input type="checkbox"/> 匿名 <input checked="" type="checkbox"/> すべてのユーザー
ルール	<input type="text" value="フィルタの作成"/>

3. 「オブジェクト・クラス」リストで、オブジェクト・クラスを選択します。

選択するオブジェクト・クラスにより、検索対象が定義されます。たとえば、製品の検索ベースを設定する場合、製品オブジェクト・クラスを選択します。

検索ベース・ドメイン・ボックスには、検索の最上位ノードが示されます。検索ベース・ドメイン・ボックスのすぐ下のフィールドで、情報を入力または編集します。

4. 検索ベース・ドメイン・ボックスの下で、オブジェクトの検索を実行するディレクトリ・ツリーの特典部分を指定します。

たとえば、製造部門の製品を対象に検索ベースを定義する場合、検索ベースの製造 (Manufacturing) ブランチを選択します。

ディレクトリ・ツリーの最上位レベルを選択すると、ドメイン全体が検索に使用されます。検索ベースを再定義するには、ツリー内でより下位のノードを選択するか、フィルタを入

力します。たとえば、検索を北米に限定するには、最上位ノードを選択し、フィルタとして `region=North America` と入力します。この例では、ディレクトリ・ツリーに北米 (North America) というブランチがあると仮定します。フィルタの記述方法の詳細は、3-25 ページの「[ルールとフィルタの使用法](#)」を参照してください。

「フィルタ」ボックスに、検索用の現在のフィルタが表示されます。「フィルタ」ボックスのすぐ下の「フィルタの追加」フィールドを使用して、別のフィルタを入力できます。

5. **オプション:** 「フィルタの追加」フィールドに別のフィルタを入力します。

6. 「保存」をクリックします。

新規フィルタが前のフィルタの下のフィールドに表示されます。

ディレクトリ・ツリーのこの部分の検索を許可するユーザーとグループは、次のパネルで定義します。

7. ディレクトリ・ツリーのこの部分の検索を許可するユーザーまたはグループを指定します。たとえば、次のようになります。

- **ターゲット・ドメイン:** 選択したノードの下のツリーに含まれる任意のユーザー・オブジェクト。

ワークフロー作成時にターゲット・ドメイン (またはワークフロー・ドメイン) のフィルタを指定する場合、完全な LDAP URL は使用しないでください。LDAP フィルタのみを使用できます。たとえば、`ldap:///ou=Partners,o=Company,c=US??sub?(cn=Shutterbug Canavan)` ではなく、`cn=Shutterbug Canavan` とするのが適切です。

- **ロール:** ユーザーのロール。

ログインしているかどうかにかかわらず、すべてのユーザーにこの権限を付与する場合、「匿名」を選択します。

User Manager、Group Manager または Organization Manager にログインしている任意のユーザーにこの権限を付与する場合、「すべてのユーザー」を選択します。

注意: 匿名アクセスは、User Manager および Organization Manager の「自己登録」機能でのみ使用されます。また、匿名アクセスは、ルールとして構成された表示タイプ属性 (チェック・ボックス、ラジオ・ボタンまたはリスト) にのみ適用されます。たとえば、LDAP フィルタの (`objectclass=organizationalunit`) を使用するルールを備えたリスト表示タイプとして `ou` 属性を構成するとします。自己登録でこの属性を構成するには、`organizationalUnit` の Organization Manager タブにアクセスし、クラス属性の属性アクセスを構成します (匿名アクセス権の付与方法の詳細は、4-31 ページの「[LDAP 属性権限の設定と変更](#)」を参照してください)。

- **ルール:** LDAP フィルタで任意の個人を指定します。「フィルタの作成」をクリックし、クエリー・ビルダーを使用してルールを作成します。詳細は、4-27 ページの「[クエリー・ビルダーを使用した LDAP フィルタの記述](#)」を参照してください。

- **人々:** 任意の個人を選択します。「ユーザーの選択」をクリックし、セレクトタを使用して各個人を選択します。

- **グループ:** 任意のグループを選択します。「グループの選択」をクリックし、セレクトタを使用して 1 つ以上のグループを選択します。

ある検索ベースから別の検索ベースにユーザーやグループをコピーするには、「コピー」のクリック、「リセット」のクリック、別の検索ベース・ドメインとターゲット・ドメインの選択、「貼付け」のクリックの順に操作を実行します。ユーザーとグループが、対応する個々のボックスに表示されます。

注意: 複数の方法 (たとえば、ルールの設定および個々のユーザーの選択) によりユーザーを指定すると、両方の方法が適用されます。唯一の例外は、「すべてのユーザー」を選択した場合です。「すべてのユーザー」は、他のすべての方法を上書きします。

8. 次のいずれかのボタンをクリックして、適切なアクションを実行します。
 - **保存:** 変更を保存および実装します。
 - **リセット:** すべての選択を消去します。
 - **削除:** すべてのルール、グループおよびユーザーの指定を消去します。
 - **レポート:** 構成済の検索ベースを要約したレポートを生成します。

グループの検索ベースを設定する場合

groupOfUniqueNames オブジェクト・クラスに検索ベースを設定し、検索ベースを定義するグループを選択できます。グループに設定された検索ベース内のエントリの参照をグループのメンバーに許可するには、グループ・クラスのグループ・プロファイル・ページに対する読取り権限を構成する必要があります。4-31 ページの「[LDAP 属性権限の設定と変更](#)」を参照してください。

非結合検索ベースの構成と削除

非結合検索ベースは、ID システム設定時に選択した検索ベースを補足する検索ベースです。非結合検索ベースを作成して、ユーザー・データの存在する追加の LDAP ディレクトリ・ツリーを指定できます。

1 つのドメインに複数の非結合検索ベースを追加できます。次の手順では、非結合検索ベースを追加および削除する方法について説明します。

非結合検索ベースの管理方法の詳細は、7-34 ページの「[複数のディレクトリ検索ベースの操作](#)」を参照してください。

非結合ドメインに非結合検索ベースを追加する手順

1. ID システム・コンソールで、「システム構成」 → 「ディレクトリ・プロファイル」をクリックします。
2. 「ディレクトリ・サーバー」リンクをクリックします。
3. 「非結合検索ベース」フィールドに非結合検索ベースを追加し、「保存」をクリックします。
4. ID システム・コンソールで、「User Manager 構成」をクリックします。
5. 左側のナビゲーション・ペインで、「タブ」を選択します。
「タブの構成」ページが表示されます。
6. タブ・リンクをクリックします。
7. 「変更」をクリックします。
8. 「タブ検索ベース」フィールドに値が含まれていないことを確認します。
9. 必要に応じて変更を保存します。

非結合検索ベースを削除する手順

1. 削除対象の検索ベースを使用しているすべてのディレクトリ・プロファイルを無効化します。

ディレクトリ・プロファイルに構成されている検索ベースは、そのプロファイルの「ネームスペース」フィールドで確認できます。非結合ドメインでは、検索ベースごとに1つのディレクトリ・プロファイルが存在します。詳細は、「[LDAP ディレクトリ・サーバー・プロファイルの作成](#)」および7-34 ページを参照してください。

2. 非結合検索ベースのすべてのアクセス制御ポリシーを削除します。

削除済の検索ベースに定義されたポリシーが存在する場合、ノードにその検索ベースを保持するユーザーは、クエリー・ビルダーを使用してその検索ベースを基準とするフィルタを作成できます。

3. ID システム・コンソールで、「システム構成」 → 「ディレクトリ・プロファイル」を選択します。
4. 「ディレクトリ・サーバー」リンクをクリックします。
5. Disjoint_domain フィールドの情報を削除し、「保存」をクリックします。

クエリー・ビルダーを使用した LDAP フィルタの記述

クエリー・ビルダーにより、検索ベースの設定などのアクティビティを実行する際に LDAP フィルタを記述できます。

ID システムでは、問合せのヒット数は 20 までに制限されています。この制限は、セレクタとクエリー・ビルダーの両方に適用されます。検索や問合せの結果が 20 ヒットを超えると、切り捨てられた結果が戻されます。検索の制限を変更する手順の詳細は、『[Oracle Access Manager カスタマイズ・ガイド](#)』に記載されている `cookieBustLimit` パラメータの説明を参照してください。

クエリー・ビルダー機能には、「フィルタの作成」ボタンからアクセスします。この機能は、検索ベースの設定時などに使用できます。詳細は、4-24 ページの「[検索ベースの設定](#)」を参照してください。

注意： 問合せの作成時に「存在する」または「存在しない」演算子を選択すると、フィルタとして存在フィルタが使用されるため、表示タイプに指定された値は考慮されません。

クエリー・ビルダーを使用する手順

1. 「User Manager」アプリケーション・タブをクリックします。

これらは ID システム・アプリケーションです。

2. 「構成」サブタブをクリックします。
3. 「検索ベースの設定」をクリックします。
4. 「検索ベースの設定」ページで、「フィルタの作成」ボタンを見つけてクリックします。

「クエリー・ビルダー」ページが表示されます。デフォルトでは、「Basic」問合せページが表示されます。

5. 「属性」リストで、検索基準として使用する属性を選択します。

たとえば、次のようになります。

Admin

6. 「追加」をクリックします。

属性がフィルタに追加されます。

7. 新規属性の横のリストで、一致方法を選択します。
たとえば、次のようになります。
次以上
使用可能な一致方法は、属性に応じて異なります。詳細は、4-29 ページの「[一致を取得するための方法](#)」を参照してください。
8. 一致方法の横のフィールドで、問合せ文字列を選択または入力します。
たとえば、次のようになります。
January 22 2003
9. 「追加」をクリックして他の属性を追加します。
10. 属性の左側のリストで、属性間の関係を選択します。
 - AND: 結果はすべての行の基準に一致します。
 - OR: 結果はいずれか 1 つの行の基準に一致します。たとえば、「管理者」属性を持ち、かつ開始日が 2003 年 1 月 22 日より後の（より大きい）すべてのユーザーを検索できます。
11. 「テスト」をクリックしてフィルタをテストします。
結果が多すぎるか少なすぎる場合は、基準の制限範囲を調整します。
12. フィルタから属性を削除するには、属性の横の「削除」をクリックします。すべての属性を削除するには、「すべて削除」をクリックします。
13. 「保存」をクリックします。
「保存」をクリックすると、前のページの「フィルタの作成」ボタンの下にフィルタが表示されます。

注意：保存時に不正なリクエストであるというメッセージが戻された場合、問合せ文字列がブラウザにとって長すぎます。ブラウザではフィルタを URL として扱うため、問合せ文字列がブラウザの最大 URL 長を超えるとエラーが発生します。

一致を取得するための方法

クエリー・ビルダーで選択できる一致方法は、属性の表示タイプに応じて異なります。たとえば、属性の表示タイプとして、リストまたはラジオ・ボタンのセットを使用できます。詳細は、3-16 ページの「属性の表示タイプ」を参照してください。クエリー・ビルダーを使用して、リストなどの複数の値を含む表示タイプの属性にフィルタを作成すると、フィルタ基準を満たすのが 1 つの値のみであっても問合せで一致結果が戻されます。

フィルタを作成する場合、属性の表示タイプがチェック・ボックスまたはラジオ・ボタンである場合にのみ、1 つの行で属性の複数の値を選択できます。

表 4-4 に、クエリー・ビルダーで使用できる一致方法をリストします。

表 4-4 クエリー・ビルダーでの一致方法

方法	説明
次と等しい	結果は指定した値と完全に一致します。
次と等しくない	結果は指定した値を含みません。
次以下	結果は指定した値以下です。たとえば、フルネームの問合せで k と指定すると、A から K の文字で始まる名前を持つ人々が戻されます。
次以上	結果は指定した値以上です。たとえば、フルネームの問合せで k と指定すると、K から Z の文字で始まる名前を持つ人々が戻されます。
次より小さい	指定した値未満の値を持つすべてのディレクトリ・エントリが戻されます。テキスト文字列をフィルタすると、「次より小さい」では、指定した値よりアルファベット順で前のエントリが戻されます。たとえば、フルネームの問合せで k と指定すると、A から J の文字で始まる名前を持つ人々が戻されます。
次より大きい	指定した値を超える値を持つすべてのディレクトリ・エントリが戻されます。テキスト文字列をフィルタすると、「次より小さい」では、指定した値よりアルファベット順で後のエントリが戻されます。たとえば、フルネームの問合せで k と指定すると、L から Z の文字で始まる名前を持つ人々が戻されます。
次を含む	指定した文字列をエントリの値のどこかに含むすべてのディレクトリ・エントリが戻されます。たとえば、st と入力すると、street や best などの値が戻されます。
次を含まない	指定した文字列をエントリの値のどこにも含まないすべてのディレクトリ・エントリが戻されます。
存在する	この属性を含むすべてのディレクトリ・エントリが戻されます。たとえば、「管理者」属性と「存在する」を選択すると、すべての管理者が戻されます。
存在しない	この属性を含まないすべてのディレクトリ・エントリが戻されます。
次で始まる	指定した値で始まるすべてのディレクトリ・エントリが戻されます。
次で終わる	指定した値で終わるすべてのディレクトリ・エントリが戻されます。
次で始まらない	指定した値で始まらないすべてのディレクトリ・エントリが戻されます。
次で終わらない	指定した値で終わらないすべてのディレクトリ・エントリが戻されます。
次と類似する	結果は指定した値の発音に類似します。このオプションは、検索対象オブジェクトのスペルが不確かな場合に使用します。発音に即したスペルを使用してください。たとえば、kiero と指定すると、cairo などの値が戻されます。 このオプションは、Novell Directory Services ではサポートされません。
次に類似しない	結果には、指定した値の発音に類似しないエントリが表示されます。発音に即した最適なスペルを使用してください。 このオプションは、Novell Directory Services ではサポートされません。

クエリー・ビルダーを使用した拡張 LDAP フィルタの作成

フィルタでは、複数の属性を操作し、AND、OR、NOT などの論理演算子を使用できます。

複雑なフィルタを作成する手順

1. ID システム・コンソールで、User Manager アプリケーションのタブをクリックします。
2. 「構成」サブタブをクリックします。
3. 「検索ベースの設定」をクリックします。
4. 「フィルタの作成」ボタンをクリックします。
5. 「クエリー・ビルダー」ページで、「拡張」タブをクリックします。

6. 「Basic」から「拡張」に切り替えて「OK」を選択すると、現在のフィルタは失われます（表示されているフィルタを維持するには、「取消」をクリックします）。

「拡張」ページが表示されます。

「拡張」タブをクリックしても「拡張」ページが表示されない場合、URL が長すぎる可能性があります。URL の長さは、ブラウザにより決定されます。

7. 「属性の選択」リストで、検索基準として使用する属性を選択します。
8. 対応するリストで一致方法を選択し、対応するテキスト入力フィールドに問合せ文字列を追加します。

詳細は、4-27 ページの「クエリー・ビルダーを使用した LDAP フィルタの記述」を参照してください。

9. 「追加」をクリックします。

属性は、「構築されたビジュアル・フィルタ」ボックスに追加されます。

10. オプションで次の手順を実行できます。

- LDAP コマンドを追加するには、「AND」、「OR」、「()」の各ボタンを使用します。
- 「構築されたビジュアル・フィルタ」ボックスから属性を削除するには、属性を選択して「削除」をクリックします。すべての属性を削除するには、「すべて削除」をクリックします。
- 「構築されたビジュアル・フィルタ」ボックスのエントリを変更するには、次の操作を実行します。
 - エントリを選択します。
 - ページ上部で問合せ特性を変更します。
 - 「変更」をクリックします。

11. 「LDAP フィルタの表示」をクリックして作成中のフィルタを表示します。

「LDAP フィルタ」ボックスに LDAP 文字列が表示されます。このボックスのテキストを編集して、「ビジュアル・フィルタの更新」をクリックできます。LDAP フィルタの例は、3-25 ページの「静的 LDAP 検索フィルタ」および 3-27 ページの「動的 LDAP 検索フィルタの例」を参照してください。

非常に複雑なフィルタを手動で入力した場合、「構築されたビジュアル・フィルタ」ボックスではそのフィルタを正しく解釈できないことがあります。ただし、フィルタは正常に動作します。

12. 「テスト」をクリックして問合せの結果を表示します。

フィルタに準拠した出力が ID システムに表示されます。

13. 「保存」をクリックしてフィルタを保存および適用します。

「保存」のクリック時に不正なリクエストであるというメッセージが戻された場合、問合せ文字列がブラウザにとって長すぎます。ブラウザではフィルタを URL として扱うため、問合せ文字列がブラウザの最大 URL 長を超えるとエラーが発生します。

表示権限と変更権限の概要

属性に対する権限が構成されるまで、どのユーザーも User Manager、Group Manager および Organization Manager に表示される属性を参照できません。たとえば、User Manager ですべてのユーザーに従業員の仕事用電話番号を表示する一方で、マネージャにのみ自宅電話番号を表示するよう設定できます。

マスター ID 管理者または適切な権限を保持する委任管理者の場合、ユーザー権限を構成できます。デフォルトでは、Identity Server のインストール時に指定されたマスター管理者は、すべての属性に対する完全なアクセス権を保持します。デフォルト設定を変更するには、次の場所の BypassAccessControlForDirAdmin パラメータを false に設定します。

```
IdentityServer_install_dir/identity/oblix/apps/common/bin
```

LDAP 属性権限の設定と変更

「属性アクセス制御」機能を使用して、各 LDAP 属性の値を参照および変更できるユーザーを決定する権限を指定します。また、属性が変更されたときに通知を受けるユーザーまたはグループのリストを作成します。検索ベースを設定した場合と同様に、この機能は LDAP 属性にのみ適用されます。テンプレート・オブジェクトに対する権限は、ワークフロー・ステップに参加者を追加するときに構成します。詳細は、第 5 章「ID 機能とワークフローの連携」を参照してください。

属性を表示するには、ユーザーは定義された検索ベースと読取り権限を保持している必要があります。たとえば、User Manager、Group Manager または Organization Manager タブでクラス属性を表示するには、ユーザーはそのクラス属性に対応する適切な検索ベース・ドメインの受託者であり、その属性の読取り権限を保持している必要があります。

属性権限を設定または変更する手順

1. User Manager、Group Manager または Organization Manager で、ページ上部の「構成」をクリックします。

「構成」ページが表示されます。

2. 「属性アクセス制御」をクリックします。

アプリケーションの証明書を信頼するかどうかを尋ねるプロンプトが表示された場合は、「常に信頼」オプションを選択してください。

「属性アクセス制御」ページが表示されます。

3. 「管理ドメイン」ボックスで、この権限を適用するディレクトリ情報ツリー (DIT) の有効範囲を指定します。

初め、このフィールドには製品設定時に定義された検索ベースが表示されます。この検索ベースは、システム設定を再実行した場合にのみ変更できます。ツリーの下位レベルを選択すると、そのブランチにアクセス制御が適用されます。たとえば、「フルネーム」属性を選択し、営業 (Sales) などの下位レベルの部門を選択すると、プロフィールにフルネームを含む営業部門のすべての人々にアクセス制御が適用されます。

4. オプションで、「フィルタ」フィールドを使用して LDAP ルールを入力し、オブジェクトと属性をより厳密に指定できます。

フィルタにより、参照または変更可能な属性が絞り込まれます。フィルタを指定しない場合、ID システムでは objectclass=* が使用されます。

注意： フィルタは、データベース設計が特にフラットな形状の場合、または特に大量のブランチが存在する場合に役立ちます。

「フィルタの追加」フィールドにフィルタを追加します。構成を保存すると、フィルタが「フィルタ」リストに追加されます。後で別のフィルタを指定する場合は、元の検索ベースを削除して新規構成を作成する必要があります。

フィルタの詳細は、3-25 ページの「ルールとフィルタの使用法」を参照してください。

5. 次の権限を指定します。
 - 読取り: 選択されたユーザーは、プロフィール・ページで属性とその値を参照できません。
 - 変更: 選択されたユーザーは、属性値を変更できます。属性値を参照できるように、これらのユーザーには読取り権限が付与されている必要があります。
 - 通知: 属性値が変更されたときに、指定のユーザーに電子メールが送信されます。

たとえば、マネージャに「役職」属性に対する読取り権限と変更権限を付与できます。ユーザー・プロフィールでこの属性値が変更されたときに、人事管理部門に通知が送信されるよう設定できます。自己登録ステップの電子メール事後通知の詳細は、5-13 ページの「ステップ・アクションの説明」を参照してください。

6. 「属性」ボックスで、この権限に関連付ける属性を選択します。

複数選択を行う場合、4-33 ページの「複数の属性を選択するためのキー」を参照してください。

注意: 複数選択の範囲内の属性に受託者の異なるセットが含まれる場合、エラーが表示されます。これにより、不注意で不適切な受託者（参加者）にアクセス権を付与することが防止されます。

7. 次の 1 つ以上の項目を対象にこの権限を付与します。

ロール: ユーザーのロールに基づいて権限を割り当てます。「ロール」領域には、データ型が DN で表示タイプが「オブジェクト・セクタ」であるすべての属性が表示されます。ID システムには、「自己」および「匿名」ロールが付属しています。各アプリケーションには、構成済の属性に大きく依存する様々なロールが含まれます。たとえば、User Manager の構成によっては、「マネージャ」ロールが含まれる一方で、秘書属性に基づくロールは含まれない可能性があります。共通ロールは、次のとおりです。

ロール	説明
すべてのユーザー	User Manager、Group Manager または Organization Manager にログインしているすべてのユーザーは、選択されたレベルの属性を参照または変更できます。たとえば、すべてのログイン・ユーザーは、ディレクトリの指定されたレベルの電話番号属性を参照できます。
匿名	すべてのユーザーは、ログインしているかどうかにかかわらずエントリを参照できます。匿名アクセスは、自己登録でのみ使用されます。
自己	User Manager アプリケーションにログインしているユーザーは、自分自身の ID に関する属性を参照または変更できます（属性に対する読取りおよび書込み権限が、そのユーザーのプロフィールを含む程度にディレクトリ・ツリー内で十分である場合）。 たとえば、「自己」を選択して最上位レベルの「名前」属性を参照できる場合、User Manager、Group Manager または Organization Manager にログインしているユーザーは、自分の名前を参照できます。ただし、ディレクトリ・ツリーのレベルとして ou=Marketing を指定した場合、マーケティング (Marketing) 部門に属していないユーザーは、自分の名前を参照できません。
マネージャ	User Manager アプリケーションにログインしているユーザーは、自分の直属の部下に関する属性を参照または変更できます。
秘書	User Manager にログインしているユーザーが補佐スタッフの場合、そのユーザーは、自分がサポートしている人々に関する属性を参照または変更できます。
グループの所有者	Group Manager にログインしているユーザーは、自分が所有しているグループに関する属性を参照または変更できます。

ロール	説明
グループ管理者	Group Manager にログインしているユーザーは、自分が管理しているグループに関する属性を参照または変更できます。
グループ・メンバー	Group Manager にログインしているユーザーは、自分が所属しているグループに関する属性を参照または変更できます。

ルール: 「フィルタの作成」をクリックし、クエリー・ビルダーを使用してルールを作成します。詳細は、4-27 ページの「クエリー・ビルダーを使用した LDAP フィルタの記述」を参照してください。

人々: 「ユーザーの選択」をクリックし、セレクトタを使用して 1 人以上のユーザーを指定します。

グループ: 「グループの選択」をクリックし、セレクトタを使用して 1 つ以上のグループを指定します。

権限の評価順序の詳細は、4-34 ページの「LDAP 属性権限の評価」を参照してください。

8. ある属性から別の属性にユーザーやグループをコピーするには、「コピー」のクリック、「リセット」のクリック、新規属性の選択、「貼付け」のクリックの順に操作を実行します。
9. 次のいずれかのボタンをクリックします。
 - **保存:** 変更を保存および実装します。
 - **リセット:** すべての選択を消去します。
 - **削除:** すべてのルール、ロール、グループおよびユーザーの指定を消去します。
 - **レポート:** 属性と、ドメイン内でのその属性のアクセス権に関するレポートを生成します。

複数の属性を選択するためのキー

次のキーを組み合わせると、複数の属性に対するアクセス制御を一度に構成できます。

- [Ctrl] + [Home]: ハイライト表示されている属性と、それより上のすべての属性が選択されます。
- [Ctrl] + [End]: ハイライト表示されている属性と、それより下のすべての属性が選択されます。
- [Ctrl] + [Page Up]: ハイライト表示されている属性より上の属性のみが選択されます。
- [Ctrl] + [Page Down]: ハイライト表示されている属性より下の属性のみが選択されます。

注意: 複数選択の範囲内の属性に受託者（参加者）の異なるセットが含まれる場合、エラーが戻されます。これにより、不適切な受託者にアクセス権を付与することが防止されます。

プラットフォーム固有のキーの組合せは、次のとおりです。

ブラウザ・タイプ	機能
Windows ブラウザ	<ul style="list-style-type: none"> ■ 複数の属性を選択する場合、[Ctrl] キーを押しながら属性を選択します。 ■ ある属性とそれより前のすべての属性を選択する場合、[Ctrl]+[Shift]+[Home] キーを押して属性を選択します。 ■ ある属性とそれより後のすべての属性を選択する場合、[Ctrl]+[Shift]+[End] キーを押して属性を選択します。 ■ ある属性とそれより後の任意の数の属性を選択する場合、属性を選択して [Shift]+[↓] を押します。 ■ ある属性とそれより前の任意の数の属性を選択する場合、属性を選択して [Shift]+[↑] を押します。
UNIX ブラウザ	<ul style="list-style-type: none"> ■ 複数の属性を選択する場合、[Esc] キーを押しながら属性を選択します。 ■ ある属性とそれより前のすべての属性を選択する場合、[Esc]+[Shift]+[Home] キーを押して属性を選択します。 ■ ある属性とそれより後のすべての属性を選択する場合、[Esc]+[Shift]+[End] キーを押して属性を選択します。

LDAP 属性権限の評価

権限を表示および変更するための複数の方法が割り当てられている場合、ID システムでは、これらの方法が次の順序で評価されます。

1. ユーザー
2. ロール
3. グループ
4. ルール (LDAP フィルタ)

ID システムは、一致を検出した時点でチェックを終了します。たとえば、User=Lou Reed に「名前」属性に対する読取り権限を付与する一方で、Lou Reed 以外のすべてのユーザーを許可する (&!(cn=Lou Reed) objectclass=person object class) というルールを指定するとします。この場合、Lou Reed は、評価順序でルールより先にユーザーとして評価されるため、アクセス権を付与されます。別の例として、人事管理部門へのアクセスを拒否するルールを指定する一方で、ユーザー・セレクトクを使用して人事管理部門の個々の従業員を指定する場合は、ルールおよびユーザー・カテゴリの組合せにより、指定した従業員にアクセス権が付与されます。

注意：「すべてのユーザー」ロールを選択した場合、すべてのユーザー、ロール、グループおよびフィルタは上書きされます。

アプリケーション構成の例

次の各項では、アプリケーション構成の様々な例について説明します。User Manager、Group Manager および Organization Manager 用の個別の例を示します。

ユーザー・プロフィールでの写真の表示

ユーザー・プロフィールのヘッダー・パネルに写真を表示できます。関連する属性に対するセルフサービス権限を保持するユーザーは、自分の写真を管理できます。

ID システムに写真を格納する場合、次の 2 つの方法があります。

- LDAP ディレクトリを使用します。
- ファイル・システム内の写真を参照します。

両方の方法を使用することはできません。ディレクトリまたはファイル・システムのいずれかにすべての写真を格納する必要があります。

ディレクトリへの写真のインポートと格納

写真またはその他のイメージをディレクトリに格納する場合、まず Identity Server に写真を配置します。次に、ID システムを使用して、それらの写真をディレクトリにインポートし、属性を写真属性として構成します。独自の属性を作成するか、既存の属性を使用することが可能です。ディレクトリでは、属性をバイナリ型として定義する必要があります。また、ID システムでは、属性を「GIF イメージ」表示タイプの「写真」セマンティック型として定義する必要があります。「GIF イメージ」表示タイプは、GIF 形式と JPEG 形式に対応しており、Web サーバーでサポートされるその他のイメージ・ファイル形式にも対応しています。ユーザーの ID に写真を関連付ける前に、写真のファイル名が「ログイン」セマンティック型の属性の値に基づいていることを確認します。たとえば、「ログイン」セマンティック型が uid 属性に割り当てられている場合、次のファイル名表記規則を使用します。

```
attribute_value_of_uid.gif  
or  
attribute_value_of_uid.jpg  
or  
attribute_value_of_uid.jpeg
```

「ログイン」セマンティック型が uid 以外の属性に割り当てられている場合、かわりにその属性をファイル名に使用します。たとえば、「ログイン」セマンティック型が電子メール属性に割り当てられている場合、写真のファイル名は次のように指定する必要があります。

```
attribute_value_of_mail.gif  
or  
attribute_value_of_mail.jpg  
or  
attribute_value_of_mail.jpeg
```

ファイル拡張子は、Web サーバーでサポートされる画像ファイル形式に準拠します。

ID システムで写真やイメージをインポートすると、ファイルは Base64 形式に変換されます。このデータは、「写真」属性の値となります。ID システムでは、「ログイン」属性と、写真またはイメージ・ファイルの名前を使用して、各ユーザー・エントリに関連付けられた写真を特定します。

次の手順では、ID システムを構成して写真を使用する方法について説明します。

写真を構成してディレクトリにインポートする手順

1. ID システム・コンソールで、「共通構成」をクリックし、次に「オブジェクト・クラス」をクリックします。
2. リストから Person オブジェクト・クラスを選択します。
3. 「属性の変更」をクリックします。
4. 「写真」属性を次のように変更します。
 - 属性: 写真
 - 表示名: 写真
 - セマンティック型: 写真
 - データ型: バイナリ
 - 属性値: 常に単一値属性
 - 表示タイプ: GIF イメージ
5. 変更を保存します。
6. User Manager の「属性アクセス制御」で、この属性に対する読取り権限と書込み権限を割り当てます。

ディレクトリに写真をインポートする手順

1. ID システム・コンソールで、「システム構成」をクリックし、次に「写真」をクリックします。
2. Identity Server に格納されている写真へのパスを指定します。
3. 「保存」をクリックします。

これで、すべての GIF イメージと JPEG イメージがディレクトリにインポートされます。

ファイル・システム内の写真の参照

ユーザー ID 用のイメージおよび写真を格納するもう 1 つの方法は、写真をディレクトリとは別の場所に格納することです。この方法は、GIF イメージと JPEG イメージに適しており、Web サーバーでサポートされるその他のイメージ・ファイル形式にも対応しています。ファイルの格納場所には、Identity Server の WebPass でアクセスできる必要があります。写真またはイメージ・ファイルの名前には、Web サーバーで認識およびサポートされる有効なファイル名を使用します。ファイル名に空白などの特殊文字を使用することは避けてください。特殊文字を使用したファイル名は、Web サーバーで認識されない可能性があります。

ファイル・システムに存在する写真を参照する手順

1. ID システム・コンソールで、「共通構成」→「オブジェクト・クラス」をクリックします。
2. 「オブジェクト・クラス」リストで、Person オブジェクト・クラスをクリックします。
3. 「属性の変更」をクリックします。
4. 写真パス属性を次のように変更します。
 - 属性: 写真パス
 - 表示名: 写真
 - セマンティック型: 写真
 - データ型: 文字列 (大 / 小文字を区別)
 - 属性値: 単一値または複数值
 - 表示タイプ: GIF イメージ URL
5. この属性に対する読取り権限と書込み権限を割り当てます。

6. 次のディレクトリに GIF または JPEG 形式でイメージを格納します。

```
WebPass_install_dir/identity/oblix/lan/langTag/style0
```

ここで、*WebPass_install_dir* は WebPass がインストールされているディレクトリであり、*langTag* は使用中の特定の言語が含まれるフォルダです。

7. 各ユーザーの「ユーザー・プロファイル」ページで写真の場所の URL を入力します。

たとえば、イメージが次の場所にある場合：

```
c:¥COREId¥WebComponent¥identity¥oblix¥apps¥lang¥en-us¥style0¥user1.gif
```

写真の場所として次のように設定します。

```
user1.gif
```

写真の URL 属性に複数值を設定すると、複数の GIF イメージを表示できます。

デフォルトの写真イメージ

ID システムには、デフォルトの写真イメージが付属しています。このイメージは、ユーザーに写真イメージが指定されていない場合に表示されます。このイメージは、Identity Server の style0 に CIMAGEdefaultphoto.gif として格納されています。

Organization Manager での「ロケーション」タブの有効化

ID システムでは、デフォルトで Organization Manager に「ロケーション」タブが含まれます。このタブにより、マップを作成し、ユーザーやオブジェクトをそれらのマップ上のロケーションに関連付けることができます。

タスクの概要：ロケーション機能の有効化

1. マスター ID 管理者は、「ロケーション」タブを変更し、User Manager および Organization Manager アプリケーションのプロファイル・ページにロケーション属性を追加します。
2. マスター ID 管理者は、ロケーション属性のアクセス制御を構成します。
3. マスター ID 管理者または委任 ID 管理者は、ロケーションを作成するためのワークフローを構成します。詳細は、[第 5 章「ID 機能とワークフローの連携」](#)を参照してください。
4. 委任 ID 管理者は、新規ロケーションを作成し、必要に応じて他のロケーションに関連付けられたロケーション階層を確立します。
5. 委任 ID 管理者またはユーザーは、ユーザー・プロファイルまたはオブジェクト・プロファイルにロケーション属性の値を割り当てます。

これで、適切な権限を保持するユーザーは、ユーザーまたはオブジェクトのロケーションを参照できます。

Group Manager でグループを作成する権限

グループの作成ワークフローを定義するときに、グループを作成する権限をユーザーに割り当てます。グループを作成できるのは、ワークフローの参加者として指定されたユーザーのみです。ワークフローの作成方法の詳細は、第 5 章「ID 機能とワークフローの連携」を参照してください。

ユーザーにグループ・タイプを変更する権限を付与できるのは、ユーザーがそのグループ・タイプに対応するグループの作成ワークフローの参加者である場合です。また、ユーザーは、そのグループ・タイプ属性に対する書き込み権限も保持している必要があります。グループ・タイプの詳細は、4-9 ページの「Group Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加」を参照してください。グループ・タイプ属性の変更権限を割り当てる方法の詳細は、4-31 ページの「LDAP 属性権限の設定と変更」を参照してください。

複数の Active Directory インスタンスで ID システムを実行し、動的フィルタを使用してグループを作成する場合、フィルタ属性は複数値属性である必要があります。

NDS ディレクトリで ID システムを実行している場合に「保存」をクリックすると、グループのメンバーとして選択したユーザーがページから消去されます。この状況を回避するには、NDS ディレクトリに移動し、`uniquemember` が最初に読み取られるよう属性の順序を変更します。また、`userCertificate` 属性が NDS の `userCertificate;binary` 属性より前に出現していることを確認します。

エンド・ユーザーの使用例

次の各項では、エンド・ユーザーが構成後の Group Manager アプリケーションとどのようにやり取りするかについて説明します。

- [Group Manager](#) でのグループ・メンバーの管理
- [グループ・メンバーの検索](#)
- [グループ・メンバーの削除](#)
- [グループ・メンバーの追加](#)
- [グループ・サブスクリプションの管理](#)
- [グループへのサブスクライブ](#)

Group Manager でのグループ・メンバーの管理

グループ・メンバーは、「グループ・プロフィール」ページで参照および管理できます（マスター ID 管理者がグループ・メンバー属性を選択して「グループ・プロフィール」ページに表示している場合）。詳細は、4-11 ページの「タブのプロファイル・ページおよびパネルの構成」を参照してください。

グループに大規模なメンバー・リストが含まれると、システム・パフォーマンスに悪影響を及ぼす可能性があります。マスター ID 管理者は、「グループ・プロフィール」ページにグループ・メンバーを表示しないよう選択できます。4-10 ページの「Group Manager タブのオプションの構成」を参照してください。

注意： グループ・メンバーは、「グループ・メンバーの管理」ページでも参照および管理できます。大規模な静的グループを管理する場合は、「グループ・メンバーの管理」ページを使用することをお勧めします。このページは、1000 以上のメンバーを含むグループの管理用に最適化されているためです。これにより、「グループ・プロフィール」ページの一部としてメンバー・セマンティック属性を定義する場合とは対照的に、大規模グループを管理する際のパフォーマンスが大幅に向上します。

グループ・メンバーの検索

「グループ・メンバーの管理」ページでは、指定した基準に従ってグループのメンバーを参照できます。このページには、次の各表が含まれます。

- 静的メンバー
- 動的メンバー
- ネストされたメンバー

検索結果は、Group Manager および User Manager アプリケーションに構成されている検索ベースと属性アクセス制御に応じて変化します。詳細は、4-31 ページの「LDAP 属性権限の設定と変更」を参照してください。

ユーザーがグループの動的メンバー属性に対する読取り権限を保持していない場合、動的メンバー表には何も表示されず、「動的メンバーに対する読取り権限がありません」というエラー・メッセージが表示されます。

ネストされたメンバー表では、グループ内にネストされた動的グループが含まれる場合に、ユーザーがネストされた一部のグループの動的メンバー属性に対する読取り権限を保持していないと、動的メンバーは表示されません。この場合、エラー・メッセージは表示されません。

グループを表示する手順

1. ID システム・コンソールで、「Group Manager」タブをクリックします。
2. ページ上部の「検索」フィールドに検索基準を入力します。
3. 「実行」をクリックします。
グループのリストが表示されます。
4. 表示するグループ名のリンクをクリックします。

グループ・メンバーを表示する手順

1. Group Manager で、「グループ」をクリックします。
2. グループ検索を実行し、適切なリンクをクリックします。
グループ・プロフィールが表示されます。
3. 「グループ・メンバーの管理」をクリックします。
4. このグループで検索するメンバー・タイプを次のように選択します。
 - ユーザーを検索するには、「人々」を選択します。検索結果には、静的ユーザー、ネストされたユーザー、および動的ユーザーが含まれます。
 - グループを検索するには、「グループ」を選択します。検索結果には、ネストされた静的グループおよび動的グループが含まれます。
5. 「次の基準でメンバーを検索します」リストで、検索の基準とする属性を選択します。
6. 検索演算子を選択します。
7. 検索基準を入力します。
8. 「実行」をクリックします。

「グループ・メンバーの管理」ページに、2つのレベルのネストされたグループとそのメンバーが検索結果として表示されます。これには、ネストされた子グループ、そのメンバー、およびその子が含まれます。

グループ・メンバーの削除

検索結果に表示されるグループ・メンバーは、「グループ・メンバーの管理」ページで削除できます。削除できるのは、静的メンバーのみです。動的メンバーやネストされたメンバーは削除できません。

グループ・メンバーを削除する手順

1. 「グループ・メンバーの管理」ページでグループ・メンバーを検索します。
4-39 ページの「[グループ・メンバーの検索](#)」を参照してください。
2. 検索で戻された結果内で、削除するユーザーまたはグループのリンクをクリックします。
3. 「グループ・メンバーの管理」ページの「保存」をクリックします。

グループ・メンバーの追加

グループにメンバーを追加できます。

グループ・メンバーを追加する手順

1. 「グループ・メンバーの管理」ページに移動します（4-39 ページの「[グループ・メンバーの検索](#)」を参照してください）。
2. 「グループ・メンバーの管理」ページで、「追加するメンバー」フィールドの横の「メンバーの選択」ボタンをクリックします。
「セレクトタ」ページが表示されます。詳細は、1-11 ページの「[セレクトタ](#)」を参照してください。
3. 「セレクトタ」ページで、次の操作を実行します。
 - このグループにユーザーを追加する場合、個人メンバー・タイプを選択します。
 - このグループにネストされたグループを追加する場合、グループ・メンバー・タイプを選択します。
4. 追加するメンバーごとに「追加」をクリックします。
5. 「完了」をクリックします。
6. 「グループ・メンバーの管理」ページの「保存」をクリックします。

グループ・サブスクリプションの管理

Group Manager では、グループを対象としたサブスクリライブとサブスクリライブ解除が可能です。

サブスクリプション・ポリシーを含むことができるのは、拡張グループとして構成されたグループのみです。グループ操作に必要とされる属性を提供するため、ID システムには oblixAdvancedGroup が付属しています。表 4-5 に、oblixAdvancedGroup の内容を示します。

表 4-5 oblixAdvancedGroup の内容

属性	特性
obGroupAdministrator	表示名: グループ管理者 セマンティック型: グループ管理者 表示タイプ: オブジェクト・セレクタ
obGroupDynamicFilter	表示名: 動的フィルタ セマンティック型: グループ動的メンバー 表示タイプ: フィルタ・ビルダー
obGroupExpandedDynamic	表示名: グループ拡張 セマンティック型: なし 表示タイプ: ラジオ・ボタン コメント: この属性は、拡張動的グループに使用されます。
obGroupPureDynamic	表示名: 動的メンバーのみ セマンティック型: なし 表示タイプ: ラジオ・ボタン コメント: この属性は、グループが完全な動的グループであるかどうかを示します。これは、サブスクリプションに関連します。
obGroupSimplifiedAccess Control	表示名: グループ・アクセス セマンティック型: なし 表示タイプ: ラジオ・ボタン コメント: この属性は、グループ・ワークフローの作成に使用されます。これにより、簡易アクセス制御機能が管理されます。
obGroupSubscribeMessage	表示名: サブスクリプション・メッセージ セマンティック型: なし 表示タイプ: 複数行テキスト コメント: この属性は、サブスクリプション通知に使用されます。
obGroupSubscribe Notification	表示名: 通知 セマンティック型: なし 表示タイプ: チェック・ボックス コメント: この属性は、サブスクリプション通知に使用されます。
obGroupSubscriptionFilter	表示名: サブスクリプション・フィルタ セマンティック型: なし 表示タイプ: フィルタ・ビルダー コメント: この属性は、フィルタを使用したグループ・サブスクリプションに使用されます。

表 4-5 oblixAdvancedGroup の内容 (続き)

属性	特性
obGroupSubscriptionType	表示名: サブスクリプション・ポリシー セマンティック型: なし 表示タイプ: 選択メニュー コメント: この属性は、グループ・サブスクリプションに使用されます。
obGroupUnsubscribeMessage	表示名: メッセージのサブスクライブ解除 セマンティック型: なし 表示タイプ: 複数行テキスト

注意: 1人以上のメンバーを含む静的グループを作成し、その後「動的メンバーのみ」フラグを true に設定するようグループを変更すると、ID システムでは警告が生成されません。

グループへのサブスクライブ

ユーザーがグループにサブスクライブするには、次の3つの方法があります (マスター ID 管理者がそのグループのグループ・サブスクリプション・ポリシーを構成している場合)。

- Group Manager の「グループ・プロフィール」ページ
ユーザーは、プロフィールに表示されている選択されたグループにサブスクライブできません。
- ユーザーの作成ワークフローの最後のステップ
ユーザーは、ユーザーの作成ワークフローの最後のステップで複数のグループにサブスクライブできます。詳細は、[第5章「ID機能とワークフローの連携」](#)を参照してください。
- Group Manager の「サブスクリプションの管理」ページ
ユーザーは、「サブスクリプションの管理」ページで複数のグループにサブスクライブできます。

グループにサブスクライブする手順

1. ID システム・コンソールで、「Group Manager」タブをクリックします。
2. 検索バーを使用してグループ検索を実行します。
3. サブスクライブするグループのリンクをクリックします。
4. 「登録」をクリックします。

複数のグループにサブスクライブする手順

1. Group Manager アプリケーションで、「サブスクリプションの管理」をクリックします。
2. 検索バーを使用してグループ検索を実行します。
3. 「サブスクリプション対象グループ」ページで、サブスクライブする各グループの横のボックスを選択します。
4. 「サブスクリプションの管理」ページの下部にある「サブスクリプションの保存」をクリックします。

サブスクライブ済のグループのリストが表示されます。内容は次のとおりです。

- オープン・サブスクリプション・ポリシーが存在するすべてのグループ。
- フィルタ・サブスクリプション・ポリシーが存在し、そのフィルタ基準がユーザーにより満たされているすべてのグループ。
- ワークフロー・サブスクリプション・ポリシーを通じて制御されるすべてのグループ（ユーザーがこれらのグループに適用される属性変更ワークフローの開始ステップの参加者である場合）。

監査ポリシーの構成

各 ID アプリケーションで実行されたユーザー・アクションに関する情報を取得できます。取得された情報は、ID システム・イベントの監査として格納されます。

監査ポリシーは、アプリケーションごとに構成します。これらの設定により、監査ファイルに取得されるデータが決定されます。Identity Server ごとに監査ファイルの出力場所を構成します。監査ファイルのパスを変更する方法の詳細は、7-15 ページの「[Identity Server の管理](#)」を参照してください。

監査ポリシーの表示

監査ポリシーは、各 ID システム・アプリケーションで表示できます。

監査ポリシーを表示する手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Org. Manager 構成」をクリックし、次に「監査ポリシー」をクリックします。

次の情報を含む「アプリケーション監査ポリシーの構成」ページが表示されます。

項目	説明
プロファイル属性	このアプリケーションにプロファイル属性が構成されている場合にのみ表示されます。
イベント名	監査対象の ID システム操作です。
アプリケーション監査有効	このイベントの監査を有効化するかどうかを示します。
監査成功	イベントの成功を監査するかどうかを示します。
監査失敗	イベントの失敗を監査するかどうかを示します。

監査ポリシーの変更

適切な権限を保持している場合、表示可能な監査ポリシーを変更できます。これらの設定は、ID システム・コンソールの「共通構成」の「グローバル監査ポリシー」に含まれる「グローバル監査ポリシー」機能とは重複しません。

監査ポリシーを設定または変更する手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Organization Manager 構成」→「監査ポリシー」をクリックします。
2. 「変更」をクリックします。
「アプリケーション監査ポリシーの変更」ページが表示されます。
3. 「プロファイル属性」リストで、監査対象のイベントを起動する可能性のある属性を選択します。
4. 「アプリケーション監査有効」列で、監査を有効化する各イベントを選択します。
5. 「監査成功」列と「監査失敗」列で、監査する各イベントを選択します。
たとえば、すべての「ロケーションの変更」イベントを監査すると同時に、「プロファイルの表示」イベントの失敗のみを監査できます。
6. 「保存」をクリックします。
前のページに戻ります。

レポートの生成

レポートを使用すると、オブジェクト・クラスに関する情報を表示できます。レポートは、検索のかわりに使用できる方法であり、検索で表示されない属性を出力できます。

レポートの構成

マスター ID 管理者は、ユーザーが User Manager アプリケーションでレポートを表示できるように、ID システム・コンソールでレポートを定義する必要があります。

たとえば、4-3 ページの「[タブ構成情報の表示と変更](#)」の手順に従って User Manager で「従業員」タブを構成すると、特定の建物内の従業員、特定の役職名の従業員、または特定の部門に属する従業員のリストを含むレポートを作成できます。

レポート機能では、クエリー・ビルダーを使用して、基本検索では使用できない複雑な検索基準を定義できます。これにより、基本検索では対応できない様々なタイプの属性を詳細に指定して検索できます。レポートには、次の2つのタイプがあります。

- **非定型レポート**：エンド・ユーザーによって User Manager、Group Manager および Organization Manager アプリケーションで作成されます。この場合、クエリー・ビルダーには、タブで構成されている検索可能属性と、サポートされるその他の表示タイプが含まれます（次の「注意」を参照してください）。
- **事前定義レポート**：管理者によってシステム・コンソールで作成されます。この場合、クエリー・ビルダーには、（タブで検索可能であるとマークされているかどうかにかかわらず）サポートされるすべての表示タイプのすべての属性が含まれます。

注意：クエリー・ビルダーでは、単一行テキスト、複数行テキスト、ラジオ・ボタン、選択リスト、チェック・ボックス、ブール、日付、メール・アドレス、電話番号、セレクト、住所および数値文字列に対応する表示タイプを備えた属性を対象にフィルタを作成できます。

レポートを構成する手順

1. ID システム・コンソールで、「User Manager 構成」 → 「レポート」 → 「レポートのリスト表示」をクリックします。

レポートを最初に作成する場合、次のページが表示されます。

ORACLE Identity Administration

ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager 構成 | Group Manager 構成 | Org. Manager 構成 | 共通構成

ログイン・ユーザー: Master Admin

- タブ
- レポート
- 監査ポリシー

レポートの構成
それぞれの User Manager タブのレポートが、作成、変更、公開および削除できます。該当タブに現在構成済のレポートをすべて表示するには、タブを選択して「レポートのリスト表示」をクリックします。

レポートのリスト表示:

レポート
現在使用できる定義済レポートはありません。

2. 「追加」をクリックして「レポートの構成」ページにクイック・ビルダーを表示します。
3. レポート基準に従って最初の属性を選択し、「追加」をクリックします。
4. 属性の横のフィールドで、適切な方法を選択します。
5. レポート基準を入力します。
この基準の形式は、属性の表示タイプに応じて変化します。
6. このレポートに別の属性を追加する場合は、手順 3～6 を繰り返します。

注意： レポートで複数の属性を選択する場合、AND 演算子と OR 演算子のいずれかを選択する必要があります。この手順のサンプル・ページを参照してください。

7. 「テスト」をクリックし、レポートでデータが正しく生成されるかどうかを検証します。
検証ページが表示されます。

- 「保存」をクリックします。

次のようなページが表示されます。いくつかのボタンが使用可能となります（次のスクリーン・ショットでハイライト表示されています）。これらのボタンは、次の手順で使用します。

レポートの構成
それぞれのUser Managerタブのレポートが、作成、変更、公開および削除できます。該当タブに現在構成済のレポートをすべて表示するには、タブを選択して「レポートのリスト表示」をクリックします。

レポートのリスト表示:

レポート
12の結果のうち1から8を表示しています。

フルネーム	組織単位	電話番号	役職	ログイン
Borneto Avellaneda	Human Resource Los Angeles Corporate HQ	714 372-5085	Director	bavellan
Dee Aimon	Sales San Jose Dealer1k4 Mercury	415 717-5707	Manager	dairmon

- 「次へ」をクリックして追加のレポート結果を表示するか、「公開」をクリックしてレポートを保存します。

レポートの書式設定を変更する手順

- 「レポート」ページで、「カスタマイズ」をクリックしてレポートの列ヘッダーをカスタマイズします。
- 表示されるフォームで列名をカスタマイズし、「保存」をクリックします。
- 「公開」ボタンをクリックします。
- このレポートの名前とオプションの説明を入力します。
- 「保存」をクリックして、このレポートを User Manager アプリケーションの「レポート」タブで使用できるようにします。

レポートの表示、変更、ローカライズおよび削除

レポートの表示は、アクセス制御と検索ベースの設定に準拠します。

適切な言語パックをインストールしており、各言語の構成を完了している場合、レポートの名前や説明を複数の言語で表示できます。詳細は、7-7 ページの「[Oracle Access Manager での複数の言語の構成](#)」を参照してください。

生成されたレポートを ID システム・アプリケーションでエクスポートする際に、レポートの値に非 ASCII 文字が含まれる場合、.txt 拡張子を使用してファイル名を変更する必要があります。これにより、Excel のインポート・ウィザードで使用可能となり、非 ASCII 文字は正しく表示されます。

OpenOffice で開かれた .csv ファイルは、インポート・ウィザードで使用できます。このアプリケーションでは、ファイル名を *.txt に変更することなくエンコーディングを選択できます。

レポートを表示または変更する手順

1. ID システム・コンソールで、「User Manager 構成」をクリックし、次に「レポート」をクリックします。
2. 表示または変更するレポートのタイプをリストから選択します。
3. 「レポートのリスト表示」をクリックします。
4. 表示するレポートのリンクを選択します。
5. 「カスタマイズ」ボタンをクリックしてレポート基準を変更します。
6. 「保存」をクリックして新規レポート形式を保存します。

他のユーザーが参照できるようにレポートを公開する方法の詳細は、4-44 ページの「[レポートの構成](#)」を参照してください。

レポートをローカライズする手順

1. ID システム・コンソールで、「User Manager 構成」をクリックし、次に「レポート」をクリックします。
2. 「レポートのリスト表示」をクリックします。
既存のすべてのレポートがページにリストされます。
3. ローカライズするレポートをクリックします。
レポートの詳細がページに表示されます。
4. 「公開」をクリックします。
「レポートの公開」ページが表示されます。このページには、すべてのインストール済言語のリンクが含まれます。
5. レポートを公開する言語をクリックします。
6. 「レポート名」フィールドに、選択した言語で表示名を入力します。
7. 「レポート説明」フィールドに、レポートの簡単な説明を入力します。
この情報はオプションです。
8. 「保存」をクリックして変更を保存します。
User Manager にレポートが表示されます。

レポートを削除する手順

1. ID システム・コンソールで、「User Manager 構成」をクリックし、次に「レポート」をクリックします。
2. 削除するレポートを含むタブを選択します。
3. 「レポートのリスト表示」をクリックします。
4. レポート名の横の「-」アイコンを選択してレポートを削除します。

拡張構成

次の各項では、動的グループの拡張、ディレクトリ検索の有効範囲の制限、および XML ファイルの編集による属性権限の構成について説明します。

動的グループの拡張

グループのメンバーシップが LDAP フィルタにより決定される場合、グループを拡張することで静的メンバーシップ・リストを生成できます。静的リストの生成により、ID システムでは、グループ・アクセスごとに LDAP フィルタを実行する必要がなくなります。

グループ拡張では、動的メンバーシップを指定する LDAP ルールを実行し、その結果を静的メンバー属性に格納することで静的リストを更新します。多くの ID システム機能で、グループのメンバーシップがテストされます。静的メンバーシップのテストは動的メンバーシップのテストより高速であるため、静的リストでメンバーを検索することが推奨されます。また、サード・パーティ・アプリケーションでチェックできるのは、静的メンバーシップのみである場合があります。サード・パーティ・アプリケーションの場合、頻繁に拡張を行うことで静的メンバーシップを正確に維持します。

グループ拡張操作は、それ自体がコストのかかるプロセスです。ただし、バックグラウンド・プロセスとしてグループを拡張することで、ユーザーへの影響を回避できます。

注意： 静的メンバーが含まれる動的グループを拡張する場合、静的メンバーの元のリストは、フィルタ基準を現在満たしているメンバーにより上書きされます。この動作は、「動的メンバーのみ」のフラグを `false` に設定している場合でも適用されます。フィルタは、他のグループ設定より優先されます。

グループを拡張するには、次の 2 つの条件が満たされている必要があります。

- `obgroupexpandeddynamic` 属性が `true` に設定されている必要があります。
- グループを拡張するユーザーは、`obgroupexpandeddynamic` 属性と `obgroupdynamicfilter` 属性に対する読取り権限を保持している必要があります。また、「グループ静的メンバー」セマンティック型が割り当てられた属性に対する書込み権限も保持している必要があります。

ID システムが提供するグループ属性の詳細は、4-41 ページの「[グループ・サブスクリプションの管理](#)」の表を参照してください。

動的グループを拡張する手順

1. Group Manager で、ページ上部の「構成」オプションをクリックします。
「構成」ページが表示されます。
2. 「動的グループの拡張」をクリックします。
「動的グループの拡張」ページが表示されます。
3. 次のいずれかのオプションを選択します。
 - 1つ以上のグループを選択するには、「グループ別」を選択して「グループの選択」をクリックします。
 - すべてのグループを拡張するには、「すべて」を選択します。
4. 「開く」をクリックします。
「拡張されたグループ」ページに、拡張されたすべてのグループのリストが表示されます。
5. グループ・リンクをクリックして、そのグループの「グループ・プロフィール」ページを表示します。
6. 「完了」をクリックします。

検索ベースのデフォルト有効範囲の変更

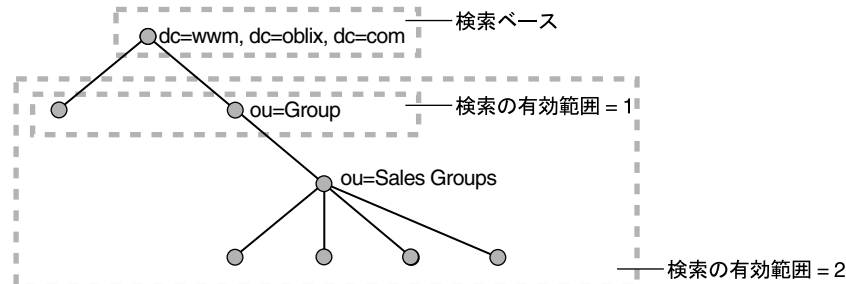
ID システムの一部の機能では、外部の XML ファイルを呼び出して構成情報を取得します。globalparams.xml ファイルは、そのようなファイルの1つです。このファイルにより、特に検索の有効範囲を制御できます。

デフォルトでは、検索の有効範囲は ID システムのサブツリーに設定されており、検索は検索ベースの開始ポイントから始まってその子までを含みます。ディレクトリのサイズによっては、ResourceFilterSearchScope パラメータを使用して検索のデフォルト有効範囲を変更できます。このパラメータに使用可能な値は、次のとおりです。

- 1: 検索ベースの最上位ノードと、その1つ下のレベルが検索されます。
- 2: 検索ベースの最上位ノードから始まり、最下位ノードまで検索されます。

図 4-1 は、ResourceFilterSearchScope の設定が 1 の場合には戻されるエントリが少数に限定される一方で、2 の場合には大量のエントリが戻されることを示しています。

図 4-1 検索の有効範囲オプション



globalparams.xml ファイルを設定する手順

1. 次のディレクトリで globalparams.xml ファイルを見つけます。
`IdentityServer_install_dir/identity/oblix/apps/common/bin`
2. ファイルをバックアップします。
3. メモ帳などの ASCII エディタまたは XML エディタでファイルを開きます。
4. ResourceFilterSearchScope パラメータを見つけ、その値を変更します。
5. WebPass および Identity Server を再起動します。

グループの簡易属性権限

簡易属性権限を使用すると、グループ作成者は、4-31 ページの「LDAP 属性権限の設定と変更」の手順に従って各属性の権限を設定することなく、読取り、書込みおよび通知の各権限を選択できます。

簡易権限は、ポリシーの管理ドメインが新規グループの DN である新規作成グループに適用されます。これらのポリシーは、後からアクセス制御機能を通じて変更できます。

簡易権限の実装

管理者は、必要に応じて希望する数の簡易権限のセットを構成できます。権限は、`IdentityServer_install_dir/oblix/apps/groupservcenter/bin/gscacparams.xml` ファイルで作成します。

このファイルには、モデルが適用されるロール、ユーザー、グループを定義するための埋込みの複合リスト、割当て権限、および権限が適用される属性が含まれます。このファイルが新規グループに適用されると、ファイル内の権限ごとにアクセス制御エントリが作成されます。

gscacparams.xml ファイルの例

次に、gscacparams.xml ファイルの権限セットの例を示します。モデル名は、Public です。

- エントリ 1 の設定では、ロールは `ob_any`、権限は読取り、属性は `description`、`uniquemember` および `owner` です。
- エントリ 2 の設定では、ロールは `owner`、権限は書込み、属性は `description`、`uniquemember` および `owner` です。

例 4-1

```
<?xml version="1.0"?>
<ParamsCtrl xmlns="http(s)://www.oblix.com" CtrlName="gscacparams">
<!--#----->
<!-- #Access Control Functions -->
<!--#----->
<!--#----->
<!-- # Public access -->
<!--#----->
<CompoundList ListName="">
<CompoundList ListName="Public">
<CompoundList ListName="entry1">
<ValList ListName="roles" >
<ValListMember Value="ob_any">
</ValList>
<ValList ListName="rights" >
<ValListMember Value="READ" Operation="Add"/>
</ValList>
<ValList ListName="attributes" >
<ValListMember Value="description"/>
<ValListMember Value="cn"/>
<ValListMember Value="uniquemember"/>
```

```

<VallistMember Value="owner"/>
</Vallist>
</CompoundList>
<CompoundList ListName="entry2">
<Vallist ListName="roles" >
<VallistMember Value="owner" Operation="Add"/>
</Vallist>
<Vallist ListName="rights" >
<VallistMember Value="WRITE" Operation="Add"/>
</Vallist>
<Vallist ListName="attributes" >
<VallistMember Value="description" Operation="Add"/>
<VallistMember Value="cn" Operation="Add"/>
<VallistMember Value="uniquemember" Operation="Add"/>
<VallistMember Value="owner" Operation="Add"/>
</Vallist>
</CompoundList>

```

簡易権限の予約語

次の表に、簡易権限の予約語をまとめます。

予約語	使用頻度	説明
rights	エントリごとに1つ	読取り、変更または通知の各権限を指定します。
attributes	エントリごとに1つ	属性を指定するリスト。任意のグループ・オブジェクト属性をリストに追加できます。
roles	エントリごとに1つ	エントリを適用するロール。ロールには、uniquemember、owner、ob_any、ob_anonymousなどの事前定義ロールを使用できます。
people	エントリごとに1つ	このエントリを適用する識別名を指定します。
source	モデルごとに1つ	このモデルを参照するユーザーのベース UID を指定します。ベース UID を指定しない場合、すべてのユーザーがこのエントリを参照できます。
target	モデルごとに1つ	このモデルを適用するターゲットのベース UID を指定します。グループがこのベースの一部ではない場合、権限は設定できません。

Organization Manager でのコンテナ制限の設定

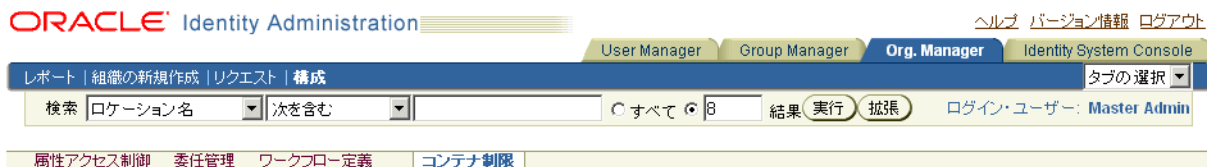
「コンテナ制限」機能を使用すると、組織単位とそのオブジェクト・クラスのオブジェクト（および子オブジェクト）の数を制御できます。管理者は、制限に到達しそうになったときに通知するユーザーを定義できます。たとえば、エクストラネットの顧客を格納しているディレクトリ・ツリーの組織単位があるとします。このとき、エクストラネットのポータルにアクセスする顧客の数を 10,000 人に制限できます。

注意：「コンテナ制限」機能では、ディレクトリのオブジェクト数をカウントします。オブジェクト数が大量であると、パフォーマンスが影響を受ける可能性があります。

コンテナ制限を表示および追加する手順

1. ID システム・コンソールで、「Org. Manager」タブをクリックし、次に「構成」→「コンテナ制限」をクリックします。

「コンテナ制限」ページが表示されます。



コンテナ制限

1) 管理
ドメイン

オブジェクト・クラスにコンテナ制限を追加

現在の数

オブジェクト・クラス	1	合計
geninventoryobject	0	626
gensiteorgperson	9	718
groupOfUniqueNames	5	243
oblxllocation	0	0
organizationalunit	3	239

すべて表示

2) オブジェクト・クラス: oblxlocation [追加]

オブジェクト・クラス	コンテナ制限	強制	通知
gensiteorgperson	1		

変更 削除 すべて削除 コピー 貼付け

レポート

この例では、ページ内の「現在の数」表から、gensiteOrgPerson オブジェクト・クラスが DIT の現在のレベルに 9 個の子を格納しており、そのレベル以下に合計 718 個の子を格納していることがわかります。

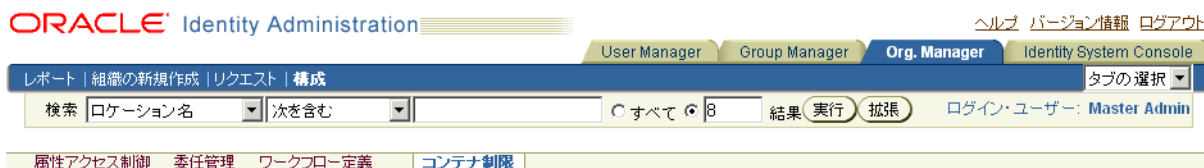
2. 「管理ドメイン」ボックスで、表示する DIT エントリを選択します。

「現在の数」ボックスに、選択したエントリに関連付けられたすべての構成済構造化クラスと、その子の数が表示されます。

「オブジェクト・クラス」表に、選択した DIT エントリのコンテナ制限、強制および通知ポリシーがオブジェクト・クラスごとにリストされます。

- 「オブジェクト・クラス」リストでオブジェクト・クラスを選択し、「追加」をクリックしてコンテナ制限を追加します。

2 番目の「コンテナ制限」ページが表示されます。このページには、前の画面で選択した管理ドメインとオブジェクト・クラスが含まれます。



コンテナ制限

管理ドメイン	<input type="text" value="o=company,c=us"/>
オブジェクト・クラス	<input type="text" value="groupOfUniqueNames"/>
コンテナ制限	<input type="checkbox"/> <input type="checkbox"/> 使い果たした場合に通知 <input type="text" value=""/> %
	<input type="checkbox"/> 下位ポリシーのオーバーライド
ルール	<input type="button" value="フィルタの作成"/> <input type="text"/>
人々	<input type="button" value="ユーザーの選択"/> <input type="text"/>
グループ	<input type="button" value="グループの選択"/> <input type="text"/>

- 「コンテナ制限」ボックスに、このオブジェクト・クラスでこの DIT レベルに格納する子の最大数を指定します。
- オブジェクト・クラスがコンテナ制限に近づいたことを電子メールで誰かに通知する場合、「使い果たした場合に通知」を選択し、電子メールを送信するときの制限割合を指定します。
- DIT のより下位のポリシーで上書きされないコンテナ制限を作成する場合、「下位ポリシーのオーバーライド」を選択します。
- 次のオプションを 1 つ以上使用して、コンテナ制限の警告を受信するユーザーを指定します。
 - 「フィルタの作成」を選択し、クエリー・ビルダーを使用してルールを作成します。
 - 「ユーザーの選択」をクリックし、セレクタを使用して 1 人以上のユーザーを指定します。
 - 「グループの選択」をクリックし、セレクタを使用して 1 つ以上のグループを指定します。

「ユーザー」、「ルール」および「ルール」フィールドには、OR 関係が適用されます。どのフィールドに指定したユーザーにも通知が実行されます。

- 「保存」をクリックしてコンテナ制限を保存し、「オブジェクト・クラス」表に追加します。

コンテナ制限のコピー

コンテナ制限は、あるドメインから別のドメインにコピーできます。

あるドメインから別のドメインにコンテナ制限をコピーする手順

1. Organization Manager で、「構成」をクリックし、次に「コンテナ制限」をクリックします。
「コンテナ制限」画面が表示されます。
2. 「管理ドメイン」ボックスで、表示するディレクトリ情報ツリー (DIT) のエントリを選択します。
「現在の数」ボックスに、選択したエントリに関連付けられた構造化クラスと、その子の数が表示されます。
「オブジェクト・クラスにコンテナ制限を追加」の表に、現在選択されている DIT エントリのコンテナ制限、強制および通知ポリシーがオブジェクト・クラスごとにリストされます。
3. 「コピー」をクリックします。
4. 「管理ドメイン」ボックスで、コンテナ制限を追加する宛先エントリの場所を指定します。
5. 「貼付け」をクリックします。
コンテナ制限ポリシーが選択した DIT エントリに追加されます。

コンテナ制限の変更

コンテナ制限は変更できます。4-52 ページの「[Organization Manager でのコンテナ制限の設定](#)」を参照してください。

コンテナ制限を変更する手順

1. Organization Manager で、「構成」をクリックします。
「構成」画面が表示されます。
2. 「コンテナ制限」をクリックします。
「コンテナ制限」画面が表示されます。
3. 「管理ドメイン」ボックスで、表示する DIT エントリを選択します。
「現在の数」ボックスに、選択したエントリに関連付けられたすべての構成済構造化クラスと、その子の数が表示されます。
4. 「オブジェクト・クラスにコンテナ制限を追加」パネルで、「オブジェクト・クラス」列からオブジェクト・クラスを選択します。
5. 「変更」をクリックします。
2 番目の「コンテナ制限」画面が表示されます。
6. 変更作業を行います。
各フィールドの詳細は、4-52 ページの「[Organization Manager でのコンテナ制限の設定](#)」を参照してください。
7. 「保存」をクリックします。
コンテナ制限は削除できます。

コンテナ制限を削除する手順

1. Organization Manager で、「構成」をクリックし、次に「コンテナ制限」をクリックします。
2. 「管理ドメイン」ボックスで、ディレクトリ情報ツリー (DIT) のエントリを選択します。
「現在の数」ボックスに、選択したエントリに関連付けられたすべての構成済構造化クラスと、その子の数が表示されます。
3. 「オブジェクト・クラスにコンテナ制限を追加」パネルで、オブジェクト・クラスを選択します。
4. 「削除」をクリックします。

オブジェクト・クラスのコンテナ制限が削除されます。

注意：DIT エントリのすべてのコンテナ制限を削除するには、「すべて削除」をクリックします。

ID 機能とワークフローの連携

この章の内容は次のとおりです。

- ワークフローの概要
- クイックスタート・ツールの使用方法
- ワークフロー・アプレットの使用方法
- サブフローの定義
- 拡張ワークフロー・チケット・ルーティング
- 非同期操作の実行
- ワークフローの使用方法
- ワークフローの管理
- 拡張ワークフロー・オプション
- 自己登録ワークフローの作成
- ロケーション・ワークフローの作成

ワークフローの概要

ID システム・ワークフローにより、マスター ID 管理者と委任 ID 管理者は、ID システム機能にビジネス・ロジックを適用できます。ワークフローにより、新規従業員用の福利厚生アカウントおよび電子メール・アカウントの作成や、ディレクトリ内のユーザー・プロフィール属性の変更といった複雑な作業手順の整理統合と自動化が実現します。

各ワークフローは、順序付けられたアクションのチェーンで構成されます。ワークフロー内のすべてのタスク処理を 1 人の担当者に任せるのではなく、特定の作業を処理するのに最も適した専門担当者に各ステップを割り当てるのが可能です。1 つのステップが完了すると、ワークフロー・エンジンにより、順序内の次のステップの担当者にワークフロー・チケットが送信されます。

ワークフロー機能の要約は、次のとおりです。

- ディレクトリでオブジェクトの作成、オブジェクトの削除、および属性の変更を行うプロセスを自動化および標準化できます。
- オブジェクトの作成、オブジェクトの削除、および属性の変更を行う場合に、データ整合性とルールに関するチェックを適用できます。
- バックエンド・アプリケーションをプロビジョニングするためのデータ入力システムとして ID システムを構成できます。

ワークフローの開始方法

ワークフローは、ユーザーにより開始できます。たとえば、新しい従業員は、自己登録ワークフローを開始できます。

ワークフローは、プログラマ的な方法でも開始できます。たとえば、IdentityXML の `workflowSaveCreateProfile` 関数を起動して、ユーザーの作成ワークフローを開始できます。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

ワークフローの URL リンクをコピーして別のアプリケーションのページに埋め込み、Portal Inserts としてアクセスすることもできます。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

典型的なワークフローの例

ワークフローは、通常、ユーザー・アクションまたは自動データ取得の任意の組合せを伴う繰り返し頻度の高い複数ステップのタスクに適しています。各ワークフローは、ID システム・アプリケーションの 1 つと関連付けられます。次に、いくつかの一般的なワークフローをリストします。

- **User Manager:** ワークフローを定義して、ユーザーに自分の部門番号および電話番号の変更を許可できます（マネージャに承認されるまでは保留）。新規ユーザーが作成された場合、そのユーザーに関する情報を適切な人々が外部システムからプログラマ的に取得できます。

別のワークフローでは、新規ユーザーを企業の電子メール・アプリケーションに追加できます。オブジェクト・テンプレート・スキーマを定義している場合、ワークフローを使用してデータを ID システム・アプリケーションからプロビジョニング用としてバックエンド・アプリケーションに送信できます。オブジェクト・テンプレートの詳細は、第 6 章「外部アプリケーションへの非 LDAP データの送信」を参照してください。

- **Group Manager:** ワークフローを作成して、グループ登録リクエストを承認担当のマネージャにルーティングできます。
- **Organization Manager:** 部品エントリの作成をサプライヤに許可し、サプライヤが追加した各エントリをマネージャが承認するまで保留できます。また、最初にユーザーが新規部品エントリを追加し、次にデータ追加のリクエストを承認担当の適切な人物にルーティングして、最後にその担当者が新規データのディレクトリへのコミットを承認するワークフローを作成できます。

拡張ワークフロー・オプション

ID システム・ワークフローでは、次の拡張機能がサポートされます。

- サブフローを使用すると、複数のワークフロー・アクティビティを並列に実行できます。

たとえば、新規ユーザーを作成するリクエストで2つの異なる部門からの承認が必要とされる場合、2つの部門で同時に承認リクエストを受信できます。詳細は、5-33 ページの「サブフローの定義」を参照してください。

- 特定のワークフロー・ステップを異なる動的参加者にルーティングできます。動的参加者は、実行時に評価される属性値またはビジネス・ロジックに基づいて選択されます。

詳細は、5-36 ページの「動的参加者の指定」を参照してください。

- タスクを割り当てられている正式な参加者が外出やその他の理由により着信チケットを処理できない場合、そのステップの職責をかわりに引き受けるサロゲート（代理人）を指定できます。

詳細は、5-42 ページの「サロゲートの指定」を参照してください。

- 時間ベース・エスカレーションを構成すると、元の参加者が割り当てられたステップを特定の期間内に完了しない場合、ワークフロー・チケットを異なる参加者にルーティングできます。

詳細は、5-45 ページの「時間ベース・エスカレーションの有効化」を参照してください。

- IdentityXML を使用すると、Portal Inserts またはアプリケーションとして任意の Web ページからワークフローを起動できます。

詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

- ワークフロー監査を使用すると、ワークフローの状態をモニターし、プロセス内の各ステップで特定のアクションを実行したユーザーを正確に特定できます。

詳細は、5-54 ページの「ワークフローのモニタリング」を参照してください。

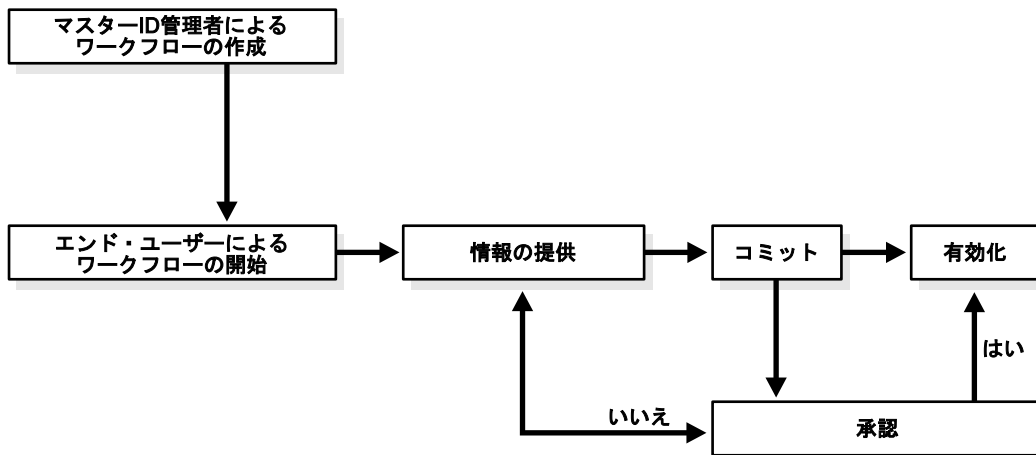
- ユーザー操作を必要としないアクションを実現するため、ワークフロー・ステップを構成して外部ソースから ID システムに必要なデータを自動的に取得できます。

詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

ワークフロー・タイプ

ワークフローには様々なタイプがあります。たとえば、ワークフローのあるタイプでは、既存オブジェクトの1つ以上の属性を変更できます。別のタイプのワークフローでは、新規オブジェクトを作成できます。図 5-1 は、ユーザーの作成ワークフローを示しています。

図 5-1 ユーザーの作成ワークフロー



ワークフローの作成

次に、ワークフローを作成する場合の手順の概要についてまとめます。実際の手順は、属性の変更ワークフローとユーザーの作成ワークフロー（またはグループの作成あるいはオブジェクトの作成ワークフロー）では多少異なります。

タスクの概要：ワークフロー定義の作成

1. 関連する ID システム・アプリケーションのタブにオブジェクトを追加します。
2. オブジェクトの属性を構成します。
3. LDAP 属性に対する読取り権限と書込み権限を構成します。

ワークフローの参加者は、ワークフローの処理中に参照および変更される LDAP 属性に対する適切な読取り権限と書込み権限を保持している必要があります。詳細は、4-21 ページの「ユーザーによる LDAP データの表示および変更の許可」を参照してください。

4. 属性をアプリケーション・パネルに追加します。

この操作は、LDAP 属性とテンプレート属性の両方に適用されます。属性の変更ワークフローの場合、ユーザーは、パネルを含むプロファイル・ページでテンプレート・オブジェクトの属性を参照できません。ただし、テンプレート属性を追加しないと、ワークフローは適切に動作しません。

5. ワークフローを構成します。

属性の変更ワークフローのステップで属性を追加する場合、リストの一番上の属性がプロファイル・ページで構成されている必要があります（詳細は、5-26 ページの「ステップ属性の定義」を参照してください）。一番上の属性が正しく構成されていれば、リスト内の後続の属性は自動的にページに追加されます。

ワークフロー定義により、ワークフローが作成された ID システム・アプリケーションの関連プロファイル・ページの外観が変化します。たとえば、属性の変更ワークフローが正しく構成されると、ターゲット・オブジェクトの「プロファイルの変更」ページに含まれる属性の横に「変更」ボタンが表示されます。ユーザーの作成ワークフローが正しく構成されると、User Manager の「ユーザー ID の作成」を選択したときに適切な属性が表示されます。

ID システム・アプリケーションでユーザーがワークフローにアクセスする方法

ワークフロー定義が作成されると、使用されるワークフロー・タイプに応じて、いずれか1つの方法でワークフローのインスタンスを開始できます。

表 5-1 ワークフローの開始方法

ワークフロー・タイプ	ユーザーがこのワークフローを開始する方法
属性の変更	ユーザーの「プロフィールの変更」ページの「変更をリクエスト」ボタン。
ユーザーの作成	User Manager の「ユーザー ID の作成」リンクからアクセスできる「ユーザー ID の作成」ページ。
ユーザーの非アクティブ化	ユーザーの「プロフィールの表示」ページの「ユーザーの非アクティブ化を開始」ボタン。
ユーザーの再アクティブ化	ユーザーの再アクティブ化ワークフローの作成時に「プロフィールの表示」ページに表示される「ユーザーの再アクティブ化の開始」ボタン。最初に User Manager の「非アクティブなユーザー ID」ページでユーザーを検索する必要があります。 ユーザーの再アクティブ化操作を実行できるのは、ディレクトリ管理者または再アクティブ化権限を保持するユーザーです。
自己登録	このタイプのワークフローを作成すると、ワークフローを開始する URL が生成されます。URL を保存し、自己登録ワークフローを開始する場合にはその URL を使用します。
グループの作成	Group Manager の「グループの作成」リンクからアクセスできる「グループの作成」ページ。
グループの削除	グループの「プロフィールの表示」ページ。
オブジェクトの作成	Organization Manager の「作成」ページ。
オブジェクトの削除	オブジェクトの「プロフィールの表示」ページ。

ワークフロー・チケットの概要

プログラムの実行がワークフローの特定のステップに到達すると、ワークフロー・エンジンによってそのステップ・インスタンスのチケットが作成されます。たとえば、ユーザーの作成ワークフローの場合、ユーザーが User Manager で「ユーザーの作成」機能を選択すると、通常はすぐに IT 部門の特定の参加者にチケットが送信されます。

各ワークフロー・チケットは、最初はリンクの形式で表示されます。参加者がこのリンクをクリックすると、ワークフロー内のそのステップに関連するアクションを実行するよう求められます。たとえば、IT 部門のユーザーがユーザーの作成ワークフローのチケットを処理する場合、通常は新規ユーザーのログイン ID とパスワードを指定するよう求められます。

ワークフローでの各ステップの完了時に、ワークフロー・ログが作成されます。

詳細は、5-50 ページの「[ワークフローの使用法](#)」を参照してください。

たとえば、「ユーザー ID の作成」ページの内容は、ユーザーの作成ワークフローで構成された属性に基づくことがあります。

新規ユーザーに関する情報がこのページに保存されると、ワークフローの開始ステップは完了します。次のスクリーン・ショットは、ワークフロー定義によってこのワークフロー・インスタンスのチケットが生成されたことを示しています。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

プロファイル | レポート | ユーザーIDの作成 | 非アクティブなユーザーID | 代替権限 | リクエスト | 構成

検索 8 ログイン・ユーザー: Master Admin

着信リクエスト 送信リクエスト **リクエストのモニター**

結果

リクエスト番号 65d2ad96207601290000C7837d600000
 リクエストタイプ ユーザーの作成
 アプリケーション名 User Manager
 リクエスト対象 new2
 ステータス 最終ステップ完了
 ワークフロー名 ユーザーの作成 - 基本
 親リクエスト番号

ステップ番号	アクション	アクション実行者	ステータス	サブフロー番号	エスカレーション数
1	開始	Josefa Collins	<input checked="" type="checkbox"/> 完了		
2	有効化	Sri Damodaran	<input checked="" type="checkbox"/> 完了		

このワークフローの参加者は、ワークフロー・ステップに対して生成されたチケットを参照し、新規ユーザーの追加を承認できます。チケット情報は、承認ラベルの横のチケット番号をクリックすることで表示できます。

ワークフローの使用例

ID システムにユーザーを追加するワークフローを作成するとします。この場合、次の手順を実行するユーザーの作成ワークフローを定義できます。

プロセスの概要：ユーザーの作成ワークフローの作成と使用

1. User Manager アプリケーションで、新規ワークフロー定義を作成します。

この例では、ワークフロー定義に3つのステップが存在し、User Manager にログインしている IT 部門の任意のユーザーがそれらのステップを通じて新規ユーザーを作成できます。このワークフローは次のとおりです。

ステップ 1 (開始)：このステップでは、User Manager にログインしているユーザーが、新規ユーザーのデータを入力します。

ステップ 2 (情報と承認の提供)：このステップでは、ユーザーのマネージャが、入力されたユーザーのデータを承認します。

ステップ 3 (アクティブ化)：このステップでは、新規ユーザーをアクティブ化します。

2. ユーザーが User Manager にログインします。
3. ユーザーは、「ユーザーの作成」ボタンを選択します。
ワークフロー・インスタンスにより、新規ユーザーの名前、ユーザー ID、パスワードと、新規ユーザーのマネージャのユーザー ID と電子メールを指定するよう求められます。
4. ワークフロー・インスタンスにより、新規ユーザーの作成リクエストが、新規ユーザーの情報とともにそのユーザーのマネージャにルーティングされます。
5. マネージャは、User Manager アプリケーションの「リクエスト」機能をクリックし、ジョブ・チケットのリンクの形式でリクエストを表示します。
6. マネージャは、チケットのリンクをクリックしてリクエストを表示します。
7. マネージャは、リクエストを承認するために「プロセス」ボタンをクリックします。
8. マネージャは、「プロセス」ページの「承認」ボタンをクリックします。
9. リクエストが処理され、新規ユーザーが ID システムで有効化されます。

新規ユーザーは、各自のディレクトリ・プロファイルと、マスター管理者によってそのプロファイルの属性に割り当てられている権限に応じて、ログイン後に適切な機能を使用できます。詳細は、4-21 ページの「ユーザーによる LDAP データの表示および変更の許可」を参照してください。

ワークフローでの LDAP 属性とテンプレート属性の比較

ワークフローを定義する場合、ほとんどのワークフロー・ステップで次の2つのタイプのオブジェクトおよび属性を使用できます。

- **LDAP オブジェクトおよび属性:** ワークフローを使用して、アプリケーション・プロファイル・ページに構成されているオブジェクトおよび属性を変更できます。ワークフローに参加するユーザーは、これらのオブジェクトおよび属性を表示または変更するための適切な権限を保持している必要があります。
- **テンプレート属性:** ワークフローを使用してバックエンド・アプリケーションをプロビジョニングする場合、テンプレート・スキーマに基づいて情報を追加するワークフロー・ステップを構成します。ワークフロー内でテンプレート属性の値がコミットされたときに、ID イベント API プラグインを使用してこのデータを捕捉し、プロビジョニング用としてバックエンド・アプリケーションに送信します。詳細は、第6章「外部アプリケーションへの非 LDAP データの送信」、および『Oracle Access Manager 開発者ガイド』を参照してください。

リリース 7.0 の時点で、プロビジョニングでは ID システムからバックエンド・システムに向かう一方方向のデータ・フローのみを使用できます。そのため、必要に応じて LDAP ディレクトリとバックエンド・システムの両方にデータを記述するためのプロビジョニング・ワークフローを構成することになります。これにより、ユーザーは、ワークフロー・ターゲットに構成されているデータを参照できます。ただし、バックエンド・アプリケーションに含まれるターゲットの現在の状態を参照するには、アプリケーションまたはそのログにアクセスする必要があります。

プロビジョニング・ワークフローでは、ワークフローを記述するスキーマごとに、「コミット」、「アクティブ化」、「有効化」、「削除」、「無効化」および「非アクティブ化」の個別ステップを用意する必要があります。

ワークフローのタイプ、ステップおよびアクション

ワークフロー・タイプにより、ワークフローの目的（ユーザーの作成など）が決定されます。ワークフロー・ステップは、ワークフローの個々のセグメントです。複数のステップが一連の順序で実行されます。ワークフロー・アクションは、ステップで実行されるアクティビティ（情報を要求するリクエストの発行など）です。

たとえば、ユーザーの作成ワークフロー・タイプでは、ユーザーのディレクトリ・エントリを作成できます。このタイプのワークフローには、ユーザー情報のリクエスト、情報の収集、リクエストの承認などに関するアクションが含まれます。

次の表に、様々なワークフロー・タイプと各 ID システム・アプリケーションの関係を示します。

表 5-2 ワークフロー・タイプ

アプリケーション	ワークフロー・タイプと説明
User Manager	<ul style="list-style-type: none"> ■ ユーザーの作成: ディレクトリにユーザーを追加します。 ■ 自己登録: ユーザーが自分自身をディレクトリに追加できます。 ■ ユーザーの非アクティブ化: ユーザーのログインを禁止し、ID システムでの表示を不可能にします。非アクティブ化の効果は、ユーザーがログアウトした後に反映されます。これにより、ユーザーは将来にわたりシステムにアクセスできなくなります。十分なアクセス権限を保持する管理者は、非アクティブなユーザーを参照し、それらのユーザーを永久に削除するか、再アクティブ化することが可能です。 ■ ユーザーの再アクティブ化: 「ユーザー・プロファイル」ページに「ユーザーの再アクティブ化の開始」ボタンを表示し、非アクティブなユーザーのステータスを変更します。これにより、再アクティブ化されたユーザーは、再びログインして ID システムを使用できます。 ■ 属性の変更: ユーザー・プロファイルの属性値を変更します。このワークフローで指定された属性には、ターゲット・プロファイル・ページに「変更をリクエスト」ボタンが表示されます。
Group Manager	<ul style="list-style-type: none"> ■ グループの作成: ディレクトリにグループを追加します。 ■ グループの削除: ディレクトリからグループを削除します。 ■ 属性の変更: グループ・プロファイルの属性値を変更します。このワークフローで指定された属性には、ターゲット・プロファイル・ページに「変更をリクエスト」ボタンが表示されます。
Organization Manager	<ul style="list-style-type: none"> ■ オブジェクトの作成: ディレクトリにオブジェクトを追加します。 ■ オブジェクトの削除: ディレクトリからオブジェクトを削除します。 ■ 属性の変更: オブジェクト・プロファイルの属性値を変更します。このワークフローで指定された属性には、ターゲット・プロファイル・ページに「変更をリクエスト」ボタンが表示されます。 ■ 自己登録: ユーザーが組織オブジェクトをディレクトリに追加できます。

ワークフロー・ステップの概要

各ワークフローでは、最低 2 つのステップ（ワークフロー・インスタンスを開始するステップとそれを終了するステップ）を定義する必要があります。1 つのステップは、次の要素で構成されます。

- **番号**: このステップの一意的識別子。
- **アクション**: アクションは、ID システムまたは外部システムで実行されるアクティビティです。たとえば、ワークフローの開始、情報の提供、承認のリクエストなどのアクションがあります。詳細は、5-10 ページの「[ステップ・アクションの概要](#)」を参照してください。
- **属性**: 属性値は、ステップの一部として追加または変更できます。

たとえば、ユーザーの電話番号属性の値を変更するステップを定義できます。ステップ属性は、必須属性、オプション属性、または別のワークフロー・ステップの完了時に設定される属性のいずれかです。

ID システム内でローカルに使用する値の場合、ワークフローの一部として LDAP 属性を構成します。バックエンド・アプリケーションにプロビジョニングする場合、ワークフロー・ステップで LDAP 属性とテンプレート属性の両方を構成します。

注意: ロケーション ID に「DN 接頭辞」セマンティック型が含まれる場合、Active Directory および ADAM では、複数値の RDN が許可されないことに注意する必要があります (iPlanet/SunOne では使用可能)。Active Directory および ADAM では、メタ属性構成で「属性値」の選択が「単一」になっていることを確認してください。

- **参加者:** アクションを実行する 1 人以上のユーザー。

たとえば、ユーザーの作成ワークフローの場合、「開始」ステップを作成し、User Manager にログインしているユーザーが誰でも新規ユーザーの作成プロセスを開始できるようにそのステップを構成できます。または、変更リクエストの承認を担当するワークフロー内の特定の参加者を定義できます。参加者は、ロール、名前、グループ・メンバーシップ、またはその他の特性に基づいて割り当てることが可能です。

LDAP 属性の場合、DN に基づいて参加者を選択する LDAP フィルタを定義することもできます。

- **ターゲット:** 作成や削除などの対象となる個人、グループ、またはその他の LDAP オブジェクト。

ワークフロー定義のターゲットは、テンプレート・オブジェクトではなく LDAP オブジェクトです。

- **エントリ条件:** 現在のステップの前に完了する必要があるステップまたはサブフロー。

たとえば、ワークフローの最初のステップが「開始」ステップであるとし、このワークフローの 2 番目のステップには、「開始」ステップの正常な完了をエントリ条件に指定できます。一般的なエントリ条件は、前のステップの正常な完了です。

- **通知:** ステップ実行の前後に電子メール通知を受信するユーザー。

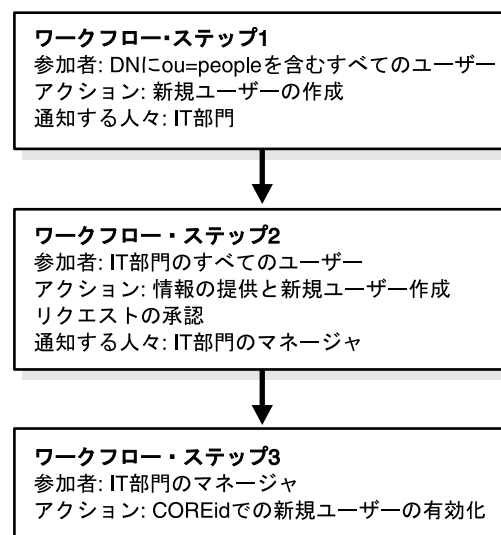
他の参加者は、電子メール通知が構成されているかどうかにかかわらず、着信リクエスト・キューの保留中のチケットを参照できます。詳細は、5-13 ページの「[ステップ・アクションの説明](#)」を参照してください。

- **前処理と後処理:** ワークフローの一環として実行される外部機能。

たとえば、ユーザーの作成ワークフローで、一意のログイン ID を割り当てる開始ステップの後に Java プログラムをコールできます。

図 5-2 は、ワークフロー・プロセスを示しています。

図 5-2 ワークフロー・プロセスの例



ステップ・アクションの概要

ワークフローのステップごとに1つのアクションを割り当てます。アクションは、ユーザーが実行するか、自動化された方法で実行します。

たとえば、ユーザーを作成するワークフローに必要なアクションは、次のとおりです。

- リクエストの開始
- ユーザーの有効化またはアクティブ化

使用可能なアクションは、ワークフロー・タイプと、前のステップに定義されているアクションに応じて異なります。たとえば、「開始」アクションは、ワークフローの最初のステップでのみ使用できます。

表 5-3 に、User Manager ワークフローのステップに関連付けることのできるアクションをリストします。

表 5-3 User Manager ワークフローで使用可能なアクション

ワークフロー・タイプ	アクション
属性の変更	リクエスト (必須) 情報の提供 承認 情報と承認の提供 サブフロー承認 コミット (必須) 外部アクション エラー・レポート
ユーザーの作成	「開始」または「自己登録」(いずれかは必須) 情報の提供 情報と承認の提供 承認 サブフロー承認 コミット 「有効化」または「アクティブ化」(いずれかは必須) グループの選択 削除 エラー・レポート 外部アクション
ユーザーの削除	開始 (必須) 情報の変更 「無効化」または「非アクティブ化」(いずれかは必須) 承認 サブフロー承認 承認の変更 コミット 削除 エラー・レポート 外部アクション

表 5-3 User Manager ワークフローで使用可能なアクション (続き)

ワークフロー・タイプ	アクション
非アクティブ化	開始
	情報の変更
	承認
	情報と承認の変更
	コミット
	外部アクション
	エラー・レポート
	非アクティブ化
	無効化
	削除
再アクティブ化	開始
	情報の提供
	承認
	情報と承認の提供
	サブフロー承認
	コミット
	外部アクション
	エラー・レポート
	アクティブ化
	有効化

表 5-4 に、Group Manager ワークフローで使用可能なアクションをリストします。

表 5-4 Group Manager ワークフローで使用可能なアクション

ワークフロー・タイプ	アクション
属性の変更	リクエスト (必須)
	情報の提供
	承認
	情報と承認の提供
	サブフロー承認
	外部アクション
	コミット (必須)
	エラー・レポート
グループの作成	開始 (必須)
	情報の提供
	情報と承認の提供
	承認
	コミット (必須)
	サブフロー承認
	削除
	外部アクション
	エラー・レポート

表 5-4 Group Manager ワークフローで使用可能なアクション (続き)

ワークフロー・タイプ	アクション
グループの削除	開始 (必須) 情報の変更 承認の変更 サブフロー承認 承認 コミット (必須) 削除 エラー・レポート 外部アクション

表 5-5 に、Organization Manager ワークフローのアクションをリストします。

表 5-5 Organization Manager ワークフローのアクション

ワークフロー・タイプ	アクション
属性の変更	リクエスト (必須) 情報の提供 承認 情報と承認の提供 サブフロー承認 外部アクション コミット (必須) エラー・レポート
オブジェクトの作成	開始 (必須) 自己登録 情報の提供 情報と承認の提供 承認 サブフロー承認 コミット 削除 エラー・レポート 外部アクション
オブジェクトの削除	開始 (必須) 情報の変更 承認 承認の変更 サブフロー承認 コミット (必須) 削除 エラー・レポート 外部アクション

ステップ・アクションの説明

表 5-6 に、ワークフローで使用可能なアクションを示します。

表 5-6 ワークフロー・ステップのアクション

アクション	説明
アクティブ化	User Manager 専用。ID システムで新規ユーザーをアクティブ化します。アクティブなユーザーは、有効化されると、ログインして管理者に許可された操作を実行できます。ユーザー・エントリの <code>obuseraccountcontrol</code> 属性により、アクティブ化と非アクティブ化のステータスが制御されます。「アクティブ化」アクションでは、マネージャなどの参加者がユーザーをアクティブ化する必要があります。
承認	このアクションは、必須属性で構成できます。必須属性の値は、実行時に承認担当の参加者に提供されます。このアクションで変更される情報はありません。
情報と承認の変更	「情報と承認の提供」アクションと同じ機能を実行しますが、ユーザーを非アクティブ化する場合にのみ使用します。
情報の変更	「情報の提供」アクションと同じ機能を実行しますが、ユーザーを非アクティブ化する場合にのみ使用します。
コミット	前のステップで収集された情報をディレクトリに書き込みます。コミット操作により、ディレクトリ内のオブジェクトの場所に情報が書き込まれます。たとえば、作成操作では、「コミット」アクションによってディレクトリに新規エントリが追加されます。ワークフローに追加の「コミット」アクションが含まれる場合、その情報は新しく作成されたオブジェクトを含むディレクトリ内の場所に書き込まれます。「コミット」アクションは、ワークフロー内で 2 回以上使用できます。ユーザー・アクションは必要ありません。
非アクティブ化	User Manager 専用。非アクティブ化の効果は、ユーザーの現行セッションが終了した後に反映されます。非アクティブなユーザーは、ログインできません。他のユーザーは、非アクティブなユーザーを検索対象とする場合を除き、ID システムで非アクティブなユーザーを検索できません。非アクティブ化では、ディレクトリのユーザーは削除されません。ユーザー・エントリの <code>obuseraccountcontrol</code> 属性により、アクティブ化と非アクティブ化のステータスが制御されます。ワークフローの非アクティブ化ステップには、参加者が必要です。 注意: 削除ユーザーを含む <code>.ldif</code> を作成する場合、「削除」のかわりに「非アクティブ化」または「無効化」ワークフロー・ステップを使用してください。「非アクティブなユーザー ID」ページに移動し、「アーカイブ」オプションを使用します。これにより、ディレクトリからユーザーが削除され、次の場所に <code>deactivateduser.ldif</code> が作成されます。 <code>IdentityServer_install_dir\oblix\data\common directory</code>
削除	ユーザーの作成、グループの作成またはオブジェクトの作成ワークフローで「削除」アクションを使用すると、ターゲット・エントリがディレクトリから永久に削除されます。ターゲット・エントリの作成後に、作成ワークフローが中断される場合があります。「削除」ステップによりディレクトリを消去することで、同じユーザーを作成する新しい操作を試行できます。
無効化	User Manager 専用。ユーザーを非アクティブ化します。これにより、ユーザーの現行セッションが終了すると、そのユーザーは ID システムから認識されなくなります。非アクティブ化の効果は、ユーザーによる次のログイン試行時に適用されます。非アクティブ化では、オブジェクトはディレクトリから削除されません。このアクションには、参加者は必要ありません。

表 5-6 ワークフロー・ステップのアクション (続き)

アクション	説明
有効化	User Manager 専用。「有効化」アクションは、「コミット」および「アクティブ化」アクションの組合せです。新規ユーザーを自動的にアクティブ化します。アクティブなユーザーは、前のステップの完了後に ID システムで認識されます。このアクションには、ユーザーをアクティブ化する参加者は必要ありません。
エラー・レポート	バックグラウンド・プロセスで処理エラーが発生した場合に、特定のユーザーにエラーを送信するようエラー・レポートを構成できます。ステップが否認される場合（承認プロセスの実行時など）にもエラー・レポートを構成できます。
外部アクション	Oracle Access Manager の外部で実行されるアクション。
開始	作成および非アクティブ化ワークフローを開始します。このアクションは、ワークフロー内で 1 回のみ使用できます。このアクションは、最初のアクションである必要があります。自己登録アクションも、ワークフローの開始アクションに指定できます。特定のワークフローの参加者として定義されているかどうかにかかわらず、すべてのユーザーのページに「プロファイルの作成」ボタンまたは「ユーザーの非アクティブ化の開始」オプションが表示されます。ワークフローの参加者として定義されていないユーザーがワークフローのボタンまたはリンクをクリックすると、エラー・メッセージが表示されます。
情報と承認の提供	「情報の提供」アクションと「承認」アクションを 1 つのアクションにまとめたものです。
情報の提供	ユーザーから情報を収集します。このアクションは、「開始」と似ていますが、ワークフローの最初のアクションには指定できません。
リクエスト	属性の変更、追加または削除を求めるユーザーのリクエスト。このアクションの参加者には、「プロファイルの変更」ページに「変更をリクエスト」または「削除をリクエスト」ボタンが表示されません。
自己登録	ユーザーは、登録フォームを完成して送信できます。他の参加者は、リクエストを承認してユーザーをアクティブ化します。このアクションは、ワークフロー内の最初のステップである必要があります。自己登録アクションでは、必ずしも他の参加者が新規ユーザーを承認およびアクティブ化する必要はありません。
グループの選択	ワークフローの参加者は、ユーザーの作成ワークフローの実行中に、1 つ以上のグループにターゲット・ユーザーをサブスクライブできます。新規ユーザーは、サブスクリプション・ポリシーを満たしている必要があります。「有効化」または「アクティブ化」ステップの後にのみ使用できます。
サブフロー承認	メイン・ワークフロー・ステップから起動されたサブフローの現在のステータスをレポートします。他のサブフローから起動されたサブフローには適用されません。

注意： 自己登録ステップの電子メール事後通知では、`globalparams.xml` の 2 つのパラメータ (`sendMailFromName` および `sendMailFromEmail`) が必要です。これらのパラメータの値は、SMTP メッセージの `mail From` (または `senders name`) の部分と `mail` (または `senders email`) の部分にそれぞれ配置されます。

自己登録では、ターゲットがまだ作成されていないため、これらの値は `globalparams.xml` を通じて提供されます。この場合、`globalparmams.xml` でこれらのパラメータを見つけ、現在の環境に応じてその値を変更する必要があります。たとえば、次のようになります。

```
<SimpleList>
  <NameValPair
    ParamName="sendMailFromName"
    Value="SelfRegistration"></NameValPair>
</SimpleList>
<SimpleList>
  <NameValPair
    ParamName="sendMailFromEmail"
    Value="SelfRegistration@Oracle.com"></NameValPair>
</SimpleList>
```

ターゲット・ユーザーが作成されると、`sendMailFromName` および `sendMailFromEmail` の値は、ログイン・ユーザーのプロファイルの名前属性と電子メール属性からそれぞれ取得されます。

サブフローの概要

単純なワークフローの場合、すべてのステップは順番に実行されます。1つのステップが保留中の状態になると、ワークフローは次のステップに進みません。ワークフローには様々な参加者が関与するのが一般的であるため、ワークフローの完了が遅れる可能性があります。ワークフローの処理を迅速化するには、平行に発生するサブフローを定義します。

サブフローにより、ワークフローは複数の作業部分に分割されます。サブフローでは、独自のサブフローを起動できます。1つのワークフローから複数のサブフローを起動できます。

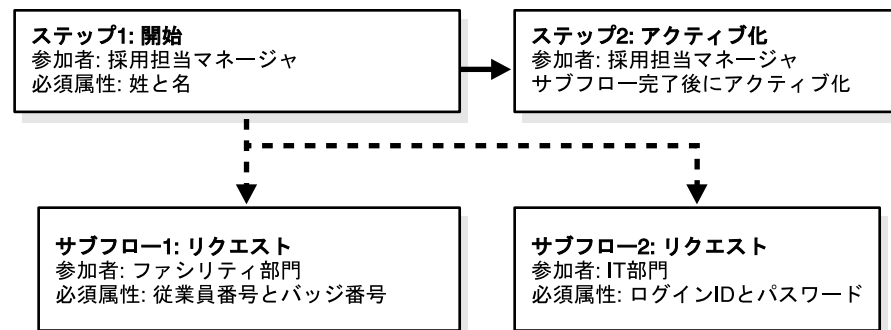
注意： サブフローは、常に属性の変更ワークフローです。

プロセスの概要：ユーザーの作成ワークフローの例

1. 採用担当マネージャがユーザーの作成ワークフローを開始します。
2. 従業員番号とバッジ番号を求めるリクエストがファシリティ部門に送信されます。
3. ログイン ID とパスワードを求めるリクエストが IT 部門に送信されます。
4. 最終承認とユーザーのアクティブ化を求めるリクエストが採用担当マネージャに送信されます。

サブフローの使用により、一部のリクエストを平行に実行できます。図 5-3 は、サブフローが完了するまで承認を待機するワークフローを示しています。

図 5-3 サブフロー使用時のステップ完了の順序



ワークフローは、サブフローが完了するまで次のステップに進みません。

注意: サブフローを起動する場合、ターゲット・オブジェクトまたは属性は、「ワークフロー・ドメイン」フィルタの指定によるフィルタ基準を満たしている必要があります。

クイックスタート・ツールの使用方法

マスター管理者は、クイックスタート・ツールを使用してデフォルト設定に基づく単純なワークフローを迅速に作成できます。

クイックスタートを使用してワークフロー定義を作成したら、ワークフロー・ツールを使用してそのワークフロー定義を変更できます。たとえば、動的参加者やサロゲートを指定できます。

クイックスタート・ツールでは、次のワークフローを定義できます。

表 5-7 クイックスタート・ツールで作成できるワークフロー

ワークフロー名	含まれるステップ
ユーザー、グループまたはオブジェクトの作成 (基本)	「自己登録」または「開始」 コミット エラー・レポート 注意: 単純なユーザーの作成ワークフローの場合、必須属性はほとんどのディレクトリ・サーバーで姓と名です (Active Directory の場合はログイン ID)。
ユーザー、グループまたはオブジェクトの作成 (拡張: 承認あり)	開始 承認 コミット エラー・レポート
ユーザーまたはオブジェクトの自己登録 (拡張: 承認あり)	自己登録 承認 コミット エラー・レポート
属性の変更 (基本)	リクエスト コミット エラー・レポート
属性の変更 (拡張: 承認あり)	リクエスト 承認 コミット エラー・レポート

クイックスタート・ツールでは、ID システムにログインしているすべてのユーザーが、ほとんどのステップに参加者として割り当てられます。User Manager では、属性の変更ワークフローの参加者は、「マネージャ」ロールが割り当てられている任意のユーザーです。Group Manager では、属性の変更ワークフローの「承認」ステップの参加者は、「グループの所有者」ロールが割り当てられている任意のユーザーです。

クイックスタート・ツールを使用してワークフローを作成すると、ワークフローのステップ、参加者、関連属性などを参照および変更できます。ワークフロー定義の参照方法の詳細は、5-55 ページの「ワークフロー・サマリーの表示とエクスポート」を参照してください。ワークフローの変更方法の詳細は、5-57 ページの「ワークフローの変更」を参照してください。

注意：ワークフローを定義できるかどうかは、保持している管理権限に応じて変化します。

クイックスタート・ツールを使用してワークフローを定義する手順

1. ID システム・コンソールで、「User Manager」、「Group Manager」または「Organization Manager」を選択します。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
デフォルトでは、構成情報を参照できる権限を保持するのは、マスター管理者、マスター ID 管理者および委任 ID 管理者のみです。
3. 「ここをクリック」というリンクをクリックします。

The screenshot shows the Oracle Identity Administration console interface. At the top, there are navigation tabs for 'User Manager', 'Group Manager', 'Org. Manager', and 'Identity System Console'. Below the navigation, there is a search bar with a dropdown menu for '検索' (Search) and a search button. The main content area shows a list of workflow types: '属性アクセス制御' (Attribute Access Control), '委任管理' (Delegation Management), 'ワークフロー定義' (Workflow Definition), and '検索ベースの設定' (Search-based Settings). The 'ワークフロー定義' tab is selected.

ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

[13]ワークフロー定義

The screenshot shows the 'Workflows' page in the Oracle Identity Administration console. The page title is '[13]ワークフロー定義'. Below the title, there is a dropdown menu for 'ワークフロー' (Workflow) with the selected option 'ユーザーの作成 - 基本 [有効]' (User Creation - Basic [Active]). Below the dropdown, there are several buttons: '新規' (New), '変更' (Edit), 'コピー' (Copy), '削除' (Delete), '表示' (View), '無効化' (Deactivate), and 'すべてをエクスポート' (Export All).

これにより、クイックスタート・ツールが起動します。

4. 作成するワークフロー・タイプを選択します。

注意：同じクイックスタート・ページで作成ワークフローと属性の変更ワークフローを定義できます。「属性の変更」フィールドとオプションを表示するには、ページの一番下までスクロールします。

ワークフローの名前も指定できます。デフォルト名が提供されますが、クイックスタート・ツールを使用してこのタイプのワークフローを複数作成する場合、その名前は変化しません。

5. 作成ワークフロー・タイプを選択する場合、ワークフローにより作成されるオブジェクトに対して1つのターゲット・ロケーションを指定できます。

デフォルトのターゲット・ロケーションは、ID システムの検索ベースです。

6. オプションで、追加属性を選択できます。

ユーザーの作成、グループの作成またはオブジェクトの作成ワークフローの場合、これらの属性は開始ステップまたは自己登録ステップの実行時に入力されます。

属性の変更ワークフローの場合、これらの属性はワークフローの実行時に変更されます。選択した属性ごとに個別のワークフローが作成されます。たとえば、5つの属性を選択すると、クイックスタート・ツールによって5つの属性の変更ワークフローが生成されます。

7. 「生成」をクリックします。

- クイックスタート・ツールにより生成されるサマリー・レポートを確認します。

ワークフロー定義 - クイックスタート(2/2)

サマリー・レポート

次のワークフローが生成されました:
ワークフロー名 警告(ある場合)
ユーザーの作成 - 基本

完了

- ワークフローをテストするには、サマリー・レポートのいずれかのワークフロー・リンクをクリックします。

これにより、ワークフロー・インスタンスが開始されます。ワークフローを使用するプロセスの詳細は、5-5 ページの「[ID システム・アプリケーションでユーザーがワークフローにアクセスする方法](#)」を参照してください。

注意：ワークフローを Portal Inserts として使用するには、出力された URL をブラウザからコピーします。Portal Inserts の作成方法の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

- 「完了」をクリックします。

クイックスタート・ツールを使用した自己登録ワークフローの作成

Web ポータルにユーザー登録ページを提供する場合、自己登録ワークフローを定義し、そのワークフローに対して出力された URL を取得できます。この URL は、Portal Inserts として使用できます。

クイックスタート・ツールを使用して自己登録ワークフローを定義する手順

- 自己登録ワークフローを作成します (5-17 ページの「[クイックスタート・ツールを使用してワークフローを定義する手順](#)」を参照してください)。
- 「生成」ボタンをクリックし、次に新しく作成されたワークフローのリンクをクリックします。
- 新規ワークフローが表示されたら、その URL をコピーします。

この URL は、Web ポータルにユーザー登録ページを設定する際に使用できます。この URL は、ワークフローの最初のページへのリンクです。自己登録ワークフローを定義するその他の方法は、5-65 ページの「[自己登録ワークフローの作成](#)」を参照してください。

ワークフロー・アプレットの使用方法

クイックスタート・ツールを使用する以外に、複数のオプションとサブフローを指定できる構成ページを使用してワークフローを定義できます。

この場合、ワークフローを定義する権限を保持している必要があります。詳細は、2-5 ページの「[管理の委任について](#)」を参照してください。

通常、ワークフローには、最低 2 つのステップ（ワークフローを開始するステップと変更をコミットするステップ）が含まれます。

タスクの概要：ワークフロー・アプレットを使用したワークフローの定義

1. 「ワークフロー定義」アプレットを起動します。

詳細は、5-20 ページの「[ワークフロー定義](#)」アプレットにアクセスする手順」を参照してください。

2. 「新規」を選択して新規ワークフロー定義の作成を開始します。

詳細は、5-20 ページの「[新規ワークフロー定義の開始](#)」を参照してください。

3. 作成ワークフロー・タイプを選択した場合、ワークフロー・ターゲットを指定します。

ターゲットは、オブジェクトの作成先となるディレクトリ・ツリー内の場所です。詳細は、5-22 ページの「[オブジェクトの作成ワークフローの LDAP ターゲットの定義](#)」を参照してください。

4. ワークフロー・ステップとアクションを定義します。

各ワークフロー・ステップには、アクションが含まれます。アクションは、ユーザーが実行するか、自動化された方法で実行します。ワークフローのステップごとに 1 つのアクションを割り当てます。各ステップには、参加者も割り当てます。詳細は、5-24 ページの「[ワークフローの最初のステップの定義](#)」を参照してください。

5. 属性をステップに関連付けます。

ステップ・アクションは、1 つ以上の属性値を対象に実行されます。これらの属性は、ディレクトリから取得されるか、オブジェクト・テンプレートから取得されます。詳細は、5-26 ページの「[ステップ属性の定義](#)」を参照してください。

6. 後続のステップのエントリ条件を定義します。

詳細は、5-30 ページの「[後続のステップの定義](#)」を参照してください。

7. 後続のステップを定義します。

8. 1 つ以上のサブフローを定義します。

サブフローは、特定のステップまたはワークフローを完了するために満たす必要のある条件です。メイン・ワークフロー・ステップと同様に、サブフローにはアクション、参加者および属性が関連付けられます。詳細は、5-33 ページの「[サブフローの定義](#)」を参照してください。

9. ワークフローを終了する 1 つ以上のコミット・ステップを定義します。

複数のスキーマ（たとえば、LDAP スキーマとテンプレート・スキーマ）を使用してワークフローを構成する場合、スキーマ・タイプごとに個別のコミット・ステップを構成する必要があります。

注意： ID システムのリリース 7.0 の時点で、テンプレート属性の値はバックエンド・システムに送信できますが、それらの値を ID システムで逆に読み取ってプロフィール・ページに表示することはできません。そのため、ワークフローが正しく構成され、ワークフローを使用するインスタンスが成功したかどうかをチェックするには、必要に応じてバックエンド・システムのデータを調査する必要があります。

「ワークフロー定義」アプレットにアクセスする手順

1. ID システム・コンソールで、「User Manager」、「Group Manager」または「Organization Manager」を選択します。
Organization Manager に複数のタブがある場合は、適切なタブを選択してください。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
一部のブラウザでは、アプリケーションの証明書を信頼するかどうかを尋ねるプロンプトが表示されることがあります。このプロンプトが表示された場合は、「常に信頼」オプションを選択してください。
User Manager および Organization Manager の場合、「ワークフロー定義」ページが表示されます。
3. Group Manager を使用している場合、必要に応じて適切なグループ・タイプを指定します。使用可能なグループ・タイプは、実際の構成に応じて異なります（4-9 ページの「Group Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加」を参照してください）。
4. Group Manager を使用している場合、「ワークフロー定義」ページで必要に応じて適切なグループ・タイプを選択し、「次へ」をクリックします。
グループ・タイプを選択しない場合、このワークフローでは「Basic」グループ・タイプが使用されます。

新規ワークフロー定義の開始

ワークフロー定義は、ユーザー・セットごとに作成できます。たとえば、エンジニアリング部門と営業部門で異なるユーザーの作成ワークフローを定義できます。

注意： 単純なユーザーの作成ワークフローの場合、必須属性はほとんどのディレクトリ・サーバーで姓と名です（Active Directory の場合はログイン ID）。

新規ワークフロー定義を開始する手順

1. 5-19 ページの「ワークフロー・アプレットの使用方法」の手順に従ってワークフロー定義ツールを起動します。
2. 「新規」をクリックし、「新規」ボタン以外のすべてのボタンが非アクティブ化されるまで待機します。
3. 「ワークフロー名」フィールドにワークフローの名前を入力します。
4. 「ワークフロー・タイプ」リストで、作成するワークフローのタイプを選択します。
ワークフロー・タイプの詳細は、5-7 ページの「ワークフローのタイプ、ステップおよびアクション」を参照してください。
サブフローを作成する場合は、5-33 ページの「サブフローの定義」を参照してください。
5. 「説明」フィールドに、オプションでこのワークフローの説明を入力できます。
6. 「ワークフロー・ドメイン」フィールドで、このワークフローを使用可能にするディレクトリ・ツリー内の開始ポイントを選択します。

ワークフロー・ドメインを、ワークフローを開始したログイン・ユーザーのディレクトリ・エントリと一致させる場合は、置換構文を使用します。たとえば、ワークフロー・ドメインの **ou** を、ワークフローを生成したユーザーの **ou** と常に一致させる場合、次のように入力します。

(ou=\$ou\$)

使用例は、3-26 ページの「置換構文：ログイン・ユーザーの DN に一致するターゲットを戻す方法」を参照してください。

注意：ワークフロー作成時にワークフロー・ドメイン（またはターゲット・ドメイン）のフィルタを指定する場合、完全な LDAP URL は使用しないでください。LDAP フィルタのみを使用できます。

ワークフローを使用可能にする特定のドメインを選択することも可能です。たとえば、ディレクトリ・ツリー内に **Engineering** と **Sales** という異なるブランチがあり、このワークフローを **Engineering** にのみ適用する場合、ディレクトリ・ツリーの **Engineering** ブランチの最上位ノードを選択します。ディレクトリ・ツリーが特にフラットな形状の場合、またはツリーに特に大量のブランチが存在する場合、LDAP フィルタを入力してワークフロー・ドメインを絞り込むことができます。3-25 ページの「**ルールとフィルタの使用法**」を参照してください。たとえば、ディレクトリ・ツリーの開始ポイントが **ou=people** で、管理者のみを対象とするワークフローを作成する場合、**(title=admin)** を含むフィルタを作成できます。

注意：フィルタを使用する場合は、必ずパフォーマンス・テストを実行してください。フィルタは実行時に評価されるため、パフォーマンスに影響する可能性があります。

7. **User Manager** または **Organization Manager** を使用している場合、「次へ」をクリックします。

ワークフロー・タイプによっては、ターゲットを選択するよう求められるか（5-22 ページの「**オブジェクトの作成ワークフローの LDAP ターゲットの定義**」を参照）、ワークフローの最初のステップを定義するよう求められます（5-24 ページの「**ワークフローの最初のステップの定義**」を参照）。

8. **Group Manager** を使用しており、拡張グループを操作している場合、必要に応じてサブスクリプション・タイプを指定します。

たとえば、グループを選択するステップや、ユーザーがグループに自分自身を追加するステップを定義する場合にこの操作が発生する可能性があります。oblixAdvancedGroup オブジェクト・クラスで **obGroupSubscriptionType** 属性が構成されている場合、参加者は「サブスクリプション・タイプ」オプションを使用できます。

使用可能なサブスクリプション・タイプは、次のとおりです。

表 5-8 ワークフローのサブスクリプション・タイプ

オプション	説明
タイプが選択されていません	サブスクリプション・タイプが定義されていません。機能的には「オープン」ポリシーと同等です。
オープン	登録は、サブスクライブするすべてのユーザーに許可されます。
フィルタでオープン	登録は、グループの動的フィルタ（LDAP ルール）を満たすすべてのユーザーに許可されます。
ワークフロー経由で制御	サブスクライブまたはサブスクライブ解除するには、ユーザーがワークフローの「グループの選択」ステップのターゲットである必要があります。
クローズ済	メンバー・リストはクローズされています。変更は許可されません。default_subscription ポリシー・パラメータのデフォルト設定は、SubscriptionPolicyClosed です。このパラメータは次の場所にあります。 <i>IdentityServer_install_dir/identity/oblix/data/common/groupdbparams.xml</i> ここで、 <i>IdentityServer_install_dir</i> は、ID システムがインストールされているディレクトリです。

9. 「追加」をクリックし、「次へ」をクリックします。

ワークフロー・タイプによっては、ターゲットを選択するよう求められるか (5-22 ページの「[オブジェクトの作成ワークフローの LDAP ターゲットの定義](#)」を参照)、最初のステップを定義するよう求められます (5-24 ページの「[ワークフローの最初のステップの定義](#)」を参照)。

オブジェクトの作成ワークフローの LDAP ターゲットの定義

定義するワークフロー・タイプとして「作成」を選択する場合 (「ユーザーの作成」など)、1つ以上のターゲットを定義する必要があります。ターゲットは、オブジェクトの作成先となるディレクトリ・ツリー内の場所です。たとえば、`ou=bestmotors,o=company,c=us` というターゲットでは、`ou=bestmotors` コンテナの下にオブジェクトが作成されます。ワークフローでこのターゲットを使用してユーザーを作成すると、そのディレクトリ・エントリは、`cn=John Smith,ou=bestmotors,o=company,c=us` のようになります。

ワークフロー・ターゲットを定義する場合、置換構文も使用できます。これにより、ユーザーの作成ワークフローの新規ユーザーの `ou` エントリを、ワークフローを開始したログイン・ユーザーの `ou` エントリと常に一致させることができます。使用例は、3-26 ページの「[置換構文: ログイン・ユーザーの DN に一致するターゲットを戻す方法](#)」を参照してください。置換構文を使用する場合、必要に応じて `globalparams.xml` の `ResourceFilterSearchScope` パラメータの値を変更する必要があります。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

ログイン・ユーザーの `ou` エントリに複数の値が含まれており、それらのいずれかの `ou` の下に新規ユーザーを作成する場合、`globalparams.xml` の `ResourceFilterSearchScope` パラメータの値を 2 に変更する必要があります。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。この場合、ワークフローの実行時に使用可能なすべてのターゲットのリストが表示されます。ユーザーは、新規ターゲット・ユーザーを作成する正確な `ou` の場所を選択できます。リスト内のターゲットは、ログイン・ユーザーの `ou` 属性の複数の値から取得されます。このリストは、`(ou=ou)` とともに `(objectclass=organizationalUnit)` などの他のフィルタ・コンポーネントを使用して制限することが可能です。

複数のターゲットを定義すると、参加者にはワークフローの実行時に選択リストが表示されます。ワークフロー・ターゲットは、常に LDAP ディレクトリ・ツリーに基づきます。テンプレート・スキーマに基づくターゲットは使用できません。

別のタイプのワークフローを定義している場合、最初のワークフロー定義ページで「次へ」をクリックし、5-24 ページの「[ワークフローの最初のステップの定義](#)」に記載されているステップ定義ページに移動します。

注意: デフォルトでは、検索ベースの直下の子ノードのみが表示されます。詳細は、4-49 ページの「[検索ベースのデフォルト有効範囲の変更](#)」を参照してください。

ワークフロー・ターゲットを定義する手順

1. まだ開始していない場合、5-20 ページの「[新規ワークフロー定義を開始する手順](#)」に従って新規ワークフロー定義を開始します。
2. 最初の「ワークフロー定義」ページで「次へ」をクリックします。
ターゲットの特性を選択するためのフィールドを含むターゲット・ページが表示されます。
3. 新規ターゲットを定義するため、「ターゲット名」フィールドに名前を入力します。
たとえば、販売代理店のターゲットを作成する場合、ターゲット名は「代理店名」などとします。
4. 「ターゲット・ドメイン」フィールドで、オブジェクトを作成するディレクトリ・ツリー内の場所を選択し、「追加」をクリックしてターゲット・ドメインを「ターゲット」フィールドに追加します。

ワークフロー・ドメインを定義すると、ワークフローが適用されるディレクトリ・ツリーのブランチが選択されます。ターゲット・ドメインは、メイン・ワークフロー・ドメインのサブセットです。フィルタを使用すると、より厳密にターゲットの場所（ツリー内で選択したノードの下に含まれる任意のユーザー・オブジェクト）を指定できます。

注意： ワークフロー作成時にターゲット・ドメイン（またはワークフロー・ドメイン）を指定する場合、完全な LDAP URL は使用しないでください。LDAP フィルタのみを使用できます。たとえば、`ldap:///ou=Partners,o=Company,c=US??sub?(cn=Shutterbug Canavan)` ではなく、`cn=Shutterbug Canavan` とするのが適切です。

詳細は、3-25 ページの「[ルールとフィルタの使用法](#)」を参照してください。

注意： ワークフロー・ドメインにフィルタを追加した場合、ターゲットのフィルタを指定することはできません。

5. 「追加」をクリックします。
6. 追加ターゲットにワークフローを適用するには、次の操作を実行します。
 - 「新規」をクリックします。
 - 別の名前とドメインを指定します。
 - 「追加」をクリックします。
7. ターゲット・ドメインの指定が完了したら、「次へ」をクリックします。

ワークフローの最初のステップの定義

ワークフローの名前を指定し、必要に応じてターゲットを定義した後、最初のワークフロー・ステップを作成するよう求められます。次のようなページが表示されます。

属性アクセス制御 委任管理 **ワークフロー定義** 検索ベースの設定

ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

ワークフロー名: New Employee ワークフロー・タイプ: ユーザーの作成

定義済ステップ:

ステップが指定されていません

新規 変更 ステップの削除 ステップを挿入

ステップ・プロパティ

アクション サブフロー 属性 参加者 外出中 エスカレーション メール通知

実行するアクションの選択:

開始

ステップの保存

ワークフローの保存 ワークフローの取消し 前へ

ワークフローの最初のステップを定義する手順

1. まだ開始していない場合、5-20 ページの「[新規ワークフロー定義を開始する手順](#)」に従って新規ワークフロー定義を開始します。
2. (作成ワークフロー・タイプで) まだ定義していない場合、5-23 ページの「[ワークフロー・ターゲットを定義する手順](#)」に従ってターゲットを定義します。
3. 「実行するアクションの選択 *」リストで、アクションを選択します。

User Manager または Organization Manager のオブジェクトの作成ワークフローでは、「開始」および「自己登録」アクションを選択できます。

Group Manager のオブジェクトの作成ワークフローでは、「開始」アクションを選択できます。

4. 「参加者」をクリックします。

ほとんどのステップで、アクションを実行する参加者が必要です。この例外は、「コミット」や「有効化」などの自動的に発生するアクションを含むステップと、「外部アクション」および「自己登録」アクションを含むステップです。

5. 次のいずれかの方法を使用して参加者を指定します。

- **ロール:** 「すべてのユーザー」というロールは、ID システムにログインしているすべてのユーザーを示します。

ロールは、ワークフロー・パラメータ・ファイルの `gsc_wf_param.xml`、`usc_wf_param.xml` および `osc_wf_param.xml` で定義します。詳細は、5-63 ページの「ワークフローのデータおよびアクションのカスタマイズ」を参照してください。

注意: 「参加者の選択 *」フィールドで「事前通知する参加者の選択」を選択した場合、ロールとして「次のステップの参加者」を選択しないでください。また、Group Manager ワークフローのコミット・ステップでは、事後通知する所有者やメンバーを選択しないでください。選択しても、所有者やメンバーに電子メール通知は実行されません。

参加者ロール（ステップを処理できるユーザーのロール）は、コミット、有効化またはアクティブ化ステップが完了した後にのみ機能します。コミット、有効化またはアクティブ化ステップにより、通知情報の決定に使用されるオブジェクトの DN が作成されます。

- **人の選択:** セレクタの使用の詳細は、1-10 ページの「[検索機能](#)」を参照してください。セレクタの構成方法の詳細は、3-23 ページの「[「オブジェクト・セレクタ」表示タイプの検索フィルタ](#)」を参照してください。
- **グループの選択:** セレクタの使用の詳細は、1-10 ページの「[検索機能](#)」を参照してください。セレクタの構成方法の詳細は、3-23 ページの「[「オブジェクト・セレクタ」表示タイプの検索フィルタ](#)」を参照してください。
- **フィルタの作成:** LDAP フィルタの作成方法の詳細は、4-27 ページの「[クエリー・ビルダーを使用した LDAP フィルタの記述](#)」を参照してください。

ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

ワークフロー名: New Employee ワークフロー・タイプ: ユーザーの作成

定義済ステップ: [ステップ1] 開始

新規 変更 ステップの削除 ステップを挿入

ステップ・プロパティ

アクション サブフロー **属性** 参加者 外出中 エスカレーション メール通知

参加者の選択

静的参加者が使用可能
 静的参加者が使用不可

ロールの選択

すべてのユーザー

フィルタの作成

フィルタの作成

人々の選択

ユーザーの選択

Channing Haramundanis

グループの選択

グループの選択

Level1 Admins

ステップの保存

ワークフローの保存 ワークフローの取消し 前へ

- 「ステップの保存」または「ワークフローの保存」をクリックするか、次の項の手順に従ってステップ属性を選択します。

ステップ属性の定義

ステップ・アクションは、1つ以上の属性値を対象に実行されます。ステップ・アクションを構成する場合、特定の属性値を必要とするかどうかと、他の構成オプションを指定します。たとえば、「情報の提供」アクションでは、電子メール属性を指定して、ステップ参加者に電子メール・アドレスの入力を促すことができます。

ステップ属性の定義には、次の手順が含まれます。

- ワークフローの特定のステップで使用可能にする属性の選択
- 属性プロパティの構成

オブジェクト・テンプレート (.tpl ファイル) に基づく属性では、ID システム・コンソールで属性を構成するときに、属性の含まれるスキーマのタイプが表示されると役立つ可能性があります。たとえば、新規ユーザーの電子メール・アカウントを設定するアプリケーションに情報を送信するワークフローの場合、属性ラベルの前にアプリケーション名を配置できます。これは、ユーザーがこの属性を参照する場合に役立ちます。プロビジョニング属性では、データ・フローが一方向であるため、ユーザーによる値の送信後は ID システムのプロファイル・ページに属性値が表示されません。ユーザーからこれに関する質問があったときに、属性ラベルがあるとその現象が通常どおりの動作であるかどうかを決定するのに役立ちます。

詳細は、3-19 ページの「属性の構成」を参照してください。

ステップで使用する属性を選択する手順

1. まだ開始していない場合、5-20 ページの「[新規ワークフロー定義を開始する手順](#)」に従って新規ワークフロー定義を開始します。
2. (作成ワークフロー・タイプで) まだ定義していない場合、5-23 ページの「[ワークフロー・ターゲットを定義する手順](#)」に従ってターゲットを定義します。
3. 5-24 ページの「[ワークフローの最初のステップを定義する手順](#)」に従ってワークフロー・ステップの定義を開始します。
4. ワークフロー・ステップの参加者を選択してから、「属性」をクリックします。
5. 「使用可能な属性」パネルで、ワークフロー・ステップに関連付ける 1 つ以上の属性を選択します。

属性の変更ワークフローの場合、選択した一番上の属性がプロファイル・ページのパネルに追加されていることを確認します。これにより、適切なプロファイル・ページに「変更をリクエスト」ボタンが表示され、ユーザーはこのワークフローのインスタンスを実行できます。

複数の属性を選択する方法の詳細は、4-33 ページの「[複数の属性を選択するためのキー](#)」を参照してください。

6. 右矢印ボタン (>>) をクリックし、選択した属性を「選択された属性」パネルに追加します。

オブジェクトの作成ワークフローのデフォルトでは、相対識別名 (RDN) を定義する属性が「選択された属性」パネルに表示されます。

属性の変更ワークフローのデフォルトでは、ワークフローの基礎として選択した属性が「選択された属性」パネルに表示されます。

ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

ワークフロー名: New Employee ワークフロータイプ: ユーザーの作成

定義済ステップ: [ステップ1]開始

新規 変更 ステップの削除 ステップを挿入

ステップ・プロパティ

アクション サブフロー **属性** 参加者 外出中 エスカレーション メール通知

属性の選択

使用可能な属性	選択された属性
名	フルネーム
国際ISDN番号	従業員番号
地域	従業員タイプ
姓	マネージャ
宛名	組織
携帯電話番号	役職
本籍地	部門番号
番地	表示名
私書箱	ビジネス・カテゴリ
秘書	電話番号
組織単位	部屋番号
自動車免許	
自宅住所	

プロパティ

ステップの保存

ワークフローの保存 ワークフローの取消し 前へ

7. ステップを保存するか、必要に応じて次の項の手順に従って属性プロパティを構成します。

注意: ワークフローのすべての必須属性（オブジェクト・クラス・スキーマの定義に基づく）が構成されるまで、ワークフローは保存できません。

属性プロパティを構成する手順

1. 「選択された属性」パネルで、構成する1つ以上の属性を選択します。

複数の属性を選択する方法の詳細は、4-33 ページの「[複数の属性を選択するためのキー](#)」を参照してください。

2. 「プロパティ」をクリックします。

次のような「属性プロパティ」ダイアログが表示されます。

属性: 電話番号 (telephoneNumber)

属性プロパティ: 電話番号 (telephoneNumber)

種類 必須 オプション

プロパティ 読取り専用 非表示

デフォルト値:

OK 取消

Java Applet Window

3. 属性の1つ以上のプロパティを選択します。

- 必須: ワークフロー参加者は、この属性の値を指定する必要があります。

注意: 必須属性は、非表示または読取り専用にはできません。

- オプション: ワークフロー参加者は、この属性の値を任意で指定できます。
- 読取り専用: ワークフロー参加者は、この属性を参照できますが変更できません。
- 非表示: ワークフロー参加者は、この属性の値を参照できません。属性は、ID イベント・プラグイン API と IdentityXML で使用可能です。
- デフォルト値: テキスト文字列を表示します。このテキスト文字列には、参加者にとって役立つ情報を指定します。たとえば、電話番号を入力する際の正しい書式を示す文字列を `phoneNumber` 属性のデフォルト値に指定できます。値は、テキスト表示タイプに制限されます。

4. 「OK」をクリックします。

5. 「ステップの保存」または「ワークフローの保存」をクリックします。

この時点で、メール通知参加者を定義するか、このワークフローの追加ステップを定義することが可能です。

注意: メール通知参加者を定義する際に、「参加者の選択 *」フィールドで「事前通知する参加者の選択」を選択した場合、ロールとして「次のステップの参加者」を選択しないでください。また、Group Manager ワークフローのコミット・ステップでは、事後通知する所有者やメンバーを選択しないでください。選択しても、所有者やメンバーに電子メール通知は実行されません。

事前通知または事後通知が機能するには、選択されたロールを対象にコミット、有効化またはアクティブ化ステップが完了している必要があります。コミット、有効化またはアクティブ化ステップの完了前には、オブジェクトはディレクトリ・ツリーのワークフロー・インスタンス情報内のみ存在します。コミット、有効化またはアクティブ化ステップにより、通知情報の決定に使用されるオブジェクトの DN が作成されます。

注意: 電子メール通知のカスタマイズの詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

後続のステップの定義

ワークフローには、少なくとも開始ステップと完了ステップが含まれますが、状況により追加のステップとサブフローも含まれます。ワークフロー内に2番目の（または3番目の、あるいはそれ以上の）ステップを作成する手順では、そのステップのエントリ条件を定義します。エントリ条件は、次の要素で構成されます。

- このステップに先行するステップの識別
- 前のステップの必須出力結果の識別

ワークフローの後続のステップを定義する手順

1. 5-24 ページの「ワークフローの最初のステップを定義する手順」に従ってワークフローの最初のステップを完成したら、「定義済ステップ」領域で「新規」をクリックします。

このページに、ワークフローの後続のステップを構成するための新規フィールドが表示されます。

2. 「前のステップ」リストで、このアクションに先行するステップを選択します。
3. 「戻り値」リストで、前のステップで **true** または **false** のどちらの値が戻されたときにこのアクションを実行するかを指定します。

前のステップが正常に完了した場合、**true** の値が戻されます。「False」を選択すると、前のステップが **false** の値を戻したときにエラー・レポートが生成されます。**false** の値が戻される場合は、次のとおりです。

- 参加者がワークフロー・チケットを否認した場合
- コミット・ステップに失敗した場合
- ID イベント・プラグイン API または IdentityXML により、強制的に **false** の値が戻される場合

4. 「アクション」リストでアクションを選択します。有効化、アクティブ化、およびその他のアクションを選択できます。

使用可能なアクションは、前のステップのアクションに応じて異なります。たとえば、次のようになります。

- 「情報の提供」は、「開始」に先行することはできません。
- 通常、エラー・レポート・アクションは、ステップが失敗した理由を提供します。たとえば、属性値の否認やユーザー・アクティブ化リクエストの拒否などです。
- 通常、**false** の状態は、エラー・レポート・ステップのエントリ条件です。たとえば、エラー・レポート・ステップの前のステップの参加者がアクティブ化操作を否認した場合に、ワークフローをエラー・レポート・ステップに進めることができます。

注意： プロビジョニングに使用するワークフローの場合、ワークフローごとに最低2つのコミット・アクションを定義する必要があります。1つのアクションでLDAPのデータをコミット（または有効化あるいはアクティブ化）し、もう1つのアクションでプロビジョニング・データを書き込みます。

5. 戻り値にかかわらず、前のステップのすべてのサブフローが完了するまでこのアクションの実行を遅延する場合、「サブフローを待機」を選択します。

このチェック・ボックスを選択すると、戻り値のエントリ条件に **:true** が追加されます。このチェック・ボックスを選択しない場合、戻り値のエントリ条件に **:false** が追加されます。詳細は、5-33 ページの「サブフローの定義」を参照してください。

6. 必要に応じて、5-24 ページの「ワークフローの最初のステップの定義」の手順に従って参加者の追加と属性の構成を行います。
7. ステップまたはワークフローを保存します。

注意：ユーザーの作成ワークフローは、「有効化」ステップで終了する必要があります。そうしない場合、ワークフローで追加されたユーザーを検索できません。

ワークフロー・ステップのコミット

ワークフローの最後のステップでは、特定のスキーマ・ドメインにデータをコミットします。デフォルトでは、スキーマ・ドメインは、ID システムがやり取りする LDAP ディレクトリです。ただし、ワークフローでテンプレート属性を構成した場合、テンプレート属性のスキーマ・ドメインにデータをコミットするための個別ステップを構成する必要があります。

テンプレート・スキーマ・ドメインの属性のコミット・ステップは、ID イベント API で処理してプロビジョニング用にバックエンド・システムに渡すことができます。

ワークフローの有効化

作成後のワークフローは、デフォルトで無効化されています。ID システムまたは外部アプリケーションで他の参加者を受け入れる準備ができたなら、ワークフローを有効化します。

ワークフローを有効化する手順

1. User Manager、Group Manager または Organization Manager にアクセスします。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. ワークフロー・メニューでワークフローを選択します。
4. 「有効化」をクリックします。

注意：属性が存在しないというメッセージが表示された場合は、各ワークフロー・ステップを調査してください。ステップごとに参加者と属性を構成する必要があります。

ワークフローのテスト

ワークフローは、テストの前に有効化する必要があります。詳細は、5-31 ページの「[ワークフローの有効化](#)」を参照してください。また、ワークフローをテストする場合はそのワークフローの参加者である必要があります。

ワークフローをテストする手順

1. ID システム・コンソールで、ワークフローを実行するアプリケーションを選択します。
たとえば、ユーザーの作成ワークフローの場合、User Manager を起動します。

2. ワークフローを開始します。

たとえば、ユーザーの作成ワークフローを定義した場合、テストするワークフローは「ユーザーの作成」ページのリストに表示されます。ワークフローを開始するには、そのワークフローをリストから選択します。

ユーザーの変更ワークフローの場合、User Manager で「変更をリクエスト」機能を選択します。

3. 各ワークフロー・ステップで指示される機能を実行します。

ワークフローは、期待どおりに動作する必要があります。たとえば、ユーザーの作成ワークフローの完了後には、ユーザーの作成操作で追加されたユーザーを検索できる必要があります。

Group Manager でワークフローを実行する手順

1. ID システム・コンソールで、「Group Manager」を選択します。
2. ワークフロー定義のグループ・タイプに対応するグループ・タイプ・パネルを選択します。
たとえば、Group 構造化オブジェクト・クラスと oblixAdvancedGroup オブジェクト・クラスでは、グループ・タイプ・パネルが異なる可能性があります。詳細は、4-8 ページの「User Manager または Organization Manager タブへの補助オブジェクト・クラスおよびテンプレート・オブジェクト・クラスの追加」を参照してください。

ワークフロー定義の例

次に、ユーザーの作成ワークフローを定義する場合の例を示します。この例では、ID システムにログインしているすべてのユーザーが任意のユーザーを作成できるワークフローを定義します。このワークフローにより、ユーザーに割り当てる名前および電子メール・アドレスを要求するチケットが生成されます。処理が完了すると、ID システムで新規ユーザーが有効化されます。

このワークフローを作成する手順

1. User Manager で、「構成」をクリックし、次に「ワークフロー定義」をクリックして「ワークフロー定義」ページに移動します。
2. 「新規」をクリックします。
3. このワークフローに「テスト用の新規ユーザー作成ワークフロー」という名前を付けます。
4. 「ワークフロー・タイプ」フィールドで、「ユーザーの作成」を選択します。
5. ターゲット定義ページで、「ターゲット名」フィールドに名前を入力し、「追加」をクリックしてデフォルト・ドメインを受け入れます。
6. 「次へ」をクリックして「ターゲット・ドメイン」ページから「ワークフロー定義」ページに移動します。
7. ワークフローの「開始」ステップを作成します。
「参加者」タブをクリックし、参加者を「すべてのユーザー」ロールとして定義します。
「属性」タブをクリックし、ワークフロー参加者に入力してほしい「姓」や「名」などの属性を選択します。
8. 「新規」をクリックし、「有効化」アクション・タイプで新規ステップを作成します。
「追加」をクリックし、「有効化」ステップのエントリ条件として「開始」ステップを追加します。
「参加者」をクリックし、参加者として「すべてのユーザー」を選択します。
「属性」をクリックし、このステップで提供される属性を追加します。
9. ワークフローを保存して有効化します。
10. User Manager で新規ユーザーの作成を試み、ワークフローをテストします。

サブフローの定義

サブフローに指定できるのは、属性の変更ワークフロー・タイプのみです。これらのワークフローは、ワークフロー定義ページでサブフローとして明示的に構成する必要があります。また、すべてのサブフローには承認ステップ・アクションが含まれる必要もあります。

注意：ワークフローをサブフローとして使用可能にするには、ワークフロー定義の最初のページにある「サブフローとして使用」を選択する必要があります。

サブフローを作成する手順

1. ID システム・コンソールで、「User Manager」、「Group Manager」または「Org. Manager」アプリケーション・タブをクリックします。
2. 「構成」をクリックします。
3. 「ワークフロー定義」をクリックします。
4. 「新規」をクリックします。
5. 「ワークフロー名」フィールドにワークフローの名前を入力します。
6. 「サブフローとして使用」チェック・ボックスを選択します。
7. 「ワークフロー・タイプ」リストで、「属性の変更」を選択します。
8. 「次へ」をクリックします。
9. ワークフローの最初のステップで、ワークフローにより変更する属性を指定します。
10. 他のワークフローと同様に、ワークフローの残り部分を完成します。

注意：すべてのサブフロー定義には承認ステップ・アクションが含まれる必要があります。

サブフローとワークフローの関連付け

サブフローは、メイン・ワークフローの特定のワークフロー・ステップに関連付ける必要があります。ワークフローの実行時、特定のステップに構成されているサブフローは、そのステップ・アクションの実行後に起動されます。

サブフローをワークフローに関連付ける手順

1. 5-20 ページの「[「ワークフロー定義」アプレットにアクセスする手順](#)」に従ってワークフロー・アプリケーションを起動します。
2. サブフローを割り当てるワークフローを選択します。
3. 「変更」をクリックします。
ページがリフレッシュされ、ステップ定義ページが表示されます。
4. 「サブフロー」タブをクリックします。
5. ページの「定義済ステップ」領域で、サブフローを挿入するワークフロー順序内の場所を選択します。
6. 「サブフロー」タブの「サブフローの選択」領域で、このワークフローの一部とするサブフローを選択します。

このステップに割り当てる 1 つ以上のサブフローを選択し、右矢印ボタン (>>) をクリックします。

注意：ここでサブフローが表示されない場合は、そのフローがサブフローとしてマークされており、有効化されていることを確認してください。また、サブフローのターゲットである属性は、サブフローの割当て先のワークフローでは使用できません。

7. ステップを保存します。
8. オプションで、後続の1つ以上のステップでサブフローの完了を待機するかどうかを指定できます。
 - a. サブフローが完了するまで遅延させるステップを選択し、「変更」をクリックします。
 - b. 「サブフローを待機」チェック・ボックスを選択します。

サブフロー・ステップの承認

「サブフロー承認」ステップでは、メイン・フローから起動されたサブフローの現在のステータスがレポートされます。デフォルトでは、ステータスは、「承認」ステップまたは承認ステップの間に「承認済」または「否認」に設定されます。このステップでは、属性の構成も可能です。

注意：サブフロー・ステータスは、ID イベント・プラグイン API または IdentityXML を使用してプログラム的に設定できます。ID イベント・プラグイン API の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

拡張ワークフロー・チケット・ルーティング

通常は、ワークフロー・ステップの作成時に指定した静的参加者が、そのステップの完了を担当するユーザーになります。処理上のボトルネックを避けるため、または各チケットをその処理に最も適した参加者に送信するため、次の3つの拡張チケット・ルーティング機能を使用して特定の状況下にある静的参加者を入れ替えることができます。

- ワークフロー作成時に静的参加者を指定するかわりに、ワークフロー・プラグインまたはアプリケーションを使用して実行時の状況に応じた動的参加者を選択できます。
- 静的または動的参加者が外出中などの理由によりワークフロー・チケットを処理できない場合、その参加者は自分のユーザー・プロファイルに「外出中」フラグを設定できます。このフラグがアクティブであるかぎり、すべての着信チケットはサロゲート参加者に転送されます。
- 所定のワークフロー・チケットを受信した参加者が一定の期間内にチケットを処理しない場合、そのチケットをエスカレーション参加者（チケット処理の責任を全面的に引き継ぐ参加者）に送信できます。

拡張チケット・ルーティングのためのワークフロー・アクションの構成

すべてのワークフロー・ステップを拡張チケット・ルーティング用に構成できるわけではありません。たとえば、ワークフローの最初のステップは、再ルーティングできません。ただし、最初のステップを再ルーティングする必要はありません。ワークフローを開始するユーザーは最初のステップの参加者でもあり、最初のステップは常にワークフローの開始操作であるためです。

ユーザー・アクションを伴わないステップは、定義上ユーザー参加者を含むことがないため、再ルーティングできません。たとえば、外部データベースからプロビジョニング・データを自動的に取得するステップは、ユーザー参加者を含まないため、参加者を入れ替えても意味がありません。

次の表に、ワークフロー・ステップに関連付けることのできるユーザー・アクションをリストします。

表 5-9 拡張チケット・ルーティングで使用できるユーザー・アクション

ユーザー・アクション	可用性
承認	
情報の提供（承認あり）	デフォルトでは、動的参加者、サロゲートおよび時間ベース・エスカレーションで使用可能です。
開始	
自己登録	
情報の提供	
サブフロー承認	
アクティブ化	デフォルトでは、動的参加者とサロゲートで使用可能です。適切なワークフロー・パラメータ・ファイルを変更することで、時間ベース・エスカレーションでも有効化できます。詳細は、5-48 ページの「 ワークフロー・パラメータ・ファイルを変更する手順 」を参照してください。
非アクティブ化	
エラー・レポート	
グループの選択	
リクエスト	
情報の変更	
情報の変更（承認あり）	

新規に割り当てられたステップ参加者への通知

ワークフロー・アプレットの「メール通知」タブを使用すると、ワークフロー・チケットの再ルーティング時にタスクを完了するよう割り当てられた参加者に電子メール通知を構成できます。チケットの再ルーティングを適用するステップごとにメール通知を構成できます。

拡張チケットの再ルーティングを伴うステップにメール通知を構成するには、次の手順を実行します。

拡張ワークフロー・チケットの再ルーティング用に電子メール通知を構成する手順

1. 変更するワークフローに応じて User Manager、Group Manager または Organization Manager に移動し、「構成」→「ワークフロー定義」をクリックします。
2. 変更するワークフローを選択し、「変更」をクリックします。
3. 属性の変更ワークフローを変更する場合、「次へ」を1回クリックします。それ以外のタイプのワークフローの場合、「次へ」を2回クリックします。
4. メール通知を設定するステップを選択し、「変更」をクリックします。
5. 「メール通知」タブをクリックします。
6. 静的、動的およびサロゲート参加者に対する通知を有効化するため、「事前通知する参加者の選択」または「事後通知する参加者の選択」を選択します。
ワークフローの最初のステップでは、「事前通知する参加者の選択」は選択できません。
7. 個人、グループ、ロールまたはルールに基づいて、通知するユーザーを指定します。
通知するユーザーを指定する場合、セレクトアやフィルタ・ビルダーなどの機能を使用できます。
8. エスカレーション参加者に通知する必要がある場合、「エスカレーション通知先の選択」をクリックし、手順7を繰り返します。
9. 「ステップの保存」をクリックしてステップ固有の変更をコミットします。
10. 「ワークフローの保存」をクリックしてワークフロー全体を保存します。

動的参加者の指定

動的参加者機能は、実行時の状況に基づいてワークフロー・チケットを代替参加者に自動ルーティングできる拡張ワークフロー・オプションの1つです。

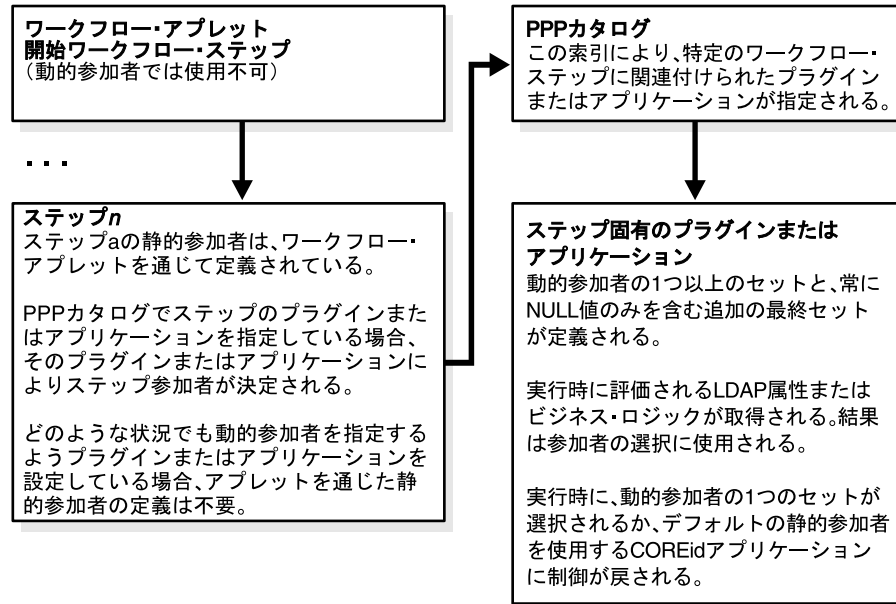
ワークフロー参加者の概要

ID システムでは、次の2つのタイプのワークフロー参加者がサポートされます。

- 静的参加者：このタイプの参加者は、通常、ワークフロー・ステップの定義時にワークフロー・アプレットを通じて指定します。たとえば、新規従業員のネットワーク・アカウントを設定するワークフローを作成する際に、すべての着信チケットをネットワーク・セキュリティ・マネージャにルーティングする承認ステップを含めることができます。後でワークフロー・プラグインまたはアプリケーションを追加しないかぎり、この事前指定された静的参加者が、ワークフロー・ステップで生成されるすべてのチケットの主要な受信者として機能します。
- 動的参加者：このタイプの参加者は、ワークフロー・アプレットではなく、ワークフロー・プラグインまたはアプリケーションで指定する必要があります。これらの状況依存型の参加者は、実行時の属性値または外部ビジネス・ロジックに基づいて選択されます。たとえば、プラグインを使用して、2,500 ドルを超えるすべての購買リクエストを経理担当マネージャに、50 ドル未満のすべてのリクエストを会計事務員に、他のすべてのリクエストを作業可能な経理担当者（経理担当者）にルーティングするよう指定できます。

ワークフロー・チケット・ルーティングの概要

次の図に示すとおり、ワークフローが実行され、動的参加者が有効化されているステップにプログラム実行が到達すると、ワークフロー・プラグインまたはアプリケーションにより、動的参加者のセットが選択されてそれらのユーザーにワークフロー・チケットが送信されます。プラグインまたはアプリケーションで動的参加者が選択されない場合、コール側のアプリケーションにより、ワークフロー・プラグインまたはアプリケーションによる介入がない場合と同じように元の静的参加者にチケットが送信されます。



動的参加者の概要

動的参加者は、静的参加者を指定する場合と同じ基準を使用して指定します。これには、個人、グループ、ロールおよびルールに基づく指定が含まれます。詳細は、5-25 ページの「次のいずれかの方法を使用して参加者を指定します。」の手順を参照してください。

動的参加者は、ワークフローのすべてのステップで定義できます（ただし、静的参加者が開始する必要のある最初のステップは除きます）。

ステップ・インスタンスが実行時に割り当てられると、静的参加者が通常取得するのと同じチケット処理権限が動的参加者により継承されます。これらの権限は、特に動的参加者に割り当てられるチケットにのみ拡張されます。つまり、動的参加者は、「代替権限」機能を使用して委任が作成される場合のように元の参加者に割り当てられたすべての権限を取得することはありません。2-10 ページの「代替管理者の追加」を参照してください。

動的参加者の ID は、関連するワークフロー・ステップが実行されるまで不明のため、特定のワークフロー・サービス（前のワークフロー・ステップにより生成される事後アクション電子メールなど）では使用できません。ただし、動的参加者を選択するワークフロー・ステップにより生成される事前アクション電子メールを使用して、動的参加者に通知を行うことは可能です。5-40 ページの「動的参加者に対応するワークフロー・ステップを準備する手順」を参照してください。

静的参加者の概要

通常の状況下のワークフロー・ステップでは、ワークフロー・アプレットを通じて指定された静的参加者が使用されます。

特定のステップに対して oblixpppcatalog カタログ・ファイルでプラグインまたはアプリケーションを指定している場合、プラグインまたはアプリケーションにより、実行時の値の評価に応じて先に動的参加者が選択されます。プラグインまたはアプリケーションが動的参加者のセットを指定できない場合にのみ、静的参加者が主要なステップ参加者として指定されているメイン・アプリケーションに制御が戻されます。

「静的参加者が使用不可」ボタンの概要

特定のステップではワークフロー・プラグインまたはアプリケーションにより常に動的参加者が選択されると事前に判明している場合、そのステップに静的参加者を定義する必要はありません。ただし、静的参加者を指定しない場合、デフォルトの「静的参加者が使用可能」ボタンを「静的参加者が使用不可」に切り替える必要があります。次の図に示すとおり、これらのラジオ・ボタンは、ワークフロー・アプレットの「参加者」タブに表示されます。このアプレットには、構成中のワークフローに適した User Manager、Group Manager または Organization Manager を通じてアクセスできます。

属性アクセス制御 委任管理 **ワークフロー定義** 検索ベースの設定

ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

ワークフロー名: test ワークフロー・タイプ: 属性の変更

定義済ステップ: [ステップ1]リクエスト

新規 変更 ステップの削除 ステップを挿入

ステップ・プロパティ

アクション サブフロー 属性 **参加者** 外出中 エスカレーション メール通知

参加者の選択

静的参加者が使用可能
 静的参加者が使用不可

ロールの選択

すべてのユーザー 自己

フィルタの作成

フィルタの作成

人々の選択

ユーザーの選択

グループの選択

グループの選択

ステップの保存

ワークフローの保存 ワークフローの取消し 前へ

動的参加者の有効化

動的参加者機能は、デフォルトでは有効化されません。この機能をアクティブ化するには、次のタスクの概要に記載されている手順を完了する必要があります。

タスクの概要：ワークフロー・ステップへの動的参加者の割当て

1. クイックスタート・ツールまたはワークフロー・アプレットを使用して、動的参加者を利用するステップを含むワークフローを作成します。

詳細は、5-16 ページの「[クイックスタート・ツールの使用方法](#)」および 5-19 ページの「[ワークフロー・アプレットの使用方法](#)」を参照してください。

2. 特定のステップで静的参加者を使用する可能性がある場合は、そのステップの静的参加者を定義する必要があります (5-25 ページの「[次のいずれかの方法を使用して参加者を指定します。](#)」の手順を参照してください)。

ただし、特定のステップで常に動的参加者が使用されると事前にわかっている場合は、そのステップに静的参加者を定義する必要はありません。詳細は、5-38 ページの「[静的参加者が使用不可](#)」ボタンの概要」を参照してください。

3. 必要に応じて、動的参加者の電子メール通知を設定します。

詳細は、5-40 ページの「[動的参加者に対応するワークフロー・ステップを準備する手順](#)」を参照してください。

4. 動的参加者を選択するための適切なプラグインまたはアプリケーションが実行時にコールされるように、oblixpppcatalog カタログ・ファイルにポインタを追加します。

詳細は、5-40 ページの「[oblixpppcatalog.lst を変更する手順](#)」を参照してください。

5. 実行時に動的参加者を選択するための事前アクション・プラグインまたはアプリケーションを作成します。

一般的なプラグインまたはアプリケーションには、次の処理を実行するコード・セクションが含まれます。

- 動的参加者の 3 つ以上のセットを指定します。最後のセットには、常に NULL 値のみが含まれます。
- 実行時に評価する属性またはビジネス・ロジックを指定します。
- 評価に基づいて動的参加者を選択します。
- 選択された参加者が実際に ID システム・ディレクトリに存在することを確認します。存在しない場合、動的参加者の選択プロセスは失敗しますが、ワークフロー・エンジンからエラー・メッセージは戻されません。
- 動的参加者のリストをコール側の ID システム・アプリケーションに渡します。

詳細は、5-41 ページの「[タスクの概要：動的参加者を選択するプラグインまたはアプリケーションの作成](#)」を参照してください。

警告：動的参加者を有効化するプラグインおよびアプリケーションは、事前アクション・タイプである必要があります。事後アクション・タイプは使用できません。

動的参加者に対応するワークフロー・ステップを準備する手順

1. User Manager、Group Manager または Organization Manager で、「構成」に移動し、「ワークフロー定義」をクリックします。
2. 「ワークフロー」リストで、動的参加者に対応するよう準備するステップを含むワークフローを選択し、「変更」をクリックします。
3. 現在のワークフロー・ステップで最終的に静的参加者を使用する可能性がある場合は、ロール、ルール、個人またはグループに基づいて静的参加者を定義します (5-25 ページの「次のいずれかの方法を使用して参加者を指定します。」の手順を参照してください)。

前述の条件が適用されない場合、またはこのステップに対してすでに静的参加者を定義している場合、直接手順 4 に進んでください。
4. 現在のワークフロー・ステップでプラグインまたはアプリケーションを使用して動的参加者を指定し、かつ現在のステップで静的参加者が最終的にワークフロー・チケットを受信するような状況が発生しない場合、「静的参加者が使用不可」ボタンを選択します (5-38 ページの「静的参加者が使用不可」ボタンの概要」を参照してください)。それ以外の場合、直接手順 5 に進んでください。
5. 必要に応じて電子メール通知を設定します。これを行うには、「メール通知」タブをクリックし、「事前通知する参加者の選択」ボタンを選択します。次に、「ロールの選択」ボックスで「現在のステップの参加者」を選択します。動的参加者が最終的に選択されると、それらの参加者は、ワークフロー・チケットが割り当てられたという内容の電子メールを受信します。

注意: 「静的参加者が使用可能」スイッチがアクティブであると、「事前通知する参加者の選択」ボタンにより静的参加者に対する電子メール通知が有効化されます。これに対し、「静的参加者が使用不可」スイッチがアクティブであると、動的参加者に通知が送信されます。

6. 「ステップの保存」をクリックしてステップ固有の情報をコミットし、「OK」をクリックして操作の確認を求めるプロンプトを閉じます。
7. 「ワークフローの保存」をクリックしてワークフロー全体に関連する情報をコミットし、「OK」をクリックして操作の確認を求めるプロンプトを閉じます。ワークフローを有効化するかどうかを尋ねる追加のプロンプトが表示されたら、「はい」をクリックします。

oblixpppcatalog.lst を変更する手順

1. 次の手順を実行して、動的参加者を設定するステップを含むワークフローのワークフロー ID を特定します。
 - a. 変更するワークフローに応じて、User Manager、Group Manager または Organization Manager を起動します。
 - b. 「構成」タブをクリックし、次に「ワークフロー定義」をクリックします。
 - c. 変更するワークフローを選択し、「表示」をクリックします。
 - d. obworkflowid の「ワークフロー定義ビュー」にレポートされる値を書き留めます。この値は、次のような文字列で示されます。

Workflow DN : obworkflowid=5985de47196a4a728a629a429b6a5194

2. 任意のプレーン・テキスト・エディタを使用して、次のディレクトリにある oblixpppcatalog.lst ファイルを開きます。

`IdentityServer_install_dir\identity\oblix\apps\common\bin`

ここで、`IdentityServer_install_dir` は、ワークフローを実行する Identity Server のルート・インストール・フォルダです。

3. 次のいずれかの文字列を `oblixpppcatalog.lst` に追加します。

```
obworkflowid_workflowstep_preaction;lib;;
Component_install_dir\identity\oblix\path\pluginName.dll;
functionName;
```

または

```
obworkflowid_workflowstep_preaction;exec;;
Component_install_dir\identity\oblix\path\applicationName.exe;
functionName;
```

この場合：

- `obworkflowid` は、この説明の手順 1d で書き留めたワークフローの ID 番号です。
- `workflowstep` は、動的参加者を定義するステップです。
- `path` は、`Component_install_directory\identity\oblix\` から `pluginName.dll` または `applicationName.exe`（実行時に動的参加者を選択するコード・オブジェクト）までのパスです。
- `functionName`: プラグインを指定する場合、動的参加者の基準を設定するダイナミック・リンク・ライブラリ・プラグイン内の関数を示す `functionName` も指定する必要があります。

プラグインを使用して動的参加者を指定する場合、前述の最初のコード行を挿入します。プラグインではなく実行可能プログラムを使用する場合、2 番目の行を挿入します。

どちらの場合でも、挿入行はセミコロンで終了する必要があります。これらの行は、既存の行を分断しないかぎり、`oblixpppcatalog.lst` ファイルのどこにでも配置できます。

挿入する行は、次のようになります。

```
wfqs20040901T17251953156_2_preaction;lib;;
Component_install_dir\identity\oblix
\unsupported\ppp\ppp_dll\ppp_dll.dll;
WorkflowPreActionSetDynamicParticipantsTest;
```

4. `oblixpppcatalog.lst` を元の場所に保存します。

`oblixpppcatalog.lst` ファイルの詳細は、『Oracle Access Manager 開発者ガイド』も参照してください。

タスクの概要：動的参加者を選択するプラグインまたはアプリケーションの作成

1. C++ を使用して、5-40 ページの「[oblixpppcatalog.lst を変更する手順](#)」で指定したワークフロー・ステップにプログラム実行が到達したときに動的参加者を選択するプラグインまたはアプリケーションを作成します。
2. LDAP 属性または独自仕様のビジネス・ロジックを様々に組み合わせて、実行時に他の参加者に優先して動的参加者の 1 つのグループを選択する条件を指定します。
3. プラグインまたはアプリケーションに次のヘッダー・ファイルをインクルードします。これらのファイルにより、動的参加者の選択に必要な事前アクション処理が有効化されます。

```
obppp.h
obpppwf.h
obpppdata.h
```

4. アプリケーションまたはプラグイン内で、ロール、ルール、個人またはグループの任意の組合せを使用して動的参加者の3つ以上のセットを定義します。各配列の最後の項目は、常に NULL である必要があります。たとえば、次のようになります。

- a. 個人を指定する場合、次のような行を挿入します。

```
PPPSetsVals[0] = "cn=Van Oman, ou=Sales, ou=Dealer1k1,
ou=Latin America, ou=Ford, o=Company,c=US";
PPPSetsVals[1] = "cn=Fabien Esser, ou=Sales, ou=Dealer1k1,
ou=Latin America, ou=Ford, o=Company,c=US";
PPPSetsVals[2] = NULL;
data->Set("DynamicParticipant.Persons", PPPSetsVals);
```

- b. グループを指定する場合、次のような行を挿入します。

```
PPPSetsVals[0] = "cn=Basic group1k1, ou=Groups, ou=Dealer1k1,
ou=Latin America, ou=Ford, o=Company,c=US";
PPPSetsVals[1] = "cn=Basic group1k2, ou=Groups, ou=Dealer1k1,
ou=Latin America, ou=Ford, o=Company,c=US";
PPPSetsVals[2] = NULL;
data->Set("DynamicParticipant.Groups", PPPSetsVals);
```

- c. ロールを指定する場合、次のような行を挿入します。

```
PPPSetsVals[0] = "ob_self";
PPPSetsVals[1] = "manager";
PPPSetsVals[2] = NULL;
data->Set("DynamicParticipant.Roles", PPPSetsVals);
Remember, of course, that only certain roles are valid for particular workflow
types. See page 200.
```

- d. ルールを指定する場合、次のような行を挿入します。

```
PPPSetsVals[0] = "(cn=rohit*)";
PPPSetsVals[1] = "(cn=beth*)";
PPPSetsVals[2] = NULL;
data->Set("DynamicParticipant.Rules", PPPSetsVals);
```

サロゲートの指定

静的または動的参加者が特定のワークフロー・ステップに割り当てられたアクションを実行できないときに、その参加者が自分のユーザー・プロファイルに「外出中」フラグを設定して、着信ワークフロー・チケットを1人以上の指定されたサロゲート参加者に転送できるよう ID システム・アプリケーションを構成できます。再ルーティングされるチケットを処理するために元の参加者が保持していたすべての権限は、サロゲートに付与されます。

「外出中」フラグのアクティブ化後に作成されたチケットのみがサロゲートに再ルーティングされます。「外出中」フラグのアクティブ化前に作成されたすべてのチケットの処理を担当するのは、引き続き元の参加者です。

「外出中」フラグを有効化すると、その効果は参加者が静的参加者または潜在的な動的参加者として指定されているすべてのワークフローのすべてのステップに適用されます。

「外出中」フラグをオフにリセットすると、新しく作成されたチケットは再び元の参加者にルーティングされます。サロゲートは、「外出中」フラグがアクティブなときに自分に対してルーティングされたすべてのチケットの処理を担当しますが、元の参加者が再度「外出中」フラグをアクティブ化しないかぎり、新規チケットはサロゲートにルーティングされません。

元の参加者にチケット割当てを送信する場合と同じワークフロー・アプレット設定により、サロゲートとその他のユーザーに「外出中」フラグのためワークフロー・チケットが再ルーティングされたという内容の通知も行われます。

タスクの概要：サロゲートの有効化

1. ID システム・コンソールの「共通構成」タブで、任意の属性を「外出中」セマンティック型に関連付けます。

この操作は1回のみ行う必要があります。詳細は、「[外出中属性を「外出中」セマンティック型に関連付ける手順](#)」を参照してください。

2. ワークフロー・アプレットの「外出中」タブで、1人以上のサロゲートを指定します。

詳細は、5-25 ページの「[次のいずれかの方法を使用して参加者を指定します。](#)」の手順を参照してください。

3. 個々のユーザーが、ユーザー・プロファイルの「外出中」フラグをアクティブ化します。

詳細は、5-44 ページの「[「外出中」フラグを使用する手順](#)」を参照してください。

外出中属性を「外出中」セマンティック型に関連付ける手順

1. 「外出中」セマンティック型に関連付ける LDAP ディレクトリの属性を選択します。

これは、ユーザーが外出中であるかどうかを示すブール値を保持する属性である必要があります。簡便化のため、製品には `obOutofOfficeIndicator` 属性が付属していますが、ディレクトリ内の適切な属性を任意に使用できます。

2. ID システム・コンソールに移動し、「共通構成」→「オブジェクト・クラス」→ `Person` オブジェクト・クラス (`gensiteorgperson` など) →「属性の変更」を選択します。

3. 属性リストで、関連付ける属性を選択します。

4. 「セマンティック型」フィールドで、「外出中 - インジケータ」を選択します。

このインジケータを保持できるのは、一部の属性のみです。たとえば、`gensiteOrgPerson` の `genuserid` 属性は、このインジケータを保持できます。

The screenshot shows the Oracle Identity Administration console interface. The breadcrumb navigation is: システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成. The user is logged in as Rohit Valiveti. The left sidebar shows navigation options: オブジェクト・クラス (selected), ワークフロー・パネル, マスター監査ポリシー, グローバル監査ポリシー. The main content area is titled '属性の変更' (Attribute Change). Below the title, there is a description: '属性の変更では、gensiteorgpersonオブジェクト・クラスに含まれている属性の表示名、セマンティック型、表示タイプおよび属性値の変更や構成ができます。変更後は、「完了」ボタンをクリックして属性情報を保存してください。' Below this, there are four input fields: '属性' (Attribute) with a dropdown menu showing 'genUserID' selected; '表示名' (Display Name) with a text box containing 'genUserID'; 'セマンティック型' (Semantic Type) with a dropdown menu showing '外出中 - インジケータ' selected; and '属性値' (Attribute Value) with radio buttons for '単一' (Single) and '複数' (Multiple), where '単一' is selected. Below these fields, there are two more fields: 'データ型' (Data Type) with a text box containing '文字列(大/小文字の区別なし)' and '表示タイプ' (Display Type) with a dropdown menu showing 'ブール' (Boolean) selected. At the bottom, there is a message: '使用可能な表示タイプ・プロパティがありません' (No available display types or properties).

5. 「表示タイプ」ボックスで「ブール」を選択し、「完了」をクリックして変更をコミットします。

注意： この手順は、1回のみ実行する必要があります。

サロゲートを指定する手順

1. 1人以上のサロゲートを指定するステップを含む特定のワークフローに応じて **User Manager**、**Group Manager** または **Organization Manager** にログインし、「構成」に移動して「ワークフロー定義」を選択します。
2. サロゲートを指定するステップを含むワークフローを選択し、「変更」をクリックします。
3. 属性の変更ワークフローを変更する場合、「次へ」を1回クリックします。
それ以外のタイプのワークフローを変更する場合、「次へ」を2回クリックします。
4. サロゲートを指定するステップを選択し、「変更」をクリックします。
ページがこのステップの情報でリフレッシュされます。ページがリフレッシュされない場合、ステップが選択されていることを確認してください。選択されていない場合、ステップを再度クリックし、次に「変更」をクリックします。
ユーザー・アクションに関連付けられた任意のワークフロー・ステップのサロゲートを指定できます。
5. 「外出中」タブをクリックします。
6. 個人、グループ、ロールおよびルールを指定するツールを組み合わせ、1人以上のサロゲートを指定します。
詳細は、5-25 ページの「次のいずれかの方法を使用して参加者を指定します。」の手順を参照してください。
「間接ロールの選択」ボックスには、ディレクトリに現在定義されている任意のロールを選択するためのチェック・ボックスが含まれます。これらのロールは、ワークフロー・ターゲットではなく現在の参加者に適用されるため、間接的であるとみなされます。
7. 「ステップの保存」をクリックしてステップの変更をコミットします。
属性を構成するよう求める警告が表示された場合、このステップに対して属性を選択していることを確認してください。
8. サロゲートを指定するワークフロー・ステップごとに前述の手順を繰り返します。
9. 「ワークフローの保存」をクリックしてワークフロー全体を保存します。

「外出中」フラグを使用する手順

1. 静的または動的参加者となる可能性のあるユーザーに対し、この手順に記載されている操作を実行するのに十分な権限（検索、読取りおよび書込み）が付与されていることを確認してください。
2. 属性に「外出中」フラグが構成されていることを確認します。
3. **User Manager** に移動し、「プロファイル」を選択して「変更」をクリックします。
4. 「個人情報」セクションで、「外出中インジケータ」を「True」に切り替えます。（デフォルトでは、この属性は「False」です。）
5. 「保存」をクリックして変更をコミットし、「OK」をクリックして操作の確認を求めらるポップアップを閉じます。

時間ベース・エスカレーションの有効化

ワークフロー・チケットの処理を割り当てられた1人以上の参加者が一定の期間内にチケットを処理しない場合、チケットを別の参加者に自動的に再ルーティングすることでそのチケットをエスカレーションできます。元の参加者は、エスカレーションされたチケットを処理できません。この場合、エスカレーション参加者がチケットを処理する必要があります。エスカレーション参加者は、チケット処理のために元の参加者に付与されていたすべての権限を継承します。

割り当てられた時間内にエスカレーション参加者がチケットを処理しない場合、チケットは再度エスカレーションされ、最終的にはエスカレーション・チケットの処理を担当できる最後の参加者であるIDシステム管理者までエスカレーションされます。

デフォルトでは、任意のワークフロー・ステップで時間ベース・エスカレーションを有効化できますが、次の2つの条件を満たしている必要があります。

- エスカレーションされるステップは、ワークフローの開始ステップではないこと。
- ステップに関連付けられたアクションがエスカレーションに対応していること。デフォルトでは、「承認」および「情報と承認の提供」のみがエスカレーションに対応していますが、適切なワークフロー・パラメータ・ファイルに行を追加することで他のアクションでも対応できます。詳細は、5-48 ページの「[ワークフロー・パラメータ・ファイルを変更する手順](#)」を参照してください。

時間ベース・エスカレーションを有効化する手順

1. 時間ベース・エスカレーションを設定する特定のワークフローに応じて User Manager、Group Manager または Organization Manager にログインし、「構成」に移動して「ワークフロー定義」をクリックします。

2. エスカレーションを設定するワークフローを選択し、「変更」をクリックします。

保留中のチケットがワークフローに存在する間に変更できるのは一部の設定のみであると警告するポップアップが表示されたら、「OK」をクリックしてポップアップを閉じます。属性の変更ワークフローを変更する場合、「次へ」を1回クリックします。それ以外のタイプのワークフローを変更する場合、「次へ」を2回クリックします。

3. エスカレーションを有効化するステップを選択し、「変更」をクリックします。

ページがこのステップの情報でリフレッシュされます。ページがリフレッシュされない場合、ステップが選択されていることを確認してください。選択されていない場合、ステップを再度クリックし、次に「変更」をクリックします。

選択するステップは、エスカレーションに対応するアクションに関連付けられている必要があります。デフォルトでは、「承認」および「情報と承認の提供」が対応しています。時間ベース・エスカレーションをサポートする追加アクションを有効化する方法の詳細は、5-48 ページの「[ワークフロー・パラメータ・ファイルを変更する手順](#)」を参照してください。

4. 「エスカレーション」タブをクリックします。

5. チケットをエスカレーションするまでに待機する期間を指定します。期間は、日、分、時間単位で設定できます。この期間は、すべてのエスカレーション・レベルに適用されます。



ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

ワークフロー名: time-based escalation ワークフロータイプ: ユーザーの作成

定義済ステップ:

- [ステップ1] 開始
- [ステップ2] 情報と承認の提供
- [ステップ3] 有効化

ステッププロパティ

アクション サブフロー 属性 参加者 外出中 **エスカレーション** メール通知

エスカレーションのアイドル時間: 5 日

エスカレーション・レベル数: 1 レベル

参加者にルーティング

間接ロールの選択: マネージャ 秘書

6. チケットのエスカレーション先となる 1 人以上の参加者を指定します。ロールは、ワークフロー・ターゲットに対してではなく、最新のエスカレーションを起動せずに済む期間内にチケットを処理できなかった参加者に対して評価されるため、間接ロールとなります。たとえば、「間接ロールの選択」ボックスで「マネージャ」を選択した場合、最初にチケットを受信した経理担当者がチケットを迅速に処理しないと、そのチケットは（ワークフロー・ターゲットのマネージャではなく）経理担当者のマネージャにエスカレーションされます。
7. チケットをエスカレーションする回数（レベル数）を指定します。この数には、最終エスカレーション・レベル（常にチケットがルーティングされる ID システム管理者）は含まれません。

エスカレーション参加者の 1 つのセットのみ指定できます。この 1 つのセットは、すべてのエスカレーション・レベルに適用されます。たとえば、ただ 1 人のユーザーを指定すると、エスカレーションが起動されるたびにそのユーザーにチケットがエスカレーションされます。そのエスカレーション参加者がいずれかのレベルにおいてチケットを処理しない場合、チケットは最終的に ID システム管理者にエスカレーションされます。

一方、各レベルの異なるユーザーにより保持されているロールを指定すると、チケットは各レベルの異なるユーザーにエスカレーションされます。たとえば、「マネージャ」を指定すると、チケットは最初にそのチケットが発行されたユーザーのマネージャにエスカレーションされます。その後、そのマネージャのマネージャに、さらにそのマネージャのマネージャにという形でエスカレーションが続きます。

8. 「ステップの保存」をクリックして「エスカレーション」タブで入力した設定をコミットします。

9. 「メール通知」タブをクリックし、エスカレーションを通知するユーザーを指定します。



ワークフロー定義

管理者は、ワークフロー定義を使用して組織ごとに異なるワークフローを定義できます。ワークフローごとにステップ、属性、参加者が異なります。クイックスタートを使用したワークフローの作成方法 [ここをクリック](#)

ワークフロー名: time-based escalation ワークフロータイプ: ユーザーの作成

定義済ステップ:

- [ステップ1] 開始
- [ステップ2] 情報と承認の提供
- [ステップ3] 有効化

新規 変更 ステップの削除 ステップを挿入

ステップ・プロパティ

アクション サブフロー 属性 参加者 外出中 エスカレーション **メール通知**

参加者の選択:

- 事前通知する参加者の選択
- 事後通知する参加者の選択
- エスカレーション通知先の選択

ロールの選択:

- 前のステップの所有者
- 現在のステップの参加者
- 次のステップの参加者
- 開始者

フィルタの作成

フィルタの作成

10. 「エスカレーション通知先の選択」を選択します。
11. 個人、グループ、ロールまたはルールに基づいて、通知するユーザーを選択します。使用可能なロールは、次のとおりです。
- **前のステップの所有者:** 前のステップを完了した参加者です。
 - **現在のステップの参加者:** エスカレーションされたチケットを処理するよう現在割り当てられているユーザーです。
 - **次のステップの参加者:** 次のステップを処理するよう割り当てられているユーザーです。この場合、次のステップに定義されている静的参加者にのみ通知が行われます。これは、実行フローが次のステップに到達し、動的参加者の ID が決定される前に電子メール通知が送信されるためです。
 - **開始者:** ワークフローを開始したユーザーです。

ワークフロー・パラメータ・ファイルを変更する手順

1. 「承認」または「情報と承認の提供」以外のユーザー・アクションで時間ベース・エスカレーションを有効化する場合にのみこの手順を実行します。時間ベース・エスカレーションに対応可能なユーザー・アクションのリストは、表 5-9 を参照してください。
2. 任意のプレーン・テキスト・エディタを使用して、時間ベース・エスカレーションを有効化するアクションを含むワークフローに適したワークフロー・パラメータ・ファイルを開きます。

表 5-10 に、様々な ID システム・アプリケーションに関連付けられたワークフローに適用されるワークフロー・パラメータ・ファイルをリストします。

表 5-10 ワークフロー・パラメータ・ファイルの名前とパス

アプリケーション	ワークフロー・パラメータ・ファイルの名前とパス
User Manager	<code>IdentityServer_install_dir/identity/oblix/apps/user servcenter/bin/usc_wf_params.xml</code>
Group Manager	<code>IdentityServer_install_dir/identity/oblix/apps/grou pservcenter/bin/gsc_wf_params.xml</code>
Organization Manager	<code>IdentityServer_install_dir/identity/oblix/apps/obj servcenter/bin/osc_wf_params.xml</code>

3. 時間ベース・エスカレーションをサポートするアクションの複合リストの場所を見つけます。例 5-1 に、この複合リストの前半部分の内容を示します。

例 5-1 ワークフロー・パラメータの複合リスト（一部）

```
<CompoundList ListName="actionName">
  <SimpleList >
    <NameValPair ParamName="occurrence" Value="n"/>
    <NameValPair ParamName="useraction" Value="true"/>
    <NameValPair ParamName="initialStep" Value="false"/>
    <NameValPair ParamName="time_based_escalation" Value="true"/>
  </SimpleList>
  . . .
</CompoundList>
```

ここで、*actionName* は、時間ベース・エスカレーションを有効化するアクションの名前です。時間ベース・エスカレーションに対応可能なアクションのリストは、表 5-9 を参照してください。

4. 次の文字列を、前述のリストで指定された位置に追加します。


```
<NameValPair ParamName="time_based_escalation" Value="true"/>
```
5. 時間ベース・エスカレーションをサポートするすべてのユーザー・アクションに対してここまでの手順を繰り返します。
6. ファイルを保存して閉じます。

非同期操作の実行

非同期ワークフローは、保留中のサブフローの完了を待機せずにステップからステップへと進みます。非同期操作は、ID イベントの一部である前処理および後処理コードです（『Oracle Access Manager 開発者ガイド』を参照してください）。保留中の非同期アクションを再開できるユーザーは、`asynch_user` パラメータにより決定します。デフォルトは `Anyone` です。

ユーザーに非同期操作の実行を許可する手順

1. 次の場所にある `asynchparams.xml` ファイルを開きます。

```
IdentityServer_install_dir/oblix/apps/asynch/bin/asynchparams.xml
```

ここで、`IdentityServer_install_dir` は、Identity Server がインストールされているディレクトリです。

2. `asynch_user` パラメータに次のいずれかの値を設定します。

- `Anyone`: すべてのユーザーが非同期操作を実行できます（デフォルト）。
- `DN`: 特定の 1 人のユーザーが非同期操作を実行できます。ユーザーの DN を指定します。

パラメータに指定できるのは、1 つの DN のみです。

3. `asynchparams.xml` ファイルを閉じます。

非同期ワークフローに関する留意事項

User Manager、Group Manager および Organization Manager は、非同期ワークフローが再開したときに自動的にロードされません。アプリケーションがロードされない状態で非同期ワークフローを再開するリクエストが Identity Server に送信されると、ワークフロー・エンジンではエラー状態を登録できない可能性があります。

例として、User Manager でユーザーの非アクティブ化ワークフローを作成する場合を検討します。このワークフローには、「開始」ステップと「無効化」ステップのみが含まれます。ここで、`STATUS_PPP_WF_ASYNC` コードを戻すワークフローのイベント・プラグインを作成するとします（この場合、「開始」ステップ中にワークフロー・インスタンスは非同期状態となり、ワークフローを再開して「無効化」ステップを実行するコマンドが待機されます）。ID システムの再起動時にこのワークフローを再開する IdentityXML リクエストが発生すると、ワークフロー・エンジンにより間違えて成功のステータスが戻されます。この場合、実際にはユーザーが無効化されていない状態で、「無効化」ステップから完了のステータスが戻されます。

注意: Identity Server の再起動時に、User Manager、Group Manager および Organization Manager が事前ロードされていることを確認してください。

User Manager、Group Manager および Organization Manager を事前ロードする手順

1. 次の場所にある ID システムのパラメータ・ファイルを開きます。
`Identity_install_dir/identity/oblix/engine/obengineparams.xml`
2. このファイルで、ID システム・アプリケーションの次の構成情報を見つけます。
 - `<ValNameList ListName="groupservcenter">`
 - `<ValNameList ListName="userservcenter">`
 - `<ValNameList ListName="objservcenter">`
3. `Dll_Load` パラメータを 0 から 1 に変更します。Group Manager の例は、次のとおりです。

```
<ValNameList ListName="groupservcenter" >
<NameValPair ParamName="Dll_Name" Value="groupservcenter"/>
<NameValPair ParamName="Dll_Dir" Value="oblix/apps/groupservcenter/bin"/>
<NameValPair ParamName="Dll_Load" Value="1"/>
<NameValPair ParamName="Work_Dir" Value="oblix/apps/groupservcenter/bin"/>
```

ワークフローの使用法

ワークフローの定義が完了すると、ユーザーは、User Manager、Group Manager または Organization Manager の関連機能からワークフローを起動できます。ワークフローの「開始」以外のステップの参加者は、チケットを検索して処理できます。ユーザーは、ワークフロー・リクエストの削除、リクエストのアーカイブ、およびワークフローの進行状況のモニターを行うことが可能です。

ワークフロー定義で指定されたアクションを実行するには、ワークフローの参加者に、ワークフローに関連する属性を参照および変更できる権限が付与されている必要があります。

4-21 ページの「ユーザーによる LDAP データの表示および変更の許可」を参照してください。

ワークフローの起動

定義されたワークフローは、User Manager、Group Manager または Organization Manager の埋込み機能の一部となります。ワークフローは、そのワークフローの「開始」ステップの参加者として定義されているユーザーであれば、誰でも起動できます。たとえば、ユーザーの作成ワークフローを定義するとします。ワークフローに指定されたドメインのユーザーは、User Manager の「ユーザーの作成」機能からこのワークフローを起動できます。作成操作のために複数のワークフローが定義されている場合、そのオブジェクトの作成ページにリストが表示されます。



ユーザーは、属性の変更ワークフローも開始できます。属性の変更ワークフローは、ユーザーがアクセスを許可されているプロフィール・ページで使用できます。たとえば、プロフィール・ページに表示されるマネージャ属性に対してワークフローが定義されているとします。ユーザーは、所属部門を変更したときに、状況に応じて自分のマネージャの名前を変更するリクエストを発行する必要があります。このリクエストは、属性の変更ワークフローによって処理されます。

属性の変更ワークフローを起動する手順

1. User Manager で、「ID」をクリックし、次に「変更」をクリックします。
変更できるすべての属性の編集可能フィールドを含むユーザー・プロフィール・ページが表示されます。
2. 「削除をリクエスト」または「変更をリクエスト」ボタンのあるプロフィール・ページの属性について、その属性値を削除または変更するリクエストを発行できます。
これらのボタンは、「削除をリクエスト」または「変更をリクエスト」アクションを伴う属性の変更ワークフローまたはサブフローが作成されている場合に表示されます。
リクエストは、チケットの形式で送信されます。このチケットを処理するユーザーは、リクエストを承認または否認できます。詳細は、5-51 ページの「[チケットの検索と処理](#)」を参照してください。

チケットの検索と処理

ワークフローが開始されると、チケットの処理により後続のステップが生成されます。保留中のワークフロー・チケットは、User Manager、Group Manager および Organization Manager で検索できます。

ワークフロー・チケットを検索する手順

1. User Manager、Group Manager または Organization Manager で、「リクエスト」をクリックします。
2. 「リクエスト」ページで、「着信リクエスト」、「送信リクエスト」または「リクエストのモニター」をクリックします。
送信リクエストは、すでに処理済のチケットです。
3. 「検索」リストで、リクエストを表示するアプリケーションを選択します。
4. テキスト・フィールドに日数を指定します。すべてのリクエストを表示する場合は、このフィールドを空白のままにします。
5. 「実行」をクリックします。
ワークフロー・チケットのリストが表示されます。このリストは、検索基準に一致します。

チケットを処理する手順

1. User Manager、Group Manager または Organization Manager で、「リクエスト」をクリックします。
2. 「リクエスト」ページで、「着信リクエスト」をクリックします。
3. 「検索」リストで、リクエストを表示するアプリケーションを選択します。
4. テキスト・フィールドに日数を指定します。すべてのリクエストを表示する場合は、このフィールドを空白のままにします。
5. 「実行」をクリックします。
6. ワークフロー・チケットのリストが表示されます。このリストは、検索基準に一致します。
7. 着信リクエストのリンクをクリックします。
8. リクエストの詳細ページで、「プロセス」ボタンをクリックします。
このワークフローの参加者の場合、ワークフローの現在のステップに構成されている属性を含むページが表示されます。
9. このワークフローの必須属性を入力します。
たとえば、「ユーザーの作成」ステップの場合、状況により新規ユーザーの電子メール・アドレスを入力するよう求められます。このページで入力する必要のある情報は、ワークフローの現在のステップがどのように構成されているかにより決定されます。

10. ワークフローの現在のステップを完了するのに適切なボタンをクリックします。

たとえば、「ユーザーの作成」リクエストの場合、通常はこのチケットの詳細ページに「承認」ボタンと「否認」ボタンが含まれます。

ユーザーの非アクティブ化と再アクティブ化

ID システムで有効化されたユーザーは、非アクティブ化および再アクティブ化することが可能です。非アクティブ化されたユーザーは、ID システムにログインできなくなり、ID システムに表示されなくなります。非アクティブ化の効果は、ユーザーが現行セッションからログアウトした後に反映されます。「リクエストのモニター」権限を保持する管理者は、非アクティブなユーザーを参照し、それらのユーザーを永久に削除するか、再アクティブ化することが可能です。

注意：非アクティブなユーザーと削除されたユーザー（およびユーザーが所属するグループ）に対する参照を削除するため、構成済のすべてのディレクトリが検索されます。ユーザー・データと構成データを別々に格納している場合、両方のディレクトリが同時に検索されます。

ユーザーを非アクティブ化するワークフローを定義する手順は、5-19 ページの「[ワークフロー・アプレットの使用方法](#)」を参照してください。ワークフローが定義されると、十分な権限を保持するユーザーは、各ユーザーのプロファイル・ページで「ユーザーの非アクティブ化を開始」ボタンを参照できます。

The screenshot shows the Oracle Identity Administration User Manager interface. At the top, there are navigation tabs for 'User Manager', 'Group Manager', 'Org. Manager', and 'Identity System Console'. Below the tabs, there is a breadcrumb trail: 'プロフィール | レポート | ユーザーIDの作成 | 非アクティブなユーザーID | 代替権限 | リクエスト | 構成'. A search bar contains 'フルネーム' and '次を含む'. There are buttons for '検索', '実行', and '拡張'. The main content area shows the user profile for 'James Watson' with the role 'フルネーム'.

ユーザーを非アクティブ化する手順は、ユーザーの非アクティブ化ワークフローで指定されているアクションに準拠します。

非アクティブなユーザーの再アクティブ化

状況に応じて、非アクティブなユーザーを再アクティブ化できます。たとえば、休職中の従業員を非アクティブ化し、職場への復帰後にその従業員を再アクティブ化できます。

非アクティブなユーザーを再アクティブ化する手順

1. この目的に使用するユーザーの再アクティブ化ワークフローを定義します。

再アクティブ化ワークフローで許可されるアクションの概要は、5-7 ページの「ワークフローのタイプ、ステップおよびアクション」を参照してください。ワークフローが定義されると、十分な権限を保持するユーザーは、非アクティブなユーザーのプロファイル・ページで「ユーザーの再アクティブ化の開始」ボタンを参照できます。

2. User Manager で、「非アクティブなユーザー ID」サブタブをクリックし、非アクティブなユーザーの検索ページを表示します。

3. 検索を実行し、再アクティブ化する ID に対応する非アクティブなユーザー名を選択します。

「プロフィールの表示」ページが表示されます。

Oracle Identity Administration User Manager 検索ページ。検索条件として「フルネーム」を選択し、「次を含む」オプションが選択されている。検索結果は 8 件と表示されている。

非アクティブなユーザーの検索基準を指定してください

フルネーム 次を含む 結果数 8

実行

非アクティブなユーザー

前へ 次へ 削除 アーカイブ

すべて選択	フルネーム	組織単位	電話番号	役職	ログイン	再アクティブ化できます
<input type="checkbox"/>	James Watson				jwatson	true

前へ 次へ 削除 アーカイブ

Oracle Identity Administration User Manager ユーザープロフィールページ。検索条件として「フルネーム」を選択し、「次を含む」オプションが選択されている。検索結果は 8 件と表示されている。

ユーザーの再アクティブ化の開始 削除 パネルの表示 変更

ユーザープロフィール

役職

フルネーム James Watson

4. 「プロフィールの表示」ページの「ユーザーの再アクティブ化の開始」ボタンをクリックします。

ユーザーが再アクティブ化されます。

注意： ユーザーを再アクティブ化する場合、そのユーザーを以前所属していたグループに手動で追加し、そのユーザーの属性ポリシーと検索ベースを再設定する必要があります。

ワークフローのモニタリング

ワークフローをモニターする権限を保持するユーザーは、他のユーザーが所有するリクエスト・チケットの状態など、ワークフローの進行状況を参照できます。

管理ドメイン内のリクエストのみがリストされます。詳細は、2-5 ページの「[管理の委任](#)」を参照してください。

ワークフローをモニターする手順

1. User Manager、Group Manager または Organization Manager で、「リクエスト」をクリックします。
2. 「リクエストのモニター」をクリックします。

注意： サブフローでは、最初のステップが処理されていない場合、「処理日」フィールドは空白です。

3. 「検索」フィールドで、検索基準を選択して「実行」をクリックします。
検索フィールドの下に結果が表示されます。
4. 必要に応じて「次へ」または「前へ」をクリックし、他の結果を参照します。
5. チケットのリクエスト番号をクリックし、そのチケットの「リクエスト」ページを表示します。

このページには、ワークフローの現在のステップ番号がリストされます。

応答していない不完全なワークフローを削除するには、「リクエストのモニター」機能を使用してワークフローを特定し、「終了」ボタンをクリックします。完了したワークフローを終了するには、「ワークフローのモニター」機能の「削除」ボタンを使用します。

リクエストのアーカイブ

ワークフローをアーカイブして参加者と時間を記録に残し、Obliv ツリーの肥大化を防ぐことができます。アーカイブされたワークフローは、LDIF 形式で保存されます。デフォルトの格納ファイルは、oblix/data/common/wfinstance.ldif です。複数のアーカイブ操作によりこのファイルに情報が追加されます。

完了済みのワークフローのみアーカイブできます。

ワークフローをアーカイブする手順

1. 5-54 ページの「[ワークフローのモニタリング](#)」の手順に従ってワークフロー・リクエストを表示します。
2. 「すべて選択」列でリクエストを選択します。
3. 「アーカイブ」をクリックします。

次のファイルのデフォルトの名前と場所は、変更できます。

ファイル名	アプリケーション
usc_wf_params.xml	User Manager
gsc_wf_params.xml	Group Manager
osc_wf_params.xml	Org. Manager

4. アーカイブの確認ページが表示されたら、「戻る」をクリックして前のページに戻ります。

注意: パラメータ・ファイルの変更後、Identity Server を再起動する必要があります。

リクエストの削除

ワークフロー・リクエストは削除できます。

リクエストを削除する手順

1. 5-54 ページの「ワークフローのモニタリング」の手順に従ってリクエストを表示します。
2. 「すべて選択」列でリクエストを選択し、「削除」をクリックします。
3. 削除の確認ページが表示されたら、「戻る」をクリックして前のページに戻ります。

他の管理者がワークフロー・チケットを操作できないようにする方法

実行時に、複数のユーザーがワークフロー・チケットを受信する場合があります。たとえば、IT グループが「ワークフローの作成」リクエストのチケットを受信するとします。このリクエストを処理する管理者は、チケットをロックできます。これにより、他のユーザーは、ロックされたチケットの情報を参照できますが、チケットの操作はできなくなります。チケットのロックを解除できるのは、チケットをロックしたユーザー（マスター ID 管理者）と、リクエストをモニターする権限を付与されているユーザーのみです。

チケットをロックまたはロック解除する手順

1. 5-51 ページの「チケットを処理する手順」に従ってチケットをオープンします。
ワークフロー・チケットの処理時に、ワークフロー・ページに「チケットのロック」および「ロック解除」ボタンが表示されます。
2. 必要に応じて「チケットのロック」または「ロック解除」を選択します。

ワークフローの管理

ワークフローの定義後、それらのワークフローを表示、コピー、変更、削除およびエクスポートできます。

ワークフロー・サマリーの表示とエクスポート

ステップや参加者などを含むワークフローのサマリーを表示して、そのレポートをカンマ区切り値 (CSV) のファイルにエクスポートできます。

注意: 次の手順は、Microsoft Internet Explorer を使用しており、ID システム・インタフェース (WebPass) を WebGate で保護している場合に適用されます。「CSV にエクスポート」機能を有効化するには、次の 2 つの WebGate パラメータを構成する必要があります。

CachePragmaHeader: 空白のままにします。

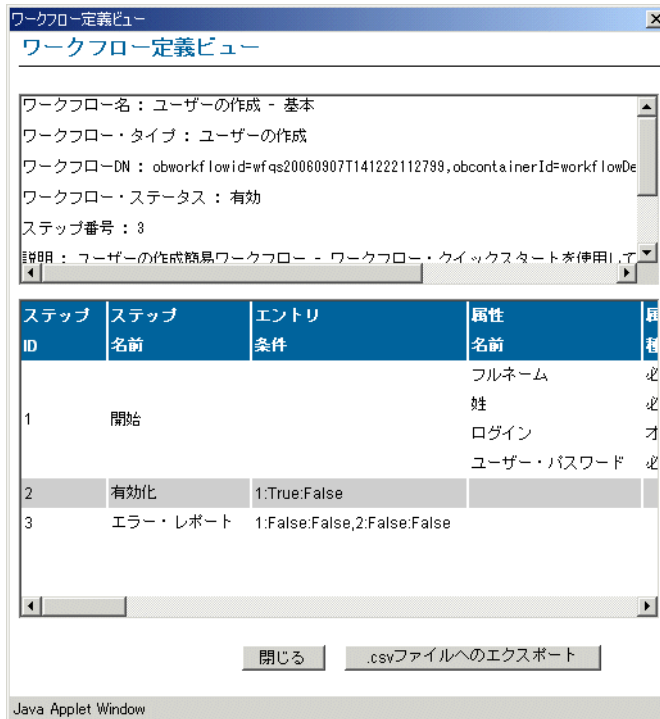
CacheControlHeader: 「プライベート」を指定するか、空白のままにします。

詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

ワークフロー・サマリーを表示およびエクスポートする手順

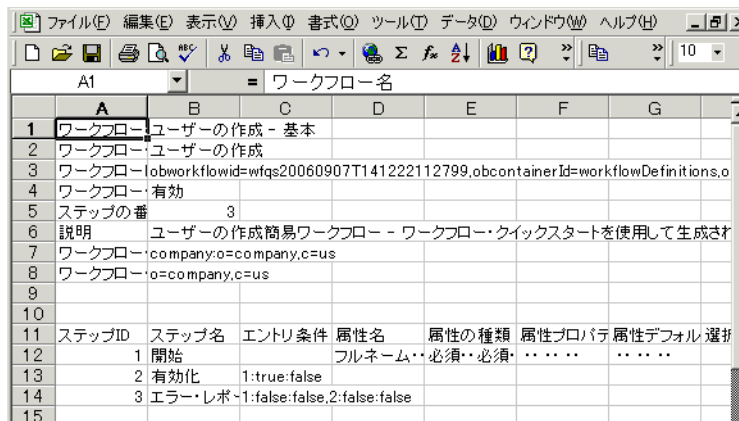
1. User Manager、Group Manager または Organization Manager にアクセスします。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. ワークフロー・メニューで、表示するワークフローを選択します。
4. 「表示」を選択します。

「ワークフロー定義ビュー」ページが表示されます。



5. 「ワークフロー定義ビュー」ページを拡大するか、右にスクロールしてワークフローのすべての内容を確認します。
6. 「.csv ファイルへのエクスポート」をクリックし、ワークフローのカンマ区切り値のファイルを保存します。
7. 「閉じる」をクリックしてページを閉じます。

サンプルの CSV ファイルをスプレッドシートで開くと、次のように表示されます。



ワークフローのコピー

ワークフローのコピーは、新規ワークフローの基盤として使用できます。また、保留中のチケットが多すぎて変更機能を適用できないワークフローを変更する場合にも、ワークフローのコピーを使用できます。

新規ワークフローの基盤としてワークフローをコピーする手順

1. User Manager、Group Manager または Organization Manager にアクセスします。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. 「ワークフロー」メニューで、コピーするワークフローを選択します。
4. 「コピー」をクリックします。
5. ワークフローのコピーがリストに表示されます。

このワークフローは、コピー元の名前に「のコピー」が付いた名前になります。必要がない場合でも、コピーしたワークフローの名前は変更することをお勧めします。

6. 必要に応じて情報を変更し、新規ワークフローを作成します。

かわりに変更するワークフローとしてワークフローをコピーする手順

1. 前の手順に従ってワークフローをコピーします。
2. ワークフローに外部アクションが含まれる場合、新規ワークフローを参照するよう oblixppcatalog カタログ・ファイルを更新します。

詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

3. コピーを変更します。

ワークフローを ID システムからのみ起動する場合、これで作業は完了です。

4. ワークフローが Portal Inserts として別のアプリケーションの Web ページに埋め込まれている場合、新規ワークフロー ID を参照するようワークフローのリンクを更新します。

ワークフローの変更

ワークフローの作成後に、そのパラメータを変更できます。選択したワークフローに保留中のインスタンスが含まれる場合は、ターゲットのリスト、任意のステップの参加者、または任意のステップの事前通知と事後通知の受信者のみを変更できます。

注意： 保留中のチケットがある場合に変更できるのはワークフローの一部のみであるため、非常にアクティブなシステムでは、ワークフローをコピーしてそのコピーを変更する必要があります。詳細は、5-57 ページの「[ワークフローのコピー](#)」を参照してください。

ワークフローを変更する手順

1. User Manager、Group Manager または Organization Manager にアクセスします。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. 「ワークフロー」メニューで、変更するワークフローを選択します。
4. 「変更」をクリックします。

選択したワークフローの情報が表示されます。「変更」をクリックすると、変更中に使用されないようにこのワークフローは無効化されます。

5. 必要に応じてワークフロー設定を変更します。
6. 「ワークフローの保存」をクリックして変更を保存します。
7. ワークフローの有効化を求めるプロンプトが表示されたら、「はい」をクリックします。

ワークフローの削除

ワークフローに保留中のリクエストが含まれなければ、ワークフローを削除できます。

ワークフローを削除する手順

1. User Manager、Group Manager または Organization Manager にアクセスします。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. 「ワークフロー」メニューで、削除するワークフローを選択します。
4. 「削除」をクリックします。
5. 確認メッセージが表示されたら、「OK」をクリックします。

ワークフローのエクスポート

すべてのワークフローをカンマ区切り値（CSV）のファイルにエクスポートできます。これは、印刷可能なテキスト・ファイルです。

注意： 次の手順は、Microsoft Internet Explorer を使用しており、ID システム・インタフェース（WebPass）を WebGate で保護している場合に適用されます。「CSV にエクスポート」機能を有効化するには、次の 2 つの WebGate パラメータを構成する必要があります。

CachePragmaHeader: 空白のままにします。

CacheControlHeader: 「プライベート」を指定するか、空白のままにします。

詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

ワークフローをエクスポートする手順

1. User Manager、Group Manager または Organization Manager にアクセスします。
2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. ワークフロー・メニューで、エクスポートするワークフローを選択します。
4. 「すべてをエクスポート」をクリックし、すべてのワークフローを含むカンマ区切り値のファイルを保存します。

ワークフロー・パネル設定の表示

4-2 ページの「[User Manager、Group Manager および Organization Manager の概要](#)」で説明したとおり、User Manager、Group Manager および Organization Manager アプリケーションに表示される要素は構成可能です。User Manager および Group Manager アプリケーションは1つのタブで構成され、Organization Manager は1つ以上のタブで構成されます。タブは、複数のプロファイル・ページの集合であり、プロファイル・ページ自体は複数のパネルの集合です。パネルは、属性と値のグループです。

これらのアプリケーションのプロファイル・ページに表示されるワークフロー・パネルは、参照および変更できます。

現在のワークフロー・パネル設定を表示する手順

1. ID システム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
2. 「ワークフロー・パネル」をクリックします。
「ワークフロー・パネル」ページに構成済のワークフロー・パネルが表示されます。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 ログイン・ユーザー: Master Admin

- オブジェクト・クラス
- **ワークフロー・パネル**
- マスター 監査ポリシー
- グローバル 監査ポリシー

ワークフロー・パネルの構成

パネル名	説明
ワークフロー・モニター表	ワークフロー・モニター検索結果に使用されます
ワークフロー・プロファイル・パネル	ワークフロー・インスタンス・ページに使用されます
ワークフロー・ステップ・プロファイル・パネル	ワークフローのステップ情報に使用されます
チケット情報パネル	チケット情報ページに使用されます
チケット検索テーブル	チケット検索結果に使用されます

次の表に、各パネルの説明を示します。

パネル	説明
ワークフロー・モニター表	ユーザーが「リクエストのモニター」ページでワークフロー検索を実行したときに、結果ページに含まれる列。
ワークフロー・プロファイル・パネル	「リクエストのモニター」ページでワークフロー・インスタンスに関して表示される情報。
ワークフロー・ステップ・プロファイル・パネル	「リクエストのモニター」ページでワークフロー・インスタンスのステップに関して表示される情報。
チケット情報パネル	「着信リクエスト」または「送信リクエスト」ページの「チケット情報」ページで表示される情報。
チケット検索テーブル	ユーザーが「着信リクエスト」または「送信リクエスト」ページでワークフロー検索を実行したときに、結果ページに表示される情報。

- 表示するパネルをクリックします。
パネルに表示される項目が、「パネルの表示」ページに表示されます。

パネル・フィールド	説明
パネル・ラベル	ID システムに表示されるパネルの名前。 このフィールドはローカライズできます。
説明	このパネルの機能の説明。 このフィールドはローカライズできます。
属性	パネルの列とその表示名に使用される属性。 このフィールドはローカライズできます。

ワークフロー・パネルの外観の変更

ワークフロー・パネルは削除できませんが、変更することはできます。

ワークフロー・パネルを変更する手順

- ID システム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
- 「ワークフロー・パネルの構成」をクリックします。
「ワークフロー・パネルの構成」ページに構成済のワークフロー・パネルが表示されます。
- 表示するパネルをクリックします。
- 「変更」をクリックします。
「パネルの変更」ページが表示されます。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 ログイン・ユーザー: Master Admin

- オブジェクト・クラス
- **ワークフロー・パネル**
- マスター監査ポリシー
- グローバル監査ポリシー

ワークフロー・パネルの変更画面では、ワークフロー・チケット検索結果、ワークフロー・ステップ情報、チケット情報ページに表示される属性情報を変更できます。

パネル・ラベル

説明

属性

ステップ番号	ステップ番号
アクション	アクション
アクション実行者	アクション実行者
ステータス	ステータス
サブフロー番号	サブフロー番号

保存 取消

- 「パネル・ラベル」フィールドに、アプリケーションに表示するこのパネルの新規名を入力します。
- 「説明」フィールドに説明を入力します。

7. 「属性」フィールドで、アプリケーションに表示する順序で属性を選択します。
8. 「保存」をクリックします。

ワークフロー・パネルのローカライズ

パネル情報を複数の言語で表示する場合、ワークフロー・パネルをローカライズできます。これを行うには、次の操作を実行する必要があります。

- 適切な言語パックをインストールします。
- 管理コンソールで、インストールした言語ごとにパネルの表示情報を手動で入力します。
属性をローカライズする方法の詳細は、第3章「IDシステムでのスキーマ・データの使用」および第4章「User Manager、Group Manager および Organization Manager の構成」を参照してください。

言語固有のワークフロー・パネル情報を表示する手順

1. IDシステム・コンソールで、「共通構成」をクリックします。
「共通構成」ページが表示されます。
2. 「ワークフロー・パネルの構成」をクリックします。
「ワークフロー・パネルの構成」ページに構成済のワークフロー・パネルが表示されます。
3. 表示するパネルをクリックします。
パネル名、説明、属性などのワークフロー・パネルの詳細がページに表示されます。
4. 「翻訳」をクリックします。

注意: 「翻訳」ボタンは、2つ以上の言語パックがインストールされている場合にのみ表示されます。

「パネル表示名のサマリー」ページが表示されます。パネル・フィールドおよび属性の言語固有の表示名が表示されます。特定の言語でまだ翻訳されていないフィールドは、「未構成」としてマークされます。

言語固有のワークフロー・パネル情報を構成する手順

1. 「パネル表示名のサマリー」ページで、「変更」をクリックします。
「パネル表示名の構成」ページが表示されます。このページには、パネル情報と、インストール済言語のリンクが含まれます。
2. ワークフロー・パネルを構成する言語をクリックします。
選択した言語の「パネル表示名の構成」ページが表示されます。
3. 次の情報を入力します。
 - **パネル・ラベル:** パネルの言語固有の表示名を入力します。
 - **説明:** パネルの簡単な説明を入力します。これはオプション設定です。
 - **属性:** 属性の各表示名に対して言語固有のテキストを入力します。
4. 「保存」をクリックして変更を保存します。変更を保存せずにページを終了する場合は、「取消」をクリックします。

ワークフロー・パフォーマンス

oblix/data/common/workflowdbparams.xml ファイルの WfInstanceNotRequired フラグを true に設定すると、ディレクトリ・サーバーへのアクセスを削減できます。このフラグにより、必要な場合を除きディレクトリ・サーバーにワークフロー・インスタンスが書き込まれなくなります。デフォルト設定の false では、ワークフロー・インスタンスはディレクトリ・サーバーに書き込まれます。

ワークフロー・パフォーマンスの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

ID 管理者の変更権限

第 2 章「ID システム管理者の指定」で説明したとおり、User Manager、Group Manager および Organization Manager を管理できるのは、ID 管理者のみです。

デフォルトでは、ID 管理者の属性アクセス制御は省略されます。その結果、属性の変更ワークフローを定義する場合に、そのワークフローの属性アクセス制御は ID 管理者に対してチェックされません。これらの管理者は自動的に変更権限を付与されますが、その他のユーザーは属性の変更をリクエストする権限のみを保持します。

この機能を制御するパラメータは、*IdentityServer_install_dir/identity/oblix/apps/common/bin/globalparams.xml* に含まれる `BypassAccessControlForDirAdmin` です。ディレクトリ管理者に自動的に変更権限を付与しない場合、このフラグを false に設定して Identity Server を再起動します。

ID 管理者に対して、属性の変更ワークフローで属性を変更する権限と、属性の変更をリクエストする権限を付与できます。

IdentityServer_install_dir/identity/oblix/apps/userservcenter/bin/userservcenter.xml などの各アプリケーション・パラメータ・ファイルで、`checkChangeAttributeEvenAllowModify` パラメータを true に設定できます。この設定により、管理者は、属性の変更を許可されている場合でも入力ボタンとワークフロー・ボタンの両方を参照できます。このパラメータは、ワークフローの変更権限と開始権限を両方とも保持する管理者に適用されます。ただし、この機能により、パフォーマンス・オーバーヘッドが発生する可能性があります。

拡張ワークフロー・オプション

次の拡張オプションを使用できます。

- ワークフロー・アクションへのカスタム・コードの追加
- ワークフロー・アクションの動作の構成

事前アクションと事後アクション

ID イベント・プラグイン API を使用して、カスタム・コードをワークフロー・アクションに追加できます。ワークフローで ID イベント・プラグイン API を使用する一般的な例は、次のとおりです。

- 外部システムによる値（一意の ID など）の自動生成
- ワークフロー・ステップのデータの検証
- 外部システムのデータの更新

カスタム・コードを記述したら、そのコードをワークフロー・アクションの前（事前アクション）か、ワークフロー・アクションの後（事後アクション）に実行するよう *oblixpppcatalog* ファイルで ID システムに指示する必要があります。

詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

外部アクション

外部アクションは事前アクションおよび事後アクションと同じ目的で使われますが、ID イベント・プラグイン API のアクションとは次の2つの点で異なります。

- 外部アクションは、既存のアクションに追加しません。
- ルーティング・パスは、外部アクションの終了状態に基づいて完全に構成可能です。

外部アクション・コードは、oblixpppcatalog ファイルにフックとして実装します。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

ワークフローのデータおよびアクションのカスタマイズ

User Manager、Group Manager および Organization Manager には、それぞれ参加者に表示するデータと選択可能なアクションを制御するためのワークフロー・パラメータ・ファイルがあります。

各パラメータ・ファイルには、次の3つのセクションが含まれます。

- Create Object (オブジェクトの作成)
- Delete Object (オブジェクトの削除)
- Change Attribute (属性の変更)

ファイルは次の場所にあります。

`IdentityServer_install_dir/identity/oblix/apps/applicationname/bin/`

ここで、`IdentityServer_install_dir` は Identity Server のインストール・ディレクトリであり、`applicationname` は次のいずれかです。

- `usc_wf_params.xml`: User Manager
- `gsc_wf_params.xml`: Group Manager
- `osc_wf_params.xml`: Org Manager

次の表に、各パラメータの説明を示します。

パラメータ	説明	設定例
<code>occurrence</code>	このアクションをワークフロー内で使用できる回数を示します。	[1] [n] 1: アクションは1回のみ使用できます。 n: アクションは複数回使用できます。
<code>useraction</code>	ステップが対話型であるかどうかを示します。	[true] [false] true: アクションにはユーザー操作が必要です。 false: これはバックグラウンド・ステップであり、ユーザー操作は必要ありません。
<code>forceCommit</code>	このアクションがコミットではない場合でも、このステップに暗黙的コミットを発行するかどうかを示します。暗黙的コミットにより、収集されたすべてのデータが特定のターゲット・エンタリに書き込まれます。	[true] [false] true: 暗黙的コミットを発行します。 false: 暗黙的コミットを発行しません。
<code>pre_action</code>	前のステップのアクションがこのリストに含まれる場合、現在のアクションを指定できることを示します。	[アクションのリスト]

パラメータ	説明	設定例
exit_condition	特定のアクションに使用可能な結果を示します。	[終了状態のリスト] たとえば、次のようになります。 true: 1 false: 0
relevant_data	このステップに構成可能な関連データのタイプを示します。バックグラウンド・ステップには、関連データは含まれません。	[関連データのリスト] Required、Provisioned または Optional の任意の組合せを使用できます。
initialStep	開始、自己登録または承認ステップに適用できるパラメータ。	値は true と false です。

ワークフローへのロールの追加

デフォルトでは、ワークフロー定義アプレットで使用できるのは、「すべてのユーザー」ロールのみです。ディレクトリに定義されているロールをワークフロー定義アプレットに追加するには、User Manager、Group Manager および Organization Manager のワークフロー・パラメータ・ファイルを変更します。

次の手順では、すべての DN ロールをワークフロー・アプレットに表示する方法について説明します。

ロールを構成する手順

- 3-19 ページの「属性の構成」の手順に従って「属性の変更」アプレットを表示します。
- Person オブジェクト・クラス、または Person オブジェクト・クラスに関連付けられた補助オブジェクト・クラスについて、DN データ型の属性を選択します。
たとえば、「マネージャ」属性を選択します。
- 「表示タイプ」リストで、選択した属性に対して「オブジェクト・セレクタ」表示タイプを選択します。
- 「ターゲット・オブジェクト・クラス」リストで、gensiteOrgPerson などの Person オブジェクト・クラスを選択します。
すべてのロールが次の手順に従って有効化されているかぎり、ワークフロー・アプレットに属性がロールとして表示されます。
- 「保存」をクリックします。

ワークフロー定義アプレットにロールを追加する手順

- 次のワークフロー・パラメータ・ファイルを編集します。
User Manager: usc_wf_params.xml を開きます。
Group Manager: gsc_wf_params.xml を開きます。
Organization Manager: osc_wf_params.xml を開きます。
- <CompoundList ListName="Roles"> セクションに移動します。
- 適切なワークフロー・タイプを見つけます。
たとえば、オブジェクトの作成ワークフローを変更するには、<CompoundList ListName="CREATE_OBJECT"> を見つける必要があります。
- このファイルの Participant (参加者) または Notiffee (通知先) セクションを見つけます。
たとえば、<ValNameList ListName="Participant"> セクションを編集します。
- 次の行を追加します。
<NameValPair ParamName="dns" Value="dns"/>

自己登録ワークフローの作成

自己登録により、ユーザーは、自分自身または所属する組織を Web ページから直接 ID システムに追加できます。ID システムには、自己登録用のユーザー・インターフェースはありません。登録フォームを表示する URL を構成する必要があります。

自己登録を行うユーザーは、初回のログイン試行後にパスワードを再設定するよう求められる場合があります。この動作は、「リセット時に変更」フィールドの設定に応じて変化します (7-47 ページの「パスワード・ポリシーの構成」を参照してください)。複数のユーザーが同じブラウザ・セッションを使用して自己登録を行う場合に、「リセット時に変更」オプションが選択されていると、最初のユーザー以降のすべてのユーザーは、初回のログイン後にパスワードを変更するよう求められます。

自己登録後にユーザーを ID システムに自動的にログインさせる場合は、`basedbparams.xml` ファイルの `SelfRegGeneratesSSOCookie` を `true` に設定する必要があります。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

自己登録ページのカスタマイズ方法の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

次の手順では、Basic 認証の自己登録ワークフローについて説明します。

自己登録ワークフローを作成する手順

1. ID システム・コンソールで、「User Manager」、「Group Manager」または「Organization Manager」を選択します。

Organization Manager に複数のタブがある場合は、適切なタブを選択してください。

2. 「構成」をクリックし、次に「ワークフロー定義」をクリックします。
3. 最初のステップに「自己登録」を使用して、ユーザーの作成または組織の作成ワークフローを定義します。
4. このワークフローにアクセスし、ワークフローの識別名とターゲット・ドメインを記録します。

この情報を自己登録 URL に追加します。

5. 次のように自己登録 URL を HTML ドキュメントに追加します。

```
https://domain_name:port/identity/oblix/apps/userservcenter/bin/
userservcenter.cgi?program=workflowSelfRegistration&ObWorkflowName=workflow_DN
&ObDomainName=target_domain
```

変数は次のとおりです。

- `domain_name:port`: ホスト・システムのドメイン名とポート番号
- `workflow_DN`: ワークフローの DN
- `target_domain`: 名前を除くターゲット・パス

`ObDomainName target_domain` の値は、自己登録ワークフローに定義されているターゲット・ドメインです。詳細は、5-22 ページの「オブジェクトの作成ワークフローの LDAP ターゲットの定義」を参照してください。

組織の自己登録では、次の形式を使用します。

```
https://domain_name:portnumber/identity/oblix/apps/objservcenter/
bin/objservcenter.cgi?program=workflowSelfRegistration&tab_id=tab_name&
ObWorkflowName=workflow_DN&ObDomainName=target_domain
```

変数は次のとおりです。

- *domain_name:portnumber*: ホスト・システム
- *tab_name*: タブの名前
- *workflow DN*: ワークフローの DN
- *target_domain*: 名前を除くターゲット・パス

自己登録用の URL は、認証を必要としないページを参照している必要があります。自己登録 URL は、通常の `/identity/oblix/apps/userservcenter/bin/userservcenter.cgi` ではありません。一般的に、ユーザーが ID システムにアクセスすると、アクセス・システムにより認証を求められます。ただし、自己登録ページおよびホスト・パスワード・ページにアクセスするユーザーについては、認証を要求しないよう WebGate を設定する必要があります。

6. 予約文字を URL 準拠のテキスト代替文字で置き換えます。

DN パスを動的拡張 URL で指定する場合、URL の予約文字（英数字以外）を、% とそれに続く文字の ASCII 16 進表現でエンコードする必要があります。たとえば、次のようになります。

- %3D: 等号 (=)
- %2C: カンマ
- %20: 空白

置換前の文字列の例：

```
cn=Engineering Team, ou=Engineering, o=Company, c=US
```

置換後の文字列：

```
cn%3DEngineering%20Team%2C%20ou%3DEngineering%2C%20o%3DCompany%2C%20c%3DUS
```

7. HTML ファイルを保存します。

次に、自己登録 URL の例を示します。

```
http://silicon/identity/oblix/apps/userservcenter/bin/userservcenter.cgi?program=workflowSelfRegistration&obdomainname=o%3DCompany%2C%3DUS&obworkflowname=obworkflowid%3D20020605T1132216476%2CobcontainerId%3Dworkflowdefinitions%2co%3Doblix%2Co%3Dconfigdata
```

注意： Sun 社の iPlanet ディレクトリを使用している場合、自己登録パスワードに UTF-8 文字は使用できません。ユーザーが UTF-8 文字を指定すると、iPlanet ディレクトリのデフォルトの 7 ビット・プラグインは操作に失敗します。7 ビット・プラグインのデフォルトでは、UID、メールおよびユーザー・パスワードの各属性値が 7 ビットである必要があります。この問題を解決するには、プラグインを無効化するか、構成からユーザー・パスワード属性を削除します。この問題は、「ユーザーの作成」操作と「プロフィールの変更」操作でも発生します。

ロケーション・ワークフローの作成

Organization Manager では、ビジネス・ロケーションを管理し、特定のユーザーにそのロケーションの管理を許可するワークフローを作成できます。個々のユーザーまたは特定のロール（ファシリティ・マネージャなど）を保持するユーザーを選択するか、IT 事業部などの特定のグループを選択することが可能です。

ユーザーが組織のロケーションを参照できるようにするには、ロケーション・マップの .gif イメージをワークフローに追加します。ユーザーがロケーションをクリックすると、建物が位置する領域のマップがロケーション・プロファイルに表示されます。

新規ロケーション・ワークフローを作成したら、その新規ワークフローを使用してロケーション・オブジェクトを作成できます。これを行うには、Organization Manager の「組織プロファイルの作成」機能を使用します。または、ロケーション・オブジェクトを先に作成し、そのオブジェクトを既存のワークフローにリンクできます。ロケーション・オブジェクトを作成したら、マップ上の特定の場所にユーザーなどの他のオブジェクトを割り当てることができます。

注意：ロケーション ID に「DN 接頭辞」セマンティック型が含まれる場合、Active Directory および ADAM では、複数値の RDN が許可されないことに注意する必要があります（iPlanet/SunOne では使用可能）。Active Directory および ADAM では、メタ属性構成で「属性値」の選択が「単一」になっていることを確認してください。

ロケーション・オブジェクトの作成後、ロケーション機能を使用可能にして、ユーザーまたはオブジェクトのロケーションを表示する適切な権限を備えたユーザーを有効化する必要があります。

タスクの概要：ロケーション機能とユーザーの有効化

1. Organization Manager の「ロケーション」タブを変更し、ロケーション属性を User Manager と Organization Manager のプロファイル・ページに追加します。
詳細は、4-37 ページの「[Organization Manager での「ロケーション」タブの有効化](#)」および 4-11 ページの「[タブのプロファイル・ページおよびパネルの構成](#)」を参照してください。
2. ロケーション属性に対する読取り権限を構成します。
詳細は、4-21 ページの「[ユーザーによる LDAP データの表示および変更の許可](#)」を参照してください。
3. ロケーションの作成ワークフローを定義します（5-68 ページの「[タスクの概要：ロケーションの作成ワークフローの定義](#)」を参照してください）。
4. 新規ロケーションを作成し、必要に応じて他のロケーションに関連付けられたロケーション階層を確立します。
詳細は、3-9 ページの「[オブジェクト・クラスの追加](#)」を参照してください。
5. ユーザーまたはオブジェクト・プロファイルのロケーション属性の値を割り当てます。
詳細は、5-19 ページの「[ワークフロー・アプレットの使用方法](#)」を参照してください。

注意：属性値は、ワークフローを使用する以外に、オブジェクト・プロファイル・ページでも追加および変更できます。

タスクの概要：ロケーションの作成ワークフローの定義

1. ワークフロー定義を開始します (5-20 ページの「[新規ワークフロー定義の開始](#)」を参照してください)。
2. 必要に応じて 1 つ以上のサブフローを作成します (5-15 ページの「[サブフローの概要](#)」を参照してください)。

注意：メイン・ワークフローを開始する前にサブフローを作成する必要があります。これにより、サブフローをメイン・ワークフローにリンクできます。

3. ワークフローに関連付ける属性を選択します (5-26 ページの「[ステップ属性の定義](#)」を参照してください)。
使用可能なデフォルトのロケーション属性は、「ロケーション ID」、「ロケーション名」、「ロケーション・タイトル」および「マップ・イメージ」です。「ロケーション ID」と「ロケーション名」は、必須属性です。
4. 参加者を指定します (5-24 ページの「[ワークフローの最初のステップの定義](#)」を参照してください)。
5. ワークフロー・プロセスを定義します (5-10 ページの「[ステップ・アクションの概要](#)」を参照してください)。
6. ワークフローを保存します。
7. ワークフローを有効化します (5-31 ページの「[ワークフローの有効化](#)」を参照してください)。
8. ワークフローをテストしてその妥当性を検証します (5-31 ページの「[ワークフローのテスト](#)」を参照してください)。

外部アプリケーションへの非 LDAP データの送信

User Manager、Group Manager および Organization Manager は、ユーザーが自分、他人、グループ、インベントリ、および管理者が使用を許可したその他の項目に関する情報を参照および変更できる ID システム・アプリケーションです。この章で説明するとおり、ユーザーに関する情報が変更される前に必ず確認や承認を行うなど、ID システム・アプリケーションで実行されるアクションにビジネス・ロジックを適用できます。

ID システムのオブジェクト・テンプレート機能により、追加、削除または変更された情報を他のアプリケーションに伝播するよう ID ワークフローを拡張できます。テンプレートの使用により、ID システムで非 LDAP スキーマを管理できるため、非 LDAP データをワークフローや ID イベント API で使用できます。

この章の内容は次のとおりです。

- [非 LDAP データの構成の概要](#)
- [ワークフローで非 LDAP データを使用する方法の概要](#)
- [テンプレート・オブジェクトの概要](#)
- [テンプレート・オブジェクト・データとワークフローの概要](#)
- [オブジェクト・テンプレートの構成](#)
- [オブジェクト・テンプレート・ファイルの例](#)
- [テンプレート属性用の ID イベント・プラグインの作成](#)

非 LDAP データの構成の概要

User Manager、Group Manager および Organization Manager アプリケーションは、LDAP ディレクトリまたはオブジェクト・テンプレートの情報に依存しています。

- **LDAP ディレクトリ**: ディレクトリの情報を構成することで、プロフィール・ページにデータを表示し、ユーザー、グループおよびオブジェクトに関するデータを操作するワークフローを構成します。LDAP ディレクトリは、ID システムの正式なデータ・ソースです。
- **オブジェクト・テンプレート**: オブジェクト・テンプレートの情報を手動で構成することで、ID ワークフロー・ステップの実行時に入力されたデータを異なるターゲット・データ・ソースに伝播できます。たとえば、非 LDAP データを使用するユーザーの追加またはユーザーの変更ワークフローを構成し、そのワークフローを ID イベント API で使用できます (詳細は、『Oracle Access Manager 開発者ガイド』を参照してください)。

ワークフローで非 LDAP データを使用する方法の概要

非 LDAP データをバックエンド・システムに送信する場合のプロセスは、次のとおりです。

タスクの概要: バックエンド・アプリケーション用の非 LDAP データの構成

1. オブジェクト・テンプレートを構成します (6-4 ページの「[オブジェクト・テンプレートの構成](#)」を参照してください)。

テンプレートには、バックエンド・アプリケーションで認識可能なオブジェクトおよび属性が含まれている必要があります。

2. このファイルを次の場所に格納します。

```
IdentityServer_install_dir\oblix\config\template\xxx.tpl
```

ここで、*IdentityServer_install_dir* は ID システムがインストールされているディレクトリであり、*xxx* は .tpl ファイルの名前です。

3. ID システム・コンソールでテンプレート・オブジェクトおよび属性を構成します (第 3 章「[ID システムでのスキーマ・データの使用](#)」を参照してください)。このとき、次のことに留意します。

- ユーザーは、ワークフロー・ステップのコンテキストでのみテンプレート属性の値を指定できます。
- テンプレート属性は、ID システムでは検索できません。
- テンプレート属性に対する表示権限または変更権限は設定できません。

テンプレート属性のアクセス制御を構成するには、ワークフロー・ステップ参加者を定義します。ステップ参加者である個々のユーザーのみが、これらの属性にアクセスできます。

- テンプレート属性は、導出属性として構成できません。

注意: ID システム・コンソールでテンプレート・オブジェクトおよび属性を構成したら、テンプレート・ファイルを変更しないでください。この制限は、構成後の変更を避ける必要のある LDAP スキーマと同様です。構成後に変更を加えると、予期しない動作が発生する可能性があります (それらの変更はサポートの対象外です)。

4. 1 つ以上のテンプレート属性を、User Manager などの ID システム・アプリケーションに含まれるタブのパネルに関連付けます (第 4 章「[User Manager、Group Manager および Organization Manager の構成](#)」を参照してください)。

5. ワークフローを作成し、テンプレート属性を1つ以上のワークフロー・ステップに関連付けます (第5章「ID機能とワークフローの連携」を参照してください)。

属性の表示名は、ワークフローに関連付けられたプロファイル・ページに表示されます。ただし、属性値は表示されません。この理由は、IDシステムからターゲット・アプリケーションに向かう一方方向のデータ・フローのみが存在するためです。(将来のリリースでは、これらの属性値の表示を可能にする双方向のデータ・フローが導入される予定です。) 詳細は、6-4ページの「テンプレート・オブジェクト・データとワークフローの概要」を参照してください。
6. ワークフローで使用される各スキーマにデータを書き込む有効化やコミットなどの個別のステップがワークフローに存在することを確認します (第4章「User Manager、Group Manager および Organization Manager の構成」を参照してください)。
7. ID イベント API および IdentityXML を使用して外部アクションを構成し、オブジェクト・テンプレートのデータをバックエンド・アプリケーションに送信します (『Oracle Access Manager 開発者ガイド』を参照してください)。

注意: 非 LDAP の属性値には、IdentityXML の Add および Replace アクションは適用できません。Replace All アクションのみ使用可能です。Add または Replace を使用して IdentityXML 文を作成すると、その文は Replace All を使用している場合と同様に処理されます。

この章の残りの部分では、オブジェクト・テンプレートの機能と、オブジェクト・テンプレートの構成方法について説明します。

テンプレート・オブジェクトの概要

ID システムでは、次の場所で一般的なオブジェクト・テンプレート・スキーマ・ファイルを提供しています。

`Identity_install_dir\oblix\config\template\`

これは、このファイルと、構成される他の任意のオブジェクト・テンプレート・ファイルに必須の場所です。

このファイルに作成されるテンプレート・オブジェクトは、LDAP オブジェクトと似ています。主な違いは、LDAP オブジェクトおよび属性はユーザー・プロファイル・ページへのデータの表示とワークフローの構成に使用するのに対し、テンプレート・オブジェクトはワークフローでのみ使用することです。

テンプレート属性に対してアクションを実行する1つ以上のステップを備えたワークフローを構成できます。ユーザーがワークフローを起動すると、ID システムにより、関連するステップの実行中に入力されたデータがオブジェクト・テンプレート・スキーマの要件に従って書式設定されます。

ワークフローでは、テンプレート属性値が一時的にステップ・インスタンスに格納されます。コミット・ステップが実行されると、データはターゲットのバックエンド・システムに書き込まれます。データ・フローは一方方向であるため、データがバックエンド・システムに書き込まれると、ID システムによるそのデータの格納は終了します。

最終的に、ID イベント・プラグインを作成して、オブジェクト・テンプレート・データをターゲットのバックエンド・システムに送信する必要があります。

テンプレート・オブジェクト・データとワークフローの概要

前の項で説明したとおり、テンプレート属性を使用するワークフロー・ステップを構成して、非 LDAP データをバックエンド・アプリケーションに送信できます。ユーザーがワークフロー・ステップの一環として入力する属性値は、一度コミットされるとプロファイル・ページには表示されません。ID システムでは、ターゲット・アプリケーションを対象とするデータの送信は可能ですが、データの取得は不可能であるためです。

オブジェクト・テンプレートを使用するワークフローを構成する場合、オブジェクト・テンプレート・データと LDAP データの両方を書き込むコミット・ステップを構成できます。これにより、ディレクトリを使用してプロファイル・ページに LDAP 属性の値を表示するとともに、テンプレート属性の値を使用してバックエンド・アプリケーションにデータを送信できます。

ID システムからバックエンド・アプリケーションに向かうデータ・フローは一方方向であるため、ユーザーは ID システムのデータを検証できません。ユーザーは、ターゲット・アプリケーションまたはそのログを参照して、ワークフローによりアプリケーションに作成されたデータを確認する必要があります。

バックエンド・システムへのデータの書き込み中にエラーが発生した場合、ID イベント API プラダインにより ID システム・ユーザーにメッセージを戻すことができます。

注意: 1 つのワークフロー・ステップですべてのデータ・ソースのデータをコミットすることはできません。ドメインごとに 1 つのコミット・ステップを構成する必要があります。

オブジェクト・テンプレートの構成

オブジェクト・テンプレート・ファイルには、オブジェクトと属性に関するスキーマに似た定義が XML 形式で格納されます。オブジェクト・テンプレート・ファイルに構成されるオブジェクトと属性は、データの書き込み先であるバックエンド・アプリケーションで認識可能な値に対応します。

すべてのオブジェクト・テンプレート・ファイルは、次の場所に存在する必要があります。

`Identity_install_dir/oblix/config/template`

ここで、`Identity_install_dir` は、ID システムがインストールされているディレクトリです。オブジェクト・テンプレート・ファイルの拡張子は、`.tpl` です。

Identity Server では、起動時にテンプレート・ファイルが読み取られます。現在のインストール環境で複数のサーバーを使用している場合、同じテンプレート・ファイルを各サーバーにコピーする必要があります。

複数のテンプレート・オブジェクト・クラスを単一のファイルまたは複数のファイルに定義できます。同じドメイン内に複数のファイルを作成する場合、ID システムでは、属性およびクラスの一意性がファイル間で確保される必要があることに注意してください。ドメイン内に属性またはクラスがすでに存在する場合、テンプレート・ファイルは Identity Server の起動時に登録されず、オブジェクトはシステム・コンソールに表示されません。

同様に、Identity Server では、構文エラーが存在する場合もテンプレート・ファイルを登録できません。かわりにログ・エントリが生成されます。

オブジェクト・テンプレート・ファイルの形式

テンプレート・ファイルは、スキーマ・ドメイン文から始まります。スキーマ・ドメインにより、同じ名前を持ちながら異なるデータ・ソースで使用されるオブジェクト・クラス（LDAP のユーザー・オブジェクトとバックエンド・アプリケーションのユーザー・オブジェクトなど）の間のあいまいさが解消されます。

スキーマ・ドメイン文の例は、次のとおりです。

```
ObTemplateDefinition domain="exchange" version="1.0"/>
```

起動時に、Identity Server によってドメイン文が読み取られます。表示用として、テンプレート・オブジェクトおよび属性は、ID システム・コンソールに次の形式で示されます。

```
attribute.class.domain
```

ここで、*domain* の名前は、.tpl ファイルのドメイン文から取得されます。

すべてのドメイン文は、一意である必要があります。一意ではないドメインが ID システムで検出されると、.tpl ファイル全体の読取りに失敗します。次のドメイン名は予約されており、.tpl ファイルでは使用できないことに注意してください。

- MIIS
- LDAP

オブジェクト・テンプレート・ファイルでは、名前 / 値ペアを任意に定義できます。これらの名前 / 値ペアは、ターゲット・アプリケーションで認識される形式に一致している必要があります。

テンプレート定義ファイルは、XML 形式です。次に、このファイルの例を示します。

```
<?xml version="1.0" encoding="iso-8859-1"?>
<ObTemplateDefinition domain="ABC_APPLICATION" version="1.0">

  <!-- ObAttributeDefinition -->
  <ObAttributeDefinition name="cn" syntax="OB_CIS" maxlen="20"/>
  </ObAttributeDefinition>
  <ObAttributeDefinition name="sn" syntax="OB_CIS" maxlen="20"/>
  <ObAttributeDefinition name="mail" syntax="OB_CIS" maxlen="20"/>
  <ObAttributeDefinition name="phone" syntax="OB_CIS" maxlen="20"/>

  <!-- ObClassDefinition -->
  <ObClassDefinition name="User">
    <ObAttributeReference name="cn" required="true">
    </ObAttributeReference>
    <ObAttributeReference name="sn" required="false">
    </ObAttributeReference>
    <ObAttributeReference name="mail" required="false">
    </ObAttributeReference>
    <ObAttributeReference name="phone" required="false">
    </ObAttributeReference>
  </ObClassDefinition>

  <ObClassDefinition name="Group">
    <ObAttributeReference name="cn" required="true"/>
    <ObAttributeReference name="sn" required="false"/>
    <ObAttributeReference name="uniqueMember" required="false"/>
  </ObClassDefinition>
</ObTemplateDefinition>
```

ID システムでのテンプレート・オブジェクトの表示

オブジェクト・テンプレート・ファイルに定義されたオブジェクトおよび属性は、次のように ID システムに表示されます。

- .tpl ファイルに定義された各オブジェクトは、ID システム・コンソールで次の項目を選択したときに表示されるページで選択できます。

「共通構成」 → 「オブジェクト・クラスの構成」 → 「追加」

ID システム・コンソールに表示されるオブジェクト・クラスの名前は、`class.domain` の形式です。クラス名は、.tpl ファイルの定義から取得されます。

- .tpl ファイルのオブジェクトに関連付けられた各属性は、「共通構成」 → 「オブジェクト・クラスの構成」 → オブジェクト・クラス・リンク → 「属性の変更」を選択したときに表示されるページで選択できます。

ID システム・コンソールに表示される属性の名前は、`attribute.class.domain` の形式です。`attribute` の名前は、.tpl ファイルの定義から取得されます。

- 各属性文の `syntax` 要素により、「共通構成」 → 「オブジェクト・クラスの構成」 → オブジェクト・クラス・リンク → 「属性の変更」を選択したときに表示される属性のデータ型が決定されます。

ID システム・コンソールでテンプレート・オブジェクト属性のデータ型を選択することはできません。データ型は、属性定義の `syntax` 要素で構成する必要があります。

- 「共通構成」 → 「オブジェクト・クラスの構成」 → オブジェクト・クラス・リンク → 「属性の変更」を選択したときに表示される属性が単一値であるか複数値であるかは、.tpl ファイルの属性定義によって決定されます。

- 属性のその他の特性（表示名やセマンティック型など）は、ID システム・コンソールで構成できます。

ID システムでは、ドメインごとにただ 1 つのセマンティック型を使用する必要があります。たとえば、「ログイン」セマンティック型や「パスワード」セマンティック型は、ドメインごとに 1 つのみを割り当てることができます。

- LDAP 属性とは異なり、.tpl ファイルに構成された属性は、検索不可能であり、導出属性として構成できません。

オブジェクト・テンプレート・ファイルの要素

オブジェクト・テンプレート・ファイルの要素は、次のとおりです。

オブジェクト・テンプレート・ファイルは、属性定義のリストから始まります。これらの属性は、後でこのファイルのオブジェクト定義内で参照されます。

表 6-1 ObAttributeDefinition の要素

要素名	説明
name	<p>属性の名前。これは、ID システム・コンソールに表示される属性名に対応します。</p> <p>このパラメータは必須です。</p> <p>長さ: 32 (最大)</p> <p>形式: [(a-z) (A-Z)][(a-z) (A-Z) (0-9)]</p>
syntax	<p>属性の構文。これは、ID システム・コンソールでの属性のデータ型に対応します。</p> <p>このパラメータは必須です。</p> <p>形式:</p> <ul style="list-style-type: none"> ■ OB_DN: LDAP DN。これは、LDAP の DN 属性と同義です。このパラメータにより、ID システム・コンソールで「オブジェクト・セクタ」表示タイプを構成できます。このパラメータは、ID システム・コンソールの「識別名」属性データ型に対応します。 ■ OB_BIN: バイナリ。このパラメータは、ID システム・コンソールの「バイナリ」属性データ型に対応します。 ■ OB_CES: 大 / 小文字を区別する文字列。このパラメータは、ID システム・コンソールの「文字列 (大 / 小文字を区別)」属性データ型に対応します。 ■ OB_CIS: 大 / 小文字を区別しない文字列。このパラメータは、ID システム・コンソールの「文字列 (大 / 小文字の区別なし)」属性データ型に対応します。 ■ OB_INT: 整数。このパラメータは、ID システム・コンソールの「整数」属性データ型に対応します。 ■ OB_TEL: このパラメータは、ID システム・コンソールの「電話」属性データ型に対応します。 ■ OB_POSTAL_ADDRESS: このパラメータは、ID システム・コンソールの「住所」属性データ型に対応します。
cardinality	<p>カーディナリティでは、単一値か複数値かを指定します。このパラメータは、ID システム・コンソールの単一または複数の属性値に対応します。このパラメータを複数値に設定した場合、ID システム・コンソールで単一値に再設定できます。ただし、.tpl ファイルで単一値に設定した場合、システム・コンソールでは再設定できません。</p> <p>このパラメータはオプションです。</p> <p>デフォルト: 特に指定のないかぎり <i>multi</i> です。</p> <p>形式: [single multi]</p>
maxlen	<p>属性値のデータの最大長。</p> <p>このパラメータはオプションです。</p> <p>デフォルト: 特に指定のないかぎり -1 です。この設定は、最大長が適用されないことを示します。</p> <p>形式: -1 または 1 ~ n</p> <p>n は、妥当な最大長を示す整数です。</p>

たとえば、次のようになります。

```
<ObAttributeDefinition name="c" syntax="OB_CIS" cardinality="single" />
<ObAttributeDefinition name="cn" syntax="OB_CIS" cardinality="single" />
```

.tpl ファイルでは、オブジェクト・クラスのリストが属性定義のリストの後に出現します。各オブジェクト・クラスには、ObClassDefinition 文が含まれ、次に ObAttributeReference 文のリストが続きます。

表 6-2 ObClassDefinition の要素

要素名	説明
name	<p>クラスの名前。この名前は、ドメイン内で一意である必要があります。</p> <p>このパラメータは必須です。</p> <p>長さ: 32 (最大)</p> <p>形式: [(a-z) (A-Z)][(a-z) (A-Z) (0-9)]</p>

たとえば、次のようになります。

```
<ObClassDefinition name="User">
<ObClassDefinition name="Group">
```

属性は、.tpl ファイルのオブジェクト・クラス定義の AttributeReference 文に含めることでオブジェクトに関連付けます。各 ObAttributeReference 文では、ObAttributeDefinition 文に定義されている属性を参照する必要があります。

表 6-3 属性とオブジェクトの関連付け

要素名	説明
name	<p>テンプレート属性の名前。</p> <p>このパラメータは必須です。</p> <p>属性参照は、オブジェクト・クラス内で一意である必要があります。name は、このドメインに含まれる既存の属性定義 (ObAttributeDefinition) の名前である必要があります。</p> <p>長さ: 32 (最大)</p> <p>形式: [(a-z) (A-Z)][(a-z) (A-Z) (0-9)]</p>
required	<p>クラス定義のコンテキストにおいて、この属性が必須であるかオプションであるかを指定します。</p> <p>このパラメータはオプションです。</p> <p>デフォルト: false</p> <p>形式: [true false]</p>

たとえば、次のようになります。

```
<ObAttributeReference name="cn" required="true">
<ObAttributeReference name="mail" required="false">
```

オブジェクト・テンプレート・ファイルの例

次に、オブジェクト・テンプレート・ファイルの例を示します。

```
<?xml version="1.0" encoding="iso-8859-1"?>

<ObTemplateDefinition domain="myapplication" xmlns:dsml="http://www.dsml.org/DSML"
xmlns:oblix="http://www.oblix.com/">
  <ObAttributeDefinition name="c" syntax="OB_CIS" cardinality="single" />
  <ObAttributeDefinition name="cn" syntax="OB_CIS" cardinality="single" />
  <ObAttributeDefinition name="department" syntax="OB_CIS" cardinality="single"/>
  <ObAttributeDefinition name="l" syntax="OB_CIS" cardinality="single" />
  <ObAttributeDefinition name="location" syntax="OB_CIS" cardinality="single" />
  <ObAttributeDefinition name="mail" syntax="OB_CIS" cardinality="single" />
  <ObAttributeDefinition name="ou" syntax="OB_CIS" cardinality="single" />
  <ObAttributeDefinition name="uid" syntax="OB_CIS" cardinality="single" />
  <ObClassDefinition name="person">
    <ObAttributeReference name="c" required="false" />
    <ObAttributeReference name="cn" required="false" />
    <ObAttributeReference name="department" required="false" />
    <ObAttributeReference name="l" required="false" />
    <ObAttributeReference name="location" required="false" />
    <ObAttributeReference name="mail" required="false" />
    <ObAttributeReference name="ou" required="false" />
    <ObAttributeReference name="uid" required="false" />
  <ObClassDefinition name="organizationalUnit">
    <ObAttributeReference name="l" required="false" />
    <ObAttributeReference name="ou" required="false" />
  </ObClassDefinition>
  <ObClassDefinition name="locality">
    <ObAttributeReference name="l" required="false" />
  </ObClassDefinition>
  <ObClassDefinition name="country">
    <ObAttributeReference name="c" required="false" />
  </ObClassDefinition>
  <ObClassDefinition name="computer">
    <ObAttributeReference name="cn" required="false" />
    <ObAttributeReference name="l" required="false" />
    <ObAttributeReference name="location" required="false" />
    <ObAttributeReference name="ou" required="false" />
  </ObClassDefinition>
  <ObClassDefinition name="group">
    <ObAttributeReference name="cn" required="false" />
    <ObAttributeReference name="mail" required="false" />
    <ObAttributeReference name="ou" required="false" />
    <ObAttributeReference name="uid" required="false" />
  </ObClassDefinition>
  <ObClassDefinition name="role">
    <ObAttributeReference name="l" required="false" />
    <ObAttributeReference name="ou" required="false" />
  </ObClassDefinition>
</ObTemplateDefinition>
```

テンプレート属性用の ID イベント・プラグインの作成

ID システム・ワークフローからバックエンド・アプリケーションにデータを送信するプラグインを作成する方法の詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。このプラグインを作成する場合の留意事項は、次のとおりです。

- ID イベント API を使用したバルク再アクティブ化操作は、実行できなくなりました。
- IdentityXML および ID イベント API を使用する場合、ID システムから属性を送信する際に使用できるアクションは、**Replace All** のみです。Add または **Replace** を使用して IdentityXML 文を作成すると、その文は **Replace All** を使用している場合と同様に処理されます。

グローバル設定の構成

この章では、複数の言語の構成方法や、ディレクトリとデータベース・サーバーの構成方法など、Oracle Access Manager の基本機能に関連するタスクについて説明します。

また、この章では、ID システム・アプリケーションの外観と機能を制御する方法についても説明します。たとえば、検索ベースとスタイルシートを使用して、ユーザーに表示する項目や、ID システム・アプリケーションで実行可能なアクションを制御できます。パフォーマンスを向上するために、別の Identity Server または WebPass を追加することも可能です。

これらのタスクを円滑に管理するため、第 2 章「ID システム管理者の指定」の手順に従って他の Oracle Access Manager 管理者およびマスター ID 管理者を指定できます。

この章には、次の各項が含まれます。

- ID システム・アプリケーションのスタイルの構成
- Oracle Access Manager での複数の言語の構成
- Identity Server 設定の構成
- Identity Server の管理
- ディレクトリ・サーバー・プロファイルの管理
- RDBMS プロファイルの管理
- WebPass の構成
- パスワード・ポリシーの構成
- ID システムの Access Manager SDK の構成
- コンポーネントのクローニングと同期化

注意： ID システムを構成するには、マスター管理者である必要があります。この章のほとんどのタスクは、ID システム・コンソールを通じて実行します。

第 8 章「トランスポート・セキュリティ・モードの変更」、付録 D「.NET 機能の実装」、第 10 章「ロギング」、第 11 章「監査」、および第 12 章「SNMP モニタリング」も参照してください。

ID システム・アプリケーションのスタイルの構成

スタイルを使用すると、ID システム・アプリケーション全体の外観を変更することや、その機能を制限することができます。スタイルは、スタイルシート、グラフィック・ファイル、およびシステムの特定のユーザー・インタフェースを定義するスクリプトを組み合わせて名前を付けたものです。スタイルは、アプリケーション・ページの各要素の外観を定義するスタイルシートに基づきます。スタイルには、フィールドと機能の名前、タブやボタンの色、形状、サイズを指定するための GIF イメージ、およびタブやボタンの名前に使用されるフォントが含まれます。

スタイルには、整形用と機能用があります。整形用のスタイルでは、色などの ID システム・アプリケーションの外観またはタブの外観を決定します。機能用のスタイルでは、ID システム・アプリケーションの機能を決定します。つまり、ID システム・アプリケーション・ページの特定の機能を追加、変更または削除できます。たとえば、3つのすべての ID システム・アプリケーションから「代替権限」機能を削除できます。ID システムには、クラシック・スタイルというデフォルト・スタイルが付属していますが、*PresentationXML* を使用して他のスタイルを開発し、ID システムの外観を変更できます。

ID システム・コンソールの「スタイルのカスタマイズ」オプションを使用すると、デフォルト・スタイルの設定、スタイルの作成、スタイルの変更、またはスタイルの削除を行うことができます。ただし、ID システム・コンソールを通じてスタイルを作成または変更する場合、システムにより既存のスタイルシートがコピーされ、その名前が変更されます。スタイルシートを開いて、手動で必要な変更を加える必要があります。

スタイルシートを作成および変更する方法の詳細は、『Oracle Access Manager カスタマイズ・ガイド』の *PresentationXML* による GUI の設計に関する内容を参照してください。

注意： 変更できるのは、ID システム・アプリケーション・ページの外観のみです。システム・コンソールでは、変更不可能なスタイル設定が使用されません。

この項には、次の各項目が含まれます。

- [スタイルの表示](#)
- [カスタム・スタイル・ディレクトリの追加](#)
- [スタイルの配布](#)
- [スタイル名の変更](#)
- [スタイルの変更](#)
- [スタイルの削除](#)
- [デフォルト・スタイルの設定](#)

スタイルの表示

現在構成されているスタイルを表示するには、次の手順を使用します。これにより、スタイル関連の操作手順の開始ポイントとなる「スタイルのカスタマイズ」ページに進みます。

現在構成されているスタイルを表示する手順

1. ID システム・コンソールで、「システム構成」を選択します。
2. 「システム構成」ページの左側のナビゲーション・ペインで、「スタイル」を選択します。「スタイルのカスタマイズ」ページが表示されます。次の例では、ID システムにデフォルトで付属するクラシック・スタイルが表示されています。



3. スタイルのリンクをクリックし、スタイルのパラメータを表示します。

スタイル名、スタイル・ファイルの格納ディレクトリ、およびスタイル・ファイルのソース（「コピー元」フィールド）が表示されます。

カスタム・スタイル・ディレクトリの追加

ID システムには、クラシック・スタイルというデフォルトの表示スタイルが初めから付属しています。`IdentityServer_install_dir/identity/oblix/lang/en-us/style0` ディレクトリには、クラシック・スタイルの XSL ラッパー・スタイルシート・ファイルが含まれます。これらのファイルの大部分は、`IdentityServer_install_dir/identity/oblix/lang/shared` ディレクトリに含まれるすべての言語のグローバル共有スタイルシート・テンプレート・ファイルを参照します。

ユーザー・アプリケーションのために ID システム・ページの表示用カスタム・スタイルを作成するプロセスは、この項で説明するとおり ID システムに新規スタイルを追加することから始まります。その結果、XSL ラッパー・スタイルシート・ファイルを含む新規カスタム・スタイル・ディレクトリが作成されます。その後、既存のスタイルをコピーして変更するか、新規スタイルシートに基づいて完全に新しいスタイルを作成します。

注意： 変更できるのは、ユーザー・アプリケーションのスタイルのみです。システム・コンソールでは、常にデフォルト・スタイルが使用されます。

どちらの場合でも、ID システムにスタイル（およびカスタム・スタイル・ディレクトリ）を追加するときには同じ方法を使用します。つまり、スタイル名と、スタイル・ファイル用のディ

レトリ名を指定します。新規スタイルの基盤とする既存のスタイルを選択することも可能です。デフォルトとして新規スタイルを選択したら、ID システムのスタイルシートのコピーをカスタマイズするか、独自のスタイルシートを作成します。このプロセスを完了するには、独自の新規スタイルシートおよび GIF をすべての Identity Server マシンと WebPass マシンにそれぞれコピーする必要があります。

最初の新規スタイルを追加する前に、次のいくつかの点に留意してください。

複数の言語: 複数の言語をサポートするために、ID システムには、インストール済の言語ごとに特定の名前付きディレクトリが存在します。たとえば、`/lang/en-us` はデフォルトの英語用言語ディレクトリであり、`/lang/fr-fr` はフランス語用ディレクトリです。ID システムのデフォルト・スタイル・ディレクトリとカスタム・スタイル・ディレクトリは、どちらもインストール済の各言語ディレクトリ内に格納されます。

たとえば、フランス語言語パックをインストールしているとします。この場合、`lang/en-us` ディレクトリと `lang/fr-fr` ディレクトリの両方に `/style0` ディレクトリが含まれます。ID システムにスタイルを追加すると、次のように新規スタイル・ディレクトリが `lang/en-us` ディレクトリと `lang/fr-fr` ディレクトリの両方に追加されます。

```
IdentityServer_install_dir/identity/oblix/lang/en-us/NewStyle
```

```
IdentityServer_install_dir/identity/oblix/lang/en-us/style0
```

```
IdentityServer_install_dir/identity/oblix/lang/fr-fr/NewStyle
```

```
IdentityServer_install_dir/identity/oblix/lang/fr-fr/style0
```

スタイル名: ID システムでは、ユーザーが指定したスタイル名が内部的に使用されます。ベスト・プラクティスとして、スタイル名はカスタム・スタイル・ディレクトリ名と一致させてください。これにより、識別が容易になります。名前には、空白、`&`、`*` またはカッコ () を含めることはできません。

スタイル・ディレクトリ名: ユーザーが指定したディレクトリ名は、関連するラッパー・スタイルシート・ファイル用のディレクトリを作成するのに使用されます。この名前は、スタイル名と同一で、同じネーミング規則に準拠している必要があります。

また、カスタム・スタイル・ディレクトリ名は、新規スタイルのステータスとコピー元を識別するために作成される XML 文書 (`style0.xml` の複製) にも割り当てられます。たとえば、新規ディレクトリの名前が `Pastel` である場合、次のファイルが作成されて格納されます。

```
IdentityServer_install_dir/identity/oblix/config/style/Pastel.xml
```

その他のファイルはこのプロセスでは作成されません。ただし、`styles.xml` ファイルは、設定したディレクトリ、スタイル名およびディレクトリ名を指定する `NameValPair` を含むように更新されます。このファイルの例は、次のとおりです。

```
IdentityServer_install_dir/identity/oblix/config/style/styles.xml
```

`config/style` のスタイル情報ファイルは、WebPass には含まれません。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

既存のスタイルからのコピー: 既存のスタイル・ディレクトリからスタイルシートをコピーできます。または、「なし」を選択して既存のスタイルに基づかないスタイルを構築するか、選択したスタイルシートのみをカスタマイズすることが可能です。

注意: 最初にスタイルを追加する場合、使用可能な唯一のスタイルは、デフォルトのクラシック・スタイルです。

「なし」の選択: 「なし」を選択した場合、作成されるディレクトリは空のため、新規スタイル用のスタイルシートのセットを手動で作成するか、操作するファイルを `/style0` ディレクトリから選択的にコピーする必要があります。

「なし」を選択すると、新規スタイルのステータスは、スタイルを選択するまで ID システム内で「作成中」と表示されます。空のスタイル・ディレクトリが自動的に作成され、`style0.xml` の複製が `IdentityServer_install_dir/identity/oblix/config/style/style0.xml` として作成されます。

スタイルの選択 : コピー元のスタイルを選択した場合、コピー元のディレクトリの複製が、指定したカスタム・ディレクトリ名で作成されます。コピーしたファイルでは、コピー元のディレクトリ (/style0 またはコピー元として選択したカスタム・スタイル) に対する相対参照が保持されます。

カスタマイズ時には、新規スタイル・ディレクトリに含まれる変更されたバージョンのスタイルシートを指し示す参照を更新するだけで済みます。

結果 : Pastel という新規スタイルを Pastel というディレクトリに追加し、デフォルトのクラシック・スタイルからコピーするとします。この場合、次のように各 langTag ディレクトリ内に Pastel ディレクトリが作成され、クラシック・スタイルのディレクトリである /style0 からの複製ファイルが格納されます。

```
IdentityServer_install_dir/identity/oblix/lang/en-us/Pastel
```

クラシック・スタイルのディレクトリである /style0 は、次のようにそのまま残ります。

```
IdentityServer_install_dir/identity/oblix/lang/en-us/style0
```

また、新規スタイルがデフォルトとして選択されると、ユーザーが作成したディレクトリの名前に基づいて style0.xml の複製である XML 文書が作成され、次のように config/style に style0.xml とともに格納されます。

```
IdentityServer_install_dir/identity/oblix/config/style/Pastel.xml
```

```
IdentityServer_install_dir/identity/oblix/config/style/Pastel.xml.lck
```

追加情報と各種ファイルの内容は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

スタイルを追加する手順

1. ID システム・コンソールで、「システム構成」を選択し、次に「スタイル」を選択して「スタイルのカスタマイズ」ページを表示します。
2. 「スタイルの追加」ボタンをクリックし、「スタイルの追加」ページを表示します。

注意 : ここで指定するスタイル名は、ID システムにより内部的に使用されるため、指定するディレクトリ名と一致させる必要があります。

3. 「スタイルの追加」ページの各フィールドに値を入力します。たとえば、次のようになります。

名前 : Pastel

ディレクトリ名 : Pastel

4. 「コピー元」フィールドで、既存のスタイルを選択して新規スタイルのテンプレートとして使用します。

たとえば、次のようになります。

Classic Style

5. 「保存」をクリックして新規スタイルを保存します（スタイルを保存せずにこのページを終了する場合は、「取消」をクリックします）。

「スタイルのカスタマイズ」ページに新規スタイル名がリストされ、新規ラッパー・スタイルシートを格納するために 1 つ以上のディレクトリが作成されます。

6. 次のように新規スタイルをデフォルト・スタイルとして選択します。

- a. 「デフォルト・スタイルの設定」ボタンをクリックして「デフォルト・スタイルの設定」ページを表示します。

- b. 新規スタイル名の横の「デフォルトに設定」ボタンをクリックし、次に「保存」をクリックします。

7. ファイル・システムで、指定した新規スタイル・ディレクトリ名を確認します。

次に、『Oracle Access Manager カスタマイズ・ガイド』の説明に従ってスタイルをカスタマイズします。

スタイルの配布

次の手順により、エンド・ユーザーがスタイルを使用できるようにします。

スタイルを配布する手順

次のように、ユーザーが ID システムを表示する最初のページの URL に、スタイルシートを含むディレクトリ名を追加します。

```
&style=directory_name
```

ここで、*directory_name* は、ID システムのスタイルシートを含むディレクトリの名前です。

スタイル名の変更

次の手順を使用してスタイル名を変更できます。

スタイル名を変更する手順

1. 「スタイルのカスタマイズ」ページで、変更するスタイルの名前をクリックします。
「スタイルの表示」ページが表示されます。
2. 「変更」をクリックします。
「スタイルの変更」ページが表示されます。
3. スタイル名を変更します。
4. 「保存」をクリックして変更を保存します（変更を保存せずに終了する場合は、「取消」をクリックします）。
「スタイルの表示」ページにスタイルの新規名が表示されます。

スタイルの変更

ID システムに付属のデフォルト・スタイルであるクラシック・スタイルは、ID システムにより使用されるため変更できません。ただし、ユーザーが作成したカスタム・スタイルは変更可能です。

スタイルを変更する手順

1. 『Oracle Access Manager カスタマイズ・ガイド』の PresentationXML によるユーザー・インタフェースの設計に関する章の説明に従って、対応するスタイルシートを変更します。
2. 変更が完了したら、そのスタイルシートを各 Identity Server と、スタイルシートが変更された Identity Server にリンクする各 WebPass にコピーします。

スタイルの削除

ID システムに付属のデフォルト・スタイルであるクラシック・スタイルは、ID システムにより使用されるため削除できません。ただし、ユーザーが作成したカスタム・スタイルは削除可能です。

カスタム・スタイルを削除する手順

1. 「スタイルのカスタマイズ」 ページで、スタイルの名前をクリックします。
「スタイルの表示」 ページが表示されます。
2. 「削除」 をクリックします。
3. プロンプトが表示されたら、削除を確認します。
「スタイルのカスタマイズ」 ページが再表示されます。
4. 他のすべての Identity Server および WebPass インストール領域の新規スタイル・ディレクトリから新規スタイルシートを削除します。

デフォルト・スタイルの設定

「デフォルト・スタイルの設定」 オプションを使用して、アプリケーションのデフォルト・スタイルを選択できます。

注意: 「作成中」 ステータスのスタイルを選択することはできません。

デフォルト・スタイルを設定する手順

1. 「スタイルのカスタマイズ」 ページで、「デフォルト・スタイルの設定」 をクリックします。
「デフォルト・スタイルの設定」 ページが表示されます。
2. 選択するスタイルの横の「デフォルトに設定」 をクリックします。
3. 「保存」 をクリックします。
「スタイルのカスタマイズ」 ページで、選択したスタイルの横に「使用可能および現在のデフォルト」と表示されます。

Oracle Access Manager での複数の言語の構成

『Oracle Access Manager インストレーション・ガイド』の説明にあるとおり、英語の言語は自動的にインストールされます。ただし、Oracle に付属する 1 つ以上の言語パックをインストールできます。言語パックにより、『Oracle Access Manager 概要』に指定されている言語でエンド・ユーザーおよび管理者にローカライズされた情報を提供できます。

一部の表示名および属性は、ID システム・アプリケーション (User Manager、Group Manager および Organization Manager) と管理者アプリケーション (ID システム・コンソール、アクセス・システム・コンソールおよび Policy Manager) のエンド・ユーザーに表示されます。

Oracle Access Manager 10g (10.1.4.0.1) では、エンド・ユーザーに対して静的アプリケーション・データ (エラー・メッセージ、およびタブ、パネル、属性の表示名など) をサポート対象のエンド・ユーザー言語で表示できます。管理情報は、サポート対象の管理者言語でのみ表示できます。

インストールおよび設定後に、使用する言語を構成して属性の表示名をローカライズする必要があります。この作業は、次のレベルで実行します。

- オブジェクト・クラス・レベル
- タブ・レベル
- パネル・レベル

- 検索結果属性レベル

注意：表示名は、最上位レベルであるオブジェクト・クラス・レベルで構成することをお勧めします。これより下位のレベルで表示名を構成する場合は、必ず各レベルですべての言語の表示名を指定してください。

タスクの概要：マルチ言語機能の構成

1. Oracle に付属する 1 つ以上の言語パックを使用して Oracle Access Manager をインストールおよび設定します（『Oracle Access Manager インストール・ガイド』を参照してください）。
2. 使用するインストール済言語を有効化します（7-14 ページの「[複数言語の管理](#)」を参照してください）。
3. 手動でラベルと属性の表示名を入力し、インストール済言語を使用するようアプリケーションを構成します。たとえば、次の作業を実行します。
 - オブジェクト・クラス属性のローカライズ（3-22 ページの「[属性表示名のローカライズ](#)」を参照）。
 - タブ、グループ・タイプ・パネル、検索結果属性およびレポートの表示名のローカライズ（第 4 章「[User Manager、Group Manager および Organization Manager の構成](#)」を参照）。
 - ワークフロー・パネル名のローカライズ（5-61 ページの「[ワークフロー・パネルのローカライズ](#)」を参照）。
 - 他の言語で表示するためのタブ名のローカライズ（4-5 ページの「[タブのローカライズ](#)」を参照）。
 - 検索結果属性のローカライズ（4-7 ページの「[検索結果に表示される属性の表示、変更およびローカライズ](#)」を参照）。

管理ページ用言語の選択

複数の言語をインストールして構成している場合、ID システム・コンソール、アクセス・システム・コンソールおよび Policy Manager の管理情報に使用する言語を指定できます。この操作は、ブラウザで実行します。詳細は、使用しているブラウザのドキュメントを参照してください。

管理情報に対応していない言語で管理ページがリクエストされた場合、製品のインストール時に選択されたデフォルト言語が管理ページの表示に使用されます。

エンド・ユーザー・アプリケーションでの言語の評価順序

インストール済言語を有効化し、インストール済言語を使用するよう属性を構成すると、エンド・ユーザーに対してアプリケーション・ページを表示するための言語が次の評価順序に従って選択されます。

評価順序

1. URL に指定された言語。

ユーザーは、URL に言語を指定できます。たとえば、User Manager で「ユーザーの作成」機能を選択する場合、ユーザーは lang=fr-fr を追加することで User Manager ページをフランス語で表示できます。アプリケーションでは、リソースの URL に指定された言語プリファレンスが最初に検索されます。ユーザーまたは管理者は、URL に lang=languageTag を追加して言語を指定できます (languageTag は RFC 1766 形式の言語タグです)。

次の例では、「ユーザー・プロファイルの作成」ページがフランス語で表示されます。

```
http://localhost/identity/oblix/apps/userservcenter/bin/
userservcenter.cgi?program=workflowCreateProfile&tab_id=
employees&lang=fr-fr
```

2. ObTEMC Cookie の LangCookie というパラメータに格納された言語。

前の手順のように URL に言語を指定すると、その言語は LangCookie パラメータに設定されます。ObTEMC Cookie は、ユーザーのログイン時に作成され、ユーザーのセッション期間中は維持されます。URL に言語指定が含まれない場合、アプリケーションでは、セッション期間中に維持される ObTEMC Cookie がチェックされます。ObTEMC Cookie は、フォームまたはページにも設定できます。

3. HTTP ヘッダー変数の HTTP_OBLIX_LANG に指定された言語。

認証または認可成功ヘッダー変数を作成してこの値を含めることができます。『Oracle Access Manager Access System Administration Guide』の認証と認可に関する章の説明を参照してください。HTTP_OBLIX_LANG ヘッダー変数の名前を変更する場合、次のファイルで実行できます。

```
IdentityServer_install_dir/oblix/apps/common/bin/globalparams.xml
```

```
PolicyManager_install_dir/access/oblix/apps/common/bin/globalparams.xml
```

ここで、IdentityServer_install_dir は Identity Server がインストールされているディレクトリであり、PolicyManager_install_dir は Policy Manager がインストールされているディレクトリです。

globalparams.xml の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

4. ユーザーの Web ブラウザに設定されている値により決定されるデフォルト言語。この値は、ヘッダー変数の Accept-Language に指定されます。

アプリケーションで HTTP_OBLIX_LANG ヘッダー変数を検出できない場合、ユーザーのブラウザに設定された Accept-Language ヘッダー変数が検索されます。

注意： HTTP_OBLIX_LANG ヘッダー変数と Accept-Language ヘッダー変数は、両方とも構成可能です。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

5. Oracle Access Manager インストール環境のデフォルト言語。

Accept-Language ヘッダー変数をユーザーのブラウザで検出できない場合、アプリケーションでは、obnls.xml 構成ファイルで Oracle Access Manager インストール環境のデフォルト言語が検索されます。

obnls.xml ファイルは、`IdentityServer_install_dir/identity/oblix/config` ディレクトリにあります。`IdentityServer_install_dir` は、Identity Server がインストールされているディレクトリです。

詳細は、7-14 ページの「複数言語の管理」を参照してください。

Identity Server 設定の構成

Identity Server の構成には、ユーザー・セッション期間の指定、ユーザー・フィードバック用の電子メール・アドレスの指定、通知イベント用のメール・サーバーの構成、キャッシュの管理、および複数の言語の有効化が含まれます。

サーバー設定を表示および変更するには、ID システム・コンソールを使用します。

この項には、次の各項目が含まれます。

- [セッション・タイムアウトの構成](#)
- [電子メール宛先のカスタマイズ](#)
- [メール・サーバーの構成](#)
- [キャッシュの管理](#)
- [複数言語の管理](#)

サーバー設定を表示または変更する手順

1. ID システム・コンソールで、「システム構成」 → 「サーバー設定」を選択します。

次のスクリーン・ショットのような「サーバー設定の表示」ページが表示されます。

The screenshot shows the Oracle Identity Administration console interface. The top navigation bar includes 'ORACLE Identity Administration' and 'Identity System Console'. The main content area is titled 'サーバー設定の表示' (Server Settings Display). It contains several sections with links to configuration pages:

- サーバー設定の表示**: This page lists all settings for the product. To change a value, click the link. To make the change effective, restart all Identity Servers.
- セッション・タイムアウトの構成**: 180 分
- 電子メール宛先のカスタマイズ**: Includes links for 'バグ・レポート', 'フィードバック', and 'Webマスター'.
- メール・サーバー**: A table of settings:

サーバー名	dd
サーバー・ポート番号	25
ドメイン名	
メール送信スタイル	Asynch
メール・キュー・サイズ	100
メール・スタイル	MHTML電子メールをサポート
- キャッシュ**: キャッシュが有効です。 (はい)
- マルチ言語**: マルチ言語が有効です。 (はい)

2. 設定の値を表示または変更するには、各設定のリンク（「メール・サーバー」や「マルチ言語」など）をクリックします。
3. 必要に応じて設定を変更します。
4. 「保存」をクリックして変更を保存します（変更を保存せずに終了する場合は、「取消」をクリックします）。
5. 新しい値を有効化するため、Identity Server を再起動します。

セッション・タイムアウトの構成

セッション・タイムアウトを構成すると、ユーザーのアイドル・セッション時間（分単位）を指定できます。ユーザー・セッションは、指定したアイドル時間が経過すると自動的に終了します。

このページの設定は、すべてのユーザーおよびすべての ID システム・アプリケーションに適用されます。ユーザーやアプリケーション別に異なる設定を構成することはできません。

WebGate などによる Web サーバー・ベースのログインを使用している場合は、WebGate インスタンスがタイムアウトを処理するため、セッション・タイムアウトは適用されません。

注意: Web シングル・サインオンにより保護されるリソースでは、アイドル・セッション・タイムアウト設定は常に無視されます。

ユーザーの ID システム・セッション期間を構成する手順

1. ID システム・コンソールで、「システム構成」→「サーバー設定」を選択し、「セッション・タイムアウトの構成」をクリックして次のページを表示します。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成

ログイン・ユーザー: Master Admin

- パスワードポリシー
- ロストパスワードポリシー
- ディレクトリ・プロファイル
- Identity Server
- WebPass
- サーバー設定**
- 診断
- 管理者
- スタイル
- 写真

セッションの構成

この画面では、シングル・サインオンで保護されていない場合は、製品に対するアクティビティがなくてもユーザーのセッションの期間が有効となるように構成できます。「タイムアウトなし」を指定すると、ブラウザがアクティブなかぎり、ユーザーはログインしなくても製品を使用できます。また、タイムアウトを分単位で指定し、セッション時間がリフレッシュされる時間を分で指定することもできます。リフレッシュ期間がゼロの場合、セッション・タイム・スタンプはリクエストごとに更新されます。

重要:「タイムアウトなし」は、ブラウザを終了しないかぎり、ユーザーのセッションが終了しないことを示します。

タイムアウトなし
 アイドル・セッション・タイムアウト 180 分 リフレッシュ期間 0 分

保存 取消

2. 次のタイムアウト・オプションを選択します。
 - **タイムアウトなし:** ブラウザがアクティブであるかぎり、ユーザー・セッションは無期限に続きます。
 - **アイドル・セッション・タイムアウト:** アイドル・セッションを終了するまでの待機分数。アクティブではない状態でこの分数が経過すると、ユーザーはアプリケーションを継続するためにログインする必要があります。

事前に指定された時間間隔の経過後にアイドル・セッションを終了することには、いくつかの理由があります。セッションを短くすることで、ユーザーにロックされないまま放置されたワークステーションが不正に使用されることを防止できます。

 - **リフレッシュ期間:** ユーザー・セッションのタイムスタンプを更新する頻度を構成します。0（ゼロ）の値は、セッション・タイムスタンプをリクエストのたびに更新することを意味します。この値は、「アイドル・セッション・タイムアウト」の値の4分の1に設定することをお勧めします。
3. 「保存」をクリックして変更を保存します（保存せずにページを終了する場合は、「取消」をクリックします）。

電子メール宛先のカスタマイズ

電子メールのカスタマイズ機能を使用して、ユーザー・フィードバック用の電子メール・アドレスを指定できます。エンド・ユーザーは、サイド・ナビゲーション・バーの「バージョン情報」をクリックし、次に「管理フィードバックを送信」または「Oracle にフィードバックを送信」をクリックすることでこれらのアドレスにアクセスできます。

電子メール宛先をカスタマイズする手順

1. ID システム・コンソールで、「システム構成」 → 「サーバー設定」 を選択します。
2. 「サーバー設定」 ページで、「電子メール宛先のカスタマイズ」 をクリックして次のページを表示します。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 ログイン・ユーザー: Master Admin

電子メール宛先のカスタマイズ

「電子メール宛先のカスタマイズ」画面では、ユーザー入力のようなカテゴリのターゲット電子メール・アドレスを指定できます。

バグ・レポートおよびユーザー・フィードバックを受信する電子メール・アドレスを入力します。

バグ・レポートの電子メール・アドレス

ユーザー・フィードバックの電子メール・アドレス

Webマスターやマスター管理者の電子メール・アドレスを指定します。このアドレスはフィードバックとリクエストに使用する内部アドレスであり、Oracleアドレスではありません。

Webマスターの電子メール・アドレス

保存 取消

3. 次のフィールドに電子メール・アドレスを入力します。
 - **バグ・レポートの電子メール・アドレス**: 組織内の担当者または代表窓口レポートを送信する場合、このアドレスを変更する必要があります。この担当者または部門は、問題を解決するか、オラクル社カスタマ・サポート・センターに連絡することが可能な宛先です。
 - **ユーザー・フィードバックの電子メール・アドレス**: 自社ユーザーがローカル・ネットワークの外部に電子メールを送信できない場合、管理者はバグおよびフィードバック用のフィールドに内部アドレスを入力できます。オラクル社への情報の転送を担当するユーザーのアドレスを指定します。
 - **Web マスターの電子メール・アドレス**: Oracle Access Manager の管理を担当する自社ユーザーの電子メール・アドレスを入力します。
4. 「保存」をクリックして変更を保存します（保存せずにページを終了する場合は、「取消」をクリックします）。

メール・サーバーの構成

ID システムでは、リクエスト・チケットの処理、グループの管理、パスワード期限切れの通知、またはプロフィール属性の変更の際に、電子メール・アラートを発行できます。SMTP サーバー構成機能を使用して、ID システムでこれらの電子メールを処理する方法を構成します。

メール・サーバーを構成する場合、オプションの 1 つに「MHTML 電子メールをサポート」があります。MHTML は、HTML などのドキュメントの集合を MIME でカプセル化したものを意味します。

MHTML により、MIME multipart/related ボディ形式のインライン・グラフィック、アプレットおよびリンク・ドキュメントを含む HTML ドキュメントを送信できます。CID (content-ID) URL またはその他の種類の URL を使用して、HTML ドキュメントに含まれる他のパートへのリンクを指定することが可能です。リンクされたボディ・パートは、content-ID (CID URL によるリンク) または content-location (他の種類の URL によるリンク) のいずれかによりそのヘッダーで識別されます。

HTML と MHTML の主な違いは、MHTML の場合、画像が HTML 形式のようにリンクで参照されるのではなく、電子メールに埋め込まれることです。

メール・サーバーを構成する手順

1. ID システム・コンソールで、「システム構成」 → 「サーバー設定」を選択します。
2. 「サーバー設定」 ページで、「メール・サーバー」をクリックして次のページを表示します。

The screenshot shows the Oracle Identity Administration console. The main content area is titled "SMTPサーバー構成". It contains the following fields and options:

- サーバー名: Server1
- サーバー・ポート番号: 25
- ドメイン名: (empty)
- メール送信スタイル:
 - 同期メーラー。
 - 非同期メーラー。 メール・キュー・サイズ: 100
- メール・スタイル:
 - テキストのみの電子メールをサポート
 - リッチHTML電子メールをサポート
 - MHTML電子メールをサポート

At the bottom of the form, there are "保存" (Save) and "取消" (Cancel) buttons.

3. 「サーバー名」フィールドに SMTP サーバー名を入力します。
4. 「サーバー・ポート番号」フィールドにメール・サーバーのポート番号を入力します。
5. 「ドメイン名」フィールドに Web サーバーのドメイン名を入力します。

注意: このフィールドはオプションですが、ドメイン名を指定すると、RFC 821 に従って SMTP 接続を設定できます。

6. 「メール送信スタイル」で次のオプションを選択します。
 - **同期メーラー**。: 電子メールを起動した「属性の変更」などのプロセスから送信します。メール・サーバーへの接続時にエラーが発生した場合や、サーバーが停止した場合、電子メールは送信されず、再生成もされません。
 - **非同期メーラー**。: すべてのアプリケーションからの電子メールをキューイングするスレッドを使用して、メールを1つずつ送信します。メール・サーバーに接続できない場合、電子メールはスレッドにより再送信されます。キューイングされたメールは、ディスクに保存されます。「非同期メーラー。」を選択する場合、メール・キュー・サイズも指定します。
 - 「メール・スタイル」のオプションを選択します。
 - 「保存」をクリックして変更を保存します（保存せずにページを終了する場合は、「取消」をクリックします）。

キャッシュの管理

Identity Server キャッシュの内容の表示、新規情報を使用したキャッシュのロード、および非一貫性を解決するためのメモリー・キャッシュの消去を行うことができます。

ID システム・キャッシュの詳細を表示する手順

1. ID システム・コンソールで、「システム構成」→「サーバー設定」を選択します。
2. 「サーバー設定」ページで、「キャッシュ」をクリックしてページを表示します。
3. キャッシュ内容を表示するオプションを選択するか、メモリー・キャッシュをロードまたは消去します。

キャッシュの管理方法の詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

複数言語の管理

新規インストールでは、デフォルトでマルチ言語機能が有効化されます。ID システム・コンソールで、優先言語の有効化、無効化および指定を行うことができます。

注意: 以前のリリースからアップグレードする場合、マルチ言語機能は無効化されます。この機能を有効化するには、次の手順を実行します。

言語を管理する手順

1. ID システム・コンソールで、「システム構成」→「サーバー設定」を選択します。
2. 「サーバー設定の表示」ページで、「マルチ言語」を選択します。

「マルチ言語の管理」ページが表示されます。このページには、使用可能な言語、優先順序、および言語が有効化されているかどうかなどの詳細情報が表示されます。
3. 有効化または無効化する言語を決定します。
 - 有効化: 言語を選択し、「有効化」をクリックしてその言語を有効化します。
 - 無効化: 言語を選択し、「無効化」をクリックしてその言語を無効化します。
4. 「戻る」をクリックして「サーバー設定」ページに戻ります。

関連項目: 7-7 ページの「Oracle Access Manager での複数の言語の構成」

Identity Server の管理

Identity Server の管理は、Identity Server の追加または削除、Identity Server のパラメータ値の変更などのタスクで構成されます。Identity Server をインストールする方法の詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。サーバーを完全に削除するには、サーバーをアンインストールする必要があります。

この項の内容は次のとおりです。

- [複数の Identity Server の設定](#)
- [Identity Server の追加](#)
- [Identity Server パラメータの表示と変更](#)
- [Identity Server パラメータの削除](#)
- [コマンドラインによる Identity Server サービスの管理](#)

複数の Identity Server の設定

次の概要では、複数の Identity Server を設定する方法について説明します。

タスクの概要：複数の Identity Server の設定

1. 最初の Identity Server と WebPass をインストールし、ID システムを設定します（『Oracle Access Manager インストレーション・ガイド』を参照してください）。
2. ID システム・コンソールで新規 Identity Server インスタンスを追加します（7-18 ページの「[Identity Server パラメータの表示と変更](#)」の手順を参照してください）。
3. 新規 Identity Server インスタンスを WebPass に関連付け、優先順位をプライマリとして設定します（7-45 ページの「[Identity Server と WebPass の関連付けの管理](#)」を参照してください）。
4. WebPass インスタンスを変更して、最大接続数をすべてのプライマリ Identity Server と通信するのに適切な数に設定します（7-40 ページの「[WebPass の追加または変更](#)」を参照してください）。

手順 5 に進む前に少なくとも 1 分間待機する必要があります。これにより、WebPass 構成ファイルの webpass.xml が新規インスタンス情報で更新されるのを待機します。待機しない場合、WebPass インスタンスで新規情報を取得できず、新規 Identity Server インスタンスに接続できない可能性があります。

5. 少なくとも 1 分間待機してから、インストール済のすべての Identity Server を停止します。
6. 新規 Identity Server をインストールし、このディレクトリ・サーバーで最初の Identity Server ではないことを示します（『Oracle Access Manager インストレーション・ガイド』を参照してください）。

スキーマを再更新する必要はありません。

7. インストールした新規 Identity Server を設定します（『Oracle Access Manager インストレーション・ガイド』を参照してください）。

Identity Server の追加

新規 Identity Server インスタンスをインストール環境に追加する場合、次の手順を使用します。

Identity Server を追加する手順

1. ID システム・コンソールで、「システム構成」→「Identity Server」を選択します。
既存の Identity Server へのリンクを含む「すべての Identity Server をリスト」ページが表示されます。
2. 「追加」ボタンをクリックします。
「新規 Identity Server の追加」ページが表示されます。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 User Manager Group Manager Org. Manager Identity System Console

ログイン・ユーザー: Master Admin

- パスワード・ポリシー
- ロスト・パスワード・ポリシー
- ディレクトリ・プロファイル
- **Identity Server**
- WebPass
- サーバー設定
- 診断
- 管理者
- スタイル
- 写真

新規 Identity Server の追加

名前	<input type="text"/>
ホスト名	<input type="text"/>
ポート	<input type="text"/>
デバッグ	<input checked="" type="radio"/> オフ <input type="radio"/> オン
デバッグ・ファイル名	<input type="text"/>
トランスポート・セキュリティ	<input checked="" type="radio"/> オープン <input type="radio"/> 簡易 <input type="radio"/> 証明書
最大セッション時間(時間)	<input type="text" value="24"/>
スレッド数	<input type="text" value="20"/>
データベースの監査フラグ(監査オン/オフ)	<input checked="" type="radio"/> オフ <input type="radio"/> オン
ファイルの監査フラグ(監査オン/オフ)	<input checked="" type="radio"/> オフ <input type="radio"/> オン
監査ファイル名	<input type="text"/>
監査ファイル最大サイズ(バイト)	<input type="text" value="100000"/>
監査ファイル・ローテーション間隔(秒)	<input type="text" value="7200"/>
監査バッファ最大サイズ(バイト)	<input type="text" value="25000"/>
監査バッファ・フラッシュ間隔(秒)	<input type="text" value="7200"/>
スコープ・ファイル名	<input type="text" value="/oblix/logs/scopefile.lst"/>
SNMP状態	<input checked="" type="radio"/> オフ <input type="radio"/> オン
SNMPエージェント登録ポート	<input type="text" value="80"/>

3. 「名前」フィールドから「スレッド数」フィールドまでを次のように入力します。
 - 名前: Identity Server の名前を入力します。
 - ホスト名: Identity Server が稼働しているマシンの名前を入力します。
 - ポート: Identity Server のポート番号を入力します。
 - デバッグ: Identity Server と WebPass 間の低レベル・トラフィックに関するデバッグ情報を格納するかどうかを指定します。
 - デバッグ・ファイル名: デバッグ・ファイルの名前とパスを入力します。デフォルト・パスは、`IdentityServer_install_dir/oblix/logs/debugfile.lst` です (`IdentityServer_install_dir` は、Identity Server がインストールされているディレクトリです)。

- **トランスポート・セキュリティ: WebPass と Identity Server 間の通信に使用するセキュリティ方式を次から選択します。**

オープン:セキュリティが不要な場合に使用します。トランスポート・セキュリティは適用されません。

簡易:基本セキュリティが提供されます。通信は、TLS v1 (Transport Layer Security、RFC 2246) を使用して暗号化されます。通信要素は、パスワード・ベースのメカニズムを使用して相互に認証を行います。簡易セキュリティを使用するすべての要素は、インストール環境全体で同じパスワードを使用する必要があります。ID システムでは、認証を実行する証明書が提供されます。

証明書:内部認証局 (CA) を管理する場合に使用します。通信は、TLS v1 を使用して暗号化されます。また、クライアントとサーバーの各要素は、接続の確立時に X.509 証明書を提出する必要があります。証明書は、VeriSign 社などのサード・パーティにより提供される必要があります。

注意: 証明書: 内部認証局 (CA) を管理する場合に使用します。通信は、TLS v1 を使用して暗号化されます。また、クライアントとサーバーの各要素は、接続の確立時に X.509 証明書を提出する必要があります。証明書は、VeriSign 社などのサード・パーティにより提供される必要があります。

- **最大セッション時間 (時間):** WebPass と Identity Server 間の接続をオープン状態のまま維持する最大時間を入力します。

この時間が経過すると、既存の接続はクローズされて新規接続がオープンされます。

- **スレッド数:** Identity Server で許可する同時リクエストの最大数を入力します。

4. 現在の環境に応じた監査情報を次のように入力します。

- **データベースの監査フラグ (監査オン / オフ):** 「オン」を選択すると、構成済のデータベースに監査情報が送信されます。デフォルトは「オフ」です。
- **ファイルの監査フラグ (監査オン / オフ):** 「オン」を選択すると、次のフィールドで指定する名前のファイルに監査情報が送信されます。デフォルトは「オフ」です。
- **監査ファイル名:** Identity Server の監査情報を書き込む監査ファイルの名前を入力します。

Access Server または Identity Server の監査ファイルの絶対パスまたは相対パスを指定できます。相対パスを指定する場合は、パスの先頭に . または .. を使用します。たとえば、次の相対パスを入力できます。

```
./auditfile.lst\
```

この相対パスにより、次の場所に監査ファイルが作成されます。

```
Component_install_dir\oblix\apps\common\bin\auditfile.lst
```

ここで、*Component_install_dir* は、関連する Access Server または Identity Server のルート・インストール・ディレクトリです。

次の相対パスを入力するとします。

```
../../../logs/auditfile.lst
```

この場合、*Component_install_dir\oblix\logs\auditfile.lst* が作成されます。

注意: IIS の配置環境では、監査ファイルを表示可能にするため、IIS ユーザー (Web サーバーを実行しているシステム・ユーザー) に %TEMP% および %TMP% ディレクトリと、監査ファイルの保存先ディレクトリに対する書き込み権限を付与する必要があります。

- 監査ファイル最大サイズ(バイト): 監査ファイルに格納するバイト数を入力します。このサイズに到達すると、監査ファイルはタイムスタンプ付きで保存され、新規ファイルが作成されます。
 - 監査ファイル・ローテーション間隔(秒): 監査ファイルのローテーション発生までの秒数を示す数値を入力します。ローテーションが発生すると、監査ファイルにタイムスタンプが記録され、新規ファイルが作成されます。デフォルト値は 7200 です。0 (ゼロ) を設定すると監査ファイルのタイムアウトはなくなり、監査情報はファイルに継続的に追加されます。
5. 「スコープ・ファイル名」フィールドを次のように入力します。
- スコープ・ファイル名: バグ・レポートを記録するファイルの名前を入力します。バグ・レポートが生成される場合、ページに表示される情報もファイルに記録されます。このパラメータにより、バグ・レポートまたは OB_SCOPE メッセージ用のファイル名を指定します。
6. 現在の環境における SNMP 状態と SNMP エージェント登録ポートの詳細を入力します。
- 詳細は、第 12 章「SNMP モニタリング」を参照してください。
- SNMP 状態: 「オン」を選択すると SNMP モニタリングが有効化されます。デフォルトは「オフ」です。
 - SNMP エージェント登録ポート: SNMP エージェントがリスニングするポートです。
-
- 注意:** SNMP モニタリングをオンにした場合でも、SNMP 統計を取得するには、独自のネットワーク管理ステーション (NMS) を構成して管理情報ベース (MIB) で定義された情報を処理する必要があります。SNMP エージェントの MIB 変数の詳細は、このマニュアルの後続の説明を参照してください。
-
7. 「保存」をクリックして新規 Identity Server の定義を終了します (保存せずに終了する場合は、「取消」をクリックします)。

Identity Server パラメータの表示と変更

ID システム・コンソールでパラメータを表示または変更するには、次の手順を使用します。

Identity Server パラメータを表示または変更する手順

1. ID システム・コンソールで、「システム構成」→「Identity Server」を選択します。

既存の Identity Server のリストが、各サーバーの名前、ホスト名およびポート番号とともに表示されます。

2. Identity Server の名前をクリックしてそのパラメータを表示します。

「Identity Server の詳細」ページが表示されます。このページには、サーバーのパラメータがリストされます。

3. 「変更」をクリックします。

「Identity Server の変更」ページが表示されます。

4. 必要に応じてパラメータを変更します。

各パラメータの詳細は、7-16 ページの「Identity Server を追加する手順」を参照してください。

5. 「保存」をクリックして変更を保存します (保存せずに終了する場合は、「取消」をクリックします)。

Identity Server パラメータの削除

ID システム・コンソールで Identity Server パラメータを削除するには、次の手順を使用します。

注意： コンソールで Identity Server を削除した場合、Identity Server パラメータがコンソールから削除されているため、コマンドラインからそのサーバーを起動しようとしても失敗します。

Identity Server パラメータを削除する手順

1. ID システム・コンソールで、「システム構成」 → 「Identity Server」を選択します。
既存の Identity Server のリストが、各サーバーの名前、ホスト名およびポート番号とともに表示されます。
2. 「すべての Identity Server をリスト」ページで、削除する Identity Server を選択します。
3. 「削除」をクリックします。
4. 削除の確認を求められたら、「OK」をクリックします。
サーバー名がサーバーのリストから削除されます。

コマンドラインによる Identity Server サービスの管理

コマンドライン・ツールの `config_ois` を使用すると、Windows のサービス・ウィンドウに含まれる Identity Server サービス関連のタスクを管理できます。

次のコマンドを使用して、Identity Server サービスのインストールや、サービスの開始または停止などのタスクを実行できます。

表 7-1 `config_ois` のコマンド

コマンド	操作
<code>[-i install_dir]</code>	Identity Server サービスのインストール・ディレクトリを指定します。
<code>-v</code>	サービス名を指定します。
<code>[-a <start, stop, query, install, remove>]</code>	実行するアクションを指定します。

```
C:¥IdentityServer_install_dir¥identity¥oblix¥apps¥common¥bin¥
config_ois.exe -q -i c:¥IdentityServer_install_dir¥identity
-v Identity_ServiceName -a query
```

ここで、`IdentityServer_install_dir` は Identity Server がインストールされているディレクトリであり、`Identity_ServiceName` は Identity Server サービスの名前です。

この問合せにより、次の情報が表示されます。

```
Sample_Srv configuration:
Service Type: 0x110
      Start Type: 0x2
Err Control: 0x1
Binary path:
c:¥COREId¥identity¥oblix¥apps¥common¥bin¥ois_server.exe
Load order group:
Dependencies:
Dependencies: LocalSystem
```

ディレクトリ・サーバー・プロファイルの管理

ディレクトリ・サーバーと通信するコンポーネントをインストールする場合、コンポーネントの通信先のディレクトリ・サーバーを指定します。各コンポーネントは、次の特定の目的でディレクトリと通信します。

- **Identity Server:** Identity Server をインストールする場合、構成データを格納する LDAP ディレクトリ・サーバーと、ユーザー・データを格納する場所を指定します。ユーザー・データは、構成データと同じディレクトリ・サーバーに格納するか、別のディレクトリ・サーバーに格納できます。
- **Policy Manager** および **Access Server:** Policy Manager または Access Server をインストールする場合も、ユーザー・データと構成データを格納する場所を指定します。また、アクセス・ポリシー・データの格納先も指定します。

注意: リリース 7.0 以上では、ユーザー・データを 1 つのディレクトリ・サーバー・タイプに格納し、構成データとポリシー・データをまとめて別のディレクトリ・サーバー・タイプに格納できます。データの格納方法の詳細は、『Oracle Access Manager インストール・ガイド』を参照してください。

次の各項目で詳細情報を提供します。

- [LDAP ディレクトリ・サーバー・プロファイルの概要](#)
- [LDAP ディレクトリ・サーバー・プロファイルの作成](#)
- [LDAP ディレクトリ・サーバー・プロファイルの表示](#)
- [LDAP ディレクトリ・サーバー・プロファイルの変更](#)
- [手動によるシステム設定の再実行](#)
- [LDAP ディレクトリ・サーバー・プロファイルへのデータベース・インスタンスの追加](#)
- [LDAP ディレクトリ・サーバー・インスタンスの削除](#)
- [複数のディレクトリ検索ベースの操作](#)

LDAP ディレクトリ・サーバー・プロファイルの概要

Oracle Access Manager に必要とされるデータのタイプ（構成データ、ユーザー・データおよびポリシー・データ）ごとに、LDAP ディレクトリ・サーバー・プロファイルによりそのデータの正確な場所が識別されます。ポリシー・データと構成データの場所は、Identity Server、Access Server および Policy Manager の .xml ファイルにも格納されます。ディレクトリ・サーバー・プロファイルには、同じネームスペースと（読取り、書込み、検索などの）操作要件を共有する 1 つ以上のディレクトリ・サーバーに対する接続情報が含まれます。接続情報には、名前、適用されるドメインまたはネームスペース、ディレクトリ・タイプ、および操作のセットが含まれます。デフォルトのディレクトリ・サーバー・プロファイルは、Identity Server をインストールして新規ディレクトリ・サーバーの接続情報を指定するときに自動的に作成されます。

ロード・バランシングおよびフェイルオーバーのために追加の LDAP ディレクトリ・サーバー・プロファイルを作成できます。ディレクトリ情報ツリー（DIT）のパーティションに対応するディレクトリ・サーバー・プロファイルを作成できます。パーティション化により、DIT の特定部分に対する読取りおよび書込み操作を実行する CPU サイクルが解放され、パフォーマンスが向上する可能性があります。これは、複数のディレクトリ・サーバーおよびマシンを含むインストール環境で特に役立ちます。

DIT のマスター・コピーとレプリケート・コピーに対して異なる操作を指定する LDAP ディレクトリ・サーバー・プロファイルを作成することも可能です。たとえば、マスターでは書込み操作にのみ対応し、レプリカでは読取り操作にのみ対応するよう指定できます。

注意：Oblix ツリーを含むディレクトリ・サーバー・プロファイルでは、常に読取り、検索、変更、作成および削除操作をサポートする必要があります。Oblix ツリーに関しては、読取り専用または書込み専用のディレクトリ・サーバー・プロファイルは作成できません。構成データまたはポリシー・データのディレクトリ・プロファイル設定を変更する場合、Identity Server および Policy Manager の設定を再実行し、Access Server を再構成する必要があります。詳細は、7-28 ページの「[手動によるシステム設定の再実行](#)」を参照してください。

- [LDAP ディレクトリ・サーバー・プロファイルの作成](#)
- [LDAP ディレクトリ・サーバー・プロファイルの表示](#)
- [LDAP ディレクトリ・サーバー・プロファイルの変更](#)

LDAP ディレクトリ・サーバー・プロファイルの作成

次のスクリーン・ショットは、ID システム・コンソールの「プロファイルの構成」ページを示しています。

「プロファイルの構成」ページの上部には、ユーザー・データと構成データを含むディレクトリ・サーバーの詳細が表示されます。ページの中央部には、LDAP ディレクトリ・サーバー・プロファイルを構成するためのリンクが含まれます。ページの下部には、RDBMS プロファイルを構成するためのリンクが含まれます。RDBMS プロファイルの詳細は、7-35 ページの「[RDBMS プロファイルの管理](#)」を参照してください。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager **Identity System Console**

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 ログイン・ユーザー: Master Admin

- パスワード・ポリシー
- ロストパスワード・ポリシー
- ディレクトリ・プロファイル**
- Identity Server
- WebPass
- サーバー設定
- 診断
- 管理者
- スタイル
- 写真

プロファイルの構成

次のものは構成ベースおよび検索ベースの設定を含んでいます。特定の値を変更するにはリンクをクリックします。

ディレクトリ・サーバー

マジン	stagh24
ポート番号	389
ルートDN	cn=orcladmin
ルート・パスワード	<非表示>
検索ベース	o=company,c=us
構成ベース	o=Obliv, o=company,c=us
ディレクトリ・サーバー・セキュリティ・モード	オープン
非結合検索ベース	

次の表にはすべてのディレクトリ・プロファイルのリストが含まれています。特定のプロファイルを変更するにはリンクをクリックしてください。新しい値を有効にするにはすべてのIdentity Serverを停止して再起動する必要があります。

LDAPディレクトリ・サーバー・プロファイルの構成

名前	ネームスペース	プライマリ・サーバー	セカンダリ・サーバー
<input type="checkbox"/> default-ID Server 10.1.3 M3 stagh24 6021	o=company,c=us	default	
<input type="checkbox"/> OracleContext-ID Server 10.1.3 M3 stagh24 6021	cn=Products,cn=OracleContext	default	
<input type="checkbox"/> AccessManager setup user profile	o=company,c=us	default	
<input type="checkbox"/> AccessServer default user profile	o=company,c=us	default	

RDBMSプロファイルの構成

名前	プライマリ・サーバー	セカンダリ・サーバー
----	------------	------------

「ディレクトリ・サーバー」リンクをクリックすると、「ディレクトリ・サーバー構成」ページが表示されます。ディレクトリ・サーバーの通信モード（またはホスト名あるいはポート番号）を変更する場合、「ディレクトリ・サーバー構成」ページの情報を更新してシステム設定を再実行する必要があります。このタイプの変更の詳細は、[第8章「トランスポート・セキュリティ・モードの変更」](#)を参照してください。

「プロファイルの構成」ページの中央部にある「LDAPディレクトリ・サーバー・プロファイルの構成」という見出しの下には、ユーザー・データ、構成データおよびポリシー・データ用のLDAPディレクトリ・サーバー・プロファイルへのリンクがリストされます。プロファイル・リンクをクリックすると、そのプロファイルに指定されている情報とサポート対象の操作を確認できます。表 7-2 にリストされているすべての操作または特定の操作を指定できます。

表 7-2 サポートされるディレクトリ・サーバー操作

カテゴリ	操作	コメント
	すべての操作	すべての操作が許可されます (デフォルト)。
検索	検索エントリ ユーザーの認証	「ユーザーの認証」操作により、ユーザーは、ディレクトリ・サーバー・プロファイルのネームスペース内での認証が可能になります。このオプションを選択すると、認証ドメインのログイン・ページのリストに含まれます。
読取り	読取りエントリ	この操作により、ディレクトリ・サーバー・プロファイルでは、スキーマの読取りもサポートされます。
書込み	エントリの作成 エントリを修正 エントリの削除 パスワードの変更	「パスワードの変更」操作により、ユーザーは、ADSI または SSL 接続を通じて各自のパスワードを変更できます。一方で、より頻繁に利用される検索などの他の操作は、別のディレクトリ・サーバー・プロファイルに割り当てることが可能です。

次の手順では、ディレクトリ・サーバー・プロファイルを作成する方法について説明します。

ディレクトリ・サーバー・プロファイルを作成する手順

1. ID システム・コンソールで、「システム構成」をクリックし、次に「ディレクトリ・プロファイル」をクリックします。
2. 「追加」をクリックして新規 LDAP ディレクトリ・プロファイルを作成します。「ディレクトリ・サーバー・プロファイルの作成」ページが表示されます。

注意：ディレクトリ・サーバー・プロファイルを変更するには、「LDAP ディレクトリ・サーバー・プロファイルの構成」のリストでプロファイル名をクリックします。この場合、「ディレクトリ・サーバー・プロファイルの変更」ページが表示されます（7-28 ページの「LDAP ディレクトリ・サーバー・プロファイルの変更」を参照してください）。

ORACLE Identity Administration

ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成

ログイン・ユーザー: Master Admin

ディレクトリ・サーバー・プロファイルの作成

名前*

ネームスペース*

ディレクトリ・タイプ

Sun Directory Server 5.x
 Oracle Internet Directory
 Novell Directory Services (NDS eDirectory)
 IBMディレクトリ・サーバー
 Siemens DirX
 Data Anywhere
 Microsoft Active Directoryアプリケーション・モード
 Microsoft Active Directory(ADSIを使用)
 認証にLDAPを使用
 Microsoft Active Directory
 AD変更/パスワードは次を使用: ADSI SSL

動的補助

はい いいえ
 すべての操作
 選択された操作

操作

検索 検索エントリ ユーザーの認証
 読取り 読取りエントリ
 書込み エントリの作成 エントリを修正
 エントリの削除 パスワードの変更

使用

すべてのOracle Access Managerコンポーネント
 Identity Server
 すべてのサーバー
 ID_Server_10.1.3_M3_staqh24_6021
 Access Server
 すべてのサーバー
 M3_AAA_staqh24
 dummy_Access_Server
 Access Manager

名前	マシン	ポート番号	サーバー・タイプ
----	-----	-------	----------

注意：* 付きのフィールドは必須です。

3. 「名前」フィールドにディレクトリ・サーバー・プロファイルの名前を入力します。
この名前は、情報目的専用です。ID システムでは、ID システムのインストール時に自動的に作成されるすべてのデフォルト・ディレクトリ・サーバー・プロファイルに対して <Identity Server id> というデフォルトのネーミング規則を使用します。
4. 「ネームスペース」フィールドにディレクトリ・サーバー・プロファイルの検索ベースを入力します。

注意：このネームスペースは他のディレクトリ・サーバー・プロファイルのネームスペースと重複しないよう注意してください。ネームスペースが重複すると、重複エントリが発生します。ネームスペースの重複の例外として、Microsoft Active Directory サブドメインのディレクトリ・サーバー・プロファイルと、構成 DN を含むディレクトリ・サーバー・プロファイルがあげられます。

5. ディレクトリ・サーバーのタイプを選択します。

Siemens DirX および Sun: Siemens DirX または Sun (旧 iPlanet) のいずれかを単独で使用する場合、データを別々に格納するか一緒に格納するかを選択できます。『Oracle Access Manager インストール・ガイド』を参照してください。

Oracle Data Anywhere: Oracle Virtual Directory Server (VDS) と統合する必要があります。

Oracle Data Anywhere は、データ管理レイヤーであり、RDBMS や LDAP ディレクトリなどの複数のソースからユーザー・データを収集して仮想 LDAP ツリーに統合します。この仮想 LDAP ツリーは、ID システムで管理可能であり、アクセス・システムを使用した認証および認可のサポートに使用できます。

構成データとポリシー・データを含む LDAP ディレクトリのブランチは、VDS またはユーザー・データをホストするディレクトリ・サーバーとは異なる 1 つ以上のディレクトリ・サーバーに存在する必要があります。ID システム・アプリケーションで認識できるのは、VDS 仮想ディレクトリの外部に存在する構成情報とポリシー情報のみです。

注意：Oracle Data Anywhere と VDS を使用するためのインストール作業を行う前に、『Oracle Access Manager 統合ガイド』の VDS との統合に関する章を必ず参照してください。

Active Directory: Active Directory を選択する場合、パスワード変更操作に ADSI (Active Directory Service Interfaces) を使用するかどうかを指定します。「ADSI」オプションを選択する場合、パスワード変更用に LDAP/SSL 接続を設定する必要はありません。ADSI を使用しない場合、Oracle Access Manager では、パスワード変更用に SSL 接続が使用されます。付録 B 「ADSI に対する構成」を参照してください。

ディレクトリ・サーバーに対する他のすべての通常操作用に LDAP/SSL を設定済の場合、証明書サーバーの設定や CA 証明書のインポートなどを行う必要はありません。それ以外の場合は、パスワード変更用に LDAP/SSL を構成する必要があります。

詳細は、『Oracle Access Manager インストール・ガイド』を参照してください。

動的補助クラス: Active Directory で動的補助クラスを使用する場合、「動的補助」で「はい」を選択し、動的補助クラスを Active Directory 2003 の構造化オブジェクト・クラスに関連付けます。

詳細は、付録 A 「Active Directory でのデプロイ」を参照してください。

注意：Active Directory 2003 では、動的補助クラスまたは静的補助クラスを有効化できます。

6. このディレクトリ・サーバー・プロファイルでサポートする操作を指定します (表 7-2 のリストを参照してください)。

7. このプロファイルを使用するサーバーを指定します。
 - すべての Oracle Access Manager コンポーネント: インストール環境の各コンポーネント・サーバーで同じプロファイルを共有する場合、このオプションを選択します。
 - Identity Server: Identity Server でのみこのプロファイルを共有する場合、このオプションを選択します。特定の Identity Server でこのプロファイルを使用する場合、付属のリスト・ボックスからサーバー名を選択します。
 - AAA Servers: AAA Server オプションは、Access Server の構成オプションを示します。新規 Access Server を追加すると、常にデータベース・プロファイルを作成するよう求められます。Access Server インスタンスを追加する方法の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

8. 「追加」をクリックしてディレクトリ・サーバー・インスタンス（データベース・インスタンス）をこのプロファイルに関連付け、プライマリまたはセカンダリのサーバー・タイプを割り当てます。

詳細は、7-31 ページの「LDAP ディレクトリ・サーバー・プロファイルのデータベース・インスタンスを追加または変更する手順」を参照してください。

9. 必要なアクティブ・サーバーの最大数（ロード・バランシングのために接続するプライマリおよびセカンダリ・データベース・インスタンスの数）を指定します。
 - デフォルト値の 1 は、ロード・バランシングを使用しないことを示します。
 - 1 を超える値では、最も短いジョブ・キューを保持するデータベース・インスタンスに従って、すべてのデータベース・インスタンス全体にデータベース・リクエストが分散されます。これにより、可能なかぎり迅速にジョブが処理されます。

ロード・バランシングの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

10. フェイルオーバーしきい値を指定します。

この値では、稼働している必要のあるプライマリ・サーバーの最小数を指定します。稼働しているプライマリ・サーバーの数がこの指定数を下回ると、フェイルオーバーが発生します。この値は、最大アクティブ・サーバー数と同じにすることをお勧めします。その結果、プライマリ・サーバーが停止すると即座にセカンダリ・サーバーへのフェイルオーバーが発生します。

デフォルト値は 1 です。この場合、Identity Server から接続できるプライマリ・ディレクトリ・サーバーが存在しない場合にのみ、セカンダリ・サーバーへのフェイルオーバーが発生します。

注意: プライマリ・サーバーが停止したときに即座にセカンダリ・サーバーへのフェイルオーバーを実行するため、この値は最大アクティブ・サーバー数と同じにすることをお勧めします。フェイルオーバーと関連パラメータの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

11. 「スリープ時間 (秒)」フィールドに、ウォッチャ・スレッドを起動して、停止している 1 つ以上のプライマリ・サーバーに対する接続を再確立するまでに待機する秒数を入力します。

注意: フェイルオーバーの発生時にプライマリ・サーバーが使用可能な場合、Identity Server は最初にプライマリ・サーバーにフェイルオーバーされます。

12. 「最長セッション時間」フィールドに、再接続を試行するまでに Identity Server でディレクトリへの接続を維持する分数を指定します。

デフォルト値は 0（無制限）です。Identity Server、Access Server または Policy Manager のメモリー使用量が増加している場合は、この値を 600（10 時間）に変更することをお勧めします。

13. このプロファイルを使用可能にする場合、「プロファイルの有効化」を選択します。
次のスクリーン・ショットは、この構成ページの下半分を示しています。

The screenshot shows the 'Identity System Console' for 'Master Admin'. The left sidebar has a menu with 'ディレクトリ・プロファイル' selected. The main area is titled '動的補助' and contains several sections:

- 動的補助:** Radio buttons for authentication methods: LDAP, Microsoft Active Directory. Below it, a note: 'AD変更/パスワードは次を使用: ADSI SSL'.
- 操作:** Radio buttons for operation types: はい, すべて, 選択された操作.
- 使用:** Radio buttons for server types: Identity Server, Access Server, Access Manager.
- データベース・インスタンス:** A table with columns '名前', 'マシ名', 'ポート番号', 'サーバータイプ'. Below the table is an '追加' button.

At the bottom, there are buttons for '保存', '取消', and 'リセット'.

14. 次のように「保存」、「取消」または「リセット」を選択します。
- 変更を保存する場合、「保存」をクリックします。
 - 保存せずにこのページを終了する場合、「取消」をクリックします。
 - すべての設定をデフォルト設定にリセットする場合、「リセット」をクリックします。
15. 「OK」をクリックして設定の追加を確認します。
16. Identity Server を再起動して新規プロファイルを有効化します。

LDAP ディレクトリ・サーバー・プロファイルの表示

「プロファイルの構成」ページの中央部にある「LDAP ディレクトリ・サーバー・プロファイルの構成」という見出しの下には、構成済のディレクトリ・サーバー・プロファイルのリストが含まれます。

LDAP ディレクトリ・サーバー・プロファイルを表示する手順

1. ID システム・コンソールで、「システム構成」をクリックします。
2. 「システム構成」ページで、「ディレクトリ・プロファイル」をクリックします。

「プロファイルの構成」ページが表示されます。

ページの中央部にある「LDAP ディレクトリ・サーバー・プロファイルの構成」という見出しの下に、構成済のディレクトリ・サーバー・プロファイルのリストが含まれます。

3. 表示するディレクトリ・サーバー・プロファイルのリンクをクリックします。

「ディレクトリ・サーバー・プロファイルの変更」ページが表示されます。

LDAP ディレクトリ・サーバー・プロファイルの変更

既存の LDAP ディレクトリ・サーバー・プロファイルの変更が必要とされる場合もあります。

LDAP ディレクトリ・サーバー・プロファイルを変更する手順

1. ID システム・コンソールで、「システム構成」を選択します。
2. 「システム構成」ページで、「ディレクトリ・プロファイル」をクリックします。
3. 「プロファイルの構成」ページの「LDAP ディレクトリ・サーバー・プロファイルの構成」という見出しの下のリストで、変更するディレクトリ・サーバー・プロファイルのリンクをクリックします。
4. パラメータの詳細は、7-22 ページの「LDAP ディレクトリ・サーバー・プロファイルの作成」を参照してください。
5. 必要に応じて変更を加え、「保存」をクリックして変更を確定します。
6. Identity Server を再起動して新規プロファイルを有効化します。

手動によるシステム設定の再実行

構成データおよびポリシー・データ用のディレクトリ・サーバー・プロファイルに対して次のいずれかの操作を実行したら、その完了後にシステム設定を再実行する必要があります。

- システム・コンソールでのディレクトリ・サーバー構成オプションの変更
- 構成データおよびポリシー・データ用の新規ディレクトリ・プロファイルの作成
- 構成データおよびポリシー・データに属するディレクトリ・プロファイルの削除
- 構成データおよびポリシー・データ用のディレクトリ・プロファイルの変更
- プロファイル内のディレクトリ・インスタンスの追加または変更

注意：「ディレクトリ・サーバー構成」ページで特定の項目（アスタリスク (*) 付きの項目）を変更した場合も、システム設定を再実行する必要があります。

設定の再実行は、特定の順序で行う必要があります。

タスクの概要：システム設定の再実行

1. ID システム設定を再実行します (7-29 ページの「ID システム設定の再実行」を参照してください)。
2. 必要に応じて Policy Manager 設定を再実行します (7-29 ページの「Policy Manager 設定の再実行」を参照してください)。
3. Access Server を再構成します (7-30 ページの「Access Server の再構成」を参照してください)。

ID システム設定の再実行

setup.xml の status パラメータを変更または削除して、インストールが未完了のため設定の再実行を許可するよう ID システムに指示します。

ID システム設定を再実行する手順

1. 複数の Identity Server が稼働している場合、1 つだけ残して停止します。
2. 稼働している唯一の Identity Server ホストに移動し、次の setup.xml ファイルを開きます。
`IdentityServer_install_dir/identity/oblix/config/setup.xml`
3. status パラメータを削除するか、次の例に示すとおり status パラメータの値を done から incomplete に変更します。

```
<NameValPair ParamName="status" Value="incomplete"></NameValPair>
```
4. ファイルを保存します。
5. Identity Server を再起動します。
6. Web ブラウザで ID システム・コンソールを起動します。
ID システムの初期設定時に表示されるページに似た「セットアップ」ページが表示されません。
7. 設定を再度開始し、新規情報を指定します。
8. 設定の完了後、他の Identity Server を再起動します。
他の Identity Server により、新規情報が検出されます。
9. 次の手順を完了して、Policy Manager 設定を再実行します。

Policy Manager 設定の再実行

実装にアクセス・システムが含まれる場合、ID システム設定の再実行後に Policy Manager を手動で設定します。setup.xml の status パラメータを変更または削除して、Policy Manager 設定の再実行を可能にします。

Policy Manager 設定を再実行する手順

1. 複数の Policy Manager Web サーバーが稼働している場合、1 つだけ残して停止します。
2. 稼働している唯一の Policy Manager ホストに移動し、次の setup.xml ファイルを開きます。
`PolicyManager\oblix\config\setup.xml`
3. status パラメータを削除するか、次の例に示すとおり status パラメータの値を done から incomplete に変更して、ファイルを保存します。

```
<NameValPair ParamName="status" Value="incomplete"></NameValPair>
```
4. Policy Manager Web サーバーを再起動します。
5. Web ブラウザでアクセス・システム・コンソールを起動します。
アクセス・システムの初期設定時に表示されるページに似た「セットアップ」ページが表示されます。
6. 設定を再度開始し、新規情報を指定します。
7. 設定の完了後、他の Policy Manager Web サーバーを再起動します。
他の Policy Manager により、新規情報が検出されます。
8. Access Server を再実行します (7-30 ページの「[Access Server の再構成](#)」を参照してください)。

Access Server の再構成

Policy Manager の設定を手動で再実行したら、次の手順に従って Access Server を再構成する必要があります。configureAAAServer ツールの使用の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

Access Server を再構成する手順

1. configureAAAServer ツールの場所を見つけます。

たとえば、次のようになります。

```
AccessServer_install_dir/access/oblix/tools/configureAAAServer
```

2. configureAAAServer ツールで次のコマンドを使用し、Access Server を設定します。

```
configureAAAServer install -i AccessServer_install_dir
```

3. 新規情報を指定します。
4. Access Server を再起動します。

LDAP ディレクトリ・サーバー・プロファイルへのデータベース・インスタンスの追加

ディレクトリ・サーバー・プロファイルには、特定の LDAP ディレクトリ・サーバーのバインド情報（サーバー名、ホスト・マシン、ポート、ルート DN、パスワードなど）が含まれます。ディレクトリ・サーバー・プロファイルの一部として、データベース・インスタンスを構成できます。このようなデータベース・インスタンスを定義すると、Oracle Access Manager により、指定されたバインド資格証明に基づいて構成済のホストとポートが検証されます。データベース・インスタンスに対応するディレクトリ・サーバーは、構成時に稼働している必要があります。

注意： LDAP ディレクトリ・サーバー・プロファイル内のデータベース・インスタンスは、RDBMS プロファイル内のデータベース・インスタンスとは異なります。RDBMS プロファイルは、Oracle Access Manager を ODBC 3.0 に準拠する外部のリレーショナル・データベースに接続する場合に使用します。7-35 ページの「[RDBMS プロファイルの管理](#)」を参照してください。

LDAP ディレクトリ・サーバー・プロファイルは、ロード・バランシングおよびフェイルオーバーに使用される 1 つ以上のデータベース・インスタンスで構成されます。ディレクトリ・サーバー・プロファイルにより、アクティブ・サーバーの最大数に応じてそのインスタンス間で負荷が分散されます。また、フェイルオーバーしきい値に応じてそのインスタンス間でフェイルオーバーが実行されます。

注意： 構成ディレクトリで新規ディレクトリ・サーバーを参照するよう ID システムを再構成すると、/IdentityServer_install_dir/data/common はリセットされます。具体的には、workflowdbparams.xml のパラメータ wfinstancenotrequired=true が false にリセットされます。ディレクトリ・サーバー・インスタンスの再構成後、パラメータ wfinstancenotrequired を手動で true に再設定する必要があります。

LDAP 参照

ディレクトリ・サーバー・インスタンスを追加する場合、LDAP 参照を有効化するかどうかを指定できます。参照を使用すると、クライアント・リクエストを別のサーバーにリダイレクトし、リクエストされた情報を別の場所で検索できます。参照には、オブジェクトの名前と場所が含まれます。

ディレクトリ・サーバー・インスタンスを追加する際に LDAP 参照を有効化する場合、次のファイルで `enableLDAPReferral` パラメータを `true` に設定する必要があります。

```
install-dir\oblix\data\common\ldapconfigdbparams.xml
```

ここで、`install_dir` は、Policy Manager、Access Server または Identity Server のインストール・ディレクトリです。

次に、Active Directory に対応するこのファイルの例を示します。

```
BEGIN:vCompoundList
  specialAttrs:
    BEGIN:vNameList
      userPassword:( 2.5.4.35 NAME 'userPassword' DESC
'Standard Attribute' SYNTAX '1.3.6.1.4.1.1466.115.121.1.5' )
      sAMAccountName:( 1.2.840.113556.1.4.221 NAME 'sAMAccountName' DESC
'sAMAccountName' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
    END:vNameList
    useOIDNamingAttribute:false
    dynamicAuxiliary:false
    enableLDAPReferral:true
  END:vCompoundList
```

LDAP ディレクトリ・サーバー・プロファイルのデータベース・インスタンスを追加または変更する手順

1. ID システム・コンソールで、「システム構成」をクリックします。
2. 「システム構成」ページで、「ディレクトリ・プロファイル」をクリックします。
3. データベース・インスタンスを追加するディレクトリ・サーバー・プロファイルのリンクをクリックします。
「ディレクトリ・サーバー・プロファイルの変更」ページが表示されます。
4. 「データベース・インスタンス」まで下にスクロールし、「追加」ボタンをクリックします（既存のデータベース・インスタンスを編集または変更する場合は、データベース・インスタンスのリストからそのインスタンスを選択します）。

「データベース・インスタンスの作成」ページ（または「データベース・インスタンスの変更」ページ）が表示されます。

注意：LDAP ディレクトリ・サーバー・プロファイルの「データベース・インスタンスの変更」ページのフィールドは、RDBMS の「データベース・インスタンスの変更」ページのフィールドとは異なります。詳細は、7-38 ページの「RDBMS データベース・インスタンスの追加または変更」を参照してください。

ORACLE Identity Administration

ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org. Manager構成 | 共通構成

ログイン・ユーザー Master Admin

データベース・インスタンスの作成

名前*
マシン*
ポート番号* 389
ルートDN*
ルート・パスワード*
時間制限 0
サイズ制限 0
フラグ SSL 参照 ファスト・バインド (Windows Server 2003のADのみ)
セキュア・ポート番号 636
最初の接続数 1
最大接続数 1

注意: アスタリスク(*)の付いたフィールドは必須フィールドです。
このDBインスタンスを変更した場合は、DBプロファイルも保存する必要があります。

保存 取消

5. 各フィールドを次のように入力します。

- 名前: ディレクトリ・サーバー・インスタンスの名前を入力します。
- マシン: ディレクトリ・サーバー・インスタンスをホストするコンピュータの名前を入力します。
- ポート番号: ディレクトリ・サーバーのポート番号を入力します。
- ルート DN: 管理権限を保持するディレクトリ・サーバー・ユーザーのルート DN (バインド DN) を入力します。
- ルート・パスワード: 管理権限を保持するディレクトリ・サーバー・ユーザーのパスワードを入力します。
- 時間制限: ディレクトリ・サーバーに対するリクエストを許可する最大時間を指定します。

デフォルト値は 0 (ゼロ) 秒であり、時間はサーバーにより決定されます。データベース・インスタンス設定は、この設定に優先します。

- サイズ制限: 検索操作でディレクトリ・サーバーが戻すことのできるエントリの最大数を指定します。

デフォルト値は 0 (ゼロ) エントリであり、エントリ数はサーバーにより決定されます。

フラグ: 次のいずれかを選択します。

- SSL: SSL を使用するディレクトリ・サーバー・プロセス。この場合、最初に証明書を構成する必要があります。詳細は、使用しているディレクトリ・サーバーのドキュメントを参照してください。
- 参照: ディレクトリ・サーバー・プロファイルでこのディレクトリ・サーバーの LDAP 参照をトレースするかどうかを指定します。参照サーバーへのログイン時には同じバインド資格証明 (ルート DN とパスワード) が使用されます。

- ファスト・バインド (Windows Server 2003 の AD のみ): 簡易バインドとは異なり、セキュリティ・トークンを戻すことなくユーザー名とパスワードを認証します。認証のみを実行するアプリケーションの場合、この方式の方が簡易バインドより高速です。
 - セキュア・ポート番号: ディレクトリ・サーバーにアクセスするためのポートを指定します。

SSL を使用していない場合、またはパスワード変更で Active Directory と ADSI を組み合わせて使用している場合、このフィールドは空白のままとします。
 - 最初の接続数: ディレクトリ・サーバーへの接続に使用する初期接続数を指定します。これらの接続は、すべてのユーザー・リクエストで共有されます。最小値は 1 です。
 - 最大接続数: ディレクトリ・サーバーに許可する最大接続数を指定します。

デフォルトは 1 です。異なるタイプの操作には、異なる DB エージェントが使用されます。「最大接続数」フィールドは、特定のエージェント向けに実装されています。オープン可能な接続の合計数は、このフィールドに指定する値よりずっと多くすることができます。詳細は、『Oracle Access Manager デプロイメント・ガイド』のディレクトリ接続プールの構成方法に関する情報を参照してください。
6. 「保存」をクリックして設定を保存します。
- 保存せずに終了する場合は「取消」をクリックし、最後に保存した設定に戻る場合は「リセット」をクリックします。

LDAP ディレクトリ・サーバー・インスタンスの削除

LDAP ディレクトリ・サーバー・インスタンスは、削除できます。

LDAP ディレクトリ・サーバー・プロファイルのディレクトリ・サーバー・インスタンスを削除する手順

1. ID システム・コンソールで、「システム構成」を選択し、次に「ディレクトリ・オプションの構成」をクリックします。

ディレクトリ・サーバー・プロファイルの構成ページが表示されます。このページには、すべてのディレクトリ・サーバー・プロファイルがリストされます。
2. インスタンスを追加するディレクトリ・サーバー・プロファイルをクリックします。

「ディレクトリ・サーバー・プロファイルの変更」ページが表示されます。
3. 「ディレクトリ・サーバー・プロファイルの変更」ページで、削除するデータベース・インスタンスを選択します。
4. 「削除」をクリックします。

ディレクトリ・サーバー・インスタンスが削除されます。

複数のディレクトリ検索ベースの操作

Oracle Internet Directory などの一部のディレクトリでは、非結合検索ベースまたはレルムとも呼ばれる複数の検索ベースを構成できます。これらの非結合検索ベースまたはレルムは、次のような重複しないディレクトリ・ツリーで構成されます。

- o=company,c=us
- o=oracle,c=us

Oracle Access Manager でこのような複数の検索ベースに含まれるデータを管理する場合、検索ベースごとに ID システムとアクセス・システムを個別に構成する必要があります。

次の手順では、ディレクトリに非結合検索ベース（またはレルム）をすでに定義してあると仮定します。

タスクの概要：非結合検索ベースを操作するための ID システムの構成

1. ID システム・コンソールで、「システム構成」をクリックし、次に「ディレクトリ・プロファイル」をクリックします。
2. サポートする新規非結合検索ベースごとに個別のディレクトリ・サーバー・プロファイルを追加します。

詳細は、7-22 ページの「[LDAP ディレクトリ・サーバー・プロファイルの作成](#)」を参照してください。指定したネームスペースがディレクトリのネームスペースと正確に一致していることを確認します。
3. Identity Server と、Identity Server を実行している Web サーバーを再起動します。
4. ID システム・コンソールで、「システム構成」→「ディレクトリ・プロファイル」をクリックし、「ディレクトリ・プロファイル」ページに戻ります。
5. 「ディレクトリ・プロファイル」ページの「ディレクトリ・サーバー」リンクをクリックします。
6. 「非結合検索ベース」フィールドに、最初の非結合検索ベースのネームスペースを入力します。

これは、ディレクトリ・サーバー・プロファイルに指定されているネームスペースと同じである必要があります。
7. 「追加」をクリックして追加の非結合検索ベースを構成します。
8. 新規非結合検索ベースごとに、検索ベースにエントリのあるユーザーの新規権限を構成します。

詳細は、4-21 ページの「[ユーザーによる LDAP データの表示および変更の許可](#)」を参照してください。
9. 非結合検索ベースごとに ID 管理者と委任 ID 管理者を追加します。

詳細は、第 2 章「[ID システム管理者の指定](#)」を参照してください。
10. 次のファイルをテキスト・エディタで開き、このファイルの whichAttrIsLogin パラメータの値がディレクトリのユーザー属性と一致していることを確認します。

`IdentityServer_install_dir/oblix/apps/common/bin/globalparams.xml`

タスクの概要：非結合検索ベースを操作するためのアクセス・システムの構成

1. 7-34 ページの「タスクの概要：非結合検索ベースを操作するための ID システムの構成」の手順を完了します。

2. 次のファイルをテキスト・エディタで開き、このファイルの `whichAttrIsLogin` パラメータの値がディレクトリのユーザー属性と一致していることを確認します。

```
PolicyManager_install_dir/oblix/apps/common/bin/globalparams.xml
```

3. アクセス・システム・コンソールで、適切な資格証明マッピング・パラメータを使用する認証スキームを作成します。

たとえば、現在の非結合検索ベースで `Person` オブジェクト・クラスとして `gensiteorgperson` を使用し、ログイン属性として `genuserid` を使用している場合、認証スキームを次のように作成します。

```
obMappingBase="%domain%",obMappingFilter="(&(&(objectclass=objectclassname)(loginattribute=%userid))(|(!(obuseraccountcontrol=*)) (obuseraccountcontrol=ACTIVATED)))",obdomain="domain"
```

ここで、`objectclassname` は `Person` オブジェクト・クラスの名前（`gensiteorgperson` など）であり、`loginattribute` は `Person` オブジェクト・クラスのログイン属性の名前（`genuserid` など）です。詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

4. Policy Manager で、適切な認証スキームを使用するよう関連する認証ルールを変更します。詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

5. Policy Manager で、認証の成功時に `HTTP_OBLIX_UID` ヘッダー変数の `obuniqueID` の値を戻すよう `/access` および `/identity` ポリシー・ドメインを構成します。

これらのポリシー・ドメインの認証ルールで、次の認証成功アクションを構成します。`obuniqueid` 属性により、特定のログイン属性に構成されている任意の値が戻されます（これらの属性は、ディレクトリの各検索ベースで使用されます）。

タイプ: HEADERVAR

名前: HTTP_OBLIX_UID

戻り属性: obuniqueid

RDBMS プロファイルの管理

Oracle Access Manager では、RDBMS プロファイルを使用して、ODBC 3.0 に準拠する外部のリレーショナル・データベースに接続します。現在のところ、ユーザー・アクセス・プロファイル・レポート機能とデータベースへの監査送信機能で RDBMS プロファイルを使用しています。各プロファイルでは、データベースのプライマリ・インスタンスが停止した場合のフェイルオーバーに備えて、複数のデータベース・インスタンスを含むことができます。

注意： RDBMS プロファイルには、データベース・インスタンスが含まれません。これらのデータベース・インスタンスは、LDAP ディレクトリ・サーバー・プロファイルの一部として構成されるデータベース・インスタンスとは異なります。LDAP ディレクトリ・サーバー・プロファイルのデータベース・インスタンスは、LDAP ディレクトリのロード・バランシングおよびフェイルオーバーに使用されます。

この項には、次の各項目が含まれます。

- [RDBMS プロファイルの追加または変更](#)
- [RDBMS データベース・インスタンスの追加または変更](#)

RDBMS プロファイルの追加または変更

RDBMS プロファイルを追加する手順と変更する手順は似ています。次に、これらの手順を説明します。表 7-3 に、入力するフィールドを示します。

表 7-3 RDBMS プロファイルを追加または変更する場合のフィールドの説明

フィールド	説明
名前	RDBMS プロファイルのわかりやすい名前を選択します。
データベース接続タイプ	データベースへの監査送信を構成している場合、データベースで使用されている接続タイプを選択します。詳細は、 第 11 章「監査」 を参照してください。
使用	RDBMS プロファイルを使用する機能に対応するボックスを選択します。現在のところ、ユーザー・アクセス権限レポート機能とデータベースへの監査送信機能を選択できます。
データベース・インスタンス	フェイルオーバーに使用するデータベースの複数のコピーを次のように作成できます。 <ul style="list-style-type: none"> ■ データベース・インスタンスを追加するには、「追加」をクリックします。「データベース・インスタンスの作成」ページが表示されたら、アスタリスク付きのフィールドに入力します。詳細は、7-38 ページの「RDBMS プロファイルのデータベース・インスタンスを追加または変更する手順」を参照してください。 ■ 既存のデータベース・インスタンスを変更するには、データベース・インスタンス・リストから変更するインスタンスを選択します。 ■ データベース・インスタンスのサーバー・タイプを設定するには、リストから「プライマリ」または「セカンダリ」を選択します。 ■ データベース・インスタンスを削除するには、削除するインスタンスの横のボックスを選択し、「削除」をクリックします。
最大アクティブ・サーバー数	これは、任意の時点でリレーショナル・データベースに接続できるサーバーの最大数です。
フェイルオーバーしきい値	接続しているプライマリ・サーバーの数がこの数を下回ると、フェイルオーバーが発生します。
スリープ時間 (秒)	接続の切断後、フェイルオーバーを実行するまでに待機する秒数です。
最長セッション時間	データベースに対する接続は、この分数が経過すると、正常に機能している場合でも破棄されて新規接続が確立されます。
プロファイルの有効化	プロファイルをアクティブにする場合、必ずこのボックスを選択します。

RDBMS プロファイルを追加または変更する手順

1. ID システム・コンソールで、「システム構成」を選択し、次に「ディレクトリ・プロファイル」をクリックします。

「プロファイルの構成」ページが表示されます。このページには、すべてのディレクトリ・サーバー・プロファイルがリストされます。

ORACLE Identity Administration

ヘルプ バージョン情報 ログアウト

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成

User Manager Group Manager Org Manager Identity System Console

ログイン・ユーザー: Master Admin

- パスワードポリシー
- ロストパスワードポリシー
- ディレクトリ・プロファイル**
- Identity Server
- WebPass

プロファイルの構成
次のものは構成ベースおよび検索ベースの設定を含んでいます。特定の値を変更するにはリンクをクリックします。

ディレクトリ・サーバー

マシン	avanur
ポート番号	3334
ルートDN	cn=Directory Manager
ルート・パスワード	<非表示>
検索ベース	o=company,c=us
構成ベース	o=Oblix,o=company,c=us
ディレクトリ・サーバー・セキュリティ・モード	オープン
非結合検索ベース	

「プロファイルの構成」ページの下部に「RDBMS プロファイルの構成」セクションがあります。

RDBMSプロファイルの構成

名前 プライマリ・サーバー セカンダリ・サーバー

Profile Instance 1

2. RDBMS プロファイルのリストで、編集するプロファイルの名前を選択します（または、「追加」をクリックして新規プロファイルを作成します）。

ORACLE Identity Administration

ヘルプ バージョン情報 ログアウト

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成

User Manager Group Manager Org Manager Identity System Console

ログイン・ユーザー: Master Admin

- パスワードポリシー
- ロストパスワードポリシー
- ディレクトリ・プロファイル**
- Identity Server
- WebPass
- サーバー設定
- 診断
- 管理者
- スタイル
- 写真

RDBMSプロファイルの作成

名前*

データベース接続タイプ* ODBC OCI

使用* レポート中 監査中 MMS

データベース・インスタンス

名前 サーバー・タイプ

最大アクティブ・サーバー数	<input type="text" value="1"/>
フェイルオーバーしきい値	<input type="text" value="1"/>
スリープ時間(秒)	<input type="text" value="60"/>
最長セッション時間(分)	<input type="text" value="0"/>

プロファイルの有効化

注意: アスタリスク(*)の付いたフィールドは必須フィールドです。

3. 「RDBMS プロファイルの作成」ページ（または「RDBMS プロファイルの変更」ページ）のフィールドを入力または変更します（表 7-3 を参照してください）。
4. フィールドへの情報の入力を完了したら、「保存」をクリックして変更をコミットします。

RDBMS データベース・インスタンスの追加または変更

RDBMS データベース・プロファイルのデータベース・インスタンスを作成する手順と変更する手順はよく似ているため、次の手順でまとめて説明します。どちらの場合も、表 7-4 の情報をフィールドに入力する必要があります。

表 7-4 RDBMS プロファイルのデータベース・インスタンスを追加または変更する場合のフィールドの説明

フィールド	説明
名前	データベース・インスタンスの名前
「DSN 名」または「グローバル・データベース名」	ODBC 接続タイプでデータベース監査を構成している場合、「DSN 名」フィールドが表示されます。これにより、特定のデータ・ソースにアクセスするすべてのクライアントの一意的データ・ソース定義が識別されます。(DSN という用語は、ODBC データ・ソース定義全体を示すものとして不正確に使用されることがよくあります。) OCI 接続タイプでデータベース監査を構成している場合、データベース・インスタンス定義にグローバル・データベース名 (GDN) を指定します。 詳細は、11-13 ページの「 データベース監査用の RDBMS プロファイルについて 」を参照してください。
ユーザー名	このデータベース・インスタンスへのアクセス権限を保持する管理者の名前
パスワード	このデータベース・インスタンスのパスワード
時間制限	データベースへの接続を切断し、新規接続で置き換えるまでの分数
サイズ制限	データベースの最大サイズ
最初の接続数	初期化時にこのデータベース・インスタンスに接続されるプライマリ・サーバーとセカンダリ・サーバーの数
最大接続数	このデータベース・インスタンスに接続できるプライマリおよびセカンダリの Access Server の合計数

RDBMS プロファイルのデータベース・インスタンスを追加または変更する手順

1. ID システム・コンソールで、「システム構成」を選択し、次に「ディレクトリ・プロファイル」をクリックします。
ディレクトリ・サーバー・プロファイルの構成ページが表示されます。
2. 「RDBMS プロファイルの構成」セクションで、「追加」をクリックして RDBMS プロファイルを作成するか、変更する RDBMS プロファイルの名前をリストから選択します。
ユーザーの選択に応じて、「RDBMS プロファイルの作成」ページまたは「RDBMS プロファイルの変更」ページが表示されます。
3. 「データベース・インスタンス」セクションで、「追加」ボタンをクリックして新規インスタンスを作成するか、編集するインスタンスの名前をリストから選択します。

- 「データベース・インスタンスの変更」ページまたは「データベース・インスタンスの作成」ページのフィールドを入力します。

各フィールドの説明は、表 7-4 を参照してください。

The screenshot shows the Oracle Identity Administration console interface. The main content area is titled 'データベース・インスタンスの作成' (Database Instance Creation). It contains a form with the following fields:

名前*	<input type="text"/>
DSN名*	<input type="text"/>
データベース名	<input type="text"/>
ユーザー名	<input type="text"/>
パスワード	<input type="password"/>
時間制限	<input type="text" value="0"/>
サイズ制限	<input type="text" value="0"/>
最初の接続数	<input type="text" value="5"/>
最大接続数	<input type="text" value="5"/>

注意: アスタリスク(*)の付いたフィールドは必須フィールドです。
このDB-インスタンスを変更した場合は、DBプロファイルも保存する必要があります。

- ページのフィールドに情報を入力したら、「保存」をクリックして変更をコミットします。

WebPass の構成

Identity Server のインストール後、最初に WebPass をインストールします。ID システムの設定後、複数の WebPass インスタンスをインストールおよび構成できます。各 WebPass インスタンスは、個別にインストールおよび構成します。WebPass インスタンスをインストールする場合、いくつかの必須パラメータを指定します。マスター管理者は、ID システム・コンソールでこれらのパラメータを変更し、追加の情報（フェイルオーバーしきい値など）を入力できます。

ユーザーから Web サーバー・リソースへのアクセス・リクエストがあると、そのリクエストは WebPass によって Identity Server にリダイレクトされます。その後、Identity Server により、ディレクトリ・サーバーを通じてユーザーの ID がチェックされます。WebPass プラグインは、Web サーバーごとに構成する必要があります。

WebPass のインストール方法の詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。この項には、次の各項目が含まれます。

- 構成済の WebPass の表示
- WebPass の追加または変更
- WebPass の削除
- コマンドラインによる WebPass の変更
- Identity Server と WebPass の関連付けの管理
- Identity Server と WebPass の関連付けの解除

構成済の WebPass の表示

WebPass の構成は、ID システム・コンソールの「WebPass の構成」機能を使用して行います。

構成済の WebPass を表示する手順

1. ID システム・コンソールで、「システム構成」→「WebPass」を選択します。
「すべての WebPass をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. WebPass の情報を表示するには、WebPass のリンクをクリックします。
「WebPass の詳細」ページが表示されます。このページには、WebPass インスタンスに関するすべての情報がリストされます。

WebPass の追加または変更

新規 WebPass を追加する場合、ID システム・コンソールでインスタンスを追加して Web サーバー・ホストに WebPass をインストールし、Web サーバー構成を更新して WebPass と Web サーバー間の通信を確立します。インスタンスを追加するには、次の手順を使用します。詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

WebPass を追加する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。
「すべての WebPass をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. 「WebPass の構成」ページで、「追加」をクリックします。
「新規 WebPass の追加」ページが表示されます。
3. 「名前」フィールドにこの WebPass インスタンスの名前を入力します。

注意： このインスタンスとともに保存する名前は、変更できません。名前を変更するには、このインスタンスを削除して別の名前で作成します。

4. 「ホスト名」フィールドに、この WebPass をホストする Web サーバー・インスタンスの名前を入力します。
5. 「Web サーバー・ポート」フィールドに、Web サーバー・インスタンスがリスニングするポート番号を入力します。
最大値は 65535 です。
6. 「最大接続数」フィールドに、この WebPass で Identity Server に対してオープンする接続の最大数を指定します。
接続の最小数は 1 です。ロード・バランシングおよびフェイルオーバーのために多くの接続を指定できます。
7. 「トランスポート・セキュリティ」フィールドで、Oracle Access Manager のインストール時に指定されたセキュリティ・モードを変更できます。
トランスポート・セキュリティ・モードにより、WebPass と Identity Server 間の通信のセキュリティ・レベルを指定します。詳細は、[第 8 章「トランスポート・セキュリティ・モードの変更」](#)を参照してください。
サポートされるトランスポート・セキュリティ・モードは、次のとおりです。
 - オープン：トランスポート・セキュリティは適用されません。
 - 簡易：基本セキュリティが提供されます。通信は、Transport Layer Security、RFC 2246 (TLS v1) を使用して暗号化されます。通信要素は、パスワード・ベースの

メカニズムを使用して相互に認証を行います。簡易セキュリティを使用するすべての要素は、インストール環境全体で同じパスワードを使用する必要があります。Oracle Access Manager では、認証を実行する証明書が提供されます。

- 証明書: 内部認証局 (CA) を管理する場合に使用します。通信は、TLS v1 を使用して暗号化されます。クライアントとサーバーは、接続の確立時に VeriSign 社などのサーブド・パーティの X.509 証明書を提出する必要があります。

注意: Identity Server と WebPass では、同じトランスポート・セキュリティ・モードを使用する必要があります。必要に応じて、インストール済のコンポーネントごとにこれらの手順を繰り返してください。

8. 「最大セッション時間 (時間)」フィールドに、WebPass と Identity Server 間の接続をクローズして新規接続をオープンするまでの最大時間 (時間単位) を指定します。
9. 「フェイルオーバーしきい値」フィールドに、プライマリ Identity Server に対する接続の最大数を指定します。

プライマリ・サーバーのみではこの数に満たない場合、WebPass ではセカンダリ・サーバーを使用してこの数を確保しようとします。たとえば、このフィールドに 4 が指定された状態で、プライマリ Identity Server に対する使用可能な接続数が 3 に減少した場合、WebPass ではセカンダリ・サーバーに対する接続をオープンしようと試みます。

WebPass と Identity Server 間のフェイルオーバーを構成する方法の詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

10. 「Identity Server タイムアウトしきい値」フィールドに、応答しない Identity Server に WebPass で接続を試みた後、そのサーバーを接続不可能とみなして別のサーバーへの接続を試みるまでの時間 (秒単位) を指定します。

値を指定しない場合、タイムアウトは適用されません。

11. 「スリープ時間 (秒)」フィールドに、WebPass で ID システムとの接続をチェックする間隔を指定します。

フェイルオーバーしきい値に満たないためにセカンダリ接続が現在使用中の場合に、最小接続数のチェックに加え、同じチェックによりプライマリ・サーバー接続の再確立も試行されます。

12. 「保存」をクリックして WebPass プラグインを追加します (保存せずにこのページを終了する場合は、「取消」をクリックします)。

「保存」をクリックすると、「すべての WebPass をリスト」ページに WebPass プラグインが表示されます。

13. WebPass プラグインを 1 つ以上の Identity Server に関連付けます (7-45 ページの「Identity Server と WebPass の関連付けの管理」を参照してください)。

WebPass を変更する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。
「すべての WebPass をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. 「すべての WebPass をリスト」ページで、変更する WebPass の名前をクリックします。
「WebPass の詳細」ページが表示されます。
3. 「変更」をクリックします。
「WebPass の変更」ページが表示されます。
4. 必要に応じてパラメータを変更します。

注意： 変更するパラメータの詳細は、7-40 ページの「[WebPass の追加または変更](#)」を参照してください。

5. 「保存」をクリックして変更を保存します（保存せずにこのページを終了する場合は、「取消」をクリックします）。

WebPass の削除

ここでの WebPass の削除は、構成済の WebPass インスタンスのリストから WebPass を除外することを意味します。WebPass を Web サーバー・インスタンスから削除するには、WebPass をアンインストールする必要があります。

WebPass を削除する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。
「すべての WebPass をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. 「すべての WebPass をリスト」ページで、削除する WebPass インスタンスの横のチェック・ボックスを選択します。
3. 「削除」をクリックします。
4. プロンプトが表示されたら、「OK」をクリックして操作を確認します。
構成済の WebPass のリストから WebPass インスタンスが削除されます。

注意： ID システム・コンソールで WebPass インスタンスを削除しても、アンインストール・プログラムを実行しなければ、その WebPass インスタンスは Web サーバーの再起動時に再度ディレクトリ・サーバーに追加されます。

コマンドラインによる WebPass の変更

状況によっては、WebPass パラメータの変更が必要となります。最大セッション時間やフェイルオーバーしきい値などの一部のパラメータは、ID システム・コンソールで変更できます。コマンドライン・ツールの `setup_webpass` を使用すると、ホスト・マシン名やトランスポート・セキュリティ・モードなどの他のパラメータを変更できます。

通常は、コマンドライン・ツールを使用してトランスポート・セキュリティ・モードを変更します。このツールは、Windows と Solaris 両方のインストール環境で使用できます。

コマンドラインにより WebPass を変更する手順

1. 次の場所に移動します。

```
WebPass_install_dir\identity\oblix\tools\setupWebPass
```

ここで、`WebPass_install_dir` は、WebPass がインストールされているディレクトリです。

2. `setupWebPass` ディレクトリで、`setup_webpass` ツールを実行します。

表 7-5 のコマンドを使用してパラメータを指定できます。

表 7-5 setup_webpass のコマンド

コマンド	操作
<code>[-i install_dir]</code>	WebPass のインストール・ディレクトリを指定します。
<code>[-q] [-n WebPass_ID]</code>	WebPass ID を指定します。
<code>[-h Identity_Server_Host_Name]</code>	Identity Server がインストールされているマシンの名前を指定します。
<code>[-p Identity_Server_port_#]</code>	Identity Server がインストールされているマシンのポート番号を指定します。
<code>[-s open simple cert]</code>	トランスポート・セキュリティ・モードを指定します。
<code>[-P simple cert mode password]</code>	簡易または証明書トランスポート・セキュリティ・モードのパスワードを指定します。
<code>[-c request install]</code>	証明書のリクエストまたはインストールを指定します。

コマンドラインによりトランスポート・セキュリティ・モードを再構成する手順

1. WebPass のトランスポート・セキュリティ・モードを再構成するには、コマンドラインで次のコマンドを実行します。

```
setup_webpass -i WebPass_install_dir -m
```

2. WebPass のトランスポート・セキュリティ・モードを選択します。

「オープン」を選択する場合

トランスポート・セキュリティ・モードは、オープン・モードで実行するよう再構成されます。

「簡易」を選択する場合

システムによりパスワードを求められます。

「証明書」を選択する場合

- システムにより証明書パスワードを求められます。

プロンプトでパスワードを入力してください。

- システムにより、証明書をリクエストするかインストールするかを指定するよう求められます。

- 証明書リクエストを指定すると、次の組織情報を求められます。

国名
 都道府県名
 市町村名
 組織名
 組織単位
 共通名 (HostName.DomainName.com など)
 電子メール・アドレス

- 証明書モードの場合、情報を入力すると、証明書リクエストが生成されて *IdentityServer_install_dir\identity\oblix\config\ois_req.pem* ファイルに配置されます (*IdentityServer_install_dir* は、ID システムがインストールされているディレクトリです)。

この証明書リクエストは、認証局の署名を受ける必要があります。

- 証明書インストールを指定した場合、証明書キー・ファイル、証明書ファイルおよび証明書連鎖ファイルの場所を示すフルパスを求められます。

パスを指定すると、トランスポート・セキュリティ・モードが再構成されます。詳細は、第 8 章「トランスポート・セキュリティ・モードの変更」を参照してください。

トランスポート・セキュリティ・モードのパスワードを変更する手順

1. コマンドラインで次のコマンドを実行します。

```
setup_webpass -i WebPass_install_dir -k
```

2. 次の情報を入力します。

- 旧パスワード
- 新パスワード
- 新パスワードの再確認

パスワードが変更されます。

Identity Server と WebPass の関連付けの管理

WebPass からのリクエストを受信する 1 つ以上の Identity Server を選択する必要があります。1 つの Identity Server は、複数の WebPass に関連付けることができます。WebPass インスタンスに関連付けられているプライマリおよびセカンダリの Identity Server のリストを表示することが可能です。また、次の手順を使用することで、ロード・バランシングおよびフェイルオーバーのために Identity Server と WebPass 間に構成されている接続の数を変更できます。

- [WebPass に関連付けられている Identity Server を表示する手順](#)
- [WebPass に対する Identity Server の接続を変更する手順](#)
- [Identity Server を WebPass に関連付ける手順](#)

WebPass に関連付けられている Identity Server を表示する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。
「すべての WebPass をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. WebPass のリンクをクリックします。
「WebPass の詳細」ページが表示されます。
3. 「Identity Server をリスト」ボタンをクリックします。
WebPass に構成されているプライマリ・サーバーとセカンダリ・サーバーをリストしたページが表示されます。
4. Identity Server のリンクをクリックしてその詳細を表示します。
「Identity Server の詳細」ページが表示されます。

WebPass に対する Identity Server の接続を変更する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」をクリックします。
「すべての Identity Server をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. 適切なサーバーのリンクをクリックします。
「Identity Server の詳細」ページが表示されます。
3. 「Identity Server の詳細」ページで、「変更」をクリックします。
Identity Server の詳細がリストされた「Identity Server の変更」ページが表示されます。
4. 必要に応じて、「スレッド数」フィールドの値を変更します。
5. 「保存」をクリックして変更を保存します。
6. Identity Server を再起動します。

Identity Server を WebPass に関連付ける手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。

「すべての WebPass をリスト」ページが表示されます。このページで、WebPass を追加、変更または削除できます。
2. 適切な WebPass のリンクをクリックします。
3. 「WebPass の詳細」ページで、「Identity Server をリスト」をクリックします。

次のページに、WebPass に関連付けられているプライマリ・サーバーとセカンダリ・サーバーがリストされます。
4. 「追加」をクリックします。

「WebPass へ新規 Identity Server を追加」ページが表示されます。
5. 「サーバーの選択」リストで Identity Server を選択します。
6. この Identity Server がプライマリ・サーバーかセカンダリ・サーバーかを指定します。

この情報は、ロード・バランシングおよびフェイルオーバーのために必要です。
7. 「接続数」ボックスで、WebPass インスタンスによりこの Identity Server に対してオープンする接続の最大数を指定します。

最小数は 1 です。ロード・バランシングおよびフェイルオーバーのためにより多くの接続を追加できます。
8. 「追加」をクリックしてこの Identity Server を WebPass に関連付けます。

Identity Server と WebPass の関連付けの解除

状況によっては、Identity Server と WebPass インスタンスの関連付けの解除が必要となります。たとえば、所属部署のマシン・リソースが再割当てされる場合です。この場合、WebPass と Identity Server の関連付けの妥当性が失われる可能性があります。そのため、相互の関連付けを解除する必要があります。関連付けを解除しないと、WebPass では引き続き同じ Identity Server がポーリングされるため、Web サーバーのパフォーマンスが低下します。

注意： WebPass にただ 1 つのプライマリ・サーバーが構成されている場合、その Identity Server との関連付けは解除できません。

Identity Server と WebPass の関連付けを解除する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。
2. 既存の WebPass をクリックします。
3. 「Identity Server をリスト」をクリックします。
4. 関連付けを解除する Identity Server の横のチェック・ボックスを選択します。
5. 「削除」をクリックします。
6. プロンプトが表示されたら、「OK」をクリックして削除を確認します。

これで、この WebPass インスタンスでは、関連付けを解除した Identity Server と通信できなくなります。

パスワード・ポリシーの構成

パスワード・ポリシーは、ユーザーが作成するパスワードの種類とパスワードの有効期間を制御する一連のルールで構成されます。パスワード・ポリシーにより、ユーザーへのパスワード期限切れの通知方法、ユーザーによる期限切れパスワードのリセット方法、およびユーザーによるロスト・パスワードの回復方法も制御されます。

パスワード・ポリシーは、ID システムで作成します。これらのポリシーは、ID システムとアクセス・システムに対してログインを試みるユーザーに適用されます。また、これらのポリシーは、アクセス・システムにより保護されているリソースにアクセスしようとするユーザーにも適用されます (7-61 ページの「[アクセス・システムでのパスワード・ポリシーの実施](#)」を参照してください)。

パスワード・ポリシーで制御されるパスワードの特性およびライフ・サイクルは、次のとおりです。

- 有効なパスワードのルール。

このルールには、パスワードとして使用できる最低文字数や、使用する必要のある文字のタイプが含まれます。たとえば、数字と文字の両方を必ず含めるよう強制できます。

パスワード・プロパティは、ID システム・コンソールで構成します。

有効なパスワードを構成するための追加ルールを定義する場合、ID イベント API に付属するパスワード・ポリシー実施用の外部フックを使用できます。詳細は、『[Oracle Access Manager 開発者ガイド](#)』を参照してください。

- ロスト・パスワード管理のためのチャレンジ・フレーズとレスポンス。

ロスト・パスワードを回復する際に、1つ以上のチャレンジ・フレーズに回答するようユーザーに強制できます。また、チャレンジ・フレーズのルールを構成できます。たとえば、複数のチャレンジに対して同じレスポンスを使用することを禁止できます。1つ以上のチャレンジ・フレーズに正しく回答した場合、ユーザーはパスワード・リセット・ページにリダイレクトされます。パスワードのリセット後、ユーザーはログインを許可されません。

- パスワード期限切れおよびパスワード・リセットの設定。

パスワードの有効期間を指定し、パスワード期限切れが迫ったときに電子メールやログイン時の画面でそのことをユーザーに通知できます。また、URL リダイレクトを構成して、パスワードのリセット後にユーザーを当初リクエストされたリソースに戻すことが可能です。

- 不適切なパスワード入力後のアカウント・ロックアウト。

一定の時間内に不適切なパスワードを何回入力したらそのユーザーをロックアウトするかを構成できます。

アクセス・システムでは、ユーザー ID またはリクエストされたリソース情報を含まないロックアウト URL を構成することもできます。

- パスワード・リセット・ページおよびロスト・パスワード管理ページ用のスタイルシート。

アクセス・システムでは、ユーザーをこれらのページにリダイレクトできますが、これらのページ自体は ID システムに存在します。これらのページに対して、ID システムに付属する様々なスタイルシートを構成できます。

- ディレクトリ内の個々のドメインに対応する一意のパスワード・ポリシー。

ディレクトリ・ツリーの異なるブランチに対応するパスワード・ポリシーの個別セットを作成できます。

- 最近の成功したログイン試行と失敗したログイン試行のログ。

ディレクトリに書き込まれたこれらのログには簡単にアクセスできます。監査ログに含まれる履歴データに加え、これらのログが提供されます。

この項には、次の各項目が含まれます。

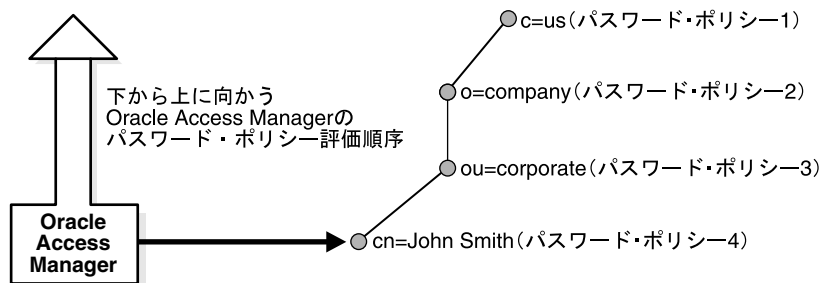
- [パスワード・ポリシーの評価順序](#)
- [パスワード・ポリシーの管理](#)
- [ロスト・パスワード管理](#)
- [アクセス・システムでのパスワード・ポリシーの実施](#)
- [パスワードのリダイレクト URL の構成](#)
- [Access Server キャッシュの更新](#)

パスワード・ポリシーの評価順序

異なるドメインに対して異なるパスワード・ポリシーを構成できます。1つのドメインは、ディレクトリ・ツリーに含まれる特定ノードの下の領域です。

ユーザーは、ドメイン内で複数のポリシーの制御下に置かれる場合があります。この場合、パスワード・ポリシーは、下から上へと評価されます。ユーザーに適用される最初のポリシーは、[図 7-1](#) のように選択されます。

図 7-1 パスワード・ポリシーの評価順序



この例では、4つのパスワード・ポリシーが John Smith に適用されています。パスワード・ポリシー 4 は、ディレクトリ・ツリーの最下位レベル (cn) に存在するため、このポリシーが最初に評価されて実施されます。

パスワード・ポリシーの管理

パスワード・ポリシーは、ID システム・コンソールで構成します。すべてのドメインに適用するデフォルト・パスワード・ポリシーを作成できます。また、特定のディレクトリ・ドメインに対応するパスワード・ポリシーを定義することや、1つのドメイン内に複数のポリシーを定義することも可能です。

この項には、次の各項目が含まれます。

- [パスワード・ポリシーの表示](#)
- [異なるタイプのパスワード・ポリシーのデフォルトの設定](#)
- [特定ドメイン用のパスワード・ポリシーの作成](#)
- [パスワード・ポリシーの変更](#)
- [パスワード・ポリシーの削除](#)

パスワード・ポリシーの表示

パスワード・ポリシーは、「パスワード・ポリシー管理」ページで参照できます。

パスワード・ポリシーのリストを表示する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックします。
2. 左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。
3. 設定を表示するポリシーのリンクをクリックします。

「パスワード・ポリシー管理」ページが表示されます。このページには、デフォルト・パスワード・ポリシーと、ドメイン固有のパスワード・ポリシーのリストが表示されます。

異なるタイプのパスワード・ポリシーのデフォルトの設定

パスワード・ポリシーのデフォルトを設定できます。これらのデフォルトは、ユーザーが作成するドメイン固有のポリシーにより上書きされます。

次のデフォルトを作成できます。

- **パスワード期限切れ警告の URL:** この設定は、アクセス・システムにより保護されているリソースにのみ適用されます。
この URL により、ユーザーは、期限切れ通知フォームにリダイレクトされます。オプションで、この URL によりユーザーをパスワード変更フォームにリダイレクトできます。また、この URL を使用して、パスワードの変更後にユーザーを当初リクエストされたリソースに戻すことも可能です。
詳細は、7-64 ページの「[デフォルトのパスワード期限切れ警告のリダイレクト URL を設定する手順](#)」を参照してください。
- **パスワード変更のリダイレクト URL:** この設定は、アクセス・システムにより保護されているリソースにのみ適用されます。
この設定は、パスワード期限切れ警告の URL とほぼ同じです。この URL は、パスワード変更ページを参照します。オプションで、この URL によりユーザーを当初リクエストされたリソースにリダイレクトできます。
詳細は、7-62 ページの「[パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成](#)」を参照してください。
- **ロスト・パスワードのリダイレクト URL:** この URL は、パスワード管理システムの一部として簡単に使用できるように、Web ページ上に Portal Inserts として設定します。
ID システム・コンソールでは、情報目的でこの URL を記録します。
詳細は、7-54 ページの「[ロスト・パスワード管理](#)」を参照してください。
- **カスタム・アカウント・ロックアウトのリダイレクト URL:** この URL は、アクセス・システムにより保護されているリソースにのみ適用されます。
詳細は、7-65 ページの「[アカウント・ロックアウトのリダイレクト URL の設定](#)」を参照してください。
Identity Server には、デフォルトでロックアウト情報を表示するメカニズムが用意されています。アカウント・ロックアウトの動作をカスタマイズする場合、IDXML プログラムで使用できるエラー・コードを ID システムから戻すことができます。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。
- **成功した認証イベント:** この設定により、ユーザーがユーザー・ディレクトリ・サーバーへのログイン試行に成功した最新の時刻が書き込まれます。
デフォルトでは、情報は OblixPersonPasswordPolicy オブジェクト・クラスの oblastSuccessfulLogin 属性に書き込まれます。この機能により、最も関連性の高いログイン情報に迅速にアクセスできます。履歴情報は、監査ログに含まれます。

- **失敗した認証イベント:** この設定により、ユーザーがユーザー・ディレクトリ・サーバーへのログイン試行に失敗した最新の時刻が書き込まれます。

デフォルトでは、ログ認証情報は `OblixPersonPasswordPolicy` オブジェクト・クラスの `oblastFailedLogin` 属性に書き込まれます。この機能により、最も関連性の高いログイン情報に迅速にアクセスできます。履歴情報は、監査ログに含まれます。

デフォルト・パスワード・ポリシーを作成する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックします。
2. 左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。
「パスワード・ポリシー管理」ページが表示されます。
3. 次の情報を入力します。

ロスト・パスワードのリダイレクト URL: これは、ユーザーが ID システムのロスト・パスワード管理ページに移動できる URL です。このフィールドに入力する URL は、情報目的の専用です。実際の URL は、Portal Inserts で提供されます。詳細は、7-54 ページの「[ロスト・パスワード管理](#)」を参照してください。

パスワード変更のリダイレクト URL: これは、パスワード変更フォームの URL です。詳細は、7-62 ページの「[パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成](#)」を参照してください。

パスワード期限切れ警告のリダイレクト URL: パスワード期限切れ警告フォームの URL を入力します。詳細は、7-63 ページの「[パスワード期限切れ警告のリダイレクト URL の設定](#)」を参照してください。

カスタム・アカウント・ロックアウトのリダイレクト URL: ロックアウト通知ページの URL を入力します。詳細は、7-65 ページの「[アカウント・ロックアウトのリダイレクト URL の設定](#)」を参照してください。

4. 次のように認証試行のロギングを設定します。

試行成功属性: デフォルトでは、この値は `oblastSuccessfulLogin` です。これは推奨値です。この値を変更するには、`Person` オブジェクト・クラスの文字列属性を入力するか、`Person` オブジェクト・クラスに関連付けられている補助クラスの文字列属性を入力します。

試行失敗属性: デフォルトでは、この値は `oblastFailedLogin` です。これは推奨値です。この値を変更するには、`Person` オブジェクト・クラスの文字列属性を入力するか、`Person` オブジェクト・クラスに関連付けられている補助クラスの文字列属性を入力します。

5. 「有効化」をクリックしてロギング機能を有効化します。
6. 「保存」をクリックします。

特定ドメイン用のパスワード・ポリシーの作成

特定ドメイン用のパスワード・ポリシーを構成できます。グローバル・デフォルト設定は、これらの設定により上書きされます。

特定ポリシー用のロスト・パスワード管理ページおよびパスワード変更ページのスタイルシートを構成することもできます。 `lpm_cr.xml` および `lpm_changepwd.xml` という ID システムのスタイルシートを元のスタイルシートとして使用できます。これらのスタイルシートをコピーしてカスタマイズします。スタイルシートの詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

これらのスタイルシートのデフォルトの格納場所は、`IdentityServer_install_dir/identity/oblix/lang/language_id/style0` です。ここで、`IdentityServer_install_dir` は Identity Server がインストールされているディレクトリであり、`language_id` は使用している言語パックが存在するディレクトリです。デフォルトの言語パックは、`en-us` です。

次の手順でページ下部の「デフォルト」ボタンを使用すると、「パスワード・ポリシー名」、「パスワード・ポリシー・ドメイン」および「パスワード・ポリシー・フィルタ」フィールド以外のすべてのフィールドに値が移入されます。

パスワード・ポリシーを作成する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。次に、「パスワード・ポリシー管理」ページの「追加」をクリックします。
2. 「パスワード・ポリシー名」フィールドに、ポリシーの名前を入力します。
3. 「パスワード・ポリシー・ドメイン」フィールドに、このポリシーを適用する LDAP ディレクトリのドメインを入力します。たとえば、次のようになります。
`ou=corporate,o=company,c=us`
4. オプションで、「パスワード・ポリシー・フィルタ」フィールドに LDAP フィルタを追加して、このパスワード・ポリシーを適用するドメインの一部をより詳細に定義できます。
たとえば、`(title=System Administrator)` と指定すると、このパスワード・ポリシーの適用先が一部のユーザーに制限されます。
5. 「ロスト・パスワード・ポリシー」リストで、実施するロスト・パスワード・ポリシーの名前を選択します。
詳細は、7-54 ページの「ロスト・パスワード管理」を参照してください。このフィールドを空白のままにすると、単一のチャレンジ・レスポンス・モデルが使用されます。
6. 「パスワードの最小長」フィールドに、パスワードに含める必要のある文字の最小数を入力します。
デフォルトは 8 です。
7. 「大文字の最小数」フィールドに、パスワードに含める必要のある大文字の最小数を入力します。
デフォルトは 2 です。
8. 「小文字の最小数」フィールドに、パスワードに含める必要のある小文字の最小数を入力します。
デフォルトは 2 です。
9. 「非英数字文字の最小数」フィールドに、パスワードに含める必要のある非英数字の最小数を入力します。
非英数字は、英字または数字以外の出力可能な任意の文字です。たとえば、+、!、@ などです。
デフォルトは 1 です。
10. 「数値文字の最小数」フィールドに、パスワードに含める必要のある数字の最小数を入力します。
11. このパスワード・ポリシーに外部ルールを適用する場合、「外部的に指定された検証ルール」を選択します。
Oracle Access Manager では、パスワード・ポリシー実施用の外部フックを提供していません。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。
12. 「パスワード有効期間」フィールドで、次のいずれかのオプションを選択します。
 - パスワードの有効期限なし。
 - パスワードが期限切れになるまでの日数: このパスワードを有効とする日数を入力します。デフォルトはありません。このオプションを選択する場合、値を指定する必要があります。
13. 「パスワード期限切れ通知期間」に、パスワード期限切れを何日前にユーザーに通知するかを指定します。

14. 「期限切れ通知の伝達モード」フィールドで、次のオプションの一方または両方を選択します。
- ログイン時: ユーザーがログインすると、パスワードが期限切れになるまでの残り日数を示すメッセージが表示されます。
ID システムがアクセス・システムにより保護されている場合、パスワード期限切れ警告のリダイレクト URL を入力する必要があります。詳細は、7-63 ページの「[パスワード期限切れ警告のリダイレクト URL の設定](#)」を参照してください。
 - 電子メール: ユーザーは、パスワードが期限切れになるまでの残り日数を電子メールで通知されます。メッセージはカスタマイズできません。
15. 「パスワードの最小期間」フィールドに、変更前にパスワードを使用し続ける必要のある日数を入力します。
16. 管理者によるパスワードのリセット後、ユーザーが最初にシステムにログインしたときにパスワードの変更を強制する場合は、「リセット時に変更」を選択します。
デフォルトでは、「リセット時に変更」フラグは設定されません。自己登録時にも「リセット時に変更」フラグは設定されません。
このフィールドは、ID システムとアクセス・システムの両方に適用されます。アクセス・システム専用の場合、パスワード変更のためのリダイレクト URL も構成できます。詳細は、7-61 ページの「[パスワードのリダイレクト URL の構成](#)」を参照してください。
17. 「パスワード履歴」フィールドに、パスワード履歴を維持するかどうかを指定します。
「パスワード履歴を保存しない」を選択するか、ユーザーごとに保存するパスワード数を入力します。保存されたパスワードはディレクトリに格納され、再利用はできません。デフォルトは5です。
Oracle Access Manager では、ディレクトリに保存されている最新のパスワードを判別できます。パスワードを削除する場合、Oracle Access Manager により、残っているうちで最も古いパスワードが特定されます。
18. 「最大ログイン試行回数」フィールドに、ユーザーのアカウントをロックするまでに許可するログイン試行回数を指定します。
デフォルト値は3です。この場合、ユーザーが不適切なログイン資格証明を使用して3回ログインを試みると、「ロックアウト継続時間」の値により指定されているロックアウト期間内に3回目のログイン試行が発生した後、ユーザーはロックアウトされます。不適切なログイン資格証明は、適切なユーザー名と不適切なパスワードで構成されます。ロックアウト期間中、ユーザーは適切な資格証明を入力してもログインできません。
-
- 注意:** この設定は、ロスト・パスワード管理におけるチャレンジ・レスポンスの試行回数にも適用されます。
-
19. 「ロックアウト継続時間」フィールドに、ユーザーによるログインの失敗回数が前の手順で指定された回数を超えた後にアカウントをロックし続ける時間数を指定します。
デフォルトは24時間です。ロックアウト継続時間の期限前にロックアウトを解除する場合、管理者はIDシステムでユーザー・パスワードをリセットできます。管理者がパスワードをリセットする前に「パスワード・ポリシー管理」ページで「リセット時に変更」が選択されていた場合、ユーザーは、ログイン時に新パスワードを選択できるページにリダイレクトされます。
管理者が新パスワードを割り当てた時点で「リセット時に変更」が選択されていなかった場合、ユーザーは、管理者に割り当てられたパスワードでシステムにログインできます。
20. 「ログイン試行のリセット」フィールドに、ログインの成功によって中断せずにログイン試行の失敗を格納する日数を指定します。
たとえば、この値を3に設定した場合、ユーザーがログインに1回失敗すると、アプリケーションではその失敗を3日間維持した後に消去します。

21. オプションで、「ロスト・パスワードのリダイレクト・スタイルシート」に XSL スタイルシートへのパスを入力できます。

スタイルシート構成の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。詳細は、7-54 ページの「[ロスト・パスワード管理](#)」を参照してください。
22. オプションで、「パスワード変更のリダイレクト・スタイルシート」に XSL スタイルシートへのパスを入力できます。

スタイルシート構成の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。パスワード変更フォームの詳細は、7-62 ページの「[パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成](#)」を参照してください。
23. オプションで、「パスワード期限切れ警告のリダイレクト URL」にデフォルト設定を上書きする URL を指定できます。

この設定は、アクセス・システムにのみ適用されます。この URL の詳細は、7-63 ページの「[パスワード期限切れ警告のリダイレクト URL の設定](#)」を参照してください。
24. 「カスタム・アカウント・ロックアウトのリダイレクト URL」に、ログイン試行回数を越えたユーザー用のリダイレクト URL を指定します。

この設定は、アクセス・システムにのみ適用されます。詳細は、7-65 ページの「[アカウント・ロックアウトのリダイレクト URL の設定](#)」を参照してください。
25. 「パスワード・ポリシー有効化」を選択してこのパスワード・ポリシーを有効化します。

後でこのフィールドの設定を変更した場合、またはこのパスワード・ポリシーになんらかの変更を加えた場合、パスワード・ポリシー・キャッシュをフラッシュする必要があります。パスワード・ポリシー・キャッシュは、アクセス・システム・コンソールでフラッシュできます。アクセス・システム・コンソールで、「共通情報の構成」をクリックし、次に「パスワード・ポリシー・キャッシュのフラッシュ」タブをクリックします。詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。
26. 「保存」をクリックしてこのポリシーを保存し、「パスワード・ポリシー管理」ページに戻ります。

ページのリストに新規ポリシーが表示されます。

注意： このページに表示される各リダイレクト URL は、アクセス・システムに適用されます。詳細は、7-61 ページの「[アクセス・システムでのパスワード・ポリシーの実施](#)」を参照してください。

パスワード・ポリシーの変更

この操作で「デフォルト」ボタンをクリックすると、「パスワード・ポリシー名」、「パスワード・ポリシー・ドメイン」および「パスワード・ポリシー・フィルタ」以外のすべてのフィールドにデフォルト値が移入されます。各パラメータの詳細は、7-48 ページの「[パスワード・ポリシーの評価順序](#)」を参照してください。

パスワード・ポリシーのパラメータを変更する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。

「パスワード・ポリシー管理」ページにパスワード・ポリシーのリストが表示されます。
2. 「パスワード・ポリシー管理」ページで、変更するポリシーをクリックします。

ポリシーのパラメータを含むページが表示されます。
3. 必要に応じてパラメータを変更します。
4. 「保存」をクリックします。

パスワード・ポリシーの削除

「パスワード・ポリシー管理」ページにパスワード・ポリシーのリストが表示されます。パスワードを保存すると、LDAP ディレクトリに格納されます。Oracle Access Manager では、最新のパスワードを判別できます。パスワードを削除する場合、Oracle Access Manager により最も古いパスワードが特定されます。

パスワード・ポリシーを削除する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。
2. 「パスワード・ポリシー管理」ページで、削除するポリシーの横のチェック・ボックスを選択します。
3. 「削除」をクリックします。
4. 削除を確認するプロンプトが表示されたら、「OK」をクリックします。

ロスト・パスワード管理

ロスト・パスワード管理により、ユーザーは、自分のパスワードを忘れた場合にパスワードをリセットできます。ロスト・パスワード管理は、次の要素で構成されるプロセスです。

- チャレンジ・フレーズに回答できるページにユーザーを移動する、Lost Password というリンク。

ロスト・パスワード管理を実装するには、ロスト・パスワード管理ページの URL を作成し、そのリンクを Web ページに配置してユーザーがロスト・パスワード管理機能にアクセスできるようにします。これらの URL は、Portal Inserts と呼ばれます。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

- チャレンジ・フレーズおよびレスポンスのフィールドを含むロスト・パスワード管理ページ。
ロスト・パスワード管理 URL により、ユーザーは、1 つ以上のチャレンジ質問を含む ID システム・ページにルーティングされます。
- ユーザーがチャレンジに正しく回答した場合に表示されるパスワード・リセット・ページ。
正しいレスポンスを入力すると、ユーザーは、ID システムで新パスワードを設定できます。
- ユーザーを当初リクエストされたページにリダイレクトできる追加機能。

パスワード・ポリシーのロスト・パスワード管理 URL は、記録保持のために ID システム・コンソールで記録します。特定のドメイン用のロスト・パスワード管理ポリシーを構成できます。

ID システムでは、RSA のライセンスに基づく暗号化スキームによりレスポンス値が暗号化されます。この暗号化スキームは、Secure Hash Algorithm (SHA) とは異なります。デフォルトの暗号化機能を独自の機能で置き換えるには、ID イベント・プラグイン API を使用してカスタム・アクションを記述します。これは、ID システムにインポートできる既存のチャレンジ属性とレスポンス属性が存在する場合に便利です。詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

ロスト・パスワード管理は、デフォルトで有効化されます。

注意： ID システムで入力する他のリダイレクト URL とは異なり、ロスト・パスワード管理のリダイレクト URL は、情報目的専用で入力します。その主な場所は、Portal Inserts です。

タスクの概要: ロスト・パスワード管理の実装

1. ディレクトリに2つの新規属性を作成します。1つの属性はユーザーに表示するチャレンジ用として使用し、もう1つの属性はユーザーがチャレンジに回答するレスポンス用として使用します。

ロスト・パスワード管理をサポートするため、ユーザーに表示するチャレンジの値とそれらのチャレンジに対するレスポンスの値を格納する属性のペアを定義します。たとえば、「チャレンジ」および「レスポンス」という属性のペアを定義します。ID システム・コンソールで、これらの属性に「チャレンジ」および「レスポンス」セマンティック型を割り当てます。詳細は、7-57 ページの「[ディレクトリでチャレンジ・タイプおよびレスポンス・タイプの属性を構成する手順](#)」を参照してください。
2. ID システム・コンソールで、Person オブジェクト・クラスの属性を変更します。

チャレンジ・フレーズを格納する属性と、そのチャレンジ・フレーズに対するユーザーのレスポンスを格納する属性を構成します。

詳細は、7-58 ページの「[ロスト・パスワード管理属性を構成する手順](#)」を参照してください。
3. User Manager で、これらの属性の属性アクセス制御を構成します。

プロフィール・ページのチャレンジとレスポンスを表示および変更する場合、ユーザーは、チャレンジとレスポンスに対する読取り権限と変更権限を保持する必要があります。詳細は、4-21 ページの「[ユーザーによる LDAP データの表示および変更の許可](#)」を参照してください。
4. ユーザーがプロフィール・ページを参照または変更するときに表示されるように、ユーザー・プロフィール・ページにチャレンジ属性とレスポンス属性を追加します。

ロスト・パスワード管理で、ユーザーはチャレンジ・フレーズを含むページに移動されます。チャレンジ・フレーズおよびレスポンスの入力フィールドを含むページは、User Manager で構成するプロフィール・ページです。詳細は、4-11 ページの「[タブのプロファイル・ページおよびパネルの構成](#)」を参照してください。ユーザーは、関連する属性に独自の読取りまたは書込み権限がない場合でも、ログイン中にチャレンジを構成できることに注意してください。
5. ワークフロー・ステップ・ページを構成してこれらの属性を使用します。

チャレンジ・フレーズとレスポンスは、後でパスワード取得に使用できるように、自己登録の実行中に構成する必要があります。あまり一般的ではありませんが、ユーザーの作成ワークフローを使用して、ワークフローの参加者に新規ユーザー用のチャレンジ・フレーズを構成させることも可能です。詳細は、[第5章「ID 機能とワークフローの連携」](#)を参照してください。ワークフロー・ステップ・ページでは、チャレンジ・パラメータに対する読取りまたは書込み権限は必要ありません。
6. ID システム・コンソールでロスト・パスワード管理ポリシーを構成します。

詳細は、7-48 ページの「[パスワード・ポリシーの管理](#)」を参照してください。
7. ロスト・パスワード管理 URL をサード・パーティ・アプリケーションまたはポータル・ページに挿入します。

詳細は、この項の情報を参照してください。Portal Inserts の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

ロスト・パスワード管理 URL の構文

ロスト・パスワード管理 URL の形式は、次のとおりです。

```
http://machinename:portnumber/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?program=passwordChallengeResponse&login=%scheme1_uid_parameter_value%&target=top
```

この URL は、7-62 ページの「パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成」で説明しているパスワード期限切れリセットの URL と似ています。2つの URL タイプの違いの1つは、次のパラメータ部分です。

```
program=passwordChallengeResponse
```

もう1つの違いは、この URL にユーザー ID などの変数を指定する場合、対応する cgi スクリプトを変更してユーザーのログイン ID を渡す必要があることです。または、次の URL 構文を使用して、ロスト・パスワード・リセット・ページへのリダイレクト後にユーザーにユーザー ID を再入力させる必要があります。

```
http://machinename:portnumber/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?program=passwordChallengeResponse&target=top
```

前述の URL の lost_pwd_mgmt.cgi は、Oracle Access Manager に付属しています。

ユーザーへのチャレンジ・フレーズの表示

ロスト・パスワード管理は、単一または複数のチャレンジ・レスポンス・システムとして構成できます。チャレンジとレスポンスのペアは、次の場所に表示されます。

- ユーザー・アカウントの作成ワークフローでは、ワークフロー・ステップにチャレンジ属性とレスポンス属性のエントリが含まれます。
- 「プロファイルの表示」および「プロファイルの変更」ページには、チャレンジとレスポンスのペアが表示されます。
- ロスト・パスワード管理では、ユーザーは1つ以上のチャレンジ・フレーズに回答する必要があります。
- 構成済のチャレンジの数が、ユーザーに適用されるロスト・パスワード・ポリシーで必要とされる数より少ない場合、ユーザーは、Oracle Access Manager へのログイン時に追加のチャレンジを指定するよう求められます。

チャレンジおよびレスポンス・ページのその他の要素

ロスト・パスワード管理ページにチャレンジとレスポンスのプロンプトを指定する以外に、このページに追加の情報を指定できます。たとえば、ロスト・パスワード管理のチャレンジに正しく回答したユーザーをパスワード・リセット・ページに移動するリンク（またはワークフロー・ステップ）を構成できます。

ロスト・パスワード管理でユーザーに複数のチャレンジが表示される場合

ロスト・パスワード管理ポリシーがユーザーに適用される場合、ユーザーがロスト・パスワード管理 URL をクリックすると、複数のチャレンジおよびレスポンス・フィールドが表示されます。ユーザーに表示されるチャレンジの数は、「回答する最小チャレンジ」フィールドにより決定されます。詳細は、7-59 ページの「パスワード・ポリシー・ドメインのロスト・パスワード管理を構成する手順」を参照してください。

7-50 ページの「特定ドメイン用のパスワード・ポリシーの作成」に記載されているとおり、パスワード・ポリシーは、特定のドメインまたはユーザー・グループに適用されます。ユーザーにロスト・パスワード・ポリシーが適用されない場合、1つのチャレンジ・フレーズおよび1つのレスポンスの入力フィールドのみが表示されます。複数のチャレンジとレスポンスを構成していても、ロスト・パスワード・ポリシーがユーザーに適用されなければ、最初に構成されたチャレンジ・フレーズとレスポンスが表示されます。

構成済のチャレンジ・フレーズとレスポンスの数が、ロスト・パスワード・ポリシーに構成されている最小数未満の場合、ユーザーは、ログイン時に追加のチャレンジ・フレーズを構成するよう求められます。例として、最初のロスト・パスワード管理ポリシーの設定後に、チャレ

ンジの最小数を増加するよう構成した場合を検査します。この場合、ユーザーがログインすると、次のいずれかの形式で追加のチャレンジ・フレーズが表示されます。

- テキスト・ボックス: ロスト・パスワード管理ポリシーで「ユーザー」設定を選択した場合に表示されます。
- 事前定義されたフレーズを含む選択ボックス: ロスト・パスワード管理ポリシーで「事前定義」設定を選択した場合に表示されます。
- 事前定義されたフレーズを含むコンボ・ボックス: ロスト・パスワード管理ポリシーで「ユーザーまたは事前定義」設定を選択した場合に表示されます。

詳細は、7-59 ページの「パスワード・ポリシー・ドメインのロスト・パスワード管理を構成する手順」を参照してください。

ロスト・パスワード管理ポリシーでソース・タイプを変更した場合（たとえば、ソースを「ユーザー」から「事前定義」に変更した場合）、最小長を変更した場合、または「重複レスポンスを許可」フラグを変更した場合、それらの変更はユーザーが自分のプロフィールを変更するときに適用されます。

追加のチャレンジの構成を求めるプロンプトでユーザーに表示されるメッセージのタイプは、ロスト・パスワード管理ポリシーで変更された設定に応じて変化します。たとえば、レスポンスの最小長を 3 文字から 8 文字に変更したとします。ユーザーが自分のプロフィールの変更を保存しようとする、「レスポンスが最小長の要件を満たしていません」というエラー・メッセージが表示されます。ポリシーでチャレンジの最小数を増やした場合、ユーザーは、ログイン時に必要な情報を指定するよう求められます。

ロスト・パスワード管理ポリシーの表示と構成

次の手順では、ロスト・パスワード管理を構成する方法について説明します。

注意: ロスト・パスワード管理ポリシーが有効である場合、プロフィール・ページやワークフロー・ページからチャレンジ・パラメータを削除することはできません。

ディレクトリでチャレンジ・タイプおよびレスポンス・タイプの属性を構成する手順

1. ユーザーのチャレンジおよびレスポンスに使用する未使用で空の属性を 2 つディレクトリに用意します。

2 つの適切な属性を使用できる場合、次の手順に進みます。

2. 新規属性を追加する必要がある場合、任意の方法を使用して属性を追加できます。

次に、新規補助オブジェクト・クラスと 2 つの新規属性を含む LDIF スキーマ・ファイルを作成する場合の例を示します。現在のディレクトリ・サーバー・タイプに適した構文を使用して、次のような属性を作成できます。

```
# ----- Attributes -----
#
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.9999.1.1094.204 NAME 'Challenge2' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 )

dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( 1.3.6.1.4.1.9999.1.1094.205 NAME 'Response2' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 )

# ----- Object class -----
#
dn: cn=schema
```

```
changetype: modify
add: objectclasses
objectclasses: ( 1.3.6.1.4.1.9999.1.1094.206 NAME 'oblixAuxPerson4LPM' DESC 'User
defined objectclass' SUP top AUXILIARY MAY ( Challenge2 $ Response2 ) )
```

3. LDIF ファイルをディレクトリにインポートします。
4. Oracle Access Manager で新規補助オブジェクト・クラスを構成するため、ID システム・コンソールで「共通構成」をクリックします。
5. 左側のナビゲーション・ペインの「オブジェクト・クラス」をクリックします。
6. 「追加」をクリックします。
7. リストから新規オブジェクト・クラスの名前を選択します。
8. Person 構造化オブジェクト・クラスのオプション・ボタンを選択します。

これで、新規補助オブジェクト・クラスが Person 構造化オブジェクト・クラスに関連付けられました。このオブジェクト・クラスでチャレンジ・タイプとレスポンス・タイプの新規属性を構成できます (7-58 ページの「ロスト・パスワード管理属性を構成する手順」を参照してください)。

ロスト・パスワード管理属性を構成する手順

1. Person オブジェクト・クラスの属性を構成してチャレンジ・フレーズを格納するには、ID システム・コンソールで「共通構成」をクリックします。
2. 左側のナビゲーション・ペインの「オブジェクト・クラス」をクリックします。
3. Person オブジェクト・クラスのリンクをクリックします。
4. 「属性の変更」をクリックします。
5. 「属性」リストで、チャレンジ・フレーズに使用する属性を選択します。

これは、空の新規属性である必要があります。

6. 次のように構成します。

詳細は、3-11 ページの「オブジェクト・クラス属性の概要」および 3-19 ページの「属性の構成」を参照してください。

- この属性のセマンティック型を「チャレンジ」に設定します。
- データ型を大 / 小文字を区別する文字列に設定します。
- 「属性値」フィールドを「単一」に設定します。
- 表示タイプは、構成するポリシーのタイプに応じて自動的に構成されます。
- 「チャレンジ」などの適切な表示名を割り当てます。

複数のチャレンジ・フレーズを構成する場合、それらのフレーズは、チャレンジ属性用のユーザー・ディレクトリ・エントリに単一値として格納されます。各値は、エンコードされた形式で格納されます。

7. 「属性」リストで、チャレンジ・フレーズに対するユーザーのレスポンスを格納する Person オブジェクト・クラスの 2 番目の属性を選択します。

これは、空の新規属性である必要があります。

8. この属性を次のように構成します。

- この属性のセマンティック型を「レスポンス」に設定します。
- データ型を大 / 小文字を区別する文字列に設定します。
- 表示タイプを「パスワード」に設定します。
- 「属性値」フィールドを「単一」に設定します。
- 「レスポンス」などの適切な表示名を割り当てます。

詳細は、3-11 ページの「オブジェクト・クラス属性の概要」および 3-19 ページの「属性の構成」を参照してください。

ロスト・パスワード管理ポリシーの一部として複数のチャレンジおよびレスポンスを構成する場合、ユーザーがレスポンスに指定した値は、レスポンス属性用のユーザー・ディレクトリ・エントリに単一値として格納されます。各値は、エンコードおよび暗号化された形式で格納されます。

- 表示する場所に応じて、これらの属性をユーザー・プロファイル・ページまたはワークフロー・ステップ・パネルに追加します。

ロスト・パスワード・ポリシーを表示する手順

- ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「ロスト・パスワード・ポリシー」をクリックします。
- 「ロスト・パスワード・ポリシー管理」ページで、表示するポリシーのリンクをクリックします。

ロスト・パスワード管理を有効化または無効化する手順

- oblixbaseparams.xml ファイルの場所を見つけます。
このファイルのデフォルト・パスは、次のとおりです。
`IdentityInstall_dir/identity/oblix/apps/common/bin/oblixbaseparams.xml`
ここで、`IdentityInstall_dir` は、ID システムがインストールされているディレクトリです。
- Apply_LostPwdMgmt パラメータに Yes が入力されていることを確認します。
デフォルトは Yes です。No を入力すると、この機能を無効化できます。
- ファイルを保存して閉じます。

パスワード・ポリシー・ドメインのロスト・パスワード管理を構成する手順

- ID システム・コンソールで、「システム構成」サブタブをクリックし、次に「ロスト・パスワード・ポリシー」をクリックします。
- 「ロスト・パスワード・ポリシー」ページで、「追加」をクリックします。
「ロスト・パスワード・ポリシーの追加」ページが表示されます。
- 「ロスト・パスワード・ポリシー名」フィールドに名前を入力します。
- 「チャレンジ・フレーズ・ソース」で、チャレンジ・フレーズの提供元を次のように選択します。
 - ユーザー**: アカウントの作成時に、ユーザーがチャレンジ・フレーズを指定する必要があります。
 - 事前定義**: ユーザー・アカウントの作成時に、事前定義されたチャレンジのリストがユーザーに表示されます。ユーザーは、指定されたチャレンジ・フレーズの中から選択する必要があります。
 - ユーザーまたは事前定義**: ユーザー・アカウントの作成時に、事前定義されたフレーズのリストがユーザーに表示されます。ユーザーは、指定されたチャレンジ・フレーズの中から選択するか、新規チャレンジ・フレーズを指定することが可能です。
- 「事前定義済チャレンジ・フレーズ」フィールドに、チャレンジ・フレーズを入力して「追加」をクリックします。
フレーズが選択リストに追加されます。選択されたフレーズをリストから削除するには、「削除」ボタンを使用します。
このロスト・パスワード・ポリシー定義の完了後、いつでも事前定義済チャレンジ・フレーズを追加することや、既存のフレーズを削除することができます。
- 「構成する最小チャレンジ」フィールドに、ユーザー・アカウントの作成時またはユーザー・プロファイルの変更時に構成する必要があるチャレンジの数を入力します。

7. 「チャレンジ・レスポンスの最小長」フィールドに、ユーザーが構成するレスポンスに許可する最小文字数を入力します。
8. 「重複レスポンスを許可」チェック・ボックスを次のように構成します。
 - 選択解除: False。ユーザーが複数のチャレンジ・フレーズに対して同じレスポンスを入力すると、エラーが表示されます。
 - 選択: True。重複チェックは無効になります。
9. 「回答する最小チャレンジ」フィールドに、ロスト・パスワード管理アプリケーションを使用してパスワードをリセットしたときに、ユーザーに回答させるチャレンジの数を入力します。

この値は、「構成する最小チャレンジ」フィールドの値以下である必要があります。たとえば、このフィールドの値を3に設定し、チャレンジとレスポンスのペアを4つ構成した場合、ユーザーが回答する必要があるチャレンジの数は3つです。ユーザーが入力する必要のある実際のレスポンスの数は、このフィールドの値に加え、正しく構成されたチャレンジとレスポンスの数に応じて変化することに注意してください。たとえば、このフィールドに2を入力しても、2つのチャレンジとレスポンスのペアのうち1つのみが正しく構成されている場合、ユーザーは1つのチャレンジにのみ回答するよう求められます。
10. 「チャレンジ・ポーズ・タイプ」フィールドで、チャレンジを一度にすべて表示するか、順番に表示するかを選択します。
 - 同時: チャレンジは一度に表示されます。チャレンジの表示順序は、毎回変化します。ユーザーは、すべてのチャレンジに正しく回答する必要があります。
 - 順番に: ユーザーが1つのチャレンジ・フレーズに回答するまで、次のフレーズは表示されません。
11. パスワードのリセット後にユーザーに電子メールを送信する場合、「パスワード変更後に電子メール送信」ボックスを選択します。

ユーザーに電子メールを送信するよう設定すると、ユーザーは、侵入者がパスワードをリセットしたときに予期しない事態が発生したことに気付くため、管理者に連絡を取ることができます。
12. 管理者がこのポリシーを使用できるようにする場合、「ロスト・パスワード・ポリシー有効化」ボックスを選択します。
13. 「保存」をクリックします。
14. このポリシーの名前をパスワード・ポリシー・ドメインに追加します。

詳細は、7-50 ページの「[特定ドメイン用のパスワード・ポリシーの作成](#)」を参照してください。

アクセス・システムでのパスワード・ポリシーの実施

ID システム・コンソールで構成したパスワード・ポリシーを、アクセス・システムにより保護されているリソースに適用できます。これを行うには、各リソースを保護する認証スキームを変更します。ユーザーがアクセス・システムにより保護されたリソースに対する認証を受ける場合、それらのユーザーがパスワード・ポリシー・ドメインに存在すると、パスワード・ポリシーが起動されます。

この項には、次の各項目が含まれます。

- [認証スキームを変更してパスワード・ポリシーを含める方法](#)

詳細は、7-48 ページの「[パスワード・ポリシーの評価順序](#)」を参照してください。認証スキームの作成方法の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

認証スキームを変更してパスワード・ポリシーを含める方法

次の手順では、認証スキームを変更してパスワード・ポリシーを含める方法について説明します。

認証スキームを変更してパスワード・ポリシーを含める手順

1. アクセス・システムにログインします。
2. アクセス・システム・コンソールで、「アクセス・システム構成」をクリックし、次に左側のナビゲーション・ペインの「認証管理」をクリックします。
構成済のすべての認証スキームがリストされた「認証管理」ページが表示されます。
3. 変更する認証スキームのリンクをクリックし、表示されたページの「変更」ボタンをクリックします。
「認証スキームの変更」が表示されます。
4. `validate_password` プラグインを選択し、次の情報を「プラグイン・パラメータ」フィールドに追加して「保存」をクリックします。

```
obReadPasswdMode="LDAP",obWritePasswdMode="LDAP"
```


たとえば、Basic Over LDAP スキームの元の `validate_password` プラグイン・パラメータ文が次のように設定されているとします。

```
obCredentialPassword="password"
```


新規パラメータは、次のように設定されます。

```
obCredentialPassword="password",obReadPasswdMode="LDAP", obWritePasswdMode="LDAP".
```


新規パラメータは、パスワード変更のリダイレクト用として追加する必要があります。
5. `credential_mapping` プラグインの `uid` パラメータ値を書き留めます。
この値は、パスワード変更のリダイレクト URL を作成する際に必要です。たとえば、`uid` パラメータ値は `%userid%` になります。
6. パスワード変更のリダイレクトを設定するすべての認証スキームでこのプロセスを繰り返します。

注意：パスワード・ポリシーになんらかの変更を加えた場合、必ず Access Server キャッシュをフラッシュしてください。詳細は、7-65 ページの「[Access Server キャッシュの更新](#)」を参照してください。

パスワードのリダイレクト URL の構成

次のページにユーザーをリダイレクトする URL を構成できます。

- [パスワード・リセット・ページ](#)

- パスワード期限切れ警告ページ
- ユーザー・アカウントがロックされていることを示すエラー・ページ

これらのリダイレクト URL は、WebGate または AccessGate により保護されているリソースにユーザーがログインした場合にのみ適用されます。つまり、『Oracle Access Manager Access System Administration Guide』の記載に従ってリソースを保護している場合に、これらの URL のいずれかを構成できます。ユーザーがリダイレクト URL に指定されたターゲット・ページでの操作を完了したときに、当初リクエストされたリソースにユーザーを戻すようこれらの URL を構成することも可能です。

これらの URL の詳細は、次の各項目を参照してください。

- [パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成](#)
- [パスワード期限切れ警告のリダイレクト URL の設定](#)
- [アカウント・ロックアウトのリダイレクト URL の設定](#)

パスワード期限切れ後にパスワード・リセット・ページにリダイレクトするための構成

パスワード・ポリシーに構成されているパスワードの有効期限が経過した後に、ユーザーがログインを試みると、そのユーザーは自動的にパスワード・リセット・ページにリダイレクトされます。このパスワード・リセット・ページの URL を構成できます。オプションで、このパスワード・リセット URL により、パスワードのリセット後にユーザーを当初リクエストされたリソースにリダイレクトできます。

パスワード変更のリダイレクト URL を入力する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。
「パスワード・ポリシー管理」ページにパスワード・ポリシーのリストが表示されます。
2. 「パスワード変更のリダイレクト URL」フィールドに、次の構文を使用して URL を入力します。

```
http://machinename:portnumber/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?program=redirectforchangepwd&login=%scheme1_uid_parameter_value%
%scheme2_uid_parameter_value%%schemeN_uid_parameter_value% &target=top
```

この場合：

- *machinename:portnumber* は、WebPass がインストールされている Web サーバーのホストとポートです。
- *%scheme1_uid_parameter_value%%scheme2_uid_parameter_value%%schemeN_uid_parameter_value%* は、パスワード変更のリダイレクトを設定するすべての認証スキームに対応する uid パラメータ値の文字列です。

たとえば、2つの認証スキームに次の credential_mapping プラグイン・パラメータが含まれるとします。

- **Form over LDAP:** obMappingBase="o=company,c=us",
obMappingFilter="(&(objectclass=genSiteOrgPerson)
(uid=%login%))"
- **Basic over LDAP:** obMappingBase="o=company,c=us",
obMappingFilter="(&(objectclass=genSiteOrgPerson)
(uid=%userid%))"

これらのパラメータに対応するパスワード変更のリダイレクト URL は、次のとおりです。

```
http://machinename:portnumber/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?program=redirectforchangepwd&login=%login%&userid%&target=top
```

3. パスワード変更フォームの送信後にユーザーを当初リクエストされたリソースに戻す場合、この URL の問合せ文字列に BackURL 文を記述できます。基本構文は次のとおりです。

```
http://machinename:portnumber/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?prtforchangepwd&login=%login%userid%&backURL=%HostTarget%RESOURCE% &target=top
```

たとえば、次のようになります。

```
http://130.35.46.141:99/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?login=%login%userid%&backUrl=%HostTarget%RESOURCE%
```

実行時に、% デリミタで囲まれた値が、当初リクエストされたリソースの URL で置き換えられます。たとえば、次のようになります。

```
http://130.35.46.141:99/identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi?login=admin&backUrl=http://www.webserver1.com/test/a.html
```

lost_pwd_mgmt.cgi スクリプトには、問合せパラメータを処理するロジックが含まれます。lost_pwd_mgmt.cgi スクリプトは、Oracle Access Manager に付属しています。ページは動的に生成されるため、手動による構成は必要ありません。

4. 「保存」をクリックします。

パスワード期限切れ警告のリダイレクト URL の設定

パスワードの有効期間は、パスワード・ポリシーで構成します。ユーザー・パスワードの期限切れが近づくと、ユーザーは、リダイレクト URL により警告ページに移動されます。Oracle Access Manager では、この警告ページを提供していません。警告を含む実際のランディング・ページを作成する必要があります。オプションで、この警告ページに、ユーザーをパスワード・リセット・ページに移動する URL を含めることもできます。

パスワード期限切れのリダイレクト URL は、アクセス・システムにより保護されているリソースにのみ適用されます。つまり、WebGate でリソースを保護している場合に、この URL を構成できます。

パスワード期限切れの URL は、パスワード変更のリダイレクト URL と似ています。この URL により、ユーザーを期限切れ通知フォームに移動できます。オプションで、ユーザーをパスワード変更フォームにリダイレクトすることや、パスワードの変更後にユーザーを当初リクエストされたリソースに戻すことも可能です。

すべてのパスワード・ポリシーに適用されるデフォルトのパスワード期限切れ URL を構成するか、個々のポリシーに適用される URL を構成します。

自動的にユーザーをこの URL にリダイレクトするか、期限切れ前に電子メールでユーザーに通知できます。詳細は、7-50 ページの「[特定ドメイン用のパスワード・ポリシーの作成](#)」を参照してください。

この URL のターゲットとして機能する組込みのページまたはポータルはありません。適切なページを作成する必要があります。たとえば、「パスワードの期限がもうすぐ切れるため、変更する必要があります」というメッセージの表示されるページを作成できます。

デフォルトのパスワード期限切れ警告のリダイレクト URL を設定する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。

「パスワード・ポリシー管理」ページにパスワード・ポリシーのリストが表示されます。

2. 「パスワード期限切れ警告のリダイレクト URL」に、次の構文を使用して URL を入力します。

```
http://machinename:portnumber/path-to-custom-page
```

この場合：

- *machinename:portnumber* は、WebPass がインストールされている Web サーバーのホストとポートです。
- *path-to-custom-page* は、パスワードの期限切れが近いことを警告するカスタム Web ページのパスです。

3. 認証後にユーザーを当初リクエストされたリソースに戻す場合、次のようにこの URL の問合せ文字列にバック URL (backURL 文) を記述できます。

```
http://machinename:portnumber/notice.cgi?prtforchangepwd&login=%login%&userid%&backUrl=%HostTarget%RESOURCE%&target=top
```

たとえば、次の URL を入力できます。

```
http://130.35.46.141:99/cgi-bin/notice.cgi?login=%login%&userid%&backUrl=%HostTarget%RESOURCE%
```

この例では、`notice.cgi` に問合せパラメータを処理するロジックが含まれます。簡単な Web ページを作成するか、または `cgi` などのスクリプトや JSP ページを記述して URL のパラメータ解析と適切なメッセージの表示、タイムアウトの処理、およびユーザーの backURL へのリダイレクトを行うことが可能です。

実行時に、問合せ文字列は、ユーザーおよび当初リクエストされたリソースの実際の値で置き換えられます。たとえば、次のようになります。

```
http://130.35.46.141:99/cgi-bin/notice.cgi?login=admin&backUrl=http://www.webserver1.com/test/a.html
```

この例では、ユーザーが記述したスクリプトの `notice.cgi` に、問合せパラメータを処理するロジックが含まれます。

カスタム・ページでは、`ExpiryDate` 問合せパラメータを使用して有効期限日を取得することもできます。次に、このパラメータの例を示します。

```
http://130.35.46.141:99/cgi-bin/notice.cgi?ExpiryDate=%PwdExpiryDate%&backUrl=%HostTarget%RESOURCE%
```

4. 「保存」をクリックします。

アカウント・ロックアウトのリダイレクト URL の設定

他のリダイレクト URL と同様に、アカウント・ロックアウトのリダイレクト URL は、Access Server にのみ適用されます。ユーザー ID またはリクエストされたリソース情報を含まないロックアウト URL を構成できます。

アカウント・ロックアウトのリダイレクトを実装するには、Web ページを作成するか、または cgi などのスクリプトや JSP ページを記述してアカウント・ロックアウト URL のパラメータを解析する必要があります。スクリプトまたは JSP では、アカウント・ロックアウトに関するメッセージの表示、タイムアウトの処理、および当初リクエストされたリソースへのユーザーのリダイレクトを行う必要があります。

アカウント・ロックアウトの URL を設定する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「パスワード・ポリシー」をクリックします。
「パスワード・ポリシー管理」ページにパスワード・ポリシーのリストが表示されます。
2. 「カスタム・アカウント・ロックアウトのリダイレクト URL」フィールドに、ユーザーをアカウント・ロックアウト・フォームにリダイレクトする URL を入力します。
3. 「保存」をクリックします。

Access Server キャッシュの更新

ID システムで発生した変更を Access Server に通知し、アクセス・システムのキャッシュを自動的にフラッシュできます。ただし、キャッシュの自動的なフラッシュを実行しないよう選択して、ID システムの「パスワード・ポリシー管理」ページで変更操作を行った場合に手動でキャッシュをフラッシュすることが可能です。この方法は、パスワード・ポリシー管理の変更の適用に大幅な遅れが生じることを回避する場合に有効です。

Access Server キャッシュをフラッシュする方法の詳細は、『Oracle Access Manager Access System Administration Guide』および『Oracle Access Manager デプロイメント・ガイド』を参照してください。

ID システムの Access Manager SDK の構成

Access Manager SDK は、Web 以外のリソースの AccessGate を構築するためのライブラリ、構築方法およびサンプルで構成されます。Access Manager SDK は、ID システムとともに `IdentityServer_install_dir/AccessServerSDK` に自動的にインストールされます。

ID システムの次の機能には、Access Manager SDK が必要です。これらの機能のため、Access Manager SDK を手動で構成する必要があります。

- ID システムとアクセス・システム間の自動キャッシュ・フラッシュ
- 自己登録後のアクセス・システムへの自動ログイン

WebPass を WebGate で保護する場合、次の手順を実行します。前述の ID システム機能ごとにこの手順を繰り返す必要はありません。

Access Manager SDK を構成する手順

1. ID システムとアクセス・システムをインストールして設定します（『Oracle Access Manager インストール・ガイド』を参照してください）。

注意： Access Manager SDK は、ID システムとともに *IdentityServer_install_dir/AccessServerSDK* に自動的にインストールされます。

2. **Windows:** 次のように PATH システム変数を変更して、パスが Access Manager SDK を参照するように設定します。

```
set PATH = %PATH%;Identityserver_install_dir\AccessServerSDK\oblix\lib
```

3. アクセス・システム・コンソールで、「アクセス・システム構成」→「AccessGate 構成」をクリックします。

4. AccessGate を追加します。

ポートを構成する必要はありません。

ID システムでは、キャッシュをフラッシュするために AccessGate を使用して Access Server と通信します。

Access Server キャッシュをフラッシュする方法の詳細は、『Oracle Access Manager Access System Administration Guide』および『Oracle Access Manager デプロイメント・ガイド』を参照してください。

5. WebGate をアップグレードした場合、アクセス管理サービスについて「オフ」を選択します。

「オン」の値は、レガシー・システムにのみ適切です。

6. AccessGate を保存します。

7. *IdentityServer_install_dir/identity/AccessServerSDK/oblix/tools/configureAccessGate* ディレクトリにアクセスし、*configureAccessGate* スクリプトを実行します。

ここで、*IdentityServer_install_dir* は、Identity Server がインストールされているディレクトリです。

AccessGate の変更方法の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

configureAccessGate を実行する場合、AccessGate ID が、手順 3 のアクセス・システム・コンソールで入力した AccessGate 名と同じであることを確認してください。

8. *IdentityServer_install_dir/identity/oblix/data/common* ディレクトリの *basedbparams.xml* パラメータ・カタログ・ファイルをテキスト・エディタで開きます。

9. *doAccessServerFlush* フラグの値を次のように **true** に変更します。

```
<NameValPair ParamName="doAccessServerFlush" Value="true" />
```

10. Identity Server を再起動します。

コンポーネントのクローニングと同期化

コマンドラインやインストール GUI を使用して Oracle Access Manager コンポーネントをインストールするかわりに、既存のインストール済コンポーネントの構成をクローニングしてコンポーネントを自動的にインストールできます。クローニングにより、既存のインストール済コンポーネントをテンプレートとして使用し、リモート・システムにコンポーネントのコピーを作成できます。

同期化では、同じコンポーネントの 2 つのインストールについて、一方が他方より新しい場合にそれらのインストールを一致させることができます。同期化を使用すると、類似したプラットフォーム上のインストールをアップグレードまたは修復できます。

詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

第 III 部

共通管理タスクの実行

特定の機能およびタスクは、Oracle Access Manager ID システムとアクセス・システムの両方に共通です。

第 III 部では、すべての Oracle Access Manager アプリケーションに共通するタスクの実行方法を説明します。

- [第 8 章「トランスポート・セキュリティ・モードの変更」](#)
- [第 9 章「レポート」](#)
- [第 10 章「ロギング」](#)
- [第 11 章「監査」](#)
- [第 12 章「SNMP モニタリング」](#)

トランスポート・セキュリティ・モードの変更

トランスポート・セキュリティの設定はこの章の主題であり、ID システムとアクセス・システムの両方に共通の管理タスクの 1 つです。

この章の内容は次のとおりです。

- トランスポート・セキュリティ・モードについて
- ID システムのトランスポート・セキュリティの変更
- アクセス・システムのトランスポート・セキュリティ・モードの変更
- ディレクトリ・サーバーのトランスポート・セキュリティの変更
- トランスポート・セキュリティ・パスワードの変更
- 複数の CA 証明書のインポート
- Access Server のセキュリティ・パスワードの変更

トランスポート・セキュリティ・モードについて

トランスポート・セキュリティ・モードは、クライアントとサーバーなどの2つのポイント間の通信を保護する方法です。保護するために、通信を認証局（CA）で暗号化できます。

Oracle Access Manager には、『Oracle Access Manager インストレーション・ガイド』で詳細に説明しているように、コンポーネント間の通信に対して次の3つのトランスポート・セキュリティ・モードが用意されています。

- **オープン**: 通信を保護するための暗号化は行われません。このモードは、セキュリティが問題になっていない場合に使用します。たとえば、ネットワークが安全であると考えるかぎり、AccessGate と Access Server 間の通信をテストする場合に使用します。「オープン」はデフォルト設定です。
- **簡易**: 通信が Oracle Access Manager の CA で暗号化されます。簡易モードは、Transport Layer Security、RFC 2246 (TLS v1) を使用して通信を暗号化します。このモードは、証明書モードよりも安全性が低くなります。このモードは、セキュリティ上の懸念があり、独自の CA の管理を希望しない場合に使用します。
- **証明書**: 通信が外部の CA で暗号化されます。証明書モードでは、通信が TLS v1 を使用して暗号化されます。また、クライアントとサーバー両方の各要素は、接続を確立する際に X.509 証明書 (base64 形式) を提示する必要があります。証明書は、自身で、おそらくサード・パーティの CA から提供する必要があります。

注意: バージョン 7.0 の時点では、デフォルトの証明書ストアの形式および名前が cert7.db から cert8.db に変更されました。バージョン 7.0 より前のバージョンからアップグレードする場合は、引き続き古い証明書ストア (cert7.db) を使用します。

configureAAAServer、setup_ouis または setup_accessmanager ユーティリティを実行すると、証明書ストアの形式および名前が自動的に cert8.db に変更されます。バージョン 7.0 以上のバージョンは、cert7.db (アップグレードされた環境) と cert8.db (新規インストール環境) の両方の証明書ストアで動作します。Windows 以外のシステムでは、start_configureAAAServer、start_setup_ouis、start_setup_accessmanager の各ツールを使用します。

次の2つのトランスポート・セキュリティ・モードが、Oracle Access Manager コンポーネントとディレクトリ・サーバー間の通信に使用されます。

- **オープン**: ディレクトリ・サーバー通信を保護するための暗号化は行われません。このモードは、セキュリティが問題になっていない場合に使用します。たとえば、ネットワークが安全であると考えるかぎり、AccessGate と Access Server 間の通信をテストの場合に使用します。「オープン」はデフォルト設定です。
- **SSL**: ディレクトリ・サーバー通信で SSL を使用します。

トランスポート・セキュリティの指定は、インストール・プロセスの一部です。ID システムまたはアクセス・システムをインストールする際の違いは、表 8-1 を参照してください。

表 8-1 インストール時のセキュリティ・モードの指定

ID システム	アクセス・システム
<ul style="list-style-type: none"> Identity Server コンポーネントをインストールします。WebPass との通信に使用するトランスポート・セキュリティ・モードを指定します。 WebPass コンポーネントをインストールします。Identity Server との通信に使用するトランスポート・セキュリティ・モードを指定します。 	<ul style="list-style-type: none"> Policy Manager をインストールします。Access Server との通信に使用するトランスポート・セキュリティ・モードを指定します。 アクセス・システム・コンソールで Access Server インスタンスを作成します。Policy Manager との通信に使用するトランスポート・セキュリティ・モードを指定します。 アクセス・システム・コンソールで WebGate インスタンスを定義します。Access Server との通信に使用するトランスポート・セキュリティ・モードを指定します。 Access Server コンポーネントをインストールします。WebGate と通信するためのトランスポート・セキュリティ・モードを構成します。 WebGate コンポーネントをインストールします。Access Server と通信するためのトランスポート・セキュリティ・モードを構成します。

関連資料： コンポーネントのインストールの詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

コンポーネント間のトランスポート・セキュリティ・モード

トランスポート・セキュリティは、次のコンポーネント間で構成できます。

- ID システム：**すべての Identity Server と WebPass インスタンス間のトランスポート・セキュリティが一致している必要があります。つまり、すべてオープン・モード、すべて簡易モード、またはすべて証明書モードのいずれかである必要があります。
- アクセス・システム：**すべての Policy Manager、Access Server および関連する WebGate 間のトランスポート・セキュリティが一致している必要があります。つまり、すべてオープン・モード、すべて簡易モード、またはすべて証明書モードのいずれかである必要があります。

アクセス・キャッシュ・フラッシングに関する通告： Identity Server でアクセス・キャッシュ・フラッシングが有効になっている場合、Identity Server は Access Server と通信します。この場合、次の 5 つのコンポーネント間のトランスポート・セキュリティ・モードはすべて同じモードである必要があります。

- Identity Server および WebPass インスタンス
- Policy Manager、Access Server および関連する WebGate

キャッシュの管理の詳細は、このマニュアルの 7-14 ページの「**キャッシュの管理**」と『Oracle Access Manager Access System Administration Guide』の両方を参照してください。キャッシングの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

インストール後にトランスポート・セキュリティ・モードを変更する必要がある場合は、システム・コンソールでセキュリティ・モードを変更できます。

ID システム (WebPass および Identity Server)： WebPass および Identity Server インスタンスのトランスポート・セキュリティ・モードは、ID システム・コンソールで選択します。WebPass および Identity Server インスタンスを構成する前に、使用するトランスポート・セキュリティ・モードのタイプを決定します。この場合も、すべてのコンポーネント間でトランスポート・セキュリティが一致している必要があります。これらは、すべてオープン、すべて簡易またはすべて証明書である必要があります。

アクセス・システム (Policy Manager、AccessGate および Access Server) : アクセス・システムで AccessGate および Access Server インスタンスを構成する際に、アクセス・システムのトランスポート・セキュリティ・モードを選択します。AccessGate および Access Server インスタンスを構成する前に、使用するトランスポート・セキュリティ・モードのタイプを決定します。この場合も、すべてのアクセス・システム・コンポーネント間でトランスポート・セキュリティが一致している必要があります。つまり、すべてオープン・モード、すべて簡易モード、またはすべて証明書モードのいずれかである必要があります。

システム・コンソールでモードを変更した後で、次の項で説明されているプロセスに従います。

- 8-11 ページの「アクセス・システムのトランスポート・セキュリティ・モードの変更」
- 8-22 ページの「ディレクトリ・サーバーのトランスポート・セキュリティの変更」

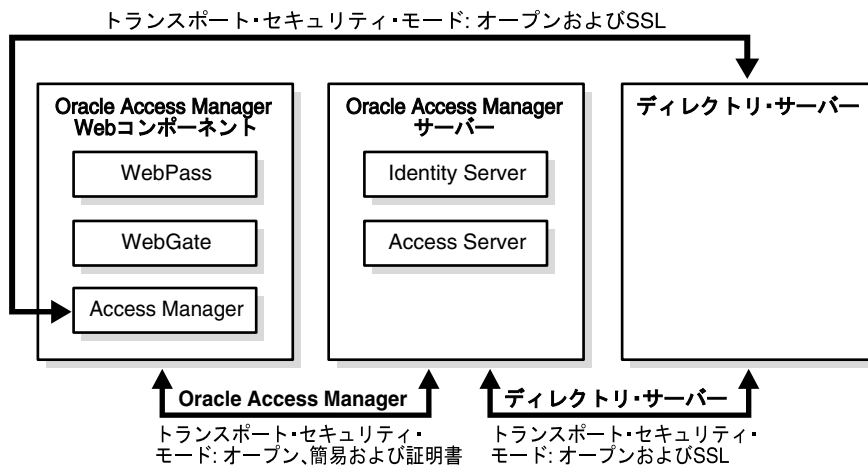
インストール後に、コンポーネントとディレクトリ・サーバー間のセキュリティ・モードを変更できます。

Identity Server または Access Server とディレクトリ・サーバー : ディレクトリ・サーバーと Identity Server または Access Server 間のトランスポート・セキュリティは、オープン・モードまたは SSL モードにすることができます。このトランスポート・セキュリティ・モードは、インストール時に指定します。SSL を選択した場合は、SSL 証明書の場所も指定します。ディレクトリ・サーバーは、指定したセキュリティ・モード情報で自動的に更新されます。

ディレクトリ・サーバーの SSL を構成する場合は、Oracle Access Manager がサーバー認証のみサポートすることに注意してください。クライアント認証はサポートされません。Oracle Access Manager は、製品設定時にインポートしたルート CA 証明書に照らしてサーバー証明書を検証します。

Policy Manager は、ディレクトリ・サーバーに対して読み取りおよび書き込みを行う Web コンポーネントです。Policy Manager とディレクトリ・サーバー間のトランスポート・セキュリティも指定します。図 8-1 に、Oracle Access Manager Web コンポーネントおよびサーバーと、Oracle Access Manager コンポーネントおよびディレクトリ・サーバーとの間でサポートされるトランスポート・セキュリティ・モードを示します。

図 8-1 トランスポート・セキュリティ・モード



SSL モードで稼働しているすべてのコンポーネントのディレクトリ・プロファイルは、これらのコンポーネントが最初に異なるモードで構成された場合でも共有できます。たとえば、Identity Server と Access Server がオープン・モードでディレクトリにインストールされ、Policy Manager がディレクトリ・サーバーに対して SSL を有効にしてインストールされたとします。この場合、cert8.db ファイルおよび key3.db ファイルは、ディレクトリ・サーバーと通信するコンポーネントごとに存在する必要があります、`component_install_dir\identity|access\oblix\config` ディレクトリに置かれている必要があります。これらのファイルが存在しない場合は、他の既存のコンポーネント・フォルダからコピーするか、この章で説明するように genCert (Policy Manager) またはその他のユーティリティを実行して生成します。

CA 証明書について

ここでは、ルート証明書、リクエストおよびその他の証明書ファイルについて説明します。

インストール時にコンポーネント間で証明書トランスポート・セキュリティ・モードを選択した場合は、ルート証明書を作成およびインストールする必要があります。ルート証明書は、認証局への CSR など、リクエストに署名する証明書を送信する際に生成される証明書のチェーンです。このリクエストは、xxx_req.pem ファイルの形式です。ルート証明書は、xxx_chain.pem というファイルとして格納します。xxx_chain.pem ファイルを証明書サーバーからダウンロードし、次のディレクトリにキーおよび cert.pem ファイルとともに格納してから、製品構成時にその場所を指定します。

`Component_install_dir\identity\access\oblix\config`

- チェーン・ファイル (ois_chain.pem)
- 証明書ファイル (ois_cert.pem)
- キー・ファイル (ois_key.pem)。インストーラはこの場所を認識している場合があります。

ほとんどのコンポーネントでは、製品設定時に証明書をインストールします。genCert ユーティリティを使用して証明書を Policy Manager にインストールします。このユーティリティのコマンドは次のとおりです。

```
genCert -i <install Dir> -m <cert | simple> -P <password> -c <request | install>
```

次に例を示します。

```
genCert -i c:\COREid\webcomponent\access\oblix\tools\gencert -m cert -P <password> -c install
```

承認された証明書は、コンポーネント・インストーラからアクセスできる任意の場所に保存できます。たとえば、/oblix/config に保存できます。

注意： 下位 CA によって生成された証明書を使用する場合は、ルート CA の証明書が下位 CA 証明書とともに xxx_chain.pem に存在している必要があります。適切な検証および正常な ID システム設定を行うには、両方の証明書が存在している必要があります。

WebGate の証明書リクエストでは、証明書リクエスト・ファイル aaa_req.pem が生成されます。この WebGate 証明書リクエストを、AAA サーバーによって信頼されているルート CA に送信する必要があります。ルート CA は、WebGate 証明書を返します。この証明書は、WebGate のインストール中またはインストール後にインストールできます。

次の各項では、証明書モードと、証明書のリクエストおよびインストールについて説明します。

ID システムのトランスポート・セキュリティの変更

インストール環境のすべての Identity Server および WebPass インスタンスは、同じトランスポート・セキュリティ・モードで実行する必要があります。インストール時に異なるコンポーネントに異なるモードを指定した場合は、それらを変更する必要があります。

タスクの概要：ID システムのトランスポート・セキュリティの変更

1. 簡易モードまたは証明書モードに変更する場合は、証明書準備のプロセスを完了します。
2. 8-6 ページの「[Identity Server のトランスポート・セキュリティ・モードを変更する手順](#)」の手順を実行します。
3. 8-6 ページの「[WebPass のトランスポート・セキュリティ・モードを変更する手順](#)」の手順を実行します。

注意： WebPass および Identity Server は、両方のトランスポート・セキュリティ・モードを変更するまで相互に通信できません。

Identity Server のトランスポート・セキュリティ・モードを変更する手順

1. 簡易モードまたは証明書モードに変更する場合は、証明書準備プロセスを完了します。
2. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」をクリックします。
3. 変更するサーバーのリンクをクリックし、「変更」をクリックします。
4. 選択するトランスポート・セキュリティ・モードに該当するボタンをクリックします。「オープン」、「簡易」または「証明書」モードを選択できます。
5. 「保存」をクリックします。
6. Identity Server を再起動します。

WebPass のトランスポート・セキュリティ・モードを変更する手順

1. 簡易モードまたは証明書モードに変更する場合は、証明書準備を完了します。
2. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「WebPass」をクリックします。
3. 変更する WebPass を選択し、「変更」をクリックします。
4. トランスポート・セキュリティ・モードを変更します。「オープン」、「簡易」または「証明書」モードを選択できます。
5. 「保存」をクリックします。
6. WebPass を停止し、Identity Server を再起動してから WebPass を再起動します。

ID システムのトランスポート・セキュリティ・モードの変更

インストール後にトランスポート・セキュリティ・モードを変更する場合は、ID システム・コンソールで新しいモードを指定してから、適切な構成ファイルでモードを変更します。各コンポーネントについて、必要に応じて表 8-2 に示す手順を繰り返します。

表 8-2 ID システムのトランスポート・セキュリティ・モードの変更

新しいセキュリティ・モード	プロセス
オープン	ID システム・コンソールでオープン・モードを指定します（詳細は、8-6 ページの「ID システムのトランスポート・セキュリティの変更」を参照してください）。
簡易	<ol style="list-style-type: none"> Identity Server を停止します。 Oracle Access Manager の内部 CA を通じて証明書を生成します（詳細は、8-8 ページの「簡易トランスポート・セキュリティ・モードへの変更」を参照してください）。 ID システム・コンソールでモードを構成します（詳細は、8-6 ページの「ID システムのトランスポート・セキュリティの変更」を参照してください）。 Identity Server を再起動します。
証明書	<ol style="list-style-type: none"> Identity Server を停止します。 証明書リクエストを生成します（詳細は、8-9 ページの「証明書トランスポート・セキュリティ・モードへの変更」を参照してください）。 外部 CA を通じて承認された証明書を取得します。 証明書をインストールします（詳細は、8-10 ページの「証明書モードの証明書をインストールする手順」を参照してください）。 ID システム・コンソールでモードを構成します（詳細は、8-6 ページの「ID システムのトランスポート・セキュリティの変更」を参照してください）。 Identity Server を再起動します。

注意： ID システム・コンポーネントがオープン・モードまたは証明書モードを使用している場合は特に、コンポーネントを実行しているコンピュータのクロックが同期している必要があります。Identity Server コンピュータのクロックが WebPass コンピュータのクロックよりも進んでいるかぎり、数秒の差異は許容されます。それ以外の場合は、証明書のタイム・スタンプが無効になり、すべてのリクエストが拒否されます。システム・クロックの同期の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

簡易トランスポート・セキュリティ・モードへの変更

簡易モードに変更する場合は、最初に Oracle Access Manager の内部 CA を通じて証明書を生成する必要があります。

CA を通じて証明書を生成する手順

1. コマンド・プロンプト・ウィンドウを開き、次のディレクトリに移動します。

```
IdentityServer_install_dir/identity/oblix/tools/setup
```

IdentityServer_install_dir は、Identity Server がインストールされているディレクトリです。

2. 変更しているコンポーネントに応じて、次のコマンドの 1 つを実行します。

表 8-3 設定コマンド

オペレーティング・システム	コマンド
UNIX	Identity Server: start_setup_ois -i <i>IdentityServer_install_dir</i> /identity -m WebPass: start_setup_webpass -i <i>WebPass_install_dir</i> /identity -m
Windows	Identity Server: setup_ois.exe -i <i>IdentityServer_install_dir</i> %identity -m WebPass: setup_webpass.exe -i <i>WebPass_install_dir</i> %identity -m <i>WebPass_install_dir</i> は、WebPass がインストールされているディレクトリです。

簡易モードまたは証明書モードの入力を求められます。

3. simple と入力し、[Enter] を押します。
4. グローバル・パスフレーズを指定し、確認します。
このパスワードは、インストール環境のすべての Identity Server および WebPass インスタンスで同じである必要があります。
5. 8-6 ページの「ID システムのトランスポート・セキュリティの変更」に進みます。

証明書トランスポート・セキュリティ・モードへの変更

証明書モードに変更する場合は、Identity Server のインストール後に次の操作を行う必要があります。

- 証明書リクエストを生成して、外部 CA から証明書を取得します。
- 署名された証明書を受信後にインストールします。

証明書モードの証明書リクエストを生成する手順

1. コマンド・プロンプト・ウィンドウを開き、次のディレクトリに変更します。

```
IdentityServer_install_dir/identity/oblix/tools/setup
```

IdentityServer_install_dir は、ID システムがインストールされているディレクトリです。

2. 表 8-4 のコマンドの 1 つを実行します。

表 8-4 ID システムの証明書リクエスト・コマンド

オペレーティング・システム	コマンド
UNIX	<p>Identity Server:</p> <pre>start_setup_ois -i IdentityServer_install_dir/identity -m</pre> <p>WebPass:</p> <pre>start_setup_webpass -i WebPass_install_dir/identity -m</pre> <p><i>WebPass_install_dir</i> は、WebPass がインストールされているディレクトリです。</p>
Windows	<p>Identity Server:</p> <pre>setup_ois.exe -i IdentityServer_install_dir\identity -m</pre> <p>WebPass:</p> <pre>setup_webpass.exe -i WebPass_install_dir\identity -m</pre> <p><i>WebPass_install_dir</i> は、WebPass がインストールされているディレクトリです。</p>

簡易モードまたは証明書モードの入力を求められます。

3. cert と入力し、[Enter] を押します。
4. 新しい証明書をリクエストしていることを指定します。
5. プロンプトに情報を入力します。
 - 2 文字の国コード（デフォルトは US）
 - 都道府県名
 - 市区町村または地域
 - 組織名（企業など）
 - 組織単位名（部門など）
 - 共通名（ホスト名など）
 - 連絡先電子メール・アドレス
6. [Enter] を押します。

次のメッセージが表示されます。

「証明書リクエストはファイル

Identity_Server_install_dir/identity/oblix/config/ois_req.pem に存在します」

setup_ois ユーティリティにより、ois_key.pem（秘密鍵を含む）と ois_req.pem の 2 つのファイルがこのディレクトリに作成されます。

7. 認証局によって署名されるように ois_req.pem ファイルを送信します。

証明書モードの証明書をインストールする手順

1. コマンド・プロンプト・ウィンドウを開き、次のディレクトリに変更します。

```
Identity_Server_install_dir/identity/oblix/tools/setup
```

IdentityServer_install_dir は、Identity Server がインストールされているディレクトリです。

2. 表 8-5 のコマンドの 1 つを実行します。

表 8-5 ID システムの証明書インストール・コマンド

オペレーティング・システム	コマンド
UNIX	<p>Identity Server:</p> <pre>start_setup_ois -i IdentityServer_install_dir/identity -m</pre> <p>WebPass:</p> <pre>start_setup_webpass -i WebPass_install_dir/identity -m</pre> <p>WebPass_install_dir は、WebPass がインストールされているディレクトリです。</p>
Windows	<p>Identity Server:</p> <pre>setup_ois.exe -i IdentityServer_install_dir\identity -m</pre> <p>IdentityServer_install_dir は、Identity Server がインストールされているディレクトリです。</p> <p>WebPass:</p> <pre>setup_webpass.exe -i WebPass_install_dir\identity -m</pre> <p>WebPass_install_dir は、WebPass がインストールされているディレクトリです。</p>

簡易モードまたは証明書モードの入力を求められます。

3. cert と入力し、[Enter] を押します。
4. 証明書をインストールしていることを指定します。
5. 次のファイルの場所を指定します。

ois_key.pem

ois_cert.pem

ois_chain.pem

Oracle Access Manager で生成された以前のリクエストの証明書をインストールした場合は、プロンプトが表示されたときに ois_key.pem のデフォルト値を使用します。

注意： 下位 CA によって生成された証明書を使用する場合は、ルート CA の証明書が下位 CA 証明書とともに ois_chain.pem に存在している必要があります。適切な検証および正常な ID システム設定を行うには、両方の証明書が存在している必要があります。

証明書がインストールされます。

6. 8-6 ページの「ID システムのトランスポート・セキュリティの変更」に進みます。

アクセス・システムのトランスポート・セキュリティ・モードの変更

AccessGate または Access Server のトランスポート・セキュリティ・モードを変更する前に、アクセス・システム・コンソールでコンポーネントのトランスポート・セキュリティ・モードを更新します。

アクセス・システム・コンソールから Policy Manager のトランスポート・セキュリティ・モードを更新することはできません。オープン・モードから別のモードに変更する場合は、表 8-2 の手順に従います。オープン・モードに変更する場合は、他の AccessGate および Access Server がオープン・モードで稼働していることが Policy Manager によって自動的に検出されるため、Policy Manager のモードを変更する必要はありません。

Access Server のトランスポート・セキュリティ・モードを指定する手順

1. アクセス・システム・コンソールで、「アクセス・システム構成」、「Access Server 構成」にナビゲートします。
2. 変更する Access Server を選択し、「変更」をクリックします。
3. トランスポート・セキュリティに該当するラジオ・ボタンを選択し、「保存」をクリックします。
4. Access Server を再起動します。

AccessGate のトランスポート・セキュリティ・モードを指定する手順

1. アクセス・システム・コンソールで、「アクセス・システム構成」、「AccessGate 構成」にナビゲートします。
2. 変更する AccessGate を選択し、「変更」をクリックします。
3. トランスポート・セキュリティに該当するラジオ・ボタンを選択し、「保存」をクリックします。
4. AccessGate をホストしている Web サーバーを再起動します。

アクセス・システムのトランスポート・セキュリティ・モードの変更

アクセス・システム・コンソールで変更を指定した後で、アクセス・システム・コンポーネントのトランスポート・セキュリティ・モードを変更できます。モードの変更のプロセスは、変更しているセキュリティ・モードによって決まります。Access Server のセキュリティ・モードを変更する場合は、この Access Server を指しているすべての Policy Manager および AccessGate のセキュリティ・モードを変更して、新しいセキュリティ・モードに一致させます。

1 つ以上の Access Server のセキュリティ・モードを変更する場合は、「トランスポート・セキュリティ・モード変更確認ページ」が表示されることがあります。このページは、Access Server で使用されるセキュリティ・モードと 1 つ以上の AccessGate 間の非互換性を通知します。

注意： AccessGate/WebGate および Policy Manager のモードを構成する前に、Access Server セキュリティ・モードを構成します。

表 8-6 に、セキュリティ・モードごとに実行するプロセスをリストします。必要に応じて、インストール済のコンポーネントごとにこれらの手順を繰り返してください。

表 8-6 アクセス・システムのトランスポート・セキュリティ・モードの変更

新しいセキュリティ・モード	プロセス
オープン	<p>Access Server:</p> <ol style="list-style-type: none"> 適切なディレクトリまたはファイルを新規フォルダに移動します（詳細は、8-15 ページの「オープン・トランスポート・セキュリティ・モードへの変更」を参照してください）。 アクセス・システム・コンソールで Access Server インスタンスを構成します（詳細は、8-11 ページの「Access Server のトランスポート・セキュリティ・モードを指定する手順」を参照してください）。 configAAAServer プログラムを実行して新規モードを指定します。ConfigureAAAServer ツールの使用の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。 <p>AccessGate/WebGate:</p> <ol style="list-style-type: none"> 適切なディレクトリまたはファイルを新規フォルダに移動します（詳細は、8-15 ページの「オープン・トランスポート・セキュリティ・モードへの変更」を参照してください）。 アクセス・システム・コンソールで AccessGate インスタンスを構成します（詳細は、8-11 ページの「AccessGate のトランスポート・セキュリティ・モードを指定する手順」を参照してください）。 configAccessGate または configWebGate プログラムを適宜実行して新規モードを指定します。コマンドラインで AccessGate を変更するには、『Oracle Access Manager Access System Administration Guide』を参照してください。 <p>Policy Manager:</p> <ol style="list-style-type: none"> Policy Manager がインストールされている Web サーバーを再起動します。

表 8-6 アクセス・システムのトランスポート・セキュリティ・モードの変更 (続き)

新しいセキュリティ・モード	プロセス
簡易	<p>Access Server:</p> <ol style="list-style-type: none"> 適切なディレクトリまたはファイルを新規フォルダに移動します (詳細は、8-8 ページの「簡易トランスポート・セキュリティ・モードへの変更」を参照してください)。 アクセス・システム・コンソールで Access Server インスタンスを構成します (詳細は、8-11 ページの「Access Server のトランスポート・セキュリティ・モードを指定する手順」を参照してください)。 configAAAServer プログラムを実行して新規モードを指定します。ConfigureAAAServer ツールの使用の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。 <p>AccessGate/WebGate:</p> <ol style="list-style-type: none"> 適切なディレクトリまたはファイルを新規フォルダに移動します (詳細は、8-8 ページの「簡易トランスポート・セキュリティ・モードへの変更」を参照してください)。オープン・モードから変更する場合は、この処理を行う必要はありません。 アクセス・システム・コンソールで AccessGate インスタンスの新規モードを構成します (詳細は、8-11 ページの「AccessGate のトランスポート・セキュリティ・モードを指定する手順」を参照してください)。 configAccessGate または configWebGate プログラムを適宜実行して新規モードを指定します。コマンドラインで AccessGate を変更するには、『Oracle Access Manager Access System Administration Guide』を参照してください。 <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは次のディレクトリにあります。</p> <p><code>PolicyManager_install_dir\access\oblix\tools\gencert</code></p> <p><code>PolicyManager_install_dir</code> は、Policy Manager がインストールされているディレクトリです。</p>

表 8-6 アクセス・システムのトランスポート・セキュリティ・モードの変更（続き）

新しいセキュリティ・モード	プロセス
証明書	<p>Access Server:</p> <ol style="list-style-type: none"> 適切なディレクトリまたはファイルを新規フォルダに移動します（詳細は、8-9 ページの「証明書トランスポート・セキュリティ・モードへの変更」を参照してください）。 アクセス・システム・コンソールで Access Server インスタンスを構成します（詳細は、8-11 ページの「Access Server のトランスポート・セキュリティ・モードを指定する手順」を参照してください）。 configAAAServer プログラムを実行して新規モードを指定します。ConfigureAAAServer ツールの使用の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。 <p>AccessGate/WebGate:</p> <ol style="list-style-type: none"> 適切なディレクトリまたはファイルを新規フォルダに移動します（詳細は、8-9 ページの「証明書トランスポート・セキュリティ・モードへの変更」を参照してください）。オープン・モードから変更する場合は、この処理を行う必要はありません。 アクセス・システム・コンソールで AccessGate インスタンスの新規モードを構成します（詳細は、8-11 ページの「AccessGate のトランスポート・セキュリティ・モードを指定する手順」を参照してください）。 configAccessGate または configWebGate プログラムを適宜実行して、証明書リクエストを生成し、証明書をインストールします。コマンドラインで AccessGate を変更するには、『Oracle Access Manager Access System Administration Guide』を参照してください。 <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは次のディレクトリにあります。</p> <p><code>PolicyManager_install_dir\access\oblix\tools\gencert</code></p> <p><code>PolicyManager_install_dir</code> は、Policy Manager がインストールされているディレクトリです。</p>

オープン・トランスポート・セキュリティ・モードへの変更

トランスポート・セキュリティ・モードを簡易または証明書からオープンに変更する場合は、適切な構成プログラムを実行します。

オープン・セキュリティ・モードに変更する手順

1. 次のディレクトリを新規フォルダに移動します。

AccessSystem_install_dir/access/oblix/config/simple (簡易モードの場合)

または

AccessSystem_install_dir/access/oblix/config/.pem and password.xml* (証明書モードの場合)

AccessSystem_install_dir は、アクセス・システム・コンポーネントがインストールされているディレクトリです。たとえば、Policy Manager、Access Server または WebGate です。

これにより、以前の構成を保存し、必要に応じてその構成に戻すことができます。

2. 表 8-7 のコマンドの 1 つを実行します。

表 8-7 アクセス・システム・コマンド: オープン・モードへの変更

オペレーティング・システム	コマンド
UNIX	<p>Access Server:</p> <pre>start_configureAAAServer reconfig <i>AccessServer_install_dir/access</i> -R<i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</pre> <p>AccessGate:</p> <pre>start_configureAccessGate -i <i>AccessGate_install_dir/access</i> -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>start_configureWebGate -i <i>WebGate_install_dir/access</i> -t WebGate -R<i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</pre> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは次のディレクトリにあります。</p> <pre><i>PolicyManager_install_dir</i>\access\oblix\tools\gencert</pre> <p><i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>

表 8-7 アクセス・システム・コマンド：オープン・モードへの変更（続き）

オペレーティング・システム	コマンド
Windows	<p>Access Server:</p> <pre>configureAAAServer.exe reconfig <i>AccessServer_install_dir</i>%access</pre> <p>-R<i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>configureAccessGate.exe -i <i>AccessGate_install_dir</i>%access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>configureWebGate.exe -i <i>WebGate_install_dir</i>%access -t WebGate</pre> <p>-R<i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは次のディレクトリにあります。</p> <pre><i>PolicyManager_install_dir</i>%access%oblix%tools%gencert</pre> <p><i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>

簡易トランスポート・セキュリティ・モードへの変更

簡易モードを実装する場合は、外部 CA の証明書をリクエストまたはインストールする必要はありません。Oracle Access Manager に、固有の内部 CA が付属しています。

簡易セキュリティ・モードに変更する手順

1. 次のファイルを新規フォルダに移動します。

AccessSystem_install_dir/access/oblix/config/*.pem

および

AccessSystem_install_dir/access/oblix/config/password.xml（証明書モードの場合）

AccessSystem_install_dir は、アクセス・システム・コンポーネントがインストールされているディレクトリです。たとえば、Policy Manager、Access Server または WebGate です。

これにより、古い構成のバックアップ・ファイルが作成されます。

2. Oracle Access Manager の内部 CA を通じて証明書を生成します。

- a. コマンド・プロンプト・ウィンドウを開き、適切な

AccessSystem_install_dir/access/oblix/tools/*componentDirectory* に変更します。

意味：

componentDirectory は、変更しているコンポーネント（configureAAAServer、configureWebGate または genCert（genCert は Policy Manager で使用されるユーティリティ））のディレクトリです。

次に例を示します。

```
cd COREid/WebComponent/access/oblix/tools/configureWebGate
```

- b. 表 8-8 のコマンドの 1 つを実行します。

表 8-8 アクセス・システム・コマンド：簡易モードへの変更

オペレーティング・システム	コマンド
UNIX	<p>Access Server:</p> <pre>start_configureAAAServer reconfig <i>AccessServer_install_dir</i>/access -R</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>start_configureAccessGate -i <i>AccessGate_install_dir</i>/access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>start_configureWebGate -i <i>WebGate_install_dir</i>/access -t WebGate -R</pre> <p><i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは、ディレクトリ <i>AccessManager_install_dir</i>\access\oblix\tools\gencert にあります。<i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>
Windows	<p>Access Server:</p> <pre>configureAAAServer.exe reconfig <i>AccessServer_install_dir</i>\access -R</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>configureAccessGate.exe -i <i>AccessGate_install_dir</i>\access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>configureWebGate.exe -i <i>WebGate_install_dir</i>\access -t WebGate -R</pre> <p><i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは、ディレクトリ <i>PolicyManager_install_dir</i>\access\oblix\tools\gencert にあります。<i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>

- c. オープン、簡易または証明書モードの入力を求めるプロンプトが表示された場合は、「簡易」モードを選択し、[Enter] を押します。
- d. グローバル・パスフレーズを指定し、確認します。

このパスワードは、すべての Access Server、AccessGate および WebGate で同じである必要があります。グローバル・パスフレーズの詳細は、『Oracle Access Manager インストール・ガイド』を参照してください。

警告： Policy Manager の簡易モード・パスワードが変更された場合、またはアクセス・システムが簡易モードから証明書モードに変更された場合は、Policy Manager を再インストールする必要があります。

証明書トランスポート・セキュリティ・モードへの変更

次の手順では、証明書トランスポート・セキュリティ・モードへの変更について説明します。

注意： WebGate の証明書リクエストでは、証明書リクエスト・ファイル `aaa_req.pem` が生成されます。この WebGate 証明書リクエストを、AAA サーバーによって信頼されているルート CA に送信する必要があります。ルート CA は、WebGate 証明書を返します。この証明書は、WebGate のインストール中またはインストール後にインストールできます。

証明書セキュリティ・モードに変更する手順

1. 次のディレクトリを新規フォルダに移動します。

`AccessSystem_install_dir/access/oblix/config/simple` (簡易モードの場合)

これにより、古い構成のバックアップが作成されます。

2. 証明書リクエストを生成します。

- a. コマンド・プロンプト・ウィンドウを開き、次のディレクトリに変更します。

`AccessSystem_install_dir/access/oblix/tools/componentDirectory`

`AccessSystem_install_dir` はアクセス・システム・コンポーネントがインストールされているディレクトリで、`componentDirectory` は変更しているコンポーネント (`configureAAAserver`、`configureWebGate`、`configureAccessGate` または `genCert` (`genCert` は Policy Manager で使用される)) のディレクトリです。

次に例を示します。

```
cd COREid/WebComponent/access/oblix/tools/genCert
```

- b. 変更しているコンポーネントに応じて、表 44 のコマンドの 1 つを実行します。

表 8-9 アクセス・システムの証明書リクエスト・コマンド

オペレーティング・システム	コマンド
UNIX	<p>Access Server:</p> <pre>start_configureAAAServer reconfig <i>AccessServer_install_dir</i>/access -R</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>start_configureAccessGate -i <i>AccessGate_install_dir</i>/access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>start_configureWebGate -i <i>WebGate_install_dir</i>/access -t WebGate -R</pre> <p><i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは、ディレクトリ <i>PolicyManager_install_dir</i>\access\oblix\tools\gencert にあります。</p> <p><i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>
Windows	<p>Access Server:</p> <pre>configureAAAServer.exe reconfig <i>AccessServer_install_dir</i>\access -R</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>configureAccessGate.exe -i <i>AccessGate_install_dir</i>\access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>configureWebGate.exe -i <i>WebGate_install_dir</i>\access -t WebGate -R</pre> <p><i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは、ディレクトリ <i>PolicyManager_install_dir</i>\access\oblix\tools\gencert にあります。</p> <p><i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>

- c. モードのプロンプトが表示されたら、「証明書」を選択して [Enter] を押します。
- d. 証明書をリクエストしていることを指定します。

- e. 次のような情報を求めるプロンプトに回答します。
 - 2文字の国コード (デフォルトは US)
 - 都道府県名
 - 市区町村または地域
 - 組織名 (企業など)
 - 組織単位名 (部門など)
 - 共通名 (ホスト・マシン名にする必要があります)
 - 連絡先電子メール・アドレス
 - f. [Enter] を押します。
 証明書リクエストがファイル `AccessServer_install_dir/access/oblix/config/aaa_req.pem` にあることを示すメッセージが表示されます。

`setup_aaa` ユーティリティは実際にこのディレクトリに次の2つのファイルを作成します。

`aaa_key.pem` (秘密鍵を含む) および `aaa_req.pem`。
 - g. リクエストに署名するために `aaa_req.pem` ファイルを認証局に送信します。
3. 承認された証明書を、インストーラがアクセスできるファイルに保存します。
 4. インストーラがアクセスできる `.pem` ファイルに CA チェーンを base64 コード形式で保存します。
 5. CA から証明書を受信した後で、署名された証明書をインストールします。

証明書モードで署名された証明書をインストールする手順

1. コマンド・プロンプト・ウィンドウを開き、
`AccessSystem_install_dir/access/oblix/tools/componentDirectory` に変更します。

`AccessSystem_install_dir` はアクセス・システムがインストールされているディレクトリで、`componentDirectory` は変更しているコンポーネント (`configureAAAServer`、`configureWebGate`、`configureAccessGate` または `genCert` (`genCert` は Policy Manager で使用されるユーティリティ)) のディレクトリです。

 次に例を示します。


```
cd COREid/access/oblix/tools/configureAAAServer
```


2. 次のコマンドの1つを実行します。

表 8-10 アクセス・システムの証明書インストール・コマンド

オペレーティング・システム	コマンド
UNIX	<p>Access Server:</p> <pre>start_configureAAAServer reconfig <i>AccessServer_install_dir</i>/access -R</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>start_configureAccessGate -i <i>AccessGate_install_dir</i>/access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>start_configureWebGate -i <i>WebGate_install_dir</i>/access -t WebGate -R</pre> <p><i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは、ディレクトリ <i>PolicyManager_install_dir</i>\access\oblix\tools\gencert にあります。</p> <p><i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>
Windows	<p>Access Server:</p> <pre>configureAAAServer.exe reconfig <i>AccessServer_install_dir</i>\access -R</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>configureAccessGate.exe -i <i>AccessGate_install_dir</i>\access -t AccessGate -R</pre> <p><i>AccessGate_install_dir</i> は、AccessGate がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>configureWebGate.exe -i <i>WebGate_install_dir</i>\access -t WebGate -R</pre> <p><i>WebGate_install_dir</i> は、WebGate がインストールされているディレクトリです。</p> <p>Policy Manager:</p> <p>genCert ユーティリティを実行して新規モードを指定します。genCert ユーティリティは、ディレクトリ <i>PolicyManager_install_dir</i>\access\oblix\tools\gencert にあります。</p> <p><i>PolicyManager_install_dir</i> は、Policy Manager がインストールされているディレクトリです。</p>

3. 簡易モードまたは証明書モードの入力を求めるプロンプトが表示された場合は、Cert と入力し、[Enter] を押します。
4. 証明書をインストールしていることを指定します。

5. キー、サーバー証明書および CA チェーン・ファイルの場所を指定します。
 - aaa_key.pem
 - aaa_cert.pem
 - aaa_chain.pem

aaa は、ファイルについて指定する名前です（証明書ファイルおよびチェーン・ファイルにのみ適用されます）。

警告： WebGate 証明書リクエストでは、証明書リクエスト・ファイル `aaa_req.pem` が生成されます。この証明書リクエストを、AAA サーバーによって信頼されているルート CA に送信する必要があります。ルート CA は、WebGate 証明書を返します。この証明書は、WebGate のインストール中またはインストール後にインストールできます。

Oracle Access Manager で生成された以前のリクエストの証明書をインストールした場合は、プロンプトが表示されたときに `aaa_key.pem` のデフォルト値を使用します。

証明書がインストールされます。

6. AccessGate または Access Server を適宜再起動します。

ディレクトリ・サーバーのトランスポート・セキュリティの変更

Identity Server および Access Server をインストールする場合は、これらの各サーバーとディレクトリ・サーバー間でオープン・モードまたは SSL モードを指定できます。インストール後にトランスポート・セキュリティ・モードを変更するには、Identity Server または Access Server を適宜再構成する必要があります。再構成時に、ディレクトリ・サーバーと Identity Server または Access Server 間のセキュリティ・モードを変更できます。

注意： インストール後のディレクトリ証明書の追加の詳細は、『Oracle Access Manager インストール・ガイド』を参照してください。

Identity Server とディレクトリ・サーバー間のトランスポート・セキュリティを変更する手順

1. コマンドラインから、プラットフォームに適した `setup_ois` ツールを検索します。

UNIX での例は次のとおりです。

```
IdentityServer_install_dir/identity/oblix/tools/setup
```

2. コマンド・プロンプトで、適切な実行可能ファイルを実行します。

UNIX での例は次のとおりです。

```
start_setup_ois -i
```

Identity Server の設定に必要な手順がガイドされます。

3. Identity Server とディレクトリ・サーバー間に SSL が必要かどうかを確認されたら、y（はい）または n（いいえ）を選択します。

注意： SSL を選択した場合、CA 証明書の場所を求められたらそのフルパスを指定します。

4. 残りの手順を実行して、再構成プロセスを完了します。

Policy Manager とディレクトリ・サーバー間のトランスポート・セキュリティを SSL に変更する手順

1. コマンドラインから、プラットフォームに適した `setup_access_manager` ツールを検索します。

UNIX での例は次のとおりです。

```
PolicyManager/identity/oblix/tools/setup
```

2. コマンド・プロンプトで、適切な実行可能ファイルを実行して `cert8.db` ファイルを作成します。

UNIX での例は次のとおりです。

```
start_setup_access_manager -i
```

Policy Manager の設定に必要な手順がガイドされます。

3. ディレクトリ・サーバーのルート CA 証明書を含むファイルのフルパスを求められたら、それを指定します。
4. 残りの手順を実行して、再構成プロセスを完了します。

Access Server とディレクトリ・サーバー間のトランスポート・セキュリティを変更する手順

1. コマンドラインから、`configureAAAServer` ツールが置かれているフォルダにナビゲートします。

次に例を示します。

```
AccessServer_install_dir/access/oblix/tools/configureAAAServer
```

2. コマンドラインで、次の実行可能ファイルを実行します。

```
start_configureAAAServer -i
```

注意： Windows 以外のシステムでは、`start_configureAAAServer` ツールを使用します。

3. 1 (Y) を選択して Access Server を再構成します。
Access Server の設定に必要な手順がガイドされます。必要な情報を指定します。
4. ディレクトリ・サーバーのモードの指定を求められたら、「オープン」または「SSL」を選択します。
5. SSL を選択した場合は、CA 証明書の場所のフルパスを指定します。
6. 残りの手順を実行して、再構成プロセスを完了します。

トランスポート・セキュリティ・パスワードの変更

相互に通信している場合、コンポーネントはパスワードベースのメカニズムを使用して相互に認証します。

- **簡易モード:** 簡易モードでは、インストール環境内の ID システムまたはアクセス・システムのすべてのコンポーネントが同じパスワードを使用します。Oracle Access Manager は、Transport Layer Security (TLS) により要求される証明書を生成します。任意のインストール環境で、有効な証明書を生成できます。
- 各コンポーネントが介入なしに開始できるように、ローカル・ファイルにパスワードを格納できます。または、起動時にコンポーネントがパスワードのプロンプトを表示することができます。プロンプトでは、各要素を手動で起動し、パスワードを入力するようシステム管理者に要求します。
- **証明書モード:** 証明書モードでは、各コンポーネントの秘密鍵ファイルのパスワードが必要です。コンポーネントごとに異なるパスワードを使用できます。

簡易モードと同様に、パスワードをローカル・ファイルに格納して、各コンポーネントを介入なしに起動することも、起動時にコンポーネントがパスワードのプロンプトを表示するようにすることもできます。プロンプトでは、各コンポーネントを手動で起動し、パスワードを入力するようシステム管理者に要求します。

証明書トランスポート・セキュリティ・モードまたは簡易トランスポート・セキュリティ・モードのパスワードは変更できます。

ID システムの証明書パスワードを変更する手順

1. コマンド・プロンプト・ウィンドウを開き、
IdentityServer_install_dir/identity/oblix/tools/setup ディレクトリに変更します。
IdentityServer_install_dir は、Identity Server がインストールされているディレクトリです。
次に例を示します。

```
cd COREid/identity/oblix/tools/setup
```

2. 表 8-11 のコマンドの 1 つを実行します。

表 8-11 証明書パスワードを変更するための ID システム・コマンド

オペレーティング・システム	コマンド
UNIX	Identity Server: <pre>start_setup_ois -i IdentityServer_install_dir/identity -k</pre> <i>IdentityServer_install_dir</i> は、Identity Server がインストールされているディレクトリです。 WebPass: <pre>start_setup_webpass -i WebPass_install_dir/identity -k</pre> <i>WebPass_install_dir</i> は、WebPass がインストールされているディレクトリです。
Windows	Identity Server: <pre>setup_ois.exe -i IdentityServer_install_dir\identity -k</pre> <i>IdentityServer_install_dir</i> は、Identity Server がインストールされているディレクトリです。 WebPass: <pre>setup_webpass.exe -i WebPass_install_dir\identity -k</pre> <i>WebPass_install_dir</i> は、WebPass がインストールされているディレクトリです。

3. このコンポーネントが使用しているトランスポート・セキュリティ・モードを指定します。

4. 旧パスワードを指定します。
5. 新規パスワードを指定し、確認します。
6. Identity Server を再起動します。

アクセス・システムの証明書パスワードを変更する手順

1. コマンド・プロンプト・ウィンドウを開き、
AccessSystem_install_dir/access/oblix/tools/componentDirectory に変更します。
AccessSystem_install_dir はアクセス・システムがインストールされているディレクトリで、*componentDirectory* は変更しているコンポーネントのディレクトリです。

次に例を示します。

```
cd COREid/access/oblix/tools/configureAccessGate
```

2. 表 8-12 のコマンドの 1 つを実行します。

表 8-12 証明書パスワードを変更するためのアクセス・システム・コマンド

オペレーティング・システム	コマンド
UNIX	<p>Access Server:</p> <pre>start_configureAAAServer chpasswd <i>AccessServer_install_dir</i>/access</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>start_configureAccessGate -i <i>AccessGate_install_dir</i>/access -t AccessGate -k</pre> <p><i>AccessGate_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>start_configureWebGate -i <i>WebGate_install_dir</i>/access -t WebGate -k</pre> <p><i>WebGate_install_dir</i> は、Access Server がインストールされているディレクトリです。</p>
Windows	<p>Access Server:</p> <pre>configureAAAServer.exe chpasswd <i>AccessServer_install_dir</i>%access</pre> <p><i>AccessServer_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>AccessGate:</p> <pre>configureAccessGate.exe -i <i>AccessGate_install_dir</i>%access -t AccessGate -k</pre> <p><i>AccessGate_install_dir</i> は、Access Server がインストールされているディレクトリです。</p> <p>WebGate:</p> <pre>configureWebGate.exe -i <i>WebGate_install_dir</i>%access -t WebGate -k</pre> <p><i>WebGate_install_dir</i> は、Access Server がインストールされているディレクトリです。</p>

3. このコンポーネントが使用しているトランスポート・セキュリティ・モードを指定します。
4. 旧パスワードを指定します。
5. 新規パスワードを指定し、確認します。
6. Access Server を再起動します。

複数の CA 証明書のインポート

Oracle Access Manager は、ユーザー・データ、構成データまたはポリシー・データ用のディレクトリ・サーバーとコンポーネント間のトランスポート・セキュリティに対して、ディレクトリ・サーバー・タイプごとに 1 つの CA 証明書を認識します。

実装で、ユーザー・データ、構成データまたはポリシー・データに別々のディレクトリ・サーバーがある場合は、それぞれに異なる CA 証明書を使用できます。このため、実装では最大 3 つの CA 証明書を使用できます。ユーザー・ディレクトリに 1 つ、構成ディレクトリに 1 つ、ポリシー・ディレクトリに 1 つを使用します。

警告： インストール環境で、異なる認証局の証明書を使用して SSL を確立したレプリケート・ディレクトリまたは複数のディレクトリを使用する場合は、各種証明書を `cert8.db` ファイルに手動でインポートする必要があります。`cert8.db` ファイルは独自の Mozilla 形式で暗号化および格納されます。

ディレクトリ・サーバー CA 証明書の追加の詳細は、『Oracle Access Manager インストール・ガイド』を参照してください。

Access Server のセキュリティ・パスワードの変更

Access Server のトランスポート・セキュリティ・モードは、コマンドラインから変更できます。簡易モードでは、AccessGate または WebGate と Access Server が相互に通信するには、これらが同じパスワードを持っている必要があります。

トランスポート・セキュリティ・モードのパスワードを変更する手順

1. 次の実行可能ファイルを実行します。

```
configureAAServer chpasswd AccessServer_install_dir
```

`AccessServer_install_dir` は、Access Server がインストールされているディレクトリです。

2. プロンプトが表示されたら、次の項目を指定します。
 - Access Server が構成されているトランスポート・セキュリティ・モード
 - 旧パスワード
 - 新パスワード
3. Access Server を再起動します。

詳細は、8-2 ページの「トランスポート・セキュリティ・モードについて」を参照してください。

この章では、レポート機能の概要、各機能が提示する情報、使用可能な出力のタイプおよびこれらのレポートの用途を示します。この章の内容は次のとおりです。

- [レポートについて](#)
- [レポート機能のサマリー](#)

レポートについて

Oracle Access Manager は、次の項目に関連する様々な情報を収集および提示できます。

- Oracle Access Manager ディレクトリ内のユーザーおよびリソース
- アクセス・システムおよび ID システムでのアクティビティ
- システムの操作、管理およびメンテナンス

Oracle Access Manager に組み込まれている多くのレポート関連機能を区別できるように、この章では、次の表で説明する特定の用語を使用して特定の機能領域を説明します。

表 9-1 レポートで使用される予約語

機能	説明
モニタリング	システムをホストするネットワーク・コンポーネントの状態およびパフォーマンスをモニターできるように収集された SNMP データのみを表します。SNMP モニタリングの詳細は、第 12 章「SNMP モニタリング」を参照してください。
ロギング	システムを構成するコンポーネントの状態の診断、実行エラーのトラブルシューティング、カスタム AccessGate およびその他のプラグインのデバッグを行えるように収集されたプログラム実行データのみを表します。ロギングの詳細は、第 10 章「ロギング」を参照してください。
監査	次の 2 種類のデータを表します。 <ul style="list-style-type: none"> ■ 動的監査データは Access Server および Identity Server から収集されます。これには、リソース・リクエスト、パスワード変更、アカウント失効などの Oracle Access Manager システム・イベントが含まれます。 ■ 静的監査データは、ディレクトリ・サーバーから収集されます。これには、ポリシー情報とプロファイル情報が含まれます。 静的および動的レポートの一般的な説明は、9-3 ページの「レポート・タイプ」を参照してください。 監査の詳細は、第 11 章「監査」を参照してください。
診断	Access Server、Identity Server およびそれらの Oracle Access Manager ディレクトリ・コンポーネントへの接続に関するパラメータ設定および状態情報を表します。アクセス・システムおよび ID システムの診断の詳細は、11-4 ページの表 11-1 を参照してください。
アクセス・テスト	特定のユーザーが特定の時点で特定のリソースにアクセスできるかどうかを迅速に判断する方法を提供する画面表示のみを表します。アクセス・テストの詳細は、11-4 ページの表 11-1 を参照してください。
フィルタ処理された問合せ	プロファイルまたはポリシー属性の特定の組合せを共有するユーザーまたはリソースのリストを生成するために様々な Oracle Access Manager アプリケーションを通じて実行されるディレクトリの拡張検索を表します。フィルタ処理された拡張問合せの詳細は、11-4 ページの表 11-1 を参照してください。
監査レポート	Oracle Access Manager サーバーおよびディレクトリ・サーバーから収集され、監査データベースに格納され、構成済の Crystal Reports プレゼンテーション・テンプレートによって抽出、コンパイルおよび書式設定されたデータのみを表します。監査レポートの詳細は、11-15 ページの「監査レポートについて」および 11-44 ページの「監査レポートの設定」を参照してください。

レポート・タイプ

各種レポート機能によって収集およびレポートされる情報は、2つの大きなカテゴリに分かれます。

- **静的レポート**：一般に、Oracle Access Manager コンポーネントまたはサード・パーティの関連コンポーネントに格納されている設定からコンパイルされます。たとえば、Oracle Access Manager ディレクトリ・サーバーに格納されているポリシーおよびプロファイル情報は、静的監査データとして分類されます。接続設定（および状態）は、診断カテゴリに分類されます。特定の監査レポートは、静的（格納された）ポリシーおよびプロファイル情報を使用して、指定された時間中に指定されたユーザーから使用可能なリソースのリストをコンパイルします。
- **動的レポート**：Oracle Access Manager システム全体を通して様々なレベルでイベントおよび状態変化に注目します。たとえば、ロギング機能では、特定のコンポーネントから発生した各ファンクション・コール（および結果）を記録できます。この低レベル・トレース機能は、開発者に役立つ場合があります。その対極で、動的監査機能は、特定の期間中に特定のサーバーについて失敗した認証試行のパターンをレポートすることにより、システム侵入の恐れを明らかにできます。

データ・ソース

レポート機能は、様々なソースからデータを収集できます。最も重要なソースを表 9-2 で説明します。

表 9-2 レポート機能のプライマリ・データ・ソース

データ・ソース	説明
Oracle Access Manager ディレクトリ	次のような数種類の静的情報を格納します。 <ul style="list-style-type: none"> ■ ユーザー、グループおよび組織のプロファイル設定 ■ リソースを保護するためのポリシー設定 ■ Oracle Access Manager コンポーネントまたは Oracle Access Manager で使用される各種データベースへの接続に使用されるような接続設定 ■ 特定のセキュリティ設定 ■ Oracle Access Manager システムの中心にある LDAP ディレクトリの編成に使用されるスキーマ
コンポーネント構成ファイル	多くのキー設定が、影響を与える Oracle Access Manager コンポーネントのディレクトリ構造内に格納されている構成ファイルに存在します。これは、データベース・ドライバへのパスから、ログ出力のキューイングに使用されるバッファのサイズまで多岐に渡る場合があります。
システム構成ファイル	各種 Oracle Access Manager コンポーネントをホストするマシンに関するこれらの設定は、コンポーネントを相互に参照できるようにする環境変数であるか、コンポーネントが同じレベルで通信できるようにするプロトコル設定です。一般に Oracle Access Manager では、このようなシステムレベル構成は直接レポートされませんが、ホスト・システム・レベルで確立された設定に一致する必要がある対応する設定をレポートできることがあります。
Access Server	他のコンポーネントと対話するためにメンテナンスする設定に関する構成情報の提供に加えて、Access Server は、認可リクエストとその結果などのアクセス・システム・イベントをレポートできます。この情報は、一定期間中に誰が何に対するアクセス権を取得した（または取得を試行した）かを判断するのに役立ちます。
Identity Server	Identity Server は、他のコンポーネントとの対話方法を左右する特定の設定も格納します。また、誰がいつ資格証明の送信を試行したか、また認証試行に成功したかどうかなどの ID システム・イベントをレポートします。

表 9-2 レポート機能のプライマリ・データ・ソース (続き)

データ・ソース	説明
その他のコンポーネント	Policy Manager などのコンポーネントは、ポリシーに対する変更およびその他のアクティビティや設定をレポートできます。

データ出力

一般に、様々なタイプのレポートが次の 1 つ以上の宛先にデータを送信できます。

- Oracle Access Manager グラフィカル・ユーザー・インタフェース
- データを送信しているコンポーネントをホストしているマシン上のプレーン・テキスト・ファイル
- データを送信しているコンポーネントをホストしているマシン上のシステム・ファイル
- 中央データベース

注意： データが監査データベースに送信された場合、一般にそのデータは、監査レポートを生成する特殊な Crystal Reports テンプレートを使用してフィルタ処理、コンパイルおよび提示されます。

レポートがグラフィカル・ユーザー・インタフェースに送信された場合、そのデータはファイルまたはデータベースに送信される同等のタイプよりも内容が若干少なくなる可能性があります。たとえば、画面上のアクセス・テスター・ツールは、出力をプレーン・テキスト・ファイルまたは監査データベースに送信するユーザー・アクセス権限ツールで利用できる複雑なユーザーおよびリソース・グループの種類をレポートできません。

出力構成

一般に、レポート出力は次のいずれか一方または両方の方法で書式設定できます。

- Oracle Access Manager グラフィカル・ユーザー・インタフェースを使用します。
- プレーンテキスト構成ファイルを手動で編集します。

制限された数のケースおよび制限された範囲で、サード・パーティ GUI を通じてレポート出力を構成できます。たとえば、Crystal Reports インタフェースを通じて監査レポートを生成するために使用されるテンプレートを編集できます。

データの用途

レポートは、次のような様々な人々に役立ちます。

- Oracle Access Manager の管理者
- ネットワーク管理者
- セキュリティ管理者
- コンプライアンス管理者
- カスタム AccessGate およびプラグインの開発者

レポート機能のサマリー

表 9-3 に、レポート機能の概要、その機能が提示する情報、およびこれらの機能を適用可能と考えられる用途を示します。

表 9-3 レポート機能の概要

機能	タイプ	出力	ソース	データ	考えられる用途
モニタリング	動的	ファイル	SNMP モニター	ネットワーク・コンポーネントの状態およびイベント	Oracle Access Manager システムをホストしているネットワークのモニタリングおよびトラブルシューティング
ロギング	動的	ファイル	Oracle Access Manager コンポーネント	プログラム実行 (状態およびイベント)	コンポーネントの状態の診断と、カスタム AccessGate およびプラグイン・コードのデバッグ
監査	動的	ファイル、DB	Oracle Access Manager サーバー	システム・イベント	使用パターン、システム・パフォーマンス、コンポーネントのロードおよびセキュリティ・コンプライアンスの追跡
監査	静的	ファイル、DB	ディレクトリ・サーバー	プロファイルおよびポリシー属性	指定したパターンに適合するユーザーおよびリソースの識別
診断	静的	GUI	ディレクトリ・サーバー	ディレクトリ・コンポーネント、サーバーおよび接続の設定と状態	サーバーとディレクトリ・サーバーの設定、状態および接続詳細の検証
アクセス・テスト	静的	GUI	ディレクトリ・サーバー	プロファイルおよびポリシー属性	特定の時点で誰が何にアクセスできるかの迅速な判断
フィルタ処理された問合せ	静的	GUI、ファイル	ディレクトリ・サーバー	プロファイルおよびポリシー属性	共有プロファイルとポリシー属性の複雑な組合せのレポート
監査レポート (監査データベースを通じて Crystal Report テンプレートから)					
グローバル・アクセス	静的	GUI、ファイル、ハードコピー	監査データベースを通じてディレクトリ・サーバー	プロファイルおよびポリシー属性	ユーザーおよびリソース・アクセス権限に関する拡張レポート
認証	動的	GUI、ファイル、ハードコピー	監査データベースを通じてコンポーネント・サーバー	認証イベント	認証イベントに関する統計
認可	動的	GUI、ファイル、ハードコピー	監査データベースを通じてコンポーネント・サーバー	認可イベント	認可イベントに関する統計

表 9-3 レポート機能の概要 (続き)

機能	タイプ	出力	ソース	データ	考えられる用途
アクティビティ	動的	GUI、 ファイル、 ハードコ ピー	監査デー タベー スを通 じたコ ンポー ネント ・サー バー	アクセ ス・シ ステ ムおよ びID システ ムの イベ ント	各種 Oracle Access Manager イベントの統 計およびリスト
ID 履歴	動的	GUI、 ファイル、 ハードコ ピー	監査デー タベー スを通 じたコ ンポー ネント ・サー バー	プロフ ァイル 属性 およ び属 性の 変更	ID プロファイル変更 の統計およびリスト

10

ロギング

この章では、ロギングを中心に説明します。内容は次のとおりです。

- [ロギングおよびログ・レベルについて](#)
- [ログ構成ファイルについて](#)
- [ログ・ライターについて](#)
- [ログ構成ファイルの構造](#)
- [ロギング・レベルの制御](#)
- [ログ構成パラメータ](#)
- [ID システム・コンソールでのログの構成](#)

ロギングおよびログ・レベルについて

ロギング機能を使用すると、広範なプログラム実行データを収集できるため、システム・パフォーマンスの問題のトラブルシューティングやコンポーネント状態の問題の診断を行うことができます。

ロギングは、Oracle Access Manager 関連情報を収集および提示するためのいくつかの機能の 1 つです。システム・イベント監査、ID システムおよびアクセス・システムの診断、SNMP モニタリングなどの他のレポート機能の概要は、第 9 章「レポート」を参照してください。

コンポーネントのロギング・アクティビティは、個々の Access Server、Identity Server、Policy Manager、WebPass、WebGate、カスタム AccessGate、およびカスタム・プラグインのログ出力を指定することで制御できます。

ロギング・アクティビティを制御するパラメータは、各コンポーネントとともに格納されている構成ファイル内にあります。各コンポーネントのログ出力は、関連構成ファイルを手動で編集することでカスタマイズします。Identity Server の場合のみ、ID システム・コンソールで特定のログ・パラメータを設定するオプションがあります。

特定のコンポーネントにより生成されたログ・データは、次の一方または両方の宛先に送信すること、またはどちらにも送信しないことができます。

- データを生成するコンポーネントのルート・インストール・ディレクトリの下ディレクトリ・ツリーに格納されているログ・ファイル。
- コンポーネント・ロギング・データをホストしているマシンのシステム・ファイル（複数のコンポーネントが同じホストに存在する場合は、すべてのコンポーネントがそのマシン上のシステム・ログ・ファイルにデータを送信できます）。

便宜上、ロギングを通じてレポート可能な何千ものプログラム・イベントおよび状態が、8 レベルのピラミッド型階層に分類されます。最上位レベルの「致命的」カテゴリには、通常はコンポーネントを強制終了する約 60 の致命的なイベントが含まれます。ピラミッドの最下部にある「トレース」レベルでは、約 900 の Oracle Access Manager API コールおよび 150 のサード・パーティ API コールとそれらの結果がレポートされます。ほとんどの場合、これらのトレース・レベル・メッセージは、開発者およびプラグインのプログラマにとってのみ意味があります。

ログ・レベル

ロギング機能では、1 つ以上の詳細レベルでロギング・データを収集できます。各レベルは個別にアクティブ化されるため、隣接していないレベルからデータを収集できます。

次の表に、ロギングに対してアクティブ化するレベルを設定するために LOG_THRESHOLD_LEVEL パラメータで使用される 8 つの階層レベルをリストします。詳細は、表 10-4 を参照してください。

この表の 9 番目のエントリである LOGLEVEL_ALL は、階層内の 8 つのレベルすべてを含みます。

表 10-1 ロギング・レベル

レベル	レポートされるイベント数	説明
LOGLEVEL_FATAL	> 60	このレベルではクリティカル・エラーがレポートされます。一般に、これらのイベントは重大であり、コンポーネントの終了の原因になります。
LOGLEVEL_ERROR	> 960	修正処理を必要とする可能性のあるイベントがログ・ファイルに記録されます。たとえば、エラーレベル・エントリは、コンポーネントが使用不能な場合に生成されます。エラー・ログ・エントリは、別のコンポーネントへの接続失敗など、一時的または自己修正可能な問題に対しても生成されることがあります。

表 10-1 ログ・レベル (続き)

レベル	レポートされる イベント数	説明
LOGLEVEL_ WARNING	> 1200	将来のある時点でエラーを引き起こす、または修正処理を必要とする可能性のある問題がログ・ファイルに書き込まれます。
LOGLEVEL_ INFO	> 400	正常に完了したアクションまたはコンポーネントの現在の状態 (たとえば、コンポーネントが初期化中の場合など) がログ・ファイルに書き込まれます。
LOGLEVEL_ DEBUG1	> 400	基本的なデバッグ情報がログ・ファイルに書き込まれます。通常は、このログ・レベルの情報は開発者にとってのみ意味があります。
LOGLEVEL_ DEBUG2	> 100	詳細な (またはめったに必要なにならない) デバッグ情報がログ・ファイルに書き込まれます。このログ・レベルは、Debug1 ログ・レベルで提供される情報を補強します。通常は、このログ・レベルの情報は開発者にとってのみ意味があります。
LOGLEVEL_ DEBUG3	> 900	大量のデバッグ情報 (またはコードの高コスト部分に関連するデータ) がログ・ファイルに書き込まれます。このレベルは、タイト・ループやパフォーマンスに敏感なファンクションのデバッグに役立ちます。通常は、このログ・レベルの情報は開発者にとってのみ意味があります。
LOGLEVEL_ TRACE	> 900 の Oracle Access Manager API、> 150 の サード・パー ティ API	このログ・レベルは、コード・パス実行のトレースまたはパフォーマンス・メトリックの取得に使用されます。この情報は、各コンポーネント・ファンクションのエントリ・ポイントおよび終了ポイントで取得されます。通常は、このログ・レベルの情報は開発者にとってのみ意味があります。
LOGLEVEL_ ALL	> 5000	この併合レベルには、8 つのレベルすべてのイベントおよび状態がすべて含まれます。 注意: LOGLEVEL_ALL を指定した場合でも、LOG_THRESHOLD_LEVEL が優先されるため、すべてのレベルでログギングがアクティブになるとはかぎりません。詳細は、 図 10-1 を参照してください。

ログ構成ファイルについて

ログ出力を制御するパラメータは、任意のプレーンテキスト・エディタで編集できる XML ベースのログ・ファイル内にあります。これらのファイルに対する変更は、即時に有効になります。

ログ構成ファイルのパス

コンポーネントをインストールすると、デフォルトのログ構成ファイルが次の場所に置かれます。

```
Component_install_dir\identity|access\oblix\config
```

Component_install_dir は、コンポーネントをインストールしているディレクトリです。

特定のコンポーネントの複数のインスタンス (たとえば、複数の Identity Server など) をインストールする場合、ログ構成ファイルはインスタンスごとにインストールされます。

重要: コンポーネントがログ構成ファイルを検索できるようにするために、デフォルト・パスは変更しないでください。

ログ構成ファイルはログ・データ・ファイルと異なります。ログ・データ・ファイルの詳細は、表 10-6 を参照してください。

ログ構成ファイル名

次の表に、各コンポーネント・タイプのログ構成ファイルの名前をリストします。コンポーネントがこのファイルを検索できるようにするために、デフォルト名は変更しないでください。

表 10-2 コンポーネントのログ構成ファイル名

コンポーネント	ロギング構成ファイル名
Access Server	oblog_config.xml
Identity Server	oblog_config.xml
Policy Manager	oblog_config_am.xml
WebGate	oblog_config_wg.xml
WebPass	oblog_config_wp.xml
Access Manager SDK (カスタム AccessGate)	oblog_config.xml

ログ構成ファイルの変更

特定のコンポーネントに関連付けられているログ構成ファイルで設定されるパラメータによって、そのコンポーネントについてログに記録される情報のタイプ、データの送信先、および場合によってはログに使用される書込みバッファのサイズとターゲット・ログ・ファイルのローテーション方法が決定されます。

すべてのコンポーネントについて、ログ構成ファイルの XML 文をプレーン・テキスト・エディタで編集します。Identity Server の場合のみ、構成ファイル内の AUTOSYNC パラメータがあらかじめデフォルト値の True に設定されている場合は、ID システム・コンソールでログ・ファイル内の構成パラメータを変更できます。詳細は、10-15 ページの「ID システム・コンソールでのログの構成」を参照してください。

埋込みコメントについて

インストール時に、各ログ構成ファイルには、ログ出力を制御するために設定したパラメータを説明する大量の埋込みコメントが含まれています。1 行または複数行にまたがるコメントは、左の山カッコ、感嘆符および 2 つのダッシュに続く 2 つの空白 ("<!-- ") から開始します。コメントは、2 つの空白に続く 2 つのダッシュ、感嘆符および右の山カッコ (" --!>") で終了します。

ID システム・コンソールを使用してコンポーネントのログ・パラメータを変更し、これらの変更をコミットした場合、そのコンポーネントに関連付けられている構成ファイルは埋込みコメントなしでディスクに記録されます。これらのコメントの有無は、ロギングにはまったく影響しません。単にログ構成ファイルの手動編集をガイドする目的で組み込まれています。

どのような場合でも、元のロギング構成ファイルの読取り専用の複製を開くことで、元のコメントを表示できます。この複製の名前は "oblog_config_original.xml" で、次のディレクトリにあります。

```
Identity_Server_install_dir/oblix/config
```

IdentityServer_install_dir は、Identity Server のルート・インストール・フォルダです。

次のリスティングは、コメントが埋め込まれた典型的なログ構成ファイルを示しています。埋込みコメントのないログ・ファイルの例は、例 10-7 を参照してください。

例 10-1 デフォルトのログ構成ファイル（埋込みコメントあり）

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!--===== -->
<!--===== -->
<!--NetPoint Logging Configuration File -->
<!-->
<!--Changes to this file to take effect upon saving the file. -->
<!-->
<!-->
<!--===== -->
<!--===== -->
<!--Set the Log Threshold -->
<!-->
<!--The log Threshold determines the amount of information to log. -->
<!--Selecting a lower level of logging includes the information -->
<!--logged at the higher levels. For example, LOGLEVEL_ERROR -->
<!--includes the information collected at LOGLEVEL_FATAL. -->
<!-->
<!--Choices are: -->
<!--LOGLEVEL_FATAL - serious error, possibly a program halt. -->
<!--LOGLEVEL_ERROR - a transient or self-correcting problem. -->
<!--LOGLEVEL_WARNING - a problem that does not cause an error. -->
<!--LOGLEVEL_INFO - reports the current state of the component. -->
<!--LOGLEVEL_DEBUG1 - basic debugging information. -->
<!--LOGLEVEL_DEBUG2 - advanced debugging information. -->
<!--LOGLEVEL_DEBUG3 - logs performance-sensitive code. -->
<!--LOGLEVEL_TRACE - used when you need to trace the code path -->
<!--execution or capture metrics. Includes all previous levels. -->
<!-->
<!--If you do not specify a threshold, the default is WARNING. -->
<!-->
<!--In addition to specifying a threshold, you need to specify -->
<!--if changes that you make to the logging configuration in -->
<!--the GUI overwrite the settings in this file. The -->
<!--AutoSync parameter accomplishes this. This parameter takes a -->
<!--value of True or False. If set to True, changes made in the -->
<!--GUI overwrite changes in this config file. If False, changes -->
<!--made in the GUI are only in effect until the server is -->
<!--stopped or restarted. The default is True. -->
<!-->
<!-->
<CompoundList xmlns="http://www.oblix.com" ListName="logframework.xml.staging">
  <SimpleList>
    <NameValPair ParamName="LOG_THRESHOLD_LEVEL" Value="LOGLEVEL_WARNING" />
    <NameValPair ParamName="AUTOSYNC" Value="True" />
  </SimpleList>
<!-->
<!-->
<!--===== -->
<!--===== -->
<!--Configure the Log Level -->
<!-->
<!-->
<!--To configure a log level, you specify a name for the -->
<!--configuration (for instance, MyErrorLog1) and -->
<!--the log level that you are configuring. You can create -->
<!--more than one configuration per log level if you want -->
<!--to output to more than one destination. You can output to -->
<!--the system log or to a file, as specified on -->
```

```

<!--the LOG_WRITER parameter. The value for the LOG_WRITER -->
<!--parameter may only be SysLogWriter, FileLogWriter or -->
<!--MPFileLogWriter. The MPFileLogWriter is a multi-process safe -->
<!--FileLogWriter. It should be used to log in webcomponents i.e -->
<!--WebGate, Policy Manager and WebPass loaded on multiprocess -->
<!--web servers like Apache and IPlanet(Unix) -->
<!-->
<!--If you do not specify an output destination, the default is -->
<!--SysLogWriter. -->
<!-->
<!--If outputting to a file, you also specify a file name and -->
<!--other parameters. Default parameter values are: -->
<!--FILE_NAME: <installdir>/oblix/log/oblog.log -->
<!--BUFFER_SIZE: 32767 (number of bytes) -->
<!--MAX_ROTATION_SIZE: 5242880 (bytes, equivalent to 5MB) -->
<!--MAX_ROTATION_TIME: 86400 (seconds, equivalent to one day) -->
<!-->
<!--Configuring the log level does not ensure that the data is -->
<!--actually collected. Data collection for a log is -->
<!--determined by the LOG_THRESHOLD_LEVEL parameter, above, -->
<!--and the LOG_STATUS parameter in the log configuration. -->
<!-->
<!--If you do not provide a LOG_STATUS, the default for -->
<!--LOGLEVEL_FATAL, LOGLEVEL_ERROR, and LOGLEVEL_WARNING, -->
<!--is On. -->
<!-->
<!--This file contains several sample configurations that are -->
<!--enclosed in comments. To use them, remove the comments. -->
<!-->
    <CompoundList xmlns="http://www.oblix.com" ListName="LOG_CONFIG">
<!--Write all FATAL logs to the system logger. -->
        <ValNameList xmlns="http://www.oblix.com" ListName="LogFatal2Sys">
            <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_FATAL" />
            <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
            <NameValPair ParamName="LOG_STATUS" Value="On" />
        </ValNameList>
<!--Write all ERROR logs to the system logger. -->
        <ValNameList xmlns="http://www.oblix.com" ListName="LogError2Sys">
            <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_ERROR" />
            <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
            <NameValPair ParamName="LOG_STATUS" Value="On" />
        </ValNameList>
<!--Write all WARNING logs to the system logger. -->
        <ValNameList xmlns="http://www.oblix.com" ListName="LogWarning2Sys">
            <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_WARNING" />
            <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
            <NameValPair ParamName="LOG_STATUS" Value="On" />
        </ValNameList>
<!--Write all logs to the Oblix log file. -->
        <ValNameList xmlns="http://www.oblix.com" ListName="LogAll2File">
            <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_ALL" />
            <NameValPair ParamName="LOG_WRITER" Value="FileLogWriter" />
            <NameValPair ParamName="FILE_NAME" Value="oblog.log" />
        </ValNameList>
<!--Buffer up to 64 KB (expressed in bytes) of log entries before flushing to the file. -->
        <NameValPair ParamName="BUFFER_SIZE" Value="65535" />
<!--Rotate the log file once it exceeds 50 MB (expressed in bytes). -->
        <NameValPair ParamName="MAX_ROTATION_SIZE" Value="52428800" />
<!--Rotate the log file after 24 hours (expressed in seconds). -->
        <NameValPair ParamName="MAX_ROTATION_TIME" Value="86400" />
        <NameValPair ParamName="LOG_STATUS" Value="On" />
    </ValNameList>

```

```
</CompoundList>
</CompoundList>
```

ログ・ライターについて

コンポーネント固有のログの内容（言い換えると、レポートされるロギングのレベル）の制御に加えて、任意のログ・レベルで収集される出力を、選択したログ・ライターに送信できます。たとえば、致命的なエラーをシステム・ログに送信する一方で、選択したディスク・ファイルにトレースレベルのデバッグ情報を送信できます。

ログ・データの送信先は、ログ構成ファイルのログハンドラ定義にある LOG_WRITER パラメータの値を設定することで決定します。

提供されている3つの各ログ・ライターは、ログ・データを適切な形式に書式設定し、出力をシステム・ログやデータ・ファイルなどの特定の宛先に送信します。これらのログ・ライターについて、表 10-3 で説明します。

表 10-3 ログ・ライター

ライター	説明
SysLogWriter	<p>このライターは、ログに記録されるコンポーネントをホストするマシンのシステム・ログ・ファイルにデータを記録します。</p> <p>Windows マシンの場合、これは「マイ コンピュータ」、「管理」、「イベントビューア」、「アプリケーション」の順にナビゲートすることで表示できるアプリケーション・ログ・ファイルです。</p> <p>UNIX プラットフォームの場合、システム・ログ・ファイルの名前と場所は、システム管理者のマシンとプリファレンスに応じて異なります。ファイルの場所は、マシンの管理者に確認してください。</p> <p>通常、システム・ログ・ファイルには、Oracle Access Manager および他のアプリケーションとホスト・オペレーティング・システムによって記録されるイベント情報が含まれます。</p> <p>デフォルトでは、ロギング構成ファイルは致命的メッセージ、エラー・メッセージおよび警告メッセージがシステム・ファイルに送信されることを指定します。</p>
FileLogWriter	<p>このライターは、ディスク・ファイルに Access Server、Identity Server またはその他のシングルプロセス・アプリケーションのログ・データを記録する場合にお勧めします。</p> <p>このライターを使用して、ファイルの書き込みに使用されるバッファのサイズ、ファイルのローテーション・サイズおよびサイズと無関係なファイルのローテーション間隔を指定できます。</p> <p>FileLogWriter は、ログ・ファイルを開き、おおよそのファイル・サイズ制限またはファイル・ローテーション間隔に達するまでディスク書き込み用にファイルを開いたままにします。このため、複数のプロセスが同じログ・ファイルに書き込む必要がある状況には適していません。マルチプロセスの場合のロギングは、この表の MPFileLogWriter を参照してください。</p>
MPFileLogWriter	<p>このライターは、FileLogWriter に似ていますが、データをファイルに書き込むたびにログ・ファイルを開いて閉じる点が異なります。これにより、複数のプロセスが順番にファイルに書き込むことができます。ただし、これによってパフォーマンスが大幅に低下します。このため、MPFileLogWriter は、マルチプロセス Web サーバー（Apache など）あるいは Linux バージョンまたは Solaris バージョンの iPlanet Web サーバーにインストールされている AccessGate など、マルチプロセス・アプリケーションに関連するプロセスの一部で、FileLogWriter がロギング・データの記録に失敗する場合にのみ使用することをお勧めします。</p>

ログ構成ファイルの構造

ログ構成ファイルは、コンポーネントの起動時およびその他の主要ポイントで解析される標準形式に準拠します。パラメータの編集や、ログハンドラ定義と呼ばれる特定のセクションの追加または除去はできますが、ログ構成ファイルの基礎となる形式の変更はできません。変更すると、構成パラメータが解析不能になることがあります。

例 10-2 に、ログ構成ファイルの要素を例とともにリストします（省略されている内容の位置は省略記号で示されています）。デフォルトのログ構成ファイルのリスタリングは、例 10-1 または例 10-7 を参照してください。

例 10-2 ログ構成ファイルの構造（サンプル・コンテンツあり）

関連 XML バージョン（常に 1.0）およびエンコーディング形式（常に ISO-8559-1）を宣言する XML ファイル・ヘッダーです。このヘッダー文は、"<?" で開始し "?>" で終了する点がこのファイルの他の XML 文と異なります。

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
```

次の内容を含む複合リスト：

```
<CompoundList...>...</CompoundList>
```

ログ構成ファイルの関連 XML ネームスペース（開始タグ内）

```
xmlns="http://www.example.com"
```

複合リストの名前（開始タグ内）

```
ListName="logframework.xml.staging"
```

次の内容を含む単純リスト：

```
<SimpleList>...</SimpleList>
```

LOG_LEVEL_THRESHOLD パラメータの名前 / 値ペア

```
<NameValPair ParamName="LOG_THRESHOLD_LEVEL" Value="LOGLEVEL_WARNING" />
```

AUTOSYNC パラメータの別の名前 / 値ペア

```
<NameValPair ParamName="AUTOSYNC" Value="True" />
```

このレベルでは、1 つ以上の複合リストがログハンドラ定義と呼ばれます。それぞれに次の内容が含まれます。

```
<CompoundList...>...</CompoundList>
```

関連 XML ネームスペース（開始タグ内）

```
xmlns="http://www.example.com"
```

複合リストの名前（開始タグ内）

```
ListName="LOG_CONFIG"
```

それぞれ次の内容を含む 1 つ以上の値 / 名前リスト：

```
<ValNameList...>...</ValNameList>
```

関連 XML ネームスペース（開始タグ内）

```
xmlns="http://www.example.com"
```

値 / 名前リストの名前（開始タグ内）

```
ValNameList ListName="LogFatal2Sys"
```

次の3つの必須の名前 / 値ペア :

LOG_LEVEL パラメータ

```
<NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_FATAL" />
```

LOG_WRITER パラメータ

```
<NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
```

LOG_STATUS パラメータ

```
<NameValPair ParamName="LOG_STATUS" Value="On" />
```

LOG_WRITER パラメータに FileLogWriter または MPFileLogWriter を指定した場合にのみ意味のある次の4つの名前 / 値ペアのうちの0個以上。

FILE_NAME パラメータ

```
<NameValPair ParamName="FILE_NAME" Value="oblog.log" />
```

BUFFER_SIZE パラメータ

```
<NameValPair ParamName="BUFFER_SIZE" Value="65535" />
```

MAX_ROTATION_SIZE パラメータ

```
<NameValPair ParamName="MAX_ROTATION_SIZE" Value="52428800" />
```

MAX_ROTATION_TIME パラメータ

```
<NameValPair ParamName="MAX_ROTATION_TIME" Value="86400" />
```

XML 要素の順序について

XML タグ言語は、ブランチ上のリーフに対応する要素のリストを持つツリー型の構造を採用します。

特定のリスト内で、並列の要素は、要素自体が変更されず、最初に囲まれていたタグ内に完全に含まれているかぎり、任意の順序で提示できます。たとえば、例 10-3 と例 10-4 の名前 / 値リストは同等です。

例 10-3 名前 / 値リスト

```
<ValNameList xmlns="http://www.example.com" ListName="LogError2Sys">
  <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_ERROR" />
  <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
  <NameValPair ParamName="LOG_STATUS" Value="On" />
</ValNameList>
```

例 10-4 名前 / 値リスト

```
<ValNameList xmlns="http://www.example.com" ListName="LogError2Sys">
  <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
  <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_ERROR" />
  <NameValPair ParamName="LOG_STATUS" Value="On" />
</ValNameList>
```

同様に、ある特定のタグ内の属性（常にタグの山カッコ内の最初の要素である必要があるタグ名を除く）は、変更されておらず、最初に囲まれていたタグ要素内にあるかぎり、並べ替えることができます。例 10-5 と例 10-6 の名前 / 値リストの開始タグは同等です。

例 10-5 名前 / 値リストの開始タグ

```
<ValNameList xmlns="http://www.example.com" ListName="LogError2Sys">
```

例 10-6 名前 / 値リストの開始タグ

```
<ValNameList ListName="LogError2Sys" xmlns="http://www.example.com">
```

ロギング・レベルの制御

最大 4 つの相互に関連する要因により、ロギングが特定のログ・レベルで特定のコンポーネントに対してアクティブかどうかが決まります。これらの要因を次の表にリストします。

表 10-4 ロギングがアクティブかどうかを決定する要因

要因	重要性	説明
LOG_THRESHOLD_LEVEL	プライマリ	このパラメータは、単一の設定でログ出力を制限する便利な手段を提供します。表 10-1 で説明したログ・レベル階層内に絶対的なしきい値を設定することで、他のすべての設定に優先します。しきい値レベルよりもきめ細かいレベルについては、他の設定にかかわらずロギングが行われません。 Identity Server の場合のみ、構成ファイルと GUI ベース設定の関係の詳細は、10-15 ページの「ID システム・コンソールでのログの構成」を参照してください。
LOG_STATUS	セカンダリ	このパラメータは、ログしきい値レベルでオーバーライドされないかぎり、ロギングのオンとオフを切り替えます。詳細は、前の行を参照してください。
AUTOSYNC	セカンダリ	このパラメータが True に設定されている場合、ID システム・コンソールでロギング・パラメータに対して行った変更は、サーバーを再起動しなくても即時に有効になり、変更は構成ファイルに保存されます。 AUTOSYNC が False の場合も、ID システム・コンソールで行った変更は即時に有効になりますが、構成ファイルには保存されず、サーバーの再起動後に破棄されます。
ログ・ハンドラの物理的な位置	セカンダリ	10-10 ページの「ログ・ハンドラの優先順位について」を参照してください。

ログ・ハンドラの優先順位について

単一のログ構成ファイルには、単一のログ・レベルについて最大 3 つのログハンドラ定義を含めることができます。出力を 3 つの各ログ・ライターに送信する場合は、3 つの異なるログ・ハンドラが必要です。

これらのログ・ハンドラの LOG_STATUS 設定が競合する場合、ログ構成ファイルの物理的な終わりに最も近いログハンドラ定義の設定が最後に読み込まれます。したがって、この設定は、同じログ・レベルの前のすべてのログハンドラ定義の LOG_STATUS 設定に優先します。

ある特定のレベルについて最後に読み込まれたログハンドラ定義の LOG_STATUS パラメータの状態は、そのレベルのすべてのログハンドラ定義に対して有効になります。たとえば、ある特定のレベルを目的とする最初の 2 つのログ・ハンドラに対して LOG_STATUS を **Off** に設定しても、LOG_STATUS は構成ファイル内の 3 番目の最後のログ・ハンドラに対しては **On** になるため、ロギングは 3 つのハンドラすべてに対して行われます。

前に述べたように、ある特定のレベルの LOG_STATUS 設定は、そのレベルが現在の LOG_THRESHOLD_LEVEL よりもきめ細かい場合には、無意味になります。このような場合、このレベルでロギングをアクティブにすることはできないため、ログ・ハンドラ内の競合する設定とログ・ハンドラの出現順序はどちらも重要ではありません。

編集の有効化

ウォッチャ・スレッドは、ログ・ファイルに対する変更を1分（60秒）ごとに取得し、その変更を有効にします。サーバーを再起動する必要はありません。

注意： Identity Server の場合、ID システム・コンソールで行った編集は、oblog_config.xml ファイル内の AutoSync パラメータが True に設定されている場合にのみ、このファイルに書き込まれます。このパラメータが False に設定されている場合、以前の構成ファイル設定はサーバーの再起動後に有効になります。

ログ構成パラメータ

最低でも、各ログハンドラ定義は、表 10-5 にリストする 5 つのパラメータを設定します。

表 10-5 必須のログ構成ファイル・パラメータ

パラメータ	コメント
xmlns	現在のリストの関連 XML ネームスペースを指定し、ある特定のロギング構成ファイル内のすべてのログハンドラ定義に対して同一です。次に例を示します。 http://www.example.com
ListName	これらの名前は、ロギング構成ファイル内のすべてのリストに必須です。可能な場合は必ずデフォルトのリスト名を保持します。 新規ログハンドラ定義を作成する場合は、関連する名前 / 値リストに対して、エントリをロギング構成ファイル内の他のすべてのエントリと簡単に区別できる名前を選択するようにしてください。次に例を示します。 <i>WarningsAndAboveToSyslog</i> は、致命的メッセージ、エラー・メッセージおよび警告メッセージをシステム・ログ・ファイルに送信します。 <i>WarningsOnlyToFileLog128KBuffer</i> は、警告レベルのメッセージを 128KB バッファに従ってディスク・ファイルに送信します。 <i>TraceOnlyToMPRotateDaily</i> は、トレース・レベルのメッセージをマルチプロセス・ファイル・ライターに送信します。これにより、ディスクへの書き込みのたびにファイルが開かれて閉じられます。このファイルは、置換時のファイルのサイズに関係なく、毎日新しい（空の）ファイルで置換されます。
LOG_LEVEL	使用可能な 9 個のログ・レベル設定の 1 つを指定します。表 10-1 を参照してください。デフォルトのロギング構成ファイルは、「致命的」、「エラー」、「警告」の 3 つのレベルのロギングをアクティブにします。出力は、システム・ログとロギングを行っているコンポーネントのログ・データ・ファイルの両方に送信されます。
LOG_WRITER	特定のログハンドラ定義の出力を処理するログ・ライターを指定します。サポートされる選択肢のリストは、表 10-3 を参照してください。
LOG_STATUS	このパラメータは、次の項で説明するようにログ・ハンドラをオンまたはオフにします。

LOG_WRITER パラメータに対して FileLogWriter または MPFileLogWriter を指定した場合は、次の表で詳細に説明する 4 つのパラメータが意味を持ちます。最初のパラメータは必須になりますが、他の 3 つのパラメータはオプションです。

表 10-6 ログ・データ・ファイル構成パラメータ

パラメータ	説明	デフォルト
FILE_ NAME	<p>FileLogWriter または MPFileLogWriter に対してのみ使用されます。ロギング情報が書き込まれるファイルの名前（および場所）を表します。</p> <p>ファイル名に絶対パスを付加して、次のデフォルトの場所以外に格納できます。</p> <p><code>Component_install_dir\oblix\logs</code></p> <p><code>Component_install_dir</code> は、システム・イベントをロギングするコンポーネントのルート・インストール・ディレクトリです。</p> <p>ファイル名を指定しない場合は、デフォルトが適用されます。</p> <p>出力を FileLogWriter または MPFileLogWriter に送信する複数のログハンドラ定義を作成した場合は、各ケースに異なるファイル名を指定して、複数のハンドラが同じファイルに書き込みを試行しないようにします。この注意事項は、SysLogWriter にアクセスしているログ・ハンドラには適用されません。</p>	oblog.log
BUFFER_ SIZE	<p>このパラメータは、ログ・ファイルに書き込まれるログ・データの格納に使用されるバッファのサイズを表します。</p> <p>バッファ値を 0 に設定した場合、バッファリングは実行されません（バッファリングをオフにする機能は、システム障害の発生時に役立つことがあります）。</p> <p>システム障害が発生した場合は、致命的レベルのメッセージが常にログ・ファイルにフラッシュされます。</p> <p>バッファ・サイズを指定しない場合は、デフォルトが適用されます。</p>	65535 (64KB)
MAX_ ROTATION_ SIZE	<p>ログ・ファイルがこのサイズ（バイト単位）に達すると、ファイル名が変更され、名前変更されたファイルで最初に使用されていたファイル名で新規ファイルが作成されます。たとえば、"oblog.log" は "oblog.log 1081303126" になります。数字は、ファイル作成時の時刻を表します。</p> <p>このパラメータを指定しない場合は、デフォルトが使用されます。</p>	52428800 (512KB)
MAX_ ROTATION_ TIME	<p>最大ローテーション・サイズに達したかどうかにかかわらず、ログ・ファイル名が変更される時間間隔（秒単位）。</p> <p>時間でトリガーされる 2 回のファイル・ローテーションの間に最大ログ・ファイル・サイズに達しない場合、作成されるログ・ファイルに追加される数字は、ローテーション間隔の秒数だけ異なります。たとえば、"oblog.log. 1081389526" および "oblog.log. 1081303126" は 86,400 だけ異なります。これは、ロギング構成ファイルで設定されたローテーション間隔である 24 時間の秒数です。</p> <p>このパラメータを指定しない場合は、デフォルトが使用されます。</p>	86400 (1 日の秒数)

デフォルトのログ設定

各コンポーネントとともにインストールされるデフォルトのログ構成ファイルは、ログに記録されるイベントの階層の上位3つのレベル（「致命的」、「エラー」および「警告」）のみアクティブにします。

また、デフォルトでは、すべてのログ出力がシステム・ログに送信されます。

Windows マシンでは、「マイ コンピュータ」、「管理」、「イベント ビューア」、「アプリケーション」にナビゲートすることで、ロギングしているコンポーネントをホストしているマシンのシステム・ログを表示できます。ログに記録されるコンポーネントのシステム・イベント・エントリは、オペレーティング・システムおよび Oracle Access Manager 以外のアプリケーションに対してレポートされるシステム・イベントに散在します。

Solaris および Linux 環境では、システム・ログの場所はシステム構成ファイルに記録されます。このシステム構成ファイルの項目はマシンごとに異なります。このシステム・ファイルの名前と場所については、システム・ログの調査対象のコンポーネントをホストしているマシンの所有者に確認してください。

次のリスティングは、各コンポーネントとともにインストールされるデフォルトのログ構成ファイルの内容を表します。ファイルの基礎となる構造を明らかにするために、ファイルの実際の機能に影響しない埋込みコメントは削除されています。

例 10-7 デフォルトのログ構成ファイル（埋込みコメントなし）

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<CompoundList xmlns="http://www.example.com ListName="logframework.xml.staging">
  <SimpleList>
    <NameValPair ParamName="LOG_THRESHOLD_LEVEL" Value="LOGLEVEL_WARNING" />
    <NameValPair ParamName="AUTOSYNC" Value="True" />
  </SimpleList>
  <CompoundList xmlns="http://www.example.com" ListName="LOG_CONFIG">
    <ValNameList xmlns="http://www.example.com" ListName="LogFatal2Sys">
      <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_FATAL" />
      <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
      <NameValPair ParamName="LOG_STATUS" Value="On" />
    </ValNameList>
    <ValNameList xmlns="http://www.example.com" ListName="LogError2Sys">
      <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_ERROR" />
      <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
      <NameValPair ParamName="LOG_STATUS" Value="On" />
    </ValNameList>
    <ValNameList xmlns="http://www.example.com" ListName="LogWarning2Sys">
      <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_WARNING" />
      <NameValPair ParamName="LOG_WRITER" Value="SysLogWriter" />
      <NameValPair ParamName="LOG_STATUS" Value="On" />
    </ValNameList>
    <ValNameList xmlns="http://www.example.com" ListName="LogAll2File">
      <NameValPair ParamName="LOG_LEVEL" Value="LOGLEVEL_ALL" />
      <NameValPair ParamName="LOG_WRITER" Value="FileLogWriter" />
      <NameValPair ParamName="FILE_NAME" Value="oblog.log" />
      <NameValPair ParamName="BUFFER_SIZE" Value="65535" />
      <NameValPair ParamName="MAX_ROTATION_SIZE" Value="52428800" />
      <NameValPair ParamName="MAX_ROTATION_TIME" Value="86400" />
      <NameValPair ParamName="LOG_STATUS" Value="On" />
    </ValNameList>
  </CompoundList>
</CompoundList>
```

デフォルトのログ構成ファイルの解析

デフォルトのログ構成ファイルは、10-8 ページの「ログ構成ファイルの構造」に示した抽象構造に従います。

ファイルの上部近くにある単純なリストは、LOG_THRESHOLD_LEVEL を警告レベルに設定します。しきい値パラメータは他のすべてのパラメータに優先するため、このファイルの他の部分の設定にかかわらず、警告よりもきめ細かいレベルはログに記録されません。

単純なリストでは、AUTOOSYNC パラメータも True に設定されます。この設定により、ID システム・コンソールで設定した構成値が Identity Server の再起動後も保持されるように、この構成ファイルに保存できます。AUTOSYNC 設定はすべてのコンポーネントのデフォルト構成ファイルにあります。Identity Server に対してのみ意味があります。

ネストした複合リストには、4つのログハンドラ定義が含まれます。LogFatal2Sys という名前の最初のログハンドラ定義は、この定義の影響を受ける LOG_LEVEL を致命的レベルに設定し、LOG_STATUS を On に設定します。前に述べたように、この構成ファイルのしきい値レベルは致命的よりもきめ細かい警告であるため、この定義はオーバーライドされません。ログ出力はシステム・ログに書き込まれます。これは LOG_WRITER パラメータで指定されています。

LogError2Sys ログハンドラ定義は、エラー・レベル・メッセージをシステム・ログに送信します。エラーは現在のしきい値レベル（警告）より前にあるため、この定義が有効になります。

LogWarning2Sys 定義は、警告レベル出力をシステム・ログに送信します。前の2つのログハンドラ定義と同様に、この定義は現在の LOG_THRESHOLD_LEVEL パラメータによってオーバーライドされません。

最後のログハンドラ定義である LogAll2File は、8つのログ・レベルすべてからの出力を oblog.log という名前のディスク・ファイルに送信するように見えます。ただし、現在警告レベルに設定されている LOG_THRESHOLD_LEVEL が優先されるため、致命的レベル、エラー・レベルおよび警告レベルからの出力のみがログ・ファイルに記録されます。

図 10-1 デフォルトのログ構成ファイルでのログレベルのアクティブ化



LogAll2File からの出力は FileLogWriter に送信されるため、ファイル名、バッファ・サイズ、ローテーション・サイズおよびローテーション間隔を制御するパラメータはすべて有効になります。

要するに、デフォルトの構成ファイルは致命的メッセージ、エラー・メッセージおよび警告メッセージをシステム・ログと oblog.log というデフォルト・ログ・データ・ファイルの両方に送信します。

ID システム・コンソールでのログの構成

Identity Server の場合のみ、ID システム・コンソールで特定のログ設定を変更できます。または、ログ構成ファイルを手動で編集できます。

ログハンドラ定義を表示または変更する手順

1. ID システムのランディング・ページで、「ID システム・コンソール」リンクをクリックします。
すでにログインしている場合は、「ID システム・コンソール」タブをクリックします。
2. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」リンクをクリックします。
「すべての Identity Server をリスト」ページが表示されます。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成

ログイン・ユーザー: Master Admin

- パスワード・ポリシー
- ロスト・パスワード・ポリシー
- ディレクトリ・プロファイル
- Identity Server

すべてのIdentity Serverをリスト

名前	ホスト名	ポート
<input type="checkbox"/> ID Server 10.1.3 M3 staqh24 6021	staqh24	6021

追加 削除

3. アクティビティをログに記録する Identity Server のリンクをクリックします。
「Identity Server の詳細」ページが表示され、ページの下部にログハンドラ定義のリストが表示されます。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成

ログイン・ユーザー: Master Admin

- パスワード・ポリシー
- ロスト・パスワード・ポリシー
- ディレクトリ・プロファイル
- Identity Server

Identity Serverの詳細

名前	ID_Server_10.1.3_M3_staqh24_6021
ホスト名	staqh24
ポート	6021
デバッグ	オフ
デバッグ・ファイル名	/oblix/logs/debugfile.lst
トランスポート・セキュリティ	オープン
最大セッション時間(時間)	24

4. 「ログ・ハンドラ定義」表の上の「ログのしきい値」設定を調べます。これは現在の LOG_THRESHOLD_LEVEL を表します。
この設定を変更する場合は、ページの下部にある「変更」をクリックし、10-16 ページの「ID システム・コンソールからログしきい値を変更する手順」に進みます。それ以外の場合は、次の手順に進みます。

5. ログハンドラ定義の表で、検証または変更するログ・ハンドラのリンクをクリックします。
「ログ・ハンドラ定義を変更します。」ページが表示されます。このページで、表 10-5 で説明した値を指定できます。「出力先」フィールドで「ファイル」を指定した場合は、表 10-6 で説明したフィールドに入力する必要があります。

表 10-6 にリストしたように、ログ・ファイル名、ログ・ファイルの最大サイズ、ログ・ファイル・ローテーション間隔およびログ・バッファの最大サイズのデフォルトを変更できます。

6. 「保存」をクリックします。

ID システム・コンソールからログしきい値を変更する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」をクリックします。
2. 設定を調べる Identity Server の名前をクリックします。
3. Identity Server の詳細ページの下部にある「変更」をクリックします。
4. リストを使用して、「ログのしきい値」を目的の値に設定します。
5. 「保存」をクリックします。

変更が即時に有効になります。ログ構成ファイル内で AUTOSYNC が True の場合は、変更がログ構成ファイルに書き込まれるため、サーバーの再起動後も変更が保持されます。

ログハンドラ定義を追加または削除する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」リンクをクリックします。
2. ログハンドラ定義を追加する Identity Server の名前をクリックします。
3. ページの下部にある「変更」をクリックします。
「Identity Server の変更」ページが表示されます。
4. 「ログ・ハンドラ定義」の下で、適切なアクションを実行します。
 - ログ出力構成を削除するには、適切なリンクの横のボックスをチェックし、「削除」をクリックします。
 - ログ・ライターを追加するには、「追加」をクリックします。

「追加」をクリックした場合は、「新規ログ・ハンドラ定義を追加します。」ページが表示されます。

5. 新規ログ・ライターの名前とログ・レベルを指定します。
6. 10-15 ページの「ログハンドラ定義を表示または変更する手順」で説明したように、ログ・レベルが現在のログしきい値レベル以上であることを確認します。

新規ログ・レベルが現在のしきい値レベルよりも低い場合は、10-16 ページの「ID システム・コンソールからログしきい値を変更する手順」で詳細に説明したように、しきい値レベルを新しいログ・レベル以下に設定します。

7. システム・ログ以外のファイルへの出力を選択する場合は、表 10-6 の説明に従ってファイル名とパスを指定する必要があります。
8. 「保存」をクリックします。

この章では、監査機能および ID システム・コンソールを使用してこれらの機能を構成する方法を中心に説明します。内容は次のとおりです。

- [監査について](#)
- [監査出力の考慮事項](#)
- [監査出力の制御](#)
- [監査要件](#)
- [データベースの監査のアーキテクチャ](#)
- [ファイルベース監査の設定](#)
- [データベース監査の設定](#)
- [監査レポートの設定](#)

注意：データベースの監査コンポーネントのインストールの詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

監査について

監査機能は、ポリシーおよびプロファイル設定、システム・イベント、および使用パターンに関連するデータを収集および提示します。Oracle Access Manager では、2 種類の監査レポートを生成できます。

- **静的:** これらのレポートは、Oracle Access Manager ディレクトリ・サーバーに格納されているポリシーおよびプロファイル情報から導出されます。

詳細は、11-4 ページの「[静的監査レポート](#)」を参照してください。

- **動的:** これらのレポートは、システム内のサーバーから収集されるアクセス・システム・イベントおよび ID システム・イベントから導出されます。

最も詳細なレベルでは、動的監査レポートは、システム・イベントがいつ何によってトリガーされたかを明らかにします。より上位のレベルでは、これらのレポートは、コンポーネントの負荷レベル、リソース・リクエスト・パターン、システム侵入の試行および全体的なシステム・パフォーマンスを明らかにできます。詳細は、11-4 ページの「[静的監査レポート](#)」を参照してください。

監査に加えて、Oracle Access Manager はロギング、SNMP モニタリングおよびその他のレポート機能もサポートします。詳細は、[第 9 章「レポート」](#)を参照してください。

監査出力の考慮事項

すべての動的監査レポートと一部の静的監査レポートは、ディスク・ファイル、リレーショナル・データベース、またはその両方に記録できます。一部の静的レポートは、グラフィカル・ユーザー・インタフェースを通じて制限された形式で表示することもできます。

監査セキュリティの考慮事項

データベース監査では、セキュリティの領域でファイル・ベースの監査に比べて次の利点があります。

- すべての監査情報は、データベースでサポートされている任意のセキュリティ方式で保護できる中央データベースに格納されます。

ファイルの監査オプションは、監査データを収集する各サーバー上のプレーンテキスト・ファイルにデータを記録します。これらのファイルは、データベースレベルのセキュリティによって保護されません。

警告: データベース・セキュリティをフルに利用するには、システム内のすべての Access Server と Identity Server に対してファイルの監査機能をオフにしてください。また、各サーバー・ホストの ODBC.ini ファイル（使用している場合）ではなく、ディレクトリ・サーバー上の RDBMS プロファイル内のデフォルトの監査データベース・ユーザー・アカウントにパスワードを格納する必要があります。

- データは、データベースに応じて ODBC または OCI でサポートされているトランスポート・セキュリティ方式を使用して監査データベースに送信できます。
- 監査データベースを使用して、Crystal Reports はセキュリティ関連の統計を生成できます。たとえば、特定の期間中に拒否されたリソース・リクエストの数を追跡したり、システムからロックされているユーザーのリストをまとめたりできます。
- データベースの監査は、Sarbanes-Oxley、Gramm-Leach-Bliley、HIPAA（1996 年の Health Information Privacy and Accountability Act）などの規制法令のコンプライアンス・レポートを支援できます。

監査パフォーマンスの考慮事項

データベースかファイルかにかかわらず、監査によって Oracle Access Manager システムのパフォーマンスが低下することがあります。監査の影響は次のように制御できます。

- 選択したサーバーに対してのみ監査をオンにします。

詳細は、11-36 ページの「各 Identity Server の監査を有効化および構成する手順」および 11-41 ページの「各 Access Server の監査を有効化および構成する手順」を参照してください。

- 選択したプロファイル属性、イベントおよび ID システム・アプリケーションに対してのみ監査をオンにします。

詳細は、11-38 ページの「監査のグローバル ID システム・イベントおよびプロファイル属性を指定する手順」および 11-39 ページの「監査する User Manager、Group Manager または Organization Manager イベントを指定する手順」を参照してください。

- データベース監査の再試行間隔を長くして、データベースへの接続が切断された場合に、接続が復元される前に失敗した書き込み試行を再送信することでサーバーがスラッシングを開始することがないようにします。

この間隔は、次のディレクトリにある `globalparams.xml` ファイル内の `DBAuditRetryInterval` パラメータで制御します。

`Component_install_dir\apps\common\bin`

`Component_install_dir` は、監査動作の制御対象とするサーバーのインストール・ディレクトリです。このパラメータは、監査データベースへのデータ書き込みの再試行を開始する前に待機する秒数を値として受け取ります。

- ファイルベース監査の場合のみ、監査バッファのサイズを増やします。

この手段により、監査機能がハード・ディスクにアクセスする回数が削減されます。詳細は、11-36 ページの「各 Identity Server の監査を有効化および構成する手順」および 11-41 ページの「各 Access Server の監査を有効化および構成する手順」を参照してください。

- ファイルベース監査の場合のみ、バッファ・フラッシュ間隔を長くします。

これにより、監査機能がディスクに書き込む回数が削減されますが、システム障害時に失われるデータ量は増えます。

警告：サーバーに障害が発生した場合は、致命的エラーのみファイルにフラッシュされます。障害の時点でバッファ内にあった他のすべての監査項目は失われます。したがって、バッファ・サイズを増やすかバッファ・フラッシュ間隔を長くすると、システム障害時に失われる可能性のある監査データの量が増えます。

静的監査レポート

静的監査レポートは、Oracle Access Manager ディレクトリ・サーバーに格納されているポリシーおよびプロファイル情報から生成されます。次の5種類の静的レポートを生成できます。

表 11-1 静的監査レポートのタイプ

レポート・タイプ	説明
ユーザー・アクセス権限レポート	指定した時点でユーザーまたはユーザーのグループがアクセスできるリソースのグローバル・リスト。これらは、フィルタ処理されたプロファイル問合せとも呼ばれます。詳細は、11-43 ページの「 ユーザー・アクセス権限レポートを作成および管理する手順 」を参照してください。
リソース・アクセス権限レポート	指定された時点で指定されたリソースまたはリソースのグループへのアクセスを認可されているユーザーのグローバル・リスト。これらは、フィルタ処理されたポリシー問合せとも呼ばれます。詳細は、11-43 ページの「 ユーザー・アクセス権限レポートを作成および管理する手順 」の手順を参照してください。
アクセス・テスト	指定されたユーザーまたはユーザーのグループが指定された時点で指定されたリソースにアクセスできるかどうかを検証する制限されたオンスクリーン表示。ランダムに定義されたリソースのグループへのアクセスを、前の2つのタイプのフィルタ処理された問合せでできるのと同じ方法でテストすることはできません。
アクセス・システム診断レポート	システム内の一部またはすべての Access Server のステータス情報を示すオンスクリーン表。これには、Access Server が接続されているディレクトリ・コンポーネントに関する詳細が含まれます。詳細は、11-5 ページの表 11-2 を参照してください。
ID システム診断レポート	システム内の一部またはすべての Identity Server のステータス情報を示すオンスクリーン表。これには、Identity Server が接続されているディレクトリ・コンポーネントに関する詳細が含まれます。詳細は、11-5 ページの表 11-2 を参照してください。

動的監査レポート

データを監査データベースに送信できるようにするには、ドメイン内のホストに次のいずれかのデータベースをインストールし、構成する必要があります。

- Oracle Access Manager サーバーがすべて Windows 上で稼働する環境では、Microsoft SQL Server。

詳細は、11-21 ページの「[SQL Server のインストールについて \(Windows\)](#)」を参照してください。

- Oracle Access Manager サーバーをホストしているコンピュータに、Oracle データベース・サーバーまたは Oracle データベース・サーバーと通信するように構成されている Oracle データベース・クライアントが含まれている環境では、Oracle Database。

Oracle Access Manager サーバーをホストしているコンピュータ上の Oracle データベース・クライアントは、Oracle データベース・サーバーとは異なるプラットフォームで実行できます。たとえば、Oracle Access Manager サーバーおよび Oracle データベース・クライアントを Linux ホストで実行し、Oracle データベース・サーバーを Windows ホストで実行することができます。

また、Crystal Reports プレゼンテーション・ソフトウェアを Oracle Access Manager ドメイン内の Windows マシンにインストールし、構成できます。詳細は、11-44 ページの「[Crystal Reports のインストール手順](#)」を参照してください。

監査出力の制御

各サーバーで収集される監査データのタイプと量を制御できます。たとえば、認証の成功ではなく認証の失敗を記録するようにマスター監査ルールを Access Server 上で構成できます。詳細は、11-42 ページの「[アクセス・システムの監査出力形式を変更する手順](#)」を参照してください。または、ログアウトまたはセッション期限切れの時刻ではなく各ユーザー・ログインの日時を記録するようにアプリケーション監査ポリシーを Identity Server 上で構成できます。詳細は、11-37 ページの「[ID システムの監査出力形式を変更する手順](#)」を参照してください。

データを監査データベースに送信する場合は、監査データを提示するように事前構成されている Crystal Reports テンプレートで収集した情報を表示できます。生成された監査レポートは、次のカテゴリに分かれます。

- グローバル・ビュー・アクセス
- 認証
- 認可
- アクティビティ
- ID 管理

詳細は、11-15 ページの「[監査レポートについて](#)」を参照してください。

監査オプションについて

すべての監査オプションは、[表 11-2](#) で詳細に説明するように Oracle Access Manager の構成ページで設定します。

表 11-2 監査オプションの設定場所

監査関連の機能	GUI での場所	有効範囲
ファイルベース監査およびデータベース監査を有効にし、個々の Identity Server 上の監査ファイル属性を変更します。	「ID システム・コンソール」、 「システム構成」、「Identity Server」、「ServerName」、「変更」 ServerName は、変更する Identity Server を指定します。	サーバーごと
日付書式、日付セパレータ、メッセージの書式、エスケープ文字、レコード・セパレータ、フィールド・セパレータなど、ファイルベース監査およびデータベース監査に使用されるデフォルト書式を変更します。 データベース監査を有効にするには、デフォルトのメッセージ書式文字列を置換する必要があります。 11-37 ページの「ID システムの監査出力形式を変更する手順 」を参照してください。	「ID システム・コンソール」、 「共通構成」、「マスター監査ポリシー」、「変更」	ID システムのファイルベース監査とデータベース監査に対してグローバル
他の属性を変更する場合は、Crystal Report テンプレートとリポジトリ設定の再構成が必要な場合があります。		
監査する ID システム・イベントを指定します。これには、ログインとログアウトの成功と失敗、およびパスワード管理が含まれます。	「ID システム・コンソール」、 「共通構成」、「グローバル監査ポリシー」、「変更」	ファイルベース監査とデータベース監査、および ID システムのすべてのアプリケーションに対してグローバル

表 11-2 監査オプションの設定場所（続き）

監査関連の機能	GUI での場所	有効範囲
RDBMS プロファイルおよび関連データベース・インスタンスを作成または変更します（これらはデータベース監査に対してのみ必要です）。	「ID システム・コンソール」、 「システム構成」、「ディレクトリ・プロファイル」、「RDBMS プロファイルの構成」、「変更」 または 「アクセス・システム・コンソール」、「システム構成」、「サーバー設定」、「RDBMS プロファイルの構成」、「変更」	データベース監査に対してのみグローバル
オンスクリーン診断表示に含める Identity Server を指定します。 注意： 「診断」 ページに特定のサーバーの現在のステータスが表示されるようにするには、「診断」画面にアクセスする前にログインまたはユーザー検索を試行することにより、そのサーバーへの接続を確認します。	「ID システム・コンソール」、 「システム構成」、「診断」	グローバル（ID システムの場合のみ）またはサーバー
「検索」、「プロファイルの表示」、「プロファイルの変更」、「ロケーションの表示」、「ロケーションの変更」、「代替権限」、「ワークフロー」、「構成」、「非アクティブなユーザー」、「再アクティブ化されたユーザー」、「作成されたユーザー」、「削除されたユーザー」および「ワークフロー継続時間」の各イベントに対して監査成功および監査失敗データの収集をアクティブにします。	「ID システム・コンソール」、 「User Manager 構成」、「監査ポリシー」、「変更」	グローバル（User Manager レポートの場合のみ）
「検索」、「プロファイルの表示」、「プロファイルの変更」、「グループの表示」、「グループ・メンバーの表示」、「グループの拡張」、「グループのサブスクライブ」、「ワークフロー」、「構成」および「ワークフロー継続時間」の各イベントに対して成功データおよび失敗データの収集をアクティブにします。	「ID システム・コンソール」、 「Group Manager 構成」、「監査ポリシー」、「変更」	グローバル（Group Manager レポートの場合のみ）
「検索」、「プロファイルの表示」、「プロファイルの変更」、「包含プロファイル」、「コンテナ制限」、「ロケーションの表示」、「ロケーションの変更」、「ワークフロー」、「構成」および「ワークフロー継続時間」の各イベントに対して成功および失敗データの収集をアクティブにします。	「ID システム・コンソール」、 「Org. Manager 構成」、「監査ポリシー」	グローバル（Organization Manager レポートの場合のみ）
ファイルベース監査およびデータベース監査を有効にし、個々の Access Server 上の監査ファイル属性を変更します。	「アクセス・システム・コンソール」、「アクセス・システム構成」、「Access Server 構成」、「ServerName」、「変更」 ServerName は、変更する Access Server を指定します。	サーバーごと

表 11-2 監査オプションの設定場所 (続き)

監査関連の機能	GUI での場所	有効範囲
RDBMS プロファイルおよび関連データベース・インスタンスを作成または変更します (これらはデータベース監査に対してのみ必要です)。	「アクセス・システム・コンソール」、「システム構成」、「サーバー設定」、「RDBMS プロファイルの構成」、「作成」 (または「変更」) または 「ID システム・コンソール」、「システム構成」、「ディレクトリ・プロファイル」、「RDBMS プロファイルの構成」	グローバル (ファイルベース監査とデータベース監査の両方)
監査イベント (認証および認可の成功と失敗)、監査イベント・マッピング、日付書式、エスケープ文字、監査レコード形式およびキャッシュ書式設定を扱うマスター監査ルールを作成または変更します。 データベース監査を有効にするには、デフォルトの監査レコード書式文字列を置換する必要があります。詳細は、11-42 ページの「 アクセス・システムの監査出力形式を変更する手順 」を参照してください。 他の属性を変更する場合は、Crystal Report テンプレートとリポジトリ設定の再構成が必要な場合があります。	「アクセス・システム・コンソール」、「アクセス・システム構成」、「共通情報の構成」、「マスター監査ルール」、「変更」	グローバル (アクセス・システムのファイルベース監査とデータベース監査の両方)
オンスクリーン診断表示に含める Access Server を指定できます。 注意: 「診断」 ページに特定の Oracle Access Manager サーバーの現在のステータスが表示されるようにするには、「診断」画面にアクセスする前にログインまたはユーザー検索を試行することにより、そのサーバーへの接続を確認します。	「アクセス・システム・コンソール」、「システム管理」、「診断」	グローバル (アクセス・システムの場合のみ) またはサーバー
ユーザー・アクセス権限レポートを作成、変更および管理します。	「アクセス・システム・コンソール」、「システム管理」、「レポートの管理」、追加」または「変更」	サーバー

監査要件

画面への監査レポートの表示またはディスク・ファイルへの監査出力の送信を行うために、特別なコンポーネントをインストールする必要はありません。

データベースの監査は、特定の Oracle Access Manager システム構成に制限され、次の各項で詳細に説明するように特別なコンポーネントのインストールを必要とします。

データベースの監査の要件

データベース監査には、次の項で概説する特別なコンポーネントが必要です。インストールの詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

データベース監査のための特別なコンポーネント

データベースの監査を有効にするには、表 11-3 にリストするコンポーネントをインストールする必要があります。

表 11-3 データベース監査に必要な特別なコンポーネント

コンポーネント	インストール上の注意
Oracle Access Manager サーバー・ホスト	<p>監査データベースに接続されている Oracle Access Manager サーバーをホストしているすべてのマシンは、次のように同じプラットフォームで実行する必要があります。</p> <ul style="list-style-type: none"> ■ SQL Server を監査する場合は、Oracle Access Manager サーバー・プラットフォームを Windows Advanced Server 2003 Enterprise Edition にすることができます。 ■ Oracle Database を監査する場合は、プラットフォームを Windows Server 2003 Enterprise Edition または Linux にすることができます。 <p>最新のプラットフォーム・サポート情報を入手するには、11-9 ページの「サポートされているバージョンおよびプラットフォームへの更新」を参照してください。</p>
データベース・サーバー	<p>Oracle Access Manager ドメイン内のコンピュータに次のデータベース・サーバー・アプリケーションをインストールします。</p> <ul style="list-style-type: none"> ■ ODBC 接続タイプを使用している SQL Server の場合、監査データベースに接続しているすべてのサーバーが Windows ホストで稼働している環境では、データベース・サーバー・マシンで Microsoft SQL Server 2000、Standard、Enterprise または Developer エディションを実行できます。 ■ Oracle データベースの場合、Oracle Access Manager サーバーをホストしているコンピュータには、Oracle データベース・サーバー 9.2.0.7 または 10.1.0.5、あるいは Oracle データベース・クライアント 10.1.0.5 が含まれている必要があります。Oracle Access Manager サーバーをホストしているコンピュータに Oracle データベース・クライアント 10.1.0.5 が含まれている場合は、10.1.0.5 または 10.2.0.2 の Oracle データベース・サーバーを使用できます。 <p>最新のプラットフォーム・サポート情報を入手するには、11-9 ページの「サポートされているバージョンおよびプラットフォームへの更新」を参照してください。</p>
Crystal Reports	<p>ODBC データベースにアクセスできる Windows マシンに、Crystal Reports に加えて必要なパッチをインストールします。詳細は、11-44 ページの「監査レポートの設定」を参照してください。Crystal Reports ホストでは Windows を実行する必要があります。</p> <p>次の Crystal Reports パッケージはテスト済です。</p> <p>Crystal Reports 9.22a、Advanced Edition、patch = CR90DBEXWIN_EN_200403</p>

表 11-3 データベース監査に必要な特別なコンポーネント (続き)

コンポーネント	インストール上の注意
ODBC ドライバ	SQL Server を使用する場合は、追加のデータベース・ドライバをインストールする必要はありません。
OCI (Oracle Call Interface)	Oracle データベースで使用できる OCI 接続タイプは、Oracle Access Manager ライブラリにバンドルされています。このタイプの接続に追加の構成は不要です。

サポートされているバージョンおよびプラットフォームへの更新

この統合に対してサポートされている最新のバージョンおよびプラットフォームを確認するには、次のように Metalink を参照してください。

Metalink で情報を表示する手順

1. 次の URL に移動します。
`http://metalink.oracle.com`
2. 「Certify」タブをクリックします。
3. 「View Certifications by Product」をクリックします。
4. 「Application Server」オプションを選択し、「Submit」をクリックします。
5. 「Oracle Application Server」を選択し、「Submit」をクリックします。

データベースの監査のアーキテクチャ

ODBC 接続タイプを使用している場合は、すべての Identity Server および Access Server が Windows で実行されている必要があります。Linux で実行されている Identity Server または Access Server がある場合は、OCI 接続タイプのみ使用できます。環境の詳細は、『Oracle Access Manager インストレーション・ガイド』で説明されているようにデータベース監査コンポーネントをインストールした人に確認してください。

次の図に、1 台以上のホスト・マシン上に Oracle Access Manager サーバー、別のホスト上に OCI または ODBC 準拠のデータベース・サーバー、さらに別のホスト上に Crystal Reports アプリケーションがある分散環境を示します。

より単純なデプロイでは、Oracle Access Manager システム全体とすべてのデータベース監査コンポーネントを 1 台の Windows コンピュータにインストールできます。単一ホスト・シナリオでは、Oracle データベースを ODBC とともにインストールする場合、ODBC データ・ソース定義の 1 つの表 (1 つの ODBC.ini ファイル) のみホストに必要です。

図 11-1 および図 11-2 に、データベースの監査を有効にするためにインストールおよび構成するコンポーネントを示します。

図 11-1 に、4 台のホスト・マシンに分散されている SQL Server 上のデータベースの監査アーキテクチャを示します。この構成では、すべての Access Server および Identity Server が Windows 上で稼働し、データベースが Windows 上で実行されている必要があります。LDAP サーバーは必ずしも Windows ベースにする必要はありません。

図 11-1 データベースの監査のアーキテクチャ : SQL Server

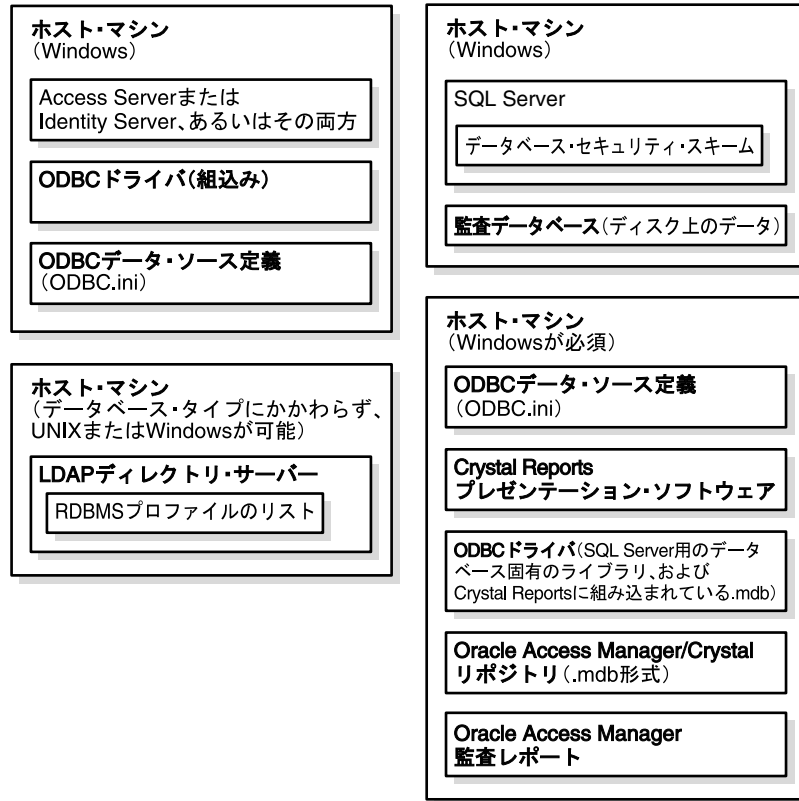
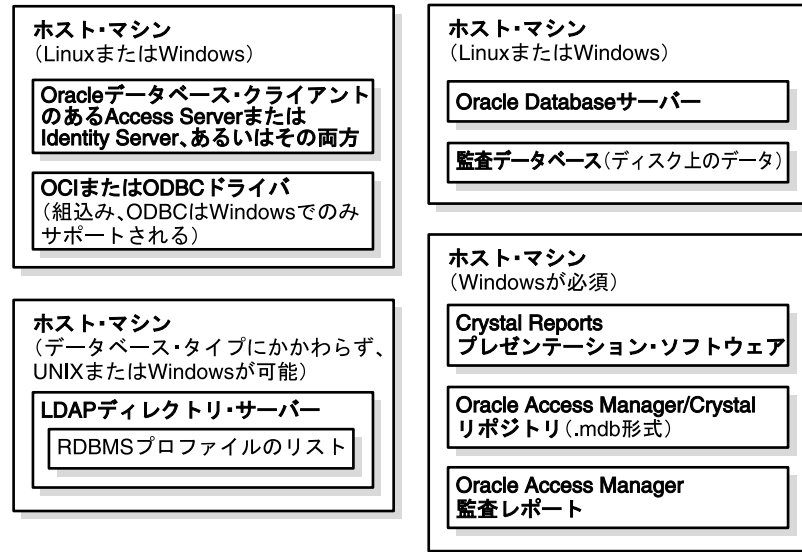


図 11-2 に、Oracle データベースを使用して監査するためのアーキテクチャを示します。示されているように、Windows システムは OCI または ODBC をホストでき、Linux システムは OCI をホストできます。LDAP ディレクトリは Windows または Linux で実行できます。OCI または ODBC データ・ソース定義、ODBC ドライバおよび Oracle Access Manager 監査レポートと Crystal リポジトリには、異なるホストを使用できます。

図 11-2 データベースの監査のアーキテクチャ : Oracle Database



OCI 設定について

OCI 接続タイプを使用する Oracle データベースを監査している場合、追加の構成はほとんど必要ありませんが、1 つの例外があります。ユーザーは、環境変数 ORACLE_HOME を設定する必要があります。

ODBC データ・ソース定義について

ODBC データ・ソース定義は、Oracle Access Manager サーバーや Crystal Reports などのクライアント・アプリケーションが SQL Server または Microsoft Access (.MCPO) 用に書式設定された ODBC 3.0 準拠のデータベースに接続するために必要な情報をすべてカプセル化します。

ODBC データ・ソース定義は、監査データベースに接続されているアプリケーションをホストする各 Windows コンピュータ上の ODBC.ini という名前のファイルに格納されます。このような ODBC データ・ソース定義のリストは、ある特定のマシンに 1 つのみ存在する必要があり、そのファイルは監査データベースに接続するすべてのアプリケーションによって共有されます。

- 一般にユーザーは、Windows 管理 GUI を使用してデータ・ソース定義を追加または変更します。

この GUI は多くの構成詳細を隠すため、ユーザーは ODBC.ini が存在すること、またその場所を意識する必要はありません。

- ODBC 接続タイプを使用する Oracle データベースを監査している場合、ユーザーは環境変数 ORACLE_HOME も設定する必要があります。このことは、監査されている Oracle Access Manager コンポーネントのホスト・マシンに、別のマシン上の Oracle データベース・サーバーと通信するように構成されている Oracle データベース・クライアントが含まれている場合に当てはまります。Oracle Database サーバーが、監査されているコンポーネントと同じマシンに存在する場合、ユーザーは ORACLE_HOME を設定する必要はありません。

次の表に、データ・ソース定義内の最も重要な属性をリストします。

表 11-4 ODBC データ・ソース定義の重要属性

属性	説明
DSN (データ・ソース名)	<p>特定のデータ・ソースにアクセスするすべてのクライアントに対する一意のデータ・ソース定義を識別します (DSN という用語は、ODBC データ・ソース定義全体を示すために間違っ使用されることがあります)。</p> <p>DSN は、Oracle Access Manager 環境内で一意である必要があります。さらに、特定の DSN を参照しているすべての ODBC.ini ファイルおよび RDBMS プロファイルには、ログイン名、パスワード、データベースなど、その DSN に関連する同一情報が含まれている必要があります。</p>
ユーザー	<p>ODBC データ・ソースのアクセスおよび変更を認可されたデータベース・ユーザー・アカウントを識別します。Oracle Access Manager サーバーまたは Crystal Reports アプリケーションは、データ・ソースにアクセスする必要がある場合に、このアカウントを使用してデータベース・セキュリティ・スキームに資格証明を提供します。</p> <p>SQL Server の場合、デフォルトのユーザー・アカウントは、システム管理者を意味する "sa" です。</p>
パスワード	<p>これは、「ユーザー名」で指定されたアカウントに関連付けられているパスワードです。このパスワードは、監査データベースのデフォルト・ユーザー・アカウントで指定し、RDBMS プロファイル、または監査データベースに接続している各 Oracle Access Manager サーバー上の ODBC.ini ファイル内の ODBC データ・ソース定義でもう一度指定します。</p> <p>ODBC データ・ソース定義と RDBMS プロファイルの両方でパスワードを指定する場合、ODBC データ・ソース定義はパスワード文字列を暗号化されていない形式で各 Oracle Access Manager ホストの ODBC.ini に格納し、RDBMS プロファイルは文字列を暗号化された形式で Oracle Access Manager LDAP ディレクトリ・サーバーに格納することに注意してください。</p>
データベース	<p>これは、ターゲット・データ・ソースの名前であり、データベースの監査機能では次のいずれかです。</p> <ul style="list-style-type: none"> ■ Oracle Access Manager 監査データを含むデータベースの名前 ■ .gif イメージ・ファイルを含む Crystal リポジトリの Microsoft Access データベース (.mdb ファイル) および監査情報を提示するために事前に構成されている Crystal Report テンプレートで使用される SQL 互換の問合せ
サーバー	<p>これは、RDBMS サーバー (SQL Server) が存在するマシンの名前です。</p>
ポート	<p>これは、RDBMS サーバーが着信リクエストをリスニングするポートです。</p>
ドライバ	<p>ローカル・マシン上の ODBC ドライバ・ライブラリへの完全修飾パスです。</p>
説明	<p>データ・ソース定義の識別に役立つ詳細です。</p>

ODBC ドライバについて

ODBC ドライバ・ライブラリは、接続先のデータベース・サーバーのタイプおよびドライバがインストールされているプラットフォームのタイプに固有です。

各 ODBC ドライバは、監査データベースへの接続を容易にするライブラリを提供します。

ODBC ドライバは、監査データベースに接続する Oracle Access Manager サーバーをホストしているマシンごとに存在する必要があります。Access Server と Identity Server の両方が同じマシンに存在する場合、そのホストには単一の ODBC ドライバのみ必要です。

Windows ODBC ドライバについて

デフォルトでは、Windows は SQL Server の ODBC ドライバを %Windows%\System32 ディレクトリにインストールします。このドライバは、「スタート」、「プログラム」、「管理ツール」、「データ ソース (ODBC)」にナビゲートすることで起動する ODBC データ・ソース・アドミニストレータを使用してアクセスできます。

ODBC データ・ソース・アドミニストレータの「About」タブには、ドライバのバージョン番号が表示されます。なんらかの理由で、インストールされているバージョンが 3.5 より低い場合、またはドライバが損傷しているか存在しない場合は、次の Web サイトからダウンロードできます。

<http://www.microsoft.com/odbc>

自己インストール・ファイルは odbc35in.exe という名前です。

データベース監査用の RDBMS プロファイルについて

RDBMS プロファイルは、すべての Identity Server および Access Server が監査データを送信する監査データベースの定義です。RDBMS プロファイルは、フェイルオーバー時に使用するためのプライマリおよびセカンダリ・データベース・インスタンスに対して定義できます。

RDBMS プロファイルは、Oracle Access Manager ディレクトリ・サーバー上に存在し、そのディレクトリ・サーバーに接続されているすべての Access Server および Identity Server によってアクセスされます。RDBMS プロファイルは、アクセス・システム・コンソールまたは ID システム・コンソールで構成します。詳細は、11-32 ページの「[RDBMS プロファイルを作成する手順](#)」を参照してください。

一般に、レポート（静的レポート）と監査（動的レポート）が 1 つの RDBMS プロファイルを共有します。特定の機能（レポートや監査など）を使用するすべての Access Server および Identity Server は、同じ RDBMS プロファイルを使用する必要があります。

LDAP データベース・プロファイルは、サーバーおよび操作に固有です。これらは、Access Server および Identity Servers により共有できますが、必ずしも共有する必要はありません。各 LDAP データベース・プロファイルが同じ LDAP サーバーおよび操作用に設定されていても、2 つ以上の Access Server または Identity Server がそれぞれ異なる LDAP データベース・プロファイルを使用できます。

ODBC 接続タイプを使用するデータベースのプロファイルについて

各 RDBMS プロファイルは、ODBC または OCI 接続タイプに対して構成できます。RDBMS プロファイルには、Access Server または Identity Server と監査データベース間の接続を構成するデータベース・インスタンス定義が含まれます。ODBC 接続タイプの場合、データベース・インスタンスには、監査データベースへの接続に使用される ODBC データ・ソース定義の DSN (データ・ソース名) が含まれます。これには、表 11-4 にリストされている属性のコピーも含まれます。

同じ DSN は、監査データベースに接続されている Access Server または Identity Server をホストする各マシンの ODBC.ini ファイル内に出現します。RDBMS プロファイル・サーバーに格納されている DSN に関連する詳細は、Oracle Access Manager システム全体の ODBC.ini ファイル内のその DSN の各インスタンスに関連付けられている詳細と完全に一致する必要があります。

関連付けられている属性が一致しない場合は、RDBMS プロファイルに記録されている USER および PASSWORD の値が、ODBC.ini に格納されている対応する値に優先します。一方、ODBC.ini に格納されている DATABASE およびその他の属性は、RDBMS プロファイル内の対応する値に優先します。1 つの場所にある値が他の場所に格納されている値で上書きされることはありません。

OCI 接続タイプを使用するデータベースのプロファイルについて

各 RDBMS プロファイルは、ODBC または OCI 接続タイプに対して構成できます。RDBMS プロファイルには、Access Server または Identity Server と監査データベース間の接続を構成するデータベース・インスタンス定義が含まれます。OCI 接続タイプの場合は、データベース・インスタンス定義でグローバル・データベース名 (GDN) を指定します。データベース・インスタンスには、表 11-4 にリストされている属性のコピーも含まれます。

監査データベースについて

監査データベースは、システム内のすべての Access Server および Identity Server からデータを収集します。Oracle Access Manager では、次のデータベースがサポートされます。

- Windows プラットフォームで稼働する SQL Server 上の ODBC 3.0 準拠データベース
- Windows および Linux マシンで稼働する ODBC 3.0 および OCI 準拠の Oracle Database

Crystal リポジトリについて

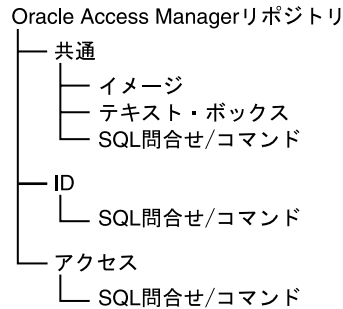
データベースの監査のコンテキストでは、orMap.ini ファイルを使用して Oracle リポジトリと Crystal リポジトリをリンクするため、この 2 つは同義です。11-46 ページの「[orMap.ini の編集手順](#)」の手順を参照してください。

このリポジトリは、次のリソースを含む Microsoft Access 形式 (.mdb) のデータベースです。

- 監査レポートで使用される .gif ファイル
- 監査レポートで使用される SQL 問合せおよびコマンド
- カスタム・ファンクション
- 監査レポートに一貫性のあるルック・アンド・フィールを与えるテンプレート
- サンプル・レポート

図 11-3 に、リポジトリ内の共通リソース、ID リソースおよびアクセス・リソースの編成を示します。

図 11-3 リポジトリ内のリソースの編成



監査レポートについて

表 11-4 で、監査レポートについて説明します。

表 11-5 監査レポート内のコンテンツ・タイプ

監査データ・タイプ	監査レポート・タイプ	説明
認証統計	認証 / 動的	特定のサーバー上または Oracle Access Manager システムで特定の期間中に発生した認証の成功および失敗の数。
認可統計	認可 / 動的	特定のサーバー上または Oracle Access Manager システムで特定の期間中に発生した認可の成功および失敗の数。
ユーザー別のアクセス失敗	認可 / アクティビティ / 動的	特定の期間中に失敗した特定のユーザーからの認可リクエストの数。
リソース別のアクセス失敗	認可 / アクティビティ / 動的	特定の期間中に失敗した特定のリソースに対する認可リクエストの数。
アクセス権限	フィルタ処理された問合せ / 静的	<p>2 種類のアクセス権限レポートがサポートされています。</p> <ul style="list-style-type: none"> 1 つ以上のリソースを含むリストへのアクセスを許可されているすべてのユーザー。 1 人以上のユーザーを含むリストからアクセス可能なすべてのリソース。 <p>この情報は、ファイルまたはデータベースに記録されると、ユーザー・アクセス権限レポートまたは拡張フィルタ処理プロファイル問合せと呼ばれるようになります。詳細は、11-43 ページの「ユーザー・アクセス権限レポートを作成および管理する手順」の手順を参照してください。</p> <p>より単純な問合せが GUI を通じて表示されると、それらの問合せはアクセス・テスター出力と呼ばれるようになります。</p> <p>このタイプの監査情報は静的です。Access Server または Identity Server からイベントごとに履歴的に収集されるのではなく、ディレクトリ・サーバーに格納されているポリシー情報から導出されます。</p>
ユーザー・プロファイル履歴	ID 管理 / 動的	すべてのユーザーのパスワード、ポリシー、プロファイルなどに対する変更です。

表 11-5 監査レポート内のコンテンツ・タイプ (続き)

監査データ・タイプ	監査レポート・タイプ	説明
グループ履歴	ID 管理 / 動的	特定の期間中にユーザーが追加または削除したグループのリストです。
失効したユーザー	ID 管理 / 動的	システムからロックアウトされたユーザーのリストです。
非アクティブなユーザー	ID 管理 / 動的	アクセス・アカウントが非アクティブ化されているユーザーのリストです。再アクティブ化されたユーザーのリストも生成できます。
パスワード変更	ID 管理 / 動的	特定の期間中にシステム全体で変更されたパスワードの数。
ユーザー・ステータス変更	ID 管理 / 動的	特定のユーザーが特定の期間中に追加されたグループ。
ID 履歴	ID 管理 / 動的	1人以上の個々のユーザーのパスワード、ポリシー、プロファイルなどに対する変更です。
ワークフロー実行時間	ID 管理 / 動的	特定の期間中にワークフローを完了するために要した平均および最大の時間です。

ファイルベース監査の設定

ファイルベース監査のオンおよびオフ、個々の Access Server または Identity Server によって生成された監査ファイルの名前と場所の変更は、Oracle Access Manager GUI を使用して行います。デフォルトでは、監査フラグはすべての Oracle Access Manager サーバーに対してオフになります。次の 2 つの手順では、それぞれ Identity Server と Access Server のファイルベース監査のアクティブ化と構成の手順を詳細に説明します。

各 Oracle Access Manager サーバーの監査フラグは個別にアクティブにする必要があります。

次の 3 つのカテゴリの監査設定のデフォルトを変更することもできます。

- **共通**: 詳細は、11-38 ページの「[監査のグローバル ID システム・イベントおよびプロファイル属性を指定する手順](#)」を参照してください。
- **Oracle Access Manager サーバー固有**: 詳細は、11-36 ページの「[各 Identity Server の監査を有効化および構成する手順](#)」および 11-41 ページの「[各 Access Server の監査を有効化および構成する手順](#)」を参照してください。
- **ID システム・アプリケーション固有**: 詳細は、11-39 ページの「[監査する User Manager、Group Manager または Organization Manager イベントを指定する手順](#)」を参照してください。

前のリストのカテゴリは、ファイルベース監査とデータベース監査の両方に適用されます。

Identity Server のファイルベース監査を構成する手順

1. ID システムのランディング・ページで、「ID システム・コンソール」をクリックします。
ID システムにすでにログインしている場合は、「ID システム・コンソール」タブをクリックします。
2. 「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」をクリックします。
3. Identity Server のリストで、変更するサーバーのリンクを選択します。
4. ファイルの監査設定を確認します。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 ログイン・ユーザー: Master Admin

- パスワード・ポリシー
- ロスト・パスワード・ポリシー
- ディレクトリ・プロファイル
- **Identity Server**
- WebPass
- サーバー設定
- 診断
- 管理者
- スタイル
- 写真

Identity Serverの変更

名前	ID_Server_10.1.3_M3_stagh24_6021
ホスト名*	staph24
ポート*	6021
デバッグ*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
デバッグ・ファイル名*	/oblix/logs/debugfile.lst
トランスポート・セキュリティ*	<input checked="" type="radio"/> オープン <input type="radio"/> 簡易 <input type="radio"/> 証明書
最大セッション時間(時間)*	24
スレッド数*	20
データベースの監査フラグ(監査オン/オフ)	<input checked="" type="radio"/> オフ <input type="radio"/> オン
ファイルの監査フラグ(監査オン/オフ)	<input checked="" type="radio"/> オフ <input type="radio"/> オン
監査ファイル名	
監査ファイル最大サイズ(バイト)	100000
監査ファイル・ローテーション間隔(秒)	7200
監査バッファ最大サイズ(バイト)	25000
監査バッファ・フラッシュ間隔(秒)	7200

表 11-6 に、ファイルの監査の構成パラメータを説明します。

表 11-6 ファイルの監査構成パラメータ

パラメータ	説明	デフォルト
ファイルの監査フラグ (監査オン / オフ)	ファイル機能を「オン」または「オフ」にするラジオ・ボタン。	オフ
監査ファイル名	<p>監査している Access Server または Identity Server の監査ファイルの絶対パスと名前を指定できます。</p> <p>次のように指定すると便利な場合があります。</p> <p><code>Component_install_dir\oblix\log\auditfile.lst</code></p> <p><code>Component_install_dir</code> は、Access Server または Identity Server のルート・インストール・ディレクトリです。</p>	[空白]
監査ファイルの最大サイズ	<p>このサイズ (バイト単位) にほぼ達すると、既存の監査ファイルが閉じられて次の名前に変更されます。</p> <p><code>AuditFileName.lst TimeStamp</code></p> <p><code>AuditFileName</code> は監査ファイルの名前で、<code>TimeStamp</code> は 1971 年 1 月 1 日からファイルが作成された時点までの秒数の数値表現です。デフォルトでは、<code>AuditFileName</code> は <code>AuditFile</code> です。</p> <p>同時に、<code>AuditFileName</code> という名前の新しい監査ファイルが作成され、入力用に開かれます。</p>	100000
監査ファイル・ローテーション間隔	<p>監査ファイル名が変更され、作成された新しい監査ファイルで置換される頻度 (秒単位)。</p> <p>時間ベースのローテーションは、監査ファイルの現在のサイズに関係なく行われます。詳細は、この表の前の行を参照してください。</p>	7200
監査バッファ最大サイズ (バイト)	この量の監査データ (バイト単位) がバッファに累積されると、バッファ全体がディスクに書き込まれます。	[空白]
監査バッファ・フラッシュ間隔	この秒数が経過すると、バッファ内のデータ量に関係なく監査バッファの内容が監査ファイルに書き込まれます。	7200

Access Server のファイルベース監査を構成する手順

1. アクセス・システムのランディング・ページで、「アクセス・システム・コンソール」のリンクをクリックします。

アクセス・システムにすでにログインして、Policy Manager で作業している場合は、ページの上にある「アクセス・システム・コンソール」リンクをクリックします。
2. 「アクセス・システム構成」タブをクリックし、左側のナビゲーション・ペインの「Access Server 構成」をクリックします。
3. 「Access Server 構成」ページのリストから、変更する Access Server を選択します。
4. 「Access Server の詳細」ページで、監査ファイル設定を確認します。

いずれかの設定を変更する場合は、ページの下部にある「変更」ボタンをクリックします。

5. 「Access Server の変更」 ページで、監査ファイル・パラメータを変更します。

ORACLE Access Administration

Policy Manager ヘルプ バージョン情報 ログアウト

システム構成 システム管理 **アクセス・システム構成**

ログイン・ユーザー: Master Admin

- Access Server のリスト
- Access Gate 構成
- 新規 Access Gate の追加
- Access Server 構成**
- 認証管理
- 認可管理
- ユーザー・アクセス構成
- 共通情報の構成
- ホスト識別子

Access Server の変更

名前	AccessServerQT
ホスト名*	dummy
ポート*	65001
デバッグ*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
デバッグ・ファイル名*	
トランスポート・セキュリティ*	<input checked="" type="radio"/> オープン <input type="radio"/> 簡易 <input type="radio"/> 証明書
最大クライアント・セッション時間(時間)*	24
スレッド数*	60
アクセス管理サービス*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
データベースの監査(オン/オフ)*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
ファイルの監査(オン/オフ)*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
監査ファイル名	
監査ファイルのサイズ(バイト)	0

データベース監査の設定

次に、データベース監査を設定するための上位レベルのタスクを示します。

タスクの概要：データベース監査の有効化

- Oracle Access Manager 環境を設定および検証します。

詳細は、11-20 ページの「データベース監査用のシステムの設定」を参照してください。

- RDBMS アプリケーション (SQL Server または Oracle データベース) をインストールおよび構成してから、Oracle Access Manager 監査データベースを作成および構成します。

詳細は、11-20 ページの「監査データベースの設定」を参照してください。

- データベース監査用に Oracle Access Manager を構成します。

OCI 接続タイプの場合は、RDBMS プロファイルを作成します。ODBC 接続タイプの場合、これには、ODBC データ・ソース定義および RDBMS プロファイルを作成することにより Oracle Access Manager サーバーが監査データベースに接続できるようにする処理が含まれます。ID システムとアクセス・システムの両方を監査用に構成し、検証する必要もあります。

詳細は、11-35 ページの「監査の構成」を参照してください。

- Crystal Reports をインストールおよび構成し、Oracle Access Manager 監査テンプレートが監査データベース情報を表示できることを確認します。

詳細は、11-44 ページの「監査レポートの設定」を参照してください。

データベース監査用のシステムの設定

データベースの監査機能を使用する前に、Oracle Access Manager システム内の Access Server および Identity Server ホストがすべて Windows で実行されているか、またはすべて Linux で実行されていることを確認する必要があります。

Oracle Access Manager 環境での混在プラットフォームの禁止は、データベースに接続する Oracle Access Manager サーバーをホストしているマシンおよびデータベース・サーバーをホストしているマシンにのみ適用されます。Oracle Access Manager LDAP サーバーをホストしているマシンは、Windows または Linux で実行できます。Crystal Reports をホストしているマシンは、使用されているデータベースのタイプにかかわらず、Windows を実行する必要があります。監査データベースに接続していない Oracle Access Manager サーバーは、任意のプラットフォームで実行できます。

監査データベースの設定

Oracle Access Manager 監査データベースは、SQL Server または Oracle Database で稼働している ODBC 3.0 準拠データベース、または OCI 準拠の Oracle Database です。

タスクの概要：監査データベースの準備

1. SQL Server をインストールしている場合は、11-21 ページの「[SQL Server のインストールについて \(Windows\)](#)」を参照してください。
2. データベース・サーバー上で Oracle Access Manager 監査データベースを作成および構成します。

11-22 ページの「[Windows 上の SQL Server: 監査データベースの作成手順](#)」、11-22 ページの「[Windows 上の Oracle Database: 監査データベースの作成手順](#)」または 11-22 ページの「[Linux 上の Oracle Database: 監査データベースの作成手順](#)」を参照してください。

Oracle データベースを作成している場合は、Unicode キャラクタ・セット (AL32UTF8) を指定します。

SQL Server インストール環境では、デフォルトで Unicode キャラクタ・セット UCS-2 を使用します。

各国語キャラクタ・セットとして「UTF-8」を選択します。

3. 監査およびレポート・スキーマを監査データベースにアップロードします。
11-23 ページの「[タスクの概要：監査スキーマのアップロード](#)」を参照してください。
4. 監査データベースにデータを送信する各 Oracle Access Manager サーバーで、ODBC データ・ソース定義 (システム DSN) を作成します。
11-29 ページの「[ODBC データ・ソース定義を作成する手順 \(Windows\)](#)」を参照してください。
5. Oracle Access Manager LDAP ディレクトリ・サーバーに RDBMS プロファイルを作成し、ディレクトリ・サーバーに接続している各 Access Server または Identity Server がホスト・マシン上の ODBC データ・ソース定義を認識できるようにします。
11-32 ページの「[RDBMS プロファイルを作成する手順](#)」を参照してください。
6. すべての Oracle Access Manager サーバーを再起動します。
11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Windows\)](#)」または 11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Linux\)](#)」を参照してください。

データベース・サーバーのインストール

システム内のすべての Oracle Access Manager サーバー・ホストが Windows を実行している場合は、SQL Server または Oracle Database をインストールします。すべての Oracle Access Manager サーバー・ホストが Linux を実行している場合も、Oracle Database をインストールできます。

SQL Server のインストールについて (Windows)

SQL Server 2000 の Standard Edition、Enterprise Edition または Developer Edition を使用できます。

SQL Server を使用する他の Oracle Access Manager 機能（たとえば、SharePoint Portal Server 統合）の実装を計画している場合、SQL インストール環境が各機能で指定されている最低要件を満たしていれば、監査機能は単一の SQL Server インストール環境をこれらの他の機能と共有できます。

Microsoft が提供している指示に従って SQL Server をインストールします。インストール・ウィザードにより、設定オプションの指定を求められます。ほとんどの場合は、ウィザード・ページを進むときにデフォルトを受け入れる必要があります。ただし、最初に次の表を確認して、デフォルトと異なる設定を入力します。

表 11-7 SQL Server インストールの特殊な設定

ウィザード・ページ設定	指定内容
autorun.exe の開始画面	「SQL Server 2000 Components」、 「Install Database Server」
インストール・ターゲット	「Local Computer」
インストール・オプション	「Create a new instance of SQL Server」
インストールのタイプ	「Server and Client Tools」
インスタンス名	「Default」
設定のタイプ	「Typical」
サービス・アカウント	「Use the same account for each service.Auto Start SQL User Service」
サービス設定	「Use Local System account」 ログイン ID またはユーザー名と呼ばれるデフォルトのログイン名は "sa" であり、「blank password」というラベルの付いたボックスが選択されている場合はパスワードを空白にできます。「blank password」が選択されていない場合は、任意のパスワードを指定できます。 どちらの場合も、ログイン名と関連パスワードを記録し、各 Oracle Access Manager サーバー・ホストで RDBMS プロファイルおよび ODBC データ・ソース定義を作成する際に正確に再現できるようにしてください。
認証モード	「Mixed Mode」

SQL Server をインストールした後で、11-22 ページの「[Windows 上の SQL Server: 監査データベースの作成手順](#)」に進みます。

監査データベースの作成

Oracle Access Manager 監査データベースを作成する手順は、SQL Server と Oracle Database のどちらを使用しているかによって異なります。

Windows 上の SQL Server: 監査データベースの作成手順

1. SQL Server をホストしているマシンで、次のようにナビゲートします。
「マイ コンピュータ」、「管理」、「サービスとアプリケーション」、「Microsoft SQL Servers」、
「hostname」
hostname は、SQL Server をホストしているマシンの Windows サービス名です。
2. 「コンピュータの管理」ウィンドウの左側のペインで、SQL Server がインストールされているマシンのホスト名の下にあるブランチで「データベース」を右クリックし、「新規データベース」をクリックします。
3. データベースの説明的な名前を選択し、「OK」をクリックします。
新規データベースを表すアイコンが、「コンピュータの管理」ウィンドウの右側のペインに表示されます。
4. 11-23 ページの「[監査スキーマのアップロード](#)」に進みます。

Windows 上の Oracle Database: 監査データベースの作成手順

1. Oracle Database サーバーを起動します。
2. 「スタート」、「プログラム」、「Oracle - OraDb10g_home1」、「Configuration and Migration tools」、「Database configuration assistant」をクリックすることにより、Database Configuration Assistant を起動します。
3. ウィザードでグローバル・データベース名を求められたら、名前を記録し、Oracle Access Manager の RDBMS プロファイルのデータベース・インスタンス定義でその名前を使用します。
4. 「初期化パラメータ」画面で、データベース・キャラクタ・セットとして「AL32UTF8」を選択し、各国語キャラクタ・セットとして「UTF8」を選択します。
5. 「[監査スキーマのアップロード](#)」に進みます。

Linux 上の Oracle Database: 監査データベースの作成手順

1. 次のディレクトリにある Oracle Database サーバーを起動します。
`ORACLE_HOME/bin/dbca`
2. Database Configuration Assistant を起動します。
3. ウィザードでグローバル・データベース名を求められたら、名前を記録し、Oracle Access Manager の RDBMS プロファイルのデータベース・インスタンス定義でその名前を使用します。
4. 「初期化パラメータ」画面で、データベース・キャラクタ・セットとして「AL32UTF8」を選択し、各国語キャラクタ・セットとして「UTF8」を選択します。
5. 「[監査スキーマのアップロード](#)」に進みます。

監査スキーマのアップロード

監査スキーマにより、Oracle Access Manager サーバーから監査データをインポートし、そのデータを Crystal リポジトリにエクスポートできます。データは Oracle Access Manager 監査レポートに表示されます。

タスクの概要：監査スキーマのアップロード

1. Oracle Access Manager 監査スキーマおよびサポートするリソースを Oracle Access Manager サーバー・ホストから Oracle Access Manager 監査データベース・ホストにコピーします。

コピー手順は、Windows 間転送と Linux 間転送のどちらを実行しているかに応じて異なります。詳細は、次の項を参照してください。

「監査およびレポート・スキーマを監査データベース・ホストにコピーする手順」

2. 監査およびレポート・スキーマを監査データベースにアップロードし、アップロードに成功したことを確認します。これは、SQL Server と Oracle Database のどちらを使用しているかによって異なります。詳細は、次の項を参照してください。
 - [Windows 上の SQL Server: 監査スキーマのアップロード手順](#)
 - [Windows 上の SQL Server: 監査スキーマの検証手順](#)
 - [Windows 上の SQL Server: アクセス・レポート・スキーマのアップロードおよび検証手順](#)
 - [Windows または Linux 上の Oracle Database: 監査スキーマのアップロードおよび検証手順](#)
 - [Windows または Linux 上の Oracle Database: アクセス・レポート・スキーマのアップロードおよび検証手順](#)

監査およびレポート・スキーマを監査データベース・ホストにコピーする手順

1. Oracle Access Manager サーバーをホストしている任意のマシンで、次の場所にナビゲートすることにより Oracle Access Manager 監査スキーマを含むディレクトリを特定します。

```
Component_Install_dir\oblix\reports\crystal
```

`Component_install_dir` は、Oracle Access Manager サーバーのルート・インストール・ディレクトリ（たとえば、`IdentityServer_install_dir\identity\`）です。

2. 特定のオペレーティング・システムおよびネットワーク・ドメインで使用可能な任意の手段を使用して、Oracle Access Manager 監査データベースをホストしているマシン上のディレクトリにファイル `audit.sql` をコピーします。

監査データベースを Oracle Access Manager サーバーのいずれかと同じマシンにインストールした場合、この手順は不要です。

3. 使用しているデータベース・アプリケーションに応じて、次の手順に進みます。
 - [Windows 上の SQL Server: 監査スキーマのアップロード手順](#)
 - [Windows 上の SQL Server: 監査スキーマの検証手順](#)
 - [Windows 上の SQL Server: アクセス・レポート・スキーマのアップロードおよび検証手順](#)
 - 「[Windows または Linux 上の Oracle Database: 監査スキーマのアップロードおよび検証手順](#)」
 - 「[Windows または Linux 上の Oracle Database: アクセス・レポート・スキーマのアップロードおよび検証手順](#)」

Windows 上の SQL Server: 監査スキーマのアップロード手順

1. SQL Server をホストしているマシンで、次のようにナビゲートします。
「スタート」、「プログラム」、「Microsoft SQL Server」、「Query Analyzer」
2. 「SQL Query Analyzer」 ウィンドウに「Connect to SQL Server」 ページが表示されていない場合は、次のようにナビゲートします。
「File」、「Connect」



3. 「Connect to SQL Server」 ページで、SQL Server ホストの Windows サービス名が「SQL Server」というフィールドに表示されていることを確認します。
4. 「Start SQL Server if it is stopped.」を選択します。
5. 「Connect using」を「SQL Server authentication」に設定します。
6. SQL Server のインストール時に選択したログイン名とパスワードを入力し、「OK」をクリックします。

「SQL Query Analyzer」ウィンドウに「Query」ウィンドウが開きます。

7. SQL クエリ・アナライザで Oracle Access Manager 監査データベースを起動します。
「SQL Query Analyzer」メニューで、次のようにナビゲートします。

「File」、「Open」

8. 前の手順で Oracle Access Manager サーバーから監査データベース・ホストにコピーしたディレクトリの下にある「audit.sql」にナビゲートします。

詳細は、11-23 ページの「監査およびレポート・スキーマを監査データベース・ホストにコピーする手順」を参照してください。audit.sql の具体的な場所は次のとおりです。

```
..\reports\crystal\audit.sql
```

9. 「Query」ウィンドウで、次の行をファイル audit.sql の先頭に追加します。

```
use AuditDBName;
```

AuditDBName は、11-22 ページの「Windows 上の SQL Server: 監査データベースの作成手順」で作成した Oracle Access Manager 監査データベースを指定します。この例では、データベースに NPAuditDB という名前を付けました。

すべての SQL 文について、行の最後にセミコロンを付けるのを忘れないでください。

```

クエリ - CRTLAB2.master.sa - C:\TestBed\audit.sql
use NPauditDB;
drop table oblix_audit_events;

create table oblix_audit_events (
  eventDateAndTime    dateTime not null,
  serverId            varchar(255) not null,
  webServerId        varchar(255),
  eventName          varchar(255) not null,
  workflowInstanceId varchar(255),
  workflowType       varchar(255),
  workflowName       varchar(255),
  workflowAction     varchar(255),
)

```

クエリ ファイル CRTLAB2 (8.0) sa (51) master 0:00:00 0行 行1、列15

10. [F5] を押してコマンドを実行します。または、「SQL Query Analyzer」メニューから「Query」、「Execute」を選択します。

最初にこれを行ったときに、アプリケーションは次のエラー・メッセージを返します。

```
cannot drop the table 'oblix_audit_events', because it does not exist in the system catalog yet
```

use コマンドの実行時に表が存在していなかったため、これは規定どおりであり論理的です。audit.sql を保存し、その後このコマンドを再実行した場合は、表が存在するためエラー・メッセージは再表示されません。

11. 「Query」 ウィンドウを閉じずに最小化します。スキーマが正常にアップロードされたことを検証する際に、別の行を audit.sql に追加する必要があります。11-25 ページの「Windows 上の SQL Server: 監査スキーマの検証手順」に進みます。

Windows 上の SQL Server: 監査スキーマの検証手順

1. oblix_audit_events 表からダミーを使用して select を実行します。

11-27 ページの「Windows 上の SQL Server: 監査スキーマのアップロード手順」で audit.sql に追加した行の直下に次の行を追加します。

```
select * from oblix_audit_events;
```

行の最後にセミコロンを忘れずに付けてください。

2. [F5] を押してコマンドを実行します。

```

クエリ - CRTLAB2.NPauditDB.sa - D:\TestBed\audit.sql
use NPauditDB;
select * from oblix_audit_events;

drop table oblix_audit_events;

create table oblix_audit_events (
  eventDateAndTime    dateTime not null,
  serverId            varchar(255) not null,
  webServerId        varchar(255),
  eventName          varchar(255) not null,
  workflowInstanceId varchar(255),
  workflowType       varchar(255),
)

```

eventDateAndTime	serverId	webServerId	eventName	workflowInstanceId

グリッド メッセージ

クエリ ファイル CRTLAB2 (8.0) sa (51) NPauditDB 0:00:00 0行 行2、列33

eventDateAndTime などの列ヘッダーが、「Query」ウィンドウのコード・ペインの直下のペインに表示されます。これらは、audit.sql スキーマが正常にアップロードされたことを示します。

3. 「SQL Query Analyzer」ウィンドウで、「File」、「Save」をクリックして、Oracle Access Manager 監査データベースにリンクされている audit.sql に変更を記録します。
4. 次の「[Windows 上の SQL Server: アクセス・レポート・スキーマのアップロードおよび検証手順](#)」に進みます。

次の手順は、前の手順（oblix_audit_events 表を使用して監査スキーマをアップロードおよび検証しました）と同様です。次の手順では、oblix_rpt_as_reports、oblix_rpt_as_resource および oblix_rpt_as_users の表定義とコマンドを audit.sql ファイルからクエリ・アナライザ・ワークスペースにコピーし、それらを実行します。

Windows 上の SQL Server: アクセス・レポート・スキーマのアップロード および検証手順

1. SQL Server をホストしているマシンで、ログインに必要な次のアクティビティを実行します。
 - 「スタート」、「プログラム」、「Microsoft SQL Server」、「Query Analyzer」にナビゲートします。
 - 「SQL Query Analyzer」ウィンドウに「Connect to SQL Server」ページが表示されていない場合は、「File」、「Connect」にナビゲートします。
 - 「Connect to SQL Server」ページで、SQL Server ホストの Windows サービス名が「SQL Server」というフィールドに表示されていることを確認します。
 - 「Start SQL Server if it is stopped.」を選択します。
 - 「Connect using」を「SQL Server authentication」に設定します。
 - SQL Server のインストール時に選択したログイン名とパスワードを入力し、「OK」をクリックします。

「SQL Query Analyzer」ウィンドウに「Query」ウィンドウが開きます。
2. 次のように、SQL クエリ・アナライザで Oracle Access Manager 監査データベースを起動します。
 - 「SQL Query Analyzer」メニューで、「File」、「Open」にナビゲートします。
 - 前に Oracle Access Manager サーバーから監査データベース・ホストにコピーしたディレクトリの下にある audit.sql ファイルにナビゲートします。次に例を示します。
3. 「Query」ウィンドウで、次の行をファイル audit.sql の先頭に追加します。

```
use AuditDBName;
```

AuditDBName は、11-22 ページの「[Windows 上の SQL Server: 監査データベースの作成手順](#)」で作成した Oracle Access Manager 監査データベースを指定します。この例では、データベースに NPAuditDB という名前を付けました。

すべての SQL 文について、行の最後にセミコロンを付けるのを忘れないでください。

4. 次のように、3つの Oracle Access Manager 表 (oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users) のすべての drop および create コマンドを「Query Analyzer」ウィンドウに追加し、一度に1つずつ実行します。
 - drop table oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users 情報 (3つの drop コマンドに続いて3つの create table コマンド) をまとめて audit.sql ファイルからコピーし、「Query Analyzer」ウィンドウに一度に貼り付けます。

注意：一度にすべてをコピーし、これらのコマンドの順序は変更しないでください。表間には依存関係があります。

 - [F5] を押して、コマンドを一度に実行します (または、「SQL Query Analyzer」メニューから「Query」、「Execute」を選択します)。
 - 「Query」ウィンドウを閉じずに最小化します。スキーマが正常にアップロードされたことを検証する際に、別の行を audit.sql に追加する必要があります。
5. 次のように、oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users 表の情報を検証します。
 - oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users 表から (個別または一度に) "dummy" select を実行します。
 - 11-27 ページの「[Windows 上の SQL Server: 監査スキーマのアップロード手順](#)」で audit.sql から追加した行の直下に次の行を追加します。


```
select * from oblix_rpt_as_reports;
select * from oblix_rpt_as_resources;
select * from oblix_rpt_as_users;
```
 - [F5] を押してコマンドを実行します。
6. 「[Access Server と Identity Server の監査データベースへの接続の有効化](#)」に進みます。次の2つの手順は、前の手順に似ています。ただし、これらは Windows または Linux 上の Oracle Database に固有です。

Windows または Linux 上の Oracle Database: 監査スキーマのアップロードおよび検証手順

1. Oracle Database サーバーおよび iSQL*Plus アプリケーションを起動します。
2. Oracle DB サーバーの iSQL*Plus Web アプリケーションに接続します。
典型的な URL は次のとおりです。

```
http://oracle_DB_host_name:port/isqlplus/
```


Oracle_DB_host_name は Oracle Database インスタンスの名前で、*port* は Oracle Database サーバーのインストール時に選択したポート番号です。
3. ユーザー名、パスワードおよびデータベースの GDN を入力して、iSQL*Plus にログインします。
4. スキーマ定義を次のファイルから iSQL*Plus ワークスペース・ページにコピーします。

```
Identity_Server_install_dir\oblix\reports\crystal\audit_oracle.sql
```
5. 「実行」ボタンをクリックします。
6. 監査スキーマを検証するには、iSQL*Plus で次のコマンドを入力します。

```
desc oblix_audit_events
```


または、iSQL*Plus で oblix_audit_events; に対して select * コマンドを入力できます。
7. 次の「[Windows または Linux 上の Oracle Database: アクセス・レポート・スキーマのアップロードおよび検証手順](#)」に進みます。

次の手順は、前の手順（oblix_audit_events 表を使用して監査スキーマをアップロードおよび検証しました）と同様です。次の手順では、oblix_rpt_as_reports、oblix_rpt_as_resource および oblix_rpt_as_users の表定義を audit.oracle.sql ファイルから Oracle DB サーバーの iSQL *Plus Web アプリケーションにコピーし、それらを実行します。

Windows または Linux 上の Oracle Database: アクセス・レポート・スキーマのアップロードおよび検証手順

1. 必要に応じて iSQL *Plus にログインします。
 - Oracle Database サーバーおよび iSQL *Plus アプリケーションを起動します。
 - Oracle DB サーバーの iSQL *Plus Web アプリケーションに接続します。
 - ユーザー名、パスワードおよびデータベースの GDN を入力して、iSQL *Plus にログインします。
2. 3 つの Oracle Access Manager 表（oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users）のすべての drop および create コマンドを追加し、次のように実行します。
 - 3 つの Oracle Access Manager 表（oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users）のすべての drop および create コマンドを次のファイルから iSQL *Plus ワークスペース・ページに追加します。

```
Identity_Server_install_dir\oblix\reports\crystal\audit_oracle.sql
```
 - 「実行」 ボタンをクリックします。
3. iSQL *Plus で次のコマンドを使用して、3 つの Oracle Access Manager 表（oblix_rpt_as_reports、oblix_rpt_as_resources および oblix_rpt_as_users）すべてのスキーマを個別にまたはすべて一度に検証します。

```
desc oblix_rpt_as_reports;  
desc oblix_rpt_as_resources;  
desc oblix_rpt_as_users;
```

または、iSQL *Plus で 3 つの Oracle Access Manager 表（oblix_rpt_as_reports; oblix_rpt_as_resources; oblix_rpt_as_users;）に対して select * コマンドを入力できます。
4. 11-28 ページの「Access Server と Identity Server の監査データベースへの接続の有効化」に進みます。

Access Server と Identity Server の監査データベースへの接続の有効化

ディレクトリ・サーバーに RDBMS プロファイルを作成し、監査データベースに接続するサーバーをホストしている各マシンに ODBC データ・ソース定義を作成することにより、サーバーを監査データベースに接続できます。単一の固有のシステム DSN（システム全体のデータ・ソース名）は、これらのオブジェクトすべてを接続します。

RDBMS プロファイルとサーバー・ホスト上の ODBC データ・ソース定義の両方で特定の DSN に関連付けられているすべての属性が厳密に一致することが非常に重要です。詳細は、11-33 ページの「[プライマリ RDBMS インスタンスを作成する手順](#)」を参照してください。

タスクの概要 : Oracle Access Manager サーバーの監査データベースへの接続の有効化

1. すべて : globalparams.xml で SQLDBType パラメータの値を設定します。
2. Windows: 各 Oracle Access Manager サーバー・ホストに ODBC データ・ソース定義 (システム DSN) を作成します。
3. すべて : ID システム・コンソールまたはアクセス・システム・コンソールを使用して、ディレクトリ・サーバーに RDBMS プロファイルを作成します。
11-32 ページの「タスクの概要 : RDBMS プロファイルの設定」を参照してください。これには、次のタスクが含まれます。
 - a. 11-33 ページの「プライマリ RDBMS インスタンスを作成する手順」で説明したように、プライマリ RDBMS インスタンスを作成します。
 - b. 11-34 ページの「タスクの概要 : セカンダリ RDBMS インスタンスを作成する手順」で説明したように、オプションで RDBMS プロファイルのセカンダリ RDBMS インスタンスを作成します。
 - c. 11-34 ページの「RDBMS プロファイルを表示可能にする手順 (Windows)」の説明に従って、すべての Oracle Access Manager サーバーを再起動します。

SQLDBType パラメータを設定する手順

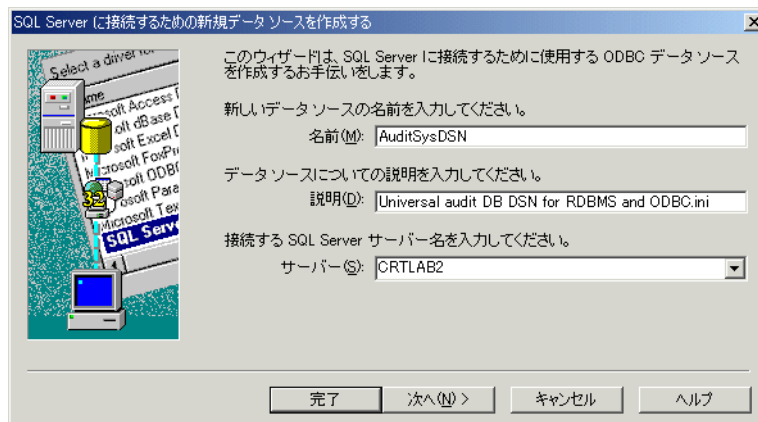
1. 次のファイルを開きます。
`Component_install_dir/identity/apps/common/bin/globalparams.xml`
`component_install_dir` は、Access Server または Identity Server がインストールされている場所です。
2. 次のように、globalparams.xml で SQLDBType パラメータの値を設定します。
Oracle: ODBC 接続タイプを使用する Oracle Database を指定します。
Oracle_OCI: OCI 接続タイプを使用する Oracle Database を指定します。
SQLServer: SQL Server データベースを指定します。

ODBC データ・ソース定義を作成する手順 (Windows)

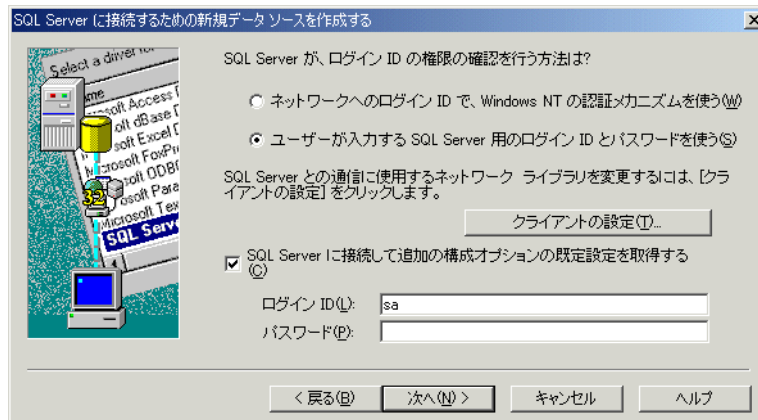
1. 監査データベースに接続する Oracle Access Manager サーバー・ホストで、「スタート」、「設定」、「コントロールパネル」、「管理ツール」、「データ ソース (ODBC)」にナビゲートします。
2. 「システム DSN」タブをクリックします。
3. 「追加」をクリックします。
4. データベース・ドライバのリストから、「SQL Server」を選択し、「完了」をクリックします。

5. 「名前」フィールドに、説明的な名前を入力します。

たとえば、AuditSysDSN は監査データベースのシステム DSN を意味します。この正確な文字列を他のすべての Oracle Access Manager サーバー・ホストの ODBC データ・ソース定義および RDBMS プロファイルのプライマリ RDBMS インスタンスで使用する必要があるため、この名前を書き留めておきます。

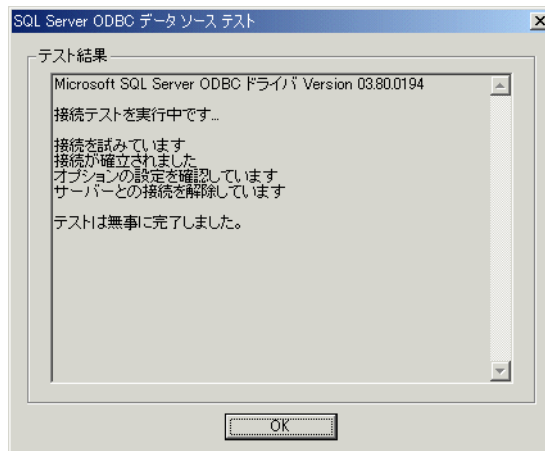
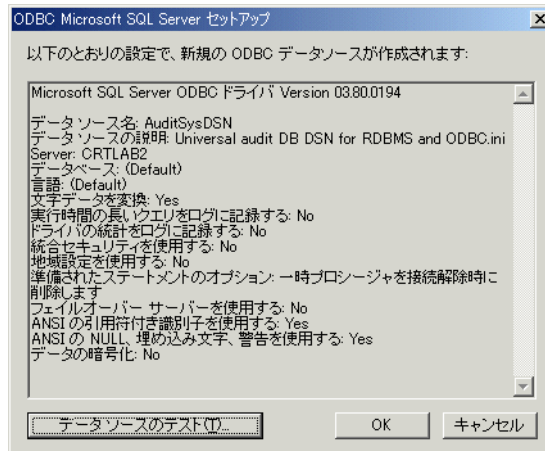


6. 「説明」フィールドに、ユーザーがこのオブジェクトを識別するのに役立つ注記を入力します。
7. 「サーバー」フィールドで、Oracle Access Manager 監査データベースが稼働しているホストの Windows サービス名を選択し、「次へ」をクリックします。
8. 次のページが表示されたら、「ユーザーが入力する SQL Server 用のログイン ID とパスワードを使う」を選択します。



9. 「SQL Server に接続して追加の構成オプションの既定設定を取得する」が選択されていることを確認します。
10. SQL Server のインストール時に指定したログイン ID とパスワードを入力します。
11. 次の 2 つのページはデフォルト設定のままにして、「次へ」、「完了」の順にクリックします。

- 新規 ODBC データ・ソース定義の設定をリストするページが表示されたら、「データソースのテスト」をクリックします。



- 成功を示すページが表示されたら、「OK」を 3 回クリックして開いているページを閉じます。
- 監査データベースに接続するすべての Oracle Access Manager サーバー・ホストでこの手順を繰り返します。

すべてのケースで、また RDBMS データベース・インスタンスに対しても、厳密に同じ設定を使用してください。「[タスクの概要: RDBMS プロファイルの設定](#)」に進みます。

タスクの概要: RDBMS プロファイルの設定

- RDBMS プロファイルを作成します。
詳細は、11-32 ページの「[RDBMS プロファイルを作成する手順](#)」を参照してください。
- プライマリ RDBMS インスタンスを作成します。
詳細は、11-33 ページの「[プライマリ RDBMS インスタンスを作成する手順](#)」を参照してください。
- セカンダリ RDBMS インスタンスを作成します (オプション)。
詳細は、11-34 ページの「[タスクの概要: セカンダリ RDBMS インスタンスを作成する手順](#)」を参照してください。
- RDBMS プロファイルを表示可能にします。
使用しているデータベース・アプリケーションに応じて、11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Windows\)](#)」または 11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Linux\)](#)」を参照してください。

RDBMS プロファイルを作成する手順

- ID システム・コンソールで、「システム構成」をクリックし、左側のナビゲーション・ペインにある「ディレクトリ・プロファイル」のリンクをクリックし、「プロファイルの構成」ページの「RDBMS プロファイルの構成」セクションで「追加」ボタンをクリックします。
または、アクセス・システム・コンソールで、「システム構成」をクリックし、左側のナビゲーション・ペインにある「サーバー設定」をクリックし、ページの「RDBMS プロファイルの構成」セクションで「追加」ボタンをクリックします。
「RDBMS プロファイルの作成」ページは、ID システム・コンソールとアクセス・システム・コンソールで同一です。

The screenshot shows the Oracle Identity Administration console interface. The top navigation bar includes 'ORACLE Identity Administration' and 'Identity System Console'. Below it, there are tabs for 'User Manager', 'Group Manager', 'Org. Manager', and 'Identity System Console'. The main content area is titled 'RDBMSプロファイルの作成' (RDBMS Profile Creation). On the left, there is a navigation menu with options like 'パスワード・ポリシー', 'ディレクトリ・プロファイル', 'Identity Server', etc. The main form area contains the following fields and options:

- 名前***: A text input field.
- データベース接続タイプ***: Radio buttons for 'ODBC' (selected) and 'OCI'.
- 使用***: Checkboxes for 'レポート中', '監査中', and 'MMS'.
- データベース・インスタンス**: A section with a '名前' and 'サーバー・タイプ' header, and an '追加' button.
- 最大アクティブ・サーバー数**: Input field with value '1'.
- フェイルオーバーしきい値**: Input field with value '1'.
- スリープ時間(秒)**: Input field with value '60'.
- 最長セッション時間(分)**: Input field with value '0'.
- プロファイルの有効化**: A checked checkbox.

At the bottom, there is a note: '注意: アスタリスク(*)の付いたフィールドは必須フィールドです。' (Note: Fields with an asterisk (*) are required fields.)

2. 「名前」フィールドに、説明的な名前を入力します。

たとえば、AuditDBSysDSN は監査データベースのシステム DSN を表します。このページで RDBMS プロファイルを作成しますが、この名前は RDBMS プロファイルと各 Oracle Access Manager サーバー・ホスト上の ODBC.ini の対応するデータ・ソース定義値のセットを識別するための便利なユニバーサル名を提供します。

ディレクトリ・サーバー上の各 RDBMS プロファイルの名前は一意である必要があります。

3. 「データベース接続タイプ」フィールドで、データベースが使用する接続のタイプを選択します。
4. 「使用」フィールドで、「レポート中」オプションと「監査中」オプションを選択します。
5. 「プロファイルの有効化」ボックスが選択されていることを確認します。
6. 11-33 ページの「[プライマリ RDBMS インスタンスを作成する手順](#)」に進みます。

プライマリ RDBMS インスタンスを作成する手順

1. 11-32 ページの「[RDBMS プロファイルを作成する手順](#)」で説明したように、「RDBMS プロファイルの作成」ページにナビゲートします。
2. 「RDBMS プロファイルの作成」ページで、「データベース・インスタンス」というラベルの付いた表の横にある「追加」ボタンをクリックします。
3. 「データベース・インスタンスの作成」ページの「名前」フィールドに、説明的な名前を入力します。
便宜上、RDBMS プロファイルに指定した AuditDBSysDSN などのユニバーサル名を使用できます。
4. 次のフィールドは DSN 名または GDN です。データベースに対して ODBC 接続タイプと OCI 接続タイプのどちらを指定したかによって決まります。

SQL Server の場合は、データベース・インスタンスと RDBMS プロファイルに AuditDBSysDSN などの同じ名前を使用できます。Oracle データベースの場合は、データベースの構成時に指定した GDN を使用します。詳細は、11-22 ページの「[Windows 上の Oracle Database: 監査データベースの作成手順](#)」または 11-22 ページの「[Linux 上の Oracle Database: 監査データベースの作成手順](#)」を参照してください。

警告： RDBMS インスタンスの DSN として指定する文字列は、各 Oracle Access Manager サーバーの ODBC データ・ソース定義に対して指定する DSN と完全に一致する必要があります。さらに、他のすべてのデータベース・インスタンス属性の値は、空であるか、Oracle Access Manager システム全体の ODBC データ・ソース定義の対応する属性の値と完全に一致する必要があります。

5. 「データベース」フィールドに、監査データベースの名前を指定します。
この例では NBAuditDB を使用します。
6. 「ユーザー名」フィールドに、監査データベースの作成時に指定したログイン名を入力します。
7. 監査データベース・ログイン名に関連付けられているパスワードを入力します。
8. 他のフィールドはデフォルト設定のままにします。
必要に応じて後で変更できます。
9. 「保存」をクリックして、入力したデータベース・インスタンス設定をコミットします。
10. 「RDBMS プロファイルの変更」ページが表示されたら、「保存」をクリックして、入力した RDBMS プロファイル設定をコミットします。

11. セカンダリ RDBMS インスタンスを作成する場合は、この直後のタスクの概要に進みます。
それ以外の場合は、11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Windows\)](#)」または 11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Linux\)](#)」に進みます。

タスクの概要：セカンダリ RDBMS インスタンスを作成する手順

1. 11-22 ページの「[監査データベースの作成](#)」の手順をすべて実行します。
便宜上、監査データベースの第 2 インスタンスに NPAuditDB_2 のような名前を付けます。
2. 11-23 ページの「[監査スキーマのアップロード](#)」の手順をすべて実行します。
3. 11-32 ページの「[RDBMS プロファイルを作成する手順](#)」の手順 5～11 を実行します。
便宜上、RDBMS インスタンスの名前と DSN 名に AuditDBSysDSN_2 のような名前を指定します。
4. 「RDBMS プロファイルの変更」ページが表示されたら、セカンダリ RDBMS インスタンスの「サーバー・タイプ」がセカンダリに設定されていることを確認します。
5. セカンダリ RDBMS インスタンスの ODBC データ・ソース定義を各 Oracle Access Manager サーバー・ホストの ODBC.ini に追加します。
使用しているデータベース・アプリケーションに応じて、11-29 ページの「[ODBC データ・ソース定義を作成する手順 \(Windows\)](#)」を参照してください。
6. 使用しているデータベース・アプリケーションに応じて、11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Windows\)](#)」または 11-34 ページの「[RDBMS プロファイルを表示可能にする手順 \(Linux\)](#)」に進みます。

RDBMS プロファイルを表示可能にする手順 (Windows)

1. 任意の Oracle Access Manager サーバー・ホストで、「マイ コンピュータ」、「管理」、「サービスとアプリケーション」、「サービス」にナビゲートします。
2. マシン上の Oracle Access Manager サーバーを表すアイコンを右クリックし、ドロップダウン・メニューから「再起動」を選択します。
Access Server と Identity Server の両方を同じマシンにインストールした場合は、両方のサーバーについてこの手順を実行します。
3. 監査データベースに接続するすべての Oracle Access Manager サーバー・ホストについて、この手順を繰り返します。
4. 11-35 ページの「[監査の構成](#)」に進みます。

RDBMS プロファイルを表示可能にする手順 (Linux)

1. Oracle Access Manager サーバーをホストしているマシンで、次のいずれかのコマンドを実行して Oracle Access Manager サーバーを停止します。
 - Access Server: stop_access_server
 - Identity Server: stop_ois_server
2. 次のいずれかのコマンドを実行して、Oracle Access Manager サーバーを起動します。
 - Access Server: start_access_server
 - Identity Server: start_ois_server
3. 監査データベースに接続するすべての Oracle Access Manager サーバー・ホストについて、この手順を繰り返します。
4. 11-35 ページの「[監査の構成](#)」に進みます。

監査の構成

ファイルベース監査とデータベース監査の両方に対して Oracle Access Manager を構成できます。

デフォルトでは、ファイルベース監査とデータベース監査はすべての Oracle Access Manager サーバーに対してオフになります。システム内の Oracle Access Manager サーバーごとに、ファイルベース監査とデータベース監査を手動で有効にできます。

システム全体、サーバーごと、イベントごとおよびアプリケーションごとに監査オプションを構成できます。サマリーは、11-5 ページの「[監査オプションについて](#)」を参照してください。

監査のデフォルトはほとんどの状況に最適です。監査する Oracle Access Manager サーバー上で目的の監査のタイプをオンにする必要があります。監査データベースにデータを送信する場合は、ID システムとアクセス・システムの両方でデフォルトの監査データ書式文字列を置換する必要もあります。詳細は、11-37 ページの「[ID システムの監査出力形式を変更する手順](#)」および 11-42 ページの「[アクセス・システムの監査出力形式を変更する手順](#)」を参照してください。

ID システム・コンソールの「共通構成」サブタブで構成するグローバル監査設定は、「User Manager 構成」、「Group Manager 構成」および「Org. Manager 構成」のサブタブから監査するアプリケーション固有のイベントとは異なります。

タスクの概要：監査の構成の手順

1. 各 Identity Server について、ファイルベース監査とデータベース監査のいずれか一方または両方をオンにし、必要に応じて監査ファイル属性を変更します。
11-36 ページの「[各 Identity Server の監査を有効化および構成する手順](#)」を参照してください。
2. ID システムの監査出力形式を構成します。
詳細は、11-37 ページの「[ID システムの監査出力形式を変更する手順](#)」を参照してください。
3. イベントが監査されるデータを指定します。
これには、次のカテゴリが含まれます。
 - a. User Manager、Group Manager および Organization Manager アプリケーションに共通のイベント
詳細は、11-38 ページの「[監査のグローバル ID システム・イベントおよびプロファイル属性を指定する手順](#)」を参照してください。
 - b. User Manager、Group Manager または Organization Manager イベント
詳細は、11-39 ページの「[監査する User Manager、Group Manager または Organization Manager イベントを指定する手順](#)」を参照してください。
4. すべての Identity Server が監査データベースにデータを記録できることを確認します。
詳細は、11-40 ページの「[すべての Identity Server が監査データベースにデータを記録できることを確認する手順 \(Windows\)](#)」を参照してください。
5. 個々の Access Server について、ファイルベース監査またはデータベース監査をオンにし、必要に応じて監査ファイル属性を変更します。
詳細は、11-41 ページの「[各 Access Server の監査を有効化および構成する手順](#)」を参照してください。
6. アクセス・システムの監査出力形式をグローバルに変更します。
詳細は、11-42 ページの「[アクセス・システムの監査出力形式を変更する手順](#)」を参照してください。

7. ユーザー・アクセス権限レポートを作成および管理します。

詳細は、11-43 ページの「ユーザー・アクセス権限レポートを作成および管理する手順」を参照してください。

各 Identity Server の監査を有効化および構成する手順

1. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「Identity Server」をクリックします。
2. 変更するサーバーのリンクをクリックし、「変更」をクリックします。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 Identity System Console

ログイン・ユーザー: Master Admin

Identity Serverの変更

名前	ID_Server_10.1.3_M3_staqh24_6021
ホスト名*	staph24
ポート*	6021
デバッグ*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
デバッグ・ファイル名*	/oblix/logs/debugfile.lst
トランスポート・セキュリティ*	<input checked="" type="radio"/> オープン <input type="radio"/> 簡易 <input type="radio"/> 証明書
最大セッション時間(時間)*	24
スレッド数*	20

データベースの監査フラグ(監査オン/オフ) オフ オン

3. プリファレンスに従ってファイル監査とデータベース監査のフラグを設定し、必要に応じて監査ファイル属性を変更します。
「保存」をクリックして変更を有効にします。

4. データベース監査の場合は、次のディレクトリにある globalparams.xml ファイルを開きます。次に例を示します。

```
Component_install_dir/identity/apps/common/bin/globalparams.xml
```

component_install_dir は、Access Server または Identity Server がインストールされている場所です。

次のように、globalparams.xml で SQLDBType パラメータの値を設定します。

Oracle: ODBC 接続タイプを使用する Oracle Database を指定します。

Oracle_OCI: OCI 接続タイプを使用する Oracle Database を指定します。

SQLServer: SQL Server データベースを指定します。これはデフォルトです。

5. Oracle Access Manager システム内のすべての Identity Server についてこの手順を繰り返し、11-37 ページの「ID システムの監査出力形式を変更する手順」に進みます。

ID システムの監査出力形式を変更する手順

1. ID システム・コンソールで、「共通構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「マスター監査ポリシー」をクリックしてから「変更」をクリックします。

2. 「メッセージの書式」テキスト・ボックス内の任意の場所をクリックし、[Ctrl] キーを押しながら [A] キーを押してテキスト・ボックスの内容をすべて選択し（グレー表示されているコンテンツも含む）、[Del] を押します。
3. 空のテキスト・ボックスに、次の文字列を挿入します。


```
%ob_datetime% - %ob_event% - %ob_operation% - %ob_serverid% - %ob_ip% - %ob_url% - %ob_target.uid% - %ob_app% - %ob_source.uid% - %ob_profileattrs% - %ob_auditapp%
```

 文字列の最後にセミコロンや改行は追加しないでください。
4. 必要に応じて、「日付タイプ」、「日付セパレータ」、「エスケープ文字」、「レコード・セパレータ」および「フィールド・セパレータ」の各フィールドのデフォルト値を変更します。これらの値のいずれかを変更する場合は、監査レポートの生成に使用される Crystal Report テンプレートを再構成する必要があります。
5. 「保存」をクリックします。新しいメッセージ書式文字列および行ったその他の変更が、「マスター監査ポリシーの構成」ページに表示されます。
6. 新規メッセージ書式文字列は ID システム全体に適用されるため、他の Identity Server に対してプロセスを繰り返す必要はありませんが、アクセス・システムに対して書式文字列を設定するには同様の手順を実行する必要があります。詳細は、11-42 ページの「アクセス・システムの監査出力形式を変更する手順」を参照してください。
7. 11-38 ページの「監査のグローバル ID システム・イベントおよびプロファイル属性を指定する手順」に進みます。

監査のグローバル ID システム・イベントおよびプロファイル属性を指定する手順

1. ID システム・コンソールで、「共通構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「グローバル監査ポリシー」をクリックしてから「変更」をクリックします。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

User Manager Group Manager Org. Manager Identity System Console

システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成 ログイン・ユーザー: Master Admin

オブジェクト・クラス
ワークフロー・パネル
マスター監査ポリシー
グローバル監査ポリシー

アプリケーション監査ポリシーの変更 プロファイル属性

イベント名	アプリケーション監査有効	監査成功	監査失敗
ログイン	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ログアウト	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
パスワード管理	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

2. 監査する最大 5 つのプロファイル属性を選択します。

プロファイル属性（「フルネーム」、「従業員番号」、「部門番号」など）は、監査されるアクション / イベント（「検索」、「プロファイルの表示」、「プロファイルの変更」など）を実行するユーザーに固有です。プロファイル属性の目的は、アクション / イベントを実行するユーザーの識別に役立ちます。

警告： チャレンジ・フレーズまたはレスポンス属性の公開を回避するために、監査のプロファイル属性としてこれらを選択しないことをお勧めします。チャレンジ・フレーズまたはレスポンスをプロファイル属性として追加すると、これらは独自のエンコード形式で監査されます。

3. 一般的な User Manager、Group Manager および Organization Manager アプリケーション・イベントのデフォルトの監査フラグ設定を変更します。
4. 「保存」をクリックして、これらの設定をシステム内のすべての Identity Server に適用します。
5. 11-39 ページの「監査する User Manager、Group Manager または Organization Manager イベントを指定する手順」に進みます。

監査する User Manager、Group Manager または Organization Manager イベントを指定する手順

1. ID システム・コンソールで、「User Manager 構成」、「Group Manager 構成」または「Org Manager 構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「監査ポリシー」をクリックしてから「変更」をクリックします。

ORACLE Identity Administration ヘルプ バージョン情報 ログアウト

システム構成 | **User Manager構成** | Group Manager構成 | Org Manager構成 | 共通構成 Identity System Console

ログイン・ユーザー: Master Admin

- タブ
- レポート
- **監査ポリシー**

アプリケーション監査ポリシーの変更

プロファイル属性

フルネーム

イベント名	アプリケーション監査有効	監査成功	監査失敗
検索	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
プロファイルの表示	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
プロファイルの変更	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ロケーションの表示	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

2. 監査する最大 5 つのプロファイル属性を選択します。

プロファイル属性（「フルネーム」、「従業員番号」、「部門番号」など）は、監査されるアクション / イベント（「検索」、「プロファイルの表示」、「プロファイルの変更」など）を実行するユーザーに固有です。プロファイル属性の目的は、アクション / イベントを実行するユーザーの識別に役立ちます。

警告： チャレンジ・フレーズまたはレスポンス属性の公開を回避するために、監査のプロファイル属性としてこれらを選択しないことをお勧めします。チャレンジ・フレーズまたはレスポンスをプロファイル属性として追加すると、これらは独自のエンコード形式で監査されます。

3. 一般的な User Manager アプリケーション・イベントのデフォルトの監査フラグ設定を適宜変更します。
4. 「保存」をクリックして、これらの設定をシステム内のすべての Identity Server に適用します。

すべての Identity Server が監査データベースにデータを記録できることを確認する手順 (Windows)

1. この時点までにすべての監査設定手順を完了した任意の Identity Server の ID システム・コンソールの任意のページで、アプリケーション・ウィンドウの右上にある「ログアウト」をクリックします。
2. 本当にログアウトするかどうかを確認されたら、「OK」をクリックします。
3. 監査ベースをホストしているマシンで SQL Server の「Query Analyzer」ウィンドウを開きます。

11-25 ページの「Windows 上の SQL Server: 監査スキーマの検証手順」を完了したときに、このウィンドウを最小化しました。

なんらかの理由でウィンドウが開かれていない場合は、「スタート」、「プログラム」、「Microsoft SQL Server」、「Query Analyzer」、「File」、「Open」、「Login_Credentials」、「OK」、「File」、「Open」、「audit_sql_path」、「OK」にナビゲートして再起動します。

Login_Credentials は、SQL Server のインストール時に指定したユーザー名およびパスワードで、audit_sql_path は、監査データベース・ホストにコピーし、その後 11-25 ページの「Windows 上の SQL Server: 監査スキーマの検証手順」で変更した audit.sql ファイルのパスです。

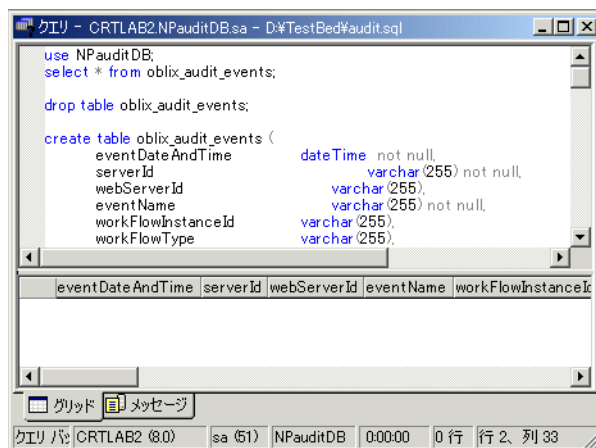
4. [F5] を押して audit.sql を実行します。

以前に次の行を追加した後で、audit.sql を保存しました。

```
use AuditDBName;
select * from oblix_audit_events;
```

AuditDBName は、11-22 ページの「Windows 上の SQL Server: 監査データベースの作成手順」で作成した監査データベースを指定します。

Oracle Access Manager スキーマの列ヘッダーが「Query」ウィンドウの下部に表示され、適切な列の下にログアウトの詳細が表示されます。



5. 11-41 ページの「各 Access Server の監査を有効化および構成する手順」に進みます。

すべての Identity Server が監査データベースにデータを記録できることを確認する手順 (Linux または Solaris)

- この時点までにすべての監査設定手順を完了した任意の Identity Server の ID システム・コンソールの任意のページで、アプリケーション・ウィンドウの右上にある「ログアウト」をクリックします。
- 本当にログアウトするかどうかを確認されたら、「OK」をクリックします。
- Oracle Database Server の iSQL *Plus Web アプリケーションで次の手順を実行します。
ユーザー名、パスワードおよびデータベースの GDN を入力して、iSQL *Plus にログインします。
iSQL*Plus ワークスペースで次のコマンドを入力します。

```
select * from oblix_audit_events;
```


Oracle Access Manager 監査スキーマの列ヘッダーが iSQL*Plus ワークスペース・ページに表示されます。ログアウトに関する情報が、適切な列ヘッダーの下に表示されます。
- 11-41 ページの「各 Access Server の監査を有効化および構成する手順」に進みます。

各 Access Server の監査を有効化および構成する手順

- 監査データベースへの接続を計画している任意の Access Server で、「アクセス・システム・コンソール」、「アクセス・システム構成」、「Access Server 構成」、「ServerName」、「変更」にナビゲートします。
ServerName は、変更する Access Server を指定します。

ORACLE Access Administration

Policy Manager ヘルプ バージョン情報 ログアウト

システム構成 システム管理 アクセス・システム構成

ログイン・ユーザー: Master Admin

- Access Serverのラスタ
- AccessGate構成
- 新規Access Gateの追加
- Access Server 構成**
- 認証管理
- 認可管理
- ユーザー・アクセス構成

Access Serverの変更

名前	M3_AAA_stagh24
ホスト名*	staph24
ポート*	6025
デバッグ*	<input checked="" type="radio"/> オフ <input type="radio"/> オン
デバッグ・ファイル名*	
トランスポート・セキュリティ*	<input checked="" type="radio"/> オープン <input type="radio"/> 簡易 <input type="radio"/> 証明書
最大クライアント・セッション時間(時間)*	24
スレッド数*	60

- プリファレンスに応じて、ファイル監査フラグとデータベース監査フラグを設定します。
- 監査ファイル属性を適宜変更し、「保存」をクリックして変更をコミットします。
アスタリスクでマークされた属性のいずれかを変更する場合は、Access Server を再起動して変更を有効にする必要があります。
- Oracle Access Manager システム内のすべての Access Server についてこの手順を繰り返し、「アクセス・システムの監査出力形式を変更する手順」に進みます。
- データベース監査の場合は、次のディレクトリにある globalparams.xml ファイルを開きます。

`Component_install_dir/apps/common/bin/`

`component_install_dir` は、Access Server または Identity Server がインストールされている場所です。

次のように、globalparams.xml で SQLDBType パラメータの値を設定します。

SQLServer: SQL Server データベースを指定します。これはデフォルトです。

Oracle: ODBC 接続タイプを使用する Oracle Database を指定します。

Oracle_OCI: OCI 接続タイプを使用する Oracle Database を指定します。

アクセス・システムの監査出力形式を変更する手順

1. 監査データベースへの接続を計画している任意の Access Server で、「アクセス・システム・コンソール」、「アクセス・システム構成」、「共通情報の構成」、「マスター監査ルール」、「追加」（または「変更」）にナビゲートします。

Oracle Access Administration

Policy Manager ヘルプ バージョン情報 ログアウト

システム構成 システム管理 アクセス・システム構成 ログイン・ユーザー Master Admin

共有シークレット マスター監査ルール リソース・タイプ定義 パスワード・ポリシー・キャッシュのフラッシュ 重複アクション

Access Serverの
リスト

AccessGate構成

新規Access
Gateの追加

Access Server構
成

認証管理

認可管理

ユーザー・アクセ
ス構成

共通情報の構成

ホスト識別子

マスター監査ルールの追加

プロファイル属性

監査イベント

監査イベント・マッピング

監査日付タイプ

監査エスケープ文字

監査レコード・フォーマット

認証成功

認証失敗

認可成功

認可失敗

認証成功 AUTHN_SUCCESS

認証失敗 AUTHN_FAIL

認可成功 AUTHZ_SUCCESS

認可失敗 AUTHZ_FAIL

12/31/1999書式

\

%ob_datetime% - %ob_event% - %ob_operation% - %ob_serverid% - %ob_ip% - %ob_url% - %ob_userid% - %ob_time_no_offset% - %ob_resrc_scheme% - %ob_wgid% - %ob_wgcontext% - %ob_reason%

キャッシュの更新

2. 「監査レコード・フォーマット」テキスト・ボックス内の任意の場所をクリックし、[Ctrl] キーを押しながら [A] を押してテキスト・ボックスの内容をすべて選択し（グレー表示されているコンテンツも含む）、[Del] を押します。
3. 空のテキスト・ボックスに、次の文字列を正確に挿入します。


```
%ob_datetime% - %ob_event% - %ob_operation% - %ob_serverid% - %ob_ip% - %ob_url% - %ob_userid% - %ob_time_no_offset% - %ob_resrc_scheme% - %ob_wgid% - %ob_wgcontext% - %ob_reason%
```

 文字列の最後にセミコロンや改行は追加しないでください。
4. 「プロファイル属性」ボックスに、監査するプロファイル属性の名前を入力し、テキスト・ボックスの右にあるプラス記号 (+) をクリックします。この手順を繰り返して、他のプロファイル属性を追加します。
5. 監査するイベントを選択します。
 - 希望する場合は、デフォルトのイベント・マッピングを変更します。
 - 必要に応じて、「監査日付タイプ」および「監査エスケープ文字」フィールドのデフォルト値を変更します。これらの値のいずれかを変更する場合は、監査レポートの生成に使用される Crystal Report テンプレートを再構成する必要があります。
6. 「保存」をクリックします。新しいメッセージ書式文字列および行ったその他の変更が、「マスター監査ルール」ページに表示されます。
7. 新規メッセージ書式文字列はアクセス・システム全体に適用されるため、他の Access Server に対してプロセスを繰り返す必要はありませんが、ID システムの書式文字列を置換するには同様の手順を実行する必要があります。

11-37 ページの「ID システムの監査出力形式を変更する手順」を参照してください。

- 11-43 ページの「ユーザー・アクセス権限レポートを作成および管理する手順」に進みます。

ユーザー・アクセス権限レポートを作成および管理する手順

- 監査データベースへの接続を計画している任意の Access Server で、「アクセス・システム・コンソール」、「システム管理」、「アクセス・システム管理」、「追加」にナビゲートします。

ORACLE Access Administration Policy Manager ヘルプ バージョン情報 ログアウト

システム構成 システム管理 **アクセス・システム構成**

ログイン・ユーザー: Master Admin

- 診断
- **レポートの管理**
- 同期レコードの管理

ユーザー・アクセス権限レポート

レポート名

説明

Access Server

結果ストレージ

データベースに保存

ファイルに保存

ファイル名

リソースのリスト

URL	リソース・タイプ	リソース操作
(追加)		

- 「レポート名」フィールドに、「深夜アクセス」などの説明的な名前を入力します。
- 「説明」フィールドに、「積荷ドック出荷目録 URL への夜間シフト・アクセス権を持つ人物」など、レポートのコンテンツの比較的長い説明を入力します。
- ローカル・ホストで監査データベースまたは監査ファイルに情報を送信するかどうかを指定します。監査ファイルを指定する場合は、ファイル名を指定する必要があります。
- 「開始 IP アドレス」フィールドで、アクセスをテストする特定の Web ブラウザのホストの IP を入力します。
- 「日付 / 時間」フィールドで、アクセスをテストする日、時刻およびタイムゾーンを選択します。

監査機能は実際のアクセス試行の履歴的な結果を実際にレポートせずに、Oracle Access Manager ディレクトリ・サーバーに格納されているポリシーおよびプロファイル情報を調べて、指定されたユーザーが指定された時刻に指定されたリソースにアクセスする権限を現在持っているかどうかを計算するため、この日時では将来を指すことができます。

- 「リソースのリスト」ラベルの近くにある「追加」ボタンをクリックして、テストするリソースのリストに URL を追加します。

「リソース・ルールの追加」ページが表示されます。

ORACLE Access Administration Policy Manager ヘルプ バージョン情報 ログアウト

システム構成 システム管理 **アクセス・システム構成**

ログイン・ユーザー: Master Admin

- 診断
- **レポートの管理**
- 同期レコードの管理

リソース・ルールの追加

URL

リソース・タイプ

リソース操作

GET POST PUT HEAD

DELETE TRACE OPTIONS CONNECT

OTHER

8. テストする URL を入力します。
9. 「リソース・タイプ」を `http` または `ejb` に設定します。
10. テストするアクションを選択します。
11. 「保存」をクリックして「新規レポートの追加」ページに戻ります。
12. もう一度「追加」をクリックして、テストする別のリソースを追加するか、次の手順に進みます。
13. すべてのユーザーのアクセスをテストすることも、「セレクトタ」を使用して特定のユーザーのアクセスをテストすることもできます。
「セレクトタ」の詳細は、1-11 ページの「セレクトタ」を参照してください。
14. 「セレクトタ」での処理が終了し、「新規レポートの追加」ページが再表示されたら、「保存」をクリックして変更をコミットします。

監査レポートの設定

Oracle Access Manager に用意されている構成済の Crystal Reports テンプレートを利用するには、Oracle Access Manager サーバー・ドメイン内の Windows マシンに Crystal Reports アプリケーションをインストールする必要があります (Crystal Reports は、UNIX マシンにインストールできませんが、UNIX マシンにインストールされている Oracle Database によって生成されたデータベース内の情報を利用することはできます)。

Crystal Reports 9 のインストールに加えて、パッチもインストールする必要があります。

Oracle Access Manager サーバー・インストール・ディレクトリには、Crystal Reports アプリケーションで使用される特定のテンプレート、サンプル・レポート、データベース・スキーマおよびデータベース・ドライバがインストールされています。これらは、Crystal Reports ソフトウェア自体とは異なります。Oracle Access Manager サーバー・インストール・ディレクトリから Crystal Reports ソフトウェアをホストしているマシンにこれらをコピーする必要があります。

タスクの概要：監査レポートの設定手順

1. SQL Server または Oracle Database をホストしているマシンに接続できる Windows マシンに Crystal Reports 9.22a をインストールします。
2. Crystal Reports 9 の必須パッチをインストールします。
3. Crystal Reports をホストしているマシンに、Oracle Access Manager 監査レポート・テンプレート、Crystal リポジトリおよび関連リソースをコピーします。
4. ODBC データ・ソース定義を作成し、`orMap.ini` を編集することにより、Crystal Reports を Oracle Access Manager 監査データベースに接続します。
5. ODBC データ・ソース定義を作成し、`orMap.ini` を編集することにより、Crystal Reports を Crystal データベースに接続します。

Crystal Reports のインストール手順

1. Crystal Reports 9.22 インストール・パッケージのコピーをバンダーから入手します。
2. `setup.exe` を起動し、プロンプトに従います。
3. 任意のインストール・ディレクトリを指定します。
4. プロンプトが表示されたら、レポート・パッケージの購入時に提供された製品キーを入力します。
5. プロンプトが表示されたら、インストール・タイプとして「`typical`」を指定します。
6. 11-45 ページの「Crystal Reports のパッチをインストールする手順」に進みます。

Crystal Reports のパッチをインストールする手順

1. 次の Web サイトから Crystal Reports 9 パッチをダウンロードします。
http://support.businessobjects.com/communityCS/FilesAndUpdates/cr90dbexwin_en.zip.asp
2. cr90dbexwinen.zip をハード・ディスク上の一時フォルダに解凍し、CR90DBEXWIN_EN_200403.EXE を起動します。
3. プロンプトに従って、パッチ・インストールを完了します。
4. 11-45 ページの「Oracle Access Manager 固有の Crystal リソースをコピーする手順」に進みます。

Oracle Access Manager 固有の Crystal リソースをコピーする手順

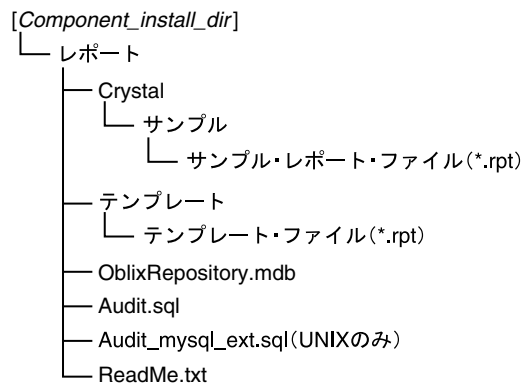
1. 任意の方法を使用して、次のリソースを Oracle Access Manager サーバー・インストール環境から Crystal Reports をホストしているマシン上の選択したディレクトリにコピーします。

```
Component_install_dir\oblix\reports
```

`Component_install_dir` は、監査データベースに接続している Identity Server のルート・インストール・ディレクトリです。

"..\reports" およびそのサブディレクトリ内のすべてのファイルを必ずコピーします。次の図に、Crystal Reports マシンにコピーされるリソースを示します。

図 11-4 Crystal Reports マシンにコピーされるリソース



2. 11-45 ページの「Crystal Reports を監査データベースに接続する手順」に進みます。

Crystal Reports を監査データベースに接続する手順

1. 11-29 ページの「ODBC データ・ソース定義を作成する手順 (Windows)」で説明した手順に従って、Crystal Reports が監査データベースに接続できるようにします。

指定した DSN および関連するすべての詳細が、監査データベースに接続している Oracle Access Manager サーバーに対して作成された RDBMS プロファイルおよび ODBC データ・ソース定義で指定した値と完全に一致していることを確認します。

2. 11-46 ページの「タスクの概要 : Crystal Reports を Oracle Repository に接続する手順」に進みます。

タスクの概要 : Crystal Reports を Oracle Repository に接続する手順

1. Crystal Reports を Oracle/Crystal リポジトリ (.mdb データベース) に接続する ODBC データ・ソース定義を作成します。
2. Oracle リポジトリが Crystal リポジトリと等しくなるように orMap.ini を編集します。

Crystal Reports を Oracle/Crystal リポジトリに接続する ODBC データ・ソース定義の作成手順

1. 11-29 ページの「[ODBC データ・ソース定義を作成する手順 \(Windows\)](#)」で説明した一般手順に従って、Crystal Reports が監査データベースに接続できるようにします。
次の手順で注記されている場合を除き、元の手順で指定した値を使用します。
2. データベース・ドライバを求めるプロンプトが表示されたら、「Microsoft Access driver (.mdb)」を選択します。
3. 「名前」パラメータには、OracleRepositorySysDSN などの自己説明的な名前を選択します。
4. 11-46 ページの「[orMap.ini の編集手順](#)」に進みます。

orMap.ini の編集手順

1. Crystal Reports をホストしているマシンで、次のようにナビゲートします。

```
C:\Program Files\Common Files\Crystal Decisions\2.5\bin
```

2. 任意のプレーン・テキスト・エディタで、ファイル orMap.ini を開きます。
3. 「Crystal Repository=Crystal Repository」の行を次の行で置換します。

```
Crystal Repository = repository_DSN
```

repository_DSN は、OracleRepository.mdb ファイルに対して作成したシステム DSN です。この例では OracleRepositorySysDSN を使用しています。

SNMP モニタリング

この章では、Simple Network Management Protocol (SNMP) を通じてモニターしているネットワークについて説明します。

SNMP モニタリングは、Oracle Access Manager システムの情報を収集する複数の方法の1つです。ロギング、監査およびレポート機能については、このガイドの他の場所で説明しています。

この章の内容は次のとおりです。

- 前提条件
- [Oracle Access Manager SNMP モニタリングおよびエージェントについて](#)
- [Oracle Access Manager MIB およびオブジェクトについて](#)
- [SNMP モニタリングの有効化および無効化](#)
- [SNMP エージェントおよびトラップの宛先の設定](#)
- [SNMP 構成設定の変更](#)
- [SNMP のロギング](#)
- [SNMP メッセージ](#)
- [Netstat 値と SNMP 値の差異](#)
- [停止間隔の構成](#)

注意： SNMP のインストールの詳細は、『Oracle Access Manager インストール・ガイド』を参照してください。

前提条件

ネットワーク管理ステーション (NMS) がインストールされている必要があります。また、管理情報ベース (MIB) から収集したネットワークの統計のアップロードおよび表示方法に精通している必要があります。この章では、Oracle Access Manager MIB オブジェクト、およびこれらのオブジェクトのオブジェクト識別子 (OID) について説明します。ただし、この章では、NMS でこれらの OID を使用して統計を収集する方法については説明しません。このような情報については、NMS のドキュメントを参照してください。

Oracle Access Manager SNMP モニタリングおよびエージェントについて

Simple Network Management Protocol (SNMP) では、ネットワーク管理ステーション上のサーバー関連の SNMP データを収集および表示することにより、Oracle Access Manager システムをホストしているネットワーク上のコンポーネント・アクティビティをモニターできます。SNMP 統計には、通常は次のようなデータが含まれます。

- ネットワーク上のホスト、ルーターおよびサーバー
- 特定のデバイスで処理されているリクエスト数
- 特定のデバイスが稼働しているかどうか
- リクエストが正常に処理されたかどうか

SNMP データは、ネットワーク管理ステーション (NMS) に表示されます。NMS は、HP OpenView などのネットワーク管理アプリケーションを実行しているワークステーションです。便利な方法でネットワーク統計を表示するように NMS を構成します。たとえば、グラフとして表示し、単純なネットワーク統計を示したり、デバイスが処理しているリクエスト数が一連の定義済制限に該当するかどうかを示したりします。

サポートされている任意のプラットフォームで実行されている Identity Server および Access Server の SNMP 統計を取得できます。Oracle Access Manager では、SNMP ポーリングおよびトラッピングがサポートされます。ポーリングでは、次のような情報が収集されます。

- コンポーネントのバージョン番号
- 構成ステータス
- 接続ステータス
- コンポーネントにより処理されたアクションの統計

イベント・トラップには、次のような情報が含まれます。

- コンポーネント障害
- イベント障害
- 接続ステータス
- アクションの完了の失敗

注意： Oracle Access Manager では、バージョン 2 の SNMP プロトコルがサポートされます。

SNMP エージェント

Simple Network Management Protocol (SNMP) は、ネットワーク・デバイスが情報を交換できるようにするアプリケーション層プロトコルです。SNMP トランスポート・データ（正常な操作や失敗条件など）を使用することにより、管理者は、ネットワーク・パフォーマンスをモニターし、問題を解決できます。Oracle Access Manager の SNMP エージェントにより、Identity Server および Access Server に対して SNMP ベースのデータ収集を実装できます。SNMP エージェントにより、Access Server によって実行された正常な認証の数や Identity Server によって処理されたリクエスト数などの情報を収集できます。

SNMP エージェントは、オプションのインストール可能コンポーネントです。エージェントは、自身がインストールされているホストの情報を収集するため、エージェントは、SNMP データを収集するホストごとにインストールする必要があります。インストールされている場合、エージェントは、そのエージェントがインストールされたのと同じサーバー・ホスト上の Identity Server または Access Server に関する情報にアクセスします。エージェントは `SNMP_install_dir` にインストールされます。

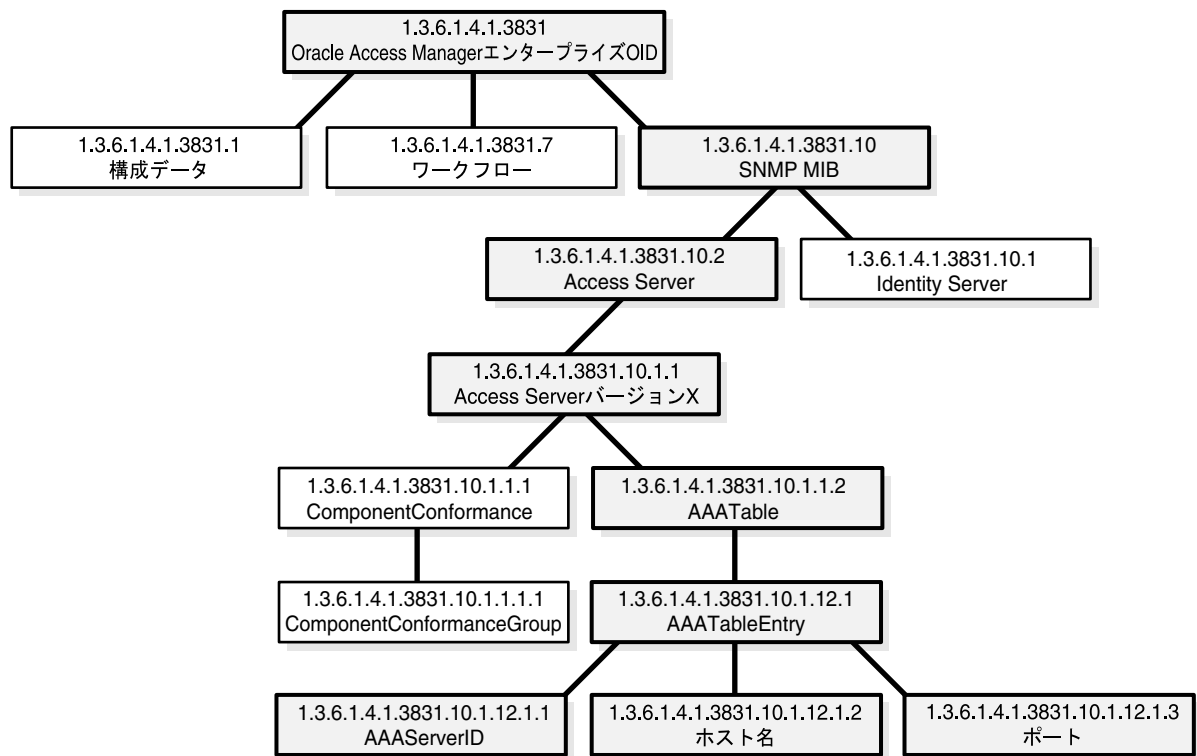
SNMP エージェントのインストールの詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

Oracle Access Manager MIB およびオブジェクトについて

管理情報ベース (MIB) は、様々な Oracle Access Manager コンポーネントのステータスに関連する変数を含む仕様ファイルです。SNMP エージェントは、MIB のフィールドの値を収集します。

図 12-1 に、Oracle Access Manager MIB 階層を示します。

図 12-1 MIB 階層



Oracle Access Manager MIB は、ブランチおよびオブジェクト識別子 (OID) の連結として表現されます。MIB ルートから MIB の最上位ノードまでのラベルは次のとおりです。

iso.org.dod.internet.private.enterprises.oblix.snmp

MIB ファイルは、`SNMP_install_dir/oblix/mibs` にあります。これらのファイルは SNMP バージョン 2 に準拠しています。

次に、Oracle Access Manager SNMP コンポーネントとともに提供される MIB オブジェクトについて説明します。

注意： NMS への MIB ファイルのアップロードの詳細は、NMS のドキュメントを参照してください。

MIB 索引フィールド

各 MIB 表には、1 つ以上の索引フィールドが含まれます。索引フィールド値は、表の一意の行を識別するのに役立ちます。

たとえば、12-5 ページの「[Identity Server の MIB オブジェクト](#)」で説明した `coreidInstanceTable` の索引フィールドは、`coreidHostname` および `coreidPort` です。これらのエントリは、インストール環境を一意に識別するため、索引として使用されます。`Identity1` および `Identity2` という 2 つの `Identity Server` があり、それぞれポート 6023 および 6024 を使用している `localhost` というホスト名が付いているとします。これらのサーバーの索引は、`localhost.6023` および `localhost.6024` になります。

`Identity1` の最初の列値を取得する場合、SNMP エージェントからリクエストするオブジェクト識別子は次の論理形式になります。

```
1.3.6.1.4.1.3831.10.1.1.2.1.1.localhost.6023
```

1.3.6.1.4.1.3831.10.1.1.2.1.1 は、`localhost.6023` の索引値を持つ要素について、`coreidInstanceTable` の最初の列の内容を示します。索引は、実際には文字列の長さ、その後文字列の文字の ASCII コードを含む数値表記 (OID の指定と同様) で表現されます。次の例について考えます。

```
1.3.6.1.4.1.3831.10.1.1.2.1.1.localhost.6023
```

この例は、実際には次のように表現されます。

```
1.3.6.1.4.1.3831.10.1.1.2.1.1.9.108.111.99.97.108.104.111.115.116.6023
```

注意： 表全体を SNMP リクエストで返す場合、索引フィールドの値を知っている必要はありません。

Identity Server の MIB オブジェクト

表 12-1 は、MIB 内の Identity Server オブジェクトを示しています。この情報へのパスは次のとおりです。

iso.org.dod.internet.private.enterprises.oblix.snmp.coreid.versionone

この表の名前は coreidInstanceTable です。その索引フィールドは、coreidHostname および coreidPort です。Identity Server インスタンスについて説明します。

表 12-1 Identity Server の MIB オブジェクト

管理対象オブジェクト	構文	説明
coreidInstanceTable OID: 1.3.6.1.4.1.3831.10.1.1.2	N/A	プライマリ表名。
coreidId OID: 1.3.6.1.4.1.3831.10.1.1.2.1.1	SnmpAdminString (サイズ 0 ~ 255)	Identity Server インスタンスの識別子。
coreidHostname OID: 1.3.6.1.4.1.3831.10.1.1.2.1.2	SnmpAdminString (サイズ 0 ~ 255)	この Identity Server が稼働しているマシンのホスト名。ホスト名は、この表の索引です。
coreidPort OID: 1.3.6.1.4.1.3831.10.1.1.2.1.3	Integer (0 ~ 65535)	Identity Server がリスニングするポート。ポート番号は、この表の索引です。
coreidMode OID: 1.3.6.1.4.1.3831.10.1.1.2.1.4	Integer (0 ~ 5)	Identity Server と WebPass 間のトランスポート・セキュリティ・モード。 0: オープン 1: 簡易 2: 証明書
coreidStartTime OID: 1.3.6.1.4.1.3831.10.1.1.2.1.5	DateAndTime	Identity Server を最後に起動した時刻。
coreidServiceThreads OID: 1.3.6.1.4.1.3831.10.1.1.2.1.6	Integer (0 ~ 65535)	Identity Server インスタンス内のサービス・スレッド数。スレッド数は管理コンソールで設定されます。scoreboard_params.lst 内のパラメータ NumberOfServiceThreads は、各サービス・スレッドの SNMP 情報をメンテナンスするために (サービス・スレッドごとに 1 つを使用して) 割り当てられるスロット数を制御します。
coreidNumOfLanguagesConfigured OID: 1.3.6.1.4.1.3831.10.1.1.2.1.7	Integer (0 ~ 65535)	この Identity Server インスタンスに対してインストールされている言語数。
coreidNumOfLogins OID: 1.3.6.1.4.1.3831.10.1.1.2.1.8	counter64	Identity Server インスタンスへの成功ログイン回数。
coreidNumOfLoginsFailure OID: 1.3.6.1.4.1.3831.10.1.1.2.1.9	Counter64	Identity Server インスタンスへの失敗したログイン試行回数。
coreidRequestsProcessed OID: 1.3.6.1.4.1.3831.10.1.1.2.1.10	Counter64	Identity Server インスタンスにより処理されたリクエスト数。
coreidNumOfRequestsSuccess OID: 1.3.6.1.4.1.3831.10.1.1.2.1.11	Counter64	この Identity Server インスタンスにより正常に処理されたリクエスト数。
coreidNumOfRequestsFail OID: 1.3.6.1.4.1.3831.10.1.1.2.1.12	Counter64	エラーを生成した、この Identity Server に対するリクエスト数。
coreidTotalServiceTime OID: 1.3.6.1.4.1.3831.10.1.1.2.1.13	Counter64	Identity Server が前回の再起動後にリクエストの処理に要した合計時間 (ナノ秒単位)。

表 12-1 Identity Server の MIB オブジェクト (続き)

管理対象オブジェクト	構文	説明
coreidTotalNumOfCacheFlushRequestSuccess OID: 1.3.6.1.4.1.3831.10.1.1.2.1.14	Counter64	Identity Server により発行された、成功したキャッシュ・フラッシュ・リクエストの合計数。
coreidTotalNumOfCacheFlushRequestFail OID: 1.3.6.1.4.1.3831.10.1.1.2.1.15	Counter64	Identity Server により発行された、不成功のキャッシュ・フラッシュ・リクエストの合計数。
coreidNumOfPluginsLoaded OID: 1.3.6.1.4.1.3831.10.1.1.2.1.16	Counter64	Identity Server インスタンスによりロードされたプラグイン数。
coreidNumOfEmailSentFail OID: 1.3.6.1.4.1.3831.10.1.1.2.1.17	Counter64	この Identity Server インスタンスからの失敗した電子メール送信試行回数。
coreidOverflowFlagDirectoryServerSlots OID: 1.3.6.1.4.1.3831.10.1.1.2.1.18	Integer (0 ~ 65535)	ディレクトリ・サーバーに対して構成された SNMP 情報スロット数が不十分であることを示すフラグ。scoreboard_params.lst 内の変数 NumberOfConfiguredDS は、ディレクトリ・サーバーごとに 1 つのスロットを使用してスロット数を定義します。NumberOfConfiguredDs の値が、Identity Server がアクセスした実際のディレクトリ数よりも小さい場合、coreidOverflowFlagDirectoryServerSlots の値は 1 に設定されます。このフラグは、オーバーフロー条件のみ示します。足りないスロット数は示しません。
coreidOverflowForPPPActionsSlots OID: 1.3.6.1.4.1.3831.10.1.1.2.1.19	Integer (0 ~ 65535)	スロットを割り当てることのできなかった、フックアップされた ID イベント API プラグイン・アクションの数。

表 12-2 に、ID イベント API プラグインに関する情報を取得するための MIB オブジェクトを示します。これらのオブジェクトにより、ワークフローの外部イベントを作成できます。このプラグインの詳細は、『Oracle Access Manager 開発者ガイド』に記載されています。この表には、coreidHostname、coreidPort、pppRowIndex という 3 つの索引フィールドがあります。この情報へのパスは次のとおりです。

iso.org.dod.internet.private.enterprises.oblix.snmp.coreid.versionone.pppActionsTable

表 12-2 ID イベント API の MIB オブジェクト

管理対象オブジェクト	構文	説明
pppActionsTable	N/A	プライマリ表名。
pppRowIndex OID: 1.3.6.1.4.1.3831.10.1.1.3.1.2	Integer (0 ~ 65535)	このフィールドは、索引付けの目的でのみ使用されます。この値とその親索引値により、行の一意識別子が形成されます。
pppActionName OID: 1.3.6.1.4.1.3831.10.1.1.3.1.2	SnmpAdminString (サイズ 0 ~ 255)	PPP アクションの名前。
pppFunctionName OID: 1.3.6.1.4.1.3831.10.1.1.3.1.3	SnmpAdminString (サイズ 0 ~ 255)	特定のフックに対して実行される外部ファンクションの名前。
pppPluginPath OID: 1.3.6.1.4.1.3831.10.1.1.3.1.4	SnmpAdminString (サイズ 0 ~ 255)	PPP プラグインのパス。
totalCount OID: 1.3.6.1.4.1.3831.10.1.1.3.1.5	Counter64	PPP アクションが実行される合計回数。

表 12-2 ID イベント API の MIB オブジェクト (続き)

管理対象オブジェクト	構文	説明
pppOKCount OID: 1.3.6.1.4.1.3831.10.1.1.3.1.6	Counter64	この PPP アクションのリターン・コード STATUS_PPP_OK が受信された回数。
pppAbortCount OID: 1.3.6.1.4.1.3831.10.1.1.3.1.7	Counter64	この PPP アクションのリターン・コード STATUS_PPP_ABORT が受信された回数。
pppWorkflowRetryCount OID: 1.3.6.1.4.1.3831.10.1.1.3.1.8	Counter64	この PPP アクションのリターン・コード STATUS_PPP_WF_RETRY が受信された回数。
pppWorkflowAsyncCount OID: 1.3.6.1.4.1.3831.10.1.1.3.1.9	Counter64	この PPP アクションのリターン・コード STATUS_PPP_WF_ASYNC が受信された回数。

表 12-3 に、Identity Server と通信するディレクトリ・サーバーに関する情報を示します。この表には、coreidHostname、coreidPort、coreidDSRowIndex という 3 つの索引フィールドがあります。この情報へのパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.coreid.versionone.coreidDirectoryServerTable
```

表 12-3 ID システム・ディレクトリの MIB オブジェクト

管理対象オブジェクト	構文	説明
coreidDirectoryServerTable	N/A	プライマリ表名。
coreidDSRowIndex OID: 1.3.6.1.4.1.3831.10.1.1.4.1.1	Integer (0 ~ 65535)	このフィールドは、索引付けの目的でのみ使用されます。この値とその親索引値により、行の一意識別子が形成されます。
coreidDirectoryServerHost name OID: 1.3.6.1.4.1.3831.10.1.1.4.1.2	SnmpAdminString (サイズ 0 ~ 255)	ディレクトリ・サーバーのホスト名。
coreidDirectoryServerPort OID: 1.3.6.1.4.1.3831.10.1.1.4.1.3	Integer (0 ~ 65535)	ディレクトリ・サーバー・ポート。
coreidDirectoryServerMode OID: 1.3.6.1.4.1.3831.10.1.1.4.1.4	Integer (0 ~ 65535)	ディレクトリ・サーバー通信モード。 0: オープン 1: SSL
coreidDirectoryServerNoOf LiveConnections OID: 1.3.6.1.4.1.3831.10.1.1.4.1.5	Integer (0 ~ 65535)	ディレクトリに対する接続数。

表 12-4 に、MIB 内の、SNMP トラップにマップできるシステム・イベントの ID システム・オブジェクトを示します。

SNMP エージェントでは、複数の NMS システムに対するトラップ・メッセージの送信がサポートされます。この情報へのパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.coreid.versionone
```

たとえば、oblixCoreidServerDown トラップへのフルパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.coreid.versionone.oblixCoreidServerDown
```

表 12-4 Identity Server トラップ

管理対象オブジェクト	トラップで送信されるフィールド	説明
oblixCoreidServerDown OID: 1.3.6.1.4.1.3831.10.1.1.0.7001	coreidId coreidHostname coreidPort	Identity Server の停止がエラーで終了したことが SNMP エージェントにより検出された場合に生成されるトラップ。このトラップには、サーバー ID、ホスト名およびポートが含まれます。
oblixCoreidServerStart OID: 1.3.6.1.4.1.3831.10.1.1.0.7002	coreidId coreidHostname coreidPort	このトラップは、Identity Server が起動または再起動されたことが SNMP エージェントにより検出された場合に生成されます。このトラップには、サーバー ID、ホスト名およびポートが含まれます。
oblixCoreidServerFailure OID: 1.3.6.1.4.1.3831.10.1.1.0.7003	coreidId coreidHostname coreidPort	このトラップは、Identity Server が正しく停止されていないか障害が発生したことが SNMP エージェントにより検出された場合に生成されます。このトラップには、サーバー ID、ホスト名およびポートが含まれます。
oblixCOREidDSFailure OID: 1.3.6.1.4.1.3831.10.1.1.0.7004	coreidId coreidHostname coreidPort coreidDirectoryServer Hostname coreidDirectoryServer Port	このトラップは、接続先のディレクトリ・サーバーが停止していることを Identity Server が検出した場合に生成されます。

Access Server の MIB オブジェクト

表 12-5 に、MIB を通じて使用可能な Access Server SNMP オブジェクトを説明します。この情報へのパスは次のとおりです。

iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.versionone

表 12-5 Access Server の MIB オブジェクト

管理対象オブジェクト	構文	説明
aaaInstanceTable OID: 1.3.6.1.4.1.3831.10.2.1.2	N/A	プライマリ表名。
aaaId OID: 1.3.6.1.4.1.3831.10.2.1.2.1.1	SnmpAdminString (サイズ 0 ~ 255)	アクセス・システム・コンソールで指定された、この Access Server インスタンスの識別子。
aaaHostname OID: 1.3.6.1.4.1.3831.10.2.1.2.1.2	SnmpAdminString (サイズ 0 ~ 255)	アクセス・システム・コンソールで指定された、Access Server がインストールされたマシンの名前。ホスト名は、この表の索引です。
aaaPort OID: 1.3.6.1.4.1.3831.10.2.1.2.1.3	Integer (0 ~ 65535)	Access Server がリスニングするポート。ポート番号は、この表の索引です。
aaaMode OID: 1.3.6.1.4.1.3831.10.2.1.2.1.4	Integer (0 ~ 65535)	Access Server と他の ID コンポーネントまたはアクセス・コンポーネント間のトランスポート・セキュリティ・モード。 0: オープン 1: 簡易 2: 証明書
aaaNoOfQueues OID: 1.3.6.1.4.1.3831.10.2.1.2.1.5	Integer (0 ~ 65535)	この Access Server インスタンスのサービス・キューの数。
aaaThreadsPerQueue OID: 1.3.6.1.4.1.3831.10.2.1.2.1.6	Integer (0 ~ 65535)	この Access Server インスタンスの各サービス・キューのスレッド数。
aaaNoOfListenerThreads OID: 1.3.6.1.4.1.3831.10.2.1.2.1.7	Integer (0 ~ 65535)	起動されたリスナー・スレッド数。 WebGate-Access Server 接続ごとに 1 つのスレッドがあります。
aaaNoofConnectionWatcherThreads OID: 1.3.6.1.4.1.3831.10.2.1.2.1.8	Integer (0 ~ 65535)	LDAP 接続ウォッチャ・スレッド数。
aaaOverflowFlagDirectoryServerSlots OID: 1.3.6.1.4.1.3831.10.2.1.2.1.9	Integer (0 ~ 65535)	Access Server に対して構成されたディレクトリ数に対してスロット数が不十分かどうかを示すフラグ。これは、管理者がファイル <i>install_dir/access/oblix/config/obscoreboardparams.xml</i> を更新する必要があることを意味します。 0: オーバーフローしていない 1: オーバーフローが発生
aaaOverflowForAuthenticationPluginSlots OID: 1.3.6.1.4.1.3831.10.2.1.2.1.10	Integer (0 ~ 65535)	情報を表示できなかった認証プラグインの数。管理者は、 <i>install_dir/access/oblix/config/obscoreboardparams.xml</i> ファイルを更新する必要があります。
aaaOverflowForAuthorizationPluginSlots OID: 1.3.6.1.4.1.3831.10.2.1.2.1.11	Integer (0 ~ 65535)	情報を表示できなかった認可プラグインの数。管理者は、 <i>install_dir/access/oblix/config/obscoreboardparams.xml</i> ファイルを更新する必要があります。

表 12-5 Access Server の MIB オブジェクト (続き)

管理対象オブジェクト	構文	説明
aaaTimeAuditLogWasRotated OID: 1.3.6.1.4.1.3831.10.2.1.2.1.12	DateAndTime	監査ログ・ファイルのローテーションが行われた時刻。この設定は、アクセス・システム・コンソールで指定された、この Access Server の構成で決定されます。
aaaStartTime OID: 1.3.6.1.4.1.3831.10.2.1.2.1.13	DateAndTime	この Access Server インスタンスを最後に起動した日時。
aaaAuthenticationsSuccess OID: 1.3.6.1.4.1.3831.10.2.1.2.1.14	Counter64	Access Server インスタンスによる成功した認証の回数。
aaaAuthenticationsSuccess OID: 1.3.6.1.4.1.3831.10.2.1.2.1.15	Counter64	この Access Server インスタンスによる成功した認証の回数。
aaaAuthenticationsDenied OID: 1.3.6.1.4.1.3831.10.2.1.2.1.16	Counter64	この Access Server インスタンスによる不成功の認証の回数。
aaaAuthorizationsSuccess OID: 1.3.6.1.4.1.3831.10.2.1.2.1.17	Counter64	この Access Server インスタンスによる成功した認可の回数。
aaaAuthorizationsDenied OID: 1.3.6.1.4.1.3831.10.2.1.2.1.18	Counter64	この Access Server インスタンスによる不成功の認可の回数。
aaaAuditRequests OID: 1.3.6.1.4.1.3831.10.2.1.2.1.19	Counter64	この Access Server インスタンスによって行われた監査リクエストの数。

表 12-6 は、Access Server と通信するディレクトリ・サーバーを説明する MIB オブジェクトのサブ表です。このサブ表には、aaaHostname、aaaPort および aaaRowIndex という索引フィールドがあります。この情報へのパスは次のとおりです。

iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.versionone.aaaDirectoryServerTable

表 12-6 アクセス・システム・ディレクトリ・サーバーの MIB オブジェクト

管理対象オブジェクト	構文	説明
aaaDirectoryServerTable OID: 1.3.6.1.4.1.3831.10.2.1.3	N/A	プライマリ表名。
aaaDSRowIndex OID: 1.3.6.1.4.1.3831.10.2.1.3.1.1	Integer (0 ~ 65535)	索引フィールド。情報は含まれていません。
aaaDirectoryServerHostname OID: 1.3.6.1.4.1.3831.10.2.1.3.1.2	SnmpAdminString (サイズ 0 ~ 255)	ディレクトリ・ホスト名。
aaaDirectoryServerPort OID: 1.3.6.1.4.1.3831.10.2.1.3.1.3	Integer (0 ~ 65535)	ディレクトリ・サーバー・ポート。
aaaDirectoryServerMode OID: 1.3.6.1.4.1.3831.10.2.1.3.1.4	Integer (0 ~ 65535)	Access Server とのディレクトリ・サーバー通信モード。 0: オープン 1: SSL
aaaDirectoryServerNoOfLiveConnections OID: 1.3.6.1.4.1.3831.10.2.1.3.1.5	Integer (0 ~ 65535)	Access Server とディレクトリ・サーバー間の接続数。

表 12-7 は、認証プラグインに関する情報を取得するための MIB オブジェクトのサブ表です。このサブ表には、aaaHostname、aaaPort および authenticationPluginName という索引フィールドがあります。この情報へのパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.
versionone.aaaauthenticationPluginsTable
```

表 12-7 認証プラグインの MIB オブジェクト

管理対象オブジェクト	構文	説明
authenticationPluginsTable OID: 1.3.6.1.4.1.3831.10.2.1.4	N/A	プライマリ表名。
authenticationPluginName OID: 1.3.6.1.4.1.3831.10.2.1.4.1.1	SnmpAdminString (サイズ 0 ~ 255)	プラグインの名前。認証プラグイン名は、この表の索引です。
AuthenticationPluginPath OID: 1.3.6.1.4.1.3831.10.2.1.4.1.2	SnmpAdminString (サイズ 0 ~ 255)	認証プラグインのパス。
AuthenticationPluginStatus OID: 1.3.6.1.4.1.3831.10.2.1.4.1.3	Integer (0 ~ 65535)	プラグインのステータス。 0: ロードされていない 1: ロード済

表 12-8 の authorizationPluginsTable には、aaaHostname、aaaPort および authorizationPluginName という索引フィールドがあります。この情報へのパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.
versionone.authorizationsPluginsTable
```

表 12-8 認可プラグインの MIB オブジェクト

管理対象オブジェクト	構文	説明
authorizationPluginsTable OID: 1.3.1.4.1.3831.10.2.1.5	N/A	プライマリ表名。
authorizationPluginName OID: 1.3.6.1.4.1.3831.10.2.1.5.1.1	SnmpAdminString (サイズ 0 ~ 255)	このプラグインの名前。
AuthorizationPluginPath OID: 1.3.6.1.4.1.3831.10.2.1.5.1.2	SnmpAdminString (サイズ 0 ~ 255)	認可プラグインのパス。
AuthorizationPluginStatus OID: 1.3.6.1.4.1.3831.10.2.1.5.1.3	Integer (0 ~ 65535)	プラグインのステータス。 0: ロードされていない 1: ロード済

表 12-9 は、Access Server のキュー内のリクエスト数を記述するサブ表です。この表には、aaaHostname、aaaPort および aaaRequestQueueNumber という索引があります。この情報へのパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.
versionone.requestQueueInfoTable
```

表 12-9 リクエスト・キューの MIB オブジェクト

管理対象オブジェクト	構文	説明
requestQueueInfoTable OID: 1.3.6.1.4.1.3831.10.2.1.5	N/A	プライマリ表名。
aaaRequestQueueNumber OID: 1.3.6.1.4.1.3831.10.2.1.6.1.1	Integer (0 ~ 65535)	リクエスト・キューの索引。
aaaRequestQueueSize OID: 1.3.6.1.4.1.3831.10.2.1.6.1.2	Integer (0 ~ 65535)	キュー内のリクエスト数。

表 12-10 は、MIB 内の、SNMP トラップにマップできるシステム・イベントのオブジェクトを示します。SNMP エージェントでは、複数の NMS システムに対するトラップ・メッセージの送信がサポートされます。この情報へのパスは次のとおりです。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.versionone
```

たとえば、oblixAAAServerDown トラップへのフルパスを追加するには、次のように指定します。

```
iso.org.dod.internet.private.enterprises.oblix.snmp.aaa.versionone.oblixAAAServerDown
```

表 12-10 Access Server トラップ

管理対象オブジェクト	トラップで送信されるフィールド	説明
oblixAAAServerDown OID: 1.3.6.1.4.1.3831.10.2.1.0.7001	aaaId aaaHostname aaaPort	Access Server が正しく停止したことが SNMP エージェントにより検出された場合に生成されるトラップ。このトラップには、Access ServerID、ホスト名およびポートが含まれます。
oblixAAAServerStart OID: 1.3.6.1.4.1.3831.10.2.1.0.7002	aaaId aaaHostname aaaPort	Access Server が再起動されるたびに生成されるトラップ。このトラップには、Access ServerID、ホスト名およびポートが含まれます。トラップは即時に生成されるため、再起動の時刻はトラップ生成の時刻です。
oblixAAAServerFailure OID: 1.3.6.1.4.1.3831.10.2.1.0.7003	aaaId aaaHostname aaaPort	Access Server の停止がエラーのため行われなかったか障害が発生したことが SNMP エージェントにより検出された場合に生成されるトラップ。このトラップには、Access ServerID、ホスト名およびポートが含まれます。
oblixAAADSFailure OID: 1.3.6.1.4.1.3831.10.2.1.0.7004	aaaId aaaHostname aaaPort aaaDirectoryServer Hostname aaaDirectoryServerPort	接続先のディレクトリ・サーバーが停止していることを Access Server が検出した場合に生成されるトラップ。

SNMP モニタリングの有効化および無効化

Identity Server および Access Server の構成ページを使用して、SNMP を有効にし、SNMP エージェントとの接続が確立される TCP/IP ポートを指定します。

注意： Oracle Access Manager には、SNMP 統計を取得するためのポーリング間隔の構成設定は用意されていません。ただし、ほとんどの NMS システムには、ポーリング構成パラメータが用意されています。このパラメータは、エージェントを定期的にポーリングして MIB 値を取得するために NMS によって使用されます。

次の手順では、Oracle Access Manager SNMP エージェントの起動および停止方法と、別のポート上のエージェントの起動方法を説明します。

SNMP 統計の収集を構成する手順

1. ID (またはアクセス) システム・コンソールで、「システム構成」、「Identity Server」(または「Access Server」) を選択します。
2. 特定のサーバーのリンクをクリックします。
3. 「変更」ボタンを選択して、次のように SNMP モニタリングをオンまたはオフにできるページを表示します。
 - **オンにする：**ページの下部にある「SNMP 状態オン」ボタンを選択します。
 - **オフにする：**ページの下部にある「SNMP 状態オフ」ボタンを選択します。
4. 「SNMP エージェント登録ポート」フィールドにポート番号を入力して、SNMP エージェントがリスニングするポートを定義または変更します。
5. Identity Server (または Access Server) を再起動します。

SNMP エージェントおよびトラップの宛先の設定

次のコマンドを使用して、SNMP マネージャに対して SNMP エージェントを設定します。

```
setup_agent -i
```

-i オプションは必須です。

次の手順では、Oracle Access Manager SNMP エージェントおよびトラップの宛先の構成方法を説明します。

SNMP エージェントおよびトラップの宛先の構成手順

1. SNMP `setup_agent` コマンドを含むディレクトリに変更します。

次に例を示します。

```
> cd $SNMPDIR/oblix/tools/setup
```

`SNMPDIR` は、SNMP エージェントをインストールしたディレクトリです。

2. 次のオプションとともに `setup_agent` コマンドを使用します。

```
-i <install_dir>
```

```
-g 一般パラメータの構成
```

```
-u <エージェント SNMP UDP ポート >
```

```
-c <エージェント・コミュニティ文字列 >
```

```
-p <エージェント TCP ポート >
```

```
-S <サイレント・モードで実行 >
```

--help ヘルプ・メッセージを出力

トラップ先をサイレント・モードで追加する手順

1. SNMP setup_agent コマンドを含むディレクトリに変更します。

次に例を示します。

```
> cd $SNMPDIR/oblix/tools/setup
```

2. 次のオプションとともに setup_agent コマンドを使用します。

```
-a
```

```
-m <マネージャ・ステーション>
```

```
-t <トラップ・ポート>
```

トラップ先をサイレント・モードで削除する手順

1. SNMP setup_agent コマンドを含むディレクトリに変更します。

次に例を示します。

```
> cd $SNMPDIR/oblix/tools/setup
```

2. 次のオプションとともに setup_agent コマンドを使用します。

```
-d
```

```
-m <マネージャ・ステーション>
```

```
-t <トラップ・ポート>
```

最初に一般パラメータを構成する手順

1. SNMP setup_agent コマンドを含むディレクトリに変更します。

次に例を示します。

```
> cd $SNMPDIR/oblix/tools/setup
```

2. 次の setup_agent コマンドを使用します。

```
> ./setup_agent -i $SNMPDIR -g -u <UDP Port> -c public -p <TCP Port>
```

これにより、「マネージャ・ステーション・トラップ構成」メニューに移動します。

一般パラメータの直後に SNMP マネージャを追加する手順

1. SNMP setup_agent コマンドを含むディレクトリに変更します。

次に例を示します。

```
> cd $SNMPDIR/oblix/tools/setup
```

2. 次の setup_agent コマンドを使用します。

```
> ./setup_agent -i $SNMPDIR -a -m <Mgr M/c> -t <Mgr Port>
```

SNMP マネージャを追加した直後に削除する手順

1. SNMP setup_agent コマンドを含むディレクトリに変更します。

次に例を示します。

```
> cd $SNMPDIR/oblix/tools/setup
```

2. 次の setup_agent コマンドを使用します。

```
> ./setup_agent -i $SNMPDIR -d -m <Mgr M/c> -t <Mgr Port>
```

任意の数のマネージャ・ステーションを追加できます。エージェントは、すべてのトラップを構成済の SNMP マネージャに送信します。

SNMP 構成設定の変更

obscoreboard_params.xml という名前の構成ファイルには、SNMP 統計のコレクションを定義する情報が含まれています。このファイルは次の場所にあります。

`Component_install_dir/identity|access/oblix/config`

`Component_install_dir` はコンポーネントがインストールされているディレクトリで、`identity|access` はそれぞれ Identity Server と Access Server を表します。

ID システム・ファイル: obscoreboard_params.xml

アクセス・システム・ファイル: obscoreboard_params.xml

このファイルでは、様々な MIB カウンタがいつアクティブになるかを決定するためのしきい値レベルを構成できます。

次のパラメータは、Access Server ファイル obscoreboard_params.xml でのみ指定されます。

- **NumberOfAuthenticationPlugins:** アクセス・システムにロードできる認証プラグインの最大数。Access Server では、ロードされているプラグイン数に関する情報がメンテナンスされます。Access Server により実際にロードされたプラグイン数が `NumberOfAuthenticationPlugins` に対して指定された値を超えた場合は、その差異がカウンタ `aaaOverflowforAuthenticationPluginSlots` として表示されます。
- **NumberOfAuthorizationPlugins:** アクセス・システムにロードできる認可プラグインの最大数。Access Server では、ロードされているプラグイン数に関する情報がメンテナンスされます。Access Server により実際にロードされたプラグイン数が `NumberOfAuthorizationPlugins` に対して指定された値を超えた場合は、その差異がカウンタ `aaaOverflowforAuthorizationPluginSlots` として表示されます。

次のパラメータは、Identity Server ファイル obscoreboard_params.xml でのみ指定されます。

- **NumberOfPPPPluginActions:** この Identity Server に接続できる ID イベント API プラグイン・アクションの数。Identity Server は、起動時にこの値を読み込み、ID イベント API プラグインの実際の数をモニターします。アクティブなプラグインの数が `NumberOfPPPPluginActions` の値を超えた場合は、その差異がカウンタ `coreidOverflowForPPPACTIONSLOTS` で示されます。

次のパラメータは、両方のスコアボード・ファイルで提供されます。

- **NumberOfServiceThreads:** このパラメータの値は、起動時に Identity Server または Access Server によって読み取られます。このパラメータは、各サービス・スレッドの SNMP 情報をメンテナンスするために（サービス・スレッドごとに 1 つ）割り当てるスロット数を制御します。サーバーは、使用されているサービス・スレッド数をモニターします。実際のサービス・スレッド数の構成は、管理コンソールで、コマンドラインから、または構成ファイルの一部として行います。このパラメータは、Identity Server が開始するスレッド数を制御しません。実際に使用されている数がこの値を超えた場合、超過スレッドについて SNMP データは生成されません。
- **NumberOfConfiguredDS:** この Identity Server または Access Server に対して構成されているディレクトリ・サーバー数。
- **DsFailureTrapTimeSpan:** 同じディレクトリ・サーバーに次の失敗トラップを送信する前に待機する時間。
- **NumOfSlotsInEventQueue:** イベント・キューで使用するスロット数。トラップが検出されない場合は、このパラメータを更新する必要があります。ただし、デフォルト値の 5 はほとんどのインストール環境に十分な値です。
- **SleepTimeInMilliSec:** SNMP エージェントが稼働しているかどうかを Identity Server または Access Server がチェックする間隔（ミリ秒単位）。
- **semaphore_filepath:** Access Server によって作成されたセマフォに関する情報。セマフォは、コンポーネント（Identity Server または Access Server）と SNMP エージェント間の同期に使用されます。この情報は、コンポーネントに障害が発生した場合にセマフォを自動的にクリーン・アップするために使用されます。
- **semaphore_id:** エージェント・セマフォ識別子。

この設定の変更は、SNMP データ収集に使用されるメモリー・マップ・ファイルに影響します。UNIX では、メモリー・マップ・ファイルは次の場所にあります。

```
/tmp/netpoint/scoreboard/component/process-id.osb
```

Windows では、このファイルは次の場所にあります。

```
Component_install_dir/oblix/scoreboard/process-id.osb
```

SNMP のロギング

SNMP エージェントでは、ロギングがサポートされます。SNMP エージェントが有効になると、常に一定のログ・レベルに設定されます。SNMP ログはトラブルシューティングに役立ちます。ログに記録する内容および生成するログのタイプをエージェント構成ファイルで構成できます。このファイルは次の場所にあります。

```
SNMP_install_dir/oblix/config/snmp_agent_config_info.xml
```

`SNMP_install_dir` は、SNMP エージェントがインストールされているディレクトリです。

エージェント構成ファイルの `log_level` パラメータには、次のいずれかの値があります。

- 0: デバッグ
- 1: 情報
- 2: 警告
- 3: エラー
- 4: ロギングなし (ロギングがオフ)

SNMP メッセージ

次に、SNMP 関連メッセージを示します。

メッセージ:

```
MErrNoConfigFile {Could not find agent configuration file at location (full path to the agent configuration file)}
```

説明: インストール・ディレクトリが正しくないか、構成ファイルが存在しません。SNMP エージェントをアンインストールし、再インストールします。

メッセージ:

```
MLogAgentStarted {Agent successfully started on port SNMP port number}
```

説明: ステータス・メッセージ。

メッセージ:

```
MErrAddressInUse {Agent was not able to bind to port port number, address already in use}
```

説明: SNMP エージェントは、構成されている TCP 登録ポートにバインドできません。別の TCP ポートを使用するようにエージェントを再構成するか、ポートを使用してアプリケーションを停止することでポートを使用可能にします。

注意: エージェント TCP 登録ポートを変更する場合は、適切なシステム・コンソールを使用して Identity Server または Access Server に対して SNMP を有効にするときに、新しいポートを指定する必要があります。

メッセージ:

Agent was not able to bind to specified port, system lacked sufficient buffer space or queue was full.

説明: SNMP エージェント・ポートが使用不能です。

メッセージ:

MErrTLUnsupported {Agent was not able to bind to specified port, address family not supported by protocol family}

説明: 指定されたポートで SNMP がサポートされていません。別のポートを構成します。

メッセージ:

MErrRetrieveIDs {Error: Unable to determine the uid/gid for which this snmp agent is installed.}

説明: SNMP エージェントを起動しようとしたユーザーに適切な権限がありません。ユーザーは、ルート・ユーザーまたはエージェントをインストールしたユーザーとして SNMP エージェントを起動する必要があります。

メッセージ:

MErrCouldNotSetIDs {Error: You don't have sufficient access rights to run this snmp agent.}

説明: SNMP エージェントをインストールできる管理権限でログインする必要があります。そうしないと、エージェントを実行できません。

メッセージ:

MLogAlreadyRunning {Agent is already running with process id (Process identifier of the agent).}

説明: ユーザーは、すでに実行されているエージェントを起動しようとしています。

メッセージ:

MErrRegBindFailed {Error: Unable to bind to configured registration port (configured registration port number).}

説明: SNMP エージェントは、Oracle Access Manager サーバー構成ページで構成されたポートにバインドできません。12-13 ページの「SNMP モニタリングの有効化および無効化」の説明に従って別のポートを指定します。

メッセージ:

MErrRegListenFailed {Error: Unable to start listening on configured registration port (configured registration port number).}

説明: このメッセージは、ポートが別のアプリケーションですでに使用されている場合に Windows に表示されます。

メッセージ:

MErrReadingMsg {Error reading message sent by component.}

説明: SNMP エージェントと Oracle Access Manager サーバーは TCP 接続を通じて通信します。エージェントは、不正な形式のメッセージを検出した場合に、エラーをログに記録します。

メッセージ:

MErrNotRegMsg {Error: Agent expects only registration messages on the registration socket.}

説明: エージェントは、接続先のサーバーからの TCP 接続に関する登録メッセージのみ想定します。メッセージが登録メッセージでないことを検出した場合は、エラーをログに記録します。

メッセージ:

`MErrMissingMmapFilename {Error: Registration message was missing the component scoreboard file name.}`

説明: Identity Server または Access Server は、エージェントによって読み取られた統計をスコアボード・ファイルに格納します。この名前は、登録時にサーバーからエージェントに通知されます。登録リクエストにファイル情報がない場合は、このメッセージがログに記録されます。

メッセージ:

`MErrMappingScoreboard {Error: Unable to memory map the scoreboard file (full path to the scoreboard file) registered by component.}`

説明: このエラーは、ファイル権限に問題があるため、エージェントがスコアボード・ファイルを読み取れない、または開けない場合に発生することがあります。

メッセージ:

`MErrUnknownComponent {Error: Unknown component type specified in scoreboard file.}`

説明: コンポーネント・タイプは、登録リクエストで指定されます。エージェントは、Identity Server および Access Server に関する情報を処理します。コンポーネント・タイプがそのどちらでもない場合は、このメッセージがログに記録されます。

メッセージ:

`MErrIndexExists {Error: A component has already registered in table (OID for the table for that component) with index (index that is already in use by some other component).}`

説明: コンポーネントの同じインスタンスが再び登録を試行しました。コンポーネントの各インスタンスは、同じ SNMP エージェントによってキーまたは索引で一意に識別されます。別のコンポーネント・インスタンスが同じキーまたは索引を使用して登録を試行した場合は、このメッセージがログに記録されます。

メッセージ:

`MErrCreatingAgentSemaphore {Error: Unable to create named semaphore (full path to the agent semaphore file) for agent-component event dispatching.}`

説明: エージェントおよびコンポーネントは、停止時にクリーン・アップされるセマフォを1つ作成します。クリーンでない停止が行われた場合、セマフォは次のサーバー / エージェント起動時に削除されます。考えられる原因として、システムのセマフォが不足したこと、またはセマフォの作成中に権限の問題が発生したことがあります。

メッセージ:

`MErrOnSelect {Error: Select() call returned error code (error code returned for the select() call).}`

説明: これは、ファンクションから直接返されるエラー・コードです。このメッセージは、トラブルシューティングの目的に使用されます。

メッセージ:

`MErrOnPoll {Error: Poll() call returned error code (error code returned for the poll() call).}`

説明: これは、ファンクションから直接返されるエラー・コードです。このメッセージは、トラブルシューティングの目的に使用されます。

メッセージ:

`MErrNotDeregMsg {Error: Agent expected a de-registration message on the socket, instead got a message with code (message code for the message received).}`

説明: エージェントは、コンポーネントの登録後にコンポーネントからの登録解除メッセージのみ想定します。

メッセージ:

```
MErrRemovingComponent {Error: Component with table oid (OID for the table for that component) and index (index which identifies the component in that table) could not be removed.}
```

説明: コンポーネントはすでに登録解除されていますが、そのコンポーネントの削除のリクエストが行われました。

メッセージ:

```
MErrMissingEvent {Error: Unable to retrieve event from component with table oid (OID for the table for that component) and index (index which identifies the component in that table).}
```

説明: コンポーネントはエージェントにイベントを送信し、エージェントはこのイベントを適切なトラップに変換します。コンポーネントは、イベントをディスパッチしたこともエージェントに通知します。エージェントが通知を受け、イベントが見つからない場合は、このメッセージがログに記録されます。

メッセージ:

```
MErrMissingTrapData {Error: Missing trap meta-data for component from table oid (OID for the table) and index (index that identifies the component in that table) with event (event identifier supplied by the component).}
```

説明: コンポーネントは、イベントの完全なデータを配信しませんでした。

メッセージ:

```
MLogMappedScoreboard {Mapped scoreboard file (full path to the scoreboard file) for a component.}
```

説明: これはステータス・メッセージです。

メッセージ:

```
MLogComponentRegistered {Component registered with table oid (OID for the table) and index (index that identifies the component).}
```

説明: これはステータス・メッセージです。

メッセージ:

```
MLogComponentDeregistered {Component with table oid (OID for the table) and index (index that identifies the component) de-registered.}
```

説明: これはステータス・メッセージです。

メッセージ:

```
MLogComponentFailed {Component with table oid (OID for the table) and index (index that identifies the component) failed.}
```

説明: これは、Oracle Access Manager コンポーネントが正しく登録解除されなかったことを示すステータス・メッセージです。このアクションは、SNMP エージェントによってコンポーネント障害として扱われます。

メッセージ:

```
MLogSentTrap {Sent trap with trap oid (OID for the trap sent) for component with table oid (OID for the component table) and index (index that identifies the component in the table).}
```

説明: これはステータス・メッセージです。

メッセージ:

MLogSemCleanup {Found left-over semaphore from previous run with key (key for the stale left-over semaphore) and file path (file path for the stale left-over semaphore), successfully cleaned up the semaphore.}

説明:ステータス・メッセージ。エージェントおよびコンポーネントは、停止時にクリーン・アップされるセマフォを1つ作成します。クリーンでない停止が行われた場合、セマフォは次のサーバー / エージェント起動時に削除されます。

メッセージ:

MErrSemCleanup {Found left-over semaphore with key (key for the stale left-over semaphore) and file path (file path for the stale left-over semaphore). Encountered errors while removing it.}

説明:エージェントおよびコンポーネントは、停止時にクリーン・アップされるセマフォを1つ作成します。クリーンでない停止が行われた場合、セマフォは次のサーバー / エージェント起動時に削除されます。このメッセージは、前回の実行からのセマフォのクリーンアップ中にエージェントがエラーを検出した場合にログに記録されます。権限に問題がある可能性があります。

メッセージ:

MSBCreateFailed {Access Server: Could not create scoreboard file (full path for the file) with size file size.}

説明:このメッセージについて考えられる原因として、領域の不足によりシステムがファイルを生成できなかったことがあります。

メッセージ:

MCreateSemFailed {Access Server: Could not create event queue semaphore with path full path.}

説明:エージェントおよびコンポーネントは、停止時にクリーン・アップされるセマフォを1つ作成します。クリーンでない停止が行われた場合、セマフォは次のサーバー / エージェント起動時に削除されます。このメッセージは、システムのセマフォが不足した場合、またはセマフォの作成中に権限の問題が発生した場合に生成されます。マシンのセマフォの制限を増やしてください。

メッセージ:

MSBDirCreateFailed {Access Server: Could not create scoreboard file file name.}

説明:おそらく権限が十分でないために、システムはスコアボード・ファイルに必要なディレクトリを作成できませんでした。

Netstat 値と SNMP 値の差異

netstat コマンドを使用している場合、このコマンドで返される値は、必ずしも MIB 変数に対して収集される情報と一致しません。

```
aaaDirectoryServerNoOfLiveConnections
coreidDirectoryServerNoOfLiveConnections
```

表 12-11 では、この差異が生じる理由と、発生するイベントのチェーンを説明します。

表 12-11 Netstat 値および表示されるライブ接続数

イベント	ライブ接続数	Netstat 値	コメント
サーバーの起動と、それに続くディレクトリ・サーバー・アクセス。	5	5	
ディレクトリ・サーバーがダウンします。	5	0	Oracle Access Manager は、リクエストを受信しないかぎりカウンタを更新しません。
Oracle Access Manager は、リクエストを処理しているディレクトリ・サーバーにアクセスするために接続を使用しようとします。	4	0	ディレクトリ・サーバーが停止しているため、ディレクトリ・サーバー・アクセスはエラーを返します。接続は停止としてマークされ、NumberOfLiveConnections が 1 つ減らされます。
ディレクトリ・サーバーが再起動され、Oracle Access Manager は切断した接続を再確立しようとします。	5	1	新規接続が形成され、NumberOfLiveConnections が 1 つ増やされます。残りの 4 つの接続すべてが停止としてマークされ、新しい接続が形成されるまで、NumberOfLiveConnections と Netstat 値には差異が見られます。残りの 4 つの接続のステータスは、使用されるまで表示可能になりません。
Oracle Access Manager は、切断した接続をすべて再確立します。	5	1	netstat 値は、すべての接続が形成された後でのみ NumberOfLiveConnections と一致します。

停止間隔の構成

ID コンポーネントまたはアクセス・コンポーネントが正しい停止を実行できるようにするには、すべてのクリーンアップ・アクティビティを完了するのに十分な時間を割り当てる必要があります。Identity Server、Access Server および SNMP エージェントの場合は、shutdown_time パラメータで、サーバーが正しい停止を試行するために割り当てる時間を指定します。このパラメータは、globalparams.xml 内にあります。デフォルトの停止時間は 5 秒です。

globalparams ファイルの場所は次のとおりです。

Access Server の場合：

```
AccessServer_install_dir/access/oblix/apps/common/bin/globalparams.xml
```

Identity Server の場合：

```
Identity_install_dir/identity/oblix/apps/common/bin/globalparams.xml
```

デフォルトの停止時間は、これらのファイルに次のように表示されます。

```
shutdown_time:5
```

値は、秒数で指定した任意の時間に変更できます。

第 IV 部

付録

ここに示す情報は、Oracle Access Manager を Microsoft Active Directory 用に構成し、.NET 機能を実装するのに役立ちます。索引も提供されています。

第 IV 部の内容は次のとおりです。

- [付録 A 「Active Directory でのデプロイ」](#)
- [付録 B 「ADSI に対する構成」](#)
- [付録 C 「LDAP を使用する Active Directory に対する構成」](#)
- [付録 D 「.NET 機能の実装」](#)
- [付録 E 「Oracle Access Manager パラメータ・ファイル」](#)
- [付録 F 「Oracle Access Manager のトラブルシューティング」](#)

Active Directory でのデプロイ

『Oracle Access Manager インストレーション・ガイド』のアクティビティを完了して Oracle Access Manager を Active Directory とともにインストールし、設定した後で、ここに示すアクティビティを実行して、日常的な使用とメンテナンス用にこれらのコンポーネントを構成できます。

この付録の内容は次のとおりです。

- [ディレクトリ・プロファイルと検索ベースの設定](#)
- [Active Directory での認証および認可](#)
- [credential_mapping プラグインの構成](#)
- [Active Directory で使用するシングル・サインオンの構成](#)
- [検索フィルタについて](#)
- [SAMAccountName の長さについて](#)
- [.NET 機能の構成](#)
- [トラブルシューティング](#)
- [Microsoft リソース](#)

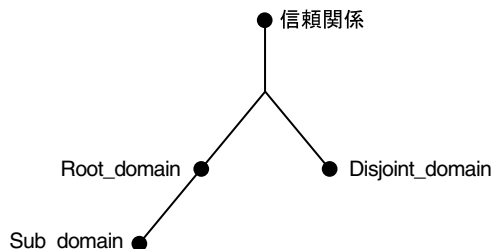
追加情報と手順は、『Oracle Access Manager インストレーション・ガイド』を参照してください。次の項も参照してください。

- [付録 B 「ADSI に対する構成」](#)
- [付録 C 「LDAP を使用する Active Directory に対する構成」](#)

ディレクトリ・プロファイルと検索ベースの設定

図 A-1 に示す Active Directory フォレストには、Root_domain、Sub_domain、Disjoint_domain という 3 つのドメインが含まれます。図 A-1 の構成は、この後の説明で参照します。

図 A-1 単一の Active Directory フォレスト内の 3 つのドメイン



『Oracle Access Manager インストール・ガイド』の説明に従って Active Directory のインストールおよび設定を終了すると、次のタスクを実行する準備ができます。

- [他のドメインのディレクトリ・サーバー・プロファイルの定義](#)
- [非結合検索ベースの設定](#)
- [グループ検索読み取り操作の構成 \(オプション\)](#)

他のドメインのディレクトリ・サーバー・プロファイルの定義

デフォルトのディレクトリ・サーバー・プロファイルは、Identity Server をインストールして新規ディレクトリ・サーバーの接続情報を指定するたびに自動的に作成されます。ディレクトリ・サーバー・プロファイルには、同じネームスペースおよび読み取り、書き込み、検索などの操作要件を共有する 1 つ以上のディレクトリ・サーバーの接続情報が含まれます。接続情報には、名前、適用されるドメインまたはネームスペース、ディレクトリ・タイプ、および操作のセットが含まれます。

注意： デフォルトのディレクトリ・サーバー・プロファイルは、Root_domain に対してのみ作成されます。インストール環境の他のドメイン (Disjoint_domain と Sub_domain など) のディレクトリ・プロファイルを設定する必要があります。

インストール後に、次の手順で概説するように、ID システム・コンソールを使用してディレクトリ・サーバー・プロファイルを変更できます。次の手順が完了したら、非結合検索ベースを設定できます。

詳細は、7-20 ページの「[ディレクトリ・サーバー・プロファイルの管理](#)」を参照してください。

追加のディレクトリ・サーバー・プロファイルを設定する手順

1. ID システム・コンソールにナビゲートします。
`http://hostname:port/identity/Obliv`
2. ディレクトリ・サーバー・プロファイルにナビゲートします（「ID システム・コンソール」、「システム管理」、「システム構成」、「ディレクトリ・オプションの構成」、リンク）。
3. 7-20 ページの「ディレクトリ・サーバー・プロファイルの管理」の説明に従って、Disjoint_domain のプロファイルを追加します（存在する場合）。
4. Sub_domain のプロファイルを追加します。
5. ID システムの設定時に収集されたデフォルト名が無意味な場合は、デフォルトのディレクトリ・プロファイルの名前を変更します。
6. 次に説明するように、非結合検索ベースを設定します。

非結合検索ベースの設定

ドメインを構成した後で、Disjoint_domain の非結合検索ベースを追加し、「タブ検索ベース」フィールドに値がないことを確認する必要があります。

注意： Root_domain をどのように構成したかに応じて、Sub_Domain の非結合検索ベースの追加が必要な場合があります。

Disjoint_domain の非結合検索ベースを追加する手順

1. ID システム・コンソールにナビゲートします。
`http://hostname:port/identity/obliv`
2. 「ディレクトリ・サーバー」リンクにナビゲートして選択します（「ID システム・コンソール」、「システム管理」、「システム構成」、「ディレクトリ・オプションの構成」、リンク）。
3. Disjoint_domain の非結合検索ベースを追加し、「保存」をクリックします。
4. 「User Manager」の「タブの構成」機能にナビゲートして選択します（「ID システム・コンソール」、「User Manager 構成」、「タブの構成」）。
5. 「タブの構成」ページでリンクを選択します。
6. 「タブ検索ベース」フィールドに値がないことを確認します。
7. Sub_domain がある場合は、これについて前述の手順を繰り返します。

非結合検索ベースの削除について

非結合検索ベースの検索ベース・ポリシーがある場合、このノードにこの検索ベースを持つユーザーは、ベースがこの検索ベースであるフィルタをクエリー・ビルダーで作成できます。削除する前に、この非結合検索ベースのアクセス制御ポリシーをすべて削除することをお勧めします。

非結合検索ベースを削除する場合は、この検索ベースを使用するすべてのデータベース・エージェントを無効にする必要があります。

グループ検索読取り操作の構成（オプション）

Active Directory は、グループ・メンバーの増分取得を使用します。このため、ID システムは複数の読取りを実行してグループ・メンバーの完全なセットを取得する必要があります。

Windows 2000 上の Active Directory の場合、1 回の読取りで取得できる最大のメンバー数は 1000 です。パラメータを変更しないかぎり、ID システムはデフォルト値の 1000 を使用します。Windows .NET Server 2003 上の Active Directory の場合、最大数は 1500 です。globalparams.xml にあるパラメータ maxForRangedMemberRetrieval に、ID システムが使用する最大値が格納されます。

注意： *install_dir* という表記法は、名前付きコンポーネントをインストールしたディレクトリを表します。たとえば、*IdentityServer_install_dir* は、Identity Server をインストールしたディレクトリを表します。

Windows 2003 でグループ検索読取り操作を構成する手順

1. `\IdentityServer_install_dir\identity\oblix\apps\common\bin\globalparams.xml` にある `globalparams.xml` ファイルを探します。

2. `maxForRangedMemberRetrieval` エントリに 1500 の値を加算します。

次に例を示します。

```
<SimpleList > <NameValPair ParamName="maxForRangedMemberRetrieval" Value="1500"/>
</SimpleList>
```

3. ファイルを保存します。
4. Identity Server を再起動します。

Active Directory での認証および認可

2 フォレスト構成については、『Oracle Access Manager インストレーション・ガイド』で概説しています。インストール後、Active Directory 用のアクセス・システムの構成には、親子ドメインでの認証と認可の設定が含まれる場合があります。

この項の内容は次のとおりです。

- [親子認証](#)
- [親子認可](#)
- [ObMyGroups アクション属性](#)

親子認証

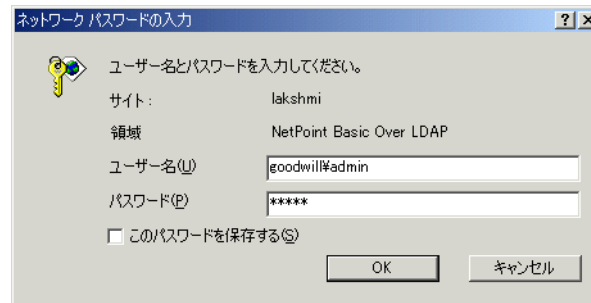
この場合は、アクセス・システムの資格証明マッピング・プラグインを使用して、親ドメインと子ドメインの両方に対してユーザーを認証する必要があります。このプラグインはユーザーの DN を取得します。

たとえば、foo.goodwill.oracle.com および goodwill.oracle.com という 2 つのドメインがあるとします。ID システムには、2 つのディレクトリ・プロファイルがあります。1 つは foo.goodwill.oracle.com に対するもので表示名は foo であり、もう 1 つは goodwill.oracle.com に対するもので表示名は goodwill です。

```
Foo.goodwill.Oracle.com:
DisplayName=foo
Searchbase = dc=foo,dc=goodwill,dc=Oracle,dc=com
User:Alice
```

```
Goodwill.Oracle.com
DisplayName=goodwill
Searchbase=dc=goodwill,dc=Oracle,dc=com
User:Bob
```

また、前の例で示した credential_mapping プラグインのフィルタを使用する Oracle Access and Identity 認証メカニズムを使用しているとします。ユーザーがアクセス・システムにログインしようとする時、「Basic Over LDAP」ダイアログ・ボックスが表示されます。



ドメインは、ログイン ID の一部であり、“\” の前に入力されます。ドメイン名から、アクセス・システムはこのユーザーの識別に使用する検索ベースを知ることができます。Alice がログインする場合はドメイン名 foo を指定する必要があり、Bob がログインする場合はドメイン名 goodwill を指定する必要があります。両方のユーザーが認証されます。

注意： Active Directory フォレスト用の Oracle Access and Identity 認証スキームで保護されているリソースにアクセスするには、ユーザーは「認証」ダイアログ・ボックスでユーザー名として *domainname\username* を入力する必要があります。この *domainname* は、このユーザーの認証の実行に使用される、Access Server に対して作成された DB プロファイルの表示名である必要があります。

親子認可

ドメインごとに別々の LDAP ルールを定義できます。たとえば、マネージャの肩書きを持つすべてのユーザーがリソースにアクセスできるようにする場合は、ドメインごとに1つずつ、合計2つの LDAP ルールを指定する必要があります。これらのルールの例を次に示します。

```
ldap:///dc=goodwill,dc=Oracle,dc=com??sub?(&(title=Manager)
(objectclass=user)
```

```
ldap:///dc=foo,dc=goodwill,dc=oracle,dc=com??sub?(&
(title=Manager)(objectclass=user)
```

これらのルールを使用して、foo と goodwill の両方のマネージャを認可できます。

ObMyGroups アクション属性

ObMyGroups アクション属性を使用して、ユーザーが属するすべてのグループをヘッダー変数で返すことができます。属性名に ObMyGroups を指定して、アクセス・システムに対して構成された検索ベースを使用します。Access Server は、返されるグループ数に制限を課しません。返されるグループ数は、ディレクトリに対して構成されているサイズ制限によってのみ制限されます。

アクセス・システムでは、1つの検索ベースのみサポートされます。したがって、goodwill.Oracle.com を製品検索ベースとして選択する場合、ObMyGroups は、goodwill.oracle.com の下のグループを検索します。この場合、アクセス・システムは参照に従うことができず、アクセス・システムには複数検索ベース機能がないため、foo.goodwill.oracle.com のグループを返すことができません。

LDAP URL で ObMyGroups を指定できます。この場合、検索ベースは LDAP URL から取得されます。ただし、1つのヘッダー変数に1つの属性のみ関連付けることができるため、2つのドメインがある場合は、ユーザーが属するすべてのグループを取得するために、少なくとも2つのヘッダー変数が必要です。

たとえば、dc=goodwill,dc=oracle,dc=com および dc=dilbert,dc=goodwill,dc=oracle,dc=com という2つのドメインがあるとします。この両方の検索ベースからグループを取得するには、表 A-1 に示すように、ドメインごとに1つずつ、合計2つのヘッダー変数を定義する必要があります。

表 A-1 2つのドメインの LDAP URL がある ObMyGroups

タイプ	名前	戻り値
headervar	HTTP_PARENT_GROUP	"obmygroups:ldap:///dc=goodwill,dc=Oracle,dc=com??sub?(group_type=role)"
headervar	HTTP_CHILD_GROUP	"obmygroups:ldap:///dc=dilbert,dc=goodwill,dc=Oracle,dc=com??sub?(group_type=role)"

- HTTP_PARENT_GROUP では、"dc=goodwill,dc=Oracle,dc=com" ツリーの中で、ログインしているユーザーがメンバーとなっており、group_type がロールであるすべてのグループが返されます。
- HTTP_CHILD_GROUP では、"dc=dilbert,dc=goodwill,dc=Oracle,dc=com" ツリーの中で、ログインしているユーザーがメンバーとなっており、group_type がロールであるすべてのグループが返されます。

次の手順では、Active Directory 用に credential_mapping 認証プラグインを構成し、必要に応じて SSO を設定します。

credential_mapping プラグインの構成

各ポリシー・ドメインには認証スキームが必要です。各認証チャレンジ方法は、1つ以上のプラグインによってサポートされます。認証チャレンジ方法のプラグインの詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

credential_mapping プラグインは、ユーザーのユーザー ID をディレクトリ内の有効な識別名 (DN) にマッピングします。ユーザー ID がマッピングされる属性を構成できます。最も一般的なマッピング先属性は uid です。ただし、obMappingFilter パラメータを変更することにより、顧客がユーザー ID を uid 以外のプロファイル属性にマッピングすることもできます。

obmappingbase はユーザー検索ベースを定義します。シングル・ドメインでは、マッピング・ベースを credential_mapping プラグインの obMappingBase パラメータで明示的に定義する必要があります。次に例を示します。

```
ou=company,dc=mydomain,dc=Oracle,dc=com).
```

Active Directory フォレストでは、ユーザーは、指定されたドメインに対するユーザー資格証明を検証するために、ログイン時にドメインに加えてユーザー ID を提供する必要があります。この場合、マッピング・ベースは obMappingBase="%domain%" に設定する必要があります。Active Directory フォレストの Oracle Access and Identity の資格証明マッピングを定義するためのテンプレートは、次のようになります。

```
obmappingbase="%domain%",obmappingfilter=(amp(objectclass=user) (samaccountname=%userid%))", obdomain="domain"
```

ドメイン情報は、ID システム・コンソールの DB プロファイルでメンテナンスします。ドメインごとに必ず DB プロファイルを作成してください。マルチドメイン・フォレストのログイン名は、Access Server DB プロファイルに定義されている表示名です。

credential_mapping プラグインの構成手順

1. 通常どおり、Policy Manager にポリシー・ドメインを作成します。

注意： 現在、アクセス・システムを Active Directory とともにデプロイする場合、ポリシー・ドメイン数の上限は 350 です。

2. 「認証管理」プラグイン・ページにナビゲートします (アクセス・システム・コンソール)、「アクセス・システム構成」、「認証管理」、「link」、「プラグイン」。

link は、変更する認証スキームの名前です。

3. Active Directory 用の credential_mapping プラグインを構成します。

次に例を示します。

- フォーム・ベースの場合：

```
obmappingbase="%domain%",obmappingfilter=(amp(objectclass=user) (samaccountname=%login%))
```

- Oracle Access and Identity の場合：

```
obmappingbase="%domain%",obmappingfilter=(amp(objectclass=user) (samaccountname=%userid%))", obdomain="domain"
```

注意： Active Directory フォレスト用の Oracle Access and Identity 認証スキームで保護されているリソースにアクセスするには、ユーザーは「認証」ダイアログ・ボックスでユーザー名として domainname\username を入力する必要があります。この domainname は、このユーザーの認証の実行に使用される、Access Server に対して作成された DB プロファイルの表示名である必要があります。

Active Directory で使用するシングル・サインオンの構成

次の手順で説明するように、ID システムまたはアクセス・システムに対してシングル・サインオンを構成できます。ポリシー・ドメインでのリソースの保護およびシングル・サインオンの構成の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

ID システムまたはアクセス・システムでシングル・サインオンを構成する手順

1. ヘッダー変数 ObUniqueId に (uid ではなく) HTTP_OBLIX_UID を渡す必要のあるポリシー・ドメイン認証ルールでアクションを変更します。

注意： 現在、Active Directory でのポリシー・ドメイン数の上限は 350 です。詳細は、A-10 ページの「[トラブルシューティング](#)」を参照してください。

2. Web サーバーで、次のファイルの WhichAttrIsLogin パラメータの値を ObUniqueId に変更します。

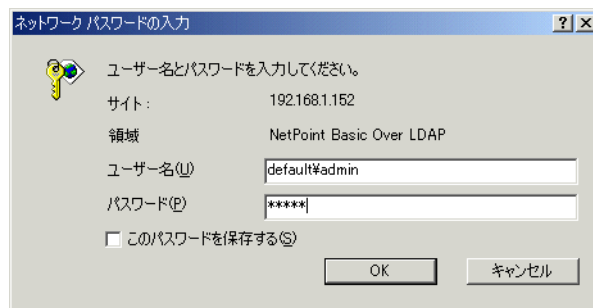
```
\IdentityServer_install_dir\identity\oblix\apps\common\bin\globalparams.xml
\PolicyManager_install_dir\access\oblix\apps\common\bin\globalparams.xml
```

WhichAttrIsLogin:ObUniqueId

ディレクトリ・サーバー・プロファイルの構成ページに、属性の数を指定する関連ディレクトリ・プロファイルが表示されます。次に例を示します。

マシン：
 ポート番号：
 ルート DN：
 ルート・パスワード：
 検索ベース：
 構成ベース：
 ディレクトリ・サーバー・セキュリティ・モード：
 非結合検索ベース：
 ADSI 有効: Yes

次に、結果として表示される、シングル・サインオンに関連する基本ログイン・ウィンドウを示します。



Active Directory フォレストに対して構成している場合、ユーザーが属するドメインは、ID システムで構成され、アクセス・システムで 사용되는ディレクトリ・プロファイルによって決まります。これらのディレクトリ・プロファイルは、ID システム・コンソールの「ディレクトリ・オプションの構成」機能からアクセスできるディレクトリ・サーバー・プロファイルの構成ページで有効または無効にできます。

- ディレクトリ・プロファイルが無効で、ユーザーがログイン時にアクセス・システムを通じてドメイン名を入力した場合、ユーザーはアクセスを許可されません。
- ディレクトリ・プロファイルが有効で、ユーザーがドメイン名としてその名前を入力した場合、ユーザーはアクセスを許可されます。

ただし、ユーザーがすでに認証されていて、有効なセッション・トークンを持っており、その後でディレクトリ・プロファイルが無効にされた場合、ユーザーは認証ルールなどに基づいてアクセスを許可されます。ディレクトリ・プロファイルの状態（有効 / 無効）は、認可時には影響しません。認証のみがプロファイルの状態を参照します。

検索フィルタについて

フィルタに、「次を含む」に評価される制約が含まれている場合（*Smith* を含む値を検索する `cn=*Smith` などのフィルタ）、Active Directory は索引付き検索を起動しません。索引付き検索では、次の制約が有効です。

- 次と等しい (`cn=Smith`)
- 次で始まる (`cn=Smith*`)

動的グループ・オプションが有効になっていて、指定された動的フィルタに「次を含む」検索フィルタが含まれている場合、「Group Manager」の「グループ」タブでは、結果の評価に長時間を要することがあります。

ユーザーが「次を含む」検索フィルタを使用しないようにするには、カタログ・ファイルを変更して使用可能なフィルタを制限します。次のディレクトリにあります。

```
Component_install_dir/identity|access/oblix/app//bin/application
```

`Component_install_dir` はコンポーネントがインストールされているディレクトリで、`identity|access` はそれぞれ ID システムとアクセス・システムを表します。

複数の `xxxparams.xml` ファイルがあります。これらのファイルで、許可される有効なフィルタのタイプを `vallist (ObEnhanceSearchList)` で指定できます。

D-2 ページの「[あいまいな名前の解決](#)」も参照してください。

SMAccountName の長さについて

Active Directory スキーマにある Security Access Manager アカウント名の属性 (`SMAccountName`) は、Windows 2000 より前の Windows バージョンとの下位互換性を保つために使用されます。これらの旧バージョンをサポートする必要がない場合は、Active Directory をネイティブ・モードで実行できます。

Active Directory を混在モードで実行する必要がある場合、Active Directory は、`SMAccountName` の値として指定できる文字数を制限します。デフォルトでは、Oracle Access Manager は混在モードに適応し、`SMAccountName` 文字列の長さを 20 文字に制限します。

Active Directory をネイティブ・モードで実行している場合は、`globalparams.xml` ファイルで `samAccountNameLength` パラメータの値を編集する必要があります。このファイルは次のディレクトリにあります。

```
Component_install_dir/apps/common/bin/globalparams.xml
```

`Component_install_dir` は、Oracle Access Manager コンポーネントがインストールされているディレクトリの名前です。このファイルで、次のエントリの値を編集します。

```
<SimpleList>
<NameValPair
  ParamName="samAccountNameLength"
  Value="20">
</NameValPair>
</SimpleList>
```

`globalparams.xml` の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

ユーザーが、`globalparams.xml` の `samAccountName` に対して設定された制限を超える名前を持つ人物またはグループを定義すると、エラーが発生します。デフォルトのメッセージは、こ

のパラメータが 20 文字を超えてはならないことを示します。メッセージ・タグは "MSamAccountNameExceeds20Error" です。

このパラメータの値を変更する場合は、メッセージ・カタログ `globalmsg.xml` でエラー・メッセージを変更する必要もあります。

.NET 機能の構成

Oracle Access Manager では、Windows Server 2003 の .NET 機能がサポートされます。詳細は、付録 D 「.NET 機能の実装」を参照してください。

次のトピックの詳細は、『Oracle Access Manager 統合ガイド』を参照してください。

- Authorization Manager との統合
- スマートカード認証との統合
- Security Connector for ASP.NET との統合

トラブルシューティング

トラブルシューティングの詳細は、付録 F 「Oracle Access Manager のトラブルシューティング」を参照してください。

Microsoft リソース

Active Directory のホームページ

<http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp>

ADSI の概要

<http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adsilinks.asp>

Active Directory プログラマ・ページ

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp?frame=true

ADSI プログラマ・ページ

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp?frame=true

ADSI に対する構成

ID システムとアクセス・システムの両方に、Active Directory Services Interface (ADSI) クライアント・アプリケーションのサポートが用意されています。この章では、Oracle Access Manager を Active Directory フォレストおよび Active Directory Services Interface (ADSI) とともに実行しているときの要件および手順をまとめます。

この付録には次の項があります。

- [Oracle Access Manager での ADSI について](#)
- [ID システムの ADSI 構成](#)
- [アクセス・システムの ADSI 構成](#)
- [ID システムに対する ADSI の構成](#)
- [デフォルトのディレクトリ・プロファイルに対する ADSI の有効化](#)
- [その他のディレクトリ・プロファイルに対する ADSI の有効化](#)
- [アクセス・システムに対する ADSI の構成](#)
- [pageSize パラメータの変更](#)
- [トラブルシューティング](#)

追加情報と手順は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

Oracle Access Manager での ADSI について

Active Directory は、Windows® 2000 および Windows Server 2003 ドメイン・コントローラ上で稼働します。ADSI を使用しているクライアント・アプリケーションを作成し、他の Windows プラットフォームで実行できます。

ADSI は、Active Directory との緊密な統合を可能にする COM インタフェースのセットです。たとえば、ADSI には次の機能があります。

- 複数のベンダーの異なるディレクトリ・サービスの機能を抽象化して、ネットワーク・リソースを管理するための単一のインタフェースを提示します。
- どのネットワーク環境にリソースが含まれているかにかかわらず、管理者および開発者がディレクトリ・サービス内のリソースを管理できるようにします。
- 管理者が、ユーザーとグループの追加、プリンタの管理、ネットワーク・リソースに対する権限の設定などの一般的なタスクを自動化できるようにします。

重要： ADSI を有効にすると、Oracle Access Manager は、Active Directory の暗黙的なフェイルオーバーおよびパスワード変更機能を利用できます。

ADSI を使用すると、Oracle Access Manager コンポーネントは、Active Directory データにアクセスするために特定のホストおよびポートにバインドする必要がありません。かわりに、ADSI により、Oracle Access Manager コンポーネントは最も近くにある使用可能ドメイン・コントローラに接続して、任意のユーザー、グループまたは Oracle Access Manager 構成情報にアクセスできます。

『Oracle Access Manager インストレーション・ガイド』で説明しているように、ADSI の資格証明を使用してフォレスト全体にバインドできます。フォレストには、複数の Active Directory ホストを含めることができます。ユーザー・データおよび構成データが異なるフォレストの異なる Active Directory ホストに格納されている場合は、ADSI を使用してこれらのデータに同時にアクセスすることはできません。

ADSI は、フォレスト内の異なるドメインに対して特定のホストおよびポート番号を必要としません。ADSI は、次のような LDAP URL を使用して Active Directory ホストに接続します。

```
LDAP://domain.oblix.com/ou=oblix,dc=domain,dc=oblix,dc=com
```

インストール時の ADSI の有効化の詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

推奨

Active Directory は、ツリー構造全体をレプリケートします。レプリケーションが遅延する可能性があるため、Oracle 構成データを含むディレクトリ・ツリーはレプリケートしないことをお勧めします。構成データに対する変更は、即時に使用可能にならない場合があります。たとえば、Policy Manager でユーザーのアクセス権限に対して行った変更は、別のドメイン・コントローラと対話している Access Server から使用できない場合があります。

Oblix ツリーをレプリケートする必要がある場合は、Active Directory 上のドメイン・コントローラ間のレプリケーション頻度を変更します。

ID システムの ADSI 構成

Oracle Access Manager は、認証オプションおよびバインド・オプションの選択に関連する ADSI および LDAP の柔軟な組合せをサポートします。

注意：SSL は、ADSI と Oracle Access Manager では不要です。ただし、業務上の他の理由で SSL が必要になる場合があります。たとえば、ディレクトリ・バインドはクリア・テキストであり、SSL は自動的に提供されません。

この項の内容は次のとおりです。

- [ADSI 認証を行う純粋な ADSI](#)
- [LDAP 認証を行う混在 ADSI](#)
- [Identity Server のバインド・メカニズム](#)
- [Oracle Access Manager ADSI 構成ファイル](#)

ADSI 認証を行う純粋な ADSI

純粋な ADSI 設定では、Active Directory ツリー内のプライマリ・ドメイン・コントローラに対する ID システムの設定時に単一の ADSI データベース・エージェントが作成されます。各子ドメインに対してエージェントを追加する必要があります。

さらに、ドメイン・ツリーの不連続フォレストがある場合は、[図 B-1](#) に示すように、プライマリ・ドメイン・コントローラごとに別々の ADSI データベース・エージェントを関連付ける必要があります。

図 B-1 ADSI での不連続フォレスト



複数のディレクトリ・プロファイルおよび DB エージェントの詳細は、7-20 ページの「[ディレクトリ・サーバー・プロファイルの管理](#)」を参照してください。

LDAP 認証を行う混在 ADSI

ADSI 認証は、LDAP よりも低速な場合があります。このため、読取り、書込み、検索などの他の操作が ADSI で処理される場合に、認証に LDAP を使用することが必要な場合があります。ADSI エージェントは、すべてのドメインと関連付ける必要があります。

ADSI エージェントをすべてのドメインと関連付ける手順

1. ID システム・コンソールの「ディレクトリ・サーバー・プロファイルの作成」ページにある「Microsoft Active Directory(ADSI を使用)」の横の「認証に LDAP を使用」チェックボックスを選択します。
2. 複数のディレクトリ・プロファイルおよび DB エージェントの詳細は、7-20 ページの「ディレクトリ・サーバー・プロファイルの管理」を参照してください。

必要に応じて繰り返します。

注意： このリリースでは、Global Catalog は不要です。

詳細は、B-7 ページの「Access Server のバインド・メカニズム」および B-5 ページの「Oracle Access Manager ADSI 構成ファイル」を参照してください。

Identity Server のバインド・メカニズム

ADSI は、Active Directory にバインドする複数の方法を Identity Server に提供します。ある特定の方法に有利な点はありません。利点は、使用する資格証明に依存します。次に例を示します。

- **暗黙的：** 現在のプロセスの資格証明を使用します。これは Identity Server に対するデフォルトです。

これは、Identity Server のサービス・ログオン資格証明に対応します。暗黙的バインドの場合、adsi_params.xml ファイル内の useImplicitBind フラグは 0 に設定する必要があります。詳細は、B-5 ページの「Oracle Access Manager ADSI 構成ファイル」を参照してください。

注意： Active Directory にバインドするには Identity Server のアカウントを作成する必要があります。

Identity Server が Active Directory にバインドできるようにするためのアカウントは、Identity Server の設定時に指定したルート DN と等価である必要があります。これには、Oracle Access Manager を使用して実行する操作の管理権限がすべて必要です。Active Directory フォレストでは、フォレスト内の他のすべてのドメインの制御をこのユーザーに委任する必要があります。

- **ユーザーの DN を使用して明示的：** adsi_params.xml ファイル内の useImplicitBind フラグを 1 に設定する必要があります。adsi_params.xml ファイルにある adsiCredential パラメータでユーザー DN を指定する必要があります。詳細は、B-5 ページの「Oracle Access Manager ADSI 構成ファイル」を参照してください。
- **userPrincipleName を使用して明示的：** adsi_params.xml ファイル内の useImplicitBind フラグを 2 に設定する必要があります。adsi_params.xml ファイル内の adsiUPN パラメータで UPN を指定する必要があります。詳細は、B-5 ページの「Oracle Access Manager ADSI 構成ファイル」を参照してください。

Oracle Access Manager ADSI 構成ファイル

ADSI 構成パラメータは、次の 2 つのファイルでメンテナンスされます。

```
\IdentityServer_install_dir\identity\oblix\apps\common\bin\globalparams.xml
\IdentityServer_install_dir\identity\oblix\config\adsi_params.xml
```

IdentityServer_install_dir は、Identity Server をインストールしたディレクトリです。

globalparams について

この項では、サンプルの globalparams.xml ファイルと、パラメータ値の表を示します。

\IdentityServer_install_dir\identity\oblix\apps\common\bin\globalparams.xml のインストール・プログラムは、デフォルトのディレクトリ・プロファイルに対して ADSI を有効にする場合に、adsiEnable パラメータを作成してその値を true に設定します。このパラメータは、Oracle 構成データを格納するシステム・レベルのディレクトリ・プロファイルを参照します。

注意： パラメータを変更した後は、Identity Server を再起動する必要があります。ただし、ADSIEnabled パラメータ値は変更しないでください。

```
<SimpleList>
<NameValPair ParamName="ActiveDirectory" Value="true" />
</SimpleList>
<SimpleList>
<NameValPair ParamName="ADSIEnabled" Value="true" />
</SimpleList>
```

表 B-1 globalparams ファイルのパラメータと値

globalparams のパラメータ	値
ActiveDirectory	true false マスター管理者が Identity Server の構成時にディレクトリ・サーバー・タイプとして Active Directory を選択した場合は true です。
ADSIEnabled	true false マスター管理者が Identity Server の構成時に ADSI を有効にした場合は true です。

adsi_params について

この項では、サンプルの adsi_params.xml ファイルと、パラメータ値の表を示します。デフォルトでは、次の例に示すように、adsi_params.xml には adsiCredential パラメータの値とパスワードが含まれます。これにより、初期設定後にバインド・メカニズムを「明示的」に変更できます。

adsiPassword は暗号化され、設定時に Oracle Access Manager でのみ生成できます。次に、このファイルの例を示します。

```
<?xml version="1.0" ?>
- <ParamsCtlg xmlns="http://www.oblix.com" CtlgName="adsi_params">
- <CompoundList ListName="adsi_params">
- <ValNameList ListName="adsi_params">
  <NameValPair ParamName="sizeLimit" Value="0" />
  <NameValPair ParamName="timeLimit" Value="0" />
  <NameValPair ParamName="pagesize" Value="100" />
  <NameValPair ParamName="useImplicitBind" Value="0" />
  <NameValPair ParamName="adsiCredential"
Value="cn=Administrator,cn=users,dc=goodwill,dc=oblix,dc=com" />
  <NameValPair ParamName="adsiPassword" Value="0243455B5B5F5C4C5651595D41" />
  <NameValPair ParamName="useGCForAuthn" Value="false" />
  <NameValPair ParamName="encryption" Value="false" />
```

```

<NameValPair ParamName="asynchronousSearch" Value="true" />
<NameValPair ParamName="useDNSPrefixedLDAPPaths" Value="false" />
</ValNameList>
</CompoundList>
..</ParamsCtlg>

```

デフォルトでは、暗号化は `adsi_params.xml` で `false` に設定されます。オープン・モードで実行しているときにこれを `true` に設定し、Identity Server を再起動すると、Identity Server が動作しなくなります。

注意： パラメータを変更した後は、Identity Server を再起動する必要があります。

表 B-2 に、`adsi_params` ファイル内のパラメータと値を説明します。

表 B-2 adsi_params ファイルのパラメータと値

adsi_params のパラメータ	値
sizeLimit	認証に対して返される問合せ結果の数を制限する整数値。
timeLimit	問合せがタイムアウトになるまでの秒数を制限する整数値。
pageSize	ADSI がサーバーにリクエストする結果のページ・サイズ。
useImplicitBind	0 = 暗黙的な資格証明 1 = 明示的な資格証明 2 = userPrincipalName を使用
adsiCredential	cn=Administrator,cn=users,dc=myhost,dc=mydomain,dc=com など、ユーザーの LDAP 指定。
adsiPassword	LDAP ユーザーのパスワードを表すエンコードされたテキスト文字列。
useGCForAuthn	true/false False
aynchronousSearch	true/false デフォルトでは、ADSI は非同期検索を実行できます。false に設定されている場合は、同期検索を実行します。
adsiUPN	このパラメータは、useImplicitBind が 2 に設定されている場合に追加する必要があります。パラメータの値は、ユーザーの UPN (userPrincipalName) にする必要があります。
pageSize	pageSize 値を有限の値 (デフォルトは 0) に設定すると、LDAP 参照はオフになります。これにより、クライアント・アプリケーションがディレクトリ検索を実行するときのパフォーマンスが向上する可能性があります。
chaseReferral	このフラグを false に設定すると、LDAP 参照がオフになります。

アクセス・システムの ADSI 構成

ID システムと同様に、アクセス・システムでは、ADSI と、LDAP 認証を行う ADSI の両方がサポートされます。

アクセス・システムでは、複数の Active Directory ドメインもサポートされ、Oracle Access Manager の設定時に作成したデフォルトのディレクトリ・プロファイルに対して ADSI を有効にする手順を実行する必要があります。

この項の内容は次のとおりです。

- [ADSI 認証を行う純粋な ADSI](#)
- [アクセス・システム ADSI 構成ファイル](#)

ADSI 認証を行う純粋な ADSI

Access Server は、ADSI を使用して Active Directory を認証します。これは、これらのコンポーネントで ADSI を有効にする場合のデフォルトです。

- Policy Manager は、Identity Server と同じ認証モードを使用します。それでも、Policy Manager に対して ADSI を有効にする必要があります。
詳細は、B-12 ページの「[アクセス・システムに対する ADSI の構成](#)」を参照してください。
- Access Server は、フォレスト内のすべてのディレクトリ・サーバーと直接通信でき、LDAP 認証に Global Catalog は不要です。

ADSI のインストールおよび設定の考慮事項のリストは、『Oracle Access Manager インストール・ガイド』の Active Directory でのインストールに関する付録を参照してください。

認証メカニズム

ユーザーが Active Directory に対して認証される場合、メカニズムはドメイン・コントローラであり、ADSI での認証にそれぞれのドメイン・コントローラを使用します。

詳細は、B-8 ページの「[アクセス・システム ADSI 構成ファイル](#)」を参照してください。

Access Server のバインド・メカニズム

ADSI は、Active Directory にバインドする複数の方法を Access Server および Policy Manager に提供します。ある特定の方法に有利な点はありません。利点は、使用する資格証明に依存します。

- **暗黙的:** 現在のプロセスの資格証明を使用します (Access Server に対するデフォルト)。
これは、Access Server のサービス・ログオン資格証明に対応します。暗黙的バインドの場合、adsi_params.xml ファイル内の useImplicitBind フラグは 0 に設定する必要があります。詳細は、B-8 ページの「[アクセス・システム ADSI 構成ファイル](#)」を参照してください。

注意: Active Directory にバインドするには Access Service のアカウントを作成する必要があります。このアカウントは、Access Server の設定時に指定するルート DN と等価である必要があります。これには、Oracle Access Manager を使用して実行する操作の管理権限がすべて必要です。Active Directory フォレストでは、フォレスト内の他のすべてのドメインの制御をこのユーザーに委任する必要があります。

- **ユーザーの DN を使用して明示的:** adsi_params.xml ファイル内の useImplicitBind フラグを 1 に設定する必要があります。
ユーザー DN は、adsi_params.xml ファイルにある adsiCredential パラメータで指定する必要があります。詳細は、B-8 ページの「[アクセス・システム ADSI 構成ファイル](#)」を参照してください。

- **userPrincipleName** を使用して明示的: adsi_params.xml ファイル内の useImplicitBind フラグを 2 に設定する必要があります。

UPN は、ads_i_params.xml ファイル内の adsiUPN パラメータで指定する必要があります。詳細は、B-8 ページの「アクセス・システム ADSI 構成ファイル」を参照してください。

マルチドメイン Active Directory フォレストでは、サポートされる明示的バインド・メカニズムは userPrincipleName のみです。Policy Manager はこのメカニズムのみサポートします。

アクセス・システム ADSI 構成ファイル

Policy Manager と Access Server の両方に、ADSI 関連のパラメータを変更するための 2 つの構成ファイルがあります。ファイルは異なる場所でメンテナンスでき、コンポーネントごとに別々に変更する必要がありますが、それらのコンテンツは同じです。Policy Manager および Access Server の構成ファイルは次のとおりです。

```
\PolicyManager_install_dir\access\oblix\apps\common\bin\globalparams.xml
\PolicyManager_install_dir\access\oblix\config\ads_i_params.xml
```

```
\AccessServer_install_dir\access\oblix\apps\common\bin\globalparams.xml
\AccessServer_install_dir\access\oblix\config\ads_i_params.xml
```

これらのファイルについて、次の各項で説明します。

Policy Manager ADSI 構成

この項では、サンプルの global-parameters 構成ファイルと、パラメータ値の表を示します。

注意： Policy Manager と Access Server をインストールする際に、ADSI オプションを選択しないと、globalparams.xml に ADSEnabled パラメータがありません。一方、ADSEnabled がないと useLDAPBind パラメータは何も目的を果しません、このパラメータは存在します。

```
BEGIN:vCompoundList
...
useLDAPBind:false
ADSEnabled:true
ActiveDirectory:true
END:vCompoundList
```

パラメータとその値について、表 B-3 で説明します。

表 B-3 globalparams ファイルのパラメータと値

globalparams のパラメータ	値
useLDAPBind	true false マスター管理者が Policy Manager の構成時に「Microsoft Active Directory (LDAP を使用)」を選択した場合は true です。このフラグを有効にするには、ADSEnabled フラグが true である必要があります。デフォルトは false です。
ADSEnabled	true false マスター管理者が Policy Manager の構成時に ADSI を有効にした場合は true です。
ActiveDirectory	true false マスター管理者が Policy Manager の構成時にディレクトリ・サーバー・タイプとして Active Directory を選択した場合は true です。

Access Server の ADSI 構成

この項では、サンプルの adsi パラメータ構成ファイルと、パラメータ値を示す表 B-4 を示します。

表 B-4 adsi_params ファイルのパラメータと値

adsi_params のパラメータ	値
sizeLimit	認証に対して返される問合せ結果の数を制限する整数値。
timeLimit	問合せがタイムアウトになるまでの秒数を制限する整数値。
pageSize	ADSI がサーバーにリクエストする結果のページ・サイズ。デフォルトは 0 です。
useImplicitBind	0 = 暗黙的な資格証明 1 = 明示的な資格証明 2 = UserPrincipalName を使用
adsiCredential	"cn=Administrator,cn=users,dc=myhost,dc=mydomain,dc=com" など、ユーザーの LDAP 指定。
adsiPassword	LDAP ユーザーのパスワードを表すエンコードされたテキスト文字列。
adsiUPN	ImplicitBind=2 を使用する場合の UserPrincipalName のテキスト文字列です。UPN 文字列は、通常は user@company.com の形式の電子メール・アドレスです。
useGCForAuthn	True/False useGCForAuthentication パラメータを false に変更します。
asynchronousSearch	True/False デフォルトでは、ADSI は非同期検索を実行できます。false に設定されている場合は、同期検索を実行します。
asynchronousSearch	adsiUPN このパラメータは、useImplicitBind が 2 に設定されている場合に追加する必要があります。パラメータの値は、ユーザーの UPN (userPrincipalName) にする必要があります。

ID システムに対する ADSI の構成

ID システムに対する ADSI の構成には、複数のタスクが関係します。詳細は、『Oracle Access Manager インストレーション・ガイド』に記載されています。

タスクの概要 : ID システムに対する ADSI の構成

- Microsoft ドキュメントと『Oracle Access Manager インストレーション・ガイド』の説明に従って、Active Directory を準備します。
- 『Oracle Access Manager インストレーション・ガイド』の説明に従って、Oracle Access Manager のインストールおよび設定時に ADSI を指定します。
デフォルトでは、これにより純粋な ADSI 構成が作成されます。この構成では、単一の ADSI ディレクトリ・プロファイル (DB エージェント) により、関連 Identity Server が、暗黙的バインドを使用して Active Directory ツリー内のプライマリ・ドメイン・コントローラですべての操作を実行できます。
- 『Oracle Access Manager インストレーション・ガイド』の説明に従って、Active Directory 属性を設定し、パスワードの変更権限を有効にします。
- B-10 ページの「デフォルトのディレクトリ・プロファイルに対する ADSI の有効化」の説明に従ってデフォルトのディレクトリ・プロファイルを構成します。

- 必要に応じて、B-10 ページの「その他のディレクトリ・プロファイルに対する ADSI の有効化」の説明に従って、追加のディレクトリ・プロファイルに対して ADSI を有効にします。

デフォルトのディレクトリ・プロファイルに対する ADSI の有効化

ID システムは、インストール時にデフォルトのディレクトリ・プロファイルを自動的に作成します。ID システムの設定時にデフォルト・プロファイルに対して ADSI を有効にできます。

デフォルトのデータベース・エージェントには、default-oid-machine name という表記法を使用して名前が自動的に割り当てられます。ユーザーが認証時にこの名前を入力する必要があるため、この名前をそれぞれのドメイン名に変更する必要があります。

その他のディレクトリ・プロファイルに対する ADSI の有効化

ドメイン・ツリーの不連続フォレストがある場合は、プライマリ・ドメイン・コントローラごとに別々の ADSI データベース・エージェントを関連付ける必要があります。次の手順で概説し、第 2 章「ID システム管理者の指定」で説明するように、追加のディレクトリ・プロファイルは ID システムのインストールおよび設定後に構成します。

追加のディレクトリ・プロファイルに対して ADSI を有効にする手順

1. ID システム・コンソールにナビゲートします。
http://hostname:port/identity/oblix
2. ID システム・コンソールで、「システム構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「ディレクトリ・プロファイル」リンクをクリックします。
3. 「追加」ボタンをクリックして、「ディレクトリ・サーバー・プロファイルの作成」ページを表示します。

The screenshot shows the Oracle Identity Administration console interface. At the top, there's a navigation bar with 'ORACLE Identity Administration' and 'Identity System Console'. Below that, a breadcrumb trail shows 'システム構成 | User Manager構成 | Group Manager構成 | Org Manager構成 | 共通構成'. The main content area is titled 'ディレクトリ・サーバー・プロファイルの作成'. On the left, there's a navigation menu with items like 'パスワード・ポリシー', 'ロストパスワード・ポリシー', 'ディレクトリ・プロファイル', 'Identity Server', 'WebPass', 'サーバー設定', '診断', '管理者', 'スタイル', and '写真'. The 'ディレクトリ・プロファイル' item is selected. The main form has several sections: '名前*' with an input field, 'ネームスペース*' with an input field, 'ディレクトリ・タイプ' with a list of radio button options (Sun Directory Server 5.x, Oracle Internet Directory, Novell Directory Services (NDS eDirectory), IBMディレクトリ・サーバー, Siemens DirX, Data Anywhere, Microsoft Active Directory アプリケーション・モード, Microsoft Active Directory (ADSIを使用), Microsoft Active Directory), and '動的補助' with radio button options (はい, いいえ, すべての操作, 選択された操作). The 'Oracle Internet Directory' option is selected under 'ディレクトリ・タイプ', and 'すべての操作' is selected under '動的補助'. There are also checkboxes for '検索', '検索エントリ', and 'ユーザーの認証' at the bottom.

ユーザーが認証時にプロファイル名を入力する必要があるため、プロファイル名としてそれぞれのドメイン名を使用することをお勧めします。

4. このディレクトリ・プロファイルの名前を入力します。

各ドメイン・コントローラおよびサブドメイン・コントローラのディレクトリ・プロファイルを作成する必要があります。詳細は、B-9 ページの「ID システムに対する ADSI の構成」を参照してください。

5. このディレクトリ・プロファイルのネームスペースを入力します。

ディレクトリ・タイプには複数の選択肢があります。ADSI を有効にしないで Active Directory を使用するには、「Microsoft Active Directory」を選択する必要があります。

注意： パスワードの変更に対して ADSI または SSL を有効にするオプションもあります。また、セカンダリ・チェック・ボックス「認証に LDAP を使用」を選択して、LDAP を有効にできます。LDAP が有効になっている場合、ADSI DB エージェントはプライマリ・ドメイン・コントローラに関連付けません。認証に使用するサブドメイン・コントローラに対して LDAP エージェントを作成する必要があります。

6. 適切なディレクトリ・タイプを選択します。次に例を示します。

ディレクトリ・タイプ

- Data Anywhere
- Microsoft Active Directory アプリケーション・モード
- Microsoft Active Directory (ADSI を使用)
 - 認証に LDAP を使用
- Microsoft Active Directory
 - AD 変更パスワードは次を使用: ADSI SSL

7. 次のように、このディレクトリ・プロファイルに対してサポートされる操作を選択します。

動的補助

- はい いいえ
- すべての操作
- 選択された操作

操作

検索	<input checked="" type="checkbox"/> 検索エントリ	<input checked="" type="checkbox"/> ユーザーの認証
読取り	<input checked="" type="checkbox"/> 読取りエントリ	
書込み	<input checked="" type="checkbox"/> エントリの作成	<input checked="" type="checkbox"/> エントリを修正
	<input checked="" type="checkbox"/> エントリの削除	<input checked="" type="checkbox"/> パスワードの変更

このディレクトリ・プロファイルがドメイン・コントローラに対して構成されている場合は、すべての操作を選択します。

8. 通常どおり、他のディレクトリ・プロファイルを完成して保存します。

ディレクトリ・プロファイルの構成の詳細は、7-20 ページの「ディレクトリ・サーバー・プロファイルの管理」を参照してください。複数のディレクトリ・プロファイル (DB エージェント) の詳細は、7-20 ページの「ディレクトリ・サーバー・プロファイルの管理」も参照してください。

アクセス・システムに対する ADSI の構成

Policy Manager は、認証に Identity Server を使用します。したがって、ログイン操作では、通信先の Identity Server と同じモード (ADSI または LDAP) を使用します。Policy Manager の設定時に、デフォルトでは、明示的なバインドを使用して、Policy Manager とアクセス・システム・コンソールが Active Directory ツリー内で認証を除くすべての操作を実行できるようにします。

注意：SSL は、Oracle Access Manager での ADSI 構成には不要です。ただし、業務上の他の理由で SSL が必要になる場合があります。たとえば、ディレクトリ・バインドはクリア・テキストであり、SSL は自動的に提供されません。

デフォルトでは、Access Server に対して ADSI を有効にすると、純粋な ADSI 構成が作成されます。この構成では、Access Server が、暗黙的バインドを使用して Active Directory ツリー内のプライマリ・ドメイン・コントローラですべての操作を実行します。

アクセス・システムでの ADSI サポートの構成には、次のタスクが含まれます。

タスクの概要：アクセス・システムに対する ADSI の構成

1. 『Oracle Access Manager インストレーション・ガイド』の付録の説明に従って、設定を検証します。
2. 『Oracle Access Manager インストレーション・ガイド』の説明に従って、Policy Manager をインストールおよび設定します。
3. 『Oracle Access Manager インストレーション・ガイド』の説明に従って、Access Server をインストールし、ADSI を設定します。
4. 『Oracle Access Manager インストレーション・ガイド』の説明に従って、WebGate をインストールします。
5. 必要に応じて、B-12 ページの「[Access Server に対する LDAP 認証の有効化](#)」の説明に従って、Access Server に対して LDAP 認証を有効にします。

Access Server に対する LDAP 認証の有効化

ADSI 認証は、LDAP よりも低速な場合があります。このため、認証や監査などの他の操作を ADSI で処理する一方で、認証に LDAP を使用することが必要な場合があります。

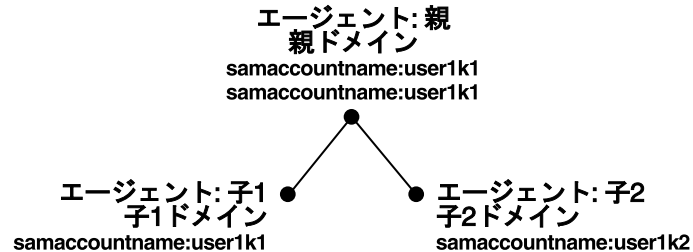
Access Server に対する LDAP 認証の有効化の手順

1. テキスト・エディタで、
`AccessServer_install_dir\access\oblix\apps\common\bin\globalparams.xml` を開きます。
2. `useLDAPBind` の値を `true` に変更します。
3. `globalparams.xml` を保存します。
4. `AccessServer_install_dir\access\oblix\config\` and name it `AppDBfailover.xml` にある `ConfigDBfailover.xml` のコピーを作成します。
両方のファイルが同じディレクトリに存在する必要があります。
5. 保存します。
6. Access Server を再起動します。

pageSize パラメータの変更

Active Directory フォレストのデプロイに基づいて、`adsi_params` ファイル内の `page-size` パラメータを変更することが必要な場合があります。たとえば、[図 B-2](#) では、Active Directory ドメイン間に親子関係があり、親ドメインと子ドメインの両方に同じ `samaccountname` を持つユーザーがいます。

図 B-2 親ドメインと子ドメインの両方にあるユーザー



認証スキームが Active Directory フォレスト用の Oracle Access and Identity であると想定します。この場合は、次のようになります。

- `user1k1` が Child1 ドメインにログインする場合、ユーザーはユーザーID を `Child1\user1k1` として入力できます。
- `user1k2` が Child2 ドメインにログインする場合、ユーザーはユーザーID を `Child2\user1k2` として入力できます。

ただし、`pageSize` パラメータが 0 に設定されている場合、親ドメインの `user1k1` が `Parent\user1k1` と入力してログインすると、「ログインに使用される資格認証 (`Parent\user1k1`) が、ID システム内の複数のユーザー・プロファイルに対応しています。対応は一意である必要があります。」というエラーが発生します。

その理由は、ページ・サイズが 0 に設定されている場合、ADSI はサブドメインを検索するため、基準を満たす 2 人のユーザーが見つかるからです。`user1k1` と `user1k2` が親ドメインにログインする場合は、`pageSize` パラメータを有限値に設定する必要があります。100 を使用することをお勧めします。

トラブルシューティング

トラブルシューティングの詳細は、[付録 F「Oracle Access Manager のトラブルシューティング」](#)を参照してください。

LDAP を使用する Active Directory に対する構成

この章では、LDAP を通信プロトコルとして使用する Active Directory フォレストとともに Oracle Access Manager を設定する手順をまとめます。

この付録の内容は次のとおりです。

- [概要](#)
- [LDAP に対する Policy Manager の設定](#)
- [LDAP に対する Access Server の設定](#)
- [LDAP での Active Directory タイムアウトの設定](#)
- [ADSI での LDAP 認証の有効化](#)

追加情報と手順は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

注意：ここで示す手順は、アクセス・システムと Active Directory 間のプロトコルとして LDAP を使用している場合にのみ適用されます。環境が異なる場合は、この説明をスキップしてください。

概要

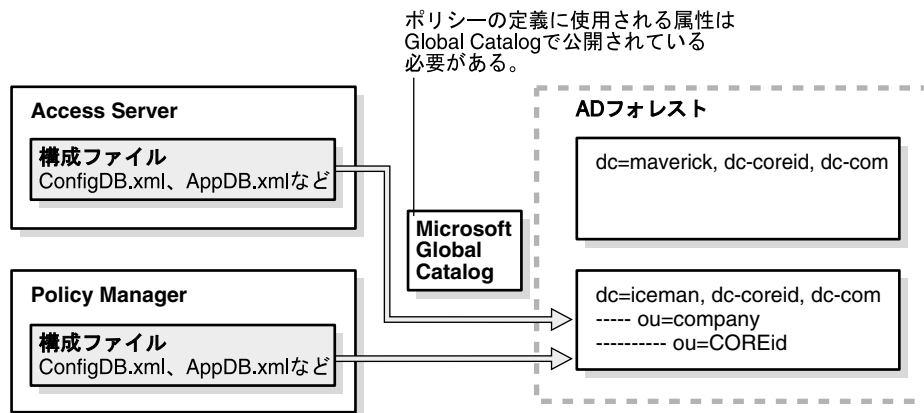
アクセス・システムは、いくつか変更された Active Directory フォレストをサポートします。

注意： Microsoft Global Catalog は、アクセス・システムでは不要になりました。

この項の手順は、次の例に基づいています。この場合、ID システムは図 C-1 に示す 2 つのドメインを使用して構成されています。次に例を示します。

- dc=maverick, dc=oblix, dc=com
- dc=iceman, dc=oblix, dc=com

図 C-1 2 つのドメインがある Active Directory フォレスト



次の手順を実行して、アクセス・システムと Active Directory 間で LDAP を使用して複数のドメインに対してアクセス・システムを設定します。

- LDAP に対する Policy Manager の設定
- LDAP に対する Access Server の設定
- LDAP での Active Directory タイムアウトの設定

注意： 次の説明では、*install_dir* は、名前付きコンポーネントに対して指定したインストール・ディレクトリを表します。たとえば、*PolicyManager_install_dir* は、Policy Manager をインストールしたディレクトリです。

LDAP に対する Policy Manager の設定

Oracle Access Manager 関連の構成情報は `\PolicyManager_install_dir\access\oblix\config\ldap` ディレクトリにあり、直接アクセスする必要があります。次に、関連ファイルを示します。

- AppDB.xml
- ConfigDB.xml
- WebResrcDB.xml

前に示したように、ID システムが `dc=iceman,dc=oblix,dc=com` ドメインの構成データで設定されたとします。

この場合は、このドメインに対して Policy Manager も設定する必要があります。この設定を行うには、Policy Manager と Identity Server に同じ構成 DN を指定する必要があります。

構成 DN の詳細は、『Oracle Access Manager インストレーション・ガイド』を参照してください。

Active Directory に対して Policy Manager を設定する手順

1. Policy Manager の設定ページにナビゲートします。

`http://hostname:port/access/oblix`

2. Identity Server と同じ構成 DN で Policy Manager を設定します。

たとえば、ドメインを含むマシンに対しては、`dc=iceman,dc=oblix,dc=com` を使用します。

3. Web サーバーを起動する前に、ポートを 3268（オープン LDAP）に変更して、両方のドメインからユーザーとグループにアクセスできるようにします。
4. 認証スキームに必要な `credential_mapping` プラグインの構成および SSO の設定の詳細は、付録 A「Active Directory でのデプロイ」を参照してください。

LDAP に対する Access Server の設定

この項は、Access Server と Active Directory 間のプロトコルとして LDAP を使用している場合にのみ適用されます。

Active Directory に対して Access Server を設定する手順

1. Identity Server と同じ構成 DN を使用して Access Server を構成します。

たとえば、ドメインを含むマシンに対しては、`dc=iceman,dc=oblix,dc=com` ドメインを使用します。

2. C-4 ページの「LDAP での Active Directory タイムアウトの設定」の説明に従って、Active Directory のタイムアウトが正しく処理されるようにします。
3. `\AccessServer_install_dir\access\oblix\apps\config` にある `ConfigDBfailover.xml` のコピーを作成し、`AppDBfailover.xml` という名前を付けます。

両方のファイルが同じディレクトリに存在する必要があります。

LDAP での Active Directory タイムアウトの設定

LDAP を使用している場合は、Active Directory に対して Access Server がインストールされている場合に、Access Server のタイムアウトを構成する必要があります。

サービスとして実行される Access Server は、Active Directory への接続を開きます。Active Directory は、非アクティブ期間の後にアイドル接続をタイムアウトにするため、Access Server がディレクトリへのアクセスを試行し、失敗することがあります。

この問題を回避するには、Active Directory の「アイドル・セッション時間」に達する前に、新しい接続を確立する必要があります。次の場合に、フェイルオーバー情報を指定できます。

- Access Server インストールの最後にフェイルオーバー情報の指定を求められます。
- インストールの完了後に、次の手順で説明するように、`AccessServer_install_dir/access/oblix/tools/configureAAAServer` にある `configureAAAServer` アプリケーションを使用して、フェイルオーバー情報を再構成しします。

次のファイルは、`ConfigAAAServer.exe` ツールを使用して、2 つ目のディレクトリ・サーバーと Access Server 間にフェイルオーバーを構成する場合に作成されます。

`ConfigDBfailover`

`AppDBfailover`

`Web...DBfailover`

インストール後に Access Server フェイルオーバーを指定する手順

1. `configureAAAServer` アプリケーションを探します。
`AccessServer_install_dir\access\oblix\tools\configureAAAServer`
2. 次のコマンドを使用して、`configureAAAServer` アプリケーションを起動します。
`configureAAAServer install AS_install_dir`
3. Access Server を再構成するかどうかを確認されたら、「いいえ」と回答します。
4. フェイルオーバー情報を指定するかどうかを確認されたら、「はい」と回答します。
5. 異なるタイプのデータを格納する場所を確認されたら、環境に合わせて応答します。

次に例を示します。

- **個別のディレクトリ・サーバーでは、オプション 8 を選択**：ポリシーと構成 DN がユーザー・データから分離されている場合は、オプション 8（共通パラメータの変更）を選択し、システムに適した値を指定します。
- **同じディレクトリ・サーバーでは、オプション 4 を選択**：ポリシー、構成 DN およびユーザー情報が同じディレクトリ・サーバーにある場合は、オプション 4（共通パラメータの変更）を選択し、システムに適した値を入力します。次に例を示します。

最大接続数：1

スリープ時間（秒）：60

フェイルオーバーしきい値：1

最大セッション時間（秒）：120

最大セッション時間が経過するたびに、Access Server がアイドルかどうかにかかわらず、Active Directory への新規接続が作成され、古い接続が破棄されます。

注意：「最大セッション時間」（秒単位）が Active Directory の「アイドル・タイムアウト」（通常は 600 秒未満）よりも短いことを確認してください。

6. オプションを選択して終了します。

7. 変更をコミットするかどうかを確認された場合は、「はい」と回答します。
フェイルオーバーの詳細は、『Oracle Access Manager デプロイメント・ガイド』を参照してください。

ADSI での LDAP 認証の有効化

ADSI 認証は、LDAP よりも低速な場合があります。このため、認証や監査などの他の操作を ADSI で処理する一方で、認証に LDAP を使用することが必要な場合があります。

Access Server に対する LDAP 認証の有効化の手順

1. テキスト・エディタで、globalparams.xml を開きます。
`AccessServer_install_dir\access\oblix\apps\common\bin\globalparams.xml`
2. useLDAPBind の値を true に変更します。
3. globalparams.xml を保存します。
4. 次の場所にある ConfigDBfailover.xml のコピーを作成します。
`AccessServer_install_dir\access\oblix\config\ldap\ConfigDBfailover.xml`
5. これに AppDBfailover.xml という名前を付けます。
両方のファイルが同じディレクトリに存在する必要があります。
6. 保存します。

.NET 機能の実装

Oracle Access Manager には、Windows Server 2003 での .NET のサポートが用意されています。サポートされる機能および Oracle Access Manager でのその実装の詳細は、この付録の次の各トピックを参照してください。

- あいまいな名前の解決
- 動的にリンクされた補助クラスの構成
- アクセス・システム認証のファスト・バインドの有効化
- 暗号化の有効化
- 統合 Windows 認証の設定
- アクセス・システム・パスワード管理の使用法
- 管理コードとヘルパー・クラスの使用法
- Authorization Manager サービスとの統合
- スマートカード認証との統合
- Security Connector for ASP.NET との統合
- トラブルシューティング
- Microsoft リソース

あいまいな名前の解決

Windows Server 2003 で実行されている Active Directory では、あいまいな名前の解決（ANR）がサポートされます。

ANR は、LDAP クライアントに関連付けられた検索アルゴリズムであり、LDAP クライアントと LDAP サーバーの両方で有効にする必要があります。ANR により、オブジェクトは複雑な検索フィルタを使用せずにバインドでき、クライアントが認識している、または認識していないオブジェクトと属性を探す場合に役立ちます。

Oracle Access Manager では、ANR はディレクトリ・サーバーに物理的には存在しない仮想属性です。Oracle Access Manager は、AD_anr.ldif ファイルを通じて仮想 ANR 属性を提供します。これにより、Oracle Access Manager は、ANR リクエストを解釈すること、ディレクトリ・サーバー・フィルタに拡張される Boolean ファンクション And および Or に ANR リクエストをマッピングして検索を拡大すること、および Active Directory に問合せを送信することができます。

注意： AD_anr.ldif ファイルは、Oracle Access Manager スキーマ・インストール環境に含まれており、手動でインポートする必要があります。詳細は、D-3 ページの「ANR に対する構成」を参照してください。

ANR 属性、検索および結果について

デフォルトでは、表 D-1 に示す属性が ANR に対して設定されます。

表 D-1 ANR 属性

ANR 属性
displayName
GivenName
LegacyExchangeDN
msExchMailNickname
name
physicalDeliveryOfficeName
proxyAddress
sAMAccountName
Surname

(anr=von) などの検索フィルタでは、サーバーは、前にリストした属性のいずれかが von* と等しいオブジェクトを返します。検索文字列にスペースが埋め込まれている場合、検索はスペースで分割され、属性に対して Or 検索も実行されます。サーバーは、姓名処理の実行を試行します。スペースが 1 つのみの場合、検索は最初のスペースでのみ分割されます。

たとえば、検索フィルタが (anr=Rob Al) だった場合、フィルタ展開は次のようになります。

```
(| (givenName=Rob Al*)
  (sn=Rob Al*)
  (displayName=Rob Al*)
  (legacyExchangeDN=Rob Al*)
  (name=Rob Al*)
  (physicalDeliveryOfficeName=Rob Al*)
  (proxyAddresses=Rob Al*)
  (sAMAccountName=Rob Al*)
  (& (givenName=Rob*) (sn=Al*))
  (& (givenName=Al*) (sn=Rob*))
)
```

ANR に対する構成

ANR で使用される属性は構成可能です。Active Directory スキーマ・スナップインを使用して属性の「Ambiguous Name Resolution」ボックスを選択することにより、ANR 検索に含める他の属性を指定できます。含める属性の attributeSchema で searchFlags 属性を直接 5 に設定できます。ANR で使用する属性を含めるには、属性に索引が付いている必要もあります。

次のタスク概要では、Oracle Access Manager で ANR を有効にするために実行する必要がある手順を概説します。ANR のメタ属性構成をディレクトリ・サーバーの構成ブランチにアップロードした後で、ANR 属性をプロファイル・ページで構成し、検索可能として定義する必要があります。属性アクセス制御も、同じプロファイル・ページで構成できます。

タスクの概要：検索時に ANR を使用する準備

1. D-3 ページの「構成データの更新」の説明に従って、Oracle 構成データを更新し、スキーマの構成ブランチに ANR メタ属性詳細を含めます。
2. D-4 ページの「ID システム・パネルでの ANR の構成」の説明に従って、ANR 属性を Identity Server サーバーの Oracle Access Manager 検索機能で使用できるようにします。
3. D-5 ページの「ANR 属性アクセス制御の検証」の説明に従って、アクセス制御権を検証します。
4. D-5 ページの「ID システム検索での ANR の使用方法」の説明に従って、ANR から Oracle Access Manager への認証および認可検索フィルタを使用します。

構成データの更新

最初に、構成ブランチの ANR メタ属性構成情報に含める構成データ（Oracle Access Manager 構成データ）を更新する必要があります。この手順の際に、次の AD_anr.ldif が実行されます。

```
#File to load ANR meta-attribute configuration to the directory tree.
dn: obattr=anr,obclass=user,OU=Oblix,<domain-dn>
changetype: add
instancetype: 4
distinguishedName:
obattr=anr,obclass=user,OU=Oblix,<domain-dn>
objectClass: oblixmetaattribute
name: anr
obattr: anr
obcardinality: ob_single
obdisplayname: ANR
obdisplaytype: ObDTextS
obsearchable: true
obvisible: true
```

この手順が完了すると、ANR が、ID システム・パネルの構成時に選択できる属性として表示されます。

Oracle 構成データの更新の手順

1. Identity Server をホストしているマシンで、AD_anr.ldif ファイル
 \IdentityServer_install_dir\identity\oblix\data.ldap\common\AD_anr.ldif を探します。
2. AD_anr.ldif ファイルを構成ディレクトリにインポートします。

次に例を示します。

```
D:\data>ldifde -i -f AD_anr.ldif -a
"cn=administrator,cn=users,dc=name,dc=company,dc=net" password
```

3. Identity Server を再起動します。

ID システム・パネルでの ANR の構成

Oracle 構成データを ANR メタ属性で更新すると、タブ（パネル）上および User Manager セレクタの検索可能属性のリスト内の ID システム検索機能で ANR 属性を使用できるようにする準備ができます。

次の手順では、ID システム・パネルでの ANR の構成をガイドします。詳細は、[第 4 章「User Manager、Group Manager および Organization Manager の構成」](#)を参照してください。

ID システム・パネルでの ANR の構成の手順

1. ID システムのランディング・ページで、ID システム・コンソールのリンクをクリックします。

すでにログインしている場合は、「ID システム・コンソール」タブをクリックします。

2. 「User Manager 構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「タブ」リンクをクリックします。
3. タブのリンクをクリックし、「オブジェクト・プロファイルの表示」をクリックします。
4. 「パネルの構成」をクリックし、構成するパネルのリンクをクリックします。

選択したパネルのすべての属性をリストするサマリーが表示されます。

5. サマリー・ページの下部にある「変更」ボタンをクリックします。

「パネルの変更」ページが表示されます。

The screenshot shows the Oracle Identity Administration console interface. At the top, there are navigation tabs for 'User Manager', 'Group Manager', 'Org. Manager', and 'Identity System Console'. Below this, there are sub-tabs for 'システム構成', 'User Manager 構成', 'Group Manager 構成', 'Org Manager 構成', and '共通構成'. The user is logged in as 'Master Admin'. The main content area is titled 'パネルの変更' (Change Panel) and shows the configuration for the 'Contact Information' panel. It includes a 'パネル・ラベル' (Panel Label) field with the value 'Contact Information', a '説明' (Description) field with the value 'Contact Information', and a '属性' (Attributes) table. The table has two columns for selecting attributes. The attributes listed are '電話番号' (Phone Number), '自宅電話' (Home Phone), '自宅住所' (Home Address), 'メール' (Email), and 'FAX番号' (FAX Number). A '追加' (Add) button is located at the bottom right of the table.

6. 「追加」ボタンをクリックし、「属性」列のリストから「ANR」を選択し、「保存」をクリックします。

すべての属性をリストするサマリー・ページが表示されます。これには ANR が含まれています。

次に、ANR がクエリー・ビルダーの検索基準リストに表示される検索可能属性であることを確認する必要があります。

7. ID システム・コンソールで、「User Manager 構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「タブ」リンクをクリックします。
8. タブのリンクをクリックします。
9. ページの下部にある「検索属性の表示」ボタンをクリックします。
すべての検索属性のリストが表示されます。
10. ANR がリストにあることを確認します。次に例を示します。
11. Identity Server を再起動します。

ANR 属性アクセス制御の検証

デフォルトでは、属性には読取り権限があります。ANR 属性には、変更権限がないようにしてください。次の手順では、ANR 属性のアクセス制御権を示します。詳細は、4-31 ページの「[LDAP 属性権限の設定と変更](#)」を参照してください。

ANR 属性アクセス制御の検証の手順

1. ID システムのランディング・ページで、「User Manager」のリンクをクリックします。
ID システムにすでにログインしている場合は、User Manager アプリケーションのタブをクリックします。
2. 「構成」サブタブをクリックし、「属性アクセス制御」のリンクをクリックします。
3. 「属性」リストから「ANR」を選択し、読取り権限しかないことを確認します。
これで、ID システム検索で ANR を使用する準備ができます。

ID システム検索での ANR の使用方法

ユーザーは、User Manager を起動するときに、検索基準リストから ANR を選択してディレクトリ検索を実行できます。

検索で ANR を使用する手順

1. ID システムのランディング・ページで、「User Manager」のリンクをクリックします。
ID システムにすでにログインしている場合は、User Manager アプリケーションのタブをクリックします。
2. 「検索」リストから「ANR」を選択し、他の検索基準を定義してから、条件を入力します。
3. 「実行」をクリックし、結果をチェックします。

動的にリンクされた補助クラスの構成

構造化オブジェクト・クラスは自立しており、ID システム・アプリケーション内で使用するのに必要な基本属性を含んでいます。構造化オブジェクト・クラスの例として、`person` や `groupOfNames` があります。`Person` オブジェクト・クラスには、名前、部門、従業員 ID、電子メール・アドレスなどの属性が含まれます。構造化オブジェクト・クラスは、ID システム・アプリケーション内でタブを作成するときに割り当てる必要があります。

補助オブジェクト・クラスは、任意の構造化クラスに追加できる混在クラスです。補助オブジェクト・クラスを使用すると、すでに構造化クラスに属しているエントリに関連属性のセットを追加できます。請求先住所、チャレンジ・フレーズ、チャレンジ・フレーズに対するレスポンスなどの項目は、補助オブジェクト・クラスでの定義に使用できる可能性があります。

Windows 2000 Server では、Active Directory は静的にリンクされた補助クラスのみサポートしていました。静的にリンクされた補助クラスは、スキーマ内のオブジェクト・クラスの `classSchema` 定義の `auxiliaryClass` 属性または `systemAuxiliaryClass` 属性に含まれているクラスです。これは、関連付けられているクラスのすべてのインスタンスの一部です。静的にリンクされた補助クラスの使用は、Active Directory とともにインストールされている Oracle Access Manager のデフォルトです。他のすべてのディレクトリでは、動的にリンクされた補助オブジェクト・クラスのみサポートされます。

Windows Server 2003 では、Active Directory および Oracle Access Manager は動的にリンクされた補助クラスをサポートします。特定のユーザー、グループまたは組織に対して定義されたスキーマでは、動的にリンクされた補助クラスにより、クラス全体のスキーマ定義の拡張の影響をフォレスト全体に与えることなく、個々のオブジェクトとともに追加属性を格納できます。動的にリンクされた補助クラス属性は、実行時にのみ混在します。

たとえば、動的リンクを使用して、セールス固有の補助クラスをセールス人員のユーザー・オブジェクトに添付したり、他の部門に固有の補助クラスを他の部門の従業員のユーザー・オブジェクトに添付したりできます。または、特定の属性を動的に追加することにより、基本グループをメール・グループに変換できます。

タスクの概要：動的補助クラスの設定

1. 『Oracle Access Manager インストール・ガイド』の説明に従って、動的補助クラスを有効にして Oracle Access Manager をインストールおよび設定します。
2. 3-2 ページの「オブジェクト・クラスの概要」の説明に従って、Organization Manager の追加の構造化オブジェクト・クラスを指定します。
3. 3-11 ページの「オブジェクト・クラス属性の概要」の説明に従って、属性を構成します。
4. 4-2 ページの「タブの構成」の説明に従って、ユーザー、グループおよび組織のアプリケーション・タブを構成します。
5. 4-11 ページの「タブのプロファイル・ページおよびパネルの構成」の説明に従って、ユーザー、グループおよび組織のプロファイル・ページを構成します。
6. 第 5 章「ID 機能とワークフローの連携」の説明に従って、ワークフローを定義します。
7. D-7 ページの「属性の動的な追加」の説明に従って、追加の補助オブジェクト・クラスを指定します。

属性の動的な追加

次の手順では例のみを提供し、User Manager でタブとパネルを作成してあることを前提とします。ここでは、目的の補助属性を動的に追加します。

注意：これは単なる例です。Group Manager または Organization Manager でも作業できます。D-8 ページの「グループの属性の追加」も参照してください。

User Manager で追加の補助オブジェクト・クラスを指定する手順

1. ID システム・コンソールで、「User Manager 構成」をクリックし、次に左側のナビゲーション・ペインの「タブ」をクリックします。
2. タブのリンクをクリックします。
3. 「オブジェクト・プロファイルの表示」ボタンをクリックし、「パネルの構成」リンクをクリックします。
4. 変更するパネルのリンクをクリックします。
5. 「変更」ボタンをクリックして、「パネルの変更」ページを表示します。
6. 「追加」ボタンをクリックし、リストから1つ以上の属性を選択してから「保存」をクリックします。

追加した属性が「パネルの表示」ページに表示されます。

The screenshot shows the Oracle Identity Administration console interface. The top navigation bar includes 'ORACLE Identity Administration' and 'Identity System Console'. The main content area is titled 'User Manager 構成' and has three sub-sections: 'ヘッダーの構成', 'パネルの構成', and 'パネルの順序付け'. The 'パネルの構成' section is active, showing a list of attributes for a panel. The attributes are listed in two columns: 'パネルの表示' (Panel Display) and '属性' (Attributes). The '属性' column lists various attributes such as 'Test Panel', 'Pocket Bell', 'Out Of Office Indicator', 'FAX番号', '自宅電話', and several image-related attributes. The status '作成中' (In Progress) is displayed at the bottom of the list.

ディレクトリ・サーバーのエントリが変更され、新規属性が含まれます。

グループの属性の追加

この手順の例は、次のような属性を追加することにより、単一の基本グループをメール・グループに動的に変換します。

属性 1	属性 2	属性 3
MailAlternateAddress	Mailhost	MailRoutingAddress

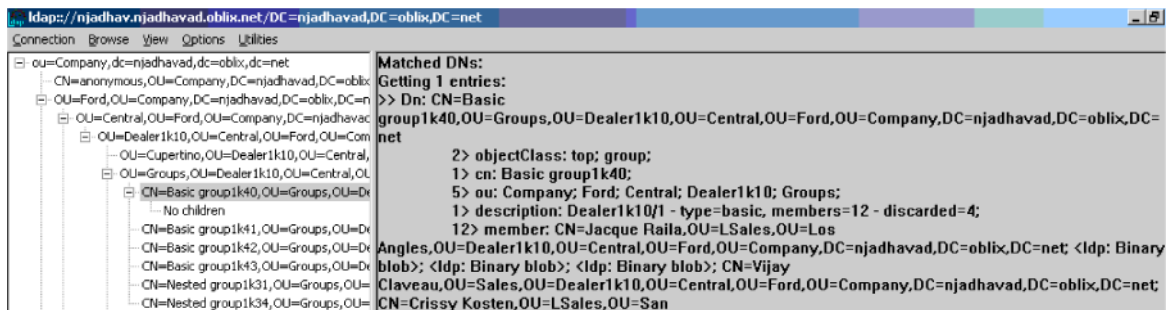
この例では、「グループ」パネルと、メール・グループを作成するためのワークフローを作成してあることを前提とします。ここでは、目的の属性を動的に追加します。これは単なる例です。User Manager または Organization Manager でも作業できます。D-7 ページの「属性の動的な追加」も参照してください。

「グループ・プロファイル」パネルに属性を追加する手順

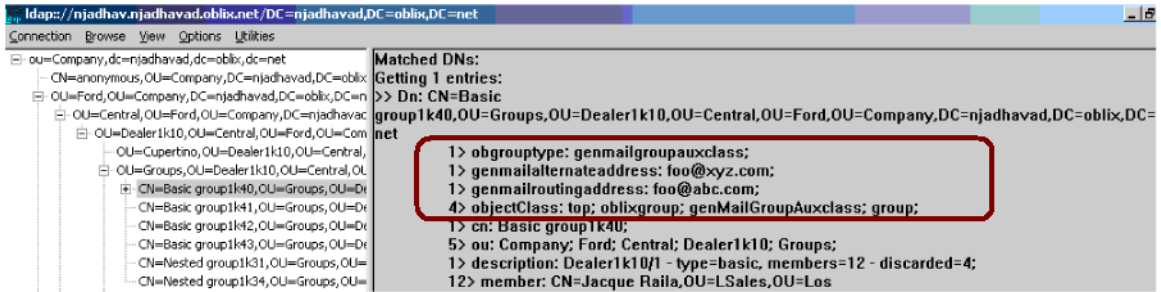
- ID システムのランディング・ページで、ID システム・コンソールのリンクをクリックします。
すでにログインしている場合は、「ID システム・コンソール」タブをクリックします。
- 「Group Manager 構成」サブタブをクリックし、次に左側のナビゲーション・ペインの「タブ」リンクをクリックします。
- 「オブジェクト・プロファイルの表示」、「パネルの構成」をクリックし、変更するパネルのリンクをクリックします。
「パネルの表示」ページが表示されます。
- 「変更」をクリックします。
「パネルの変更」ページが表示されます。
- ページの「属性」セクションで、「追加」ボタンをクリックし、リストから 1 つ以上の属性を選択してから「保存」をクリックし、追加した属性が「パネルの表示」ページに表示されることを確認します。
- 右上にある「アプリケーションの選択」リストから、「Group Manager」を選択します。
- 「セレクト」に検索基準を入力し、「実行」をクリックします。
結果が返されます。「グループ」を選択して確認すると、1 つのグループに動的に追加した属性が、そのグループでのみ使用可能であることがわかります。
- 「変更」、「+」ボタンの順にクリックしてから、特定の値を追加して通常どおりに保存します。

ディレクトリ内のエントリも変更されています。たとえば、次のスクリーン・ショットは補助クラスが追加される前のサンプル・エントリを示します。

図 D-1 動的補助クラスが追加される前のサンプル・エントリ



次のスクリーン・ショットは、補助クラスが追加された後の同じエントリを示します。



アクセス・システム認証のファスト・バインドの有効化

Windows Server 2003 で実行されている Active Directory は、同じ LDAP 接続上で複数の認証を可能にする同時バインド（ファスト・バインドとも呼ぶ）機能を提供します。

アクセス・システムは、次の利点があるこの機能をサポートおよび使用します。

- ファスト・バインドでは、2つのスレッドが1つの接続で同時にバインドをリクエストできます。
- ファスト・バインドでは、パスワードとアカウント・フラグのみ検証され、チケットは作成されないため、より高速な認証メカニズムが提供されます。

各データベース・インスタンスに対してファスト・バインド・オプションを有効にする必要があります。このオプションは、アクセス・システム・コンソールの個々のデータベース・プロファイルにあります。

ファスト・バインドを使用するようにアクセス・システムを構成する手順

1. アクセス・コンソールで、「システム構成」タブをクリックします。
2. 左側のナビゲーション・ペインで「サーバー設定の表示」リンクをクリックします。

このページの LDAP ディレクトリ・サーバー・プロファイルの構成セクションでは、変更するディレクトリ・プロファイルを選択します。

LDAPディレクトリ・サーバー・プロファイルの構成

名前	ネームスペース	プライマリ・サーバー	セカンダリ・サーバー
<input type="checkbox"/> default-ID Server 10.1.3 M3 stagh24 6021	o=company,c=us	default	
<input type="checkbox"/> OracleContext-ID Server 10.1.3 M3 stagh24 6021	cn=Products,cn=OracleContext	default	
<input type="checkbox"/> AccessManager setup user profile	o=company,c=us	default	
<input type="checkbox"/> AccessServer default user profile	o=company,c=us	default	

3. ファスト・バインド機能を有効にするディレクトリ・サーバー・インスタンスの名前をクリックします。
「ディレクトリ・サーバー・プロファイルの変更」ページが表示され、変更するディレクトリ・サーバー・プロファイルのインスタンス（データベース・インスタンスとも呼ぶ）をページの下部で探すことができます。
4. 目的のディレクトリ・サーバー・プロファイル・インスタンス（データベース・インスタンス）の名前を探し、クリックします。次に例を示します。

名前	マシン	ポート番号	サーバー・タイプ
データベース・インスタンス*	<input type="checkbox"/> default	stagh24	389 <input type="button" value="プライマリ"/>

- このインスタンスのリンクをクリックし、ファスト・バインド・オプションの横のボックスをチェックします。次に例を示します。

ORACLE Access Administration Policy Manager ヘルプ バージョン情報 ログアウト

システム構成 システム管理 アクセス・システム構成
ログイン・ユーザー: Master Admin

- 管理者
- **サーバー設定**

データベース・インスタンスの作成

名前*	<input type="text" value="FastBind"/>
マシン*	<input type="text" value="chromium"/>
ポート番号*	<input type="text" value="389"/>
ルートDN*	<input type="text" value="o=oracle,c=com"/>
ルート・パスワード*	<input type="password"/>
時間制限	<input type="text" value="0"/>
サイズ制限	<input type="text" value="0"/>
フラグ	<input type="checkbox"/> SSL <input type="checkbox"/> 参照 <input checked="" type="checkbox"/> ファスト・バインド(Windows Server 2003のADのみ)
セキュア・ポート番号	<input type="text" value="636"/>
最初の接続数	<input type="text" value="1"/>
最大接続数	<input type="text" value="1"/>

- 「保存」をクリックします。
- 「ディレクトリ・サーバー・プロファイルの変更」ページで、プロファイルが有効になっていることを確認します。
 - プロファイルの有効化
- 必要に応じて手順を繰り返し、他のデータベース・インスタンスに対してファスト・バインド・オプションを有効にします。

暗号化の有効化

Windows 環境では、すべてのプロセスとスレッドがセキュリティ・コンテキストで実行されます。暗号化は、スレッドを所有するプロセスとは異なるセキュリティ・コンテキストでスレッドを実行する機能です。暗号化の主な目的は、クライアントの ID に対してアクセス・チェックをトリガーすることです。

IIS で有効になっている暗号化をオーバーライドする Oracle Access Manager の暗号化の有効化の詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

統合 Windows 認証の設定

Oracle Access Manager では、統合 Windows 認証 (IWA) がサポートされています。環境には次のものが含まれます。

- Windows Server 2000、Windows Server 2003 または Solaris
- Internet Information Services (IIS) 5.5 または 6.x
- Active Directory または iPlanet ディレクトリ・サーバー

たとえばユーザーのディレクトリ・サーバーに NT ログオン ID がある場合、またはユーザー名がすべての場所で同じ場合、ユーザーは任意のディレクトリ・サーバーに対して認証できます。

Windows 2000 および Windows Server 2003 で最も一般的な認証メカニズムは Kerberos です。

Oracle Access Manager による IWA の使用はシームレスです。ユーザーは、デスクトップにログインし、Internet Explorer (IE) ブラウザを開き、保護されている Web リソースをリクエストしてシングル・サインオンを完了するときに、通常の認証と IWA の違いに気付きません。

この統合に対してサポートされているバージョンおよびプラットフォームを確認するには、次のように Metalink を参照してください。

Metalink で情報を表示する手順

1. 次の URL に移動します。
`http://metalink.oracle.com`
2. 「Certify」タブをクリックします。
3. 「View Certifications by Product」をクリックします。
4. 「Application Server」オプションを選択し、「Submit」をクリックします。
5. 「Oracle Application Server」を選択し、「Submit」をクリックします。

プロセスの概要：IWA 認証の使用方法

1. ユーザーがデスクトップ・マシンにログインすると、Windows Domain Administrator 認証スキームを使用してローカル認証が完了します。
2. ユーザーは、Internet Explorer (IE) ブラウザを開き、アクセス・システムで保護された Web リソースをリクエストします。
3. ブラウザは、ローカル認証に注目し、IIS Web サーバーにトークンを送信します。
4. IIS Web サーバーは、トークンを使用してユーザーを認証し、クライアントによって指定され、サーバーによって認証されたユーザー名を指定する REMOTE_USER HTTP ヘッダー変数を設定します。
5. IIS Web サーバーにインストールされている WebGate は、外部認証の非表示機能を使用して REMOTE_USER ヘッダー変数値を取得し、それを DN にマッピングして ObSSOCookie の生成と認可を行います。
6. WebGate は、ObSSOCookie を作成し、それをブラウザに送信します。
7. アクセス・システム認可およびその他のプロセスは通常どおりに進められます。

WebGate に対して構成されている最大セッション・タイムアウト期間が、生成された ObSSOCookie に適用されます。

タスクの概要 : IWA 認証の設定

- 『Oracle Access Manager インストール・ガイド』の説明に従って、IWA を設定したのと同じ IIS Web サーバーに WebGate をインストールします。
 - サイト・レベルで WebGate をインストールした場合は、サイト・レベルでタスクを実行する必要があります。
 - 異なる仮想サイトに複数の WebGate をインストールした場合は、各仮想サイトに対してタスクを実行する必要があります。
- D-12 ページの「WebGate Web サーバーでの IWA の有効化」の説明に従って、WebGate 上で IWA を有効にします。
- D-13 ページの「IWA に対する WebGate の構成」の説明に従って、IWA を使用するように WebGate を構成します。
- D-13 ページの「Oracle Access Manager での IWA 認証スキームの作成」の説明に従って、Oracle Access Manager に IWA の認証スキームを作成します。
- D-14 ページの「IWA 実装のテスト」の説明に従って、IWA 実装をテストします。

WebGate Web サーバーでの IWA の有効化

最初の手順は、WebGate をホストしているマシンでの IWA の有効化です。

- サイト・レベルで WebGate をインストールした場合は、サイト・レベルでタスクを実行する必要があります。
- 異なる仮想サイトに複数の WebGate をインストールした場合は、各仮想サイトに対してタスクを実行する必要があります。

WebGate をホストしているマシンで IWA を有効にする手順

- WebGate をホストしているマシンでインターネット・サービス・マネージャを起動します（「スタート」、「プログラム」、「管理ツール」、「インターネット サービス マネージャ」）。
- 「Default Web site」（デフォルトの Web サイトの名前を変更した場合は Web サーバーの名前）を右クリックし、「Properties」を選択します。

注意： WebGate をサイト・レベルでインストールした場合は、「Site」を右クリックし、「Properties」を選択します。

- 「Master Properties」の横の「Edit」ボタンをクリックします。
- 「Directory Security」タブをクリックし、「Anonymous access and authentication control」の横の「Edit」をクリックします。
- 「Anonymous Access on the IIS Web Server」を無効にします。
- 「Integrated Windows Authentication」を有効にします。
- 「OK」をクリックし、もう一度「OK」をクリックします。
- IIS Web サーバーを再起動します。

IWA に対する WebGate の構成

IWA に対して WebGate を構成するには、アクセス・システム・コンソールでユーザー定義パラメータ UseIISBuiltinAuthentication を true に設定する必要があります。詳細は、『Oracle Access Manager Access System Administration Guide』のアクセス・システムの構成に関する章を参照してください。

アクセス・システム・コンソールで AccessGate を変更する手順

1. アクセス・システム・コンソールを起動し、「アクセス・システム構成」タブをクリックし、次に左側のナビゲーション・ペインの「AccessGate 構成」リンクをクリックします。
「Access Gate の検索」ページが表示されます。
2. 検索属性と条件をリストから選択するか、「すべて」を選択してすべての AccessGate を検索します。
「検索」リストは、検索できる属性の選択リストです。残りのフィールドで、選択した属性に適した検索基準を指定できます。
3. 「実行」をクリックします。
検索結果がページに表示されます。
4. 変更する AccessGate または WebGate の名前をクリックします。
AccessGate の詳細ページが表示されます。
5. 「変更」をクリックします。
「AccessGate の変更」ページが表示されます。このページで新規情報を入力できます。
AccessGate または WebGate の名前は変更できません。名前を変更するには、アクセス・システム・コンソールから削除し、アンインストールする必要があります。その後で、新しい AccessGate または WebGate を作成します。
6. 必要に応じて新しい値を入力します。
7. 「保存」をクリックして変更を保存します。

Oracle Access Manager での IWA 認証スキームの作成

特定のチャレンジ・メソッド、チャレンジ・パラメータおよびプラグインを使用するには、次の手順で説明するように、アクセス・システムの IWA 認証スキームを作成する必要があります。

アクセス・システムで IWA 認証スキームを作成する手順

1. 通常どおり、アクセス・システム・コンソールにナビゲートします。次に例を示します。
`http://hostname:port/access/oblix`
2. 「認証管理」ページにナビゲートし、「追加」をクリックします（アクセス・システム・コンソール、「アクセス・システム構成」、「認証管理」、「追加」）。
3. 統合 Windows 認証スキームを作成します。
次に例を示します。
名前: 統合 Windows 認証
説明: このスキームは、組込みの Windows 認証メカニズムを使用した統合 Windows 認証です。
レベル: 1
チャレンジ・メソッド: Ext
チャレンジ・パラメータ: creds: REMOTE_USER
SSL 必須: No

チャレンジ・リダイレクト

4. 「プラグイン」タブをクリックし、「変更」をクリックします。
5. リストからプラグイン名を選択し、プラグイン・パラメータを入力して「追加」をクリックし、終了したら保存します。

次に例を示します。

プラグイン

プラグイン名	プラグイン・パラメータ
credential_mapping	obMappingBase=<"Domain name">,obMappingFilter="(&(objectclass=user)(samaccountname=%REMOTE_USER%))"

6. 通常どおり、認証スキームを保存し、このスキームを使用してリソースを保護します。

IWA 実装のテスト

実装をロールアウトする前に、必ずテストすることをお勧めします。

IWA のテストの手順

1. Oracle Access Manager と Windows オペレーティング・システムの両方のユーザーである人物としてマシンにログインします。
2. 保護されたリソースの URL を入力します。

アクセス・システム・パスワード管理の使用方法

アクセス・システム・パスワード管理機能を Active Directory フォレストとともに使用する場合は、次の点に注意してください。

- 「リセット時に変更」、「パスワードの期限切れ」および「パスワードの期限切れ警告」機能は動作しません。
- 「取得数」機能は動作しません。

この制限は、アクセス・システムでパスワード管理に LDAP モードを使用している場合、およびフォレスト構成で Active Directory を使用している場合にのみ適用されます。

管理コードとヘルパー・クラスの使用方法

.NET Framework には、コードの安全な実行を保証し、スクリプト化された環境でのパフォーマンスの問題を排除するためのオブジェクト指向プログラミング環境が用意されています。

.NET Framework では、ランタイムを対象とするコードは管理コードと呼ばれます。

また、MANAGEDLIB アクションは、次のような管理コードの利点を提供します。

- **言語の選択:** プラグインを VisualBasic、C#、Managed C++ (MC++)、Java または PERL で記述できます。
- **言語の統合:** 異なるソース言語からコンパイルされた MIL モジュールを 1 つのアセンブリまたはプラグインに結合できます。

これにより、プラグインの作成者に対して、プラグイン開発用により多様な言語の選択肢が提供されます。

- **メモリー管理のサポート:** 共通言語ランタイム (CLR) は、ガベージ・コレクションを提供し、プラグインの作成者をほとんどのメモリー管理から解放します。

ガベージ・コレクタは、メモリーが参照されなくなると、そのメモリーをヒープに戻します。ただし、プラグイン作成者は、オブジェクトへのぶら下がり参照がないことを確認する必要があります。ぶら下がり参照がある場合、未使用のメモリーに対してガベージ・コレクションは行われません。

- **.NET Framework サポート:** .NET framework SDK には、様々な機能が含まれています。これにより、プラグイン・コードでのサード・パーティ・サポートの必要性が削減されます。

Oracle Access Manager は、管理コードおよび Managed C++ (MC++)、Visual Basic.Net などの言語を含む多くの言語で API を使用およびコールできます。

管理コードおよび管理ヘルパー・クラスの詳細は、『Oracle Access Manager 開発者ガイド』を参照してください。

Authorization Manager サービスとの統合

アクセス・システムには、Microsoft Windows Server 2003 Authorization Manager (AzMan) サービスを使用して WebGate や Access Server API のコール元を含む Access Server クライアントの認可の決定を行う認可プラグインが用意されています。

AzMan プラグインのポリシー・ドメインの構成の詳細は、『Oracle Access Manager 統合ガイド』を参照してください。

スマートカード認証との統合

Oracle Access Manager は、同種の Windows 環境の Active Directory および IIS Web サーバーによるスマートカード認証をサポートします。スマートカード認証は、「ユーザーが認識しているもの」および「ユーザーが持っているもの」に基づいているため、これを使用すると、ユーザー名とパスワードのみ使用する場合よりも強力な形式の認証が提供されます。

- 「ユーザーが認識しているもの」は、ユーザーの秘密の個人識別番号 (PIN) です。この概念は、個人の銀行コード PIN と同様です。
- 「ユーザーが持っているもの」は、コンピュータに接続されているスマートカード・リーダーに挿入したスマートカード・デバイスにより生成された暗号ベースの ID および所有の証明です。

スマートカード認証との統合の構成の詳細は、『Oracle Access Manager 統合ガイド』を参照してください。

Security Connector for ASP.NET との統合

Oracle Access Manager は、Microsoft .NET Framework の ASP.NET コンポーネントをサポートします。開発者はこのコンポーネントを使用して、Web アプリケーションおよび分散アプリケーションを構築、デプロイおよび実行できます。Oracle Access Manager Security Connector for ASP.NET は、ネイティブの .NET ロールベース・セキュリティをサポートおよび拡張します。

Oracle Access Manager Security Connector for ASP.NET を使用して新規 `OblivPrincipal` オブジェクトをインスタンス化し、それにルール（アクセス・システム認可ルール）とネイティブ `WindowsPrincipal` オブジェクトを移入する方法の詳細は、『Oracle Access Manager 統合ガイド』を参照してください。

トラブルシューティング

トラブルシューティングの詳細は、付録 F「Oracle Access Manager のトラブルシューティング」を参照してください。

Microsoft リソース

Active Directory のホームページ

<http://www.microsoft.com/windows2000/technologies/directory/ad/default.asp>

ADSI の概要

<http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adsilinks.asp>

Active Directory プログラマ・ページ

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp?frame=true

ADSI プログラマ・ページ

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp?frame=true

Oracle Access Manager パラメータ・ファイル

Oracle Access Manager には、指定したパラメータ・ファイル（カタログ・ファイルとも呼ぶ）の内容を変更することでユーザーがその動作を変更できる簡単な方法が用意されています。この付録では、ファイル形式を説明し、ファイルのリストを提供し、Oracle Access Manager システム操作をカスタマイズするために変更できる値について説明します。

ファイルのカテゴリ

すべてのパラメータ・ファイルは、ID システムのインストール・ディレクトリの相対で配置されます。このディレクトリの例を次に示します。

Windows の場合：

```
c:\COREid\identity\oblix
```

UNIX の場合：

```
/var/COREid/identity/oblix
```

パラメータ・ファイルは、複数のカテゴリの 1 つに属するとみなすことができ、そのファイルに含まれるパラメータのタイプによって区別されます。

- 管理アプリケーション (User Manager Admin、Group Manager Admin および Organization Manager Admin) に影響するパラメータ。
- ユーザー・アプリケーション (User Manager、Group Manager、Organization Manager、Asynch Mailer、パスワード管理、クエリー・ビルダー、セレクト) に影響するパラメータ。
- 影響が多くのアプリケーション (ユーザー・アプリケーション、管理アプリケーションおよび Comm Server (バイナリ・ストリーミング・データ・モジュール)) に共通するパラメータ。
- Oracle Access Manager とディレクトリ・データベース (DB) の相互作用に影響し、さらにユーザー、グループ、組織、アプリケーション、構成、ワークフローおよび LDAP 参照整合性に分類されるパラメータ。
- Oracle Access Manager 複数層アーキテクチャ (たとえば、WebPass Web アプリケーションまたは Identity Server エンジン) に影響するパラメータ。

パラメータ・ファイルの詳細情報

詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

Oracle Access Manager の トラブルシューティング

この付録では、Oracle Access Manager の実行またはインストール中に発生する可能性のある一般的な問題について説明します。次の項があります。

- [問題と解決策](#)
- [詳細情報](#)

問題と解決策

この項では、Oracle Access Manager の一般的なエラー・メッセージ、問題および解決策を説明します。内容は次のとおりです。

- ディレクトリ・サーバー・プロファイルの構成後に Identity Server のメモリー使用量が増える
- ディレクトリ・サーバー・プロファイルを保存できない
- Active Directory: メンバーを追加するとグループ・サイズが縮小する
- ディレクトリ・プロファイルに対して ADSI を有効にできない
- データベースの検証に失敗する
- 簡易トランスポート・セキュリティ・モードが 1 年後に期限切れになる
- スタイルシートの検証に失敗する
- ワークフローを使用しているときに「xenroll.cab が見つかりません」エラーが発生する
- ワークフローを使用しているときに「有効化に失敗しました」エラーが発生する
- JPEG 写真イメージが更新されない

ディレクトリ・サーバー・プロファイルの構成後に Identity Server のメモリー使用量が増える

ディレクトリ・サーバー・プロファイルの構成後に、Identity Server のメモリー使用量が非常に多くなります。この問題は、Access Server または Policy Manager にも適用されます。

問題

ディレクトリ・サーバー・プロファイルの構成時に、最大セッション時間を指定するよう求められます。セッション時間のデフォルト値は 0（無制限）です。これにより、Identity Server への LDAP 接続のキャッシュ・サイズが徐々に増えるため、パフォーマンスの問題が発生することがあります。Oracle Access Manager では、これらのキャッシュは直接制御されません。

解決策

キャッシュ・サイズがパフォーマンスの問題の原因となるのを防ぐには、次のようにディレクトリ・サーバー・プロファイルの「最大セッション時間」（分単位）の値を 10 時間などの有限値に設定します。

1. ID システム・コンソールで、「システム構成」をクリックし、次に「ディレクトリ・プロファイル」をクリックします。
2. 変更するプロファイルのリンクをクリックします。
3. 「最長セッション時間」フィールドで、値を 600 に設定します。

ディレクトリ・サーバー・プロファイルを保存できない

ID システムおよびアクセス・システム・コンポーネントで使用するディレクトリ・サーバー・プロファイルを保存する際に、次のようなエラーが表示されることがあります。

「ディレクトリ・サーバー・プロファイルが保存できません。アプリケーションが正常に機能するために、ディレクトリ・サーバー・プロファイルは検索、変更および削除の各操作でポリシー・ベースにアクセスする必要があります。また、このディレクトリ・サーバー・プロファイルはサーバー間のロード・バランスもできません。」

問題

アクセス・システム (少なくとも Policy Manager) のインストール時に、ディレクトリ内でのポリシー情報の場所を識別するよう求められます。ディレクトリ内のこのブランチは、ID システム構成データが格納されているブランチと同じである場合または異なる場合があります。また、Policy Manager のインストール時に、ポリシー・ブランチに対する権限を Identity Server に付与するディレクトリ・プロファイルが作成されます。

Identity Server は、ID システムとアクセス・システム間の参照整合性を保つために、アクセス・システムのポリシー・ブランチ内のオブジェクトを検索、変更および削除できる必要があります。たとえば、アクセス・システムのポリシーの「アクセスの許可」ページで特定のリソースへのアクセスをユーザーに許可するとします。ID システムからユーザーを削除した場合、参照整合性により、ユーザーがアクセス・システムのポリシーからも削除されることが保証されます。

ID システムとアクセス・システム間に参照整合性を提供するディレクトリ・プロファイルがない場合、「... を保存できません」というエラーが発生します。このメッセージが表示される場合は、このプロファイルを削除または編集した可能性があります。

解決策

ディレクトリのポリシー・ブランチへのアクセス権を持つ別のディレクトリ・サーバー・プロファイルを作成します。

Active Directory: メンバーを追加するとグループ・サイズが縮小する

静的グループへのユーザーの追加は、ある程度までしか正しく動作しません。

問題

静的グループにメンバーを追加し続けると、グループ・サイズが縮小します。

解決策

globalparams.xml でパラメータ maxForRangedMemberRetrieval の値を必要なグループ・メンバーシップ・サイズより大きい数値に変更します。

- Windows 2003 で Active Directory を使用している場合は、globalparams.xml でパラメータ maxForRangedMemberRetrieval を 1500 に設定します。
- Windows 2000 で Active Directory を使用している場合は、1000 に設定します。

ディレクトリ・プロファイルに対して ADSI を有効にできない

Active Directory を使用している場合は、ID システム・コンソールを使用して、ユーザー・データのディレクトリ・プロファイルを ADSI から LDAP に、または LDAP から ADSI に変更できます。ただし、構成またはポリシー・データに対してこの処理を行うことはできません。

問題

ID システム・コンソールからポリシーまたは構成データのディレクトリ・プロファイルを変更しようすると、エラーが発生します。たとえば、LDAP を使用して Active Directory フォレストにユーザー・データを格納し、ADSI を使用して別の Active Directory フォレストに構成およびポリシー・データを格納するとします。ID システム・コンソールを使用して構成データ・データベース・プロファイル内の ADSI フラグを LDAP に変更する場合は、Oracle Access Manager サーバーおよびサービスの再起動後に、ADSI フラグは有効なままになり、次のメッセージが表示されます。

「別のフォレスト内のユーザーおよび構成 DB プロファイルに対して ADSI を有効化することができます。この DB プロファイルには ADSI が有効化できません。」

構成またはポリシー・データのディレクトリ・プロファイルを ADSI に変更しようすると、Oracle Access Manager はプロファイルを ADSI 対応と認識するためエラーが発生します。

解決策

構成およびポリシー・データのディレクトリ・プロファイルを変更するには、設定プログラムを再実行します。詳細は、7-28 ページの「[手動によるシステム設定の再実行](#)」を参照してください。

データベースの検証に失敗する

ID システム・コンソールで、RDBMS プロファイルの新規データベース・インスタンスを保存しようすると、「データベースの検証に失敗しました。」というメッセージが表示されることがあります。

問題

この問題は、7-35 ページの「[RDBMS プロファイルの管理](#)」の説明に従って RDBMS プロファイルを作成するときに発生することがあります。通常は、次のファイルの SQLDBType パラメータの値が不正なために問題が発生します。

```
Component_install_dir/identity/apps/common/bin/globalparams.xml
```

`component_install_dir` は、Identity Server がインストールされている場所です。

解決策

SQLDBType パラメータの値を次のように設定します。

- ODBC 接続タイプの場合は、値を Oracle に設定します。
- OCI 接続タイプの場合は、値を Oracle_OCI に設定します。
- SQL Server データベースの場合は、値を SQLServer に設定します。

簡易トランスポート・セキュリティ・モードが1年後に期限切れになる

簡易トランスポート・セキュリティ・モード証明書の有効期間のデフォルト値は365日です。

問題

Oracle Access Manager コンポーネント間のトランスポート・セキュリティを構成する際に、「オープン」、「簡易」および「証明書」モードから選択できます。詳細は、[第8章「トランスポート・セキュリティ・モードの変更」](#)を参照してください。

デフォルトでは、「簡易」モードは1年間のみ動作します。

解決策

次のように、簡易モード証明書の有効期限を延長できます。

1. 次のファイルを開きます。

```
component_install_dir/identity|access/oblix/tools/openssl/openssl_silent.cnf
```

`component_install_dir` は、アクセス・システムまたはIDシステム・コンポーネントがインストールされているディレクトリです。

2. このファイルで、`default_days` という名前のパラメータを探します。

デフォルトでは、次のようにこのパラメータの値は365日です。

```
default_days = 730 # Duration to certify for
```

3. デフォルトの日数を増やすことで、証明書の有効期限を延長できます。

たとえば、次のように証明書の有効期限を2年に延長できます。

```
default_days = 730 # Duration to certify for
```

4. `openssl_silent.cnf` ファイルで設定した期間の簡易モード証明書を再生成するには、次のいずれかのツールを使用してコンポーネントを再構成および再起動します。

- Access Server: `configureAAAServer.exe` を使用します。

詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

- WebGate: `configureWebGate` を使用します。

詳細は、『Oracle Access Manager Access System Administration Guide』を参照してください。

- WebPass: `setup_webpass.exe` を使用します。

詳細は、[第8章「トランスポート・セキュリティ・モードの変更」](#)を参照してください。

- Identity Server: `setup_ois.exe`

詳細は、[第8章「トランスポート・セキュリティ・モードの変更」](#)を参照してください。

スタイルシートの検証に失敗する

プレゼンテーション XML を使用してスタイルシートを作成またはカスタマイズするときに、スタイルシートのコンパイル・エラーが発生します。

問題

この問題は、次の処理を行うときに発生します。

1. テキスト・エディタまたは XML エディタ（推奨）でスタイルシートを開いたとき。
2. ファイルのパラメータを変更し、変更を保存したとき。
3. User Manager などの ID アプリケーションを開いて変更を参照したとき。

予期した結果 : 変更が予想どおりに表示されます。

実際の結果 : ID システムでバグ・レポートが発行されます。

解決策

この問題は様々な理由で発生しますが、おそらくスタイルシートのコーディング方法にエラーがあります。

Internet Explorer ウィンドウで XSL ファイルを開きます。コードにエラーがある場合は、ブラウザに、エラーのある行番号が表示されます。プレゼンテーション XML の詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

ワークフローを使用しているときに「xenroll.cab が見つかりません」エラーが発生する

ワークフローを実行しているときに、「xenroll.cab が見つかりません」という 404 エラーが発生することがあります。

問題

この問題は、ユーザーが次のように ID システム・アプリケーションでワークフローを実行したときに発生します。

1. User Manager を開きます。
2. ユーザー・プロファイルを表示します。
3. 「証明書登録」ワークフローを起動するプロファイルで「変更」ボタンをクリックします。

旧バージョンの Oracle Access Manager では、ファイル xenroll.cab は「証明書登録」ワークフローおよび「証明書失効」ワークフローに使用されていました。ただし、これらのワークフローのサポートは削除されました。現在このファイルは使用されていません。

解決策

スタイルシートから、xenroll.cab への参照を安全に削除できます。次に、この参照の例を示します。詳細は、『Oracle Access Manager カスタマイズ・ガイド』を参照してください。

```
<head>
... <object id="cenroll" classid="{clsid:43F8F289-7A20-11D0-8F06-00C04FC295E1}"
codebase="/identity/oblix/apps/common/bin/xenroll.cab" />
... <script
src="http://km.oraclecorp.com/identity/oblix/apps/common/bin/installCert.vbx"
language="VBScript" />
</head>
```


ワークフローを使用しているときに「有効化に失敗しました」エラーが発生する

ユーザーがワークフローを実行したときに、そのワークフローが失敗します。

問題

この問題は、ユーザーが次のように ID システム・アプリケーションでワークフローを実行したときに発生します。

1. User Manager を開きます。
2. ユーザー・プロフィールを表示します。
3. 「属性の変更」ワークフローを起動するプロフィールで「変更」ボタンをクリックします。

予期した結果: ワークフローが予想どおりに動作します。

実際の結果: 「有効化に失敗しました」エラーが発生します。

解決策

ワークフロー構成は多くの理由で失敗するため、この問題に対する明確な解決策はありません。ただし、可能性の高い原因として、ワークフロー構成中に無効な検索ベースを選択したことが考えられます。検索ベースを削除し、ワークフローを再構成します。詳細は、4-22 ページの「[検索ベースの概要](#)」を参照してください。

JPEG 写真イメージが更新されない

ID アプリケーションで写真を変更しようとしたときに、JPEG 写真イメージが更新されません。

問題

この問題は、「写真」属性に対する書き込み権限を持つユーザーが次の処理を行ったときに発生します。

1. User Manager を開きます。
2. 写真を含むユーザー・プロフィールを表示します。
3. パネル・ビューを選択します。
4. 新規写真のアップロードを試行します。

予期した結果: 写真が更新されます。

実際の結果: 写真が変更されません。

解決策

ページ・ビューで JPEG 写真イメージを変更します。

詳細情報

Oracle MetaLink (<http://metalink.oracle.com>) には、さらに多くの解決策が記載されています。問題の解決策が見つからない場合は、サービス・リクエストを記録してください。

索引

A

AAA Server

「Access Server」を参照

Access Manager

SDK, 構成, 7-65

現名称 Policy Manager, xviii

Access Manager API

旧名称 Access Server API, xviii

Access Manager SDK, 7-65

旧名称 Access Server SDK, xviii

Access Server, 1-3

AAA Server 構成オプション, 7-26

configureAAAServer ツール, 7-30, 8-26

Policy Manager の設定後の再構成, 7-30

SNMP モニタリング, 12-2

アカウント・ロックアウトのリダイレクト URL の設定, 7-65

オープン・モードへの変更, 8-15

簡易モードへの変更, 8-16

監査, 9-2

キャッシュの更新, 7-65

キャッシュ・フラッシュ, 通告, 8-3

証明書モードへの変更, 8-18

セキュリティ・パスワードの変更, 8-26

トランスポート・セキュリティ, 8-4

トランスポート・セキュリティ・モードの変更, 8-11

ファイルベース監査, 11-18

ユーザー・データと構成データの場所, 7-20

ロギング, 10-2

Access Server API

現名称 Access Manager API, xviii

Access Server SDK

現名称 Access Manager SDK, xviii

AccessGate

トランスポート・セキュリティ, 8-4

トランスポート・セキュリティ・モードの変更, 8-11

ロギング, 10-2

Access 管理 API

現名称 Policy Manager API, xviii

Access ドメイン

旧名称 NetPoint Access Manager ドメインまたは
COREid Access Manager ドメイン, xviii

Active Directory, 7-33

ADSI での LDAP 認証, C-5

credential_mapping プラグイン, A-7

LDAP でのタイムアウト, C-4

LDAP を使用した構成, C-1

LDAP を使用する Access Server, C-3

LDAP を使用する Policy Manager 設定, C-3

Microsoft Global Catalog, C-2

.NET 機能, A-10

ObMyGroups アクション属性, A-6

Oracle Access Manager での ADSI 構成, B-2

SAM アカウント名の文字数増加, xxi

親子認可, A-6

親子認証, A-5

下位互換性, A-9

グループ検索読取り操作, A-4

このリリースの新機能, xxi

ディレクトリ・サーバー・プロファイルの定義, A-2

デプロイ, A-1

トラブルシューティング, A-10

認可, A-4

認証, A-4

非結合検索ベース, A-3

非結合検索ベースの削除, A-3

必要なスキーマの変更, 3-19

プロファイルと検索ベースの設定, A-2

AD Forest 用の COREid Basic Over LDAP 認証

現名称 AD Forest 用の Oracle Access and Identity
Basic over LDAP, xix

AD Forest 用の NetPoint Basic Over LDAP 認証

現名称 AD Forest 用の Oracle Access and Identity
Basic over LDAP, xix

AD Forest 用の Oracle Access and Identity Basic over LDAP

旧名称 AD Forest 用の NetPoint Basic Over LDAP ま
たは COREid Basic Over LDAP, xix

ADSI, 7-33

Access Server のバインド・メカニズム, B-7

ADSI と LDAP の混在構成, B-4

Identity Server のバインド・メカニズム, B-4

ID システムに対する構成, B-9

pageSize パラメータ, B-13

アクセス・システムに対する構成, B-7, B-12

構成, B-1

構成ファイル, B-5, B-8

トラブルシューティング, B-13

AM サービス状態

現名称 Policy Manager API サポート・モード, xix

ANR, D-2

B

backURL, 7-62, 7-64

C

CA 証明書

- セキュリティ
- CA 証明書, 8-5
- 複数のインポート, 8-26

cert7.db, 8-2

cert8.db, 8-2

configureAAAServer コマンド, 8-15, 8-17

configureAAAServer ツール, 8-2

configureAccessGate, 8-17

COREid

現名称 Oracle Access Manager, xviii

COREid Access Manager ドメイン

現名称 Access ドメイン, xviii

COREid Basic Over LDAP 認証

現名称 Oracle Access and Identity, xviii

COREid Identity ドメイン

現名称 Identity ドメイン, xviii

COREid None 認証

現名称匿名認証, xviii

COREid 管理者

現名称マスター管理者, xviii

COREid システム・コンソール

現名称 ID システム・コンソール, xviii

D

DIT

重複しないディレクトリ・ツリー, 7-34

複数のブランチの検索, 7-34

G

genCert ユーティリティ, 8-5, 8-17

GIF

Chystal Repository データベース内のファイル,
11-12

ID システムの UI に使用されるイメージ, 7-2

イメージ, ファイル・システム内での参照, 4-36

イメージ, ワークフローのロケーション・マップでの
使用, 5-67

セマンティック型, 3-14, 3-15

タイトル・イメージ, 4-15

タブ・イメージ, 4-4

データ型, 3-12

表示タイプ, 3-12, 3-16

写真, 4-35

表示タイプ, 構成, 3-28

「ロケーション座標」セマンティック型, 3-15

globalparams.xml ファイルの設定, 4-50

Group Manager

「Group Manager 構成」タブ, 4-2

インストール時に構成されるオブジェクト, 3-3

オブジェクトの構成, 3-2

概要, 4-2

クラス属性, 3-8

クラス属性を通じたオブジェクト・クラスに対する読
取り権限の制御, 3-8

グループ作成権限, 4-38

グループ・タイプ・パネル, 4-17

「グループ」タブ, 4-2, 4-17

「グループ」ページ, 4-10

グループへのサブスクライブ, 4-42

検索

DIT での検索の開始ポイント, 4-21

検索で戻される項目の構成, 4-7

検索フィールドの構成, 4-6

構成, 4-10

構成, 概要, 4-1

構成済のオブジェクト・クラスの表示, 3-4

サポートされるワークフロー・タイプ, 5-8

ただ1つのタブ, 4-3

タブ

構成, 4-2

表示, 4-3

変更, 4-3

導出属性の追加, 3-30

動的グループの拡張, 4-49

動的メンバーのみ, 4-42

バックエンド・システムへのデータの送信, 6-2

パネル, 4-11

構成, 4-13

削除, 4-13

並べ替え, 4-17

表示, 4-13

ローカライズ, 4-20

複数の言語の構成, 7-7

プロファイル・ページ, 4-11

補助オブジェクト・クラスの追加, 4-8

メンバー・プロファイルの表示, 4-10

ユーザーによるデータの表示および変更の許可, 4-31

レポート, 4-44

ローカライズ, 4-5

ワークフロー・タイプ, 5-8

I

Identity Server

Group Manager アプリケーション, 1-2

Organization Manager アプリケーション, 1-3

SNMP モニタリング, 12-2

User Manager アプリケーション, 1-2

WebPass プラグイン, 1-3

インストール, 1-3

監査, 9-2

監査, 構成, 11-36

管理, 7-15

キャッシュ, 7-14

キャッシュ・フラッシュに関する通告, 8-3

構成, 7-10

構成者, 2-2

コマンドラインによる管理, 7-19

セッション・タイムアウト設定, 7-11

設定, 構成, 7-10

設定の表示, 7-10

設定の変更, 7-10

追加, 7-16

定義, 1-2

トランスポート・セキュリティ

変更, 8-6

パラメータの削除, 7-19

表示, 7-18

フィードバック用の電子メール・アドレス, 設定,
7-12

複数, 設定, 7-15

変更, 7-18
メール・サーバー・アラート, 構成, 7-13
ロギング, 10-2
Identity Server からの情報の取得, 1-3
Identity ドメイン
旧名称 COREid Identity ドメイン, xviii
旧名称 NetPoint Identity ドメイン, xviii
ID アプリケーション
「Group Manager」を参照
「Org. Manager」を参照
「User Manager」を参照
概要, 1-4
構成
「オブジェクトおよび属性」を参照
構成, 例, 4-35
構成の例, 4-35
タブ, 4-2, 4-3
変更, 4-3
用途, 1-4
ID システム
Access Manager SDK の構成, 7-65
ADSI 構成, B-3
Identity Server, 1-2
WebPass, 1-3
インストールのサマリー, 1-3
管理, 概要, 1-2, 1-5
管理者, 2-1
構成, xv
構成, 概要, 1-2, 1-4
コンポーネント, 1-2
トランスポート・セキュリティ, 8-3
変更, 8-6
ログイン, 1-7
ID システム・コンソール
旧名称 COREid システム・コンソール, xviii

L

LDAP
オブジェクト, パネル, 4-12
クライアント・リクエストのリダイレクト, 7-31
参照, 7-31, 7-32
データ
Oracle Access Manager 用の構成, 3-1
プロセスの概要, 3-3
プロファイル・ページでの表示, 3-2
読取りおよび書込み権限, 4-31
フィルタ
拡張, 4-30
クエリー・ビルダー, 4-27
検索, 4-27
プロファイル, 7-21
ワークフローのオブジェクト, 5-7

M

MTHML, 7-13

N

.NET, A-10
ANR, D-2
AzMan との統合, D-15

Microsoft リソース, D-16
Security Connector for ASP.NET との統合, D-16
あいまいな名前, 解決, D-2
アクセス・システム・パスワード管理, D-14
暗号化の有効化, D-10
概要, D-1
管理コードとヘルパー・クラス, D-15
グループの属性の追加, D-8
スマートカード認証との統合, D-15
属性の動的な追加, D-7
統合 Windows 認証, D-11
動的にリンクされた補助クラス, D-6
トラブルシューティング, D-16
ファスト・バインドの有効化, D-9
NetPoint
現名称 Oracle Access Manager, xviii
NetPoint Access Manager ドメイン
現名称 Access ドメイン, xviii
NetPoint Access プロトコル
現名称 Oracle Access プロトコル, xviii
NetPoint Basic Over LDAP 認証
現名称 Oracle Access and Identity, xviii
NetPoint Identity ドメイン
現名称 Identity ドメイン, xviii
NetPoint ID プロトコル
現名称 Oracle ID プロトコル, xviii
NetPoint None 認証
現名称匿名認証, xviii
NetPoint SAML サービス
現名称 Oracle Identity Federation, xviii
NetPoint 管理者
現名称マスター管理者, xviii
Novell Directory Server
構成の要件, 3-19

O

oblixAdvancedGroup, 4-41
oblixppcatalog.lst, 5-40
Oblix ツリー
現名称構成ツリー, xviii
Oblix データ
現名称構成データ, xviii
OctetString Virtual Directory Engine (VDE)
現名称 Oracle Virtual Directory, xviii
ois_cert.pem, 8-5
ois_chain.pem, 8-5
ois_key.pem, 8-5
Oracle Access and Identity 認証
旧名称 NetPoint Basic Over LDAP または COREid
Basic Over LDAP, xviii
Oracle Access Manager
概要, xv, 1-6
旧名称 NetPoint または COREid, xviii
Oracle Access プロトコル
旧名称 NetPoint Access プロトコル, xviii
Oracle Application Server 10g リリース 2 (10.1.2)
Oracle COREid 7.0.4 としても利用可能, xviii
Oracle COREid リリース 7.0.4
Oracle Application Server 10g リリース 2 (10.1.2) の
一部としても利用可能, xviii
Oracle Identity Federation, xviii
旧名称 SHAREid, xviii

Oracle ID プロトコル
旧名称 NetPoint ID プロトコル, xviii

Oracle Virtual Directory Server, 7-25
旧名称 OctetString Virtual Directory Engine (VDE), xviii

Org. Manager
「Org. Manager 構成」タブ, 4-2
インストール時に構成されるオブジェクト, 3-3
オブジェクトの構成, 3-2
オブジェクトの削除, 5-12
オブジェクトの作成, 5-12
概要, 4-2
クラス属性, 3-8
クラス属性を通じたオブジェクト・クラスに対する読取り権限の制御, 3-8

検索
DIT での検索の開始ポイント, 4-21
検索で戻される項目の構成, 4-7
検索フィールドの構成, 4-6
構成, 概要, 4-1
構成済のオブジェクト・クラスの表示, 3-4
コンテナ制限, 4-52
コンテナ制限, 削除, 4-55
コンテナ制限の変更, 4-54
サポートされるワークフロー・タイプ, 5-8
属性の変更, 5-12
タブ, 3-4
構成, 4-2
表示, 4-3
変更, 4-3
タブの削除, 4-11
タブの追加, 4-6
タブの並べ替え, 4-11
定義, 1-3
導出属性の追加, 3-30
ドメイン間でのコンテナ制限のコピー, 4-54
任意のタブ, 4-2
バックエンド・システムへのデータの送信, 6-2

パネル
構成, 4-13
削除, 4-13
表示, 4-13
ローカライズ, 4-20
複数の言語の構成, 7-7
複数のタブ, 4-3
ヘッダー・パネル, 4-12
補助オブジェクト・クラスの追加, 4-8
ユーザーによるデータの表示および変更の許可, 4-31
レポート, 4-44
ローカライズ, 4-5
「ロケーション」タブ, 4-37
ワークフロー・タイプ, 5-8

P

PEM ファイル, 8-5

Policy Manager
オープン・モードへの変更, 8-15
簡易モードへの変更, 8-16
旧名称 Access Manager, xviii
構成データとユーザー・データの場所, 7-20
証明書モードへの変更, 8-18
トランスポート・セキュリティ, 8-4

ロギング, 10-2

Policy Manager API, xviii
旧名称 Access 管理 API, xviii

Policy Manager API サポート・モード
旧名称 AM サービス状態, xix

R

RDBMS プロファイル
追加, 7-36, 7-37
データベース・インスタンス, 7-38
データベース・インスタンス, 追加, 7-38
変更, 7-37

ResourceFilterSerachScope, 4-50

S

SAMAccountName, xxi, A-9

setup_accessmanager, 8-2

setup_ois, 8-2

setup_ois コマンド, 8-8

setup_ois ユーティリティ, 8-10

SHAREid
現名称 Oracle Identity Federation, xviii

SMTP サーバー構成, 7-13

SNMP, 12-1

Access Server トラップ, 12-12

Access Server の MIB オブジェクト, 12-9

Identity Server トラップ, 12-8

Identity Server の MIB オブジェクト, 12-5

ID イベント API の MIB オブジェクト, 12-6

ID システム・ディレクトリの MIB オブジェクト, 12-7

MIB 階層, 図, 12-3

MIB 索引フィールド, 12-4

Netstat 値と SNMP 値, 12-21

NMS, SNMP モニタリングでの使用, 12-2

obscoreboard_params.xml, 12-15

Oracle Access Manager MIB, 12-3

SNMP モニタリングについて, 12-2

アクセス・システム・ディレクトリ・サーバーの MIB オブジェクト, 12-10

イベント・トラップ, 12-2

エージェント, 宛先, 12-13

エージェント, 概要, 12-3

エージェントおよびトラップの宛先, 12-13

管理情報ベース, 12-3

構成, 12-13

構成設定, 12-15

サポートされるバージョン, 12-2

前提条件, 12-2

停止間隔, 12-21

データ, 宛先, 12-13

統計, 収集, 12-13

トラップ, 12-2

トラップ, 宛先, 12-13

認証プラグインの MIB オブジェクト, 12-11

ネットワーク管理ステーション, 12-2

ポーリング, 12-2

ポーリング間隔, 12-13

メッセージ, 12-16

モニタリング, 無効化, 12-13

モニタリング, 有効化, 12-13

モニタリングの無効化, 12-13
モニタリングの有効化, 12-13
ライブ接続数, 12-21
リクエスト・キューの MIB オブジェクト, 12-12
ロギング, 12-16

U

User Manager

「ID」タブ, 4-2
「User Manager 構成」タブ, 4-2
インストール時に構成されるオブジェクト, 3-3
オブジェクトの構成, 3-2
概要, 4-2
クラス属性, 3-8
クラス属性を通じたオブジェクト・クラスに対する読取り権限の制御, 3-8
検索
DIT での検索の開始ポイント, 4-21
検索で戻される項目の構成, 4-7
検索フィールドの構成, 4-6
構成, 概要, 4-1
構成済のオブジェクト・クラスの表示, 3-4
サポートされるワークフロー・タイプ, 5-8
ただ1つのタブ, 4-3
タブ
構成, 4-2
表示, 4-3
変更, 4-3
定義, 1-2
導出属性の追加, 3-30
バックエンド・システムへのデータの送信, 6-2
パネル, 4-11
構成, 4-13
削除, 4-13
表示, 4-13
ローカライズ, 4-20
複数の言語の構成, 7-7
プロファイル・ページ, 4-11
プロファイル・ページの例, 3-2
ヘッダー・パネル, 4-12
補助オブジェクト・クラスの追加, 4-8
ユーザーによるデータの表示および変更の許可, 4-31
レポート, 4-44
ローカライズ, 4-5
ワークフロー・タイプ, 5-8
ワークフローの例, 5-2, 5-6

V

VDS, 7-25

W

WebGate

オープン・モードへの変更, 8-15
簡易モードへの変更, 8-16
証明書モードへの変更, 8-18
証明書リクエスト, 8-5
セッション・タイムアウト, 7-11
ロギング, 10-2

WebPass

Identity Server 導入後のインストール, 7-39

Identity Server との関連付け, 7-45
Identity Server との関連付けの解除, 7-46
Identity Server との関連付けの表示, 7-45
setup_webpass コマンド, 7-44
構成, 7-39
構成者, 2-2
コマンドラインによる変更, 7-43
削除, 7-42
追加, 7-40
定義, 1-3
トランスポート・セキュリティ
変更, 8-6
表示, 7-40
変更, 7-40
ロギング, 10-2

あ

アクセス・システム

オープン・セキュリティ・モードへの変更, 8-15
簡易トランスポート・セキュリティへの変更, 8-16
トランスポート・セキュリティ, 8-3, 8-4
トランスポート・セキュリティ・モードの変更, 8-11
ロギング, 1-8
暗号化
有効化, D-10

い

委任 ID 管理者

「委任管理者」も参照
実行するタスク, 2-3
定義, 2-2

委任管理

ASP モデル, 2-7
委任管理者の追加, 2-8
委任できる項目, 2-5
イントラネット・モデル, 2-7
エクストラネット・モデル, 2-6
モデル, 2-6

インストール, 7-67

お

オープン・モード

概要, 8-2

オブジェクト

「オブジェクト・クラス」も参照
「属性」も参照
Group, 3-6
Location, 3-6
Person, 3-6
インストール時の構成, 3-3
インストール時のデフォルト構成, 3-3
オブジェクト・クラスの削除, 3-10
オブジェクト・クラスの追加, 3-9
オブジェクト・テンプレート, 6-2
クラス種別, 3-6
クラス属性, 3-7
選択, 3-8
クラス属性, 概要, 3-11
クラス・タイプ, 3-6
継承, 3-4

- 検索のキーとして使用される属性, 3-7
- 構成のためのプロセス, 3-3
- 構造化オブジェクト・クラスの変更, 3-9
- テンプレート・オブジェクト, 3-2
 - 変更に関する留意事項, 6-2
- テンプレート・オブジェクト, ID システムでの使用方法, 3-5
- テンプレート・オブジェクト, 概要, 6-1
- テンプレート・オブジェクト・クラス, 3-5
- 汎用, 3-6
- 表示, 3-6
- プロビジョニングで使用, 3-2
- プロファイル・ページでの表示, 3-2
- 変更, 3-7
- 補助オブジェクト・クラス, 3-4, 3-10
- ミックスイン, 3-4
- ユーザーが参照および変更できるようにする方法, 概要, 3-1
- ワークフロー, 5-7
- オブジェクト・クラス
 - 概要, 3-2
 - 構造化, 3-4
 - テンプレート・オブジェクト・クラス, 3-5
 - 補助, 3-4
- オブジェクト・クラス種別, 3-6
- オブジェクト・クラス・タイプ, 3-6
- 「オブジェクト・クラス」フィールド, 4-4
- 「オブジェクト・セクタ」表示タイプ
 - 検索フィルタ, 3-23
- オブジェクト・テンプレート
 - 「テンプレート・オブジェクト」も参照
 - 「プロビジョニング」も参照
- オブジェクト・テンプレート・ファイル, 6-5
- 構成, 6-4
- ファイル, 形式, 6-5
- ファイル, 例, 6-7
- ファイルの要素, 6-7
- オブジェクトの削除ワークフロー, 5-5
- オブジェクトの作成ワークフロー, 5-5

か

- 「外出中」フラグ, 5-44
- 書込み権限, 4-21
- 簡易モード
 - 概要, 8-2
- 監査, 11-1
 - Access Server と Identity Server のデータベースへの接続, 11-28
 - Access Server に対する有効化, 11-6
 - Crystal Reports, 11-4
 - Crystal Reports テンプレート, 使用, 11-44
 - Crystal リポジトリ, 11-14
 - Identity Server での有効化, 11-5
 - ID アプリケーションのアクション, 4-43
 - ID システム・アクションの成功と失敗, 11-6
 - OCI 接続タイプ, 11-14
 - ODBC データ・ソース定義, 11-11
 - ODBC ドライバ, 11-13
 - RDBMS プロファイル, 11-6
 - RDBMS プロファイル構成, 11-13
 - RDBMS プロファイル, 11-7
 - SQL Server, インストール, 11-21

- 概要, 11-2
- 監査機能の GUI の場所, 11-5
- 監査する ID イベント, 11-5
- 監査データベース, 概要, 11-14
- 監査データベース, 作成, 11-22
- 監査データベース, 設定, 11-20
- 監査リポジトリとしての Oracle Database, xx
- 監査レポート, 設定, 11-44
- グローバル・ユーザー・アクセス権限レポート, 11-7
- 出力タイプと量, 11-5
- 書式, 11-5
- 新機能, xx
- 診断, 11-7
 - 診断, オンスクリーン, 11-6
- 静的レポート, 11-4
- セキュリティの考慮事項, 11-2
- データベース監査, 設定, 11-19
- データベースの監査のアーキテクチャ, 11-9
- データベースの監査の要件, 11-8
- 動的, 11-4
- 認証イベント, 7-49
- パフォーマンスの考慮事項, 11-3
- ファイル監査とデータベース監査, 11-2
- ファイルベース, 設定, 11-16
- プロファイル情報, 11-4
- ポリシー情報, 11-4
- マスター監査ルール, 11-7
- レポート, タイプ, 11-15

管理

- 準備, 1-1
- 管理者
 - ID 管理者について, 2-2
 - ID システム, 2-1
 - 委任 ID 管理者, 2-2, 2-3
 - 委任管理
 - 委任管理者の追加, 2-8
 - 構成, タスクの概要, 2-5
 - モデル, 2-6
 - 委任管理者, 2-5
 - 管理者の削除, 2-4
 - 構成, 2-1, 2-4
 - すべての属性にアクセスできる管理者, 4-31
 - 代替管理者, 2-10
 - 別の管理者の ID の取得, 2-10
 - 別の人物への一時的な権限付与, 2-10
 - マスター ID 管理者, 2-2, 2-3
 - マスター管理者, 2-2
- 管理の準備, 1-1

き

機能

- 新機能, xvii
- キャッシュ
 - Access Server キャッシュの更新, 7-65
 - Identity Server キャッシュの管理, 7-14
 - アクセス・キャッシュ・フラッシュ, 通告, 8-3

<

- クイックスタート・ツール, 5-16
- 例, 5-18

- クエリー・ビルダー
 - 概要, 4-27
 - 拡張フィルタ, 4-30
- グループ, 4-41
 - Group Manager アプリケーション, 1-2
 - Group Manager での管理, 1-2
 - ID システムでの管理, 1-2
 - LDAP フィルタにより決定されるメンバーシップ, 4-48
 - URL パラメータを使用したカスタマイズ, 4-10
 - 管理, 4-38
 - 管理者であるグループ, 4-10
 - グループ・タイプ・パネル, 4-17
 - グループの削除, 5-12
 - グループの作成, 5-11
 - 検索, 4-39
 - 作成権限, 4-38
 - サブスクライブ, 4-41, 4-42
 - 静的, 4-10
 - 静的メンバー, 表示, 4-10
 - 属性の変更, 5-11
 - 通知用のメール・サーバー, 7-13
 - 動的, 4-10, 4-48
 - 動的グループの拡張, 4-49
 - 動的メンバー, 表示, 4-10
 - ネスト, 4-10
 - ネストされたメンバー, 表示, 4-10
 - メンバーとして所属, 4-10
 - メンバーの削除, 4-40
 - メンバーの追加, 4-40
- グループの削除ワークフロー, 5-5
- グループの作成ワークフロー, 5-5
- 「グループ」ページ, 4-10
- クローニング, 7-67
- グローバリゼーション
 - 「ローカライズ」も参照
 - サポート, xix

け

- 言語
 - 「ローカライズ」を参照
- 検索, 1-10
 - 「属性, 検索」も参照
 - DIT の複数のブランチ, 4-26
 - ID アプリケーションで表示できないデータの検索, 4-44
 - 基本, 1-10
 - グループ・メンバー, 4-39
 - 結果, ローカライズ, 4-7
 - 検索結果, 構成, 4-7
 - 検索結果属性, 4-7
 - 検索結果の集計, 1-11
 - 検索する DIT のレベル, 4-50
 - 検索で返された項目の選択, 1-11
 - 検索の有効範囲の変更, 4-50
 - 検索フィルタの定義, 3-24
 - 検索ベース
 - 概要, 4-22
 - 設定, 4-24
 - 設定のガイドライン, 4-22
 - 検索ベースの設定, 4-22
 - セレクタを使用, 1-11

- 対象とする DIT のレベル数, 4-49
- 置換構文, 3-26
- フィルタ, 4-27
 - 「オブジェクト・セレクタ」表示タイプ, 3-23
 - 静的, 3-25
 - 置換構文, 3-26
 - 動的, 3-27
 - 複数値による動的検索, 3-27
 - 複数のターゲットによる静的検索, 3-26
 - ワイルド・カードによる静的検索, 3-25
 - ワイルド・カードによる動的検索, 3-27
- 複数の検索ベースの操作, 7-34
- 複数のターゲット, 3-25, 3-26
- プロファイル・ページの属性に一致する結果を戻す方法, 3-27
- 戻される属性の選択, 4-7
- 有効範囲, 4-49
- ログイン・ユーザーと同じ DIT レベルでのユーザー検索, 3-26

検索ベース

- Active Directory の非結合検索ベース, A-3
- DIT の複数のブランチ, 4-26
- 概要, 4-22
- グループ用の設定, 4-26
- 削除, A-3
- 設定, 4-24
- 設定のガイドライン, 4-22
- 非結合, 4-26
- 複数, xx
- 複数の検索ベースの構成, xx

こ

- 構成ツリー
 - 旧名称 Oblix ツリー, xviii
- 構成データ
 - 格納用のプロファイル, 7-21
 - 旧名称 Oblix データ, xviii
 - 新規ディレクトリ・サーバーの参照, 7-30
- このリリースの新機能, xvii
- コンポーネント
 - コピー, 7-67

さ

- サブスクリプションの管理, 4-41
- サブフロー
 - 概要, 5-15

し

- 自己登録, 4-25
- 自己登録ワークフロー, 5-5
- 写真
 - ディレクトリへのインポート, 4-36
 - デフォルト・イメージ, 4-37
 - ファイル・システム内での参照, 4-36
 - ユーザー・プロファイルでの表示, 4-35
- 証明書
 - インストール, 8-10
- 証明書モード
 - アクセス・システムの変更, 8-18
 - 概要, 8-2

証明書のインストール, 8-10

新機能

Oracle Database の監査, xx

ログイン, xx, xxi

シングル・サインオン

Active Directory に対する構成, A-8

『Oracle Access Manager アクセス管理ガイド』も参照

す

スキーマ・データ

構成, 3-3

スタイル

カスタム・スタイル・ディレクトリの追加, 7-3

構成, 7-2

削除, 7-7

スタイルのディレクトリ, 7-4

追加, 7-5

デフォルトの設定, 7-7

配布, 7-6

表示, 7-3

複数の言語用の構成, 7-4

変更, 7-6

せ

セキュリティ

「トランスポート・セキュリティ」も参照

セッション・タイムアウト, 7-11

設定

手動による再実行, 7-28

セマンティック型

グループ静的メンバー, 3-14

グループ動的メンバー, 3-14

グループの所有者, 3-14

写真, 3-14

チャレンジ, 3-15

なし, 3-15

パスワード, 3-13

フルネーム, 3-13

マップ, 3-15

役職, 3-14

優先電子メール・アドレス, 3-15

レスポンス, 3-15

ログイン, 3-13

セレクトタ, 3-23

そ

属性

ID アプリケーションでの使用方法, 3-2

クラス属性, 3-7, 3-11

選択, 3-8

クラス属性に対するユーザー・アクセスの付与, 3-8

検索

検索のキーとして使用される属性, 3-7

異なる属性からの同じ値の検出, 3-28

動的, 3-27

複数値による動的検索, 3-27

プロフィール・ページの属性に一致する結果を戻す方法, 3-27

ログイン・ユーザーの DN に一致するターゲット

を戻す方法, 3-26

ワイルド・カードによる動的検索, 3-27

検索可能項目の選択, 4-6

検索キー (クラス) 属性, 3-7

検索で使用するフィルタ, 3-24

構成, 3-11, 3-19

セマンティック型, 3-12

DN 接頭辞, 3-13

Group Manager での使用, 3-14

グループ静的メンバー, 3-14

グループ動的メンバー, 3-14

グループの所有者, 3-14

システム設定時の定義, 3-13

写真, 3-14

チャレンジ, 3-15

なし, 3-15

パスワード, 3-13

フルネーム, 3-13, 3-14

プロフィール・ページでの使用, 3-14

マップ, 3-15

役職, 3-14

優先電子メール・アドレス, 3-15

レスポンス, 3-15

ログイン, 3-13

ロケーション座標, 3-15

ロスト・パスワード, 管理用の属性, 3-15

選択キー, 4-33

属性の静的リストのルール, 定義, 3-20

ディレクトリ問合せを使用した値リストの構成 (フィルタ), 3-20

データ型, 3-12

識別名, 3-12

住所, 3-12

整数, 3-12

電話, 3-12

バイナリ, 3-12

文字列, 3-12

テンプレート・オブジェクト・クラスのクラス属性, 3-8

テンプレート属性, 3-5

導出

User Manager タブへの追加, 3-30

概要, 3-28

注意事項, 3-29

例, 3-29

パスワード, 3-15

表示, 3-18

表示タイプ, 3-16

GIF イメージ, 3-16

GIF イメージ URL, 3-16

S/MIME 証明書, 3-17

オブジェクト・セレクトタ, 3-17

住所, 3-17

数値文字列, 3-17

選択メニュー, 3-17

単一行テキスト, 3-17

チェック・ボックス, 3-16

電子メール, 3-16

なし, 3-16

日付, 3-16

フィルタ・ビルダー, 3-16

ブール, 3-16

- 複数行テキスト, 3-16
- メディア, 3-16
- ラジオ・ボタン, 3-17
- ロケーション, 3-16
- 表示名, ローカライズ, 3-22
- プロビジョニング (テンプレート) 属性, 3-5
- ラジオ・ボタン、チェック・ボックスなどのリストの構成, 3-20
- リスト, 定義, 3-21
- ローカライズ, 3-22
- 属性の変更ワークフロー, 5-5

た

タスクの概要

- Crystal Reports を Oracle Repository に接続する手順, 11-46
- ID システムに対する ADSI の構成, B-9
- IWA 認証の設定, D-12
- Oracle Access Manager サーバーの監査データベースへの接続の有効化, 11-29
- RDBMS プロファイルの設定, 11-32
- アクセス・システムに対する ADSI の構成, B-12
- アプリケーションでの情報の表示, 4-2
- 監査スキーマのアップロード, 11-23
- 監査データベースの準備, 11-20
- 監査の構成の手順, 11-35
- 監査レポートの設定手順, 11-44
- 管理者の委任, 2-5
- 検索時に ANR を使用する準備, D-3
- サロゲートの有効化, 5-43
- セカンダリ RDBMS インスタンスを作成する手順, 11-34
- データベース監査の有効化, 11-19
- 動的参加者を選択するプラグインまたはアプリケーションの作成, 5-41
- 動的補助クラスの設定, D-6
- 複数の Identity Server の設定, 7-15
- マルチ言語機能の構成, 7-8
- ロケーション機能とユーザーの有効化, 5-67
- ロケーション機能の有効化, 4-37
- ロケーションの作成ワークフローの定義, 5-68
- ワークフロー・アプレットを使用したワークフローの定義, 5-19
- ワークフロー・ステップへの動的参加者の割当て, 5-39
- ワークフロー定義の作成, 5-4
- タブ, 1-9, 3-4
- Org. Manager への追加, 4-6
- 「オブジェクト・クラス」構成フィールド, 4-4
- 検索, 4-6
- 構成, 4-2
- 削除, 4-11
- 「タブ・フィルタ」フィールド, 4-4
- 並べ替え, 4-11
- パネル, 構成, 4-11
- 表示, 4-3
- プロファイル・ページ, 構成, 4-11
- 変更, 4-3
- 補助オブジェクト・クラスとテンプレート・オブジェクト・クラスの追加, 4-8
- ローカライズ, 4-5
- 「タブ・フィルタ」フィールド, 4-4

ち

- 置換構文, 3-26, 5-22
- チャレンジ属性, 7-58
- チャレンジ・フレーズ削除, 7-57

て

- ディレクトリ・サーバー
 - トランスポート・セキュリティ, 8-4
 - トランスポート・セキュリティの変更, 8-22
 - 複数の検索ベースの操作, 7-34
 - プロファイル, 7-21
- ディレクトリ・サーバー・プロファイル作成, 7-22
- データベース・インスタンス, 構成, 7-31
- データベース・インスタンスの削除, 7-33
- 表示, 7-27
- プロファイルの共有, 8-4
- 変更, 7-28
- 変更後の設定の再実行, 7-28
- データ, エクスポート
 - 「データのエクスポート」を参照
- データ型, 3-12
- 識別名, 3-12
- 住所, 3-12
- 整数, 3-12
- 電話, 3-12
- バイナリ, 3-12
- 文字列, 3-12
- データのエクスポート
 - 「オブジェクト・テンプレート」も参照
 - IdentityXML アクション, 6-3
 - オブジェクト・テンプレート, 6-2
 - 概要, 3-2, 6-1
 - 制限, 5-19
 - ワークフローの使用, 6-2
- データベース・インスタンス
 - LDAP プロファイル, 7-30
 - RDBMS プロファイル, 7-30
 - 構成, 7-31
 - 削除, 7-33
 - 追加, 7-30
- 手順
 - Access Manager SDK
 - Access Manager SDK の構成, 7-66
 - Active Directory
 - Access Server に対する LDAP 認証の有効化の手順, C-5
 - Active Directory に対して Access Server を設定する手順, C-3
 - Active Directory に対して Policy Manager を設定する手順, C-3
 - credential_mapping プラグインの構成手順 (AD), A-7
 - Disjoint_domain の非結合検索ベースを追加する手順 (AD), A-3
 - ID システムまたはアクセス・システムで SSO を構成する手順 (AD), A-8
 - Windows 2003 でグループ検索読み取り操作を構成する手順, A-4

- インストール後に Access Server フェイルオーバーを指定する手順, C-4
- 追加のディレクトリ・サーバー・プロファイルを設定する手順, A-3
- 追加のディレクトリ・サーバー・プロファイルを設定する手順 (AD), A-3
- ADSI
 - Access Server に対する LDAP 認証の有効化の手順, B-12
 - ADSI エージェントをすべてのドメインと関連付ける手順, B-4
 - 追加のディレクトリ・プロファイルに対して ADSI を有効にする手順, B-10
- ID アプリケーション
 - globalparams.xml ファイルの設定, 4-50
 - Organization Manager でのタブの並べ替え, 4-11
 - User Manager、Group Manager または Organization Manager 固有の属性の変更, 4-20
 - あるドメインから別のドメインへのコンテナ制限のコピー, 4-54
 - エンド・ユーザーの ID システム・アプリケーションでのパネルの表示, 4-13
 - 監査ポリシーの設定または変更, 4-44
 - 監査ポリシーの表示, 4-43
 - クエリー・ビルダーの使用, 4-27
 - 「グループ」および「メンバー・プロファイルの表示」に表示する項目の選択, 4-10
 - グループ・タイプ・パネルの追加、変更または削除, 4-18
 - グループ・タイプ・パネルの表示, 4-17
 - グループの表示, 4-39
 - グループへのサブスクライブ, 4-42
 - グループ・メンバーの削除, 4-40
 - グループ・メンバーの追加, 4-40
 - グループ・メンバーの表示, 4-39
 - 検索結果属性の表示, 4-7
 - 検索結果のローカライズ, 4-7
 - 検索に使用できる属性の指定, 4-6
 - 検索ベースの設定, 4-24
 - コンテナ制限の削除, 4-55
 - コンテナ制限の表示および追加, 4-52
 - コンテナ制限の変更, 4-54
 - 写真の構成とディレクトリへのインポート, 4-36
 - 属性権限の設定または変更, 4-31
 - 属性の表示名のローカライズ, 4-21
 - タブ構成情報の表示または変更, 4-3
 - タブの削除, 4-11
 - タブの追加, 4-6
 - タブへの補助オブジェクト・クラスまたはテンプレート・オブジェクト・クラスの追加, 4-8
 - ディレクトリへの写真のインポート, 4-36
 - 導出属性のアプリケーション・タブへの追加, 3-30
 - 動的グループの拡張, 4-49
 - パネルの構成の表示または変更, 4-16
 - パネルの作成または追加, 4-14
 - パネルの表示順序の変更, 4-17
 - パネルの表示名のローカライズ, 4-19
 - パネルのローカライズ, 4-16
 - 非結合検索ベースの削除, 4-27
 - 非結合ドメインへの非結合検索ベースの追加, 4-26
 - ファイル・システムに存在する写真の参照, 4-36
 - 複雑なフィルタの作成, 4-30
 - 複数のグループへのサブスクライブ, 4-43
 - ヘッダー・パネルの構成, 4-12
 - レポートの構成, 4-45
 - レポートの削除, 4-48
 - レポートの書式設定の変更, 4-46
 - レポートの表示または変更, 4-47
 - レポートのローカライズ, 4-47
 - ローカライズされたタブ構成の作成、表示および変更, 4-5
- ID システム
 - カスタム・スタイルの削除, 7-7
 - 現在構成されているスタイルの表示, 7-3
 - スタイルの配布, 7-6
 - スタイルの変更, 7-6
 - スタイル名の変更, 7-6
 - デフォルト・スタイルの設定, 7-7
- .NET
 - ID システム・パネルでの ANR の構成の手順, D-4
 - IWA のテストの手順, D-14
 - User Manager で追加の補助オブジェクト・クラスを指定する手順, D-7
 - WebGate をホストしているマシンで IWA を有効にする手順, D-12
 - アクセス・システム・コンソールで AccessGate を変更する手順, D-13
 - アクセス・システムで IWA 認証スキームを作成する手順, D-13
 - 「グループ・プロファイル」パネルに属性を追加する手順, D-8
 - 検索で ANR を使用する手順, D-5
 - 構成データの更新の手順, D-4
 - ファスト・バインドを使用するようにアクセス・システムを構成する手順, D-9
- WebPass
 - Identity Server と WebPass の関連付けの解除, 7-46
 - WebPass の削除, 7-42
 - WebPass の追加, 7-40
 - WebPass の変更, 7-42
 - 構成済の WebPass の表示, 7-40
 - コマンドラインによる WebPass の変更, 7-43
 - コマンドラインによるトランスポート・セキュリティ・モードの再構成, 7-44
 - トランスポート・セキュリティ・モードのパスワードを変更する手順, 7-44
- オブジェクト
 - 「GIF イメージ」表示タイプの構成, 3-28
 - アプリケーション固有の「属性の変更」ページの表示, 3-18
 - オブジェクト・クラス・タイプの変更, 3-7
 - オブジェクト・クラスの追加, 3-9
 - クラス属性の選択, 3-8
 - 構成済のオブジェクト・クラスの表示, 3-6
 - システム・コンソールでの「属性の変更」ページの表示, 3-18
 - 静的フィルタの作成, 3-25
 - 属性の構成, 3-19
 - 導出属性のアプリケーション・タブへの追加, 3-30
 - 導出属性の構成, 3-30

フィルタの作成, 3-24
補助オブジェクト・クラスの削除, 3-10
ユーザーまたはグループの構造化オブジェクト・
クラスの変更, 3-9
リストの定義, 3-21
ルールの定義, 3-21
ローカライズされた属性表示名の作成、表示また
は変更, 3-22
ワイルド・カードを使用した静的検索フィルタの
作成, 3-26
監査、ログおよびレポート
Access Server のファイルベース監査を構成する手
順, 11-18
Crystal Reports のインストール手順, 11-44
Crystal Reports のパッチをインストールする手
順, 11-45
Crystal Reports を Oracle/Crystal リポジトリに接
続する ODBC データ・ソース定義の作成手
順, 11-46
Crystal Reports を監査データベースに接続する手
順, 11-45
Identity Server のファイルベース監査を構成する
手順, 11-17
ID システム・コンソールからログしきい値を変更
する手順, 10-16
ID システムの監査出力形式を変更する手順,
11-37
ODBC データ・ソース定義を作成する手順
(Windows), 11-29
Oracle Access Manager 固有の Crystal リソースを
コピーする手順, 11-45
orMap.ini の編集手順, 11-46
RDBMS プロファイルを作成する手順, 11-32
RDBMS プロファイルを表示可能にする手順
(Linux), 11-34
RDBMS プロファイルを表示可能にする手順
(Windows), 11-34
SNMP エージェントおよびトラップの宛先の構成
手順, 12-13
SNMP 統計の収集を構成する手順, 12-13
SNMP トラップ先をサイレント・モードで削除す
る手順, 12-14
SNMP トラップ先をサイレント・モードで追加す
る手順, 12-14
SNMP マネージャを追加した直後に削除する手
順, 12-14
アクセス・システムの監査出力形式を変更する手
順, 11-42
一般パラメータの直後に SNMP マネージャを追加
する手順, 12-14
各 Access Server の監査を有効化および構成する手
順, 11-41
各 Identity Server の監査を有効化および構成する
手順, 11-36
監査スキーマのアップロードおよび検証手順
(Windows または Linux 上の Oracle
Database), 11-27, 11-28
監査スキーマのアップロード手順 (Windows 上の
SQL Server), 11-24, 11-26
監査スキーマの検証手順 (Windows 上の SQL
Server), 11-25
監査スキーマを監査データベース・ホストにコ
ピーする手順, 11-23

監査する User Manager、Group Manager または
Org. Manager イベントを指定する手順,
11-39
監査データベースの作成手順 (Linux 上の Oracle
Database), 11-22
監査データベースの作成手順 (SQL Server または
Windows), 11-22
監査データベースの作成手順 (Windows 上の
Oracle Database), 11-22
監査のグローバル ID システム・イベントおよび
プロファイル属性を指定する手順, 11-38
監査ポリシーの設定または変更, 4-44
監査ポリシーの表示, 4-43
最初に一般パラメータを構成する手順, 12-14
すべての Identity Server が監査データベースに
データを記録できることを確認する手順
(Linux または Solaris), 11-41
すべての Identity Server が監査データベースに
データを記録できることを確認する手順
(Windows), 11-40
プライマリ RDBMS インスタンスを作成する手順,
11-33
ユーザー・アクセス権限レポートを作成および管
理する手順, 11-43
レポートの構成, 4-45
レポートの削除, 4-48
レポートの書式設定の変更, 4-46
レポートの表示または変更, 4-47
レポートのローカライズ, 4-47
ログハンドラ定義を追加または削除する手順,
10-16
ログハンドラ定義を表示または変更する手順,
10-15
管理者
ID を取得する手順, 2-10
管理者の削除の手順, 2-4
管理の委任の手順, 2-8
自身の ID を回復する手順, 2-11
代替の割当てまたは削除の手順, 2-10
マスター管理者およびマスター ID 管理者を指定
する手順, 2-4
基本
ID システムへのログインの手順, 1-7
アクセス・システムへのログインの手順, 1-8
クエリー・ビルダーの使用, 4-27
検索機能の使用手順, 1-10
サーバー
Access Server の再構成, 7-30
Identity Server パラメータの削除, 7-19
Identity Server パラメータの表示または変更,
7-18
ID システム設定の再実行, 7-29
ID システムの詳細の表示, 7-14
LDAP ディレクトリ・サーバー・プロファイルの
ディレクトリ・サーバー・インスタンスの削
除, 7-33
LDAP ディレクトリ・サーバー・プロファイルの
データベース・インスタンスの追加または変
更, 7-31
LDAP ディレクトリ・サーバー・プロファイルの
表示, 7-27
LDAP ディレクトリ・サーバー・プロファイルの
変更, 7-28

- Policy Manager 設定の再実行, 7-29
- RDBMS プロファイルの追加または変更, 7-37
- RDBMS プロファイルのデータベース・インスタンスの追加または変更, 7-38
- カスタム・スタイルの削除, 7-7
- 言語の管理, 7-14
- 現在構成されているスタイルの表示, 7-3
- サーバー設定の表示または変更, 7-10
- スタイルの追加, 7-5
- スタイルの配布, 7-6
- スタイルの変更, 7-6
- スタイル名の変更, 7-6
- ディレクトリ・サーバー・プロファイルの作成, 7-24
- デフォルト・スタイルの設定, 7-7
- 電子メール宛先のカスタマイズ, 7-12
- メール・サーバーの構成, 7-13
- ユーザーの ID システム・セッション期間の構成, 7-11
- トランスポート・セキュリティ
 - Access Server とディレクトリ・サーバー間のトランスポート・セキュリティを変更する手順, 8-23
 - Identity Server とディレクトリ・サーバー間のトランスポート・セキュリティを変更する手順, 8-22
 - Identity Server のトランスポート・セキュリティ・モードを変更する手順, 8-6
 - ID システムの証明書パスワードを変更する手順, 8-24
 - Policy Manager とディレクトリ・サーバー間のトランスポート・セキュリティを SSL に変更する手順, 8-23
 - アクセス・システムの証明書パスワードを変更する手順, 8-25
 - オープン・セキュリティ・モードに変更する手順, 8-15
 - 簡易セキュリティ・モードに変更する手順, 8-16
 - 証明書セキュリティ・モードに変更する手順, 8-18
 - 証明書モードで署名された証明書をインストールする手順, 8-20
 - トランスポート・セキュリティ・モードのパスワードを変更する手順, 8-26
- パスワード, 7-54
 - アカウント・ロックアウトの URL の設定, 7-65
 - デフォルトのパスワード期限切れ警告のリダイレクト URL の設定, 7-64
 - デフォルト・パスワード・ポリシーの作成, 7-50
 - 認証スキームを変更してパスワード・ポリシーを含める方法, 7-61
 - パスワード変更のリダイレクト URL の入力, 7-62
 - パスワード・ポリシー・ドメインのロスト・パスワード管理の構成, 7-59
 - パスワード・ポリシーのパラメータの変更, 7-53
 - パスワード・ポリシーのリストの表示, 7-49
 - ロスト・パスワード管理属性の構成, 7-58
 - ロスト・パスワード管理の有効化または無効化, 7-59
 - ロスト・パスワード・ポリシーの表示, 7-59
- ワークフロー
 - Group Manager でのワークフローの実行, 5-32
 - oblixppcatalog.lst の変更, 5-40
- User Manager、Group Manager および Organization Manager の事前ロード, 5-50
- 外出中属性と「外出中」セマンティック型の関連付け, 5-43
- 「外出中」フラグの使用, 5-44
- かわりに変更するワークフローとしてのワークフローのコピー, 5-57
- クイックスタート・ツールを使用した自己登録ワークフローの定義, 5-18
- クイックスタート・ツールを使用したワークフローの定義, 5-17
- 言語固有のワークフロー・パネル情報の構成, 5-61
- 言語固有のワークフロー・パネル情報の表示, 5-61
- 現在のワークフロー・パネル設定の表示, 5-59
- この (例の) ワークフローの作成, 5-32
- サブフローとワークフローの関連付け, 5-33
- サブフローの作成, 5-33
- サロゲートの指定, 5-44
- 時間ベース・エスカレーションの有効化, 5-45
- 自己登録ワークフローの作成, 5-65
- 新規ワークフロー定義の開始, 5-20
- 新規ワークフローの基盤としてのワークフローのコピー, 5-57
- 属性の変更ワークフローの起動, 5-51
- チケットのロックまたはロック解除, 5-55
- 動的参加者に対応するワークフロー・ステップの準備, 5-40
- 非アクティブなユーザーの再アクティブ化, 5-53
- ユーザーによる非同期操作の実行の許可, 5-49
- リクエストの削除, 5-55
- ロールの構成, 5-64
- ワークフロー・サマリーの表示およびエクスポート, 5-56
- ワークフロー・ステップで使用する属性の選択, 5-27
- ワークフロー・ステップのための電子メール通知の構成, 5-36
- ワークフロー・ターゲットの定義, 5-23
- ワークフロー・チケットの検索, 5-51
- ワークフロー・チケットの処理, 5-51
- 「ワークフロー定義」アプレットへのアクセス, 5-20
- ワークフロー定義へのロールの追加, 5-64
- ワークフローのアーカイブ, 5-54
- ワークフローのエクスポート, 5-58
- ワークフローの後続のステップの定義, 5-30
- ワークフローの最初のステップの定義, 5-24
- ワークフローの削除, 5-58
- ワークフローの属性プロパティの構成, 5-28
- ワークフローのテスト, 5-31
- ワークフローの変更, 5-57
- ワークフローのモニター, 5-54
- ワークフローの有効化, 5-31
- ワークフロー・パネルの変更, 5-60
- ワークフロー・パラメータ・ファイルの変更, 5-48
- 電子メール
 - ユーザー・フィードバック用のアドレスの設定, 7-12
- テンプレート・オブジェクト
 - ID システムでの表示, 6-6
 - 概要, 3-2

クラス
タブへの追加, 4-8
パネルでの使用, 4-12
変更に関する留意事項, 6-2
ワークフローでの使用, 6-4
テンプレート属性
ワークフロー, 5-7

と

同期化, 7-67
導出属性
「属性, 導出」も参照
匿名アクセス, 4-25
匿名認証スキーム
旧名称 NetPoint None または COREid None, xviii
トラブルシューティング, F-1
Oracle Access Manager での一般的な問題, F-1
トランスポート・セキュリティ
Access Server に対する変更, 8-11
AccessGate に対する変更, 8-11
Identity Server に対する変更, 8-6
PEM ファイル, 8-5
WebPass に対する変更, 8-6
アクセス・システムのオープン・モードへの変更,
8-15
アクセス・システムの簡易モードへの変更, 8-16
アクセス・システムの証明書モードへの変更, 8-18
インストール時の指定, 8-3
概要, 8-2
簡易モードへの変更, 8-8
コンポーネント間での設定, 8-3
証明書モードへの変更, 8-9
パスワード, 8-24

に

認可, xv
Active Directory, A-4
ADSI, C-5
AzMan プラグイン, D-15
認可イベントの監査, 11-15
認可イベントのモニタリング, 12-10
認可プラグインの MIB オブジェクト, 12-11
認可プラグインのモニタリング, 12-9
プラグイン API, xv
認証, xv
Active Directory, A-4
ADSI, B-12, C-5
自己登録では不要, 5-66
スキーム
デフォルト・スキーム, xviii
スキーム, 変更してパスワード・ポリシーを含める方
法, 7-61
トランスポート・セキュリティ, 7-17, 7-41
認証アクションのモニタリング, 12-10
認証イベントの監査, 7-49, 11-15
認証試行のレポート, 9-3
認証プラグインのモニタリング, 12-9, 12-11
非結合検索ベースのスキーム, 7-35
ファスト・バインド, 7-33
プラグイン API, xv

は

「バージョン情報」ページ, 1-12
パスワード, 3-17
「ロスト・パスワード管理」も参照
Access Server セキュリティ, 8-26
Access Server パスワードの変更, 8-26
password.xml, 8-16
Person オブジェクト・クラスに必要なセマンティク
型, 3-13
Sun iPlanet の制限, 5-66
期限切れの通知, 7-13
グローバル・パズフレーズ, 8-8
構成, 7-48
このリリースの新機能, xx
チャレンジ・フレーズ, 削除, 7-57
トランスポート・セキュリティ, 変更, 8-24
トランスポート・セキュリティ・パスワード, 8-24
「パスワード」セマンティック型, 3-12, 3-13, 6-6
パスワード・ポリシー
アカウント・ロックアウト継続時間, 7-52
アカウント・ロックアウトの URL, 7-53
アクセス・システムが保護するリソースへの適用,
7-61
アクセス・システムでの実施, 7-61
大文字または小文字の最小数, 7-51
外部指定の検証ルール, 7-51
カスタム・アカウント・ロックアウトのリダイレ
クト URL, 7-49
管理者リセット後の変更の強制, 7-52
期限切れ警告の URL, 7-53
期限切れ通知, 7-52
許可するログイン試行回数, 7-52
このリリースの新機能, xx
最小期間, 7-52
最小長, 7-51
削除, 7-54
作成, 7-51
失敗した認証イベント, 7-50
数字または非英数字の最小数, 7-51
成功した認証イベント, 7-49
デフォルト, 7-49
デフォルト・ポリシーの構成, 7-50
特定ドメイン, 7-50
ドメインの制限, 7-51
認証スキームに含める方法, 7-61
パスワード期限切れ警告の URL, 7-49
パスワード変更のリダイレクト URL, 7-49
パスワード・リセット・ページ用のスタイルシー
ト, 7-53
パスワード履歴, 7-52
表示, 7-49
変更, 7-53
有効化, 7-53
有効期間, 7-51
ロスト・パスワード通知ページ用のスタイルシー
ト, 7-53
ロスト・パスワードのリダイレクト URL, 7-49
パスワード・ポリシーの評価順序, 7-48
ポリシーの構成, 概要, 7-47
ロスト・パスワード管理
新機能, xx
ロスト・パスワード管理属性, 7-58

ロスト・パスワード管理のためのセマンティック型、
3-15
パスワード・ポリシー
「パスワード」を参照
パスワード・ポリシーの削除、7-54
パネル、4-13
概要、4-11
グループ・タイプ・パネル、4-17
追加、ローカライズ、変更および削除、4-18
削除、4-13
追加、4-13
並べ替え、4-17
パネルでのオブジェクトの使用、4-12
表示、4-13
変更、4-13
パラメータ・ファイル、E-1
概要、E-1

ひ

非結合検索ベース、7-34
表示タイプ
GIF イメージ、3-16
GIF イメージ URL、3-16
S/MIME 証明書、3-17
オブジェクト・セレクトラ、3-17、3-23
住所、3-17
数値文字列、3-17
選択メニュー、3-17
単一行テキスト、3-17
チェック・ボックス、3-16
電子メール、3-16
なし、3-16
パスワード、3-17
日付、3-16
フィルタ・ビルダー、3-16
ブール、3-16
複数行テキスト、3-16
メディア、3-16
ラジオ・ボタン、3-17
ロケーション、3-16

ふ

ファスト・バインド、7-33
フィルタ
「LDAP フィルタ」を参照
使用方法、3-25
静的 LDAP、3-25
ワイルド・カードによる静的検索、3-25
フェイルオーバー、7-36
プラグイン
Active Directory、A-7
ロギング、10-2
フルネーム、3-14
プロセスの概要
IWA 認証の使用法、D-11
ユーザーの作成ワークフローの作成と使用、5-6
ユーザーの作成ワークフローの例、5-15
プロファイル・ページ、4-11

へ

ヘッダー・パネル、4-12
ヘルプ、1-12

ほ

補助オブジェクト・クラス
タブへの追加、4-8
ポリシー・データ
格納用のプロファイル、7-21
ポリシー・ドメイン
デフォルト、xviii

ま

マスター ID 管理者
実行するタスク、2-3
定義、2-2
マスター管理者
旧名称 COREid 管理者、xviii
旧名称 NetPoint 管理者、xviii
実行するタスク、2-2
定義、2-2

め

名称、新、xviii
名称変更、xviii
メンバー・プロファイルの表示、4-10

も

モニタリング
「SNMP」を参照

ゆ

ユーザー
Group Manager のグループ・メンバーシップ、1-2
ID システム・セッション、7-11
LDAP 属性権限、4-31
Person オブジェクト・クラス・タイプ、3-6
User Manager による管理、1-2
一般的に表示されるユーザー情報、3-3
管理、2-1
権限、4-21、4-31
再アクティブ化、5-11
削除、5-10、5-11
作成、5-10
自己登録、1-2、5-18
セッション・タイムアウト、7-11
属性の変更、5-10
追加
置換構文の使用、5-22
動的、xx、3-26、5-22
ログイン・ユーザーと同じ DIT レベル、xx、
3-26、5-22
通知用のメール・サーバー、7-13
認可、xv
認証、xv
表示権限、4-5、4-21、4-31
変更権限、4-21、4-31

- ユーザー・アプリケーション, 4-1
- ユーザーが参照可能なデータの構成, 3-1
- 読取りおよび書き込み権限, 1-2, 4-21, 4-31
- ユーザー・インタフェース, 1-9
 - スタイル
 - 「スタイル」も参照
 - カスタマイズ, 7-2
 - スタイル
 - 表示, 7-3
 - ナビゲーション要素, 1-9
- ユーザー・データ
 - 格納用のプロファイル, 7-21
- ユーザーの再アクティブ化ワークフロー, 5-5
- ユーザーの作成ワークフロー, 5-5
- ユーザーの非アクティブ化ワークフロー, 5-5

よ

- 読取り権限, 4-21

り

- リスト
 - 概要, 3-20
 - 定義, 3-21

る

- ルール
 - 概要, 3-20
 - 使用方法, 3-25
 - 定義, 3-21

れ

- レスポンス属性, 7-58
- レポート, 9-1
 - ID アプリケーションで表示できない属性, 4-44
 - 「SNMP」も参照
 - 「監査」も参照
 - 「ロギング」も参照
- レルム, 7-34

ろ

- ローカライズ, 3-22
 - 概要, 7-7, 7-8
 - 管理ページ, 7-8
 - 言語の評価順序, 7-9
 - 言語の有効化, 7-14
 - 検索結果, 4-7
 - 属性の表示名, 4-21
 - タブ, 4-5
 - パネル, 4-13
 - パネルの表示名, 4-19
 - 複数言語の管理, 7-14
 - レポート, 4-47
- ロギング
 - autosync, 10-10
 - Buffer_Size, 10-12
 - File_Name, 10-12
 - ID システム・コンソールでの構成, 10-15
 - ListName, 10-11

- Log_Level, 10-11
- Log_Status, 10-10, 10-11
- Log_Threshold_Level, 10-10
- Log_Writer, 10-11
- Max_Rotation_Size, 10-12
- Max_Rotation_Time, 10-12
- SNMP, 12-16
- xmlns, 10-11
- 概要, 10-2
- 構成ファイル, 10-3
 - エントリの評価順序, 10-10
 - 構造, 10-8
 - コメント, 10-4
 - 名前, 10-4
 - パラメータ, 10-11
 - 変更, 10-4
 - 要素の順序, 10-9
- 構成ファイルと ID システム・コンソール設定の同期, 10-10
- 構成ファイル内の要素の順序, 10-9
- このリリースの新機能, xx, xxi
- サーバーの再起動が必要な場合, 10-11
- 自動アップデート, xx, xxi
- 出力, 送信先, 10-7
- デフォルトの構成ファイル, 10-5
- レベル, 10-10
- ログ出力先, 10-7
- ログ・データの送信先, 10-7
- ログ・ライター, 10-7
- ログ・レベル, 概要, 10-2
- ログ・レベル, 表, 10-2
- ログアウト, 1-12
 - ID システム, 1-12
- ログイン, 1-6
 - ID システム, 1-7
 - アクセス・システム, 1-8
- ロスト・パスワード管理
 - URL, 構文, 7-56
 - 概要, 7-54
 - 構成, 7-59
 - 構成の概要, 7-55
 - このリリースの新機能, xx
 - チャレンジおよびレスポンス用のセマンティック型, 3-15
 - チャレンジ・フレーズとレスポンス, 7-47
 - チャレンジ・フレーズの削除, 7-57
 - パスワード・リセット・ページへのリダイレクト, 7-62
 - パスワード・リセット・ページ用のスタイルシート, 7-47
 - 複数のチャレンジ・フレーズの表示, 7-56
 - ポリシーの表示, 7-59
 - 有効化, 7-59
 - リダイレクト URL, 7-49
 - ロスト・パスワード管理のためのスタイルシート, 7-50

わ

- ワークフロー
 - DIT の場所へのユーザーの動的割当て, xx
 - アクション
 - オブジェクトの削除, 5-12

- オブジェクトの作成, 5-12
- グループの削除, 5-12
- グループの作成, 5-11
- 属性の変更, 5-10, 5-11, 5-12
- ユーザーの再アクティブ化, 5-11
- ユーザーの削除, 5-10, 5-11
- ユーザーの作成, 5-10
- アクション, 概要, 5-7, 5-8
- エクスポート, 5-58
- エスカレーション, 5-45
- エントリ条件, 5-9
- 開始方法, 5-2
- 外出中属性, 5-43
- 「外出中」フラグ, 5-44
- 外部アクション, 5-63
- 概要, 5-2
- 起動, 5-50
- クイックスタート・ツール, 5-16
- コピー, 5-57
- 削除, 5-58
- 作成されるオブジェクトの DIT の場所の選択, 5-22
- 作成の概要, 5-4
- 作成の例, 5-31
- サブフロー, 5-33
- サブフロー, 概要, 5-3, 5-15
- サブフロー, 承認, 5-34
- サブフロー, ワークフロー・ステップとの関連付け, 5-33
- サマリー・レポート, エクスポート, 5-55
- サマリー・レポート, 表示, 5-55
- サロゲート, 5-44
- サロゲート参加者, 5-3
- サロゲート参加者, 概要, 5-42
- 参加者, 5-9
- 参加者を選択するアプリケーション, 5-41
- 参加者を選択するプラグイン, 5-41
- 時間ベース・エスカレーション, 5-45
- 自己登録, 5-18
 - メール通知, 5-14
- 自己登録, 作成, 5-65
- 事前アクションと事後アクション, 5-62
- 使用方法, 5-50
- ステップ, 5-30
 - コミット, 5-31
 - 属性, 5-26
- ステップ, 概要, 5-7, 5-8
- ステップ・アクション, 5-10
- ステップ・アクション, 概要, 5-8
- ステップ参加者への通知, 5-36
- ステップで実行可能なアクション, 5-13
- 「すべてのユーザー」ロール, 5-64
- 静的参加者, 5-36, 5-38
- ターゲット, 5-9, 5-22
- ターゲットの定義, 5-23
- タイプ, 5-4
 - オブジェクトの削除, 5-5
 - オブジェクトの作成, 5-5
 - グループの削除, 5-5
 - グループの作成, 5-5
 - 自己登録, 5-5
 - 属性の変更, 5-5
 - ユーザーの再アクティブ化, 5-5
 - ユーザーの作成, 5-5
- ユーザーの非アクティブ化, 5-5
- チケット, 概要, 5-5
- チケット, 拡張ルーティング, 5-34
- チケット処理用のメール・サーバー, 7-13
- チケットの検索と処理, 5-51
- チケットのロック, 5-55
- チケット・ルーティング, 5-37
- 通知, 5-9
 - 定義, 5-20
 - 定義の開始, 5-20
 - 定義の例, 5-32
- データのコミット, 5-31
- テスト, 5-31
- テンプレート・オブジェクト, 3-5
- テンプレート・オブジェクトの使用, 6-3
- 動的参加者, 5-3, 5-36, 5-37
 - 割当ての概要, 5-39
- バックエンド・システムへのワークフロー・データの送信, 3-5
- パフォーマンス, 5-62
- 非同期操作, 5-49
- 前処理と後処理, 5-9
- モニタリング, 5-54
- 有効化, 5-31
- ユーザーによるワークフローへのアクセス方法, 5-5
- ユーザーの作成ワークフローの図, 5-4
- ユーザーの非アクティブ化と再アクティブ化, 5-52
- リクエストのアーカイブ, 5-54
- 例, 5-2, 5-15
- ローカライズ, 5-61
- ロールの追加, 5-64
- ロケーション・ワークフローの作成, 5-67
- ワークフロー・アプレットの使用, 5-19
- ワークフロー・タイプ, 5-8
- ワークフロー・パネル設定の表示, 5-59
- ワークフロー・パネルの外観の変更, 5-60