

Oracle® Application Server Single Sign-On

管理者ガイド

10g (9.0.4)

部品番号 : B12372-02

2004 年 6 月

Oracle Application Server Single Sign-On 管理者ガイド, 10g (9.0.4)

部品番号 : B12372-02

原本名 : Oracle Application Server Single Sign-On Administrator's Guide, 10g (9.0.4)

原本部品番号 : B13791-01

原著者 : Henry Abrecht

原協力者 : Gaurav Bhatia, Kamalendu Biswas, Margaret Chou, Lee Cooper, Mike Hwa, Ganesh Kirti, Pei-fung Lam, Jeffrey Levinger, Mark Nelson, Saurabh Shrivastava, Arun Swaminathan, Huiping Wang, Tim Willard

Copyright © 1996, 2004 Oracle Corporation. 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 Corporation, 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 は Oracle Corporation およびその関連会社の登録商標です。その他の名称は、Oracle Corporation または各社が所有する商標または登録商標です。

目次

はじめに	xiii
対象読者	xiv
このマニュアルの構成	xiv
関連ドキュメント	xvi
表記規則	xvii
OracleAS Single Sign-On の新機能	xxiii
OracleAS Single Sign-On の新機能	xxiv
Oracle9iAS Single Sign-On における新機能	xxiv
1 コンポーネントとプロセス：概要	
シングル・サインオン・システムの主要コンポーネント	1-2
Single Sign-On Server	1-2
パートナ・アプリケーション	1-2
外部アプリケーション	1-3
mod_osso	1-3
Oracle Internet Directory	1-4
Oracle Identity Management インフラストラクチャ	1-4
Single Sign-On プロセス	1-4
Single Sign-On Server へのアクセス	1-5
パートナ・アプリケーションへのアクセス	1-5
外部アプリケーションへのアクセス	1-6
OracleAS Portal の外部アプリケーション・ポートレットへのアクセス	1-6
外部アプリケーションに対する初めての認証	1-6
外部アプリケーションに対する 2 回目以降の認証	1-7

外部アプリケーションからのログアウト	1-7
シングル・サインオフ	1-7
パスワードの変更	1-8
グローバル・ユーザーの非アクティビティ・タイムアウト	1-8
ワイヤレス・オプションによるサインオン	1-9

2 基本的な管理

Single Sign-On 管理者ロール	2-2
管理権限の付与	2-2
policy.properties	2-4
Single Sign-On コンポーネントの停止と起動	2-4
Oracle HTTP Server の停止と起動	2-4
OC4J_SECURITY インスタンスの停止と起動	2-5
シングル・サインオン中間層の停止と起動	2-5
すべてのコンポーネントの停止と起動	2-5
OracleAS Single Sign-On 用ブラウザの作業環境の設定	2-6
管理ページへのアクセス	2-6
「SSO Server の編集」ページを使用したサーバーの構成	2-8
グローバリゼーション・サポートの構成	2-8
グローバル・ユーザーの非アクティビティ・タイムアウトの構成	2-9
サンプル・ファイルの取得	2-11

3 ディレクトリ対応 Single Sign-On

Oracle Internet Directory におけるユーザー管理	3-2
パスワード・ポリシー	3-3
パスワード・ルール	3-3
パスワードの有効期限の構成	3-3
パスワードの変更ページの動作	3-4
パスワードが失効している場合	3-4
パスワードが間もなく失効する場合	3-4
猶予期間ログインの実施	3-4
パスワードの変更の強制	3-4
アカウント・ロックアウトの構成	3-4
ユーザーのロック解除	3-5
パスワード・ポリシーの構成	3-5
OracleAS Single Sign-On のディレクトリ・ツリー	3-5

ディレクトリ・アクセス用 Single Sign-On Server の設定変更	3-7
ディレクトリ変更による Single Sign-On Server の更新	3-8

4 パートナ・アプリケーションの設定と管理

パートナ・アプリケーションの登録:登録方法	4-2
mod_osso の登録	4-2
ossoereg.jar の構文とパラメータ	4-3
コマンド例	4-5
Oracle HTTP Server の再起動	4-6
ロード・バランサを使用した複数のパートナ・アプリケーションの配置	4-6
使用例	4-6
構成手順	4-8
パートナ・アプリケーションのインストール	4-8
パートナ・アプリケーション中間層での Oracle HTTP Server の構成	4-8
HTTP ロード・バランサの構成	4-9
パートナ・アプリケーション中間層での mod_osso の再登録	4-10
仮想ホストでの mod_osso の構成	4-11

5 外部アプリケーションの設定と管理

インタフェースを使用した外部アプリケーションの配置と管理	5-2
外部アプリケーションの追加	5-2
外部アプリケーションの編集	5-5
Single Sign-On データベースへの外部アプリケーション証明書の格納	5-5
Basic 認証アプリケーションのプロキシ認証	5-6
Basic 認証のプロキシとしての Oracle HTTP Server の設定	5-6
構成の要件	5-8
構成手順	5-8

6 マルチレベル認証

マルチレベル認証とは	6-2
マルチレベル認証の仕組み	6-2
マルチレベル・システムのコンポーネント	6-3
認証レベル	6-3
認証プラグイン	6-4
マルチレベル認証の構成	6-5

使用例	6-5
構成手順	6-5

7 デジタル証明書を使用したサインオン

証明書を使用した認証の仕組み	7-2
システム要件	7-3
証明書用のシングル・サインオン・システムの構成	7-3
Oracle HTTP Server	7-4
SSL パラメータの構成	7-4
認証局の選択	7-5
Single Sign-On Server	7-5
クライアント証明書のパラメータを受信するためのサーバー構成	7-6
デフォルトの認証プラグインによる policy.properties の構成	7-7
認証プラグインの構成ファイルの変更 (オプション)	7-7
ユーザー名マッピング・モジュールのカスタマイズ (オプション)	7-8
シングル・サインオン中間層の再起動	7-10
Oracle Internet Directory	7-10
証明書失効リストのメンテナンス	7-11

8 Windows ネイティブ認証

Windows ネイティブ認証の概要	8-2
Windows ネイティブ認証の仕組み	8-2
システム要件	8-3
Windows ネイティブ認証の構成	8-4
Microsoft Active Directory が設定済で機能していることの確認	8-4
Oracle Internet Directory と OracleAS Single Sign-On のインストール	8-4
Oracle Internet Directory と Microsoft Active Directory の同期化	8-4
Windows 認証プラグイン用の Oracle Internet Directory の構成	8-4
同期化の確認と認証プラグインが機能していることの確認	8-5
Single Sign-On Server の構成	8-5
Single Sign-On Server の Kerberos サービス・アカウントの設定	8-5
Sun JAAS ログイン・モジュール用の Single Sign-On Server の構成	8-7
保護されたアプリケーションとしての Single Sign-On Server の構成	8-9
エンド・ユーザーのブラウザの構成	8-11
Internet Explorer 5.0 以上	8-11
Internet Explorer 6.0 のみ	8-12

ローカル・アカウントの再構成	8-12
フォールバック認証	8-13
ログインの例	8-14

9 拡張構成

SSL の有効化	9-2
シングル・サインオン中間層での SSL の有効化	9-2
Identity Management インフラストラクチャ・データベースの再構成	9-4
シングル・サインオン URL の変更	9-4
targets.xml の更新	9-5
管理アプリケーションのログアウトの再構成	9-5
シングル・サインオン URL の保護	9-6
Java リンクの URL	9-6
PL/SQL リンクの URL	9-6
Oracle HTTP Server とシングル・サインオン中間層の再起動	9-7
パートナ・アプリケーションの登録	9-7
Single Sign-On Server と Oracle Internet Directory 間の SSL の構成	9-8
配置例	9-9
1 つのシングル・サインオン中間層、1 つの Oracle Internet Directory	9-9
複数のシングル・サインオン中間層、1 つの Oracle Internet Directory	9-10
使用例	9-11
構成手順	9-13
Identity Management インフラストラクチャでの OracleAS Active Failover Clusters の使用	9-17
使用例と構成手順	9-18
複数のシングル・サインオン中間層、レプリケートされた Oracle Internet Directory	9-18
使用例	9-18
構成手順	9-19
地理的に分散している複数のシングル・サインオン・インスタンス	9-22
使用例	9-22
構成手順	9-24
その他の高可用性の配置	9-25
OracleAS Cold Failover Cluster	9-25
障害時リカバリ	9-25
バックアップおよびリカバリ	9-25
識別情報管理データベースのレプリケート	9-26
レプリケーションのメカニズム	9-26

レプリケーション用の識別情報管理データベースの構成	9-28
レプリケーション・グループへのノードの追加	9-29
レプリケーション・グループからのノードの削除	9-29
プロキシ・サーバーを使用する OracleAS Single Sign-On の配置	9-29
IP チェックの無効化	9-30
プロキシ・サーバーの有効化	9-30
ユーザー・ニックネームの変更におけるディレクトリ同期の設定	9-32

10 アプリケーション・サービス・プロバイダに対するサポートの有効化

アプリケーション・サービス・プロバイダ: 複数のレルムの配置に関する決定	10-2
複数のレルムのセットアップと有効化	10-2
Single Sign-On Server による複数のレルムの認証の有効化	10-3
Oracle Internet Directory でのレルムの検索	10-3
パートナ・アプリケーションでのレルムに属するユーザーの検証	10-5
複数のレルムに対する Single Sign-On Server の構成	10-7
複数のレルム用の管理権限の付与	10-10

11 Single Sign-On Server の監視

監視用ページへのアクセス	11-2
スタンドアロン・コンソールのホームページの解説と使用方法	11-2
「失敗ログインの詳細」 ページの表示内容と使用方法	11-4
Single Sign-On の監視ターゲットのポート・プロパティの更新	11-5

12 配置固有ページの作成

Single Sign-On Server での配置固有ページの使用方法	12-2
配置固有ページの記述方法	12-3
ログイン・ページのパラメータ	12-3
パスワードを忘れた場合	12-5
パスワードの変更ページのパラメータ	12-5
シングル・サインオフ・ページのパラメータ	12-7
ページのエラー・コード	12-7
ログイン・ページのエラー・コード	12-7
パスワードの変更ページのエラー・コード	12-8
グローバリゼーション・サポートの追加	12-9
表示されるページの言語の決定	12-9

Accept-Language ヘッダーを使用してページを決定する方法	12-9
ページのロジックを使用して言語を決定する方法	12-9
ページのレンダリング	12-10
配置固有ページに関するガイドライン	12-10
配置固有ページのインストール	12-11
policy.properties ファイルを使用したログイン・ページとパスワードの変更ページの インストール	12-11
policy.properties ファイルを使用したワイヤレスのログイン・ページとパスワードの変更ページの インストール	12-11
WSSO_LS_CONFIGURATION\$ を使用したシングル・サインオフ・ページのインストール	12-12
配置固有ページの例	12-12

13 サードパーティのアクセス管理システムとの統合

サードパーティのアクセス管理の仕組み	13-2
使用例 1: ユーザーが、サードパーティのサーバーに認証されていない場合	13-3
使用例 2: ユーザーが、サードパーティのサーバーに認証されている場合	13-3
サードパーティ・リポジトリと Oracle Internet Directory の同期化	13-4
サードパーティ統合モジュール	13-4
ベンダーから提供されたパッケージを使用する場合	13-4
独自のパッケージを構築する場合	13-4
インタフェースの使用に関するガイドライン	13-5
インタフェース	13-5
構成手順	13-6
統合事例: SSOAcme	13-8
サンプル統合パッケージ	13-8
統合システムからのログアウト	13-10
リリース 9.0.2 のサンプル実装からリリース 9.0.4 への移行	13-11
新しい認証インタフェース	13-11
HTTP ヘッダーからのユーザー名の取得	13-12
ユーザー名が存在しない場合のエラー処理	13-12
Single Sign-On Server に戻すユーザー名	13-13

14 データのエクスポートとインポート

エクスポートされるデータとインポートされるデータ	14-2
エクスポートとインポートのスクリプト: 構文とパラメータ	14-2
スクリプト構文	14-2

スクリプト・パラメータ	14-3
サーバー間でのデータのエクスポート	14-4
エクスポートとインポートの使用例およびスクリプトの例	14-4
エクスポートの使用例	14-5
インポートの使用例	14-5
スクリプトの実行	14-6
エクスポートとインポートの成功の確認	14-6
複数のサーバーの統合	14-7
エラー・メッセージ	14-8

A トラブルシューティング

ログ・ファイル	A-2
エラー・メッセージとその他の問題	A-3
基本的なエラー・メッセージと問題	A-3
Windows ネイティブ認証	A-8
証明書による認証	A-10
証明書によるサインオンのデバッグ	A-10
エラー・メッセージ	A-10
パスワード・ポリシー	A-11
デバッグ・レベルの引上げ	A-12
Single Sign-On データベースでのデバッグ・オプションの有効化	A-13
UI 操作に関する LDAP トレースの有効化	A-14
シングル・サインオン監査レコードの管理	A-15
LDAP 接続キャッシュのリフレッシュ	A-16
Oracle Internet Directory 変更後の OC4J の再起動	A-16
レプリケーションのトラブルシューティング	A-17
Advanced Replication 構成の検証	A-17
Advanced Replication 構成の検証と修正	A-17

B Single Sign-On スキーマのパスワードの取得

C policy.properties

用語集

索引

図リスト

1-1	mod_osso によるシングル・サインオン	1-5
2-1	Oracle Directory Manager の「iASAdmins」タブ	2-3
2-2	「SSO Server 管理」ページ	2-7
3-1	OracleAS Single Sign-On のディレクトリ情報ツリー	3-6
4-1	複数のパートナ・アプリケーションで使用するロード・バランサ	4-7
5-1	「外部アプリケーション・ログイン」ページ	5-5
5-2	mod_osso/mod_proxy を使用した認証の流れ	5-7
6-1	マルチレベル認証の流れ	6-2
7-1	証明書を使用したシングル・サインオン	7-2
8-1	Windows ネイティブ認証の流れ	8-3
9-1	デフォルトの Single Sign-On インストール: 1 台のコンピュータ	9-10
9-2	Single Sign-On インストール: 2 台のコンピュータ	9-10
9-3	2 つのシングル・サインオン中間層、1 つの Oracle Internet Directory	9-12
9-4	OracleAS Active Failover Clusters を使用したシングル・サインオン	9-18
9-5	レプリケート・ディレクトリを含む複数のシングル・サインオン中間層	9-21
9-6	地理的に分散している高可用性シングル・サインオン・システム	9-23
9-7	マルチマスター・レプリケーションのアーキテクチャ	9-27
10-1	全体図: 複数のレルムでのシングル・サインオン	10-4
10-2	同じ名前を持つユーザーの mod_osso ヘッダー	10-6
11-1	OracleAS Single Sign-On の監視用ホームページ	11-3
11-2	「失敗ログインの詳細」ページ	11-4
13-1	サードパーティのサーバーを使用した Oracle パートナ・アプリケーションへのアクセス	13-2

表リスト

2-1	SSO セッション・ポリシー	2-8
5-1	外部アプリケーション・ログイン	5-2
5-2	認証方式	5-3
5-3	追加フィールド	5-3
6-1	デフォルトの認証レベル	6-3
7-1	証明書を使用したシングル・サインオンの構成時に使用する HTTP パラメータ	7-4
8-1	Internet Explorer での Single Sign-On ログインのオプション	8-14
9-1	ssoReplSetup のパラメータ	9-28
10-1	enblhstg.csh と addsub.csh のパラメータ	10-8
12-1	Single Sign-On Server によってページに送信されるログイン・ページのパラメータ	12-3
12-2	ページから Single Sign-On Server に送信されるログイン・ページのパラメータ	12-4
12-3	パスワードの変更ページに送信されるパラメータ	12-5
12-4	ページで送信されるパスワードの変更ページのパラメータ	12-6
12-5	シングル・サインオフ・ページに送信されるパラメータ	12-7
12-6	ログイン・ページのエラー・コード	12-7
12-7	パスワードの変更ページのエラー・コード	12-8
14-1	ssomig に渡すパラメータ	14-3
14-2	エクスポートおよびインポートに関するエラー・コード	14-8
A-1	Replication Environment Management Tool のパラメータ	A-17

はじめに

『Oracle Application Server Single Sign-On 管理者ガイド』では、Oracle Application Server (OracleAS) のユーザー認証を管理するための概要と手順について説明します。このマニュアルは、UNIX および Windows NT/2000 プラットフォームを対象にしています。

注意： このマニュアルでは、シングル・サインオン・ファイルを参照する際に UNIX 表記を使用しています。ssocfg スクリプト以外のファイルの名前および場所は、UNIX と Windows で共通しています。Windows 版のシングル・サインオン・ファイルにアクセスするには、次のディレクトリに移動します。

```
%ORACLE_HOME%\directory_path
```

「はじめに」の項目は次のとおりです。

- [対象読者](#)
- [このマニュアルの構成](#)
- [関連ドキュメント](#)
- [表記規則](#)

対象読者

『Oracle Application Server Single Sign-On 管理者ガイド』は、次のユーザーを対象にしています。

- OracleAS の認証の構成および管理を担当する管理者。
- OracleAS Single Sign-On を使用した機能の開発者。特にそれらを mod_osso (Oracle HTTP Server 上の認証モジュール) と統合する開発者。
- OracleAS Single Sign-On を使用して Web アプリケーションへのアクセスを保護する方法に関心のあるユーザー。

このマニュアルの読者は、OracleAS の基礎知識があり、リリース 9.0.4 をインストールしている、またはインストールできることを前提にしています。

このマニュアルの構成

このマニュアルは、次の章および付録から構成されています。

第1章「コンポーネントとプロセス：概要」

OracleAS Single Sign-On の顕著な機能について概説します。この章は、クイック・リファレンスとして利用できます。

第2章「基本的な管理」

Single Sign-On Server の停止と起動、Single Sign-On へのアプリケーションの対応付け、管理権限の割当てなど、基本的な管理タスクについて説明します。

第3章「ディレクトリ対応 Single Sign-On」

Oracle Internet Directory が Single Sign-On で果たす役割について説明します。このディレクトリは、OracleAS ユーザーのネイティブ・リポジトリです。これ自体が、ユーザー管理において主要な役割を果たします。

第4章「パートナ・アプリケーションの設定と管理」

パートナ・アプリケーションを Single Sign-On Server に登録する方法について説明します。ロード・バランサを使用して複数のパートナ・アプリケーションを配置する方法についても説明します。

第5章「外部アプリケーションの設定と管理」

Single Sign-On UI を使用して、外部アプリケーションの追加と削除を行う方法について説明します。Oracle HTTP Server を使用して、これらのアプリケーションをプロキシ認証用に構成する方法についても説明します。

第 6 章「マルチレベル認証」

特定のアプリケーションに認証レベルやアダプタを割り当てる方法について説明します。これにより、アプリケーションのセキュリティ・ニーズに認証の動作を合わせることができます。

第 7 章「デジタル証明書を使用したサインオン」

OracleAS Single Sign-On での、SSL を介した X.509 証明書の使用を構成する方法について説明します。

第 8 章「Windows ネイティブ認証」

OracleAS Single Sign-On で、Windows 2000 ワークステーションへの自動サインオンを構成する方法について説明します。そのためには、SPNEGO プロトコルを使用して Kerberos 資格証明を受け入れるように Single Sign-On Server を構成する必要があります。

第 9 章「拡張構成」

OracleAS Single Sign-On をデフォルト以外で構成する方法について説明します。Single Sign-On Server の可用性が向上する、配置方法を示します。そのほかにも、SSL を使用したシングル・サインオン、およびプロキシ・サーバーを使用したシングル・サインオンの方法などが扱われます。

第 10 章「アプリケーション・サービス・プロバイダに対するサポートの有効化」

OracleAS Identity Management インフラストラクチャの 1 つのインスタンス内に、複数の識別情報管理レルムを配置する方法について説明します。サーバーからの複数レルムへのログインを可能にする方法も示します。

第 11 章「Single Sign-On Server の監視」

オラクル社のシステム管理コンソールである Oracle Enterprise Manager を使用して、サーバー・ロードおよびユーザー動作を監視する方法について説明します。

第 12 章「配置固有ページの作成」

シングル・サインオン・ページの起動方法について説明します。また、企業のニーズに合わせてこれらのページをカスタマイズする方法についても説明します。

第 13 章「サードパーティのアクセス管理システムとの統合」

OracleAS Single Sign-On をサードパーティのシングル・サインオン・システムと統合する方法について説明します。サードパーティ・システムは、この統合によって OracleAS 補完製品へのアクセスが得られます。また、架空の統合事例が紹介されています。

第 14 章「データのエクスポートとインポート」

複数の Single Sign-On Server 間でデータを移動する方法について説明します。データ移動が必要な条件が、様々な使用例によって示されます。

付録 A 「トラブルシューティング」

エラー・メッセージとその他の問題に対処するためのヒントがあります。エラー・メッセージと問題は、機能ごとにグループ分けされています。また、シングル・サインオン・ログ・ファイルの一覧と説明があります。

付録 B 「Single Sign-On スキーマのパスワードの取得」

Single Sign-On スキーマのパスワードを返す LDAP コマンドを示します。このパスワードは、シングル・サインオン・スクリプトの実行に必須です。

付録 C 「policy.properties」

policy.properties ファイル全体を記載しています。このファイルは、基本パラメータを含む多用途の構成ファイルです。マルチレベル認証の構成にも使用されます。

用語集

このマニュアルの用語を定義しています。

関連ドキュメント

詳細は、次の Oracle ドキュメントを参照してください。

- 『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』
- 『Oracle Internet Directory 管理者ガイド』

リリース・ノート、インストール関連ドキュメント、ホワイト・ペーパーまたはその他の関連ドキュメントは、OTN-J (Oracle Technology Network Japan) から、無償でダウンロードできます。OTN-J を使用するには、オンラインでの登録が必要です。登録は、次の Web サイトから無償で行えます。

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

すでに OTN-J のユーザー名およびパスワードを取得している場合は、次の URL で OTN-J Web サイトのドキュメントのセクションに直接接続できます。

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

OracleAS Single Sign-On の開発に関する最新情報は、次の Web サイトから参照できます。

<http://otn.oracle.co.jp/products/ias/index.html>

表記規則

この項では、このマニュアルの本文およびコード例で使用される表記規則について説明します。この項の内容は次のとおりです。

- 本文の表記規則
- コード例の表記規則
- Microsoft Windows オペレーティング・システム環境での表記規則

本文の表記規則

本文では、特定の項目が一目でわかるように、次の表記規則を使用します。次の表に、その規則と使用例を示します。

規則	意味	例
太字	太字は、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。	この句を指定すると、 索引構成表 が作成されます。
固定幅フォントの大文字	固定幅フォントの大文字は、システム指定の要素を示します。このような要素には、パラメータ、権限、データ型、 Recovery Manager キーワード、SQL キーワード、SQL*Plus またはユーティリティ・コマンド、パッケージおよびメソッドがあります。また、システム指定の列名、データベース・オブジェクト、データベース構造、ユーザー名およびロールも含まれます。	NUMBER 列に対してのみ、この句を指定できます。 BACKUP コマンドを使用して、データベースのバックアップを作成できます。 USER_TABLES データ・ディクショナリ・ビュー内の TABLE_NAME 列を問い合わせます。 DBMS_STATS.GENERATE_STATS プロシージャを使用します。
固定幅フォントの小文字	固定幅フォントの小文字は、実行可能ファイル、ファイル名、ディレクトリ名およびユーザーが指定する要素のサンプルを示します。このような要素には、コンピュータ名およびデータベース名、ネット・サービス名および接続識別子があります。また、ユーザーが指定するデータベース・オブジェクトとデータベース構造、列名、パッケージとクラス、ユーザー名とロール、プログラム・ユニットおよびパラメータ値も含まれます。	sqlplus と入力して、SQL*Plus をオープンします。 パスワードは、orapwd ファイルで指定します。 /disk1/oracle/dbs ディレクトリ内のデータ・ファイルおよび制御ファイルのバックアップを作成します。 hr.departments 表には、department_id、department_name および location_id 列があります。 QUERY_REWRITE_ENABLED 初期化パラメータを true に設定します。 oe ユーザーとして接続します。

規則	意味	例
	注意: プログラム要素には、大文字と小文字を組み合わせて使用するものもあります。これらの要素は、記載されているとおりに入力してください。	JRepUtil クラスが次のメソッドを実装します。
固定幅フォントの小文字のイタリック	固定幅フォントの小文字のイタリックは、プレースホルダまたは変数を示します。	<code>parallel_clause</code> を指定できます。 <code>Uold_release.SQL</code> を実行します。ここで、 <code>old_release</code> とはアップグレード前にインストールしたりリリースを示します。

コード例の表記規則

コード例は、SQL、PL/SQL、SQL*Plus または他のコマンドライン文の例です。次のように固定幅フォントで表示され、通常のテキストと区別されます。

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

次の表に、コード例で使用される表記規則とその使用例を示します。

規則	意味	例
[]	大カッコは、カッコ内の項目を任意に選択することを表します。大カッコは、入力しないでください。	DECIMAL (<i>digits</i> [, <i>precision</i>])
{ }	中カッコは、カッコ内の項目のうち、1つが必須であることを表します。中カッコは、入力しないでください。	{ENABLE DISABLE}
	縦線は、大カッコまたは中カッコ内の複数の選択項目の区切りに使用します。項目のうち1つを入力します。縦線は、入力しないでください。	{ENABLE DISABLE} [COMPRESS NOCOMPRESS]
...	水平の省略記号は、次のいずれかを示します。 例に直接関連しないコードの一部が省略されている。 コードの一部を繰り返すことができる。	CREATE TABLE ... AS <i>subquery</i> ; SELECT <i>col1</i> , <i>col2</i> , ... , <i>coln</i> FROM employees;

規則	意味	例
.	垂直の省略記号は、例に直接関連しない複数の行が省略されていることを示します。	<pre>SQL> SELECT NAME FROM V\$DATAFILE; NAME ----- /fsl/dbs/tbs_01.dbf /fsl/dbs/tbs_02.dbf . . . /fsl/dbs/tbs_09.dbf 9 rows selected.</pre>
その他の記号	大カッコ、中カッコ、縦線および省略記号以外の記号は、記載されているとおりに入力する必要があります。	<pre>acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;</pre>
イタリック体	イタリック体は、特定の値を指定する必要があるプレースホルダや変数を示します。	<pre>CONNECT SYSTEM/system_password DB_NAME = database_name</pre>
大文字	大文字は、システム指定の要素を示します。これらの要素は、ユーザー定義の要素と区別するために大文字で示されます。大カッコ内にかぎり、表示されているとおりの順序および綴りで入力します。ただし、大/小文字が区別されないため、小文字でも入力できます。	<pre>SELECT last_name, employee_id FROM employees; SELECT * FROM USER_TABLES; DROP TABLE hr.employees;</pre>
小文字	小文字は、ユーザー指定のプログラム要素を示します。たとえば、表名、列名またはファイル名などです。 注意: プログラム要素には、大文字と小文字を組み合わせて使用するものもあります。これらの要素は、記載されているとおりに入力してください。	<pre>SELECT last_name, employee_id FROM employees; sqlplus hr/hr CREATE USER mjones IDENTIFIED BY ty3MU9;</pre>

Microsoft Windows オペレーティング・システム環境での表記規則

次の表に、Microsoft Windows オペレーティング・システム環境での表記規則とその使用例を示します。

規則	意味	例
ファイル名およびディレクトリ名	ファイル名およびディレクトリ名は大 / 小文字が区別されません。特殊文字の左山カッコ (<)、右山カッコ (>)、コロンの (:)、二重引用符 (")、スラッシュ (/)、縦線 () およびハイフン (-) は使用できません。円記号 (¥) は、引用符で囲まれている場合でも、要素のセパレータとして処理されます。Windows では、ファイル名が ¥¥ で始まる場合、汎用命名規則が使用されていると解釈されます。	<pre>c:¥winnt"¥"system32 は C:¥WINNT¥SYSTEM32 と同じです。</pre>
Windows コマンド・プロンプト	Windows コマンド・プロンプトには、カレント・ディレクトリが表示されます。このマニュアルでは、コマンド・プロンプトと呼びます。コマンド・プロンプトのエスケープ文字はカレット (^) です。	<pre>C:¥oracle¥oradata></pre>
特殊文字	Windows コマンド・プロンプトで二重引用符 (") のエスケープ文字として円記号 (¥) が必要な場合があります。丸カッコおよび一重引用符 (') にはエスケープ文字は必要ありません。エスケープ文字および特殊文字の詳細は、Windows オペレーティング・システムのドキュメントを参照してください。	<pre>C:¥>exp scott/tiger TABLES=emp QUERY=¥"WHERE job='SALESMAN' and sal<1600¥" C:¥>imp SYSTEM/password FROMUSER=scott TABLES=(emp, dept)</pre>
HOME_NAME	Oracle ホームの名前を表します。ホーム名には、英数字で 16 文字まで使用できます。ホーム名に使用可能な特殊文字は、アンダースコアのみです。	<pre>C:¥> net start OracleHOME_NAME_TNSListener</pre>

規則	意味	例
<p><code>ORACLE_HOME</code> および <code>ORACLE_BASE</code></p>	<p>Oracle8i より前のリリースでは、Oracle コンポーネントをインストールすると、すべてのサブディレクトリが最上位の <code>ORACLE_HOME</code> の直下に置かれました。<code>ORACLE_HOME</code> ディレクトリの名前は、デフォルトでは次のいずれかです。</p> <p><code>C:\orant</code> (Windows NT の場合)</p> <p><code>C:\orawin98</code> (Windows 98 の場合)</p> <p>このリリースは、Optimal Flexible Architecture (OFA) のガイドラインに準拠しています。<code>ORACLE_HOME</code> ディレクトリ下に配置されないサブディレクトリもあります。最上位のディレクトリは <code>ORACLE_BASE</code> と呼ばれ、デフォルトでは <code>C:\oracle</code> です。他の Oracle ソフトウェアがインストールされていないコンピュータに最新リリースの Oracle をインストールした場合、Oracle ホーム・ディレクトリは、デフォルトで <code>C:\oracle\ora90</code> に設定されます。Oracle ホーム・ディレクトリは、<code>ORACLE_BASE</code> の直下に配置されます。</p> <p>このマニュアルに示すディレクトリ・パスの例は、すべて OFA の表記規則に準拠しています。</p>	<p><code>%ORACLE_HOME%\rdbms\admin</code> ディレクトリへ移動します。</p>

OracleAS Single Sign-On の新機能

このマニュアルでは、Oracle Application Server Single Sign-On リリース 9.0.4 の新機能について説明します。また、リリース 9.0.4 へ移行するユーザーのために、リリース 9.0.2 から追加された新機能についても説明します。

OracleAS Single Sign-On の新機能

リリース 9.0.4 では、Single Sign-On Server へのアクセスがさらに容易になりました。新機能は次のとおりです。

- マルチレベル認証
認証レベルは、アプリケーションごとに異なるレベルを割り当てられるようになりました。これにより、アプリケーションのセキュリティのニーズに認証の動作を合せることができます。詳細は、第 6 章「[マルチレベル認証](#)」を参照してください。
- Windows ネイティブ認証
Windows ワークステーションには、Kerberos チケットを使用して自動的にサインオンできるようになりました。詳細は、第 8 章「[Windows ネイティブ認証](#)」を参照してください。
- 柔軟な配置オプション
Single Sign-On Server は、複数台配置することによって可用性を向上できます。詳細は、第 9 章「[拡張構成](#)」を参照してください。

Oracle9iAS Single Sign-On における新機能

リリース 9.0.2 では、新しい認証オプションが追加され、アプリケーションに Single Sign-On Server を統合することが容易になっています。また、サーバーのパフォーマンスを監視できるようになっています。このリリースで追加された機能は次のとおりです。

- パートナ・アプリケーションの実装に使用する mod_osso モジュール
Oracle HTTP Server のこのモジュールは、Single Sign-On SDK のかわりに簡単に利用できます。詳細は、『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』の第 2 章「[mod_osso を使用したアプリケーションの開発](#)」を参照してください。
- 証明書対応のサインオン
ユーザーの認証には、ユーザー名とパスワードのかわりに X.509 証明書を使用できます。詳細は、第 7 章「[デジタル証明書を使用したサインオン](#)」を参照してください。
- パートナ・アプリケーションからのシングル・サインオフ
ユーザーは、シングル・サインオン・セッションを終了することで、すべてのアクティブなパートナ・アプリケーションから同時にログアウトできます。詳細は、第 1 章の「[シングル・サインオフ](#)」の項を参照してください。
- ワイヤレス・デバイスによるシングル・サインオン
ユーザーは、PDA や携帯電話などのモバイル・デバイスまたはワイヤレス・デバイスを使用して OracleAS にサインオンできます。詳細は、第 1 章の「[ワイヤレス・オプションによるサインオン](#)」の項を参照してください。

- Oracle Enterprise Manager による Single Sign-On の監視

管理者は、Oracle Enterprise Manager Console を使用して、サーバーの負荷やユーザーの動作を監視できます。詳細は、[第 11 章「Single Sign-On Server の監視」](#)を参照してください。

コンポーネントとプロセス：概要

OracleAS Single Sign-On によって、ユーザーは、一組のユーザー名とパスワードおよびレلم ID (オプション) を使用して、他の Web アプリケーションだけでなく、OracleAS のすべての機能にログインできるようになります。

OracleAS Single Sign-On には、次の利点があります。

- 管理コストの削減
Single Sign-On Server によって、複数のアカウントおよびパスワードをサポートする必要がなくなります。
- ログインの簡素化
ユーザーは、アクセスするアプリケーションごとに異なるユーザー名とパスワードを使用する必要がなくなります。
- セキュリティの向上
パスワードの入力が一度だけなので、ユーザーは、パスワードを簡単に覚えやすいものにしたたり、書き留めておく必要がなくなります。

この章の項目は次のとおりです。

- [シングル・サインオン・システムの主要コンポーネント](#)
- [Single Sign-On プロセス](#)

シングル・サインオン・システムの主要コンポーネント

OracleAS Single Sign-On が対話するコンポーネントは次のとおりです。

- [Single Sign-On Server](#)
- [パートナ・アプリケーション](#)
- [外部アプリケーション](#)
- [mod_osso](#)
- [Oracle Internet Directory](#)
- [Oracle Identity Management](#) インフラストラクチャ

Single Sign-On Server

Single Sign-On Server は、OracleAS データベース、Oracle HTTP Server および OC4J サーバーのプログラム・ロジックで構成されています。これにより、ユーザーは経費報告、電子メール、福利厚生情報などのアプリケーションに安全にログインできます。これらのアプリケーションには、パートナ・アプリケーションと外部アプリケーションの2つのフォームがあります。いずれの場合も、一度の認証で複数のアプリケーションにアクセスできます。

パートナ・アプリケーション

OracleAS アプリケーションでは、認証機能が Single Sign-On Server に委譲されます。このことから、パートナ・アプリケーションと呼ばれます。mod_osso と呼ばれる認証モジュールまたは Single Sign-On SDK により、パートナ・アプリケーションは、ユーザーが一度 Single Sign-On Server にログインしていれば、ユーザー名とパスワードのかわりに認証済のユーザー情報を受け取ることができます。

パートナ・アプリケーションは、OracleAS Single Sign-On で認証されたユーザーにパートナ・アプリケーションの各権限を付与するかどうかを決定します。

パートナ・アプリケーションには、OracleAS Portal や OracleAS Discoverer などがあり、Single Sign-On Server 自体も含まれます。

外部アプリケーション

外部アプリケーションでは、認証は Single Sign-On Server に委譲されません。そのかわり、HTML ログイン・フォームが表示され、アプリケーションのユーザー名とパスワードが要求されます。外部アプリケーションでは、それぞれに一意のユーザー名とパスワードが要求される場合があります。HTML ログイン・フォームを使用する外部アプリケーションには、Yahoo! Mail などがあります。

Single Sign-On Server は、ユーザーが一度 Single Sign-On Server にログインすれば、ユーザーにかわってユーザー名とパスワードを外部アプリケーションに提供するように構成できます。また、アプリケーション用の資格証明を Single Sign-On データベースに格納するように選択することもできます。サーバーでは、Single Sign-On ユーザー名を使用して、アプリケーション名とパスワードを検索および取得し、ユーザー・ログインを実行します。資格証明を保存するには、最初のログイン時に、「このアプリケーションのログイン情報を保存する」チェック・ボックスを選択します。

mod_osso

mod_osso は、OracleAS アプリケーションに認証を提供する Oracle HTTP Server モジュールです。これは、OracleAS Single Sign-On の以前のリリースでパートナ・アプリケーションを統合するために使用されていた Single Sign-On SDK にかわるものです。mod_osso は、アプリケーション・サーバーに配置すると、Single Sign-On Server の唯一のパートナ・アプリケーションとして機能して認証プロセスを単純化します。このようにして、mod_osso は、透過的な OracleAS アプリケーションの認証を実現します。結果として、OracleAS アプリケーションの管理者は、SDK との統合作業から解放されます。

注意： Single Sign-On SDK は旧式のツールです。リリース 9.0.2 の SDK を使用してアプリケーションを構築している場合は、mod_osso に変更することをお勧めします。ただし、9.0.2 アプリケーションは 9.0.4 で引き続き機能します。

SDK の詳細は、『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』を参照してください。

ユーザーの認証後、アプリケーションでユーザーを検証するために必要な単純なヘッダー値が mod_osso によって送信されます。ヘッダー値には次のものが含まれます。

- ユーザー名
- ユーザー DN
- ユーザー GUID
- 言語および地域

Single Sign-On Server から URLC トークンの mod_osso に渡される属性の詳細は、『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』の表 D-1 を参照してください。mod_osso を使用してアプリケーションを開発する方法は、前述のマニュアルの第 2 章を参照してください。

Oracle Internet Directory

Oracle Internet Directory は、すべての Single Sign-On ユーザー、すなわち管理者や非管理者のアカウントとパスワード用のリポジトリです。Single Sign-On Server は、このディレクトリ内のユーザー・エントリに基づいてユーザーを認証します。同時に、アプリケーションでのユーザー検証が可能となるユーザー属性をこのディレクトリから取得します。

Oracle Identity Management インフラストラクチャ

OracleAS Single Sign-On は、統合されたインフラストラクチャのリンクの 1 つで、このインフラストラクチャには Oracle Internet Directory、Oracle Directory Integration and Provisioning、Oracle Delegated Administration Services および OracleAS Certificate Authority も組み込まれています。Oracle Identity Management インフラストラクチャと呼ばれるこれらのコンポーネントは、連携して、ユーザーのセキュリティ・ライフ・サイクルとその他のネットワーク・エンティティを効率的かつ経済的に管理します。

Oracle Identity Management の利点については、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。

Single Sign-On プロセス

この項では、次のプロセスについて説明します。

- [Single Sign-On Server](#) へのアクセス
- [外部アプリケーションへのアクセス](#)
- [シングル・サインオフ](#)
- [パスワードの変更](#)
- [グローバル・ユーザーの非アクティビティ・タイムアウト](#)
- [ワイヤレス・オプションによるサインオン](#)

Single Sign-On Server へのアクセス

管理者以外のユーザーは、最初に OracleAS Portal や OracleAS Discoverer などのパートナ・アプリケーションの URL を入力して、Single Sign-On Server にアクセスする必要があります。URL を入力すると、Single Sign-On ログイン画面が表示されます。正しいユーザー名とパスワードを一度入力すると、再度資格証明書を入力せずに、他のパートナ・アプリケーションや外部アプリケーションにアクセスできます。

管理ユーザーは、次のフォームの URL を入力すると、シングル・サインオンの管理ホームページにアクセスできます。

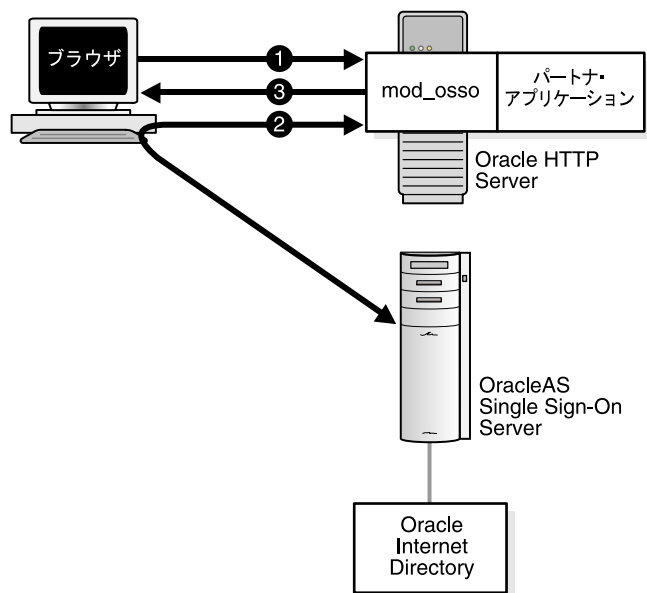
`http://host:port/pls/single_sign-on_DAD`

host は Single Sign-On Server が配置されているコンピュータの名前を示し、*port* はサーバーのポート番号を示します。*single_sign-on_DAD* は、Single Sign-On スキーマ用のデータベース・アクセス記述子 (DAD) を示します。デフォルトの DAD は、*orasso* です。

パートナ・アプリケーションへのアクセス

図 1-1 は、ユーザーが *mod_osso* によって保護されているパートナ・アプリケーションの URL を要求した場合のプロセスを示しています。

図 1-1 *mod_osso* によるシングル・サインオン



1. ユーザーは、パートナ・アプリケーションにアクセスします。
2. ユーザーが、Single Sign-On Server へリダイレクトされます。サーバーで、ユーザーの資格証明がチェックされます。Oracle Internet Directory の資格証明の検証が完了すると、サーバーは資格証明をパートナ・アプリケーションに渡します。
3. パートナ・アプリケーションは要求されたコンテンツを提供します。

外部アプリケーションへのアクセス

外部アプリケーションは、Single Sign-On パートナ・アプリケーションの OracleAS Portal を通じて利用できます。

この項の項目は次のとおりです。

- [OracleAS Portal の外部アプリケーション・ポートレットへのアクセス](#)
- [外部アプリケーションに対する初めての認証](#)
- [外部アプリケーションに対する2回目以降の認証](#)
- [外部アプリケーションからのログアウト](#)

OracleAS Portal の外部アプリケーション・ポートレットへのアクセス

外部アプリケーションにアクセスするには、OracleAS Portal ホームページで「外部アプリケーション」ポートレットを選択し、表示される外部アプリケーションのリストからアプリケーションを選択します。

外部アプリケーションに対する初めての認証

「外部アプリケーション」ポートレットからアプリケーションを選択すると、外部アプリケーションのログイン・プロシージャが開始されます。アプリケーションに初めてアクセスした場合は、次の手順が実行されます。

1. 外部アプリケーションのログイン・プロシージャは、シングル・サインオンのパスワード・ストアで資格証明をチェックします。資格証明が見つからない場合、Single Sign-On Server は資格証明の入力を求めるプロンプトを表示します。
2. ユーザー名とパスワードを入力します。アプリケーションのログイン画面で「このアプリケーションのログイン情報を保存する」チェック・ボックスを選択すると、これらの資格証明をパスワード・ストアに保存できます。
3. 資格証明をパスワード・ストアに保存する場合、Single Sign-On Server はこの資格証明を使用してログイン・フォームを作成し、アプリケーションのログイン処理ルーチンに送信します。このルーチンは、管理者によってあらかじめ構成されており、要求されたアプリケーションに関連付けられています。
4. Single Sign-On Server は、クライアント・ブラウザに対して、フォームと、そのフォームを外部アプリケーションにただちに送信する命令を送信します。

5. クライアントは、外部アプリケーションにフォームを送信してログインします。

資格証明をパスワード・ストアに保存しない場合は、ログインするたびにユーザー名とパスワードを入力する必要があります。

外部アプリケーションに対する 2 回目以降の認証

外部アプリケーションに初めてアクセスしたときに資格証明を保存した場合、Single Sign-On Server では以降のログイン時にその資格証明が使用されます。プロセスは次のとおりです。

1. ユーザーが、OracleAS Portal の「外部アプリケーション」ポートレットからリンクの 1 つをクリックします。
2. 外部アプリケーションのログイン・プロシージャは、パスワード・ストアで資格証明をチェックします。
3. Single Sign-On Server は資格証明を見つけます。この資格証明を使用してログイン・フォームを作成し、アプリケーションのログイン処理ルーチンに送信します。このルーチンは、管理者によってあらかじめ構成されており、要求されたアプリケーションに関連付けられています。
4. Single Sign-On Server は、クライアント・ブラウザに対して、フォームと、そのフォームを外部アプリケーションにただちに送信する命令を送信します。
5. クライアントは、外部アプリケーションにフォームを送信してログインします。

外部アプリケーションからのログアウト

パートナ・アプリケーションとは異なり、外部アプリケーションではログアウト制御が Single Sign-On Server に渡されません。ユーザーが、これらの各アプリケーションからログアウトすることになります。

シングル・サインオフ

実行しているアプリケーションからログアウトすることによって、シングル・サインオン・セッションを終了し、アクティブなすべてのパートナ・アプリケーションから同時にログアウトできます。パートナ・アプリケーションで「ログアウト」をクリックすると、「シングル・サインオフ」ページが表示され、そこでログアウトを実行できます。

サインオフに成功すると、「シングル・サインオフ」ページの各アプリケーション名の横にチェック・マークが表示されます。アプリケーション名の横に壊れたイメージが表示された場合、ログアウトに失敗したことを示しています。

1 つのセッションでアクティブ化されていたすべてのアプリケーション名にチェック・マークが表示されれば、「戻る」を選択して、ログアウトを開始したアプリケーションに戻ることができます。

パスワードの変更

パスワードの変更画面は、パスワードの有効期限が切れている場合や期限切れが近い場合のみ、ログインしようとする则表示されます。パスワードがまだ有効な場合は、この画面で「取消」をクリックしてログインを続行できます。

その他の状況でパスワードを変更またはリセットするには、管理者でないユーザーは Oracle Delegated Administration Services へ移動する必要があります。これは、Oracle Internet Directory のサービスの 1 つで、ユーザーとグループの管理機能を実行します。

Oracle Delegated Administration Services ホームページは、次のフォームの URL によってアクセスできます。

`http://host:port/oiddas/`

host は、Oracle Delegated Administration Services が配置されているコンピュータの名前を示します。*port* は、このサーバーのポート番号を示します。Oracle Delegated Administration Services と OracleAS Single Sign-On は、通常は同じホスト名になります。

注意： Single Sign-On ユーザー名とは異なり、Single Sign-On パスワードは、大 / 小文字を区別します。また、Oracle Internet Directory のルールに準拠します。

グローバル・ユーザーの非アクティビティ・タイムアウト

グローバル・ユーザーの非アクティビティ・タイムアウトは、あらかじめ構成されたアイドル時間を経過した場合、アプリケーションで再認証を要求できるようにする機能です。このタイムアウトは、シングル・サインオン・セッションのタイムアウトよりも短い非アクティビティ・タイムアウトが必要なセキュリティ重視のアプリケーションにとって有用な機能です。

グローバル・ユーザーの非アクティビティ・タイムアウトの制限時間の超過後にアプリケーションにアクセスすると、通常の認証リクエストがアプリケーションから Single Sign-On Server に送信されます。非アクティビティ・タイムアウトの制限時間を超過していることが Single Sign-On Server で確認されると、ログインを要求するプロンプトが表示されます。制限時間を超過していない場合、ユーザーはセッション Cookie によって認証されます。

注意： シングル・サインオン・セッションが有効な場合でも、グローバル・タイムアウトの制限時間を超過している場合は、資格証明が要求されます。

関連項目： 第 2 章「基本的な管理」の「グローバル・ユーザーの非アクティビティ・タイムアウトの構成」

ワイヤレス・オプションによるサインオン

OracleAS アプリケーションには、PDA や携帯電話、音声認識システムなどのモバイル・デバイスまたはワイヤレス・デバイスを使用してアクセスできます。PC ベース・システムの場合と同様に、認証メカニズムは OracleAS Single Sign-On です。ワイヤレス・オプションは、OracleAS のインストール時に選択できます。ワイヤレス・オプションを選択すると、モバイル・デバイス用のゲートウェイである Wireless deviceportal が Single Sign-On Server に自動的に登録されます。

OracleAS Wireless の詳細は、『Oracle Application Server Wireless 管理者ガイド』および『Oracle Application Server Wireless 開発者ガイド』を参照してください。

基本的な管理

この章では Single Sign-On 管理者について説明し、基本的な管理タスクを示します。この章の項目は次のとおりです。

- Single Sign-On 管理者ロール
- 管理権限の付与
- policy.properties
- Single Sign-On コンポーネントの停止と起動
- OracleAS Single Sign-On 用ブラウザの作業環境の設定
- 管理ページへのアクセス
- 「SSO Server の編集」 ページを使用したサーバーの構成
- グローバリゼーション・サポートの構成
- グローバル・ユーザーの非アクティビティ・タイムアウトの構成
- サンプル・ファイルの取得

Single Sign-On 管理者ロール

Single Sign-On Server への初回アクセス時には、`orcladmin` という名前の Single Sign-On 管理者、すなわち OracleAS スーパー・ユーザーのみが存在します。OracleAS のインストール時に、インストールを行った人がこのユーザーのパスワードを設定します。`orcladmin` アカウントは、シングル・サインオンの管理グループである `iASAdmins` のアカウントなど、他のアカウントを作成するために使用されます。

Single Sign-On 管理者には、Single Sign-On Server に対する完全な権限が与えられます。管理ページを使用して、次の作業を実行できます。

- サーバー設定の構成
- パートナ・アプリケーションの管理
- 外部アプリケーションの管理

管理権限の付与

Single Sign-On 管理者の権限を使用するには、管理グループ `iASAdmins` のメンバーになる必要があります。すなわち、このグループの既存メンバーが、新しい管理者をグループに追加する必要があります。Single Sign-On Server サーバーは、インストール時に `iASAdmins` のメンバーになります。

ユーザーを `iASAdmins` に割り当てるには、次の手順を実行します。

1. Oracle Directory Manager を起動します。このツールの起動方法については、『Oracle Internet Directory 管理者ガイド』を参照してください。
2. `cn=orcladmin` すなわちディレクトリ・スーパー・ユーザーとしてログインします。Oracle Internet Directory のインストール時は、このユーザーに割り当てたパスワードを使用してください。

注意： ディレクトリ・スーパー・ユーザー `cn=orcladmin` は、OracleAS スーパー・ユーザー `orcladmin` と同一ではありません。これらは、階層的に等しくない個別アカウントです。

3. 「システム・オブジェクト」フレームで、次のエントリを続けてクリックします。
 - Entry Management
 - `cn=default_identity_management_realm`
 - `cn=OracleContext`
 - `cn=Groups`
 - `cn=iASAdmins`

例：

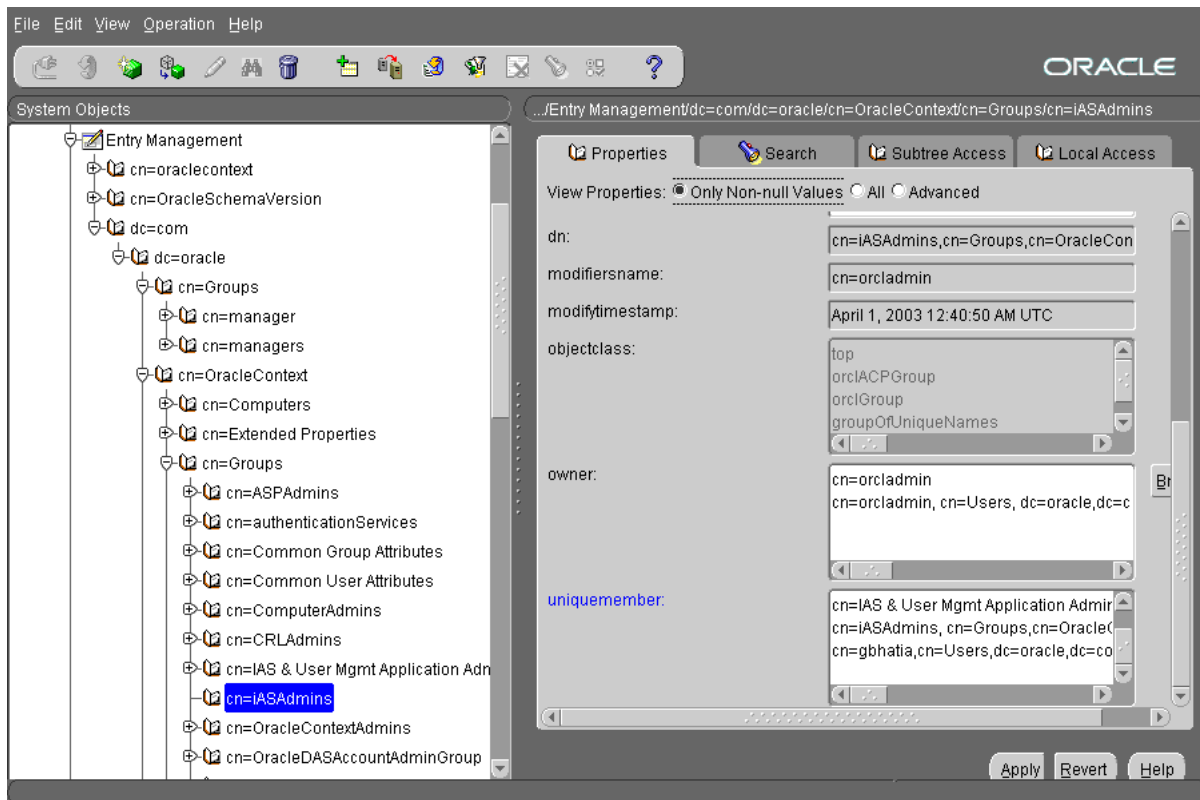
```
cn=iASAdmins,cn=Groups,cn=OracleContext,dc=oracle,dc=com
```

dc=oracle,dc=com は、デフォルトの識別情報管理レベルを示します。実際には、多くの場合、インストール先のドメイン名がデフォルトとして使用されます。

4. 「iASAdmins」タブの「uniquemembers」テキスト・ボックスに、そのユーザーのエントリを追加します。uniquemembers は、エントリ iASAdmins の属性の1つです。それ自体で、グループ iASAdmins のメンバーが定義されます。
5. 「適用」をクリックします。

2-3 ページの図 2-1 は、管理権限を付与するためのインタフェースを再現したものです。

図 2-1 Oracle Directory Manager の「iASAdmins」タブ



新規ユーザーを作成するには、Oracle Delegated Administration Services を使用します。このツールの使用方法は、『Oracle Internet Directory 管理者ガイド』を参照してください。

policy.properties

policy.properties は、OracleAS Single Sign-On の多目的構成ファイルです。このファイルには、Single Sign-On Server で必要とされる基本パラメータが組み込まれています。これらのパラメータのデフォルト値は、大部分のインストールに適合します。したがって、このファイルは変更しないでそのまま使用できます。

policy.properties は、マルチレベル認証などのシングル・サインオン拡張機能の実装にも使用されます。付録 C 「[policy.properties](#)」に、このファイルのコピーがあります。

policy.properties は、\$ORACLE_HOME/sso/conf のシングル・サインオン構成ディレクトリにも格納されています。

注意： policy.properties を編集するときは、各行の末尾に空白を入れないでください。

Single Sign-On コンポーネントの停止と起動

コマンドを個別に発行することで、Oracle HTTP Server のみ、またはシングル・サインオン中間層全体を停止および起動できます。他のコマンドで、OC4J_SECURITY インスタンスのみを停止および起動することもできます。インフラストラクチャのすべてのコンポーネントを停止および起動するコマンドもあります。

Oracle HTTP Server の停止と起動

Oracle HTTP Server を停止して起動するには、次の 2 つのコマンドを発行します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=ohs
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
```

また、次のコマンドを発行して、Oracle HTTP Server を停止して起動することができます。

```
$ORACLE_HOME/opmn/bin/opmnctl restartproc type=ohs
```

OC4J_SECURITY インスタンスの停止と起動

OC4J_SECURITY インスタンスを停止して起動するには、次の 2 つのコマンドを発行します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
$ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

また、次のコマンドで OC4J_SECURITY インスタンスを停止して起動することもできます。

```
$ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

シングル・サインオン中間層の停止と起動

シングル・サインオン中間層を停止して起動するには、Oracle HTTP Server と OC4J_SECURITY インスタンスの両方を停止して起動します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=ohs
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
```

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
$ORACLE_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

すべてのコンポーネントの停止と起動

Oracle HTTP Server、Single Sign-On Server、OC4J および Oracle Internet Directory を停止して起動するには、次のコマンドを発行します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopall
$ORACLE_HOME/opmn/bin/opmnctl startall
```

このコマンドでは、インフラストラクチャ・コンポーネントがすべて同じ Oracle ホーム・ディレクトリに格納されていることを前提としています。

OracleAS Single Sign-On 用ブラウザの作業環境の設定

OracleAS Single Sign-On でログインおよびログアウトするには、次のブラウザ設定を行う必要があります。

キャッシュ設定

正しくキャッシュを設定する手順は次のとおりです。

1. 次のように選択して、キャッシュ設定のダイアログ・ボックスに移動します。
 - Internet Explorer: 「ツール」 → 「インターネットオプション」 → 「全般」 → 「設定」
 - Netscape Communicator: 「編集」 → 「設定」 → 「詳細」 → 「キャッシュ」
2. Internet Explorer では「ページを表示するごとに確認する」を選択し、Netscape Communicator では「ページにアクセスするたび」を選択します。

イメージ設定

イメージを自動的にロードする手順は次のとおりです。

1. 次のように移動します。
 - Internet Explorer: 「ツール」 → 「インターネットオプション」 → 「詳細設定」
 - Netscape Communicator: 「編集」 → 「設定」 → 「詳細」
2. Internet Explorer では「画像を表示する」を選択し、Netscape Communicator では「自動的に画像を読み込む」を選択します。

管理ページへのアクセス

シングル・サインオン UI の管理ページでは、シングル・サインオン・セッションの長さを設定したり、サーバーによる IP アドレスの検証を有効にすることができます。また、これらのページでは、パートナ・アプリケーションおよび外部アプリケーションを管理することもできます。

管理ページにアクセスするには、次の手順を実行します。

1. 次のフォームの URL を入力します。

```
http://host:port/pls/single_sign_on_DAD
```

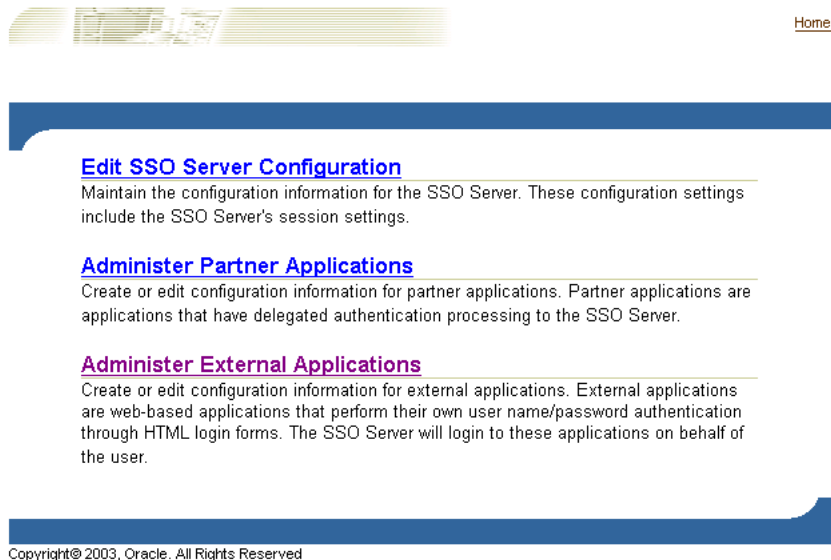
host には、Single Sign-On Server が配置されているコンピュータの名前を代入し、*port* にはこのサーバーのポート番号を代入し、*single_sign_on_DAD* には Single Sign-On スキーマ用のデータベース・アクセス記述子を代入します。デフォルトの DAD は、*orasso* です。

「パートナ・アプリケーションへのアクセス」ページが表示されます。

2. 「パートナー・アプリケーションへのアクセス」ページの右上にある「ログイン」をクリックします。
「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て、「ログイン」をクリックします。
4. ホーム・ページが表示されます。管理機能を実行するには、「SSO Server 管理」をクリックします。

図 2-2 は、「SSO Server 管理」ページを再現したものです。

図 2-2 「SSO Server 管理」ページ



「SSO Server の編集」 ページを使用したサーバーの構成

シングル・サインオン・セッションの長さの修正と IP アドレスの検証を行うには、「SSO Server の編集」 ページを使用します。「SSO Server の編集」 ページにアクセスするには、「SSO Server 管理」 ページで「SSO Server 構成の編集」をクリックします。

「SSO Server の編集」 ページには、次のヘッダーとフィールドが表示されます。

表 2-1 SSO セッション・ポリシー

フィールド	説明
シングル・サインオン・セッションの持続期間	タイムアウトが発生せず再ログインすることなしに、サーバーへのログインを継続できる時間を入力します。
Single Sign-On Server へのリクエストで使用される IP アドレスを検証します。	ブラウザの IP アドレスと認証リクエストに使用される IP アドレスが一致することを検証するときに選択します。

グローバルゼーション・サポートの構成

Single Sign-On UI は、ユーザーのブラウザで構成された任意の言語で表示できます。OracleAS をインストールすると、英語およびオペレーティング・システムの言語がインストールされます。その他の言語をインストールするには、「インストールする製品の選択」画面で「製品の言語」 ボタンをクリックします。OracleAS のインストール時に他の言語のインストールを忘れた場合でも、ossoca.jar ツールを実行すれば、他の言語のシングル・サインオン UI を有効にすることができます。

インストールの後で Single Sign-On Server に言語を追加するには、次の手順を実行します。

1. Repository Configuration Assistant の CD ホーム (REPCD_HOME) から、目的の言語のファイルを OracleAS Single Sign-On の Oracle ホームにコピーします。

```
cp REPCD_HOME/portal/admin/plsql/nlsres/ctl/lang/*.* ORACLE_HOME/sso/nlsres/ctl/lang/
```

lang は目的の言語のコードです。たとえば、日本語の場合、この値は *ja* になります。ossoca.jar を実行する前に、Single Sign-On のホームに *lang* ディレクトリを作成しておく必要があります。

2. ライブラリ・パス環境変数に \$ORACLE_HOME/lib を追加します。
3. 次のコマンドを発行します。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar langinst lang make_lang_avail $ORACLE_HOME
```

変数 *lang* には、インストールする言語のコードを代入します。追加言語を使用可能に設定する場合、変数 *make_lang_avail* に 1 を代入します。追加言語を使用不能に設定する場合、0 を代入します。

次の例では、韓国語がインストールされます。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar langinst ko 1
$ORACLE_HOME
```

サポートされている言語コードの詳細なリストについては、『Oracle Application Server 10g グローバリゼーション・ガイド』の付録 A を参照してください。

グローバル・ユーザーの非アクティビティ・タイムアウトの構成

この項に進む前に、第 1 章「コンポーネントとプロセス:概要」の「[グローバル・ユーザーの非アクティビティ・タイムアウト](#)」を一読してください。

グローバル・ユーザーの非アクティビティ・タイムアウトは、1つのドメインにのみ適用されます。つまり、タイムアウトを有効にしたコンピュータは、同じ Cookie ドメインに属している必要があります。これらのコンピュータ上のアプリケーションは、ドメインの Cookie を使用してユーザーのアクティビティを追跡します。たとえば、Single Sign-On Server に login.acme.com を使用している場合は、システム内の他のコンピュータでも、ホスト名に .acme.com が含まれている必要があります。たとえば、あるコンピュータは host1.acme.com、別のコンピュータは host2.acme.com というようになります。また、Single Sign-On Server を含み、これらすべてのコンピュータのクロックが同期化されている必要があります。

グローバル・ユーザーの非アクティビティ・タイムアウトは、デフォルトでは構成されていません。`$ORACLE_HOME/sso/admin/plsql/sso` にある `ssogito.sql` スクリプトを実行して、非アクティビティ・タイムアウトを有効にする必要があります。次の手順には、`ssogito.sql` の例も含まれています。

グローバル・ユーザーの非アクティビティ・タイムアウトを構成する手順は次のとおりです。

1. シングル・サインオンのスキーマ名とパスワードを使用して、SQL*Plus にログインします。デフォルトのスキーマ名は `orasso` です。パスワードの取得方法については、付録 B を参照してください。
2. 次のコマンドを入力して `ssogito.sql` を実行します。

```
SQL> @ssogito.sql
```

フィールドのリストが表示されます。

3. 「`{timeout_cookie_domain}` の値の入力」フィールドに、Single Sign-On Server に対応しているすべてのアプリケーションに共通のドメイン名を入力します。ドメイン名の前に期間を付加してください。

注意： このフィールドを空白にした場合、ドメイン名は、デフォルトで Single Sign-On Server のホスト名に設定されます。

4. 「[inactivity period] の値の入力」フィールドに、必要な非アクティブ期間（たとえば、15分）を入力します。
5. この新規設定を有効にする場合は、[Return] キーまたは [Enter] キーを押します。このトランザクションを取り消す場合は、[Return] または [Enter] キーを2回押します。

トランザクションを完了すると、スクリプトによって、新しいタイムアウト設定のサマリーが提供されます。ssogito.sql の例は次のようになります。

```
SQL> @ssogito
=====
SSO Server Inactivity Timeout Configuration
=====
Timeout          : DISABLED
Cookie name      : OSSO_USER_CTX
Cookie domain    :
Inactivity period: 15 minutes
Encryption key   : 093D678526DAA66D
Note: timeout cookie domain will be defaulted
to the SSO Server hostname
-----
To disable timeout set inactivity period to 0, (zero)
Press return key twice if you do not want
to change timeout configuration.

PL/SQL procedure successfully completed.

Enter value for timeout_cookie_domain: .oracle.com
Enter value for inactivity_period: 15
Timeout          : ENABLED
New timeout cookie domain: .oracle.com
New inactivity period   : 15 minutes

PL/SQL procedure successfully completed.

No errors.
```

6. シングル・サインオン中間層を再起動します。「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

7. 非アクティビティ・タイムアウトを有効にするアプリケーション中間層で、`mod_osso.conf` ファイルを編集します。OssoIdleTimeout パラメータがあり、`on` に設定されていることを確認します。このファイルは `$ORACLE_HOME/Apache/Apache/conf` にあります。正しい設定のファイルは次のようになります。

```
LoadModule osso_module libexec/mod_osso.so
<IfModule mod_osso.c>
    OssoIpCheck off
    OssoIdleTimeout on
    OssoConfigFile /u01/oracleas10g/Apache/Apache/conf/osso/osso.conf
#
#Insert Protected Resources
#
.
.
.
</IfModule>
```

8. アプリケーション中間層で Oracle HTTP Server を再起動します。「[Oracle HTTP Server の停止と起動](#)」の項を参照してください。

Oracle Delegated Administration Service と Single Sign-On Server が同じ中間層にあり、前者にグローバル・ユーザーの非アクティビティ・タイムアウトを適用する場合は、シングル・サインオン中間層で手順 7 と 8 を実行します。

サンプル・ファイルの取得

`ipassample.jar` ファイルには、証明書を使用したサインオンや配置固有のページなど、シングル・サインオン機能のサンプル・コードが組み込まれています。このファイルを抽出するには次のコマンドを使用します。

```
$ORACLE_HOME/jdk/bin/jar -xvf $ORACLE_HOME/sso/lib/ipassample.jar
```

ディレクトリ対応 Single Sign-On

この章では、Oracle Internet Directory に依存している OracleAS Single Sign-On の機能について説明します。Oracle Internet Directory は、すべての Single Sign-On ユーザー、すなわち管理者と非管理者のアカウントおよびパスワード用のリポジトリです。ユーザーとグループの管理機能はこのディレクトリですべて処理されます。

この章の項目は次のとおりです。

- [Oracle Internet Directory](#) におけるユーザー管理
- [パスワード・ポリシー](#)
- [OracleAS Single Sign-On](#) のディレクトリ・ツリー
- [ディレクトリ・アクセス用 Single Sign-On Server](#) の設定変更
- [ディレクトリ変更による Single Sign-On Server](#) の更新

Oracle Internet Directory におけるユーザー管理

Single Sign-On ユーザーを管理するには、次のツールを使用します。

- Oracle Delegated Administration Services

Oracle Delegated Administration Services は、管理者がユーザーとグループの管理に使用できるセルフサービス・アプリケーションです。たとえば、ユーザーの作成や削除、パスワードの変更を行うことができます。

次のフォームの URL を入力すると、Oracle Delegated Administration Service にアクセスできます。

`http://host:port/oiddas/`

host には Oracle Delegated Administration Services サーバーが配置されているコンピュータ名を代入し、*port* にはこのサーバーのポート番号を代入します。インフラストラクチャの通常のインストールでは、Oracle Delegated Administration Service と OracleAS Single Sign-On は同じホスト名になります。

- Oracle Directory Manager

Oracle Directory Manager は、Oracle Internet Directory のほとんどの機能を管理する Java ベースのツールです。このツールを使用して、パスワード・ポリシーを構成できます。

- LDAP コマンドライン・ツール

ldapmodify などのコマンドライン・ツールは、Oracle Delegated Administration Services と Oracle Directory Manager のかわりに使用できます。これらのツールを使用して、テキスト・ファイルを操作できます。これらは、LDAP データ交換 (LDIF) フォーマットを使用する引数を取ります。

パスワード・ポリシー

Single Sign-On ユーザーのパスワードは、Oracle Internet Directory にユーザー・エントリの属性として格納されます。ユーザーは、Single Sign-On UI で自分のパスワードを変更できます。または、Oracle Delegated Administration Services に移動して変更することもできます。Oracle Directory Manager を使用することで、ディレクトリ管理者はパスワードの有効期限に関する動作を企業ニーズに適合するように調整できます。

この項の項目は次のとおりです。

- [パスワード・ルール](#)
- [パスワードの有効期限の構成](#)
- [パスワードの変更ページの動作](#)
- [アカウント・ロックアウトの構成](#)
- [ユーザーのロック解除](#)
- [パスワード・ポリシーの構成](#)

パスワード・ルール

Oracle Directory Manager のフィールドでは、パスワードに必要な最小文字数を指定できます。デフォルト値の詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

パスワードの有効期限の構成

Oracle Directory Manager または LDAP コマンドライン・ツールを使用すると、パスワードの有効期限の構成や、ユーザーにパスワードの変更を要求する時間を指定できます。ユーザーの猶予期間ログインを構成することもできます。これは、ユーザーのパスワードが有効期限切れになった後の期間を示します。ユーザーがこの期間内にパスワードを変更しなかった場合は、そのパスワードを管理者にリセットしてもらう必要があります。

パスワードの変更ページの動作

パスワードの有効期限が切れている場合や期限切れが近いときにユーザーがログインすると、サーバーは次のように動作します。

パスワードが失効している場合

パスワードの失効を表す画面が表示されます。ユーザーは、ディレクトリ管理者に連絡してパスワードのリセットを要求する必要があります。

パスワードが間もなく失効する場合

パスワードの変更ページが表示されます。この場合、このページを取り消すか、パスワードを変更することができます。いずれの場合でも、パスワードの変更ページが表示されないときと同様に認証が行われます。

猶予期間ログインの実施

猶予期間ログインがディレクトリで構成されている場合は、パスワードの有効期限が切れるとパスワードの変更ページが表示されます。この場合、このページを取り消すか、パスワードを変更することができます。いずれの場合でも、認証の手順はユーザーのパスワードが有効であるときと同じです。

パスワードの変更の強制

OracleAS Single Sign-On では、パスワードの変更の強制機能がサポートされていません。この機能は、管理者によるパスワードのリセット後にパスワードの変更をユーザーに要求します。ディレクトリ側では、pwdMustChange 属性を設定することで、パスワードの変更を強制できます。

アカウント・ロックアウトの構成

アカウント・ロックアウトは、ユーザーが不適切なユーザー名とパスワードの組合せを Oracle Internet Directory で許可されている回数を超えて送信したために、いずれのワークステーションからも Single Sign-On Server にアクセスできなくなったときに発生します。デフォルトの回数は 10 です。この制限回数に達すると、有効なユーザー名とパスワードの組合せを使用してもログインできなくなります。

Single Sign-On ユーザーのアカウントは Oracle Internet Directory で管理されているため、ディレクトリ管理者は、アカウント・ロックアウト・ポリシーを決めておく必要があります。Oracle Directory Manager のフィールドを使用して、ロックアウトの有効化と無効化を設定したり、ロックアウト期間を指定できます。

デフォルトのロックアウト期間は 1 日です。

ユーザーのロック解除

ユーザーのロック解除の方法については、『Oracle Internet Directory 管理者ガイド』を参照してください。

パスワード・ポリシーの構成

パスワード・ポリシーの構成方法については、『Oracle Internet Directory 管理者ガイド』を参照してください。

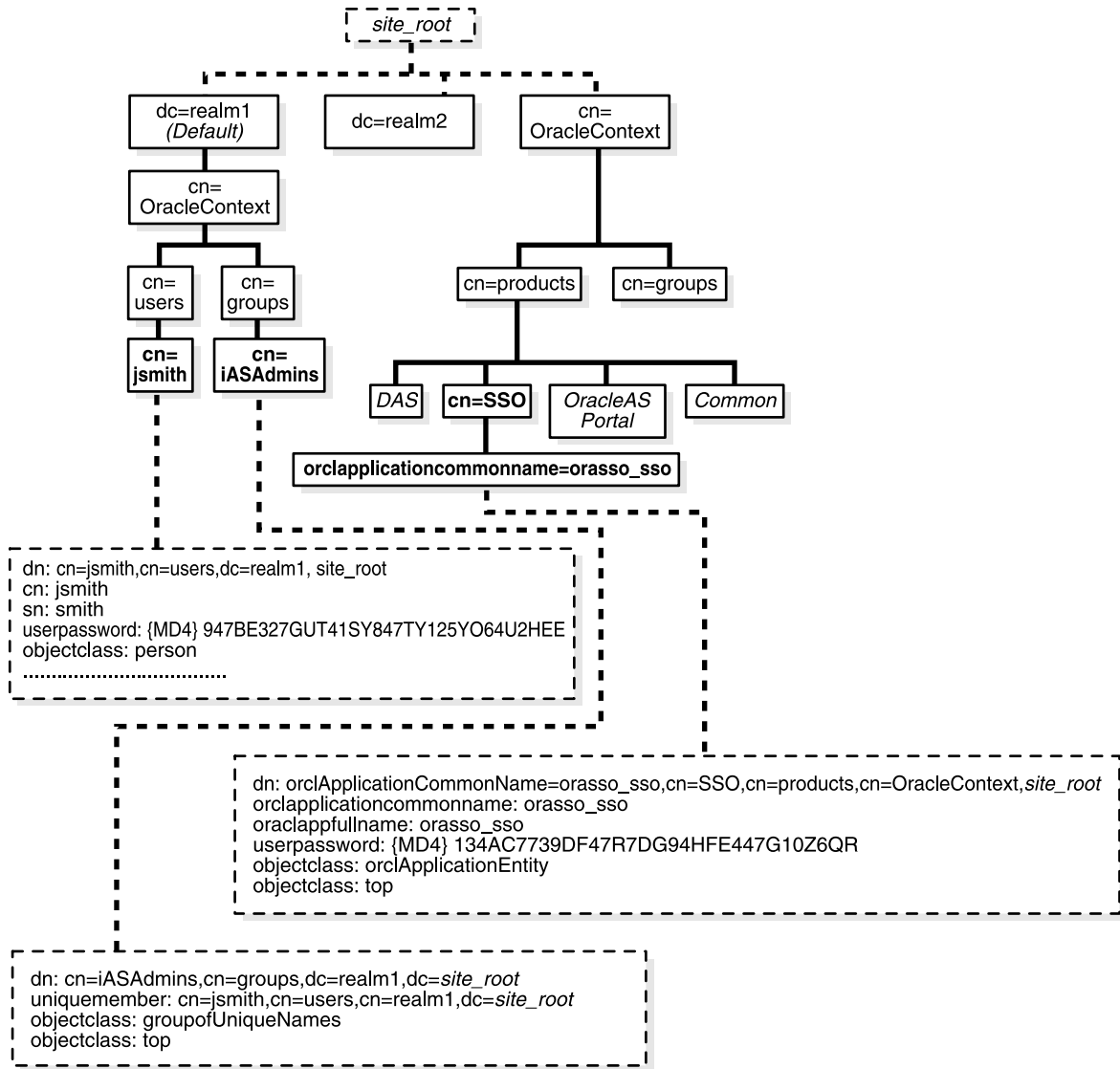
OracleAS Single Sign-On のディレクトリ・ツリー

他の OracleAS 補完コンポーネントと同様に、OracleAS Single Sign-On では、ディレクトリ情報ツリー (DIT) 内に独自のコンテナがあります。このコンテナは、すべての Oracle 固有データのルートとしての役割を果たすエン트리である Oracle Context 内にあります。3-6 ページの図 3-1 に示す DIT の簡略図では、ルート Oracle Context とレلم固有 Oracle Context の両方が開かれています。ルート Oracle Context は、サイト全体の情報 (すべての識別情報管理レلمと製品に適用される情報) のリポジトリです。レلم固有の Oracle Context は、構造的にはルート・コンテキストのミラー・イメージですが、含まれる情報は特定のレلمのみに関連する情報です。これらのレلمには、特定のユーザー固有の構成情報とその他のネットワーク・エンティティが格納されます。レلمの詳細は、第 10 章「アプリケーション・サービス・プロバイダに対するサポートの有効化」を参照してください。

図 3-1 に示すように、Single Sign-On コンテナは、エン트리 cn=SSO によって識別されます。このエン 트리には、1 つのエン 트리 orclApplicationCommonName=orasso_sso のみが含まれています。これは Single Sign-On Server のエン 트리です。図では、このエン 트리が開かれて、そのエン 트리を定義しているオブジェクト・クラスと属性が示されています。たとえば、orclapplicationcommonname 属性では、Single Sign-On Server のデフォルト名 orasso が指定されています。また、Single Sign-On Server には、orclapplicationcommonname に加えて、独自のパスワードがあることに注意してください。Single Sign-On Server がユーザー検索を実行するときに、ディレクトリ・サーバーはこのパスワードを使用して Single Sign-On Server を認証します。

コンテナ Common は、すべての OracleAS 製品に共通の情報リポジトリです。たとえば、製品がレلم検索ベースやノード、レلم・ニックネームを識別するための属性がこのコンテナに格納されています。この図には記載されていませんが、レلم固有の Common コンテナには、製品がレلم・サブツリー内でユーザーを検索するための属性が格納されています。図では、SSO コンテナのほかに、管理者でもある OracleAS ユーザーのエン 트리も開かれています。

図 3-1 OracleAS Single Sign-On のディレクトリ情報ツリー



ディレクトリ・アクセス用 Single Sign-On Server の設定変更

ssooconf.sql スクリプトを使用して、ディレクトリ内の次の設定を変更できます。

- ディレクトリ・ホスト名
- ディレクトリ・ポート
- Single Sign-On Server 用のパスワード
- ディレクトリへの SSL 接続

注意： Oracle Internet Directory の新規インスタンスは、レプリケート・インスタンスである必要があります。

Single Sign-On Server 用のディレクトリ設定を変更する手順は次のとおりです。

1. \$ORACLE_HOME/sso/admin/plsql/sso にあるスクリプトに移動します。
2. SQL*Plus にスキーマ orasso としてログインします。スキーマのパスワードの取得方法については、[付録 B](#) を参照してください。

注意： このスクリプトは、sys で実行することはできません。

3. 次のコマンドを発行して ssooconf.sql を実行します。

```
SQL> @ssooconf.sql
```

4. 「値を入力してください」という文字列に続くフィールドで、必要な変更を行います。
5. [Return] または [Enter] を押して、ファイルを更新します。

Single Sign-On Server の更新された設定がスクリプトによって表示されます。

スクリプトの起動後に、変更を加えないことにした場合は、[Return] または [Enter] を押すと、既存の値のままになります。

ディレクトリ変更による Single Sign-On Server の更新

Single Sign-On Server では、Oracle Internet Directory DIT に関するメタデータがキャッシュされます。このメタデータには、ユーザー検索ベース、ユーザー・ニックネーム属性、レルム関連メタデータなどがあります。ディレクトリ DIT を変更した場合は、Single Sign-On Server のキャッシュを更新する必要があります。この作業を行うには、`ssoreoid.sql` スクリプトを実行します。

1. `$ORACLE_HOME/sso/admin/plsql/sso` にあるスクリプトに移動します。
2. 次のように入力して、Single Sign-On スキーマにログインします。

```
SQL> connect orasso/orasso_password
```

スキーマのパスワードの取得方法については、付録 B を参照してください。

注意： このスクリプトは、`sys` で実行することはできません。

3. 次のスクリプトを実行します。

```
SQL> @ssoreoid.sql
```

4. Single Sign-On Server を再起動します。第 2 章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

スクリプトの実行を必要とする DIT 変更の一例を次に示します。

- デフォルトのレルム名またはレルム DN の変更あるいは両方の変更
- デフォルトのレルムの新規作成
- デフォルトのレルムのユーザー検索ベースまたはグループ検索ベースの変更あるいは両方の変更
- ユーザー・ニックネーム属性の変更

Oracle Internet Directory におけるレルム情報の変更方法については、『Oracle Internet Directory 管理者ガイド』を参照してください。

パートナ・アプリケーションの設定と管理

この章では、Single Sign-On でパートナ・アプリケーションを使用可能にする方法について説明します。このプロセスでは、Oracle HTTP Server の認証モジュールである `mod_osso` を Single Sign-On Server に登録する必要があります。パートナ・アプリケーションの定義については、第1章の「パートナ・アプリケーション」の項を参照してください。

この章の項目は次のとおりです。

- [パートナ・アプリケーションの登録:登録方法](#)
- [mod_osso の登録](#)
- [ロード・バランサを使用した複数のパートナ・アプリケーションの配置](#)
- [仮想ホストでの mod_osso の構成](#)

パートナ・アプリケーションの登録：登録方法

Single Sign-On パートナ・アプリケーションは、OracleAS インストーラによって自動的に登録されます。パートナ・アプリケーションを登録すると、そのエントリが Identity Management インフラストラクチャ・データベースに作成され、パートナ・アプリケーション・コンピュータで登録が構成されます。

mod_osso 統合アプリケーションは、ossoreg.jar ツールで登録します。SDK 統合アプリケーションの OracleAS Portal は、ptlasst で登録します。これらのツールはインストーラで起動します。ここでは、ossoreg.jar についてのみ説明します。ptlasst スクリプトの詳細は、Portal のドキュメントを参照してください。

mod_osso の登録

特定の状況下では、シングル・サインオン登録ツールを使用して mod_osso を手動で登録する必要があります。これに該当する状況は次のとおりです。

- OracleAS のインストール後に Oracle HTTP Server のホスト名とポート番号を変更した場合。
- osso.conf ファイルを削除または壊した場合。
- OracleAS のインストール後に Single Sign-On Server で SSL を有効にした場合。

3つのケースではいずれも、シングル・サインオン登録ツールを実行して osso.conf の mod_osso 登録レコードを更新します。このツールを実行すると、必ずこのファイルが生成されます。

この項の項目は次のとおりです。

- [ossoreg.jar の構文とパラメータ](#)
- [コマンド例](#)
- [Oracle HTTP Server の再起動](#)

ossoreg.jar の構文とパラメータ

アプリケーションの登録には `ossoreg.jar` ツールを使用します。次のコマンドを実行します。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/ssl/lib/ossoreg.jar
-oracle_home_path orcl_home_path
-site_name site_name
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u userid
[-virtualhost]
[-update_mode CREATE | DELETE | MODIFY]
[-config_file config_file_path]
[-admin_info admin_info]
[-admin_id adminid]
```

ツールに渡されるパラメータ記述は、次のとおりです。

oracle_home_path

Oracle ホームの絶対パスです。

site_name

サイト名です。通常は、パートナ・アプリケーションの有効なホスト名とポートが使用されます。たとえば、`application.mydomain.com` のように指定します。

config_mod_osso

TRUE に設定すると、登録するアプリケーションが `mod_osso` であることがこのパラメータで指定されます。`osso.conf` を生成するには、`config_mod_osso` を挿入する必要があります。

mod_osso_url

パートナ・アプリケーションの有効な URL です。この URL は、パートナ・アプリケーションへのアクセスに使用されます。値は、次の URL 形式で指定します。

```
http://oracle_http_host.domain:port
```

例：

```
http://application.mydomain.com:7777
```

パートナの Oracle HTTP Server が HTTP のデフォルトのポート 80 または HTTPS のデフォルトのポート 443 をリスニングする場合は、ポート番号を省略します。

u

Oracle HTTP Server を起動するユーザー名です。UNIX では、一般にこのユーザー名は root です。Windows NT/2000 では SYSTEM です。パラメータ u は必須です。

virtualhost

オプション。このパラメータは、Oracle HTTP 仮想ホストを Single Sign-On Server に登録する場合にのみ使用します。仮想ホストを登録しない場合は省略します。

HTTP 仮想ホストを作成する場合は、httpd.conf ファイルを使用して、保護された URL ごとに次のディレクティブを入力します。

```
<VirtualHost host_name>
  OossoConfigFile $ORACLE_HOME/Apache/Apache/conf/osso/host_name/osso.conf
  OossoIpCheck off
  #<Location /your_protected_url>
  # AuthType basic
  # Require valid-user
  #</Location>
  #Other configuration information for the virtual host
</VirtualHost>
```

一方、HTTPS 仮想ホストを作成する場合は、ssl.conf ファイルを使用して同じディレクティブを入力します。コメント行は、アプリケーションを配置する前に削除する必要があります。httpd.conf と ssl.conf は、どちらも \$ORACLE_HOME/Apache/Apache/conf に格納されています。

仮想ホストを作成したら、次のコマンドを実行して、Distributed Cluster Management スキーマを更新します。

```
$ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

config_file

構成する仮想ホストの osso.conf ファイルの場所です。例: \$ORACLE_HOME/Apache/Apache/conf/osso/virtual_host_name/osso.conf

仮想ホストを登録する場合、このパラメータは必須です。config_file を省略した場合、非仮想ホストであると見なされます。この場合、ossoreg.jar によって、osso.conf という名前のファイルが \$ORACLE_HOME/Apache/Apache/conf/osso に作成されます。

update_mode

オプション。パートナ登録レコードの作成、削除および変更を行います。CREATE はレコードを新規に作成します (デフォルト)。DELETE は既存のレコードを削除します。MODIFY は、既存のレコードを削除して新規にレコードを作成します。

admin_info

オプション。mod_osso 管理者のユーザー名です。このパラメータを省略すると、「パートナー・アプリケーションの編集」ページの「管理者の情報」フィールドが空白のままになります。

admin_id

オプション。電子メール・アドレスなどの管理者の追加情報です。このパラメータを省略すると、「パートナー・アプリケーションの編集」ページの「管理者の電子メール」フィールドが空白のままになります。

コマンド例

次のコマンド・シーケンスは、Single Sign-On Server に登録する mod_osso インスタンスを示しています。

■ UNIX:

```
setenv $ORACLE_HOME /private/oracle/gitml

setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:$ORACLE_HOME/lib

$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/ssolib/ossoreg.jar
-oracle_home_path $ORACLE_HOME
-site_name portal.mydomain.com
-config_mod_osso TRUE
-mod_osso_url http://portal.mydomain.com
-u root
```

■ Windows NT/2000:

```
set ORACLE_HOME=c:\private\oracle\gitml

set PATH=%PATH%;%ORACLE_HOME%\bin;%ORACLE_HOME%\lib

%ORACLE_HOME%\jdk\bin\java -jar %ORACLE_HOME%\ssolib\ossoreg.jar
-oracle_home_path %ORACLE_HOME%
-site_name portal.mydomain.com
-config_mod_osso TRUE
-mod_osso_url http://portal.mydomain.com
-u SYSTEM
```

Oracle HTTP Server の再起動

ossoreg.jar を実行した後、Oracle HTTP Server を再起動します。手順については、第 2 章の「Oracle HTTP Server の停止と起動」の項を参照してください。

ロード・バランサを使用した複数のパートナ・アプリケーションの配置

可用性の高い配置で複数のパートナ・アプリケーション・インスタンスを構成するには、これらのインスタンスをインストールする前にロード・バランサを配置します。ロード・バランサによって、複数のパートナ・アプリケーションを 1 つのアドレスで公開でき、また実際にリクエストを処理するアプリケーション・サーバーの障害に備えることができます。

HTTP ロード・バランサは、Oracle HTTP Server インスタンスの 1 つで発生した障害を検出し、別のインスタンスにリクエストをフェイルオーバーできます。

ここに示す使用例では、ロード・バランサを利用するパートナ・アプリケーションの構成に必要な手順を説明します。

使用例

この使用例では、次の架空の構成を前提としています。

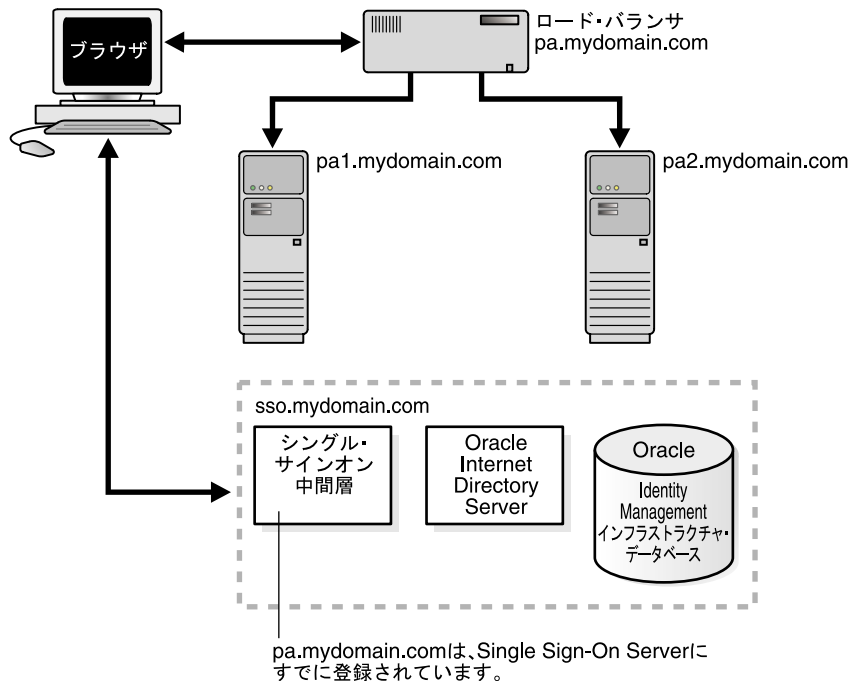
- pa1.mydomain.com と pa2.mydomain.com の 2 台のパートナ・アプリケーション・コンピュータがあります。これらのアプリケーション・サーバーは、非 SSL ポート 7777 をリスニングしています。
- これらのパートナ・アプリケーション・コンピュータは、sso.mydomain.com にある Single Sign-On Server を使用するように構成されています。
- ユーザーに公開されているパートナ・アプリケーションの有効なホスト名は pa.mydomain.com です。HTTP ロード・バランサは、このアドレス（ポート 80）をリスニングするように構成されています。HTTP ロード・バランサは負荷を分散し、ユーザーのリクエストのフェイルオーバーを pa1.mydomain.com と pa2.mydomain.com の間で行います。
- Single Sign-On Server、ディレクトリ・サーバーおよび Identity Management インフラストラクチャ・データベースは、sso.mydomain.com に配置されています。

注意：

- この使用例では、ロード・バランサが非 SSL ポート番号のポート 80 をリスニングします。ロード・バランサが SSL を使用してブラウザと対話するように構成されている場合は、別のポート番号を選択する必要があります。デフォルトの SSL ポート番号は 443 です。
- この使用例では、2 台のパートナ・アプリケーション・コンピュータが示されています。実際には、任意の数のコンピュータを使用できます。

図 4-1 は、この架空システムの構成を示しています。

図 4-1 複数のパートナ・アプリケーションで使用するロード・バランサ



構成手順

図 4-1 に示すシステムを設定するには、次の作業を行います。

- パートナ・アプリケーションのインストール
- パートナ・アプリケーション中間層での Oracle HTTP Server の構成
- HTTP ロード・バランサの構成
- パートナ・アプリケーション中間層での `mod_osso` の再登録

パートナ・アプリケーションのインストール

パートナ・アプリケーションを `pa1.mydomain.com` および `pa2.mydomain.com` にインストールします。インストーラがディレクトリの場所を要求したら、`sso.mydomain.com` に配置されたサーバーを選択します。

注意： ここで紹介するパートナ・アプリケーションは、任意の Web ベース・アプリケーションと置き換えて考えることができます。単純な例としては、Oracle HTTP Server と OC4J を含む OracleAS コア・インストールなどがあります。各アプリケーションのインストール・マニュアルを参照してください。

パートナ・アプリケーション中間層での Oracle HTTP Server の構成

OracleAS 中間層で、ユーザーと Oracle HTTP Server の間にロード・バランサを設置すると、パートナ・アプリケーションの有効な URL が変更されます。両方の中間層の構成ファイル `httpd.conf` を修正し、この変更を反映する必要があります。このファイルは、`$ORACLE_HOME/Apache/Apache/conf` にあります。

次の手順を実行します。

1. OracleAS 中間層で、Oracle HTTP Server を変更して、外部に公開する名前（使用例では `pa.mydomain.com`）をリスニングします。

`pa1.mydomain.com` および `pa2.mydomain.com` の `httpd.conf` ファイルに、次の行を追加します。

```
ServerName pa.mydomain.com
Port 80
```

注意： `httpd.conf` に複数のポートが記述されている場合、変更されるポートは必ず最後のものになります。

2. ブラウザとロード・バランサの間に SSL を構成し、SSL 接続がロード・バランサで終了する場合は、pa1.mydomain.com と pa2.mydomain.com の両方に mod_certheaders を構成します。このモジュールによって、Oracle HTTP Server では、HTTP で受信するリクエストを SSL リクエストとして処理できるようになります。手順は次のとおりです。

- a. httpd.conf に次の行を入力します。

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

- b. OracleAS Web Cache をロード・バランサとして使用する場合は、次の行を入力します。

```
AddCertHeader HTTPS
```

ハードウェア・ロード・バランサを使用する場合は、次の行を入力します。

```
SimulateHttps on
```

ステップ a と b は、httpd.conf ファイルの末尾に追加できます。このファイルにおけるステップの記述位置は重要ではありません。

HTTP ロード・バランサの構成

HTTP ロード・バランサには、BigIP、Alteon、Local Director などのハードウェアや、OracleAS Web Cache などのソフトウェアを使用することができます。

- ハードウェア・ロード・バランサ

ハードウェアのロード・バランサを使用する場合は、実サーバーの 1 つのプールをアドレス pa1.mydomain.com および pa2.mydomain.com で設定します。1 つの仮想サーバーをアドレス pa.mydomain.com に構成します。この仮想サーバーは、ロード・バランサの外部インタフェースです。構成手順の詳細は、ロード・バランサのベンダーが提供するドキュメントを参照してください。

- ソフトウェア・ロード・バランサ

接続要求のロード・バランサに OracleAS Web Cache を使用する場合は、次のドキュメントを参照してください。

- 『Oracle Application Server Web Cache 管理者ガイド』の Oracle Identity Management インフラストラクチャの利用に関する項
- 『Oracle Application Server Web Cache 管理者ガイド』の Single Sign-On Server のリクエストのルーティングに関する項

注意： 最高のパフォーマンスを得るには、ハードウェア・ロード・バランサを使用してください。

パートナ・アプリケーション中間層での mod_osso の再登録

mod_osso を両方のパートナ・アプリケーション・インスタンスで、パートナ・アプリケーション pa.mydomain.com として登録します。

pa1.mydomain.com で mod_osso を登録するには、登録スクリプトを実行します。次の例では、実際のインストール環境に合わせて適切な値を代入してください。pa.mydomain.com というパートナ・アプリケーションが登録スクリプトによって作成されます。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path orcl_home_path
-site_name site_name
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u userid
[-virtualhost]
[-update_mode CREATE | DELETE | MODIFY]
[-config_file config_file_path]
[-admin_id adminid]
[-admin_info admin_info]
```

コマンドの例とコマンド・パラメータの説明については、「[mod_osso の登録](#)」の項を参照してください。

注意： パートナ・アプリケーション・コンピュータを Distributed Cluster Management 用に構成する場合は、以降の手順を省略してください。かわりに、pa1.mydomain.com で次のコマンドを実行します。

```
$ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```

mod_osso を pa2.mydomain.com に登録する手順は次のとおりです。

1. pa2.mydomain.com で、Single Sign-On 管理者としてシングル・サインオン管理ページにログインします。次の URL にログインしてください。

`http://sso.mydomain.com/pls/orasso`

2. 「パートナ・アプリケーションの管理」ページを使用して、パートナ・アプリケーション pa2.mydomain.com の既存エントリを削除します。
3. pa1.mydomain.com から osso.conf ファイルをコピーします。ファイルを FTP で転送する場合は、バイナリ・モードを使用してください。このファイルのデフォルトのディレクトリは、\$ORACLE_HOME/Apache/Apache/conf/osso です。

4. **Distributed Cluster Management** リポジトリとコピーしたファイルを同期化します。これには、pa2.mydomain.com で次のコマンドを実行します。

```
$ORACLE_HOME/Apache/Apache/bin/ssotransfer $ORACLE_
HOME/Apache/Apache/conf/osso/osso.conf
```

注意： ssotransfer コマンドは、Distributed Cluster Management リポジトリと仮想ホストに作成された mod_osso 構成ファイルとの同期化には使用しないでください。仮想ホストの mod_osso を登録する方法については、「仮想ホストでの mod_osso の構成」の項を参照してください。

5. **Oracle HTTP Server** を再起動します。手順については、第 2 章の「**Oracle HTTP Server の停止と起動**」の項を参照してください。
6. 次の有効な URL を使用して、パートナ・アプリケーションをテストします。

```
http://pa.mydomain.com
```

パートナ・アプリケーションと mod_osso を統合する方法については、『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』の「シングル・サインオン対応のアプリケーションの開発」を参照してください。

仮想ホストでの mod_osso の構成

1 つの Oracle HTTP Server に複数の Web サイトを配置する必要がある場合があります。たとえば、HTTP と HTTPS の両方でアプリケーションを使用可能にする必要がある場合などです。次の例では、SSL 仮想ホストが mod_osso で保護されるように構成しています。この場合の仮想ホストは SSL ホストですが、この例はどの仮想ホストにも適用されます。

この例では、次の条件を前提としています。

- アプリケーション中間層のホスト名が app.mydomain.com であること。
- 中間層がすでに非 SSL パートナ・アプリケーションとして構成されていること。これは通常、アプリケーションを最初にインストールするときに、OracleAS インストーラによって行われます。
- アプリケーション中間層のデフォルトの SSL ポート番号が 4443 であること。

app.mydomain.com を SSL 仮想ホストとして構成するには、次の手順を実行します。

1. Oracle Identity Management のコンポーネント（特に、Oracle Internet Directory と Single Sign-On Server）が実行されていることを確認します。
2. app.mydomain.com が SSL 仮想ホストとして定義されていることを確認します。リリース 9.0.4 の OracleAS インストーラでは、この処理を ssl.conf ファイルの VirtualHost セクションで行います。リリース 9.0.2 のインストーラでは、httpd.conf ファイルの VirtualHost セクションで SSL 仮想ホストを定義します。どちらのファイルも \$ORACLE_HOME/Apache/Apache/conf に格納されています。
3. SSL サイトにパートナ・アプリケーションを作成します。

- a. 中間層の Oracle ホームが正しいパスで設定されていることを確認します。

* UNIX:

```
setenv LD_LIBRARY_PATH ${LD_LIBRARY_PATH}:%ORACLE_HOME/lib
```

* Windows NT/2000:

```
set PATH=%PATH%;%ORACLE_HOME%\bin;%ORACLE_HOME%\lib
```

- b. リリース 9.0.4 の中間層では、次のコマンドを実行します。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path $ORACLE_HOME
-site_name app.mydomain.com
-config_mod_osso TRUE
-mod_osso_url https://app.mydomain.com:4443
-u root
-virtualhost
-config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
```

- c. リリース 9.0.2 の中間層では、\$ORACLE_HOME/Apache/Apache/conf に移動して、次のコマンドを実行します。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-virtualhost
-site_name https://app.mydomain.com
-oracle_home_path $ORACLE_HOME
-success_url https://app.mydomain.com:4443/osso_login_success
-logout_url https://app.mydomain.com:4443/osso_logout_success
-cancel_url https://app.mydomain.com:4443/
-home_url https://app.mydomain.com:4443/
-config_mod_osso TRUE
-u root
-sso_server_version v1.2
-config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
```

4. `$ORACLE_HOME/Apache/Apache/conf` にある `mod_osso.conf` ファイルに移動します。このファイルを開いたら、次の行をコメントアウトします。

```
LoadModule osso_module libexec/mod_osso.so
```

5. `httpd.conf` で、`LoadModule wchandshake_module libexec/mod_wchandshake.so with a default setup` の真下に次のディレクティブを追加します。

```
LoadModule osso_module libexec/mod_osso.so
```

6. 仮想ホストの `osso.conf` ファイルが追加されるように `VirtualHost` を更新します。SSL 仮想ホストのこのディレクティブは、リリース 9.0.4 では `ssl.conf` に、リリース 9.0.2 では `httpd.conf` に構成されることに注意してください。デフォルトの `osso.conf` ファイルと競合しないよう、ファイル `osso-https.conf` に名前を付けます。

```
<VirtualHost _default_:4443>
.
.
.
OssoConfigFile $ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
OssoIpCheck off
<Location /your_protected_url_for_the_virtual_site>
    AuthType basic
    Require valid-user
</Location>
.
.
.
</VirtualHost>
```

7. アプリケーション中間層で Oracle HTTP Server を再起動します。手順については、第 2 章の「[Oracle HTTP Server の停止と起動](#)」の項を参照してください。
8. SSL と非 SSL サイトの両方をテストします。

外部アプリケーションの設定と管理

この章では、外部アプリケーションをシングル・サインオン対応に構成する方法について説明します。通常、これらのアプリケーションは、Single Sign-On Server に認証を委譲するように変更できない古い Web アプリケーションです。そのため、これらのアプリケーションはレガシー・アプリケーションとも呼ばれます。これらのアプリケーションの定義の詳細は、第 1 章の「[外部アプリケーション](#)」の項を参照してください。

この章の項目は次のとおりです。

- [インタフェースを使用した外部アプリケーションの配置と管理](#)
- [Basic 認証アプリケーションのプロキシ認証](#)

インタフェースを使用した外部アプリケーションの配置と管理

外部アプリケーションを追加、編集または削除するには、「SSO Server 管理」ページのリンクから、「外部アプリケーションの管理」ページにアクセスします。追加した外部アプリケーションは、OracleAS Portal の「外部アプリケーション」ポートレットでアクセスできます。

この項の項目は次のとおりです。

- 外部アプリケーションの追加
- 外部アプリケーションの編集
- [Single Sign-On データベースへの外部アプリケーション証明書の格納](#)

外部アプリケーションの追加

「外部アプリケーションの追加」リンクをクリックすると、「外部アプリケーションの作成」ページが表示されます。このページには、次のヘッダーとフィールドが含まれています。

表 5-1 外部アプリケーション・ログイン

フィールド	説明
アプリケーション名	外部アプリケーションを識別する名前を入力します。この名前は、外部アプリケーションのデフォルト名になります。
ログイン URL	外部アプリケーションの HTML ログイン・ページを認証する送信先 URL を入力します。たとえば、Yahoo! Mail のログイン URL は、次のようになります。 <code>http://login.yahoo.com/config/login?6p4f5s403j3h0</code>
ユーザー名 /ID フィールド名	外部アプリケーションの HTML ログイン・フォームのユーザー名またはユーザー ID フィールドを識別する文字列を入力します。この文字列は、フォームの HTML ソースを表示するときに使用されます（後続の手順に続く例を参照）。このフィールドは、Basic 認証を使用している場合は適用できません。
パスワード・フィールド名	アプリケーションの HTML ログイン・フォームのパスワード・フィールドを識別する文字列を入力します。この文字列は、フォームの HTML ソースを表示するときに使用されます（後続の手順に続く例を参照）。このフィールドは、Basic 認証を使用している場合は適用できません。

表 5-2 認証方式

フィールド	説明
使用する認証タイプ	<p>プルダウン・メニューから、アプリケーションで使用するフォーム送信方法を選択します。これによって、ブラウザからメッセージ・データを送信する方法が決まります。この文字列は、ログイン・フォームの HTML ソースを表示するときに使用されます。次の3つの方法の1つを選択します。</p> <p>POST: Single Sign-On Server にデータを転送して、フォーム本体内のログイン資格証明を送信します。</p> <p>GET: サーバーにページ・リクエストを提示して、ログイン URL の一部としてログイン証明書を送信します。</p> <p>BASIC AUTHENTICATION: アプリケーション URL 内のログイン資格証明を送信します。この送信は、HTTP Basic 認証で保護されます。</p>

表 5-3 追加フィールド

フィールド	説明
フィールド名	ログイン時にユーザー入力を要求するフィールドを HTML ログイン・フォームに追加した場合は、そのフィールドの名前を入力します。このフィールドは、Basic 認証を使用している場合は適用できません。
フィールド値	対応するフィールド名のデフォルト値を入力します（該当する場合）。このフィールドは、Basic 認証を使用している場合は適用できません。

外部アプリケーションを追加する手順は次のとおりです。

1. 「外部アプリケーションの管理」 ページから、「外部アプリケーションの追加」を選択します。
「外部アプリケーションの作成」 ページが表示されます。
2. 「外部アプリケーション・ログイン」 フィールドに、外部アプリケーション名と HTML ログイン・フォームの送信先 URL を入力します。Basic 認証を使用する場合は、保護された URL を入力します。
3. アプリケーションで HTTP POST 認証または HTTP GET 認証が使用されている場合は、「ユーザー名 /ID フィールド名」 フィールドに、HTML ログイン・フォームのユーザー名またはユーザー ID フィールドを識別する文字列を入力します。この名前は、ログイン・フォームの HTML ソースを表示するときに使用されます。
アプリケーションで Basic 認証方式が使用されている場合は、「ユーザー名 /ID フィールド名」 フィールドを空にします。

4. アプリケーションで HTTP POST 認証または HTTP GET 認証が使用されている場合は、「パスワード・フィールド名」フィールドに、アプリケーションのパスワード・フィールドを識別する文字列を入力します。ログイン・フォームの HTML ソースを参照してください。

アプリケーションで Basic 認証方式が使用されている場合は、「パスワード・フィールド名」フィールドを空にします。

5. ログイン時にユーザー入力を要求するフィールドを HTML ログイン・フォームに追加した場合は、「追加フィールド」フィールドに、そのフィールドの名前とデフォルト値を入力します。

アプリケーションで Basic 認証方式が使用されている場合は、このフィールドを空にします。

6. HTML ログイン・フォームでユーザーが追加フィールドのデフォルト値を変更できるようにする場合は、「ユーザーに表示」チェック・ボックスを選択します。
7. 「OK」をクリックします。新しい外部アプリケーションが、「外部アプリケーションの管理」ページの「外部アプリケーションの編集 / 削除」ヘッダーの下に、その他の外部アプリケーションとともに表示されます。
8. アプリケーションのリンクをクリックして、ログインをテストします。

次の例は、Yahoo! Mail で使用される値のソースです。

```
<form method=post action="http://login.yahoo.com/config/login?6p4f5s403j3h0"
autocomplete=off name=a>
...
<td><input name=login size=20 maxlength=32></td>
....
<td><input name=passwd type=password size=20 maxlength=32></td>
...
<input type=checkbox name=".persistent" value="Y" >Remember my ID & password
...
</form>
```

このソースでは、次の要素の値を指定しています。

- ログイン URL:
http://login.yahoo.com/config/login?6p4f5s403j3h0
- ユーザー名 /ID フィールド名 : login
- パスワード・フィールド名 : passwd
- 使用する認証タイプ : POST
- フィールド名 : .persistent Y
- フィールド値 : [off]

外部アプリケーションの編集

アプリケーションの横にある鉛筆アイコンをクリックすると、「外部アプリケーションの編集」ページが表示されます。ここで、アプリケーションを追加したときに入力した値を編集できます。編集が終了したら、次の操作を行います。

「適用」をクリックして変更を入力し、再度ページを表示して、更新した値を確認します。

Single Sign-On データベースへの外部アプリケーション証明書の格納

ユーザーがアプリケーションにログインするたびに、それぞれの外部アプリケーションでは、ユーザー名とパスワードの受信を待機しています。これらのアプリケーションへのシングル・サインオンを有効にするには、ログイン時に、資格証明を Single Sign-On データベースに保存するように指定できます。

Single Sign-On ユーザーが初めて外部アプリケーションにログインすると、「外部アプリケーション・ログイン」ページが表示されます。資格証明書を入力した後、「このアプリケーションのログイン情報を保存する」チェック・ボックスを選択できます。このオプションを選択すると、次回アプリケーションにアクセスするときは、Single Sign-On Server がログインを代行します。

図 5-1 は、「外部アプリケーション・ログイン」ページを再現したものです。

図 5-1 「外部アプリケーション・ログイン」ページ

The screenshot shows a web browser window titled "Login - My.Oracle.Com". The page content includes:

- A blue header bar with the text "Login - My.Oracle.Com" and a question mark icon on the right.
- Two buttons: "Login" and "Close".
- A section titled "External Application Login".
- Text: "Enter your user name (or other form of application identification) and password for this application. You may also enter custom values for any additional login parameters shown. The SSO Server uses this information to login on your behalf. If you click Remember My Login Information For This Application, you will then be logged in automatically each time you access this application."
- Form fields: "Application Name: My.Oracle.Com", "User Name/ID", and "Password".
- A checkbox labeled "Remember My Login Information For This Application" which is checked.
- Two buttons: "Login" and "Close" at the bottom right.
- Footer text: "Copyright© 2003, Oracle. All Rights Reserved".

注意： パスワードを変更した場合、「外部アプリケーション・ログイン」ページのパスワードも更新する必要があります。更新しないと、ログインしようとしたときに、このページからエラー・メッセージが返されます。

Basic 認証アプリケーションのプロキシ認証

シングル・サインオン対応の外部アプリケーションには、SDK 対応パートナー・アプリケーションである OracleAS Portal の「外部アプリケーション」ポートレットを使用してアクセスするのが一般的です。この方法でアクセスするアプリケーションには、GET 認証、POST 認証または Basic 認証を構成できます。

これに代わるものとして、別の Web サーバーにあるアプリケーションへのセキュアなプロキシとして Oracle HTTP Server を使用する方法があります。この方法では、モジュール `mod_osso` と `mod_proxy` を設定してシングル・サインオン対応の Basic 認証をサポートする必要があります。プロキシ認証の利点は、標準の方法で外部アプリケーションにアクセスしたときに発生する短時間の画面のちらつきがなくなることです。

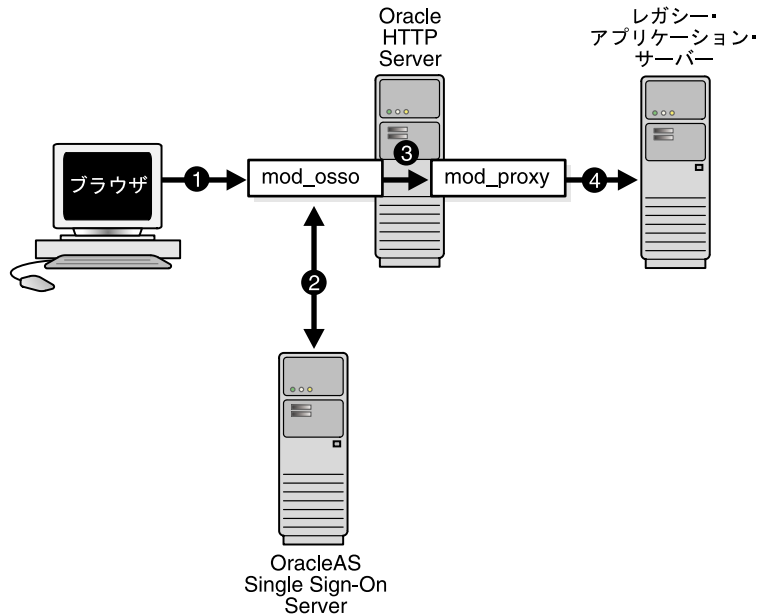
この項の項目は次のとおりです。

- [Basic 認証のプロキシとしての Oracle HTTP Server の設定](#)
- [構成の要件](#)
- [構成手順](#)

Basic 認証のプロキシとしての Oracle HTTP Server の設定

適切に構成された `mod_osso` 対応の外部アプリケーションの認証は、パートナー・アプリケーションの認証と類似しています。すなわち、`mod_osso` は URL リクエストを取得して Single Sign-On Server にリダイレクトします。図 5-2 に、このプロセスを示します。

図 5-2 mod_osso/mod_proxy を使用した認証の流れ



1. Single Sign-On ユーザーは、ブックマークを選択するか仮想 URL を入力して外部アプリケーションをリクエストします。この仮想 URL によって、Oracle HTTP Server はリクエストを取得できます。
2. mod_osso は、取得したリクエストに認証ヘッダーを追加して、Single Sign-On Server からユーザーの資格証明を取得します。
3. mod_osso は、Single Sign-On Server から取得したユーザーの資格証明でヘッダー値を設定し、このヘッダー値を mod_proxy に渡します。
4. mod_proxy は、ユーザーの資格証明を Basic 認証ヘッダーのフォームで実 URL に渡します。この転送は、仮想 URL を実 URL にマップするディレクティブによって行われます。

構成の要件

Oracle HTTP Server でレガシー・アプリケーションの Basic 認証を構成するには、次の条件を満たす必要があります。

- プロキシ処理を使用するアプリケーションは、Basic 認証アプリケーションとして Single Sign-On Server に登録する必要があります。詳細は、「[外部アプリケーションの追加](#)」の項を参照してください。
- Oracle HTTP Server に `mod_osso` をインストールして有効にする必要があります。
- Oracle HTTP Server にデフォルトの `mod_proxy` をインストールして有効にする必要があります。
- 外部アプリケーションをホストする Web サーバーで Oracle HTTP Server がプロキシとして使用されている場合、その Web サーバーでは `mod_osso` を有効にできません。

構成手順

Oracle HTTP Server で外部アプリケーションの Basic 認証を構成するには、次のセクションを `mod_osso.conf` に追加します。

```
<IfModule mod_proxy.c>
<Location /application_virtual_path>
    require valid user
    AuthType Basic
    OsoLegacyApp on | off
</Location>

ProxyPass /application_virtual_path/ http://host:port/application_real_path/
ProxyPassReverse /application_virtual_path/ http://host:port/application_real_path/
</IfModule>
```

`OsoLegacyApp` ディレクティブは、保護された URL がレガシー・アプリケーションであるかどうかを示します。このディレクティブが見つからないか `off` に設定されている場合は、アプリケーションのユーザー名とパスワードを Single Sign-On データベースから取得するコードは実行されません。2つの `mod_proxy` ディレクティブ `ProxyPass` と `ProxyPassReverse` によって、仮想 URL が実 URL にマップされます。

次の行を `httpd.conf` に追加します。

```
Listen 5000
```

このパラメータは、非 SSL ポート 5000 を使用して外部アプリケーションに関する情報にアクセスするように `mod_osso` に指定します。

注意：

- 仮想 URL のディレクトリを指定する必要はありません。便宜上、この URL はアプリケーション名のみで構成できます。
 - SSL が有効な場合は、アプリケーションの実 URL の http を https に置き換えます。
-
-

6

マルチレベル認証

この章では、各種のパートナ・アプリケーションに異なる認証レベルを割り当てるシングル・サインオン・システムの構成方法について説明します。このシステムでは、リクエストされたアプリケーションのセキュリティ・レベルに認証動作を合せることができます。

この章の項目は次のとおりです。

- [マルチレベル認証とは](#)
- [マルチレベル認証の仕組み](#)
- [マルチレベル・システムのコンポーネント](#)
- [マルチレベル認証の構成](#)

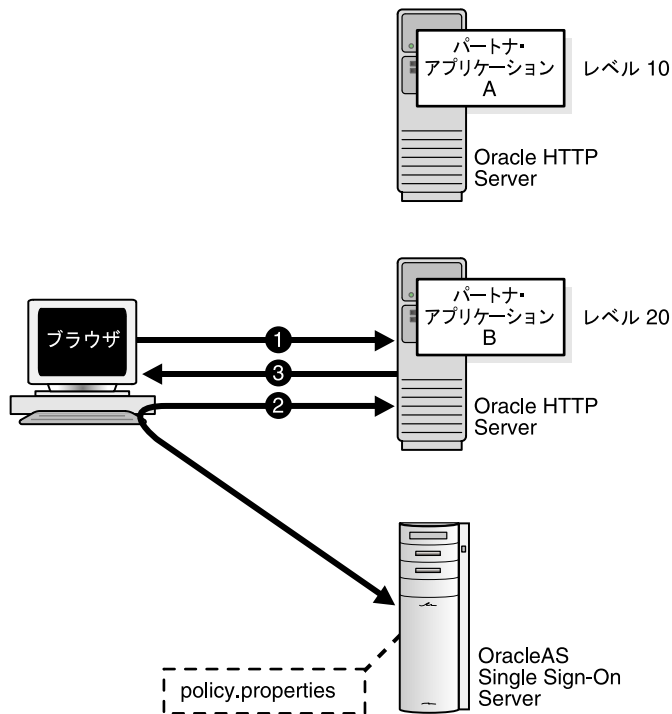
マルチレベル認証とは

OracleAS Single Sign-On では、保護するアプリケーションに異なる認証レベルを割り当てることができます。次に、これらの認証レベルを特定の認証プラグインにマップできます。たとえば、セキュリティが重視されるアプリケーションではユーザー証明書を要求するように構成し、セキュリティがさほど重要でないアプリケーションではユーザー名とパスワードを要求するように構成することもできます。

マルチレベル認証の仕組み

6-2 ページの図 6-1 にマルチレベル認証の仕組みを示します。

図 6-1 マルチレベル認証の流れ



1. ユーザーは、アプリケーション A ですでに認証されています。このユーザーは、次にアプリケーション B に移動します。
2. アプリケーション B は、このユーザーを Single Sign-On Server にリダイレクトします。
3. アプリケーション B の認証レベルはアプリケーション A よりも高いため、このユーザーは、より高いレベルの資格証明による再認証を Single Sign-On Server から要求されます。

注意： リリース 9.0.4 では、認証はパートナ・アプリケーションのルート・レベルで行われます。ルートの下 URL に認証レベルを割り当てることはできません。

マルチレベル・システムのコンポーネント

次の項目は、マルチレベル認証の仕組みを理解するためのキー・ポイントです。

- [認証レベル](#)
- [認証プラグイン](#)

認証レベル

認証レベルは、アプリケーションに特定の認証動作を指定するためのパラメータです。policy.properties ファイルを使用すると、パラメータを構成する認証レベルの名前と値を設定できます。このファイルは \$ORACLE_HOME/sso/conf に格納されています。[付録 C](#) にこのファイルのコピーがあります。

[表 6-1](#) に認証レベルの例を示します。これらの認証レベルは、ユーザーの配置要件に合わせてカスタマイズおよび追加できます。

表 6-1 デフォルトの認証レベル

認証レベル名	認証レベル値
LowSecurity	20
LowMediumSecurity	30
MediumSecurity	40
MediumHighSecurity	50
HighSecurity	60

認証レベル名は一意にする必要があります。たとえば、NoSecurity=10 と NoSecurity=20 の両方を含むシステムは認められません。認証レベルの数値が低くなるほどセキュリティ・レベルも低くなります。

ユーザーが MediumHighSecurity などの高いレベルでログインし、低いレベルのアプリケーションにアクセスしようとする場合は、資格証明を再度要求されません。反対に、ユーザーが LowMediumSecurity などの低いレベルのアプリケーションでログインし、高いレベルのアプリケーションにアクセスしようとする、必要なレベルを要求されます。

認証プラグイン

認証プラグインは、特定の認証方式を実装したものです。この方式によってユーザーの資格証明が収集され、ユーザーが認証されます。

前項で説明した認証レベルのいずれかと、次の箇条書きに示す認証方式のいずれかを組み合わせることができます。認証プラグインがマップする認証レベルは配置固有です。この組み合わせを実現するには `policy.properties` を使用します。

- パスワード認証
デフォルトの標準方式です。
- デジタル証明書
証明書による認証の詳細は、第 7 章を参照してください。
- Windows ネイティブ認証
このタイプの認証の詳細は、第 8 章を参照してください。
- サードパーティのアクセス管理
第 13 章を参照してください。

マルチレベル認証の構成

特定の認証レベルが構成されていないアプリケーションは、デフォルトでパスワード認証が構成され、MediumSecurity の認証レベルが割り当てられます。異なる認証レベルが必要な場合は、policy.properties を変更する必要があります。次の構成例を指針として使用してください。

使用例

この使用例では、架空の2つのパートナ・アプリケーションで異なる認証レベルとプラグインを使用するように構成する方法について説明します。ここでは、次の条件を前提としています。

- アプリケーション pa1 はホスト pa1.mydomain.com に配置されています。pa1 はポート 7777 をリスニングします。
- pa1 は、Single Sign-On Server にすでに登録されています。
- pa1 では、証明書による認証を使用する必要があります。
- アプリケーション pa2 はホスト pa2.mydomain.com に配置されています。pa2 はポート 7777 をリスニングします。
- pa2 は、Single Sign-On Server にすでに登録されています。
- pa2 では、パスワード認証を使用する必要があります。

構成手順

次の構成を使用して policy.properties を変更します。

1. 認証レベルの名前を policy.properties ファイルから選択します。必要な場合は、新しい認証レベルと対応する名前をこのファイルに追加します。
2. 2つのパートナ・アプリケーションのルート URL に、認証レベルを次のように割り当てます。

```
pa1.mydomain.com¥:7777 = HighSecurity  
pa2.mydomain.com¥:7777 = MediumSecurity
```

注意： ドメイン名の後に円記号を挿入してください。

- 手順 1 で割り当てた認証レベル名に、認証プラグインを次のように割り当てます。

```
HighSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOX509CertAuth  
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerAuth
```

認証プラグイン名は、手順 1 で割り当てた認証レベル名と接頭辞 `_AuthPlugin` を連結したものです。

- `policy.properties` を保存し、シングル・サインオン中間層を再起動します。詳細は、「[\[OC4\]_SECURITY インスタンスの停止と起動](#)」の項を参照してください。
- パートナ・アプリケーションをテストします。

デジタル証明書を使用したサインオン

X.509 クライアント証明書を使用したシングル・サインオンでは、セキュリティ・レベルが簡易認証よりも強化されます。パートナ・アプリケーションでは、Single Sign-On Server が PKI に対応しているとき、デフォルトで PKI を使用できるという利点があります。

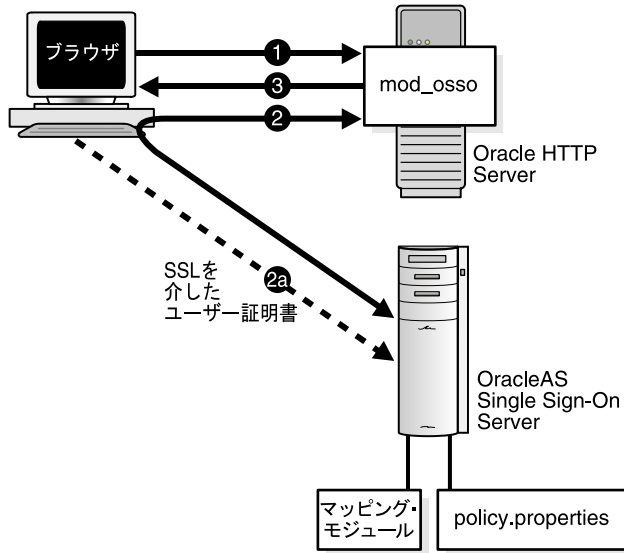
この章の項目は次のとおりです。

- [証明書を使用した認証の仕組み](#)
- [システム要件](#)
- [証明書用のシングル・サインオン・システムの構成](#)
- [証明書失効リストのメンテナンス](#)

証明書を使用した認証の仕組み

図 7-1 に、証明書を使用したシングル・サインオンでの認証の流れを示します。

図 7-1 証明書を使用したシングル・サインオン



1. ユーザーは、パートナ・アプリケーションにアクセスします。
2. パートナ・アプリケーションは、認証のためにユーザーを Single Sign-On Server にリダイレクトします。このリダイレクションにおいて、ユーザーの証明書が Single Sign-On Server のログイン URL に送信されます (2a)。証明書が検証されると、Single Sign-On Server はリクエストされたアプリケーションをユーザーに返します。
3. アプリケーションはコンテンツを配信します。

注意： ブラウザが証明書ストアのパスワードを要求するように構成されている場合、その構成方法によっては、パスワードを一度入力するだけでよい場合があります。ログアウトしてからパートナ・アプリケーションにアクセスしようとする、ユーザーの証明書がブラウザから Single Sign-On Server に自動的に転送されます。つまり、実際にはログアウトしていないこととなります。正式にログアウトするには、ブラウザを閉じる必要があります。

システム要件

証明書を使用したシングル・サインオンを行うには、次の条件を満たしている必要があります。

- Single Sign-On Server と Oracle Internet Directory がインストールされていること。
- Oracle HTTP Server に、有効なサーバー証明書がインストールされていること。
- クライアント証明書の識別名が選択され、次の2つの条件のいずれかを満たしていること。
 - ユーザー証明書の識別名が Oracle Internet Directory のユーザーの識別名と同じである
 - ユーザー証明書の識別名にユーザー・ニックネームと、ユーザーが属するレルムの名前（オプション）が含まれている
- クライアント証明書発行者の証明書が、信頼できる証明書として Single Sign-On Server にインストールされていること。
- サーバー証明書発行者の証明書が、信頼できる証明書としてユーザーのブラウザにインストールされていること。

証明書用のシングル・サインオン・システムの構成

証明書を使用したシングル・サインオンは OracleAS のデフォルト・オプションではないので、手動で構成する必要があります。証明書による認証を構成するには、事前にシングル・サインオン・システムで SSL を使用可能にする必要があります。第9章の「[SSLの有効化](#)」の作業を実行してからこの項に戻り、証明書用に次のコンポーネントを構成します。

- [Oracle HTTP Server](#)
- [Single Sign-On Server](#)
- [Oracle Internet Directory](#)

Oracle HTTP Server

Oracle HTTP Server を証明書用に構成するには、`ssl.conf` ファイルにパラメータを追加します。さらに、任意でサーバーおよびユーザー証明書を発行する認証局を選択します。

SSL パラメータの構成

必要な SSL パラメータを構成する手順は次のとおりです。

1. `$ORACLE_HOME/Apache/Apache/conf` にある `ssl.conf` に移動します。
2. `ssl.conf` ファイルの SSL Virtual Host Context セクションに、表 7-1 に示すパラメータを追加するか編集します。同時に、`SSLEngine` パラメータが `on` に構成されているのを確認します。これは、SSL 用の Oracle HTTP Server の構成で設定されているはずですが。

表 7-1 証明書を使用したシングル・サインオンの構成時に使用する HTTP パラメータ

パラメータ	説明
<code>SSLWallet</code>	<p>サーバーの Wallet の場所（パス）。デフォルトの場所は、<code>\$ORACLE_HOME/Apache/Apache/conf/ssl.wlt/default</code> です。</p> <p>注意：</p> <p>Oracle ホームの実際の格納場所に変数を置き換えてください。</p> <p>OracleAS Certificate Authority が OracleAS Single Sign-On と同じ Oracle ホームにインストールされ、この認証局を使用して証明書を発行する場合、Wallet の場所は <code>\$ORACLE_HOME/oca/wallet/ssl</code> になります。</p> <p>詳細は、「認証局の選択」の項を参照してください。</p>
<code>SSLWalletPassword</code>	サーバーの Wallet のパスワード。
<code>SSLVerifyClient</code>	<p>クライアント証明書の検証タイプ。次の3つのタイプがあります。</p> <ul style="list-style-type: none"> ■ <code>none</code>: 証明書のない SSL ■ <code>optional</code>: サーバー証明書のみ ■ <code>require</code>: サーバー証明書およびクライアント証明書 <p><code>optional</code> または <code>require</code> を選択する必要があります。</p>

認証局の選択

OracleAS Certificate Authority がインストール済で、この認証局を使用して証明書を発行する場合は、目的の Oracle 認証局 Wallet を指定するように `ssl.conf` を編集します。Wallet は、表 7-1 に示す Oracle 認証局 Wallet を使用するか、Single Sign-On Server 専用の Wallet を Oracle 認証局で発行します。前者の場合は、`$ORACLE_HOME/oca/wallet/ssl` にある Wallet を `$ORACLE_HOME/Apache/Apache/conf/ssl.wlt/default` にコピーします。後者の場合は、『Oracle Application Server Certificate Authority 管理者ガイド』の第 7 章の操作手順を参照してください。該当する項は「[サーバー / 下位 CA 証明書] タブ」です。この項は、「[ユーザー証明書] タブ」に含まれている項です。Wallet を取得したら、その Wallet の場所を指すように `ssl.conf` を編集します。

第三者の認証局も使用することができます。この場合も、表 7-1 の説明のとおり `ssl.conf` を編集して Wallet の場所を指定する必要があります。

OracleAS Certificate Authority と OracleAS Single Sign-On を併用すると、証明書プロビジョニング・プロセスが単純になります。Oracle 認証局は、Oracle 認証局の UI の URL をシングル・サイン・オン・ユーザーにブロードキャストするように構成できます。ユーザーは、このリンクを使用してシングル・サインオンの証明書を要求できます。この証明書は、Oracle Internet Directory のユーザー・エントリに自動的にリンクされます。

Single Sign-On Server

証明書を受け入れるように Single Sign-On Server を構成するには、次の作業が必要です。

- クライアント証明書のパラメータを受信するためのサーバー構成
- デフォルトの認証プラグインによる `policy.properties` の構成
- 認証プラグインの構成ファイルの変更 (オプション)
- ユーザー名マッピング・モジュールのカスタマイズ (オプション)
- シングル・サインオン中間層の再起動

少なくとも最初の 2 つの作業は行う必要があります。ユーザー名マッピング・モジュールをカスタマイズする場合は、他の 2 つの作業も行います。ユーザー名マッピングのデフォルト・モジュールでは、クライアント証明書の識別名 (DN) が Oracle Internet Directory の Single Sign-On ユーザーと照合されます。デフォルトの実装では、ディレクトリ内にあるユーザーの識別名と証明書の識別名が同じであると想定しています。Oracle Internet Directory のユーザー名に証明書の識別名のフィールドをマップするモジュールも使用できます。識別名マッピング・モジュールのかわりにこのモジュールを使用する場合は、3 番目の作業の指示に従って `CertificateMappingModule` パラメータを変更します。

クライアント証明書のパラメータを受信するためのサーバー構成

1. \$ORACLE_HOME/sso/conf にある sso_apache.conf ファイルの末尾に次の行を追加します。

```
#Allow single sign-On server to receive client certificate parameters
<IfModule mod_oss1.c>
    Oc4jExtractSSL on
    <Location /sso>
        SSLOptions +ExportCertData +StdEnvVars
    </Location>
</IfModule>
```

2. \$ORACLE_HOME/j2ee/OC4J_SECURITY/application-deployments/sso/web にある orion-web.xml ファイルに次のタグを追加します。

```
<jazn-web-app runas-mode="true" />
```

このタグは </orion-web-app> の前に挿入します。次の例は、タグが正しく挿入された orion-web.xml ファイルを示しています。

```
<?xml version="1.0"?>
<!DOCTYPE orion-web-app PUBLIC "-//ORACLE//DTD OC4J Web Application 9.04//EN"
"http://xmlns.oracle.com/ias/dtds/orion-web-9_04.dtd">

<orion-web-app
    deployment-version="9.0.4.0.0"
    jsp-cache-directory="/persistence"
    temporary-directory="/temp"
>
<!--
Uncomment this element to control web application class loader behavior.
<web-app-class-loader search-local-classes-first="true"
include-war-manifest-class-path="true"/>
-->
<jazn-web-app runas-mode="true" />
</orion-web-app>
```

デフォルトの認証プラグインによる policy.properties の構成

適切な証明書サインオンの認証レベルで policy.properties ファイルの DefaultAuthLevel セクションを更新します。このファイルは \$ORACLE_HOME/sso/conf にあります。デフォルトの認証レベルを次の値に設定します。

```
DefaultAuthLevel = MediumHighSecurity
```

次に、Authentication plugins セクションで、デフォルトの認証プラグインを組み合わせます。

```
MediumHighSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOX509CertAuth
```

便宜上、policy.properties は付録 C 「policy.properties」にも添付されています。

認証プラグインの構成ファイルの変更（オプション）

X509CertAuth.properties ファイルには次のパラメータがあります。このファイルのパスは \$ORACLE_HOME/sso/conf です（DN ベースのマッピング・モジュールを使用する場合は、この手順を省略してください）。

CertificateMappingModule このパラメータは、ユーザー名マッピングを実行するクラス・ファイル名に構成します。このパラメータには、次の 2 つのデフォルト値のいずれかを指定します。

```
oracle.security.sso.server.auth.SSOCertMapperDn
```

または

```
oracle.security.sso.server.auth.SSOCertMapperNickname
```

最初のモジュールでは、ディレクトリ内にあるユーザーの識別名と証明書の識別名が同じであることを前提としています。このモジュールは、そのまま使用できるデフォルト設定です。2 番目のモジュールでは、ユーザー証明書の識別名の最初の cn 値が Oracle Internet Directory のデフォルト・レルムのユーザー・ニックネームであることを前提としています。これらのモジュールのかわりに独自のモジュールを使用する場合は、パラメータに実装するクラス・ファイル名を設定します。

CheckUserCertificate このパラメータは、ユーザー証明書を Oracle Internet Directory で検証するかどうかを指定します。デフォルト値は TRUE です。Oracle HTTP Server の SSL 保護で十分な場合は、このパラメータを FALSE に設定します。

CertificateAuthFailureUrl 証明書による認証に失敗すると、この URL にリダイレクトされ、エラー・メッセージが表示されます。

CertificateAuthFallback 有効な証明書なしにログインしようとしているユーザーに、パスワード認証を使用させる場合は、このパラメータを **TRUE** に設定します。リリース 9.0.2 では、デフォルトでこのフォールバックが実行されます。リリース 9.0.4 では、フォールバックを有効にする必要があります。このパラメータを **FALSE** に設定したり、空の状態にした場合、ユーザーには有効な証明書を要求するメッセージが表示されます。CertificateAuthFallback をファイルに追加する必要がある場合は、次のようにファイルの末尾に追加します。

```
#Allow authentication fallback
CertificateAuthFallback=true
```

注意： CertificateAuthFallback を TRUE に設定した場合、マルチレベル認証は使用できません。

ユーザー名マッピング・モジュールのカスタマイズ（オプション）

ユーザー名マッピング・モジュールをカスタマイズするには、oracle.security.sso.ias904.toolkit.IPASUserMappingInterface に基づくマッピング・モジュールを実装します。このリリースに添付されているサンプル・マッピング・モジュールを参照してください。このサンプル・マッピング・モジュールには、SSOCertMapperDN.java と SSOCertMapperNickname.java があります（独自のマッピング・モジュールを記述しない場合は、この手順を省略してください）。

サンプル・モジュールは次のクラスで構成されています。

- マッピング・モジュール・インタフェース

このインタフェースには、次のメソッドが組み込まれています。

```
public IPASUserInfo getUserInfo(
    javax.servlet.http.HttpServletRequest request)
    throws IPASException;
```


- ユーザー情報クラス

このクラスには、ユーザー・ニックネームやユーザー識別情報などのユーザー情報が格納されています。パッケージ名は、`oracle.security.sso.ias904.toolkit.IPASUserInfo` です。コンストラクタは次のとおりです。

```
Public IPASUserInfo(
    String userNickName
    String realmNickname)
```

```
Public IPASUserInfo(
    String userNickName,
    String userDN,
    String userGUID,
    String realmNickname,
    String realmDN,
    String realmGUID)
```

- 例外クラス

ユーザー名マッピングで問題が発生すると、この例外が生成されます。クラス名は `oracle.security.sso.ias904.toolkit.IPASException` です。スーパー・クラスは `java.lang.Exception` です。コンストラクタは次のとおりです。

```
public IPASException()
public IPASException(String Message)
```

1. サンプル・モジュールを格納したファイル `ipassample.jar` を抽出します。第2章の「[サンプル・ファイルの取得](#)」の項を参照してください。

2. 次のインタフェースを実装する Java クラスを作成します。

```
oracle.security.sso.ias904.toolkit.IPASUserMappingInterface
```

3. 次のカスタム実装をコンパイルします。

```
$ORACLE_HOME/jdk/bin/javac -classpath $ORACLE_HOME/sso/lib/
ipastoolkit.jar:$ORACLE_HOME/lib/servlet.jar -d $ORACLE_HOME/
sso/plugin java_file_name -d class_directory
```

4. クラス・ファイルを JAR ファイル化して `$ORACLE_HOME/sso/plugin` に配置します。

```
$ORACLE_HOME/jdk/bin/jar -cvf $ORACLE_HOME/sso/plugin/CertMapImpl.jar -C class_
directory
```

この手順では、プラグイン・ディレクトリに個別のクラス・ファイルがなく、クラス・ファイルが重複する可能性のある状況を想定しています。

5. `x509CertAuth.properties` を実装内容で更新します。「[認証プラグインの構成ファイルの変更 \(オプション\)](#)」の項を参照してください。

シングル・サインオン中間層の再起動

サーバーを構成したら、中間層を再起動します。「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

Oracle Internet Directory

証明書による認証を正しく行うには、ユーザー証明書が Oracle Internet Directory にあることが必要です。証明書が OracleAS Certificate Authority によって発行されている場合、その証明書は Oracle Internet Directory で自動的に公開されます。証明書が社内の認証局によって発行されている場合も同様です。証明書の発行者が第三者の認証局である場合は、セルフサービス・アプリケーションでこの機能を実現できます。また、ディレクトリ管理者は、コマンドライン・ツールの `ldapmodify` を使用して証明書を LDIF ファイルとしてディレクトリに追加できます。

`ldapmodify` を使用して証明書を公開する場合は、ツールを実行する前に、環境に合わせて適切なグローバル変数・サポート変数を設定します。次に例を示します。

- UNIX:

```
setenv NLS_LANG AMERICAN_AMERICA.UTF8
```

- Windows NT/2000:

```
set NLS_LANG=AMERICAN_AMERICA.UTF8
```

UNIX では、`csh` または `tcsh` 以外のシェルを使用している場合、別の手順でこの変数を設定する必要があります。

`ldapmodify` は `$ORACLE_HOME/bin` に格納されています。このツールの構文は次のとおりです。

```
ldapmodify -h host -p port -D "directory_administrator" -w password -f file_name.ldif
```

次に示すサンプルの LDIF ファイルでは、ユーザー `jsmith` の証明書はディレクトリでのエントリの属性に従って示されています。属性のタイプは `usercertificate` です。属性値は長精度文字列型で、属性のタイプの後に続きます。

```
dn: cn=jsmith,cn=users,dc=realml,dc=oracle,dc=com
changetype: modify
replace: usercertificate
usercertificate::MIIC3TCCAkYCAgP3MA0GCSqGSIb3DQEBAUAMIG8MQswCQ
YDVOQGEwJVUzETIMBEGA1UECBMKQ2FsaWZvcml5PTEYEXMBUGA1UEBxMOUmVkd29vZCBTaG9yZXMxGzAZBgNV
BAoTEk9yYWNSZSBDb3Jwb3JhdG1vb2FfMB0GA1UECxmWV2ViIFNpbmVzZSBTaWduLU9uL0CBTVDEeMBwGA1
UEAxMVQ2VydG1maWNhYoEHmF4gomt c4mxSKh/ zAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAkwXoCLDRqmK1
Y9LQtIjLnCaIJKUZmS1Qj +bhu/ IHeZLGHg4TJg3O2XVA5u/ VxwjLeGBqLXy2z7o3RuJNKx2CVx6p/ 0Hkjn
w4w6KvAu2hcBgC9m4kzUGhHJ9b65v/ zx7dIUkyJr4RF+1JhJg4/ oYXxLrYHp5NAkHP4htT0gqCXiI=
```

属性値は ASCII 値ではないので、ここで示すように、証明書を BASE64 形式でエンコードする必要があります。他の属性とは異なり、BASE64 属性では区切り記号に二重コロンの (::) を使用します。また、タブを使用すると、BASE64 属性を折り返すことができます。

証明書失効リストのメンテナンス

無効な証明書や期限切れの証明書を使用したユーザーがログインできないようにするため、管理者は Oracle HTTP Server の証明書失効リスト (CRL) を最新の状態に保つ必要があります。証明書を発行した認証局は、このリストを提供する必要があります。リストのメンテナンスには、ca-bundle.crl ファイルを使用できます。CRL ファイルのパスには \$ORACLE_HOME/Apache/Apache/conf を指定する必要があります。

認証にデジタル証明書を使用する OracleAS ユーザーについては、ディレクトリ・エントリの userCertificate 属性を更新できないようにする必要があります。これは、証明書の失効から CRL の更新までの時間が長くなるおそれがあるからです。Oracle Internet Directory では、デフォルトで userCertificate へのユーザー・アクセスが拒否されます。この属性の変更には、Single Sign-On Server、OracleAS Certificate Authority、第三者の認証局など、信頼できるエンティティのみを使用してください。

CRL の実装とメンテナンスの詳細は、ssl.conf ファイルの SSL Virtual Host Context セクションのコメントを参照してください。

Windows ネイティブ認証

この章では、自動サインオン（Windows ネイティブ認証）の OracleAS Single Sign-On を Windows デスクトップから配置する方法について説明します。自動サインオンと Windows ネイティブ認証は同義語です。このマニュアルでは用語として Windows ネイティブ認証を使用します。

この章の項目は次のとおりです。

- [Windows ネイティブ認証の概要](#)
- [Windows ネイティブ認証の仕組み](#)
- [システム要件](#)
- [Windows ネイティブ認証の構成](#)
- [フォールバック認証](#)
- [ログインの例](#)

Windows ネイティブ認証の概要

Windows ネイティブ認証は、Windows 2000 で Internet Explorer を使用するユーザーのための認証方式です。この機能を OracleAS Single Sign-On で使用可能にすると、ユーザーは、Windows 2000 コンピュータへのログイン時に取得される Kerberos 資格証明によって Single Sign-On パートナ・アプリケーションに自動的にアクセスできます。

SPNEGO プロトコルを使用することにより、Kerberos 対応の Web サーバーがユーザーの Kerberos 資格証明を要求するとき、Internet Explorer 5.0 以上のブラウザは資格証明を Web サーバーに自動的に転送できます。これにより、Web サーバーは資格証明を復号化してそのユーザーを認証できます。

SPNEGO は、Kerberos バージョン 5 と NTLM の両方の認証方式をサポートしていますが、OracleAS リリース 9.0.4 は SPNEGO による Kerberos バージョン 5 のみをサポートしていません。

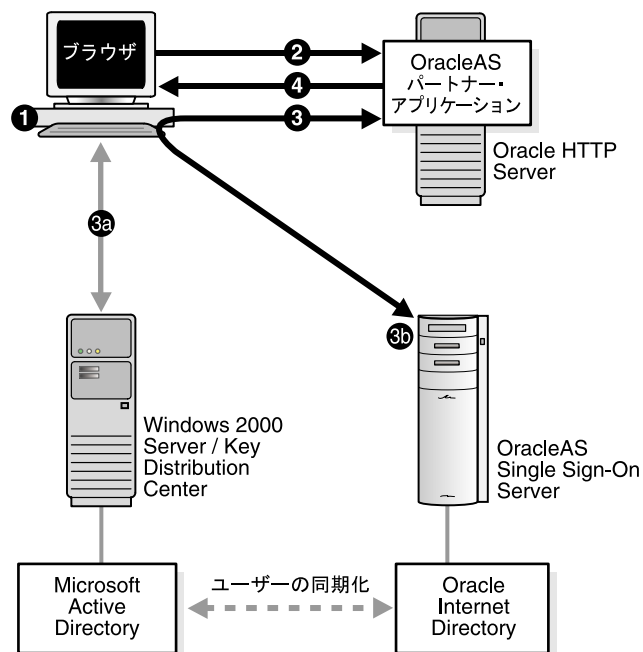
注意： ここでは Windows 2000 についてのみ説明しますが、Windows XP プラットフォームも Windows ネイティブ認証をサポートしています。

Windows ネイティブ認証の仕組み

次の手順は、シングル・サインオンで保護されたアプリケーションにユーザーがアクセスするときのプロセスを示しています (8-3 ページの図 8-1 を参照)。

1. ユーザーは Windows 2000 コンピュータで Kerberos レalm (またはドメイン) にログインします。
2. ユーザーは、Internet Explorer を使用して Single Sign-On パートナ・アプリケーションへのアクセスを試みます。
3. アプリケーションは、ユーザーを認証するために Single Sign-On Server にリダイレクトします。このリダイレクションの一環として、次の操作が行われます。
 - a. ブラウザは、Key Distribution Center (KDC) から Kerberos セッション・チケットを取得します。
 - b. Single Sign-On Server は Kerberos セッション・チケットを検証し、リクエストされた URL をユーザーに返します。
4. このアプリケーションによって、ユーザーの必要とするコンテンツが表示されます。

図 8-1 Windows ネイティブ認証の流れ



ユーザーは、Windows コンピュータからログアウトすることにより、このアプリケーションと後からアクセスした Single Sign-On アプリケーションからログアウトします。

システム要件

Windows ネイティブ認証は、イントラネットの Web アプリケーションを対象にしています。イントラネットでの配置に必要な要素は次のとおりです。

- Microsoft Active Directory を搭載した Windows 2000 Server
- Single Sign-On Server 用に設定した Kerberos サービス・アカウント
- インストール済の OracleAS リリース 9.0.4 Infrastructure

注意： 次の構成は OracleAS Infrastructure を UNIX にインストールすることを前提としていますが、Windows にインストールすることも可能です。

- Kerberos レルム用に構成したシングル・サインオン中間層

- Microsoft Active Directory と Oracle Internet Directory の同期
- Windows 認証プラグイン用に構成した Oracle Internet Directory

Windows ネイティブ認証の構成

Windows ネイティブ認証を設定する際は、Oracle Internet Directory、Single Sign-On Server およびユーザーのブラウザがすべて構成済である必要があります。

次の構成作業を順番に実行します。

- [Microsoft Active Directory](#) が設定済で機能していることの確認
- [Oracle Internet Directory](#) と [OracleAS Single Sign-On](#) のインストール
- [Oracle Internet Directory](#) と [Microsoft Active Directory](#) の同期化
- [Windows 認証プラグイン用の Oracle Internet Directory](#) の構成
- [同期化の確認と認証プラグインが機能していることの確認](#)
- [Single Sign-On Server](#) の構成
- [エンド・ユーザーのブラウザ](#) の構成
- [ローカル・アカウントの再構成](#)

Microsoft Active Directory が設定済で機能していることの確認

Windows 2000 Server のマニュアルを参照し、Microsoft Active Directory が設定されて機能していることを確認します。

Oracle Internet Directory と OracleAS Single Sign-On のインストール

Oracle Internet Directory と OracleAS Single Sign-On をインストールします。インストール環境に適した配置構成を確認するには、[第 9 章「拡張構成」](#)を参照してください。インストール手順については、Oracle Application Server 10g のインストール・ガイドを参照してください。

Oracle Internet Directory と Microsoft Active Directory の同期化

Oracle Internet Directory と Microsoft Active Directory のユーザー・エントリを同期化する必要があります。Oracle Internet Directory と Microsoft Active Directory の同期化については、『Oracle Internet Directory 管理者ガイド』を参照してください。

Windows 認証プラグイン用の Oracle Internet Directory の構成

『Oracle Internet Directory 管理者ガイド』を参照してください。

同期化の確認と認証プラグインが機能していることの確認

2つのディレクトリ間でユーザー・エントリが同期していることを確認します。その後、Windows 認証プラグインが機能していることを確認します。これらは、Single Sign-On Server にログインして試みることで確認できます。

1. ログイン・ページに移動します。

```
http://host:port/pls/orasso
```

2. 次の書式でユーザー名を入力します。

```
user_name@active_directory_domain
```

次にパスワードを入力します。

Single Sign-On Server の構成

次の作業を実行して Single Sign-On Server を構成します。

- Single Sign-On Server の Kerberos サービス・アカウントの設定
- Sun JAAS ログイン・モジュール用の Single Sign-On Server の構成
- 保護されたアプリケーションとしての Single Sign-On Server の構成

Single Sign-On Server の Kerberos サービス・アカウントの設定

シングル・サインオン中間層で Kerberos レalmを構成し、Single Sign-On Server のサービス・アカウントを Microsoft Active Directory で作成します。最後に、Single Sign-On Server の keytab ファイルを作成し、サービス・プリンシパルをアカウント名にマップします。

1. 中間層で `krb5.conf file/etc/krb5/krb5.conf` (Windows の `system_drive:¥krb5¥krb5`) を構成します。この作業を行うには、ファイルの書式を次の例のように更新します。

```
[libdefaults]
default_realm = ADUSERS.ACME.COM
[realms]
ADUSERS.ACME.COM = {
    kdc = kdc.acme.com
}
[domain_realm]
.acme.com = ADUSERS.ACME.COM
```

ADUSERS.ACME.COM は Microsoft Active Directory のデフォルトのレalm、`kdc.acme.com` は KDC のホスト名、`.acme.com` は UNIX コンピュータの DNS ドメイン名です。それぞれのインストール環境に適した値に例の値を置き換えてください。置き換える値は、例の中で太字で表示されています。このファイルは、UNIX システムの場合は `/etc/krb5`、Windows システムの場合は `system_drive:¥krb5` にあります。

注意： krb5.conf のレルム名では、大文字と小文字が区別されます。このレルム名は、Microsoft Active Directory のレルム名と一致している必要があります。通常、レルム名には大文字が使用されます。

2. シングル・サインオン中間層と Windows 2000 Server 間でシステム・クロックを同期化します。この手順を省略すると、クロック・スキュー・エラーが発生するため、認証に失敗します。
3. シングル・サインオン・コンピュータで Kerberos サーバーのポート番号を確認します。Kerberos サーバーがリスニングするポートは、デフォルトでは /etc/services から選択されます。Windows システムの場合、services ファイルは `system_drive:\%WINDIR%\system32\drivers\etc` にあります。サービス名は Kerberos です。通常、ポートは Windows 2000 Server で 88/udp および 88/tcp に設定されます。services ファイルへの追加を適切に行うと、これらのポート番号のエントリは次のようになります。

```
kerberos5      88/udp      kdc          # Kerberos key server
kerberos5      88/tcp      kdc          # Kerberos key server
```

4. services ファイルと同じディレクトリにある hosts ファイルで、シングル・サインオン中間層のエントリを確認します。シングル・サインオン・コンピュータの完全修飾ホスト名が、IP アドレスと短縮名の上に配置されている必要があります。正しいエントリの例を次に示します。

```
130.111.111.111 sso.acme.com sso loghost
```

5. Windows 2000 Server で Active Directory 管理ツールにログインし、「ユーザー」→「新規」→「ユーザー」をクリックします。

Single Sign-On ホストの名前をドメイン名を省略して入力します。たとえば、ホスト名が `sso.acme.com` の場合は、`sso` のみを入力します。これは、Active Directory のアカウント名です。

アカウントに割り当てたパスワードを書き留めておいてください。このパスワードは後で必要になります。次のオプションは選択しないでください。

「ユーザーは次回ログオン時にパスワードの変更が必要」

6. Single Sign-On Server の keytab ファイルを作成し、アカウント名をサービス・プリンシパル名にマップします。これらの 2 つの作業を行うには、次のコマンドを Windows 2000 サーバーで実行します。

```
C:> Ktpass -princ HTTP/sso.acme.com@ADUSERS.ACME.COM -pass password -mapuser sso
-out sso.keytab
```

-princ はサービス・プリンシパルです。この値は、HTTP/*single_sign-on_host_name*@*KERBEROS_REALM_NAME* の書式で指定する必要があります。HTTP と Kerberos レalmは大文字で指定します。

-pass は、手順 4 で取得したアカウント・パスワードです。-mapuser は、シングル・サインオン中間層のアカウント名です。このアカウントは手順 4 で作成したものです。
-out は、サービス鍵を格納する出力ファイルです。

ここでも、それぞれのインストール環境に適した値に例の値を置き換えてください。置き換える値は、例の中で太字で表示されています。

注意： コンピュータで ktpass が見つからない場合は、Windows リソース・キットをダウンロードしてこのユーティリティを取得します。

- 手順 4 で作成した keytab ファイル (sso.keytab) をシングル・サインオン中間層にコピーまたは FTP 転送し、\$ORACLE_HOME/j2ee/OC4J_SECURITY/config に配置します。

シングル・サインオン中間層の Web サーバー UID に keytab ファイルの読取り権限を付与してください。

Sun JAAS ログイン・モジュール用の Single Sign-On Server の構成

- \$ORACLE_HOME/opmn/conf/opmn.xml を変更して、JVM に関する次の 4 つのコマンドライン・パラメータを追加します。

```
-Djavax.security.auth.useSubjectCredsOnly=false
-Doracle.security.jazn.config=$ORACLE_HOME/j2ee/OC4J_SECURITY/config/jazn.xml
-Djava.security.krb5.realm=default_realm_in_Active_Directory
-Djava.security.krb5.kdc=Active_Directory_host_name
```

これらのパラメータは、opmn.xml の OC4J_SECURITY プロセス構成セクションに追加する必要があります。"start-parameters" と "stop-parameters" の両方のカテゴリ ID タグに値として追加します。

- XML プロバイダを指すように \$ORACLE_HOME/j2ee/OC4J_SECURITY/config/jazn.xml を変更します。

```
<jazn provider="XML" location="./jazn-data.xml" />
```

次の行がコメントアウトされていない場合は、コメントアウトします。

```
<jazn provider="LDAP" location="ldap://myoid.us.oracle.com:389" />
```

- 以降に示すエントリを `$ORACLE_HOME/j2ee/OC4JSECURITY/config/jazn-data.xml` に追加します。この手順では、Krb5LoginModule (Sun JAAS ログイン・モジュール) を使用できるように Single Sign-On Server を構成します。

XML エントリで、KeyTab は keytab ファイルの場所を示します。principal は Single Sign-On Server のサービス・プリンシパル名です。整合性を維持するために、この例では keytab ファイルとプリンシパルがエントリで保持されています。太字で表示されている値を実際の値と置き換えてください。

次に示すエントリをカット・アンド・ペーストするか、サンプル・ファイル `$ORACLE_HOME/sso/conf/wna-jazn-data.xml` をコピー・アンド・ペーストします。

```
<jazn_data>
  <jazn-loginconfig>
    .
    .
    .
  <application>
    <name>com.sun.security.jgss.accept</name>
    <login-modules>
    <login-module>
      <class>com.sun.security.auth.module.Krb5LoginModule</class>
      <control-flag>required</control-flag>
      <options>
        <option>
          <name>debug</name>
          <value>>false</value>
        </option>
        <option>
          <name>addAllRoles</name>
          <value>>true</value>
        </option>
        <option>
          <name>useKeyTab</name>
          <value>>true</value>
        </option>
        <option>
          <name>keyTab</name>
          <value>Oracle_home/j2ee/OC4J_SECURITY/config/sso.keytab</value>
        </option>
        <option>
          <name>principal</name>
          <value>HTTP/sso.acme.com</value>
        </option>
        <option>
          <name>doNotPrompt</name>
          <value>>true</value>
        </option>
      </options>
    </login-module>
  </login-modules>
</application>
</jazn-loginconfig>
</jazn_data>
```

```

    <option>
      <name>storeKey</name>
      <value>true</value>
    </option>
  </options>
</login-module>
</login-modules>
</application>
.
.
.
</jazz-loginconfig>
</jazz-data>

```

保護されたアプリケーションとしての Single Sign-On Server の構成

- 以降に示すエントリを \$ORACLE_HOME/j2ee/OC4J_SECURITY/applications/sso/web/WEB-INF/web.xml に追加します。

次に示すエントリをカット・アンド・ペーストするか、\$ORACLE_HOME/sso/conf/wna-web.xml にあるサンプル・ファイルをコピー・アンド・ペーストします。

```

<web-app>
.
.
.
  <security-role>
    <role-name>{{PUBLIC}}</role-name>
  </security-role>
  <security-constraint>
    <web-resource-collection>
      <web-resource-name>SSO</web-resource-name>
      <url-pattern>auth</url-pattern>
    </web-resource-collection>
    <!-- authorization -->
    <auth-constraint>
      <role-name>{{PUBLIC}}</role-name>
    </auth-constraint>
  </security-constraint>
  <!-- authentication -->
  <login-config>
    <auth-method>BASIC</auth-method>
  </login-config>
.
.
.
</web-app>

```

2. Single Sign-On Server の Kerberos サービス名を \$ORACLE_HOME/j2ee/OC4J_SECURITY/application-deployments/sso/ orion-application.xml で構成します。この作業を行うには、次のエントリを追加します。太字で表示されている値を実際の値と置き換えてください。\$ORACLE_HOME/sso/conf にあるサンプル・ファイルを使用することもできます。

```
<orion-application>
.
.
.
  <security-role-mapping name="{{PUBLIC}}">
    <group name="{{PUBLIC}}"/>
  </security-role-mapping>
  <jazn provider="LDAP" location="ldap://directory_server.domain:port"
  default-realm="default_realm_in Oracle Internet Directory">
  <jazn-web-app auth-method="WINDOWS_KERBEROS_AUTH"/>
  <property name="kerberos-servicename" value="HTTP@sso.acme.com"/>
  </jazn>
.
.
.
</orion-application>
```

注意： ディレクトリに1つのレルムしかない場合は、default-realmパラメータを省略できます。ディレクトリに複数のレルムがある場合は、レルム名のみを入力します。レルム DN は入力しません。たとえば、レルム DN が dc=uk,dc=oracle,dc=com の場合、レルム名は uk になります。

3. Kerberos 認証プラグインを使用できるように Single Sign-On Server を構成します。\$ORACLE_HOME/sso/conf/policy.properties で、Kerberos プラグインをデフォルトの認証プラグインに指定します。

MediumSecurity_Authplugin パラメータを次の書式のように編集します。

```
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOKerbeAuth
```

4. シングル・サインオン中間層を再起動します。手順については、第2章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

エンド・ユーザーのブラウザの構成

Windows ネイティブ認証を使用できるように Internet Explorer を構成します。構成作業は、ブラウザに応じて次の 2 つの部分に分かれます。

- [Internet Explorer 5.0 以上](#)
- [Internet Explorer 6.0 のみ](#)

Internet Explorer 5.0 以上

1. 次の順序でクリックします。
 - ツール
 - インターネット オプション
 - セキュリティ
 - イン트라ネット
 - サイト
2. 「イン트라ネット」ダイアログ・ボックスで「プロキシ サーバーを使用しないサイトをすべて含める」を選択し、「詳細」をクリックします。
3. もう 1 つの「イン트라ネット」ダイアログ・ボックスで、シングル・サインオン中間層の URL を入力します。次に例を示します。
`http://sso.mydomain.com`
4. 「OK」をクリックし、「イン트라ネット」ダイアログ・ボックスを終了します。
5. 「インターネット オプション」ダイアログ・ボックスで「セキュリティ」タブをクリックし、「イン트라ネット」をクリックして「レベルのカスタマイズ」をクリックします。
6. 「セキュリティの設定」ダイアログ・ボックスで「ユーザー認証」セクションまでスクロールし、「イン트라ネットゾーンでのみ自動的にログオンする」を選択します。
7. 「OK」をクリックし、「セキュリティ設定」ダイアログ・ボックスを終了します。
8. 次の順序でクリックします。
 - ツール
 - インターネット オプション
 - 接続
9. 「接続」タブで「LAN の設定」をクリックします。
10. プロキシ・サーバーのアドレスとポート番号が正しく指定されていることを確認し、「詳細」をクリックします。

11. 「プロキシの設定」ダイアログ・ボックスの「例外」セクションに Single Sign-On Server のドメイン名 (acme.com など) が入力されていることを確認します。
12. 「OK」をクリックし、「プロキシの設定」ダイアログ・ボックスを終了します。

Internet Explorer 6.0 のみ

Internet Explorer 6.0 を使用している場合は、「Internet Explorer 5.0 以上」の手順 1 ~ 12 の実行後に、次の手順を実行します。

1. 次の順序でクリックします。
 - ツール
 - インターネット オプション
 - 詳細設定
2. 「詳細設定」タブで「セキュリティ」セクションまでスクロールします。
3. 「統合 Windows 認証を使用する (再起動が必要)」を選択します。

ローカル・アカウントの再構成

Windows ネイティブ認証を正しく構成したら、orcladmin と他のローカル Windows ユーザーのアカウントを再構成する必要があります。ユーザーによっては、Oracle Internet Directory にアカウントが存在している場合があります。この作業を省略すると、これらのユーザーがログインできなくなります。

Oracle Internet Directory の管理コンソールを使用して、次の手順を実行します。

1. Oracle Internet Directory のローカル・ユーザー・エントリに orclADUser クラスを追加します。
2. ユーザー・エントリの orclSAMAccountName 属性にローカル・ユーザーのログイン ID を追加します。たとえば、orcladmin アカウントのログイン ID は orcladmin です。
3. 外部認証プラグインの exceptionEntry プロパティにローカル・ユーザーを追加します。

フォールバック認証

SPNEGO-Kerberos 認証は、Internet Explorer 5.0 以上のブラウザでのみサポートされています。OracleAS Single Sign-On では、Netscape Communicator などのサポート外のブラウザでフォールバック認証を利用できます。ブラウザのタイプと構成内容に応じて、Single Sign-On ログイン・フォームまたは HTTP Basic 認証のダイアログ・ボックスが表示されます。いずれの場合でも、ユーザーはユーザー名とパスワードを入力する必要があります。ユーザー名は Kerberos レalm名とユーザー ID を連結したものです。次の書式で入力します。

```
domain_name¥user_id
```

例：

```
acme¥jdoe
```

ユーザー名とパスワードは、大文字と小文字が区別されます。また、Microsoft Active Directory のパスワード・ポリシーは適用されない点に留意してください。

フォールバック認証は、Oracle Internet Directory の外部認証プラグインによって Microsoft Active Directory に対して実行されます。

注意：

- HTTP Basic 認証は、ログアウトをサポートしていません。ブラウザのキャッシュから資格証明を消去する場合、ユーザーは開いているブラウザをすべて閉じる必要があります。あるいは、Windows コンピュータからログアウトします。
 - Basic 認証が起動している場合、ユーザーは使用する言語を Internet Explorer で手動で設定する必要があります。これを行うには、「ツール」→「インターネット オプション」→「言語」の順に移動し、使用する言語を追加します。
-
-

ログインの例

使用している Internet Explorer のバージョンに応じて、ログインの方法が異なる場合があります。8-14 ページの表 8-1 は、自動サインオンとフォールバック認証が起動する状況を示しています。

表 8-1 Internet Explorer での Single Sign-On ログインのオプション

ブラウザのバージョン	デスクトップ・プラットフォーム	デスクトップの認証タイプ	Internet Explorer ブラウザの統合認証	Single Sign-On ログインのタイプ
>= 5.0.1	Windows 2000/XP	Kerberos バージョン 5	オン	自動サインオン
>= 5.0.1 かつ < 6.0	Windows 2000/XP	Kerberos バージョン 5	オフ	シングル・サインオン
>= 6.0	Windows 2000/XP	Kerberos バージョン 5 または NTLM	オフ	HTTP Basic 認証
>= 5.0.1 かつ < 6.0	Windows NT/2000/XP	NTLM	オンまたはオフ	シングル・サインオン
>= 6.0	NT/2000/XP	NTLM	オン	シングル・サインオン
>= 5.0.1	Windows 95、Windows ME、Windows NT 4.0	該当せず	該当せず	シングル・サインオン
< 5.0.1	該当せず	該当せず	該当せず	シングル・サインオン
他のすべてのブラウザ	他のすべてのプラットフォーム	該当せず	該当せず	シングル・サインオン

この章では、OracleAS Single Sign-On をデフォルト以外で使用方法について説明します。ここでは、本番環境で起りえる使用例を示します。一部の使用例は複雑であり、そこで配置および構成する機能は他の OracleAS コンポーネントに影響することがあります。

この章の項目は次のとおりです。

- [SSL の有効化](#)
- [Single Sign-On Server と Oracle Internet Directory 間の SSL の構成](#)
- [配置例](#)
- [識別情報管理データベースのレプリケート](#)
- [プロキシ・サーバーを使用する OracleAS Single Sign-On の配置](#)
- [ユーザー・ニックネームの変更におけるディレクトリ同期の設定](#)

SSL の有効化

この項では、Single Sign-On Server と関連するコンポーネントで SSL を使用可能にする方法について説明します。Single Sign-On Server のデフォルトの構成では、Oracle HTTP Server の SSL ポートを使用できません。インストール時に SSL を構成することもできません。次の作業を順番に実行します。

- [シングル・サインオン中間層での SSL の有効化](#)
- [Identity Management インフラストラクチャ・データベースの再構成](#)
- [シングル・サインオン URL の保護](#)
- [Oracle HTTP Server とシングル・サインオン中間層の再起動](#)
- [パートナ・アプリケーションの登録](#)

シングル・サインオン中間層での SSL の有効化

次の手順では Oracle HTTP Server を構成します。この手順はシングル・サインオン中間層で実行します。実行する際は、次の点に留意してください。

- SSL の構成は、シングル・サインオン中間層を実行しているコンピュータで行う必要があります。
- SSL サーバーを構成します。
- 簡易ネットワークの暗号化に対して SSL を有効にします。PKI 認証は必要ありません。

Oracle HTTP Server で SSL をすぐに使用できるようにする手順は次のとおりです。

1. opmn.xml ファイルで、start-mode パラメータの値を ssl-enabled に変更します。このパラメータは、次のコードで xml タグに囲まれ太字で示されています。このファイルは \$ORACLE_HOME/opmn/conf に格納されています。

```
<ias-component id="HTTP_Server">
  <process-type id="HTTP_Server" module-id="OHS">
    <module-data>
      <category id="start-parameters">
        <data id="start-mode" value="ssl-enabled"/>
      </category>
    </module-data>
    <process-set id="HTTP_Server" numprocs="1"/>
  </process-type>
</ias-component>
```

次のように指定して、変更した opmn 構成ファイルをリロードします。

```
$ORACLE_HOME/opmn/bin/opmnctl reload
```

2. 非 SSL ポートをアクティブな状態で保持します。外部アプリケーション・ポートレットが非 SSL ポートを介して Single Sign-On Server と通信します。HTTP ポートはデフォルトで有効になっています。無効になっている場合を除き、ここでの操作は必要ありません。
3. ルール `mod_rewrite` を SSL 構成に適用します。この手順では、中間層コンピュータで `ssl.conf` ファイルを変更します。このファイルは `$ORACLE_HOME/Apache/Apache/conf` に格納されています。

次の各行を SSL Virtual Hosts セクションに追加します。

```
<VirtualHost ssl_host:port>
.
.
.
RewriteEngine on
RewriteOptions inherit
</VirtualHost>
```

ファイルを保存して閉じます。

4. Oracle HTTP Server を再起動します。手順については、第 2 章の「[Oracle HTTP Server の停止と起動](#)」の項を参照してください。
5. SSL のシングル・サインオン中間層が有効になっていることを確認します。これには、OracleAS の最初のページで、`https://host:port` の書式を使用してログインします。

注意： インストール環境に複数の中間層がある場合は、「[シングル・サインオン中間層での Oracle HTTP Server の構成](#)」の手順 2 が完了していることを確認してください。これは、この章の後の項で示す配置例のうち、「複数のシングル・サインオン中間層、1 つの Oracle Internet Directory」のケースで要求される手順です。

SSL 用に Oracle HTTP Server を構成する方法については、Oracle HTTP Server の管理者ガイドを参照してください。

Identity Management インフラストラクチャ・データベースの再構成

まず、シングル・サインオン URL の `http` のすべての参照を、Identity Management インフラストラクチャ・データベース内の `https` に変更します。次に、SSL を有効にしたときにシングル・サインオンの管理アプリケーションが正しく削除されるよう、データベースを構成します。データベース内のシングル・サインオン URL を変更するときは、シングル・サインオン中間層でも `targets.xml` ファイル内の同じ URL を変更する必要があります。`targets.xml` は、Oracle Enterprise Manager で監視される様々なターゲットの構成ファイルです。そのターゲットの 1 つが OracleAS Single Sign-On です。

シングル・サインオン URL の変更

シングル・サインオン中間層が配置されているコンピュータで慎重にコマンドを入力して、`ssocfg` スクリプトを実行します。使用する構文は次のとおりです。

- UNIX:

```
$ORACLE_HOME/sso/bin/ssocfg.sh protocol host port
```

- Windows NT/2000:

```
%ORACLE_HOME%\sso\bin\ssocfg.bat protocol host port
```

この場合、`protocol` は `https` です (HTTP に戻す場合は、`http` を使用します)。`host` は、Single Sign-On Server の Oracle HTTP リスナーのホスト名またはサーバー名です。

次に例を示します。

```
ssocfg.sh https login.acme.com 4443
```

正しいポート番号を確認するには、`$ORACLE_HOME/Apache/Apache/conf` にある `ssl.conf` ファイルを調べます。OracleAS のインストール時にインストーラによって割り当てられるポート番号は `4443` です。

`ssocfg` スクリプトが正常に終了すると、ステータス `0` が返されます。成功したことを確認するには、Single Sign-On Server にそのサーバーの SSL アドレスでログインします。

```
https://host:port/pls/orasso/
```

targets.xml の更新

ssocfg を実行したら、シングル・サインオン中間層で targets.xml ファイルを更新します。
targets.xml を更新するには、次の手順を実行します。

1. ファイルをバックアップします。

```
cp $ORACLE_HOME/sysman/emd/targets.xml $ORACLE_
HOME/sysman/emd/targets.xml .backup
```

2. ファイルを開いて、ターゲット・タイプ oracle_sso_server を検索します。このターゲット・タイプ内で、ssocfg に渡した次の 3 つの属性を検索し、編集します。

- HTTPMachine: サーバーのホスト名
- HTTPPort: サーバーのポート番号
- HTTPProtocol: サーバーのプロトコル

たとえば、次のように ssocfg を実行したとします。

```
$ORACLE_HOME/sso/bin/ssocfg.sh http sso.mydomain.com" 80
```

この場合は、次のように 3 つの属性を更新します。

```
<Property NAME="HTTPMachine" VALUE="sso.mydomain.com"/>
<Property NAME="HTTPPort" VALUE="80"/>
<Property NAME="HTTPProtocol" VALUE="HTTP"/>
```

3. ファイルを保存して閉じます。
4. OracleAS Console をリロードします。

```
$ORACLE_HOME/bin/emctl reload
```

管理アプリケーションのログアウトの再構成

次の手順を実行して、パートナ・アプリケーションからログアウトしたときに管理アプリケーションが正しく削除されるようにします。

1. Single Sign-On スキーマのパスワード (orasso) を取得します。手順については、付録 B を参照してください。
2. Oracle 識別情報管理データベースに orasso スキーマとして接続します。

```
sqlplus orasso/password
```

3. 次の SQL*Plus コマンドを実行します。

```
SQL>update orasso.wwctx_cookie_info$ set secure='N';
SQL>commit;
```

シングル・サインオン URL の保護

シングル・サインオン URL を SSL 用に変更した後、URL を保護するディレクティブを適用します。この手順もシングル・サインオン中間層を配置しているコンピュータで行います。ただし、これらのディレクティブは特定の URL、たとえばログイン URL とパスワード変更 URL で使用する必要があります。すべてのシングル・サインオン URL では使用できません。

ディレクティブは、Java と PL/SQL の両方の認証リンクで提供されます。ログインおよびパスワード変更モジュールの PL/SQL ディレクティブには、下位互換性があります。

Java リンクの URL

SSL のみで Java ログインおよびパスワード変更のページにアクセスできるようにするには、\$ORACLE_HOME/sso/conf にある sso_apache.conf ファイルを編集します。

次のディレクティブをこのファイルの末尾に追加します。

```
<IfDefine SSL>
  <location "/sso/auth">
    SSLRequireSSL
  </location>

  <location "/sso/ChangePwdServlet">
    SSLRequireSSL
  </location>
</IfDefine>
```

PL/SQL リンクの URL

PL/SQL リンクに対して SSL を有効にするには、\$ORACLE_HOME/Apache/modplsql/conf にある dads.conf ファイルを編集します。次のディレクティブをファイルの末尾に追加します。

SSL のみでログイン URL、パスワード変更 URL および外部アプリケーション URL にアクセスできるようにするには、次のディレクティブを使用します。

```
<IfDefine SSL>

  #Login URL for single sign-on server and external applications
  <Location "/pls/orasso/*[Ll][Oo][Gg][Ii][Nn]">
    SSLRequireSSL
  </Location>

  #Change password page
  <Location "/pls/orasso/*[Pp][Aa][Ss][Ss][Ww][Oo][Rr][Dd]">
    SSLRequireSSL
  </Location>

  #External application login URL
```



```
<Location "/pls/orasso/* [Ff] [Aa] [Pp] [Pp] [Uu] [Ss] [Ee] [Rr]">  
    SSLRequireSSL  
</Location>
```

```
</IfDefine>
```

Single Sign-On Server で SSL を有効にしている場合は、HTTP を介してサーバーにアクセスするホストに HTTP アクセスを制限するように指定する必要があります。これは、OracleAS インストーラおよび OracleAS Portal をホストするコンピュータに特に当てはまりません。

下位互換性のために次のディレクティブを追加します。このディレクティブによって、インストーラは HTTP による Single Sign-On Server へのアクセスが可能になります。your_domain_name をそれぞれのドメイン名に置き換えてください。

```
<Location "/pls/orasso/* [Ss] [Ss] [Oo] [Pp] [Ii] [Nn] [Gg]">  
    Order deny,allow  
    Deny from all  
    Allow from your_domain_name  
</Location>
```

OracleAS Portal では、外部アプリケーションのリストを表示する URL に HTTP を介してアクセスする必要があります。このアクセスは、次のディレクティブで可能になります。さらに、your_domain_name をそれぞれのドメイン名に置き換えてください。

```
<Location "/pls/orasso/* [Aa] [Pp] [Pp] [Ss]_[Ll] [Ii] [Ss] [Tt]">  
    Order deny,allow  
    Deny from all  
    Allow from your_domain_name  
</Location>
```

Oracle HTTP Server とシングル・サインオン中間層の再起動

第 2 章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

パートナ・アプリケーションの登録

Single Sign-On Server で SSL を有効にしたら、mod_osso をシングル・サインオン中間層とアプリケーション中間層に登録します。この手順では、有効なシングル・サインオン URL を使用できるように mod_osso を構成します。手順については、第 4 章の「[mod_osso の登録](#)」の項を参照してください。

Single Sign-On Server と Oracle Internet Directory 間の SSL の構成

Single Sign-On Server と Oracle Internet Directory の間に SSL リンクを構成する際は、Single Sign-On データベースが配置されているコンピュータで `ssooconf.sql` スクリプトを実行する必要があります。 `ssooconf.sql` スクリプトは、`$ORACLE_HOME/sso/admin/plsql/sso` にあります。

SSL リンクを構成する手順は次のとおりです。

1. SQL*Plus に Single Sign-On スキーマとしてログインします。デフォルトのユーザー一名は `orasso` です。パスワードの取得方法については、[付録 B](#) を参照してください。

2. 次のコマンドを発行して、ディレクトリ・ポートと SSL フラグを変更します。

```
SQL> @ssooconf.sql
```

次のプロンプトが表示されます。

```
Enter value for new_oid_host:
```

3. [Return] または [Enter] を押して、次のプロンプトに移動します。

次のプロンプトが表示されます。

```
Enter value for new_oid_port:
```

4. ディレクトリの SSL ポート番号を入力します。

5. 次のプロンプトが表示されるまで、[Return] または [Enter] を押します。

```
Enter value for new_ldapussl:
```

6. Y を入力し、[Return] または [Enter] を押します。

値 `new_ldapussl` が更新されたことを伝えるメッセージが表示されます。

スクリプトの実行後、シングル・サインオン中間層を再起動します。第 2 章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

配置例

この項では、可用性を高めるための Single Sign-On Server の様々な配置例を示します。この項の項目は次のとおりです。

- 1つのシングル・サインオン中間層、1つの Oracle Internet Directory
- 複数のシングル・サインオン中間層、1つの Oracle Internet Directory
- Identity Management インフラストラクチャでの OracleAS Active Failover Clusters の使用
- 複数のシングル・サインオン中間層、レプリケートされた Oracle Internet Directory
- 地理的に分散している複数のシングル・サインオン・インスタンス
- その他の高可用性の配置

注意： 以降の使用例で示す IP アドレスとホスト名は、単に例として示したものです。これらのアドレスと名前は、実際の実装では機能しない場合があります。実際のインストールでは、該当する値に置き換えてください。

1つのシングル・サインオン中間層、1つの Oracle Internet Directory

OracleAS Single Sign-On を配置する最も簡単で迅速な方法は、OracleAS Infrastructure のコンポーネントを同一のコンピュータにインストールすることです。この作業を行うには、インストール・タイプに「OracleAS Infrastructure 10g」を選択し、インストール・オプションに「Identity Management and OracleAS Metadata Repository」を選択します。このインストール・タイプのコンポーネント・リストが表示されたら、デフォルトで選択されているコンポーネントを受け入れます。

または、「OracleAS Infrastructure 10g」、「Identity Management」、「Single Sign-On」を続けて選択し、シングル・サインオン中間層を別のコンピュータにインストールすることもできます。これは、最も簡単な分散構成です。

図 9-1 は、最初のインストールのタイプを示しています。図 9-2 は、2 番目のタイプを示しています。最初のタイプは、一般にテスト環境、ステージング環境または開発環境で使用されます。2 番目のタイプは、Single Sign-On と Oracle Internet Directory の各コンピュータ間にファイアウォールを設置する場合に適しています。これらのサーバーを別々のコンピュータに配置すると、パフォーマンスが向上するという付加的な利点があります。

図 9-1 デフォルトの Single Sign-On インストール : 1 台のコンピュータ

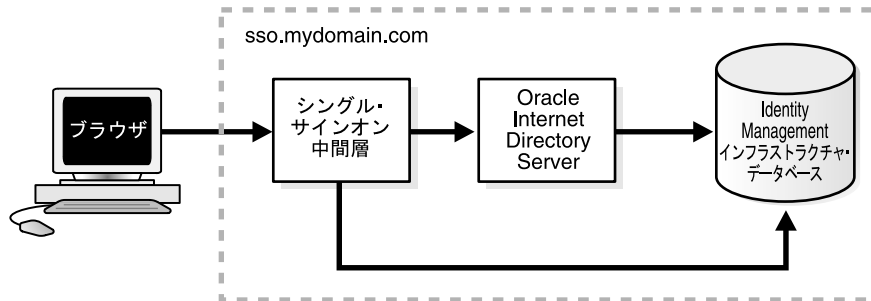
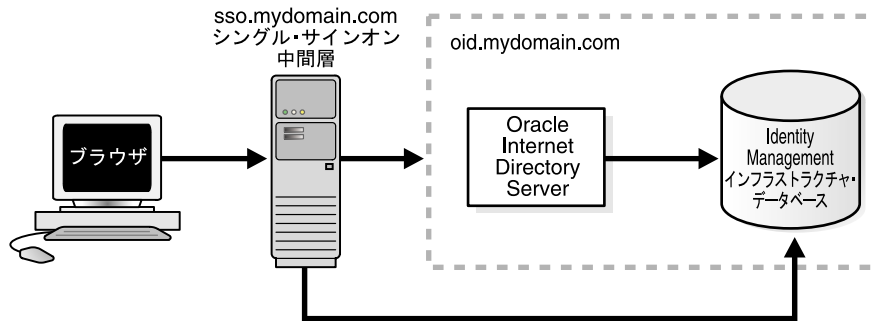


図 9-2 Single Sign-On インストール : 2 台のコンピュータ



複数のシングル・サインオン中間層、1つの Oracle Internet Directory

最も単純な高可用性の使用例では、中間層のシングル・サインオン・インスタンス自体にフェイルオーバーの機能を組み込みます。複数の中間層を追加するとスケーラビリティが向上するため、Single Sign-On Server の可用性が向上します。

この構成では、複数の Oracle HTTP Server の前に HTTP ロード・バランサを1つ配置します。バックエンドには、ディレクトリ・サーバーと Identity Management インフラストラクチャ・データベースを1つずつ配置します。ロード・バランサの目的は、複数の Single Sign-On パートナ・アプリケーションに単一のアドレスを公開するとともに、複数のシングル・サインオン中間層のファームを提供することです。ファーム内の中間層で実際にアプリケーションのリクエストが処理されます。HTTP ロード・バランサは、Oracle HTTP Server インスタンスの1つで発生した障害を検出し、別のインスタンスにリクエストをフェイルオーバーできます。

使用例

この使用例では、次の架空の構成を想定しています。

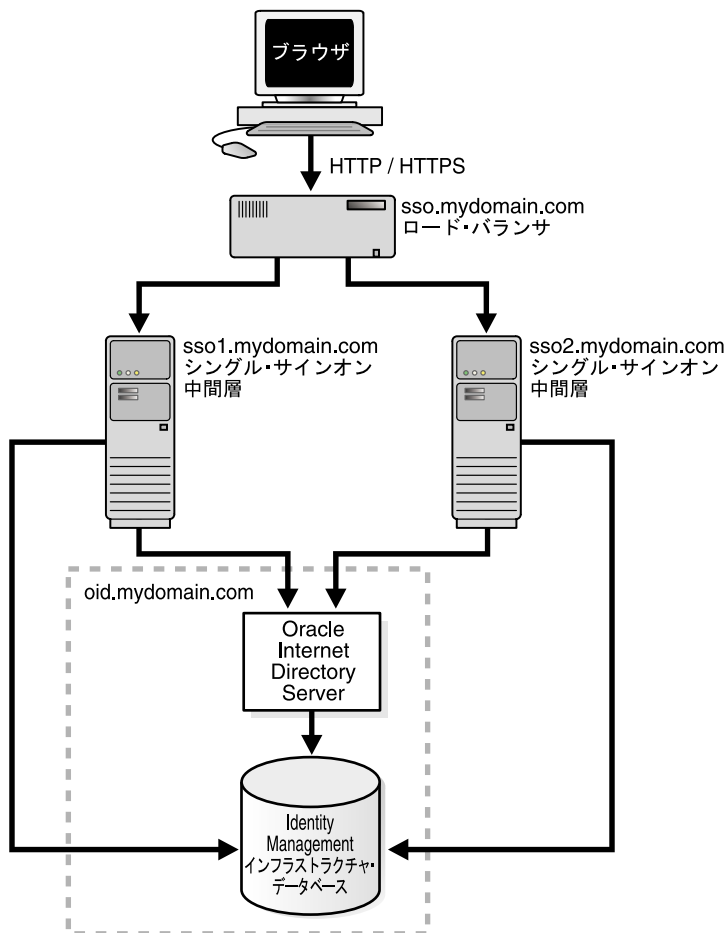
- ディレクトリ・サーバーと Identity Management インフラストラクチャ・データベースは、oid.mydomain.com に配置されています。
- 2つのシングル・サインオン中間層があります。1つはホスト sso1.mydomain.com (IP アドレス 138.1.34.172) にインストールされています。もう1つは sso2.mydomain.com (IP アドレス 138.1.34.173) にインストールされています。これらのサーバーは非 SSL ポート 7777 をリスニングしています。さらに、oid.mydomain.com に配置されているディレクトリ・サーバーと Identity Management インフラストラクチャ・データベースを使用するように構成されています。
- パートナ・アプリケーションに公開されている Single Sign-On Server の有効な URL は、sso.mydomain.com (IP アドレス 138.1.34.234) です。HTTP ロード・バランサは、sso.mydomain.com のポート 80 をリスニングするように構成されています。HTTP ロード・バランサは、ユーザーのリクエストによる負荷を sso1.mydomain.com と sso2.mydomain.com の間で平均化します。

注意：

- この使用例では、ロード・バランサが非 SSL ポート番号のポート 80 をリスニングします。
 - ロード・バランサが SSL を使用してブラウザと対話するように構成されている場合は、別のポート番号を選択する必要があります。デフォルトの SSL ポート番号は 4443 です。
 - この使用例とその次の使用例では、2つのシングル・サインオン中間層が使用されています。実際には、任意の数の中間層を使用できます。
-
-

9-12 ページの図 9-3 は、Oracle Internet Directory のシングル・インスタンスを使用するように構成した 2つのシングル・サインオン中間層を示しています。

図 9-3 2 つのシングル・サインオン中間層、1 つの Oracle Internet Directory



構成手順

図 9-3 に示すシングル・サインオン・システムをセットアップするには、次の作業を行います。

- Identity Management インフラストラクチャ・データベース、ディレクトリ・サーバーおよび Single Sign-On Server のインストール
- シングル・サインオン中間層での Oracle HTTP Server の構成
- HTTP ロード・バランサの構成
- Identity Management インフラストラクチャ・データベースの構成
- シングル・サインオン中間層での mod_osso の登録

Identity Management インフラストラクチャ・データベース、ディレクトリ・サーバーおよび Single Sign-On Server のインストール

1. パートナ・アプリケーションに公開する Single Sign-On Server 名を選択します。この名前はロード・バランサのアドレスにもなります。この配置例の場合、このアドレスは sso.mydomain.com です。
2. 「Identity Management and OracleAS Metadata Repository」のオプションを選択して、OracleAS Infrastructure を oid.mydomain.com にインストールします。このインストール・タイプのコンポーネント・リストが表示されたら、Oracle Internet Directory のみを選択します。
3. 中間層 sso1.mydomain.com および sso2.mydomain.com に OracleAS Infrastructure をインストールし、オプション「Identity Management」を選択します。このインストール・タイプのコンポーネント・リストが表示されたら、OracleAS Single Sign-On のみを選択します。Oracle Universal Installer で、これらのシングル・サインオン・インスタンスに名前を付けるように求められたら、oid.mydomain.com と入力します。

注意： デフォルトでは、OracleAS インストーラはある範囲の数値からポート番号を割り当てます。インストーラでコンポーネントに異なるポート番号を割り当てる場合は、Oracle Application Server 10g のインストレーション・ガイドの第 4 章、静的なポート番号に関する項を参照してください。

シングル・サインオン中間層での Oracle HTTP Server の構成

ユーザーと Oracle HTTP Server の間にロード・バランサを配置すると、Single Sign-On Server の有効な URL が変更されます。両方のシングル・サインオン中間層の Oracle HTTP 構成ファイル `httpd.conf` を修正し、この変更を反映する必要があります。このファイルは、`$ORACLE_HOME/Apache/Apache/conf` にあります。

1. `sso1.mydomain.com` および `sso2.mydomain.com` で `httpd.conf` の次の行を編集します。

```
KeepAlive off
ServerName sso.mydomain.com
Port 80
```

注意： `httpd.conf` に複数のポートが記述されている場合、変更されるポートは必ず最後のものになります。

この手順では、シングル・サインオン中間層で Oracle HTTP Server を構成し、有効な URL をリスニングします（この使用例では `sso.mydomain.com`）。

2. ブラウザとロード・バランサの間に SSL を構成し、SSL 接続がロード・バランサで終了する場合は、`sso1.mydomain.com` と `sso2.mydomain.com` の両方に `mod_certheaders` を構成します。このモジュールによって、Oracle HTTP Server では、HTTP で受信するリクエストを SSL リクエストとして処理できるようになります。次のステップを追加します。これらのステップは `httpd.conf` の最後に記述します。順序は重要ではありません。

- a. 両方の中間層の `httpd.conf` で次の行を入力します。

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

- b. OracleAS Web Cache をロード・バランサとして使用する場合は、次の行を入力します。

```
AddCertHeader HTTPS
```

ハードウェア・ロード・バランサを使用する場合は、次の行を入力します。

```
SimulateHttps on
```

3. これらの 2 つの中間層のシステム・クロックを同期化します。
4. 次のコマンドを実行して、Distributed Cluster Management スキーマを変更内容で更新します。

```
$ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
```


HTTP ロード・バランサの構成

HTTP ロード・バランサには、BigIP、Alteon、Local Director などのハードウェアや、OracleAS Web Cache などのソフトウェアを使用することができます。

- ハードウェア・ロード・バランサ

ハードウェアのロード・バランサを使用する場合は、実サーバーの 1 つのプールをアドレス 138.1.34.172 および 138.1.34.173 で構成します。1 つの仮想サーバーをアドレス 138.1.34.234 で構成します。この仮想サーバーは、ロード・バランサの外部インタフェースです。構成手順の詳細は、ロード・バランサのベンダーが提供するドキュメントを参照してください。

- ソフトウェア・ロード・バランサ

接続要求のロード・バランサに OracleAS Web Cache を使用する場合は、次のドキュメントを参照してください。

- 『Oracle Application Server Web Cache 管理者ガイド』の Oracle Identity Management インフラストラクチャの利用に関する項
- 『Oracle Application Server Web Cache 管理者ガイド』の Single Sign-On Server のリクエストのルーティングに関する項

注意： 最高のパフォーマンスを得るには、ハードウェア・ロード・バランサを使用してください。

Identity Management インフラストラクチャ・データベースの構成

シングル・サインオン中間層の 1 つで ssocfg スクリプトを実行します。このスクリプトによって、外部に公開された Single Sign-On Server のアドレスによる認証リクエストを受け入れるように Single Sign-On Server が構成されます。この例では、スクリプトは次のように実行します。

- UNIX:

```
$ORACLE_HOME/sso/bin/ssocfg.sh http sso.mydomain.com 80
```

- Windows NT/2000:

```
%ORACLE_HOME%\sso\bin\ssocfg.bat http sso.mydomain.com 80
```

これらのコマンドの例では、ロード・バランサのリスナー・プロトコル、ホスト名、ポート番号が引数として指定されています。ロード・バランサのアドレスは、外部に公開されている Single Sign-On Server のアドレスであることを思い出してください。SSL を使用するようにロード・バランサを構成する場合には、非 SSL ポートの 80 を SSL ポートの 4443 に置き換え、http を https に置き換えてください。

シングル・サインオン中間層での mod_osso の登録

両方の中間層コンピュータで、mod_osso をパートナー・アプリケーション sso.mydomain.com として登録します。

mod_osso を sso1.mydomain.com に登録する手順は次のとおりです。

1. sso1.mydomain.com の Oracle ホームを指すように環境変数 ORACLE_HOME を設定します。PATH 変数に \$ORACLE_HOME/jdk/bin を追記します。
2. 登録スクリプトを実行します。URL は、実際のインストール環境の該当する値に置き換えてください。スクリプトによって、sso.mydomain.com という名前のパートナー・アプリケーションが作成されます。

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path orcl_home_path
-site_name site_name
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u userid
[-virtualhost]
[-update_mode CREATE | DELETE | MODIFY]
[-config_file config_file_path]
[-admin_id adminid]
[-admin_info admin_info]
```

コマンド・パラメータの説明については、第 4 章の「[mod_osso の登録](#)」の項を参照してください。

3. sso1.mydomain.com で中間層を再起動します。手順については、第 2 章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

mod_osso を sso2.mydomain.com に登録する手順は次のとおりです。

1. コンピュータ sso2.mydomain.com で、Single Sign-On 管理者としてシングル・サインオン管理ページにログインします。次の URL にログインしてください。

```
http://sso.mydomain.com/pls/orasso
```

2. 「パートナー・アプリケーションの管理」ページを使用して、パートナー・アプリケーション sso2.mydomain.com の既存エントリを削除します。
3. コンピュータ sso1.mydomain.com から osso.conf ファイルをコピーします。ファイルを FTP で転送する場合は、バイナリ・モードを使用してください。このファイルを \$ORACLE_HOME/Apache/Apache/conf/osso にコピーします。
4. Distributed Cluster Management リポジトリとコピーしたファイルを同期化します。これには、sso2.mydomain.com で次のコマンドを実行します。

```
$ORACLE_HOME/Apache/Apache/bin/ssotransfer $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf
```

注意： ssotransfer コマンドは、Distributed Cluster Management リポジトリと仮想ホストに作成された mod_osso 構成ファイルとの同期化には使用しないでください。仮想ホストの mod_osso を登録する方法については、第4章の「仮想ホストでの mod_osso の構成」の項を参照してください。

1. sso2.mydomain.com で中間層を再起動します。手順については、第2章の「シングル・サインオン中間層の停止と起動」の項を参照してください。
2. Oracle Delegated Administration Services がインストールされている場合は、そのベース URL を Oracle Directory Manager によって次の手順で変更します。
 - a. ツールを起動します。

```
$ORACLE_HOME/bin/oidadmin
```
 - b. cn=orcladmin として Oracle Directory Manager にログインします。
 - c. 次のように指定して、orcldasurlbase 属性を含むエントリに移動します。

```
cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext,Entry Management
```
 - d. 属性を次の値に変更します。

```
http://sso.mydomain.com/
```

ホスト名の後にスラッシュを挿入してください。
 - e. 次の URL でパートナ・アプリケーション oiddas をテストします。

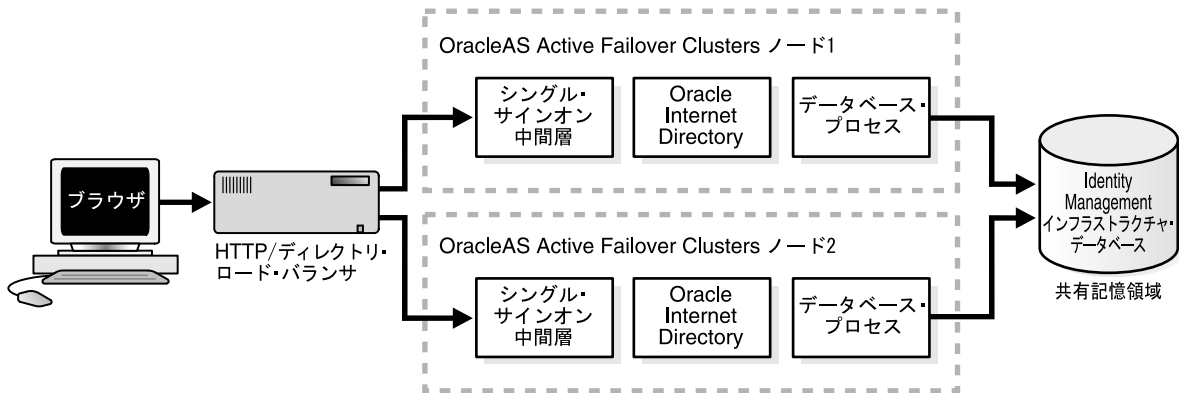
```
http://sso.mydomain.com/oiddas
```
3. 次の URL で Single Sign-On 管理アプリケーションをテストします。

```
http://sso.mydomain.com/pls/orasso
```

Identity Management インフラストラクチャでの OracleAS Active Failover Clusters の使用

OracleAS リリース 9.0.4 では、アクティブ・フェイルオーバー・クラスタに OracleAS Infrastructure をインストールすることもできます。このオプションを選択すると、インフラストラクチャの全コンポーネント (Single Sign-On、Oracle Internet Directory およびデータベース) が1つのノードにインストールされます。図 9-4 では、2 ノードのアクティブ・クラスタの前段にロード・バランサを配置し、インフラストラクチャの全コンポーネントでスケラビリティ、高可用性、フェイルオーバーを実現しています。

図 9-4 OracleAS Active Failover Clusters を使用したシングル・サインオン



インストール後の注意 : policy.properties、web.xml またはその他のシングル・サインオン構成ファイルがあるアクティブなクラスター・ノードで変更した場合は、他のアクティブなフェイルオーバー・クラスター・ノードにそのファイルを手動でコピーする必要があります。または、これらのファイルに共有ディスク・ドライブへのソフト・リンクを構成します。

使用例と構成手順

OracleAS Active Failover Clusters の構成方法と使用方法については、『Oracle Application Server 10g 高可用性ガイド』の第3章「Infrastructure の高可用性」を参照してください。

複数のシングル・サインオン中間層、レプリケートされた Oracle Internet Directory

通信量の多い Local Area Network (LAN) では、複数のシングル・サインオン中間層を Oracle Internet Directory のレプリケート・インスタンスで補強すると有効な場合があります。9-21 ページの図 9-5 に示す配置では、中間層とディレクトリ・サーバーの両方でフェイルオーバーを実行できます。

使用例

以降の使用例では、次の架空の構成を想定しています。

- 2つのシングル・サインオン中間層があります。1つはホスト sso1.mydomain.com にインストールされています。もう1つは sso2.mydomain.com にインストールされていません。
- HTTP ロード・バランサは、ブラウザと2つのシングル・サインオン中間層の間に配置されています。

- パートナ・アプリケーションに公開されている Single Sign-On Server のアドレスは、`sso.mydomain.com` です。このアドレスは、ロード・バランサの外部アドレスでもあります。
- 2つの Identity Management インフラストラクチャ・データベースがあり、1つは `oid1.mydomain.com` に、もう1つは `oid2.mydomain.com` に配置されています。これらのノードにある2つのディレクトリ・サーバーによって、レプリケーション・グループが構成されています。
- レプリケーションにおいては、`oid1.mydomain.com` がマスター定義サイト (MDS) になります。このサイトではレプリケーション・スクリプトが実行され、データが最初にレプリケートされます。`oid2.mydomain.com` はリモート・マスター・サイト (RMS) になります。このサイトは、データのレプリケート先のサイトです。
- ロード・バランサは、レプリケートされたディレクトリ・サーバーの前端に配置されています。このロード・バランサは、ロード・バランシング用ではなくフェイルオーバー用に構成されています。
- シングル・サインオン中間層に公開されているディレクトリ・サーバーのアドレスは、`oid.mydomain.com` です。このアドレスは、ディレクトリ・ロード・バランサの外部アドレスでもあります。

構成手順

次の手順は、ディレクトリ・レプリケーションのドキュメントの操作手順と「[複数のシングル・サインオン中間層、1つの Oracle Internet Directory](#)」の操作手順を組み合わせたものです。後者の操作手順は、この章で前述した配置例に基づくものです。

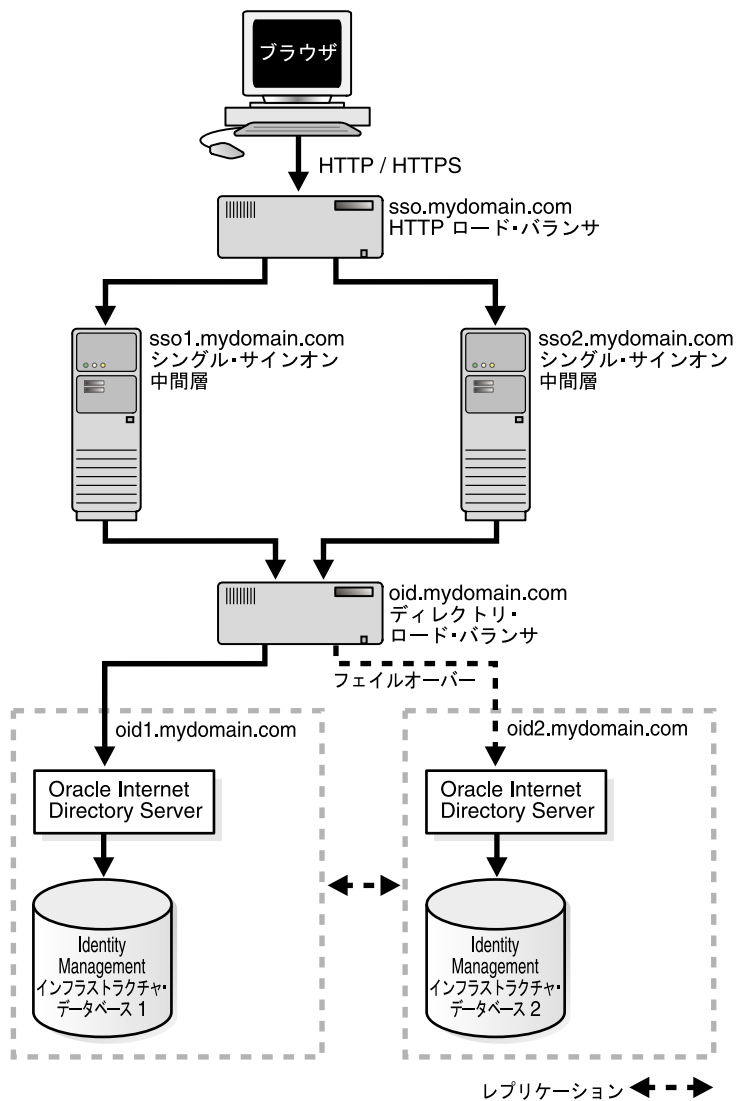
1. Oracle Internet Directory と OracleAS Single Sign-On に使用しているロード・バランサの有効なホスト名を選択します。前述の使用例では、この作業はすでに完了しています。
2. `oid1.mydomain.com` および `oid2.mydomain.com` に Oracle Internet Directory をインストールし、これらのサーバーをレプリケーション・グループとして設定します。詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。この手順には、インストールとレプリケーションの両方が含まれています。レプリケーションの概念については、『Oracle Internet Directory 管理者ガイド』を参照してください。
3. ディレクトリ・ロード・バランサで、実サーバーの1つのプールをアドレス `oid1.mydomain.com` および `oid2.mydomain.com` で構成します。1つの仮想サーバーをアドレス `oid.mydomain.com` で構成します。このディレクトリ・ロード・バランサはフェイルオーバー用に構成し、ロード・バランシング用には構成しません。ロード・バランサは、永続 (ステートフル) ルーティングで構成する必要があります。

4. 中間層 `sso1.mydomain.com` および `sso2.mydomain.com` に OracleAS Infrastructure をインストールし、オプション「Identity Management」を選択します。このインストール・タイプのコンポーネント・リストが表示されたら、「Single Sign-On」のみを選択します。Oracle Universal Installer で、これらのシングル・サインオン・インスタンスに名前を付けるように求められたら、`oid.mydomain.com` と入力します。
5. この使用例では 2 つの Oracle HTTP Server を構成して、Single Sign-On Server の仮想アドレス (`sso.mydomain.com`) を実際の内部ホスト名 `sso1.mydomain.com` と `sso2.mydomain.com` に解決します。詳細は、「[シングル・サインオン中間層での Oracle HTTP Server の構成](#)」の項を参照してください。
6. Single Sign-On Server の有効な URL による認証リクエストを受け入れるように Single Sign-On Server を構成します。この作業を行うには、シングル・サインオン中間層の 1 つで `ssocfg` スクリプトを実行します。この例では、スクリプトは次のように実行します。
 - UNIX:

```
$ORACLE_HOME/sso/bin/ssocfg.sh http sso.mydomain.com 80
```
 - Windows NT/2000:

```
%ORACLE_HOME%\sso\bin\ssocfg.bat http sso.mydomain.com 80
```これらのコマンドの例では、ロード・バランサのリスナー・プロトコル、ホスト名、ポート番号が引数として指定されています。ロード・バランサのアドレスが Single Sign-On Server の有効な URL であることを思い出してください。SSL を使用するようにロード・バランサを構成する場合には、非 SSL ポートの 80 を SSL ポートの 4443 に置き換え、`http` を `https` に置き換えてください。  
`ssocfg` を実行したら、シングル・サインオン中間層で `targets.xml` ファイルを更新します。詳細は、「[targets.xml の更新](#)」の項を参照してください。
7. シングル・サインオン中間層で `mod_osso` を登録します。「[シングル・サインオン中間層での mod_osso の登録](#)」の手順に従います。

図 9-5 レプリケート・ディレクトリを含む複数のシングル・サインオン中間層



地理的に分散している複数のシングル・サインオン・インスタンス

事業が地理的に広く分散している企業にとって、サーバーの可用性は非常に重要です。企業が1台のサーバーで Wide Area Network を介してリモート・ユーザーを認証している場合は、認証に長時間を要することがあります。ネットワーク・ラウンドトリップを短縮してアプリケーションへのアクセスを高速化するために、企業では、複数の Single Sign-On Server インスタンスを地理的に分散して実装できます。この配置では、アプリケーションの格納場所に関係なく、ユーザーはリモート・ロケーションに移動して、最も近いサーバーで認証を受けることができます。

この使用例では、Single Sign-On データベース表が Local Area Network (LAN) または Wide Area Network を介してレプリケートされます。Single Sign-On Server の有効なアドレスがユーザーの最寄りのシングル・サインオン・インスタンスに解決されるように、各シングル・サインオン中間層サイトに配置されている DNS サーバーを構成する必要があります。

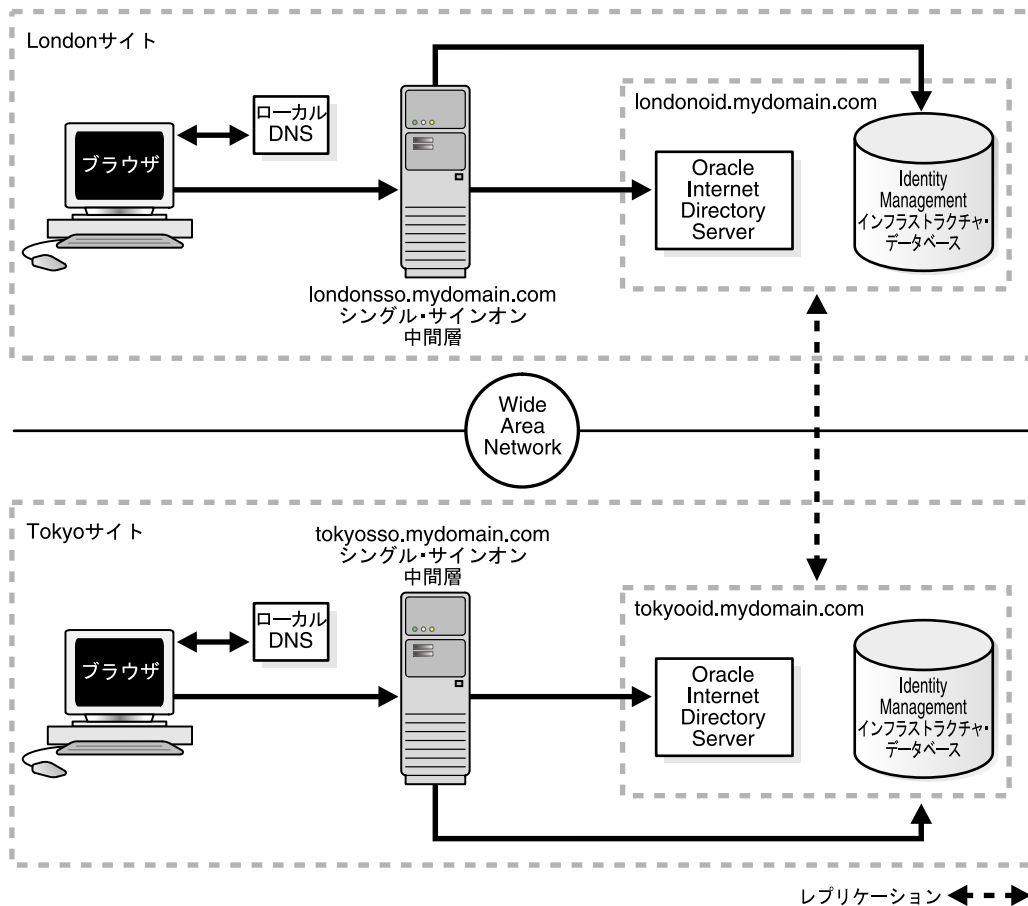
使用例

この使用例では、次の架空の構成を想定しています。

- londonso.mydomain.com と tokyosso.mydomain.com の2つのシングル・サインオン中間層があります。Single Sign-On Server の有効なアドレスは sso.mydomain.com です。
- 2つのシングル・サインオン中間層 (londonoid.mydomain.com、tokyoid.mydomain.com) に2つのディレクトリ・サーバーと Identity Management インフラストラクチャ・データベースが関連付けられています。
- レプリケーションにおいては、londonoid.mydomain.com がマスター定義サイト (MDS) になります。このサイトではレプリケーション・スクリプトが実行され、データが最初にレプリケートされます。tokyoid.mydomain.com はリモート・マスター・サイト (RMS) になります。このサイトは、データのレプリケート先のサイトです。
- シングル・サインオン中間層と Identity Management インフラストラクチャ・データベースは、異なるコンピュータに配置されています。

9-23 ページの図 9-6 は、この地理的に分散しているシステムの配置後の構成を示しています。

図 9-6 地理的に分散している高可用性シングル・サインオン・システム



構成手順

図 9-6 に示す地理的に分散しているシングル・サインオン・システムは、「複数のシングル・サインオン中間層、1 つの Oracle Internet Directory」と「レプリケーション用の識別情報管理データベースの構成」で示した手順を組み合わせたものです。

1. MDS (londonoid.mydomain.com) と RMS (tokyooid.mydomain) に Oracle Internet Directory をインストールし、これらのサーバーをレプリケーション・グループとして設定します。詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。この手順には、インストールとレプリケーションの両方が含まれています。レプリケーションの概念については、『Oracle Internet Directory 管理者ガイド』を参照してください。
2. OracleAS Infrastructure を中間層 londonosso.mydomain.com にインストールし、オプション「Identity Management」を選択します。このインストール・タイプのコンポーネント・リストが表示されたら、「Single Sign-On」のみを選択します。Oracle Universal Installer で、このシングル・サインオン・インスタンスに名前を付けるように求められたら、londonoid.mydomain.com と入力します。
3. 中間層 tokyosso.mydomain.com で手順 2 を繰り返します。ここでは、tokyooid.mydomain.com にあるディレクトリ・サーバーを Single Sign-On Server に関連付ける必要があります。
4. Single Sign-On スキーマのパスワードを MDS と RMS のデータベース間で同期化します。この作業を行うには、「レプリケーション用の識別情報管理データベースの構成」の手順 2 と 3 を実行します。
5. 2 つのシングル・サインオン・インスタンスは別々の場所で実行されていますが、パートナ・アプリケーションに公開されている有効なサーバー URL は 1 つだけです。この URL を使用できるように Single Sign-On Server を構成します。この使用例では、この URL を sso.mydomain.com と呼びます。詳細は、「シングル・サインオン中間層での Oracle HTTP Server の構成」の項を参照してください。
6. シングル・サインオン中間層を指す、DNS エイリアスの sso.mydomain.com を追加します。シングル・サインオン認証が必要なときに、ユーザーを最も近い中間層にルーティングするように DNS サーバーを構成します。たとえば、London ユーザーが http://sso.mydomain.com にリダイレクトされる時、DNS サーバーはそのユーザーを http://londonosso.mydomain.com にルーティングする必要があります。同様に http://sso.mydomain.com にリダイレクトされる Tokyo ユーザーは、http://tokyosso.mydomain.com にルーティングする必要があります。

高機能の DNS サーバー製品の中には、地理的位置に基づいてユーザーを最寄りのサーバーにルーティングできるものもあります。

その他の高可用性の配置

OracleAS は、シングル・サインオンやその他の OracleAS コンポーネントで、コールド・フェイルオーバー・クラスタ、障害時リカバリ、バックアップおよびリカバリをサポートしています。

OracleAS Cold Failover Cluster

コールド・フェイルオーバー・クラスタは、ネットワーク・サービスの単一ビューを連携して提供する、疎結合のコンピュータのグループです。1 次ノードで障害が発生した場合は、クラスタ・ソフトウェアによって 1 次ノードの論理 IP アドレスと処理を 2 次ノードに移動できます。インフラストラクチャを実行しているノードはホットと呼ばれます。引き継ぎを待機しているノードはコールドと呼ばれます。このため、コールド・フェイルオーバーという用語が使用されます。

コールド・フェイルオーバー・クラスタの詳細は、『Oracle Application Server 10g 高可用性ガイド』の「Infrastructure の高可用性」の章を参照してください。

障害時リカバリ

障害時リカバリの配置は、構成が同一の 2 つのサイト、プライマリ（本番）とセカンダリ（スタンバイ）で構成されます。2 つのサイトは、地理的に離れ、Wide Area Network で接続されていることもあります。障害のためにプライマリ・サイトが使用できない場合は、適切な時間内にセカンダリ・サイトを操作可能にできます。クライアントのリクエストは、本番の役割を担うサイトに常にルーティングされます。フェイルオーバーの発生後、クライアントのリクエストはセカンダリ・サイトにルーティングされ、その後セカンダリ・サイトは本番の役割を引き継ぎます。プライマリ・サイトとセカンダリ・サイトには同一の中間層サーバーが配置されており、これらのサーバーは 2 つのサイト間でも同一です。障害時のリカバリの詳細は、『Oracle Application Server 10g 高可用性ガイド』のこのトピックに関する章を参照してください。

バックアップおよびリカバリ

バックアップおよびリカバリは、データ損失の防止と損失データの復元についての方針と手順を述べるときに使用する用語です。バックアップおよびリカバリの詳細は、『Oracle Application Server 10g 管理者ガイド』のこのトピックに関する章を参照してください。

識別情報管理データベースのレプリケート

この項では、識別情報管理データベースを複数のインスタンス間でレプリケートする方法について説明します。OracleAS Single Sign-On と Oracle Internet Directory は、データベース表をレプリケートするスクリプトと手順を共有しています。次の事項を十分に理解してからこの項に進んでください。

- 『Oracle Internet Directory 管理者ガイド』のディレクトリ・レプリケーションの概念に関する項
- 『Oracle Internet Directory 管理者ガイド』の Oracle ディレクトリのレプリケーション管理に関する項
- 『Oracle Internet Directory 管理者ガイド』のレプリケーション管理コマンドライン・ツールの構文に関する項

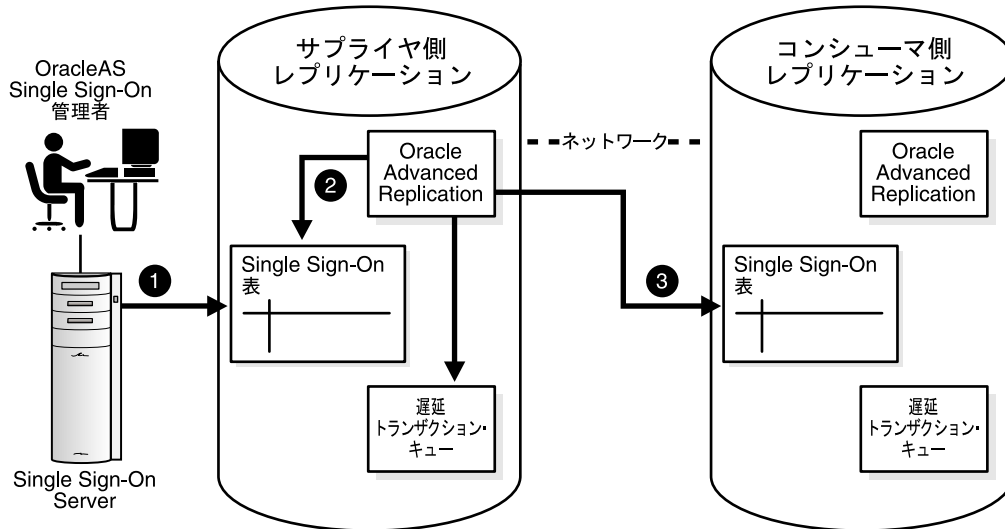
この項の項目は次のとおりです。

- [レプリケーションのメカニズム](#)
- [レプリケーション用の識別情報管理データベースの構成](#)
- [レプリケーション・グループへのノードの追加](#)
- [レプリケーション・グループからのノードの削除](#)

レプリケーションのメカニズム

Identity Management インフラストラクチャでは、2つのデータベース間の表のレプリケーションに Advanced Replication を使用します。この機能は、データの変更を複数のデータベースに非同期に伝播します。つまり、サブライヤは変更をシングル・サインオン表に書き込み、バッチされた変更をコンシューマに定期的に送信します。コンシューマは、このデータをレプリケートするサーバーです。地理的に分散している複数のシステムで、すべてのサーバーがデータを伝播または受信できます。この配置をマルチマスター・レプリケーションと呼びます。図 9-7 にそのプロセスを示します。

図 9-7 マルチマスター・レプリケーションのアーキテクチャ



1. Single Sign-On 管理者は Single Sign-On 管理アプリケーションを使用して Single Sign-On パートナ・アプリケーションまたは構成データを変更します。このプロセスでは、Identity Management インフラストラクチャ・データベースの対応する表エントリが変更されます。
2. Advanced Replication によって、遅延トランザクション・キューに変更がコピーされます。
3. Advanced Replication は、スケジュールされた間隔で、遅延トランザクション・キューのトランザクションをコンシューマ側のシングル・サインオン表にプッシュします。

レプリケーション用の識別情報管理データベースの構成

『Oracle Internet Directory 管理者ガイド』でマルチマスター・レプリケーションの概念を理解してからこの項に進んでください。

また、「**地理的に分散している複数のシングル・サインオン・インスタンス**」で示した配置例について理解しておくこともお薦めします。この項では、シングル・サインオン・レプリケーションが発生する状況について説明します。

識別情報管理データベースでレプリケーションを使用可能にする作業手順を次に示します。

1. 『Oracle Internet Directory 管理者ガイド』の操作手順に従って、マルチマスター・レプリケーション・グループをインストールして構成します。シングル・サインオン表は、このプロセスにおいてレプリケートされます。
2. レプリケーション・スクリプトの実行後、管理者はスクリプトを実行してレプリケート・ノード間でスキーマのパスワードを同期化し、Single Sign-On Server とディレクトリ間の接続を確立する必要があります。

MDS で ssoReplSetup.jar ツールを実行し、Single Sign-On スキーマのパスワードを MDS と RMS のデータベース間で同期化します。この手順を RMS ごとに繰り返します。表 9-1 は、このツールのパラメータの定義です。

スクリプトを実行する手順は次のとおりです。

- a. \$ORACLE_HOME/sso/lib に移動します。
- b. 次のスクリプトを実行します。

```
$ORACLE_HOME/jdk/bin/java -jar ssoReplSetup.jar mds_oid_host mds_oid_port
mds_oid_admin mds_oid_password rms_oid_host rms_oid_port rms_oid_admin
rms_oid_password rms_db_sys_password
```

表 9-1 ssoReplSetup のパラメータ

| パラメータ | 説明 |
|-------------------------|-----------------------------------|
| <i>mds_oid_host</i> | MDS ディレクトリ・サーバーのホスト名。 |
| <i>mds_oid_port</i> | MDS ディレクトリ・サーバーのポート番号。 |
| <i>mds_oid_admin</i> | バインド DN: MDS ディレクトリ・サーバーへのユーザー認証。 |
| <i>mds_oid_password</i> | MDS ディレクトリ・サーバーのバインド・パスワード。 |
| <i>rms_oid_host</i> | RMS ディレクトリ・サーバーのホスト名。 |
| <i>rms_oid_port</i> | RMS ディレクトリ・サーバーのポート番号。 |
| <i>rms_oid_admin</i> | バインド DN: RMS ディレクトリ・サーバーへのユーザー認証。 |
| <i>rms_oid_password</i> | RMS ディレクトリ・サーバーのバインド・パスワード。 |

表 9-1 ssoReplSetup のパラメータ (続き)

| パラメータ | 説明 |
|----------------------------------|------------------------|
| <code>rms_db_sys_password</code> | RMS データベースの SYS パスワード。 |

- デフォルトでは、HTTP を介して Oracle Internet Directory と通信するように、`ssoReplSetup` によって RMS の Single Sign-On Server が構成されます。かわりに SSL 接続を使用する場合は、RMS ノードで `ssooconf.sql` スクリプトを実行し、ディレクトリのホスト名、ポートおよび SSL 設定を要求に応じて指定します。Single Sign-On Server のホスト名、ポートおよびパスワードが (この順序で) 要求されたら、単純に [Return] または [Enter] を押します。SSL 値が要求されたら、Y を入力します。

`ssooconf.sql` を実行するには、第 3 章の「ディレクトリ・アクセス用 Single Sign-On Server の設定変更」の操作手順に従います。

注意: 追加する RMS ノードごとに手順 2 と 3 を繰り返します。

レプリケーション・グループへのノードの追加

既存のシングル・サインオン・レプリケーション・グループにノードを追加する場合、Oracle Internet Directory をこのノードにレプリケートしていないときは、『Oracle Internet Directory 管理者ガイド』の操作手順に従います。この新しいノードをシングル・サインオン用に構成するには、シングル・サインオン中間層をインストールして、「レプリケーション用の識別情報管理データベースの構成」の手順 2 と 3 を繰り返します。

レプリケーション・グループからのノードの削除

シングル・サインオン・レプリケーション・グループからノードを削除するには、『Oracle Internet Directory 管理者ガイド』の操作手順に従います。

プロキシ・サーバーを使用する OracleAS Single Sign-On の配置

OracleAS Single Sign-On の前段にはリバース・プロキシを配置できます。プロキシは、次の様々な機能を備えています。

- Single Sign-On Server のホスト名を非表示にします。
- Single Sign-On Server ではなくプロキシで SSL 接続を終了します。
- ファイアウォールで公開するポート数を制限します。

Single Sign-On Server の前段で使用するプロキシには、以降の構成を適用します。これらの構成は、OracleAS Single Sign-On とプロキシ・サーバーがインストール済であることを前提としています。プロキシをインストールするには、プロキシのベンダーから提供されている操作手順に従ってください。

注意： 操作手順については仮想ホストも同様です。仮想ホストをインストールするには、Oracle HTTP Server に関するドキュメントを参照してください。

IP チェックの無効化

Single Sign-On Server の前段で、特定の範囲にわたるプロキシ・アドレスを使用しているネットワーク構成では、シングル・サインオンの IP チェック機能をオフにする必要があります。IP チェックはデフォルトではオフになっていますが、これを確認するには「SSO Server の編集」ページに移動する必要があります。このページにアクセスする方法については、第 2 章の「[管理ページへのアクセス](#)」の項を参照してください。「SSO Server の編集」ページが表示されたら、「SSO Server に出されたリクエストの IP アドレスを確認します」ボックスの選択が解除されていることを確認します。

プロキシ・サーバーの有効化

プロキシ・サーバーを有効にする手順は次のとおりです。

1. シングル・サインオン中間層で `ssocfg` スクリプトを実行します。このスクリプトによって、Single Sign-On Server に格納されているホスト名がプロキシのホスト名に変更されます。次のコマンドの構文を使用して、プロキシ・サーバーのプロトコル、ホスト名およびポートの値を入力します。

- UNIX:

```
$ORACLE_HOME/sso/bin/ssocfg.sh http proxy_server_name proxy_port
```

- Windows NT/2000:

```
%ORACLE_HOME%\sso\bin\ssocfg.bat http proxy_server_name proxy_port
```

サーバーが SSL 用に構成されている場合は、`http` を `https` に置き換えます。

`ssocfg` を実行したら、シングル・サインオン中間層で `targets.xml` ファイルを更新します。詳細は、「[targets.xml の更新](#)」の項を参照してください。

2. シングル・サインオン中間層の `httpd.conf` ファイルに以降の行を追加します。このファイルは `$ORACLE_HOME/Apache/Apache/conf` に格納されています。

- a. これらの行によって、ディレクティブ `ServerName` が実際のサーバー名からプロキシ名に変更されます。

```
KeepAlive off
ServerName proxy_host_name
Port proxy_port
```

SSL を使用している場合は、ポートに 4443 などの SSL ポートを指定する必要があります。

- b. (SSL のみ) ブラウザとプロキシ・サーバー間で SSL 通信を構成している場合は、中間層に `mod_certheaders` を構成します。このモジュールによって、Oracle HTTP Server では、SSL リクエストとして受信する HTTP プロキシ・リクエストを処理できるようになります。

これらのステップは `httpd.conf` ファイルの末尾に追加できます。順番は重要ではありません。

- * 次の行を入力します。

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

- * OracleAS Web Cache をプロキシとして使用する場合は、次の行を入力します。

```
AddCertHeader HTTPS
```

他のプロキシを使用する場合は、次の行を入力します。

```
SimulateHttps on
```

3. シングル・サインオン中間層で `mod_osso` を登録します。この手順によって、実際のホスト名のかわりにプロキシのホスト名を使用するように `mod_osso` を構成します。登録ツールの実行方法については、第 4 章の「[mod_osso の登録](#)」の項を参照してください。
4. シングル・サインオン中間層を再起動します。手順については、第 2 章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。
5. 複数のシングル・サインオン中間層を配置する場合は、追加する中間層ごとに手順 2～4 を繰り返します。
6. 次のシングル・サインオン・ログイン URL を使用して、Single Sign-On Server にログインします。

```
http://proxy_host_name:proxy_port/pls/orasso/
```

この URL によって、Single Sign-On ホームページが表示されます。ログインできる場合は、プロキシが正しく構成されています。

ユーザー・ニックネームの変更におけるディレクトリ同期の設定

Single Sign-On データベースでは、外部アプリケーションのユーザー・データの格納と参照にユーザー・ニックネームを使用します。ニックネームの属性値が Oracle Internet Directory で変更されると、ユーザーは、新しいユーザー ID でログインするときに資格証明を再入力する必要があります。ユーザーの便宜を図るために、ディレクトリと Single Sign-On データベース間でユーザー名の変更を自動的に同期することができます。Directory Integration Platform によるこの同期メカニズムは、ユーザーのエントリがディレクトリから削除されると、外部アプリケーションのデータを Single Sign-On データベースから削除します。

ディレクトリと Single Sign-On データベース間でニックネームの変更を同期化する手順は次のとおりです。

1. Directory Integration Platform サーバーを起動します。詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。
2. Directory Integration Platform 同期パッケージをロードします。最初に、\$ORACLE_HOME/sso/admin/plsql/sso に移動して Single Sign-On スキーマに接続します。

```
sqlplus orasso/password
```

パスワードの取得方法については、付録 B を参照してください。

3. 次のパッケージを順番に実行します。

```
SQL> @ssodip.sql  
SQL> @ssodip.pks  
SQL> @ssodip.pkb
```

4. シングル・サインオン・プロファイルを Oracle Internet Directory に登録します。この作業を行うには、次の構文でプロビジョニング・サブスクリプション・ツール (oidprovtool) を実行します。

```
$ORACLE_HOME/bin/oidprovtool  
operation=create  
ldap_host=oid_host  
ldap_port=oid_port  
ldap_user_dn=cn=orcladmin ldap_user_password=orcladmin_password  
schedule=synchronization_interval_in_seconds  
organization_dn=realm_DN  
application_dn=orclApplicationCommonName=ORASSO_SSOSERVER,cn=SSO,  
cn=Products,cn=OracleContext  
interface_name=LDAP_NOTIFY interface_type=PLSQL  
interface_connect_info=sso_database_host:sso_database_port:sso_database_  
SID:orasso:orasso_schema_password  
event_subscription=USER:user_search_base_for_realm:ADDnickname  
event_subscription=USER:user_search_base_for_realm:MODIFYnickname  
event_subscription=USER:user_search_base_for_realm:DELETE
```

レルムを変更する場合は、プロフィールを登録します。ニックネーム属性やユーザー検索ベースを変更する場合などです。

oidprovtool の使用に関する詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

5. Directory Integration Platform の権限を ORASSO のプロキシに付与します。これには、ディレクトリの ORASSO エントリを変更します。

最初に、次の構文で LDIF ファイルを作成します。

```
dn: orclApplicationCommonName=ORASSO_SSOSERVER,cn=SSO,cn=Products,
cn=OracleContext
changetype: modify
add: orclaci
orclaci: access to entry by group="cn=odisgroup,cn=odi,cn=oracle internet
directory" (proxy)
```

6. スーパー・ユーザー cn=orcladmin として、LDIF ファイルをディレクトリにロードします。

7. Directory Integration Platform が実行中であることを確認します。

これらの手順が完了している場合は、同期化が行われ、ユーザーが新規ユーザー ID でログインすると、ただちに外部アプリケーションの情報を利用できます。

アプリケーション・サービス・プロバイダに対するサポートの有効化

この章では、Oracle Identity Management インフラストラクチャの単一インスタンスで複数のレルムをサポートできるように Single Sign-On Server を有効にする方法を説明します。

この章の項目は次のとおりです。

- [アプリケーション・サービス・プロバイダ](#): 複数のレルムの配置に関する決定
- [複数のレルムのセットアップと有効化](#)
- [Single Sign-On Server](#) による複数のレルムの認証の有効化
- [複数のレルムに対する Single Sign-On Server の構成](#)
- [複数のレルム用の管理権限の付与](#)

アプリケーション・サービス・プロバイダ:複数のレルムの配置に関する決定

アプリケーション・サービス・プロバイダとは、Oracle アプリケーションや Oracle 以外のアプリケーションをインストールしてメンテナンスし、通常は有料でこれらのアプリケーションを顧客が利用できるようにする企業です。このような企業は、同一のアプリケーション・インスタンスで複数のユーザーのグループにサービスを提供することで、規模拡大による収益率の向上を図ります。アプリケーション・サービス・プロバイダは、Oracle Identity Management インフラストラクチャの単一インスタンス内で異なるレルム（または異なるネームスペース）を使用して、別々の顧客に一意の Oracle 構成情報を設定し、格納する場合があります。

複数のレルムを配置するかどうかを決定する際にはユーザー ID が唯一の判断基準であり、ID 間で競合が存在しない場合は、単一のデフォルト・レルムでユーザーを管理することをお勧めします。アプリケーション・サービス・プロバイダのユーザーは、一意の電子メール ID でログインする場合があります。ユーザー ID 間で競合がある場合は、レルムを別々にする必要があります。複数のレルムの配置は、Oracle 10g の中間層コンポーネントと顧客アプリケーションの配置方法に影響する点にも注意してください。

注意： Oracle Identity Management の詳細は、『Oracle Identity Management 概要および配置プランニング・ガイド』を参照してください。

複数のレルムのセットアップと有効化

複数のレルムのセットアップ作業では、OracleAS Single Sign-On を上回るリソースと管理オーバーヘッドが必要となる場合があります。このプロセスには他のコンポーネントが関係します。レルムの構成は実際に、次の 3 つから成るプロセスです。

- Oracle Internet Directory でのレルムの作成
- OracleAS Single Sign-On での複数のレルムの有効化
- パートナ・アプリケーションによる識別情報管理レルムの認識

最初のプロセスについては、『Oracle Internet Directory 管理者ガイド』を参照してください。2 番目のプロセスは、この章で説明します。3 番目のプロセスは、製品関連のドキュメントを参照してください。

Single Sign-On Server による複数のレルムの認証の有効化

複数のレルムに対するシングル・サインオンの認証シーケンスは、単一のデフォルト・レルムでのシングル・サインオンの場合とほぼ同様です。ユーザーにとって唯一異なる点は、レルムの最初のタイプに属していたユーザーにログイン画面が表示されたときに（[10-4 ページ](#)の [図 10-1](#) を参照）、ユーザーはユーザー名とパスワードだけでなく、新しい資格証明（レルム・ニックネーム）も入力する必要がある点です。入力する値の大 / 小文字は、区別されません。

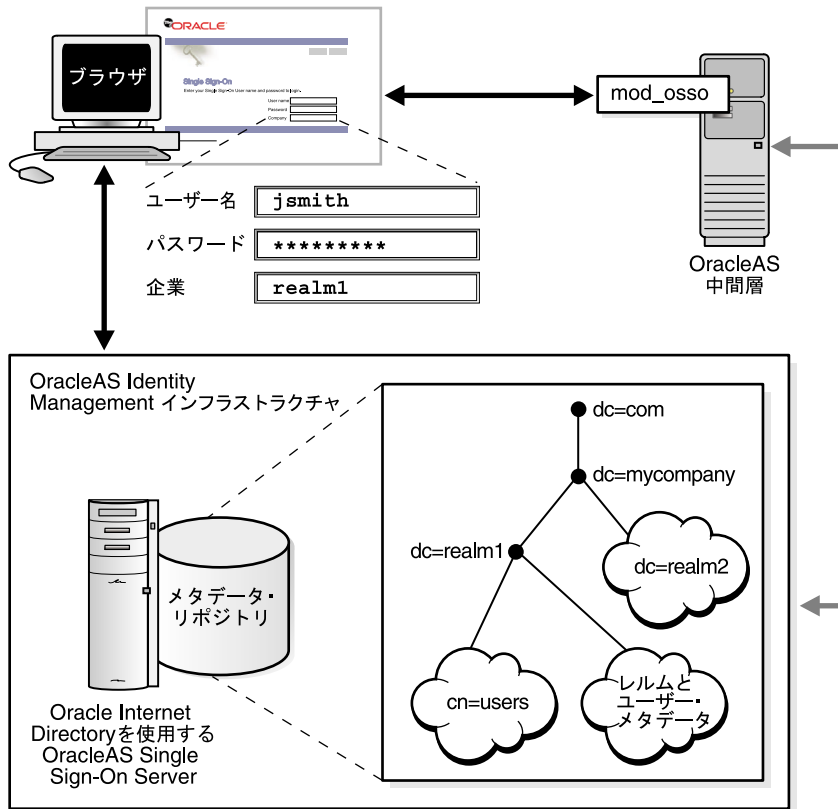
この項の項目は次のとおりです。

- [Oracle Internet Directory](#) でのレルムの検索
- [パートナ・アプリケーション](#)でのレルムに属するユーザーの検証

Oracle Internet Directory でのレルムの検索

ユーザーが資格証明を入力すると、レルム・ニックネームとユーザー名が [Oracle Internet Directory](#) 内のエンTRIES にマップされます。具体的には、[Single Sign-On Server](#) がディレクトリ・メタデータを使用して、[Oracle Internet Directory](#) 内のレルムのエンTRIES を検索します。レルムのエンTRIES を検出すると、[Single Sign-On Server](#) はレルム・メタデータを使用してユーザーを検索します。ユーザーのエンTRIES が検出されると、パスワード（エンTRIES の属性）が検証されます。パスワードの検証が完了すると、ユーザーは認証されます。

図 10-1 全体図：複数のレルムでのシングル・サインオン



パートナ・アプリケーションでのレルムに属するユーザーの検証

同じニックネームを持ち、異なるレルムに属する 2 人のユーザーが存在する場合、パートナ・アプリケーションではこれらのユーザーを区別するメカニズムが必要になります。パートナ・アプリケーションではコンテンツ（株価ニュースと株式相場表を表示する OracleAS Portal ページなど）を要求するレルムのニーズに合うようにコンテンツを対応させる必要があるため、このようなメカニズムが必要となります。したがって、OracleAS リリース 9.0.4 では `mod_osso` に渡される属性として、レルム・ニックネーム、レルム DN、レルム GUID が追加されています。`mod_osso` によって Cookie が設定され、取得された属性が HTTP ヘッダーとして格納されます。提供するコンテンツを決定する場合、アプリケーションではファンクション・コールを使用して `mod_osso` ヘッダーからこれらの属性の 1 つを取得することもあります。

`mod_osso` ヘッダーと、`mod_osso` ヘッダーへのアクセスに使用するメソッドの詳細は、『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』の付録 D を参照してください。

10-6 ページの図 10-2 では、`mod_osso` で実行されるアプリケーションが、どのように 2 人のユーザーの HTTP ヘッダーを認識するかを示しています。2 人のユーザーは同じニックネームを持ち、異なるレルムに属しています。アプリケーションでは太字のヘッダーを使用して、2 人のユーザーを区別します。この場合のホスト（またはデフォルト・レルム）は `mycompany.com` です。

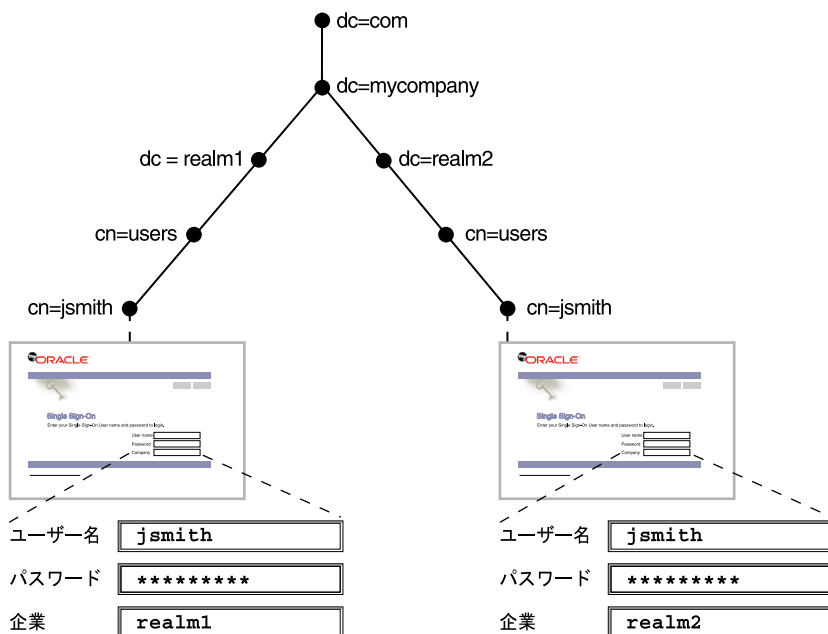
図 10-2 同じ名前を持つユーザーの mod_osso ヘッダー

```

レルム 1
REMOTE_USER = "jsmith"
HTTP_OSSO_USER_DN = "cn=jsmith,cn=users,dc=realm1,dc=mycompany,dc=com"
HTTP_OSSO_USER_GUID = "5D92F6E61F7A4CA7854BF59BA890EBFC"
HTTP_OSSO_SUBSCRIBER = "REALM1"
HTTP_OSSO_SUBSCRIBER_DN = "dc=realm1,dc=mycompany,dc=com"
HTTP_OSSO_SUBSCRIBER_GUID = "F76B7C1945AB4F8DB9391B45D3021334"
    
```

```

レルム 2
REMOTE_USER = "jsmith"
HTTP_OSSO_USER_DN = "cn=jsmith,cn=users,dc=realm2,dc=mycompany,dc=com"
HTTP_OSSO_USER_GUID = "6786605E41604E18B74D5B90708F5CA4"
HTTP_OSSO_SUBSCRIBER = "REALM2"
HTTP_OSSO_SUBSCRIBER_DN = "dc=realm2,dc=mycompany,dc=com"
HTTP_OSSO_SUBSCRIBER_GUID = "D9D52D0DC8FF4B6FAF19A795B9B2EA23"
    
```



複数のレルムに対する Single Sign-On Server の構成

複数のレルムに対して Single Sign-On Server を構成する場合は、Single Sign-On スキーマで各レルムのエントリを作成します。Oracle Internet Directory に作成する各レルムには、Single Sign-On スキーマの対応するエントリが必要です。

注意：

- Oracle Internet Directory でレルムを作成してから、Single Sign-On スキーマでレルムを作成します。
 - 次の構成スクリプトは UNIX プラットフォームでのみ実行できます。Windows プラットフォームでは実行できません。
-
-

複数のレルムに対して Single Sign-On Server を構成する手順は次のとおりです。手順 1、2、5 は一度だけ実行してください。これらの手順によって、複数のレルムに対する Single Sign-On Server が有効になります。手順 3 と 4 は、レルムを追加するたびに実行する必要があります。

1. OracleAS Infrastructure がインストールされていることを確認します。このインフラストラクチャをインストールすると、Single Sign-On Server もインストールされます。
2. \$ORACLE_HOME/sso/admin/plsql/wwhost に移動します。

次の構文を使用して、enblhstg.csh スクリプトを実行します。スクリプト・パラメータの詳細は、[10-8 ページの表 10-1](#) を参照してください。

```
enblhstg.csh -mode sso
              -sc sso_schema_connect_string
              -ss orasso
              -sw sso_schema_password
              -h oid_host_name
              -p oid_port
              -d "cn=orcladmin"
              -w oid_bind_password
```

注意： Single Sign-On Server が分散配置の一部分である場合、Identity Management インフラストラクチャのコンピュータでスクリプトを実行します。

次に例を示します。

```
enblhstg.csh -mode sso
             -sc webdbsvr2:1521:s901dev3
             -ss orasso
             -sw orasso
             -h dlsun670.us.oracle.com
             -p 389
             -d "cn=orcladmin"
             -w welcome123
```

3. Oracle Internet Directory にレルムを追加します。これを行うには、『Oracle Internet Directory 管理者ガイド』の操作手順に従います。
4. Single Sign-On データベースでレルムのエントリを作成します。スクリプト \$ORACLE_HOME/sso/admin/plsql/wwhost/addsub.csh を使用します。Single Sign-On Server が分散配置の一部である場合、Identity Management インフラストラクチャでスクリプトを実行します。

次の構文を使用して、スクリプトを実行します。

```
addsub.csh -name realm_nickname
           -id realm_ID
           -mode sso
           -sc sso_schema_connect_string
           -ss sso_schema_name
           -sw sso_schema_password
           -h oid_host_name
           -p oid_port
           -d oid_bind_dn
           -w oid_bind_dn_password
           -sp sys_schema_password
```

10-8 ページの表 10-1 では、enblhstg.csh と addsub.csh のパラメータを定義します。

表 10-1 enblhstg.csh と addsub.csh のパラメータ

| パラメータ | 説明 |
|-------|---|
| -mode | この値は sso にする必要があります。 |
| -sc | Single Sign-On スキーマの接続文字列。host:port:sid の形式を使用します。 |
| -ss | Single Sign-On スキーマの名前。このパラメータは orasso にする必要があります。 |
| -sw | Single Sign-On スキーマのパスワード。取得方法については、付録 B を参照してください。 |

表 10-1 enblhstg.csh と addsub.csh のパラメータ (続き)

| パラメータ | 説明 |
|-------|---|
| -h | Oracle Internet Directory Server のホスト名。 |
| -p | Oracle Internet Directory Server のポート番号。 |
| -d | Oracle Internet Directory Server のバインド DN。このパラメータの値は cn=orcladmin です。これはディレクトリ・スーパー・ユーザーです。 |
| -w | Oracle Internet Directory スーパー・ユーザー (cn=orcladmin) のパスワード。 |
| -name | レルム・ニックネーム。これはログイン・ページの「企業」フィールドに入力する値です。 |
| -id | レルム ID。2 以上の整数を選択します。値 1 はデフォルト・レルム用に予約されています。Single Sign-On Server の内部ではレルム ID が索引として使用されます。 |
| -sp | sys スキーマのパスワード。このパスワードは、OracleAS のインストール時に選択されます。 |

注意： スクリプトで重複するサブスクリイバ・エントリについて尋ねられた場合は、既存のエントリを使用するオプションを選択します。

5. サンプルのログイン・ページを、複数のレルム用のバージョンに更新します。更新するには、login.jsp ページ (\$ORACLE_HOME/j2ee/OC4J_SECURITY/applications/sso/web/jsp 内) を編集します。

注意： 分散配置では、このファイルはシングル・サインオン中間層にあります。

ファイルのバックアップ・コピーを作成したら、次のセクションのコメントを解除します。

```
<!-- UNCOMMENT TO ENABLE MULTIPLE REALM SUPPORT
<tr>
<label>
<th id="c6"><font
class="OraFieldText"><%=msgBundle.getString(ServerMsgID.COMPANY_LBL)%></font></th>
<td headers="c6"> <INPUT TYPE="text" SIZE="30" MAXLENGTH="50"
NAME="subscribername" value=""></td>
</label>
</tr>
-->
```

6. シングル・サインオン中間層を停止して起動します。手順については、第2章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

複数のレルム用の管理権限の付与

Oracle Internet Directory では、レルムの作成時にデフォルト・レルムの DIT 構造がレルム間で伝播されます。ただし、デフォルト・レルムの DIT に存在するユーザー、グループおよび権限は、伝播されないので注意してください。ディレクトリ・スーパー・ユーザーまたはレルム管理者は、Oracle Directory Manager を使用して権限を割り当てる（再度割り当てる）必要があります。この用途でのツールの使用方法については、第2章にある「[管理権限の付与](#)」の項を参照してください。

Single Sign-On Server の監視

この章では、Oracle システム管理コンソールである Oracle Enterprise Manager を使用して、Single Sign-On Server を監視する方法を説明します。

この章の項目は次のとおりです。

- [監視用ページへのアクセス](#)
- [スタンドアロン・コンソールのホームページの解説と使用方法](#)
- [「失敗ログインの詳細」ページの表示内容と使用方法](#)
- [Single Sign-On の監視ターゲットのポート・プロパティの更新](#)

監視用ページへのアクセス

スタンドアロン・コンソールでの Single Sign-On の監視 UI は、ホームページと「失敗ログインの詳細」ページの2つのページで構成されています。ホームページには、サーバーの負荷やユーザーの動作についての一般的な情報が表示されます。「失敗ログインの詳細」ページには、特定のユーザーについての失敗したログインの統計情報が表示されます。

Single Sign-On の監視用ホームページにアクセスするには、次の手順を実行します。

1. 管理対象の Oracle Enterprise Manager インスタンスのスタンドアロン・コンソールに移動します。スタンドアロン・コンソールに移動するには、OracleAS インスタンスをホスティングしているコンピュータのホスト名と Oracle Enterprise Manager のポート番号を入力します。デフォルトのポート番号は 1812 ですが、1 ずつ大きなポート番号を選択して構成することもできます（最大 1816）。
2. OracleAS 管理者の資格証明を使用してログインします。
3. 「ファーム」ページの「スタンドアロン・インスタンス」セクションで、適切な OracleAS インスタンスを選択します。
4. 「アプリケーション・サーバー」ページの「システム・コンポーネント」リストで、Single Sign-On Server を選択します。

スタンドアロン・コンソールのホームページの解説と使用方法

ホームページ（11-3 ページの図 11-1 を参照）では、「一般」セクションに次のメトリックが表示されます。

- 状態
緑の上向き矢印によって、Single Sign-On スキーマを提供するデータベースが実行中であることが示されます。赤の下向き矢印によって、データベースが停止していることが示されます。
- 起動時間
Single Sign-On スキーマを提供するデータベースの開始時刻。
- データベース
Single Sign-On スキーマを提供するデータベースの SID/ インスタンス名。
- データベースのバージョン
Single Sign-On スキーマを提供するデータベースのバージョン。


「過去 24 時間の状態の詳細」セクションには、次のメトリックがあります。

- ログイン
- 成功ログイン
- 失敗ログイン


セクション名のとおり、24 時間前から現在までの統計情報が表示されます。

「過去 24 時間の失敗ログイン」セクションでは、24 時間以内に発生したログインの失敗数を確認できます。「過去 24 時間の失敗ログイン」表で名前を選択します。「失敗」ヘッダーの下にある関連するリンクを選択します。このリンク先には、ユーザーのログインの失敗数が含まれています。リンクをクリックすると、「失敗ログインの詳細」ページが表示されます。

図 11-1 OracleAS Single Sign-On の監視用ホームページ

Single Sign-On:orasso Page Refreshed Nov 3, 2003 4:34:57 PM 

General

Status 
 Start Time **Oct 31, 2003 6:10:36 AM**

Database **asdb**
 Database Version **9.0.1.5.0**

Last 24 Hours Status Details

Logins **31**
 Successful Logins **96.8%**
 Failed Logins **3.2%**

Login Failures During The Last 24 Hours

| Username | Failures |
|-----------|----------|
| ORCLADMIN | 1 |

Related Links

[HTTP Server](#)
[Administer via Single Sign-On Web Application](#) Single Sign-On administration requires you to authenticate as a privileged user defined in Oracle Internet Directory. Log in as 'orcladmin' or another user belonging to the 'IAS Administrators' group.

「関連リンク」セクションには、次のリンクがあります。

- HTTP Server
Oracle HTTP Server の監視用ホームページが表示されます。
- Single Sign-On Web アプリケーション経由で管理
Single Sign-On の管理用のホームページが表示されます。

「失敗ログインの詳細」ページの表示内容と使用方法

「過去 24 時間の失敗ログイン」表のリンクをクリックすると、「失敗ログインの詳細」ページ（[図 11-2](#)）が表示されます。このページの表には、特定のユーザーについてのログインに失敗した回数および関連 IP アドレスが表示されます。

図 11-2 「失敗ログインの詳細」ページ

The screenshot shows the Oracle Enterprise Manager 10g Application Server Control interface. The breadcrumb trail is: Farm > Application Server: sso123.isun6221.us.oracle.com > Single Sign-On: orasso > Details of Login Failures: ORCLADMIN. The page title is 'Details of Login Failures: ORCLADMIN'. A refresh button indicates the page was refreshed on Nov 3, 2003 5:59:39 PM. Below the title is a table with two columns: 'I.P. Address' and 'Failure Login Time'. The table contains one row with the IP address 144.25.174.159 and the failure time Nov 3, 2003 2:26:51 PM. At the bottom, there are links for 'Logs | Preferences | Help' and a copyright notice for Oracle 1996, 2003.

ORACLE Enterprise Manager 10g
Application Server Control

Logs Preferences Help

Farm > Application Server: sso123.isun6221.us.oracle.com > Single Sign-On: orasso > Details of Login Failures: ORCLADMIN

Details of Login Failures: ORCLADMIN

Page Refreshed Nov 3, 2003 5:59:39 PM

Details of Login Failures:

| I.P. Address | Failure Login Time |
|----------------|------------------------|
| 144.25.174.159 | Nov 3, 2003 2:26:51 PM |

Logs | Preferences | Help

Copyright © 1996, 2003, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control

Single Sign-On の監視ターゲットのポート・プロパティの更新

Oracle HTTP Server のポート番号を変更した場合、そのサーバー上にある Single Sign-On の監視ターゲットのポート・プロパティも変更する必要があります。次の手順を実行して、変更を適用します。

1. targets.xml ファイルをバックアップします。

```
cp $ORACLE_HOME/sysman/emd/targets.xml $ORACLE_
HOME/sysman/emd/targets.xml .backup
```

このファイルは、Oracle Enterprise Manager で監視される様々なターゲット (OracleAS Single Sign-On など) の構成ファイルです。

2. targets.xml でターゲット・タイプ oracle_sso_server を検索し、このターゲット・タイプに関連付けられた HTTP ポート値を見つけて編集します。

```
<Property NAME="HTTPPort" VALUE="7777"/>
```

3. ファイルを保存して閉じます。
4. OracleAS Console をリロードします。

```
$ORACLE_HOME/bin/emctl reload
```

注意： ポート依存性の変更の詳細は、『Oracle Application Server 10g 管理者ガイド』を参照してください。

配置固有ページの作成

OracleAS Single Sign-On のフレームワークでは、配置固有のログイン・ページ、パスワードの変更ページ、シングル・サインオフ・ページを Single Sign-On Server と統合できます。つまり、ユーザーは適切な Web テクノロジを使用して、独自のロック・アンド・フィール要件やグローバリゼーション要件に合わせてこれらのページをカスタマイズできます。ただし、オラクル社では JavaServer Pages (JSP) ページの使用をお勧めします。製品に付属のサンプル・ページは、同じフレームワークを使用して統合されています。

この章の項目は次のとおりです。

- [Single Sign-On Server](#) での配置固有ページの使用方法
- [配置固有ページの記述方法](#)
- [ページのエラー・コード](#)
- [グローバリゼーション・サポートの追加](#)
- [配置固有ページに関するガイドライン](#)
- [配置固有ページのインストール](#)
- [配置固有ページの例](#)

Single Sign-On Server での配置固有ページの使用法

シングル・サインオンのページを有効にするプロセスは、複数の手順にまとめられます。

1. ユーザーはパートナ・アプリケーションを要求し、Single Sign-On Server にリダイレクトされます。
2. ユーザーが認証されない場合、Single Sign-On Server はユーザーをサンプル・ログイン・ページにリダイレクトするか、配置固有ページにリダイレクトします（配置固有ページを使用するように構成されている場合）。このリダイレクションの一環として、[12-3 ページの表 12-1](#) に示すパラメータがページに渡されます。
3. ユーザーはログイン・ページを送信します。これにより、[12-4 ページの表 12-2](#) に示すパラメータが次の認証 URL に渡されます。

```
http://sso_host:sso_port/pls/orasso/orasso.wssso_app_admin.ls_login
```

これらのパラメータのうち少なくとも 2 つ（ssouusername、password）は変更可能なフィールドとしてページに表示されます。

4. ユーザー・パスワードの有効期限が切れるまでに十分な時間があり、Single Sign-On Server でユーザー名とパスワードが正しく検証されると、ユーザーはアプリケーションの成功 URL にリダイレクトされます。認証に失敗した場合、ユーザーはログイン・ページに再度リダイレクトされ、エラー・メッセージが表示されます。
5. ユーザー・パスワードの有効期限が近い場合は、ログイン・ページではなく、パスワードの変更ページが表示されます。また、配置固有のパスワードの変更ページを使用するようにサーバーが構成されている場合、ユーザーはこのページの URL にリダイレクトされ、[12-5 ページの表 12-3](#) に示すパラメータがページに渡されます。

注意： 手順 5 では、ディレクトリ管理者がユーザーにパスワードの変更を強制した場合、パスワードの有効期限が過ぎているかどうかにかかわらず、前述の同じ条件が当てはまります。

ユーザーは古いパスワード、新しいパスワード、確認用の新しいパスワードを入力して、パスワードの変更ページを送信します。このページからは、[12-6 ページの表 12-4](#) に示すパラメータが次のパスワードの変更 URL に渡されます。

```
http://sso_host:sso_port/sso/ChangePwdServlet
```

エラーが発生した場合、ユーザーはパスワードの変更ページにリダイレクトされ、エラー・メッセージが表示されます。エラーが発生する条件の詳細は、第 3 章の「[パスワードの変更ページの動作](#)」の項を参照してください。

パスワードの変更に成功した場合、ユーザーは、認証リクエストをトリガーしたパートナ・アプリケーション URL にリダイレクトされます。

6. ユーザーのシングル・サインオン・セッションを終了するには、作業中のパートナ・アプリケーションで「ログアウト」をクリックします。これにより、アプリケーションのログアウト URL が同時にコールされ、ユーザーはすべてのアプリケーションからログアウトされ、シングル・サインオン・セッションが終了します。
7. ユーザーは、シングル・サインオフ・ページを表示する Single Sign-On Server にリダイレクトされます。配置固有ページを使用するようにサーバーが構成されている場合、ユーザーはこのページの URL にリダイレクトされ、12-7 ページの表 12-5 に示すパラメータがページに渡されます。
8. ユーザーはシングル・サインオフ・ページで「戻る」をクリックすると、ログアウトを開始したアプリケーションに戻ることができます。

配置固有ページの記述方法

ログイン・ページ、パスワードの変更ページおよびシングル・サインオフ・ページの URL では、ページが適切に動作するために、以降の表に示すパラメータを受け入れる必要があります。

この項の項目は次のとおりです。

- ログイン・ページのパラメータ
- パスワードを忘れた場合
- パスワードの変更ページのパラメータ
- シングル・サインオフ・ページのパラメータ

ログイン・ページのパラメータ

ログイン・ページの URL では、12-3 ページの表 12-1 に示すパラメータを受け入れる必要があります。

表 12-1 Single Sign-On Server によってページに送信されるログイン・ページのパラメータ

パラメータ	説明
site2pstoretoken	ログイン処理用の認証リクエスト・トークンが含まれます。
ssousername	ユーザー名が含まれます。
p_error_code	認証時にエラーが発生した場合、VARCHAR2 型のエラー・コードが含まれます。
p_cancel_url	「取消」がクリックされたときにリダイレクトする URL が含まれません (ログイン・ページに「取消」ボタンがある場合)。この URL は、ログアウトを開始したパートナ・アプリケーションのホーム URL を指します。

ログイン・ページでは、表 12-2 に示すパラメータを次の認証 URL に渡す必要があります。

```
http://sso_host:sso_port/pls/orasso/orasso.wvssso_app_admin.ls_login
```

表 12-2 ページから Single Sign-On Server に送信されるログイン・ページのパラメータ

パラメータ	説明
site2pstoretoken	ログイン処理のリダイレクト URL 情報が含まれます。
ssusername	ユーザー名が含まれます。UTF-8 形式でエンコードされている必要があります。
password	ユーザーによって入力されたパスワードが含まれます。UTF-8 形式でエンコードされている必要があります。
subscribername	レلمが有効な場合のサブスクリバ・ニックネーム。UTF-8 形式でエンコードされている必要があります。 注意: このフィールドは、Single Sign-On Server で複数のレلمが有効な場合にのみ、ログイン・ページで必須になります。
locale	ユーザーの言語 (オプション)。ISO 形式にする必要があります。 例: フランス語の場合は fr-fr 「グローバル化・サポートの追加」の項を参照してください。
v	ページ・バージョンが含まれます。推奨されていますが、オプションです。パラメータが渡される場合、値は v1.4 にする必要があります。

ログイン・ページには少なくとも、パラメータ名が `ssusername` のテキスト・フィールドと、パラメータ名が `password` のパスワード・フィールドが必要です。これらの値は認証 URL に送信されます。ログイン・ページからは、`site2pstoretoken` も隠しパラメータとして送信する必要があります。

ログイン・ページでは、これらのパラメータの送信に加え、`p_error_code` に指定された適切なエラー・メッセージの表示、「取消」がクリックされた場合の `p_cancel_url` へのリダイレクトが行われます。

パスワードを忘れた場合

配置固有ページには、ユーザーがパスワードをリセットするためのリンクを構成できます。この URL からは、Oracle Delegated Administration Service のホームページまたは Oracle Delegated Administration Service 内の「パスワードを忘れた場合」リンクに移動できます。「パスワードを忘れた場合」リンクをクリックしたユーザーには質問が用意されています。その質問に正確に答えないと、ユーザーはパスワードをリセットできません。

Oracle Delegated Administration Service は通常、OracleAS Single Sign-On と同じコンピュータで、次のフォームの URL によってアクセスできます。

```
http://sso_host:sso_port/oiddas/
```

「パスワードを忘れた場合」のログイン・ページを構成するには、『Oracle Internet Directory アプリケーション開発者ガイド』の第 10 章「DAS_URL インタフェース・リファレンス」を参照してください。

パスワードの変更ページのパラメータ

パスワードの変更ページの URL では、表 12-3 に示すパラメータを受け入れる必要があります。

表 12-3 パスワードの変更ページに送信されるパラメータ

パラメータ	説明
p_username	ページの上に表示されるユーザー名が含まれます。
p_subscribername	ホスティングが有効な場合のサブスクライバ・ニックネーム。 注意：このフィールドは、ログイン・ページに必須です。
p_error_code	前回のパスワード変更時にエラーが発生していた場合、文字列形式のエラー・コードが含まれます。
p_done_url	パスワードの保存後に戻る、ページの URL が含まれます。
site2pstoretoken	パスワードの有効期限が過ぎているか、近い場合に、LS_LOGIN ルーチンから要求される site2pstoretoken が含まれます。
p_pwd_is_exp	パスワードの有効期限が過ぎているか、近いことを示すフラグ値が含まれます。
locale	ユーザーの言語（オプション）。ISO 形式にする必要があります。 例：フランス語の場合は fr-fr 「グローバル化・サポートの追加」の項を参照してください。

パスワードの変更ページでは、表 12-4 に示すパラメータを次のパスワードの変更 URL に渡す必要があります。

`http://sso_host:sso_port/sso/ChangePwdServlet`

表 12-4 ページで送信されるパスワードの変更ページのパラメータ

パラメータ	説明
<code>p_username</code>	ページの上に表示されるユーザー名が含まれます。パスワードの変更ページから、隠しフィールドとして送信する必要があります。UTF-8 形式でエンコードされている必要があります。
<code>p_old_password</code>	古いパスワードが含まれます。UTF-8 形式でエンコードされている必要があります。
<code>p_new_password</code>	新しいパスワードが含まれます。UTF-8 形式でエンコードされている必要があります。
<code>p_new_password_confirm</code>	新しいパスワードの確認入力が含まれます。UTF-8 形式でエンコードされている必要があります。
<code>p_done_url</code>	パスワードの保存後に戻る、ページの URL が含まれます。
<code>p_pwd_is_exp</code>	パスワードの有効期限が過ぎているか、近いことを示すフラグ値が含まれます。
<code>site2pstoretoken</code>	ログイン処理のリダイレクト URL 情報が含まれます。
<code>p_action</code>	変更をコミットします。値は OK (コミット) または CANCEL (無視) にする必要があります。
<code>p_subscribername</code>	ページの上に表示されるユーザー名が含まれます。
<code>p_request</code>	ユーザーが要求する、保護された URL。
<code>locale</code>	ユーザーの言語 (オプション)。ISO 形式にする必要があります。 例: フランス語の場合は <code>fr-fr</code> 「グローバル化・サポートの追加」の項を参照してください。

パスワードの変更ページには、少なくとも `p_old_password`、`p_new_password`、`p_new_password_confirm` の 3 つのパスワード・フィールドが必要です。このページでは、これらのフィールドをパスワードの変更 URL に送信する必要があります。

パスワードの変更ページからは、隠しパラメータとして `p_done_url` もパスワードの変更 URL に送信する必要があります。また、`p_error_code` の値に応じて、エラー・メッセージを表示する必要があります。

シングル・サインオフ・ページのパラメータ

シングル・サインオフ・ページの URL では、表 12-5 に示すパラメータを受け入れる必要があります。

表 12-5 シングル・サインオフ・ページに送信されるパラメータ

パラメータ	説明
p_app_name [1..n]	ページの上に表示されるアプリケーション名が含まれます。変数 n は、シングル・サインオフで管理するパートナ・アプリケーションの数です。
p_app_logout_url [1..n]	アプリケーションのログアウト URL が含まれます。変数 n は、シングル・サインオフで管理するパートナ・アプリケーションの数です。
p_done_url	戻るページの URL が含まれます。この URL により、ユーザーはログアウトを開始したアプリケーションに戻ります。
locale	ユーザーの言語 (ISO 形式)。ログイン時にユーザーが同じ値を渡さない場合にのみ、送信されます。

ページのエラー・コード

ログイン・ページおよびパスワードの変更ページの URL では、ページが適切に動作するために、以降の表に示すプロセス・エラーを受け入れる必要があります。

ログイン・ページのエラー・コード

ログイン・ページでは、表 12-6 に示すエラー・コードを処理する必要があります。

表 12-6 ログイン・ページのエラー・コード

p_error_code の値	対応するエラー
acct_lock_err	ユーザーがログインに失敗した回数が多すぎます。
pwd_expiry_warn_err	ユーザー・パスワードの有効期限が近づいています。
pwd_exp_err	ユーザー・パスワードがすでに期限切れです。
pwd_force_change_err	ユーザーはパスワードを変更する必要があります。
pwd_grace_login_err	ユーザー・パスワードはログイン猶予期間内です。
null_uname_pwd_err	ユーザー名が入力されていません。
auth_fail_exception	認証に失敗しました。
null_password_err	パスワードが入力されていません。

表 12-6 ログイン・ページのエラー・コード (続き)

p_error_code の値	対応するエラー
sso_cookie_expired_err	ログイン Cookie の有効期限が過ぎています。再度ログインする必要があります。
unexpected_exception	認証時に予期しないエラーが発生しました。
unexp_err	予期しないエラーが発生しました。
internal_server_err	サーバーの内部エラーです。
internal_server_try_again_err	サーバーの内部エラーです。再度試してください。
gito_err	アクティビティがないため、ユーザーのセッションがタイムアウトしました。再度ログインする必要があります。
paranoid_login_err	ユーザーはアプリケーションにアクセスするために再度サインオンする必要があります。
cert_auth_err	証明書によるサインオンに失敗しました。証明書が有効であることを確認し、有効でなければ管理者に連絡してください。

パスワードの変更ページのエラー・コード

パスワードの変更ページでは、[表 12-7](#) に示すエラー・コードを処理する必要があります。

表 12-7 パスワードの変更ページのエラー・コード

p_error_code の値	対応するエラー
confirm_pwd_fail_txt	古いパスワードと新しいパスワードが一致しません。
pwd_expiry_warn_err	パスワードの有効期限が近づいています。
pwd_force_change_err	ユーザーは先に進む前に、パスワードを変更する必要があります。
pwd_grace_login_err	パスワードは期限切れですが、猶予期間ログインが許可されています。
account_deactivated_err	ユーザー・アカウントが無効です。
act_lock_err	ユーザー・アカウントがロックされています。
pwd_illegal_value	パスワードに無効な値が含まれています。
pwd_in_history	パスワードがパスワード履歴に存在します。
pwd_min_length	パスワードが最小文字数の要件を満たしていません。
pwd_numeric	パスワードが数字の要件を満たしていません。

グローバル化・サポートの追加

OracleAS Single Sign-On のフレームワークでは、配置のニーズに合わせて配置固有ページをグローバル化できます。表示されるページの言語を決定するための様々な方法があります。ここでは2種類の方法について説明します。

表示されるページの言語の決定

この項では、HTTP Accept-Language ヘッダーまたは配置ページのロジックを使用して、表示する言語を選択する方法について説明します。

Accept-Language ヘッダーを使用してページを決定する方法

ブラウザを使用すると、エンド・ユーザーは、Web コンテンツを表示する言語（ロケール）を決定できます。ブラウザでは、ユーザーが選択した言語が、HTTP Accept-Language ヘッダーとしてサーバーに送信されます。配置固有ページのロジックでは、このヘッダーを調べ、ページをレンダリングする必要があります。Single Sign-On Server では、このページを受け取ると、Accept-Language ヘッダーの値を読み取り、ユーザー ID の伝播時にその値をパートナ・アプリケーションに送信します。

Accept-Language ヘッダーは、言語を決定する際の推奨メカニズムです。この方法の主な利点は、エンド・ユーザーが他の Web サイトを参照している間に、言語をすでに設定している可能性が高いということです。そのため、これらのページとシングル・サインオンのページ間で参照の一貫性が保たれます。

ページのロジックを使用して言語を決定する方法

オラクル社では前述の方法をお勧めします。ただし、ブラウザで設定された言語を拡張（または無視）するメカニズムに基づいてグローバル化を実装することもできます。たとえば、次のいずれかの方法があります。

- ログイン・ページに言語一覧を表示し、ユーザーが選択できるようにします。ユーザーの便宜を考慮して、永続 Cookie を設定してこの選択を永続的なものにすることもできます。
- 言語を1つ設定して、ページをレンダリングします。複数のユーザーが1つの言語を使用する場合は、この方法が適しています。
- 集中管理されたアプリケーション・リポジトリまたはディレクトリから言語を取得します。ユーザー設定項目、システム設定項目、構成データの集中管理されたストアは、言語を格納するのに最適です。

ページのロジックを使用して言語を設定する場合、ページではこの情報を Single Sign-On Server に伝播する必要があります。Single Sign-On Server では、この情報をパートナ・アプリケーションに伝播する必要があります。最終的には、一貫性のあるグローバリゼーションが保たれます。ページでは、ログイン・フォームの locale パラメータ (表 12-2) を使用して、ISO-639 形式で言語を渡す必要があります。多くのサイトには、ISO-639 の 2 文字言語コードの全一覧があります。次のサイトにもこの一覧があります。

<http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt>

次のサイトには、ISO-3166 の 2 文字国コードの全一覧があります。

http://www.chemie.fu-berlin.de/diverse/doc/ISO_3166.html

注意： Single Sign-On Server では、locale が渡されない場合に、Accept-Language ヘッダーをパートナ・アプリケーションに送信します。

ページのレンダリング

エンド・ユーザーのロケールが決定されると、配置固有ページでは対応する翻訳文字列を使用して、ページをレンダリングする必要があります。これらの文字列の格納方法および取得方法については、『Oracle Application Server 10g グローバリゼーション・ガイド』の第 2 章「ロケール認識の開発」を参照してください。Java 開発に関する標準的なドキュメントも参照してください。次に 2 つのリンクを紹介します。

- Java Internationalization Guide:

<http://java.sun.com/j2se/1.4.1/docs/guide/intl/index.html>

- Java ドキュメントの一般的なリンク :

<http://java.sun.com/j2se/1.4.1/docs>

配置固有ページに関するガイドライン

配置固有ページを実装する場合は、次のガイドラインに従ってください。

- ログイン・ページとパスワードの変更ページは、SSL で保護することをお勧めします。
- ログイン・ページとパスワードの変更ページでは、クロスサイト・スクリプティング攻撃に備えてコーディングする必要があります。
- ログイン・ページとパスワードの変更ページでは、自動埋込みとキャッシュを off に設定する必要があります。これによって、ユーザーの資格証明がブラウザに保存されたり、キャッシュされる恐れはなくなります。AutoComplete タグの例を次に示します。

```
FORM NAME="foo" AutoComplete="off" METHOD="POST" ACTION="bar"
```

配置固有ページのインストール

policy.properties ファイルを使用して、配置固有のログイン・ページとパスワードの変更ページをインストールします。WSSO_LS_CONFIGURATION_INFO\$ 表を使用して、配置固有のシングル・サインオフ・ページをインストールします。

policy.properties ファイルを使用したログイン・ページとパスワードの変更ページのインストール

独自のログイン・ページとパスワードの変更ページをインストールするには、\$ORACLE_HOME/sso/conf/policy.properties の次のパラメータを編集します。

```
#Custom login page link
loginPageUrl = login_page_URL

#Custom change password page link
chgPasswordPageUrl = change_password_page_URL
```

最後に、Single Sign-On Server を再起動します。手順については、第 2 章の「[OC4J SECURITY インスタンスの停止と起動](#)」の項を参照してください。

policy.properties ファイルを使用したワイヤレスのログイン・ページとパスワードの変更ページのインストール

OracleAS Wireless のフレームワークでは、配置固有のワイヤレスのログイン・ページとパスワードの変更ページを統合できます。これらのページのインストール手順は、標準ページのインストール手順と同様です（前述の項を参照）。まず、policy.properties (\$ORACLE_HOME/sso/conf 内) に移動し、次のパラメータを編集（追加）します。

```
#Wireless login page link
wirelessLoginPageUrl = wireless_login_page_url
wirelessChgPasswordPageUrl = change_password_page_URL
```

最後に、Single Sign-On Server を再起動します。手順については、第 2 章の「[OC4J SECURITY インスタンスの停止と起動](#)」の項を参照してください。

WSSO_LS_CONFIGURATIONS\$ を使用したシングル・サインオフ・ページのインストール

Single Sign-On スキーマの WSSO_LS_CONFIGURATION_INFO\$ 表には、LOGIN_URL 列があります。この列を使用して、シングル・サインオフ・ページを有効にします。

LOGIN_URL には、空白で区切られた 3 つの値があります。最初の 2 つの値は、下位互換性を維持するために予約済です。これらの値は編集できません。3 つ目の値は、シングル・サインオフ・ページを指定します。独自のシングル・サインオフ・ページをインストールする場合は、この値を編集する必要があります。

1. Single Sign-On Server がインストールされたデータベースで、SQL*Plus を使用して Single Sign-On スキーマにログインします。

```
sqlplus orasso/password
```

Single Sign-On スキーマのパスワードの取得方法については、[付録 B](#) を参照してください。

2. LOGIN_URL を更新します。サンプル・ページを独自のページに置き換えるには、この列の 3 番目の値を更新します。次の例では、`single_signoff.jsp` が配置固有ページです。

```
UPDATE WSSO_LS_CONFIGURATION_INFO$  
SET LOGIN_URL='UNUSED UNUSED http:// server.domain[:port]/single_signoff.jsp';
```

3. Oracle ページに戻すには、元の値を再度設定します。

```
UPDATE WSSO_LS_CONFIGURATION_INFO$  
SET LOGIN_URL='UNUSED UNUSED UNUSED';
```

注意： 最初の 2 つの値は UNUSED にする必要があります。

配置固有ページの例

ipassample.jar ファイルには、`login-ex.jsp`、`password-ex.jsp`、`signoff-ex.jsp` の各ファイルが含まれます。これらのファイルをカスタマイズして、配置に対応させることもできます。これらのファイルの使用方法については、第 2 章の「[サンプル・ファイルの取得](#)」の項を参照してください。

サードパーティのアクセス管理システムとの統合

この章では、OracleAS Single Sign-On とサードパーティのアクセス管理製品を統合する方法について説明します。サードパーティとの統合がどのように機能するかを説明し、統合 API を紹介します。この章の最後では、OracleAS Single Sign-On とサードパーティのアクセス管理システムを統合する例を示します。

サードパーティのシステムを設置している企業では、OracleAS Single Sign-On Server をサードパーティのシステムと Oracle アプリケーション間の認証ゲートウェイとして動作させることができる API を使用することによって、OracleAS スイートを利用できるようになります。

この章の項目は次のとおりです。

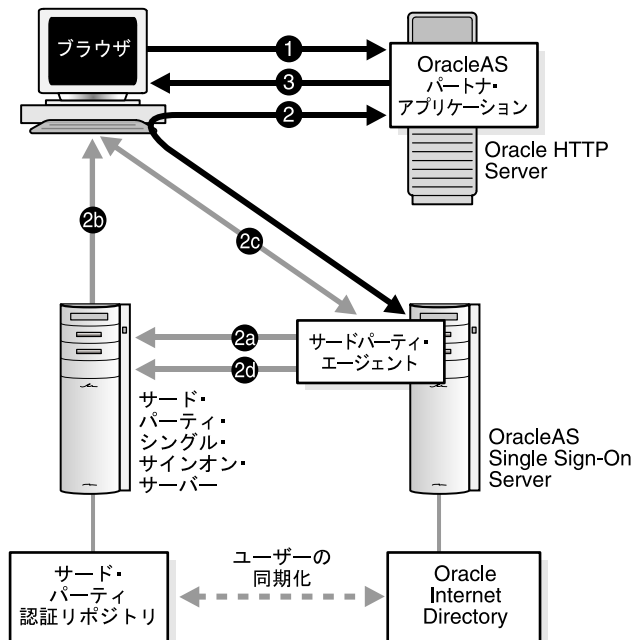
- サードパーティのアクセス管理の仕組み
- サードパーティ・リポジトリと Oracle Internet Directory の同期化
- サードパーティ統合モジュール
- 統合事例 : SSOAcme

サードパーティのアクセス管理の仕組み

サードパーティのアクセス管理では、OracleAS Single Sign-On Server、サードパーティのアクセス管理サーバーおよびパートナー・アプリケーションによって信頼の連鎖が形成されます。OracleAS Single Sign-On Server は、サードパーティのアクセス管理サーバーに認証を委譲するため、本質的にはサードパーティのアクセス管理サーバーのパートナー・アプリケーションとなります。Oracle アプリケーションは OracleAS Single Sign-On Server とのみ連携し、サードパーティのアクセス管理サーバーは認識しません。ただし、暗黙的にはサードパーティ製のサーバーを信頼します。

OracleAS Single Sign-On がこのような配置の下でユーザーに認証トークンを発行できるようにするには、サードパーティのアクセス管理サーバーが HTTP ヘッダーを設定するか、他のメカニズムを使用して、OracleAS Single Sign-On Server にユーザーの ID を渡す必要があります。ユーザーの ID を取得すると、OracleAS Single Sign-On Server はこれまでのように機能し、ユーザーの認証、パートナー・アプリケーションへのユーザーのリダイレクトを行います。13-2 ページの図 13-1 に、このプロセスを示します。

図 13-1 サードパーティのサーバーを使用した Oracle パートナ・アプリケーションへのアクセス



この図から 2 つの使用例が考えられます。

使用例 1: ユーザーが、サードパーティのサーバーに認証されていない場合

1. 認証されていないユーザーが、OracleAS Single Sign-On によって保護されているアプリケーションへのアクセスを試みます。
2. アプリケーションは、ユーザーを認証するために OracleAS Single Sign-On Server にユーザーをリダイレクトします。このリダイレクションの一環として、次の操作が行われます。
 - a. OracleAS Single Sign-On Server は、ユーザーの認証をサードパーティのサーバーに任せます。
 - b. サードパーティのサーバーは、ユーザーのブラウザにトークンを設定します。
 - c. OracleAS Single Sign-On Server は、ブラウザからトークンを取得します。
 - d. OracleAS Single Sign-On Server は、サードパーティのサーバーでこのトークンを検証します。

OracleAS Single Sign-On Server はトークンを検証した後、ユーザーを要求されたアプリケーションに戻します。

3. このアプリケーションによって、ユーザーの必要とするコンテンツが表示されます。

使用例 2: ユーザーが、サードパーティのサーバーに認証されている場合

1. 認証されているユーザーが、OracleAS Single Sign-On によって保護されているアプリケーションへのアクセスを試みます。
2. アプリケーションは、ユーザーを認証するために OracleAS Single Sign-On Server にユーザーをリダイレクトします。このリダイレクションの一環として、次の操作が行われます。
 - a. OracleAS Single Sign-On Server は、ブラウザからトークンを取得します（使用例 1 の手順 2c）。
 - b. OracleAS Single Sign-On Server は、サードパーティのサーバーでこのトークンを検証します（使用例 1 の手順 2d）。

OracleAS Single Sign-On Server はトークンを検証した後、ユーザーを要求されたアプリケーションに戻します。

3. このアプリケーションによって、ユーザーの必要とするコンテンツが表示されます。

注意： 関連するシングル・サインオン・システムにすべての認可ユーザーがアクセスできるようにするには、ユーザー・リポジトリを 1 箇所で集中管理する必要があります。つまり、配置の前に、Oracle Internet Directory と外部リポジトリ間でユーザーを同期化する必要があります。

サードパーティ・リポジトリと Oracle Internet Directory の同期化

前の手順で説明した認証プロセスでは、ユーザーのリポジトリが Oracle Internet Directory であるか、またはリポジトリがサードパーティのディレクトリかデータベースであることを前提としています。リポジトリがサードパーティのディレクトリかデータベースである場合には、ユーザー名情報を Oracle Internet Directory 内のユーザー・エン트리と同期化する必要があります。同期化することにより、Single Sign-On Server は、シングル・サインオンが有効になったアプリケーションで要求されたユーザー属性を取得できます。

注意： 同期メカニズムが搭載されていない場合、サードパーティのアクセス管理を統合できません。

サードパーティのリポジトリと Oracle Internet Directory を同期化するには、Oracle Directory Integration Platform または一括ロード・ツールのいずれかを使用します。詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

サードパーティ統合モジュール

サードパーティとの統合を実現するには、2通りの方法があります。ベンダーから提供された既存のパッケージを使用する方法と、Oracle から提供されたインタフェースを使用して、サードパーティのアダプタを独自に構築する方法です。

ベンダーから提供されたパッケージを使用する場合

サードパーティのアクセス管理ベンダーによっては、OracleAS Single Sign-On Server 用の認証アダプタを提供しているところがあります。これらの製品を使用すると、独自のコードを記述しなくても、サードパーティのシステムを Oracle のシステムに統合できます。この方法に関心がある場合は、ベンダーに直接お問い合わせください。

独自のパッケージを構築する場合

この章の後の項で提供されている Java ツール・キット oracle.security.sso.ias904 を使用して、サードパーティとの統合用アダプタを独自に構築することができます。このツール・キットには、認証の実行および配置固有の Cookie の設定に使用する 2 つのインタフェースが含まれています。OracleAS Single Sign-On Server では、認証時に前者のインタフェースが使用されます。Cookie 用のアダプタである後者のインタフェースは、ユーザー ID の確認に成功した後で使用されます。

この項の項目は次のとおりです。

- [インタフェースの使用に関するガイドライン](#)
- [インタフェース](#)
- [構成手順](#)

インタフェースの使用に関するガイドライン

認証用のインタフェースは、サードパーティとの統合用アダプタを独自に構築する場合のみ必要です。OracleAS Single Sign-On Server は、このインタフェースを実装することで、認証時にユーザー ID を確認します。便宜上 Cookie 用のインタフェースが用意されています。ユーザーが認証されたら、このインタフェースを使用して、追加の Cookie を設定できます。たとえば、この機能を使用して、ユーザー設定項目を指定することができます。サードパーティとの統合には Cookie 用のインタフェースは必要ありません。これを使用する場合は、独自のアダプタにも、ベンダーから提供されたアダプタにも追加できます。

インタフェース

キット内の 2 つのインタフェースは次の機能を実行します。

- トークンを使用した認証
- 外部 Cookie の設定

トークンを使用した認証 IPASAuthInterface.java パッケージは、OracleAS Single Sign-On Server によって認証時に起動されます。トークンを使用した認証をサポートする場合、このインタフェースの実装者は、安全に設定された HTTP ヘッダーや安全な Cookie などから、安全な方法でユーザーの ID を取得して、ユーザー名を OracleAS Single Sign-On Server に戻す必要があります。次にインタフェースを示します。

```
/**
 * returns IPASUserInfo
 * The returned object should contain user information
 * nicknames
 *
 * @param request The user's HTTP request object
 *
 * @throws IPASAuthException if the authentication fails for whatever
 * reasons.
 * The exception message will be propagated to the login page
 * directly.
 *
 * @throws IPASInsufficientCredException if all the required
 * credentials
 * @return IPASUserInfo authenticated user information
 */

public IPASUserInfo authenticate(HttpServletRequest request)
throws IPASAuthException, IPASInsufficientCredException;
```

外部 Cookie の設定 IPASCustomCookieInterface.java パッケージを使用すると、配置固有の Cookie を設定できます (省略可能)。認証に成功し、Cookie アダプタが適切な認証レベルに対応する場合にのみ、これらの Cookie は設定されます。

```
/**
 * A custom cookie can be implemented using this interface.
 * SSO server sends the cookie to the user browser.
 *
 * @param user user object that contains the authenticated user
 *         information
 *
 * @param req HTTP user request object
 *
 * @return array of Cookie objects
 */
public Cookie[] getCustomCookie(IPASUserInfo user, HttpServletRequest req);
```

構成手順

インタフェースを使用してサードパーティとの統合用アダプタを独自に作成するには、次の手順を実行します。

1. サードパーティのアクセス管理システムで、次の URI を保護するルールを作成します。

```
/pls/orasso/ORASSO.wvssso_app_admin.ls_login
/sso/auth/*
```

2. 次のログアウト URI を、サードパーティのアクセス管理システムに登録します。

```
/pls/orasso/ORASSO.wvssso_app_admin.ls_logout
```

注意： この後の手順およびサンプル・パッケージでは、"acme" と "SSOAcme" の部分をすべて実際の会社名に置き換えてください。

3. パッケージ用の Java ファイルを作成します。詳細は、「[統合事例:SSOAcme](#)」のサンプル・ファイルを参照してください。サンプル・ファイルは SSOAcmeAuth.java と呼ばれます。コンパイルの前に、次のパッケージ・ディレクティブをこのファイルに追加する必要があります。

```
package acme.security.ssoplugin;
```

4. クラス・パス内の \$ORACLE_HOME/sso/lib/ipastoolkit.jar とともに、このファイルをコンパイルします。サンプル・ファイル SSOAcmeAuth.java は、次のようにコンパイルします。

```
javac -classpath /usr1/ias/infra/sso/lib/ipastoolkit.jar:/usr1/ias/infra/j2ee/
home/lib/servlet.jar SSOAcmeAuth.java
```

5. ディレクトリ `$ORACLE_HOME/sso/plugin` に、手順 3 で指定したパッケージ階層に対応するディレクトリ構造を作成します。サンプル・プラグインのパスは次のようになります。

```
$ORACLE_HOME/sso/plugin/acme/security/ssoplugin
```

6. 手順 4 で生成したクラスを `ssoplugin` ディレクトリに配置します。
7. `policy.properties` ファイルで、簡易認証プラグインを手順 3 で作成したプラグインに置き換えます。簡易認証プラグインは、次のように記述されています。

```
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOAuthProvider
```

サンプルのプラグインは、次のようになります。

```
MediumSecurity_AuthPlugin = acme.security.ssoplugin.SSOAcmeAuth
```

注意： `policy.properties` を編集するときは、行の末尾に空白を入れないでください。

8. カスタム Cookie インタフェースを実装する場合は、実装のクラス名を `policy.properties` に追加します。

```
# Custom Cookie Provider Class name
# -----
# Sample custom cookie tester provider class
```

```
CustomCookie_ProviderPlugin = class_name
```

9. ユーザーの認証が成功した場合にカスタム Cookie が設定される、最低の認証レベルを指定します。

```
# Custom Cookie auth level
# -----
CustomCookieAuthLevel = authentication_level
```

マルチレベル認証を使用せず、認証アダプタ・レベルのデフォルト設定を使用する場合は、この値を次の値に設定できます。

```
CustomCookieAuthLevel = MediumSecurity
```

10. シングル・サインオン中間層を再起動します。詳細は、「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。
11. 統合したシステムをテストします。

統合事例 : SSOAcme

SSOAcme の事例を考えます。SSOAcme は、保護されたリソースに対するシングル・サインオン認証を提供する製品です。SSOAcme は、SSOAcme ポリシー・サーバーと SSOAcme エージェントの 2 つのコンポーネントで構成されています。SSOAcme ポリシー・サーバーはユーザー管理、セッション管理、認証、認可などの様々なサービスをユーザーに提供します。SSOAcme エージェントは Web サーバーおよび Web アプリケーション・サーバーに配置します。リソースのリクエストをチェックして、リソースが SSOAcme によって保護されているかどうかを確認します。

SSOAcme をすでにインストールしている顧客は、SSOAcme を使用して OracleAS アプリケーションにアクセスしたいと思うことがあります。このようなアクセスを実現するには、SSOAcme が OracleAS Single Sign-On を経由して Oracle アプリケーションとデータをやり取りできるようにする API を使用します。

注意： SSOAcme は架空の製品です。ここでは、説明の目的でのみ使用しています。

この項の項目は次のとおりです。

- [サンプル統合パッケージ](#)
- [統合システムからのログアウト](#)
- [リリース 9.0.2 のサンプル実装からリリース 9.0.4 への移行](#)

サンプル統合パッケージ

ここに示す SSOAcme.java パッケージは、SSOAcme の既存の実装と OracleAS Single Sign-On との統合に使用できます。

```
/**
 * returns IPASUserInfo
 **/

/* Copyright (c) 2002, 2003, Oracle Corporation. All rights reserved. */

/*
DESCRIPTION
    Sample class for SSOAcme integration with SSO Server

PRIVATE CLASSES

NOTES
    This class implements the SSOServerAuthInterface.
    To enable this integration, replace:
```



```
        oracle.security.sso.server.auth.SSOAcmeAuth
    with
        acme.security.ssoplugin.SSOAcmeAuth
    for the desired security level in policy.properties.
*/

import java.io.PrintWriter;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import oracle.security.sso.ias904.toolkit.IPASAuthInterface;
import oracle.security.sso.ias904.toolkit.IPASAuthException;
import oracle.security.sso.ias904.toolkit.IPASUserInfo;
import oracle.security.sso.ias904.toolkit.IPASInsufficientCredException;

public class SSOAcmeAuth implements IPASAuthInterface {

    private static String CLASS_NAME = "SSOAcmeAuth";
    private static String ACME_USER_HEADER = "ACME_USER";

    public SSOAcmeAuth() {

    }

    public IPASUserInfo authenticate(HttpServletRequest request)
        throws IPASAuthException, IPASInsufficientCredException {

        String AcmeUserName = null;

        try
        {
            AcmeUserName = request.getHeader(ACME_USER_HEADER);
        }
        catch (Exception e)
        {
            throw new IPASInsufficientCredException("No Acme Header");
        }

        if (AcmeUserName == null)
            throw new IPASInsufficientCredException("No Acme Header");

        IPASUserInfo authUser = new IPASUserInfo (AcmeUserName);

        return authUser;

    }
}
```

```
public String getUserCredentialPage(HttpServletRequest request,
    String msg) {

    // This function will never have been reached in the case of SSOAcme
    // because the SSOAcme Agent will intercept all requests
    return "http://error_url;

}

}
```

統合システムからのログアウト

サードパーティ製品のログアウトには2つの方法があります。

- ユーザーはサードパーティのアクセス管理システムを使用して、ログアウト・リクエストを開始します。

この場合、ユーザーは SSOAcme システムで、ログアウト・ハンドラを起動するログアウト・リンクをクリックします。SSOAcme のログアウト・フローにより、SSOAcme 自身のセッションがクリーンアップされます。クリーンアップ後、SSOAcme システムは OracleAS Single Sign-On のログアウト・ハンドラを起動する必要があります。

OracleAS Single Sign-On のログアウト・ハンドラを起動すると、OracleAS Single Sign-On Server で保護されるすべてのアプリケーションからユーザーがログアウトされます。シングル・サインオンのログアウトを実行するには、SSOAcme システムはユーザーを次の URL にリダイレクトする必要があります。

```
http://single_sign-on_host:single_sign-on_port/pls/orasso/ORASSO.wvssso_app_admin.ls_logout?p_done_url=done_url
```

done_url は、ログアウト後にユーザーがリダイレクトされる URL です。

- ユーザーは OracleAS Single Sign-On システムを使用して、ログアウト・リクエストを開始します。

この使用例では、Oracle パートナ・アプリケーションでログアウト・リンクをクリックします。これにより、OracleAS Single Sign-On のログアウト・ハンドラが起動されます。ログアウトが終了したら、ユーザーは SSOAcme システムからもログアウトする必要があります。SSOAcme システムに Oracle ログアウト・ハンドラ (前述の URL 内の *ls_logout*) を登録すると、同時ログアウトを実行できます。SSOAcme システムで Oracle ログアウト・ハンドラの起動が検出されると、SSOAcme セッションがクリーンアップされます。

リリース 9.0.2 のサンプル実装からリリース 9.0.4 への移行

リリース 9.0.2 の外部認証パッケージを使用してサードパーティ製品での認証を実行していたユーザーは、この項を参照してください。リリース 9.0.2 のパッケージは PL/SQL で記述されていました。リリース 9.0.4 のパッケージは Java で記述されています。以降では、2つのパッケージの関連するセクションを一緒に示します。

新しい認証インタフェース

リリース 9.0.4:

```
package acme.security.ssoplugin;

import java.io.PrintWriter;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import oracle.security.sso.server.util.SSODebug;
import oracle.security.sso.ias904.toolkit.IPASAuthInterface;
import oracle.security.sso.ias904.toolkit.IPASAuthException;
import oracle.security.sso.ias904.toolkit.IPASUserInfo;
import oracle.security.sso.ias904.toolkit.IPASInsufficientCredException;

public class SSOAcmeAuth implements IPASAuthInterface {

    private static String CLASS_NAME = "SSOAcmeAuth";
    private static String ACME_USER_HEADER = "ACME_USER";

    public SSOAcmeAuth() {
    }

    public IPASUserInfo authenticate(HttpServletRequest request)
    throws IPASAuthException, IPASInsufficientCredException {
```

リリース 9.0.2:

```
FUNCTION authenticate_user
(
    p_user OUT VARCHAR2
)
return PLS_INTEGER
IS
    l_http_header varchar(1000);
    l_ssouser wwsec_person.user_name%type := NULL;
BEGIN
```

HTTP ヘッダーからのユーザー名の取得

リリース 9.0.4:

```
String AcmeUserName = null;

try
{
    AcmeUserName = request.getHeader(ACME_USER_HEADER)
```

リリース 9.0.2:

```
l_http_header := owa_util.get_cgi_env('HTTP_Acme_USER');
debug_print('Acme ID : ' || l_http_header);
```

ユーザー名が存在しない場合のエラー処理

リリース 9.0.4:

```
}
catch (Exception e)
{
    DebugUtil.debug(SSODebug.ERROR, "exception: " + CLASS_NAME, e);
    throw new IPASInsufficientCredException("No Acme Header");
}
```

```
if (AcmeUserName == null)
throw new IPASInsufficientCredException("No Acme Header");
```

リリース 9.0.2:

```
IF ( (l_ssouser IS NULL) or
    ( INSTR(l_ssouser, GLOBAL_SEPARATOR) != 0 ) ) THEN
    debug_print('malformed user id: '
        || l_ssouser
        || ' returned by wvso_auth_external.authenticate_user');
    RAISE EXT_AUTH_FAILURE_EXCEPTION;
ELSE
```

Single Sign-On Server に戻すユーザー名

リリース 9.0.4:

```
IPASUserInfo authUser = new IPASUserInfo(AcmeUserName);  
  
return authUser;  
  
}
```

リリース 9.0.2:

```
p_user := NLS_UPPER(l_ssouser); -- p-user is the out parameter  
return 0; -- SUCCESS error code  
END IF;
```

データのエクスポートとインポート

この章では、複数の Single Sign-On Server 間でデータを移動する方法について説明します。データのエクスポートまたはインポートが必要になる様々な状況があります。たとえば、テスト・サーバーでデータを用意してから、本番サーバーにデータを移動することがあります。また、複数のサーバーを1つに統合することもあります。既存のサーバーをバックアップすることもあります。

この章の項目は次のとおりです。

- [エクスポートされるデータとインポートされるデータ](#)
- [エクスポートとインポートのスクリプト: 構文とパラメータ](#)
- [サーバー間でのデータのエクスポート](#)
- [複数のサーバーの統合](#)
- [エクスポートとインポートの成功の確認](#)
- [エラー・メッセージ](#)

エクスポートされるデータとインポートされるデータ

エクスポートとインポートのスクリプト (ssomig) によって、次の3つのカテゴリのデータが移動されます。

- 外部アプリケーションの定義とユーザー・データ
- パートナ・アプリケーションの登録 URL とトークン
- OracleAS Discoverer で様々なデータソースへのアクセスに使用する接続情報

ユーザー・アカウントを移動する必要がある場合は、LDAP コマンドライン・スクリプト (ldapsearch など) を使用してソース・ディレクトリからデータを抽出します。ldapadd または ldapmodify を使用して、ターゲット・ディレクトリにデータをロードします。これらのスクリプトの使用方法については、『Oracle Internet Directory アプリケーション開発者ガイド』を参照してください。

エクスポートとインポートのスクリプト: 構文とパラメータ

ssomig スクリプトは Perl、Oracle SQL*Plus、exp ツールおよび imp ツールを使用して、リリース 9.0.4 の2つのサーバー間でデータを移動します。エクスポート・モードとインポート・モードは別々に実行する必要があります。ssomig は \$ORACLE_HOME/sso/bin にあります。

スクリプト構文

次の構文を使用して、ssomig を実行します。

```
ssomig -s sso_schema
-p sso_password
-c net_service_name
-log_d log_dir
{
  -export [-prompt]
          [-noextappusrs]

  -import {-merge | -overwrite}
          [-discoforce | -disconoforce]
}
[-log_f log_file]
[-d dump_file_name]
[-help]
```


スクリプト・パラメータ

表 14-1 では、ssomig に渡すパラメータを定義します。

表 14-1 ssomig に渡すパラメータ

パラメータ	説明	追加情報
-s	OracleAS Single Sign-On のデータベース・スキーマ名。	デフォルトは ORASSO です。
-p	OracleAS Single Sign-On のデータベース・スキーマ・パスワード。	OracleAS Infrastructure のインストール時にパスワードはランダム化されます。パスワードの取得方法については、付録 B を参照してください。
-c	OracleAS Single Sign-On データベースのネット・サービス名。	-
-log_d	ログ・ディレクトリ名。	このディレクトリは書込み可能にする必要があります。ログ・ファイルとダンプ・ファイルがこのディレクトリに書き込まれます。 スクリプトの実行時にはディレクトリの絶対パスを使用します。デフォルトは \$ORACLE_HOME/sso/log です。
-export	シングル・サインオン表からデータを抽出し、ダンプ・ファイルにロードします。	-
-prompt	パートナ・アプリケーションと外部アプリケーションを選択してエクスポートします。	export で使用します。
-noextappusrs	外部アプリケーションのユーザーがエクスポートされないように指定します。	export で使用します。 段階的なサーバーから本番サーバーにデータを移動するが、テスト・ユーザーは移動しない場合に、このモードを選択します。
-import	ダンプ・ファイルからデータを抽出し、シングル・サインオン表にロードします。	-
-merge	ターゲット・サーバーに存在しないパートナ・アプリケーションと外部アプリケーションのみをインポートします。	複数のサーバーから最初のサーバーをインポートした後、このモードを選択します。 import で使用します。
-overwrite	ターゲット・サーバーに存在するか否かにかかわらず、すべてのパートナ・アプリケーションと外部アプリケーションをインポートします。	複数のサーバーから最初のサーバーを移行する場合に、このモードを選択します。 import で使用します。
-discoforce	OracleAS Discoverer 情報をインポートして、ターゲット・サーバーの Discoverer 情報を置き換えます。	-

表 14-1 ssomig に渡すパラメータ (続き)

パラメータ	説明	追加情報
-disconoforce	ターゲット・サーバーに Discoverer データが存在しない場合にのみ、OracleAS Discoverer 情報をインポートします。	-
-log_f	ログ・ファイル名。	このファイルには、エクスポート結果と、SQL*Plus、exp、imp などのツールのランタイム・ステータスが含まれます。デフォルトのファイル名は ssomig.log です。
-d	ダンプ・ファイル名。	デフォルトは ssomig.dmp です。
-help	ssomig の構文とパラメータを記述します。	-

サーバー間でのデータのエクスポート

エクスポートとインポートのスク립トが実行される際の使用例は、2つのカテゴリに分けられます。単一サーバーからのエクスポートと、複数のサーバーからのエクスポートです。カテゴリに応じて、スク립トは上書きモードまたはマージ・モードで実行されます。また、カテゴリに応じて、パートナ・アプリケーションと外部アプリケーションを選択してエクスポートするかどうかも指定します。この項では、単一サーバーでのエクスポートおよびインポートについて説明します。複数のサーバーのエクスポートおよびインポートについては、「[複数のサーバーの統合](#)」の項を参照してください。

この項の項目は次のとおりです。

- [エクスポートとインポートの使用例およびスク립トの例](#)
- [スク립トの実行](#)

エクスポートとインポートの使用例およびスク립トの例

以降では、Single Sign-On Server 間でデータを移動する場合の使用例について説明します。各使用例では適切なコマンドを紹介합니다。

注意： 以降の例は、UNIX を念頭において記述されていますが、これらは Windows NT と 2000 でも動作します。ログ・ディレクトリ・パスで、フォワード・スラッシュを円記号 (¥) に置き換えてください。

エクスポートの使用例

- パートナ・アプリケーションと外部アプリケーションをすべてエクスポートします。OracleAS Discoverer のデータ全体をエクスポートします。サーバーをバックアップする場合は、次のコマンドを使用します。

```
ssomig -export -s orasso -p password -c net_service_name -log_d /tmp
```

- パートナ・アプリケーションと外部アプリケーションを選択してエクスポートします。OracleAS Discoverer のデータ全体をエクスポートします。段階的なデータを本番サーバーに移動する場合は、次のコマンドを実行します。

```
ssomig -export -prompt -s orasso -p password -c net_service_name -log_d /tmp
```

- パートナ・アプリケーションを選択してエクスポートします。外部アプリケーションの定義を選択してエクスポートします。外部アプリケーションのユーザー・データはエクスポートしません。OracleAS Discoverer のデータ全体をエクスポートします。段階的なデータを本番サーバーに移動するが、テスト・ユーザーの外部アプリケーション情報を移動しない場合は、次のコマンドを実行します。

```
ssomig -export -prompt -noextappusrs -s orasso -p password -c net_service_name -log_d /tmp
```

インポートの使用例

- パートナ・アプリケーションと外部アプリケーションをインポートします。インポートするエン트리と同じエントリのみを上書きします。OracleAS Discoverer データは除外します。Discoverer を配置しない場合は、次のコマンドが便利です。

```
ssomig -import -overwrite -s orasso -p password -c net_service_name -log_d /tmp
```

- パートナ・アプリケーション、外部アプリケーション、OracleAS Discoverer データをインポートします。インポートするエン트리と同じエン트리であるかどうかにかかわらずなく、すべてのエントリを上書きします。ターゲット・サーバーでデータをリフレッシュする場合は、次のコマンドを実行します。

```
ssomig -import -overwrite -s orasso -p password -c net_service_name -log_d /tmp -discoforce
```

- パートナ・アプリケーションと外部アプリケーションをインポートします。インポートするエン트리と同じエン트리であるかどうかにかかわらずなく、すべてのエントリを上書きします。OracleAS Discoverer 情報は、ターゲット・サーバーに存在しない場合にのみインポートします。

```
ssomig -import -overwrite -s orasso -p password -c net_service_name -log_d /tmp -disconoforce
```

スクリプトの実行

データをエクスポートする手順は、次のとおりです。

1. エクスポート元のコンピュータにログインします。
2. リリース 9.0.4 の Single Sign-On Server の Oracle ホームを指すように、Oracle ホームの環境変数 `ORACLE_HOME` を設定します。
3. スクリプトを実行します（「[エクスポートとインポートの使用例およびスクリプトの例](#)」の項を参照）。

これにより、ダンプ・ファイル `ssomig.dmp`、ログ・ファイル `ssoconf.log`、シングル・サインオンの構成ファイル `ssoconf.log` が作成されます。これら 3 つのファイルはログ・ディレクトリに作成されます。

注意： エクスポート・モードでプロンプト・オプションを使用して `ssomig` を実行すると、エクスポートから除外するアプリケーションを指定するよう要求されます。同時に、その選択が終了したら任意のキーを押すよう要求されます。ここでは、かわりに **[Return]** キーまたは **[Enter]** キーを押してください。このスクリプトでは、他のキーは無視されます。

データをインポートする手順は、次のとおりです。

1. インポート先のコンピュータにログインします。
2. リリース 9.0.4 の Single Sign-On Server の Oracle ホームを指すように、環境変数 `ORACLE_HOME` を設定します。
3. `log_d` パラメータは、エクスポートのログ・ファイルがあるログ・ディレクトリを指すようにします。インポート・モードで実行される場合、スクリプトは `ssomig.dmp`、`ssoconf.log` の各ファイルを参照する必要があります。エクスポート・サーバーがあるコンピュータから、これらのファイルをコピーする場合があります。
4. `import` モードを選択して、スクリプトを実行します（「[エクスポートとインポートの使用例およびスクリプトの例](#)」の項を参照）。

エクスポートとインポートの成功の確認

エクスポート操作とインポート操作が完了したら、`ssomig.log` を開いてエラーをチェックします。ファイル内のメッセージについて確認する場合は、「[エラー・メッセージ](#)」の項を参照してください。

複数のサーバーの統合

企業内の複数の部門でそれぞれ Single Sign-On Server を設置している場合は、この使用例が当てはまります。このようなサーバーを統合して、統合識別情報管理サービスを実現する場合があります。

次の方法で、複数のサーバーをエクスポートおよびインポートします。

1. ターゲット・サーバーを除き、すべての関連サーバーからデータをエクスポートします。スクリプトの実行方法については、「[サーバー間でのデータのエクスポート](#)」の項を参照してください。
2. 最初に移行する Single Sign-On Server に対して、import モード、overwrite オプションでスクリプトを実行します。詳細については、「[インポートの使用例](#)」の項を参照してください。
3. 以降のサーバーについては、merge モードでスクリプトを実行します。パートナ・アプリケーションと外部アプリケーションをターゲット・サーバーに1つずつインポートします。

```
ssomig -import -merge -s orasso -p password -c net_service_name -log_d /tmp -d  
ssomig.dmp
```

このコマンドでは、パートナ・アプリケーションと外部アプリケーションのみがマージされます。

注意： 複数のサーバーをインポートする場合は、overwrite モードでスクリプトを実行して、前回の実行結果を取り消すことができます。

エラー・メッセージ

エクスポートおよびインポートの際には、次に示すエラー・メッセージが表示されることがあります。表 14-2 には、問題解決に役立つエラー・メッセージが定義されています。

表 14-2 エクスポートおよびインポートに関するエラー・コード

エラー	原因	処置
SSO-80000: The operation was unsuccessful.	1つ以上のエラーによって、インポートまたはエクスポート（あるいは両方）が失敗しました。	ログ・ファイルまたはスクリーン画面の内容からエラーを判別します。
SSO-80001: The environment variable ORACLE_HOME is not set.	リリース 9.0.4 の Oracle ホームに変数が設定されていません。	「スクリプトの実行」の手順に従ってください。
SSO-80002: Invalid ORACLE_HOME specified.	ORACLE_HOME で示されるディレクトリは存在しないか、ディレクトリ内の必要なスクリプトを入手できません。	Oracle ホームを有効な Oracle インスタンスに設定します。
SSO-80004: Invalid log directory. String is not writable.	指定されたログ・ディレクトリに対する書き込み権限がありません。	書き込み権限が付与されているディレクトリを指定します。
SSO-80005: Invalid log directory. String is not directory.	指定されたログ・ディレクトリは存在しません。	有効なディレクトリを指定します。
SSO-80008: Duplicate option string.	コマンドライン・パラメータ文字列が繰り返されているか、相補的なオプションのセットが2つとも指定されています。	コマンドライン・パラメータ文字列は繰り返さないでください。 相補的なオプションのセット (export と import など) を2つとも指定しないでください。
SSO-80009: Mandatory parameter missing: string.	必須のコマンドライン・パラメータ文字列が指定されていません。	適切な値でパラメータ文字列を指定します。
SSO-80010: Invalid SSO Server version detected.	スクリプトでは、ソース・サーバーまたはターゲット・サーバーのバージョンをサポートしません。	リリース 9.0.4 のサーバーを使用してエクスポート操作およびインポート操作を実行していることを確認します。
SSO-80011: Invalid option string.	パラメータ文字列が、認識されたコマンドライン・パラメータではありません。	help オプションを使用して有効なパラメータの一覧を取得します。
SSO-80012: Invalid SSO schema information.	スキーマ名、パスワードまたはネット・サービス名が無効です。	コマンドを再入力します。

表 14-2 エクスポートおよびインポートに関するエラー・コード (続き)

エラー	原因	処置
SSO-80014: Invalid log file. String is not writable.	指定されたログ・ファイルに対する書き込み権限がありません。	書き込み権限が付与されているログ・ファイルを指定します。
SSO-80015: Failed to drop temporary tables.	必要なスクリプト・ファイルがなかったか、オペレーティング・システム・エラーまたはデータベース・エラーが発生しました。	ログ・ファイルで詳細を確認します。エラーがあれば修正します。
SSO-80050: Data export unsuccessful.	1つ以上のエラーによって、エクスポート操作が失敗しました。	ログ・ファイルまたはスクリーン画面の内容からエラーを判別します。
SSO-80051: Copying data into the temporary tables failed.	スクリプト・ファイルがないか、オペレーティング・システム・エラーまたはデータベース・エラーが発生しました。	ログ・ファイルで詳細を確認します。エラーがあれば修正します。
SSO-80052: Invalid dump file. String not writable.	指定されたダンプ・ファイルに対する書き込み権限がありません。	書き込み権限が付与されているダンプ・ファイルを指定します。
SSO-80076: Cannot determine NLS information.	スクリプト・ファイルがないか、オペレーティング・システム・エラーまたはデータベース・エラーが発生しました。	ログ・ファイルで詳細を確認します。エラーがあれば修正します。
SSO-80077: The file string does not exist.	外部でファイル文字列が削除されたか、名前が変更されました。	スクリプト実行時には、外部でファイル文字列を編集または削除しないようにします。
SSO-80078: Creating the table that represents the config file failed.	スクリプト・ファイルがないか、オペレーティング・システム・エラーまたはデータベース・エラーが発生しました。	ログ・ファイルで詳細を確認します。エラーがあれば修正します。
SSO-80100: Data import unsuccessful.	1つ以上のエラーによって、インポート操作が失敗しました。	ログ・ファイルまたはスクリーン画面の内容からエラーを判別します。エラーがあれば修正します。
SSO-80101: Cannot read the import dump file: string.	ダンプ・ファイル文字列に対する読取り権限がありません。	指定されたダンプ・ファイルに対する読取り権限を取得します。
SSO-80102: The dump file string is of size zero.	エクスポート時にエラーが発生しました。	ログ・ファイルを表示します。エラーがあれば修正します。

表 14-2 エクスポートおよびインポートに関するエラー・コード (続き)

エラー	原因	処置
SSO-80103: Config file not found: string.	ダンプ・ファイルやログ・ファイルなどの必要な構成ファイルがインポート時に見つからない場合に、このエラーが発生します。	構成ファイルがログ・ディレクトリに存在することを確認します。
SSO-80104: Corrupted or invalid config file.	構成ファイルが変更されました。	ソースからターゲットへの送信時には、構成ファイルが変更されないようにします。
SSO-80150: Package loading into the SSO schema failed.	スクリプト・ファイルがないか、オペレーティング・システム・エラーまたはデータベース・エラーが発生しました。	ログ・ファイルで詳細を確認します。エラーがあれば修正します。

トラブルシューティング

この付録の項目は次のとおりです。

- ログ・ファイル
- エラー・メッセージとその他の問題
- デバッグ・レベルの引上げ
- Single Sign-On データベースでのデバッグ・オプションの有効化
- UI 操作に関する LDAP トレースの有効化
- シングル・サインオン監査レコードの管理
- LDAP 接続キャッシュのリフレッシュ
- Oracle Internet Directory 変更後の OC4J の再起動
- レプリケーションのトラブルシューティング

ログ・ファイル

次の OracleAS ログ・ファイルには、シングル・サインオン操作についてのデータが記録されます。

- シングル・サインオン・ログ：

`$ORACLE_HOME/sso/log/ssoServer.log`

使用上の注意：

最も使用頻度の高いファイルです。Single Sign-On Server は、すべてのエラーをこのファイルに書き込みます。

- Single Sign-On Server の起動エラー・ログ：

`$ORACLE_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1`

使用上の注意：

OC4J で生成されたこのファイルには、Single Sign-On Server 起動時のすべてのエラーが記録されます。OC4J_SECURITY インスタンスの起動時に `opmnctl` コマンドがハングアップしたり、コマンドラインでエラーがレポートされた場合には、このファイルでエラー・メッセージをチェックします。

- Web アプリケーション・ログ：

`$ORACLE_HOME/j2ee/OC4J_SECURITY/application-deployments/sso/OC4J_SECURITY_default_island_1/application.log`

使用上の注意：

OC4J で生成されたこのファイルには、ランタイム・アプリケーション・エラーが記録されます。

- OC4J サーブレット・アクセス・ログ：

`$ORACLE_HOME/j2ee/OC4J_SECURITY/log/OC4J_SECURITY_default_island_1/default-web-access.log`

使用上の注意：

これも OC4J で生成されたファイルです。シングル・サインオンでのサーブレット・アクセス・ログが記録されます。ファイルをチェックして、認証サーブレットで認証リクエストが受け取られたかどうかを確認します。

- Oracle HTTP Server のエラー・ログ：
\$ORACLE_HOME/Apache/Apache/logs/error_log
使用上の注意：
Oracle HTTP Server が複数のログ・ファイルを切り替えながら使用するよう構成されている場合、それぞれのファイルにはタイムスタンプが追加されます。このタイムスタンプで、最新のログ・ファイルを判別してください。
- Oracle HTTP Server のアクセス・ログ：
\$ORACLE_HOME/Apache/Apache/logs/access_log
使用上の注意：
Oracle HTTP Server が複数のログ・ファイルを切り替えながら使用するよう構成されている場合、それぞれのファイルにはタイムスタンプが追加されます。このタイムスタンプで、最新のログ・ファイルを判別してください。

エラー・メッセージとその他の問題

この項では、エラー・メッセージとその他の問題に対する対処方法について説明します。この項の項目は次のとおりです。

- [基本的なエラー・メッセージと問題](#)
- [Windows ネイティブ認証](#)
- [証明書による認証](#)
- [パスワード・ポリシー](#)

基本的なエラー・メッセージと問題

内部サーバー・エラーです。管理者に通知してください。

原因：Single Sign-On Server が正しく起動されない場合に、このエラー・メッセージが表示されます。

処置：次の手順で問題を解決します。

1. Single Sign-On Server が正しく起動されたかどうかを確認します。確認するには、起動ログ・ファイルでエラーをチェックします。
2. ファイルにデータベース・エラーまたは Oracle Internet Directory のエラーが記録されている場合は、Single Sign-On Server の起動前にデータベースと Oracle Internet Directory が両方とも起動および稼働されていることを確認します。「SSOLoginServlet.init: SSO server started」というメッセージがある場合は、サーバーが正しく起動されています。

3. 次に、ssoServer.log (Single Sign-On Server のログ・ファイル) をチェックします。
4. ログ・ファイルにエラー・メッセージ「NumberFormatException or a specific configuration parameter not found」が記録されている場合は、policy.properties で空白をチェックします。問題のありそうな構成が設定された行の行端にある空白を削除し、Single Sign-On Server を再起動します。
5. ファイル \$ORACLE_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1 にエラー・メッセージ「Orion Launcher SSO Server initialization failed」が記録されている場合は、次の手順を実行します。
 - * データベースが使用可能であることを確認し、Single Sign-On Server を再起動します。
 - * データベースが使用可能である場合、ディレクトリの接続に問題がある可能性があります。opmn ログをチェックします。次のエラー・メッセージがある場合、ssoconf.sql を実行して、Single Sign-On データベースでディレクトリ・アクセスが適切に構成されるようにします。

```
java.lang.NumberFormatException: null
    at java.lang.Integer.parseInt(Integer.java:442)
    at java.lang.Integer.parseInt(Integer.java:524)
    at oracle.security.sso.server.conf.DatabaseConfigReader.
        setSSOServerConfig(DatabaseConfigReader.java:322)
```

6. ssoconf.sql の実行方法については、第 3 章の「ディレクトリ・アクセス用 Single Sign-On Server の設定変更」の項を参照してください。

内部サーバー・エラーです。後で操作を実行してください。

原因: インフラストラクチャ・データベースまたは Oracle Internet Directory が使用不可能であるか停止している場合に、このエラー・メッセージが表示されます。

処置: ssoServer.log でメッセージの詳細をチェックして、データベースまたは Oracle Internet Directory の再起動を試みます。

予期しないエラーが発生しました。管理者に通知してください。

原因: このメッセージは、サーバー側のエラーを示している可能性があります。policy.properties ファイルが正しく構成されていないか、Java クラスがロードされていない可能性があります。また、パートナ・アプリケーションが正しく登録されていない場合もあります。

処置: サーバーに関する問題の場合、ssoServer.log で実際のエラー・メッセージをチェックします。このファイルにメッセージが記録されていない場合は、Oracle HTTP Server のエラー・ログをチェックしてください。アプリケーションの登録に関する問題の場合は、管理ページにログインします。

`http://single_sign-on_host:single_sign-on_port/pls/orasso`

cn=orcladmin ではなく、orcladmin でログインします。ログインできる場合は、サーバーの問題ではなく、パートナ・アプリケーションの登録かアプリケーション自体に問題があります。アプリケーションが正しく登録されているかどうかを確認するには、登録パラメータを出力する Perl スクリプトを記述します。

```
printenv cgi script (REMOTE_USER, HTTP_OSSO_USER_DN, HTTP_OSSO_USER_GUID,  
HTTP_OSSO_SUBSCRIBER, HTTP_OSSO_SUBSCRIBER_DN, HTTP_OSSO_SUBSCRIBER_GUID)
```

mod_osso を使用してスクリプトを保護します。手順については、次のマニュアルの「mod_osso を使用したアプリケーションの保護:2つの方法」の項を参照してください。

『Oracle Application Server Single Sign-On アプリケーション開発者ガイド』

パラメータが正しい場合は、アプリケーションが正しく登録されています。したがって問題はアプリケーションにあります。

問題を特定して修正したら、Single Sign-On Server を再起動します。第2章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

ファイルが見つかりません。

原因: Single Sign-On Server へのアクセス時にこのメッセージが表示される場合があります。

処置: 次の2つのチェックを実行します。

1. Oracle HTTP Server のエラー・ログをチェックします。

メッセージ「file not found」がある場合、Apache は認証リクエストを OC4J に委譲していません。

mod_oc4j.conf で Single Sign-On アプリケーションのマッピングをチェックします。マウント構成 Oc4jMount/ssso OC4J_SECURITY が設定されている必要があります。

2. default-web-access.log をチェックして、サブレットで認証リクエストが受け取られたかどうかを確認します。

許可されていません。このサーバーの /pls/orasso/orasso.home へのアクセス権限がありません。

原因: シングル・サインオンの管理 URL へのアクセス時にこのメッセージが表示される場合があります。ORASSO スキーマのパスワードがデータベースで変更され、dads.conf ファイルでは変更されていない可能性があります。

処置: 次の手順を実行します。

1. \$ORACLE_HOME/Apache/modplsql/conf の dads.conf ファイルを更新します。
2. Oracle HTTP Server を再起動します。第2章の「[Oracle HTTP Server の停止と起動](#)」の項を参照してください。

- スキーマ・パスワードが正しい場合は、Oracle HTTP Server のエラー・ログでエラー・メッセージをチェックします。

監査ログの挿入例外:ORA-00018: 最大セッション数を超えました。

原因: Single Sign-On Server で過剰負荷が発生している場合に、このメッセージが表示されます。要求されたデータベース・セッション数が、init.ora ファイルで指定された数を超えています。

処置: Identity Management インフラストラクチャ・データベースのプロパティを変更します。具体的には、processes パラメータと sessions パラメータの値を増加して、予測される負荷に対応するようにします。データベース固有の構成ファイル (init.ora など) を使用して変更を行います。init.ora は \$ORACLE_HOME/db に格納されています。

接続制限を超えました。

原因: 前述のメッセージと関連性があります。

処置: 操作を再度実行します。

Single Sign-On の管理 UI が動作していません。管理者が「ログイン」をクリックしても、空白のページが表示されます。

原因: この問題には次の 4 つのケースが考えられます。

- ケース 1: Oracle Internet Directory に PUBLIC ユーザー・エントリがありません。ディレクトリに PUBLIC ユーザー・エントリがないか、ユーザー・ニックネーム属性が変更されても新しい属性が PUBLIC エントリに追加されていません。
- ケース 2: ディレクトリには不適切な情報を使用して、Single Sign-On Server が構成されています。
- ケース 3: インストールに問題 (Enabler エントリがない、または、不適切な SSL 登録) がある可能性があります。
- ケース 4: ディレクトリ DIT が変更されたが、この変更内容で Single Sign-On Server が更新されていません。

処置:

- ケース 1: ディレクトリのユーザー検索ベースで PUBLIC ユーザー・エントリを追加します。ユーザー・ニックネーム属性が変更されている場合は、属性を PUBLIC ユーザー・エントリに追加します。
- ケース 2: ssooconf.sql を実行して、正しいディレクトリ情報で Single Sign-On Server を構成します。スクリプトの実行方法については、第 3 章の「[ディレクトリ・アクセス用 Single Sign-On Server の設定変更](#)」の項を参照してください。
- ケース 3: ssooconf.sql を実行して、Enabler エントリで Single Sign-On Server を更新するか、SSL のシングル・サインオン URL を変更します。

- ケース 4: `ssoreoid.sql` を実行して、ディレクトリ DIT の変更内容で Single Sign-On Server を更新します。

認証に失敗しました。

原因: ユーザーのパスワードが正しくないか、サーバーにユーザー認証に必要な権限がありません。

処置:

1. ユーザー DN が適切なレルムに対応することを確認して、ユーザーとしてディレクトリへのバインドを試みます。

```
ldapbind -h directory_server -D user_dn -w user_password
```

バインドに失敗した場合は、ユーザーのパスワードが正しくありません。パスワードを再設定します。バインドに成功した場合は、手順 2 に進みます。

2. Single Sign-On Server としてディレクトリへのバインドを試みます。

```
ldapbind -h directory_server
-p directory_port
-D orclApplicationCommonName=ORASSO_
  SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
-w single_sign-on_server_password
```

バインドに失敗した場合は、バインドで使用したサーバー・パスワードが正しくない可能性があります。正しいパスワードを設定するには、第 3 章の「[ディレクトリ・アクセス用 Single Sign-On Server の設定変更](#)」の説明に従って `ssooconf.sql` を実行します。バインドに成功した場合は、手順 3 に進みます。

3. Single Sign-On アプリケーションが `SecurityAdmins` グループのメンバーであるかどうかを確認します。このグループのメンバーでない場合は、ユーザーを認証できません。

```
ldapcompare -h directory_host
-p directory_port
-D orclApplicationCommonName=ORASSO_
  SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
-w orasso_password
-b "cn=user_dn,cn=users,realm_dn"
-a userpassword
-v user_password
```

メンバーでない場合は、`SecurityAdmins` グループにアプリケーションを追加し (`cn=OracleUserSecurityAdmins,cn=Groups,cn=OracleContext`)、ユーザーを再度認証します。アプリケーションがメンバーである場合は、問題の原因がディレクトリにある可能性があります。

管理者が /pls/orasso にログインしても、管理ページが表示されません。

原因: 管理者が iASAdmins グループのメンバーではありません。

`cn=iASAdmin,cn=Groups,cn=OracleContext,realm_dn`

処置: ディレクトリで iASAdmins エントリの `uniquemember` 属性をチェックします。

```
ldapsearch -h directory_host
-p directory_port
-D orclApplicationCommonName=ORASSO_
  SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
-w orasso_password
-b "cn=iasadmins,cn=groups,cn=oraclecontext,realm_dn"
  "uniquemember=cn=user,cn=users,realm_dn"
```

コマンド内の `user` が iASAdmins の一意のメンバーでない場合は、第 2 章の「[管理権限の付与](#)」の手順に従ってください。

Windows ネイティブ認証

内部サーバー・エラーです。管理者に通知してください。

原因: 中間層コンピュータで、Windows ネイティブ認証が正しく構成されていません。

処置: 次の手順を実行します。

1. `opmn` ログ・ファイルでエラーをチェックします。
2. `ssoServer.log` でエラーをチェックします。
3. `keytab` ファイルが適切な場所にあることを確認します。`jazn-data.xml` に構成されているプリンシパル名が正しいことも確認します。
4. Key Distribution Center にアクセスできるように、シングル・サインオンの中間層コンピュータが正しく構成されていることを確認します。第 8 章の「[Single Sign-On Server の Kerberos サービス・アカウントの設定](#)」の項を参照してください。

パートナ・アプリケーションにアクセスすると、Windows のログイン・ダイアログ・ボックス（ユーザー名、パスワードおよびドメイン・フィールド付きで）が表示されます。

原因: Oracle Internet Directory で対応するユーザー・エントリが見つからないため、Single Sign-On Server で Kerberos トークンを認証できませんでした。

処置: ディレクトリにユーザー・エントリを追加します。

KDCで認証できませんでした。

原因: krb5.conf のレルム名が正しく構成されていない場合に、このエラー・メッセージが表示されることがあります。

処置: /etc/krb5/krb5.conf で default_realm と domain_realm の値をチェックします。レルム名では、大文字 / 小文字を区別します。

Single Sign-On Server が起動しません。ログ・ファイルに「Credential not found.」というメッセージの例外があります。

原因: kerberos-servicename パラメータが正しく構成されていない可能性があります。

処置:

1. orion-application.xml ファイルと jazn-data.xml ファイルで kerberos-servicename が正しく構成されていることを確認します。orion-application.xml ファイルでは、このパラメータのフォーマットは HTTP@sso.ACME.COM です。jazn-data.xml ファイルでは、このパラメータのフォーマットは HTTP/sso.ACME.COM です。
2. ssoServer.log でエラーをチェックします。
3. keytab ファイルが適切な場所にあることを確認します。jazn-data.xml に構成されているプリンシパル名が正しいことも確認します。
4. Kerberos ドメイン・コントローラにアクセスできるように、シングル・サインオン の中間層コンピュータが構成されていることを確認します。第 8 章の「[Single Sign-On Server の Kerberos サービス・アカウントの設定](#)」の項を参照してください。

ブラウザが Windows の Kerberos 認証をサポートしていないか適切に構成されていません。

原因: ユーザーのブラウザがサポートされていないか、正しく構成されていません。

処置: 第 8 章にある「[エンド・ユーザーのブラウザの構成](#)」の手順に従ってください。

「アクセスが許可されていません」、HTTP エラー・コード 403、または「Windows のネイティブ認証に失敗しました。管理者に連絡してください。」

原因: これらのエラー・メッセージは、同じ原因、つまりユーザー・エントリが Oracle Internet Directory にないことに起因します。Windows デスクトップで作業するローカル管理者が、Oracle Internet Directory と同期化されていないエントリを持つシングル・サインオンのパートナ・アプリケーションへのアクセスを試みている可能性があります。

処置: ディレクトリにユーザー・エントリがあるかどうかを確認します。ユーザーの Kerberos プリンシパル属性が、Microsoft Active Directory で適切に同期化されているかどうかを確認します。

証明書による認証

この項では、証明書による認証をデバッグする方法と、エラー・メッセージの内容について説明します。

証明書によるサインオンのデバッグ

1. `policy.properties` でデバッグ・レベルを `DEBUG` に設定し、シングル・サインオン中間層を再起動します。
2. デバッグ時にブラウザの証明書情報を表示するには、`$ORACLE_HOME/sso/lib/ipassample.jar` から `certinfo.jsp` ファイルを抽出します。
3. ファイルを `$ORACLE_HOME/j2ee/applications/sso/web/jsp` に配置します。
4. 次の URL でファイルを表示します。

`https://host:port/sso/.jsp/certinfo.jsp`

エラー・メッセージ

ネットワーク・エラー:接続は拒否されました。

原因: ユーザーが SSL を介してパートナ・アプリケーションへのアクセスを試みると、このメッセージが表示されます。 `httpd.conf` に `SSL Engine on` パラメータがないか、このパラメータが正しく入力されていない可能性があります。

処置: 第7章の「[SSL パラメータの構成](#)」の説明に従って、欠落しているパラメータを追加します。パラメータが存在し、正しく入力されている場合は、Oracle HTTP Server のログ・ファイルに問題が示されている可能性があります。

Single Sign-On Server がユーザーの証明書を要求しません。

原因: オプション・パラメータ `SSLVerifyClient` が `httpd.conf` にないか、正しく入力されていません。

処置: 第7章の「[SSL パラメータの構成](#)」の説明に従って、欠落しているパラメータを追加します。パラメータが存在し、正しく入力されている場合は、Oracle HTTP Server のログ・ファイルに問題が示されている可能性があります。

証明書による認証が失敗し、ユーザーにログイン・ページが表示されます。

原因: ユーザーの証明書がディレクトリにないか、正しく入力されていません。
`ssoServer.log` で詳細を確認します。

処置: ユーザーの証明書をディレクトリに再入力します。第7章にある「[Oracle Internet Directory](#)」の手順を参照してください。

ユーザーのブラウザの証明書がありません。

原因: ユーザーの証明書がブラウザにありません。

処置: 有効な証明書をインストールします。

マッピング・モジュールのクラス名が見つかりません。

原因: x509CertAuth.properties にマッピング・モジュールのクラス名がないか、クラス名が正しくありません。

処置: パラメータ CertificateMappingModule に値が割り当てられていることを確認します。割り当てられている場合は、この値が正しいことを確認します。

マッピング・モジュールのインスタンスを作成できませんでした。

原因: カスタマイズしたマッピング・モジュールが正しく実装されていません。

処置: カスタム・モジュールにデフォルト・コンストラクタがあることを確認します。

マッピング・モジュール・オブジェクトを作成できません。

原因: カスタマイズしたマッピング・モジュールが正しく実装されていません。

処置: 第7章の「[ユーザー名マッピング・モジュールのカスタマイズ \(オプション\)](#)」に従って、指定されたインタフェースをカスタマイズしたモジュールで実装してください。

マッピング・モジュールの作成中に例外が発生しました。

原因: カスタマイズしたマッピング・モジュールが正しく実装されていません。

処置: 第7章の「[ユーザー名マッピング・モジュールのカスタマイズ \(オプション\)](#)」に従って、指定されたインタフェースをカスタマイズしたモジュールで実装してください。

証明書が一致しませんでした。

原因: ユーザーの証明書がディレクトリにないか、正しく入力されていません。ssoServer.log で詳細を確認します。

処置: ユーザーの証明書をディレクトリに再入力します。第7章にある「[Oracle Internet Directory](#)」の手順を参照してください。

パスワード・ポリシー

管理者が [Oracle Internet Directory](#) の orclIsEnabled 属性を使用してユーザーを無効にしましたが、ユーザーはまだログインできます。

原因: orclIsEnabled 属性が正しくありません。

処置: コマンドラインでユーザーとして ldapbind を実行します。これによりアカウント無効のエラーが発生する場合は、属性値を再度入力します。

管理者が [Oracle Internet Directory](#) の orclIsEnabled 属性を使用してユーザーを無効にしましたが、ユーザーはアカウント無効のエラーではなく、認証失敗のエラーを受け取りません。

原因: これは予期されている結果です。ユーザーのアカウントが無効になった場合、ユーザーは認証失敗のエラーを受け取ります。

処置: ありません。

ログイン時にユーザーはパスワードの期限切れのメッセージを受け取ります。

原因: ユーザー・パスワードの期限が切れています。

処置: 管理者はパスワードを再設定する必要があります。管理者はディレクトリでパスワードの有効期限に関する警告を有効にできます。このような警告によって、パスワードの期限切れ前にユーザーはパスワードを変更できます。

ユーザーがシングル・サインオンでログインしますが、パスワードの有効期限が近づいているため、パスワードの変更が要求されます。しかし、ユーザーがコマンドラインでバインドしようとする、このメッセージは表示されず、バインドに成功します。

原因: コマンドラインのツールを使用すると、特定の拡張ディレクトリ・メッセージが表示されません。LDAP のクライアント側 API でのみこれらのメッセージが表示されません。

処置: ありません。

管理者が Oracle Internet Directory のパスワード変更の強制機能を有効にすると (パスワード・ポリシー・エントリの `pwdMustChange` 属性で設定)、ユーザーに対してパスワードの変更が要求されます。パスワードの変更後、ログイン・ページが表示されますが、そこに新しいパスワードで再ログインしようとする、パスワードの変更ページが再度表示されません。

原因: OracleAS Single Sign-On では、パスワードの変更の強制機能がサポートされません。

処置: Oracle Internet Directory でこの機能を有効にしないでください。

デバッグ・レベルの引上げ

OracleAS Single Sign-On には 4 つのデバッグ・レベルがあります。デバッグ・レベル (昇順) と詳細を次に示します。

- ERROR: エラーのみのログ
- WARN: エラー、警告メッセージのログ
- INFO: 情報メッセージ (現在の日付、時間など)、エラー、警告メッセージのログ
- DEBUG: プログラム実行についての詳細、エラー、警告メッセージ、情報メッセージのログ

デバッグの途中で、デバッグ・レベルを DEBUG などに上げる必要性が生じる場合があります。これには、`$ORACLE_HOME/sso/conf` にある `policy.properties` ファイルを変更します。

デバッグ・レベルを変更したら、OC4J_SECURITY インスタンスを再起動します。手順については、第 2 章の「OC4J_SECURITY インスタンスの停止と起動」の項を参照してください。

Single Sign-On データベースでのデバッグ・オプションの有効化

外部アプリケーションへのアクセスに使用する `mod_plsql` コードをデバッグする場合があります。この手順では、Single Sign-On データベースでデバッグを有効にして、詳細ログを表示する必要があります。パートナ・アプリケーションのデバッグにはこの手順を使用できないので注意してください。パートナ・アプリケーションのデバッグ情報は `ssoServer.log` (`$ORACLE_HOME/sso/log` 内) にのみ格納されます。

`mod_plsql` デバッグを有効にするには、ORASSO スキーマにログインして、`ssolsdbg.sql` スクリプトを実行します。スキーマのパスワードの取得方法については、付録 B を参照してください。スクリプト内にあるコメント行をコメント解除してから、スクリプトを実行します。スクリプトのコピーは、`$ORACLE_HOME/sso/admin/plsql/sso` にあります。

次にスクリプトを示します。

```
set scan off;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

-- NOTE: make sure to place slash after each definition to avoid
-- strange looking compiler errors, such as
-- PLS-00103: Encountered the symbol "CREATE"

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS
-- PRAGMA autonomous_transaction;
BEGIN

    /* should probably have session ID and username too being logged */

    INSERT INTO wwsso_log$ VALUES (wwsso_log_pk_seq.nextval,
        substr(str, 1, 1000),
        sysdate, dbms_session.unique_session_id);

    commit;

    null;

END debug_print;
/

show errors;

デバッグ・ログを問い合わせるには、次のコマンドを発行します。

SELECT * FROM WWSO_LOG$ ORDER BY ID;
```

デバッグを無効にするには、ORASSO スキーマにログインして次の PL/SQL スクリプトを作成します。デバッグの終了時にはこの手順を実行する必要があります。この手順を実行しないと、データベース表に不必要なレコードが作成されます。スキーマのパスワードの取得方法については、[付録 B](#) を参照してください。

```
set scan off;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

-- NOTE: make sure to place slash after each definition to avoid
-- strange looking compiler errors, such as
-- PLS-00103: Encountered the symbol "CREATE"

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS
-- PRAGMA autonomous_transaction;
BEGIN

    null;

END debug_print;
/

show errors;
```

UI 操作に関する LDAP トレースの有効化

シングル・サインオンの管理ホームページでは、`dbms_ldap` パッケージを使用してディレクトリ操作を実行します。このような操作に関する詳細は、[Single Sign-On データベースのデバッグ・ログ](#)で取得できます。ただしエラーを特定するには、クライアント側の LDAP トレースを有効にする必要があります。たとえば、管理者と思われる人物が管理者としてログインできない原因を特定する場合、LDAP のクライアント側 API によって、エラーが返される正確な位置を特定できます。その後、RDBMS トレース・ディレクトリ内にあるトレース結果を参照できます。

次の手順に従い、トレースを有効にします。

1. ORASSO スキーマに `debugonldap.sql` をロードします。

```
SQL> connect orasso/password
```

スキーマのパスワードの取得方法については、[付録 B](#) を参照してください。

2. 次のスクリプトを実行します。

```
SQL> @debugonldap.sql
```

debugonldap.sql は次のとおりです。

```
set scan off;
set feedback ON;
set verify ON;
set pages 50000;
set serveroutput ON;

CREATE OR replace PROCEDURE debug_print (str VARCHAR2) AS
BEGIN

    dbms_ldap.set_trace_level(65535);

    INSERT INTO wwsso_log$ VALUES
        (wwsso_log_pk_seq.nextval, substr(str, 1, 1000), sysdate,
        dbms_session.unique_session_id);

    commit;

END debug_print;
/

show errors;
```

シングル・サインオン監査レコードの管理

Single Sign-On Server では、認証の失敗と成功が Oracle 識別情報管理データベースに記録されます。やがて、監査表 ORASSO.WWSSO_AUDIT_LOG_TABLE_T の領域は一杯になります。このような場合、次のエラー・メッセージがデータベースの警告ログに出力されません。

```
ORA-1654: unable to extend index ORASSO.AUDIT_INDEX1 by 128 in tablespace IAS_META
```

さらに、後続の認証リクエストも失敗します。

ORASSO.WWSSO_AUDIT_LOG_TABLE_T を定期的に監視してください。この表が一杯になったら、バックアップを作成して空領域を作るか、領域を追加します。これは製品固有の内部表です。SQL*PLUS からの直接アクセスはサポートされていません。

LDAP 接続キャッシュのリフレッシュ

パフォーマンス上の理由から、Single Sign-On Server は Oracle Internet Directory への接続をキャッシュします。ディレクトリ・サーバーに、スケジューリングした停止またはスケジューリングしていない停止が設定されている場合、Single Sign-On Server では不適切なディレクトリ接続が維持され、ユーザーが外部アプリケーションにアクセスしようとするときディレクトリ設定エラーが発生することがあります。LDAP 接続キャッシュが無効な場合、Oracle HTTP Server を再起動する必要があります。第 2 章の「[Oracle HTTP Server の停止と起動](#)」の項を参照してください。

LDAP 接続キャッシュをリフレッシュする必要があるかどうかを確認するには、次の手順を実行します。

1. Single Sign-On スキーマに接続します。スキーマのパスワードの取得方法については、付録 B を参照してください。
2. 次のコマンドを発行します。

```
SELECT * FROM WWSO_LOG$
```

3. ログ内に次のエラーがある場合は、Oracle HTTP Server を再起動します。
'INVALID LDAP CONNECTION CACHE: RESTART ORACLE HTTP SERVER'
4. WWSO_LOG\$ からエラー・メッセージを削除します。

Oracle Internet Directory 変更後の OC4J の再起動

Oracle Internet Directory 内の値を変更した場合は、その変更内容で Single Sign-On Server を更新する必要があります。たとえば、ディレクトリ内でユーザー、サブスクリイバ、またはグループ検索ベースを変更しても、Single Sign-On Server にその旨を通知しなかった場合、変更されたコンテナのユーザーはログインできなくなります。ssoreoid.sql スクリプトによって、ディレクトリの変更内容で Single Sign-On Server が更新されます。スクリプトの実行方法については、第 3 章の「[ディレクトリ変更による Single Sign-On Server の更新](#)」の項を参照してください。

スクリプトを実行したら、Single Sign-On Server を再起動する必要があります。手順については、第 2 章の「[シングル・サインオン中間層の停止と起動](#)」の項を参照してください。

レプリケーションのトラブルシューティング

地理的に分散したシングル・サインオン・インスタンスを配置する場合、まず Identity Management インフラストラクチャ・データベースをレプリケートする必要があります。データベースをレプリケートするたびに、各レプリケート・ノードでレプリケーション・プロセスを検証し、エラーがある場合は修正する必要があります。Replication Environment Management Tool (remtool) を使用して両方のタスクを実行します。

remtool はマスター定義サイトで実行されます。このツールは \$ORACLE_HOME/ldap/bin にあります。次の各項で説明するように、このツールは 2 つのモードで実行できます。

Advanced Replication 構成の検証

ディレクトリ・レプリケーション・グループが正しく構成されていることを検証するには、次のコマンドを発行します。

```
remtool -asrverify
```

コマンド・オプション `-asrverify` では、検証の進行状況に応じて検証に関するレポートが表示されますが、問題は修正されません。

Advanced Replication 構成の検証と修正

ディレクトリ・レプリケーション・グループが正しく構成されていることを検証し、問題を修正するには、次のコマンドを実行します。

```
remtool -asrrectify -v -connect repadmin/repadmin_password@net_service_name
```

コマンド・オプション `-asrrectify` を使用すると、検証の進行状況に応じて検証に関するレポートが表示され、問題が修正されます。表 A-1 は、他の 2 つのコマンド・パラメータの定義です。

表 A-1 Replication Environment Management Tool のパラメータ

パラメータ	説明
-v	冗長モード。このオプションを指定すると、remtool の進行状況が表示されるだけでなく、remtool.log にツールのすべての動作が記録されます。このファイルは \$ORACLE_HOME/ldap/log にあります。

表 A-1 Replication Environment Management Tool のパラメータ (続き)

パラメータ	説明
-connect	RMS データベースの接続文字列。コマンドの構文に示されるように、この文字列には次の 3 つの構成要素があります。 <ul style="list-style-type: none">■ <code>repadmin</code>: レプリケーション管理者名■ <code>repadmin_password</code>: レプリケーション管理者のパスワード■ <code>net_service_name</code>: RMS データベースのネットワーク・サービス名

Replication Environment Management Tool の詳細は、『Oracle Internet Directory 管理者ガイド』を参照してください。

Single Sign-On スキーマのパスワードの取得

Single Sign-On スキーマのパスワードは、Oracle Application Server Infrastructure のインストール時にランダム化されます。パスワードを取得するには、次の LDAP コマンドを発行します。

```
ldapsearch -h directory_host_name
           -p directory_port
           -D directory_bind_dn
           -w directory_bind_dn_password
           -b "orclReferenceName=infrastructure_database"
              "orclresourcename=ORASSO"
              orclpasswordattribute
```

次の表は、ldapsearch に渡されるパラメータの定義です。

パラメータ	説明
<i>directory_host_name</i>	ディレクトリ・サーバーのホスト名。
<i>directory_port</i>	ディレクトリ・サーバーのポート番号。
<i>directory_bind_dn</i>	ディレクトリに対するユーザー認証の識別名。
<i>directory_bind_dn_password</i>	ディレクトリに対するユーザー認証のパスワード。
<i>infrastructure_database</i>	パスワード属性 (orclpasswordattribute) が定義されているディレクトリ・エントリの識別名。

次に例を示します。

```
ldapsearch -h oid.acme.com
-p 389
-D "cn=orcladmin"
-w welcome1
-b "orclReferenceName=disco.us.acme.com,cn=IAS Infrastructure
Databases,cn=IAS,cn=Products,cn=oraclecontext"
"orclresourcename=ORASSO"
orclpasswordattribute
```

policy.properties

```
# SSO Server policy configurations

#####
# Authentication Levels
# -----
# Set the auth levels from lower value to higher value.
# 10 being the lowest authentication level
# The auth level names (on the right hand side) can be changed to
# some other names if desired as long as the change is consistent
# in other places of the file.

NoSecurity = 10
LowSecurity = 20
LowMediumSecurity = 30
MediumSecurity = 40
MediumHighSecurity = 50
HighSecurity = 60

# DefaultAuthLevel
# -----
# DefaultAuthLevel entry must have a value assigned. This is a mandatory
# requirement if any of the partner app URLs are not listed with the
# auth level mapping.
# If partner app url does not specify the auth level, then the DefaultAuthLevel
# will be used.

DefaultAuthLevel = MediumSecurity

#####
# Protected URL configurations
# -----
# Assign a auth level to each protected (partner) application that is
```

```

# participating in SSO. If any of the partner apps are not listed with
# a specific auth level, then the DefaultAuthLevel will be used.
#
# Protected application URL configuration format:
# "Partner Application Root URL" = "AuthenticationLevel"
# host.company.com¥:port = AuthLevelName
# NOTE: The required backslash(escape character) before the
# colon (:) character above.
# There should be a corresponding auth plugin configured for the
# "AuthenticationLevel" used.
#
# Examples:
# The following example configures a SSO partner application hosted
# on host1.company.com:7777 machine using LowSecurity authentication level.
# This configuration will secure all URLs hosted on this host/port.
# host1.company.com¥:7777 = LowSecurity
#
# The following example configures a SSO partner application hosted
# on host2.company.com:7777 machine using MediumSecurity authentication level.
# This configuration will secure all URLs hosted on this host/port.
# host2.company.com¥:7777 = MediumSecurity

#####
# Authentication plugins
# -----
# Assign a class name that implements SSOServerAuthInterface for each auth
# level defined
#
# Note: also see the WeakAuthLevel attribute which must be set to
# the same auth level corresponding to the weak auth mechanism
#
# The Authentication level name must be appended with "_AuthPlugin"
# keyword.
LowSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerWeakAuth
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerAuth

#####
# Custom Cookie Provider Class name
# -----
# Sample custom cookie tester provider class
# CustomCookie_ProviderPlugin = oracle.security.sso.server.auth.CustomCookieTester

# Custom Cookie auth level
# -----
# This is a mandatory attribute. If custom cookies are not needed it should

```

be set to a higher value than any of the authentication levels used.

CustomCookieAuthLevel = HighSecurity

#SSO Server specific configurations

set the cache size in kbytes

#default is 1000

cacheSize = 1000

#set the minimum number of connections in the connection pool

#default is 5

minConnectionsInPool = 5

#set the maximum number of connections in the connection pool

#default is 150

maxConnectionsInPool = 150

#Debug level {ERROR, WARN, INFO, DEBUG}

default debug level is set to ERROR

debugLevel = ERROR

#Debug file location

#This is a mandatory property that needs to be passed

#the SSO server. A valid file location should be specified here

debugFile = %ORACLE_HOME%/sso/log/ssoServer.log

#Custom login page link

loginPageUrl = /sso/jsp/login.jsp

#Custom weak authentication login page link

weakAuthLoginPageUrl = /sso/jsp/ssWeakAuthLogin.jsp

#Custom change password page link

chgPasswordPageUrl = /sso/jsp/password.jsp

#Wireless login page link

wirelessLoginPageUrl = /wirelessso/wirelesslogin.jsp

wirelessChgPasswordPageUrl = /wirelessso/wirelesscpwd.jsp

用語集

Basic 認証 (basic authentication)

ログイン資格証明がアプリケーション URL で送信される認証方式。アプリケーション URL は HTTP Basic 認証で保護される。

dads.conf

データベース・アクセス記述子 (DAD) の構成に使用する、Oracle HTTP Server 上のファイル。

Directory Integration Platform

企業が外部ユーザー・リポジトリを使用して Oracle 製品に対する認証を行えるようにする、Oracle Internet Directory の機能。

GET

ログイン資格証明がログイン URL の一部として送信される認証方式。

httpd.conf

Oracle HTTP Server の構成に使用するファイル。

iASAdmins

OracleAS でユーザーとグループの管理機能を統括する管理グループ。Single Sign-On 管理者は、iASAdmins グループのメンバーである。

Identity Management インフラストラクチャ・データベース (Identity Management infrastructure database)

OracleAS Single Sign-On と Oracle Internet Directory を含むデータベース。

Infrastructure

識別情報を管理する OracleAS コンポーネント。これらのコンポーネントは、OracleAS Single Sign-On、Oracle Delegated Administration Services、Oracle Internet Directory である。

Kerberos

秘密鍵暗号化を使用するネットワーク認証プロトコル。

Key Distribution Center

Kerberos で認証されたユーザーにサービス・チケットを発行するコンピュータ。このチケットにはユーザーの資格証明が含まれる。

keytab ファイル (keytab file)

Kerberos 認証で、ネットワーク・サービス鍵を格納するファイル。

LDAP 接続キャッシュ (LDAP connection cache)

Single Sign-On Server では、スループットが向上するように、Oracle Internet Directory への接続をキャッシュし、再使用する。

mod_ossli

Oracle HTTP Server 上の SSL モジュール。

mod_osso

Oracle HTTP Server 上のモジュール。これにより、ユーザーが一度 Single Sign-On Server にログインすると、OracleAS Single Sign-On で保護されるアプリケーションがユーザー名とパスワードのかわりに HTTP ヘッダーを受け取ることができる。これらのヘッダーの値は、mod_osso Cookie に格納される。

mod_osso Cookie

HTTP Server に格納されるユーザー・データ。Cookie はユーザーの認証時に作成される。同じユーザーが別のアプリケーションを要求した場合、Web サーバーは mod_osso Cookie の情報を使用してアプリケーションにユーザーをログインさせる。この機能によって、サーバーのレスポンス時間が短縮される。

mod_proxy

Oracle HTTP Server 上のモジュール。これにより、mod_osso を使用してレガシー（または外部）アプリケーションを有効にできる。

Oracle Containers for J2EE (OC4J)

Java2 Enterprise Edition 用の、軽量でスケーラブルなコンテナ。

Oracle Delegated Administration Services

ユーザーとグループの管理機能を実行する、Oracle Internet Directory の Web サービス。

Oracle Directory Manager

Oracle Internet Directory のほとんどの機能を管理する Java ベースの GUI。iASAdmins グループのメンバーの作成に使用する。また、パスワード・ポリシーの管理にも使用する。

Oracle Enterprise Manager

Single Sign-On Server 上でのサーバーの負荷とユーザー・アクティビティを監視する GUI。Oracle Enterprise Manager は他の OracleAS コンポーネントも監視する。

Oracle HTTP Server

Hypertext Transfer Protocol (HTTP) を使用する、Web トランザクションを処理するソフトウェア。オラクル社では、Apache Group が開発した HTTP ソフトウェアを使用する。

OracleAS Portal

ファイル、イメージ、アプリケーション、Web サイトを統合するメカニズムを提供する、シングル・サインオンのパートナー・アプリケーション。「外部アプリケーション」ポートレットで、外部アプリケーションにアクセスできる。

policy.properties

OracleAS Single Sign-On の多用途な構成ファイル。Single Sign-On Server で必要な基本パラメータが含まれる。マルチレベル認証など、拡張機能の構成にも使用する。

POST

ログイン資格証明がログイン・フォーム本体内で送信される認証方式。

Secure Sockets Layer (SSL)

幅広く使用されるセキュリティ・プロトコル。このプロトコルは、公開鍵暗号を使用してクライアントとサーバー間の通信を保護する。クライアントはサーバーで提供される公開鍵を使用して、秘密鍵交換を実行する。

Simple and Protected GSS-API Negotiation Mechanism (SPNEGO)

Windows ベースの Kerberos 認証が行われるプロトコル。

Single Sign-On SDK

シングル・サインオンのパートナー・アプリケーションを有効にする API。SDK は、PL/SQL API および Java API、さらにこれらの API を実装する方法を実証するサンプル・コードで構成される。

Single Sign-On Server

Single Sign-On アプリケーション（経費報告、電子メール、福利厚生情報など）に安全にログインできるようにするプログラム・ロジック。

URLC トークン (URLC token)

認証されたユーザー情報をパートナ・アプリケーションに渡すコード。パートナ・アプリケーションはこの情報を使用してセッション Cookie を作成する。

アカウント・ロックアウト (account lockout)

Single Sign-On ユーザーが、任意の数のワークステーションから、Oracle Internet Directory で許可されている回数を超えるアカウントとパスワードの組合せを送信したときに発生する。デフォルトのロックアウト時間は 24 時間である。

アプリケーション・サービス・プロバイダ (application service provider)

Web アプリケーションをインストールしてメンテナンスし、通常は有料でこれらのアプリケーションを顧客が利用できるようにする企業。

外部アプリケーション (external application)

Single Sign-On Server に認証を委譲しないアプリケーション。そのかわり、HTML ログイン・フォームが表示され、アプリケーションのユーザー名とパスワードが要求される。最初のログイン時に、ユーザーは Single Sign-On Server でこれらの資格証明を取得するように選択できる。その後、ユーザーは外部アプリケーションに透過的にログインできるようになる。

仮想ホスト (virtual host)

実際のサーバーの代理となるサーバー。OracleAS Single Sign-On では、仮想ホストを使用して複数の Single Sign-On Server 間のロード・バランシングを実現する。また、仮想ホストはセキュリティの追加層を提供する。

強制認証 (forced authentication)

ユーザーが事前に設定された時間アイドル状態であった場合に、再認証をユーザーに強制する動作。OracleAS Single Sign-On では、グローバル・ユーザーの非アクティビティ・タイムアウトを指定できる。この機能はセキュリティ重視のアプリケーションがインストールされている場合に使用する。

グローバリゼーション・サポート (globalization support)

Graphical User Interface (GUI) に対する複数言語サポート。OracleAS Single Sign-On では 29 言語がサポートされている。

グローバルな一意のユーザー ID (globally unique user ID)

ユーザーを一意に識別する数値。ユーザー名、パスワード、識別名は変更または追加できるが、グローバルな一意のユーザー ID は常に同じである。

グローバル・ユーザーの非アクティビティ・タイムアウト (global user inactivity timeout)

Single Sign-On ユーザーが事前に設定された時間アイドル状態であった場合に、再認証を強制するオプション機能。グローバル・ユーザーの非アクティビティ・タイムアウトは、シングル・サインオン・セッションのタイムアウトよりかなり短い。

サードパーティのアクセス管理システム (third-party access management system)

OracleAS Single Sign-On を使用して OracleAS アプリケーションにアクセスするように変更できる、Oracle 以外のシングル・サインオン・システム。

サービス鍵 (service key)

Kerberos 認証における、サーバーの秘密鍵。

識別情報管理レルム (identity management realm)

Oracle Identity Management インフラストラクチャの単一インスタンス内にある個々のネームスペース (または DIT)。

識別名 (distinguished name)

LDAP 準拠のディレクトリのエントリの場所を識別する名前。DN とも呼ばれる。次の例にあるユーザーの識別名は、名前エントリと親エントリが左から右に昇順で並ぶ。

```
cn=jsmith,cn=users,cn=defaultsubscribers,cn=acme,cn=com
```

証明書失効リスト (certificate revocation list)

X.509 証明書が失効したユーザーのリスト。アプリケーションはこのリストを使用して、アプリケーションにアクセスするユーザーを決定する。

シングル・サインオフ (single sign-off)

シングル・サインオン・セッションを終了し、すべてのアクティブなパートナ・アプリケーションから同時にログアウトするプロセス。作業中のアプリケーションからログアウトすると、シングル・サインオフを実行できる。

成功 URL (success URL)

アプリケーションのセッションとセッション Cookie を設定するルーチンへの URL。

セッション鍵 (session key)

Kerberos 認証で、クライアントによるチケットの取得、さらにはユーザーの資格証明の取得を可能にするデータ構造。

中間層 (middle tier)

Oracle HTTP Server と OC4J で構成される、シングル・サインオン・インスタンスの一部。シングル・サインオンの中間層は、Identity Management インフラストラクチャ・データベースとクライアントの間にある。

データベース・アクセス記述子 (database access descriptor: DAD)

特定の OracleAS コンポーネント (Single Sign-On スキーマなど) のデータベース接続情報。

ディレクトリ情報ツリー (directory information tree: DIT)

LDAP ディレクトリを構成するエントリの階層コレクション。

デジタル証明書 (digital certificate)

非対称型暗号化で、公開鍵所有者の ID を保証するデータ構造。証明書は、認証局という信頼できる第三者が発行する。したがって、メッセージの暗号化に公開鍵を安全に使用できることを鍵所有者に対して保証する。

認証プラグイン (authentication plugin)

特定の認証方式の実装。OracleAS Single Sign-On には、パスワード認証、デジタル証明書、Windows ネイティブ認証、サードパーティのアクセス管理用に Java プラグインが用意されている。

認証レベル (authentication level)

アプリケーションに特定の認証動作を指定できるパラメータ。このパラメータと特定の認証プラグインをリンクできる。

パートナ・アプリケーション (partner application)

Single Sign-On Server に認証機能を委譲する、OracleAS アプリケーションまたは Oracle 以外のアプリケーション。このようなアプリケーションでは、`mod_osso` ヘッダーを受け取ったり、ユーザーをサーバー自体にリダイレクトできるので、ユーザーを再認証する必要がない。ユーザーをサーバー自体にリダイレクトするには、パートナ・アプリケーションと Single Sign-On SDK を統合する必要がある。

プロキシ・サーバー (proxy server)

実際のサーバー (またはホスト) の代理となるサーバー。OracleAS Single Sign-On では、プロキシを使用してロード・バランシングを実現する。またプロキシは、セキュリティの追加層として使用される。「ロード・バランサ」を参照。

ユーザー名マッピング・モジュール (user name mapping module)

ユーザー証明書をユーザーのニックネームにマップする Java モジュール。マップ後、ニックネームは認証モジュールに渡される。認証モジュールはこのニックネームを使用して、ディレクトリからユーザーの証明書を取得する。

レガシー・アプリケーション (legacy application)

Single Sign-On Server に認証を委譲するように変更できない、古いアプリケーション。外部アプリケーションとも呼ばれる。

ロード・バランサ (load balancer)

過剰負荷またはフェイルオーバーにより、複数の Single Sign-On Server 間で接続リクエストを振り分ける、ハードウェア・デバイスおよびソフトウェア。BigIP、Alteon、Local Director などは、一般的なハードウェア・デバイスである。ロード・バランシング・ソフトウェアには、OracleAS Web Cache がある。

索引

A

addsub.csh スクリプト, 10-8

B

Basic 認証方式, 5-3, 5-8

D

Distributed Cluster Management, 4-10, 9-14

E

enblhstg.csh スクリプト, 10-7

G

GET 認証方式, 5-3

H

httpd.conf ファイル, 4-8, 4-9, 4-12, 4-13, 9-14, A-10

I

iASAdmins 管理グループ, 2-2

Identity Management インフラストラクチャ・データベース

SSL 用の構成, 9-4

複数のレルムのサポート, 10-2

レプリケート, 9-26 ~ 9-29

IP チェック, 2-8

J

jazn-data.xml ファイル, 8-8

K

Kerberos プロトコル, 8-2

krb5.conf ファイル, 8-6

L

LDAP コマンドライン・ツール, 3-2

LDAP 接続キャッシュ, A-16

log files, A-3

M

mod_osso

Single Sign-On SDK との比較, 1-3

概要, 1-3

登録, 4-2 ~ 4-5, 4-10, 4-11, 9-16, 9-31

mod_osso.conf ファイル, 2-11, 4-13

O

oidprovtool, 9-33

opmn.xml ファイル, 8-7

Oracle Delegated Administration Services, 1-8, 3-2

Oracle Directory Manager, 2-3, 3-2

Oracle HTTP Server

SSL 構成, 9-3

起動と停止, 2-4

構成

証明書対応のサインオン, 7-4, 7-5

シングル・サインオン中間層, 9-14

パートナ・アプリケーション中間層, 4-8

Oracle Internet Directory

- Microsoft Active Directory との同期化, 13-4
- SSL 用の構成, 9-7, 9-8
- Windows ネイティブ認証の構成, 8-4
- サードパーティのアクセス管理における役割, 13-4
- 証明書対応サインオンの構成, 7-10, 7-11

OracleAS Active Failover Clusters, 9-17, 9-18

OracleAS Certificate Authority, 7-5

OracleAS Cold Failover Cluster, 9-25

OracleAS Discoverer, 14-2, 14-4, 14-5

OracleAS Portal

- 「外部アプリケーション」ポートレット, 5-6
- 登録, 4-2

OracleAS Single Sign-On

- 管理者, 2-2 ~ 2-4
- 管理ページ, 1-5
- 外部アプリケーション, 5-2, 5-4, 5-5
- グローバリゼーション・サポート, 2-8, 12-9
- サンプル・ファイル, 2-11
- スキーマ, 1-5
- スクリプト

 - addsub.csh, 10-8
 - enblhstg.csh, 10-7
 - ssocfg, 9-15, 9-20, 9-30
 - ssogito.sql, 2-9
 - ssomig, 14-2
 - ssooconf.sql, 3-7, 9-29, A-4, A-6
 - ssoreoid.sql, 3-8, A-7, A-16

- タイムアウト, 1-8
- ディレクトリ・アクセスの構成, 3-7
- ディレクトリ情報ツリー, 3-5, 3-6
- デフォルト以外の構成, 9-1
- パスワード, 1-8
- パスワード・ポリシー, 3-3, 3-5
- ブラウザの環境設定, 2-6
- ホームページ, 1-5
- ユーザー・アカウント, 3-2
- ユーザー属性, 1-3
- 利点, 1-1

OracleAS Web Cache, 4-9, 9-15, 9-31

OracleAS Wireless, 1-9

ossoca.jar ツール, 2-8

osso.conf ファイル, 4-2 ~ 4-4, 4-10, 9-16

ossoreg.jar ツール

- 構文, 4-3

パラメータ, 4-3, 4-5

例, 4-5

P

policy.properties ファイル

- サードパーティのアクセス管理, 13-9
- サンプル, C-1
- 証明書対応のサインオン, 7-7
- デバッグ, A-12
- マルチレベル認証, 6-3 ~ 6-6
- 目的, 2-4

POST 認証方式, 5-3

R

Replication Environment Management Tool, A-17

S

Single Sign-On Server

- LDAP 接続キャッシュ, A-16
- Windows ネイティブ認証の構成, 8-5 ~ 8-10
- アクセス, 1-5
- 概要, 1-2
- 起動と停止, 2-5
- キャッシュ, 3-8
- サードパーティのアクセス管理における役割, 13-2
- ディレクトリ・アクセスの構成, 3-7
- 配置オプション

 - OracleAS Active Failover Clusters, 9-17, 9-18
 - 地理的に分散しているインスタンス, 9-22 ~ 9-24
 - 複数の中間層, 9-10, 9-18
 - レプリケートされたディレクトリ, 9-18, 9-20
 - リバース・プロキシ, 9-29

single sign-on server

- log files, A-3

Single Sign-On 管理者

- 権限の付与, 2-2
- 任務, 2-2

SSL (Secure Sockets Layer), 9-2 ~ 9-7

ssl.conf ファイル, 4-12, 4-13, 7-4, 7-5

- 「SSO Server 管理」ページ, 2-7
- 「SSO Server の編集」ページ, 2-8

sso_apache.conf ファイル, 9-6

ssocfg スクリプト, 9-15, 9-20, 9-30
ssogito.sql スクリプト, 2-9
ssomig.log ファイル, 14-6
ssomig スクリプト
 構文, 14-2
 実行, 14-6
 パラメータ, 14-3, 14-4
ssooconf.sql スクリプト, 3-7, 9-29, A-4, A-6
ssoreoid.sql スクリプト, 3-8, A-7, A-16
ssoReplSetup.jar ツール, 9-28, 9-29

T

targets.xml ファイル, 11-5

U

URL、SSL 用の構成, 9-7
URL、保護, 9-4 ~ 9-7, 9-15

W

web.xml ファイル, 8-9
Windows ネイティブ認証
 エラー・メッセージ, A-8, A-9
 概要, 8-2
 構成, 8-4 ~ 8-12
 システム要件, 8-3, 8-4
 認証の流れ, 8-2, 8-3
 フォールバック認証, 8-13
 ブラウザ設定, 8-11, 8-12
 ログインの例, 8-14

X

X509CertAuth.properties ファイル, 7-7, 7-9

あ

アカウント・ロックアウト, 3-4
アプリケーション・サービス・プロバイダ, 10-2
エクスポートおよびインポート
 エラー・メッセージ, 14-8, 14-10
 使用例, 14-5
 スクリプト, 14-6
エラー・メッセージ
 Windows ネイティブ認証, A-8, A-9

エクスポートおよびインポート, 14-8 ~ 14-10
基本, A-3, A-8
証明書対応のサインオン, A-10, A-11
パスワード・ポリシー, A-11

か

仮想ホスト, 4-11, 4-13, 9-30
監視用ページ
 アクセス, 11-2
 ポート, 11-5
監視用ホームページ, 11-2
管理ページ
 アクセス, 2-6
 外部アプリケーション, 5-2
 デバッグ, A-14, A-15
外部アプリケーション
 mod_osso/mod_proxy によるアクセス, 5-6 ~ 5-9
 管理ページ, 5-2
 概要, 1-3
 追加, 5-2 ~ 5-4
 認証の流れ, 1-6, 1-7
 認証方式
 Basic, 5-3, 5-8
 GET, 5-3
 POST, 5-3
 編集, 5-5
 ログイン, 5-5, 5-6
「外部アプリケーションの管理」ページ, 5-2 ~ 5-5
「外部アプリケーション」ポートレット, 5-6
グローバルゼーション・サポート
 配置固有ページ, 12-9
 標準ページ, 2-8
グローバル・ユーザーの非アクティビティ・タイムアウト
 概要, 1-8
 構成, 2-9, 2-11
 スクリプト, 2-9
構成ファイル
 httpd.conf, 4-8, 4-9, 9-14, A-10
 jazn-data.xml, 8-8
 krb5.conf, 8-6
 opmn.xml, 8-7
 osso.conf, 4-2, 4-4, 4-10, 9-16
 policy.properties, 6-3, 6-6, 7-7, A-12, C-1
 ssl.conf, 7-4, 7-5
 sso_apache.conf, 9-6

targets.xml, 11-5
web.xml, 8-9
x509CertAuth.properties, 7-7,7-9
「このアプリケーションのログイン情報を保存する」
チェック・ボックス, 5-5

く

サードパーティのアクセス管理
移行, 13-11 ~ 13-13
コード例, 13-8, 13-10
認証の流れ, 13-2, 13-3
ログアウト, 13-10
サーバー・キャッシュ, 3-8
サーバーの高可用性
構成, 9-25
配置オプション
OracleAS Active Failover Clusters, 9-17, 9-18
地理的に分散しているインスタンス, 9-22, 9-24
複数の中間層, 9-10 ~ 9-17
レプリケートされたディレクトリ, 9-18, 9-20
サンプル・ファイル
証明書対応のサインオン, 2-11
配置固有ページ, 2-11
識別情報管理レلم
オーバーヘッド, 10-2
管理権限, 10-10
概要, 10-2
構成, 10-7 ~ 10-10
認証の流れ, 10-5, 10-6
パートナ・アプリケーションのサポート, 10-5
利点, 10-2
「失敗ログインの詳細」ページ, 11-4
障害時リカバリ, 9-25
証明書失効リスト, 7-11
証明書対応のサインオン
CRL メンテナンス, 7-11
エラー・メッセージ, A-10, A-11
構成
Oracle HTTP Server, 7-4, 7-5
Oracle Internet Directory, 7-10, 7-11
Single Sign-On Server, 7-5 ~ 7-10
ユーザー名マッピング・モジュール, 7-7, 7-9
サンプル・ファイル, 2-11
認証の流れ, 7-2
シングル・サインオフ・ページ
インストール, 12-12

パラメータ, 12-7
シングル・サインオン・セッションのタイムアウト
, 2-8
スクリプト
ssogito.sql, 2-9
ssomig, 14-2, 14-3
ssooconf.sql, 3-7
ssoreoid.sql, 3-8
スクリプトの更新, 3-8

た

タイムアウト
グローバル・ユーザーの非アクティビティ・タイム
アウト, 1-8, 2-9, 2-11
シングル・サインオン・セッションのタイムアウト
, 2-8
ディレクトリ・アクセス
構成, 3-7
スクリプト, 3-7
ディレクトリ・エントリ, OracleAS Single Sign-On 用
, 3-5, 3-6
デバッグ
PL/SQL ページ, A-13, A-14
管理ページ, A-14, A-15
同期化
Microsoft Active Directory と Oracle Internet
Directory 間, 8-4
サードパーティのディレクトリと Oracle Internet
Directory 間, 13-4
ディレクトリと Single Sign-On Server 間, 9-32,
9-33

な

認証アダプタ, 「認証プラグイン」を参照
認証の流れ
Windows ネイティブ認証, 8-2, 8-3
サードパーティのアクセス管理, 13-2, 13-3
識別情報管理レلم, 10-5, 10-6
証明書対応のサインオン, 7-2
認証プラグイン, 6-4
認証レベル, 6-3, 6-4

は

配置固有ページ

- OracleAS Wireless のサポート, 12-11
- インストール, 12-11, 12-12
- ガイドライン, 12-10
- グローバリゼーション・サポート, 12-9
- サンプル・ファイル, 2-11
- 例, 12-12
- 配置例
 - 地理的に分散しているインスタンス, 9-22
 - パートナー・アプリケーション, 4-6
 - 複数の中間層, 9-11
 - マルチレベル認証, 6-5, 6-6
 - レプリケートされたディレクトリ, 9-18
- バックアップおよびリカバリ, 9-25
- パートナー・アプリケーション
 - 概要, 1-2
 - 高可用性の設定, 4-6
 - 登録, 4-2, 4-5, 4-10, 4-11, 9-7, 9-16
 - 配置, 4-6
 - 例, 1-2
- パスワード
 - 管理, 3-3
 - 外部アプリケーション, 1-3
 - 構成, 3-5
 - スキーマ, 3-8, B-1
 - パスワードの変更の強制機能, 3-4
 - 変更, 1-8, 3-4
 - 有効期限, 3-3
 - リセット, 1-8, 3-4, 12-5
 - ルール, 3-3
- パスワードの変更の強制機能, 3-4
- パスワードの変更ページ
 - インストール, 12-11
 - エラー・メッセージ, 12-8
 - 概要, 1-8
 - 動作, 3-4
 - パラメータ, 12-6
- パスワード・ポリシー, 3-3, 3-5
- ブラウザ設定
 - Windows ネイティブ認証, 8-12
 - Internet Explorer 5.0, 8-11
 - Internet Explorer 6.0, 8-11, 8-12
 - 標準, 2-6
- プロキシ・サーバー
 - 機能, 9-29
 - 構成, 9-30, 9-31
- プロキシ認証, 5-6, 5-9

ま

- マスター定義サイト, 9-19
- マルチマスター・レプリケーション, 9-26
- マルチレベル認証
 - 構成, 6-5, 6-6
 - 流れ, 6-2
 - 認証レベル, 6-3, 6-4
 - プラグイン, 6-4

や

- ユーザー・アカウント
 - 管理, 3-2
 - ロックアウト, 3-4
- ユーザー管理ツール, 3-2
- ユーザー名マッピング・モジュール, 7-7
 - カスタム実装, 7-8, 7-9
 - デフォルトの実装, 7-7
- 猶予期間ログイン, 3-4

ら

- リバース・プロキシ, 9-29 ~ 9-31
- リモート・マスター・サイト, 9-19
- ロード・バランサ
 - OracleAS Active Failover Clusters, 9-17
 - OracleAS Web Cache, 9-15
 - 複数のシングル・サインオン中間層, 9-10, 9-13, 9-15, 9-18, 9-19, 9-20
 - 複数のパートナー・アプリケーションの使用, 4-6, 4-9
- ログインの例
 - Windows ネイティブ認証, 8-14
 - サードパーティでのアクセス, 13-2
- ログイン・ページ
 - インストール, 12-11
 - エラー・メッセージ, 12-7, 12-8
 - パスワードのリセット機能, 12-5
 - パラメータ, 12-3, 12-4

