Oracle® Application Server Certificate Authority

管理者ガイド

10*g*（10.1.4.0.1）

部品番号 : B31506-01

2006 年 10 月

ORACLE®

Oracle Application Server Certificate Authority 管理者ガイド , 10*g*（10.1.4.0.1）

部品番号 : B31506-01

原本名 : Oracle Application Server Certificate Authority Administrator's Guide, 10*g* (10.1.4.0.1)

原本部品番号 : B15989-01

原本著者 : Vinaye Misra

原本協力者 : Amit Agarwal, Howard Bae, Pratik Datta, Lakshmi Kethana, Belinda Leung, Valarie Moore, Mehul Poladia, Deepak Ramakrishnan, Gary Truong

目次

3 OracleAS Certificate Authority 配置ガイドライン

8 Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース

A コマンドライン管理

B CA の階層の設定

C OracleAS Certificate Authority のトラブルシューティング

D 拡張領域

E SSO での SSL および PKI の有効化

F 保護された OracleAS Certificate Authority への外部アクセス

G OracleAS Certificate Authority での S/MIME

H OracleAS Certificate Authority で使用するための OracleAS WebCache の構成

I Oracle Application Server Certificate Authority の Web インタフェース

表一覧

図一覧

はじめに

Oracle Application Server Certificate Authority（OCA）では、PKI（公開鍵インフラストラクチャ）テクノロジに基づいて、デジタル証明を発行および管理できます。Oracle Application Server Certificate Authority が提供する簡単な管理方法によってこの証明を行うと、セキュリティが向上し、ユーザー認証にかかる時間とリソースが削減されます。

Oracle Application Server Certificate Authority を使用すると、エンド・エンティティ（ユーザーおよびサーバー）は自分自身を認証できます。この認証では、OracleAS Single Sign-On、SSL またはその他の既存の認証方式に基づいて OracleAS Certificate Authority が発行する証明書を使用します。これらの証明書を使用すると、証明書を識別することによって認証をより速く、より安全に処理できます。各証明書は、発行時に Oracle Internet Directory に公開され、期限切れまたは失効時に削除されます。ユーザーは、OracleAS Certificate Authority の Web インタフェースにアクセスして、ユーザー自身の証明書の発行、失効または更新をリクエストできます。エンド・ユーザーが OracleAS Certificate Authority の Web インタフェースにアクセスするために特別な権限は必要ありません。ただし、証明書の発行、失効または更新を行うには、OCA から以前に発行された証明書を使用して、OracleAS Single Sign-On または SSL による認証を済ませておく必要があります。これが済んでいないと、OCA の管理者が手動で認証することが必要になります。

このマニュアルでは、公開鍵証明書の管理方法について説明します。

ここでは、次の項目について説明します。

対象読者

このマニュアルは、次のような方を対象としています。

- 証明書リクエストおよび証明書関連の操作を管理する Oracle Application Server Certificate Authority の管理者
- 認証、暗号化およびその他の様々な目的で OCA により発行された証明書のユーザー

ドキュメントのアクセシビリティについて

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

ドキュメント内のサンプル・コードのアクセシビリティについて

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

外部 Web サイトのドキュメントのアクセシビリティについて

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

Oracle サポート・サービスへの TTY アクセス

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

Oracle Identity Management

Oracle Application Server Certificate Authority は、Oracle Identity Management のコンポーネントです。Oracle Identity Management は統合されたインフラストラクチャであり、Oracle 製品および他のエンタープライズ・アプリケーションに対して分散セキュリティ・サービスを提供します。Oracle Identity Management インフラストラクチャには、次のコンポーネントおよび機能が含まれます。

- **Oracle Internet Directory**。Oracle Database に実装されている、スケーラブルで強力な LDAP V3 準拠のディレクトリ・サービスです。
- **Oracle Directory Integration**。Oracle Internet Directory の一部で、Oracle Internet Directory などのディレクトリとユーザー・リポジトリの同期を可能にします。また、Oracle のコンポーネントおよびアプリケーションに対して自動プロビジョニング・サービスを提供します。標準インタフェースを使用して、サード・パーティのアプリケーションに対しても同様のサービスを提供します。
- **Oracle Delegated Administration Services**。Oracle Internet Directory の一部で、ユーザーおよびアプリケーション管理者が信頼できる、プロキシ・ベースのディレクトリ情報管理を提供します。
- **Oracle Application Server Single Sign-On**。Oracle およびサード・パーティの Web アプリケーションに対して、シングル・サインオン・アクセスを提供します。

- **Oracle Application Server Certificate Authority**。X.509 バージョン 3（以降 v3）PKI 証明書を生成して公開し、厳密な認証方式、保護メッセージなどをサポートします。

  SSL、OC4J および HTTP Server を使用することに加えて、OCA は、OracleAS Single Sign-On および Oracle Internet Directory に依存するように構成されています。OracleAS Certificate Authority は、使用中の DN の Oracle Internet Directory エントリにすべての有効な証明書を公開し、Netscape、Internet Explorer または Mozilla による証明書の登録および保存またはインストールをサポートします。OracleAS Certificate Authority では、失効した証明書は即座に、期限切れの証明書は定期的に Oracle Internet Directory から削除されるため、OracleAS Single Sign-On などのコンポーネントはこれらの Oracle Internet Directory エントリに依存できます。また、管理者も、OracleAS Single Sign-On を使用して URL を公開できるように OracleAS Certificate Authority を構成することができます。この構成を選択すると、証明書を所有していないすべての OracleAS Single Sign-On 認証済ユーザーが、証明書リクエスト用の OracleAS Certificate Authority ページを表示できます。OracleAS Certificate Authority 証明書は、すべての Oracle コンポーネントの認証、または OracleAS Single Sign-On 対応のすべてのアプリケーションの使用の認可に使用できます。

通常のエンタープライズ・アプリケーションの配置では、1 つの Oracle Identity Management インフラストラクチャが複数のサーバーおよびコンポーネント・インスタンスで構成されて配置されます。この構成には、高可用性、情報のローカライズ、委任コンポーネント管理などのメリットがあります。企業に配置された各追加アプリケーションは、ID 管理サービスに共有インフラストラクチャを使用します。この配置モデルには次のメリットがあります。

- **一時的な作業 :** ID 管理インフラストラクチャの計画および実装は、エンタープライズ・アプリケーションを配置するたびに行う必要はなく、一時的な作業になります。その結果、ポータル、J2EE アプリケーション、E-Business アプリケーションなどの新しいアプリケーションを、迅速に配置できます。
- **集中管理 :** 複数の場所で管理されている場合でも、識別情報を集中管理します。変更は、すべてのエンタープライズ・アプリケーションですぐに有効になります。
- **ユーザーのシングル・サインオン :** 集中セキュリティ・インフラストラクチャを使用すると、エンタープライズ・アプリケーション全体でユーザーのシングル・サインオンを実現できます。
- **単一の統合ポイント :** ID 管理インフラストラクチャを一元化すると、企業の Oracle 環境と他の ID 管理システムの間に単一の統合ポイントが提供されます。これによって、複数の「ポイントツーポイント」のカスタム統合ソリューションを使用する必要がなくなります。

Oracle Identity Management インフラストラクチャの計画、配置および使用の詳細は、『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。

OCA のデフォルトの配置構成については、Oracle Application Server のインストレーション・ガイドのインストール手順に関する項を参照してください。推奨の配置構成およびインストール手順は、そのマニュアルの 11.9 項を参照してください。

関連ドキュメント

- Oracle Application Server のインストレーション・ガイド
- 『Oracle Application Server 管理者ガイド』
- 『Oracle Application Server セキュリティ・ガイド』
- 『Oracle Application Server Single Sign-On 管理者ガイド』
- 『Oracle Application Server 高可用性ガイド』
- 『Oracle Database バックアップおよびリカバリ・アドバンスト・ユーザーズ・ガイド』
- 『Oracle Internet Directory 管理者ガイド』
- 『Oracle Advanced Security 管理者ガイド』.

このマニュアルの多くの例で、Oracle インストール時にデフォルトでインストールされるシード・データベースのサンプル・スキーマを使用しています。これらのスキーマの作成方法および使用方法は、『Oracle Database サンプル・スキーマ』を参照してください。

表記規則

このマニュアルでは次の表記規則を使用します。

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

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

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

```
http://www.oracle.co.jp/support/
```

製品マニュアル

製品のマニュアルは、次の URL にあります。

```
http://otn.oracle.co.jp/document/
```

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

```
http://www.oracle.co.jp/education/
```

その他の情報

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

```
http://www.oracle.co.jp
http://otn.oracle.co.jp
```

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

1

公開鍵インフラストラクチャと OracleAS

公開鍵インフラストラクチャは、パブリック・ネットワークおよびプライベート・ネットワーク上でセキュアな通信ができるように設計されています。さらに、PKI では、電子メールの保護、否認防止用のデジタル署名、データ整合性という重要な機能が実現されます。過去 25 年以上の間 PKI で問題となっていることの 1 つに、PKI に関連する必要なインフラストラクチャを配置できないことがあります。実際、このインフラストラクチャのコストおよび複雑さが、PKI が広範囲に使用されない主な原因となっています。

Oracle Identity Management インフラストラクチャは、高可用性、スケーラビリティ、ディレクトリ・サービス、シングル・サインオン、委任管理サービスおよびディレクトリ統合サービスを組み合せて、PKI に理想的な環境を提供します。このインフラストラクチャは、これらのメリットによって、Oracle Application Server Certificate Authority が常駐する理想的な場所になります。その結果、OCA は、Oracle Identity Management インフラストラクチャの一部となり、このインフラストラクチャが持つ集中管理機能とスケーラビリティによって、PKI を配置するコストと複雑さが軽減されます。

この章では、PKI について詳しく説明します。説明する内容は次のとおりです。

PKI とは

PKI は次の要素を統合します。

- データの転送および格納を保護する暗号化アルゴリズム
- 異なるユーザーに対して一意の暗号化を実行できる暗号鍵
- 広範囲なネットワークで暗号をセキュアに使用でき、なおかつ、適切な受信者のみがセキュアに復号化できる鍵の配布方法
- 鍵とその正当な所有者の関係を保証する信頼できるエンティティ

こうした要素が一体になることで、この章で説明しているとおり、イントラネット、エクストラネットおよび E-Commerce アプリケーションに、高度なセキュリティが実現します。安全で信頼できるユーザー認証、データ整合性、署名されたメッセージの否認防止、転送または格納された情報への不正アクセスの防止などの利点があります。

この項では、PKI の主要機能について説明します。説明する内容は次のとおりです。

- 鍵のペア
- 認証局（CA）およびデジタル証明書
- 登録局（RA）

鍵のペア

暗号化は、データをわかりにくくして不正アクセスまたは改ざんから保護することを意味します。ただし、認可された受信者が元のデータに復元できる方法を使用します。元のデータを暗号化または置換する方法には、送信者と受信者のみが知っている鍵と呼ばれるテキストまたは数値を使用します。送信者と受信者の両方が同じ鍵を使用する場合、その暗号化方法は「対称型」と呼ばれます。対称型方式で暗号化する場合は、必要な機密性を損なわずに、傍受者が取得できないようにその鍵を送信者と受信者の両方に配布する方法が問題となります。また、送信者と受信者のペアごとに個別の鍵が必要となるため、各通信者が多くの鍵（受信者ごとに 1 つ）を保持する必要があるという問題もあります。

PKI の根幹は、秘密鍵と公開鍵の**鍵のペア**を使用することです。このペアは、公開鍵と秘密鍵が異なるため「非対称型」と呼ばれます。各ユーザーは、通信相手のユーザーの数に関係なく、鍵のペアを 1 つしか所有しません。

PKI の各鍵は、2 進数で構成されています。通常は 512 ～ 2048 ビットです。512 は弱い暗号、1024 は強い暗号で、2048 は軍事用です。アルゴリズムは、これらの鍵ビットとデータ・ビットを組み合せてデータを暗号化します。

鍵のペアの各所有者は、公開鍵は公開しますが、秘密鍵は公開しません。他のユーザーは、公開鍵を使用して、鍵のペアの所有者に送信するプライベート・メッセージを暗号化できます。それに対して、鍵のペアの所有者は、秘密鍵を使用してそのメッセージを復号化するか、または重要な送信メッセージに署名します。この方式の有効性は、公開鍵は簡単かつ安全に配布でき、復号化に必要な秘密鍵は共有しないという考えに基づいています。

認証局（CA）およびデジタル証明書

認証局は、公開鍵の所有者の識別情報を保証する信頼できる第三者機関です。このマニュアルで説明している Oracle Application Server Certificate Authority は、こうしたエンティティの 1 つです。他には VeriSign 社、Thawte 社などがあります。認証局は、**デジタル証明**を作成して特定のユーザーへの公開鍵のリンクを検証します。このデジタル証明書には、公開鍵、および鍵の所有者と署名を行う認証局についての情報が含まれます。PKI の証明書を使用してユーザーの識別情報を認証することは、運転免許証やパスポートによる身元確認と類似しています。これらの証明書を忘れたり、変更することはほとんどあり得ないためです。

この項は次のトピックで構成されています。

CA 署名

CA は、秘密鍵を使用してデジタル証明に署名します。この署名によって、すべてのユーザーが、CA の公開鍵を使用して、署名が認証されていて証明書が有効であることを検証できます。証明書が検証されると、証明書の所有者の公開鍵は、所有者に対するメッセージの暗号化またはメッセージに残した所有者の署名の検証に使用できます。

信頼のレベル

様々なレベルの CA が存在します。各 CA がより信頼できるソース（上位レベルの CA）から証明書を受信すると、信頼の階層が確立されます。ルート CA から下位 CA を経由して、下位レベルのトラスト・ポイントに至る信頼できる各リンク行は、高信頼パスと呼ばれます。

トップ・レベルの CA はルート CA と呼ばれ、信頼関係の原点となっています。ルート CA の下の CA は、下位 CA と呼ばれます。同じルート CA を共有するすべてのエンド・ユーザーは、最終的に同じ認証ソースを信頼しているため、信頼できる方法で相互に通信できます。

公開鍵とリンクされた識別情報が検証済であることを正式に表す証明書を信頼することは、証明書を発行した機関（CA）を信頼することを意味します。これに対して CA は、証明書のリクエスト時に提供される情報の検証を、登録局（RA）という別のエンティティに任せています。

デジタル証明書の内容および使用方法

OracleAS Certificate Authority が発行するデジタル証明書は、ISO 規格の X.509 v3、および Internet Engineering Task Force（`http://www.ietf.org/`）の PKIX ワーキング・グループが公開している RFC 2459 に準拠します。

X.509 v3 規格では、SSL、暗号化およびデジタル署名用に別々の証明書を有効にする拡張領域が導入されました。X.509 v3 証明書には、次のユーザー情報が含まれます。

- 証明書所有者の識別名（DN）
- 証明書を発行した認証局の DN

注意：

DN の DC コンポーネントおよび EMAIL コンポーネントでは、印刷可能な（ASCII）文字のみを使用する必要があります。

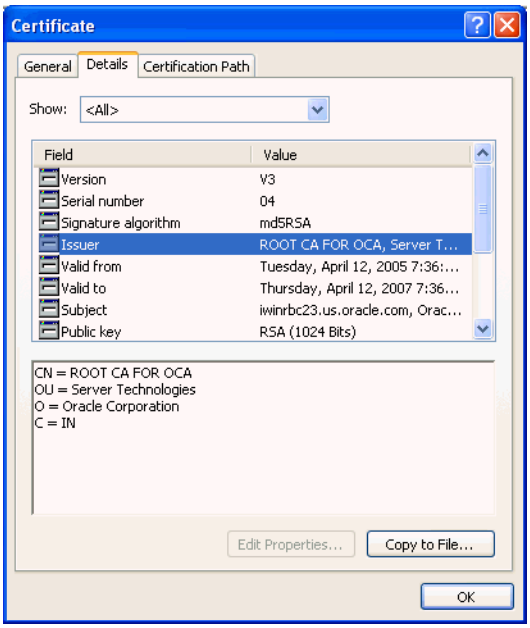
この制限は、マルチバイト・キャラクタ・セットを使用するロケールでも、識別名の DC コンポーネントおよび EMAIL コンポーネントには ASCII 文字を使用する必要があるという意味です。

- 証明書所有者の公開鍵
- 証明書発行者のデジタル署名

- 証明書の有効期間
- 証明書のシリアル番号

図 1-1 に、これらのすべての要素を含む、新規発行の証明書を示します。

図 1-1 OracleAS Certificate Authority が発行する証明書



OCA は、X.509 証明書を発行および処理します。また、複数の証明書タイプをサポートするので、X.509 CRL（証明書失効リスト）の発行および処理も行います。

PKI 資格証明のコンテナ

コンテナは、メッセージの署名や検証などの PKI 操作に使用する様々な関連資格証明の保持に使用します。このようなコンテナのデータ構造に、ユーザーの秘密鍵、証明書およびユーザーが信頼するルート証明書のリストが安全に格納されます。SSL 接続でのピアの識別情報または受信された署名の検証には、信頼できる証明書を使用します。Netscape や Internet Explorer などのブラウザでは、証明書のコンテナを「証明書データベース」や「証明書キャッシュ」と呼ぶことがあります。Oracle Identity Management インフラストラクチャでは、このコンテナを「Oracle Wallet」と呼びます。

登録局（RA）

登録局はオプションのシステムであり、エンド・エンティティ識別情報の検証や認証など、一部の管理機能を CA から委任されます。これは、CA とユーザー間のインタフェースとして動作します。RA は、新しい証明書の発行、期限切れの証明書の更新および証明書の失効のリクエストを受信します。RA は、リクエストを行ったユーザーが指定した識別情報を評価して、そのユーザーが、本人であるかどうかを検証します。既存の証明書の場合、RA は、リクエストを行ったユーザーと指定した識別情報および公開鍵との関連を検証し、承認されたリクエストを CA に送信します。

注意： OracleAS では、RA の機能は、Oracle Application Server Certificate Authority 自体が実行します。

PKI の利点

PKI には次の利点があります。

- セキュアで信頼できるユーザー認証

  信頼できる認証は 2 つの要素に依存しています。1 つ目の要素は、公開鍵 / 秘密鍵のペアの秘密鍵部分を所有していることの証明です。これは、公開鍵を使用する自動処理によって検証されます。2 つ目の要素は、認証局による、公開鍵が特定の識別情報に属することの検証です。PKI ベースのデジタル証明書によって、鍵のペアに基づいた識別情報の接続が検証されます。

- データ整合性

  確立された公開鍵 / 秘密鍵のペアの秘密鍵を使用してデジタル・トランザクションに署名すると、送信中にデータを変更することが難しくなります。ユーザー X によるこのデジタル署名は、ユーザー X の秘密鍵で暗号化された元のメッセージのコード化されたダイジェストです。受信者は、ユーザー X の対応する公開鍵を使用して、メッセージが変更されていないか、およびそのメッセージが実際に、X によって送信されたものかを検証できます。メッセージまたはダイジェストが変更されていると、公開鍵を使用した検証に失敗し、メッセージまたはダイジェストが信頼できないものであることが受信者にわかります。

- 否認防止

  デジタル署名により、メッセージ発信者は、メッセージを作成したことを否認することも難しくなります。

- 送信または格納された情報への不正アクセスの防止

  公開鍵から秘密鍵を導出するために必要な時間と手間を考慮すると、鍵のペアの所有者以外のユーザーがメッセージを復号化することはまずできません。

OracleAS PKI の概要

この項では、OracleAS PKI の概要について説明します。説明する内容は次のとおりです。

- 以前のコストおよび問題
- OracleAS PKI の利点
- OracleAS PKI のコンポーネント

以前のコストおよび問題

OracleAS PKI を導入するまでは、認証に使用する証明書の取得に多くの手順と時間が必要でした。適切なフォームを取得して必要事項を正確に入力し、適切な登録局に配信する必要がありました。登録局によって識別情報が検証され、承認済フォームがユーザーに戻されると、ユーザーはそのフォームを認証局に配信する必要がありました。認証局はこの承認済フォームを処理し、実際の証明書を発行しました。この配信を行うために、承認済のリクエストの内容を別のフォームにカット・アンド・ペーストすることも、たびたび必要になりました。認証局がこの新しいフォームを受信した後、実際の証明書が届くまで数日または数週間かかることもありました。

OracleAS PKI の利点

OracleAS PKI によって、多くのコストと時間を必要とした以前の手順のほとんどが不要になり効率化されます。OracleAS PKI は、認証機能、ユーザー・リポジトリおよびアプリケーションを緊密に統合します。また、第三者機関に証明書をリクエストし、手動でその証明書をアプリケーションおよび中央ディレクトリに送信するというユーザーの負担を軽減します。

OracleAS PKI の主要部分である Oracle Application Server Certificate Authority は、わかりやすいワンストップ・ソリューションで、使いやすい Web インタフェースが用意されており、登録局（RA）は CA に統合されています。ユーザーは、リクエストをオンラインで送信し、認証情報を提供して自動的に証明書を取得します。この証明書は、Oracle Internet Directory 内のユーザーのエントリに自動的にリンクされ、シングル・サインオンを有効にして、対応するディレクトリのエントリに対してチェックを行い、ユーザーを認証します。この Identity Management インフラストラクチャおよび OCA は、データベースや Oracle Collaboration Suite など、他の多くの Oracle コンポーネントで使用されます。

証明書は、ユーザーに対して発行された後、シングル・サインオン資格証明のかわりに使用できます。その結果、認証要件が PKI ほど厳しくないシングル・サインオン・アプリケーションだけでなく、PKI 用に構成されたすべてのシングル・サインオン・アプリケーションに即座にアクセスできます。前述のとおり、ユーザーの鍵のペアを使用してデジタル署名を有効にでき、整合性および否認防止が保証されます。

OracleAS PKI のコンポーネント

OracleAS PKI は業界標準仕様に準拠し、次のコンポーネントを使用します。

- コンテナ、Oracle Wallet および Oracle Wallet Manager（OWM）
- Secure Sockets Layer（SSL）
- Oracle Internet Directory および Single Sign-On（SSO）
- Oracle Application Server Certificate Authority

コンテナ、Oracle Wallet および Oracle Wallet Manager（OWM）

証明書の形式と内容および証明書のコンテナは、いくつかの国際規格で定義されています。X.509 v3 規格で、これらの証明書の仕様が定義されています（「デジタル証明書の内容および使用方法」を参照）。PKCS #12（個人情報交換構文）規格で、コンテナの仕様が定義されています。

既存の標準 PKI 資格証明を所有するユーザーは、その資格証明を PKCS #12 形式でエクスポートし、Netscape Communicator、Microsoft Internet Explorer などのブラウザまたは Oracle Wallet Manager にインポート（インストール）できます。PKCS #12 規格によって、相互運用性が高まり、組織にかかる PKI 配置のコストが軽減されます。

> **関連項目：** 第 8 章の次の項を参照してください。
>
> 「ブラウザへの新規発行の証明書のインポート」
>
> 「ブラウザからの Wallet のエクスポート（バックアップ）」
>
> 「ファイル・システムからの証明書のインポート」

Oracle Wallet Manager を使用すると、このような証明書の取得、使用および格納を簡単に実行できます。Oracle Wallet Manager には、証明書およびそのコンテナを使用して行う通常の操作、または証明書およびそのコンテナに対して行う通常の操作を標準化したグラフィカル・ユーザー・インタフェース（GUI）が用意されています。この GUI を、OracleAS では Oracle Wallet と呼びます。

関連資料：『Oracle Advanced Security 管理者ガイド』

サーバー管理者は、OWM を使用して PKCS #10 証明書リクエストを作成できます。完了したリクエストが OWM で生成された後、管理者は、そのリクエストをファイル・システムに保存したり、OCA のサーバー / 下位 CA 証明書フォームにコピー・アンド・ペーストして、OracleAS Certificate Authority 証明書をリクエストできます。前述の「関連項目」の最後のリンクを参照してください。

これらの Wallet は PKCS #12 規格に準拠し、OCA で使用されるコンテナです。Netscape Communicator、Microsoft Internet Explorer などのサード・パーティ・アプリケーションと相互運用性があるため、オペレーティング・システム間に貴重な移植性が実現します。

Secure Sockets Layer（SSL）

Secure Sockets Layer は、インターネットの保護に最も広く使用されているプロトコルです。公開鍵を暗号化して認証、暗号化、データ整合性を有効にします。また SSL では、これらのツールを使用して、サーバーとクライアントの両方で使用する一意のワンタイム・セッション・パスワードを暗号化することにより、セッション鍵の管理をセキュアにできます。このパスワードは、セキュアに送受信された後、サーバーとクライアント間で行われる後続の通信すべての暗号化に使用されます。この暗号化によって、他のユーザーはそれらのメッセージを解読できなくなります。Oracle HTTP Server、Web Cache、Oracle Internet Directory、Oracle データベースなど、すべてのサーバー・コンポーネントで、通信の保護に SSL が使用されます。

Oracle Internet Directory および Single Sign-On（SSO）

Oracle Internet Directory は、LDAP バージョン 3 のディレクトリです。LDAP は、Lightweight Directory Access Protocol の略称です。このディレクトリによって、OCA が発行した証明書の公開などの認証資格証明用に中央リポジトリが提供されるため、PKI ベースのシングル・サインオンが可能になります。Oracle Internet Directory によって、アクセスが属性レベルで制御されるため、特定のユーザーによる特定の属性の読取り、書込みまたは更新権限が制限されます。また、SSL を使用して、ディレクトリに対する問合せとレスポンスを保護および認証します。

Oracle Application Server Certificate Authority

OracleAS 製品スイートに新しく追加された OracleAS Certificate Authority を使用すると、証明書のライフ・サイクル全体を管理できます。このライフ・サイクルには、新しい証明書に対するリクエストの記録および処理、ユーザー資格証明の検証、これらの証明書の発行、更新または失効が含まれます。以前、これらの処理には、単調でエラーが発生しやすい、記録保持操作およびカット・アンド・ペースト操作が別々に必要でした。OCA では、数回のクリックで証明書の生成、送信および格納を実行できます。これによって、資格証明の検証および認証が単純かつ高速になりました。

OCA は、Oracle Application Server のインフラストラクチャ・コンポーネントです（必須ではありません）。

2

ID 管理および OracleAS Certificate Authority の機能

Oracle Application Server Certificate Authority はセキュアなメカニズムで、クライアントおよびサーバーに対して X.509 v3 デジタル証明書の作成および署名を行います。OracleAS Certificate Authority は、管理者が選択または作成したポリシーを適用します（第 6 章を参照）。また、その管理者によって、スケーラブルな Web ベースのインタフェースを使用して制御されます（第 5 章を参照）。OracleAS Certificate Authority は、Web ベースのユーザー・インタフェース（第 8 章を参照）を含む、このような証明書をサポートおよび管理するための安全なインフラストラクチャを提供します。

この章では、OracleAS Certificate Authority の機能および処理を有効にするアーキテクチャについて説明します。内容は次のとおりです。

- ID 管理のコンポーネントとアーキテクチャ
- Oracle Application Server Certificate Authority の主要機能
- 証明書の自動または手動プロビジョニング
- 階層的な認証局のサポート

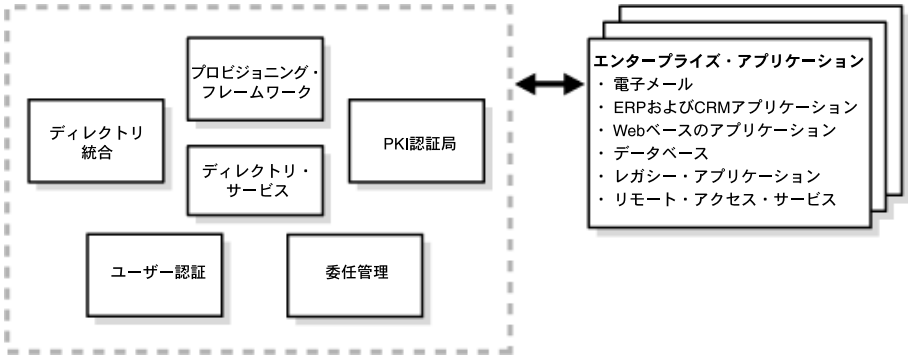
ID 管理のコンポーネントとアーキテクチャ

完全な ID 管理ソリューションには、次のコンポーネントが含まれます。

- ユーザー情報を格納および管理するための、スケーラブルで安全な、規格準拠のディレクトリ・サービス
- エンタープライズ・プロビジョニング・システム（HR アプリケーションなど）にリンク可能、またはスタンドアロンで動作可能なユーザー・プロビジョニング・フレームワーク
- ID 管理システムの管理者が、個々のアプリケーションの管理者または直接エンド・ユーザーにアクセス権を選択して委任できる委任管理モデルおよびアプリケーション
- 様々な要件に対応する適切なセキュリティ・モデルおよびユーザー・インタフェース・モデル
- 企業が、ID 管理ディレクトリを、レガシー・ディレクトリまたはアプリケーション固有のディレクトリに接続できるディレクトリ統合プラットフォーム
- ユーザー認証用のランタイム・モデルおよびアプリケーション
- PKI 証明書を作成および管理するシステム

図 2-1 に、企業 ID 管理ソリューションのモデルを示します。

図 2-1 企業 ID 管理ソリューションのモデル



次の項で、Oracle Identity Management インフラストラクチャの詳細を説明します。

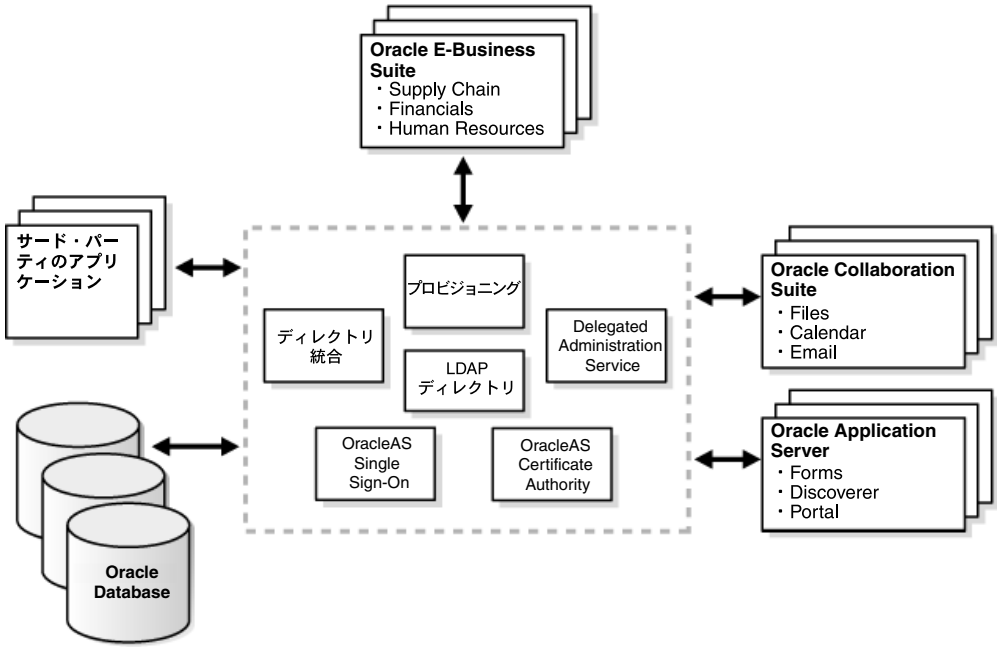
- Oracle Identity Management
- 企業での Oracle Identity Management の使用
- Oracle セキュリティ・アーキテクチャでの Oracle Identity Management の役割
- Oracle Identity Management での OracleAS Certificate Authority の役割
- SSO 統合を介した簡易プロビジョニング

Oracle Identity Management

Oracle Identity Management は、企業全体でユーザーおよびアプリケーションを保護する場合に Oracle 製品が依存する統合インフラストラクチャです。Oracle Identity Management の代表的なリリース手段は Oracle Application Server ですが、これは、他の Oracle 製品でもインフラストラクチャの一部として付属しています。Oracle Identity Management インフラストラクチャには、次のコンポーネントが含まれます。

- Oracle Internet Directory。Oracle Database に実装されている、スケーラブルで堅牢な LDAP V3 準拠のディレクトリ・サービスです。
- Oracle Directory Integration。Oracle Internet Directory と他のディレクトリの同期を可能にし、Oracle コンポーネントおよびアプリケーションに対して自動プロビジョニング・サービスを提供します。また、標準インタフェースを使用して、サード・パーティのアプリケーションに対しても、自動プロビジョニングを提供します。
- Oracle Delegated Administration Services。ユーザーおよびアプリケーション管理者によるディレクトリ情報を、プロキシ・ベースで信頼できる形で管理できます。このコンポーネントは、ポータルや電子メールなどのアプリケーションで活用できます。
- Oracle Application Server Single Sign-On。Oracle およびサード・パーティの Web アプリケーションへのシングル・サインオン・アクセスをエンド・ユーザーに提供します。
- Oracle Application Server Certificate Authority。X.509 v3 証明書を生成および公開して、PKI ベースの強固な認証方式をサポートします。

図 2-2 企業統合型の ID 管理



企業での Oracle Identity Management の使用

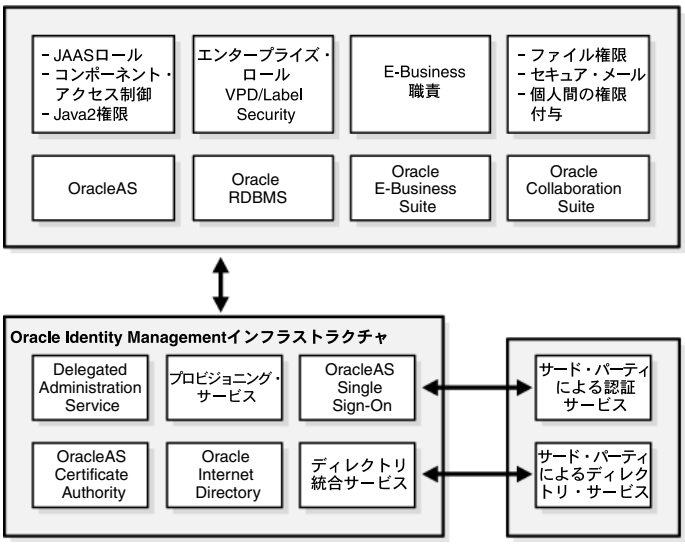
Oracle Identity Management は、Oracle 製品にエンタープライズ・インフラストラクチャを提供するように設計されていますが、カスタムおよびサード・パーティのエンタープライズ・アプリケーション、ハードウェアおよび企業のネットワーク・オペレーティング・システム用の、堅牢でスケーラブルな ID 管理ソリューションとしても機能します。

また、オラクル社は、サード・パーティのアプリケーション・ベンダーと提携しているので、Oracle Identity Management をインストールした後、サード・パーティのアプリケーションですぐに使用できるようになっています。

Oracle セキュリティ・アーキテクチャでの Oracle Identity Management の役割

各 Oracle テクノロジ・スタック（Oracle Database（RDBMS）、Oracle Application Server 10*g*、E-business Suite および Oracle Collaboration Suite）では、それぞれの設計の核として適切なセキュリティ・モデルをサポートします。それでも、これらのすべてで、それぞれのセキュリティ・モデルおよび機能の実装に、Oracle Identity Management インフラストラクチャを使用しています。図 2-3 はこのアーキテクチャを図で示したものです。

図 2-3 Oracle Identity Management のセキュリティ・モデル



OracleAS は、Java Authentication and Authorization Service（JAAS）と呼ばれる J2EE 準拠のセキュリティ・サービスをサポートします。JAAS は、Oracle Internet Directory で定義したユーザーおよびロールを利用できるように構成できます。同様に、データベースのセキュリティ機能である、エンタープライズ・ユーザーおよび Oracle Label Security という手段によって、Oracle Internet Directory で定義したユーザーおよびロールを活用できます。つまり、これら両方のプラットフォームがあることで、それぞれ固有のセキュリティ機能を使用して開発されたアプリケーションで、基盤となる Identity Management インフラストラクチャを透過的に活用できるようになります。

Oracle Collaboration Suite および Oracle E-Business Suite は、RDBMS および OracleAS プラットフォーム上に階層化されたアプリケーション・スタックです。前述のとおり、この階層化によって、Oracle Identity Management インフラストラクチャとの間接統合があるレベルで行われます。また、これらの製品には、Oracle Identity Management に依存した独立機能もあります。たとえば、Oracle E-mail や Oracle Voicemail & Fax などの Oracle Collaboration Suite コンポーネントでは、Oracle Internet Directory を使用して、製品固有のユーザー設定項目、ユーザーの連絡先およびアドレス帳などを管理します。これらのコンポーネントは、電子メールを保護するために、OCA に依存します。

これらの Oracle テクノロジ製品では、Provisioning Integration Service を活用して、ユーザー・アカウントとユーザー権限のプロビジョニングおよびプロビジョニング解除を、自動的に行い

ます。Delegated Administration Services は、ユーザーの設定項目および連絡先のセルフ・サービス管理に広く使用されています。また、これらの製品のセキュリティ管理インタフェースは、サービス・ユニットと呼ばれるユーザー管理およびグループ管理の基本単位を活用します。

Oracle Identity Management での OracleAS Certificate Authority の役割

Oracle Application Server Certificate Authority は、Oracle Internet Directory および Single Sign-On を介して、Oracle Identity Management インフラストラクチャを使用します。Oracle Internet Directory によって、証明書を発行時に公開し、その情報をすべての接続データベースに伝播できます。Single Sign-On は、アプリケーションなどの Oracle コンポーネント（Oracle Collaboration Suite のエンタープライズ・ユーザーおよび電子メール保護機能など）が依存する標準インタフェースを提供します。OCA が発行した証明書は、単純かつ高速で、整合性のある ID 管理に求められるセキュアな認証をサポートします。

SSO 統合を介した簡易プロビジョニング

OracleAS Single Sign-On に対して認証を行うアプリケーション・ユーザーは、透過的に証明書を取得でき、技術教育や PKI の理解は必要ありません。その後は、アプリケーションで、新しく発行された証明書を使用して OracleAS Single Sign-On によるこのアプリケーション・ユーザーの認証が透過的に行われ、セキュリティが強化されます。発行された PKI 証明書は、Oracle Internet Directory に自動的に公開されます。この強力な機能を提供することにより、Oracle Database、Oracle Internet Directory および OracleAS Single Sign-On のセキュリティ、高可用性およびスケーラビリティが高まります。

OCA の管理者は、オプションで OracleAS Certificate Authority を構成し、OracleAS Single Sign-On を介して URL をブロードキャストできます。これを実行すると、OracleAS Single Sign-On を介して認証を行うユーザーは、OCA の簡単なグラフィカル・インタフェースを使用して証明書を要求できます。この証明書があれば、その後の OracleAS Single Sign-On 認証がさらに簡単になります。これは、OracleAS Single Sign-On が Oracle Internet Directory を使用してユーザーのブラウザから自動的に提供される証明書を検証できるためです。OracleAS Certificate Authority は、失効および有効期限切れの証明書をディレクトリから定期的に自動削除するため、OracleAS Single Sign-On はディレクトリの情報を信頼することができます。

Oracle Identity Management でのサード・パーティの PKI のサポート

OCA は Oracle Identity Management の一部です。Oracle 製品は、Oracle 製品どうしが緊密に統合されているのみでなく、規格準拠の任意の認証局とも一緒に使用できます。証明書プロビジョニング・ツールである Oracle Wallet Manager は、X.509-v3 規格準拠の認証局を使用できます。

> **関連資料：** Oracle Wallet Manager の詳細は、『Oracle Application Server 管理者ガイド』および『Oracle Application Server セキュリティ・ガイド』を参照してください。

Oracle Wallet Manager は、PKCS#12 形式で表示された既存のサーバー証明書をサポートできます。このような証明書をインポートする手順は、『Oracle Application Server 管理者ガイド』の、サード・パーティにより作成された証明書および Wallet のインポートに関する項を参照してください。

Oracle Application Server Single Sign-On および Oracle Internet Directory は、サード・パーティの規格準拠認証局を使用できます。このようなサード・パーティから Oracle Internet Directory に証明書をロードし、Single Sign-On での PKI 認証を可能にする手順は、『Oracle Application Server Single Sign-On 管理者ガイド』の第 7 章を参照してください。

Oracle Application Server Certificate Authority の主要機能

OracleAS Certificate Authority の主要機能は、スケーラブルな Web ブラウザ・インタフェースを介して使用できます。これらの機能は、業界標準の証明書の管理、LDAP ディレクトリとの統合およびポリシーの適用をサポートします。説明する内容は次のとおりです。

- オープン規格に対するサポート
- 柔軟なポリシー
- 管理者およびエンド・ユーザーにとっての使いやすさ
- OCA 画面でのグローバリゼーション・サポート
- スケーラビリティ、パフォーマンスおよび高可用性
- S/MIME デジタル暗号化および署名を介する電子メールの保護

オープン規格に対するサポート

OracleAS Certificate Authority は、オープン規格をサポートするので、異機種間コンピューティング環境での通信ができます。OCA は次の規格をサポートしています。

- X.509 v3 証明書および証明書失効リスト（CRL）
- IETF PKIX 規格
- 最長 4096 ビットの署名鍵（RSA）
- スマートカード
- Microsoft Internet Explorer および Netscape Communicator を使用した証明書リクエスト
- 様々な PKCS 規格（5、7、8、10、12 など）
- 証明書リクエストの複数の登録プロトコル（証明書リクエストの Signed Public Key and Challenge（SPKAC）や Public Key Cryptography Standard（PKCS）#10 など）
- S/MIME（Secure Multipart Internet Mail Extensions）

柔軟なポリシー

ポリシーはルールおよび制限のセットであり、ユーザーに対して許可する処理、アクセスまたは権限を制限します。Oracle Application Server Certificate Authority はユーザー（グループ）が取得可能な証明書プロパティの制限に使用できる、構成可能なポリシー・ルールのセットを提供します。サイトでは、これらのルールをカスタマイズして、特定の PKI 要件を満たすように、OCA を構成できます。デフォルトのポリシー・ルールがいくつか用意されていますが、独自のポリシー・ルールも適用できます。

管理者およびエンド・ユーザーにとっての使いやすさ

Oracle Application Server Certificate Authority の Web ベースの管理インタフェースには、「認証管理」および「構成管理」という 2 つの主要タブがあります。これらを使用する場合、管理者は、最初のエントリ時にフォームに必要事項を入力し、その後証明書をインポート（インストール）して登録する必要があります。

「認証管理」タブを使用すると、管理者は、証明書リクエストの承認または拒否、および証明書失効リスト（CRL）の生成または更新ができます。また、様々な理由（セキュリティが損なわれた場合など）によって、発行された証明書を失効させることもできます。（OracleAS Certificate Authority を停止および起動する場合、管理者は、コマンドライン・ツール `ocactl` を使用する必要があります。このツールには管理者のパスワードが必要です。）

OCA の Web ベースのエンド・ユーザー・インタフェースにも、「ユーザー証明書」および「サーバー / 下位 CA 証明書」という 2 つのタブがあります。「ユーザー証明書」タブをクリックすると、ユーザーは、OracleAS Single Sign-On 名およびパスワードを使用してユーザー自身を認証できます。OracleAS Single Sign-On 認証を選択して**「送信」**をクリックすると、OracleAs Single Sign-On ウィンドウが表示され、OracleAS Single Sign-On ユーザー名とパスワードが入力できます。

「ユーザー証明書」ページには、すべての証明書リクエストやそのステータス（保留、認可済、拒否済）などが表示されます。新しい証明書のリクエスト、ディスクへの証明書失効リスト（CRL）の保存、ブラウザへの CRL のインストール、または認証方式の変更を実行できます。

「サーバー / 下位 CA 証明書」タブをクリックすると、新しいサーバー / 下位 CA 証明書のリクエスト、ディスクへの CRL の保存、ブラウザへの CRL のインストール、または CA 証明書の保存およびインストールを実行できます。また、ID/ シリアル番号または一般名で、特定の証明書または証明書リクエストを検索できます。

関連項目：

- 管理インタフェースの詳細は、第 5 章「Oracle Application Server Certificate Authority の構成」を参照してください。
- エンド・ユーザー・インタフェースの詳細は、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」を参照してください。

OCA 画面でのグローバリゼーション・サポート

特定の前提を満たす場合は、OracleAS Certificate Authority の管理者用画面およびユーザー用画面を、クライアントまたはサーバーの言語で表示できます。それには、データベースのキャラクタ・セットが UTF8 であると同時に、必要な言語が OracleAS Certificate Authority によりサポートされている必要があります。この前提が満たされない場合は、英語が使用されます。管理コマンドライン・ツールの `ocactl` で使用できるのは英語によるコマンドのみですが、メッセージ（情報メッセージやエラー・メッセージなど）は、サポートされている場合にかぎり、サーバー・ロケールの言語で表示されます。サポートされていない場合は、英語で表示されます。

関連項目： 第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「画面でのグローバリゼーション・サポートの構成」

スケーラビリティ、パフォーマンスおよび高可用性

OracleAS Certificate Authority は、OracleAS をアプリケーション・サーバーとして統合し、Oracle Database を次の情報のリポジトリとして統合することによって、自動的にこれらの機能を利用できます。

- ユーザー、ロールおよび権限
- 保留中および承認済の証明書リクエスト
- 発行された証明書
- ユーザー・アクティビティのロギング情報および JAZN 認証情報

S/MIME デジタル暗号化および署名を介する電子メールの保護

OracleAS Certificate Authority 管理者は、OCA のコマンドライン・ツールを使用して、OCA および電子メール・クライアント（Outlook、Mozilla/Netscape）ですぐに使用できる **S/MIME** 証明書および Wallet を作成できます。暗号化または署名された電子メールの送受信が簡単になります。OCA 管理者は、安全な Web インタフェースを使用して、S/MIME を使用するように OCA の通知およびアラートを構成できます。

関連項目：

暗号化または署名された電子メールに必要な S/MIME Wallet を作成する手順は、第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「CA SSL Wallet および CA S/MIME Wallet の再生成」を参照してください。

S/MIME を使用するように OCA を構成する手順は、第 5 章「Oracle Application Server Certificate Authority の構成」の「「通知」サブタブ」を参照してください。

一般的な S/MIME 操作については、付録 G「OracleAS Certificate Authority での S/MIME」を参照してください。

証明書の自動または手動プロビジョニング

手動プロビジョニングでは、管理者がユーザーに証明書を発行します。Oracle Application Server Certificate Authority が OracleAS Single Sign-On および SSL を使用して提供する自動プロビジョニングでは、PKI のサポートに使用してきた従来の方法でのコストおよび遅延を削減できます。

OracleAS Single Sign-On 認証を行うため、OracleAS Certificate Authority は mod_osso および OracleAS Single Sign-On を使用します。OracleAS Single Sign-On で自動的に認証されているユーザーに OracleAS Certificate Authority から証明書を発行する場合にこれらの方式を使用すると、証明書の管理が簡単になります。

以前に X.509 v3 証明書を発行されているユーザーは、OracleAS Certificate Authority に対する認証手段として、その証明書を HTTPS 経由で送信できます。証明書が同じ OracleAS Certificate Authority で発行され、まだ失効していない場合、証明書リクエストは自動的に認可されます。承認が迅速に行われるため、ユーザーは、管理者またはセキュリティ担当者がリクエストを承認するまで待たずに、暗号化または署名の追加証明書を取得できます。

また、OracleAS Certificate Authority は、Netscape と Internet Explorer を統合することによってスマートカードをサポートし、ブラウザのロケール設定で指定されている言語でそのフォームを表示できます。

OracleAS Certificate Authority は、次の認証方式をサポートします。次の項で、その内容を説明します。

- OracleAS Single Sign-On 認証
- Secure Sockets Layer（SSL）を使用した証明書ベースの認証
- 手動による承認

OracleAS Single Sign-On 認証

OracleAS デフォルトのユーザー管理および認証プラットフォームは、Single Sign-On および Oracle Internet Directory から構成されます。Oracle Application Server Certificate Authority は、Oracle Internet Directory を証明書の格納リポジトリとして使用します。このアーキテクチャでは、証明書を集中管理できるため、証明書のプロビジョニングおよび失効が簡素化されます。

OracleAS Certificate Authority を OracleAS Single Sign-On Server および Oracle Internet Directory と統合することによって、これらに依存するアプリケーション用に、透過的な証明書プロビジョニング・メカニズムが提供されます。Oracle Internet Directory でプロビジョニングされ、OracleAS Single Sign-On に対して認証されたユーザーは、OracleAS Certificate Authority にデジタル証明書をリクエストできます。OracleAS Single Sign-On では、「SSO 統合を介した簡易プロビジョニング」で説明しているとおりに OracleAS Certificate Authority が構成されている場合、「証明書の取得」ポップアップ・ページが表示され、この操作が容易になります。このユーザーは、ユーザー名 / パスワードまたは既存の SSL 証明書（あるいはその両方）を使用して認証できます。「証明書のリクエスト」ボタンをクリックするだけで、証明書はすぐに Oracle Internet Directory で自動的にプロビジョニングされます。

この方式では、OracleAS Single Sign-On の機能を活用してユーザーが識別され、Oracle Internet Directory のデータを使用して、証明書リクエストの必要なフィールドに必要事項が入力されます。同様に、Oracle 認証局の管理者または証明書の所有者は、リアルタイムで証明書を失効させることができます。その場合、証明書は Oracle Internet Directory から自動的に削除されます。その後は、失効した証明書を OracleAS Single Sign-On 認証に使用しようとしても失敗します。

詳細は、付録 E「SSO での SSL および PKI の有効化」を参照してください。

Secure Sockets Layer（SSL）を使用した証明書ベースの認証

Oracle Application Server Certificate Authority は、証明書ベースの認証をサポートするため、ユーザーは、以前から持っていて失効になっていない X.509 v3 証明書によって、HTTPS 経由で OracleAS Certificate Authority により認証されます。この方式でユーザーを認証した場合、OracleAS Certificate Authority は、SSL や署名などの目的で、新しい証明書を遅延なく自動的に発行できます。

手動による承認

組織のセキュリティ・ポリシーでは、自動処理で証明書を発行するかわりに、手動で証明書リクエストを承認するように指示できます。この操作を選択すると、認可および認証に従来型の手動モードが使用され、Single Sign-On モードと SSL モードはオフになります。OracleAS Certificate Authority は、このような認可処理を適用して、リクエストを行ったユーザーの識別情報を手動で検証するように、管理者またはセキュリティ担当者に要求できます。

手動で認証を認可する場合、OracleAS Certificate Authority に受入れ可能な証明書リクエストには、すべての CA に必要な基本入力フィールドを使用します。この手動処理では、ユーザーが、名前、電子メール・アドレス、場所などの個人情報の入力が求められます。（ユーザーは、オプションとして、ドメイン・コンポーネントなどの詳細な DN 属性を指定することで、証明書リクエストをカスタマイズできます。）手動方式は、OracleAS Single Sign-On 認証や Secure Socket Layer 認証より複雑です。ただし、この方式では、既存の証明書を表示したり、保存またはインストールする追加オプションを使用できます。サーバーおよび下位 CA でも、この手動処理を実行して証明書をリクエストできます。

階層的な認証局のサポート

OracleAS Certificate Authority は、認証局の階層をサポートします。階層的な PKI では、セキュリティ・ドメインのルート CA は、最終的にすべてのユーザーによって信頼される、唯一の基点となる CA です。その識別情報は、信頼できるパスの先頭に使用されます。

OracleAS Certificate Authority は、ルート CA として動作できます。また、別の CA の証明書を検証して下位 CA を作成することもできます。そのかわりに、下位のインストール環境の署名および SSL 証明書は、別にインストールした OracleAS Certificate Authority など、規格準拠の認証局からも取得できます。この下位 CA は、さらに下位レベルの CA に対しても証明書を発行できます。各認可レベルの証明書は上位レベルの CA によって署名されているため、ユーザーは、認証局のパスを信頼できる認可レベルまたはルート CA までトレースすることによって、証明連鎖を検証できます。

別々の認証局からの下位 CA 証明書の取得は、PKI インフラストラクチャがすでに整備されている場合に有効です。階層的な CA のサポートは、地理的に分散している組織で有効です。

関連項目： 付録 B「CA の階層の設定」

階層的な CA の使用には、コストおよび安全性の面でも重要な利点があります。この場合、通常の操作は下位 CA に担当させ、ルート CA は特別に保護できます。こうした保護には、高度にセキュアな場所でのオフライン化も含まれます。この方法であれば、オンラインの下位 CA が危殆化した場合でも、それを失効させ、新しい下位 CA を作成して置換することができます。それ以前のすべての操作では、発行済の証明書を引き続き使用できます。ただし、ルート CA が危殆化した場合は、まったく新しいインフラストラクチャを構築して、元のルート CA に依存するアプリケーションをすべて更新する必要があります。

3

OracleAS Certificate Authority 配置ガイドライン

この章は、CA の配置に関する問題の理解と、スムーズで効率的な配置に必要な情報の収集に役立ちます。これらの問題に対処するためには、整合性の取れた証明書の作成、保護、送信および保証に関する適切な理解が要求されます。この章では、主要な機能が説明されており、証明書のセキュリティに関するサイトの要件を満たす OracleAS Certificate Authority の配置計画を作成できます。内容は、次のとおりです。

認証局設定のロードマップ

Oracle Application Server Certificate Authority は信頼できるエンティティであり、デジタル証明書を使用するための安全なインフラストラクチャとなります。証明書は次のように様々な場合に使用されます。

- Web サーバー用 SSL 暗号化および認証を使用した E-Commerce の保護
- ユーザー認証
- 電子メールの保護
- ドキュメントへのデジタル署名

前述またはその他のアプリケーション用に OracleAS Certificate Authority を配置する管理者は、これがサイトのデジタル取引で信頼できるエンティティとして使用されるよう配置および管理する必要があります。

次の事項に関する正確な知識が必要です。

- OracleAS PKI のコンポーネント、および OracleAS Certificate Authority の各機能

  この問題に対する詳細な処置に関しては、第 1 章「公開鍵インフラストラクチャと OracleAS」を参照してください。

  OracleAS Certificate Authority は Oracle Identity Management インフラストラクチャのコンポーネントであり、このインフラストラクチャの機能を活用します。たとえば、OracleAS Certificate Authority が発行した証明書は Oracle Internet Directory で公開されます。Oracle Application Server Single Sign-On で認証されたユーザーは、PKI に関する予備知識がなくても、何の困難もなく証明書を取得できます。Oracle Identity Management インフラストラクチャに関する詳細は、第 2 章「ID 管理および OracleAS Certificate Authority の機能」を参照してください。

- 証明書を必要とするユーザーおよびサーバー数、およびその使用先のアプリケーション

  次にあげるようなエンド・ユーザーの要求を特定するためには、完全な調査が必要です。何人のユーザー、および何台のサーバーが証明書を必要とするか。どのようなタイプの証明書が必要か。証明書のリクエストおよび使用時にはどのようなガイドラインが必要か。ユーザー証明書およびサーバー証明書の適切な有効期限はどのくらいか。予想される需要増加も可能であれば考慮します。

  前述およびその他の証明書設計上の問題の詳細は、「証明書の要件およびポリシー」を参照してください。

- サイトの機能要求に対して最適な配置トポロジ

  所属する組織独自のニーズを考慮し、次のような質問に答える必要があります。外部 CA とのどのような信頼関係が必要か。認証局は集中型にすべきか、それとも分散型にすべきか。ファイアウォールの外に置くべきコンポーネントはあるか。インストールする CA は組織構造の発展および変化をサポートしているか。

  CA インフラストラクチャの設計に関する問題は「OracleAS Certificate Authority アーキテクチャの計画」を参照してください。ネットワークおよびアーキテクチャに関する問題は「配置に際しての考慮事項および基本シナリオ」を参照してください。

- セキュリティ要件

  PKI の中心コンポーネントとなる認証局は、安全な施設に設置する必要があります。サーバー、ストレージ・デバイスおよび関連するコンポーネントの設置場所を決定する必要があります。CA のコンポーネントに対する不正アクセスを防止し、有資格担当者のみが操作および管理できるようにするため、適切な保護手段を検討してください。

- 可用性要件

  認証局は戦略的な役割を担うことになるため、悪意のある攻撃、コンポーネントの障害および自然災害から保護するためのフェイルオーバー機能を組み込むことが重要です。詳細は「高可用性配置オプション」を参照してください。

- テストおよびパイロット配置フェーズ

  これらのフェーズは、CA の動作および処理の効率、有効性およびセキュリティを検証するために重要です。

- 研修

  研修は、エンド・ユーザー、ヘルプデスク担当者、セキュリティ担当者および管理者のニーズに合うように調整する必要があります。

- まとめ

  PKI および OracleAS Certificate Authority に関する適切な理解を得て、実装に関する次の重大な問題に対処するための準備ができました。

  – PKI ポリシー、証明書ポリシーおよび認証局運用規定（CPS）の定義。次を参照してください。

    * 証明書の要件およびポリシー

    * 付録 D「拡張領域」

  – 認証局階層の設計。設計では、階層の最適なレベル数を検討する必要があります。レベル数はユーザー数などの要素に依存します。次を参照してください。

    * CA 信頼階層

    * 信頼のレベル

  – 必要な CA インスタンスをインストールおよび構成することによる CA 階層の実装。

  – 侵入の企ておよび攻撃に対する、CA 階層のコンポーネントの保護。次を参照してください。

    * CA の保護

    * 『Oracle Application Server セキュリティ・ガイド』。Oracle Application Server セキュリティ・アーキテクチャの詳細が記載されています。

  – 証明書失効リスト（CRL）による証明書検証の設定。「証明書失効リスト（CRL）の更新」を参照してください。

  – CA 管理者、Web 管理者、エンド・ユーザーなど、CA と対話する実体に対するロールおよび責任の定義。

  – サイトの可用性要件の定義およびその要件を満たすための環境の構成。「高可用性配置オプション」を参照してください。

  – 外部企業との信頼関係の構築（必要に応じて）。図 3-5 を参照してください。

  組織が OracleAS Certificate Authority 配置を計画および実装する場合に必要な計画データのリスト、およびそれらの決定点の例を示したユースケースは、「実装チェックリスト」および「ユースケース : MyPKIsite.com」を参照してください。

証明書の要件およびポリシー

所属組織の証明書要件を効率的に満たすように OracleAS Certificate Authority を配置するには、次のコンポーネントを計画する必要があります。

- 証明書の要件およびプロパティの定義
- 証明書のポリシーおよび手順の定義
- CRL ポリシーの定義
- アラートおよび通知の定義

証明書の要件およびプロパティの定義

初期計画段階では、ユーザー・ベースの要件を考慮に入れて、証明書のライフ・サイクルおよび使用する証明書のタイプを検討する必要があります。この項では次について説明します。

- 証明書のプロビジョニング
- 証明書タイプ
- 証明書のプロパティ
- 証明書の更新および失効
- CA 証明書の配布

証明書のプロビジョニング

OracleAS Certificate Authority では、ユーザー証明書を手動または自動のどちらかのモードでプロビジョニングできます。

- 手動プロビジョニングは従来からある伝統的な証明書プロビジョニングの方法であり、CA 管理者は証明書リクエストを手動で認可することになります。OracleAS Certificate Authority は、Single Sign-on および SSL プロビジョニング・モードを無効にして、手動認可プロセスを強制できます。

  これは、証明書を慎重に発行する必要があり、リクエストの数が多くない組織で適切な方法です。

- OracleAS Certificate Authority における自動プロビジョニングでは、選択肢として、OracleAS Single Sign-On または SSL の機構が用意されています。

  – OracleAS Single Sign-On で認証済であり、Oracle Internet Directory でプロビジョニングされるユーザーは、ユーザー名 / パスワードの入力かまたはそれとは異なる方式である構成済シングル・サインオン認証を使用して OracleAS Certificate Authority に対してデジタル証明書をリクエストできます。

  – 既存の証明書を使用すればユーザーを SSL で認証でき、OracleAS Certificate Authority で新しい証明書を自動的に発行できます。

  手動と比較した場合の自動プロビジョニングの利点としては、コストの削減、時間の短縮などがあげられます。自動プロビジョニングが推奨されるのは、ID 管理ソリューションまたは集中管理ディレクトリを配置済の場合です。

詳細は、第 2 章の「証明書の自動または手動プロビジョニング」を参照してください。

証明書タイプ

表 3-1 で示しているように、証明書タイプは、組織内におけるユーザーのロール、証明書がクライアントまたはサーバーのどちらで使用されるか、および対象とするアプリケーションによって異なります。

表 3-1 証明書タイプ

クライアントの証明書	サーバーの証明書	説明
認証	認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。）
暗号化	暗号化	電子ドキュメントおよび電子メールの暗号化および復号化を可能にします。
署名	署名	電子メールを含む電子ドキュメントに、S/MIME を使用した検証可能な署名を提供します。また、これらの改ざんを防ぎます。
コード署名	コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します。また、これらの改ざんを防ぎます。
NA	CA 署名	下位 CA 証明書をリクエストできるようにします。

OracleAS Certificate Authority は最初の 3 タイプの証明書を組み合せて、複数の要求を満たす証明書を作成できます。

- 認証、暗号化
- 認証、署名
- 署名、暗号化
- 認証、署名、暗号化

OracleAS Certificate Authority は各ユーザーに発行する証明書の数を制限しません。したがって、複数の証明書を発行することが可能です。ただし、通常は、組織内におけるユーザーの役割と一致した証明書をタスクごとに一度に 1 つ発行すれば十分です。

たとえば、ユーザー A には認証の証明書を 1 つ、暗号化の証明書を 1 つ発行し、ユーザー B には認証の証明書のみを発行できます。（このようにするには、UniqueCertificateConstraint ポリシー・ルールを使用します。第 6 章を参照。）別の例をあげると、企業ポータルへのセキュアなログインを行うアプリケーションを最初に検討する場合は、使用できるのは認証のみです。ただし、セキュアな電子メールなどのアプリケーションを追加する可能性がある場合は、署名および暗号化の証明書も追加が必要になります。

証明書の一般的用途

使用する証明書タイプを決定する場合は、証明書の適用範囲を考慮に入れる必要があります。

- SSL 対応サーバーに対する証明書

  証明書の最も一般的な用途は、Web サーバーのセキュアな SSL 通信を可能にすることです。クライアント・ブラウザによる Web サーバー ID の検証、およびブラウザと Web サーバーの間のデータ・フローのセキュアな暗号化が可能になります。このタイプの用途では、スケーラビリティは重要な問題ではありません。すべての認可は手動で行われ、ディレクトリ・サービスとの統合も不要です。

サーバーを SSL 認証対応にする際には、次の点に注意してください。

- サーバーを認証するためのサーバーの CA 証明書をクライアントが取得する方法。オプションには、OracleAS Certificate Authority を認証済 CA の下位 CA にすることや、CA 証明書を配布することがあります。
- 通信者双方で証明書失効がないかをテストする方法。ブラウザおよびサーバーが、証明書失効リストがないかどうかを認識する必要があります。

詳細は次を参照してください。

- CA 信頼階層
- ブラウザへの CRL のインストール
- ディスクへのバイナリ CRL または BASE64 CRL の保存

■ 証明書によるユーザー認証

これは証明書の一般的な適用対象であり、次のように様々な形態があります。

- OracleAS Single Sign-On 上での PKI 証明書の有効化による企業ポータルへのログオン
- 証明書を使用した仮想プライベートネットワーク（VPN）へのアクセス

ユーザー・コミュニティで証明書を使用するには、証明書の取得方法、および必要に応じた証明書の更新または失効方法についてユーザーに周知する必要があります。秘密鍵が紛失または危殆化した場合の証明書所有者の責任について、よく説明してください。鍵の格納にスマートカードを使用する場合は、研修を行い、カードが常に適切に使用され、保護されるようにしてください。

証明書に関するユーザーのタスクの詳細は、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」を参照してください。

エンド・ユーザーは通常、自分の証明書を取得および管理できます。これに対して管理者は、証明書のプロビジョニングおよびライフ・サイクル管理全般について責任を持ちます。更新された CRL を管理して不正使用を防ぐ、従業員が組織を離れた後にユーザー証明書を失効させる、などが管理者の仕事になります。

■ 証明書を使用した電子メールおよびドキュメントの署名

PKI 証明書を使用してドキュメントにデジタル署名することによって、データ・セキュリティおよびドキュメントの作成元の認証という 2 つの利点がもたらされます。電子メール・クライアントへの証明書の取得方法に関する詳細は、付録 G「OracleAS Certificate Authority での S/MIME」を参照してください。

■ 証明書を使用した電子メールの暗号化

Outlook または Netscape メール・クライアントなどの S/MIME アプリケーションでは、証明書を使用して、電子メール・メッセージに署名し、そのメッセージを暗号化できます。OracleAS Certificate Authority を使用すると、署名および暗号化にそれぞれ独立した証明書を使用できます。また前述したように、これらの機能を実現するのに同一の証明書を使用することもできます。

メッセージの暗号化機能を実装するサイトでは、ユーザーは必ず鍵を適切な手段でバックアップする必要があります。これは暗号化キーを紛失するとメールを復号化できなくなるためです。

証明書のプロパティ

OracleAS Certificate Authority の管理者は、日次ベースで証明書およびエンド・ユーザー（個人またはサーバー・エンティテイ）からの証明書リクエストを検証し、証明書の更新および失効を行い、証明書リクエストを認可または拒否します。これらの職務を実行するため、管理者は次のような各種証明書構成オプションについて理解しておく必要があります。

- 証明書の名前付け
- 証明書鍵サイズ
- 証明書の有効期間
- サポートされる拡張機能
- スマートカードのサポート

注意： 構成は、OracleAS Certificate Authority のインストール時に決定される場合もあり、また証明書のリクエスト時に決定される場合もあります。一部の変更はルート証明書の再生成によってのみ有効になります。

証明書構成の詳細は、第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」を参照してください。

証明書の名前付け 識別名（DN）はグローバルで一意な識別子であり、個人または個人以外のエンティティの ID を表します。これは各証明書に含まれます。OracleAS Certificate Authority は DN の使用については明確に推奨していませんが、これはいくつかの一般的なルールに準拠する必要があるためです。

注意： 自動プロビジョニングを使用している場合は、ディレクトリは配置済のため、この作業は不要です。

- DC コンポーネントおよび EMAIL コンポーネントでは、印刷可能な ASCII 文字のみを使用する必要があります。これはサイトでマルチバイト・キャラクタ・セットを使用している場合も同様です。
- CA の DN は、組織を明確に識別する一意なものである必要があります。
- CA の DN に対しては、サーバー・ホスト名を CN として指定できません。
- DN には必ず組織名が含まれている必要があります。含まれていない場合はブラウザが混乱する可能性があります。
- SSL サーバー証明書では、DN の cn コンポーネントには（CA、Web サーバーなどの）ホスト名を指定します。

Oracle Internet Directory でプロビジョニング済のユーザーには、この名前が Oracle Internet Directory プロビジョニングの一部として割当済です。OracleAS Certificate Authority はシングル・サインオン・ユーザーの DN 情報を Oracle Internet Directory から取得して使用します。

注意： DN は、証明書ポリシーを構成する際に中心的に使用する要素です。詳細は、表 6-9「条件の属性」を参照してください。また、DN の構成ガイドラインの続きは、第 6 章を参照してください。

証明書鍵サイズ 一般的には、証明書にはできるだけ強度の高い鍵サイズを使用します（サイズが大きくなるとパフォーマンスが低下するので、パフォーマンスを考慮してサイズを決定します）。

- 512 ビットの鍵サイズは、暗号化レベルが最も低くなります。
- 1024 ビットの鍵サイズは、暗号化レベルがこれより高くなり、広く使用されています。
- 高いセキュリティが要求される場合は、サイズが 2048 ビット以上の鍵を使用します。

推奨される鍵サイズを次にあげます。

意図されている使用方法	推奨される鍵サイズ（バイト）	コメント
CA 証明書	2048 以上	インストール時に定義
サーバーの証明書	1024 以上	
ユーザー証明書	1024 以上	最小鍵サイズ 1024 ビットを推奨

証明書の有効期間 エンド・ユーザーが有効期間を指定するのは、証明書を手動でリクエストする場合ですが、管理者は、ValidityRule ポリシー・ルールを使用して証明書の実際の有効期間を管理できます。このルールを使用して、管理者は最短有効期間（デフォルトでは 90 日）、最長有効期間（デフォルトでは 3650 日）、デフォルト値、証明書タイプ、ルール適用先 DN を指定できます。

（OracleAS Single Sign-On Server 認証または SSL 認証による）自動証明書リクエストでは、ValidityRule により有効期間が自動設定されます。

> **関連項目：** 詳細は第 6 章の「ValidityRule」を参照してください。

サポートされる拡張機能 拡張機能を使用すると、組織は、証明書をカスタマイズして、標準の証明書フィールドが許可していない情報を提供できるようになります。拡張機能には重要および非重要の 2 つのタイプがあります。

- 証明書を使用するシステム（アプリケーション）は、認識できない重要拡張機能に遭遇した場合、または値が意図されている使用方法に合わない場合は、証明書を拒否します。
- 非重要拡張機能は可能な場合には実行されますが、認識されない場合または意図されている使用方法と合わない場合にはアプリケーションが無視される可能性があります。

OracleAS Certificate Authority は、IETF X.509 V3 証明書フォーマットに準拠し、複数の標準証明書拡張機能をサポートしています。これにより、目的のアプリケーションに適した証明書を構成し、サブジェクトについての追加情報を指定できます。デフォルトでは、OracleAS Certificate Authority は次をサポートします。

- 選択した証明書タイプをベースにして自動構成される鍵の使用方法。
- 選択した証明書タイプをベースにして自動構成される拡張された鍵の使用方法。
- CRL の場所を証明書に埋め込むことができる CRL 配布。この拡張機能は、依存するアプリケーションによって CRL の検索に使用されます。
- サブジェクト代替名（subjectAltName）拡張機能。管理者は、SSO 認証ユーザーに発行する証明書に、事前定義済の代替名識別子が表示されるようにシステムを構成できます。この拡張機能には通常、電子メール・アドレスや代替ユーザー名があり、電子メールの暗号化、署名または他アプリケーションでの使用が可能になります。

  この拡張機能は必須として指定できます。この場合、Oracle Internet Directory に代替名が見つからないと、証明書リクエストは拒否されます。

> **注意：** サブジェクト代替名拡張機能は手動認証ユーザーおよび SSO 証明書リクエストで使用できます。

詳細は次を参照してください。

- 付録 D「拡張領域」
- 第 5 章の「サブジェクト代替名拡張機能」

スマートカードのサポート エンド・ユーザーは、証明書のリクエスト時に暗号トークンまたはスマートカードのどちらに保存するかを指定できます。スマートカードは、セキュリティ向上のために取り外して別個に保管できます。OracleAS Certificate Authority は一般的なスマートカード・ベンダーをサポートしており、ハードウェアを使用してスマートカードと通信できます。

ユーザーはカードをリストから選択します。ユーザーのシステムに実際に装着されているカードのみがリストに表示されます。

証明書の更新および失効

使用中の証明書には有効期間があり、期限切れになった証明書は使用できません。OracleAS Certificate Authority 管理者は次を構成できます。

- 更新を許可するかどうか。
- 更新する証明書の有効期間。たとえば、最初の証明書の有効期間を 5 年、更新する証明書の有効期間を 2 年のみ、などと設定できます。
- 証明書を更新できる、満了日前後の時間枠。これを指定しない場合、デフォルトの時間枠は満了日の前後 10 日間になります。

証明書の更新担当者は証明書タイプに応じて異なります。

- 手動認可でリクエストされた証明書（手動証明書）は管理者が更新する必要があります。
- OracleAS Single Sign-On Server 認証または SSL 認証を使用して発行された証明書（自動証明書）は、証明書の所有者または管理者が更新できます。

関連項目： 証明書更新に関する追加情報は次の項を参照してください。

- 第 4 章の「証明書の更新」
- 第 6 章の「ValidityRule」（管理者による有効期限の構成用）
- 第 8 章の「証明書の検索、更新および失効」

証明書を失効できるのは、その証明書のユーザーまたは OracleAS Certificate Authority の管理者です。次のような場合は通常、管理者が失効処理を行います。

- 証明書の所有者が証明書を使用する権利または必要性がなくなった場合（役職変更があった場合など）
- 証明書所有者の秘密鍵（署名鍵または復号化鍵）が危殆化した場合

関連項目： 証明書失効に関する追加情報は次の項を参照してください。

- 第 4 章の「証明書の失効」
- 第 8 章の「証明書の検索、更新および失効」

CA 証明書の配布

OracleAS Certificate Authority を使用するためには、CA 証明書に信頼性があることが必要です。CA 証明書に信頼性が要求されるのは、ユーザーが発行元認証局から受け取る証明書を信頼できるようにするため、または認証局から発行された証明書を持つサーバーを信頼できるようにするためです。

ユーザーが OracleAS Certificate Authority とこのような信頼関係を確立するための CA 証明書配布方法としては、次のようなものがあります。

1. ユーザーは証明書をブラウザに明示的にインストールできます。第 8 章の「OracleAS Certificate Authority が信頼されるブラウザの構成」および「CA 証明書のインストール」を参照してください。
2. CA 証明書はインストールしてマシンの基本イメージの一部とすることができます。CA をインストール済のブラウザを使用するエンド・ユーザーは、CA 証明書を自動的に取得します。
3. パッチ適用およびセキュリティ更新のプッシュ・メカニズムに従うと、これらの変更がクライアント・マシンにプッシュされます。
4. CA 証明書は SMS 経由でプッシュできます。
5. グループ・ポリシーを使用すると、Windows ドメイン全体で CA 証明書を信頼させることができます。

証明書のポリシーおよび手順の定義

認証局運用規定（CPS）は、証明書サービス提供時に認証局が従うポリシーおよび手順を記述したものです。次が含まれます。

- 証明書タイプおよび使用方法
- 証明書のライフ・サイクル管理
- エンド・ユーザー制御の手順およびポリシー
- 証明書の技術的仕様

CPS には、次のような情報が含まれています（ただし、これのみではありません）。

- 一般情報
  - 法律上の注意事項、義務および損害賠償
  - 公開鍵インフラストラクチャを使用する際に必要な知識
- 認証および識別に関する問題
  - CA 名、サーバー名および DNS アドレスなどによる、CA の明確な識別
  - CA に対するユーザーの認証方法
  - 意図されている証明書の用途
  - CA によって実装される証明書ポリシーおよび発行される証明書のタイプ
  - 証明書の発行、更新および失効のポリシー、手順およびプロセス
- 物理的および個人的なセキュリティ
  - CA の物理的、ネットワーク上および手順上のセキュリティ
  - 証明書の登録および更新に関する要件
  - 証明書ユーザーに関する要件（ユーザーが秘密鍵を紛失したかまたは危殆化させた場合のユーザーによる処置を含む）
  - 証明書の失効ポリシー（退職およびユーザー権限の不正使用などの証明書失効条件を含む）
  - 証明書の使用についての警告

- 技術的セキュリティ要件
  - 暗号化アルゴリズム、暗号サービス・プロバイダ（CSP）および CA 証明書で使用する鍵の長さ
  - 公開鍵 / 秘密鍵ペアの最小長
  - 証明書の鍵の強度およびセキュリティ関連事項
  - CA 証明書の存続期間
  - 証明書のライフ・サイクルの詳細
  - 使用されている規格またはプロトコル
  - 秘密鍵の管理要件（保管先をローカル・ディスク、スマートカードまたは他のハードウェア・デバイスのいずれにするかなど）
- 証明書プロファイル
  - 証明書タイプおよび使用方法
  - サポートおよび使用される拡張機能とその制限
  - 証明書の制限
- CRL ポリシー
  - CRL 配布ポイントの設定先
  - CRL の公開頻度

認証局運用規定を追加または変更するには、`$ORACLE_HOME/j2ee/oca/applications/ocaapp/oca/helpsets/oca_practice_stmt/ocaadmin_cs_practicestmt.html` ファイルを編集します。

OracleAS Certificate Authority を再起動した後、各ページに表示される「運用規定」アイコンをクリックすると、「運用規定」ページに変更内容が表示されます。

注意： この手順に従って OracleAS Certificate Authority 管理者が作成する認証局運用規定は、外国語には対応していません。したがって、認証局運用規定は、クライアントのロケールには関係なく、編集する管理者のロケールに翻訳されます。すなわち、クライアント側では作成に使用された言語でのみ表示できます。

CRL ポリシーの定義

証明書を使用するには、失効した証明書が認証で使用されないように、信頼できる環境下のアプリケーションで証明書のステータスを検証できる必要があります。OracleAS Certificate Authority が失効した証明書のリストとして定期的に作成、保存している証明書失効リスト（CRL）を、この目的で使用できます。

注意： OracleAS Certificate Authority の証明書失効リストは、CRL 配布ポイント（CRLDP）拡張機能を持つ Oracle Internet Directory、およびデータベースに配置されます。失効した証明書の不正使用を防ぐため、アプリケーションで証明書から CRLDP を抽出し、CRL を Oracle Internet Directory から取得するために使用します。他方、エンド・ユーザーは、ブラウザから OracleAS Certificate Authority をクリックして、CRL をデータベースから取得します。

CRL には 2 種類の生成方法があります。

- デフォルトでは、OracleAS Certificate Authority は CRL を自動生成します。管理者は、CRL 生成に失敗したときの電子メール通知用の通知パラメータを構成できます。
- 管理者は更新対象 CRL を手動で生成することもできます。

CRL 管理の推奨事項をいくつか記載します。

- CRL の適切な有効期間、および新しい CRL を生成する（失効日前後の）期間を指定する必要があります。後者の期間は有効期間より短く設定するようにし、またアプリケーションが最新の CRL を取得する猶予期間ができるようにします。これにより、次の CRL の生成から CRL の有効期間終了までの時間の余裕ができるので、CRL が無効になって証明書認証エラーとなるのを回避できます。
- 自動 CRL 生成の構成上位証明書を失効させる必要がある場合など、特殊なケースに備えて手動 CRL 生成を可能にしておきます。

関連項目：

- CRL 生成に関する詳細は、第 4 章の「証明書失効リスト（CRL）の更新」を参照してください。
- `ldapsearch` を使用した CRL へのプログラム的なアクセスの詳細は、第 4 章の「証明書失効リストの取得」を参照してください。
- OracleAS Certificate Authority のユーザー・ホームページから CRL を取得する方法は、第 8 章の「証明書失効リスト（CRL）の使用」を参照してください。

アラートおよび通知の定義

OracleAS Certificate Authority には、主要なイベントの発生時にエンド・ユーザーおよび管理者にアラートを出したり、管理ジョブのスケジュールに使用したりするためのパラメータが用意されています。

- 保留証明書リクエストの数が指定したしきい値を超えたときにアラートを受信する。
- 指定した時間隔で CRL を自動的に生成するジョブをスケジュールする。
- CRL の自動生成に失敗した場合、常にアラートを受信する。
- 証明書情報を Oracle Internet Directory と同期させるためのジョブをスケジュールする（これは Oracle Internet Directory が停止した場合に有効です。OracleAS Certificate Authority は、証明書をキューに入れておき、Oracle Internet Directory がリカバリすると Oracle Internet Directory と同期できるからです）。
- OracleAS Certificate Authority ユーザーに自動送信される電子メールをカスタマイズして、証明書の認可および拒否などの管理アクションがユーザーに通知されるようにする。

このトピックの詳細は、第 5 章の「「通知」サブタブ」を参照してください。

OracleAS Certificate Authority アーキテクチャの計画

OracleAS Certificate Authority の実装を開始する前に、システム・アーキテクチャ上のいくつかの懸案について検討することが重要です。必要な信頼階層の種類、オフライン CA を構成するかどうかおよび OracleAS Certificate Authority インストールのセキュリティについて検討します。適切な計画を立てることによって、信頼できるスケーラブルな認証局を実装できます。

この項は次のトピックで構成されています。

- CA 信頼階層
- CA の保護

CA 信頼階層

CA 信頼階層では、セキュリティ・ドメインのルート CA は、最終的に組織の全ユーザーから信頼される基本 CA です。ルート CA は他の CA に対して証明書を発行し、下位 CA を作成できます。

下位 CA のインストールはいつでも行うことができます。また、証明書リクエストの作成およびファイルへの保存、ルート CA への証明書リクエストの送信ができます。認可された証明書は、下位 CA にインポートし、下位 CA 署名証明書として使用できます。下位 CA はさらにその下位レベルの CA に対して証明書を発行できます。

OracleAS Certificate Authority が完全にサポートしているこれらのテクニックを適切に使用すると、セキュアかつ高信頼性の効率的なデジタル通信手段が提供されるので、エンド・ユーザー（またはユーザーのかわりに処理を行うアプリケーション）が CA 証明書連鎖をルート CA（つまり、階層の当初の認証源）まで遡ってトレースできる、という信頼階層を構築できます。

オンライン CA とオフライン CA

最も単純なシナリオでは、組織全体で利用する認証局が 1 つ存在するのみです。この CA はルート CA、証明書発行者など複数の役割を担います。このシナリオは図 3-1 に図で示されています。

図 3-1 ルート CA

ただし、この構成は比較的小さなサイトであってもお薦めできません。セキュリティ、信頼性、可用性およびコスト削減の面で重要なメリットをもたらす、複数の CA からなる階層を構築することをお薦めします。たとえば、階層内の CA を、攻撃から重要な CA を保護するという特別な目的専用に使用できます。

図 3-2 にはルート CA の保護方法が示されています。これは地理的に離れた 2 つのサイトで構成される組織で使用されている、単純な認証局階層です。各サイトは下位 CA を使用します。2 つの下位 CA はオフラインのルート CA の下位 CA になります。下位 CA は両方ともオンライン状態であり、各サイトのエンド・ユーザーからの証明書リクエストを処理します。

図 3-2 単純な CA 階層

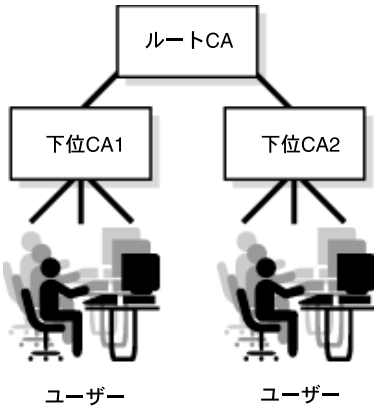
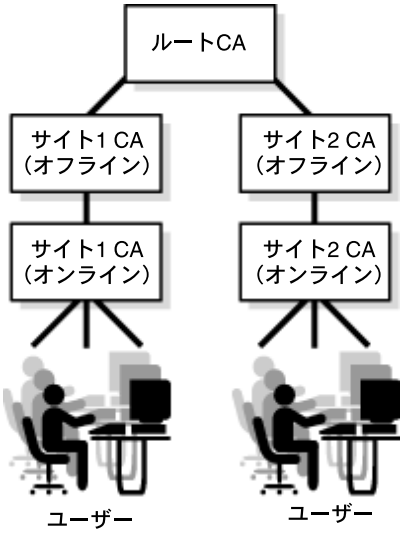


図 3-3 は先に示した同じ組織の認証局階層を拡張したものです。各サイトに 2 つの下位 CA があります。1 つの下位 CA はオンラインであり、証明書を発行する認証局として動作しています。それより上位にあるもう 1 つの下位 CA は、セキュリティ確保のためオフラインになっています。ルート CA の下位には、2 つの下位 CA ペアがあります。ルート CA 自体はオフラインです。

この構成では、証明書を発行する下位 CA がなんらかの理由で危殆化した場合、階層の上位にあるオフラインの下位 CA がその CA 証明書を失効させ、新しい下位 CA を作成して置き換えます。

図 3-3 2 レベルの下位 CA を持つ CA 階層



信頼階層の持つもう 1 つの利点は、独立した認証局を持つ会社または組織間で信頼関係を構築できることです。

図 3-4 では、会社 A および B が独立した CA を持っています。すなわち、会社 A はサード・パーティの CA を使用しており、会社 B は OracleAS Certificate Authority を使用しています。このシナリオでは、各 CA が独立しているため、組織間には信頼関係は確立されていません。

図 3-4 信頼関係がない複数の組織

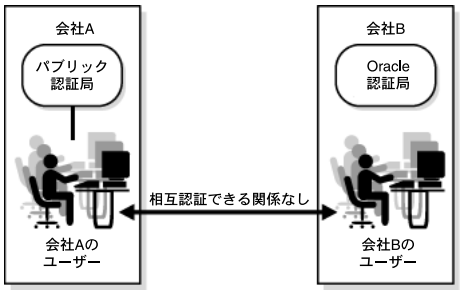
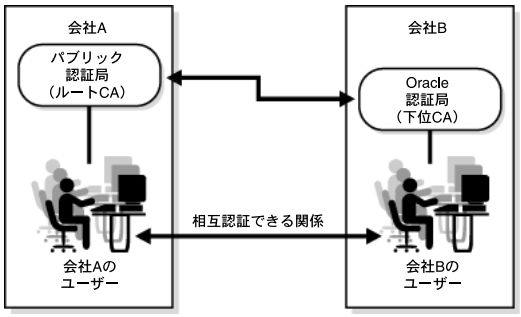


図 3-5 では、2 つの会社は、会社 B の認証局、OracleAS Certificate Authority を会社 A のサード・パーティ CA の下位 CA とすることにより、信頼関係を構築しています。2 つの会社のユーザーは、CA 間で構築された信頼階層をベースにしたセキュアな通信が互いに可能になります。

図 3-5 信頼階層で関連付けられた複数の組織



セキュリティおよび可用性の要件に応じて、その要件に適合する信頼階層を選択する必要があります。構成の詳細は、付録 B の「別の CA の下位 CA にするための OracleAS Certificate Authority インスタンスの構成」を参照してください。

CA の保護

CA インストール全体（特にルート CA）の保護は、最重要事項です。CA の再配置および証明書の再発行の作業を考慮すると、ルート CA の危殆化は中間 CA または証明書発行 CA の危殆化よりもコストがかかります。

ルート CA を保護するには、次の手順をお薦めします。

- 専用のマシンへの OracleAS Certificate Authority のインストール。
- 物理的に安全な位置にサーバーを設置することによる、侵入者からの攻撃に対する保護。
- 信頼できる管理者のみへのアクセスの制限。
- 管理者キー用のハードウェア・ストレージの使用。
- さらに保護を強化するためのルート CA（可能な場合は下位 CA も）のオフライン化。詳細は「オンライン CA とオフライン CA」を参照してください。
- 証明書発行などの日々の作業で使用するオンラインの下位 CA のセットアップ。
- ホストの強化および Oracle Application Server のインストールのための標準ガイドラインの順守。
- 不要なサービスの削除とホスト・マシンにアクセスするユーザーの制限。

詳細は図 3-3「2 レベルの下位 CA を持つ CA 階層」および関連する説明を参照してください。

配置に際しての考慮事項および基本シナリオ

サイトの要件に応じて、OracleAS Certificate Authority の配置方法を複数の中から選択できます。この項ではいくつかのシナリオを説明します。次のトピックで構成されます。

- OracleAS Certificate Authority に必要なコンポーネント
- デフォルトの配置
- 本番配置
- DMZ 配置
- 高可用性配置オプション

OracleAS Certificate Authority に必要なコンポーネント

OracleAS Certificate Authority を実行するには次のコンポーネントが必要です。

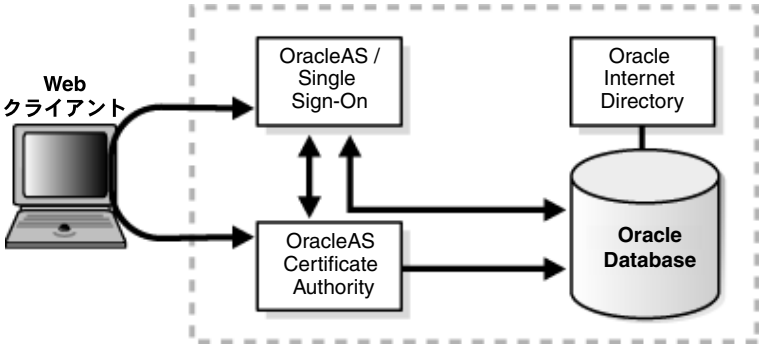
- Oracle HTTP Server（OHS）（OracleAS Certificate Authority と同じマシンにインストール）
- OracleAS Certificate Authority で使用する OC4J（OracleAS Certificate Authority と同じマシンにインストール）
- Infrastructure Metadata Repository
- Oracle Internet Directory
- Single Sign-On （オプション）

注意： OCA は、デフォルトの選択として自動的にインストールされるわけではありません。OCA をインストールするには、インストールの対象として明示的に選択する必要があります。

デフォルトの配置

デフォルトの配置では、これら必須のコンポーネントはすべて同じマシン上および同じ Oracle ホームにインストールされます（図 3-6 を参照）。この構成は、開発および非本番環境に適しており、インストール時に他の選択を行わない場合のデフォルトの構成です。

図 3-6 Oracle Application Server Certificate Authority のデフォルトのインストール

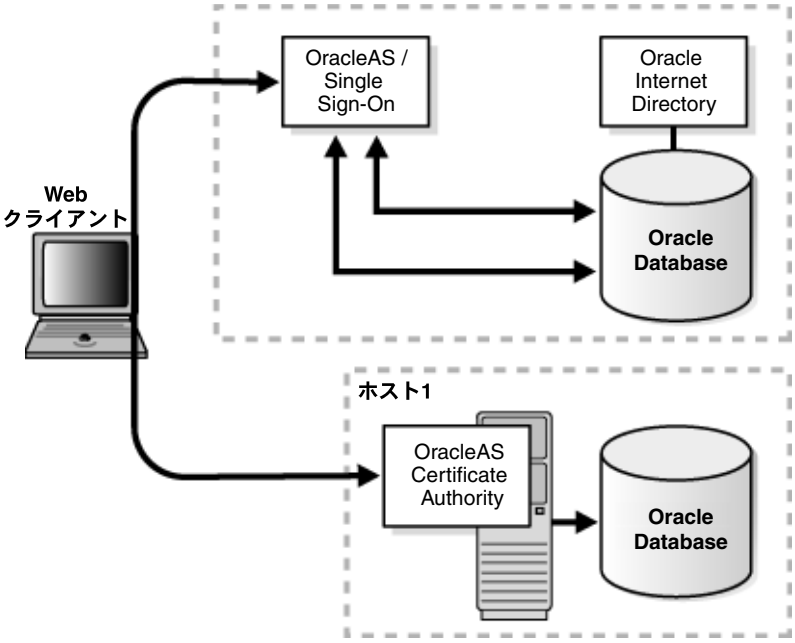


OracleAS Certificate Authority のこのデフォルトの配置構成のインストール手順は、Oracle Application Server のインストレーション・ガイドを参照してください。

本番配置

推奨される本番配置では、OHS、OC4J、OracleAS Certificate Authority および OracleAS Infrastructure Metadata Repository は、同じマシン上の同一の Oracle ホーム内に配置されます。OracleAS Single Sign-On および Oracle Internet Directory など、他のコンポーネントは、別の同一マシン上の同一の Oracle ホーム内に配置されます。このように物理的に分離することによって、OracleAS Certificate Authority を安全なロケーション内に保護することで、分離したそのロケーションのセキュリティを強化できます。OracleAS Certificate Authority は証明書の信頼連鎖の最上位にあるため、本番環境ではこれらの保護が必要になります（図 3-7 を参照）。同様に、OracleAS Certificate Authority のセキュリティ上の理由から、これらのコンポーネントの開始および停止にはリモート管理機能を使用しないことをお薦めします。

図 3-7 OracleAS Certificate Authority の推奨される本番インストール

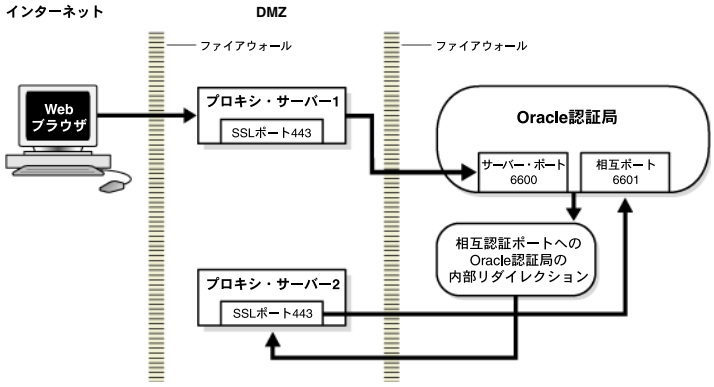


この推奨される配置構成のインストール手順は、Oracle Application Server のインストレーション・ガイドの 6.20 項を参照してください。

DMZ 配置

DMZ の構成では、OracleAS Certificate Authority は外部ネットワークに接します。DMZ は、たとえば、インターネット・ユーザーからこの認証局へのアクセスを許可する場合に構成する必要があります。

図 3-8 OracleAS Certificate AuthorityDMZ のインストール



このシナリオ（図 3-8 を参照）では、DMZ 内にプロキシ・サーバーを構成して OracleAS Certificate Authority へのリクエストを処理させます。

OracleAS Certificate Authority の実行には 2 つのポートが必要です。外部のユーザーは OracleAS Certificate Authority にポート 443（SSL ユーザー。推奨設定）またはポート 80（非 SSL ユーザー）経由でアクセスします。すべてのリクエストは、サーバー認証のため、たとえばポート 6600（または使用可能な範囲の別のポート）を使用してプロキシ・サーバー 1 経由でルーティングされます。リクエストが相互認証を要求する場合（そしてその場合のみ）、リクエストは、OracleAS Certificate Authority 内部でプロキシ・サーバー 2 にリダイレクトされ、さ

らにプロキシ・サーバー 2 からたとえばポート 6601 によって相互認証にルーティングされます。

プロキシ・サーバーでポート 443 のみが使用可能な場合は、2 つのプロキシ・サーバーを使用する必要があります。また、OracleAS Certificate Authority リポジトリのプロキシ・サーバー情報を更新することも必要です。

このシナリオの設定に関する詳細は、付録 F「保護された OracleAS Certificate Authority への外部アクセス」を参照してください。

注意： これは OracleAS Certificate Authority の配置ではお薦めしていないトポロジです。ただし、このトポロジを DMZ 内に配置することが必要になった場合は、次の手順を実行することをお薦めします。

1. 外部ユーザー用の下位 CA を用意する。
2. OracleAS Certificate Authority に対しては手動認証のみを許可し、管理者が証明書を発行する。

高可用性配置オプション

認証局配置を保護する高可用性オプションには大きく分けて 2 種類があります。

- 人為的なミス、ならびにマシンおよびメディアの障害は、個別データ・センターでのローカルな高可用性保護で解決できます。
- 自然災害やリージョンのネットワーク障害は、地理的に分散した障害時リカバリ用配置で対処できます。

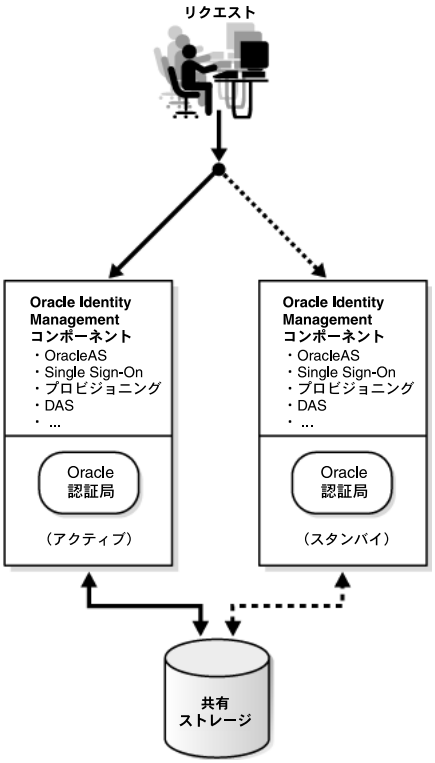
この項では、OracleAS Certificate Authority 配置の高可用性オプションを 3 つ示します。ローカル保護のためのコールド・フェイルオーバー・クラスタ、障害時リカバリ・ソリューション、両方のタイプの障害から保護するためのこれらの保護手段の組合せです。

関連資料： ここで示されている配置オプションは、『Oracle Application Server 高可用性ガイド』で詳しく説明されています。

コールド・フェイルオーバー・クラスタ

図 3-9 で示されているコールド・フェイルオーバー・クラスタは、アクティブ / パッシブ・モードで動作し、ローカルでの高可用性を実現します。アクティブ・ノードは、OracleAS Certificate Authority および他の Oracle Identity Management コンポーネントを含む Oracle Application Server インスタンスを実行するものです。パッシブ・ノードは、アクティブ・ノードが停止するまでは起動されず、アクティブ・ノードと同様に、OracleAS Certificate Authority および関連するコンポーネントで構成される Oracle Application Server インスタンスのホストとなります。このクラスタ環境では、OracleAS Infrastructure の *ORACLE_HOME* は共有ストレージ・システム上にあります。

図 3-9 コールド・フェイルオーバー・クラスタ



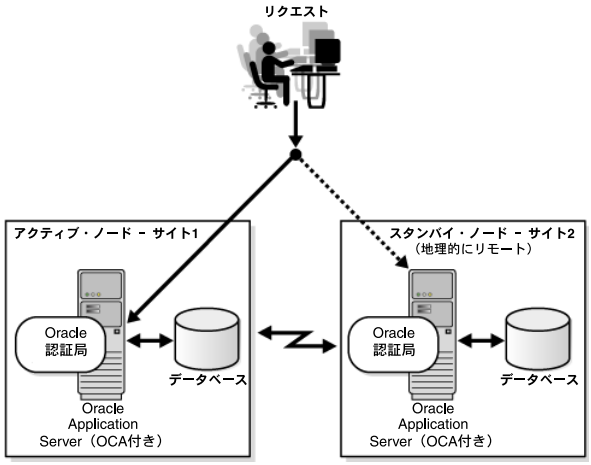
名前が示しているように、アクティブ・ノードは証明書リクエストを能動的（アクティブ）に処理します。これに対して、パッシブ・ノードはアクティブ・ノードでコンポーネントに障害が発生するまでは動作しません。障害が発生すると、ユーザー・リクエストはこの 2 次ノードにリダイレクトされます。この 2 次ノードはファイル・システムをマウントし、共有ストレージに対する制御を引き継ぎ、処理を続行します。

注意： この仮想ホストはネットワークから参照可能なホスト名を提供し、そのホスト名はロード・バランサまたはハードウェア・クラスタによって 1 台以上の物理マシンにマッピングされます。仮想ホストはスタンドアロンにすることも、また、OracleAs Infrastructure 内に設定することもできます。

障害時リカバリ

図 3-10 はアクティブ・ノードとスタンバイ・ノードを使用した障害時リカバリ構成です。この 2 種類のノードは同期されていますが地理的には分散しています。各ノードは、OracleAS Certificate Authority および他の Oracle Identity Management コンポーネントを含む Oracle Application Server インスタンスのホストとなります。各インスタンスは、独自の ORACLE_HOME 上で動作します。このシナリオでは、アクティブなサイトが本番サイトであり、クライアント・リクエストをアクティブに処理しています。一方、スタンバイ・サイトには、本番サイトのアプリケーション（OracleAS Certificate Authority を含む）およびデータ・リポジトリがミラー化されています。サイトの同期は Oracle Data Guard によって提供されます。OracleAS Guard によって、必要な構成ファイルのバックアップおよびリストアに必要な手順が提供されます。

図 3-10 障害時リカバリ



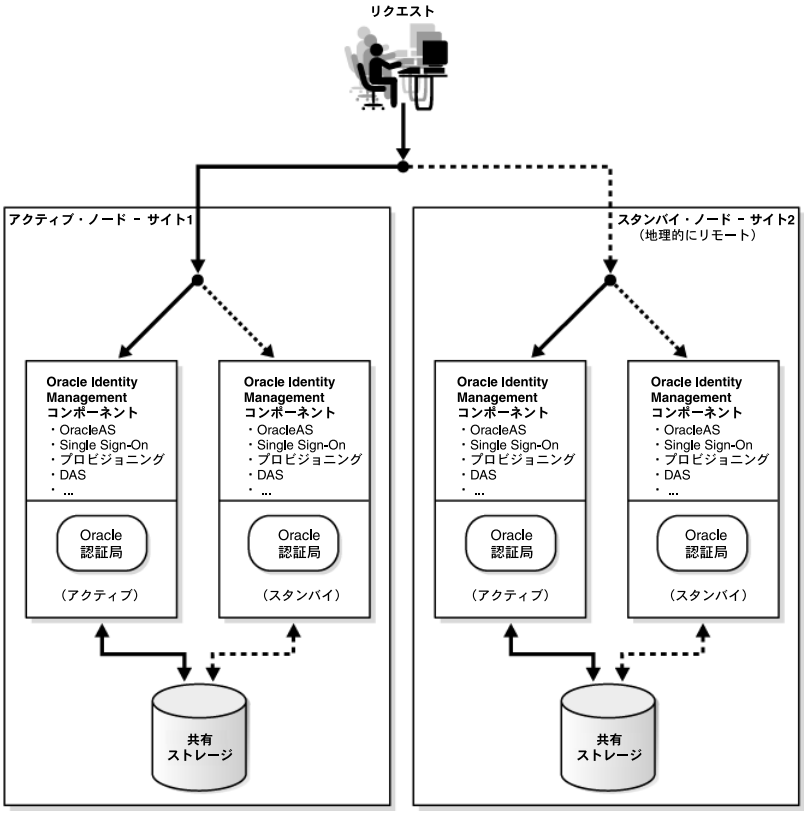
アクティブ・サイトで壊滅的障害が発生した場合は、OracleAS Guard がフェイルオーバー・タスクを実行し、スタンバイ・サイトをアクティブ・モードに切り替えます。ユーザー・リクエストは切り替えられたノードにリダイレクトされ、処理が続行されます。

コールド・フェイルオーバー・クラスタおよび障害時リカバリ

この構成は「コールド・フェイルオーバー・クラスタ」および「障害時リカバリ」の両ソリューションを 1 つのシステムとして統合し、サイト全体に影響する壊滅的障害からの保護および個々の問題からの保護を可能にします。

図 3-11 で示されているこの構成では、アクティブ・サイトおよびスタンバイ・サイトがそれぞれ独立したコールド・フェイルオーバー・クラスタ・サービスを提供しています。各サイトの仮想ホストは、サイト内のローカルな障害を処理するため、リクエストをパッシブな Oracle Application Server インスタンスにリダイレクトします。グローバルな仮想ホストは、壊滅的障害が発生したときにスタンバイ・サイトにリクエストをフェイルオーバーして、上位レベルでのロード・バランシングを提供します。

図 3-11 コールド・フェイルオーバー・クラスタと障害時リカバリの統合



OracleAS Certificate Authority 実装およびユースケース

この項では、OracleAS Certificate Authority の配置にとって重要となる特性および決定ポイントの定義に役立つ、認証局実装のベースになる論理的および物理的コンセプトを説明します。

実装チェックリスト

次のチェックリストは OracleAS Certificate Authority の配置に必要な、主要な計画項目をまとめたものであり、配置を開始する際には必ずこのリストを使用します。

表 3-2 実装チェックリスト

計画項目	推奨（提案）値	注意
証明書ポリシーおよび実装の詳細		
CA DN		
CA 証明書の存続期間		デフォルト値は表 4-4 を参照。
CA Wallet タイプ		署名、SSL または S/MIME を入力。
CA Wallet の鍵サイズ		デフォルト値は表 4-4 を参照。
CA 証明書の有効期間		デフォルト値は表 4-4 を参照。
下位 CA 証明書の有効期間		
総ユーザー数		
認証証明書の数		
暗号化証明書の数		
署名証明書の数		
コード署名証明書の数		
新規証明書の有効期間		デフォルト値およびその他の詳細に関しては第 8 章の「「ユーザー証明書」タブ」を参照。
更新された証明書の有効期間		デフォルト値は表 6-7 を参照。
更新の時間枠		証明書を更新できるようにする、満了日前後の日数を入力。デフォルト値は表 6-7 を参照。
RSA 公開 / 秘密鍵の長さ		デフォルト値およびその他の詳細に関しては第 8 章の「「ユーザー証明書」タブ」を参照。
同一の名前に対して同一用途の複数証明書を許可		これは UniqueCertificateConstraint ポリシー。
CRL 配布ポイント		詳細は次を参照。 ■ 証明書失効リスト（CRL）の更新 ■ 証明書失効リスト（CRL）の使用
CRL 公開頻度		
証明書の保管方法		ファイルまたはトークンなどの保管要件を入力。
アーキテクチャ		
CA 階層のレベル数		
ルート CA の役割		オンライン / オフライン、および証明書を発行するかどうかを入力。

表 3-2 実装チェックリスト（続き）

計画項目	推奨（提案）値	注意
下位 CA タイプ		オンラインかオフラインかを入力。
下位 CA の追加データ		
配置		
OracleAS Certificate Authority 用に独立したリポジトリを用意		
DMZ の配置		
高可用性		
コールド・フェイルオーバー		
障害時リカバリ		

ユースケース : MyPKIsite.com

このユースケースは MyPKIsite.com における架空の配置シナリオです。OracleAS Portal および OracleAS Certificate Authority を使用した、PKI 対応企業への配置を説明しています。タスクを網羅的に列挙せずに、OracleAS Certificate Authority の配置時に考慮する必要がある主要な要素を特定しています。

シナリオ

MyPKIsite.com は実在しないオンラインのトラベル・サービスです。旅行者は、このサイトを使用して、旅程の作成、予約、2 つの大陸のトラベル・アドバイザーとのセキュアなメッセージ交換ができます。同社は、PKI 証明書を使用したセキュアな Web サイトを構築する必要があります。

> **注意 :** MyPKIsite.com は説明の目的のみで使用される架空の会社です。

次に、会社およびそのセキュリティ要件に関する基本的事実を示します。

- アメリカとイギリスにオフィスがあります。
- アメリカとイギリスの従業員の他に、顧客および取引先を含む外部ユーザーをサポートする必要があります。
- 会社のセキュリティ要件は次のようなものです。
  - サーバーの SSL 認証を有効にする。
  - 認証用のクライアント証明書を使用した、アプリケーションへのシングル・サインオンを実装できる。
  - S/MIME を使用して、電子メールの署名および暗号化ができる。

管理者の役割

現在のニーズに基づいて、1 人の従業員に OracleAS Certificate Authority 管理者および Web 管理者の職務を割り当てることに決定しました。

MyPKIsite.com の CA 階層

実装チームは次にあげる基本的な 2 レベルの階層を実装することを決定しました。

1. オフラインのルート CA
2. 4 つの発行下位 CA
   - アメリカには 2 つの発行下位 CA を置き、1 つを内部ユーザー用、もう 1 つを外部ユーザー用として使用します。これらの発行下位 CA はルート CA の下位 CA です。
   - イギリスには 2 つの発行下位 CA を置き、1 つを内部ユーザー用、もう 1 つを外部ユーザー用として使用します。これらの発行下位 CA はルート CA の下位 CA です。

代替階層オプション

計画中、チームは次の 3 レベル階層で構成される代替オプションも検討しました。

1. オフラインのルート CA
2. オフラインの下位 CA（1 つをアメリカ、1 つをイギリスに置く）
3. 4 つの発行下位 CA
   - アメリカには 2 つの発行下位 CA を置き、1 つを内部ユーザー用、もう 1 つを外部ユーザー用として使用します。これらの発行下位 CA はアメリカのオフライン下位 CA の下位 CA です。
   - イギリスには 2 つの発行下位 CA を置き、1 つを内部ユーザー用、もう 1 つを外部ユーザー用として使用します。これらの発行下位 CA はイギリスのオフライン下位 CA の下位 CA です。

後になって、セキュリティ上の問題で保護を強化する必要が生じた場合は、このオプションの要件を満たす下位 CA レイヤーを追加することによって 3 レベル階層に移行できます。

Oracle Internet Directory のユーザー・エントリ

ユーザーの証明書を含むユーザー・エントリを Oracle Internet Directory に追加する必要があります。証明書をリクエストするユーザーが多いため、Oracle Internet Directory のバルク・ローディング・ツールを使用してディレクトリのユーザー・エントリを定義および更新することを決定しました。

`bulkload` は LDIF ファイルを使用して、Oracle Internet Directory に大量のエントリをロードおよび追加します。`bulkload` は次のような手順を実行します。

- 入力ファイルのスキーマおよびデータ整合性のチェック
- LDIF データの、ローダーで使用する適切なフォーマットへの変換
- データのロードおよび索引付け

参考のため、チームがユーザー・エントリ作成時に他にも使用できるツールをあげておきます。

- 委任管理サービス
- コマンドライン・ツール
- Oracle Directory Manager

各コンポーネント・インスタンス

サイトは共有の Oracle Internet Directory および Oracle Application Server Single Sign-On コンポーネントを使用します。

> **注意：** Oracle Internet Directory の複数の物理インスタンスを、マルチマスター・モードでセットアップできます（1 つはアメリカに、1 つはイギリスに設置）。

チームは 1 つのルート CA と 4 つの発行下位 CA、合計 5 インスタンスの OracleAS Certificate Authority をインストールする必要があります。各インスタンスは独自のメタデータ・リポジトリを独自のマシン上に持ちます。

MyPKIsite.com の証明書要件

証明書のプロビジョニングおよび使用方法に関して、チームは次のように決定しました。

プロビジョニング

エンド・ユーザーはシングル・サインオン証明書を使用してサイトで認証されます。サーバーの手動証明書が発行されます。

> **関連項目：** 詳細は「証明書のプロビジョニング」を参照してください。

証明書の存続期間

MyPKIsite.com が発行する証明書の有効期間は次のようになっています。

表 3-3 証明書の存続期間

証明書	初期有効期間	更新の時間枠	更新の有効期間
ユーザー	2 年	満了日の前後 30 日	1 年
サーバー	10 年	満了日の前後 30 日	5 年

一度証明書が無効になると更新されません。（ただし、会社の慣例として、満了後 30 日間は証明書の更新を許可しています。これを実装するために、管理者は更新の猶予期間を提供するパラメータを設定できます。ただし、満了から 30 日経過しても更新しなかった場合は更新できなくなります。）

証明書鍵サイズ

MyPKIsite.com では次の鍵サイズを使用します。

- ユーザー証明書には 1024 バイト
- サーバー証明書には 1024 バイト
- CA 証明書には 2048 バイト

証明書の使用方法

サイトでは 2 種類の証明書を使用します。

- 認証および署名に 1 つの証明書
- 暗号化にもう 1 つの証明書

1 人のユーザーが認証および署名の証明書を 1 つ、暗号化の証明書を 1 つのみ持つようにするため、UniqueCertificateConstraint が適用されます。

> **関連項目：** 詳細は「証明書タイプ」を参照してください。

証明書の配布

チームは、ルート CA 証明書および下位 CA 証明書の配布に関しては次の 2 つのオプションを検討しました。

1. ユーザーはこれらの証明書を手動でインポートします。
2. 証明書を各ユーザーのマシンの基本イメージに含めます。

基本イメージの再構築を不要にするため、ユーザーが手動で証明書をインポートする方法を採用しました。ユーザーは OracleAS Certificate Authority のホームページから CA 証明書をダウンロードし、ブラウザに組み込みます。

証明書の保管

MyPKIsite.com のユーザーは、デスクトップ・マシンにスマートカードを装備します。秘密鍵はスマートカードに保管します。

失効

次の標準失効理由に該当する場合、証明書は失効します。

- 鍵危殆化
- 所属変更
- CA 危殆化
- 証明書保留
- 運用停止
- CRL からの削除
- 破棄

CRL の決定および公開

CRL は 3 日ごとに午前零時に公開します。CRL の有効期間は 7 日間に設定します。

ルート CA の CRL は 6 か月有効です。

> **関連項目：** 詳細は第 4 章の「証明書失効リスト（CRL）の更新」を参照してください。

セキュリティ関連の考慮事項

認証局保護のためにチームは次の基準を採用しました。

- OracleAS Certificate Authority のルート・インスタンス、および関連のメタデータ・リポジトリを専用のマシンにインストール
- 物理的に安全な場所での CA サーバーの保持
- 発行に使用しない CA はすべてオフライン化（概要は「MyPKIsite.com の CA 階層」を参照）

高可用性関連の考慮事項

すべてのユーザー・リクエストを処理するため、4 つの証明書発行下位 CA には高可用性が要求されます。これらの CA をサポートするため、Dataguard によるコールド・フェイルオーバー・クラスタおよび障害時リカバリの統合が使用されます。

オフラインおよびオンラインのすべての CA インスタンスのバックアップを、定常的にスケジュールする必要があります。

MyPKIsite.com の詳細な実装チェックリスト

MyPKIsite.com の実装チームは、OracleAS Certificate Authority インストールの設計および運用について最終決定を下しました。表 3-4 のチェックリストはその最終決定をまとめたものであり、各種設定タスクの実行方法の説明に対するリンクも含まれています。

これは表 3-2 のチェックリストからの派生ではあるものの、より詳細になっており、具体的な OracleAS Certificate Authority タスクおよび機能について記載しています。

注意： ユーザー証明書リクエストなど、リスト内の項目の一部は、緊急のタスクというよりは将来必要となる作業です。これらはリストを完全なものにするためにここに記載してあります。

表 3-4 MyPKIsite.com の実装チェックリスト

タスク / 項目	値	関連資料
コンポーネントのインストール	-	プラットフォーム固有の Oracle Application Server インストール・ガイド
ユーザー・エントリの作成	-	『Oracle Internet Directory 管理者ガイド』
下位 CA のセットアップ	4 つの下位 CA インスタンス	付録 B「CA の階層の設定」、特に「別の CA の下位 CA にするための OracleAS Certificate Authority インスタンスの構成」
パスワードの設定	-	付録 A の「権限付きパスワードの変更」
管理者証明書のリクエスト	-	第 4 章の「管理者の証明書のリクエスト」
サーバー証明書のリクエスト	-	第 8 章の「「サーバー / 下位 CA 証明書」タブ」
ユーザー証明書（更新）のリクエスト	-	■ 第 8 章の「エンド・ユーザー用のタブおよび処理」 ■ 付録 I の「「証明書リクエスト」フォーム」
期限切れの証明書を失効するか	はい（猶予期間あり。「証明書更新時間枠の設定」を参照。）	第 6 章の「RevocationConstraints」
証明書更新時間枠の設定	満了日の前後 30 日	第 6 章の「RenewalRequestConstraint」
一意のユーザー証明書	はい	第 6 章の「UniqueCertificateConstraint」
証明書有効期間の設定	サーバー証明書は 10 年 ユーザー証明書は 2 年	第 6 章の「ValidityRule」
証明書鍵サイズの設定	2048（CA） 1024（サーバー、ユーザー）	第 6 章の「RSAKeyConstraints」
鍵保管方法の設定	スマートカード	-
電子メール・パラメータの定義	-	第 5 章の「メール詳細」および「電子メールのテンプレート」
通知の設定	日次	第 5 章の「アラート」
CRL 生成頻度の構成	7 日ごと	第 5 章の「スケジュールされたジョブ」
高可用性		第 7 章の「OracleAS Certificate Authority および高可用性機能」
CPS の記述		■ 「CRL ポリシーの定義」 ■ 「証明書のポリシーおよび手順の定義」

4

OracleAS Certificate Authority Administration および証明書の管理の概要

Oracle Application Server Certificate Authority の Web ベースの管理インタフェースは、次に示す 3 つの大きな事項を対象としています。各事項は、ホームページのタブからアクセスできます。

- 証明書に関する事項の管理 : 証明書の発行、失効または更新のリクエスト、すでに発行されている証明書、および証明書失効リスト（CRL）
- 構成に関する事項の管理 : OracleAS Certificate Authority のアクション用パラメータおよび証明書のセキュリティ・ポリシーを実装するためのパラメータ
- OracleAS Certificate Authority アクティビティのログの表示

この章では、前述の 1 つ目の事項（証明書の管理）について説明します。他の 2 つの事項は、第 5 章「Oracle Application Server Certificate Authority の構成」を参照してください。

管理操作には、付録 A「コマンドライン管理」で説明するコマンドライン・インタフェースが必要な場合があります。これらの操作のうち 2 つは、OracleAS Certificate Authority の起動および停止です。詳細は、後の項を参照してください。管理者の証明書のリクエストまたは置換とともに説明します。

エンド・ユーザーが OracleAS Certificate Authority と対話する際には、Web ベースの独立したインタフェースを使用できます。このインタフェースにより、個人的な証明書関連の操作を実行可能なフォームが提供されます。詳細は、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」を参照してください。

この章の内容は、次のとおりです。

Oracle Application Server Certificate Authority の起動および停止

セキュリティ上の理由から、OracleAS Certificate Authority の起動および停止の操作は、コマンドライン・ツール ocactl を使用しないと実行できません。このツールには管理者のパスワードが必要です。これらの操作の使用例は、「管理者の証明書の置換」を参照してください。このツールの詳細は、付録 A「コマンドライン管理」を参照してください。

OracleAS Certificate Authority を起動するには、次の 5 つのコンポーネントが動作中または使用可能である必要があります。

- Infrastructure Metadata Repository
- Oracle Internet Directory
- OracleAS Single Sign-On（オプション）
- Oracle HTTP Server（OHS）
- OracleAS Certificate Authority 用の OC4J

OracleAS Certificate Authority が、他のインフラストラクチャ・コンポーネントとは異なる $ORACLE_HOME にインストールされている場合は、リポジトリの後に、OHS および OracleAS Certificate Authority 用の OC4J を別々に起動する必要があります。このコマンドは次のように、OracleAS Certificate Authority の $ORACLE_HOME で使用します。

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

OracleAS Certificate Authority を含むすべてのインフラストラクチャ・コンポーネントが 1 つの $ORACLE_HOME にインストールされている場合は、前述の第 4.3 項に記述したように、OHS および OC4J はすでに起動されています。

OracleAS Certificate Authority を起動、停止または再起動するには、対応するコマンドを次のコマンド行に入力します。

1. OracleAS Certificate Authority を停止するには、次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   ```

2. OracleAS Certificate Authority を起動するには、次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl start
   ```

3. OracleAS Certificate Authority を再起動するには、手順 1 に記載されている停止コマンド、次に手順 2 に記載されている起動コマンドを使用します。

4. Oracle Application Server Certificate Authority のステータスを取得するには、次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl status
   ```

注意： OracleAS Certificate Authority では、同じ Oracle Process Manager and Notification Server（OPMN）による複数のプロセスの管理はサポートしていません。OPMN 内に複数の OracleAS Certificate Authority プロセスが存在する場合、OracleAS Certificate Authority を起動または停止すると、予測不可能な問題が発生することがあります。たとえば、この場合に単に ocactl start と入力しても、OracleAS Certificate Authority は正しく起動されません。

管理者の証明書のリクエスト

Web ベースのインタフェースで Oracle Application Server Certificate Authority の管理オプションおよび制御を使用するには、管理者の証明書が必要です。インストール中に管理者のパスワードを作成しておくと、この証明書は簡単に取得できます。他のタスクを実行する前に、最初にこの証明書を取得する必要があります。

他のシステムでは、管理者の PKI 証明書のリクエスト、取得およびインストールに、コマンドライン、フロッピー・ディスクおよびカット・アンド・ペースト操作が必要です。

ただし、OracleAS Certificate Authority を使用すると、この処理は単純で簡単になります。

ユーザー認証用に管理者の証明書をリクエストするには、OracleAS Certificate Authority を初めて起動した後に表示されるフォームに、必要事項を入力して送信するだけです。管理者として使用するコンピュータから OracleAS Certificate Authority にアクセスしている必要があります。「認証管理」タブをクリックすると、「ようこそ」ページが表示された後、識別情報データの入力を求めるフォームが表示されます。

このフォームには、一般名、組織およびインストール中に作成した OracleAS Certificate Authority 管理者のパスワードを入力する必要があります。電子メール・アドレス、組織単位、地域、州および国など、他の DN 情報も指定できます。

証明書の鍵のサイズ（デフォルトは 2048）および有効期間（デフォルトは 1 年）を選択できます。

管理者の証明書が発行されたら、それをブラウザにインストールします。ブラウザでこの証明書を使用すると、管理および構成インタフェースで OracleAS Certificate Authority の機能にアクセスして、証明書のリクエスト、証明書の失効または更新、およびポリシーの管理ができます。

この簡単な処理（簡単なリクエスト・フォームに必要事項を記入して実行する簡単なインストール）は、PKI 証明書の取得や使用のために（OracleAS Certificate Authority より前で）実行する必要のあったすべての操作のかわりに実行できます。

証明書をリクエストするには、次の手順を実行します。

1. OracleAS Certificate Authority の管理インタフェースにアクセスします。

   Web ブラウザを起動して、インストールの最後に表示されたとおりに URL および管理サーバーのポート番号を入力します。たとえば、次のように入力します。

   ```
   https://Oracle_HTTP_host:ssl_port/oca/admin
   ```

   `Oracle_HTTP_host` は、OracleAS Certificate Authority のインストール先ホストです。`ssl_port` は、`$ORACLE_HOME/install/portlist.ini` の Oracle Certificate Authority SSL Server Authentication port に記載されています。Windows の場合、このパスは `%ORACLE_HOME¥install¥portlist.ini` です。

   > **注意：** インストール後にポートが変更されると、`portlist.ini` に最新情報が保管されません。この場合は、Oracle Enterprise Manager Control にサインオンし、OracleAS Certificate Authority がインストールされているインスタンスをクリックします。次に、「ポート」リンクをクリックし、「タイプ」列で OracleAS Certificate Authority Server Authentication（SSL）というエントリを探して、その横の「使用中のポート」という見出しの列に表示されている数値を使用します。

   画面に、「ようこそ」ページが表示されます。このページに表示されたリンクをクリックすると、管理者の証明書をリクエストするためのフォームが表示されます。

2. このフォームに DN、パスワードおよび証明書情報を入力して、証明書をリクエストします。

   - **DN 情報 :** 管理者を証明書の認証済所有者として識別する識別名（DN）用のデータを入力します。

表 4-1 管理者の証明書の DN 情報

フィールド名	入力情報
一般名	証明書に記載する名前
電子メール・アドレス	管理者の電子メール・アドレス
組織単位	管理者が属する組織単位または部門の名前
組織	管理者が属する企業または組織の名前
場所	管理者の所在地
都道府県	管理者が所在する都道府県
国	管理者の国を表す 2 文字のコード

注意 :

DN の DC コンポーネントおよび EMAIL コンポーネントでは、印刷可能な（ASCII）文字のみを使用する必要があります。

この制限は、マルチバイト・キャラクタ・セットを使用するロケールでも、識別名の DC コンポーネントおよび EMAIL コンポーネントには ASCII 文字を使用する必要があるという意味です。

   - **Certificate Authority 管理者パスワード :** 証明書および構成の管理を実行できるのは、OracleAS Certificate Authority 管理者のみです。OracleAS Certificate Authority のインストール時に「OCA 管理者パスワードの指定」画面で入力したパスワードをこのセクションに入力すると、この管理者が初期認証されます。

     パスワードには、次の制限が適用されます。

     – 先頭文字には、データベースのキャラクタ・セットに含まれるアルファベットを使用します。
     – 8 文字以上の長さにする必要があります。
     – アルファベットとアルファベット以外の文字（数値または特殊文字）を、それぞれ 1 文字以上使用します。
     – ASCII キャラクタ・セットに含まれる文字のみを使用します。
     – Oracle の予約語は使用できません。
     – データベースのキャラクタ・セットに含まれる英数字のみを使用します。必要に応じて、アンダースコア（_）、ドル記号（$）または番号記号（#）を使用できますが、オラクル社では、$ と # の使用は避けるよう強くお薦めします。

     したがって、インストール時に選択する OracleAS Certificate Authority 管理者のパスワードは、これらの制限に従う必要があります。

パスワードの複雑さを検証する Oracle のルーチン（PL/SQL スクリプト UTLPWDMG.SQL によって指定）をデータベースで使用する場合は、パスワードは次の要件（またはそのスクリプトに追加する要件）も満たす必要があります。

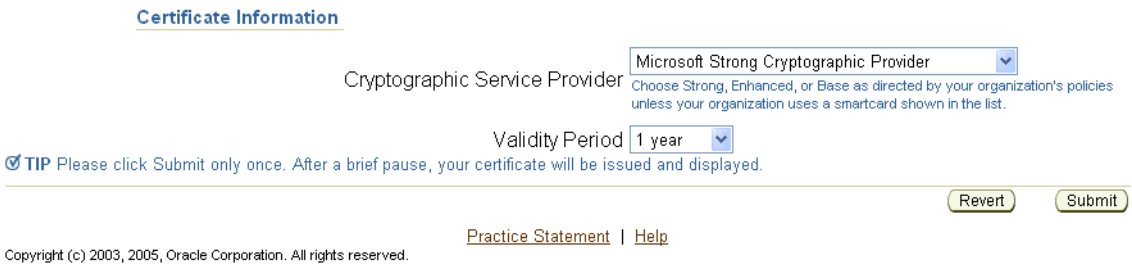
- 4 文字以上の長さにする必要があります。
- ユーザー名と同じものは使用できません。
- アルファベット、数字および句読記号をそれぞれ 1 文字以上使用します。
- welcome、account、database、user など、単純明快な語は使用できません。
- 一度設定したパスワードを後から変更する場合は、元のパスワードを 3 文字以上変更する必要があります。

- **証明書情報 :** 新しい証明書の作成に必須の 2 つの要素は、証明書の鍵のサイズおよび有効期間（または満了日）です。フォームのこのセクションで、これらのパラメータを選択します。

  * **Netscape** の場合は、512、1024、2048 など、生成される鍵のペアのサイズ（ビット単位）を示す**「証明書鍵サイズ」**が表示されます。サイトに適したサイズを選択します。2048 ビットは OracleAS Certificate Authority のデフォルトで、高いセキュリティが実現します。高い数値を選択すると、パフォーマンスは低下しますが、セキュリティは向上します。

  * Internet Explorer の場合は、暗号化サービス用に選択可能なプロバイダを示す**「暗号サービス・プロバイダ」**が表示されます。鍵のサイズの標準的な選択肢は、512 ビット（Microsoft Basic Crypto Provider）、1024 ビット（Microsoft Enhanced Crypto Provider）および 2048 ビット（Microsoft Strong Cryptographic Provider）です。OracleAS Certificate Authority ではデフォルトで、Microsoft Strong Cryptographic Provider（選択可能な場合）、Microsoft Enhanced Crypto Provider（選択可能な場合）、Microsoft Basic Crypto Provider の順に選択されます。また、スマートカードを使用する場合の Gemplus など、その他の選択肢が表示される場合もあります。要件に応じて、サイズを選択します。

    フォームのこのセクションは、次のように表示されます。



    OracleAS Certificate Authority では、管理者の証明書に対して Microsoft Strong Cryptographic Provider を使用することをお薦めします。ただし、Gemplus や Schlumberger などのスマートカード・リーダーが使用可能な場合は、それらを使用してください。リーダーがインストールされていない場合に、スマートカード・サプライヤを選択するとエラーになります。

- **有効期間 :** 証明書の有効期間。標準的なデフォルト値である 1 年が表示されますが、目的に合った期間も選択できます。

3. 最初からやりなおす必要がある場合は、「回復」ボタンをクリックします。
4. 管理者の証明書に対するリクエストを送信するには、**「送信」**をクリックします。（ブラウザのセキュリティ・パスワードの指定が必要になる場合もあります。）
5. 鍵のペアの生成時には、ブラウザに表示される手順に従います。この処理は、選択した鍵のサイズおよびプロセッサ / メモリーの制限によって、数分かかる場合があります。

6. **「ブラウザへのインストール」**をクリックします。（ブラウザのセキュリティ・パスワードの指定が必要になる場合もあります。）

   指定した一般名にクライアント認証の証明書が格納されます。

   これで、OracleAS Certificate Authority の Web ベースのインタフェースを介して実行可能なタスクを、すべて実行できるようになりました（第 5 章「Oracle Application Server Certificate Authority の構成」を参照）。

7. **「管理ホーム」**をクリックして、OracleAS Certificate Authority の初期ページにアクセスします。

管理者の証明書の置換

管理者の証明書を置換する必要が発生する場合があります。その原因には、秘密鍵のパスワードの紛失、秘密鍵の危殆化または盗難、新しい人間への管理者ロールの付与などがあります。

管理者の証明書を置換するには、サーバーを停止し、現行の管理者証明書を失効させて、サーバーを再起動する必要があります。これらのタスクは、コマンドライン・ツール `ocactl` を使用して実行します。このツールには OracleAS Certificate Authority 管理者のパスワードが必要です。セキュリティ上の理由から、これらのコマンドはコマンドラインでのみ使用可能です。グラフィカル・ユーザー・インタフェース（GUI）では使用できません。

次に、管理者は、Oracle Application Server Certificate Authority の Web ページにナビゲートし、「Web 管理者登録」に表示されるフォームに必要事項を入力します（「管理者の証明書のリクエスト」のここまでの記述を参照）。

次に、3 つの関連コマンドライン・タスクを示します。

1. OracleAS Certificate Authority サーバーを停止するには、コマンドラインで次のコマンドを入力します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   ```

2. 管理者の証明書を失効させるには、次のコマンドを入力します。

   ```
   $ORACLE_HOME/oca/bin/ocactl revokecert -type WEBADMIN -reason REASON_CODE
   ```

   注意：次の（| で区切られた）いずれかの理由コードを選択できます。

   ```
   {KEY_COMPROMISE | CA_COMPROMISE | AFFILIATION_CHANGE | SUPERSEDED |
   CESSATION_OF_OPERATION | CERTIFICATE_HOLD | REMOVE_FROM_CRL | UNSPECIFIED}
   ```

3. 管理パスワードの変更もできます。詳細は、付録 A「コマンドライン管理」の「権限付きパスワードの変更」を参照してください。

4. コマンドラインで、次のいずれかのコマンドを入力して、OracleAS Certificate Authority のサービスを起動します。

   UNIX の場合：`$ORACLE_HOME/oca/bin/ocactl start`

   Windows の場合：`%ORACLE_HOME%¥oca¥bin¥ocactl start`

この時点で、「管理者の証明書のリクエスト」の手順に従って、管理者の証明書を取得し、すべての管理機能を使用可能にします。

OracleAS Certificate Authority 管理インタフェースの概要

管理タスクを実行するには、有効な管理者の証明書を所有している必要があります。最初のサインインを、管理者としてではなく一般ユーザーとして行うと、付録 C「OracleAS Certificate Authority のトラブルシューティング」の「基礎的な問題および警告」の項目、「証明書リクエストで鍵のペアが生成されない（Windows）。」で説明されているエラー・メッセージが表示される場合があります。

OracleAS Certificate Authority 管理インタフェースにアクセスするには、Web ブラウザを起動します。インストールの最後に表示されたとおりに、URL および管理サーバーのポート番号を入力します。

```
https://Oracle_HTTP_host:ssl_port/oca/admin
```

URL のホストおよびポート番号の詳細は、「管理者の証明書のリクエスト」の手順 1 を参照してください。

OracleAS Certificate Authority の起動コマンドを発行すると、次の図に示すように、3 つのサブタブが追加された OracleAS Certificate Authority のホームページが表示されます。

これらの 3 つのサブタブを使用して、証明書または認証局の構成を管理する特定のタスクを実行できます。

- 「「認証管理」タブ」については、この章で説明しています。
- 「「構成管理」タブ」（説明は第 5 章「Oracle Application Server Certificate Authority の構成」）
- 「「ログの表示」タブ」（説明は第 5 章）

「認証管理」タブ

「認証管理」タブには、証明書の保留リクエストがすべて表示されます。表示されるページは次のようになります。

管理者は、このページを使用して、この後の各項で説明するタスクを選択できます。

証明書の管理

Oracle Application Server Certificate Authority では、すべての証明書リクエストおよびそれらの現行ステータス（保留、拒否済または認証済）のマスター・リストが保持されます。「認証管理」タブをクリックすると、アクションの必要な証明書リクエスト（保留）がすべて表示されます。管理者には、このようなリクエストの承認または拒否、必要に応じて証明書の失効または更新、および証明書失効リスト（CRL）生成の管理を実行する役割があります。

これらのタスクを管理者として実行する場合は、証明書または証明書リクエストのマスター・リストを名前または番号で検索した後、特定の証明書または所定のリクエストを検証できます。

その後、次のタスクを実行できます。

- 個々の証明書リクエストの承認または拒否
- 発行された特定の証明書の失効（退職したユーザーが所有しているなどの理由で、証明書が危殆化されたか、適切でなくなっている場合）または有効期限前後の短期間での既存の証明書の更新

  関連項目： この更新期間の時間枠を指定できます。詳細は第 6 章「Oracle Application Server Certificate Authority でのポリシー管理」の、次の項を参照してください。

  - 「Oracle Application Server Certificate Authority の「ポリシー」サブタブ」の「製品に付属の証明書更新ポリシー」
  - 「ポリシー操作」の「編集」

次の項で、これらのすべての証明書管理タスクについて説明します。

- 証明書リクエストの承認または拒否
- 証明書の詳細の表示
- 証明書の失効
- 証明書の更新
- 単一の証明書リクエストまたは発行済証明書の表示
- 拡張検索の使用方法

証明書リクエストの承認または拒否

「認証管理」タブの開始画面には、証明書の保留リクエストすべてのリストが表示されます。証明書を認可または却下するには、それぞれの処理に対応する手順に従います。

証明書リクエストの承認方法

1. 隣のラジオ・ボタンをクリックして、目的の証明書リクエストを選択します。
2. 「詳細表示」をクリックします。
   「証明書リクエストの詳細」画面が表示され、選択した証明書の情報が示されます。リクエストを行ったユーザーの連絡先が表示されます。ユーザーに電子メールを送信するか、電話するなどして、組織で定めたユーザー認証手順に従う必要があります。
3. 有効期間を確認し、必要に応じて変更します。
4. 下位 CA 証明書を発行する場合は、(信頼できる認証局を表示する）デフォルトのパス長は 2 と表示されます（この値は、必要に応じて変更できます)。
5. 「承認」をクリックします。
   証明書リクエストが承認されたことを示すメッセージが表示されます。
   証明書リクエストの所有者が証明書をインストールできるように、その所有者に通知してください。

証明書リクエストの拒否方法

1. 隣のラジオ・ボタンをクリックして、目的の証明書リクエストを選択します。リクエストを行ったユーザーを確認できない場合または証明書のプロパティに誤りがある場合は、証明書リクエストを拒否する必要があります。
2. 「詳細表示」をクリックします。
   「証明書リクエストの詳細」画面が表示され、選択した証明書の情報が示されます。
3. 「拒否」をクリックします。
   選択した証明書リクエストが拒否されたことを示すメッセージが表示されます。リクエストを行ったユーザーに拒否を通知してください。

証明書の詳細の表示

「認証管理」タブで、証明書を選択して詳細を表示できます。

単一の証明書を選択する方法は、「単一の証明書リクエストまたは発行済証明書の表示」を参照してください。

証明書のリストを表示する方法は、「拡張検索の使用方法」を参照してください。

検索結果から、表示する証明書を選択して「詳細表示」をクリックします。「証明書」ページが表示され、証明書の詳細が示されます。(このページを使用して、選択した証明書の失効、更新またはインストールも実行できます。)

証明書の失効

管理者は、証明書を指定期間前に失効させることができます。次のいずれかの場合は、失効させる必要があります。

- 証明書の所有者がステータスを変更し、証明書を使用する権限を持たなくなった場合
- 証明書の所有者の秘密鍵が危殆化された場合

失効コードの完全なリストについては、「失効理由」を参照してください。

ターゲットの証明書を検索する方法は、4-12 ページの「単一の証明書リクエストまたは発行済証明書の表示」または 4-13 ページの「拡張検索の使用方法」に記載された手順を参照してください。正しい証明書を選択した後、「詳細表示」をクリックして詳細を表示するか、次の手順で証明書を失効させます。

1. 失効リクエストを送信するには、「失効」ボタンをクリックします。**失効確認**画面が表示されます。この画面で、「鍵危殆化」、「所属変更」、「CA 危殆化」、「証明書保留」、「運用停止」、「CRL から削除」、「破棄」または「未指定」の 8 つから、いずれかの失効理由を選択する必要があります。
2. その後、「取消」をクリックして証明書を有効にしておくか、「OK」をクリックして証明書を失効させることができます。

関連項目: OracleAS Single Sign-On または SSL の認証を使用しているエンド・ユーザーは、自分自身の証明書を失効させることもできます。詳細は、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「証明書の失効」を参照してください。

注意:

- 管理者およびルート CA の証明書は、Web ベースのインタフェースを介して失効させることはできません。失効は、`ocactl` コマンドライン・ツール以外ではできません。
- ルート CA 証明書の失効は、影響が大きい操作です。インストールした OracleAS Certificate Authority が機能しなくなり、すでに発行されている証明書が無効になります。この失効操作を実行するのは、「コマンドライン管理」の「ルート CA 証明書の失効」で説明するとおり、CA 鍵が危殆化された場合のみです。
- 管理者の証明書の失効が必要になるのは、鍵の危殆化または盗難、または新しい人間に管理者ロールが付与された場合などです。第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「OracleAS Certificate Authority Web 管理者証明書の失効」を参照してください。

失効理由

管理者は、次のいずれかの理由を指定して証明書を失効できます。

- affiliationChange: 組織と証明書の所有者との関係が終了しました。
- cACompromise: 証明書に署名した認証局の秘密鍵が危殆化されました。
- certificateHold: この時点で証明書が保留されました。（これは、一時的な失効状態であり、これ以降に証明書に異なるステータスを割り当てることができる唯一の理由コードです。異なるステータスとは、証明書を失効にせず使用する、または別の理由コードを使用して証明書を失効するのいずれかです。
- cessationOfOperation: 証明書が発行された組織が稼働を中止したため、CA の証明書をこのコードを使用して失効します。
- keyCompromise: この証明書の秘密鍵が危殆化されました。
- removeFromCRL: 証明書が certificateHold になりましたが、現在は失効になっていません。
- superseded: 既存の証明書のかわりに新しい証明書が発行されました。
- unspecified: 特定の理由コードを使用せずに証明書を失効しますが、証明書の失効理由がわかりにくいため、この失効理由の使用はお薦めしません。

証明書の更新

管理者は、ユーザーの証明書を中断することなく継続して使用できるように、期限切れ前後の 10 日間（デフォルトのポリシー）に更新できます。（管理者は、期限切れ前後の許容日数を変更できます。）期限切れの証明書は、満了日の前後に設定した許容日数中に更新できます。証明書が期限切れになり、この許容日数中に更新しなかった場合、その証明書は使用できなくなります。このため、新しい証明書リクエストを送信して承認を得ることによって置換する必要があります。

証明書を更新する場合、管理者は、証明書を選択し（表示および検索に関する項を参照）、「詳細表示」をクリックして「証明書」ページを表示した後、「更新」をクリックします。日付が、証明書の満了日の前後に設定された時間枠（デフォルトでは前後 10 日間）内の場合は、証明書を更新できます。時間枠外の場合は、設定した時間枠に関するエラー・メッセージが表示されます。

OracleAS Single Sign-On または SSL の認証済更新リクエストの場合は、ユーザーの証明書更新を制御するポリシーと同じポリシー（RenewalCertificateRequestConstraints）が自動的に適用されます。Oracle Application Server Certificate Authority で、エンド・エンティティからの更新リクエストが処理されると、このポリシーによって、更新された証明書に対して新しい有効期間が設定されます。

単一の証明書リクエストまたは発行済証明書の表示

Web ベースのユーザー・インタフェースの最初のページで、Oracle Application Server Certificate Authority 管理インタフェースを使用して、特定の証明書または証明書リクエストを表示できます。（指定した条件を満たす証明書またはリクエストのリストを生成する方法は、「拡張検索の使用方法」を参照。）

特定の証明書または証明書リクエストを検索するには、次の手順を実行します。

1. 「検索」プルダウン・メニューを使用します。
   - 証明書の保留リクエストをすべて表示するには、**「すべての保留中のリクエスト」**を選択します。
   - 発行済の特定の証明書を表示するには、「証明書」を選択します。
   - 特定の証明書リクエストを表示するには、**「証明書リクエスト」**を選択します。
   - 特定のリクエストの ID またはシリアル番号を検索するには、**「ID / シリアル番号」**を選択します。
   - 特定の一般名を検索するには、**「一般名」**を選択します。
2. 「検索」条件フィールドに、検索リクエストに適した値を入力します。
   - 「すべての保留中のリクエスト」には、値を指定する必要はありません。
   - 「ID/ シリアル番号」には、目的の証明書またはリクエストのシリアル番号またはリクエスト ID を入力します。
   - 「一般名」には、目的の一般名を入力します。
3. 「実行」をクリックします。（**「実行」**のかわりに **[Enter]** を押しても動作しません。）
   - 単一の証明書リクエストが正常に検索されると、その証明書リクエストを表す行が表示されます。「詳細表示」をクリックすると、リクエストに関する情報（連絡先、リクエストを行ったユーザー、有効期間など）が、「承認」および「拒否」のラベルが付いたボタンとともに表示されます。いずれのボタンをクリックしても、そのリクエストと対応するステータスが関連付けられます。このステータスは、今後検索結果として表示した場合、常に、この証明書リクエストとともに表示されます。
   - 証明書の保留リクエストがすべて正常に検索されると、それらがリストに表示されます。25 件を超える場合は、25 件ずつ表示されます。リクエストを識別する番号をクリックすると、詳細が表示され、リクエストの承認または拒否を実行できます。
   - 単一の発行済証明書が正常に検索されると、「詳細表示」ボタンとともに、その証明書を表す行が表示されます。「詳細表示」をクリックすると、**「失効」**、**「更新」**または**「ブラウザへのインストール」**ボタンとともに証明書のデータが表示されます。「失効」ボタンを使用すると、証明書が無効になり、データベース内で「失効」というタグが付けられます。今後、「証明書失効リスト (CRL) の更新」ボタンを選択したとき、または CRL が自動的に再生成されるとき、失効済証明書の最新リストが Oracle Internet Directory にアップロードされます。信頼できる環境にあるアプリケーションで、CRL を使用して失効済証明書の付いたエンティティが認証されないようにできます。

     関連項目： 詳細は、4-15 ページの「証明書失効リスト（CRL）の更新」を参照してください。

拡張検索の使用方法

「拡張検索」機能を使用すると、次のように、より複雑な検索条件を指定して複数の証明書または証明書リクエストを検索および表示できます。

- 証明書リクエストの場合は、個別の検索で、保留リクエスト、拒否済リクエストまたは認証済リクエストをすべて表示できます。
- リクエストまたは発行済証明書の場合は、電子メール・アドレス、拡張 DN、シリアル番号または範囲、あるいは DN 内の特定のエントリ（名前、組織、州、国など）で検索できます。これらの構成要素は、連続した文字列として指定する必要があります。たとえば、cn=lakshmi, ou=st, o=oracle が所有する証明書は、検索条件として cn=lakshmi, o=oracle を指定しても、選択も検出もされません。この指定では、ou=st が指定されていないため、検索文字列が連続していません。

管理者は、検索結果から次のことを実行できます。

- 証明書検索で検索された単一の証明書のいずれかを選択し、詳細を表示した後、更新または失効（あるいはブラウザへのインストール）を実行できます。
- 証明書リクエストの検索で検出された単一の証明書リクエストのいずれかを選択し、詳細を表示した後、証明書発行の承認または拒否のいずれかを実行できます。

各タイプの検索で、検索パラメータを指定した後、**「実行」**ボタンをクリックします。OracleAS Certificate Authority では、一度に 25 件のレコードが表示されます。

証明書リクエストまたは発行済証明書に対して拡張検索を実行するには、次の手順を実行します。

1. 「認証管理」ページの「拡張検索」をクリックします。

   結果ページは、次のセクションで構成されています。これらのセクションから特定の検索タイプを選択できます。

   - リクエスト・ステータスを使用した証明書リクエストの検索 （「保留」、「却下」または「認証済」）
   - 「識別名 (DN) を使用した検索」（証明書または証明書リクエスト）
   - 「拡張識別名を使用した検索」（証明書または証明書リクエスト）
   - 「シリアル番号 / リクエスト ID の範囲を使用した検索」（証明書または証明書リクエスト）
   - 「証明書のステータスを使用した検索」（有効、失効済または満了の証明書）

2. 検索タイプを指定した後、「実行」ボタンをクリックして結果のリストを表示します。

   すべての検索結果に対して、OracleAS Certificate Authority では、一度に 25 件のレコードが表示されます。残りのレコードを表示するには、「前へ」および「次へ」ボタンを使用してナビゲートします。

リクエスト・ステータスを使用した証明書リクエストの検索

「拡張検索」ページのこのセクションを使用して、ステータス別に証明書リクエストを表示します。ドロップダウン・メニューから、「保留」、「拒否済」または「認証済」を選択して「実行」をクリックします。選択したステータスと一致する証明書リクエストのリストに、レコードが 25 件ずつ表示されます。

識別名 (DN) を使用した検索

「拡張検索」ページのこのセクションを使用して、特定の所有者別の証明書を表示します。所有者にはサーバーまたはエンド・ユーザーを指定できます。発行済証明書別またはリクエストされた証明書別に検索できます。

表 4-2 検索要素

検索要素	範囲指定要素の意味 / 内容
一般名	検索する証明書上の名前
電子メール・アドレス	DN の一部である電子メール・アドレス
組織単位	所有者が属する企業または組織内部の単位名
組織	所有者が属する企業または組織の名前
市 / 地域	所有者の所在地
都道府県	所有者が所在する都道府県
国	所有者の国を表す 2 文字のコード

注意： DN および拡張 DN を使用した検索について

DN および拡張 DN を使用した検索では、順序が連続した検索が必要になります。複数のフィールドを選択する場合または拡張 DN を使用する場合は、連続した文字列を形成する必要があります。たとえば、cn=johnDoe, ou=st, o=oracle, c=us, ou=st という有効な証明書では、o=oracle は検索文字列として有効ですが、ou=st, c=us は有効ではありません。

拡張識別名を使用した検索

「拡張検索」ページのこのセクションを使用して、所有者の識別名別に、発行済証明書（「証明書」）またはリクエストされた証明書（「証明書リクエスト」）を検索します。各 RDN 文字列に対する値を入力するかわりに、完全な DN 文字列を入力できます。

関連項目：「ドメイン・コンポーネント属性」

シリアル番号 / リクエスト ID の範囲を使用した検索

「拡張検索」ページのこのセクションを使用して、発行済証明書またはリクエストされた証明書をすべて、シリアル番号の範囲内で検索します。発行済証明書別またはリクエストされた証明書別に検索できます。いずれかを選択し、対象となる最小および最大のシリアル番号を指定して「実行」をクリックします。

表 4-3 証明書のシリアル番号の検索範囲を指定する要素

範囲指定要素	範囲指定要素の意味 / 内容
最小シリアル番号	範囲内の最小シリアル番号を入力します。
最大シリアル番号	範囲内の最大シリアル番号を入力します。

証明書のステータスを使用した検索

「拡張検索」ページのこのセクションを使用して、有効、失効済または満了の証明書をすべて検索します。これら 3 つのいずれかを選択して「実行」をクリックします。

証明書失効リスト（CRL）の更新

証明書を失効にすると、ユーザーの環境で使用できなくなります。失効したことを公開して、失効済証明書が誤って使用されないようにします。証明書失効リスト（CRL）と呼ばれる、失効済証明書のリストを公開すると、認証を行うエンティティは、最初にこのリストを確認できるため、誤使用を防止できます。たとえば、信頼できる環境のすべてのアプリケーションで、CRL を使用して失効済証明書の認証を防止できます。

OracleAS Certificate Authority をインストールするとき、デフォルトで自動 CRL 生成が有効になります。必要な電子メール情報を入力した後は、CRL 生成が失敗した場合、自動的に電子メールがユーザーに送信されます。

関連項目： 5-4 ページの「メール詳細」

最初の CRL は、1 日の有効期間（再生成間隔）で午前 0 時に生成されます。これらの値（および自動生成）は、管理者の Web インタフェースの「構成管理」タブの中にある「通知」サブタブの「スケジュールされたジョブ」セクションで構成可能です。

更新済の CRL を手動で生成するには、次の手順を実行します。

1. 「認証管理」のメイン・ページで、「証明書失効リスト（CRL）の更新」ボタンをクリックします。
   「証明書失効リストの更新」フォームが表示されます。
2. **「CRL の有効期間」**に、次の更新までの日数を数値で指定します。
3. **「署名アルゴリズム」**で、「RSA 付き MD5」や「RSA 付き SHA1」などをドロップダウン・メニューから選択します。（SHA-1 のほうが大きなダイジェストであり、反転攻撃や総当たり攻撃などの既知の攻撃に対して安全性が高いため、SHA-1 の使用をお薦めします。）

フォームに必要事項を入力した後、「送信」ボタンをクリックします。これによって CRL が生成されます。

この CRL を表示または保存用に取得するには、**「CRL の保存」**を選択した後、**「ブラウザへのインストール」**または**「ディスクへの保存」**を選択します。

関連項目： 第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「証明書失効リスト（CRL）の使用」

Oracle HTTP Server は、このリストを使用して、受信した SSL 証明書の妥当性を確認し、証明書が CRL にあるエンド・エンティティとの SSL 接続を拒否します。システムでこのようなサーバーが複数使用されている場合は、それらのサーバーが使用する適切なパスまたはファイル名に、サーバーの CRL としてその CRL をコピーする必要があります。各サーバーの CRL を設定するには、サーバーごとに決められた手順を実行します。

同様に、ブラウザおよび電子メールのクライアントは、これらの CRL を使用して受信した S/MIME 電子メールを検証し、接続しているサーバーを検証できます。

Oracle Internet Directory Integration

OracleAS Certificate Authority は、次を Oracle Internet Directory に公開します。

- 証明書が、userCertificate 属性と userSMIMECertificate 属性のユーザーのディレクトリのエントリに公開されます。
- 証明書失効リスト（CRL）が、cn=oca1,cn=CRLValidation,cn=Validation,cn=PKI, cn=Products,cn=OracleContext のロケーションに公開されます。

注意：

- 証明書公開を有効にして、Oracle Internet Directory に証明書を公開できるようにする必要があります。詳細は、第 5 章の「証明書の公開」を参照してください。
- 「ディレクトリの同期化」オプションを有効にして、ディレクトリが一時的に利用できない場合、ディレクトリが再度利用可能になったときに証明書がキューに入れられ公開されるようにできます。詳細は、第 5 章の「スケジュールされたジョブ」を参照してください。

このセクションでは、ディレクトリ統合に関連する次のトピックについて説明します。

- 証明書失効リストの取得

証明書失効リストの取得

OracleAS Certificate Authority は、失効済証明書のリストを含む証明書失効リスト（CRL）を Oracle Internet Directory に公開します。他のアプリケーションまたは別のユーザーは、必要に応じて CRL を使用して作業する必要があります。

CRL は OracleAS Certificate Authority ユーザーのホームページから直接取得できます。詳細は、第 8 章の「証明書失効リスト（CRL）の使用」を参照してください。

または、プログラムで規定されたアクセスについては、ディレクトリの特定のエントリを検索する **ldapsearch** コマンドを使用して OracleAS Certificate Authority の CRL を取得できます。

```
ldapsearch -p port -h ldaphost -b
  "cn=oca1,cn=CRLValidation,cn=Validation,cn=PKI,cn=Products,cn=OracleContext"–s scope -L "objectclass=*"
certificaterevocationlist
```

次のようになります。

- -p は、指定したポートでディレクトリに接続します。
- -h は、ldap のホスト・マシンを指定します。
- -b は、DN ロケーションを指定します。
- -s は、検索範囲を指定します。
- -L は、LDIF フォーマットでエントリを印刷します。
- "objectclass=*" は、検索フィルタを指示します。
- certificaterevocationlist は、取得するための属性です。

たとえば、次のように入力します。

```
ldapsearch -p 3060 -h rjackson-sol -b
  "cn=oca1,cn=CRLValidation,cn=Validation,cn=PKI,cn=Products,cn=OracleContext"
  –s base -L "objectclass=*" certificaterevocationlist
```

次の CRL 出力を生成します。

```
dn: cn=oca1,cn=CRLValidation,cn=Validation,cn=PKI,cn=Products,cn=OracleContext
certificaterevocationlist:: MIICADCB6QIBATANBgkqhkiG9w0BAQUFADA8MQswCQYDVQQGE
 wJVUzEPMA0GA1UEChMGb3JhY2xlMRwwGgYDVQQDExNDQS1sa2V0aGFuYS1zdW4tOTA0Fw0wNTAxM
 DQyMjA2MjZaFw0wNTAxMDkyMjA2MjZaMCIwIAIBBRcNMDUwMTA0MjIwNTQzWjAMMAoGA1UdFQQDC
 gEBoFUwUzBRBgNVHSMBAf8ERzBFoUCkPjA8MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGb3JhY2xlM
 RwwGgYDVQQDExNDQS1sa2V0aGFuYS1zdW4tOTA0ggEBMA0GCSqGSIb3DQEBBQUAA4IBAQAwBRgih
 GOB08sWRg2sIaelqLFlUYNvnbtOe4QjdyTPaAy6k31+15jGi1vA7UBw7c0HqLv9r9iHLn7x9MtBj
 Ei8GKj+OJ5GGvrVVnj7ngoSAfpMMhg805m+sgZu0UoBbBkuh9tyAGFzUbxqMCadwakUgEwi7OVsn
 2jaDJilPD/1Lcp975hhlO0JH5hAwpERttSzaZcLqNEPGc9GMiAEUkTVCEa9rPwaw+C42msTZg38N
 7hChaqVf6gj/NpwTOZw98tVyOfU/Iy5tndh5ghbx4PMQ8HoxjXuw0xh6VHTvjmV6q51eTfiAFD3e
 M+IWjxO7fdgL8zUTZ/6HA8fNxZgaJen
```

この出力をアプリケーションに適したフォーマットに解析できます。アプリケーションが CRL へのアクセスを定期的に必要とする場合、自動化スクリプトを設定して定期的に CRL をファイル・システムにコピーできます。

Single Sign-On および OracleAS Certificate Authority

OracleAS Certificate Authority と OracleAS Single Sign-On は相互補完の関係にあり、ユーザー証明書のプロビジョニングを簡単にし、OracleAS Single Sign-On を使用するすべてのアプリケーションに対する PKI 認証を、それらの証明書を使用して有効にします。この項で説明する 2 つの構成オプションを選択すると、この連携がより容易になります。

- SSO 認証済ユーザーへの OracleAS Certificate Authority 証明書リクエスト URL のブロードキャスト
- OracleAS Certificate Authority 証明書リクエスト URL への SSO 認証済ユーザーのアクセス

最初の構成オプションであるブロードキャストを使用すると、OracleAS Single Sign-On ユーザーは、デフォルトの OracleAS Certificate Authority 構成を使用するよりも簡単に、証明書リクエストを配信できるようになります。OracleAS Certificate Authority のデフォルトでは、OracleAS Single Sign-On 認証済ユーザーが証明書リクエストを配信すると証明書を提供するように構成されていますが、それにはいくつかの手順が必要になります。このプロセスは、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「Single Sign-On（SSO）認証」で説明します。

ブロードキャスト・オプションでは、送信可能なリンクがすべてのユーザーに提供され、ユーザーは OracleAS Single Sign-On/OracleAS Certificate Authority 証明書を直接リクエストできるようになるため、リクエストはさらに容易になります。

2 番目の構成オプションは、最初のオプションの説明に続いて、「OracleAS Certificate Authority 証明書リクエスト URL への SSO 認証済ユーザーのアクセス」で説明します。そこでは、OracleAS Single Sign-On 構成を簡略化することで、構成プロセスを大幅に短縮する OracleAS Certificate Authority 構成コマンドについて説明します。OracleAS Single Sign-On のデフォルト配置では、PKI 認証に必要な SSL が自動的に使用されるわけではありません。このため、OracleAS Certificate Authority 提供のユーザー証明書を実行時に OracleAS Single Sign-On で使用するには、SSL および証明書を使用できるように OracleAS Single Sign-On Server を構成する必要があります。この 2 番目の構成オプションを説明する「ユーザー証明書と SSO の使用」では、通常のデフォルト構成を活用して、このプロセスをさらに簡略化する方法について説明します。

2 番目の構成オプションの説明には、次の 2 つの項があります。

- SSO および OracleAS Certificate Authority を使用した PKI 認証の有効化
- ユーザー証明書と SSO の使用

ここでは、OracleAS Certificate Authority および OracleAS Single Sign-On Server を使用する PKI 認証に必要なすべての手順と、Single Sign-On の認証プロセスについて説明します。

SSO 認証済ユーザーへの OracleAS Certificate Authority 証明書リクエスト URL のブロードキャスト

OracleAS Single Sign-On ユーザーが OracleAS Certificate Authority 証明書の取得に使用する URL は、埋込みの HTML リンクとして電子メールで送信できます。または、エンタープライズ・ポータルのリンクとして公開できます。これらの方法を使用することで、証明書を必要とするユーザーに対して、より柔軟にこの機能を公開できます。

SSO 証明書リクエストの URL は、次のとおりです。

```
https://<Oracle_HTTP_host>:<oca_ssl_port>/oca/sso_oca_link
```

電子メールを送る際には、<Oracle_HTTP_host> をホストの Web または IP アドレスに、<oca_ssl_port> を Oracle 認証局 SSL サーバーの認証ポート番号に置換する必要があります。

URL のホストおよびポート番号の詳細は、「管理者の証明書のリクエスト」の手順 1 を参照してください。

これでユーザーは、このリンクをクリックし、次の項の「OracleAS Certificate Authority 証明書リクエスト URL への SSO 認証済ユーザーのアクセス」で説明する手順と同様の手順を実行できます。

注意： インストール後にポートが変更されていると、portlist.ini に最新情報が保管されていません。この場合は、Oracle Enterprise Manager Control にサインオンし、OracleAS Certificate Authority がインストールされているインスタンスをクリックします。次に、「ポート」リンクをクリックし、「タイプ」列で OracleAS Certificate Authority Server Authentication（SSL）というエントリを探して、その横の「使用中のポート」という見出しの列に表示されている数値を使用します。

OracleAS Certificate Authority 証明書リクエスト URL への SSO 認証済ユーザーのアクセス

Oracle Application Server Certificate Authority は、OracleAS Single Sign-On 認証を実行するようにデフォルトで構成されますが、いくつかの手順があります。ユーザーは、OracleAS Certificate Authority ユーザー・インタフェースにアクセスし、SSO 認証を選択した後、証明書をリクエストする必要があります。（詳細は、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「Single Sign-On（SSO）認証」を参照。）一部のユーザーには、この処理の実行が難しい場合があります。

そのため、OracleAS Certificate Authority には、OracleAS Single Sign-On Server による認証後、OracleAS Certificate Authority 証明書リクエスト URL にユーザーを直接送ってユーザー・インタフェースを簡単にするメカニズムがあります。

この URL を OracleAS Single Sign-On に提供し、OracleAS Single Sign-On が証明書を使用しないでユーザーを認証するときはいつでもこの URL を表示するように Oracle Application Server Certificate Authority を構成できます。OracleAS Single Sign-On は、証明書を使用しないでユーザーを認証すると、そのユーザーが証明書をリクエストできる OracleAS Certificate Authority 画面を表示します。証明書を作成し、ユーザーのブラウザにインストールすると、その後の認証では、その証明書が自動的に使用されるだけです。（ただし、このポップアップ画面は、ユーザーの興味の有無に関係なくすべてのユーザーに対して表示されるため、無関係のユーザーには不便な場合もあります。）

注意： ポップアップを表示するには、ユーザーはブラウザでポップアップのブロック化をオフに切り替える必要があります。

この方法で OracleAS Certificate Authority を構成する場合、管理者は（管理者用パスワードで）、ocactl コマンドライン・ツールを使用して、次のコマンドを発行します。

```
ocactl linksso
```

また、管理者は（管理者用パスワードで）、ocactl コマンドライン・ツールを使用して、OracleAS Single Sign-On 経由でこの URL の使用を取り消すことができます。この処理には、次のコマンドを発行します。

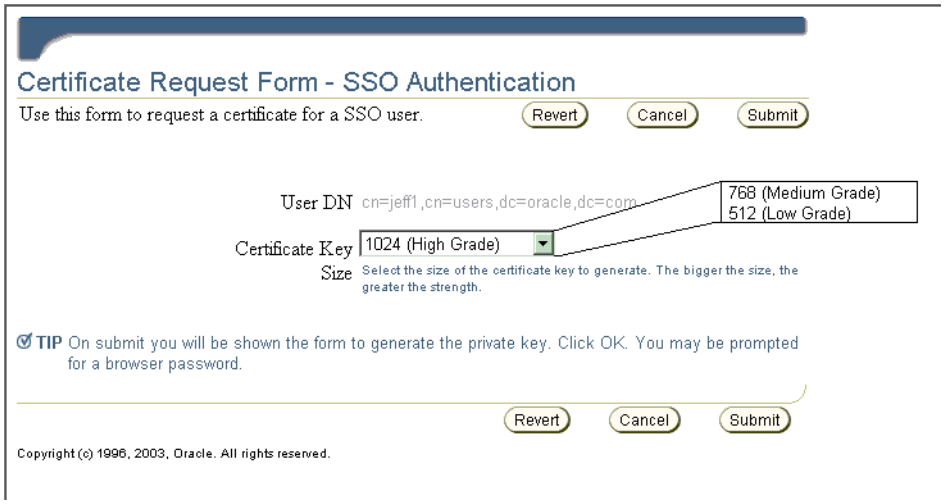
```
ocactl unlinksso
```

これらのコマンドを使用する場合、OracleAS Certificate Authority サービスを停止する必要はありません。ただし、OracleAS Single Sign-On Server の ORACLE_HOME で次のコマンドを使用し、OracleAS Single Sign-On Server を再起動して有効にする必要があります。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=oc4j instancename=oca
$ORACLE_HOME/opmn/bin/opmnctl startproc type=oc4j instancename=oca
```

ocactl linksso コマンドを実行し、OracleAS Single Sign-On server を再起動すると、OracleAS Single Sign-On が証明書を使用しないでユーザーを認証している場合は、常に、OracleAS Certificate Authority の初期ページが表示されます。次のようなページが表示されます。

OracleAS Single Sign-On ユーザーが「ここ」リンクをクリックすると、次に示す OracleAS Certificate Authority 証明書リクエストのページが表示されます。



この合成図では、SSO ユーザーが鍵のサイズを選択し、その選択したサイズが指定どおり設定された後、「送信」をクリックする必要があることを示しています。（「回復」をクリックすると、選択内容がデフォルトに戻ります。）リクエストの送信後、この証明書の鍵が自動的に生成されます（この処理には数分かかる場合があります）。その後、この証明書は、Oracle Internet Directory にインポートされ、ユーザーに表示されます。ユーザーが証明書の情報を確認し、

「ブラウザへのインストール」をクリックすると、証明書はユーザーのブラウザにインストールされ、自動使用できるようになります。

ユーザー証明書と SSO の使用

Single Sign-On Server への OracleAS Certificate Authority の再登録が完了したら、Single Sign-On を使用して OracleAS Certificate Authority への認証を行っていたユーザーは、以前と同様に証明書を使用できます。

新規ユーザーは、前述の項の説明に従い、OracleAS Single Sign-On 用の OracleAS Certificate Authority 証明書リクエスト URL を使用して証明書をプロビジョニングできます。

OracleAS Single Sign-On がユーザーを証明書で認識できるようになると、ユーザーは、ユーザー名 / パスワード・ログインまたは証明書のいずれかを使用して、OracleAS Certificate Authority などのアプリケーションにアクセスできます。

つまり、ユーザーは、ユーザー名 / パスワードを使用してログインし、手順に従って証明書を作成してブラウザにインストールした後、PKI を介して OracleAS Single Sign-On Server に対して自己認証を実行できます。

ユーザーのブラウザに、一部のアプリケーションの使用に認証を求める、OracleAS Single Sign-On に対する証明書が表示されると、OracleAS Single Sign-On は、ディレクトリを参照してその証明書を確認します。ユーザーのニックネーム（場合によってはサブスクライバ名も）で格納されている証明書とブラウザに表示されている証明書が一致している場合、認証は正常に実行されています。

注意： Oracle Internet Directory の一致規則によって、提供された証明書がディレクトリ内の証明書と照合される方法が決まります。次の資料を参照してください。

- 『Oracle Internet Directory 管理者ガイド』の「Oracle Internet Directory での認証」
- 『Oracle Internet Directory 管理者ガイド』の「ディレクトリでのユーザー証明書の検索」

Single Sign-On Server は、リクエストされた URL にユーザーをリダイレクトできるように、ユーザー情報を含む URLC トークンをアプリケーションに提供します。この後、リクエストされた内容を配信できます。

OracleAS Certificate Authority のインストールのデフォルト値

表 4-4 に、インストールのデフォルト値と、一部の重要な Wallet のデフォルト・ロケーションや有効期間などの情報を示します。

下位 CA の深度、つまりパス長を変更する場合は、コマンドラインを使用して CA 署名 Wallet を再生成する必要があります。付録 A「コマンドライン管理」の「OracleAS Certificate Authority からの下位 CA 署名 Wallet の生成」の説明に従い、`ocactl` を使用してください。

ただし、CA を再生成すると、以前に発行された証明書はすべて無効になります。そのため、パス長の値を変更する場合は、インストール後に CA 署名 Wallet をただちに再生成する必要があります。SSL Wallet など、依存する Wallet もすべて同様です。

注意： 1 つのリポジトリでの OracleAS Certificate Authority のスキーマは、1 つの OCA とのみ併用できます。

別の OracleAS Certificate Authority をインストールする場合、先行する OracleAS Certificate Authority のインストールに使用したリポジトリは選択できません。同じリポジトリを選択すると、OracleAS Certificate Authority 構成ツールが正常に実行されません。

それによって、インストール処理を途中で終了し、インストール全体をしなおすことが必要になります。

表 4-4 Wallets、CRL および OHS ポートに対するインストールの値（注記 1 を参照）

Wallet または値のタイプ	デフォルト DN	デフォルトの鍵のサイズ	デフォルトの有効期間	その他の値	この Wallet または値のロケーション
CA 署名 Wallet	この DN はインストール時に入力される	2048（注記 2 と 3 を参照）	3560 日	デフォルトのパス長 = 3	データベース
CA SSL Wallet	cn=<hostname> + CA の DN（CA の CN を除く）	1024（注記 4 を参照）	730 日	--	*$OH/oca/wallet/ssl*（注記 5 を参照）
OracleAS Certificate Authority 仮想ホスト用 OHS ポート	--	--	--	6600 および 6601（注記 6 を参照）	*$OH/Apache/Apache/conf/ocm_apache.conf*（注記 7 を参照）
証明書失効リスト	--	--	1 日	--	--

表 4-4 の注記：

1. 別のプロパティを設定するには、ocactl を使用します。
2. 証明書の署名に CA 署名 Wallet を使用する場合、インストール時に変更できるのは DN および鍵のサイズのみです。

注意：

DN の DC コンポーネントおよび EMAIL コンポーネントでは、印刷可能な（ASCII）文字のみを使用する必要があります。

この制限は、マルチバイト・キャラクタ・セットを使用するロケールでも、識別名の DC コンポーネントおよび EMAIL コンポーネントには ASCII 文字を使用する必要があるという意味です。

---

3. CA 署名 Wallet の場合は、`ocactl generatewallet -type CA` を実行して CA 署名 Wallet を再生成することで、インストール後にすべての要素を変更できます。また、デフォルトの有効期間は、新しい有効期間で証明書を更新することで変更できます。
4. Certificate Authority をホストする HTTP Server で使用されます。すべての CA SSL Wallet 値は、`ocactl generatewallet -type CASSL` を実行することで変更できます。CA SSL Wallet は、コマンドライン・オプションを使用して、いつでも再生成できます（期限切れの後も含む）。また、VeriSign などの異なる CA の SSL Wallet と置換することもできます。この置換を実行すると、最初に OracleAS Certificate Authority に接続したときに、CA 証明書が信頼できないという警告を回避できます。選択可能な鍵のサイズは、512、768、1024 および 2048 であり、1024 がデフォルトです。
5. $OH は `$ORACLE_HOME` を意味します。したがって、完全なロケーションは `$ORACLE_HOME/oca/wallet/ssl` です。
6. OracleAS Certificate Authority を複数インストールする場合などは、6602 から 6619 までのポートを使用できます。
7. $OH は `$ORACLE_HOME` を意味します。したがって、完全なロケーションは `$ORACLE_HOME/Apache/conf/ocm_apache.conf` です。

注意： `ocm_apache.conf` ファイルには、OracleAS Certificate Authority のリスナー・ポートが 2 つ定義されています。

2 つ必要な理由は、証明書を必要としない機能と必要とする機能があるためです。

Apache で ClientCertificate オプション・ディレクティブを使用した場合、証明書に関連するダイアログが常に表示されることになるため、この方法より、リスナー・ポートを 2 つ使用する方法のほうが適切です。

SSO および OracleAS Certificate Authority を使用した PKI 認証の有効化

証明書を使用するように OracleAS Single Sign-On を構成するには、いくつかの手順を実行する必要があります。付録 E にこれらの手順のすべてを示していますが、詳細なコンテキストと説明については、『Oracle Application Server Single Sign-On 管理者ガイド』に記載しているため、そちらのガイドも参照してください。

一般的な実行手順の概要を次に示します。

1. SSL の有効化については、『Oracle Application Server Single Sign-On 管理者ガイド』の第 7 章「SSL の有効化」に記載されています。
2. 証明書用 OracleAS Single Sign-On の構成については、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。
3. 付録 E「SSO での SSL および PKI の有効化」の「SSL を有効化した SSO への仮想ホストの再登録」の説明に従い、OracleAS Certificate Authority の仮想ホストを Single Sign-On Server に再登録します。

PKI を有効にすると、OracleAS Single Sign-On Server は、ユーザー名およびパスワードをリクエストするかわりに、証明書を使用してアプリケーションのユーザーを認証できます。OracleAS Single Sign-On のパートナ・アプリケーションのユーザーが OracleAS Single Sign-On 認証を選択すると、そのアプリケーションへのログインに使用する証明書を選択するよう、ブラウザから指示されます。使用する証明書は、以前にブラウザにインストールした証明書です。目的の証明書を選択すると、OracleAS Single Sign-On Server はその証明書を使用してユーザーを認証し、ユーザーがリクエストしたパートナ・アプリケーションにユーザーをリダイレクトします。

この処理では、次のことが問題になります。

- ユーザーは OracleAS Certificate Authority にログオンして自分の証明書を取得する必要があります。
- OracleAS Certificate Authority も OracleAS Single Sign-On 認証サービスを使用するため、証明書のないユーザーは OracleAS Certificate Authority にログオンできません。

この問題は、OracleAS Single Sign-On Server で複数の認証レベルを使用することによって解決されます。PKI が有効化されると、どのパートナ・アプリケーションでも、中 - 高レベルのセキュリティ（証明書による認証）が使用されますが、OracleAS Certificate Authority では、ユーザー名 / パスワードまたは Windows のネイティブ認証による中レベルのセキュリティを使用できます。それによって、OracleAS Certificate Authority は証明書を発行する前にパスワードを使用してユーザーを認証できるようになり、その一方で、それ以外の OracleAS Single Sign-On Server 対応アプリケーションには、証明書を使用した認証が強制されます。

ユーザー名 / パスワードによる中レベルのセキュリティを OracleAS Certificate Authority で使用するための構成手順など、すべての手順は、付録 E を参照してください。セキュリティ・レベル固有の手順は、付録 E の「SSO での PKI の有効化」に記載しています。

同様に、Windows のネイティブ認証など、他の認証メカニズムを使用するように OracleAS Certificate Authority を構成することもできます。目的の認証メカニズムを実装するプラグインにセキュリティ・レベルを割り当て、（「SSO での PKI の有効化」の）手順 3 で説明しているように、そのセキュリティ・レベルを使用するように OracleAS Certificate Authority URL を割り当てます。

> **関連資料：** 詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』の第 6 章「マルチレベル認証」を参照してください。

ルーチン管理タスク

表 4-5 に、一般的な管理タスクを示します。これらは OracleAS Certificate Authority 管理者にとって非常に重要なタスクです。その手間に応じて、大規模、中規模および小規模に分類されます。

表 4-5 ルーチン管理タスク

タスク	情報
大規模なタスク	-
証明書のプロビジョニング	2-8 ページの「証明書の自動または手動プロビジョニング」
Web 管理者の証明書の失効	A-2 ページの表 A-2「OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ」の `revokecert` コマンド
（鍵危殆化からリカバリするための）CA 署名鍵の失効	■ A-9 ページの「ルート CA 証明書の失効」 ■ 4-10 ページの「証明書の失効」
カスタム・ポリシー・プラグインの作成	6-22 ページの「カスタム・ポリシー・プラグインの開発」
バックアップおよびリカバリ	C-13 ページの「バックアップの保護の問題」
中規模のタスク	-
証明書リクエストの承認	4-9 ページの「証明書リクエストの承認または拒否」
下位 CA 証明書の認可	■ B-2 ページの「下位 CA 署名 Wallet の生成」 ■ 4-9 ページの「証明書リクエストの承認または拒否」
再関連付け（関連付けられた Oracle Internet Directory、OracleAS Single Sign-On およびデータベース・インスタンスの調整）	7-13 ページの「インフラストラクチャ・サービスの変更」
CA 署名、CA S/MIME および CA SSL Wallet の更新	7-2 ページの「OracleAS Certificate Authority の Wallet 操作」
ポリシー・パラメータおよび条件の調整	■ 6-3 ページの「Oracle Application Server Certificate Authority のポリシー」 ■ 6-16 ページの「ポリシー・ルールの条件」
DN の作成	6-17 ページの表 6-9「条件の属性」の DN のエントリおよびその説明
認証局運用規定の制定および保守	3-10 ページの「証明書のポリシーおよび手順の定義」
小規模のタスク	-
パスワードの変更	■ 7-4 ページの「パスワードの変更」 ■ A-7 ページの「権限付きパスワードの変更」
ユーザー証明書の更新および失効	■ 4-11 ページの「証明書の更新」 ■ 4-10 ページの「証明書の失効」
証明書失効リストの管理	■ 3-11 ページの「CRL ポリシーの定義」 ■ 4-15 ページの「証明書失効リスト（CRL）の更新」 ■ 8-12 ページの「証明書失効リスト（CRL）の使用」

5

Oracle Application Server Certificate Authority の構成

Oracle Application Server Certificate Authority の Web ベースの管理インタフェースは、次に示す 3 つの大きな事項を対象としています。各事項は、ホームページのタブからアクセスできます。

- 発行済証明書に関する事項 : 証明書の発行、失効および更新のリクエスト、および証明書失効リスト（CRL）
- 構成に関する事項 : OracleAS Certificate Authority のアクション用パラメータおよび証明書のセキュリティ・ポリシーを実装するためのパラメータ
- OracleAS Certificate Authority アクティビティのログの表示

この章では、これらの事項の 2 つ目と 3 つ目（構成管理およびログの表示）について説明します。この章の内容は、次のとおりです。

注意 : 証明書の構成問題および証明書のポリシー文の概要については、最初に第 3 章の「証明書の要件およびポリシー」を読んでから、先に進んでください。

管理インタフェースの構成

次の図に示すように、Oracle Application Server Certificate Authority のグラフィカル・ユーザー・インタフェース（GUI）のホームページには、この他に 3 つのタブがあります。

これらの 3 つのサブタブを使用して、証明書を管理または認証局を構成する特定のタスクを実行できます。

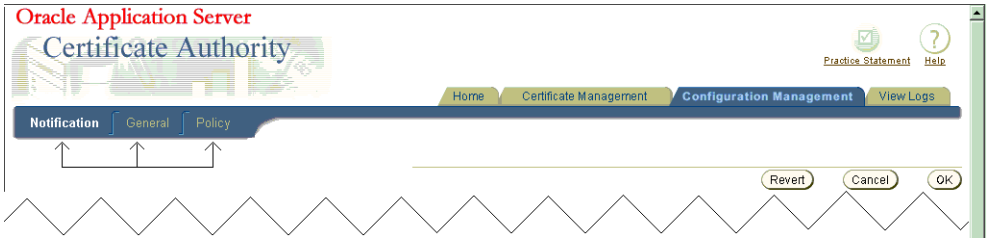
- 「「認証管理」タブ」については、第 4 章で説明しています。特に「証明書の管理」を参照してください。
- 「「構成管理」タブ」については、この章で説明しています。
- 「「ログの表示」タブ」については、この章で説明しています。

「構成管理」タブ

「構成管理」タブは、OracleAS Certificate Authority の Web 環境に初めてアクセスする際に選択可能な 4 つの項目のうちの 1 つです。ホームページで「構成管理」タブをクリックすると、1 つ目のサブタブが表示されます。各サブタブでは、OracleAS Certificate Authority の構成管理機能が分類されています。

次の項で、これらのサブタブの内容および使用方法について説明します。

- 構成タスクの概要
- 「通知」サブタブ
- 「一般」サブタブ
- 「Oracle Application Server Certificate Authority の「ポリシー」サブタブ」および「ポリシー操作」については、第 6 章「Oracle Application Server Certificate Authority でのポリシー管理」で説明しています。



構成タスクの概要

表 5-1、表 5-2 および表 5-3 に、「構成管理」の「通知」、「一般」および「ポリシー」という各サブタブで実行するタスクを示します。

表 5-1「構成管理」の「通知」サブタブのタスクおよび説明

「通知」サブタブのタスクおよびデータ	参照先
アラートと通知の宛先となるサーバー名および電子メール・アドレスを指定する。 表示するアラート・タイプを指定する。 CRL の自動生成を有効にし、その開始時刻と CRL 生成間隔、およびディレクトリ同期の開始時刻と間隔を指定する。	■ メール詳細 ■ アラート ■ スケジュールされたジョブ

表 5-2「構成管理」の「一般」サブタブのタスクおよび説明

「一般」サブタブのタスクおよびデータ	参照先
Oracle Internet Directory とあわせて、SSL 通信チャネルまたは非 SSL 通信チャネルを、証明書の公開に使用することを指定する。	■ 証明書の公開
証明書の管理のために、エンド・ユーザーが SSL 認証および OracleAS Single Sign-On 認証を使用できることを指定する。	■ SSL 認証および SSO 認証
「クライアント証明書のデフォルト使用方法」を指定する。	■ クライアント証明書のデフォルト使用方法
「サブジェクト代替名拡張機能」を指定する。	■ サブジェクト代替名拡張機能
ロギングまたはトレース（両方を実行すること、あるいはどちらも実行しないこと）を指定する。	■ ロギングおよびトレース
登録情報に示される DN コンポーネントのデフォルト値を指定する。	■ デフォルト・ベース DN コンポーネント
データベースおよびディレクトリの構成パラメータを表示する。	■ データベースの設定、ディレクトリの設定

表 5-3「構成管理」の「ポリシー」サブタブのタスクおよび説明

Oracle Application Server Certificate Authority の「ポリシー」サブタブのタスクおよびデータ（第 6 章）	参照先
使用可能な操作（証明書のリクエスト、失効、更新など）に適用可能なポリシーを参照する。	■ デフォルトの証明書リクエスト・ポリシー ■ デフォルトの証明書失効ポリシー ■ 製品に付属の証明書更新ポリシー
ポリシーの編集、有効化、無効化、削除、追加および並び替え。	■ ポリシー操作

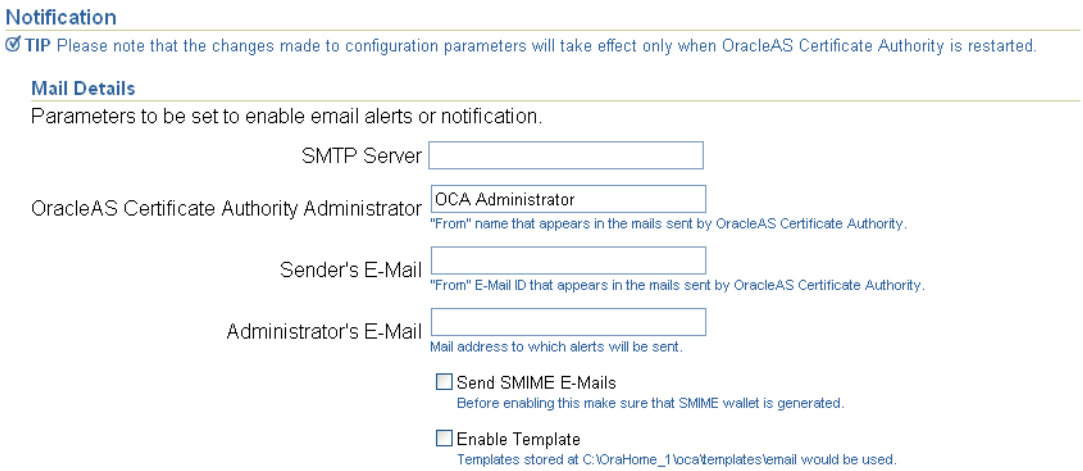
「通知」サブタブ

「通知」パラメータでは、管理者への通知電子メールをトリガーするイベント、通知電子メールの生成方法およびこれらのイベントを検出する頻度を制御します。

「通知」構成パラメータの変更を有効にするには、OracleAS Certificate Authority を再起動する必要があります。

メール詳細

メール・パラメータを使用すると、管理者として指定した電子メール・アドレスおよび OracleAS Certificate Authority ユーザー（必要に応じて判断される）に電子メール通知を送信できるようになります。（暗号化（S/MIME）電子メールを選択するには、まず S/MIME 証明書および Wallet を作成する必要があります。）通知電子メールでは、指定したサーバー、送信者およびテンプレートが使用されます。「通知」サブタブ画面の次の部分で、項目を指定します。



インストール後は、**「テンプレートの有効化」**の次のヒントに、テンプレート・ディレクトリへの正確なパスが表示されます。たとえば、インストール時に `$Oracle_Home` を `/private/sitename/username` に定義した場合は、このヒントには「/private/sitename/username/oca/email に格納されているテンプレートが使用されます。」と表示されます。

関連項目：

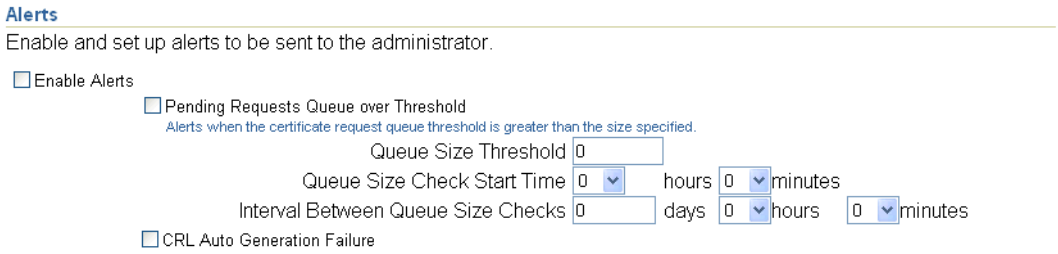
- 第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「CA SSL Wallet および CA S/MIME Wallet の再生成」
- 付録 G「OracleAS Certificate Authority での S/MIME」

アラート

「アラート」パラメータを使用すると、次の場合にアラートを受信するかどうかを指定できます（電子メール情報を指定した場合）。

- 証明書の保留リクエストの数が、ここで指定したキューのしきい値を超え、指定したスケジュール（開始時刻および繰返し間隔）で検証が行われる場合。開始時刻は、サーバーのタイムゾーンを参照し、24 時間の形式で指定されます。たとえば、14 時 30 分の開始時刻は、最初のチェックをサーバー時刻の午後 2 時 30 分に開始します。間隔（デフォルトは 1 日）がその時刻に追加されて、次回の検証の時刻が指定されます。この間隔はゼロ以外の値である必要があります。変更した内容は、再起動しても保持されます。
- CRL の自動生成に失敗した場合。たとえば、データベースまたは Oracle Internet Directory が一時的に使用できない場合、CRL の自動生成に失敗します。他にも、メモリー、入出力または接続性に関連する、予期しないランタイム・エラーまたは構成エラーが発生した場合も、CRL の自動生成に失敗します。

「通知」サブタブ画面の次の部分で、項目を指定します。

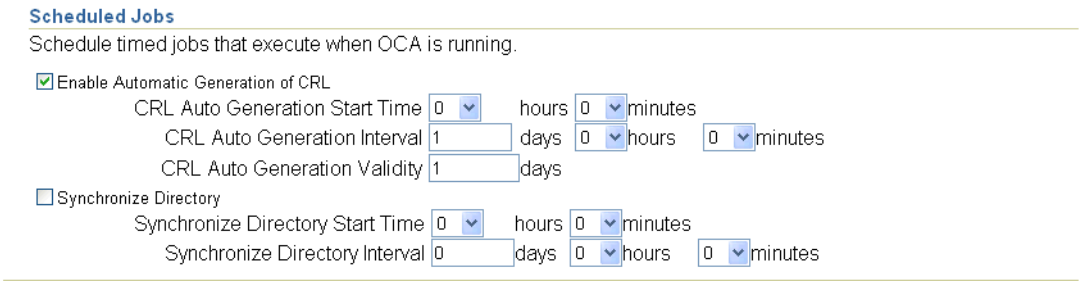


スケジュールされたジョブ

「スケジュールされたジョブ」パラメータを使用すると、自動ジョブについて次の項目を選択できます。

- CRL を自動生成するかどうか、その開始時刻および間隔。この機能は、OracleAS Certificate Authority のインストール時にデフォルトで有効になります。この機能によって、失効または期限切れになった証明書の検出に CRL を使用するアプリケーションをサポートする処理を、定期的かつ確実に実行できます。開始時刻は、サーバーのタイムゾーンを参照し、24 時間の形式で指定されます。たとえば、14 時 30 分の開始時刻は、最初のジョブをサーバー時刻の午後 2 時 30 分に開始します。指定した間隔がその開始時刻に追加されて、次回の CRL 生成の時刻が指定されます（デフォルトは 1 日）。この間隔はゼロ以外の値である必要があります。変更した内容は、再起動しても保持されます。
- ディレクトリを同期化するかどうか、その開始時刻および間隔。この機能によって、Oracle Internet Directory に格納されている証明書の情報が、適切なタイミングで定期的に更新されます。ディレクトリが一時的に停止している間に証明書を発行（または失効や期限切れ）した場合でも、同期化中は公開（または削除）されます。開始時刻は、サーバーのタイムゾーンを参照し、24 時間の形式で指定されます。たとえば、14 時 30 分の開始時刻は、最初のジョブをサーバー時刻の午後 2 時 30 分に開始します。指定した間隔（デフォルトは 1 日）がその開始時刻に追加されて、次回の同期化の時刻が指定されます。この間隔はゼロ以外の値である必要があります。変更した内容は、再起動しても保持されます。

「通知」サブタブ画面の次の部分で、項目を指定します。



電子メールのテンプレート

電子メールのアラートおよび通知の本文をテンプレートを使用して指定し、カスタマイズできます。これらのテンプレートは次のディレクトリに格納されています。

```
$ORACLE_HOME/oca/templates/email
```

> **注意：** テンプレートは、デフォルトでは無効になっているため、明示的に有効にする必要があります。

トークンを使用して電子メールの書式を設定することで、特定の情報を提供できます。これらのトークンは電子メールの送信前に置換されます。表 5-4 に、通知、電子メールの書式のファイル名、およびサポートされているトークンを示します。

表 5-4 電子メールのカスタマイズ用トークン

通知	テンプレートのファイル名	サポートされているトークン
CertificateRequestNotify	`reqacc.txt`	#NAME#、#REQUESTID#、#SUBJECTDN#、#PHONE#、#EMAIL#
RequestApprovalNotify	`reqapp.txt`	#NAME#、#REQUESTID#、#SUBJECTDN#、#SERIALNUM#、#OCAURL#、#PHONE#、#EMAIL#、#VALIDITY#
RequestRejectionNotify	reqrej.txt	#NAME#、#REQUESTID#、#SUBJECTDN#、#PHONE#、#EMAIL#
PendingRequestsAlert	`pendreq.txt`	#NAME#、#NUMBERREQUESTS#
CRLAutoGenFailureAlert	`crlfail.txt`	#NAME#

> **注意：**「通知」画面の**「構成管理」**で**テンプレートを使用するための**チェック・ボックスを選択していないと、テンプレートは使用されません。すべてのアラートおよび通知のテキストは事前に定義されており、変更はできません。

トークンの値

表 5-5 に、アラートまたは通知の送信前に各トークンと置換される値を示します。

表 5-5 サポートされているトークンの値

通知およびテンプレートのファイル名	サポートされているトークンおよびそれと置換されるデータ
CertificateRequestNotify テンプレート *=reqacc.txt*	#NAME#: 証明書リクエストに指定された連絡先データの名前に置換されます。 #REQUESTID#: このリクエストに対して OracleAS Certificate Authority が発行するリクエスト ID に置換されます。 #SUBJECTDN#: 証明書リクエストの DN に置換されます。 #PHONE#: 証明書リクエストの連絡先データの電話番号に置換されます。 #EMAIL#: 証明書リクエストの連絡先データの電子メール・アドレスに置換されます。
RequestApprovalNotify テンプレート *=reqapp.txt*	#NAME#: 証明書リクエストに指定された連絡先データの名前に置換されます。 #REQUESTID#: このリクエストに対して OracleAS Certificate Authority が発行するリクエスト ID に置換されます。 #SUBJECTDN#: 証明書リクエストの DN に置換されます。 #SERIALNUM#: 証明書のシリアル番号に置換されます。 #OCAURL#: ユーザーのホームページの URL に置換されます。 #PHONE#: 証明書リクエストの連絡先データの電話番号に置換されます。 #EMAIL#: 証明書リクエストの連絡先データの電子メール・アドレスに置換されます。 #VALIDITY#: 管理者によるその証明書リクエストの承認の有効期間に置換されます。
RequestRejectionNotify テンプレート *=reqrej.txt*	#NAME#: 証明書リクエストの連絡先データの名前に置換されます。 #REQUESTID#: このリクエストに対して OracleAS Certificate Authority が発行するリクエスト ID に置換されます。 #SUBJECTDN#: 証明書リクエストの DN に置換されます。 #PHONE#: 証明書リクエストの連絡先データの電話番号に置換されます。 #EMAIL#: 証明書リクエストの連絡先データの電子メール・アドレスに置換されます。
PendingRequestsAlert テンプレート *=pendreq.txt*	#NAME#: 「通知」画面の「構成管理」にある「OracleAS Certificate Authority 管理者」フィールドに指定されている値に置換されます。 #NUMBERREQUESTS#: OracleAS Certificate Authority リポジトリ内の保留リクエストの数に置換されます。
CRLAutoGenFailureAlert テンプレート *=crlfail.txt*	#NAME#: 「通知」画面の「構成管理」にある OCA 管理者フィールドに指定されている値に置換されます。

注意：

これらのテンプレートの編集に使用した言語が最終的な結果でも使用されるため、編集にはサーバーの言語を使用することをお薦めします。メッセージ本文はサーバーのロケールの言語でエンコードされます。

テンプレートを使用しない場合、アラートと通知はすべて、サーバーのロケールの言語で表示されます。

「一般」サブタブ

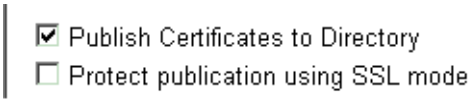
このサブタブを使用すると、次のタスクを制御するパラメータを設定できます。

- 証明書の公開
- SSL 認証および SSO 認証
- クライアント証明書のデフォルト使用方法
- サブジェクト代替名拡張機能
- ロギングおよびトレース
- デフォルト・ベース DN コンポーネント
- データベースの設定
- ディレクトリの設定

「一般」構成パラメータの変更を有効にするには、OracleAS Certificate Authority を再起動する必要があります。

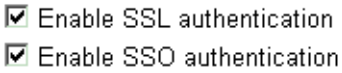
証明書の公開

この項の手順を実行することで、ディレクトリへの証明書を公開できます。OracleAS Certificate Authority は常に、SSL ポートを使用して Oracle Internet Directory に接続しているため、ここに表示される 2 番目のチェック・ボックス（「SSL モードを使用した発行の保護」）は不要になります。Diffie-Hellman による SSL 直接接続は認証を必要としないため、OracleAS Certificate Authority は、セキュアになった SSL 接続でユーザー名とパスワードを送信することによって、ディレクトリ・サーバーに対して自己認証します。



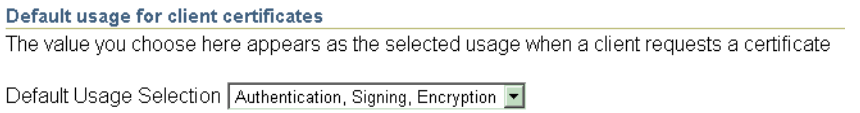
SSL 認証および SSO 認証

ここでは、SSL ユーザーまたは OracleAS Single Sign-On ユーザーが自動認識可能かどうかを指定できます。この指定によって、ユーザーの既存の証明書（または OracleAS Single Sign-On 認証）が、ユーザーの識別情報を認証しているものとして受け入れられます。これらの項目は、デフォルトでは有効になっており、管理者が介入しなくても、OracleAS Certificate Authority によって、新しい証明書がユーザーに発行されます。



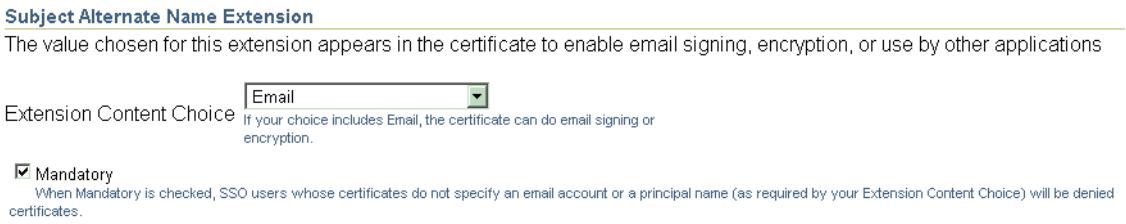
クライアント証明書のデフォルト使用方法

クライアントが証明書をリクエストしたとき、ここで選択した値が、選択された使用方法として表示されます。ユーザーはドロップダウン・リストから、別の使用方法を選択することもできます。「認証」、「暗号化」、「署名」およびこれらの組合せに加え、「CA 署名」と「コード署名」があります。



サブジェクト代替名拡張機能

SSO ユーザーの場合、この拡張機能に対して選択した値が証明書に表示され、電子メールの暗号化、署名、または他のアプリケーションによる使用が可能になります。選択した内容は、「拡張機能コンテンツの選択」に表示されます。

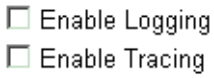


拡張機能コンテンツの選択「なし」、「電子メール」、「プリンシパル名 (UID)」または「電子メール、プリンシパル名 (UID)」から選択します。ここで選択した値は、証明書にサブジェクト代替名として表示され、電子メールの暗号化、署名、または他のアプリケーションによる使用が可能になります。(UID は、ユーザー識別子または一意の識別子を表します。)「電子メール、プリンシパル名 (UID)」を選択すると、証明書にその両方が表示されます。

必須 このチェック・ボックスを選択した場合、すべての SSO 認証証明書について「サブジェクト代替名拡張機能」が必須になります。SSO 認証証明書リクエストに指定されたユーザーの電子メール・アドレスまたはプリンシパル名が Oracle Internet Directory 内に見つからない場合、そのリクエストは否認されます。「Oracle Internet Directory 内に電子メール・アカウントが見つからないため、SSO 認証証明書を発行できません。リクエスト者は管理者に問い合せてください」というエラー・メッセージが表示されます。

ロギングおよびトレース

ここでは、すべてのユーザー・アクティビティのログ・ファイルを作成するかどうか、またはすべてのエラー詳細のトレース・ファイルを作成するかどうか、あるいはその両方を作成するかを指定できます。



ログは OracleAS Certificate Authority リポジトリに格納されます。「ログの表示」タブから、これらのログを参照できます。トレースは、ファイル・システムの *$ORACLE_HOME/oca/logs/oca.trc* ファイルに格納されます。

デフォルト・ベース DN コンポーネント

ここで入力した値は、手動の登録情報申請フォームにあるいくつかの識別名要素の事前入力に使用され、証明書リクエストの送信に使用されます。

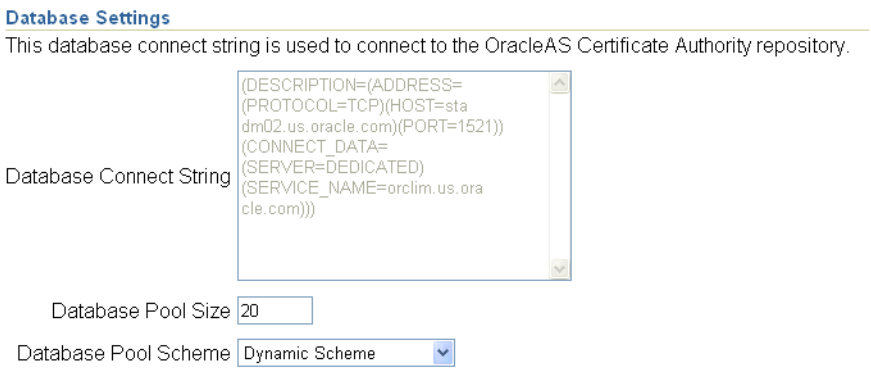
この機能はユーザーの利便性のみを目的としており、一般的なフィールドを補うためのものです。ここで入力した値は、必要に応じて変更できます。

データベースの設定

ここでは、データベース接続文字列、データベース・プール・サイズおよびデータベース・プール・スキームが表示されます。接続文字列は、OracleAS Certificate Authority リポジトリへの接続に使用される文字列です。

「データベース・プール・サイズ」テキスト・ボックスで、同時に OracleAS Certificate Authority にアクセスすると予測されるユーザー数を表す、データベースへの接続数（デフォルト : 20）を入力します。予測よりも少し大きい数を指定してください。たとえば、約 25 人の同時ユーザーが予測される場合、**「データベース・プール・サイズ」**には 27 または 28 を指定します。その接続プール内のユーザーが OracleAS Certificate Authority を終了すると、次の新規ユーザーに対してユーザー接続が使用可能になります。ユーザーがその数を超えるたびに新しい接続がオープンされ、そのユーザーが OracleAS Certificate Authority を終了すると同時にクローズされます。

「データベース・プール・スキーム」で、**「データベース・プール・サイズ」**で指定した接続すべてが使用中のときに発行された接続リクエストを処理する方法を選択します。デフォルトの「動的」は、新しいユーザーに対して新しい接続を即時にオープンし、そのユーザーが OracleAS Certificate Authority を終了した後にその接続をクローズするという意味です。「固定待機スキーム」を選択した場合、20 人（または指定した数）のユーザーが OracleAS Certificate Authority に接続された後、それ以降に接続しようとする各ユーザーは最初の 20 人のユーザーのうち 1 人が終了するまで待機します。「固定 NULL 戻し」を選択した場合、元のプール・サイズ制限数に達した後、接続しようとする新しいユーザーにはエラー・メッセージが表示されます。既存の OracleAS Certificate Authority ユーザーが終了するまで、新しいユーザーは接続できません。



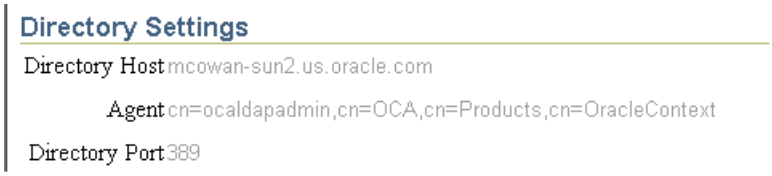
データベース接続文字列は、OracleAS Certificate Authority のリポジトリが新しい場所に移動された場合（または接続文字列が直接変更された場合）にのみ変更されます。これには、接続に使用するノードやポートの変更などがあります。この場合、`ocactl updateconnection` コマンドを使用して、リポジトリの接続設定を更新できます。その後、OracleAS Certificate Authority を再起動すると、新しい接続情報が使用されます。

関連項目：

- 第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「OracleAS Certificate Authority のパフォーマンス・チューニング」(7-8 ページ)
- 付録 A「コマンドライン管理」の表 A-2「OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ」の `updateconnection`

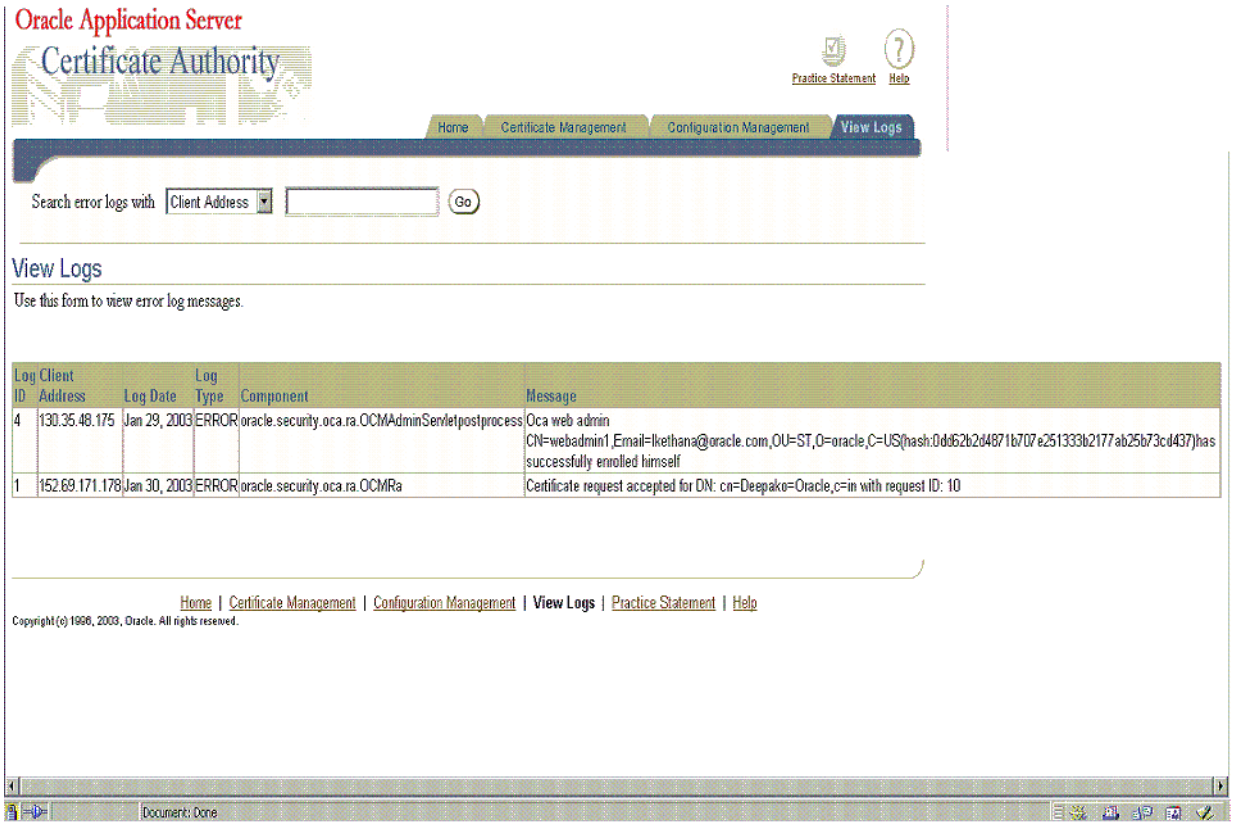
ディレクトリの設定

ここでは、Oracle Internet Directory との接続に使用されているホスト、エージェントおよびポートが表示されます。接続文字列が変更された場合、`ocactl updateconnection` コマンドを使用して、リポジトリの接続設定を更新できます。その後、OracleAS Certificate Authority を再起動すると、新しい接続情報が使用されます。



「ログの表示」タブ

「ログの表示」ページでは、OracleAS Certificate Authority の使用中に発生するトランザクションまたはエラーに関して、メッセージを記録したログを参照できます。次のような画面が表示されます。



これらのログの各行は、ログの ID 番号、クライアントのアクティビティが開始された IP アドレスおよび操作の実行日で始まる 6 つの要素で構成されています。各行には、ログのエントリ・タイプ、エントリを生成した OracleAS Certificate Authority のコンポーネントおよびアクティビティに関するコンポーネントのメッセージも含まれます。

これらのログは、クライアント（IP）アドレスやメッセージ内容などによって検索できます。ログを使用すると、管理者はリクエストの発行場所、およびそれらのリクエストに対して発行されたメッセージを調べることができます。検索によって、拒否関連のものなど特定のメッセージ・タイプ、およびこのようなメッセージの原因となった操作を開始した可能性のある特定のソース IP アドレスを確認できます。

関連項目： 第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「OracleAS Certificate Authority のログ情報またはトレース情報の消去」（7-13 ページ）

6

Oracle Application Server Certificate Authority でのポリシー管理

Oracle Application Server Certificate Authority は、組織で指定したポリシーを自動的に施行して、証明書の発行、失効または更新のリクエストに適用します。OracleAS Certificate Authority で提供されるポリシー・ルールは、標準的な必要事項をサポートします。ただし、OracleAS Certificate Authority の Web ベースのインタフェースの「構成管理」タブを使用したり、サイトの必要性に応じたカスタム・ポリシー・プラグインを追加することによって、管理者が構成することもできます。管理者は、必要に応じてこれらのポリシーを無効にして回避することもできます。

この章では、カスタム・ポリシー・プラグインを開発するツールなど、OracleAS Certificate Authority のポリシー管理コンポーネントについて説明します。

この章の内容は、次のとおりです。

定義

表 6-1 OracleAS Certificate Authority でのポリシーの概念、用語および定義

概念または用語	定義
ポリシー・ルールまたはポリシー	Oracle Application Server Certificate Authority におけるポリシー・ルールとは、証明書やリクエストなどに適用されるパラメータ値のデフォルトおよび範囲のセットです。たとえば、有効期間のポリシー・ルールには、365 日（最小有効期間）、730 日（デフォルト）および 3650 日（最大有効期間）を指定できます。 ポリシー・ルールには、ルールの用途を制限または変更する条件を含めることもできます。条件を指定しない場合、更新などの特定の操作へのポリシー・ルールが、すべてのリクエストに適用されます。
条件	OracleAS Certificate Authority における条件とは、証明書または証明書リクエストのタイプを識別するために作成する式および対応する値です。証明書または証明書リクエストのタイプが条件式と一致すると、リクエストの妥当性を評価するために、ポリシーのデフォルト値のかわりに、これらの対応する値が使用されます。 条件が使用できるのは OracleAS Certificate Authority のデフォルト・ポリシーのみで、「カスタム・ポリシー・プラグインの開発」で説明するカスタム・ポリシーでは使用できません。 例 : Type=="client"
プラグイン	ポリシー・ルールを実装する Java クラス。

ポリシー管理の概要

ポリシー管理とは、組織的な制約を施行するために Oracle Application Server Certificate Authority 管理者が選択したポリシー（ルールのセット）の定式化および適用を意味します。制約には、鍵のサイズおよび有効期間をユーザーが選択するための項目などがあります。

管理者は、OracleAS Certificate Authority で提供されたポリシーを使用して、次の操作を定義できます。

- OracleAS Certificate Authority が、受信したリクエスト（証明書の発行、失効および更新）を評価する方法
- CA が証明書のパラメータ（有効期間や鍵の長さなど）に適用する制限、またはサブジェクト名および使用方法が同じ証明書を複数発行する際に適用する制限

OracleAS Certificate Authority の Web ベースのインタフェースで、「構成管理」タブの編集機能を使用して、ポリシー・ルールの有効化、無効化または変更を行うことができます。「Oracle Application Server Certificate Authority の「ポリシー」サブタブ」を参照してください。

新しいルールを作成したり、ルールを具体化するポリシー・プラグインを開発することもできます。各ルールは、管理者が選択した評価または制限を実装するポリシー・プラグイン（Java クラス）に具体化されます。ポリシー・ルールとポリシー・プラグインは、1 対 1 でマッピングされます。OracleAS Certificate Authority のデフォルトのプラグインは、一般的に必要なほぼすべてのポリシー構成を対象としています。ポリシー・プラグインを作成する場合、6-22 ページの「カスタム・ポリシー・プラグインの開発」で説明するように、管理者は適切なプログラミング手法に従い、OracleAS Certificate Authority パッケージが提供する API を使用する必要があります。

サイト固有のポリシーを定義する新しいプラグインを開発した後、同じ「ポリシー」サブタブを使用して、そのプラグインに名前を付け、OracleAS Certificate Authority に登録することができます。プラグインを有効にすると、OracleAS Certificate Authority は、プラグインに定義されているとおりに新しいルールを施行します。

ポリシー・ルールは、OracleAS Certificate Authority エンジンのポリシー・プロセッサ・モジュールによって施行されます。このプロセッサ・モジュールは、すべての有効なルールを順次施行します。有効化されていないルール、または無効化されたルールは施行されません。「ポリシー」サブタブの各操作の「ポリシー・ルール」ページで指定した順序が使用されます。つ

まり、プロセッサ・モジュールは、各操作の「ポリシー・ルール」ページで指定した順に、ポリシー・プラグインをコールします。受信したあらゆるリクエストは、操作のタイプ（リクエスト、更新、失効など）に対応する、適切で有効なすべてのポリシー・ルールの対象となります。ルールが有効で、受信したリクエストと条件が一致しない場合、そのリクエストは拒否されます。

各ポリシー・ルールは、証明書の発行、失効または更新のリクエストのうち、1 つ以上の属性に関係します。たとえば、ある属性は、RSA アルゴリズムで使用する鍵の最小サイズおよび最大サイズに関係します。関係するデフォルト・ポリシーは、このようなすべての属性が、アルゴリズムの有効範囲内にあることを検証します。

ポリシーは、管理インタフェースの「ポリシー」サブタブを使用した Web ベースのインタフェースを介して管理されます。

条件を含むポリシー処理の詳細は、「ポリシー・ルールの条件」を参照してください。

Oracle Application Server Certificate Authority のポリシー

Oracle Application Server Certificate Authority では、制約固有のポリシー・ルールを提供しています。このポリシー・ルールは、証明書の登録、失効または更新の受信リクエストをポリシー・プロセッサが評価する際に使用します。各ルールの範囲内で、OracleAS Certificate Authority を構成して、特定の属性について、受信したリクエストを検証できます。また、これらの属性を受け入れたり、変更したり、リクエストを却下することもできます。

ポリシー・ルールが有効な場合、OracleAS Certificate Authority サーバーによって、処理中の証明書リクエストにルールが適用されます。

表 6-2 に、制約固有のデフォルトのポリシー・ルールを示します。最初の列に、各ポリシー・ルールについての参照先を示します。

表 6-2 制約固有のデフォルトのポリシー・ルール

ポリシー・ルール名	機能	デフォルトの状態
RSAKeyConstraints	鍵の長さに制約を施行する	有効
ValidityRule	指定した有効期間を証明書に施行する	有効
UniqueCertificateConstraint	同じ使用方法で同じ名前のサブジェクトに複数の証明書を発行することを禁止する	有効
RevocationConstraints	期限切れの証明書の失効リクエストを許可または拒否する	有効
RenewalRequestConstraint	期限切れの証明書の更新リクエストを許可または拒否する	有効

RSAKeyConstraints

RSAKeyConstraints ポリシー・ルールは、RSA の公開鍵 / 秘密鍵に使用する鍵の最小サイズおよび最大サイズの制約を適用します。

表 6-3 に、RSA 鍵の制約モジュールのパラメータを示します。

表 6-3 RSAKeyConstraints ポリシー・ルールのパラメータ

パラメータ	説明
Status（有効または無効） デフォルト : 有効	「ポリシー・ルール」ページで、ルールが有効か無効かを指定します。 ルールを有効にして他のパラメータを適切に設定すると、Oracle Certificate Manager は、条件式で指定した証明書にルールを適用します。 ルールを無効にすると、Oracle Certificate Manager は、512 ～ 4096 で 16 の倍数の RSA 鍵のサイズを許可します。
predicate デフォルト : "*"	このルールの条件式を指定して、ルールを適用する証明書のタイプを制限します。証明書リクエストにルールを適用する場合は、このフィールドに「*」を入力します。 例 : Type=="client" Type=="*" 「ポリシー・ルールの条件」を参照してください。
minSize デフォルト : 1024	RSA 鍵の最小の長さ（ビット単位のモジュールの長さ）を指定します。maxSize パラメータで指定した値以下の値を設定する必要があります。 有効値 : 512、1024、2048 または 4096 ビット
maxSize デフォルト : 2048	RSA 鍵の最大の長さ（ビット単位のモジュールの長さ）を指定します。minSize パラメータで指定した値以上の値を設定する必要があります。 有効値 : 512、1024、2048 または 4096 ビット

管理者は、複雑な条件式を使用して、複数の組合せで predicate、minSize および maxSize を指定できます。

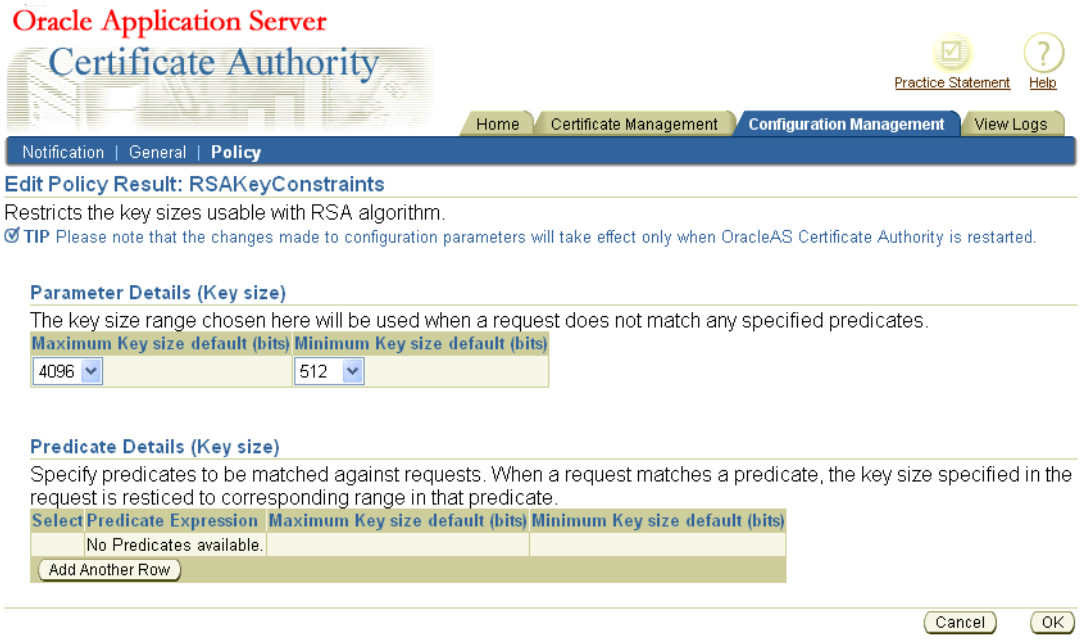
たとえば、ある組織では、最小サイズと最大サイズが、Sales 部門では 512 と 1024、Marketing 部門では 1024 と 2048 に設定する必要があるとします。複数の条件式および値のセットを使用して、この要件を指定できます。

条件 1: dn=="ou=Sales"

minSize は 512、maxSize は 1024 に指定します。

条件 2: dn=="ou=Marketing"

minSize は 1024、maxSize は 2048 に指定します。



ValidityRule

ValidityRule ポリシー・ルールは、証明書リクエストの有効期間が適切かどうかを判断し、次の方法で最小および最大の有効期間を施行します。

- （OracleAS Single Sign-On Server 認証または SSL 認証による）自動認証ユーザーの証明書リクエストでは、このルールにより有効期間が設定されます。
- 手動認証ユーザーの証明書またはサーバーの証明書に対するリクエストがポリシーと一致しない場合、そのリクエストは拒否されます。
- このルールによって設定された有効期間にかかわりなく、証明書の満了日を CA 証明書の満了日以降にすることはできません。このチェックを無効にすることはできません。

表 6-4 に、発行有効期間の制約モジュールのパラメータを示します。この項の最後に、Web ベースのインタフェースでの表示を示します。

表 6-4 ValidityRule ポリシーのパラメータ

パラメータ	説明
Status（有効または無効） デフォルト : 有効	「ポリシー・ルール」ページで、ルールが有効か無効かを指定します。 ルールを有効にして他のパラメータを適切に設定すると、predicate パラメータに指定した、構成済の証明書の有効期間が Oracle Application Server Certificate Authority によって検証されます。 ルールを無効にすると、Oracle Application Server Certificate Authority が、構成済の証明書の有効期間を検証する際に、ルールに指定した有効期間は使用されません。かわりに、リクエストに指定した有効期間が使用されます。
Minimum Validity デフォルトの最小期間 : 90 日	証明書の最小有効期間（日数）を指定します。 有効値 : 0（ゼロ）より大きく、Maximum Validity パラメータで指定した値より小さい整数。

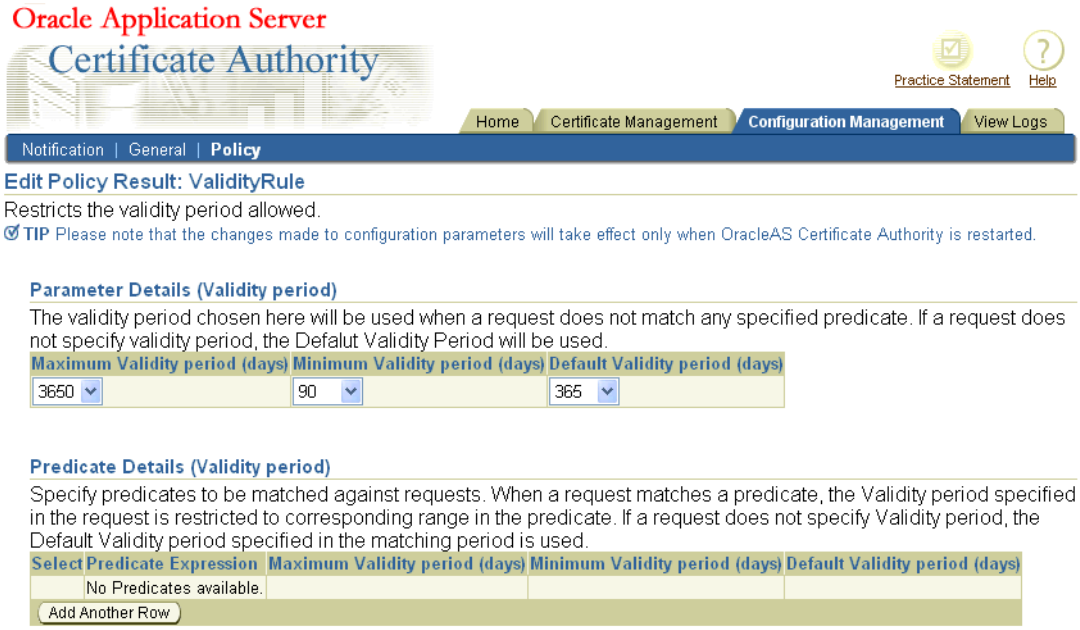
表 6-4 ValidityRule ポリシーのパラメータ（続き）

パラメータ	説明
Maximum Validity デフォルトの最大期間 : 3650 日	証明書の最大有効期間（日数）を指定します。 有効値 : 0（ゼロ）より大きく、Minimum Validity パラメータで指定した値より大きい整数。 デフォルトの有効期間は Default Maximum: 3650 日。
validityPeriod デフォルト : 365 日	OracleAS Single Sign-On ユーザーおよび SSL ユーザーの有効期間を指定します。最小有効期間と最大有効期間の間の値を指定する必要があります。 値は 365 日に設定されています。
predicate	このルールの条件式を指定して、ルールを適用する証明書のタイプを制限します。ルールをすべての証明書リクエストに適用する場合は、フィールドに「*」を入力します。 例 : Type=="client" Type=="*" 「ポリシー・ルールの条件」を参照してください。

このルールを無効にすると、OracleAS Certificate Authority によって、証明書リクエストに指定した有効期間の証明書が発行されます。その期間は、CA の証明書の有効期間以内に設定されます。

自動認証のクライアント・ユーザー（OracleAS Single Sign-On Server 認証ユーザーや SSL 認証ユーザーなど）の場合、有効期間は、ポリシーに指定した条件と一致するデフォルト有効期間を使用して、自動的に設定されます。その他のユーザーの場合、有効期間は、証明書リクエストに指定したとおりになります。この機能によって、自動認証ユーザーが取得する有効期間は管理者が正確に指定できるため、これらのユーザーがこの値を入力する必要はなくなります。

認証局には、5 ～ 10 年の有効期間を適用できます。CA に対する有効期間を長めに設定すると、更新や置換の必要がなく、発行した証明書は長期にわたって有効となります。OracleAS Certificate Authority のインストール処理では、ルート CA に対してデフォルト値である 10 年が使用されます。次の図に、ValidityRule パラメータを示します。



UniqueCertificateConstraint

UniqueCertificateConstraint ポリシー・ルールは、OracleAS Certificate Authority が、同じ使用方法で、同じサブジェクト名に複数の証明書を発行することを禁止します。有効に設定すると、ポリシーのパラメータがこのような複数の証明書を禁止するように設定されている場合に、このリクエストを拒否することができます。

ポリシーは、受信した証明書リクエストと同じサブジェクト DN を持つ証明書が Oracle Application Server Certificate Authority リポジトリにないか確認します。サブジェクト DN が同じ証明書が見つかった場合は、次に、証明書の使用方法（暗号化、署名など）を確認します。リクエストしている DN を持つ証明書が存在し、同じ使用方法が指定されている場合は、ポリシーに複数の証明書を拒否するように設定していると、そのリクエストは拒否されます。

表 6-5 に、UniqueCertificateConstraint モジュールのパラメータを示します。

表 6-5 UniqueCertificateConstraint ポリシー・ルールのパラメータ

パラメータ	説明
Status（有効または無効） デフォルト：有効	「ポリシー・ルール」ページで、ルールが有効か無効かを指定します。 ルールが有効な場合は、使用方法が同じ複数の証明書を許可するチェック・ボックスを使用します。サブジェクト名および使用方法が同じ複数の証明書を禁止する場合は、リクエストは拒否されます。 ルールを無効にすると、OracleAS Certificate Authority は、サブジェクト名および使用方法が同じ複数の証明書リクエストを認可します。
同じ DN と同じ使用方法を持つ複数の証明書を許可するチェック・ボックス デフォルト：選択	選択すると、OracleAS Certificate Authority は、使用方法が同じでも、すでに証明書を持っている DN にも新しい証明書を発行できます。 選択を解除すると、OracleAS Certificate Authority は、新旧の証明書の使用方法が同じ場合に、すでに証明書を持っている DN に新しい証明書を発行できません。

RevocationConstraints

OracleAS Certificate Authority 管理者は、このポリシーをユーザーからの証明書失効リクエストに適用することにより、期限切れの証明書の失効を制限できます。このポリシーが有効な場合は、満了後でも期限切れの証明書を失効させることができます。PKI の設定で期限切れの証明書の失効を許可しない場合は、このポリシーを使用して、期限切れの証明書を失効させないように Oracle Application Server Certificate Authority を構成できます。

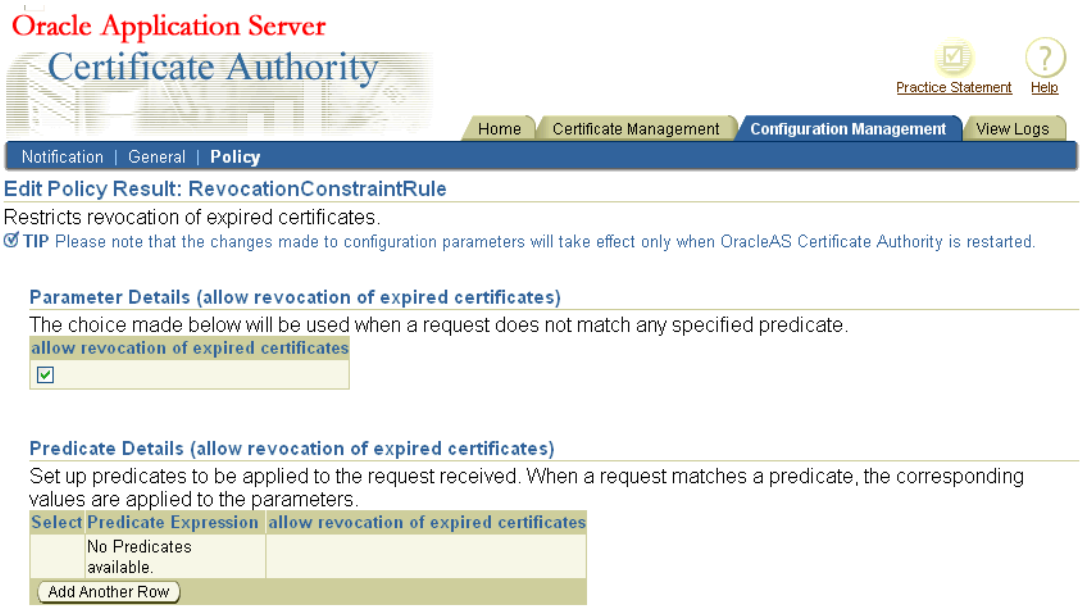


表 6-6 に、失効制約モジュールのパラメータを示します。

表 6-6 RevocationConstraints ポリシー・ルールのパラメータ

パラメータ	説明
Status（有効または無効） デフォルト：有効	「ポリシー・ルール」ページで、ルールが有効か無効かを指定します。 ルールを有効にして他のパラメータを適切に設定すると、OracleAS Certificate Authority は、失効させる証明書の有効期間、および allowExpiredCerts パラメータに割り当てられる値を確認し、それに従って失効リクエストを許可または拒否します。 ルールを無効にすると、OracleAS Certificate Authority は、失効させる証明書の有効期間および期限が切れているかどうかの確認は行いません。証明書は失効されるだけです。
allowExpiredCerts デフォルト：TRUE	期限切れの証明書の失効を許可するか（TRUE）、拒否するか（FALSE）を指定します。 デフォルトは、TRUE（許可）です。

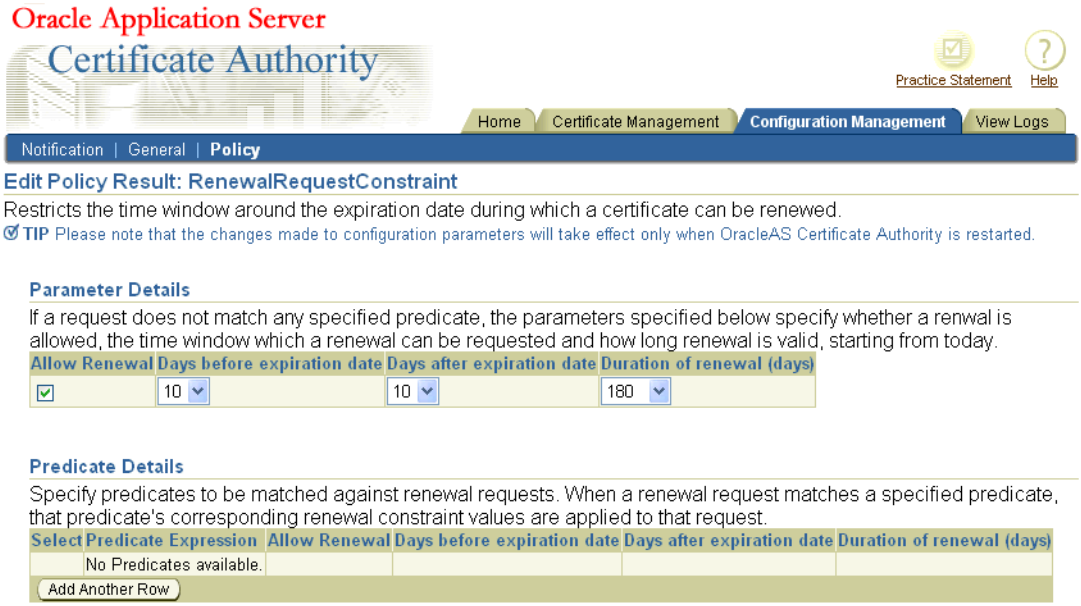
RenewalRequestConstraint

OracleAS Certificate Authority 管理者は、このポリシーを証明書の更新リクエストに適用することによって、証明書の更新（管理者の証明書の更新も含む）が可能な時間枠を制限できます。このポリシーが有効な場合、ユーザーは、満了日の前後に指定した日数以外では証明書を更新できません。このポリシーを構成することによって、PKI の設定で期限切れの証明書の更新を除外または制約することができます。

表 6-7 に、更新を制約するポリシー・ルールのパラメータを示します。

表 6-7 RenewalConstraints ポリシー・ルールのパラメータ

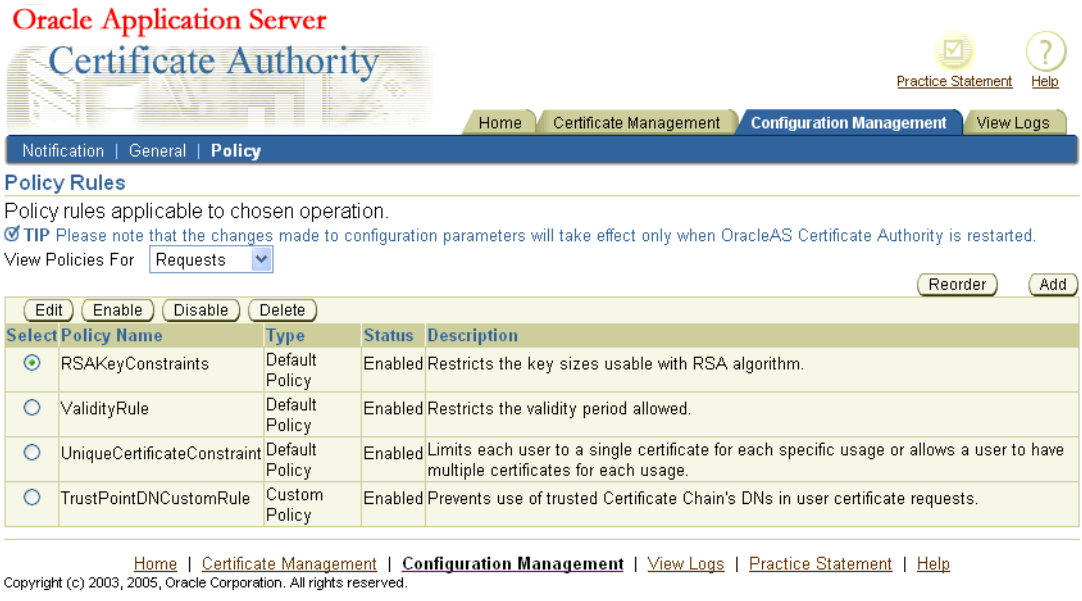
パラメータ	説明
Status（有効または無効） デフォルト : 有効	「ポリシー・ルール」ページで、ルールが有効か無効かを指定します。 ルールを有効にして他のパラメータを適切に設定すると、Oracle Application Server Certificate Authority は renewalNotBefore パラメータおよび renewalNotAfter パラメータを確認し、満了日の前後に指定した日数内にリクエストが行われたかどうかを検証します。確認が正常に終了すると、有効期間が validityPeriod パラメータに指定した値に設定されます。 ルールを無効にすると、OracleAS Certificate Authority によって、証明書の更新がリクエストされた日付を確認せずに、そのまま更新し、有効期間を 365 日に設定します。
predicate （デフォルトはなし）	このルールの条件式を指定します。ルールをすべての証明書リクエストに適用する場合は、このフィールドに「*」を入力します（デフォルト）。自動認証ユーザーの場合、クライアントのタイプは常に「ocmcert」であるため、「DN=="ou=ST,o=Oracle,c=US"」のような、タイプの条件式は必須ではありません。（DN エントリは、連続して指定する必要があります。「C=」エントリまで完全に指定する必要がありますが、「CN」で始める必要はありません。DN フィールドと DN フィールドの区切りには、カンマを使用する必要があります。） 「ポリシー・ルールの条件」を参照してください。
allowRenewal デフォルト : TRUE	証明書の更新を許可するか（TRUE）、拒否するか（FALSE）を指定します。
renewalNotBefore デフォルト : 10	満了日の何日前まで証明書の更新が可能かを指定します。 有効な値は、10、15、20、25 または 30 です。
renewalNotAfter デフォルト : 10	満了日の何日後まで証明書の更新が可能かを指定します。 有効な値は、10、15、20、25 または 30 です。
validityPeriod デフォルト : 365 日	証明書の更新有効期間（日数）を指定します。有効な値は数値で、期間は任意です。



OracleAS Certificate Authority のすべてのポリシーは、OracleAS Certificate Authority 管理者が、Web ベースの管理インタフェースの「ポリシー」サブタブを使用して管理します。

Oracle Application Server Certificate Authority の「ポリシー」サブタブ

「ポリシー」サブタブを最初に選択すると、証明書リクエストに適用可能なすべてのポリシー・ルールが Oracle Application Server Certificate Authority に表示されます。



「ポリシーの表示」のラベルが付いたドロップダウン・ボックスから「失効」と「更新」のどちらかを選択することによって、表示するポリシー・ルールを、失効に適用するものと更新に適用するものに切り替えることができます。その後、Oracle Application Server Certificate Authority に、これらのポリシーが表示されます。次の項で、OracleAS Certificate Authority に付属のポリシー、および管理者が使用できるアクションについて説明します。

- デフォルトの証明書リクエスト・ポリシー
- デフォルトの証明書失効ポリシー
- 製品に付属の証明書更新ポリシー
- ポリシー操作

ポリシーは、証明書リクエストの評価に使用するルール、および発行された証明書の更新または失効に使用するルールを指定します。リクエスト、失効または更新のポリシーを追加することができます。また、複数のポリシーが存在する場合は、ポリシーを並び替えて、適用順序を変更することもできます。指定したタイプの各ポリシーで、パラメータと条件を参照および編集したり、そのポリシーを有効化または無効化することができます。OracleAS Certificate Authority のデフォルト・ポリシーは削除できませんが、カスタム・ポリシーは削除できます。

ポリシーを追加するには、名前と説明を指定し、さらに `$ORACLE_HOME/oca/policy` ディレクトリに jar として事前に追加したクラスを指定する必要があります。（Windows の場合は `%ORACLE_HOME¥oca¥policy`。）

関連項目：「カスタム・ポリシー・プラグインの開発」

管理者は、すべてのポリシーを無効にすることができます。ポリシーを無効にしても削除されないため、今後使用できなくなるわけではありません。ただし、OracleAS Certificate Authority リポジトリのエントリは、後で再度有効にできるためリセットされます。ポリシーを削除すると、別のポリシーとして追加しないかぎり、永続的に使用できません。

ポリシーは、OracleAS Certificate Authority リポジトリのエントリによって有効になります。無効なポリシー（または OracleAS Certificate Authority リポジトリには指定されていたが有効ではないポリシー）を有効にすると、そのポリシーのパラメータおよび条件が再び有効になります。

通常、ポリシーのパラメータは、デフォルトの制限または範囲を指定します。証明書リクエストは、この制限または範囲に従う必要があり、違反すると自動的に拒否されます。機能や制約を有効または無効にするだけのパラメータもあります。パラメータは、条件に指定された場合を除き、すべての場合に適用されます。

ポリシーの条件は、ポリシーのパラメータの制限、範囲または制約が、他のすべての証明書またはリクエストのデフォルトとは異なるように指定されている、特定の証明書またはリクエストのタイプを識別します。

「ポリシー」構成パラメータの変更を有効にするには、OracleAS Certificate Authority を再起動する必要があります。手順は第 4 章の「Oracle Application Server Certificate Authority の起動および停止」を参照してください。

次の項で説明するとおり、OracleAS Certificate Authority には、証明書のリクエスト、失効および更新に適用するポリシーが用意されています。

証明書を発行するときに「ポリシーを適用」チェック・ボックスの選択を解除すると、管理者は、ポリシーを上書きすることができます。

デフォルトの証明書リクエスト・ポリシー

証明書リクエストは、セキュリティ上重要な 4 つの要因を制限するポリシーのパラメータおよび条件を満たしている必要があります。デフォルトのポリシーで、次の要因に関係するパラメータおよび条件を調整できます。

- 鍵サイズの範囲の調整および RSA の公開鍵 / 秘密鍵のデフォルトの設定
- 有効期間の範囲の調整およびデフォルトの設定
- ユーザーが、使用方法（署名、鍵の暗号化、またはデータおよび電子メールの暗号化、個別に指定された署名、証明書署名または暗号化（S/MIME: Secure Multipurpose Internet Mail Extensions））ごとに、複数の証明書を持つことに対する許可または禁止
- 信頼できる証明書の DN を、証明書の申請者または所有者として使用することに対する許可または禁止

デフォルトの証明書失効ポリシー

RevocationConstraintRule は、Oracle Application Server Certificate Authority に付属する OracleAS Certificate Authority のデフォルト・ポリシーです。期限切れの証明書の失効を許可または禁止するなど、このポリシーのパラメータおよび条件は、必要に応じて設定できます。

製品に付属の証明書更新ポリシー

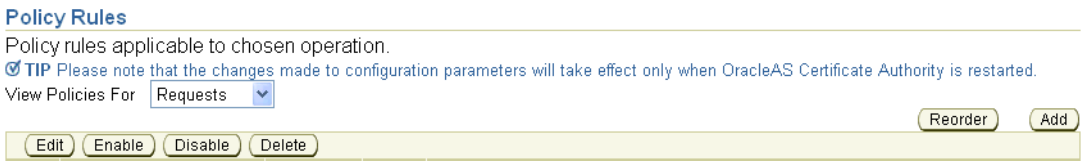
RenewalRequestConstraint ポリシーのパラメータおよびデフォルトを設定できます。このポリシーは、証明書の更新可否、更新するタイミングおよびその期間を設定します。設定された満了日前後の日数を設定して、更新が許可されている範囲内で時間枠を指定します。デフォルトは、満了日の前後 10 日です。デフォルトの更新期間は 365 日ですが、変更もできます。

製品に付属の TrustPointDNCustomRule

TrustPointDNCustomRule は、OracleAS Certificate Authority ポリシー例のサンプル・プラグインであるカスタム・ポリシーであり、OracleAS Certificate Authority に付属しています。このポリシーにより、ユーザー証明書リクエストは、信頼できる証明連鎖の DN の名前で証明書を取得することが不可能になります。このようなプラグインの場合、このポリシーを実装するクラスの説明および名前を設定し、このポリシーを有効にするかどうかをチェック・ボックスで指定します。

ポリシー操作

「ポリシー・ルール」画面には、実行可能な操作のボタンが表示されます。それぞれのボタンについては、「編集」、「有効化または無効化」、「削除」、「ポリシーの並替え」および「ポリシーの追加」の各項で説明します。



編集

ポリシーを選択して「編集」をクリックすると、ポリシーの画面が表示され、現在設定されているパラメータおよび条件が示されます。たとえば、鍵の制約ポリシーの画面では、鍵の最大サイズおよび最小サイズのデフォルトが表示されます。また、特定の証明書タイプでこれらのデフォルトを変更する条件も示されます。

どのページにおいても、デフォルトのパラメータまたは既存の条件に関連付けられた特定の値とは異なる値を選択できます。標準的なポリシーでは、式テキスト・ボックスに入力してこれらの条件を変更したり、「並び替え」ボタンを使用して条件の順序を変更したり、「追加」ボタンを使用して条件を追加することもできます。(「条件の並替え」および「条件の追加」を参照。)

カスタム・ポリシーを選択して「編集」をクリックすると、「カスタム・ポリシー」編集画面が表示されます。通常の編集画面には、デフォルト・ポリシーしか表示されません。

有効化または無効化

ポリシーを作成すると、そのポリシーを有効にできます。これによって、指定した操作（リクエスト、失効または更新）にポリシーが適用されます。有効にしない場合、またはポリシーを作成した際に無効にした場合、ポリシーのパラメータ、デフォルトおよび条件は、どの操作（リクエスト、失効または更新）にも適用されません。

ただし、ポリシーを無効にしても、データベースには使用可能な状態で残ります。後でこのポリシーを有効にすることもできます。

これに対して、ポリシーを削除すると、データベースからも削除されます。まったく別のポリシーとして再度入力しないかぎり、永続的に使用できなくなります。

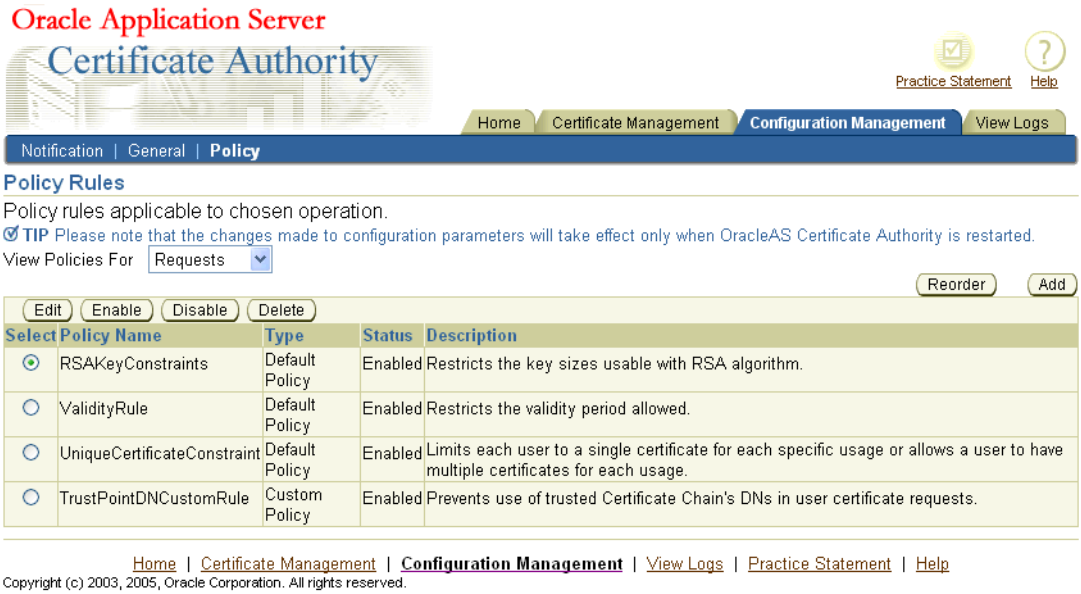
削除

「ポリシー・ルール」ページでは、OracleAS Certificate Authority のデフォルト・ポリシーを削除できません。削除できるのはカスタム・ポリシーのみです。追加したカスタム・ポリシーがリストに表示されるので、ポリシーを選択して「削除」をクリックできます。

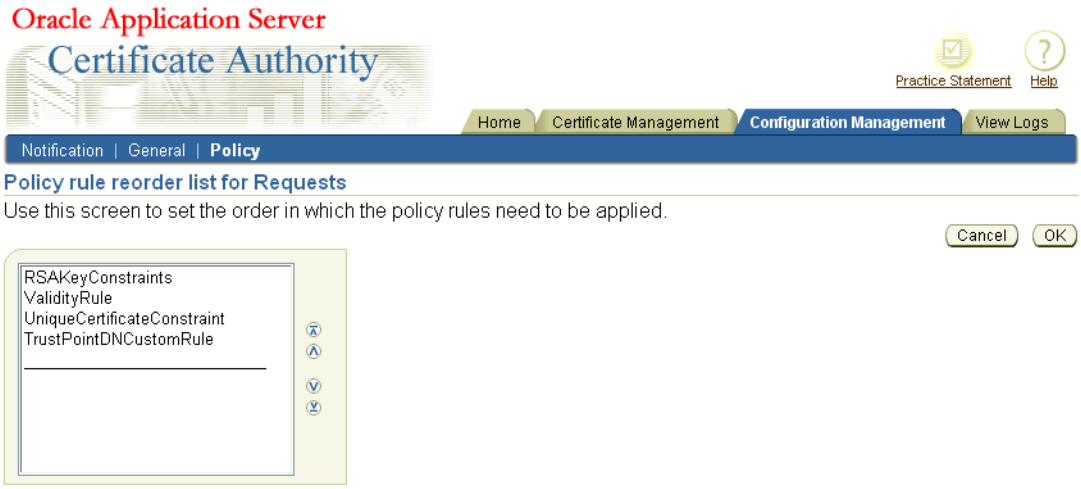
特定のルールに対する「編集」ページで、条件を選択して**「削除」**をクリックできます。すぐにその条件が削除され、削除したことを示す情報メッセージが表示されます。

ポリシーの並替え

管理者は、ポリシーの適用順序を変更できます。たとえば、証明書リクエストのデフォルト・ポリシーが、次に示す順序で表示されているとします。

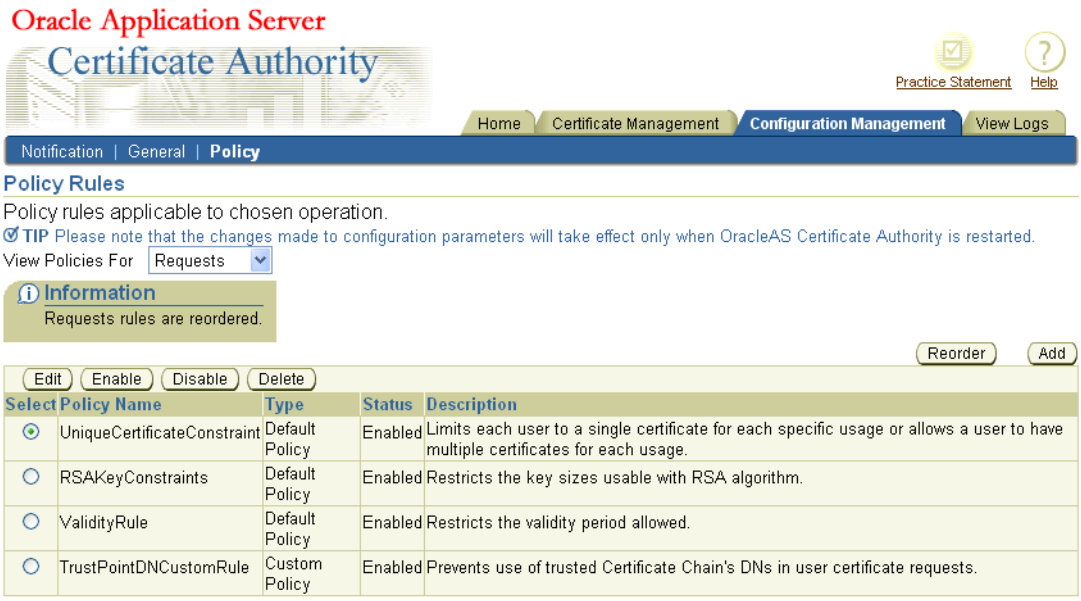


「**並び替え**」をクリックすると、既存のポリシーのリストが表示されます。次の画面で、ポリシーを選択して並び替え、目的の順序になるように変更します。



UniqueCertificateConstraint ポリシーを 2 つ上に移動するには、このポリシーをクリックして選択し、上矢印のボタンを 2 回クリックします。そうすると、次のような画面になります。

「OK」をクリックすると、次の画面に示すとおり、そのポリシーは、以前の場所ではなく一番上に表示されます。

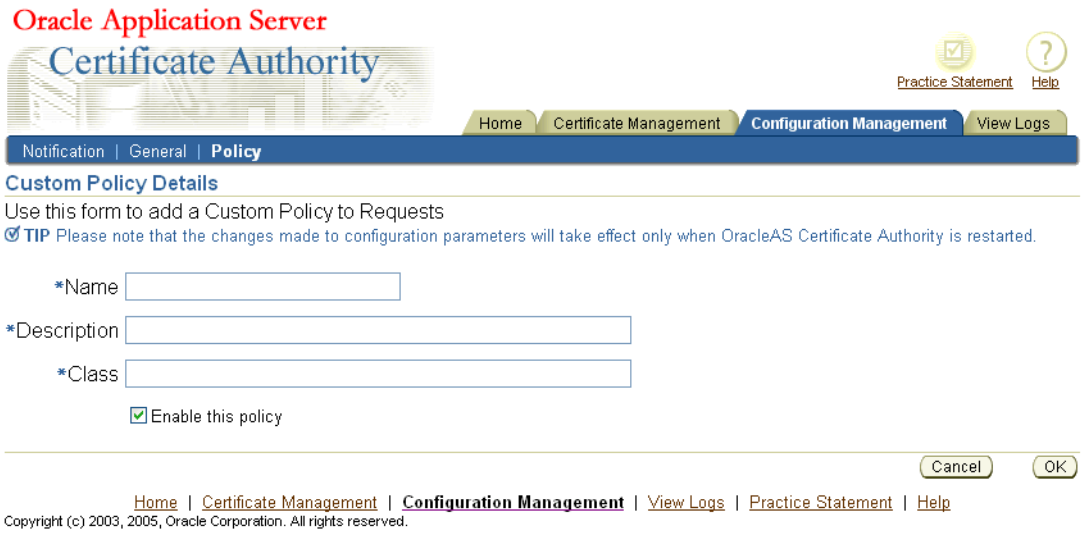


OracleAS Certificate Authority から、変更に対するアラートを示す情報メッセージが表示されます。

ポリシー・ルールに含まれる条件も、同じ方法で並び替えることができます。「条件の並替え」を参照してください。

ポリシーの追加

「ポリシー・ルール」では、**「追加」**ボタンをクリックして、操作（リクエスト、失効または更新）に新しいポリシーを追加できます。`$ORACLE_HOME\oca\policy` ディレクトリに jar として定義し、使用可能にしていたオブジェクト・クラスに具体化されているカスタム・ポリシーのみ追加できます。新しいポリシーの名前、説明およびオブジェクト・クラスを入力し、有効にするかどうかを指定するフォームが表示されます。カスタム・ポリシーの開発の詳細は、「カスタム・ポリシー・プラグインの開発」を参照してください。



詳細は、6-22 ページの「カスタム・ポリシー・プラグインの開発」を参照してください。

また、ポリシー・ルールに含まれる条件を、そのポリシーの「編集」ページに表示される任意のデフォルト・ポリシーに追加できます。（カスタム・ポリシーには条件を追加できません。）「条件の追加」を参照してください。

ポリシー・ルールの条件

「ポリシー管理の概要」に説明するように、ポリシー・ルールは、特定の規則に従って指定および施行されます。この項では、ポリシー・ルールの条件の使用について説明します。また、次の項で、例を示します。

- 「複数の条件による評価」（次の項で構成されます。）
  - 複数の条件による評価の例
  - 複数の条件による評価の例 2
  - 条件の並替え
  - 条件の追加

注意： ポリシー・ルールは、複数のタイプのリクエスト（証明書の発行、失効または更新のリクエスト）で共有することはできません。

条件には、受信した証明書リクエストの検証に使用する特定の値および式を指定します。指定した値は、条件式が証明書リクエストの対応する要素と一致する場合に、ポリシーのデフォルトのかわりに使用されます。一致する場合は、その条件式に関連付けられた値を使用して、リクエストの妥当性が評価され、ポリシーのデフォルト値のかわりにパラメータが設定されます。

条件の指定は任意です。また、条件はカスタム・ポリシーには使用できません。

デフォルト・ポリシーに含まれるルールに対しては、Web ベースのインタフェースから条件を指定できます。条件の指定後は、ポリシーを適用する特定の証明書操作（リクエスト、失効、更新など）のすべての受信リクエストに対して、指定した条件が照合されます。

受信した証明書または証明書リクエストがどの条件式とも一致しない場合、またはルールに条件がない場合は、ポリシーに指定されたデフォルトの値、範囲またはアクションを使用して、リクエストが評価されます。たとえば、リクエストの値は、ポリシーに指定された適切なデフォルトの範囲内にあるかどうかが検証されます。範囲内の場合、リクエストは許可されます。値が、指定されたデフォルトと一致しない場合、または指定された範囲内にない場合は、内容を記したエラー・メッセージが表示され、リクエストが拒否されます。

受信した証明書または証明書リクエストが、条件で指定したタイプと一致した場合、ルールのデフォルトまたは範囲は、その証明書または証明書リクエストに適用されません。適用できるのは、その条件に対応するものとして指定した値だけです。

このように、管理者は、デフォルト・ポリシーのルールを拡張し、様々なユーザー用に構成することができます。たとえば、Sales 部門に設定した有効期間より長い有効期間を、Development 部門に設定することができます。

条件式は論理式です。変数および関係演算子を使用して式を作成します。たとえば、条件を設定し、様々なグループのユーザーの証明書に対して、異なる有効期間を設定することができます。

次に、有効な条件式の例を示します。

```
Type==client AND DN=="ou=Sales,o=oracle,c=us"
Type==server AND DN=="o=Oracle,c=us"
```

表 6-8 に、条件式に使用する論理演算子を示します。

表 6-8 論理演算子

演算子	説明
==	等しい
!=	等しくない
AND	論理演算子 AND

次のルールでは、デリミタ「:=」を使用して、ポリシーの式の名前とその有効な構文を区切ります。ポリシーの式を構成する際に有効な構文を示します。

```
Predicate expression := Expression | AndExpression

AndExpression := Expression AND Expression

Expression := Attribute op Value

Attribute :=  <attrib_name>

op:    ==  or    !=

Value :=  a string
```

OracleAS Certificate Authority では、OR、<、> などの演算子はサポートしていません。条件を複数の条件に分割して同じ値を指定することにより、OR 論理式を実装できます。（ポリシー・プラグインおよび API は、複数の条件をサポートします。）条件では、二重引用符で囲んだ文字列を値に指定できます。属性は、常に <attrib_name> として指定します。すべての条件式および文字列の値では、大文字と小文字が区別されません。式の値に「"*"」を設定して、対象となるすべての属性と照合することができます。たとえば、「type=="*"」と指定すると、すべての証明書タイプが一致します。ただし、「"*"」を他の文字列とともに使用した文字列の部分一致はサポートされていません。

表 6-9 に、属性および指定可能な値を示します。

表 6-9 条件の属性

属性	変数名	説明
type	type	証明書タイプを指定します。指定可能な値は、次のとおりです。 ■ type=="client" ■ type=="server" ■ type=="ca "
usage	usage	証明書の使用方法を指定します。使用可能な値は引用符で囲んだ整数 1 ～ 9 であり、暗号化、署名および認証の一部または全部の機能、コード署名、証明書署名を表します。 ■ usage=="1": 暗号化 ■ usage=="2": 署名 ■ usage=="3": 署名、暗号化 ■ usage=="4": 認証 ■ usage=="5": 認証、暗号化 ■ usage=="6": 認証、署名 ■ usage=="7": 認証、署名、暗号化 ■ usage=="8": コード署名 ■ usage=="9": 証明書（CA）署名

表 6-9 条件の属性（続き）

属性	変数名	説明
DN	DN	識別名を指定します。有効なパラメータは、有効な部分 DN または完全 DN です。（DN エントリは、連続して指定する必要があります。「C=」エントリまで完全に指定する必要がありますが、「CN」で始める必要はありません。）

RFC1779 に指定されるように、OracleAS Certificate Authority では、最大の構成要素を末尾に指定した DN を使用します。たとえば、適切な書式で記述された DN「cn=user31415,ou=security,ou=ST,o=Oracle,c=US」では、「cn」は最小の構成要素で、「c」は最大の構成要素です。DN フィールドと DN フィールドは、カンマで区切る必要があります。

RDN とは、相対識別名（Relative Distinguished Name）の略語で、エントリを一意に指定するうえでこれ以上の修飾を必要としない、最も詳細なローカル・エントリ名を意味します。RDN が複数回出現する場合は、最初に指定された最小の RDN が、次に出現する RDN の子として判断されます。前述の例では、「ou=security」が「ou=ST」の前に出現するため、「security」は「ST」に従属する単位と判断されます。

条件で指定する DN は、どの RDN からでも始めることができますが、ルートまで完全に指定する必要があります。たとえば、「ou=ST,o=Oracle,c=US」は場所を指定する有効な部分 DN ですが、「ou=ST,o=Oracle」は「o=Oracle」で終わり、ルート（たとえば「c=US」）が含まれていないため、無効な部分 DN です。

ビッグ・エンディアン（最大の構成要素を最初に指定）の順序をサポートするために、OracleAS Certificate Authority は、ポリシーの評価のためのみに、DN を照合する前に内部的にリトル・エンディアンの順序に変換します。

DN の構成要素を、条件式に指定した DN の式と照合する場合、次のルールが適用されます。

条件は、条件全体が DN の最後の部分と一致するかどうかを照合します。

たとえば、次の条件式があるとします。

```
DN=="ou=ST,o=Oracle,c=US"
```

この条件式は、次のすべての DN と一致します。

```
"cn=user31415,ou=ST,o=Oracle,c=US"

"cn=quser2787,ou=security,ou=ST,o=Oracle,c=US"

"cn=kuser987,ou=security, ou=DAS,ou=ST,o=Oracle,c=US"
```

ただし、条件式は次の DN とは一致しません。

```
"cn=user31415,ou=DAS,ou=ST,o=Oracle,c=IN"

"cn=quser2787,ou=ST, ou=pki, o=Oracle,c=US"

"cn=kuser987,ou=ST,o=Oracle, st=CA,c=US"
```

複数の条件による評価

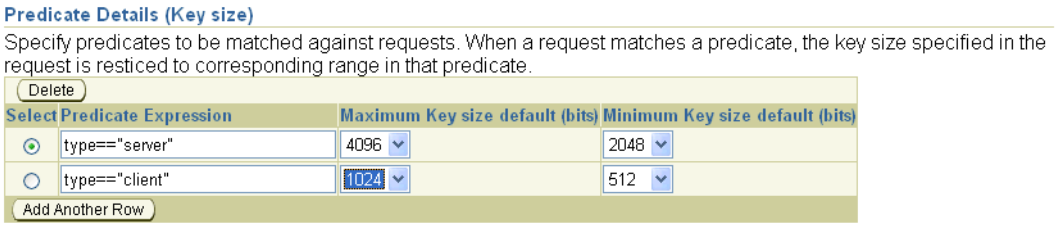
ポリシー・ルールには、複数の条件を指定できます。ポリシー・ルールに複数の条件が指定されている場合は、最初の条件式と受信した証明書リクエストのオブジェクトの比較から、評価が開始されます。一致する場合は、ルールが適用されます。一致しない場合は、次の条件式とリクエストを比較して評価されます。この処理は、条件が証明書リクエスト・オブジェクトと一致するまで、または照合する条件がなくなるまで続行され、照合する条件がない場合は、ポリシー・ルールのデフォルト値が適用されます。

最適な一致の検出は試行されず、最初に一致したものが使用されます。管理者は、組織に最適な順序で条件を指定する必要があります。

ある基準をルールの最上位に指定し、その条件式が特定の照合および最小の RDN を対象とする場合は、その条件式が最初に評価されます。

複数の条件による評価の例

次の例では、ルールによって、複数の条件がどのように評価されるかを示します。この例は、RSA ルールが使用する鍵のサイズのポリシー・ルールです。ルールには、サーバー証明書およびクライアント証明書についての 2 つの条件式が含まれます。条件式には、対応する最小および最大の鍵のサイズが指定されています。受信したサーバー証明書リクエストまたはクライアント証明書リクエストで指定された鍵のサイズが、対応する条件で指定した範囲外の場合、そのリクエストはルールによって拒否されます。



どちらの条件式も、受信した証明書リクエストと一致しない場合は、リクエストされた鍵のサイズが、デフォルトとして指定されている最小および最大の鍵のサイズと比較されます。リクエストされた鍵のサイズが範囲外の場合は、リクエストは拒否されます。範囲内の場合は承認されます。（実際の出荷時デフォルト範囲は、512 ～ 4096 です。管理者が Microsoft Strong Cryptographic Provider を選択した場合、生成される鍵のデフォルト・サイズは通常、1024 になります。ただし、一部の Windows 環境では、Microsoft Strong Cryptographic Provider を選択すると、4096 ビットの鍵が作成されます。）

複数の条件による評価の例 2

複数の条件を使用すると、微細な評価ができます。条件は、Oracle Application Server Certificate Authority の Web ベースのインタフェースの「構成管理」タブにある「編集」ページのリストに従って、上から順に適用されます。順序は重要です。

ポリシーの最初の条件に「`Type=="client"`」、「`OU=="Oracle"`」および「`CN=="Clay"`」と指定され、鍵の長さが 2048 に設定されているとします。

次に、同じポリシーの後続の条件に「`Type=="client"`」および「`OU=="Oracle"`」と指定され、鍵の長さが 512 に設定されているとします。

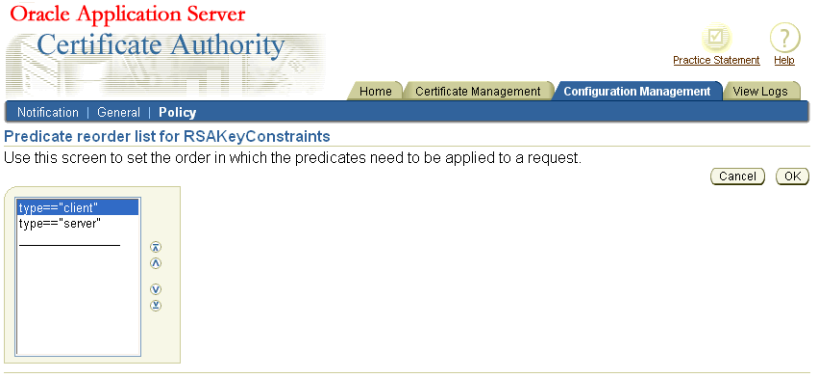
この場合、鍵の長さが 2048 に設定されるのは、Clay からのクライアント・リクエストだけで、他のすべての Oracle クライアント・リクエストの鍵の長さは 512 に設定されます。

ただし、順序が逆の場合はポリシー内で一般的な条件が先になるので、Clay の鍵の長さも 512 に設定されます。順序の中で 1 つ上の条件（より一般的な条件）のみがこのポリシーの対象となるため、より限定的な条件は適用されません。

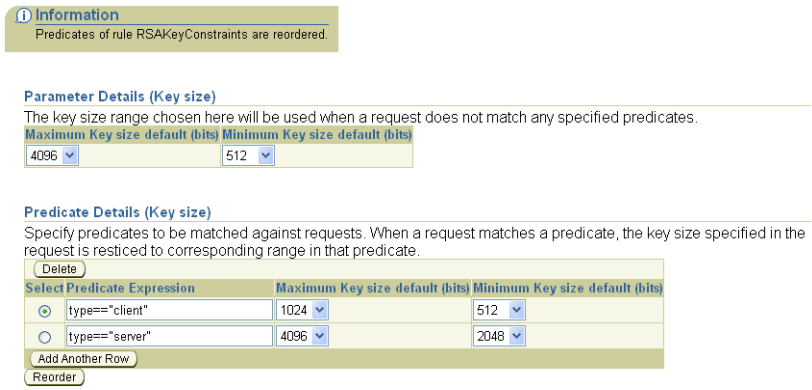
条件の並替え

条件の並替えは、ポリシーの並替えと同じ方法で変更できます（6-13 ページの「ポリシーの並替え」を参照）。「複数の条件による評価の例」に登場するページのように、条件を表示するページで**「並替え」**をクリックすると、次のような画面が表示されます。

移動する条件をクリックして選択し、いずれかの矢印ボタンをクリックします。条件は、選択した方向に移動します。たとえば、「複数の条件による評価の例」に示された条件の順序を逆にすると、次のような画面が表示されます。



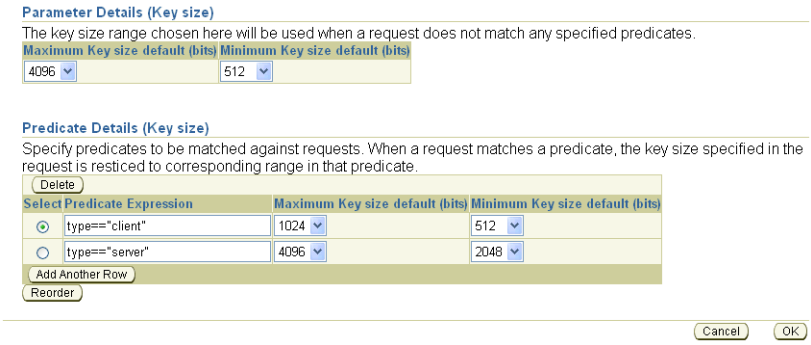
「OK」をクリックすると、次に示すとおり、ルールに対する条件の順序が決定します。



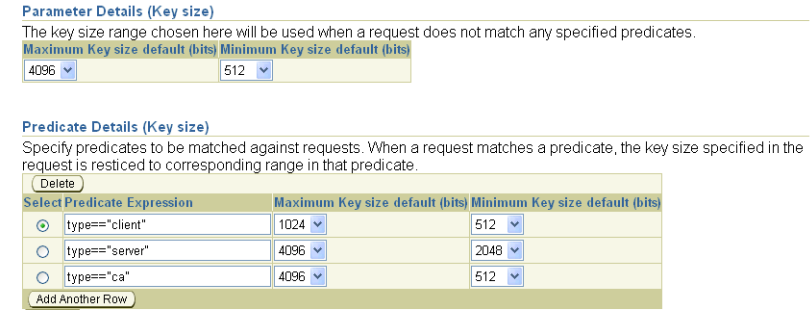
OracleAS Certificate Authority から、順序が変更されたことを知らせる情報メッセージが表示されます。

条件の追加

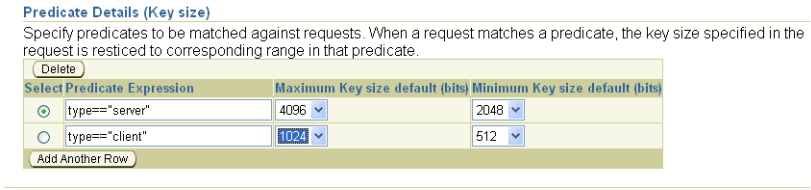
条件を表示するページで**「行の追加」**をクリックすると、条件を追加できます。空の入力行が表示されます。



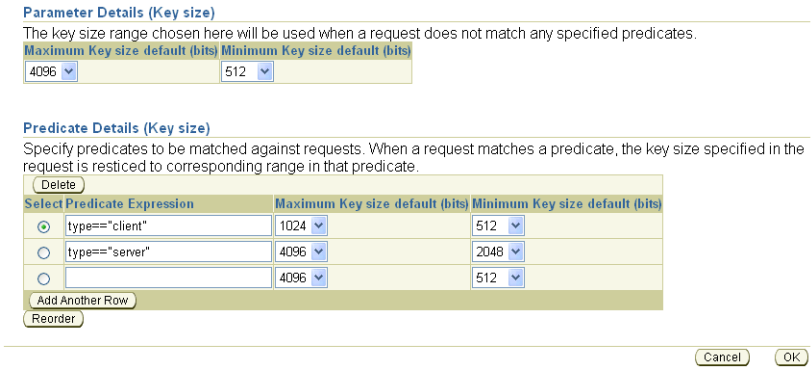
この画面に示すように、空の行に有効な式を入力して**「OK」**を押すと、その式が受け入れられ、ポリシーのメイン・ページに戻ります。



特定のポリシーの「編集」ページで「1 行追加」をクリックすると、条件を追加できます。次の画面に示す条件の例では、サーバー証明書のリクエストには、エンド・ユーザーの証明書リクエストよりも、大きいサイズの鍵を使用する必要があります。



「行の追加」をクリックすると、条件を指定する空の行が追加表示されます。この行の「述語式」ボックスに新しい条件を入力できます。条件が一致するときに使用する機能またはデフォルトのパラメータ範囲も指定します。



無効な条件またはこのルールにすでに存在するルールを指定すると、エラー・メッセージが表示されます。

必要な条件の指定が完了したら、「**OK**」をクリックします。このルールの元のページが、新しい条件の式が一番下に追加された状態で表示されます。

カスタム・ポリシー・プラグインの開発

OracleAS Certificate Authority に付属のデフォルトのポリシー・プラグインは汎用のプラグインです。組織の具体的な要件にあわせてポリシーの構造を拡張するために、管理者は、OracleAS Certificate Authority が提供するフレームワークを使用してカスタム・プラグインを作成できます。このフレームワークには、証明書と証明書リクエストの情報を取得するための API、およびいくつかの汎用的な機能が含まれます。カスタム・プラグインを実装するために、管理者は、Java クラスを作成し、OracleAS Certificate Authority に登録する必要があります。これを「ポリシーの追加」と呼びます。

次のような状況に対処する場合は、カスタム・プラグインを開発することをお薦めします。

- 企業の追加アカウント・リポジトリを使用して、ユーザーのリクエストを検証する場合
- 他のユーザー・リポジトリに基づいて追加のフィールドを設定する場合

OracleAS Certificate Authority が提供する API を使用すると、管理者のカスタム・プラグインで、リクエストのパラメータ、および証明書と証明書リクエストの属性を取得できます。

> **関連資料：** Oracle Application Server Certificate Authority に付属の Javadoc

次の項では、管理者がカスタム・プラグインを開発する際に役立つツールおよび例について説明します。

- ポリシーにより実行される処理について
- 新しいポリシー・プラグインを作成する手順
- カスタム・ポリシーのルール
- カスタム・ポリシー・プラグインの例
- 汎用エラー・メッセージ

ポリシーにより実行される処理について

カスタム・プラグインは、OCACustomPolicyPlugin インタフェースを実装することで記述できます。このインタフェースの enforce メソッドに渡される OCAPolicyRequest オブジェクトには、（証明書および証明書リクエストの）重要な属性とその値セットがすべて含まれています。カスタム・プラグインは、このオブジェクトを読み取り、証明書リクエストまたは証明書の属性を取得または設定できます。

カスタム・ポリシー・プラグインでは、次の手順で処理が実行されます。

表 6-10 カスタム・ポリシー・プラグインの処理手順

手順	結果
OracleAS Certificate Authority カスタム・プラグインの enforce メソッドが、ポリシー・プロセッサから OCAPolicyRequest を受け取る。	登録、更新または失効のリクエストで設定された実際のパラメータ値の取得に必要なオブジェクトが、自動的に取得されます。これらのパラメータには、DN、有効期間、シリアル番号などがあります。
OCAPolicyRequest から取得したパラメータと、プラグインの想定するパラメータ値をプラグインが検証する。	ポリシーが正常に検証された場合は、setPluginResult メソッドを使用してプラグインの結果が設定され、ポリシー・プロセッサに TRUE が返されます。正常に検証できなかった場合は、setError() を使用してエラーが設定され、ポリシー・プロセッサに FALSE が返されます。

新しいポリシー・プラグインを作成する手順

新しいポリシー・プラグインを作成するには、次の手順を使用します。

1. 次の項に示すサンプル実装を参考にして、`OCACustomPlugin` インタフェースを実装する Java クラスを記述します。
2. 手順 1 で実装した Java クラスを保存します。次に、Java の `CLASSPATH` に `$ORACLE_HOME/oca/lib/oca-1_3.jar` を追加して、クラス・ファイルを取得してから、保存したクラスをコンパイルします。
3. **jar** ユーティリティを使用して、クラス・ファイルから jar ファイルを生成します。
   a. たとえば、前の項のコードから `jar` ファイルが生成され、`example.jar` に格納されます。

      クラスから jar ファイルを生成するには、`$ORACLE_HOME/jdk/bin` ディレクトリにある `jar` ユーティリティを使用します。

      * `example.jar` を作成するには、次を実行します。

        ```
        $ORACLE_HOME/jdk/bin/jar cvf example.jar oca
        ```

      * ここで、`example.jar` は jar ファイルの名前で、OracleAS Certificate Authority は `custom/policy/plugin/examplePlugin.class` を格納するパッケージ・ディレクトリです。

   b. `jar tvf example.jar` を実行すると、`oca/custom/policy/plugin` というディレクトリ構造の下に、`examplePlugin.class` ファイルが置かれます。
4. この `jar` ファイルを `$ORACLE_HOME/oca/policy` ディレクトリに配置します。（Windows プラットフォームの場合は、次のようにスラッシュが円記号になります。）

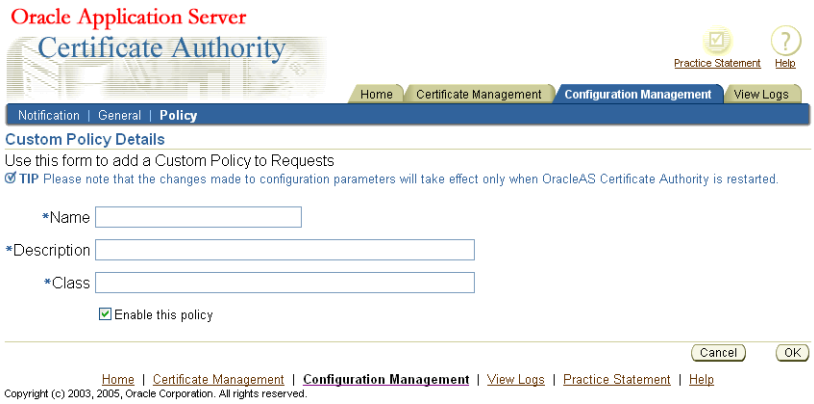
   ```
   $ORACLE_HOME¥oca¥policy¥
   ```

   このディレクトリは、Oracle Application Server Certificate Authority によって事前に作成されています。
5. OracleAS Certificate Authority、OracleAS Certificate Authority の OC4J および OHS を停止します。`ORACLE_HOME` で次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   $ORACLE_HOME/opmn/bin/opmnctl stopproc type=oc4j instancename=oca
   $ORACLE_HOME/opmn/bin/opmnctl stopproc type=ohs
   ```

6. OHS、OracleAS Certificate Authority の OC4J および OracleAS Certificate Authority を、この順で起動します。同種のコマンドを使用します。

```
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
$ORACLE_HOME/opmn/bin/opmnctl startproc type= oc4j instancename=oca
$ORACLE_HOME/oca/bin/ocactl start
```



7. OracleAS Certificate Authority Administrator 管理者の Web ベースのインタフェースを使用して、カスタム・ポリシーを追加し、新しいルールを定義します。

   「構成管理」の「ポリシー」サブタブ内にある「ポリシー・ルール」ページに移動して、「追加」ボタンをクリックし、フィールドに必要事項を入力します。カスタム・ポリシーの名前、説明およびクラスを指定します。「有効化」チェック・ボックスを選択してポリシーを有効にし、「OK」をクリックします。

8. 第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」の「Oracle Application Server Certificate Authority の起動および停止」の説明に従い、OracleAS Certificate Authority を再起動します。新しい jar ファイルが検出および認識され、そのルールが有効になるには、OracleAS Certificate Authority を再起動する必要があります。この手順が完了したら、プラグインの追加により変更された項目に応じて、証明書、更新または失効のリクエストにカスタム・ポリシーが適用されます。

カスタム・ポリシーのルール

カスタム・ポリシーのプラグインを開発するときは、次の基本原則に注意してください。

- ポリシー名に空白がないようにしてください。
- 指定したディレクトリにクラスが存在していることを確認してください。
- クラスに特定のインタフェースが実装されている必要があります。

カスタム・ポリシー・プラグインの例

カスタム・ポリシー・プラグインを記述するには、OCACustomPolicyplugin インタフェースを実装する必要があります。

独自のポリシー・プラグインを用意するための最初の手順は、新しい Java クラスの作成です。

この項では、証明書リクエストの国コードが US でないことを確認するカスタム・ポリシー・プラグインの例を紹介します。

```
1:    package oca.custom.policy.plugin;
2:    import oracle.security.oca.exception.OCMException;
3:    import oracle.security.oca.policy.custom.OCACustomPolicyplugin;
4:    import oracle.security.oca.policy.OCAPolicyRequest;
5:    import oracle.security.oca.policy.OCMPolicyConstants;
6:    public class PolicyCustomPlugin implements OCACustomPolicyPlugin
7:    {                                  // ends at line 35
8:       public boolean enforce (OCAPolicyRequest policyRequest)
9:       {                          // ends at line 34
10:      // Add the functionality here.
11:      // Assume the plug-in should reject all requests with country code as US.
12:              if (!policyRequest.getCountry().equals("US"))
13:              {
14:                     //Plug-in check succeeded. Country ID in request is not US.
15:                       //Hence return true.
16:                       return true;
17:               }
18:               else
19:               {                   // ends at line 33
20:                      //Plug-in check failed: Country ID in request is US. Set
error and return false.
21:    try
22:    {
23:
policyRequest.setError("PolicyCustomPlugin",OCMPolicyConstants.POLICY_ERROR,
                                                    "Country ID cannot be US.");
24:                     //The first parameter is the plug-in name.
25:                    //The second parameter is the status, which is an ERROR.
26:                   //The third parameter is the Message to be displayed.
27:     }
28:   catch(OCMException e)
29:  {
30:     //enter exception handling here
31:   }
32:                       return false;
33:               }
34:        }
35:    }
```

この例で、行 1 は、このカスタム・ポリシー・プラグインが入っているパッケージです。カスタム・ポリシー・プラグインは、頭文字が oracle.security.oca 以外のパッケージに入れることができます。

行 2 ～ 5 は、必要なクラス・ファイルをインポートします。これらのファイルの詳細は、Javadoc API のドキュメントを参照してください。

行 6 は、OCACustomPolicyPlugin インタフェースを実装します。このカスタム・ポリシー・インタフェースは、すべてのカスタム・プラグインで実装する必要があります。OracleAS Certificate Authority が提供するインタフェースは、パッケージ oracle.security.oca.policy.custom に入っていて、`$ORACLE_HOME/oca/lib/oca-1_3.jar` にあります。

行 8 は、このプラグインの機能を格納するメソッドを実装します。ポリシー・プロセッサがこのプラグインを起動すると、enforce メソッドが起動されます。

行 9 ～ 28 は、このプラグインの機能を開始します。

行 12 は、国コードが US でないか確認します。policyRequest で使用できるメソッドの詳細は、OracleAS Certificate Authority に付属する API ドキュメントを参照してください。

行 16 は、ポリシー・プロセッサに成功を返します。

行 18 は、リクエストの国コードが US のときに発生するエラー状態の処理を定めます。

行 23 は、policyRequest にエラー・コードを設定します。このエラー・コードはポリシー・プロセッサにより読み取られ、画面にレンダリングされます。新しい OracleAS Single Sign-On ユーザー証明書を取得し、すぐに証明書の更新を試みると、同じようなエラーが表示されます。更新用のプラグインにより、エラーが生成されます。

行 30 は、例外を処理するコードに置き換えてください。

行 32 は、ポリシー・プロセッサにエラー・ステータスを返し、リクエストがポリシー・チェックに失敗したため処理されないことを示します。

汎用エラー・メッセージ

次に示すのは、汎用エラー・メッセージとそれに関連付けられた定数です。これは、ポリシーの適用中にエラーが検出された場合に設定できます。これらのメッセージは、OracleAS Certificate Authority がサポートする各言語に変換され、次のような 3 つの内容が表されます。

- 有効期間が無効

  "OCA_POLICY_INVALID_VALIDITY"

- リクエストされた有効期間が CA 証明書の有効期間を超過

  "OCA_POLICY_INVALID_VALIDITY_CA"

- 識別名が無効

  "OCA_POLICY_INVALID_DN"

たとえば、前述のカスタム・ポリシーの例で、行 13 を次のように変更したとします。

```
13:
policyRequest.setError("examplePlug-in",OCMPolicyConstants.POLICY_ERROR,
OCAPolicyMessage.OCA_POLICY_INVALID_DN);
```

この場合、「無効な識別名です。」というエラーが出力に表示されます。

関連資料： OracleAS Certificate Authority カスタム・プラグインに用意されているクラスとメソッド、および使用できる定数の説明は、他のドキュメントに付属する Javadoc を参照してください。

注意： OracleAS Certificate Authority がサポートする汎用エラー・メッセージは、OracleAS Certificate Authority がサポートする各言語に変換されるので、カスタム・プラグインでも使用できます。これらの定数を使用すると、OracleAS Certificate Authority がサポートする言語であれば、エラー・メッセージをレンダリングできます。

これらのメッセージを使用しない場合は、あらゆる有効な java 文字列を使用できます。ただし、これらの java 文字列は他の言語に変換されないので、指定された文字列そのままでレンダリングされます。

7

OracleAS Certificate Authority 管理 : 高度なトピック

この章では、Oracle Application Server Certificate Authority の管理機能、高可用性機能およびバックアップとリカバリの手順について、追加のコンテキストおよび詳細を説明します。内容は、次のとおりです。

OracleAS Certificate Authority の Wallet 操作

Wallet は、証明書および信頼できる認証局の証明書のコンテナです。OracleAS Certificate Authority は、Wallet を使用して、これらの必須要素のセキュアな格納およびアクセスを行います。証明書、信頼できる認証局またはパスワードを変更する場合、管理者は整合性とセキュリティを維持しながらそれらを使用できるようにアクションを実行する必要があります。次の項で、そのようなアクションについて説明します。

CA 署名 Wallet の再生成

警告： この操作では CA 署名証明書が再生成されるため、既存の CA 証明書が置換され、既存の CA が発行した証明書がすべて無効になります。このため、この操作を試行する際は、十分に注意する必要があります。既存の CA 証明書および CA が発行したすべての証明書が失われた場合の備えをした上で、操作を行ってください。

OracleAS Certificate Authority をルート認証局（CA）としてインストールすると、CA 署名証明書および CA SSL Wallet も作成されます。CA SMIME Wallet は自動的には生成されないので、管理者が生成する必要があります。CA 鍵が危殆化した場合は、次の項の説明に従い、`ocactl` 管理コマンドライン・ツールを使用して、この証明書および Wallet を再生成できます。

新しい CA 証明書および秘密鍵は OracleAS Certificate Authority リポジトリに格納されます。この秘密鍵は、元の CA のインストール中にリクエストおよび設定されたパスワードによって暗号化されます。以前の CA 署名証明書のエントリ、および以前の CA 署名証明書が発行したその他のすべての証明書は無効になります。

CA SSL Wallet や CA S/MIME Wallet など、その他の重要な Wallet も再生成する必要があります。これらの Wallet を再生成すると、新しいパスワードが要求されます。CA 署名 Wallet を再生成した後、以前の CA が発行した CRL は無効になります。

CA 署名 Wallet を生成するコマンドの例を示します。

```
ocactl generatewallet -type CA
```

このコマンドを実行するには、OracleAS Certificate Authority を停止する必要があります。また、この処理には数分かかる場合があります。OCA の再起動の手順は、第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」の「Oracle Application Server Certificate Authority の起動および停止」を参照してください。

CA SSL Wallet および CA S/MIME Wallet の再生成

この項では、CA SSL Wallet および CA S/MIME Wallet の再生成について、個々に説明します。

CA SSL Wallet

CA SSL Wallet はインストール時に生成され、これを使用すると、Oracle Application Server Certificate Authority エンジンが HTTPS モードでリスニングできるようになります。状況によっては、OracleAS Certificate Authority サーバーとのセキュアな通信を確立するために、CA SSL Wallet および CA S/MIME Wallet の再生成が必要になります。こうした状況には、Wallet が危殆化または破壊された場合、CA 署名 Wallet が再生成された場合、新しい下位 CA 証明書がインストールされた場合などがあります。

CA SSL Wallet を生成するコマンドの例を示します。

```
ocactl generatewallet -type CASSL
```

このコマンドを実行する場合は、OracleAS Certificate Authority の OC4J および OHS をすべて停止する必要があります。このコマンドを実行した後で、OHS、OC4J および OracleAS Certificate Authority をこの順序で再起動します。

この Wallet は、ディレクトリ `$ORACLE_HOME/oca/wallet/ssl` に ewallet.p12（PKCS #12）として格納され、生成時に指定したパスワードによって暗号化されます。また、このコマンドでは OracleAS Single Sign-On 形式の CA SSL Wallet も生成され、`$ORACLE_HOME/oca/wallet/ssl`. に cwallet.sso として格納されます。

cwallet.sso を使用するメリットは、Oracle HTTP Server の管理者が、Wallet のパスワードを指定しなくても、HTTP Server を SSL モードで起動できることです。通常、このパスワードは、PKCS #12 Wallet を使用して HTTP Server を SSL モードで起動する際にリクエストされます。

OracleAS Single Sign-On Server 形式の Wallet は暗号化されており、ユーザーは、ファイルを開いたり鍵を抽出することができません。ただし、この Wallet は所有者権限のみで作成されるため、Wallet を保護するには、オペレーティング・システムのファイル権限が必要です。次回、OPMN で OracleAS Certificate Authority インスタンスを起動したときに、SSL サーバー認証でこの Wallet が使用されます。（CA SSL Wallet および OracleAS Single Sign-On Wallet の生成後、OPMN `stopall` コマンドおよび `startall` コマンドが要求されます。）

CA S/MIME Wallet

CA S/MIME Wallet を使用すると、OracleAS Certificate Authority はアラート・メッセージおよび通知メッセージに署名できます。OracleAS Certificate Authority 管理ページの「構成管理」の「通知」サブタブで、「SMIME 電子メールの送信」を選択する前に、CA S/MIME Wallet を生成する必要があります。生成後、この Wallet は OracleAS Certificate Authority データベース・リポジトリ内に置かれます。

> **関連項目：** 第 5 章「Oracle Application Server Certificate Authority の構成」の「メール詳細」

この S/MIME Wallet が危殆化または破壊された場合、または CA 署名 Wallet が再生成されたときは、CA S/MIME Wallet を再生成する必要があります。この Wallet は、管理者のパスワードによって暗号化されます。パスワードは、この Wallet を生成するコマンドを実行する場合に必要です。また、管理者の識別名および電子メール・アドレスの入力も要求されます。

CA S/MIME Wallet を生成するコマンドの例を示します。

```
ocactl generatewallet -type CASMIME
```

次の手順に従って、CA S/MIME Wallet を生成および使用します。

1. **「構成管理」→「通知」**と選択します。**「SMIME 電子メールの送信」**を選択します。
2. 次のコマンドを使用して、OracleAS Certificate Authority を停止します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   ```

3. 次のコマンドを使用して、CA S/MIME Wallet を生成します。

```
ocactl generatewallet -type CASMIME
```

4. 次のコマンドを使用して、OracleAS Certificate Authority を起動します。

```
$ORACLE_HOME/oca/bin/ocactl start
```

CA S/MIME Wallet を再生成すると、以前の CA S/MIME Wallet は無効になります。新しい CA S/MIME Wallet を使用して、アラート・メッセージおよび通知メッセージに署名します。

重要な Wallet の更新

証明書の満了日が近づくと、Wallet の更新が必要になります。CA 署名 Wallet、CA SSL Wallet および CA S/MIME Wallet は、`ocactl` 管理コマンドライン・ツールを使用して更新できます。`renewcert` コマンドの実行中、`ocactl` から新しい有効期間の入力が求められます。入力値は証明書の更新期間（日数）です。

CA 署名証明書を更新すると、新しい有効期間が設定された新しい証明書が作成され、OracleAS Certificate Authority のメタデータ・リポジトリに格納されます。

CA SSL Wallet を更新すると、`$ORACLE_HOME/oca/wallet/ssl/` に格納されている以前の Wallet ewallet.p12 は、更新された Wallet で上書きされます。また、CA SSL Wallet の更新によって、`$ORACLE_HOME/oca/wallet/ssl/` の cwallet.sso も上書きされます。

CA S/MIME Wallet を更新すると、データベース・リポジトリに格納されている以前の CA S/MIME Wallet は、新しい Wallet で上書きされます。

CA 署名 Wallet を更新するコマンドの例を示します。

```
ocactl renewcert -type CA
```

更新した CA S/MIME Wallet は、OracleAS Certificate Authority を再起動するのみで使用できます。更新した CA Wallet および CA SSL Wallet を有効にするには、第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」の「Oracle Application Server Certificate Authority の起動および停止」の説明に従い、OHS、OracleAS Certificate Authority の OC4J および OracleAS Certificate Authority を、この順序で再起動する必要があります。

パスワードの変更

インストール後、CA、CA SSL、CA S/MIME および DB のパスワードを変更するには、OracleAS Certificate Authority を停止し、`ocactl setpasswd` コマンドを発行した後、OracleAS Certificate Authority を再起動します。

> **関連項目：** `ocactl` の使用方法の詳細は、付録 A「コマンドライン管理」を参照してください。

注意： OracleAS Certificate Authority スキーマのパスワードは、`ocactl setpasswd -type DB` コマンドを実行しないと変更できません。sqlplus などを使用してデータベースに直接アクセスすると、OracleAS Certificate Authority が停止するため、パスワードを変更できません。

これらのコマンドを実行して変更された内容は、次回、OracleAS Certificate Authority を起動したときに有効になります。`ocactl` を使用するたびに、OracleAS Certificate Authority 管理者のパスワードが必要になります。このパスワードが認証されると、コマンドで指定したロール・タイプの新しいパスワードの入力がリクエストされ、パスワード・ストアのパスワードと置換されます。この結果は、OracleAS Certificate Authority 管理者の最新のパスワードを使用して再度暗号化されます。

OracleAS Certificate Authority リポジトリ・パスワードを変更するコマンドの例を示します。

```
ocactl setpasswd -type DB
```

注意： CA SSL Wallet のパスワードを変更した場合は、OHS、OracleAS Certificate Authority の OC4J および OracleAS Certificate Authority を、この順序で再起動する必要があります。ただし、OracleAS Certificate Authority が cwallet.sso を使用するデフォルトのインストール・シナリオの場合、OHS の再起動は必要ありません。

OracleAS Certificate Authority の構成操作

OracleAS Certificate Authority の管理者は、OracleAS Certificate Authority を使用する現場のニーズを満たすように、OracleAS Certificate Authority を構成する必要があります。これらの操作の一部は、Web ベースのインタフェースを介して行います。その他の操作では、`ocactl` など、OracleAS Certificate Authority が依存するコンポーネントを制御する OracleAS Certificate Authority 管理コマンドライン・ツールを使用する必要があります。次の項で、これらの構成操作および、管理者が実行する必要のあるアクションについて説明します。

- 第三者の SSL Wallet を使用するための Oracle HTTP Server の構成
- 認証局の証明書の失効
- OracleAS Certificate Authority Web 管理者証明書の失効
- 画面でのグローバリゼーション・サポートの構成

第三者の SSL Wallet を使用するための Oracle HTTP Server の構成

OracleAS Certificate Authority をインストールすると、自動的に SSL モードで構成されます。ブラウザで、CA 証明書をインストールするまではこのサイトを信頼できないという旨の警告が表示されます。（CA を明示的にインストールするか、またはブラウザで CA エントリを編集することができます。）この警告が表示されないように、OracleAS Certificate Authority 管理者は VeriSign などの既知の CA から OracleAS Certificate Authority サーバーの SSL 証明書を取得できます。

convertwallet コマンドを使用して、SSL サーバーの Wallet（PKCS #12 形式の `ewallet.p12`）を、OracleAS Single Sign-On 形式の Wallet（ファイル名 `cwallet.sso`）に変換します。`cwallet.sso` を使用するメリットは、Wallet のパスワードを指定しなくても、HTTP Server を SSL モードで起動できることです。通常、このパスワードは、PKCS #12 Wallet を使用して HTTP Server を SSL モードで起動する際にリクエストされます。OracleAS Single Sign-On Server 形式の Wallet は暗号化されており、ユーザーはファイルを開いたり鍵を抽出することができません。ただし、この Wallet は所有者権限のみで作成されるため、Wallet を保護するには、オペレーティング・システムのファイル権限が必要です。つまり、convertwallet コマンドを使用すると、OracleAS Single Sign-On Server では、Wallet パスワードを要求することなく、自動的に SSL モードで Web サーバーを起動できます。

既知の CA から Wallet をインストールするには、次の手順を実行します。

1. OracleAS Certificate Authority、OCA の OC4J および OHS を停止します。
2. `$ORACLE_HOME/oca/wallet/ssl` に Wallet をバックアップします。
3. Oracle Wallet Manager を使用して、完全な SSL サーバー Wallet を作成します。
   a. SSL 証明書をリクエストします。
   b. サーバー証明書を発行した第三者 CA の証明書をインストールします。
   c. リクエストしたサーバー証明書をインストールします。
4. OWM を使用して、現行の OracleAS Certificate Authority CA の証明書をトラスト・ポイントとしてこの Wallet にインポートします。

関連資料：『Oracle Advanced Security 管理者ガイド』

5. $ORACLE_HOME/oca/wallet/ssl に Wallet を保存します。

   これで、OCA が発行した証明書は、CA SSL サーバーの証明書であるこの Wallet に対して、クライアントの証明書として信頼されます。

6. 第三者の CA（PKCS #12 形式）から作成された Wallet を、$ORACLE_HOME/oca/wallet/ssl/ewallet.p12 にコピーします。

7. convertwallet -format SSO を実行します。

8. OHS、OracleAS Certificate Authority の OC4J および OracleAS Certificate Authority を、この順序で起動します。

認証局の証明書の失効

CA 署名証明書の失効は、OracleAS Certificate Authority のインストールが機能しなくなり、すでに発行されている証明書が無効になるため、非常に影響が大きい操作です。この失効操作は、CA 鍵が危殆化された場合以外は実行しないでください。この操作を実行すると、新しい認証局をインストールできます。

下位 CA を使用すると、こうしたリスクとコストが軽減されます。階層的な CA 構造では、通常の操作は下位 CA で実行でき、ルート CA は高度にセキュアな場所でオフライン化されるなど特別に保護されます。この方法であれば、オンラインの下位 CA が危殆化した場合でも、それを失効させ、新しい下位 CA を作成して置換することができます。それ以前のすべての操作では、発行済の証明書を引き続き使用できます。

ただし、ルート CA が危殆化した場合は、まったく新しいインフラストラクチャを構築して、元のルート CA に依存するアプリケーションをすべて更新する必要があります。

こうした理由により、CA を階層化して、ルート CA を特別に保護することをお薦めします。

revokecert コマンドを使用すると、ルート認証局または OracleAS Certificate Authority 管理者の証明書を失効させることができます。このコマンドが使用できるのは、OracleAS Certificate Authority サービスが実行されていない場合に限られます。ルート認証局の証明書の失効は、実行中の OracleAS Certificate Authority 操作用に新しい CA 署名証明書をインストールする前に実行する必要があります。

新しい CA をインストールする場合、最初に、既存の CA が発行したすべての証明書を失効させ、証明書失効リストを更新します。新しい CA 署名証明書が生成されるまで、以前の CA が署名したすべての証明書が OracleAS Certificate Authority リポジトリで「無効」のマークが付けられるため、この手順は必須です。

その後、revokecert を使用して、パラメータで理由コードを指定し、以前の CA 署名 Wallet を失効させます。CA 署名証明書が失効になると、CA が発行したすべての証明書を失効させていない場合は、それらは一貫性のない状態になります。

OracleAS Certificate Authority 管理者の証明書を失効させると、新しい証明書を取得するまで、管理者は、Web 上のすべての管理機能にアクセスできません。管理者が管理ホームページを開くと、新しい管理者の証明書を取得するために、新規登録が要求されます。

鍵が危殆化された場合に、CA 証明書を失効させるコマンドの例を示します。

```
ocactl revokecert -type CA -reason KEY_COMPROMISE
```

CA 証明書を失効させ、OracleAS Certificate Authority を再起動するには、次の手順を実行します。

1. OracleAS Certificate Authority を停止します。次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   ```

2. 前述のコマンドを使用して、CA 署名 Wallet を失効させます。

3. CA SSL Wallet を再生成します。

4. OracleAS Certificate Authority を起動します。次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl start
   ```

OracleAS Certificate Authority Web 管理者証明書の失効

管理者の証明書を置換する必要が発生する場合があります。その原因には、秘密鍵のパスワードの紛失、秘密鍵の危殆化または盗難、新しい人間への管理者ロールの付与などがあります。この失効操作を実行するのは、Web 管理者の鍵が危殆化された場合のみです。この操作によって新しい OracleAS Certificate Authority Web 管理者を登録できます。

管理者の証明書を置換するには、サーバーを停止し、現行の管理者証明書を失効させて、サーバーを再起動する必要があります。これらのタスクは、サーバーのコマンドライン・ツール `ocactl` および OracleAS Certificate Authority のコマンドライン・ツールを使用して実行します。このツールには OracleAS Certificate Authority 管理者のパスワードが必要です。

OracleAS Certificate Authority 管理者の証明書を失効させると、新しい証明書を取得するまで、管理者は、Web 上のすべての管理機能にアクセスできません。管理者が管理ホームページを開くと、新しい管理者の証明書を取得するために、新規登録が要求されます。

次に、管理者は、OracleAS Certificate Authority の Web ページにナビゲートし、OracleAS Certificate Authority Web 管理者の登録フォームに必要事項を入力します。

鍵が危殆化された場合に、Web 管理者の Wallet を失効させるコマンドの例を示します。

```
ocactl revokecert -type WEBADMIN -reason KEY_COMPROMISE
```

Web 管理者の証明書を失効させ、OCA を再起動するには、次の手順を実行します。

1. OracleAS Certificate Authority を停止します。次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   ```

2. 次のコマンドを使用して、Web 管理者の証明書を失効させます。

   ```
   ocactl revokecert -type WEBADMIN -reason <REASON>
   ```

3. OracleAS Certificate Authority を起動します。次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl start
   ```

注意： Web 管理者の証明書は失効したため、この証明書を使用して OracleAS Certificate Authority の Web インタフェースにログインすることはできません。OracleAS Certificate Authority Web インタフェースをオープンする前に、ブラウザ証明書ストアから Web 管理者の証明書を削除する必要があります。これで、OCA の Web インタフェースを表示し、新たに管理者として登録できるようになります。

画面でのグローバリゼーション・サポートの構成

次の条件を満たす場合は、OracleAS Certificate Authority の管理者用画面およびユーザー用画面を、クライアントまたはサーバーの言語で表示できます。

1. データベースのキャラクタ・セットは UTF8 である必要があります。
2. OracleAS Certificate Authority の UI およびオンライン・ヘルプは、日付と同様、クライアントのロケールへの翻訳が行われます。（時刻は、サーバーのタイムゾーンに変換されます。）クライアントのロケールがサポートされない場合は、画面はサーバーのロケールでレンダリングされます。サーバーのロケール言語も OracleAS Certificate Authority によりサポートされない場合は、英語が使用されます。
3. 認証局運用規定は、管理者が認証局運用規定の編集に使用したロケールでレンダリングされ、クライアントのロケールには左右されません。
4. ocactl が提供するグローバリゼーション・サポートは、サーバーのロケールによって決まります。サーバーのロケールが OracleAS Certificate Authority のサポート対象言語でない場合、表示は英語になります。
5. どのロケールでも、実際の ocactl コマンド自体は英語です。

6. アラート、通知、エラー・メッセージなどの情報メッセージは、サーバーのロケールの言語で表示されます。サーバーとクライアントでロケールの言語が異なる場合でも、クライアントの言語では表示されません。たとえば、OracleAS Certificate Authority のインストール先サーバーのロケールの言語が英語のときに、クライアントから日本語でリクエストが送信された場合、通知は英語で出力されます。

   アラートまたは通知のカスタマイズにテンプレートを使用する場合（これについては次の項で説明）、テンプレートの編集に使用した言語が使用されます。メッセージの本文はサーバーのロケールの言語でエンコードされるため、テンプレートの編集はサーバーの言語で行うことをお薦めします。

   テンプレートを使用しない場合、アラートと通知はすべて、サーバーのロケールの言語で表示されます。

OracleAS Certificate Authority のパフォーマンス・チューニング

次の項で説明されているように、データベース、Single Sign-On およびメモリーに対するカスタマイズ可能なパラメータを設定することにより、OracleAS Certificate Authority インスタンスのパフォーマンスを強化できます。

- データベース接続のチューニング
- OracleAS Single Sign-On との相互作用のチューニング
- 最大メモリーのチューニング

データベース接続のチューニング

表 7-1 データベース使用のチューニング

方法	参照先
データベース・プール・サイズを、予測される同時ユーザーの数（デフォルトは 20）にする。	5-10 ページの「データベースの設定」
データベース・プール・スキームを動的にする。（デフォルト）	5-10 ページの「データベースの設定」

データベース専用プロセスは、接続プール内の各接続によって全部使用されます。このため、これらのサイズを調整する場合は、PROCESSES というデータベース・パラメータが次の 5 つの数値の合計よりも大きいことを確認する必要があります。

- OracleAS Certificate Authority プールのサイズ
- プール内の Single Sign-On 最大接続に割り当てられた数
- mod_plsql 接続の数（Single Sign-On はログアウトに `mod_plsql` を使用するため、同時にログアウトするユーザーの数と同じになっている可能性があります。）
- Oracle Internet Directory 接続の数。これは、Oracle Internet Directory プロセスと、プロセス当たりのデータベース接続数の積として計算されます。
- 他の Oracle 製品により使用されるデータベース接続の数

関連資料：『Oracle Database 管理者ガイド』の PROCESSES に関する説明を参照してください。

OracleAS Single Sign-On との相互作用のチューニング

最適なパフォーマンスを実現するため、必ず Single Sign-On データベース・プール・サイズが OracleAS Certificate Authority データベース・プール・サイズ以上になるようにしてください。

OracleAS Certificate Authority では、最小データベース・プール・サイズが 3 としてハードコードされているため、OracleAS Certificate Authority には最大値のみを調整できます。Single Sign-On では、最小プール・サイズと最大プール・サイズの両方を構成できます。どちらも、`policy.properties` ファイル内のパラメータ（minConnectionsInPool および maxConnectionsInPool）で設定します。

> **関連資料 :**『Oracle Application Server Single Sign-On 管理者ガイド』のポリシー・プロパティの項を参照してください。

最大メモリーのチューニング

OracleAS Certificate Authority は、最大メモリーとして 256MB を使用するように構成されています。ほとんどの場合、この値で間に合います。ただし、OutOfMemory エラーが発生する場合は、JVM ヒープ・サイズを設定して、さらに大きなメモリーを使用するように構成を変更できます。

> **関連資料 :**『Oracle Application Server パフォーマンス・ガイド』の JVM ヒープに関する説明を参照してください。

Oracle Internet Directory 接続のチューニング

Oracle Internet Directory により使用されるデータベース接続数は、Oracle Internet Directory プロセスの数、およびプロセス当たりのデータベース接続の数によって決まります。これらのパラメータをチューニングするには、単一のディレクトリ・サーバー・プロセスで使用可能な同時データベース接続の数、および単一のインスタンスで生成可能なサーバー・プロセスの数を調整します。

> **関連資料 :**『Oracle Internet Directory 管理者ガイド』の Graphical User Interface に関する付録の接続の説明、および「Oracle Directory Manager のサーバーの管理フィールド」を参照してください。

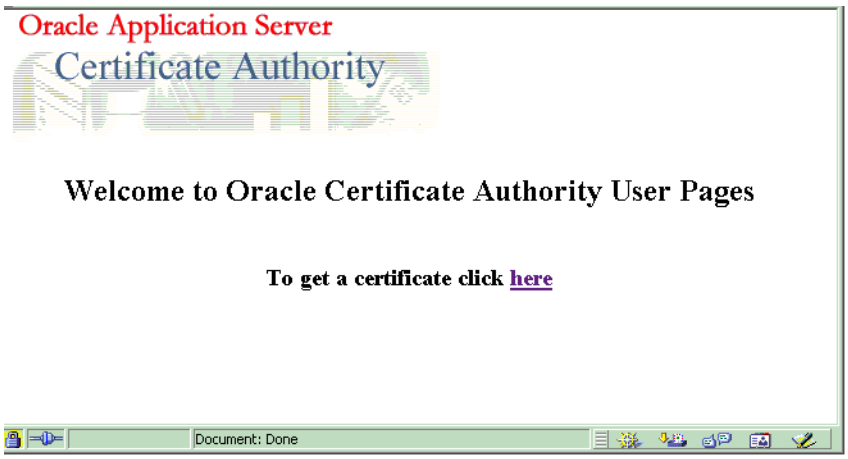
その他のコンポーネントのチューニング

その他のインストール済 Oracle コンポーネントにも、システムのパフォーマンスのチューニングに役立つ追加のパラメータがあります。パフォーマンスを強化するためにユーザーのサイトで実行可能な手順については、それぞれのコンポーネントのマニュアルを参照してください。

カスタマイズのサポート

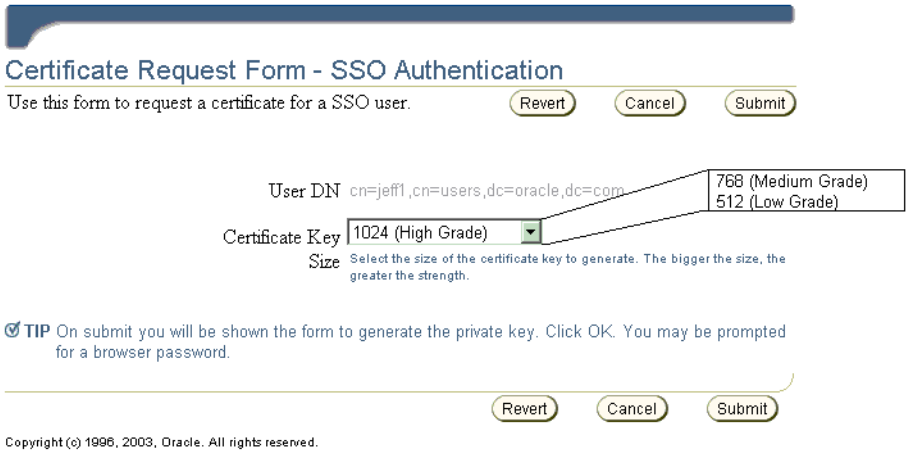
OracleAS Certificate Authority では、次の 3 つのプロビジョニング・ページに独自のヘッダーおよびフッターを指定することで、SSO と OracleAS Certificate Authority 間のインタフェースをカスタマイズできます。

1. 「ようこそ」画面

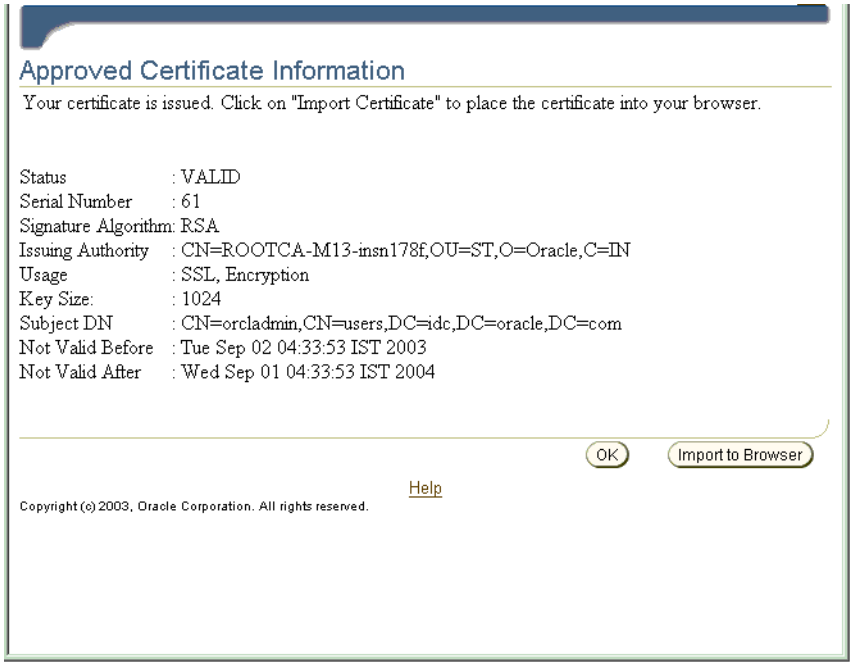


注意： このポップアップを表示するには、ブラウザでポップアップのブロック化を無効にする必要があります。

2. 「登録」画面



3. 証明書のインストール画面



関連項目： 第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」の「Single Sign-On および OracleAS Certificate Authority」

デフォルトでは、OracleAS Certificate Authority の既存画面はカスタマイズなしでレンダリングされますが、OracleAS Certificate Authority 管理者は固有のヘッダーまたはフッターを使用して、これら 3 つのいずれの画面もカスタマイズできます。OracleAS Certificate Authority 管理者は、これらの各画面にカスタム HTML ファイルを指定することで、対応するデフォルト画面ではなくカスタマイズした画面を使用するように OracleAS Certificate Authority に通知します。これらのカスタム HTML ファイルには、静的な HTML コンテンツを含めることができます。カスタマイズされた HTML ファイルがない場合、またはそのサイズが 0（ゼロ）の場合は、デフォルト画面が使用されます。

こうしたカスタム HTML ファイルの作成に使用できるテンプレートは、`$ORACLE_HOME/oca/templates/screens` という名前のディレクトリにあります。管理者は、このコンテンツのルック・アンド・フィールを制御します。

サイズが 0 でない画面カスタマイズ用の HTML ファイルがある場合は、その内容がデフォルトの画面に、表 7-2 で指示された特定の位置において追加されます。

注意：

これらの HTML ファイルのいずれかを変更した後は、変更内容を有効にするために、OracleAS Certificate Authority を再起動する必要があります。

画面、メッセージ、アラート、通知など、カスタマイズされたものの内容、翻訳およびアクセス可能性に関しては、OracleAS Certificate Authority は関与しません。カスタマイズされた内容はそのまま表示されます。

表 7-2 Single Sign-On のポップアップ画面のカスタマイズ

画面名	テキストを置換できる位置	置換目的のテキストを含むファイル[1]
「ようこそ」画面	ヘッダーの場合 : OracleAS Certificate Authority の「OracleAS Certificate Authority へようこそ」と書かれた行と「証明書を取得するにはここをクリックしてください。」と書かれた行の間 フッターの場合 :「証明書を取得するにはここをクリックしてください。」と書かれた行の下	`$ORACLE_HOME/oca/templates/screens/homeheader.html` `$ORACLE_HOME/oca/templates/screens/homefooter.html`
「登録」画面	ヘッダーの場合 : OCA の最上部にある青いバーと、「ユーザー DN」と書かれた行の間 フッターの場合 : 最下部にある「鍵サイズ」と書かれた行と「SKI」と書かれた行の下	`$ORACLE_HOME/oca/templates/screens/enrollheader.html` `$ORACLE_HOME/oca/templates/screens/enrollfooter.html`
証明書のインストール画面	ヘッダーの場合 : OracleAS Certificate Authority の証明書の表示と書かれた行と証明書詳細と書かれた行の間 フッターの場合 : 最下部にある「証明書詳細の後」と書かれた OracleAS Certificate Authority 行と「SKI」と書かれた OracleAS Certificate Authority 行の間	`$ORACLE_HOME/oca/templates/screens/importheader.html` `$ORACLE_HOME/oca/templates/screens/importfooter.html`

[1] この列に示すいずれかのファイルが 0 以外のサイズで存在する場合は、対応するヘッダーまたはフッターが、そのファイルの静的 HTML で置換される。

OracleAS Certificate Authority アクションのログまたはトレース

`ocactl` set コマンドを使用すると、ログおよびトレースが有効になり、ログおよびトレースのストレージに記録された OracleAS Certificate Authority 操作および管理操作を参照できます。

表 7-3 OracleAS Certificate Authority のログ・データおよびトレース・データの格納場所

データ型	格納の形態	場所
OracleAS Certificate Authority ログ	OracleAS Certificate Authority リポジトリ	OracleAS Certificate Authority リポジトリ
OracleAS Certificate Authority トレース	ファイル : oca.trc	$ORACLE_HOME/oca/logs
ADMIN ログ	ファイル : admin.log	$ORACLE_HOME/oca/logs
ADMIN トレース	ファイル : admin.trc	$ORACLE_HOME/oca/logs

設定コマンドの形式は次のとおりです。

```
ocactl set  -type {LOG | TRACE} -mode {OCA|ADMIN} -state {ON|OFF}
```

例 :

1. `ocactl set -type LOG -mode OracleAS Certificate Authority -state ON`

   OracleAS Certificate Authority リポジトリへのログ・メッセージの格納を有効にします。

2. `ocactl set -type TRACE -mode OracleAS Certificate Authority -state ON`

   `oca.trc` ファイルへのトレース・メッセージの格納を有効にします。

3. `ocactl set -type LOG -mode ADMIN -state ON`

   `admin.log` ファイルへのログ・メッセージの格納を有効にします。

4. `ocactl set -type TRACE -mode ADMIN -state ON`

   `admin.trc` ファイルへのトレース・メッセージの格納を有効にします。

5. `ocactl set -type TRACE -state OFF`

   トレースをオフにします。トレース・データは格納されません。

OracleAS Certificate Authority のログ情報またはトレース情報の消去

`ocactl` 管理コマンドライン・ツールを使用すると、管理者の選択で既存のログ・ストレージまたはトレース・ストレージを消去できます。OracleAS Certificate Authority ログは、OracleAS Certificate Authority リポジトリに格納されます。また、OracleAS Certificate Authority トレースは、`$ORACLE_HOME/oca/logs` の `oca.trc` に格納されます。ADMIN LOG は `$ORACLE_HOME/oca/log` の `admin.log` に、ADMIN TRACE は `$ORACLE_HOME/oca/logs` の `admin.trc` に格納されます。

有効な形式およびモードで消去コマンドを実行すると、このようなログまたはトレースのストレージの古い情報は消去されます。このようなコマンドによる影響を受けるファイル（oca.trc、admin.trc または admin.log）は、ファイル・システムから削除されます。

消去コマンドの形式は次のとおりです。

```
ocactl clear -type {LOG |TRACE}  -mode {OCA|ADMIN}
```

例 :

1. `ocactl clear -type LOG -mode ADMIN`

   `$ORACLE_HOME/oca/logs` から ADMIN LOG ファイル `admin.log` を削除します。

2. `ocactl clear -type TRACE -mode ADMIN`

   `$ORACLE_HOME/oca/logs` から ADMIN TRACE ファイル `admin.trc` を削除します。

3. `ocactl clear -type LOG -mode OCA`

   OracleAS Certificate Authority リポジトリのログ・メッセージを削除します。

4. `ocactl clear -type TRACE -mode OCA`

   `$ORACLE_HOME/oca/logs` から OracleAS Certificate Authority TRACE ファイル `oca.trc` を削除します。

インフラストラクチャ・サービスの変更

新しいポートやホストを使用するなど、OracleAS Single Sign-On（SSO）および Oracle Internet Directory に対する変更は、次に示す状況など、様々な形で発生します。

- バックアップ後の操作のリストア
- LDAP（ディレクトリ）または Oracle Database の構成の変更
- パイロット・シナリオから本番環境への移行

関連資料 :『Oracle Application Server 管理者ガイド』

OracleAS Certificate Authority は、OracleAS Identity Management（IM）インフラストラクチャのコンポーネントとしてインストールされ、Oracle Internet Directory、OracleAS Single Sign-On および Metadata Repository のサービスを使用します。これらのコンポーネントのいずれかが置換またはリストアされた場合は、それらの新しいサービスを使用するように OracleAS Certificate Authority を構成できます。OracleAS Certificate Authority は、新しい Oracle Internet Directory、OracleAS Single Sign-On および Metadata Repository を使用することも、または、これら 3 つのコンポーネントの既存バージョンを使用することもできます。

Oracle Application Server では、次の 2 つのタイプのインフラストラクチャの変更がサポートされます。

- ID 管理（IM）サービスの変更
- Metadata Repository（MR）サービスの変更

次の項では、これらのサービスに関するデータの表示について説明します。

- 接続情報の格納場所および表示場所

ID 管理（IM）サービスの変更

新しい OracleAS Single Sign-On または Oracle Internet Directory のインストール後に、OracleAS Certificate Authority が使用する IM サービスを変更するには、次の 2 つの手順を実行する必要があります。

- 新しい IM をインストールし既存データを移行します。
- 新しくインストールした IM サービスを使用できるように、OracleAS Certificate Authority を構成します。

OracleAS には、新しい IM（OracleAS Single Sign-On および Oracle Internet Directory）がインストールされたという前提で、ある IM インスタンスから別のインスタンスにデータを移行するスクリプトが用意されています。ただし、Application Server Control コンソールの「インフラストラクチャ」ページの ID 管理の変更ウィザードを使用して、OracleAS Certificate Authority サービスを変更することはできません。OracleAS Certificate Authority 自体がインフラストラクチャ・コンポーネントのためです。そのため、OracleAS Certificate Authority では、OracleAS Certificate Authority が使用する IM サービスの変更は、OracleAS Certificate Authority 管理コマンドライン・ツール `ocactl` の changesecurity コマンドによりサポートされます。

関連項目：

- OracleAS Certificate Authority 管理コマンドライン・ツールの詳細は、付録 A「コマンドライン管理」を参照してください。
- スクリプトを含む、Identity Management インフラストラクチャの IM サービスおよびメタデータ・サービスの変更の詳細は、『Oracle Application Server 管理者ガイド』を参照してください。

OracleAS Certificate Authority に新しい IM サービスを構築するには、次の手順を実行します。

1. マシン 1 に、Identity Management および Metadata Repository をインストールします。
2. マシン 2 に、Identity Management をインストールします。
3. OracleAS に用意されているスクリプトを使用して、マシン 1 からマシン 2 に IM データを移行します。
4. OracleAS Certificate Authority が稼働するマシン（マシン 1）で、OracleAS Certificate Authority、OracleAS Certificate Authority の OC4J および OHS を停止します。次のコマンドを使用します。

   ```
   $ORACLE_HOME/oca/bin/ocactl stop
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

5. マシン 1 で、`ias.properties` ファイルを編集し、`$ORACLE_HOME/config` ディレクトリの下にある OIDhost パラメータおよび OIDport パラメータが、新しい IM（マシン 2）を指すようにします。
6. マシン 1 で、次のコマンドを実行します。

   ```
   $ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port portno
   ```

   このコマンドは、次の 2 つのアクションを実行します。

   - IM サービスの新しいマシン（マシン 2）を指すよう、`$ORACLE_HOME/oca/conf` にある `oca.conf` ファイルを更新します。
   - 新しい OracleAS Single Sign-On Server（マシン 2）に OracleAS Certificate Authority を登録します。

注意： Identity Management（IM）の再関連付けは、スケーラビリティやフェイルオーバーの目的で行った OracleAS Single Sign-On または Oracle Internet Directory のサービスの構成変更、またはパイロット IM から本番 IM への移行に対応するために使用できます。

このような再関連付けの詳細は、『Oracle Application Server 管理者ガイド』を参照してください。

Metadata Repository（MR）サービスの変更

元の物理データベースから別の物理データベースへの OracleAS Certificate Authority のメタデータ・サービスの変更は、サポートされていません。ただし、リスナーやポートの変更など、接続文字列の変更は、`updateconnection` コマンドを使用することで対応できます（付録 A を参照）。

接続情報の格納場所および表示場所

OracleAS Certificate Authority リポジトリおよびディレクトリへの接続を定義する情報（証明書の公開に使用）は、Oracle Internet Directory に格納されます。この接続情報は、最初に、Oracle Application Server のインストール時に Oracle Internet Directory に書き込まれます。同時にこの接続情報は Oracle Internet Directory からフェッチされ、OracleAS Certificate Authority の構成ファイル `$ORACLE_HOME/oca/conf/oca.conf` に書き込まれます。

この接続情報は、OracleAS Certificate Authority 管理者用の Web ベースのインタフェースの「一般」サブタブにある設定セクションに表示されます。

関連項目： 付録 A「コマンドライン管理」の表 A-2「OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ」の `updateconnection`

OracleAS Certificate Authority および高可用性機能

Oracle Application Server の高可用性機能は、『Oracle Application Server 高可用性ガイド』で詳細に説明されています。ここでの説明は、これらの機能を紹介するための概要です。

OracleAS Certificate Authority を使用すると、実際の高可用性システムで、迅速かつ容易に証明書を使用できます。『Oracle Application Server 高可用性ガイド』で、Oracle Application Server の Cold Failover Clusters および Real Application Clusters（RAC）の高可用性機能をサポートするリンク、手順、表記規則および準備事項について説明します。

- OracleAS Certificate Authority コールド・フェイルオーバーを使用した配置
- Real Application Clusters を使用した OracleAS Certificate Authority の配置

OracleAS Certificate Authority コールド・フェイルオーバーを使用した配置

コールド・フェイルオーバー構成では、複数の物理ホストから共有ディスク上の共通のストアにアクセスでき、各物理ノードは、同時に 1 つ以上の論理ホストをホスティングできます。Oracle Application Server Cold Failover Cluster を使用すると、Oracle Application Server インスタンスを障害ノードからバックアップに透過的にフェイルオーバーできます。また、メンテナンスのためにフェイルオーバーを手動で開始することもできます。

この例では、ソフトウェアとデータベースをそれぞれ 1 つしかインストールしていません。また、2 つの物理ホストが、OracleAS Certificate Authority および Oracle Application Server のソフトウェアとデータベースがインストールされたディスクへのアクセスを共有します。Oracle Application Server のハードウェアがマシンのクラスタとして構成される場合は、インストーラはそのノードをクラスタの一部と認識し、仮想ホストの名前の入力を要求します。物理ホスト 1 に障害が発生した場合、またはメンテナンスのためにオフラインになっている場合、その論理ホスト名（仮想ホスト A）は他の物理ホストに移行されます。ベンダー固有のスクリプトとハードウェア・クラスタ・ソフトウェアを使用すると、必要なデータベース、リスナーおよび OracleAS Certificate Authority/Oracle Application Server の各プロセスを起動して、透過的フェイルオーバーを有効にできます。クライアントは、最小限のサービス停止で、以前と同じ論理ホストへの接続を継続できます。HTTP Server および OC4J を起動した後は、`ocactl start` コマンドを使用して、OracleAS Certificate Authority も再起動する必要があります。

関連資料：『Oracle Application Server 高可用性ガイド』

Real Application Clusters を使用した OracleAS Certificate Authority の配置

OracleAS Certificate Authority では、Real Application Clusters (RAC) は完全にサポートされません。OracleAS Certificate Authority では、Oracle Internet Directory、Oracle Database、OracleAS Single Sign-On など、RAC 構成の他のインフラストラクチャ・コンポーネントを使用できますが、OracleAS Certificate Authority 自体は RAC モードにできません。

関連資料： これらのコンポーネントを RAC モードでインストールする方法は、『Oracle Application Server 高可用性ガイド』を参照してください。

注意： OracleAS Certificate Authority 10*g*（10.1.4.0.1）では、RAC は Windows でサポートされていません。

OracleAS Certificate Authority のバックアップおよびリカバリでの考慮事項

バックアップおよびリカバリという言葉は、データの消失に対する防御とデータを消失した場合の再構築の両方に際して行う様々な戦略と手順を指しています。Oracle Application Server Backup and Recovery Tool は、障害が発生した場合に、Oracle Application Server 環境のバックアップとリカバリを支援します。

関連資料： Backup and Recovery Tool の詳細な説明と手順は、次のドキュメントを参照してください。

- 使用可能な各種バックアップおよびリカバリ方法、Oracle Application Server Backup and Recovery Tool のインストールおよび構成、コンポーネント単位のバックアップおよびリカバリのそれぞれの詳細は、『Oracle Application Server 管理者ガイド』にあるバックアップとリカバリの説明を参照してください。
- データベースのバックアップは、『Oracle Database バックアップおよびリカバリ・アドバンスト・ユーザーズ・ガイド』に示すバックアップおよびリカバリに関する Oracle のガイドラインを参照してください。
- Oracle Internet Directory のバックアップについては、『Oracle Internet Directory 管理者ガイド』を参照してください。

この後の説明はあくまで概要です。詳細な情報は、前述のドキュメントを参照してください。

次のような状況で、バックアップ / リカバリ技法を使用してデータをリカバリできます。

表 7-4 バックアップおよびリカバリの使用例

状況	対応策
ホストの消失	ホスト名および IP アドレスが同じ新しいホストにリストアできます。 あるいは、ホスト名および IP アドレスが異なる新しいホストにリストアすることもできます。
Oracle ソフトウェア / バイナリの消失または破損	Oracle バイナリが破損または消失した場合は、インフラストラクチャ全体をリカバリする必要があります。
データベース・インスタンスの障害など、Metadata Repository インスタンスの障害	データベース・インスタンスのリカバリ方法を使用して、Metadata Repository インスタンスをリカバリします。
Metadata Repository データベースの障害（Metadata Repository のみが破損し、インフラストラクチャの Oracle ホームにある他のファイルは破損していない場合）	B/R スクリプトを使用して Metadata Repository をバックアップし、OracleAS Backup and Recovery Tool を使用してデータベースをリカバリします。
Oracle Application Server コンポーネントのランタイム構成ファイルの削除または破損	B/R スクリプトを使用して、構成ファイルをリストアします。
Metadata Repository リスナーの障害	リスナー・プロセスを停止して再起動します。

メンテナンスが必要な場合や、サービスが予期せず消失した場合は、様々なバックアップおよびリカバリ手順によって、OracleAS Certificate Authority の情報と機能が保護および保持されます。

バックアップ方法および対応するリカバリ方法は、次の Backup and Recovery Tool によりサポートされます。

表 7-5 Backup and Recovery Tool

ツール名	機能
コールド・バックアップ / リカバリ	Oracle Application Server Infrastructure の全プロセスおよび Metadata Repository のクリーンな通常停止の完了後にバックアップされた Oracle ホーム、構成ファイル、データベース・ファイルなど、Oracle Application Server Infrastructure インスタンス全体をリストアすることを指します。
部分オンライン（ホット）バックアップ / リカバリ	Oracle Application Server のインスタンスおよび Metadata Repository の適切なオンライン・バックアップの完了後に、バックアップされた OracleAS Infrastructure の構成ファイルおよびデータベース・ファイルをリストアします。
構成ファイルの増分バックアップ / リカバリ	オンライン・バックアップから取得した Oracle Application Server Infrastructure 構成ファイルのみをリストアします。

OracleAS Certificate Authority は、Oracle Database をプライマリ・リポジトリとして使用しているため、データベースに格納されている OracleAS Certificate Authority の情報は、データベースがバックアップされる際に自動的にバックアップされます。同様に、OracleAS Certificate Authority は、証明書の公開用および特定の OracleAS Single Sign-On 操作用に Oracle Internet Directory を使用します。この項の冒頭に記載した 3 つのドキュメントには、関連するバックアップ操作およびリカバリ操作がすべて詳細に説明されています。

データベースおよびディレクトリに格納されている情報に加え、OracleAS Certificate Authority は多くの重要なオペレーティング・システム・ファイルも作成します。これらのファイルは、通常のバックアップ処理の一部としてバックアップする必要があります。次のようなファイルがあります（$ORACLE_HOME は OracleAS Certificate Authority がインストールされているホーム・ディレクトリを表します）。

- $ORACLE_HOME/oca/templates/*
- $ORACLE_HOME/oca/policy/*
- $ORACLE_HOME/oca/logs/admin.*
- $ORACLE_HOME/oca/conf/oca.conf
- $ORACLE_HOME/oca/conf/ocaplugin.xml
- $ORACLE_HOME/oca/pwdstore/ocmpassword.p12
- $ORACLE_HOME/oca/wallet/ssl/cwallet.sso
- $ORACLE_HOME/oca/wallet/ssl/ewallet.p12
- $ORACLE_HOME/oca/wallet/ldap/ewallet.p12
- $ORACLE_HOME/Apache/Apache/conf/ocm_apache.conf
- $ORACLE_HOME/Apache/Apache/conf/osso/oca/osso.conf

証明書公開レルムの制限

各部門が地理的に分散している大規模な組織では、より効率的なローカル管理のために、部門ごとに別々の認証局を確立できます。これらの部門は、Wyoming や New York など複数の州、または米国や英国など複数の国に存在する場合もあります。OracleAS Certificate Authority の様々なインスタンスは、下位 CA や相互信頼関係のある独立した CA です。

デフォルトでは、OracleAS Certificate Authority のインスタンスを特定のマシンにインストールすると、エントリは Oracle Internet Directory に格納されます。インストールされた OracleAS Certificate Authority インスタンスは、次の識別名で表されます。

cn=ocaN,cn=OCA,cn=PKI,cn=Products,cn=OraclContext

（N は 1、2 …n）

現行の OracleAS Certificate Authority に対応するエントリを確認するには、「管理」ページに進み、さらに「構成管理」タブの「一般」サブタブを参照します。「エージェント」の「ディレクトリの設定」エントリの下の DN に、現行の Oracle Internet Directory での現行の OracleAS Certificate Authority が示されます。

デフォルトでは、このような各 CA は最上位の Oracle コンテキストであるグループ cn=PKIAdmins,cn=Groups,cn=OracleContext のメンバーです。

このような CA がユーザー証明書を公開すると、その証明書は自動的に Oracle Internet Directory 内の対応するサブスクライバ・レルムのユーザーの DN エントリに格納されます。デフォルトでは、すべての CA が信頼され、ディレクトリ全体のあらゆるユーザー・エントリに公開できます。たとえば、US レルムのユーザーは UK の OracleAS Certificate Authority から証明書を受信でき、ユーザー証明書は US レルムのそのユーザーの DN エントリに格納されます。

ただし、OracleAS Certificate Authority インスタンスの公開権限を制限して、特定のサブスクライバ・レルム以外には公開しないようにできます。たとえば、UK の OracleAS Certificate Authority を UK サブスクライバ・レルムにのみ公開するように制限できます。このように制限した場合、ユーザーの通常のレルムは UK の OracleAS Certificate Authority にアクセスできないため、UK の OracleAS Certificate Authority が US ユーザーに発行した証明書は公開できません。

OracleAS Certificate Authority を特定のレルムに制限する場合は、最上位のグループ（cn=PKIAdmins,cn=Groups,cn=OracleContext）から削除し、指定したグループにその OracleAS Certificate Authority エントリを追加する必要があります。たとえば、OCA2 の公開

をサブスクライバ dc=com,dc=acme のみに制限する場合は、次の 2 つのコマンドを使用します。

```
-remove cn=oca2,cn=cn=OCA,cn=PKI,cn=Products,cn=OraclContext from group
cn=PKIAdmins,cn=Groups,cn=OracleContext

-add cn=oca2,cn=cn=OCA,cn=PKI,cn=Products,cn=OraclContext to group
cn=PKIAdmins,cn=Groups,cn=OracleContext,dc=acme,dc=com
```

さらには、CA を制限するカスタム・プラグインを記述することで、特定の一連の DN からの証明書のみを管理できます。たとえば、第 6 章「Oracle Application Server Certificate Authority でのポリシー管理」で開発したカスタム・プラグインでは、米国以外のドメインからの証明書のみを発行するように CA を制限しています。

この制限は、第 5 章の「カスタム・ポリシー・プラグインの例」に示した例の 12 行目、すなわち次の行で記述されています。

```
12:             if (!policyRequest.getCountry().equals("US"))
```

「!」を削除して「US」を目的のレルムに変更するように少し変更し、さらに後続の数行を修正すると、これに依存する行によって、証明書の発行が、指定したレルムに制限されます。

CA の置換および OracleAS Certificate Authority の削除

秘密鍵が危殆化したなどの理由で、まれにルート CA を抜本的に置換する必要が生じることがあります。このような場合は、OracleAS Certificate Authority を一度、削除してから再インストールします。OCA を削除すると、元々インストールされていたデータベースおよび Oracle Internet Directory エントリのトレースはすべて削除されます。

このような削除を実行するには、Oracle Application Server 10*g* のインストレーション・ガイドの説明に従ってください。

ディレクトリ統合タスク

OracleAS Certificate Authority 操作に必要なデータは、Oracle Internet Directory 内で保守されます。多くの場合、管理者は様々なディレクトリ統合タスクおよび管理タスクを実行する必要があります。次のリストのトピックについては、このドキュメントに追加情報が記載されています。各トピックは対応する項にリンクしています。

- 証明書失効リスト（CRL）の場所とリストの管理方法の詳細は、3-11 ページの「CRL ポリシーの定義」を参照してください。
- CRL の生成および更新手順の詳細は、4-15 ページの「証明書失効リスト（CRL）の更新」を参照してください。
- Oracle Internet Directory 内で保守されるデータの内容、ディレクトリへの公開方法、およびディレクトリからの CRL の取得方法は、4-16 ページの「Oracle Internet Directory Integration」を参照してください。
- OracleAS Certificate Authority 操作に必要なその他の Oracle Identity Management コンポーネントの詳細は、4-2 ページの「Oracle Application Server Certificate Authority の起動および停止」を参照してください。
- Oracle Internet Directory Server 管理については、『Oracle Internet Directory 管理者ガイド』のインストール後のタスクおよび管理に関する項を参照してください。
- ユーザー証明書を公開したときに Oracle Internet Directory に移入される属性のリストは、『Oracle Identity Management ユーザー・リファレンス』の orclCertIdMapping に関する項を参照してください。

8

Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース

「エンド・ユーザー」は、ユーザーのみでなく、サーバーとアプリケーション間の認証を容易にするために証明書を取得するサーバー・エンティティも表します。

エンド・ユーザーおよび管理者が OracleAS Certificate Authority サーバーと対話するための HTML インタフェースが、それぞれ用意されています。エンド・ユーザーは、これらの HTML インタフェースを使用して、証明書に関連する個人的な操作を実行でき、管理者は証明書を管理できます。

> **関連項目：** OracleAS Certificate Authority の Web ベースの管理インタフェースについては、次を参照してください。
>
> - 第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」
> - 第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」

この章の内容は、次のとおりです。

Netscape および Internet Explorer の両方がサポートされます。

ユーザー・インタフェースへのアクセス

OracleAS Certificate Authority のエンド・ユーザー・インタフェースのホームページにアクセスするには、Web ブラウザを起動して、インストールの最後に表示された管理サーバーの URL およびポート番号を入力します。たとえば、次のように入力します。

```
https://server1.example.com:6600/oca/user
```

次のような、Oracle Application Server Certificate Authority のユーザー・ホームページが表示されます。

このページに説明されているとおり、この Web ベースのインタフェースを使用して、証明書のリクエストや、証明書または証明書リクエストの更新、失効または検索を行うことができます。これらの機能を使用するには、「ユーザー証明書」タブと「サーバー / 下位 CA 証明書」タブのいずれかをクリックします。

また、**「ここをクリック」**リンクを使用して、認証局の証明書または最新の証明書失効リスト（CRL）をブラウザにインストールすることもできます。

同様に、管理者は、管理者用の**「ここをクリック」**リンクを使用して、追加使用の目的で CA 証明書または CRL をファイル・システムに保存できます。

エンド・ユーザー用のタブおよび処理

OracleAS Certificate Authority の Web ベースのインタフェースでは、次に示すとおり、エンド・ユーザーは OracleAS Certificate Authority と 2 つのタイプの対話を実行できます。

「ユーザー証明書」タブでは、次の処理を行うことができます。

- OracleAS Certificate Authority から自身について認証を受けること。この処理を実行するには、既存の Single Sign-On または SSL 証明書を使用するか、管理者による手動の認証をリクエストします。
- OracleAS Certificate Authority 管理者がエンド・ユーザー用またはサーバー用に手動で認可できる新しい証明書リクエストを作成すること。
- 証明書の自動的なリクエストおよび受信（SSL ユーザーおよび OracleAS Single Sign-On ユーザーの場合）。
- 証明書のインストール、表示、失効または更新。
- 認証方式の変更。
- CA 証明書の保存またはインストール。
- 最新の証明書失効リスト（CRL）の保存またはインストール。

表 8-1 に、Oracle Application Server Certificate Authority がサポートしている証明書のタイプと、それぞれについての簡単な説明を示します。

表 8-1 証明書の使用方法の選択項目

機能	説明
認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。） 「認証」証明書を使用する場合、SSL 認証時に証明書が使用されます。
暗号化	SMIME を使用して、電子メール・メッセージなどの電子ドキュメントの暗号化および複合化を可能にします。 「暗号化」証明書を使用して電子メールを暗号化する場合、ユーザーは他のユーザーに証明書を提供して、公開鍵で暗号化されたメッセージを他のユーザーが送信できるようにします。その後は、そのユーザーのみが秘密鍵を使用してメッセージを解読できます。 Outlook や Mozilla などのメール・クライアントで暗号化証明書を使用する方法は、付録 G「OracleAS Certificate Authority での S/MIME」を参照してください。
署名	（S/MIME（Secure Multipurpose Internet Mail Extension）を使用して）電子メールなどの電子ドキュメントに対する検証可能な署名を可能にします（また、これらの電子ドキュメントの改ざんを防ぎます）。 「署名」証明書のユーザーは、証明書を使用して秘密鍵でメッセージ・ダイジェストに署名します。これによって、他のユーザーは公開鍵を使用して、このユーザーがメッセージを送信したこと、およびその内容が変更されていないことを検証できます。 Outlook や Mozilla などのメール・クライアントで署名証明書を使用する方法は、付録 G「OracleAS Certificate Authority での S/MIME」を参照してください。
認証、暗号化	この両方の目的に証明書を使用できます。
認証、署名	この両方の目的に証明書を使用できます。
認証、署名、暗号化	この 3 つの目的すべてに証明書を使用できます。
署名、暗号化	この両方の目的に証明書を使用できます。

表 8-1 証明書の使用方法の選択項目（続き）

機能	説明
CA 署名	下位 CA 証明書をリクエストできるようにします。 認証局は、発行する証明書に「CA 署名」証明書の秘密鍵を使用して署名します。これによって、受信者は公開鍵を使用して、証明書がこの特定の認証局によって署名されていることを検証できます。
コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します（また、これらの改ざんを防ぎます）。 「コード署名」証明書のユーザーは、秘密鍵でソフトウェアに署名します。これによって、クライアントは公開鍵を使用して、このユーザーがソフトウェアの配布元であることを検証できます。

「サーバー / 下位 CA 証明書」タブでは、次の処理を行うことができます。

- ID、シリアル番号、一般名などによる、証明書および証明書リクエストの検索
- サーバー証明書および下位 CA 証明書のリクエスト
- CA 証明書または証明書失効リスト（CRL）のインストール

「ユーザー証明書」タブ

このタブを初めて表示するときに、「認証」ページが表示されます。このページでは、Oracle Application Server Certificate Authority に対する、ユーザー自身の認証方法を選択できます。

表 8-2 に、使用可能な認証タイプおよび認証方式を示します。

表 8-2 認証タイプ

認証タイプ	説明	方式の概要（詳細は次の項を参照）
Single Sign-On	認証は、Single Sign-On Server に基づいて自動化されます。通常は、パスワード・ベースです。	**「自分の OracleAS Single Sign-On 用の名前とパスワードを使用」**というラベルが付いたラジオ・ボタンをクリックし、**「送信」**をクリックします。
Secure Sockets Layer（SSL）	認証は、事前に発行された SSL 証明書に基づいて自動化されます。	**「既存の証明書の使用」**というラベルが付いたラジオ・ボタンをクリックし、**「送信」**をクリックします。
手動	認証は自動化されません。「証明書リクエスト」フォームに必要事項を入力して送信し、管理者からの承認を待ちます。	**「手動認可 / 認証を使用」**というラベルが付いたラジオ・ボタンをクリックし、**「送信」**をクリックします。

関連項目： 認証については、第 2 章「ID 管理および OracleAS Certificate Authority の機能」を参照してください。

次の項で、これらの認証タイプおよび認証方式について詳しく説明します。

- Single Sign-On（SSO）認証
- OracleAS Certificate Authority が信頼されるブラウザの構成
- Secure Sockets Layer（SSL）認証
- 手動認証
- 証明書の検索、更新および失効
- 「サーバー / 下位 CA 証明書」タブ
- 下位 CA 証明書

注意： Mozilla では、エンド・ユーザーおよび管理者のいずれの場合にも、デフォルトの鍵のサイズは 2048 です。

Internet Explorer では、512 ビット（basic）または 1024 ビット（enhanced）または 2048 ビット（strong）です。デフォルトは「strong」で、「strong」が選択できない場合は「enhanced」、「enhanced」も選択できない場合は「basic」になります。コンピュータにスマートカード・リーダーが装備されていない場合、Gemplus を選択すると、鍵のサイズの解決法が見つからないためにエラーが表示されます。カード・リーダーが装備されている場合は、スマートカードに選択した項目によって鍵のサイズが決定されます。

Single Sign-On（SSO）認証

次の手順を実行して、必須の OracleAS Single Sign-On 認証情報（ユーザー名やパスワードなど）を提供することにより、OracleAS Single Sign-On ユーザーは自動的に証明書を取得したり、証明書を管理できます。

1. 「認証」フォームで、**「自分の OracleAS Single Sign-On 用の名前とパスワードを使用」**というラベルが付いたオプションを選択し、**「送信」**をクリックします。OracleAS Single Sign-On のログイン・ページにリダイレクトされます。
2. OracleAS Single Sign-On のユーザー名およびパスワードを入力します。有効な証明書を示す「ユーザー証明書 - SSO」フォームが表示され、次の作業を行うことができます。
   - 証明書の取得
   - 選択した証明書の詳細の表示
   - 現行の証明書の更新
   - 現行の証明書の失効

   証明書を取得するには、手順 3 ～ 5 を実行します。
3. 「ユーザー証明書 - SSO」フォームの**「証明書のリクエスト」**をクリックして、「証明書リクエスト」フォームを表示します。
4. 「証明書リクエスト」フォームで、適切な情報を入力し、フォームを送信します。使用しているブラウザが Netscape の場合と Internet Explorer の場合では、表示される選択肢が少し異なります。
   - **Netscape の場合は**、512、1024 など、生成される鍵のペアのサイズ（ビット単位）を示す**「証明書鍵サイズ」**が表示されます。

     Internet Explorer の場合は、暗号化サービス用に選択可能なプロバイダを示す**「暗号サービス・プロバイダ」**が表示されます。標準の選択肢は、Microsoft Basic Crypto Provider、Microsoft Enhanced Crypto Provider、Microsoft Strong Crypto Provider です。OracleAS Certificate Authority ではデフォルトで、Microsoft Strong Cryptographic Provider（選択可能な場合）、Microsoft Enhanced Crypto Provider（選択可能な場合）、Microsoft Basic Crypto Provider の順に選択されます。また、スマートカードを使用する場合の Gemplus など、その他の選択肢が表示される場合もあります。要件に応じて、サイズを選択します。
   - **証明書の使用方法 :** この証明書を使用する操作のタイプを選択します。リストに最初に表示される標準デフォルトは OracleAS Certificate Authority 管理者が設定しますが、表 8-1 に示すように、ユーザーがドロップダウン・リストから別の項目を選択することもできます。
   - **有効期間 :** 証明書の有効期間を日数で指定します。ただし、ValidityRule ポリシーのデフォルト有効期間に指定されている数値を使用して、Oracle Application Server Certificate Authority が自動的に設定するため、OracleAS Single Sign-On ユーザーが有効期間に関する情報を入力する必要はありません。

   必要事項を入力したフォームを送信すると、「証明書」フォームが表示され、証明書に記録された情報が示されます。

5. 情報が正しいことを確認した後、証明書の署名者の名前を書き留めます。この名前は後で必要です。次に、**「ブラウザへのインストール」**ボタンをクリックして、ブラウザに証明書をインストールします。Netscape と Internet Explorer では、インストールが成功したことを伝える方法は異なります。

注意：「ブラウザへのインストール」ではなく**「OK」**をクリックすると、証明書が作成されて OracleAS Certificate Authority リポジトリに格納され、Oracle Internet Directory に公開されます。ただし、インストールするまで、証明書はブラウザからサーバーに渡されません。「ブラウザへの新規発行の証明書のインポート」を参照してください。

- **Netscape の場合は**、証明書がインストールされると、ブラウザの左下のステータス・バーに「ドキュメント：完了。」と表示されます。この時点で「OK」をクリックします。カーソルが砂時計のままでも、処理は完了しています。対応する CA（署名者）の証明書も、インストールされています。

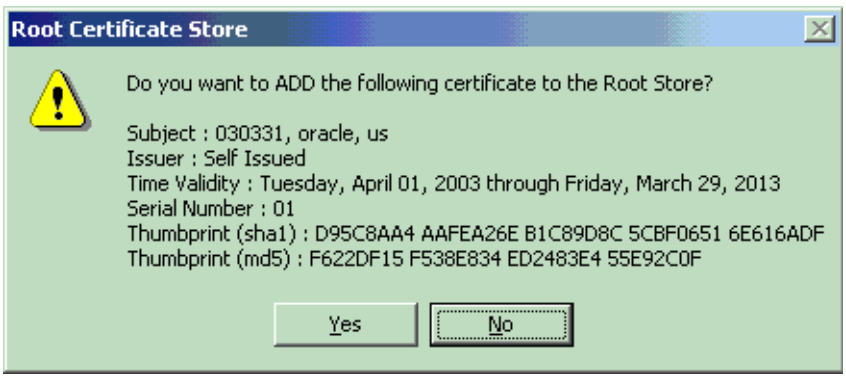
注意： 信頼できる証明書にするには、CA 証明書の使用方法を編集して、その認証局が発行した証明書を、ネットワーク・サイト、電子メール・ユーザー、ソフトウェア開発者のいずれかまたはすべてに対して信頼すると指定します。これらの選択肢のチェック・ボックスは、Netscape のメニュー・バーの「セキュリティ」から表示できます。「Netscape での証明書発行元への信頼」を参照してください。

- **Internet Explorer の場合は**、証明書がインポートされると、証明書が正常にインストールされたというメッセージが表示されます。また、CA の詳細が表示されたウィンドウで、署名者の証明書をインストールするかどうかを確認するメッセージが表示されます。「OK」をクリックして、署名者の証明書もインストールすることを確認します。Internet Explorer では、これらの証明書は信頼できると自動的に判断されます。

OracleAS Certificate Authority が信頼されるブラウザの構成

この処理は、Internet Explorer、Netscape および Mozilla Firefox の間で少し異なります。

Internet Explorer での証明書発行元への信頼 Internet Explorer を使用して証明書をインストールする場合、その証明書をルート・ストアに追加するかどうかを確認するメッセージが表示されます。



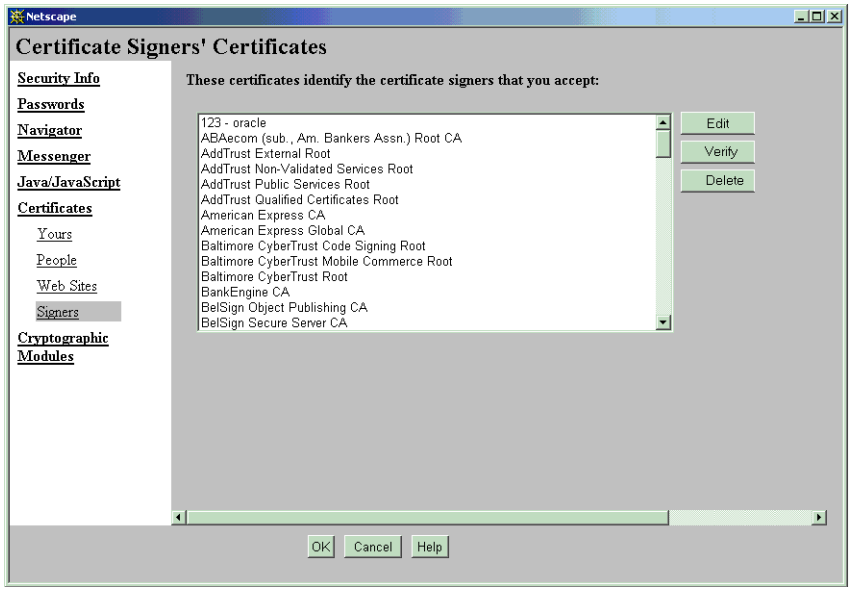
「はい」をクリックすると、証明書がインストールされ、発行元が「信頼できる」と設定されます。証明書は、メニューから「ツール」→「インターネット オプション」→「コンテンツ」→「証明書」を選択して表示できます。次に、4 つのタブが表示されます。それぞれのタブでは、ユーザー自身の証明書、他のユーザーを認証するために提供された他人の証明書、証明書を提供した中間認証局、信頼できると設定したルート認証局を参照できます。

Netscape での証明書発行元への信頼 Netscape を使用して証明書をインストールする場合、リクエストした証明書と、新しい CA 証明書に署名して発行した認証局を示す証明書の両方がインストールされます。通知されるのは、ブラウザの左下のステータス・バー領域に表示される「ドキュメント : 完了。」というメッセージのみです。ただし、新しい証明書が信頼できるようになるのは、署名者の証明書を信頼させるアクティビティを Netscape に対して明示的に指定した時点です。

証明書を信頼させるアクティビティを指定するには、次の手順を実行します。

1. Netscape の左下のステータス・バーにあるロック・アイコンをクリックして、「セキュリティ情報」ページを開きます。（または、メニュー・バーから「Communicator」→「ツール」→「セキュリティ情報」を選択します。）次のようなページが表示されます。

2. 「署名者」リンクをクリックします。次のようなページが表示されます。

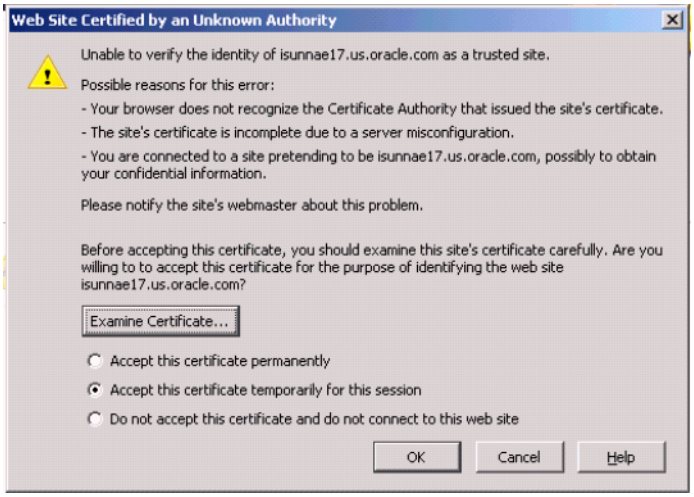


3. 証明書の詳細を参照したときに書き留めておいた署名者の名前をクリックし、「**編集**」をクリックします。次のようなページが表示されます。

4. 画面例で選択状態になっている 3 つのチェック・ボックスを選択して、「**OK**」をクリックします。

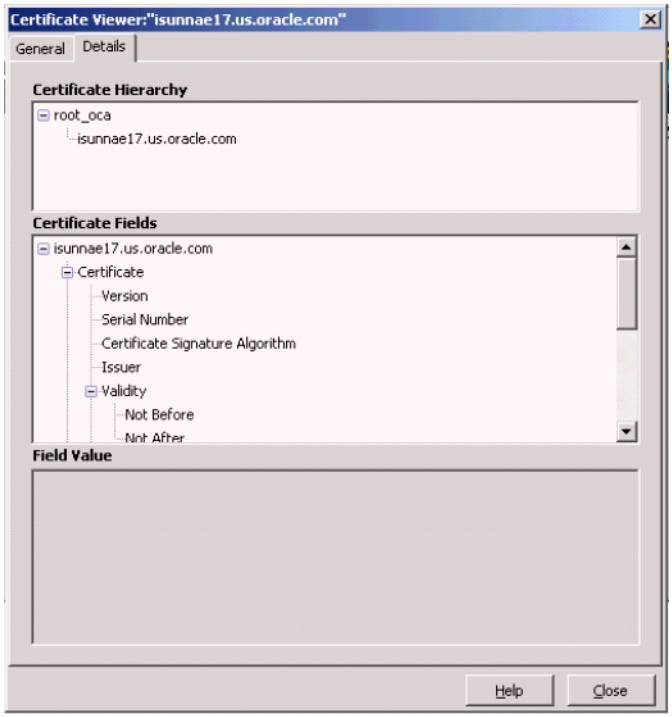
これで、CA 証明書は信頼され、ブラウザで接続するネットワーク・サイト、署名または暗号化された受信メッセージ、あるいは署名されたソフトウェアの証明書を検証できます。

Mozilla Firefox での証明書発行元への信頼 Mozilla Firefox を使用して証明書をインストールすると、証明書を発行する認証局が不明である旨が通知されます。



これを信頼できる証明書にするには、「**この証明書の永続的な受付**」を選択して「**OK**」をクリックします。

証明書を受け付ける前にその証明書を検査できます。検査するには、**「証明書の検査」**をクリックします。次のような画面が表示されます。



フィールドを選択してその値を表示します。

Secure Sockets Layer（SSL）認証

認証局から SSL 証明書をすでに取得している場合は、現行の SSL 証明書を ID として使用して、今後の認証で使用するために、OracleAS Certificate Authority 証明書を取得できます。手順は、次のとおりです。

1. 「認証」フォームの**「既存の証明書の使用」**オプションを選択して、**「送信」**をクリックします。**「ユーザー証明書 - SSL」**フォームが表示され、次の作業を行うことができます。
   - 証明書の取得
   - 選択した証明書の詳細の表示
   - 現行の証明書の更新
   - 現行の証明書の失効

   証明書を取得するには、手順 2 ～ 5 を実行します。
2. **「ユーザー証明書 - SSL」**フォームの**「証明書のリクエスト」**をクリックして、「証明書リクエスト」フォームを表示します。
3. **「証明書リクエスト」**フォームで、適切な情報を入力して、フォームを送信します。前述の「Single Sign-On（SSO）認証」で説明しているとおり、インタフェースは、Netscape と Internet Explorer で少し異なります。

   必要事項を入力したフォームを送信すると、「証明書」フォームが表示され、証明書に記録された情報が示されます。
4. 情報が正しいことを確認した後、**「ブラウザへのインストール」**ボタンをクリックして、ブラウザに証明書をインストールします。
5. 「OK」をクリックして戻ります。

手動認証

手動認証を使用して証明書を取得するには、次の手順を実行します。

1. 「認証」フォームの**「手動承認 / 認証を使用」**を選択して、**「送信」**をクリックします。**「ユーザー証明書」**フォームが表示され、DN および連絡先情報の指定や、鍵のサイズ、使用方法およびリクエストする証明書の有効期間の選択を行うことができます。
2. 「ユーザー証明書」フォームの**「証明書のリクエスト」**をクリックして、「証明書リクエスト」フォームを表示します。
3. 「証明書リクエスト」フォームで、適切な DN および連絡先情報を入力して、フォームを送信します。（DN エントリと DN エントリは、カンマで区切ります。）登録フォームのドロップダウン・リストを使用して、鍵のサイズと認証（SSL）証明書（および必要な場合は暗号化証明書または署名証明書）を選択し、Oracle 認証局の管理者にフォームを送信します。

このユーザー・リクエストに固有のリクエスト ID が割り当てられます。証明書が承認されると、その検索にはこの ID を使用します。

管理者の承認を受信するまでは、証明書は使用可能になりません。

証明書が承認されたことを管理者から伝えられた後、証明書の取得フォームに移動して、リクエスト ID または DN を使用して証明書を検索し、証明書をインストールします。

証明書の検索、更新および失効

証明書リクエストが承認された後は、発行された証明書を取得して、確認およびインストールできます。証明書をリクエストしたときと同じマシンとブラウザを使用します。

OracleAS Single Sign-On 証明書または SSL 証明書は、一定の期間使用した後、満了日の前後に設定した期間内に更新できます。

発行された証明書は、確認時に、対象のユーザーまたはアクティビティに対してなんらかの理由で不適切または無効な場合は、失効させることができます。

次の項で、これらの証明書の操作について説明します。

- 証明書の取得
- 証明書の更新
- 証明書の失効

証明書の取得

手動認証による証明書リクエストの承認が通知された後、証明書を確認してインストールする必要があります。証明書は、通知されたシリアル番号を「ユーザー証明書」ページの「検索」フィールドに入力して検索できます。検索後にシリアル番号の横のラジオ・ボタンをクリックして選択してから**「詳細表示」**をクリックすると、生成時に使用されたデータを確認できます。「ブラウザへの新規発行の証明書のインポート」の説明に従って証明書をインストールできるようになります。

特定の証明書に対してこれらのデータが不適切な場合は、新しい証明書を申請して、不適切な証明書を失効させ、新しい証明書に置換する必要があります。

証明書の更新

OracleAS Single Sign-On 証明書および SSL 証明書のユーザーは、証明書を更新できます。

ユーザーは、証明書の満了予定日の前後に設定された一定日数の間、証明書を更新できます。デフォルトでは、この期間は、証明書の満了日の前後、それぞれ 10 日間です。ただし、管理者は、Web ベースの管理インタフェースの構成タブを使用して、この期間を変更することができます。ユーザーは、証明書を選択して**「詳細表示」**をクリックして、証明書を更新できます。

証明書の失効

OracleAS Single Sign-On 証明書および SSL 証明書のユーザーは、証明書を失効させることができます。

証明書にエラーまたは問題が見つかった場合や秘密鍵が盗まれた場合などには、証明書を失効させる必要があります。ユーザーは、新しい証明書に正しい情報を提供します。新しい証明書を使用すると、以前の証明書に関連する問題はすべてなくなります。

証明書を失効させると、OracleAS Certificate Authority リポジトリで失効済のマークが付けられ、次回 CRL が生成されるときに CRL に追加されます。ただし、失効した証明書は、ブラウザのデータベースから自動的には削除されません。手動で削除する必要があります。Netscape の場合、ブラウザのセキュリティ・アイコンをクリックして、「証明書」の下の「あなたの証明書」をクリックし、表示されたリストから失効した証明書を選択して「削除」をクリックします。

「サーバー / 下位 CA 証明書」タブ

どのサーバーの管理者も、サーバー証明書を取得して、他のサーバーまたはユーザーに対するそのサーバーの PKI 認証を有効にできます。そのためには、Oracle Wallet Manager（またはサード・パーティによる同等ツール）を使用して生成される PKCS #10 リクエスト・フォームが必要です。『Oracle Application Server セキュリティ・ガイド』の Oracle Wallet Manager に関する章を参照してください。

「サーバー証明書」タブ・ページで、次の手順を実行します。

1. 「ホーム」ページで**「サーバー / 下位 CA 証明書」**タブを選択して、サーバー証明書フォームを表示します。
2. **「証明書のリクエスト」**ボタンをクリックします。
3. **サーバー / 下位 CA 証明書リクエスト・フォーム**に、Oracle Wallet Manager で生成済の、必要事項が入力された PKCS #10 リクエスト・フォームを貼り付けて、必要な証明書のタイプを選択します。「認証（SSL）、「暗号化」、「署名」、「コード署名」または「CA 署名」のサーバー証明書をリクエストできます。下位 CA として使用するには、登録フォームの証明書の使用方法に**「CA 署名」**を指定します。表示されるドロップダウン・リストの選択肢から、リクエストした証明書の有効期間も選択します。
4. 適切な情報を入力し、管理者にフォームを送信します。

管理者がこのリクエストを承認するまで、サーバーの管理者は認証を取得できません。

下位 CA 証明書

1 つの企業内で異なる大陸に部門が存在するなど、単一の CA では実用的でない場合は、PKI 構造内に複数の CA を保持することができます。階層的な PKI では、ルート CA は、すべてのユーザーによって信頼されている単一の CA です。ルート CA の公開鍵は、セキュリティ・ドメインに対する信頼できるパスの開始位置として機能します。

OracleAS Certificate Authority は、ルート CA となる場合と、第三者 CA から下位 CA 証明書を取得する場合があります。OracleAS Certificate Authority が、別の CA の証明書署名を認証することで、下位 CA を作成することもできます。下位 CA がさらに下位レベルの CA に対して証明書を発行する場合、いわゆる証明連鎖が生まれます。いずれかの下位 CA が署名した個々の証明書には、ルート CA までのすべての CA の証明書が表示されている必要があります。それぞれの認証局の証明書は上位の CA によって署名されているため、特定の証明書の妥当性を検証するには、認証局のパスをルート CA までトレースします。

下位 CA 証明書を取得するには、次の手順を実行します。

1. 「ホーム」ページで**「サーバー / 下位 CA 証明書」**タブを選択して、下位 CA 証明書フォームを表示します。
2. **「証明書のリクエスト」**ボタンをクリックします。
3. **サーバー / 下位 CA 証明書リクエスト・フォーム**に適切な情報を入力した後、証明書の使用方法のタイプに**「CA 署名」**を選択して、管理者にフォームを送信します。

要求者は、管理者がこのリクエストを承認するまで、証明書を取得できません。

CA 証明書のインストール

Netscape の場合、**「証明書のリクエスト」**をクリックすると、OracleAS Certificate Authority によって、一連のダイアログ・ボックスが表示されます。これらのダイアログ・ボックスには、OracleAS Certificate Authority 証明書の受付けに必要な操作の説明が表示されます。表示されるそれぞれのダイアログ・ボックスで**「次へ」**をクリックし、最後のダイアログ・ボックスでは**「終了」**をクリックします。CA 証明書がブラウザに自動的にインストールされます。

Internet Explorer の場合は、CA 証明書のインストールを承認するか拒否するかを確認するメッセージが表示されるだけです。証明書を取得しない場合でも、この CA が証明書を発行しているサーバーを信頼するためだけに承認できます。ブラウザによって、証明書を保存するかどうか、または現在の位置から開くかどうかを確認するメッセージが表示されます。ブラウザに CA 証明書をインストールする場合は、**「このファイルを上記の場所から開く」**を選択して「OK」をクリックします。次に表示されるウィンドウで**「証明書のインストール」**を選択し、証明書のインストールを承認して、ブラウザのリポジトリに CA 証明書を格納します。

証明書失効リスト（CRL）の使用

CRL をブラウザにインストールしたり、ディスクに保存することにより、期限切れになった証明書や失効した証明書を認識および拒否できます。

「CRL の保存」をクリックすると、CRL に失効した証明書と期限切れになったすべての証明書が表示されます。ページの一番下に、**「ブラウザへの CRL のインストール」**ボタン、**「バイナリ CRL をディスクに保存」**ボタンおよび**「BASE64 CRL をディスクに保存」**ボタンが表示されます。

ブラウザへの CRL のインストール

証明書失効リストをインストールすると、個人または企業から提供された証明書が失効している場合、ブラウザに警告を表示できます。失効した証明書を使用すると、偽装の問題がある可能性、あるいは提供または使用している製品に問題がある可能性が示される場合があります。警告が表示されることによって、不適切である可能性がある操作を回避できます。

CRL のインストール手順は、ブラウザに応じて異なります。

- Netscape 7.x および Mozilla Firefox への CRL のインストール
- Internet Explorer（IE）への CRL のインストール

CRL をファイル・システムに保存する操作については、「ディスクへのバイナリ CRL または BASE64 CRL の保存」を参照してください。

Netscape 7.x および Mozilla Firefox への CRL のインストール

Oracle Application Server Certificate Authority の「ユーザー証明書」タブから、次の操作を実行します。

1. **「ブラウザへの CRL のインストール」**ボタンをクリックします。Netscape のダイアログ・ボックスが表示され、インポートが正常に終了したことが伝えられます。この CRL に対して自動更新が有効になっている場合、**「はい」**をクリックするとその設定が表示され、**「いいえ」**をクリックするとダイアログを終了できます。
2. **「はい」**をクリックすると、次の更新がスケジュールされている時間、およびその更新が実行されるサイトが表示されます。

次のナビゲーション・パスを使用して、CRL を手動で削除または更新できます。

- **Netscape** で、「編集」→「設定」→「プライバシーとセキュリティ」→「確認」→「CRL の管理」と選択します。
- **Firefox** では、「ツール」→「オプション」→「詳細」→「検証」→「CRL マネージャ」と選択します。

すでに CRL を取得していて、その CRL がインストール中の CRL 以降まで有効の場合は、インストールしようとしている CRL が、ブラウザにすでに存在する CRL より有効期間が短いことを示す小さなダイアログ・ボックスが表示されます。

Internet Explorer（IE）への CRL のインストール

IE の場合、CRL はブラウザに直接インポートされません。CA 証明書をインポートする場合と同様、IE では、「ディスクに保存する」または「このファイルを上記の場所から開く」のどちらを選択するかを確認するメッセージが表示されます。後者を選択すると、CRL はインポートされません。**「ディスクに保存する」**を選択した場合は、次の操作を実行します。

1. CRL を格納するディレクトリを選択します。
2. **「OK」**をクリックします。

ディスクへのバイナリ CRL または BASE64 CRL の保存

ブラウザに CRL をインストールする以外にも、次のことを実行できます。

- **「バイナリ CRL をディスクに保存」**をクリックし、CRL を格納するディレクトリを選択することにより、CRL のバイナリ・コピー（OCAcrl.crl）を保存する。
- **「BASE64 CRL をディスクに保存」**をクリックし、ターゲット・ディレクトリを選択することにより、Base64 形式のコピー（OCAcrlBase64.txt）を保存する。

ファイル・システム内のディスクに証明書失効リスト（CRL）を保存すると、他のプログラムはそれを使用して、個人または企業から提出された証明書のうち、失効しているものや期限切れのものを検出できます。こうした証明書の使用を回避することで、不適切なユーザーや不正なユーザーから、リソースおよびアプリケーションを保護できます。

CRL をディスクに保存するには、次の手順を実行します。

1. OracleAS Certificate Authority の「ユーザー証明書」ページに進みます。
2. **「ディスクへの CRL の保存」**をクリックします。
3. **「バイナリ CRL をディスクに保存」**または**「バイナリ BASE64 CRL をディスクに保存」**をクリックします。
4. 選択したディレクトリに CRL を保存します。
5. `$ORACLE_HOME/apache/apache/conf`, にある `http.conf` ファイルを変更し、SSLCARevocationFilePath パラメータを入れ、新しい CRL ファイルの入っているディレクトリをそのパラメータが指すようにします。たとえば、次のように入力します。

   ```
   SSLCARevocationFilePath=/usr/myname/certstoreject.crl
   ```

ブラウザへの新規発行の証明書のインポート

証明書に対するリクエストが認可された後、OracleAS Certificate Authority では、新しいウィンドウに詳細が表示されます。これにより、詳細が意図する内容と一致しているかどうかを確認できます。証明書の名前や有効期間などの属性が適切かどうかを確認します。詳細に重大なエラーがある場合は、この証明書を失効させて、リクエスト・フォームに正しい情報を指定して新しい証明書を申請します。

確認後、**「証明書のインポート」**ボタンをクリックして、ブラウザに証明書のコピーをインポートします。ブラウザの左下のステータス・バー領域に、「ドキュメント： 完了。」というメッセージが表示されます。次に「OK」をクリックします。

「証明書のインポート」をクリックしないで**「OK」**のみをクリックすると、サーバーには証明書のコピーが保持されますが、ブラウザには保持されません。このため、アプリケーション、ディレクトリまたは別のサーバーに対する認証が必要な場合は、証明書を提供できません。

証明書のインポート処理では、ルート CA までの CA の連鎖もインポートされます。ただし、Netscape および Mozilla Firefox では、ユーザー証明書とともにインポートされた CA 証明書は自動的には信頼されません。次の手順を実行して、信頼を確立する必要があります。

- **Netscape:**
  - 「編集」→「設定」→「プライバシーとセキュリティ」→「証明書」→「証明書の管理」をクリックします。
- **Mozilla Firefox:**
  - 「ツール」→「オプション」とクリックします。
  - 左側のペインで、「詳細」タブを選択します。
  - 右側のペインで、「証明書」項目を開きます。
  - 「証明書マネージャ」をクリックします。
- Netscape および Mozilla Firefox:
  1. **「認証局」**タブをクリックします。
  2. 適切な CA 証明書の名前を選択します。（リポジトリ用のパスワードの入力を要求される場合があります。）
  3. 「編集」をクリックします。
  4. Web サイトを識別して Web サイト接続を暗号化する、電子メール・ユーザーの署名または暗号化を行う、またはソフトウェア・メーカーを識別する場合に、この証明書を信頼することを指定する適切なチェック・ボックスを選択します。
  5. 「OK」を選択します。

  この手順により適切な信頼関係が確立されるため、SSL セッションを確立しようとすると、**「証明書の使用方法」**に選択した目的でこのインポート済証明書が発行した証明書は、ブラウザで信頼されます。

ブラウザからの Wallet のエクスポート（バックアップ）

システムまたはブラウザが破壊された場合に Wallet のコンテンツをリストアできるように、Wallet をエクスポートしてファイル・システムに保管してください。Wallet には、証明書、秘密鍵、および証明書を発行した信頼できる認証局に対する証明書の連鎖が含まれます。

次の手順を使用して、証明書をエクスポートします。

- **Netscape:**
  - 「編集」→「設定」→「プライバシーとセキュリティ」→「証明書」→「証明書の管理」をクリックします。
- **Mozilla Firefox:**
  - 「ツール」→「オプション」とクリックします。
  - 左側のペインで、「詳細」タブを選択します。
  - 右側のペインで、「証明書」項目を開きます。
  - 「証明書マネージャ」をクリックします。

Netscape 7.x と Mozilla Firefox のどちらについても、続けて次を行います。

1. エクスポートが必要な証明書を選択して「バックアップ」をクリックします。
2. PKCS #12 Wallet のファイル名を入力して「保存」をクリックします。
3. Netscape リポジトリのパスワードを入力して「OK」をクリックします。

   ウィンドウが開き、「セキュリティ デバイスのマスター パスワードを入力してください」というプロンプトが表示されます。正しいパスワード（ブラウザのリポジトリのパスワード）を入力すると、新しいウィンドウが表示されます。
4. この**「証明書バックアップ パスワードの選択」**ウィンドウで、PKCS #12 Wallet の暗号化に使用するパスワードを入力します。確認のため、同じパスワードをもう一度入力する必要があります。このウィンドウのパスワード品質メーターにより、パスワードの質に関する情報が示されます。
5. 「OK」をクリックします。アラートが表示され、バックアップが正常に終了したことが伝えられます。

Internet Explorer の場合は、次の手順で証明書をエクスポートします。

1. 「ツール」メニューから、**「インターネット オプション」**を選択します。

   ウィンドウが表示され、選択可能な 6 つのタブが示されます。
2. 「コンテンツ」タブを選択して、「証明書」ボタンをクリックします。

   「証明書マネージャ」ウィンドウが表示され、4 つのタブが示されます。これらのタブで、ユーザー自身の証明書、他人の証明書、信頼できる中間証明機関の名前および有効期限を参照できます。
3. 「個人」タブでは、エクスポートする特定の証明書をクリックします。
4. ウィンドウの下の**「エクスポート」**ボタンをクリックします。
5. 「証明書のエクスポート ウィザード」で「次へ」をクリックします。
6. 秘密鍵をエクスポートする場合は、「はい」ラジオ・ボタンをクリックします。（秘密鍵をエクスポートしない場合は、「いいえ」ラジオ・ボタンをクリックします。）「はい」をクリックすると、秘密鍵も格納されます。
7. 「次へ」をクリックします。
8. PKCS #12 を選択し、その下にある 2 つのチェック・ボックスを選択して、「次へ」をクリックします。

9. メッセージが表示されたら、パスワードを入力して、秘密鍵のセキュリティを保持します。パスワードは、2 回入力するように求められます。入力した内容が一致している必要があります。

   通常どおり、このパスワードは、この秘密鍵を検索または再利用するために記録しておきます。パスワードがないと、使用できません。

10. メッセージが表示されたら、暗号化された証明書および鍵の格納先のファイル・システム、パス名およびファイル名を入力します。

11. 新しいウィンドウに、選択した項目が表示されます。この情報を確認した後、「終了」をクリックします。

    「エクスポートが完了しました。」というメッセージが表示されます。

12. 「OK」→「閉じる」→「OK」をクリックして、この処理で使用したウィンドウを終了します。

ファイル・システムからの証明書のインポート

ファイル・システムに格納されているファイルから、ブラウザに証明書をインポートすることができます。ファイルのタイプは、拡張子が `.p12` の PKCS #12 である必要があります。ブラウザに証明書をインポートするには、Wallet の暗号化に使用したパスワードが必要です。

次の手順を使用して、Netscape ブラウザおよび Mozilla Firefox ブラウザで PKCS #12 Wallet から証明書をインポートします。

- **Netscape:**
  - 「編集」→「設定」→「プライバシーとセキュリティ」→「証明書」→「証明書の管理」をクリックします。
- **Mozilla Firefox:**
  - **「ツール」→「オプション」**とクリックします。
  - 左側のペインで、**「詳細」**タブを選択します。
  - 右側のペインで、「証明書」項目を開きます。
  - 「証明書マネージャ」をクリックします。

Netscape と Mozilla Firefox のどちらについても、続けて次を行います。

1. 「インポート」をクリックします。
2. インポートする証明書と鍵が入った PKCS #12 Wallet を選択して、**「開く」**をクリックします。
3. 表示されるポップアップ・ウィンドウで、Netscape リポジトリのパスワードを入力して**「OK」**をクリックします。

   ウィンドウが開き、「セキュリティ デバイスのマスター パスワードを入力してください」というプロンプトが表示されます。パスワードを入力すると、**「パスワード入力ダイアログ」**という新しいウィンドウが表示されます。
4. この新しいウィンドウで、PKCS #12 Wallet の復号化に使用するパスワードを入力して**「OK」**をクリックします。
5. アラートが表示され、証明書と秘密鍵のリストアが正常に終了したことが伝えられます。

Internet Explorer（IE）の場合は、次の手順で PKCS #12 Wallet から証明書をインポートします。

1. 「ツール」メニューから、「インターネット オプション」を選択します。

   ウィンドウが表示され、選択可能な 6 つのタブが示されます。

2. 「コンテンツ」タブを選択して、「証明書」ボタンをクリックします。「個人」タブには、ユーザー自身の証明書が表示されます。

3. 「インポート」をクリックします。「証明書のインポート ウィザード」ウィンドウが表示されます。

4. 「次へ」をクリックした後「参照」をクリックして、目的の証明書が含まれているディレクトリを選択します。

5. ダブルクリックしてフルパスをウィザードに入力し、「次へ」をクリックします。

6. 選択した Wallet のパスワードを入力します。

7. 「次へ」をクリックします。

8. Internet Explorer では、証明書のタイプに基づいて自動的に証明書ストアを選択することも、その他のラジオ・ボタンをクリックして、証明書ストアへのパスを入力し、証明書の格納先を指定することもできます。

9. 「次へ」をクリックします。

10. 「終了」をクリックします。

    IE によって使用される証明書ストアに、証明書を発行した CA の証明書が含まれていない場合は、証明書をストアに追加するかどうかを確認するダイアログ・ボックスが表示されます。

11. 「はい」をクリックします。この証明書があると、この CA（または同じ信頼連鎖の他の認証局）によって証明書が発行されているその他のサーバーまたはユーザーを認証できます。

    ダイアログ・ボックスが表示され、インポートが正常に終了したことが伝えられます。

12. 「閉じる」および「OK」をクリックして、IE の証明書およびセキュリティ領域を終了します。

A

コマンドライン管理

この付録は、Oracle Application Server Certificate Authority コマンドライン・ツール `ocactl` で使用可能なコマンドおよびオプションへのクイック・ヘルプ・リファレンスです。これらのコマンドの詳細な使用方法については、ユースケースとあわせて第 6 章を参照してください。

この付録では、管理コマンドライン・ツール `ocactl` を使用した OracleAS Certificate Authority 管理タスクの実行方法、および OracleAS Certificate Authority インスタンスのホストであるコンピュータを介した操作方法について説明します。

この付録の内容は、次のとおりです。

表 A-1 コマンドおよび構成操作へのリンク

一般的なトピック	参照先
基本的な管理 : コマンドおよび操作	■ コマンドライン・ツール ■ Oracle Certificate Authority Server の起動 ■ Oracle Application Server Certificate Authority Server の停止 ■ Oracle Certificate Authority サービスの状態の検索 ■ 権限付きパスワードの変更 ■ OracleAS Certificate Authority リポジトリ接続情報の更新
ルート証明操作	■ ルート認証局の証明書の再生成 ■ ルート CA 証明書の失効
SSL および OracleAS Single Sign-On の操作	■ CA SSL サーバー Wallet の SSO 形式への変換 ■ 認証局の SSL 証明書および Wallet の再生成 ■ SSO 認証の設定（linksso および unlinksso コマンド）
下位 CA 操作	■ OracleAS Certificate Authority からの下位 CA 署名 Wallet の生成 ■ 下位 CA 署名 Wallet のインストール / インポート ■ 下位 CA 用の CA SSL Wallet の生成
ログ / トレース操作	■ ログ / トレース・オプションの設定 ■ ログまたはトレース記憶域の消去

コマンドライン・ツール

OracleAS Certificate Authority 管理者は、コマンドライン・ツール ocactl を使用して、OracleAS Certificate Authority の様々な操作に必要なパラメータを指定します。（パスに oca/bin を追加することが必要になる場合もあります。）このツールを起動するたびに、OracleAS Certificate Authority 管理者のパスワードの入力が求められます。このパスワードは CA 署名のパスワードと常に同一です。（パスワードの入力時に、低速な telnet/rlogin セッションおよび [Back Space] を使用した場合は、パスワードの一部が表示されます。）

このコマンドの一般的な形式は次のとおりです。

```
ocactl operation -type related-parameters, if any
```

たとえば、OracleAS Certificate Authority を起動する場合は、次のコマンドを入力します。

```
ocactl start
```

別の例として、OracleAS Certificate Authority と Oracle Internet Directory の間で相互認証を行う証明書を公開する場合に、CASSL 操作の証明書および Wallet を生成するには、次のコマンドを入力します。

```
ocactl generatewallet -type CASSL
```

パラメータを含まないコマンドがあることに注意してください。パラメータを使用しないコマンドでは、キーワード「-type」も使用しません。

パラメータを必要とするコマンドでは、パラメータの前にキーワード -type を使用する必要があります。

唯一の例外は convertwallet コマンドで、表 A-2 の後で説明しているように、特別な構文になっています。

表 A-2 に、主な操作（アルファベット順）および関連パラメータを示します。その表の後で、convertwallet コマンドの追加パラメータについて説明します。

次の操作は、表に直接リンクされています。

changesecurity、clear、generatewallet、help、importwallet、linksso, renewcert、revokecert、set、setpasswd、start、stop、unlinksso、updateconnection

表 A-2 OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ

操作	パラメータ	意味
changesecurity	-server_auth_port port	OracleAS Certificate Authority により使用される ID 管理サービス（Oracle Internet Directory および OracleAS Single Sign-On Server）を新しい Oracle Internet Directory および OracleAS Single Sign-On に変更します。 新しい IM マシンおよびポート番号で oca.conf を更新し、OracleAS Certificate Authority を新しい OracleAS Single Sign-On Server に登録するときに指定されたポートを使用します。
clear	LOG、TRACE OracleAS Certificate Authority または ADMIN	選択したログまたはトレース・データのタイプ（OracleAS Certificate Authority または ADMIN）に対し、前述の set コマンドで指定した格納場所（ファイルまたはデータベース表）を消去します。（OracleAS Certificate Authority を実行中でない場合は、該当するデータがすべて消去されます。） 各コマンドの例は、第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「OracleAS Certificate Authority アクションのログまたはトレース」を参照してください。
convertwallet	次の列を参照	この表の後の「CA SSL サーバー Wallet の SSO 形式への変換」を参照してください。

表 A-2 OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ（続き）

操作	パラメータ	意味
generatewallet	CA、 CASSL、 または CASMIME	指定されたタイプの証明書および Wallet を生成します。このタイプには、認証局署名証明書と認証局 SSL 証明書があります。 generatewallet コマンドの例を示します。 `ocactl generatewallet -type CASSL` 次のタイプの Wallet が、指定された場所に格納されます。 ■ CA　OracleAS Certificate Authority リポジトリ ■ CASSL　`$ORACLE_HOME/oca/wallet/ssl` ■ CASMIME　OracleAS Certificate Authority リポジトリ CA の場合、鍵のサイズの選択肢は、512、1024、2048 および 4096 です。デフォルトは 2048 です。 CASSL および CASMIME の場合、鍵のサイズの選択肢は 512、768、1024 および 2048 で、1024 がデフォルトです。
help	コマンド名	コマンド名を指定するとコマンドの構文が表示されます。 help コマンドの例を示します。 `ocactl help setconfig`
importwallet	SUBCA	このコマンドは、Wallet を格納するディレクトリおよび管理者のパスワードの入力を要求した後、ewallet.p12 という Wallet を下位 CA サーバーの Wallet としてインストールします。 `importwallet` コマンドの例を示します。 `ocactl importwallet -type SUBCA` **注意：**Wallet をインポートする前に、Wallet に破損がなく、かつ自分で署名した証明書が 1 つ以上含まれることを確認してください。`Wallet` 表示コマンド `orapki` を使用して Wallet を検証できます。
linksso	なし	OracleAS Certificate Authority を OracleAS Single Sign-On に登録し、証明書を所有していない OracleAS Single Sign-On ユーザーが証明書をリクエストできるように OracleAS Certificate Authority 証明書の登録フォームを表示します。 （このコマンドでは OracleAS Certificate Authority サービスを停止する必要はありません。ただし、OracleAS Single Sign-On Server を再起動するまでこのサービスは有効になりません。）
renewcert	CA、 CASSL、 CASMIME	OracleAS Certificate Authority が実行中でない場合にこのコマンドを使用すると、新しい有効期間（日数）を入力するプロンプトが表示され、管理者は指定した証明書を更新できます。 renewcert コマンドの例を示します。 `ocactl renewcert -type CA`
revokecert （CA を失効させると、インストールしてある OracleAS Certificate Authority が動作しなくなります。）	CA WEBADMIN （この操作には、注意と確認が必要です。）	OracleAS Certificate Authority が動作中でない場合しか使用できません。ルート CA 証明書を失効させます。CA パラメータで指定可能なその他の理由コードについては、「ルート CA 証明書の失効」を参照してください。 revokecert コマンドの例を示します。 `ocactl revokecert -type CA -reason SUPERSEDED` 失効理由の詳細は、表 A-5 を参照してください。

表 A-2 OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ（続き）

操作	パラメータ	意味
set	LOG または TRACE ON または OFF OracleAS Certificate Authority または ADMIN	OracleAS Certificate Authority 構成を設定して、LOG または TRACE の後に指定した状態（ON または OFF）あるいはモード（OracleAS Certificate Authority または ADMIN）の追加パラメータを使用します。詳細は次を参照してください。 各コマンドの例は、第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「OracleAS Certificate Authority アクションのログまたはトレース」を参照してください。 この付録では、「ログ / トレース・オプションの設定」で説明しています。
setpasswd	CA、 DB、 CASSL、 または CASMIME	指定したロール（管理者、データベース管理者、認証局 SSL サーバーまたは電子メール暗号化）のパスワードをリクエストおよび再設定します。パスワードを変更する前に、OracleAS Certificate Authority を停止する必要があります。証明書の生成および使用方法に関するパスワードの使用、設定および格納については、このマニュアルの該当する項を参照してください。 `setpasswd` コマンドの例を示します。 `ocactl setpasswd -type DB`
start	パラメータなし	OracleAS Certificate Authority サービスを起動します。（OracleAS Certificate Authority を起動するには、OC4J、OHS およびデータベースが実行されている必要があります。OC4J および OHS は、コマンドライン・ツール `opmn` で制御します。） start コマンドの例を示します。 `ocactl start`
status	パラメータなし	OracleAS Certificate Authority サービスの状態を表示します。 status コマンドの例を示します。 `ocactl status`
stop	パラメータなし	OracleAS Certificate Authority サービスを停止します。 （データベース、Web サーバー、Oracle Application Server は停止されません。データベース接続プールが停止され、ログ出力、トレース出力および構成データ・ファイルが閉じられます。） stop コマンドの例を示します。 `ocactl stop`
unlinksso	なし	OracleAS Single Sign-On Server から OracleAS Certificate Authority を登録解除します。初期画面および登録フォーム画面は表示されなくなります。 （このコマンドでは OracleAS Certificate Authority サービスを停止する必要はありません。ただし、OracleAS Single Sign-On Server を再起動するまでこのサービスは有効になりません。）

表 A-2 OracleAS Certificate Authority（OCA）ocactl ツールの操作およびパラメータ（続き）

操作	パラメータ	意味

updateconnection	パラメータなし	Oracle Internet Directory に格納されている接続情報を OracleAS Certificate Authority 構成ファイルに書き込みます。*$ORACLE_HOME/oca/conf/oca.conf* この文字列は次の用途に使用します。
		■ OracleAS Certificate Authority リポジトリへの接続
		■ （証明書の公開に使用する）ディレクトリへの接続
		（この接続情報は、OracleAS Certificate Authority 管理者用の Web ベースのインタフェースの「一般」サブタブにある設定セクションに表示されます。）
		OracleAS Certificate Authority の接続情報は、最初に Oracle Application Server のインストール時に Oracle Internet Directory に書き込まれます。さらに、このデータは、Oracle Internet Directory からフェッチされて *oca.conf* にも書き込まれます。この情報は、OracleAS Certificate Authority が別のデータベースに移動された場合、または構成情報の変更があった場合には、同様に変更されます。その例として、RAC 対応データベースでの RAC ノードの追加や削除など、接続文字列内のノードやポートの変更があります。（データの移行は必要ありません。ポートを変更する場合は、『Oracle Application Server 管理者ガイド』のインフラストラクチャ・ポートの変更に関する項で説明している手順に従ってください。）
		注意：構成の設定を変更したら、その後で `ocactl updateconnection` を実行する必要があります。また、このコマンドの使用後に、次のコマンドを発行して OracleAS Certificate Authority を再起動する必要があります。
		`$ORACLE_HOME/oca/bin/ocactl stop`
		`$ORACLE_HOME/oca/bin/ocactl start`

CA SSL サーバー Wallet の SSO 形式への変換

表 A-2 では、`ocactl` を使用して発行できる大部分のコマンドの例を示しています。ただし、`convertwallet` コマンドは異なる構文を使用します。構文については、この項で例を示して説明します。

`ocactl` の `convertwallet` コマンドを使用して、CA SSL サーバーの Wallet（PKCS#12 形式の ewallet.p12）を、Oracle Single Sign-On 形式の Wallet（ファイル名 cwallet.sso）に変換します。このコマンドは、他のディレクトリを指定しないかぎり、現行の CA SSL Wallet の場所を使用します。

cwallet.sso を使用するメリットは、Wallet のパスワードを指定しなくても、HTTP Server を SSL モードで起動できることです。cwallet.sso を使用しない場合、PKCS #12 Wallet を使用して HTTP Server を SSL モードで起動する際に、Wallet パスワードがリクエストされます。

SSO 形式の Wallet は暗号化されており、ユーザーはファイルを開いたり鍵を抽出することができません。ただし、この Wallet は所有者権限のみで作成されるため、Wallet を保護するには、オペレーティング・システムのファイル権限が必要です。

つまり、`convertwallet` コマンドを使用すると、Wallet パスワードを要求することなく、OracleAS Single Sign-On Server で自動的に SSL モードで Web サーバーを起動できます。

`convertwallet` コマンドはルート・ユーザーとして実行する必要があります。*wlt-location* を目的の格納先で置き換えます。コマンドの構文は次のとおりです。

```
convertwallet -format SSO [-walletwrl wallet-location]
```

次に例を示します。

```
convertwallet -format SSO -walletwrl $ORACLE_HOME/wallets
```

オプションのパラメータ -walletwrl は、CA SSL PKCS #12 Wallet が、ファイル名 ewallet.p12 で格納されているディレクトリを指定する次のパラメータを識別します。

-walletwrl を指定すると、ocactl は、OCA によって作成されていない（OCA 以外から取得された）CA SSL Wallet を管理者が変換しようとしているとみなします。OCA のパスワード・ストアにはパスワードが含まれないため、管理者は元の CA SSL Wallet のパスワードを指定して、指定したディレクトリの Wallet を読み取る必要があります。Wallet が開かれた後、証明書は .sso 形式に変換され、-walletwrl *wallet-location* で指定した同一の場所に戻されます。

-walletwrl を指定しない場合、ocactl は、この Wallet を OracleAS Certificate Authority のインストール時に OracleAS Certificate Authority によって生成された CA SSL Wallet であるとみなします。そのため、このコマンドは、ocactl コマンドの使用を有効にする際に指定した OracleAS Certificate Authority 管理者のパスワードを使用して、CA SSL パスワードを含む内部パスワード・ストアを開きます。その後、このパスワードを使用し、CA SSL Wallet（$ORACLE_HOME/oca/wallet/ssl ディレクトリに格納）を開いて変換します。

Wallet の格納先を示す *wlt-location* を指定しない場合、デフォルトでこの Wallet は $ORACLE_HOME/oca/wallet/ssl（またはインストール時に指定した場所）に格納されます。

OracleAS Certificate Authority は、OHS、OracleAS Certificate Authority の OC4J、および OracleAS Certificate Authority がこの順序で再起動された後にのみ、$ORACLE_HOME/oca/wallet/ssl/ に格納されている新しい OracleAS Single Sign-On Wallet を使用します。（必要なインフラストラクチャを起動する手順は、『Oracle Application Server 管理者ガイド』の 4.1 項を参照してください。OHS、OC4J などの中間層コンポーネントを起動する方法については、4.2 項を参照してください。）

Oracle Certificate Authority Server の起動

OC4J、OHS およびデータベースを起動した後、管理者およびユーザーがアクセスするフォームをサポートする OracleAS Certificate Authority サービスを起動できます。OHS および OracleAS Certificate Authority の OC4J を起動するには、opmnctl コマンドを次の順序で使用します。

```
$ORACLE_HOME/opmn/bin/opmnctl startproc type=oc4j instancename=OracleAS Certificate
Authority
$ORACLE_HOME/opmn/bin/opmnctl startproc type=ohs
```

Oracle Application Server Certificate Authority を起動するには、次のコマンドを発行します。

```
ocactl start
```

このコマンドには管理者のパスワードが必要です。コマンドを実行すると、Oracle Application Server Certificate Authority エンジンが起動して、データベース接続プール、ログ出力ファイルおよびトレース出力ファイルが作成され、構成が初期化されます。

Oracle Application Server Certificate Authority Server の停止

stop コマンドを実行すると、OracleAS Certificate Authority サービスが停止します。その他のサービスには影響はありません。つまり、データベース、OracleAS および Web サーバーは変更されません。

OracleAS Certificate Authority サービスを停止するには、次のコマンドを発行して、OracleAS Certificate Authority の OC4J プロセスおよび OracleAS Certificate Authority そのものを停止します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=oc4j \
    instancename=OracleAS Certificate Authority
ocactl stop
```

Oracle Certificate Authority サービスの状態の検索

status コマンドを発行すると、Oracle Application Server Certificate Authority サービスの状態を表示できます。このコマンドには管理者のパスワードが必要です。コマンドを実行すると、OracleAS Certificate Authority エンジンにクエリーが行われます。レスポンスには、データベース接続プール、ログ出力、トレース出力およびパスワード・ストアの開閉状態が表示されます。

OracleAS Certificate Authority サービスの状態を取得するには、次のコマンドを発行します。

```
ocactl status
```

権限付きパスワードの変更

インストール時に、Oracle Application Server Certificate Authority のパスワード・ストアが作成されます。これには、OracleAS Certificate Authority 操作に必要な初期パスワードが格納されています。

表 A-3 パスワードのタイプおよび使用方法

パスワードのタイプ	パスワードの使用方法
OracleAS Certificate Authority データベース・ユーザー	OracleAS Certificate Authority 情報を含むデータベース表にアクセスできます。
CA SSL	認証局が SSL を使用して通信できます。また、Oracle Wallet Manager がこの Wallet にアクセスして、トラスト・ポイントを追加することもできます。インストール時に、ランダムに選択されたパスワードを使用して Wallet を暗号化します。このパスワードを使用して、Wallet に既知のパスワードを設定すると、この Wallet を Oracle Wallet Manager で開くことができます。

このパスワード・ストアの情報は、CA 署名パスワードでもある OracleAS Certificate Authority 管理者のパスワードを使用して暗号化されます。OCA 管理者のパスワードは、パスワード・ストアに格納されません。

インストール後、様々な管理者の権限付き操作のパスワードを変更できます。次に示すように、`ocactl` ツールで `setpasswd` コマンドを使用します。

表 A-4 権限付きロールおよび setpasswd コマンド

権限付きロール	ロールのパスワードの変更コマンド	新しいパスワードのその他の使用方法
Oracle Application Server Certificate Authority 管理者	`ocactl setpasswd -type CA`	認証局署名パスワード
CA SSL サーバー	`ocactl setpasswd -type CASSL`	CA SSL Wallet パスワード
Oracle Application Server Certificate Authority データベース管理者	`ocactl setpasswd -type DB`	OracleAS Certificate Authority がデータベースへのログインに使用する、データベース内の DB 用パスワード
管理者の署名通知メール	`ocactl setpasswd -type CASMIME`	パスワード・ストア内の CA SMIME パスワード

パスワードを変更する前に、OracleAS Certificate Authority を停止する必要があります。

これらのコマンドを実行して変更された内容は、次回、OracleAS Certificate Authority を起動したときに有効になります。OracleAS Certificate Authority を再起動した後、新しいパスワードが有効になります。

`ocactl` を使用するたびに、OracleAS Certificate Authority 管理者のパスワードが必要になります。このパスワードが認証されると、コマンドで指定したロール・タイプの新しいパスワードの入力がリクエストされ、パスワード・ストアのパスワードと置換されます。この結果は、OracleAS Certificate Authority 管理者の最新のパスワードを使用して再度暗号化されます。

ルート認証局の証明書の再生成

OracleAS Certificate Authority をルート認証局（CA）としてインストールすると、ルート CA 証明書および Wallet が作成されます。CA 鍵が危殆化した場合は、`ocactl` 管理コマンドライン・ツールを使用して、この証明書を再生成できます。新しい CA 証明書および秘密鍵は OracleAS Certificate Authority リポジトリに格納されます。この秘密鍵は、生成中にリクエストされたパスワードによって暗号化されます。

以前の CA 署名証明書のエントリ、および以前の CA 署名証明書が発行したその他のすべての証明書は無効になります。CA SSL、CA SMIME などの重要な Wallet は、再生成する必要があります。CA 署名 Wallet を再生成した後、以前の CA が発行した CRL は無効になります。

関連項目：

- 第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」。特に、「CA 署名 Wallet の再生成」および「CA SSL Wallet および CA S/MIME Wallet の再生成」。
- S/MIME の一般的な情報は、付録 G「OracleAS Certificate Authority での S/MIME」を参照してください。

CA 署名 Wallet およびその他の重要な Wallet を再生成できるのは、OracleAS Certificate Authority が正常にインストールされた後で、OracleAS Certificate Authority サービスが実行されていない場合のみです。

ルート CA 署名 Wallet を生成できるのは、OracleAS Certificate Authority を実行していない場合のみです。OracleAS Certificate Authority を実行中の場合は停止し、次のコマンドを使用してルート CA 署名 Wallet を再生成します。

```
ocactl generatewallet -type CA
```

この証明書は、OracleAS Certificate Authority リポジトリに格納されます。

署名鍵も OracleAS Certificate Authority リポジトリに格納され、OracleAS Certificate Authority 管理者のパスワードによって暗号化されます。

パスワード・ストアは、管理者のパスワードで暗号化されて、ディレクトリ `$ORACLE_HOME/oca/pwdstore` に保持されます。DB パスワードは、最初は管理者のパスワードと同じです。

関連項目： 付録 C「OracleAS Certificate Authority のトラブルシューティング」の「Metadata Repository のパスワードの記憶とリストア」

認証局の SSL 証明書および Wallet の再生成

CA SSL 証明書および Wallet はインストール時に生成され、OracleAS Certificate Authority のエンジンが HTTPS モードでリスニングするために使用されます。これらが危殆化または破壊された場合、あるいは CA 署名 Wallet が再生成された場合は、セキュアな通信を再度確立するために、これらを再生成する必要があります。

CA SSL Wallet を生成できるのは、OracleAS Certificate Authority を実行していない場合のみです。OracleAS Certificate Authority を実行中の場合は停止し、次のコマンドを使用して CA SSL 証明書および Wallet を再生成します。

```
ocactl generatewallet -type CASSL
```

この Wallet は、ディレクトリ `$ORACLE_HOME/oca/wallet/ssl` に格納され、生成中に指定したパスワードによって暗号化されます。

また、このコマンドでは OracleAS Single Sign-On 形式の CA SSL Wallet も生成され、$ORACLE_HOME/oca/wallet/ssl に `cwallet.sso` として格納されます。

ルート CA 証明書の失効

ルート CA 証明書の失効は、影響が大きい操作です。インストールした OracleAS Certificate Authority が機能しなくなり、すでに発行されている証明書が無効になります。この失効操作は、CA 鍵が危殆化された場合以外は実行しないでください。この操作を実行すると、新しい認証局をインストールできます。

`revokecert` コマンドを使用すると、ルート認証局または OracleAS Certificate Authority 管理者の証明書を失効させることができます。このコマンドが使用できるのは、OracleAS Certificate Authority が実行されていない場合のみです。

ルート認証局の証明書が失効した場合は、実行中の OracleAS Certificate Authority 操作用の新しいルート CA をインストールする前に証明書が必要になります。

新しい CA をインストールする場合、最初に、`revokecert` を使用して、パラメータで理由コードを指定し、以前の CA 署名 Wallet を失効させます。ルート証明書が失効すると、CA が発行したすべての証明書は整合性のない状態になります。そのため、ルート CA 証明書を失効させる前に、最初に、既存の CA が発行した証明書をすべて失効させ、証明書失効リストを更新します。この操作を実行しない場合、新しい CA 署名証明書の生成時に、以前の CA が署名した古い証明書すべてに、OracleAS Certificate Authority リポジトリで「無効」のマークが付けられます。

OracleAS Certificate Authority 管理者の証明書を失効させると、新しい証明書を取得するまで、管理者は、Web 上のすべての管理機能にアクセスできません。管理者が管理ホームページを開くと、新しい管理者の証明書を取得するために、新規登録が要求されます。

ルート認証局の証明書を失効させるには、最初に、OracleAS Certificate Authority を停止する必要があります。その後、次のコマンドを発行します。

```
ocactl revokecert -type CA -reason why
```

CA 証明書を失効させる主な理由は鍵の危殆化なので、実際のコマンドは次のようになります。

```
ocactl revokecert -type CA -reason KEY_COMPROMISE
```

それ以外の状況で失効が必要な場合は、失効理由エントリを、次の 8 つの句のうち、最も適したものに置換することができます。

表 A-5 `revokecert` コマンドで使用する失効理由

失効理由	説明
AFFILIATION_CHANGE	組織が、別の CA の使用を決定した。
CA_COMPROMISE	（CA 鍵が危殆化しているなど）なんらかの理由でルート CA を信頼できないため、新しい CA が必要になった。
CERTIFICATE_HOLD	なんらかの疑惑があるために証明書が保留されている。
CESSATION_OF_OPERATION	現在のルート CA が稼働を中止したため、新しい CA が必要になった。
KEY_COMPROMISE	ユーザーの秘密鍵が危殆化している。
REMOVE_FROM_CRL	証明書の状態は REVOKED であるが、この失効した証明書が CRL に追加されない。
SUPERSEDED	ルート CA の証明書が置換された。以前の証明書は削除し、新しい証明書をインストールする必要がある。
UNSPECIFIED	使用可能な理由がない、または指定されていない。これがデフォルトの理由コード。

OracleAS Certificate Authority からの下位 CA 署名 Wallet の生成

次の手順で、OracleAS Certificate Authority から下位 CA 署名 Wallet を生成できます。

1. 新しい Wallet を作成し、Oracle Wallet Manager または他の同等ツールを使用して証明書リクエストを生成します。

   関連資料：『Oracle Advanced Security 管理者ガイド』

2. サーバー / 下位 CA 登録フォームを使用して PKCS #10 リクエストを送信し、証明書の使用方法に「CA 署名」を選択します。
3. OracleAS Certificate Authority の管理フォームを使用して、下位 CA 証明書を発行します。パス長（下位 CA が所有できるレベルの数）を指定します。
4. サーバー / 下位 CA 登録フォームに移動します。**「CA 証明書のダウンロード」**をクリックすると、CA 証明書が表示されます。上位 CA が存在する場合は、その内容も記述されます。
5. CA の BASE64 証明書を画面からコピーして、信頼できる証明書として Oracle Wallet Manager にインポートします。CA とともにトラスト・ポイントが存在する場合は、**「信頼できる証明書のインポート」**オプションを使用して、1 つずつ Oracle Wallet Manager にコピーします。
6. サーバー / 下位 CA 登録フォームを使用して、下位 CA のシリアル番号または一般名を指定して、証明書の詳細を取得します。**「詳細表示」**をクリックして、下位 CA 証明書を BASE64 形式で表示します。
7. BASE64 形式の下位 CA 証明書をコピーして、ユーザー証明書として Oracle Wallet Manager にインポートします。
8. Oracle Wallet Manager を使用して、下位 CA 署名 Wallet を保存します。Wallet は `ewallet.p12` として格納されます。

下位 CA 署名 Wallet のインストール / インポート

この項の手順を実行すると、下位 CA 署名 Wallet をインストールおよび使用して、CA の階層を作成できます。この Wallet は、「OracleAS Certificate Authority からの下位 CA 署名 Wallet の生成」で説明されているように OracleAS Certificate Authority から生成したものか、自分で署名した Wallet、`mkwallet` または `orapki` ユーティリティで作成したもの、あるいは CMS などの X.509v3 準拠 CA から取得したもののいずれかです。

関連資料： X.509 v3 CA から SSL Wallet をインポートする場合、『Oracle Application Server 10*g* セキュリティ・ガイド』に示す Oracle HTTP Server の構成手順に従ってください。また、『Oracle Advanced Security 管理者ガイド』の Oracle Wallet Manager の説明も参照してください。

下位 CA 署名 Wallet をインポートする前に次を実行する必要があります。

- OracleAS Certificate Authority のインストールが成功すると、リポジトリ、パスワード・ストア、ルート CA 署名 Wallet および CA SSL Wallet が作成されます。
- Wallet に破損がなくかつ自分で署名した証明書が 1 つ以上含まれることを確認してください。`Wallet` 表示コマンド `orapki` を使用して Wallet を検証できます。

その後、次の手順を実行します。

1. OC4J および OHS が実行されている場合は、次のコマンドを使用して停止します。

```
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=oc4j instancename=OracleAS Certificate Authority
$ORACLE_HOME/opmn/bin/opmnctl stopproc type=ohs
```

2. `ocactl importwallet` コマンドを使用して、下位 CA 署名 Wallet をインストールします。

```
ocactl importwallet -type SUBCA
```

このコマンドを実行すると、管理者のパスワード、新しい下位 CA（`ewallet.p12`）の Wallet が格納されているディレクトリ、およびその Wallet のパスワードを入力するように要求されます。その後、その Wallet から新しい CA の証明書および秘密鍵がフェッチされ、OracleAS Certificate Authority リポジトリに格納されます。コマンドからの要求に対して入力する、新しい CA の Wallet に使用されるパスワードは、新しい CA の署名パスワードです。このパスワードは、OracleAS Certificate Authority 管理者のパスワードになります。

詳細は、付録 B「CA の階層の設定」を参照してください。

以前のルート CA 証明書のエントリ、および以前のルート CA が署名したその他のすべての証明書は無効になります。OracleAS Certificate Authority リポジトリに格納されている以前の CA 証明書および CA 鍵は、それぞれ新しい下位 CA 証明書および下位 CA 鍵によって上書きされます。新しい下位 CA が発行する証明書は、以前の下位 CA 証明書よりもシリアル番号が大きいため、新しい下位 CA 証明書のエントリおよびシリアル番号がリポジトリに追加されます。また、以前の CA が発行した管理者証明書はパスワード・ストアから削除されます。下位 CA 署名 Wallet のインポート中に、`ocactl` は、BasicConstraintsExtension と KeyUsageExtensions が DIGITAL_SIGNATURE、KEY_CERT_SIGN、CRL_SIGN および NON_REPUDIATION になるように、正しいビット数が設定されていることを確認します。これらの拡張子が設定されていない場合、この Wallet は下位 CA 署名 Wallet として受け入れられません。

下位 CA 用の CA SSL Wallet の生成

「認証局の SSL 証明書および Wallet の再生成」に示すとおり、CA SSL 証明書および Wallet はインストール時に生成されます。これらを使用すると、OracleAS Certificate Authority は、HTTPS モードでリスニングできるようになります。また、これらが危殆化または破壊された場合は、セキュアな通信を確立するために再生成できます。

下位 CA SSL Wallet は、OracleAS Certificate Authority が実行されていない場合に次のコマンドで生成することもできます。

```
ocactl generatewallet -type CASSL
```

この Wallet は下位 CA によって署名され、Wallet の生成中に指定したパスワードで暗号化されて、ディレクトリ `$ORACLE_HOME/oca/wallet/ssl` に格納されます。

ルート・ユーザーは、次のコマンドを使用して、この Wallet を OracleAS Single Sign-On 形式に変換できます。

```
ocactl convertwallet -format SSO
```

下位 CA をインストールすると、SSL 証明書を発行した以前の CA は存在しなくなります。OracleAS Certificate Authority に接続中のクライアントは、現行の CA 証明書を信頼します。以前の CA が発行した CA SSL は信頼できないため、下位 CA をインポートした後、または CA SSL Wallet が破壊または危殆化された後、CA SSL 証明書を再生成する必要があります。

この CA SSL 証明書および Wallet を生成した後、次の手順を実行します。

1. HTTP Server を起動します。
2. OC4J を起動します。
3. OracleAS Certificate Authority を起動します。

OracleAS Certificate Authority は下位 CA 証明書を使用して証明書リクエストへの署名ができるようになります。

ログまたはトレース記憶域の消去

次の管理コマンドライン・ツールを使用すると、既存のログ・ファイルまたはトレース・ファイルを管理者が選択して消去できます。消去コマンドの形式は次のとおりです。

```
ocactl clear -type {LOG |TRACE}  -mode {OCA|ADMIN}
```

コマンドは次のとおりです。

- `ocactl clear -type LOG -mode ADMIN`
- `ocactl clear -type TRACE -mode ADMIN`
- `ocactl clear -type LOG -mode OCA`
- `ocactl clear -type TRACE -mode OCA`

各コマンドを実行すると、対応するログ・データまたはトレース・データが消去されます。ログ・データを消去すると、OracleAS Certificate Authority リポジトリからデータが削除され、トレース・データを消去すると、`$ORACLE_HOME/oca/logs` からファイル `oca.trc` が削除されます。

OracleAS Certificate Authority リポジトリ接続情報の更新

証明書の公開に使用されるこの接続情報は、OracleAS Certificate Authority 管理者用の Web ベースのインタフェースの「一般」サブタブにある設定セクションに表示されます。この情報には、OracleAS Certificate Authority がリポジトリや Oracle Internet Directory に接続するときに使用する接続文字列などがあります。

`ocactl` コマンド `updateconnection` は、OracleAS Certificate Authority 構成ファイル `$ORACLE_HOME/oca/conf/oca.conf` に接続情報を書き込みます。

関連項目： changesecurity、clear、generatewallet、help、importwallet、linksso、renewcert、revokecert、set、setpasswd、start、stop、unlinksso および updateconnection については、表 A-2 を参照してください。

OracleAS Certificate Authority の接続情報は、最初に Oracle Application Server のインストール時に Oracle Internet Directory に書き込まれます。さらに、このデータは、Oracle Internet Directory からフェッチされて `oca.conf` にも書き込まれます。この情報は、OracleAS Certificate Authority が別のデータベースに移動すると、変更されます。

SSO 認証の設定（linksso および unlinksso コマンド）

Single Sign-On 認証を使用すると、リソースおよびアプリケーションへのアクセス速度が上がります。また、ユーザー名とパスワードのかわりに証明書を使用すると、より迅速かつ効果的にアクセスできるようになります。

OracleAS Certificate Authority には優先プロセスがあり、それによって、OracleAS Single Sign-On Server 認証済ユーザーはこのような証明書をリクエストおよび受信できます。

OracleAS Certificate Authority 管理者が `ocactl linksso` コマンドを実行すると、OracleAS Certificate Authority は OracleAS Single Sign-On Server に登録され、OracleAS Certificate Authority の証明書登録フォームが、証明書を持たない OracleAS Single Sign-On ユーザーに表示されます。このような高速処理機能を使用すると、SSO ユーザーは証明書をリクエストでき、その証明書を OracleAS Certificate Authority が発行した後、今後の認証で使用するためにその証明書をブラウザにインポートできます。

この処理機能の詳細は、第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」の「Single Sign-On および OracleAS Certificate Authority」を参照してください。概要は、第 7 章「OracleAS Certificate Authority 管理 : 高度なトピック」の「OracleAS Certificate Authority および高可用性機能」を参照してください。

`ocactl linksso` コマンドでは OracleAS Certificate Authority サービスを停止する必要はありません。ただし、OracleAS Single Sign-On Server を再起動するまでこのサービスは有効になりません。

ログ / トレース・オプションの設定

管理者は、ocactl set コマンドでデータのタイプおよびそのデータ生成のオン / オフを指定して、ロギング操作およびトレース操作を開始できます。このコマンドの形式は次のとおりです。

- ocactl set -type LOG -mode OCA -state ON
- ocactl set -type LOG -mode ADMIN -state ON
- ocactl set -type TRACE -mode OCA -state ON
- ocactl set -type TRACE -mode ADMIN -state ON

これらのコマンドで生成されたデータは、次の場所に格納されます。

- OracleAS Certificate Authority ログ・データの場合は、OracleAS Certificate Authority リポジトリ。
- ADMIN LOG データの場合は、$ORACLE_HOME/oca/logs にある admin.log ファイル。
- TRACE データは、$ORACLE_HOME/oca/logs にある次の 2 つのいずれかのファイルに格納されます。
  - OracleAS Certificate Authority トレースは、oca.trc（$ORACLE_HOME/oca/logs/oca.trc）に格納されます。
  - ADMIN トレースは、admin.trc（$ORACLE_HOME/oca/logs/admin.trc）に格納されます。

OFF コマンドを使用すると、ログ・データまたはトレース・データの生成処理が停止します。すでに収集されたデータは、ocactl clear コマンドを発行するまで、指定された場所に格納されています。このような ocactl clear コマンドの影響を受けるファイル（oca.trc、admin.trc または admin.log）は、ファイル・システムから削除されます。

B

CA の階層の設定

この付録では、下位認証局の取得方法およびインポート方法について説明します。下位認証局とは、証明書が上位の CA 機関で署名される CA です。下位 CA は、遠隔地の部門で使用するために、企業の本社にインストールされている元の Oracle Application Server Certificate Authority によって認可することができます。あるいは、新しい下位 CA は、OracleAS Certificate Authority とは異なる階層やルートを持った別の認証局によって認可（署名）することもできます。

次に、取得およびインポート処理の概要について説明します。

OracleAS Certificate Authority の管理者は、Oracle Wallet Manager（OWM）や第三者機関による同様の方式を使用して、下位 CA 署名 Wallet および証明書を取得します。最初の手順は、PKCS #10 証明書リクエストを生成することであり、これには通常、フォームに必要事項を入力します。OWM は、入力の完了したフォームを使用してリクエストを作成します。このリクエストは、リクエスト元のエンティティの認証に必要な情報がすべて記載されたテキストを暗号化した本文となります。

関連資料：『Oracle Advanced Security 管理者ガイド』

次に、管理者は、OWM インタフェースからこのリクエスト・フォームをコピーして、第三者機関の証明書発行インタフェースに貼り付け、証明書のリクエスト ID を受信します。この ID は、BASE64 形式の証明書が発行時にフェッチおよび表示するために使用できます。その他の CA については、CA 固有の手順を実行します。CA によっては、証明書がユーザーのメール ID に送信される場合もあります。

証明書を受信した後、OWM を使用してユーザー証明書としてインポートし、証明書の発行元である CA をトラスト・ポイントとして追加します。証明書が承認された後、OWM によって PKCS #12 形式の Wallet に格納されます。この Wallet は、下位 CA 署名 Wallet として使用できます。

OracleAS Certificate Authority の管理ツールにはインポート・オプションが用意されているので、管理者は、格納された下位 CA 署名 Wallet および証明書を、下位 CA として実行中の OracleAS Certificate Authority インスタンスにインポートできます。インポート操作では、OracleAS Certificate Authority の標準的な操作に適応するように、暗号化および格納場所の自動的な変更も行われます。この付録では、次のトピックでこれらの手順を説明します。

- 下位 CA 署名 Wallet の生成
- 新しい下位 CA 署名 Wallet のインストールおよび使用
- 下位 CA 用の CA SSL Wallet および CA SMIME Wallet の生成

下位 CA 署名 Wallet の生成

この後の手順では、OracleAS Certificate Authority の管理者向けに、下位 CA 署名 Wallet を生成する方法について説明します。

1. Oracle Wallet Manager またはサード・パーティによるツールを使用して、PKCS #10 リクエストを生成します。
2. OracleAS Certificate Authority のサーバー / 下位 CA 登録フォームを使用して PKCS #10 リクエストを送信し、証明書の使用方法として**「CA 署名」**を選択します。

   関連項目： 第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「「サーバー / 下位 CA 証明書」タブ」

3. OCA 管理フォームを使用して、下位 CA 証明書を発行します。（第三者機関への登録を使用した場合は、証明書が通知されるのを待ちます。）

   関連項目： 第 4 章「OracleAS Certificate Authority Administration および証明書の管理の概要」の「証明書リクエストの承認または拒否」

4. 証明書が承認されたら（第三者機関の発行元を使用した場合は、第三者機関から承認通知を受信したら）、サーバー / 下位 CA 登録フォームに移動して、**「CA 証明書の保存」**をクリックします。「拡張」ボタンが表示されます。「拡張」をクリックすると、CA 証明書が PKCS #7 形式の CA 連鎖の下に表示されます。トラスト・ポイントが存在する場合は、トラスト・ポイントも表示されます。
5. CA の BASE64 証明書を画面からコピーして、Oracle Wallet Manager に移動し、信頼できる証明書として OWM にインポートします。CA とともにトラスト・ポイントが存在する場合は、OWM の「信頼できる証明書のインポート」オプションを使用して、1 つずつ Oracle Wallet Manager にコピーします。

   関連資料：『Oracle Advanced Security 管理者ガイド』

6. サーバー / 下位 CA 登録フォームを使用して、下位 CA のシリアル番号または一般名を指定して、証明書の詳細を取得します。**「詳細表示」**をクリックして、下位 CA 証明書を BASE64 形式で表示します。
7. BASE64 形式の下位 CA 証明書をコピーして、ユーザー証明書として OWM にインポートします。
8. OWM を使用して、指定したファイル格納先に下位 CA 署名 Wallet を保存します。

新しい下位 CA 署名 Wallet のインストールおよび使用

この項の手順を実行することで、CA の階層を作成できます。新しい下位 CA の Wallet は、OCA または X.509 v3 準拠の CA で生成できます。下位 CA の Wallet は、それをインストールした後、証明書が発行される前に、Oracle Wallet Manager でただちに作成する必要があります。その時点で作成しておかないと、新しい下位 CA のインストール後に、こうした証明書は無効になります。第三者機関の発行元には、iPlanet Certificate Management System（CMS）や VeriSign 社などがあります。第三者機関の証明書を使用するには、証明書が、付録 D「拡張領域」で説明する OracleAS Certificate Authority 拡張機能の要件を満たしている必要があります。

関連項目： 第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「下位 CA 証明書」

1. Oracle Application Server Certificate Authority をインストールすると、OracleAS Certificate Authority リポジトリ、パスワード・ストア、ルート CA 署名 Wallet および CA SSL Wallet が作成されます。

   注意： 1 つのリポジトリでの OracleAS Certificate Authority のスキーマは、1 つの OCA とのみ併用できます。

   別の OracleAS Certificate Authority をインストールする場合、先行する OCA のインストールに使用したリポジトリは選択できません。同じリポジトリを選択すると、OCA 構成ツールが正常に実行されません。

   それによって、インストール処理を途中で終了し、インストール全体をやり直すことが必要になります。

   ---

2. OC4J および Oracle HTTP Server（Apache）が実行されている場合は、次のコマンドを使用して停止します。

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopproc type=oc4j instancename=oca
   $ORACLE_HOME/opmn/bin/opmnctl stopproc type=ohs
   ```

3. 次のコマンドを実行して、下位 CA 署名 Wallet をインストールします。

   ```
   ocactl importwallet -type SUBCA
   ```

   関連項目： 詳細は、付録 A「コマンドライン管理」を参照してください。たとえば、下位 CA 署名 Wallet をインポートするとき、`ocactl` では、適切な拡張領域に正しいビットが設定されている必要があります。Wallet が下位 CA 署名 Wallet として機能できるのは、正しいビットが設定されている場合だけです。BasicConstraintsExtension には、DIGITAL_SIGNATURE が設定されている必要があります。KeyUsageExtensions では、KEY_CERT_SIGN（証明書署名）、CRL_SIGN および NON_REPUDIATION の 3 つのビットがすべて設定されている必要があります。

   注意： importwallet を実行してエラー・メッセージが表示された場合は、ブラウザに証明書をインポートし、その詳細を表示してエラーを確認してください。Internet Explorer では、BasicConstraintsExtension と KeyUsageExtensions のどちらかに、適切な設定がされていないことが示されます。

下位 CA 署名 Wallet をインストールすると、次の処理が行われます。

a. 既存の管理者のパスワード、新しい下位 CA の Wallet（ewallet.p12）が格納されているディレクトリおよびその Wallet のパスワードを入力するように要求されます。

   コマンドからの要求に対して入力する、新しい CA の Wallet に使用されるパスワードは、新しい CA の署名パスワードです。このパスワードは、OracleAS Certificate Authority 管理者のパスワードになります。

b. その Wallet から新しい下位 CA の証明書、秘密鍵およびシリアル番号がフェッチされ、OracleAS Certificate Authority リポジトリに格納されます。

   この操作により、以前から OracleAS Certificate Authority リポジトリ内にあるレコードのうち、対応するものが上書きされます。したがって、以前のルート CA 証明書、鍵および署名証明書のパスワードは、新しい下位 CA 証明書、鍵およびパスワードにそれぞれ置換されます。

c. この下位 CA が発行する証明書のシリアル番号が下位 CA 証明書のシリアル番号より大きくなるように、下位 CA 証明書の現行のシリアル番号が更新されます。また、以前の CA が発行した管理者証明書はパスワード・ストアから削除されます。

この時点で、ルート・ユーザーとして、次の手順を実行する必要があります。

1. 既存の CA SSL は以前の CA によって署名されているため、新しい CA SSL Wallet を生成します。次のコマンドを使用します。

   ```
   ocactl generatewallet -type CASSL.
   ```

   生成された CA SSL Wallet は、新しい下位 CA 証明書によって署名されます。

2. 次のコマンドを実行して、この Wallet を OracleAS Single Sign-On 形式に変換します。

   ```
   ocactl convertwallet -format SSO
   ```

3. コマンドライン・ツール opmn を使用して、HTTP Server を起動します。

4. 同じコマンドライン・ツールを使用して、OC4J を起動します。

5. OracleAS Certificate Authority を起動します。その後の証明書リクエストはすべて、新しい下位 CA 証明書を使用して署名されます。

   関連資料：『Oracle Advanced Security 管理者ガイド』

別の CA の下位 CA にするための OracleAS Certificate Authority インスタンスの構成

大規模な組織で複数の部門が各地に分散している場合、ルート CA から下位 CA 署名 Wallet を取得して、その下位 CA を、別にインストールしてある OracleAS Certificate Authority にインストールすることをお薦めします。ルート CA 署名 Wallet を持つ親組織は、下位の組織または部門のそれぞれに、下位 CA 署名 Wallet を発行できます。このような下位 CA は、それぞれの場所で認証局（CA）として機能し、その組織に固有の証明書を管理します。下位 CA が別の下位 CA 署名 Wallet を発行しないようにするには、その下位 CA の Wallet がルート CA によって発行されていないときにパス長を設定します。

次の手順を実行すると、OracleAS Certificate Authority から下位 CA 署名 Wallet を生成および使用できます。

1. 新しい Wallet を作成し、Oracle Wallet Manager（OWM）を使用して PKCS #10 証明書リクエストを生成します。リクエストをコピーして OracleAS Certificate Authority に送信します。

   関連資料：『Oracle Advanced Security 管理者ガイド』

2. 第 8 章で説明したユーザー・インタフェースのサーバー / 下位 CA 登録フォームを使用して、OWM で生成した PKCS #10 リクエストに貼り付け、証明書の使用方法に「CA 署名」を選択します。

3. 第 4 章で説明した管理インタフェースの OracleAS Certificate Authority 管理フォームを使用して、下位 CA 証明書を発行します。パス長（下位 CA が所有できるレベルの数）を指定します。
4. 証明書が承認されたら、サーバー / 下位 CA 登録フォームに戻り、**「CA 証明書の保存」**をクリックすると、CA 証明書が表示されます。上位 CA が存在する場合は、その内容も記述されます。

   関連項目： 第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の「「サーバー / 下位 CA 証明書」タブ」

5. **「拡張」**をクリックして、BASE64 エンコード済の証明書を表示します。
6. CA の BASE64 証明書を画面からコピーして、信頼できる証明書として Oracle Wallet Manager にインポートします。この CA が CA 階層中で下位 CA の場合は、階層内のすべての CA を OWM にインポートする必要があります。「信頼できる証明書のインポート」オプションを使用して、1 つずつ Oracle Wallet Manager にコピーします。

この時点で、次の手順を実行し、証明書の詳細を OWM にコピーし、その Wallet を保存する必要があります。

1. サーバー / 下位 CA 登録フォームで、下位 CA のシリアル番号または一般名を使用して、目的の証明書を検索します。
   a. シリアル番号を使用する場合は、その左側にあるラジオ・ボタンをクリックして選択し、右側のハイパーテキスト・リンクをクリックして証明書を表示します。
   b. 一般名を使用する場合は、それを入力して「実行」をクリックし、表示されたリストから目的の証明書を選択します。
2. **「詳細表示」**をクリックして、下位 CA 証明書を BASE64 形式で表示します。
3. BASE64 形式の下位 CA 証明書をコピーして、ユーザー証明書として Oracle Wallet Manager にインポートします。
4. Oracle Wallet Manager を使用して、下位 CA 署名 Wallet を保存します。Wallet は ewallet.p12 として格納されます。

下位 CA 用の CA SSL Wallet および CA SMIME Wallet の生成

第 7 章の「CA SSL Wallet および CA S/MIME Wallet の再生成」に示すとおり、CA SSL Wallet はインストール時に生成されます。CA SSL Wallet を使用すると、OracleAS Certificate Authority は、HTTPS モードでリスニングできるようになります。また必要に応じて、セキュアな通信を再確立するために CA SSL Wallet を再生成できます。こうした再生成が必要になる状況には、Wallet が危殆化または破壊された場合、CA 署名 Wallet が再生成された場合、新しい下位 CA 証明書がインポートされた場合などがあります。

下位 CA SSL Wallet は、OracleAS Certificate Authority が実行されていない場合に次のコマンドで生成することもできます。

```
ocactl generatewallet -type CASSL
```

この Wallet は下位 CA によって署名され、Wallet の生成中に指定したパスワードで暗号化されて、ディレクトリ `$ORACLE_HOME/oca/wallet/ssl` に格納されます。

下位 CA をインストールすると、SSL 証明書を発行した以前の CA は存在しなくなります。OracleAS Certificate Authority に接続中のクライアントは、現行の CA 証明書を信頼します。以前の CA が発行した CA SSL は信頼されないため、下位 CA をインポートした後、または CA SSL Wallet が破壊または危殆化された後に、CA SSL 証明書を再生成する必要があります。

同様に、下位 CA をインポートした後、以前の CA が発行した CA SMIME Wallet は無効になります。「SMIME 電子メールの送信」が、OracleAS Certificate Authority 管理ページの「構成管理」の「通知」ページで有効な場合は、CA SMIME Wallet を生成して、アラートおよび通知に署名する必要があります。次のコマンドを使用して、CA SMIME Wallet を生成します。

```
ocactl generatewallet -type CASMIME
```

CA SSL Wallet および CA SMIME Wallet を生成した後、次の手順を実行します。

1. OC4J および HTTP Server を起動します。
2. OracleAS Certificate Authority を起動します。

OracleAS Certificate Authority は下位 CA 証明書を使用して証明書リクエストへの署名ができるようになります。

C

OracleAS Certificate Authority のトラブルシューティング

この付録では、OracleAS Certificate Authority の使用時に発生することがある一般的な問題とその解決策について説明します。説明する内容は次のとおりです。

問題と解決策

この項では、一般的な問題とその解決策について説明します。説明する内容は次のとおりです。

基礎的な問題および警告

この項では、OracleAS Certificate Authority の使用を進める前にあらかじめ対処しておく必要があるいくつかの問題について説明します。このような問題は「前提条件」と呼ばれます。

証明書リクエストで鍵のペアが生成されない（Windows）。

問題

Windows クライアント・マシンでは、この操作には、Service Pack 5 以上が必要です。

解決策

Microsoft 社の Web サイトにアクセスして、構成に必要なアップグレードをダウンロードします。

通常のユーザーでログインした後、管理者でログインできない。

問題

最初に SSL を介して通常のユーザーで OracleAS Certificate Authority にログインし、次に「認証管理」に移動しようとすると、JAZN エラーが発生します。これは、Web 管理者として登録されている場合でも、その権限でログインしなければ Web 管理者として認識されないためです。OracleAS Certificate Authority と管理者以外のユーザーの間に確立された SSL セッションはアクティブなままで、SSL セッションは変更されません。

解決策

Web 管理者でログインするには、次の手順を実行します。

1. Web 管理者の証明書がない場合は、Web 管理者として登録します。
2. ブラウザを終了します。
3. 認証用の Web 管理者証明書を選択して、Web 管理者としてログインします。

詳細は、第 5 章「Oracle Application Server Certificate Authority の構成」を参照してください。

注意： このログイン問題は、Netscape ブラウザの問題が原因です。

パスワードの変更には、OracleAS Certificate Authority のコマンドライン・ツール ocactl を使用する必要がある。

問題

OracleAS Certificate Authority では、多くのタスクにパスワードが使用されます。たとえば、CA SSL Wallet、内部 Metadata Repository および OracleAS Certificate Authority 管理者にはそれぞれ使用するパスワードがあります。場合によっては、パスワードは変更することをお薦めします。`ocactl` 以外のツールを使用して、これらのパスワードのいずれかを変更すると、通常、OracleAS Certificate Authority が停止します。

たとえば、`ocactl` 以外のツールを使用して OracleAS Certificate Authority の外部から Metadata Repository のパスワードを変更した場合、OracleAS Certificate Authority は起動しなくなります。

解決策

ここでは、OracleAS Certificate Authority の外部から各パスワードを変更する場合について個々に説明します。

OracleAS Certificate Authority の Metadata Repository のパスワード

OracleAS Certificate Authority のメタデータ・スキーマのパスワードは最初（インストール時）は管理者と同じパスワードに設定されていますが、いずれのパスワードも ocactl setPassword –type DB コマンドおよび ocactl setPassword –type CA コマンドを使用して個別に変更できます。前述のとおり、OracleAS Certificate Authority の外部から（すなわち、ocactl ツールを使用せずに）このパスワードを変更した場合、OracleAS Certificate Authority は起動しなくなります。このような状況が発生すると、`ocactl` を使用してリポジトリのパスワードをリセットすることもできなくなります。このような問題を解決するには、SYS や SYSTEM などの DBA としてデータベースにログインし、パスワードを元の値に戻す必要があります。

このパスワードの詳細は、「Metadata Repository のパスワードの記憶とリストア」を参照してください。

OracleAS Certificate Authority の管理者のパスワード

管理者のパスワードは、OracleAS Certificate Authority の外部からは変更できません。

OracleAS Certificate Authority の SSL のパスワード

OracleAS Certificate Authority の SSL のパスワード（*oca/wallet/ssl* にある SSL Wallet のパスワード）は、`ocactl` を使用してのみ変更する必要があります。Oracle Wallet Manager を使用してこのパスワードを変更すると、変更したパスワードが OracleAS Certificate Authority のパスワード・ストアには反映されなくなるため、OracleAS Certificate Authority が使用不能になります。ただし、`ocactl setpasswd CASSL` を使用して SSL のパスワードをリセットすることで、この状況から回復できます。

OracleAS Certificate Authority の S/MIME のパスワード

OracleAS Certificate Authority の S/MIME のパスワード（ファイル・システムではなくデータベースに格納されている S/MIME Wallet のパスワード）は、Oracle Wallet Manager を使用して変更することはできません。このパスワードは、`ocactl` を使用してのみ変更できます。

OracleAS Certificate Authority の Oracle Internet Directory のパスワード

これは、ランダムに生成されるパスワードです。このパスワードは、ocactl を使用して変更することはできません。しかし、Oracle Internet Directory の管理ツールを使用してこのパスワードを変更した場合、OracleAS Certificate Authority は新しいパスワードを知らないため、Oracle Internet Directory と通信を行うことはできません。

警告：一般的に、前述したルールにより、OracleAS Certificate Authority に関連するパスワードを変更する場合は、必ず `ocactl` を使用してください。その他のツールは、使用すると OracleAS Certificate Authority が停止するため、使用しないでください。

Metadata Repository のパスワードの記憶とリストア

問題

様々な機能、コンポーネントまたは組織に対して別々の管理者が存在する複雑なサイトでは、競合が発生することがあります。たとえば、あるデータベース管理者が、OracleAS Certificate Authority の Metadata Repository（スキーマ）のパスワードを変更する際は OracleAS Certificate Authority 自体を使用する必要があることを知らずに、変更したとします。この場合、OracleAS Certificate Authority は動作しなくなります。

解決策

次の各シナリオを理解しておくと、このような競合の回避または解決に役立ちます。

1. パスワード・ストア内の DB パスワードがデフォルト（インストール時に設定された `OCA-admin-password`）から変更されていない場合、（当初にリポジトリにより認識されていたパスワードを誰かが変更した後で）データベースへのアクセスを回復するには、次のコマンドを使用します。

   ```
   alter user OracleAS Certificate Authority identified by OCA-admin-password
   ```

   このようにしてリポジトリのパスワードを `OCA-admin-password` にリセットすることで、パスワード・ストア内にリポジトリのパスワードとして存在するパスワードと一致させます。

2. パスワード・ストア内の DB パスワードが変更されたが、OracleAS Certificate Authority 管理者がそのパスワード（たとえば、`new_DB_pswd_in_store`）を知っている場合、（データベース管理者などが）リポジトリ・パスワードを変更した後、OracleAS Certificate Authority 管理者は次のコマンドを使用してデータベース・アクセスを回復できます。

   ```
   alter user OracleAS Certificate Authority identified by new_DB_pswd_in_store
   ```

3. パスワード・ストア内の DB パスワードが変更されたが、OracleAS Certificate Authority 管理者がそのパスワードを知らない（または忘れた）場合、リポジトリのパスワードを変更すると、OracleAS Certificate Authority は動作しなくなります。これは、OracleAS Certificate Authority がパスワード・ストアに対して提供するパスワードが現在のリポジトリのパスワードと一致しない場合、データベース・アクセスが許可されないためです。リポジトリのパスワードが変更された場合、そのパスワードとパスワード・ストア内の DB パスワードが一致するようにどちらかを変更する必要があります。パスワード・ストア内の DB パスワードがわからないので、管理者は alter user コマンドでパスワードを入力できません。また、`ocactl` では、DB パスワードの変更に現在の DB パスワードの入力が求められるため、パスワード・ストア内の DB パスワードも変更できません。したがって、回復は不可能です。不明な DB パスワードは、いつまでも変更不可能です。

これらの解決策はすべて、alter user oca の起動に必要な権限を OracleAS Certificate Authority 管理者が保持していることを前提にしています。

ocactl を使用すると、「エラー : パスワード・ストアが存在しません。」というメッセージが表示される。

問題

Oracle Application Server 10*g* を当初インストールしたときに、OracleAS Certificate Authority をインストールするオプションが選択されていません。このため、パスワード・ファイルが作成されていません。パスワード・ファイルは、事後に当初の Oracle ホームに作成することはできません。OracleAS Certificate Authority ファイルの大部分はインストールされますが、OracleAS Certificate Authority は、Oracle Application Server 10*g* のインストール当初にインストールおよび構成されていないため、使用できません。

解決策

OracleAS Certificate Authority の新しいインスタンスを新しい Oracle ホームにインストールします。このインスタンスのインストール方法には次があります。

- OracleAS Infrastructure と同じコンピュータにインストールします。
- 別のコンピュータにインストールします。
- 独自の OracleAS メタデータ・リポジトリも同時にインストールします。
- 既存の OracleAS メタデータ・リポジトリを使用します。

次に示すように、実用性を考慮してこれらのオプションの組合せ方法を決めます。

OracleAS Certificate Authority のみのインストール

この場合、OracleAS Certificate Authority は、前にインストールされた OracleAS メタデータ・リポジトリを共有します。OracleAS Certificate Authority を OracleAS Infrastructure インスタンスと同じコンピュータにインストールする場合、パフォーマンス上の理由により、リポジトリを共有することをお薦めします。

OracleAS Certificate Authority とその独自の OracleAS メタデータ・リポジトリのインストール

OracleAS Certificate Authority を独自のリポジトリとともにインストールする場合、OracleAS Infrastructure とは別のコンピュータ上にインストールすることをお薦めします。別のコンピュータ上にインストールしない場合、同じコンピュータ上で 2 つのデータベースを実行する必要があり、パフォーマンスが低下する可能性があります。

関連資料

- Oracle Application Server のインストレーション・ガイドの Identity Management コンポーネントのみ（Oracle Internet Directory は除く）のインストールに関する項
- Oracle Application Server のインストレーション・ガイドの OracleAS Certificate Authority のトポロジに関する項

ブラウザの問題

この項では、ブラウザに関連する既知の問題について説明します。

注意： これらの問題は、ブラウザに関連していることが明白であり、特定の種類やバージョンのブラウザを使用している場合にのみ発生します。特に明記していないかぎり、これらの問題は通常ブラウザ自体の内部で解決できます。サポートが必要な場合は、ブラウザのベンダーにお問い合せください。

CA SSL サーバーの CN がマシン名と一致しない場合に、ブラウザが警告を表示する。

マシン名は、広範囲で使用されるため変更が煩雑になります。したがって、CA SSL サーバーの CN は、マシン名と同一にする必要があります。この場合、新しい証明書が必要です。

証明書リストですべてのユーザーが「USERS」として表示される。

問題

DN に複数の CN 構成要素があるとき、その DN の証明書の名前には、（右から）最初の CN 構成要素しか使用されません。このため、SSL 相互認証のポップアップでは、（MicroSoft Internet Explorer でも Netscape/Mozilla でも）すべての証明書のユーザーが「USERS」として一覧表示され、ユーザーを識別できません。

解決策

証明書を表示することにより、ユーザーを識別し、詳細情報を取得できます。

Netscape/Mozilla の場合

次の問題は Netscape クライアントにのみ影響します。

証明書の期限が切れているという警告が表示される。

問題

クライアントのタイムゾーンがサーバーのタイムゾーンよりも遅れている場合は、証明書の有効期限が切れたという警告が、一定期間表示される場合があります。これは、ユーザーのタイムゾーンでは、CA SSL 証明書がまだ有効ではないためです。

解決策

この問題は、タイムゾーンの差に応じて、比較的短時間で自然に解決されます。

下位 CA と CA の両方の SSL クライアント証明書が表示される。

問題

ユーザーが、CA からとその CA の下位 CA からの 2 つの SSL クライアント証明書を持つ場合は、下位 CA に対するクライアントの認証時に、両方の証明書が一覧表示されます。

解決策

その SSL サイトで使用されている CA に適した証明書を選択してください。

Internet Explorer（IE）の場合

次の問題は Internet Explorer クライアントにのみ影響します。

- ブラウザに CRL をインポートできない。
- セキュアな情報とセキュアでない情報の両方がページに含まれているというメッセージが表示される。
- オンライン・ヘルプを開くと、セキュリティ・アラートが生成される。
- 証明書リクエストの生成数が超過しているというメッセージが表示される。
- 証明書のインポート時に VB スクリプトのエラーが発生する。

ブラウザに CRL をインポートできない。

問題

Internet Explorer で「インポート ...」ボタンを使用すると、CRL は表示されますが、ブラウザには実際にはインストールされません。

解決策

CRL をディスクに保存し、Internet Explorer のメニューから、「ツール」→「インターネット オプション」→「コンテンツ」→「証明書」→「インポート」コマンドを選択します。これにより、「証明書のインポート ウィザード」が表示されます。ウィザードに示される手順に従い、インポートを実行します。

セキュアな情報とセキュアでない情報の両方がページに含まれているというメッセージが表示される。

問題

「ユーザー・ページ」→「手動認証」→「CA 証明書の保存」→「拡張」で**「ヘルプ」**をクリックすると、新しいウィンドウが開きます。このウィンドウに、セキュアな情報とセキュアでない情報の両方がページに含まれているというエラー・メッセージが表示される場合があります。これは、セキュリティが侵害されているわけではありません。

オンライン・ヘルプを開くと、セキュリティ・アラートが生成される。

問題

OracleAS Certificate Authority の使用中にオンライン・ヘルプを開くと、セキュリティ・アラートが表示されます。https URL を使用しているときに第 2 の https URL をコールすると、アラートが生成されることが報告されています。

解決策

「ツール」→「インターネット オプション」→「セキュリティ」→「レベルのカスタマイズ」でセキュリティのオプションを変更すると、この動作を回避できます。「設定」で「混在したコンテンツを表示する」を探し、その下の「有効にする」オプションを選択します。

証明書リクエストの生成数が超過しているというメッセージが表示される。

問題

Internet Explorer を使用して多数の証明書リクエストを生成した後で、追加のダイアログ・ボックス内にこのようなメッセージが表示されることがあります。

解決策

認証局に証明書リクエストを生成することを示す「はい」をクリックすることにより、続行できます。

Microsoft Internet Explorer のオンライン・ガイドで証明書リクエストの削除に関する項の手順を使用して、超過した証明書リクエストを削除できます。

証明書のインポート時に VB スクリプトのエラーが発生する。ブラウザにユーザー証明書をインポートしようとすると、次のような VB スクリプトのエラー・メッセージが表示されることがあります。

証明書のインポートに失敗しました。ブラウザのリポジトリをチェックしてください。管理者に問い合せてください。

このエラーが発生するのは、リクエストの発行時に間違った証明書キーストアを指定した場合です。

解決策

Internet Explorer で新しい証明書をリクエストする場合、正しいキーストア（Microsoft Enhanced Cryptographic Provider v1.0 など）を指定します。証明書のリクエスト画面に表示されるキーストアの選択肢は、証明書がリクエストされたマシンでのブラウザやスマートカード・サービスの存在有無およびタイプによって異なります。詳細は、第 8 章の「「ユーザー証明書」タブ」を参照してください。

ネットワークの問題

次のネットワークに関連するメッセージや問題は、OracleAS Certificate Authority の操作中に発生することがあるものです。

- SSO ユーザー名 / パスワードを使用して OracleAS Certificate Authority にログインすると、エラー・メッセージが表示される。
- ネットワーク・エラーのメッセージが表示される。
- OracleAS Certificate Authority が動作しなくなる。あるいはネットワークまたはサーバーのメッセージが表示される。

SSO ユーザー名 / パスワードを使用して OracleAS Certificate Authority にログインすると、エラー・メッセージが表示される。

問題

次のメッセージが表示されます。

禁止されています。このサーバーにある /oca/sso/ssoInitServlet にアクセスする権限がありません。

このメッセージは、IP アドレスの確認時に、ブラウザと OracleAS Single Sign-On Server の間で、複数の IP アドレスを持つプロキシ・サーバーが使用されている場合に表示されます。

解決策

- イントラネットを介してアクセスしている場合は、ブラウザのドキュメントに従って、プロキシを使用しないようにブラウザを構成する必要があります。
- イントラネットを介してアクセスしていない場合、または前述のとおりに変更しても問題が解決しない場合は、OracleAS Single Sign-On 構成ファイルの OssoIpCheck ディレクティブの値を、「off」に設定します。このサーバー側の変更を行うには、次のファイルに移動します。

  ```
  $ORACLE_HOME/Apache/Apache/conf/mod_osso.conf
  ```

  OssoIpCheck を含む行を編集して、次のようにします。

  ```
  OssoIpCheck off
  ```

- 構成ファイルを変更した後、次の停止コマンドおよび起動コマンドを実行して、Oracle HTTP Server を再起動します。

  ```
  dcmctl updateConfig -v -d
  opmnctl stopproc process-type=HTTP_Server
  opmnctl startproc process-type=HTTP_Server
  opmnctl stopproc process-type=OC4J_SECURITY
  opmnctl startproc process-type=OC4J_SECURITY
  ```

ネットワーク・エラーのメッセージが表示される。

問題

このメッセージは、Oracle Application Server Certificate Authority がある期間アクティブでなかった後に操作しようとしたため、ブラウザの認証が再度必要になるときに表示される場合があります。

解決策

「認証管理」タブに移動し、必要に応じて Web 管理者証明書を選択し、OracleAS Certificate Authority から認証を再度受ける必要があります。

OracleAS Certificate Authority が動作しなくなる。あるいはネットワークまたはサーバーのメッセージが表示される。

問題

このような問題は、OracleAS Certificate Authority がリポジトリや（証明書の公開に使用する）Oracle Internet Directory への接続に使用する接続文字列が、構成変更によって変更された場合に発生することがあります。変更の例としては、ポートや Real Application Clusters（RAC）ノードの変更があります。「接続を確立できません」または「内部サーバー・エラー」というメッセージが表示される場合があります。

解決策

次のコマンドを発行して、OracleAS Certificate Authority を有効にして新しい接続文字列を再取得します。

```
$ORACLE_HOME/oca/bin/ocactl updateconnection
```

このコマンドが完了すると、`$ORACLE_HOME/oca/conf/oca.conf` にある構成ファイルが更新されています。

このコマンドの使用後は、次のコマンドを発行して、OracleAS Certificate Authority を再起動する必要があります。

```
$ORACLE_HOME/oca/bin/ocactl stop
```

```
$ORACLE_HOME/oca/bin/ocactl start
```

証明書の問題

次の問題は、主に証明書または証明書管理に関連しています。

- ユーザー証明書をインストールしても CA 証明書がインストールされない（Netscape/Mozilla）。
- 「認証管理」タブへのアクセスまたは使用ができない。
- 管理者が別のマシンから作業する必要がある。
- 証明書リクエストの属性エラー

ユーザー証明書をインストールしても CA 証明書がインストールされない（Netscape/Mozilla）。

問題

ユーザー証明書をインストールしようとしても、失敗します。

解決策

- すべての CA 証明書または下位 CA 証明書には、サブジェクト DN に O（組織）という構成要素が含まれている必要があります。CA または下位 CA の DN に必須の構成要素は C、O および CN であり、各構成要素はカンマで区切る必要があります。
- Oracle Application Server Certificate Authority のインストール時またはルート CA の再生成時には、ユーザーは、少なくとも国、組織および一般名（C、O、CN）を含む DN を入力する必要があります。
- 下位 CA のインストール時には、CA 署名証明書のサブジェクト DN に、O（組織）RDN が含まれていることを確認します。

「認証管理」タブへのアクセスまたは使用ができない。

問題

「認証管理」の機能にアクセス、またはその機能を使用しようとしたら失敗します。

解決策

「認証管理」にアクセスするには、有効な Web 管理者証明書がブラウザにインポートされている必要があります。それらの証明書を申請して受信した上で、「認証管理」をクリックしてください。証明書を申請するには、管理設定タブで「Web 管理者登録」というラベルの付いたボタンをクリックします。

管理者が別のマシンから作業する必要がある。

問題

OracleAS Certificate Authority 管理者は、複数のマシンのうち、任意のマシンから証明書の管理タスクを行う場合があります。ただし、Web 管理者証明書は、OracleAS Certificate Authority Web 管理者としての認証を最初に行ったマシンのブラウザに存在します。

解決策

あるマシンから別のマシンに切り替えても証明書の管理タスクが行えるようにするには、以前のブラウザから証明書をエクスポートして、新しいブラウザにインポートする必要があります。手順は次のとおりです。

- Netscape/Mozilla で証明書をエクスポートするには、「セキュリティ」→「証明書」→「あなたの証明書」で Web 管理者証明書を選択し、「バックアップ」を選択します。
- Netscape/Mozilla で証明書をインポートするには、「セキュリティ」→「証明書」→「あなたの証明書」→「インポート」を選択します。
- Internet Explorer で証明書をエクスポートするには、「インターネット オプション」→「コンテンツ」→「証明書」→「個人」→「Web 管理者証明書を選択」→「エクスポート」を選択します。
- Internet Explorer で証明書をインポートするには、「インターネット オプション」→「コンテンツ」→「証明書」→「個人」→「インポート」を選択します。

証明書リクエストの属性エラー

問題

証明書リクエストで属性またはポリシーのエラーに関するメッセージが返されます。

このエラーは通常、リクエストで指定された DN 内に間違った属性タイプが使用されていることが原因で発生します。

解決策

リクエストの DN に次の X.500 属性タイプのみが含まれていることを確認します。

属性タイプ	説明
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
Email	emailAddress
DC	domainComponent

たとえば、次のリクエストは、サポートされていない `uid` 属性を使用しているため、無効です。

```
uid=mkhan,ou=People,o=sspwd.pk.
```

この問題を解決するには、表に示されたサポートされる属性タイプのみを使用して、リクエスト DN を記述しなおします。

シングル・サインオンの問題

一部の問題は、主にシングル・サインオン機能に関連しています。

- SSO の証明書に表示される名前が「USER」になる。
- 鍵の生成中に VB スクリプトのエラー・メッセージが表示される。
- 「ページを表示できません」というメッセージが表示される（Internet Explorer）。
- IE で SSO ログイン・ページに進むと、セキュリティ警告ダイアログが表示される。
- Single Sign-On を介して取得した証明書が SSL 認証用に表示されない。

SSO の証明書に表示される名前が「USER」になる。

問題

これらの証明書には、一般名または DN は表示されません。証明書は、証明書のシリアル番号によってのみ区別されます。

解決策

「表示」をクリックして証明書のシリアル番号を確認し、目的のシリアル番号で特定される証明書を選択します。

鍵の生成中に VB スクリプトのエラー・メッセージが表示される。

問題

Oracle Application Server Single Sign-On では、ポップアップ・ウィンドウの「送信」をクリックして、証明書をリクエストします。待機するように求めるメッセージや進行状況が表示されないため、ユーザーが「送信」を再度クリックすることがあります。この場合にこのエラーが発生します。

解決策

「送信」を 1 回だけクリックして、証明書が戻されるまで待機します。

「ページを表示できません」というメッセージが表示される（Internet Explorer）。

問題

ユーザー名とパスワードを入力して OracleAS Single Sign-On にログインした後、SSL を選択して認証を変更した場合、Internet Explorer の既知の不具合のため、「ページを表示できません」というエラーが表示されます。

解決策

ページの再ロードを試行します。これでも問題が解決しない場合は、ブラウザの現行セッションを終了し、OracleAS Certificate Authority に戻って再試行します。

IE で SSO ログイン・ページに進むと、セキュリティ警告ダイアログが表示される。

これは想定内の動作です。これは、SSL プロトコル（https）から SSL 以外のプロトコル（http）に切り替えたために発行される警告です。特に処理は必要ありません。

Single Sign-On を介して取得した証明書が SSL 認証用に表示されない。

問題

Mozilla ブラウザを使用して OracleAS Single Sign-On にログインし、証明書を取得してインポートした後も、インポートした証明書がクライアント認証ウィンドウに表示されない場合があります。

解決策

- ユーザーが証明書をリクエストするとき、目的の「使用方法」に「認証」を指定しなかった場合、その証明書は認証用のクライアント認証ボックスに表示されません。

  選択した使用方法を確認するには、シリアル番号で証明書を検索し、その詳細を表示します。「使用方法」に「クライアント認証」が表示されない場合、この証明書は SSL 認証用には使用できません。

  この場合の解決方法は、新しい証明書をリクエストし、必ず証明書の「使用方法」の 1 つに「認証」を指定します。

- この他、証明書が表示されない理由として、CASSL 証明書がなんらかの原因で使用不能になっていることがあります。この場合、管理者は CASSL 証明書を置き換える必要があります。

関連項目：

第 4 章の「OracleAS Certificate Authority のインストールのデフォルト値」
第 7 章の「CA SSL Wallet および CA S/MIME Wallet の再生成」

バックアップの保護の問題

次の問題は、障害が発生した後に実行できるリカバリに関連しています。

OracleAS Certificate Authority の内部リポジトリのリカバリ可能性を保証する。

問題

エラーおよび予測できない事象によって、OracleAS Certificate Authority 操作を継続できなくなる可能性があります。

解決策

Metadata Repository のバックアップを定期的に取ります。詳細は、『Oracle Application Server 管理者ガイド』のバックアップの戦略および手順に関する項、ならびにリカバリの戦略および手順に関する項を参照してください。

リカバリの問題

この項では、OracleAS Certificate Authority の操作に影響する大きな問題からの回復方法について説明します。

- OracleAS Certificate Authority 管理ページの「認証管理」タブをクリックすると、ブラウザの 404 エラーが返される。

OracleAS Certificate Authority 管理ページの「認証管理」タブをクリックすると、ブラウザの 404 エラーが返される。

問題

特定の状況下では、OracleAS Certificate Authority 管理者が「認証管理」ページにアクセスできない場合があります。ブラウザには、「404/Page Not Found」というエラーが表示されます。このエラーの原因として次の要因が考えられます（ただし、これらに限定されません）。

- 管理者の証明書が 1 つのブラウザにインストールされているが、別のブラウザから「認証管理」ページにアクセスしようとしました。
- CA 証明書を申請したときに、DN はマシン名のみを指定し、ドメイン情報が省略されました。たとえば、「CN=asunmach17.us.mycompany.com admin user,C=US」ではなく「CN=asunmach17 admin user,C=US」が指定されました。

解決策

CA 証明書のドメイン情報が正しくないことがこの問題の原因である場合、次の手順を使用して、CA の SSL Wallet を再作成し、影響を受けたコンポーネントをリフレッシュします。

> **警告：これは最終手段の解決策であるため、不用意に使用しないようにしてください。これ以外に選択肢がなくなった場合のみ実行してください。**

1. 新しい CA SSL Wallet を再生成します。CN がホスト名と同じであることを確認します。ドメインはオプションです。

   詳細は、第 7 章の「CA SSL Wallet および CA S/MIME Wallet の再生成」を参照してください。
2. OHS を再起動します。
3. CA 証明書が再生成された後、CASSL Wallet を作成します。この操作は新しい CA によって実行されます。
4. OHS を再起動し、新しい CA SSL Wallet を採用します。
5. クライアントのブラウザと OracleAS Certificate Authority サーバー間の SSL セッションをリフレッシュします。

一般的な問題

次の問題は一般的な性質の問題であり、前述のどのカテゴリにも分類されません。

- ページのロードに時間がかかりすぎる、またはページがハングアップする。
- Outlook Express に S/MIME 署名証明書が表示されない。
- CA SSL サーバーの CN について、警告が表示される。

ページのロードに時間がかかりすぎる、またはページがハングアップする。

問題

OracleAS Certificate Authority が長時間稼働していた後などに、こうした処理の遅延が生じることがあります。

解決策

OracleAS Certificate Authority の OC4J インスタンスを再起動すると、操作が再び高速になります。

関連項目： パフォーマンスに関する追加のヒントは、第 7 章の「OracleAS Certificate Authority のパフォーマンス・チューニング」を参照してください。

再起動の操作については、第 4 章の「Oracle Application Server Certificate Authority の起動および停止」を参照してください。

Outlook Express に S/MIME 署名証明書が表示されない。

問題

一部の Windows 環境では、Outlook Express で SMIME 署名証明書を選択しても、証明書は表示されません。これは、Microsoft Outlook がインストールされているためです。

解決策

Outlook Express ではなく、Microsoft Outlook を使用する必要があります。

関連項目： 付録 G「OracleAS Certificate Authority での S/MIME」

CA SSL サーバーの CN について、警告が表示される。

問題

CA SSL サーバーの CN がマシン名と一致しない場合に、この警告が表示されます。

解決策

CN とマシン名を同じにする必要があります。

その他の問題

その他の解決策については、*MetaLink*、`http://metalink.oracle.com` を参照してください。問題の解決策が見つからない場合は、オラクル社カスタマ・サポート・センターに問い合せてください。

関連資料： Oracle Application Server のリリース・ノート : Oracle Technology Network のサイト `http://www.oracle.com/technology/documentation/index.html` から入手できます。

D

拡張領域

Oracle Application Server Certificate Authority は、X.509 v3 および IETF の PKIX の規格に準拠しています。また、この付録で説明する標準拡張領域もサポートしています。

証明書の使用方法

OracleAS Certificate Authority では、ユーザーは、意図した用途およびエンタープライズ・ポリシーに合うように、リクエストする証明書の機能を選択できます。出荷時のデフォルトは「認証、署名、暗号化」ですが、管理者が別の選択項目を構成することもできます。この場合、その項目が、そのサイトの事前選択済デフォルトになります。表 D-1 に選択可能な項目を示します。

表 D-1 証明書の使用方法のタイプ

機能	説明
認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。）
暗号化	電子ドキュメントの暗号化および復号化を可能にします。
署名	（S/MIME（Secure Multipurpose Internet Mail Extension）を使用して）電子メールなどの電子ドキュメントに対する検証可能な署名を可能にします（また、これらの電子ドキュメントの改ざんを防ぎます）。
認証、暗号化	この両方の目的に証明書を使用できます。
認証、署名	この両方の目的に証明書を使用できます。
認証、署名、暗号化	この 3 つの目的すべてに証明書を使用できます。
署名、暗号化	この両方の目的に証明書を使用できます。
CA 署名	ユーザーの証明書または証明書失効リスト（CRL）の署名に使用します。
コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します（また、これらの改ざんを防ぎます）。

証明書へのポリシー適用

表 D-2 に説明するように、証明書には、意図された使用方法によって異なるポリシーが適用されます。

表 D-2 特定の証明書使用方法に適用されるポリシー

証明書の使用方法	BasicConstraints（重要）	KeyUsage（重要でない）	拡張された KeyUsage（重要でない）	サブジェクト代替名 拡張機能（重要でない）
CA 証明書	CA フラグは TRUE に設定されています。 PathLength: + ルート CA（インストール時に生成）、値は 3 にハードコードされています。 ルート CA（OCACTL を使用して生成）、値は選択可能です。	署名証明書（鍵） 署名 CRL		
クライアント認証		デジタル署名	clientAuth	rfc822Name=email AND/OR otherName=UID
サーバー認証		デジタル署名 キー暗号化	serverAuth	rfc822Name=email AND/OR otherName=UID
署名		デジタル署名 否認防止	emailProtection	rfc822Name=email AND/OR otherName=UID
暗号化		データ暗号化 キー暗号化	emailProtection	
コード署名		デジタル署名	codeSigning	rfc822Name=email AND/OR otherName=UID

E

SSO での SSL および PKI の有効化

この付録では、OracleAS 10*g*（10.1.4.0.1）において、Oracle Application Server Single Sign-On での SSL と PKI の有効化に必要なすべての手順について説明します。コンテキストの追加説明の詳細な説明は、次のマニュアルに収録されています。

- 『Oracle Application Server Single Sign-On 管理者ガイド』
- 『Oracle HTTP Server 管理者ガイド』
- 『Oracle Advanced Security 管理者ガイド』

デフォルトでは、OracleAS Single Sign-On は Oracle HTTP サーバーの HTTP ポートを使用し、Single Sign-On の認証はユーザー名およびパスワードに基づきます。ただし、ユーザーを本人の証明書に基づいて認証するよう、SSL に対して OracleAS Single Sign-On を構成することができます。構成手順については、OracleAS Single Sign-On および OHS のドキュメントですでに説明していますが、それらの説明は様々な場所に分散しています。ユーザーの便宜を図るため、それらの手順をこの付録でまとめます。

この機能を構成するためには、OracleAS Single Sign-On Server に対する SSL の有効化、証明書を使用するための OracleAS Single Sign-On の構成、および SSL を有効化した OracleAS Single Sign-On Server への OracleAS Certificate Authority の登録という、3 つの手順を個別に実行する必要があります。

注意： このドキュメントは、UNIX と Windows の両方のプラットフォームに適用されます。ただし、Windows の場合、パスのセパレータはスラッシュ（/）ではなく円記号（¥）が使用されており、変数はドル記号（$）ではなくパーセント（%）を使用して間接参照されています。

OracleAS Single Sign-On での SSL および PKI の有効化という目的を達成するには、次の 3 つの手順を実行する必要があります。

- SSO での SSL の有効化
- SSO での PKI の有効化
- SSL を有効化した SSO への仮想ホストの再登録

SSO での SSL の有効化

自動または手動のいずれかの方法を使用して OracleAS Single Sign-On に SSL を構成できます。

SSL の自動構成

一般的なトポロジ用に、SSL 構成ツールでは、Oracle HTTP サーバーのインストール後に SSL の有効化に必要な手順を実行できます。このツールおよびその実行方法の詳細は、『Oracle Application Server 管理者ガイド』の SSL 構成ツールの使用方法に関する項を参照してください。

SSL の手動構成

注意： 詳細は、『Oracle Application Server Single Sign-On 管理者ガイド』（特に、SSL の有効化に関する章）を参照してください。

この項で使用する ORACLE_HOME は、OracleAS Single Sign-On Server がインストールされている場所です。

1. $ORACLE_HOME/opmn/conf/opmn.xml ファイルを編集します。
2. 「id="HTTP_Server"」を検索し、その 4 行下にある次の行を見つけます。

   ```
   <data id="start-mode value="ssl-disabled">
   ```

   この行を次のように変更します。

   ```
   <data id="start-mode value="ssl-enabled">
   ```

3. 新しい xml ファイルを使用して opmn を再起動します。

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

4. $ORACLE_HOME/Apache/Apache/conf/ssl.conf ファイルを編集します。
5. </VirtualHost> の前の行で、次の記述を追加します。

   ```
   RewriteEngine on
   RewriteOptions inherit
   ```

6. 次のように、SSL セッションのキャッシュを無効にして、OracleAS Single Sign-On からのログアウト時にハンドシェイクを実行します。

   ssl.conf.sec の SSLSessionCache ディレクティブと SSLSessionCacheTimeout ディレクティブをコメントアウトします。

   ```
   # SSLSessionCache
   # SSLSessionCacheTimeout 15
   ```

   その後、次の行を追加します。

   ```
   SSLSessionCache none
   ```

7. Wallet を更新します。OracleAS Certificate Authority が同じマシンにインストールされている場合は、OracleAS Certificate Authority の SSL Wallet を OracleAS Single Sign-On Server 用に使用できます。

   そうでない場合は、Oracle Wallet Manager を使用して OracleAS Single Sign-On Server 用の Wallet を生成する必要があります。『Oracle Advanced Security 管理者ガイド』内の関連項目を参照してください。

   通常、OracleAS Certificate Authority によって生成された既存の SSL Wallet は、/app/oracle/oca/wallet/ssl にあります。このファイル（ssl.conf）内の SSLWallet ディレクティブを探して、コメントアウトします。

   ```
   # SSLWallet file:/app/oracle/product/sec_inf/Apache/Apache/conf/ssl.wlt/default
   ```

その後、次のような新しいディレクティブを挿入します。

```
SSLWallet file:/app/oracle/oca/wallet/ssl
```

8. 次の行をコメントアウトすることによって、クライアント認証を設定します。

```
# SSLVerifyClient require
```

その後、次のような新しい行を挿入します。

```
SSLVerifyClient optional
```

9. SSL ポートを使用するよう、OracleAS Single Sign-On Server を再構成します。コマンドの形式は次のとおりです。

```
$ORACLE_HOME/sso/bin/ssocfg.sh https  hostname  ohs_ssl_port
```

したがって、ホスト名が sso.us.oracle.com で、ohs_ssl_port が 4443 の場合、コマンドは次の行になります。

```
$ORACLE_HOME/sso/bin/ssocfg.sh https  sso.us.oracle.com 4443
```

10. OracleAS Single Sign-On がインストールされている Oracle ホームで、次のコマンドを実行して sso に mod_osso を再登録します（UNIX）。

```
$ORACLE_HOME/sso/bin/ssoreg.sh \
-oracle_home_path $ORACLE_HOME   -site_name sso   -config_mod_osso TRUE \
-mod_osso_url  https://hostname.domain.com:ohs_ssl_port \
–update_mode CREATE   -u root
```

注意： Windows の場合、コマンドは次のとおりです。

```
%ORACLE_HOME%¥sso¥bin¥ssoreg.bat
-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
```

---

11. 次のコマンドを実行して、OracleAS Single Sign-On 用の OHS を再起動します。

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

SSO での PKI の有効化

この項で使用する ORACLE ホームは、OracleAS Single Sign-On Server がインストールされている場所です。

次の手順に従って、OracleAS Single Sign-On で PKI を有効化します。

1. `$ORACLE_HOME/sso/conf/policy.properties` を編集するために、次のように、デフォルトの認証レベルを高に設定し、対応する正しいプラグインを設定します。

```
DefaultAuthLevel = MediumHighSecurity

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

2. 次の形式の行を使用して、プロビジョニングにユーザー名とパスワードを使用するよう OracleAS Certificate Authority を構成します。

```
MediumSecurity_AuthPlugin = oracle.security.sso.server.auth.SSOServerAuth
Oca_hostname\:port = MediumSecurity
```

たとえば、Oca_hostname が oca.us.oracle.com で、OracleAS Certificate Authority のポート番号が 6600 の場合、このオプションは次のように記述されます。

```
oca.us.oracle.com\:6600=MediumSecurity
```

3. これらのオプションをすべて設定すると、どのパートナ・アプリケーションにログインするユーザーも、証明書が必要になります。ただし、OracleAS Certificate Authority では証明書を取得できるので不要です。

次のコマンドを使用して、OracleAS Single Sign-On Server を再起動します。

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

SSL を有効化した SSO への仮想ホストの再登録

この項で使用する *ORACLE_HOME* は、OracleAS Certificate Authority がインストールされている場所です。

管理者は、OracleAS Single Sign-On Server で SSL を使用可能にするたびに、SSL が使用可能になった OracleAS Single Sign-On Server に OracleAS Certificate Authority の仮想ホストを再登録する必要があります。OracleAS Single Sign-On を使用するすべてのアプリケーションも同様です。再登録には、シングル・サインオン登録ツールの `ossoreg.jar` を使用します。ここでは、OracleAS Certificate Authority でのこのツールの使用方法について説明します。Single Sign-On 対応アプリケーションでの一般的な使用方法は、『Oracle Application Server Single Sign-On 管理者ガイド』を参照してください。

1. 次のコマンドを実行して、OracleAS Certificate Authority 用の mod_osso を再登録します。

```
$ORACLE_HOME/sso/bin/ssoreg.sh \
-oracle_home_path $ORACLE_HOME -site_name OracleAS Certificate Authority \
-config_mod_osso TRUE \
-mod_osso_url https://hostname.domain.com:oca_ssl_port  -u root \
-virtualhost \
-config_file $ORACLE_HOME/Apache/Apache/conf/osso/oca/osso.conf
```

OracleAS Single Sign-On Server のホストとなっているマシンでこのツールを実行すると、OracleAS Single Sign-On Server の SSL 設定を反映して、OracleAS Certificate Authority の mod_osso レコードが osso.conf ファイルに生成されます。

2. 次のコマンドを実行して、OracleAS Certificate Authority 用の OHS を再起動します。

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

再登録の例

OracleAS Certificate Authority ホスト名が myoca.mysite.com で、OracleAS Certificate Authority サーバーの認証ポート番号が 6600 だとします。この場合、再登録を完了するには、次の手順を実行します。

1. 次の 2 つのコマンドを使用して、（手順 2 の）実際のコマンドで使用される変数を設定します。

   csh および tcsh:

   ```
   setenv ORACLE_HOME /sso_server/oracle_home
   setenv LD_LIBRARY_PATH $ORACLE_HOME/lib
   ```

   ksh および Bourne シェル :

   ```
   set ORACLE_HOME=/sso_server/oracle_home; export ORACLE_HOME
   set LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
   ```

2. これらの変数をセットとして使用すると、UNIX システムでの実際のコマンドは次のようになります（実際は 1 行です）。

   ```
   $ORACLE_HOME/sso/bin/ssoreg.sh \
   -oracle_home_path $ORACLE_HOME -site_name my_oca_site_name \
   -config_mod_osso TRUE  -mod_osso_url https://myoca.mysite.com:6600 \
   -u root -config_file $ORACLE_HOME/Apache/Apache/conf/osso/oca/osso.conf \
   -virtualhost
   ```

   Windows の場合、コマンドは次のとおりです。

   ```
   set ORACLE_HOME=c:¥sso_server¥oracle_home

   %ORACLE_HOME%¥sso¥bin¥ssoreg.bat
   -oracle_home_path $ORACLE_HOME
   -site_name "my_oca_site_name"
   -config_mod_osso TRUE
   -mod_osso_url https://myoca.mysite.com:6600
   -u SYSTEM
   -config_file $ORACLE_HOME¥Apache¥Apache¥conf¥osso¥oca¥osso.conf
   -virtualhost
   ```

F

保護された OracleAS Certificate Authority への外部アクセス

OracleAS Certificate Authority のようにファイアウォールの背後で保護されている安全なプロセスでも、プロキシ・サーバーを使用することにより、ファイアウォールの外部からカスタマにサービスを提供できます。

中間サーバーは、証明書サービスに対するすべてのユーザー・リクエストを安全に取得し、これらのリクエストを OracleAS Certificate Authority に転送します。プロキシ・サーバーは、ポート 443（SSL 通信用）とポート 80（非 SSL 通信用）の 2 つのポートのみを使用します。

次の例に示すように、OracleAS Certificate Authority は、サーバー認証用と相互認証用に 1 つずつ、2 つの仮想ホストを持つため、2 つのプロキシ・サーバーが必要です。

例 F-1 プロキシ・サーバーの例

サーバー認証用のプロキシ・サーバーは、次の URL を使用します。

`https://myproxy_server1.acme.com`（デフォルトの SSL ポートは 443）

これが、次の URL にマッピングされます。

`https://myoca.acme.com:6600`（サーバー認証）

2 番目の相互認証用プロキシ・サーバーは、次の URL を使用します。

https://myproxy_server2.acme.com（デフォルトの SSL ポートは 443）

これが、次の URL にマッピングされます。

https://myoca.acme.com:6601（相互認証）

この付録では、OracleAS Certificate Authority でのプロキシ・サーバーのサポートを有効にする方法、およびプロキシ・サーバーを OracleAS Certificate Authority 仮想ホストにマッピングする方法について説明します。

OracleAS Certificate Authority でのプロキシ・サーバーのサポートの有効化

次の手順を実行すると、OracleAS Certificate Authority でのプロキシ・サーバーのサポートが有効になります。

1. OracleAS Certificate Authority ユーザーとしてデータベースにログオンします。
2. スクリプト `$ORACLE_HOME/oca/sql/ocabigipon.sql` を実行します。
3. プロキシ・サーバーのホスト名と、OracleAS Certificate Authority 相互認証ポートにマッピングされる SSL ポート（「プロキシ・サーバーの例」では myproxy_server2.acme.com およびポート 443）を入力します。
4. プロキシ・サーバーを OracleAS Certificate Authority 仮想ホストにマッピングします。

OracleAS Certificate Authority でのプロキシ・サーバーのサポートの無効化

次の手順を実行すると、OracleAS Certificate Authority でのプロキシ・サーバーのサポートが無効になります。

1. OracleAS Certificate Authority ユーザーとしてデータベースにログオンします。
2. スクリプト `$ORACLE_HOME/oca/sql/ocabigipoff.sql` を実行します。

G

OracleAS Certificate Authority での S/MIME

Outlook、Mozilla または Netscape メール・クライアントなどの S/MIME アプリケーションでは、PKI に基づいてメール・メッセージの署名および暗号化を行うことができます。

S/MIME 操作

送信者は、署名秘密鍵を使用してメッセージに署名できます。受信者は、送信者の署名証明書（通常は署名されたメール・メッセージとともに送信される）を使用して、その署名を検証できます。

送信者は、受信者の暗号証明書を使用してメッセージを暗号化できます。受信者は、暗号秘密鍵を使用してメッセージを解読できます。

ユーザーは、ブラウザ（Internet Explorer、Mozilla または Netscape）を使用して、OracleAS Certificate Authority から署名または暗号（あるいは両方）の証明書をリクエストおよび取得できます。

設定

S/MIME 操作を設定するには、証明書を取得し、S/MIME パラメータを設定する必要があります。

証明書の取得

OracleAS Certificate Authority から S/MIME 証明書を取得する手順は、第 8 章「Oracle Application Server Certificate Authority のエンド・ユーザー・インタフェース」の 8-4 ページの「「ユーザー証明書」タブ」を参照してください。必ず、ブラウザに証明書をインストールしてください。

各ユーザーは、署名と暗号の両方を行う 1 つの証明書を取得できますが、署名用と暗号化用に 1 つずつ、2 つの証明書を取得するほうが、セキュリティは強化されます。署名鍵は、否認防止の目的で、ユーザーのマシンまたはスマートカード上に安全に保持しておく必要があります。暗号鍵が失われた場合に暗号化メッセージをリカバリできるように、暗号鍵はアーカイブする必要があります。

S/MIME パラメータの設定

Outlook メール・クライアント、または Mozilla および Netscape メール・クライアントで S/MIME パラメータを設定できます。

Outlook メール・クライアント Outlook で、**「ツール」→「オプション」→「セキュリティ」→「電子メールの保護設定」**を選択します。

- **「セキュリティ設定名」**に目的の名前を入力します。
- **「証明書とアルゴリズム」**で、次のように設定します。
  - 署名証明書を選択します。送信メッセージに署名するときには、この証明書を使用します。
  - 暗号証明書を選択します。他のユーザーから自分に送信されるメッセージが暗号化されるときは、この証明書が使用されます。
- **「署名済みメッセージで証明を送信する」**というチェック・ボックスを選択します。
- この設定プロセスが完了するまで、**「OK」**を繰り返しクリックします。

Mozilla/Netscape メール・クライアント Mozilla および Netscape メール・クライアントでは、**「編集」→「Mail & Newsgroup アカウントの設定」→「セキュリティ」**を選択します。

- **「デジタル署名」**ペインで**「選択」**をクリックして、その目的で作成する署名証明書を選択します。
- **「暗号化」**ペインで**「選択」**をクリックして、その目的で作成する暗号証明書を選択します。（選択した**使用方法**に暗号化と署名の両方が含まれている場合、同じ証明書を両方の目的に適うように使用できます。）

OCA の構成 通知は、OCA により管理者およびユーザーに送信されます。これらの通知は、S/MIME を使用して暗号化できます。詳細は、第 5 章「Oracle Application Server Certificate Authority の構成」の「「通知」サブタブ」を参照してください。

メッセージの送信

メール・メッセージを構成した後、メッセージの送信前に次の手順を実行します。

Outlook メール・クライアント

Outlook で、次の手順を実行してメッセージの暗号化または署名（あるいはその両方）を行います。

- メッセージを暗号化する場合、**「オプション」**を選択し、**「送信メッセージの内容と添付ファイルを暗号化する」**というチェック・ボックスを選択します。受信者ごとに暗号証明書が存在することを確認してください。（受信者の暗号証明書を取得する手順は、「他のユーザーの暗号証明書の取得」を参照してください。）
- メッセージに署名する場合、**「オプション」**を選択し、**「送信メッセージにデジタル署名を追加する」**というチェック・ボックスを選択します。

Mozilla/Netscape メール・クライアント

Mozilla および Netscape メール・クライアントでの手順は、次のとおりです。

- メッセージを暗号化する場合、**「セキュリティ」→メッセージの暗号化**をクリックします。
- メッセージに署名する場合、**「セキュリティ」→「メッセージにデジタル署名する」**をクリックします。

メッセージの受信

メッセージの暗号化に使用された証明書の秘密鍵を持っている場合、暗号化されたメッセージを読むことができます。また、送信者の署名証明書に署名する CA を信頼する場合は、この秘密鍵を使用して送信者の署名を検証することもできます。メッセージのセキュリティ情報を表示するには、そのメッセージをクリックし、次のように各メール・クライアントに対応する手順を実行します。

Outlook メール・クライアント

「ファイル」→「プロパティ」→「セキュリティ」を選択します。

Mozilla/Netscape メール・クライアント

「表示」→「メッセージのセキュリティに関する情報」を選択します。

他のユーザーの暗号証明書の取得

特定の受信者に送信するメッセージを暗号化するには、その受信者の証明書を使用します。これらの証明書を取得する手順は、次のとおりです。

- 送信者の暗号証明書が含まれるメッセージを受信した場合、その証明書は自動的に受信者の証明書ストアに保存されます。
- （秘密鍵なしの）暗号証明書の送信を他のユーザーに依頼すれば、自分の証明書ストアにその証明書を保存できます。
- また、LDAP ディレクトリから暗号証明書を取得することもできます。
  - Outlook では、次のような状況が発生すると、他のユーザーの証明書が LDAP ディレクトリから自動的に取得されます。
    * 標準の LDAP サーバーでインターネット専用モードを使用している場合、暗号化された電子メール・メッセージをその LDAP サーバー内のユーザーに送信すると、そのユーザーの証明書が取得されます。これが正常に行われるためには、S/MIME セキュリティに登録し、電子メール・アカウント用のデジタル ID を設定しておく必要があります。
    * Microsoft Exchange Server で「企業 / ワークグループ」モードを使用している場合、グローバル・アドレス・ブックから証明書を取得できます。Exchange の高度なセキュリティに登録されている必要があります。
    * Mozilla では、LDAP からの証明書の自動取得はまだサポートされていません。

      LDAP コマンドを直接使用すると、ディレクトリから目的の証明書を個別に取得し、ファイルに格納し、最終的にそれを証明書ストアに保存できます。

H

OracleAS Certificate Authority で使用するための OracleAS WebCache の構成

オラクル社では、Web サイトや Web ベース・アプリケーションのパフォーマンスの問題を抱える E-Business を支援するために、OracleAS Web Cache を提供しています。OracleAS Web Cache はコンテンツ対応のサーバー・アクセラレータ、つまりリバース・プロキシ・サーバーであり、Oracle Application Server 上で稼働する Web サイトのパフォーマンス、スケーラビリティおよび可用性を高めます。

この付録では、Oracle Application Server Certificate Authority と共用する場合の OracleAS Web Cache の配置方法を説明します。主要な手順と構成時に役立つ参考情報が記載されています。

次の手順でインストールを行います。

- OracleAS WebCache のインストール
- OracleAS Certificate Authority で使用するための OracleAS WebCache の構成
- OracleAS WebCache で使用するための OracleAS Certificate Authority 仮想ホストの構成
- OracleAS Certificate Authority で使用するための OracleAS WebCache の有効化

OracleAS WebCache のインストール

OracleAS Web Cache をインストールするには、Oracle Application Server のインスタンスを「J2EE and Web Cache」コンポーネント・オプション付きでインストールします。実際には、このインスタンスは OracleAS Certificate Authority と同じマシンにインストールしてもかまいませんが、テストという目的上、別のホスト名を持つ別のマシンにインストールすることをお薦めします。

詳細は次を参照してください。

- OracleAS Web Cache 関連の無償のリリース・ノート、インストール・ドキュメント、ホワイト・ペーパーまたはその他の関連資料を、`http://www.oracle.com/technology/index.html` の Oracle Technology Network（OTN）からダウンロードできます。
- 構成に関する詳細は、『Oracle Application Server Web Cache 管理者ガイド』、その中の特に、OracleAS Web Cache の構成および管理についての記載がある第 II 部を参照してください。

OracleAS Certificate Authority で使用するための OracleAS WebCache の構成

OracleAS Certificate Authority および OracleAS Single Sign-On での使用に適するように OracleAS Web Cache を構成します。次の手順を実行します。

1. OracleAS Web Cache がインストールされているマシン用に SSL サーバー Wallet を取得します。このタスクのために Oracle Wallet Manager を使用します。

   注意： CN は Web Cache のホスト名です。

   詳細は『Oracle HTTP Server 管理者ガイド』を参照してください。

2. OracleAS Web Cache を構成するために Oracle Enterprise Manager 10*g* を使用します。Application Server Control から次の手順を実行します。
   - **「webcache」→「管理」**を選択します。
   - **「webcache」→「ポート」**を選択し、Web Cache のリスナー・ポートを作成します。各サーバーに必要なポートは 1 つです。すなわち、OracleAS Certificate Authority のポート 6600（サーバー認証）に対しては Web Cache リスナー・ポート 4600、OracleAS Certificate Authority のポート 6601（相互認証）に対しては Web Cache リスナー・ポート 4601、SSO ポート 7777（非 SSL）に対しては Web リスナー・ポート 7778 を構成します。

     各ポートを構成する際、必ず、HTTPS がチェックされ、かつ、SSL サーバー（たとえば OracleAS Certificate Authority サーバー）用の Web Cache SSL Wallet が指定され、また、必要な場合は相互認証ポート用クライアント証明書が指定されるようにします。たとえば、ポート 4601 は、HTTPS である必要があり、クライアント証明書を要求するようにします。
   - **「アプリケーション」→「オリジナル・サーバー」**を選択し、オリジナル・サーバーを作成します。

     オリジナル・サーバーは Web サーバーを記述したもの（ホスト、ポートおよびプロトコル）です。OracleAS Certificate Authority には 2 つのオリジナル・サーバーがあります。1 つは https://*hostname*:6600、もう 1 つは https://*hostname*:6601 です。

     OracleAS Single Sign-On にもオリジナル・サーバーがあります。

– **「アプリケーション」→「サイト」**を選択し、サイトを作成します。サイトは、Web Cache ホスト名、前述のリスナー・ポートおよびプロトコルから構成されます。必要に応じて**「拡張」**をクリックして、HTTPS および要求されているクライアント証明書を選択します。

  サイトはオリジナル・サーバーにもマッピングされます。

– Web Cache で使用する SSL Wallet を設定します。これを行うには、**「webcache」→「セキュリティ」**を選択し、SSL Wallet の場所を入力します。

3. OracleAS Web Cache を再起動します。

注意： Web Cache は、ファイル記述子が不足すると再起動できなくなります。この問題を解決するには、『Oracle Application Server Web Cache 管理者ガイド』を参照してください。

OracleAS Web Cache の構成に関する詳細は、『Oracle Application Server Web Cache 管理者ガイド』を参照してください。

OracleAS Web Cache で使用する OracleAS Single Sign-On の構成に関する情報は、『Oracle Application Server Single Sign-On 管理者ガイド』内の、プロキシ・サーバー付きの OracleAS Single Sign-On の配置に関する項を参照してください。

OracleAS WebCache で使用するための OracleAS Certificate Authority 仮想ホストの構成

次の手順を実行して、OracleAS WebCache ホストおよびポートでの使用に適するように OracleAS Certificate Authority 仮想ホストを構成します。

1. `ocm_apache.conf` ファイルの server auth virtual host セクションを次のように編集します。
   1. `ServerName` を、実際の OracleAS Certificate Authority ホスト名でなく Web Cache ホスト名に変更します。
   2. この仮想ホストに Web Cache ポートの Port ディレクティブを追加します（たとえば、Port 4600）。
   3. 次の行を追加します。

      ```
      LoadModule certheaders_module libexec/mod_certheaders.so
      AddCertHeader HTTPS
      AddCertHeader SSL_CLIENT_CERT
      ```

   4. 次の行をコメントアウトします。

      ```
      SSLOptions +FakeBasicAuth +ExportCertData +CompatEnvVars +StrictRequire
      ```

2. 次のコマンドを実行します。

   ```
   dcmctl updateconfig -ct ohs
   ```

3. Oracle HTTP Server を再起動します。

   ```
   opmnctl restartproc type=ohs
   ```

4. Internet Explorer 上で不具合に遭遇することがあります。その場合は、次のように `$ORACLE_HOME/webcache/internal.xml` ファイルを変更することで解決します。IEHOSTHEADERBUG=*SSO_WEBC_PORT* を <MISCELLANEOUS/> タグに追加します。ここで、*SSO_WEBC_PORT* は、SSO ポートにマッピングされた Web Cache ポートです。

5. OracleAS WebCache を再起動します。

注意： Web Cache は、ファイル記述子が不足すると再起動できなくなります。この問題を解決するには、『Oracle Application Server Web Cache 管理者ガイド』を参照してください。

OracleAS Certificate Authority で使用するための OracleAS WebCache の有効化

OracleAS Certificate Authority で使用するために OracleAS Web Cache を有効化する場合は、次のコマンドを実行します。

```
$ORACLE_HOME/bin/sqlplus oca/ocadbpass
    @$ORACLE_HOME/oca/sql/ocabigipon.sql
```

OracleAS Certificate Authority で使用する Web Cache サイトのホストおよびポートを変更する場合は、次のコマンドを実行します。

```
$ORACLE_HOME/oca/sql/ocabigipoff.sql
```

続けて、次のコマンドを実行します。

```
$ORACLE_HOME/oca/sql/ocabigipon.sql
```

OracleAS Certificate Authority で使用している OracleAS Web Cache を無効化する場合は、次のコマンドを実行します。

```
$ORACLE_HOME/bin/sqlplus oca/ocadbpass
    @$ORACLE_HOME/oca/sql/ocabigipoff.sql
```

Oracle Application Server Certificate Authority の Web インタフェース

この付録では、Oracle Application Server Certificate Authority の Web インタフェースの様々なウィンドウ、フィールドおよび制御デバイスについて説明します。内容は、次のとおりです。

- 管理インタフェースのウィンドウとフィールド
- エンド・ユーザー・インタフェースの各ウィンドウや各フィールド

管理インタフェースのウィンドウとフィールド

この項では、Web 管理インタフェースのウィンドウとフィールドについて説明します。

Web 管理者登録 -- 拡張 DN

識別名（DN）が存在する場合で、その完全な名前と LDIF 形式での入力方法がわかっている際に、このページを使用して Web 管理者として登録します。この機能は、「Web 管理者登録」ページの識別名情報ヘッダーのショートカットで、「拡張 DN」リンクとして表示されます。DN は、Oracle Internet Directory のユーザー・エントリのロケーションです。Oracle Application Server Certificate Authority では、証明書はこのディレクトリ・エントリに格納され、ここから取得されます。

登録の手順は、「管理者の証明書のリクエスト」を参照してください。

「拡張」画面

「拡張」画面を使用して、証明書リクエストや既存の証明書に対する検索の精度を高めます。「拡張」画面には、次の 5 つの検索方法が用意されています。

1. リクエスト・ステータスを使用した証明書リクエストの検索

   「保留」、「却下」および「認証済」の 3 つの証明書検索カテゴリから選択します。却下された証明書を検索するには、このオプションを使用する必要があります。

2. 識別名 (DN) を使用した検索

   「検索」リストから「証明書」または「証明書リクエスト」を選択し、証明書所有者または証明書リクエスタを指定します。証明書所有者または証明書リクエスタの識別名の構成要素を入力します。すべてのフィールドはオプションです。

3. 拡張識別名を使用した検索

   証明書リクエスタまたは証明書所有者の完全な DN を知っており、それの LDIF 形式での入力方法がわかっている場合に、このオプションを選択します。次の例で、属性間に空白を入れるかどうかは任意です。

   cn=Margarita Redmond,ou=sales,o=yourcorp,l=Bismarck,st=SD,c=US

4. シリアル番号 / リクエスト ID の範囲を使用した検索

   一定範囲内の証明書に関する情報を取得するには、このオプションを選択します。「証明書」リストを使用して、リクエストした証明書と既存の証明書の間で切替えができます。どちらの場合も、シリアル番号フィールドは必須です。

5. 証明書ステータスを使用した証明書検索

   「有効」、「失効」および「期限切れ」の 3 つの証明書ステータス・カテゴリから選択します。

これらの方法を使用した検索の詳細は、「「拡張検索」画面」を参照してください。

証明書詳細

このページを使用して、BASE64 エンコーディングを含む証明書の完全な説明を取得します。このページで変更できないフィールドは、次のとおりです。

フィールド	説明
ステータス	これの値は、「有効」、「失効」または「期限切れ」。
シリアル番号	Oracle Application Server Certificate Authority によって割り当てられた証明書のシリアル番号。
署名アルゴリズム	オブジェクト識別番号（OID）によって示される使用アルゴリズム（RSA 暗号化付き MD5 など）。
使用方法	証明書機能。
発行局	証明書を発行した CA。
サブジェクト DN	証明書の所有者の識別名。
有効期間の開始日	証明書の有効期間の開始日時。
有効期間の終了日	証明書の有効期間の終了日時。
PKCS#7 形式の CA 証明連鎖で Base64 でエンコードされた証明書	PKCS#7 形式でエンコードされた証明書と信頼できる認証局のツリー。この形式では、単一操作を使用して、信頼できる連鎖からルート CA 証明書までのすべての証明書を転送できる。
Base64 でエンコードされた証明書	エンコードされた証明書。

ページの下部にあるボタンの 1 つを選択して、目的のタスクを実行します。

ボタン名	説明
OK	認証管理のメイン・ページに戻る。
失効	証明書を失効する。失効理由を指定する必要がある。
更新	証明書を更新する。新しい有効期間を指定する必要がある。
ブラウザへのインストール	証明書をブラウザにインストールする。

証明書リクエストの却下

このページを使用して、手動証明書リクエストを却下します。リクエストを却下するには、「送信」を選択します。「取消」を選択すると、「リクエスト」ページに戻ります。

このページには、証明書リクエスタのプロファイルを構成する変更不可能なフィールドがあります。これらのフィールドの説明は、次のとおりです。

フィールド	説明
ステータス	この値は常に「保留」。
証明書タイプ	この値は、「クライアント」、「サーバー」または「CA」（認証局）。
証明書の使用方法	証明書の機能（SSL クライアント、署名またはその他）。
シリアル番号	証明書リクエストを参照するために使用されるシリアル番号。証明書リクエストを認可すると、OracleAS Certificate Authority によって新しい値が割り当てられる。
サブジェクト DN	リクエスタの識別名（DN）。DN は、Oracle Internet Directory におけるリクエスタのユーザー・エントリのロケーション。
リクエスト日時	ユーザーが手動リクエスト・フォームにリクエストを入力した日時。
アルゴリズム	証明書を暗号化するために使用されるアルゴリズム。
指数	公開鍵の指数。この数値が大きいほど、クライアントがメッセージを暗号化するのに要する時間が長くなる。

このタスクの実行方法の詳細は、「証明書リクエストの却下」を参照してください。

証明書リクエストの認可 - 手動

このページを使用して、証明書リクエストを認可または却下します（「認可」または「却下」をクリックします）。「取消」を選択すると、「リクエスト」ページに戻ります。

このページでは、承認リクエストの詳細が表示され、次の機能とフィールドを有効化または編集できます。

- **証明書リクエストの認可時にポリシー・チェックを適用**

  ポリシー・チェックが無効である（選択解除されている）場合、証明書リクエストにはポリシー・ルールが適用されません。ポリシー・ルールに準拠していない特別な証明書を発行する場合に、この機能が役に立ちます。

- **サブジェクト（リクエスタ）**

  ユーザーによって DN が誤って入力された場合、管理者はこの DN を編集できます。

- **有効期間**

  管理者は、証明書リクエストを認可する前にその有効期間を変更できます。

「証明書リクエスト情報」の読取り専用フィールドは、次のとおりです。

フィールド	説明
ステータス	この値は常に「保留」。
証明書タイプ	この値は「クライアント」または「サーバー」。
証明書の使用方法	「認証」、「暗号化」、「署名」、「認証、暗号化」、「認証、署名」、「署名、暗号化」、「認証、署名、暗号化」または「コード署名」の 8 つの値のいずれか。
シリアル番号	証明書リクエストが保留中であるか認可されたときに、証明書リクエストを参照するために使用されるシリアル番号。証明書リクエストを認可すると、Oracle Application Server Certificate Authority によって新しい値が割り当てられる。
サブジェクト DN	リクエスタの識別名（DN）。DN は、Oracle Internet Directory におけるリクエスタのユーザー・エントリのロケーション。
リクエスト日時	ユーザーが手動リクエスト・フォームにリクエストを入力した日時。
アルゴリズム	証明書と指数を暗号化するために使用されるアルゴリズム。
指数	公開鍵の指数。この数値が大きいほど、クライアントがメッセージを暗号化するのに要する時間が長くなる。

このタスクの実行方法の詳細は、「証明書リクエストの承認または拒否」を参照してください。

「リクエスト」ページ

「リクエスト」ページには、管理者が注意している必要があるすべての保留証明書リクエストが記載された表が表示されます。

このページのボタンを使用して、次のタスクを実行します。

- 証明書と証明書リクエストの検索および表示
- 証明書失効リストの更新

次のタスクの 1 つを実行するには、リクエストを選択して「詳細表示」をクリックします。

- 証明書リクエストの認可
- 証明書リクエストの却下
- 証明書の失効

タスクの詳細は、リンクをクリックしてください。

カスタム・ポリシーの追加

Oracle Application Server Certificate Authority に付属のデフォルトのポリシー・プラグインは汎用のプラグインです。必要に応じて、デフォルト・ポリシー・フレームワークを組織にあわせて拡張し、カスタム・ポリシー・プラグインを作成します。証明書リクエスト、証明書およびその他の汎用的な機能に関する情報を取得するために、Application Program Interface（API）が用意されています。ポリシーの追加は、ポリシーの Oracle Application Server Certificate Authority への登録とも言い換えられています。

カスタム・ポリシーを追加する手順は、次のとおりです。

1. OCACustomPolicyPlugin インタフェースを実装する Java クラスを作成します。
   - OCACustomPolicyPlugin に用意されているクラスとメソッドの詳細は、このドキュメントに付属する Javadoc の oracle.security.oca.policy パッケージを参照してください。
   - カスタム・ポリシー Java クラスの詳細は、「カスタム・ポリシー・プラグインの開発」を参照してください。
2. カスタム・ポリシー Java クラスを `.jar` ファイルにパッケージ化し、プラットフォームに応じて次のロケーションに配置します。
   - `$ORACLE_HOME/oca/policy`（UNIX）
   - `ORACLE_BASE¥ORACLE_HOME¥oca¥policy`（Windows）

   ポリシーのサブディレクトリがない場合は、作成します。
3. カスタム・ポリシーを Oracle Application Server Certificate Authority に登録するには、Web 管理インタフェースにログインします。
4. 「構成管理」タブのメイン・ページである「ポリシー」で、追加するカスタム・ポリシーのタイプとして**「操作」**を選択し、**「実行」**をクリックします。この操作の「ポリシー・ルール」ページが表示されます。
5. 選択した「操作」タイプの「ポリシー・ルール」ページで、ページの右端にある**「追加」**をクリックします。「カスタム・ポリシー詳細」ページが表示されます。
6. 「カスタム・ポリシー詳細」ページで、用意されているフィールドにカスタム・ポリシーに関する情報を入力します。各フィールドに必要な情報のタイプは、次のとおりです。
   - **名前**: カスタム・ポリシーの名前（AuditCertDetails など）。
   - **説明**: カスタム・ポリシーの内容の説明。
   - **クラス**: カスタム・ポリシーを実装する Java クラスの名前。手順 1 および 2 を参照してください。
7. **「このポリシーの有効化」**を選択してカスタム・ポリシーをアクティブにし、**「OK」**をクリックします。新しいポリシーが追加されたことを確認するメッセージが表示されます。
8. このポリシーの優先順位が正しいかどうかを確認します。ポリシーの優先順位を付け替える方法の詳細は、「ポリシー操作」を参照してください。
9. Oracle Application Server Certificate Authority サーバーを再起動し、カスタム・ポリシーを有効にします。「Oracle Application Server Certificate Authority の起動および停止」を参照してください。

関連項目

次のトピックの詳細は、「ポリシー操作」を参照してください。

- ポリシーの表示
- ポリシーの編集
- ポリシーの有効化
- ポリシーの無効化
- ポリシーの削除
- ポリシーの優先順位の付替え
- ポリシー管理

RenewalRequestConstraint の編集

このページを使用して、RenewalRequestConstraint ポリシーのデフォルト値と制限を設定します。このポリシーは、クライアントまたはサーバー / 下位 CA の証明書の更新リクエストに適用され、期限切れの証明書を更新できるかどうかを制御します。このポリシーは、SSL ユーザーに適用できます。

このポリシーについては、次のデフォルト値と制限を変更できます。

パラメータ詳細

パラメータ	デフォルト値	説明
更新の許可	選択済（TRUE）	証明書を更新可能にするかどうかを指定する。選択されている場合（TRUE）、証明書は更新可能。
満了日までの日数	15 日	満了日の何日前まで証明書が更新可能かを指定する。0（ゼロ）を指定すると、満了日の前は証明書は更新不可能。*（アスタリスク）を指定すると、満了日の前はいつでも証明書が更新可能。
満了日後の日数	15 日	満了日の何日後まで証明書が更新可能かを指定する。0（ゼロ）を指定すると、満了日の後は証明書が更新不可能。*（アスタリスク）を指定すると、満了日の後はいつでも証明書が更新可能。
更新の継続期間（日）	365 日	更新する証明書の有効期間を指定する。

述語詳細

条件式はオプションであり、ポリシーは、受信したリクエストがその条件式と一致するときにのみ適用されます。条件のないポリシーは、受信したすべてのリクエストに適用されます。たとえば、次の条件式は、日本にある Acme Company の Marketing 部門（ou=marketing,o=acme,c=japan）からのすべてのクライアント更新リクエストが、この条件に選択されているパラメータ設定と照合されることを示しています。

Type=="client" AND DN=="ou=marketing,o=acme,c=japan"

条件式の構文の詳細は、「ポリシー・ルールの条件」を参照してください。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータと条件を前の値にリセットする。
適用	このボタンをクリックし、このページで行われた変更を適用する。
取消	このボタンをクリックし、このページで行われた変更を取り消し、メイン・ページである「ポリシー」に戻る。
OK	このボタンをクリックし、メイン・ページである「ポリシー」に戻る。このページで行われた変更は自動的に保存される。

関連項目

次のトピックの詳細は、「ポリシー・ルールの条件」を参照してください。

- ポリシーの編集
- ポリシー・ルールへの条件の追加
- ポリシー・ルールの条件の優先順位の付替え
- ポリシー・ルールからの条件の削除

RevocationConstraintRule の編集

このページを使用して、期限切れの証明書を失効できるかどうかを指定します。

注意 : このポリシーは、有効化されると、クライアントとサーバー両方からのすべての証明書失効リクエストに適用されます。特定の DN からの証明書失効リクエストに対して様々な制限を課すには、次の項で説明する条件を使用します。

このポリシーについては、次のパラメータと制限を変更できます。

パラメータ詳細

期限が切れた証明書の失効の許可

このパラメータを選択してオンにします。選択すると、期限切れの証明書を失効できます。選択しないと、失効できません。デフォルトでは、このパラメータは選択されています。

述語詳細

条件式はオプションであり、ポリシーは、受信したリクエストがその条件式と一致するときにのみ適用されます。条件のないポリシーは、すべてのリクエストに適用されます。たとえば、次の条件式は、英国の Acme Company の Sales 部門（ou=sales,o=acme,c=uk）からのクライアント証明書が、この条件に選択されているパラメータ設定と照合されることを示します。

Type=="client" AND DN=="ou=sales,o=acme,c=uk"

条件式の構文の詳細は、「ポリシー・ルールの条件」を参照してください。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータと条件を前の値にリセットする。
適用	このボタンをクリックし、このページで行われた変更を適用する。
取消	このボタンをクリックし、このページで行われた変更を取り消し、メイン・ページである「ポリシー」に戻る。
OK	このボタンをクリックし、メイン・ページである「ポリシー」に戻る。このページで行われた変更は自動的に保存される。

関連項目

次のトピックの詳細は、「ポリシー・ルールの条件」を参照してください。

- ポリシーの編集
- ポリシー・ルールへの条件の追加
- ポリシー・ルールの条件の優先順位の付替え
- ポリシー・ルールからの条件の削除

RSAKeyConstraints の編集

このページを使用して、RSAKeyConstraints ポリシーのデフォルト値と制限を設定します。このポリシーは、公開鍵または秘密鍵の長さの最大値と最小値をビット単位で指定します。ドロップダウン・リストには、指定した条件を満たさない証明書リクエストに対する選択肢が表示されます。指定した条件を満たす証明書リクエストに対する制限は、その条件と同じ行に表示されます。

注意： このポリシーのデフォルト値は、有効化されると、クライアントとサーバー両方からのすべての証明書リクエストに適用されます。特定の **DN** からの証明書リクエストまたは特定の証明書タイプや証明書使用方法に対して様々な制限を課すには、次の項で説明する条件を使用します。

このポリシーについては、次のデフォルト値と制限を変更できます。

パラメータ詳細

パラメータ	デフォルト値	説明
最大サイズのデフォルト値	2048	最大鍵サイズ。
最小サイズのデフォルト値	1024	最小鍵サイズ。このパラメータを使用して、最小レベルのセキュリティを確保する。

述語詳細

条件式はオプションであり、ポリシーは、受信したリクエストがその条件式と一致するときにのみ適用されます。条件のないポリシーは、すべてのリクエストに適用されます。たとえば、次の条件式では、クライアント SSL 証明書リクエストはこの条件に指定されている鍵の長さを使用する必要があります。

OCMCert.Type=="client" AND OCMCert.Usage=="ssl"

条件式の構文の詳細は、「ポリシー・ルールの条件」を参照してください。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータと条件を前の値にリセットする。
適用	このボタンをクリックし、このページで行われた変更を適用する。
取消	このボタンをクリックし、このページで行われた変更を取り消し、メイン・ページである「ポリシー」に戻る。
OK	このボタンをクリックし、メイン・ページである「ポリシー」に戻る。このページで行われた変更は自動的に保存される。

関連項目

次のトピックの詳細は、「ポリシー・ルールの条件」を参照してください。

- ポリシーの編集
- ポリシー・ルールへの条件の追加
- ポリシー・ルールの条件の優先順位の付替え
- ポリシー・ルールからの条件の削除

TrustPointDNCustomRule の編集

このページを使用して、TrustPointDNCustomRule ポリシーを有効化または無効化できます。このポリシーは、OracleAS Certificate Authority に用意されている Application Program Interface（API）を使用して開発できるカスタム・プラグイン・ポリシーの例です。詳細は「カスタム・ポリシー・プラグインの開発」を参照してください。

TrustPointDNCustomRule ポリシーは、有効化されると、すべての証明書リクエストの DN を証明連鎖内のすべての CA および下位 CA の証明書の DN と照合します。証明書リクエストに指定されている DN が CA の DN のいずれかと一致する場合、OracleAS Certificate Authority はこのリクエストを却下します。（証明連鎖とは、エンド・エンティティの証明書とそれの対応する CA 証明書が含まれる、順序付きの証明書リストです。）

関連項目

- カスタム・ポリシーの追加

UniqueCertificateConstraints の編集

このページを使用して、UniqueCertificateConstraints ポリシーのデフォルト値と制限を有効化および設定します。これにより、特定の各使用方法に対する単一の証明書に各ユーザーを制限、または各使用方法に対して複数の証明書を許可します。このポリシーを有効化すると、受信した証明書リクエストのサブジェクト DN と一致する証明書がリポジトリにないかどうかが検証されます。一致する DN を持つ証明書が見つかり、**「複数の証明書の許可」**の選択が解除（FALSE）されている場合、証明書の使用方法が同じであるかどうかも検証されます。使用方法が同じ証明書が見つかると、同じサブジェクト DN に対して、同じ使用方法を持つ別の証明書は発行されません。

このポリシーについては、次のパラメータと制限を変更できます。

パラメータ詳細

複数の証明書のデフォルト値の許可

このパラメータを選択すると（TRUE）、同じサブジェクト DN と同じ使用方法を持つ証明書を複数発行できます。このパラメータを選択しないと（FALSE）、同じサブジェクト DN に対して、同じ使用方法を持つ証明書は複数発行されません。

述語詳細

条件式はオプションであり、ポリシーは、受信したリクエストがその条件式と一致するときにのみ適用されます。条件のないポリシーは、すべてのリクエストに適用されます。たとえば、次の条件式は、米国ニュージャージー州トレントンにある Acme Company の買掛金部門（ou=acct_pay,loc=trenton,o=acme,c=us）からのクライアント証明書リクエストにより、同じ DN と使用方法を持つ複数の証明書が取得可能であることを示します。

Type=="client" AND DN=="ou=acct_pay,loc=trenton,o=acme,c=us"

複数の証明書の許可の値は、TRUE に設定されます。

条件式の構文の詳細は、「ポリシー・ルールの条件」を参照してください。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータと条件を前の値にリセットする。
適用	このボタンをクリックし、このページで行われた変更を適用する。
取消	このボタンをクリックし、このページで行われた変更を取り消し、メイン・ページである「ポリシー」に戻る。
OK	このボタンをクリックし、メイン・ページである「ポリシー」に戻る。このページで行われた変更は自動的に保存される。

関連項目

- 編集（ポリシーの編集）
- 条件の追加
- 条件の並替え
- 削除（条件の削除）

ValidityRule の編集

このページを使用して、ValidityRule ポリシーのデフォルト値と制限を設定します。これにより、手動で認証されたリクエストが証明書の有効期間として指定できる最大および最小の有効期間を設定します。たとえば、デフォルトの最大有効期間が 1825 日（5 年）に設定されているときに、証明書リクエストによって 3650 日（10 年）が要求された場合、このリクエストは却下されます。このパラメータの値はすべて日数単位で指定する必要があります。

SSL または OracleAS Single Sign-On（SSO）認証ユーザーについては、これらのタイプのリクエストに対して自動的に値が移入されるデフォルト有効期間パラメータを設定できます。

注意 : このポリシーは、有効化されると、クライアントとサーバー両方からのすべての証明書リクエストに適用されます。特定の DN からの証明書リクエストに対して様々な制限を課すには、次の項で説明する条件を使用します。

このポリシーについては、次のパラメータと制限を変更できます。

パラメータ詳細

パラメータ	デフォルト値	説明
最大有効期間	3650	証明書が有効な最大有効期間（日数単位）。
最小有効期間	90	証明書が有効な最小有効期間（日数単位）。
デフォルト有効期間	365	SSO または SSL 認証証明書リクエストの有効期間（日数単位）。

述語詳細

条件式はオプションであり、ポリシーは、受信したリクエストがその条件式と一致するときにのみ適用されます。条件のないポリシーは、すべてのリクエストに適用されます。たとえば、次の条件式は、クライアント SSL 証明書リクエストが、この条件で選択されている最大および最小有効期間を使用することを指定しています。

Type=="client" AND Usage=="ssl"

条件式の構文の詳細は、「ポリシー・ルールの条件」を参照してください。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータと条件を前の値にリセットする。
適用	このボタンをクリックし、このページで行われた変更を適用する。
取消	このボタンをクリックし、このページで行われた変更を取り消し、メイン・ページである「ポリシー」に戻る。
OK	このボタンをクリックし、メイン・ページである「ポリシー」に戻る。このページで行われた変更は自動的に保存される。

関連項目

- 編集（ポリシーの編集）
- 条件の追加
- 条件の並替え
- 削除（条件の削除）

構成管理 -- 一般

「構成管理」タブの**「一般」**ページを使用して、データベースおよびディレクトリ情報の表示、ディレクトリへの証明書公開の有効化、ロギングおよびトレースの有効化、識別名（DN）コンポーネントのデフォルト値の指定を行います。

次のパラメータを表示または構成できます。

証明書の公開

「公開」を選択すると、証明書は発行されると自動的にディレクトリに格納され、失効されると自動的に削除されます。OracleAS Certificate Authority は、SSL を使用してディレクトリに接続します。

SSL 認証および SSO 認証

デフォルトでは、SSL または OracleAS Single Sign-On によって認証されたユーザーは、独自の証明書を自動的に発行、失効または更新できます。この機能を無効にするには、「SSL 認証の有効化」または「SSO 認証の有効化」の選択を解除します。

クライアント証明書のデフォルト使用方法

クライアントが証明書をリクエストしたとき、ここで選択した値が、選択された使用方法として表示されます。ユーザーはドロップダウン・リストから、別の使用方法を選択することもできます。「認証」、「暗号化」、「署名」およびこれらの組合せに加え、「CA 署名」と「コード署名」があります。

サブジェクト代替名拡張機能

SSO ユーザーの場合、この拡張機能に対して選択した値が証明書に表示され、電子メールの暗号化、署名、または他のアプリケーションによる使用が可能になります。選択した内容は、「拡張機能コンテンツの選択」に表示されます。

拡張機能コンテンツの選択

「なし」、「電子メール」、「プリンシパル名（UID）」または「電子メール、プリンシパル名（UID）」から選択します。ここで選択した値は、証明書にサブジェクト代替名として表示され、電子メールの暗号化、署名、または他のアプリケーションによる使用が可能になります。（UID は、ユーザー識別子または一意の識別子を表します。）「電子メール、プリンシパル名（UID）」を選択すると、証明書にその両方が表示されます。

必須

このチェック・ボックスを選択した場合、すべての SSO 認証証明書について「サブジェクト代替名拡張機能」が必須になります。SSO 認証証明書リクエストに指定されたユーザーの電子メール・アドレスまたはプリンシパル名が Oracle Internet Directory 内に見つからない場合、そのリクエストは否認されます。「Oracle Internet Directory 内に電子メール・アカウントが見つからないため、SSO 認証証明書を発行できません。リクエスト者は管理者に問い合せてください。」という旨のエラー・メッセージが表示されます。

ロギングおよびトレース

ロギングまたはトレースを有効にできます。OracleAS Certificate Authority サーバーは、管理しているすべてのコンポーネントのエラー情報をログに記録します。デフォルトでは、ロギングは有効です。

「ロギングの有効化」を選択すると、システム・イベントとエラー・メッセージが、管理者の Web インタフェースの「ログの表示」タブから表示可能な認証局ログ表に書き込まれるようになります。

「トレースの有効化」を選択すると、オラクル社カスタマ・サポート・センター用のデバッグ・メッセージが `ORACLE_HOME/oca/logs/admin.trc`（コマンドライン・アクションのトレース用）および `ORACLE_HOME/oca/logs/oca.trc`（Web アクションのトレース用）に記録されます。この情報は管理者用ではありません。

デフォルト・ベース DN コンポーネント

登録情報申請に指定されている DN のほとんどが同じ構成要素を持つ場合（一意の識別子構成要素を除く）、それらの同じ構成要素をここで指定できます。これにより、OracleAS Certificate Authority によって生成される手動登録情報申請フォームのフィールドには、これらのデフォルトの構成要素が事前に移入されます。ユーザーは必要に応じてこれらを上書きできます。すべてのフィールドはオプションです。

データベースの設定

OracleAS Certificate Authority リポジトリに接続するためのデータベース接続文字列が表示されます。このフィールドは読取り専用です。

この項では、次のように、「データベース・プール・サイズ」および「データベース・プール・スキーム」の設定を指定することもできます。

データベース・プール・サイズ : OracleAS Certificate Authority に同時にアクセスするユーザー数の見込みを表す、データベースへの接続数（デフォルト : 10）を入力します。最初のグループのユーザーが OracleAS Certificate Authority を終了すると、このユーザーの接続を次の新規ユーザーが使用できるようになります。ユーザーがその数を超えるたびに新しい接続がオープンされ、そのユーザーが OracleAS Certificate Authority を終了すると同時にクローズされます。

データベース・プール・スキーム : デフォルトの「固定待機スキーム」では、10 人（デフォルトのプール・サイズ、または指定した数）のユーザーが OracleAS Certificate Authority に接続すると、それ以降に接続を試行するユーザーは 10 人のいずれかが終了するまで待機します。「動的」を選択すると、新しいユーザーに対して新規の接続が即時にオープンされ、そのユーザーが OracleAS Certificate Authority を終了するとその接続がクローズされます。固定増分では、元のプール・サイズ制限数に達すると、次の制限数に達するまで、新しいユーザーごとに新規接続がオープンされます。2 番目の制限数に達すると、既存の OracleAS Certificate Authority ユーザーが終了するまで新しいユーザーは接続できません。

ディレクトリの設定

ディレクトリ・ホスト・マシン、リスナー・ポート、およびディレクトリ・ホスト・ポートへの権限を持つバインド DN（Oracle Internet Directory にユーザーの証明書を公開する OracleAS Certificate Authority LDAP エージェント）を表示します。すべてのフィールドは読取り専用です。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータを前の値にリセットする。
取消	このボタンをクリックし、このページで行われた変更を取り消し、「構成管理」のメイン・ページ（「通知」）に戻る。
OK	このボタンをクリックし、このページで行われた変更を保存する。画面の上部には、構成ファイルが更新されたことを確認するメッセージが表示される。「Oracle Application Server Certificate Authority の起動および停止」の説明に従い、サーバーを再起動し、変更を有効にする。

関連項目

- 「構成管理 -- 一般」
- 「証明書の公開」
- 「構成管理 -- 一般」の「ロギングおよびトレース」
- デフォルト・ベース DN コンポーネントの設定（「構成管理 -- 一般」内）

構成管理 -- 通知

「構成管理」タブの**「通知」**ページを使用して、自動通知用の電子メール・サーバー・ホスト名と電子メール・テンプレートを構成します。また、このページを使用して、管理者アラートの有効化、CRL（証明書失効リスト）を自動生成するジョブのスケジュール、OracleAS Certificate Authority とディレクトリの同期化を行うこともできます。

通知は、証明書リクエスト、失効または更新などの OracleAS Certificate Authority の処理イベントの後にユーザーに対して送信されます。アラートは、CRL の生成が失敗した場合や、保留リクエストのキュー・サイズが指定のしきい値より大きい場合などに、管理者に対して送信されます。

次のパラメータを構成できます。

メール詳細

このリージョンを使用して、送信電子メール（SMTP）サーバーのホスト名、通知電子メールに表示する管理者の名前と電子メール・アドレス、管理者アラートの送信先の電子メール・アドレスを指定します。また、セキュアな MIME プロトコルの使用と電子メール・メッセージの本文テンプレート（「電子メールのテンプレート」を参照）を有効にすることもできます。

注意： OracleAS Certificate Authority によって送信される電子メールは、`ORACLE_HOME/oca/wallet/smime` にあるサーバーの S/MIME Wallet を使用して署名されます。

アラート

注意 : アラートを有効にするには、「メール詳細」に情報を指定する必要があります。

このリージョンを使用して、次のように管理者アラートを有効にします。

- 証明書処理イベントの管理者アラートを送信するには、「アラートの有効化」を選択します。その他のタイプのアラートを有効にするには、このボックスとともに次のいずれかまたは両方を選択します。
- リクエスト・キューが指定したサイズに達したときに管理者アラートを送信するには、「しきい値を越える保留リクエスト・キュー」を選択します。「キュー・サイズのしきい値」にサイズ（証明書リクエストの数）を指定します。このアラートを有効にする場合、次のように、サーバーが最初にキュー・サイズをチェックする時間とそれ以降のチェック頻度も指定する必要があります。
  - 「キュー・サイズ・チェック開始時間」に、24 時間のクロック・タイムを使用して開始時間を入力します（デフォルトは午前 0 時です）。たとえば、午前 2 時 30 分は 2 hours 30 minutes、午後 2 時 30 分は 14 hours 30 minutes となります。
  - 「キュー・サイズ・チェックの間隔」に、この開始時間に追加する時間隔（デフォルトは 1 日）を入力することで、次回のチェックの時間を指定します。この時間隔はゼロ以外の値である必要があります。
  - 変更した内容は、再起動しても保持されます。
- CRL の自動生成が失敗したときに管理者アラートを送信するには、「CRL 自動生成失敗」を選択します。

スケジュールされたジョブ

このリージョンを使用して、次のように自動ジョブをスケジュールします。

- CRL の自動生成を有効にするには、「CRL の自動生成の有効化」チェック・ボックスを選択します。次のように、最初の生成時間とこれ以降の生成時間隔を指定します。
  - 「CRL 自動生成開始時間」に、24 時間のクロック・タイムを使用して開始時間を入力します（デフォルトは午前 0 時です）。たとえば、午前 2 時 30 分は 2 hours 30 minutes、午後 2 時 30 分は 14 hours 30 minutes となります。
  - 「CRL 自動生成の間隔」に、この開始時間に追加する時間隔（デフォルトは 1 日）を入力することで次回の CRL 生成の時間を指定します。この時間隔はゼロ以外の値である必要があります。
  - 「CRL 自動生成の有効性」に、各 CRL が有効だとみなされる日数を入力します。
  - 変更した内容は、再起動しても保持されます。
- ディレクトリとの自動同期化を有効にするには、「ディレクトリの同期化」を選択し、次のように、最初の同期開始時間とこれ以降の時間隔を指定します。
  - 「ディレクトリ同期開始時間」に、24 時間のクロック・タイムを使用して開始時間を入力します（デフォルトは午前 0 時です）。たとえば、午前 2 時 30 分は 2 hours 30 minutes、午後 2 時 30 分は 14 hours 30 minutes となります。
  - 「ディレクトリ同期化の間隔」に、この開始時間に追加する時間隔（デフォルトは 1 日）を入力することで次回の CRL 生成の時間を指定します。この時間隔はゼロ以外の値である必要があります。
  - 変更した内容は、再起動しても保持されます。

  ディレクトリと同期化すると、ディレクトリから期限切れのすべての証明書が削除され、また、すべての証明書と CRL がそのディレクトリに公開されます。同期を行っていなかった場合、このような削除や公開は、ディレクトリが一時的に使用不可能になるなどのシステム・エラーのために失敗していた可能性のあるものです。

ページの下部にあるボタンの機能は、次の表のとおりです。

ボタン	説明
回復	このボタンをクリックし、変更されているすべてのパラメータを前の値にリセットする。
取消	このボタンをクリックし、このページで行われた変更を取り消し、「通知」ページをリフレッシュする。
OK	このボタンをクリックし、このページで行われた変更を保存する。画面の上部には、構成ファイルが更新されたことを確認するメッセージが表示される。「Oracle Application Server Certificate Authority の起動および停止」の説明に従い、サーバーを再起動し、変更を有効にする。

構成管理 -- ポリシー

「構成管理」タブの**「ポリシー」**ページを使用して、ポリシーを管理します。このページに表示されるポリシーは、左隅にある**「ポリシーの表示」**リストに表示される操作に適用されます。このリストから「リクエスト」、「更新」または「失効」を選択すると、その選択した操作に適用されるすべてのポリシーが表示されます。各ポリシーの**「タイプ」**、**「ステータス」**および**「説明」**が表示されます。**「デフォルト・ポリシー」**は、OracleAS Certificate Authority に用意されているポリシーです。**「カスタム・ポリシー」**は、ユーザー自身が作成するポリシーです。デフォルトのポリシーは削除できません（無効化のみ可能です）。

編集、有効化、無効化または削除するポリシーを選択するには、その左側にあるラジオ・ボタンをクリックし、ポリシー・リストの右上から目的のアクションをクリックします。**「編集」**をクリックしてポリシーを表示し、その詳細を表示できます。表示されているポリシーが適用される順序を変更、または新しいポリシーを追加するには、**「並び替え」**または**「追加」**ボタンをクリックします。

ポリシーの詳細は、第 6 章を参照してください。

ポリシー構成の変更は、サーバーを再起動するまでは有効になりません（「Oracle Application Server Certificate Authority の起動および停止」を参照）。

このページで実行可能なポリシー管理タスクの詳細は、次のページを参照してください。

関連項目

- ポリシーの編集
- ポリシーの有効化または無効化
- カスタム・ポリシーの追加
- ポリシーの削除
- ポリシーの並替え

証明書失効リストの更新

新しい証明書失効リスト（CRL）を生成します。CRL は、X.509 規格によって定義されており、すべての失効済証明書のリストが含まれる署名付きのデータ構造です。アプリケーションは、ユーザーにアクセス権を付与する前に、このリストを使用して、証明書が有効かどうかを確認します。

このページのフィールドとボタンの説明は、次のとおりです。

フィールドまたはボタン	説明
CRL の有効期間	新しい CRL の有効日数を設定する。
署名アルゴリズム	CRL を署名するためのアルゴリズム（「RSA 付き SHA1」や「RSA 付き MD5」など）を選択する。
取消	変更を行わずに終了する。
OK	CRL の前回の更新以降に失効したすべての証明書を使用して CRL を更新する。

証明書の失効方法の詳細は、「証明書の失効」を参照してください。

OracleAS Certificate Authority 管理ページへようこそ

このウィンドウの各タブを使用して、OracleAS Certificate Authority Administrative 管理ページのそれぞれにナビゲートします。

- 「ホーム」タブを使用すると、このページに戻ります。
- 「認証管理」タブを使用して、証明書リクエストを認可または却下できます。
- 「構成管理」タブを使用して、通知、アラート、証明書失効リスト生成、ロギング / トレースを設定、ならびに証明書ポリシーを管理できます。
- 「ログの表示」タブを使用して、エラー・ログを検索および表示できます。

これらのタブのショートカットは、ページの下部に並んでいます。「運用規定」をクリックすると、`ORACLE_HOME/j2ee/oca/applications/ocaapp/oca/helpsets/Help/ocaadmin_cs_practicestmt.html` ファイル（UNIX）または `ORACLE_HOME¥j2ee¥oca¥applications¥ocaapp¥oca¥helpsets¥Help¥ocaadmin_cs_practicestmt.html` ファイル（Windows）を編集して追加できる、サイトの認証局運用規定を表示できます。

Web 管理者登録

このページを使用して、証明書をリクエストします。認証管理機能を実行する管理者は、証明書所有者である必要があります。証明書をリクエストするには、このページを使用して次の手順を実行します。

1. 識別名情報を入力します。

   識別名（DN）は、Oracle Internet Directory におけるユーザー・エントリのロケーションです。OracleAS Certificate Authority は、このディレクトリ・エントリを使用してユーザーの証明書を格納および取得します。このヘッダー内で青いアスタリスクがあるフィールドは、必須です。これらのフィールドは、次のとおりです。

   - 一般名

     OracleAS Certificate Authority 管理者の名前

   - 組織

     管理者が属する企業

2. 管理者パスワードを入力します。

   OracleAS Certificate Authority の管理者パスワードを入力します。

3. 証明書情報を入力します。

   このヘッダーのフィールドを使用して、証明書鍵の強度や証明書の有効期間を指定します。Internet Explorer を使用している場合は、鍵の強度ではなく保管方法を指定します。

   - 証明書鍵サイズ（Netscape Communicator/Mozilla/Safari ユーザー）

     ブラウザによって生成される秘密鍵の長さです。使用可能なオプションから鍵の強度を選択します。通常は、「512」（低レベル）、「1024」（中レベル）または「2048」（高レベル）です。
     注意 : 一部のブラウザでは使用できないオプションもあります。

   - 暗号サービス・プロバイダ（Internet Explorer ユーザー）

     証明書の保管タイプまたは鍵サイズです。ドロップダウン・リストをクリックし、**「Microsoft Base Cryptographic Provider」**、**「Microsoft Enhanced Cryptographic Provider」**または**「Microsoft Strong Cryptographic Provider」**のいずれかを選択します。

     スマートカードは、対応するスマートカード・デバイスがシステムにインストールされている場合にのみ選択してください。たとえば、Gemplus スマートカード・リーダーがインストールされている場合、「Gemplus GemSAFE Card CSP」を選択できます。ただし、このリーダーがインストールされていない場合、これを選択するのは不適切です。

   - 有効期間（すべてのブラウザ）

     証明書の有効期間の長さです。ドロップダウン・リスト・ボックスをクリックし、4 つの選択肢のいずれかを選択します。

4. リクエストを処理するには、**「送信」**をクリックします。最初からやり直すには、**「リセット」**をクリックします。

   「認可済証明書の情報」ページが表示されます。このページには、証明書に関する詳細が含まれています。

5. **「ブラウザへのインストール」**をクリックして、ブラウザに証明書をインストールします。このインストール・プロセスはブラウザによって異なります。

   - Netscape Communicator/Mozilla

     「ブラウザへのインストール」をクリックすると、対応する CA の証明書とともに証明書がインストールされます。プロセスが完了したことを示すメッセージは表示されませんが、ブラウザのステータス・バーには「ドキュメント : 完了。」と表示されます。

- Internet Explorer

  「ブラウザへのインストール」をクリックすると、対応する CA の証明書とともに証明書がインストールされます。ブラウザにより、「証明書は正常にインポートされました。」というメッセージが表示されます。インストール後、署名者の証明書をインポートする必要があるかどうかを確認するメッセージが表示されます。Internet Explorer により、インポート対象の CA に関する詳細が記載されたウィンドウが表示されます。このウィンドウを使用して、署名者をインポートするかどうかを選択します。

- Safari

  このブラウザに証明書を直接インストールすることはできません。証明書をインストールする手順は、次のとおりです。

  – Web ユーザー・インタフェース https://hostname:port/oca/user に移動します。

  – **「ユーザー証明書 - 手動認証」**を選択します。

  – 前に確認したシリアル番号を使用して Web 管理者の証明書を検索します。

  – 証明書を選択して**「詳細表示」**をクリックします。

  – BASE64 でエンコードされた証明書（PKCS#7 形式の CA 連鎖を持った、Base64 でエンコードされた証明書ではない）をコピーし、適切な拡張子（`.pem/.der/.cer`）を持つファイルに保存します。

  – このファイルをダブルクリックします。鍵連鎖アクセス・ユーティリティがポップアップ・ダイアログとともに開き、証明書を鍵連鎖にインポートするかどうかの確認を求められます。（注意 : システムには複数の鍵連鎖がありますが、証明書は必ず、ロックが解除された状態のデフォルトのログイン鍵連鎖にインポートしてください。）

  – 証明書を表示するためのボタンがあります。証明書を表示し、これが管理者の証明書であることを確認します。「OK」をクリックし、証明書を鍵連鎖にインポートします。

管理者証明書をインストールし終わると、管理 Web インタフェースに「認証管理」および「構成管理」タブが表示されます。

登録の手順の詳細は、第 4 章を参照してください。管理者を変更する必要がある場合、第 4 章を再度使用するか、次のトピックを参照してください。

「Web 管理者登録」

ログの表示

このページを使用して、Oracle Application Server Certificate Authority のエラー・ログを検索します。OracleAS Certificate Authority サーバーは、管理しているすべてのコンポーネントのエラー・メッセージをログに記録します。検索基準を入力すると、検索基準と一致するすべてのメッセージが表に表示されます。検索基準を入力する手順は、次のとおりです。

1. 検索基準としてクライアント・アドレス（IP アドレス）またはメッセージの内容を選択します。メッセージの内容を検索基準にする場合は、DN やユーザー名などの情報を入力します。
2. 「実行」をクリックします。

検索基準と一致する最新のメッセージが「ログの表示」表に表示されます。この場合、ページごとに 10 のメッセージが表示されます。

関連項目

「構成管理 -- 一般」の「ロギングおよびトレース」

エンド・ユーザー・インタフェースの各ウィンドウや各フィールド

この項では、Web ユーザー・インタフェースのウィンドウとフィールドについて説明します。

「拡張検索」画面

「拡張」画面を使用して、証明書リクエストや既存の証明書に対する検索の精度を高めます。「拡張」画面には、次の 3 つの検索方法が用意されています。

1. **識別名（DN）を使用した検索**

   証明書所有者または証明書リクエスタの識別名の構成要素を入力します。「検索」リストを使用して、証明書リクエスタと証明書所有者の間で切替えができます。

2. **拡張識別名を使用した検索**

   証明書リクエスタまたは証明書所有者の完全な DN を知っており、それの LDIF 形式での入力方法がわかっている場合に、このオプションを選択します。検索結果を得るには、一続きになった DN を入力する必要があります。たとえば、cn=Margarita Redmond,ou=sales,o=yourcorp は許容されますが、cn=Margarita Redmond,,o=yourcorp は許容されません。次の例で、属性間に空白を入れるかどうかは任意です。

   cn=Margarita Redmond,ou=sales,o=yourcorp,l=Bismarck,st=SD,c=US

3. **シリアル番号 / リクエスト ID の範囲を使用した検索**

   一定のシリアル番号範囲の証明書に関する情報を取得するには、このオプションを選択します。「検索」リストを使用して、リクエストした証明書と既存の証明書の間で切替えができます。

これらの方法を使用した検索の詳細は、「「拡張検索」画面」を参照してください。

「認証」ページ

「認証」ページを使用して、OracleAS Certificate Authority サーバーに対してユーザー自身を認証します。選択するモードは、既存の OracleAS 資格証明に応じて決まります。モードはラジオ・ボタンとして示されます。モードには次があります。

- 自分の OracleAS Single Sign-On 用の名前とパスワードを使用

  OracleAS Single Sign-On ユーザーであり、デジタル証明書を取得または失効する必要がある場合、このオプションを使用します。

- 既存の証明書の使用

  現行の OracleAS Certificate Authority によって発行された有効な証明書がある場合、このオプションを使用します。このような証明書がある場合、Secure Sockets Layer（SSL）プロトコルを使用して OracleAS Certificate Authority に対してユーザー自身を認証できます。

- 手動認可 / 認証を使用

  識別用として OracleAS Single Sign-On または SSL プロトコルを使用しておらず、デジタル証明書を取得する必要がある場合、このオプションを使用します。管理者は、ユーザーの証明書を発行する前にユーザーの識別情報を手動で検証します。

このページで説明するタスクの実行方法の詳細は、次のトピックを参照してください。

- 証明書リクエスト・フォーム - SSL 認証
- SSO 証明書リクエスト・フォーム
- 「証明書リクエスト」フォーム（手動リクエスト）

CA 証明書詳細

このページには、BASE64 形式の認証局（CA）とともに、PKCS#7 形式の CA 証明連鎖で Base64 でエンコードされた証明書が表示されます。Oracle Wallet Manager を使用して PKCS#10 証明書リクエストを作成する場合、エンコードされた CA 証明書を Oracle Wallet Manager にコピー・アンド・ペーストできます。サーバー証明書または下位 CA 証明書をリクエストするには、この方法を使用する必要があります。

CA 証明書の保存

この画面を使用して、認証局（CA）証明書をブラウザにインストールします。BASE64 または PKCS #7CA 形式でエンコードされた CA 証明書を表示するには、「拡張」をクリックします。CA 証明書をブラウザにインストールするには、「ブラウザへのインストール」をクリックします。現行の CA が下位 CA である場合、上位 CA 証明書も表示されます。このフォームを使用して、CA 証明書を Oracle Wallet Manager（OWM）にインポートします。証明連鎖全体が PKCS #7 でエンコーディングされています。

このページには、次の CA 証明書詳細も表示されます。

フィールド	説明
ステータス	「有効」は、証明書が信頼できる状態にあることを示す。ここに表示される値はこの値のみ。
シリアル番号	証明書を参照するために使用される番号。
署名アルゴリズム	オブジェクト識別番号（OID）によって示される使用アルゴリズム。
使用方法	証明書の機能。CA 証明書の場合、この値は常に「証明書署名」か「CRL 署名」のいずれか。
発行局	証明書を発行した CA。ルート CA によって証明書が発行された場合、リクエスタと発行者は同じ。
サブジェクト DN	証明書の所有者の識別名。
有効期間の開始日	証明書の有効期間の開始日時。
有効期間の終了日	証明書の有効期間の終了日時。

関連項目

- CA 証明書の保存

証明書の認可 -- Single Sign-On (SSL)

このページを使用して、新しい証明書に関する詳細を表示し、ブラウザにこの証明書をインストール（「ブラウザへのインストール」をクリック）します。証明書をインストールした後に「OK」を再クリックすると、「ユーザー証明書」ページに戻ります。新しい証明書は、このページの「証明書」バーに表示されます。証明書の認可ページには、次のフィールドがあります。

フィールド	説明
ステータス	この値は常に「有効」。
シリアル番号	これは証明書のシリアル番号。
署名アルゴリズム	オブジェクト識別番号（OID）によって示される使用アルゴリズム。
使用方法	証明書機能。
発行局	証明書を発行した CA。
サブジェクト DN	証明書の所有者の識別名。
有効期間の開始日	証明書の有効期間の開始日時。
有効期間の終了日	証明書の有効期間の終了日時。

ページの下部にあるボタンの 1 つを選択して、目的のタスクを実行します。

ボタン名	機能の説明
OK	「ユーザー証明書」タブのメイン・ページに戻る。
ブラウザへのインストール	証明書をブラウザにインストールする。
ディスクへの保存	証明書をローカル・システム上のファイルに保存する。

証明書詳細

このページを使用して、BASE64 エンコーディングを含む証明書の完全な説明を取得します。このページで変更できないフィールドは、次のとおりです。

フィールド	説明
ステータス	これの値は、「有効」、「失効」または「期限切れ」。
シリアル番号	これは OracleAS Certificate Authority によって割り当てられた証明書のシリアル番号。
署名アルゴリズム	使用アルゴリズム（RSA 暗号化付き MD5 など）を示すオブジェクト識別番号（OID）。
使用方法	証明書機能。
発行局	証明書を発行した CA。
サブジェクト DN	証明書の所有者の識別名。
有効期間の開始日	証明書の有効期間の開始日時。
有効期間の終了日	証明書の有効期間の終了日時。
Base64 でエンコードされた証明書	エンコードされた証明書。
PKCS#7 形式の CA 証明連鎖で Base64 でエンコードされた証明書	PKCS#7 形式でエンコードされた証明書と信頼できる認証局のツリー。この形式では、単一操作を使用して、信頼できる連鎖からルート CA 証明書までのすべての証明書を転送できる。

ページの下部にあるボタンの 1 つを選択して、目的のタスクを実行します。

ボタン名	機能の説明
OK	「ユーザー証明書」タブのメイン・ページに戻る。
失効	証明書を失効する。失効理由を指定する必要がある。
更新	証明書を更新する。新しい有効期間を指定する必要がある。
ブラウザへのインストール	証明書をブラウザにインストールする。

「証明書リクエスト」フォーム

このフォームを使用して、証明書を手動でリクエストします。「証明書リクエスト」フォームには、次のヘッダーがあります。

識別名情報

識別名（DN）は、Oracle Internet Directory におけるユーザー・エントリのロケーションです。OracleAS Certificate Authority は、このディレクトリ・エントリを使用してユーザーの証明書を格納および取得します。このヘッダー内で青いアスタリスクがあるフィールドは、必須です。これらのフィールドは、次のとおりです。

- **一般名**

  証明書リクエスタの名前

- **組織**

  証明書リクエスタが属する企業

連絡情報

証明書リクエスタの名前、電子メール・アドレスおよび電話番号です。「名前」フィールドおよび、「電子メール ID」または「電話番号」フィールドに入力する必要があります。

証明書情報

このヘッダーの下の各フィールドを使用して、証明書の鍵サイズまたは保管方式、証明書の機能および証明書の有効期間を指定します。これらのフィールドの説明は、次のとおりです。

- **証明書鍵サイズ**（Netscape Communicator/Mozilla/Safari ユーザー）

  ブラウザによって生成される秘密鍵の長さです。使用可能なオプションから鍵の強度を選択します。通常は、「512」（低レベル）、「1024」（中レベル）または「2048」（高レベル）です。
  注意 : 一部のブラウザでは使用できないオプションもあります。

- **暗号サービス・プロバイダ**（Internet Explorer ユーザー）

  証明書の保管タイプです。リストをクリックし、保管方法の 1 つを選択します。保管方法は鍵の強度に影響します。**「Microsoft Base Cryptographic Provider」**、**「Microsoft Enhanced Cryptographic Provider」**および**「Microsoft Strong Cryptographic Provider」**から選択します。スマートカードは、対応するスマートカード・デバイスがシステムにインストールされている場合にのみ選択してください。たとえば、Gemplus スマートカード・リーダーがインストールされている場合には、**「Gemplus GemSAFE Card CSP」**を選択できます。ただし、このリーダーがインストールされていない場合、これを選択するのは不適切です。

- **証明書の使用方法**（全種類のブラウザ）

  証明書の機能です。意図した用途およびエンタープライズ・ポリシーに合う使用方法を選択します。どの使用方法が合うかわからない場合は、「認証、署名、暗号化」を選択します。（サイトのデフォルトは事前に選択されています。）次のリストは、選択可能な項目を示します。

機能	説明
認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。）
暗号化	電子ドキュメントの暗号化および復号化を可能にします。
署名	（Secure Multipurpose Internet Mail Extension（S/MIME）を使用して）電子メールなどの電子ドキュメントに対する検証可能な署名を可能にします（また、これらの電子ドキュメントの改ざんを防ぎます）。
認証、暗号化	この両方の目的に証明書を使用できます。
認証、署名	この両方の目的に証明書を使用できます。
認証、署名、暗号化	この 3 つの目的すべてに証明書を使用できます。
署名、暗号化	この両方の目的に証明書を使用できます。
CA 署名	下位 CA 証明書をリクエストできるようにします。
コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します（また、これらの改ざんを防ぎます）。

- **有効期間**（全種類のブラウザのユーザー）

  証明書の有効期間の長さです。リストをクリックし、4 つの選択肢から 1 つを選択します。証明書は最長 10 年間有効です。

関連項目

- 「証明書リクエスト」フォーム（手動リクエスト）

証明書失効リスト

このページには、現行の証明書失効リストが表示されます。このページには、いつリストが最後に更新されたかが示されます。このリストには、失効した証明書ごとにシリアル番号および失効日が表示されます。

このページの各ボタンを使用して、CRL をブラウザにインストール、または CRL をバイナリ・ファイルや BASE64 でエンコードされたテキスト・ファイルとして保存します。（BASE64 でエンコードされたテキスト・ファイルの方が情報を簡単にコピー、貼付けまたは電子メール送信できます。）

CRL をインストール、または選択した方法で保存した後は、**「OK」**をクリックして**「ユーザー証明書」**ページに戻ります。

失効理由

このページを使用して、失効理由を選択します。使用可能なオプションの説明は、次のとおりです。

失効理由	説明
鍵危殆化	ユーザーの秘密鍵が紛失した、または公開された。
所属変更	組織が、別の CA の使用を決定した。
CA 危殆化	CA が下位 CA に置換されたか、CA 証明書が危殆化された。
証明書保留	証明書が一時的に保留されている。
運用停止	既存のルート CA の運用が停止している。新しいルート CA が必要。
CRL から削除	証明書が証明書失効リスト（CRL）から削除されている。
破棄	ルート CA の証明書が置換された。以前の証明書は削除し、新しい証明書をインストールする必要がある。
未指定	理由がないかまたは指定されていない。

証明書の失効方法の詳細は、「証明書の失効」を参照してください。

「証明書リクエスト」フォーム -- 拡張

完全な識別名（DN）が存在していてそれを知っており、それの LDIF 形式での入力方法がわかっている場合、このフォームを使用して証明書をリクエストします。この機能は、標準の「証明書リクエスト」フォームの**識別名情報**ヘッダーのショートカットで、**「拡張 DN」**リンクとして表示されます。「拡張」フォームは、標準フォームと同じ DN コンポーネントをサポートします。DN は、Oracle Internet Directory におけるユーザー・エントリのロケーションです。証明書はこのディレクトリ・エントリに保管され、ここから取り出されます。

関連項目

「証明書リクエスト」フォーム（手動リクエスト）

サーバー / 下位 CA 証明書

このページを使用して、証明書および証明書リクエストに関する情報を検索および表示、または新しいサーバーまたは下位 CA の証明書をリクエストします。**「証明書のリクエスト」**をクリックすると、入力を行うための**「サーバー / 下位 CA 証明書」**フォームが表示されます。

指定した検索の結果として証明書または証明書リクエストのリストが表示された場合、**「選択」**ボタン（左端）をクリックしてから**「詳細表示」**をクリックすると、特定のエントリの詳細を表示できます。最初の 25 行の検索結果より多くの検索結果を表示するには、**「次の 25 行」**をクリックするか、ドロップダウン・リストをクリックして表示範囲を選択します。

関連項目

「サーバー / 下位 CA 証明書」ページのボタンを使用して選択できる機能の詳細は、次のリンクを参照してください。

- 単一の証明書リクエストまたは発行済証明書の表示
- 「サーバー / 下位 CA 証明書」タブ
- 証明書失効リストの更新
- CA 証明書の保存

サーバー / 下位 CA 証明書リクエスト・フォーム

このフォームを使用して、Web サーバーまたは下位認証局に対して証明書をリクエストします。サーバー / 下位 CA 証明書リクエスト・フォームには、次のヘッダーがあります。

証明書リクエスト

証明書をリクエストするには、openSSL reqtool または Oracle Wallet Manager を使用して、BASE64 形式の PKCS#10 エンコーディングで証明書を生成します。次に、エンコードした証明書リクエストを「PKCS#10 リクエスト」フィールドに貼り付けます。

連絡情報

証明書リクエスタの名前、電子メール・アドレスおよび電話番号です。**「名前」**フィールドおよび、**「電子メール ID」**または**「電話番号」**フィールドに入力する必要があります。

証明書情報

このヘッダーの下にある各フィールドを使用して、証明書の機能と有効期間を指定します。これらのフィールドの説明は、次のとおりです。

- **証明書の使用方法**

  証明書の機能です。意図した用途およびエンタープライズ・ポリシーに合う使用方法を選択します。どの使用方法が合うかわからない場合は、「認証、署名、暗号化」を選択します。（サイトのデフォルトは事前に選択されています。）次のリストは、選択可能な項目を示します。

機能	説明
認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。）
暗号化	電子ドキュメントの暗号化および復号化を可能にします。
署名	（Secure Multipurpose Internet Mail Extension（S/MIME）を使用して）電子メールなどの電子ドキュメントに対する検証可能な署名を可能にします（また、これらの電子ドキュメントの改ざんを防ぎます）。
認証、暗号化	この両方の目的に証明書を使用できます。
認証、署名	この両方の目的に証明書を使用できます。
認証、署名、暗号化	この 3 つの目的すべてに証明書を使用できます。
署名、暗号化	この両方の目的に証明書を使用できます。
CA 署名	下位 CA 証明書をリクエストできるようにします。
コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します（また、これらの改ざんを防ぎます）。

- **有効期間**

  証明書の有効期間の長さです。リストをクリックし、有効期間として 6 か月、1 年または 5 年を選択します。

関連項目

- 「サーバー / 下位 CA 証明書」タブ

証明書リクエスト・フォーム - SSL 認証

証明書は持っているが、鍵サイズまたは保管方式が異なる証明書が必要であるかまたは別の目的でその証明書を使用する場合、このフォームを使用します。このフォームには、次のヘッダーとフィールドがあります。

識別名情報

識別名情報ヘッダーの下の**「ユーザー DN」**フィールドには、最初の証明書が割り当てられた DN が表示されます。このフィールドは変更できません。

証明書情報

このヘッダーの下の各フィールドを使用して、証明書の鍵サイズまたは保管方式、証明書の機能および証明書の有効期間を指定します。これらのフィールドの説明は、次のとおりです。

- **証明書鍵サイズ**（Netscape Communicator/Mozilla/Safari ユーザー）

  ブラウザによって生成される秘密鍵の長さです。使用可能なオプションから鍵の強度を選択します。通常は、「512」（低レベル）、「1024」（中レベル）または「2048」（高レベル）です。注意 : 一部のブラウザでは使用できないオプションもあります。

- **暗号サービス・プロバイダ**（Internet Explorer ユーザー）

  証明書の保管タイプまたは鍵サイズです。ドロップダウン・リストをクリックし、**「Microsoft Base Cryptographic Provider」**、**「Microsoft Enhanced Cryptographic Provider」**または**「Microsoft Strong Cryptographic Provider」**のいずれかを選択します。スマートカードは、対応するスマートカード・デバイスがシステムにインストールされている場合にのみ選択してください。たとえば、Gemplus スマートカード・リーダーがインストールされている場合には、**「Gemplus GemSAFE Card CSP」**を選択できます。ただし、このリーダーがインストールされていない場合、これを選択するのは不適切です。

- **証明書の使用方法**（全種類のブラウザのユーザー）

  証明書の機能です。意図した用途およびエンタープライズ・ポリシーに合う使用方法を選択します。どの使用方法が合うかわからない場合は、「認証、署名、暗号化」を選択します。（サイトのデフォルトは事前に選択されています。）次のリストは、選択可能な項目を示します。

機能	説明
認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。）
暗号化	電子ドキュメントの暗号化および復号化を可能にします。
署名	（Secure Multipurpose Internet Mail Extension（S/MIME）を使用して）電子メールなどの電子ドキュメントに対する検証可能な署名を可能にします（また、これらの電子ドキュメントの改ざんを防ぎます）。
認証、暗号化	この両方の目的に証明書を使用できます。
認証、署名	この両方の目的に証明書を使用できます。
認証、署名、暗号化	この 3 つの目的すべてに証明書を使用できます。
署名、暗号化	この両方の目的に証明書を使用できます。
CA 署名	下位 CA 証明書をリクエストできるようにします。
コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します（また、これらの改ざんを防ぎます）。

関連項目

- 証明書リクエスト・フォーム - SSL 認証

SSO 証明書リクエスト・フォーム

OracleAS Single Sign-On サーバーによって認証されており、新規または追加の証明書をリクエストする場合、このフォームを使用します。SSO 証明書リクエスト・フォームには、次のヘッダーとフィールドがあります。

識別名情報

識別名情報ヘッダーの下の**「ユーザー DN」**フィールドには、証明書が発行された DN が表示されます。このフィールドは変更できません。

証明書情報

このヘッダーの下の各フィールドを使用して、証明書の鍵サイズまたは保管方式、証明書の機能および証明書の有効期間を指定します。これらのフィールドの説明は、次のとおりです。

- **証明書鍵サイズ**（Netscape Communicator/Mozilla/Safari ユーザー）

  ブラウザによって生成される秘密鍵の長さです。使用可能なオプションから鍵の強度を選択します。通常は、「512」（低レベル）、「1024」（中レベル）または「2048」（高レベル）です。注意 : 一部のブラウザでは使用できないオプションもあります。

- **暗号サービス・プロバイダ**（Internet Explorer ユーザー）

  証明書の保管タイプまたは鍵サイズです。ドロップダウン・リストをクリックし、**「Microsoft Base Cryptographic Provider」**、**「Microsoft Enhanced Cryptographic Provider」**または**「Microsoft Strong Cryptographic Provider」**のいずれかを選択します。スマートカードは、対応するスマートカード・デバイスがシステムにインストールされている場合にのみ選択してください。たとえば、Gemplus スマートカード・リーダーがインストールされている場合には、**「Gemplus GemSAFE Card CSP」**を選択できます。ただし、このリーダーがインストールされていない場合、これを選択するのは不適切です。

- **証明書の使用方法**（全種類のブラウザのユーザー）

  証明書の機能です。意図した用途およびエンタープライズ・ポリシーに合う使用方法を選択します。どの使用方法が合うかわからない場合は、「認証、署名、暗号化」を選択します。（サイトのデフォルトは事前に選択されています。）次のリストは、選択可能な項目を示します。

機能	説明
認証	エンタープライズ・ポータルへのログイン時など、アクセスまたはサービスをリクエストまたは提供する際に、安全な識別を可能にします。（通常、SSL プロトコルが使用されます。）
暗号化	電子ドキュメントの暗号化および復号化を可能にします。
署名	（Secure Multipurpose Internet Mail Extension（S/MIME）を使用して）電子メールなどの電子ドキュメントに対する検証可能な署名を可能にします（また、これらの電子ドキュメントの改ざんを防ぎます）。
認証、暗号化	この両方の目的に証明書を使用できます。
認証、署名	この両方の目的に証明書を使用できます。
認証、署名、暗号化	この 3 つの目的すべてに証明書を使用できます。
署名、暗号化	この両方の目的に証明書を使用できます。
CA 署名	下位 CA 証明書をリクエストできるようにします。
コード署名	Java コード、JavaScript およびその他の署名されたファイルの提供側に対する検証可能な署名を提供します（また、これらの改ざんを防ぎます）。

関連項目

OracleAS Single Sign-On のユーザー名およびパスワードを使用して証明書をリクエストする方法の詳細は、次を参照してください。

- SSO 証明書リクエスト・フォーム

ユーザー証明書 - 手動認証

このページの**「証明書のリクエスト」**ボタンを使用して、証明書をリクエストします。このページには、認証局（CA）の証明書または証明書失効リスト（CRL）を保存するためのボタンもあります。また、証明書をリクエストするための認証モードを変更することもできます。**「認証の変更」**をクリックすると、「認証」ページに戻り、別の選択を行うことができます。

証明書リクエストを送信した後、「ユーザー証明書 - 手動認証」ページの検索機能を使用してリクエストのステータスをチェックできます。

関連項目

- 単一の証明書リクエストまたは発行済証明書の表示
- 「サーバー / 下位 CA 証明書」タブ
- 証明書失効リストの更新
- CA 証明書の保存
- ユーザー証明書 - 手動認証

ユーザー証明書 - SSL 認証

既存の証明書を使用して OracleAS Certificate Authority にアクセスした場合、このページの**「証明書の取得」**ボタンを使用して証明書を追加できます。また、このフォームには、証明書失効リスト（CRL）を保存するボタンや、証明書をリクエストするための認証モードを変更するボタンもあります。**「認証の変更」**をクリックすると、「認証」ページに戻り、変更を行うことができます。

有効な証明書はすべて**「証明書」**バーの下のマスター表に表示されます。各行には、シリアル番号、有効期間および使用方法タイプなど、特定の証明書に関する情報が記載されています。行の左端の列にあるボタンをクリックすると、証明書に関する追加情報を表示、または証明書を失効できます。秘密鍵が紛失、破損または盗難された場合、証明書を失効する必要があります。

関連項目

- 既存の証明書を使用して証明書を追加する方法の詳細は、「証明書リクエスト・フォーム - SSL 認証」を参照してください。
- CRL を保存する方法の詳細は、「証明書失効リスト」を参照してください。

ユーザー証明書 - SSO 認証

このページの**「証明書の取得」**ボタンを使用して、新しい証明書をリクエストまたは追加します。また、このページには、証明書失効リスト（CRL）を保存するボタンや、証明書をリクエストするための認証モードを変更するボタンもあります。**「認証の変更」**をクリックすると、「認証」ページに戻り、選択を行うことができます。

有効な証明書はすべて**「証明書」**バーの下のマスター表に表示されます。各行には、シリアル番号、有効期間および使用方法タイプなど、特定の証明書に関する情報が記載されています。証明書に関する追加詳細を表示、または証明書を失効するには、その証明書の行の**「選択」**列にあるボタンをクリックし、**「詳細表示」**をクリックします。秘密鍵が紛失、破損または盗難された場合、証明書を失効する必要があります。

関連項目

- OracleAS Single Sign-On のユーザー名およびパスワードを使用して証明書をリクエストする方法の詳細は、「SSO 証明書リクエスト・フォーム」を参照してください。
- CRL を保存する方法の詳細は、「証明書失効リスト」を参照してください。

OracleAS Certificate Authority ホームページへようこそ。

Oracle Certificate Authority のユーザー・ページには、X.509 証明書をリクエスト、表示および失効する機能や、証明書失効リストを保存する機能があります。「認証」ページを使用して、これらのタブにアクセスします。このウィンドウの各タブを使用して、Oracle Certificate Authority のユーザー・ページ間を移動できます。

- **「ホーム」**タブを使用すると、このページに戻ります。
- **「ユーザー証明書」**タブでは、証明書を表示および失効、証明書リクエストを作成、認証方式を変更、証明書失効リストを保存できます。
- **サーバー / 下位 CA** タブでは、「サーバー / 下位 CA 証明書」フォームを使用して証明書および証明書リクエストを検索できます。また、このフォームを使用して、Web サーバーまたは下位認証局の PKCS#10 エンコード済証明書をリクエスト、および Oracle Certificate Authority の認証局証明書を保存またはインストールできます。
- **「ログの表示」**タブを使用して、エラー、警告および監査ログを検索できます。

また、このページを使用して、次の 4 つのタスクを自由に組み合せて実行できます。

- **認証局の証明書をブラウザにインストールします：**
  - Netscape の場合、**新しい認証局**ダイアログ・ボックスが表示されます。

    各ダイアログ・ボックスを順にクリックしていき、証明書を受け入れるかどうかを決定します。最後のダイアログ・ボックスで、証明書を受け入れる場合は**「終了」**をクリックし、証明書を拒否または受入れを延期する場合は**「取消」**をクリックします。
  - Internet Explorer の場合、警告ダイアログ・ボックスにファイルの名前、タイプおよびソースが表示され、このファイルをオープンまたは保存するかを確認するメッセージが表示されます。**「保存」**をクリックし、ファイル・システム上の保存先を選択します。
  - Safari の場合、証明書はブラウザに直接インポートできません。**「ファイルシステムに認証局の証明書を保存してください」**の手順に従い、証明書をインストールします。
- **証明書失効リストをブラウザにインストールします：**
  - Netscape の場合、CRL をブラウザにインストールすると、CRL が正常にインポートされたことを示すダイアログ・ボックスが表示されます。また、発行者や次回の更新時が示される他、必要に応じて CRL の自動生成を有効化することもできます。（自動生成を有効化する場合、更新の頻度を指定できます。）
  - Internet Explorer の場合、警告ダイアログ・ボックスにファイルの名前、タイプおよびソースが表示され、このファイルをオープンまたは保存するかを確認するメッセージが表示されます。**「保存」**をクリックし、ファイル・システム上の保存先を選択します。

- **ファイルシステムに認証局の証明書を保存してください：**
  - Netscape の場合、認証局証明書をファイル・システムに保存すると、このファイル（OCABase64.cert）に対して行う処理を確認するダイアログ・ボックスが表示されます。**「ディスクに保存」**を選択し、**「OK」**をクリックします。表示された「保存」ダイアログで、保存先を選択し、**「保存」**をクリックします。
  - Internet Explorer の場合、警告ダイアログ・ボックスにファイルの名前、タイプおよびソースが表示され、このファイルをオープンまたは保存するかを確認するメッセージが表示されます。**「保存」**をクリックし、ファイル・システム上の保存先を選択します。
  - Safari の場合、認証局の BASE64 エンコード済証明書を示すページが表示されます。この証明書をコピーして `.der/.pem/.cer` ファイルに貼り付けます。このファイルをダブルクリックします。鍵連鎖アクセス・ユーティリティがポップアップ・ダイアログとともに開き、証明書を鍵連鎖にインポートするかどうかの確認を求められます。（注意：システムには複数の鍵連鎖がありますが、証明書は必ず、ロックが解除された状態のデフォルトのログイン鍵連鎖にインポートしてください。）
- **ファイルシステムに証明書失効リストを保存してください：**
  - Netscape の場合、証明書失効リストをファイル・システムに保存すると、このファイル（OCAcrlBase64.txt）に対して行う処理を確認するダイアログ・ボックスが表示されます。**「ディスクに保存」**を選択し、**「OK」**をクリックします。表示された「保存」ダイアログで、保存先を選択し、**「保存」**をクリックします。
  - Internet Explorer の場合、警告ダイアログ・ボックスにファイルの名前、タイプおよびソースが表示され、このファイルをオープンまたは保存するかを確認するメッセージが表示されます。**「保存」**をクリックし、ファイル・システム上の保存先を選択します。

用語集

1 次ノード（Primary Node）

Oracle Application Server Cold Failover Cluster（Identity Management）で、任意の指定時間にアプリケーションを実行できるクラスタ・ノード。

関連項目：「**2 次ノード**」

2 次ノード（Secondary Node）

Oracle Application Server Cold Failover Cluster（Identity Management）で、フェイルオーバー時におけるアプリケーションの移動先クラスタ・ノード。

関連項目：「**1 次ノード**」

3DES

「**トリプル・データ暗号化規格**」を参照。

ACI

「**アクセス制御項目**」を参照。

ACL

「**アクセス制御リスト**」を参照。

ACP

「**アクセス制御ポリシー・ポイント**」を参照。

AES

「**拡張暗号化規格**」を参照。

API

「**Application Program Interface**」を参照。

Application Program Interface（API）

コンピュータのアプリケーションとそれより下位レベルのサービスおよび機能（オペレーティング・システム、デバイス・ドライバおよびその他のソフトウェア・アプリケーションなど）の間のインタフェースとなる一連のソフトウェア・ルーチンおよび開発ツール。API は、プログラマにとってはソフトウェア・アプリケーションを構築するための基礎的要素として使用される。たとえば、LDAP 対応クライアントは、LDAP API で使用可能なプログラム・コールを介して Oracle Internet Directory にアクセスする。

ASN.1

抽象構文記法 1（ASN.1）は、情報データの構文を定義するために使用される国際電気通信連合（ITU）の表記法。構造化情報（通常、複数の通信メディアを介して伝達する必要がある情報）の記述に使用される。広く、インターネット・プロトコルの仕様の中で使用されている。

ASR

「**Oracle Database アドバンスト・レプリケーション**」を参照。

Basic 認証（Basic Authentication）

大部分のブラウザによってサポートされている**認証**プロトコル。Web サーバーは、データ転送を介して渡されたエンコード済ユーザー名およびパスワードを使用してエンティティを認証する。Base64 エンコーディングは誰でも簡単に入手可能なデコード・ユーティリティを使用してデコードできるため、Basic 認証は平文認証とも呼ばれる。なお、エンコーディング（encoding）は**暗号化**（encryption）とは異なるので注意。

BER

「**基本エンコーディング・ルール**」を参照。

Blowfish

1993 年に Bruce Schneier によって開発された、**DES** のより高速な後継の**対称型暗号化**アルゴリズム。64 ビットのブロックと最大 448 ビットの鍵を使用した**ブロック暗号**である。

CA

「**認証局**」を参照。

CA 証明書（CA certificate）

認証局は、発行するすべての証明書に**秘密鍵**によって署名する。これに対応する認証局**公開鍵**が、CA 証明書と呼ばれる証明書（ルート証明書とも呼ばれる）に含まれる。CA の秘密鍵によって署名されたメッセージをブラウザが信頼するには、ブラウザの持つ信頼できるルート証明書のリストに当該の CA 証明書が含まれる必要がある。

CBC

「**暗号ブロック連鎖**」を参照。

CMP

「**認証管理プロトコル**」を参照。

CMS

「**暗号化メッセージ構文**」を参照。

configset

「**構成設定エントリ**」を参照。

CRL

「**証明書失効リスト**」を参照。

CRMF

「**証明書リクエスト・メッセージ・フォーマット**」を参照。

dads.conf

データベース・アクセス記述子の構成に使用される Oracle HTTP Server 構成ファイル。

DAS

「**Oracle Delegated Administration Services**（DAS）」を参照。

DER

「**識別エンコーディング・ルール**」を参照。

DES

「**データ暗号化規格**」を参照。

DIB

「**ディレクトリ情報ベース**」を参照。

Diffie-Hellman

Diffie-Hellman（DH）は、送信者と受信者がセキュアでない通信チャネルを介して共有の秘密を保持できる公開鍵暗号化プロトコル。1976 年に初公開された、実用的な公開鍵暗号化システムとしては初のシステム。

関連項目：「**対称型アルゴリズム**」

Directory Manager

「**Oracle Directory Manager**」を参照。

DIS

「**ディレクトリ統合サーバー**」を参照。

DIT

「**ディレクトリ情報ツリー**」を参照。

DN

「**識別名**」を参照。

Document Type Definition（DTD）

特定の **XML** ドキュメントで有効とするタグおよびタグ・シーケンスについての制約を指定するドキュメント。XML の親言語である Simple Generalized Markup Language（SGML）のルールに準拠する。

DRG

「**ディレクトリ・レプリケーション・グループ**」を参照。

DSA

「**デジタル署名アルゴリズム**」または「**ディレクトリ・システム・エージェント**」を参照。

DSE

「**ディレクトリ固有エントリ**」を参照。

DTD

「**Document Type Definition**」を参照。

ECC

「**楕円曲線暗号**」を参照。

ECDSA

「**楕円曲線デジタル署名アルゴリズム**」を参照。

EJB

「**Enterprise JavaBeans**」を参照。

Enterprise JavaBeans（EJB）

多層クライアント / サーバー・システムのコンポーネント・アーキテクチャを定義する Sun 社によって開発された Java API。EJB システムは、Java で作成されるため、プラットフォームには依存しない。EJB システムはオブジェクト指向であるため、再コンパイルや構成はほとんどまたはいっさいしないで既存のシステムに実装できる。

Enterprise Manager

「**Oracle Enterprise Manager**」を参照。

FIM

「フェデレーテッド ID 管理」を参照。

FIPS

「米国連邦情報処理標準」を参照。

GET

ログイン資格証明をログイン URL の一部として送信する認証方式。

Global Unique Identifier（GUID）

エントリがディレクトリに追加されるときにシステムによって生成され、エントリに挿入される識別子。マルチマスター・レプリケーション環境では、GUID（DN ではない）はエントリを一意に識別する。ユーザーはエントリの GUID を変更できない。

GUID

「Global Unique Identifier」を参照。

HMAC

「ハッシュ・メッセージ認証コード」を参照。

HTTP

Hyper Text Transfer Protocol（HTTP）は、ドキュメントをリクエストしてその内容を送信するために、Web ブラウザとサーバー間で使用されるプロトコルである。この仕様は World Wide Web Consortium によって制定および保守されている。

HTTP Server

「Oracle HTTP Server」を参照。

httpd.conf

Oracle HTTP Server の構成に使用されるファイル。

iASAdmins

Oracle Application Server でユーザーおよびグループの管理機能に関与する管理グループ。OracleAS Single Sign-On 管理者は iASAdmins グループのメンバーである。

ID 管理（identity management）

組織内でネットワーク・エンティティのセキュリティ・ライフ・サイクル全体を管理するプロセス。通常、組織のアプリケーション・ユーザーを管理することを指す。セキュリティ・ライフ・サイクルの手順には、アカウントの作成、停止、権限変更およびアカウントの削除が含まれる。管理対象のネットワーク・エンティティには、ユーザー以外にも、デバイス、プロセス、アプリケーションなど、ネットワーク環境で通信する必要があるものはすべて含まれる。この他にも、ID 管理プロセスによって管理されるエンティティには、カスタマ、取引先、Web サービスなど、組織外のユーザーを含めることもできる。

ID 管理インフラストラクチャ・データベース（Identity Management Infrastructure Database）

OracleAS Single Sign-On および Oracle Internet Directory のデータが含まれるデータベース。

ID 管理レルム（Identity Management Realm）

同じ管理ポリシーによって管理されるすべての識別情報のコレクション。企業では、通常、イントラネットへのアクセス権を持つすべての従業員が 1 つのレルムに属し、企業のパブリック・アプリケーションにアクセスするすべての外部ユーザーが別のレルムに属す。ID 管理レルムは、ディレクトリにおいて、特別なオブジェクト・クラスが関連付けられた固有のエントリによって表される。

ID 管理レルム固有の Oracle コンテキスト（Identity Management Realm-Specific Oracle Context）

ID 管理レルムごとに含まれる Oracle コンテキスト。次の情報が格納されている。

- ID 管理レルムのユーザー・ネーミング・ポリシー（ユーザーのネーミングおよびロケーティングの方法）
- 必須認証属性
- ID 管理レルム内のグループのロケーション
- ID 管理レルムにおける権限割当（例 : レルムにユーザーを追加する権限を誰が持つか）
- そのレルムのアプリケーション固有データ（認可など）

Internet Directory

「**Oracle Internet Directory**」を参照。

Internet Engineering Task Force (IETF)

新しいインターネット標準仕様の制定を主催している団体。インターネット・アーキテクチャの発展とインターネットの円滑な運用に関心のあるネットワーク設計者、オペレータ、ベンダーおよび研究者の国際的コミュニティ。

Internet Message Access Protocol（IMAP）

クライアントがサーバー上の電子メール・メッセージにアクセスして操作するためのプロトコル。リモート・メッセージ・フォルダ（メールボックスとも呼ばれる）をローカル・メールボックスと機能的に同等の方法で操作できる。

J2EE

「**Java 2 Platform, Enterprise Edition**」を参照。

Java 2 Platform, Enterprise Edition（J2EE）

Sun 社によって定義された、エンタープライズ・アプリケーションを開発および配置するための環境。J2EE プラットフォームは、多層の Web ベース・アプリケーションを開発するための機能を提供する一連のサービス、Application Program Interface（API）およびプロトコルで構成される。

Java Server Page（JSP）

Sun 社によって開発された Java サーブレット技術の拡張機能としてのサーバー・サイド・テクノロジ。HTML コードと連携するがそのページのロジックを静的要素（ページの設計および表示）から切り離す動的スクリプト機能が用意されている。この Java ソース・コードとその拡張機能が HTML ページに埋め込まれることにより、HTML の機能が向上し、動的データベース問合せなどに使用できるようになる。

JSP

「**Java Server Page**」を参照。

LDAP

「**Lightweight Directory Access Protocol**」を参照。

LDAP Data Interchange Format（LDIF）

システム間でディレクトリ・データを交換するためのテキスト・ベースの共通の形式。LDAP コマンドライン・ユーティリティへの入力ファイルのフォーマットの標準のセット。

LDAP 接続キャッシュ（LDAP Connection Cache）

スループットを向上させるために、OracleAS Single Sign-On Server は Oracle Internet Directory への接続をキャッシュし、再使用する。

LDIF

「**LDAP Data Interchange Format**」を参照。

Lightweight Directory Access Protocol（LDAP）

ディレクトリ内の情報にアクセスするための一連のプロトコル。すべての種類のインターネット・アクセスに必要である TCP/IP をサポートしている。その設計規定の枠組みでは、Oracle Internet Directory など、業界標準のディレクトリ製品がサポートされる。LDAP は **X.500** 規格の簡易バージョンであるため、X.500 light とも呼ばれる。

MAC

「**メッセージ認証コード**」を参照。

MD2

メッセージ・ダイジェスト 2（MD2）は、メッセージ・ダイジェストの**ハッシュ関数**の 1 つ。入力テキストを処理し、128 ビットの**メッセージ・ダイジェスト**を作成する。このメッセージ・ダイジェストは、メッセージに対して一意であり、データの整合性を検証するために使用できる。MD2 は、RSA Security 社の Ron Rivest によって開発された関数で、スマートカードのような小型メモリーを搭載するシステムでの使用を目的としている。

MD4

メッセージ・ダイジェスト 4（MD4）は、**MD2** と似ているが、特にソフトウェアでの高速処理を目的として設計されている。

MD5

メッセージ・ダイジェスト 5（MD5）は、メッセージ・ダイジェストの**ハッシュ関数**の 1 つ。入力テキストを処理し、128 ビットの**メッセージ・ダイジェスト**を作成する。このメッセージ・ダイジェストは、メッセージに対して一意であり、データの整合性を検証するために使用できる。**MD4** における潜在的な弱点が報告された後、Ron Rivest によって開発された。MD4 と似ているが、元のデータに対する操作が多くなるため、低速になる。

MDS

「**マスター定義サイト**」を参照。

mod_osso

ユーザーが OracleAS Single Sign-On にログインした後、OracleAS Single Sign-On によって保護されてい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 ヘッダーを受け入れることを可能にする Oracle HTTP Server のモジュール。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 に保管されるユーザー・データ。ユーザーが認証されるときに作成される。同じユーザーによって別のアプリケーションがリクエストされると、Web サーバーは mod_osso Cookie の情報を使用してこのユーザーをそのアプリケーションにログインさせる。この機能により、サーバーのレスポンス時間が短縮される。

mod_proxy

mod_osso を使用してレガシー・アプリケーションまたは**外部アプリケーション**に対するシングル・サインオンを可能にする Oracle HTTP Server のモジュール。

MTS

「**共有サーバー**」を参照。

OASIS

Organization for the Advancement of Structured Information Standards。E-Business 標準の策定、集約および採用を推進する国際的な非営利コンソーシアム。

OC4J

「**Oracle Containers for J2EE**」を参照。

OCA

「**Oracle Certificate Authority**」を参照。

OCI

「**Oracle Call Interface**」を参照。

OCSP

「**オンライン証明書ステータス・プロトコル**」を参照。

OEM

「**Oracle Enterprise Manager**」を参照。

OID

「**Oracle Internet Directory**」を参照。

OID 制御ユーティリティ（OID Control Utility）

run-server および stop-server コマンドを発行するためのコマンドライン・ツール。これらのコマンドは、**OID モニター**プロセスによって解釈および実行される。

OID データベース・パスワード・ユーティリティ（OID Database Password Utility）

このユーティリティを使用して、Oracle Internet Directory が Oracle Database に接続するためのパスワードを変更する。

OID モニター（OID Monitor）

Oracle Internet Directory Server プロセスを開始、モニターおよび終了する Oracle Internet Directory コンポーネント。また、レプリケーション・サーバー（インストールされている場合）および Oracle Directory Integration Platform Server を制御する。

Oracle Application Server Single Sign-On

費用レポート、メールおよび給付金などのアプリケーションにセキュアにログインできるようにするためのプログラム・ロジックで構成されている。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**という 2 つの形式がある。いずれの場合も、認証を 1 回行うのみで複数のアプリケーションにアクセスできる。

Oracle Call Interface（OCI）

第三世代言語のネイティブ・プロシージャまたはファンクション・コールを使用して Oracle Database Server にアクセスし、SQL 文実行のすべてのフェーズを制御するアプリケーションを作成するための Application Program Interface（API）。

Oracle Certificate Authority

Oracle Application Server 環境で使用するための**認証局**。Oracle Internet Directory を証明書の格納リポジトリとして使用する。OracleAS Certificate Authority を OracleAS Single Sign-On および Oracle Internet Directory と組み合せて使用すると、これらに依存するアプリケーションがシームレスな証明書プロビジョニングを行うことができるようになる。Oracle Internet Directory でプロビジョニングされ、OracleAS Single Sign-On で認証されたユーザーは、OracleAS Certificate Authority にデジタル証明書をリクエストできる。

Oracle CMS

IETF の**暗号化メッセージ構文**プロトコルを実装したもの。セキュアなメッセージ・エンベロープを実現するデータ保護方式を定義する。

Oracle Containers for J2EE（OC4J）

Java 2 Platform, Enterprise Edition 用のスケーラブルな軽量コンテナ。

Oracle Crypto

コア暗号化アルゴリズムを提供する Pure Java ライブラリ。

Oracle Database アドバンスト・レプリケーション（Oracle Database Advanced Replication）

2 つの Oracle データベース間で、データベース表を継続的に同期化できる Oracle Database の機能。

Oracle Delegated Administration Services

ユーザーのかわりにディレクトリを操作するために事前定義された個々のサービス（Oracle Delegated Administration Services 単位と呼ばれる）。Oracle Internet Directory Self-Service Console を使用すると、Oracle Internet Directory を使用する Oracle アプリケーションとサード・パーティ・アプリケーションの両方を対象とした管理ソリューションを開発およびデプロイしやすくなる。

Oracle Directory Integration

Oracle Internet Directory と複数の関連するプラグインおよびコネクタを使用して複数のディレクトリを統合するためのインタフェースとサービスのコレクション。企業が外部ユーザー・リポジトリを使用して Oracle 製品から認証されるようにする Oracle Internet Directory の機能。

Oracle Directory Integration Platform

Oracle Internet Directory のコンポーネント。Oracle Internet Directory などのセントラル LDAP ディレクトリを中心として各アプリケーションを統合するために開発されたフレームワーク。

Oracle Directory Integration Server

Oracle Directory Integration Platform 環境で、変更イベントがないかどうか Oracle Internet Directory をモニターし、**ディレクトリ統合プロファイル**に記載されている情報に基づいてアクションを実行するデーモン・プロセス。

Oracle Directory Manager

Oracle Internet Directory を管理するためのグラフィカル・ユーザー・インタフェースを備えた Java ベースのツール。

Oracle Enterprise Manager

グラフィカル・コンソール、エージェント、共通サービスおよびツールを組み合せて、Oracle 製品を管理するために統合された包括的システム管理プラットフォームを提供する、独立した Oracle 製品。

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。Oracle では、Apache Group によって開発された HTTP を使用する。

Oracle Identity Management

すべての企業 ID とこれら ID による企業内の様々なアプリケーションへのアクセスをデプロイメントでセキュアに集中管理できるようにするインフラストラクチャ。

Oracle Internet Directory

分散したユーザーおよびネットワーク・リソースに関する情報を取得するための汎用ディレクトリ・サービス。**Lightweight Directory Access Protocol** バージョン 3 と、Oracle Database の高度なパフォーマンス、スケーラビリティ、堅牢性および可用性を組み合せたもの。

Oracle Liberty SDK

リバティ・アライアンス・プロジェクトの仕様を実装するためのもの。リバティに準拠したサード・パーティ・アプリケーション間のフェデレーテッド・シングル・サインオンを実現する。

Oracle Net Services

各サービスやそれらのクライアント・アプリケーションが様々なコンピュータ上に分散して通信できるようにする Oracle ネットワーク製品ファミリの基盤。主な機能は、ネットワーク・セッションを確立し、クライアント・アプリケーションとサーバー間でデータを転送すること。ネットワーク内のコンピュータごとに配置される。ネットワーク・セッションが確立された後は、クライアントとサーバーのデータ・クーリエとして動作する。

Oracle PKI SDK

公開鍵インフラストラクチャ実装内で必要となるセキュリティ・プロトコルを実装する。

Oracle PKI 証明書使用（Oracle PKI certificate usages）

証明書がサポートする Oracle アプリケーションのタイプを定義する。

Oracle SAML

異なるシステムおよびアプリケーション間で XML ベース形式のセキュリティ資格証明を交換するためのフレームワークを提供する（「**Security Assertions Markup Language**」の「**OASIS**」仕様を参照）。

Oracle Security Engine

X.509 証明書の管理機能を付けることで Oracle Crypto を拡張したもの。Oracle Crypto のスーパーセット。

Oracle S/MIME

セキュアな電子メールを実現するために、**Internet Engineering Task Force** の **Secure/Multipurpose Internet Mail Extension** 仕様を実装したもの。

Oracle Wallet Manager

セキュリティ管理者がクライアントとサーバーで公開鍵のセキュリティ資格証明を管理するために使用する Java ベースのアプリケーション。

関連資料：『Oracle Advanced Security 管理者ガイド』

Oracle Web Services Security

既存のセキュリティ技術を使用した認証および認可用のフレームワーク（Oracle Web Services Security の「**OASIS**」仕様を参照）。

OWM

「**Oracle Wallet Manager**」を参照。

Oracle XML Security

XML 暗号化および XML 署名に関する W3C 仕様を実装したもの。

OracleAS Portal

ファイル、イメージ、アプリケーションおよび Web サイトを統合するためのメカニズムを提供する、OracleAS Single Sign-On の**パートナ・アプリケーション**。この外部アプリケーション・ポートレットは、外部アプリケーションへのアクセスを提供する。

Oracle コンテキスト（Oracle Context）

「**ID 管理レルム固有の Oracle コンテキスト**」および「**ルート Oracle コンテキスト**」を参照。

peer-to-peer レプリケーション（Peer-To-Peer Replication）

マルチマスター・レプリケーションまたは *n* 方向レプリケーションとも呼ばれる。対等に動作する複数のサイトがレプリケート・データ・グループを管理できるようにする、レプリケーションの 1 タイプ。このようなレプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードでもあり、各ノード上でディレクトリ全体がレプリケートされる。

PKCS#1

Public Key Cryptography Standards（PKCS）は、RSA Laboratories によって作成された仕様。PKCS#1 には、RSA アルゴリズムに基づく公開鍵暗号方式の実装に関する推奨事項が記載されている。暗号の基本型、暗号方式、署名方式、鍵の記述と方式の識別に使用する ASN.1 構文について記載されている。

PKCS#10

Public Key Cryptography Standards（PKCS）は、RSA Laboratories によって作成された仕様。PKCS #10 には、公開鍵、名前および場合によっては一連の属性についての証明書をリクエストする構文が記載されている。

PKCS#12

Public Key Cryptography Standards（PKCS）は、RSA Laboratories によって作成された仕様。PKCS #12 には、秘密鍵、証明書、その他の秘密および拡張領域を含む個人の識別情報の送信構文が記載されている。この規格に準拠するシステム（ブラウザやオペレーティング・システムなど）を使用すると、個人の識別情報の単一セットを、通常は **Wallet** と呼ばれる形式で、インポート、エクスポートおよび送信できる。

PKCS#5

Public Key Cryptography Standards（PKCS）は、RSA Laboratories によって作成された仕様。PKCS#5 には、パスワード・ベースの暗号化の実装に関する推奨事項が記載されている。

PKCS#7

Public Key Cryptography Standards（PKCS）は、RSA Laboratories によって作成された仕様。PKCS #7 には、デジタル署名やデジタル・エンベロープなどの暗号化の適用対象となるデータの一般構文が記載されている。

PKCS#8

Public Key Cryptography Standards（PKCS）は、RSA Laboratories によって作成された仕様。PKCS #8 には、公開鍵アルゴリズム用の秘密鍵や一連の属性など、秘密鍵情報の構文が記載されている。また、暗号化された秘密鍵の構文も記載されている。

PKI

「**公開鍵インフラストラクチャ**」を参照。

Point-to-Point レプリケーション（Point-to-Point Replication）

多分岐レプリケーションとも呼ばれる、サプライヤがコンシューマに直接レプリケートする、レプリケーションの 1 タイプ。この後、このコンシューマは、他の 1 つ以上のコンシューマにレプリケートできる。その際は、完全レプリケーションと部分的レプリケーションのいずれでも可。

policy.properties

OracleAS Single Sign-On Server が必要とする基本パラメータが含まれる Oracle Application Server Single Sign-On 用の多目的の構成ファイル。マルチレベルの認証など、OracleAS Single Sign-On の拡張機能を構成するためにも使用される。

POSIX

Portable Operating System Interface for UNIX。オペレーティング・システム間でアプリケーションが移植できるようにアプリケーション・ソース・コードの記述方法を決定するプログラム・インタフェース規格のセット。後続の規格の制定が **Internet Engineering Task Force** によって推進されている。

POST

ログイン資格証明をログイン・フォームの本文の一部として送信する認証方式。

RC2

Rivest Cipher Two（RC2）は、RSA Security 社の Ronald Rivest によって開発された 64 ビットの**ブロック暗号**で、**データ暗号化規格**の後継技術として設計された。

RC4

Rivest Cipher Four（RC4）は、RSA Security 社の Ronald Rivest によって開発された**ストリーム暗号**のことを指す。最大 1024 ビットの可変鍵を使用できる。**Secure Sockets Layer** プロトコルを使用する Web サイト間のトラフィックを暗号化してデータ通信を保護する目的で最も広範に使用されている。

RDN

「**相対識別名**」を参照。

RFC

Internet Request For Comments（RFC）ドキュメントには、インターネットのプロトコルとポリシーの定義が記載されている。Internet Engineering Task Force（IETF）は、新しい規格の討議、策定および普及を推進している。規格は、RFC の頭字語と参照番号を使用して公開される。たとえば、電子メールの公式規格は RFC 822。

RSA

考案者（Rivest、Shamir および Adelman）の頭文字を取って命名された**公開鍵暗号化**アルゴリズム。最も一般的に使用されている暗号化および認証のアルゴリズムで、Netscape 社や Microsoft 社の Web ブラウザ、およびその他多くの製品の一部として組み込まれている。

RSAES-OAEP

RSA Encryption Scheme - Optimal Asymmetric Encryption Padding（RSAES-OAEP）は、**RSA** アルゴリズムと OAEP 方式を組み合せた公開鍵暗号化方式。Optimal Asymmetric Encryption Padding（OAEP）は、Mihir Bellare および Phil Rogaway によって開発されたメッセージ・エンコード方式。

S/MIME

「**Secure/Multipurpose Internet Mail Extension**」を参照。

SAML

「**Security Assertions Markup Language**」を参照。

SASL

「**Simple Authentication and Security Layer**」を参照。

Secure Hash Algorithm（SHA）

入力に基づいて 160 ビットの**メッセージ・ダイジェスト**を生成する**ハッシュ関数**アルゴリズム。デジタル署名標準（DSS）で使用される。128、192 および 256 ビットの 3 つの鍵サイズが用意された拡張暗号化規格（AES）が導入されたことに伴い、同レベルのセキュリティを持つ対のハッシュ・アルゴリズムが必要になった。新しいハッシュ・アルゴリズム SHA-256、SHA-284 および SHA-512 は、この拡張要件に準拠するものである。

Secure Sockets Layer（Secure Sockets Layer: SSL）

ネットワーク（インターネットなど）間で暗号化および認証された通信を実現するために Netscape 社によって設計されたプロトコル。RSA の**公開鍵暗号化**システムを使用するが、このシステムに含まれているデジタル証明も使用することになる。SSL では、セキュアな通信の 3 つの要素である**機密保護**、**認証**および**整合性**が実現されている。

SSL が進化したものが **Transport Layer Security**。TLS と SSL は相互運用できない。ただし、TLS を使用して送信されたメッセージは、SSL 対応のクライアントで処理できる。

Secure/Multipurpose Internet Mail Extension（S/MIME）

デジタル署名と**暗号化**を使用して MIME を保護するための Internet Engineering Task Force（IETF）の規格。

Security Assertions Markup Language（SAML）

インターネットを介してセキュリティ情報を交換するための **XML** ベースのフレームワーク。SAML がないと相互運用できない様々なセキュリティ・サービス・システム間で**認証**および**認可**情報を交換できるようにする。SAML 1.0 仕様は、2002 年に **OASIS** によって採用された。

SGA

「**システム・グローバル領域**」を参照。

SHA

「**Secure Hash Algorithm**」を参照。

Signed Public Key And Challenge（SPKAC）

Netscape Navigator ブラウザが証明書をリクエストするために使用する専用プロトコル。

Simple Authentication and Security Layer（SASL）

コネクションベースのプロトコルに認証サポートを追加する方式。この仕様を使用するため、プロトコルには、ユーザーを識別してサーバーに認証させるためのコマンドと、オプションで、後続のプロトコル対話に使用するセキュリティ・レイヤーを取り決めるためのコマンドが含まれる。このコマンドには、SASL メカニズムを識別するために必要な引数が用意されている。

Single Sign-On Server

ユーザーが費用レポート、メールおよび給付金などのシングル・サインオン・アプリケーションにセキュアにログインできるようにするプログラム・ロジック。

SLAPD

スタンドアロン LDAP デーモン。レプリケーションを除く、ディレクトリの大部分の機能を受け持つ LDAP ディレクトリ・サーバー・サービス。

SOAP

Simple Object Access Protocol（SOAP）は、HTTP を使用してインターネットを介してシステム間でメッセージを交換するためのフレームワークを定義する **XML** ベースのプロトコル。SOAP メッセージは、3 つの部分で構成される。すなわち、メッセージとその処理方法が記載されたエンベロープ、アプリケーションで定義されたデータ型のインスタンスを表現するための一連のエンコーディング・ルール、およびリモート・プロシージャ・コールおよびレスポンスを表現するための規約である。

SPKAC

「**Signed Public Key And Challenge**」を参照。

SSL

「**Secure Sockets Layer**」を参照。

subACLSubentry

アクセス制御リスト情報が含まれる特殊なタイプの**サブエントリ**。

subSchemaSubentry

スキーマ情報が含まれる特殊なタイプの**サブエントリ**。

TLS

「**Transport Layer Security**」を参照。

Transport Layer Security（TLS）

インターネットを介して通信プライバシを提供するプロトコル。このプロトコルにより、クライアント / サーバー・アプリケーションは、傍受、改ざんまたはメッセージの偽造を防ぎながら通信が可能になる。

TSP

「タイムスタンプ・プロトコル」を参照。

Unicode

汎用キャラクタ・セットの 1 タイプで、16 ビット空間でエンコードされた 64,000 文字からなるコレクション。既存のほとんどすべてのキャラクタ・セット規格のほぼすべての文字をエンコードしており、世界中で使用されている大部分の手書き文字を網羅している。Unicode は Unicode によって所有および定義されている。Unicode はエンコーディングの標準である。つまり、その値は様々なロケールで順に渡すことができるということである。ただし、Unicode とすべての Oracle キャラクタ・セットの間での、情報の破損なしでのラウンドトリップ変換までは保証されない。

UNIX Crypt

UNIX の暗号化アルゴリズム。

URI

Uniform Resource Identifier（URI）。テキスト・ページ、ビデオまたはサウンド・クリップ、静止画または動画、あるいはプログラムなど、Web 上の任意の位置にあるコンテンツを識別するための方法。URI の最も一般的な形式は、**URL** と呼ばれる、URI の特別な形式またはサブセットである Web ページ・アドレス。

URL

Uniform Resource Locator（URL）。インターネット上でアクセス可能なファイルのアドレス。このファイルは、テキスト・ファイル、HTML ページ、イメージ・ファイル、プログラム、または HTTP によってサポートされているその他任意のファイルである。URL には、リソースにアクセスするために必要なプロトコル名、インターネット上の特定のコンピュータを識別するドメイン名、およびコンピュータ上のファイル・ロケーションの階層的記述が含まれる。

URLC トークン（URLC token）

認証ユーザー情報を**パートナ・アプリケーション**に渡す OracleAS Single Sign-On 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 を生成する。

UTF-16

Unicode の 16 ビットのエンコーディング。この規格の最初の 256 個のコード・ポイントは Latin-1 文字。

UTF-8

各文字について 1 ～ 4 バイトのバイト・シーケンスを使用する **Unicode** の、可変幅の 8 ビットのエンコーディング。0 ～ 127 の文字（7 ビットの ASCII 文字）は 1 バイトを使用してエンコードされ、128 ～ 2047 の文字は 2 バイト、2048 ～ 65535 の文字は 3 バイト、65535 を超える文字は 4 バイトを必要とする。これの Oracle キャラクタ・セット名は AL32UTF8（Unicode 3.1 規格）。

Wallet

個別エンティティのセキュリティ資格証明を格納および管理するための抽象概念。様々な暗号サービスで使用する資格証明の格納 / 取得先。Wallet Resource Locator（WRL）は、Wallet を検索するために必要なすべての情報を提供する。

Wallet Manager

「**Oracle Wallet Manager**」を参照。

Web サービス（Web Service）

HTTP、XML および SOAP などの標準インターネット・プロトコルを使用してアクセス可能なアプリケーションまたはビジネス・ロジック。コンポーネント・ベースの開発と World Wide Web の最も優れた部分を組み合せたもの。コンポーネントと同様、サービスの実装方法とは関係なく使用および再使用が可能なブラックボックス機能を提供する。

Web サービス記述言語（Web Services Description Language: WSDL）

XML を使用して Web サービスを記述するための標準形式。Web サービスへのアクセス方法と Web サービスが実行する処理内容を記述する。

WS-Federation

Web Services Federation（WS-Federation）言語は、Microsoft 社、IBM 社、BEA 社、VeriSign 社および RSA Security 社によって開発された仕様である。参加している Web サービス・プロバイダ間に識別情報、属性および認証に対する信頼関係を構築および仲介することにより、異種または同種のメカニズムを使用するエンティティ間のフェデレーションを実現するメカニズムを定義する。

関連項目：「リバティ・アライアンス」

WSDL

「Web サービス記述言語」を参照。

X.500

グローバル・ディレクトリの構成方法を定義する国際電気通信連合（ITU）の規格。X.500 ディレクトリは、情報のカテゴリごとに、国、州および市など、様々なレベルで階層化されている。

X.509

デジタル証明を定義するために最も広範に使用されている規格。認証サービスの階層ディレクトリに関する国際電気通信連合（ITU）の規格。多くの公開鍵インフラストラクチャ実装で使用される。

XML

Extensible Markup Language（XML）は、World Wide Web Consortium（W3C）によって開発された仕様。Web ドキュメント専用として設計された Standard Generalized Mark-Up（SGML）言語の軽量バージョン。開発者が多くのドキュメント・クラスに使用するマークアップ言語を独自にカスタマイズ定義するためのメタ言語（タグ・セットの定義方法）。

XML 正規化（XML Canonicalization: C14N）

論理的に同等の 2 つの XML ドキュメントを同じ物理表現として解決するプロセス。デジタル署名の場合、最初に処理されたデータと同じ物理表現を使用してのみ署名を検証できるため、このプロセスは重要性を持つ。詳細は、W3C の XML 正規化仕様を参照。

アカウント・ロックアウト（Account Lockout）

指定された時間内においてログイン試行が繰り返し失敗した場合、セキュリティ・ポリシー設定に基づいてユーザー・アカウントをロックするセキュリティ機能。OracleAS Single Sign-On では、ユーザーが Oracle Internet Directory で許可されている回数を超えて任意数のワークステーションからアカウントとパスワードの組合せを送信すると、アカウント・ロックアウトが発生する。デフォルトのロックアウト期間は 24 時間。

アクセス制御項目（Access Control Item: ACI）

アクセス制御情報は、様々なエンティティやサブジェクトがディレクトリ内の特定のオブジェクトに対する操作の実行用に持っている権限。この情報は、ユーザーが変更可能な操作属性として Oracle Internet Directory に格納される。この個々の操作属性がアクセス制御項目（ACI）と呼ばれる。ACI により、ディレクトリ・データに対するユーザーのアクセス権が決まる。ACI には、エントリ（構造アクセス項目）および属性（コンテンツ・アクセス項目）へのアクセスを制御するためのルール・セットが含まれる。1 人以上のユーザーまたは 1 つ以上のグループに対して、構造アクセス項目とコンテンツ・アクセス項目の両方へのアクセス権を付与できる。

アクセス制御ポリシー・ポイント（Access Control Policy Point: ACP）

ディレクトリ・エントリ。**ディレクトリ情報ツリー**内で、これより下位にあるすべてのエントリに対して、このディレクトリ・エントリのアクセス制御ポリシー情報が適用される。この情報は、エントリ自体とそれより下位にあるすべてのエントリに影響する。Oracle Internet Directory では、ACP を作成することにより、ディレクトリの**サブツリー**全体にわたってアクセス制御ポリシーを適用できる。

アクセス制御リスト（Access Control List: ACL）

コンピュータ・システム内のリソースに対するアクセスが許可されたユーザーのユーザー名とリソースのリスト。Oracle Internet Directory では、ディレクトリ・オブジェクトに関連付けられた**アクセス制御項目**の**属性値**のリスト。このリストの属性値は、様々なディレクトリ・ユーザー・エンティティ（サブジェクト）が特定のオブジェクトに対して持つ権限を示す。

アドバンスト対称型レプリケーション（Advanced Symmetric Replication: ASR）

「**Oracle Database アドバンスト・レプリケーション**」を参照。

アドバンスト・レプリケーション（Advanced Replication）

「**Oracle Database アドバンスト・レプリケーション**」を参照。

アプリケーション・サービス・プロバイダ（Application Service Provider）

アプリケーション・サービス・プロバイダ（ASP）は、広域ネットワークにわたるカスタマに対してセントラル・データ・センターからソフトウェア・ベースのサービスおよびソリューションを配布して管理するサード・パーティ企業。本質的には、他の企業が情報技術上のニーズの一部または大部分の側面をアウトソーシングするための手段。

暗号（Cipher）

「**暗号化アルゴリズム**」を参照。

暗号化（Cryptography）

情報を読取り不可能な形式に変換して保護するプロセス。情報は**鍵**を使用して暗号化され、データが読取り不可能になる。後で情報を再使用する必要が生じると、復号化される。「**公開鍵暗号化**」および「**対称型暗号化**」も参照。

暗号化（encryption）

暗号化アルゴリズムを適用して平文を暗号文に変換するプロセス。

暗号化アルゴリズム（Cryptographic Algorithm）

読取り可能データ（平文）を読取り不能データ（暗号文）に変換（またはこの逆）する一連のプロセスを定義したもの。このような変換を行うには、通常**鍵**に含まれている秘密の情報が必要となる。暗号化アルゴリズムの例として **DES**、**AES**、**Blowfish** および **RSA** がある。

暗号化証明書（Encryption Certificate）

電子メッセージ、ファイル、ドキュメントまたはデータ通信の暗号化、あるいは同じ目的のセッション鍵の構築または交換に使用する**公開鍵**を含む**証明書**。

暗号化メッセージ構文（Cryptographic Message Syntax: CMS）

デジタル・メッセージの署名、ダイジェスト、認証および暗号化を行うために **RFC** 3369 に定義されている構文。

暗号スイート（Cipher Suite）

Secure Sockets Layer では、ネットワーク・ノード間でメッセージを交換するための認証、暗号化およびデータ整合性アルゴリズムの組合せを示す。SSL ハンドシェイク時には、2 つのノードが交渉して、メッセージを交換するときに使用する暗号スイートを確認する。

暗号ブロック連鎖（Cipher Block Chaining: CBC）

ブロック暗号の操作モード。一定長の、いわゆる初期化ベクトル（IV）を使用する。その主な特徴の 1 つは、前のすべての暗号文ブロックに依存して暗号文のブロックを復号化する連鎖メカニズムが採用されていることである。このため、前のブロックすべての妥当性が直前の暗号文ブロックに含まれることになる。

暗号文（Ciphertext）

適切な**鍵**を所有するエンティティ以外のすべてのエンティティに対してデータを読取り不能にするために、読取り可能なデータ（平文）に**暗号化アルゴリズム**を適用したもの。

一方向関数（One-Way Function）

関数それ自身の計算は簡単だが、逆関数の計算、すなわち、逆方向の計算が非常に困難な関数。

一方向ハッシュ関数（One-Way Hash Function）

可変サイズの入力を使用し、固定サイズの出力を生成する**一方向関数**。

関連項目：「**ハッシュ関数**」

一致規則（Matching Rule）

検索または比較操作で、検索対象の属性値と格納されている属性値の等価性を判断するためのもの。たとえば、`telephoneNumber` 属性の一致規則では、「(650) 123-4567」を、「(650) 123-4567」と「6501234567」またはこれら両方と一致することができる。**属性**の作成時には、これに一致規則を関連付ける。

委任管理（Delegated Administrator）

ホストされる側の環境では、1 つの企業（アプリケーション・サービス・プロバイダなど）が、Oracle コンポーネントをその他の複数企業が使用できるようにし、これらの情報を保管する。このような環境では、グローバル管理者がディレクトリ全体にわたるアクティビティを実行する。委任管理者と呼ばれるその他の管理者は、特定の ID 管理レルムのロールや特定のアプリケーションのロールを実行できる。

委任管理サービス（Delegated Administration Services）

「**Oracle Delegated Administration Services**」を参照。

インスタンス（Instance）

「**ディレクトリ・サーバー・インスタンス**」を参照。

インフラストラクチャ層（Infrastructure Tier）

ID 管理を担当する各 Oracle Application Server コンポーネント。OracleAS Single Sign-On、Oracle Delegated Administration Services および Oracle Internet Directory がそのコンポーネントである。

インポート・エージェント（Import Agent）

Oracle Directory Integration Platform 環境で、データを Oracle Internet Directory にインポートするエージェント。

インポート・データファイル（Import Data File）

Oracle Directory Integration Platform 環境で、**インポート・エージェント**によってインポートされたデータが含まれるファイル。

エクスポート・エージェント（Export Agent）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory からデータをエクスポートするエージェント。

エクスポート・データファイル（Export Data File）

Oracle Directory Integration Platform 環境で、**エクスポート・エージェント**によってエクスポートされたデータが含まれるファイル。

エクスポート・ファイル（Export File）

「**エクスポート・データファイル**」を参照。

エンドツーエンド・セキュリティ（END-To-End Security）

ビジネス・エンティティ内またはビジネス・エンティティ間の複数のアプリケーションの全ルート上でセキュアであるメッセージ・レベル・セキュリティのプロパティ。このセキュリティは、メッセージがそのようなルートを横断するときに確保される。

エントリ（Entry）

個人などのオブジェクトを記述する、ディレクトリ内の一意のレコード。エントリ・オブジェクトを記述する**オブジェクト・クラス**によって規定される**属性**とその**属性値**で構成される。LDAP ディレクトリ構造内のすべてのエントリは、その**識別名**によって一意に識別される。

オブジェクト・クラス（object class）

LDAP で、情報をグループ化するために使用される。通常、個人やサーバーなど、現実世界のオブジェクトをモデリングする。各ディレクトリ・エントリは 1 つ以上のオブジェクト・クラスに属す。オブジェクト・クラスにより、エントリを構成する属性が決まる。1 つのオブジェクト・クラスは別のオブジェクト・クラスから導出できる。このため、その別のクラスのなんらかの特性を継承できる。

オンライン証明書ステータス・プロトコル（Online Certificate Status Protocol: OCSP）

デジタル証明の妥当性を確認する 2 つの一般的な方式のうちの 1 つ。もう 1 つは、旧型の方式である**証明書失効リスト**だが、これは様々な場面で OCSP に取って代わられた。OCSP は **RFC** 2560 に規定されている。

下位 CA（subordinate CA）

階層的な**公開鍵インフラストラクチャ**で、下位**認証局**は、証明書署名鍵が別の CA に承認され、アクティビティもその CA に制約される CA。

介在者（Man-In-The-Middle）

メッセージ不正傍受などのセキュリティ攻撃を行う第三者。この第三者、つまり介在者は、メッセージを復号化して再暗号化し（元のメッセージを変更する場合と変更しない場合がある）、元のメッセージの宛先である受信者に転送する。これらの処理はすべて、正当な送受信者が気付かないうちに行われる。この種のセキュリティ攻撃は、**認証**が行われていない場合にのみ発生する。

外部アプリケーション（External Application）

認証を OracleAS Single Sign-On Server に委任しないアプリケーション。かわりに、HTML ログイン・フォームを表示し、アプリケーションのユーザー名とパスワードを要求する。ユーザーは、初回のログイン時に、OracleAS Single Sign-On Server に資格証明を取得させるかどうかを選択できる。以後、ユーザーはこれらのアプリケーションに透過的にログインする。

外部エージェント（External Agent）

Oracle Directory Integration Platform Server とは無関係のディレクトリ統合エージェント。Oracle Directory Integration Platform Server は、このエージェントに対してスケジューリング、マッピングまたはエラー処理サービスは提供しない。通常、サード・パーティのメタディレクトリ・ソリューションが Oracle Directory Integration Platform と統合されたときに使用される。

鍵（key）

特定のデータ・ブロックを正常に暗号化または復号化するために必要となる秘密の情報が含まれるデータ構造。鍵を長くするほど、暗号化されたデータ・ブロックを解読するのが困難になる。たとえば、256 ビットの鍵の方が 128 ビットの鍵よりセキュアである。

鍵のペア（Key Pair）

公開鍵および対応する**秘密鍵**。

関連項目：「**公開鍵と秘密鍵のペア**」

拡張暗号化規格（Advanced Encryption Standard: AES）

データ暗号化規格の後継。**対称型暗号化**アルゴリズム。商業データと行政データを暗号化するための米国連邦情報処理標準（FIPS）。

仮想 IP アドレス（Virtual IP Address）

Oracle Application Server Cold Failover Cluster（Identity Management）では、各物理ノードは、独自の物理 IP アドレスと物理ホスト名を持つ。クラスタは、クラスタ内の任意の物理ノードに移動可能な動的 IP アドレスを使用することで、外部世界にシステム・イメージが単一であるように提示する。これは仮想 IP アドレスと呼ばれる。

仮想ホスト（virtual host）

1 つ以上の Web サイトまたはドメインをホストしている単一の物理的な Web サーバー・マシン、またはその他のマシンのプロキシとして動作しているサーバー（受信リクエストを受け入れ、これらを適切なサーバーにあらためてルーティングするサーバー）。

OracleAS Single Sign-On の場合、複数の OracleAS Single Sign-On Server 間のロード・バランシング用として使用される。また、追加のセキュリティ・レイヤーも提供する。

仮想ホスト名（Virtual Host Name）

Oracle Application Server Cold Failover Cluster（Identity Management）で、特定の仮想 IP アドレスに対応するホスト名。

簡易認証（Simple Authentication）

クライアントが、暗号化していない DN およびパスワードをネットワーク上で送信して、サーバーから認証を受けるプロセス。サーバーは、クライアントによって送信された DN およびパスワードを、ディレクトリに格納されている DN およびパスワードと照合する。

管理領域（Administrative Area）

ディレクトリ・サーバー上の**サブツリー**。このサブツリー内のすべてのエントリが、1 人の管理者によって制御されている。指定された管理者が管理領域内の各**エントリ**、およびこれらのエントリのディレクトリ・**スキーマ**、**アクセス制御リスト**、**属性**を制御する。

基本エンコーディング・ルール（Basic Encoding Rules: BER）

ASN.1 に定義されているデータ単位をエンコーディングするための標準ルール。ASN.1 と誤って対にされることがあるが、ASN.1 はエンコーディング技術ではなく抽象構文記述言語にのみ適用されるものである。

機密保護（Confidentiality）

暗号化で、不正なエンティティによるデータの読取りを阻止する機能。プライバシとも呼ばれる。通常、**暗号化**を介して実現される。

キャッシュ（Cache）

通常、コンピュータ内で高速アクセスが可能なメモリー量を指す。しかし、Web 関連では、ブラウザがダウンロードしたファイルとグラフィックを格納するユーザーのコンピュータ上の場所を指すことが多い。

競合（Contention）

リソースの競合。

強制認証（Forced Authentication）

ユーザーが一定時間アイドル状態だった場合に再認証するよう強制すること。Oracle Application Server Single Sign-On では、グローバル・ユーザーの非アクティブのタイムアウトを指定できる。この機能は、機密事項を扱うアプリケーションがあるシステムで使用される。

兄弟関係（Sibling）

他の 1 つ以上のエントリと同じ親を持つエントリ。

協定世界時（Coordinated Universal Time: UTC）

世界中のあらゆる場所に共通する標準時。かつて、そして現在でも広く、グリニッジ標準時（GMT）と呼ばれるとともに世界時とも呼ばれる UTC は、地球の子午線に沿った平均太陽時の代名詞である。200011281010z のように、値の最後に z があることによって UTC であることが示される。

共有サーバー（Shared Server）

サポート可能なユーザー数を増やすために、多くのユーザー・プロセスがわずかなサーバー・プロセスを共有できるよう構成されたサーバー。共有サーバー構成を使用して、多くのユーザー・プロセスがディスパッチャに接続する。ディスパッチャは、受信した複数のネットワーク・セッション・リクエストを一般キューに転送する。このキューから、サーバー・プロセスの共有プールにあるアイドル状態の共有サーバー・プロセスがリクエストを取得する。これにより、小さいサーバー・プロセス・プールが多数のクライアントにサービスを提供できるようになる。専用サーバーと対照のこと。

クライアント SSL 証明書（Client SSL Certificates）

Secure Sockets Layer を介してサーバーにクライアント・マシンを認証（クライアント認証）させるための**証明書**の 1 タイプ。

クラスタ（Cluster）

インターコネクトされた使用可能なコンピュータのコレクション。単一のコンピューティング資源として使用される。ハードウェア・クラスタにより、高可用性と高スケーラビリティが実現される。

グループ検索ベース（Group Search Base）

Oracle Internet Directory のデフォルトの**ディレクトリ情報ツリー**において、すべてのグループを検索できる ID 管理レルム内のノード。

グローバリゼーション・サポート（Globalization Support）

グラフィカル・ユーザー・インタフェース用の多言語サポート。Oracle Application Server Single Sign-On は、29 の言語をサポートしている。

グローバル管理者（Global Administrator）

ホストされる側の環境では、1 つの企業（アプリケーション・サービス・プロバイダなど）が、Oracle コンポーネントをその他の複数企業が使用できるようにし、これらの情報を保管する。このような環境では、グローバル管理者がディレクトリ全体にわたるアクティビティを実行する。

グローバルに一意のユーザー ID（globally unique user ID）

ユーザーを一意に識別する数値文字列。個人はユーザー名、パスワードおよび識別名を変更または追加できるが、グローバルに一意のユーザー ID は常に不変。

グローバル・ユーザーの非アクティブのタイムアウト（Global User Inactivity Timeout）

ユーザーが事前設定された時間アイドル状態だった場合に再認証するよう強制する Oracle Application Server Single Sign-On のオプションの機能。シングル・サインアウト・セッションのタイムアウトよりも時間が短い。

継承（Inherit）

別のクラスから導出された**オブジェクト・クラス**が多くの特性もそのクラスから導出すること。同様に、属性のサブタイプはそのスーパータイプを継承する。

ゲスト・ユーザー（Guest User）

匿名ユーザーではないと同時に、特定のユーザー・エントリを持たないユーザー。

検証（verification）

署名と署名が適用されたと主張するデータ・ブロックを作成したと主張する**秘密鍵**に、対応する**公開鍵**が与えられたときに、特定の**デジタル署名**が有効であるかどうかを確認するプロセス。

コード署名証明書（Code Signing Certificates）

Java プログラム、Java スクリプトまたはその他の署名ファイルに署名したエンティティを識別するための**証明書**の 1 タイプ。

コールド・バックアップ（Cold Backup）

Oracle Internet Directory で、データベース・コピー手順を使用して新しい**ディレクトリ・システム・エージェント**ノードを既存のレプリケーション・システムに追加する手順。

公開鍵（public key）

公開鍵暗号化で使用される**公開鍵と秘密鍵のペア**のうち、秘密鍵ではない方の鍵。公開鍵を使用することにより、公開鍵の所有者が**秘密鍵**を使用したときにのみ復号化できる暗号データを、エンティティは作成できる。また、公開鍵を使用して、対応する秘密鍵で作成されたデジタル署名を検証することもできる。

公開鍵暗号化（Public Key Cryptography）

公開鍵暗号化（非対称型暗号化とも呼ばれる）では、公開鍵と秘密鍵という 2 つの鍵が使用される。これらの鍵は鍵のペアと呼ばれる。秘密鍵は秘密にしておく必要があるが、公開鍵は任意のユーザーに送信できる。秘密鍵と公開鍵は数学的に関連している。秘密鍵で署名されたメッセージは、対応する公開鍵を使用して検証できる。同様に、公開鍵で暗号化されたメッセージは、秘密鍵を使用して復号化できる。この方法の場合、メッセージを復号化できるのは秘密鍵の所有者のみであるため、プライバシが保証される。

公開鍵暗号化（Public Key Encryption）

メッセージの送信者が受信者の公開鍵を使用してメッセージを暗号化するプロセス。送信後、メッセージは受信者の秘密鍵を使用して復号化される。

公開鍵インフラストラクチャ（Public Key Infrastructure: PKI）

公開鍵と**秘密鍵**の発行、配布および認証を管理するシステム。通常、次のコンポーネントで構成される。

- **認証局**：デジタル証明を生成、発行、公開および失効する役割を果す。
- **登録局**：CA に対する証明書リクエストに指定されている情報を検証する役割を果す。
- ディレクトリ・サービス：CA が**証明書**または**証明書失効リスト**を公開し、公開された証明書を信頼したサード・パーティが証明書を取得する場所。
- 証明書を信頼するサード・パーティ：CA が発行した証明書とその中に含まれる**公開鍵**を使用し、**デジタル署名**の検証およびデータの暗号化を行う。

公開鍵証明書（Public Key Certificate）

「**証明書**」を参照。

公開鍵と秘密鍵のペア（Public/Private Key Pair）

数学的に関連している 2 つの数値のセットで、1 つは秘密鍵、もう 1 つは公開鍵と呼ばれる。通常、公開鍵は一般的に使用可能な鍵として作成されるが、秘密鍵はその所有者のみが使用可能な鍵として作成される。公開鍵を使用して暗号化されたデータは、関連する秘密鍵を使用してのみ復号化できる（また、この逆も成り立つ）。公開鍵を使用して暗号化されたデータは、同じ公開鍵を使用しても復号化できない。

構成設定エントリ（Configuration Set Entry）

ディレクトリ・サーバーの特定のインスタンスの構成パラメータを保持する Oracle Internet Directory のエントリ。実行時には複数の構成設定エントリを保存および参照できる。構成設定エントリは、**ディレクトリ固有エントリ**の `subConfigsubEntry` 属性によって指定されたサブツリーに設定される。DSE 自体は、サーバーの起動に使用された**ディレクトリ情報ベース**に格納されている。

コンシューマ（Consumer）

レプリケーションの更新先となるディレクトリ・サーバー。スレーブと呼ばれることもある。

コンテキスト接頭辞（Context Prefix）

ネーミング・コンテキストのルートの**識別名**。

サード・パーティ・アクセス管理システム（Third-Party Access Management System）

Oracle Application Server アプリケーションにアクセスするために OracleAS Single Sign-On を使用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。

サーバーの証明書（server certificate）

セキュアな Web サーバーを使用してデータを提供する組織の識別情報を証明する**証明書**。サーバー証明書は、相互信頼関係にある**認証局**から発行されている**公開鍵と秘密鍵のペア**と関連付ける必要がある。サーバー証明書は、ブラウザと Web サーバー間のセキュアな通信を行う上で必要となる。

サービス時間（Service Time）

リクエストの開始からリクエストへのレスポンスの完了までの時間。

サービス・プロバイダ（Service Provider）

Web ベースのサービスをユーザーに提供するエンティティとして**トラスト・サークル**のメンバーから認められた組織。サービス・プロバイダは、**フェデレーション**のすべてのエンティティによって一般ユーザーがセキュアなシングル・サインオンを使用できる環境を実現することを目的として、その他のサービス・プロバイダおよび識別情報プロバイダと提携している。

サブエントリ（Subentry）

サブツリー内のエントリ・グループに適用可能な情報が格納されている、一種のエントリ。この情報には次の種類がある。

- アクセス制御ポリシー・ポイント
- スキーマ・ルール
- 共通属性

サブエントリは、管理領域のルートの直下に置かれる。

サブクラス（Subclass）

別のオブジェクト・クラスから導出されたオブジェクト・クラス。導出元のオブジェクト・クラスは**スーパークラス**と呼ばれる。

サブスキーマ DN（Subschema DN）

独立した**スキーマ**定義を持つ**ディレクトリ情報ツリー**領域のリスト。

サブタイプ（Subtype）

1 つ以上のオプションがある属性は、オプションがない同じ属性のサブタイプである、という。たとえば、オプションとして American English を持つ commonName（cn）属性は、このオプションがない commonName（cn）属性のサブタイプ。逆に、オプションがない commonName（cn）属性は、オプションがある同じ属性の**スーパータイプ**。

サブツリー（Subtree）

ディレクトリ階層のセクションで、**ディレクトリ情報ツリー**とも呼ばれる。通常、特定のディレクトリ・ノードから始まり、ディレクトリ階層内でこのノードより下位にあるすべてのサブディレクトリおよびオブジェクトが含まれる。

サプライヤ（Supplier）

レプリケーションで、**ネーミング・コンテキスト**のマスター・コピーを保持するサーバー。マスター・コピーの更新を**コンシューマ**・サーバーに提供する。

参照（Referral）

ディレクトリ・サーバーがクライアントに提供する情報で、クライアントがリクエストする情報を検索するためにコンタクトする必要があるその他のサーバーを指し示す。

関連項目：「**ナレッジ参照**」

識別エンコーディング・ルール（Distinguished Encoding Rules: DER）

バイト・シーケンスの **ASN.1** オブジェクトをエンコードするためのルール・セット。**基本エンコーディング・ルール**の特殊ケース。

識別情報プロバイダ（Identity Provider）

ユーザーを認証し、ユーザーのデジタル識別情報を**フェデレーション**内の他のエンティティに提供する役割を果すエンティティとして、**トラスト・サークル**のメンバーから認められた組織。サービス・プロバイダと提携し、フェデレーション内のすべてのエンティティによって策定された合意済手順に準拠したサービスを提供する。

識別名（distinguished name: DN）

X.500 の識別名（DN）は、ディレクトリ・ツリーのノードの一意名を示す。個人またはその他のディレクトリ・エントリの一意名を示すために使用される。DN は、ツリー内でルート・ノードから特定のエントリ・ノードまでのすべてのノードから選択された**属性**を連結したものである。たとえば、LDAP の表記法では、オラクル社の米国オフィスで働く John Smith という名前の社員は「cn=John Smith, ou=People, o=Oracle, c=us」となる。

思考時間（Think Time）

ユーザーがプロセッサを実際に使用していない時間。

システム・グローバル領域（System Global Area: SGA）

1 つの Oracle データベース・インスタンスのデータおよび制御情報が含まれる共有メモリー構造のグループ。複数のユーザーが同じインスタンスに同時に接続する場合、インスタンスの SGA のデータはユーザー間で共有される。このため、SGA は共有グローバル領域と呼ばれることもある。バックグラウンド・プロセスとメモリー・バッファの組合せが Oracle インスタンスと呼ばれる。

システム操作属性（System Operational Attribute）

ディレクトリ自体の操作に関する情報を保持する属性。サーバーを制御するための一部の操作情報（エントリのタイムスタンプなど）は、ディレクトリによって指定される。その他の操作情報（アクセス情報など）は、管理者によって定義され、ディレクトリ・プログラムによってその処理中に使用される。

従属参照（Subordinate Reference）

ディレクトリ情報ツリーでエントリの直下から始まって下方向に向く**ネーミング・コンテキスト**を指し示す**ナレッジ参照**。

上位参照（Superior Reference）

ディレクトリ情報ツリーにおいて、参照元の DSA が保持するすべてのネーミング・コンテキストより上位のネーミング・コンテキストを保持する**ディレクトリ・システム・エージェント**を指し示す**ナレッジ参照**。

条件（predicates）

Oracle Application Server Certificate Authority（OCA）で、受信証明書リクエストまたは失効に対するポリシーの適用方法を制限するためにポリシーに適用できる論理式。たとえば、次の条件式では、「ou=sales,o=acme,c=us」を含む DN を持つクライアントからのリクエストまたは失効に対して、異なる処理を行うように指定できる。

```
Type=="client" AND DN=="ou=sales,o=acme,c=us"
```

証明書（certificate）

公開鍵をその所有者の識別情報と関連付けるために特別にフォーマットされたデータ構造。**認証局**によって発行される。特定エンティティの名前、シリアル番号、有効期限および公開鍵が含まれる。受信者が、証明書が本物であることを検証できるように、発行元の CA によってデジタル署名されている。大部分のデジタル証明書は **X.509** 規格に準拠している。

証明書失効リスト（Certificate Revocation List: CRL）

発行元の**認証局**によって失効されたデジタル**証明書**のリスト。

証明書リクエスト・メッセージ・フォーマット（Certificate Request Message Format: CRMF）

X.509 証明書のライフ・サイクル管理に関連するメッセージに使用されるフォーマット（**RFC** 2511 の仕様を参照）。

証明連鎖（Certificate Chain）

1 人以上のユーザーの**証明書**とその関連する **CA 証明書**が含まれる証明書が順序付けられたリスト。

シングル・サインオフ（Single Sign-Off）

OracleAS Single Sign-On 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。これを行うには、現在操作しているアプリケーションからログアウトするのみでよい。

シングル・サインオン（Single Sign-On: SSO）

ユーザーが認証を 1 回行うのみで複数のコンピュータ・プラットフォームまたはアプリケーション・システムにアクセスできるプロセスまたはシステム。

シングル・サインオン SDK（Single Sign-On SDK）

OracleAS Single Sign-On パートナ・アプリケーションがシングル・サインオンできるようにするためのレガシー API。PL/SQL API、Java API、およびこれらの API の実装方法を示すサンプル・コードで構成される。ただし、現在では使用不可であり、**mod_osso** がかわりに使用されている。

申請（Claim）

エンティティによる宣言（名前、識別情報、鍵、グループなど）。

信頼できる証明書（trusted certificate）

必要な信頼レベルを備えたサード・パーティの識別情報。この信頼は、識別情報が申請しているエンティティのものと一致するかどうかを検証するときに使用される。通常、信頼できる証明書は、ユーザー証明書の発行元として信頼している**認証局**のものである。

信頼ポイント（trustpoint）

「**信頼できる証明書**」を参照。

スーパークラス（Superclass）

別のオブジェクト・クラスの導出元の**オブジェクト・クラス**。たとえば、オブジェクト・クラス `person` は、オブジェクト・クラス `organizationalPerson` のスーパークラス。後者の `organizationalPerson` は、`person` の**サブクラス**であり、`person` に含まれる属性を継承する。

スーパータイプ（Supertype）

オプションがない属性は、1 つ以上のオプションがある同じ属性のスーパータイプである、という。たとえば、オプションがない `commonName`（`cn`）属性は、オプションがある同じ属性のスーパータイプ。逆に、オプションとして American English を持つ `commonName`（`cn`）属性は、このオプションがない `commonName`（`cn`）属性の**サブタイプ**。

スーパーユーザー（Super User）

ディレクトリ情報へのフルアクセス権を通常持っている特別なディレクトリ管理者。

スキーマ（Schema）

属性、**オブジェクト・クラス**およびこれらに対応する**一致規則**のコレクション。

スケーラビリティ（scalability）

システムのスループットを、使用可能なハードウェア・リソースによって増減できることを指す。

ストリーム暗号（Stream Cipher）

対称型アルゴリズムの 1 タイプ。小単位（通常は 1 ビットまたは 1 バイトずつ）で暗号化し、なんらかの形のフィードバック・メカニズムを実装することにより、鍵が常に変更されるようにする。**RC4** はその 1 例。

関連項目：「**ブロック暗号**」

スポンサ・ノード（Sponsor Node）

レプリケーションで、新しいノードに初期データを提供するノード。

スマート・ナレッジ参照（Smart Knowledge Reference）

ナレッジ参照エントリが検索範囲内に含まれているときにのみ戻される**ナレッジ参照**。リクエストした情報が格納されているサーバーをユーザーに指し示す。

スループット（Throughput）

時間単位当たり Oracle Internet Directory によって処理されたリクエスト数。通常、毎秒の操作数として表される。

スレーブ（Slave）

「**コンシューマ**」を参照。

成功 URL（Success URL）

Oracle Application Server Single Sign-On の使用時に、アプリケーションのセッションおよびセッション Cookie を確立する機能を持つルーチンの URL。

整合性（integrity）

暗号化において、データを変更する権限のないエンティティによってデータが変更されたことを検出する機能。

セッション鍵（Session Key）

1 つのメッセージ / 通信セッションの間に使用される**秘密鍵**。

接続記述子（Connect Descriptor）

ネットワーク接続先を特別なフォーマットで記述したもの。接続先サービスとネットワーク・ルート情報が含まれる。

接続先サービスは、Oracle Database のサービス名や、Oracle のリリース 8.0 またはバージョン 7 のデータベース用の Oracle システム識別子（SID）を使用して指定する。ネットワーク・ルートは、ネットワーク・アドレスを使用して、少なくともリスナーのロケーションを示す。

接続ディレクトリ（Connected Directory）

Oracle Directory Integration Platform 環境で、Oracle Application Server Certificate Authority との完全な同期化を必要とする情報リポジトリ（例 : Oracle Human Resources データベース）。

セントラル・ディレクトリ（Central Directory）

Oracle Directory Integration Platform 環境で、セントラル・リポジトリとして機能するディレクトリ。Oracle Directory Integration Platform 環境では、Oracle Internet Directory がセントラル・ディレクトリである。

相対識別名（Relative Distinguished Name: RDN）

最も詳細なローカル・エントリ名。エントリを一意に指定するための修飾をすべて取り除いて残るもの。たとえば、`cn=Smith,o=acme,c=US` の場合、RDN は `cn=Smith` である。

属性（Attribute）

ディレクトリ属性は、名前、電話番号または職種など、特定のデータ要素を持つ。各ディレクトリ・**エントリ**は一連の属性で構成され、各属性は**オブジェクト・クラス**に属す。また、各属性は、属性の情報の種類を示すタイプと、実際のデータが含まれる値を持つ。

属性構成ファイル（Attribute Configuration File）

Oracle Directory Integration Platform 環境において、接続ディレクトリの特定の属性を指定するファイル。

属性タイプ（Attribute Type）

データ型、最大長、単一値または多値のどちらかなど、データ要素に関する情報を指定する。値に対して現実世界での意味を付与し、名前や電子メール・アドレスなどの特定のデータを作成および保存するためのルールを規定する。

属性値（Attribute Value）

特定の**エントリ**の**属性**に含まれる実際のデータ。たとえば、属性タイプ `email` の値は `sally.jones@oracle.com`。

属性の一意性（Attribute Uniqueness）

2 つの**属性**が同じ値を持たないようにするための Oracle Internet Directory の機能。これにより、企業ディレクトリと同期化するアプリケーションが属性を一意のキーとして使用できるようになる。

その他の情報リポジトリ（Other Information Repository）

Oracle Internet Directory が**セントラル・ディレクトリ**として機能する Oracle Directory Integration Platform 環境で、Oracle Internet Directory を除くすべての情報リポジトリ。

待機時間（Latency）

特定のディレクトリ操作が完了するまでクライアントが待機する必要がある時間。浪費された時間として定義できる。ネットワーキングでは、パケットがソースから宛先まで移動する時間として定義される。

待機時間（Wait Time）

リクエストの送信からレスポンスの開始までの時間。

ダイジェスト（Digest）

「**メッセージ・ダイジェスト**」を参照。

対称鍵（Symmetric Key）

「**秘密鍵**」を参照。

対称型アルゴリズム（Symmetric Algorithm）

暗号化と復号化で同じ鍵を使用する暗号化アルゴリズム。基本的に、**ストリーム暗号**と**ブロック暗号**の 2 タイプの対称型（または秘密鍵）アルゴリズムがある。

対称型暗号化（Symmetric Cryptography）

対称型暗号化（または共有秘密暗号化）システムでは、同じ鍵を使用してデータを暗号化および復号化する。対称型暗号化上の問題は、送信者と受信者が秘密鍵について合意できるセキュアな方式を確保することにある。第三者が送信中の秘密鍵を傍受した場合、この第三者は、この秘密鍵を使用して暗号化されたすべての情報を、この秘密鍵を使用して復号化できる。通常、対称型暗号化は非対称型暗号化よりも処理が高速で、多くの場合、大量のデータを交換する必要があるときに使用される。対称型暗号化アルゴリズムの例には、**DES**、**RC2** および **RC4** がある。

タイムスタンプ・プロトコル（Time Stamp Protocol: TSP）

RFC 3161 に規定されているとおり、デジタル・メッセージのタイムスタンプ発行に関わる参加エンティティ、メッセージ形式および転送プロトコルを定義する。TSP システムでは、信頼できるサード・パーティのタイムスタンプ局（TSA）がメッセージのタイムスタンプを発行する。

楕円曲線暗号（Elliptic Curve Cryptography: ECC）

巨大整数の素因数分解にでなく楕円曲線の離散対数問題の解決の困難さに基づいた、**RSA** 暗号化システムの代替システム。ECC は、Certicom によって開発および販売され、計算能力が限られていながら高速な処理が求められるモバイル機器や PC カードなどの環境に特に適している。ECC は、任意の鍵のサイズ（ビット単位）に対して RSA より強固なセキュリティを提供する（鍵なしでの復号化がより困難）。

楕円曲線デジタル署名アルゴリズム（Elliptic Curve Digital Signature Algorithm: ECDSA）

楕円曲線の**デジタル署名アルゴリズム**規格版。RSA 方式と比較した場合、ECDSA には、鍵の長さが短くなり、署名と復号化が高速になるという利点がある。たとえば、160（210）ビットの ECC 鍵は、1024（2048）ビットの RSA 鍵と同じセキュリティを実現できると考えられており、セキュリティのレベルを上げようとするほど利点が大きくなる。

多分岐レプリケーション（Fan-Out Replication）

サプライヤがコンシューマに直接レプリケートする、レプリケーションの 1 タイプ。Point-to-Point レプリケーションとも呼ばれる。この後、このコンシューマは、他の 1 つ以上のコンシューマにレプリケートできる。その際は、完全レプリケーションと部分的レプリケーションのいずれでも可。

単一鍵ペア Wallet（Single Key-Pair Wallet）

単一ユーザーの**証明書**および関連する**秘密鍵**が含まれる **PKCS#12** 形式の Wallet。**公開鍵**は証明書に埋め込まれている。

中間層（Middle Tier）

Oracle HTTP Server と OC4J で構成される OracleAS Single Sign-On インスタンスの一部。OracleAS Single Sign-On の中間層は、ID 管理インフラストラクチャ・データベースとクライアントの中間にある。

データ暗号化規格（Data Encryption Standard: DES）

1974 年に IBM によって開発され、広範に使用されている**対称型暗号化**アルゴリズム。64 ビットの各データ・ブロックに対して 56 ビットの鍵を適用する。通常、DES と 3DES が **S/MIME** によって暗号化アルゴリズムとして使用される。

データ整合性（data integrity）

受信したメッセージの内容が送信された元のメッセージの内容から変更されていないことの保証。

関連項目：「**整合性**」

データベース・アクセス記述子（Database Access Descriptor: DAD）

OracleAS Single Sign-On スキーマなど、特定の Oracle Application Server コンポーネントに関するデータベース接続情報。

ディレクトリ（directory）

「Oracle Internet Directory」、「Lightweight Directory Access Protocol」および「X.500」を参照。

ディレクトリ固有エントリ（Directory-Specific Entry: DSE）

ディレクトリ・サーバーに固有のエントリ。複数のディレクトリ・サーバーは、同一のディレクトリ情報ツリー名を持ちながら異なる内容を持つことができる。したがって、内容は、その内容を収容するディレクトリに固有にできる。DSE は、内容収容先のディレクトリ・サーバーに固有の内容を持っているエントリである。

ディレクトリ・サーバー・インスタンス（Directory Server Instance）

起動された個々のディレクトリ・サーバー。同じまたは異なる構成設定エントリおよび起動フラグを使用してディレクトリ・サーバーを複数個起動した場合、これらは異なるディレクトリ・サーバー・インスタンスとみなされる。

ディレクトリ・システム・エージェント（Directory System Agent: DSA）

ディレクトリ・サーバーを意味する X.500 用語。

ディレクトリ情報ツリー（Directory Information Tree: DIT）

各エントリの DN で構成された階層ツリー型構造。

ディレクトリ情報ベース（Directory Information Base: DIB）

ディレクトリに格納されているすべての情報の完全なセット。ディレクトリ情報ツリー内で相互に階層的に関連付けられているエントリで構成される。

ディレクトリ同期プロファイル（Directory Synchronization Profile）

Oracle Internet Directory と外部システムを同期する方法を記述する特殊なディレクトリ統合プロファイル。

ディレクトリ統合サーバー（Directory Integration server）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory と接続ディレクトリ間でデータを同期化するサーバー。

ディレクトリ統合プロファイル（Directory Integration Profile）

Oracle Directory Integration Platform 環境で、Oracle Directory Integration Platform による外部システムとの通信方法とその通信内容が記述された Oracle Internet Directory 内のエントリ。

ディレクトリ・ネーミング・コンテキスト（Directory Naming Context）

「ネーミング・コンテキスト」を参照。

ディレクトリ・プロビジョニング・プロファイル（Directory Provisioning Profile）

Oracle Directory Integration Platform がディレクトリ対応アプリケーションに送信するプロビジョニング関連の通知の性質が記述された特殊なディレクトリ統合プロファイル。

ディレクトリ・ユーザー・エージェント（Directory User Agent: DUA）

ディレクトリ・ユーザーのかわりにディレクトリ・サービスにアクセスするソフトウェア。ディレクトリ・ユーザーは個人である場合や別のソフトウェア要素である場合がある。

ディレクトリ・レプリケーション・グループ（Directory Replication Group: DRG）

レプリケーション承諾に参加している複数のディレクトリ・サーバー。

デジタル証明（Digital Certificate）

「証明書」を参照。

デジタル署名（digital signature）

デジタル署名は、特定のデータ・ブロックに次の 2 ステップ・プロセスを適用した結果である。最初に、データに**ハッシュ関数**を適用して結果を取得する。次に、署名者の**秘密鍵**を使用してこの結果を暗号化する。デジタル署名により、整合性、メッセージ認証およびデータ否認防止が実現される。デジタル署名アルゴリズムの例には、**DSA**、**RSA** および **ECDSA** がある。

デジタル署名アルゴリズム（Digital Signature Algorithm: DSA）

デジタル署名標準（DSS）の一部として使用される**非対称型アルゴリズム**。暗号化用としては使用できず、デジタル署名用としてのみ使用可能。署名者を認証するために大きな数を 1 組生成することにより、添付データの整合性を実現する。DSA は、デジタル署名の生成と検証の両方で使用される。

関連項目：「**楕円曲線デジタル署名アルゴリズム**」

デフォルト ID 管理レルム（Default Identity Management Realm）

ホストされる側の環境では、1 つの企業（アプリケーション・サービス・プロバイダなど）が、Oracle コンポーネントをその他の複数企業が使用できるようにし、これらの情報を保管する。このようなホストされる側の環境では、ホスト側企業はデフォルト ID 管理レルムと呼ばれ、ホストされる側の各企業は**ディレクトリ情報ツリー**で自分の ID 管理レルムと関連付けられる。

デフォルト・ナレッジ参照（Default Knowledge Reference）

ベース・オブジェクトがディレクトリ内になく、操作がローカルに保存されていない**ネーミング・コンテキスト**でサーバーによって実行されるときに返される**ナレッジ参照**。デフォルト・ナレッジ参照により、通常、ユーザーは、ディレクトリのパーティション配置に関してより多くのナレッジを持つサーバーに送信される。

デフォルト・レルムの場所（Default Realm Location）

デフォルト ID 管理レルムのルートを識別する**ルート Oracle コンテキスト**の属性。

同時クライアント（Concurrent Clients）

Oracle Internet Directory とのセッションを確立したクライアントの合計数。

同時実行性（Concurrency）

複数のリクエストを同時に処理する機能。同時実行性メカニズムの例としてマルチスレッドとマルチプロセスがあげられる。

同時操作（Concurrent Operations）

すべての**同時クライアント**によって Oracle Internet Directory 上で実行されている操作の数。一部のクライアントのセッションはアイドル状態である可能性があるため、この数は必ずしも同時クライアントの数と同じであるとはかぎらない。

登録局（Registration Authority: RA）

証明書が**認証局**によって発行される前に、ユーザーを検証および登録する役割を果す。新しく申請された証明書に対して、各申請者に相対識別値または相対識別名を割り当てることができる。証明書の署名や発行は行わない。

特定管理領域（Specific Administrative Area）

各管理領域は次を制御する。

- サブスキーマ管理
- アクセス制御管理
- 共通属性管理

これらの管理面の 1 つを制御する。特定管理領域は自律型管理領域の一部である。

匿名認証（Anonymous Authentication）

ユーザー名とパスワードの組合せを必要とせずにディレクトリがユーザーを認証するプロセス。この場合、匿名ユーザーはすべて匿名ユーザー用に指定されている権限を実行する。

ドメイン・コンポーネント属性（Domain Component Attribute）

ドメイン・コンポーネント（dc）属性は、ドメイン名から**識別名**を構築するときに使用できる。たとえば、「oracle.com」などのドメイン名を使用して「dc=oracle, dc=com」から始まる DN を作成し、次に、この DN を、ディレクトリ情報のサブツリーのルートとして使用できる。

トラスト・サークル（Circle Of Trust）

リバティ・アライアンスのアーキテクチャおよび業務契約に基づくビジネス関係を持つ**サービス・プロバイダ**と**識別情報プロバイダ**の**フェデレーション**。これにより、ユーザーはセキュアで外観上シームレスな環境でビジネスを行うことができる。

トリプル・データ暗号化規格（Triple Data Encryption Standard: 3DES）

1974 年に IBM が開発した**データ暗号化規格**アルゴリズムに基づいており、1977 年に国家規格として採用された。64 ビット長の鍵を 3 つ使用する（全体的な鍵の長さは 192 ビットだが、実際の鍵の長さは 56 ビット）。データは最初の鍵を使用して暗号化され、2 つ目の鍵を使用して復号化され、最後に 3 つ目の鍵を使用して再度暗号化される。このため、3DES は標準的な DES よりも 3 倍遅くなるが、3 倍セキュアになる。

ナレッジ参照（Knowledge Reference）

リモート・**ディレクトリ・システム・エージェント**のアクセス情報（名前およびアドレス）と、リモート DSA が保持する**ディレクトリ情報ツリー**のサブツリーの名前。参照とも呼ばれる。

ニックネーム属性（Nickname Attribute）

ディレクトリ全体でユーザーを一意に識別するための属性。デフォルト値は `uid`。アプリケーションはこの属性を使用して、単純なユーザー名を完全な識別名として解決する。ユーザーのニックネーム属性は多値にはできない。つまり、1 人のユーザーが同じニックネーム属性名の下に複数のニックネームを持つことはできない。

認可（Authorization）

サービスまたはネットワーク・リソースに対するアクセス権を付与または拒否するプロセス。大部分のセキュリティ・システムは、2 ステップのプロセスに基づく。第 1 ステップでは、ユーザーが自分の識別情報を証明する認証を行う。第 2 ステップでは、認可を行う。これにより、ユーザーは、自分の識別情報および定義されている**認可ポリシー**に基づいて様々なリソースへのアクセスを許可される。

認可ポリシー（Authorization Policy）

保護されているリソースへのアクセスの制御方法を記述したもの。システム・モデルに基づいて識別情報とオブジェクトを権限コレクションにマップする。たとえば、ユーザーが販売レポートにアクセスできるのはユーザーが販売グループに属している場合のみであることが記述された認可ポリシーなどがある。

認証（authentication）

エンティティから申告された識別情報をエンティティの資格証明に基づいて検証するプロセス。通常、ユーザーの認証は、ユーザーが把握または所有しているもの（パスワードや証明書など）に基づいて行われる。

電子メッセージの認証では、ある種のシステム（**公開鍵暗号化**など）を使用して、ファイルまたはメッセージが特定の個人または会社からのものであるという申告が正しいかどうかを確認し、転送中に変更されていないかどうかをメッセージの内容に基づいてチェックする。

認証管理プロトコル（Certificate Management Protocol: CMP）

証明書の作成と管理に関するすべての側面を処理する。**認証局**または**登録局**などの**公開鍵インフラストラクチャ**コンポーネントと、証明書を発行されるユーザーやアプリケーション間の相互作用をサポートする。

認証局（Certificate Authority: CA）

デジタル**証明書**を発行、更新および失効させる信頼できるサード・パーティ。基本的には、エンティティの識別情報が正しいかどうかの保証を行うが、申請者の検証を**登録局**に委任することもある。一般的な認証局（CA）として Digital Signature Trust 社、Thawte 社および VeriSign 社がある。

認証プラグイン（Authentication Plugin）

特定の認証方式を実装するもの。OracleAS Single Sign-On には、パスワード認証、デジタル証明、Windows のネイティブ認証およびサード・パーティのアクセス管理を行うための Java プラグインが用意されている。

認証レベル（Authentication Level）

アプリケーションの特定の認証動作を指定するための OracleAS Single Sign-On のパラメータ。このパラメータは特定の**認証プラグイン**とリンクできる。

ネーミング・コンテキスト（Naming Context）

1 つのサーバー内に全体が存在するサブツリー。1 サーバー内のこのサブツリーは連続している必要がある。つまり、最上位となるエントリのみでなく、リーフ・エントリか、または下位ネーミング・コンテキストに対する**ナレッジ参照**（参照とも呼ばれる）までが存在している必要がある。その大きさは、1 エントリのみでもかまわないし、**ディレクトリ情報ツリー**全体にわたってもかまわない。

ネーミング属性（Naming Attribute）

Oracle Delegated Administration Services または Oracle Internet Directory Java API を介して作成される新しいユーザー・エントリの RDN を作成するために使用される属性。デフォルト値は `cn`。

ネイティブ・エージェント（Native Agent）

Oracle Directory Integration Platform 環境で、**ディレクトリ統合サーバー**の制御下で動作するエージェント。**外部エージェント**と対照をなしている。

ネット・サービス（Net Services）

「**Oracle Net Services**」を参照。

ネット・サービス名（Net Service Name）

接続記述子として解決されるサービスの単純名。接続リクエストを開始するには、接続対象サービスの接続文字列としてユーザー名およびパスワードとともにネット・サービス名を渡す。例：

```
CONNECT username/password@net_service_name
```

必要に応じて、次を含む様々な場所に格納できる。

- 各クライアント上のローカル構成ファイル（`tnsnames.ora`）
- ディレクトリ・サーバー
- Oracle Names Server
- NDS、NIS または CDS などの外部ネーミング・サービス

パーティション（Partition）

1 つのディレクトリ・サーバーに格納されている、重複していない一意のディレクトリ・ネーミング・コンテキスト。

パートナ・アプリケーション（Partner Application）

認証機能を OracleAS Single Sign-On Server に委任する Oracle Application Server アプリケーションまたは Oracle 以外のアプリケーション。このタイプのアプリケーションでは、**mod_osso** ヘッダーが受け入れられるため、ユーザーはあらためて認証を受けないで済む。

バインド（Binding）

ネットワーキングでは、通信エンティティ間の論理的接続を確立すること。

Oracle Internet Directory では、ディレクトリに関する認証を行うこと。

また、（背後で作動する）別のプロトコルを使用して **SOAP** メッセージを交換用に伝達するための正規のルール・セットもバインドと呼ばれる。

ハッシュ（Hash）

アルゴリズムを使用してテキストの文字列から生成される数値。ハッシュ値はテキスト自体よりもかなり小さい。ハッシュ値は、セキュリティ用として使用される他、データに高速にアクセスするために使用される。

関連項目：「**ハッシュ関数**」

ハッシュ関数（Hash Function）

暗号化において、ハッシュ関数または一方向ハッシュ関数は、特定のデータ・ブロックに適用されたときに一定値を生成するアルゴリズムを意味する。ハッシュ関数の結果を使用して、特定のデータ・ブロックの整合性を保証できる。ハッシュ関数がセキュアなものであるとみなされるためには、あるデータ・ブロックに対する結果と同一の結果が生成される別のデータ・ブロックの作成が困難である必要がある。

ハッシュ・メッセージ認証コード（Hashed Message Authentication Code: HMAC）

秘密のハッシュ関数出力を作成するためのハッシュ関数技術。MD5 や SHA など、既存のハッシュ関数を強化する。Transport Layer Security（TLS）で使用される。

ハンドシェイク（Handshake）

2 台のコンピュータが通信セッションを開始するために使用するプロトコル。

非対称型アルゴリズム（Asymmetric Algorithm）

暗号化用と**復号化**用とで異なる**鍵**を使用する**暗号化アルゴリズム**。

関連項目：「**公開鍵暗号化**」

非対称型暗号化（Asymmetric Cryptography）

「**公開鍵暗号化**」を参照。

否認防止（non-repudiation）

暗号化で、特定の**デジタル署名**が特定のエンティティの**秘密鍵**を使用して作成され、メッセージが改ざんされずに特定の時刻に送信されたことを証明する機能。

秘密鍵（private key）

公開鍵暗号化で使用される**公開鍵と秘密鍵のペア**の秘密鍵。エンティティは、秘密鍵を使用して、**公開鍵**によって暗号化されたデータを復号化する。また、エンティティは、秘密鍵を使用して**デジタル署名**を作成することもできる。エンティティの公開鍵を使用して暗号化されたデータや秘密鍵を使用して作成された署名のセキュリティは、秘密鍵の機密性によって決まる。

秘密鍵（Secret Key）

対称型アルゴリズムで使用される**鍵**。暗号化と復号化の両方で使用されるため、暗号文の送信者と受信者間で共有する必要があるが、すべての不正エンティティには秘密にしておく必要がある。

秘密鍵暗号化（Private Key Cryptography）

「対称型暗号化」を参照。

秘密鍵暗号化（Secret Key Cryptography）

「対称型暗号化」を参照。

フィルタ（Filter）

ディレクトリに対するリクエストまたは検索から戻されるエントリを定義する式。通常、DN として表現される。例：`cn=susie smith,o=acme,c=us`

フェイルオーバー（Failover）

障害の認識とリカバリのプロセス。Oracle Application Server Cold Failover Cluster（Identity Management）では、1 つのクラスタ・ノード上で動作するアプリケーションが別のクラスタ・ノードに透過的に移行される。この移行時に、移行するクラスタ上のサービスにアクセスするクライアントにとってはサービスが一時的に停止することになり、フェイルオーバーが完了した後でサービスに再接続する必要が出てくる。

フェデレーション（Federation）

共有のユーザー・ベースを持つエンティティ（会社および組織）のグループ。ユーザーが 1 回ログインするのみで**トラスト・サークル**内のすべてのサービスにアクセスできるよう ID および認可トークンを提供することに合意している。フェデレーション内では、少なくとも 1 つのエンティティがユーザーを認証する役割を果す**識別情報プロバイダ**として機能する。ユーザーにサービスを提供するエンティティは、**サービス・プロバイダ**と呼ばれる。

フェデレーテッド ID 管理（Federated Identity Management: FIM）

ID と資格を複数の自律型ドメイン間で移植可能にする契約、規格および技術。認証済ユーザーを認識し、複数のドメインにおいて自分で選択したサービスに参加できるようにする。異なるアカウント間における識別情報のリンクを実現しながら、個人情報の集中管理による思いがけない危険を回避する。フェデレーテッド ID には、信頼と規格という 2 つのキー・コンポーネントが必要となる。フェデレーテッド ID 管理の信頼モデルは、**トラスト・サークル**に基づいている。規格は、**リバティ・アライアンス**・プロジェクトによって制定されている。

復号化（decryption）

暗号化したメッセージ（暗号文）の内容を読取り可能な元の形式（平文）に再変換するプロセス。

プロキシ・サーバー（Proxy Server）

Web ブラウザなどのクライアント・アプリケーションと実サーバーの間にあるサーバー。実サーバーに対するすべてのリクエストを傍受し、プロキシ自体でリクエストに対応できるかどうかを確認する。できない場合、リクエストを実サーバーに転送する。OracleAS Single Sign-On では、プロキシは、ロード・バランシングおよびセキュリティの追加レイヤーとして使用される。

関連項目：「**ロード・バランサ**」

プロキシ・ユーザー（Proxy User）

プロキシ・ユーザーとは、ファイアウォールなどの中間層がある環境で通常使用される一種のユーザー。このような環境では、エンド・ユーザーは中間層に対して認証を行う。次に、中間層がエンド・ユーザーのかわりにディレクトリにログインする。プロキシ・ユーザーは、識別情報を切り替える権限を持っているため、ディレクトリにログインした後でエンド・ユーザーの識別情報に切り替える。次に、このエンド・ユーザーに適した認可を使用してエンド・ユーザーのかわりに操作を実行する。

ブロック暗号（Block Cipher）

対称型アルゴリズムの 1 タイプ。メッセージを固定サイズのブロック（通常は 64 ビット）に分割し、鍵を使用して各ブロックを暗号化することにより、メッセージを暗号化する。一般的なブロック暗号として **Blowfish**、**DES** および **AES** がある。

関連項目：「**ストリーム暗号**」

プロビジョニング・アプリケーション（Provisioned Applications）

ユーザーおよびグループ情報が Oracle Internet Directory で集中管理されている環境にあるアプリケーション。通常、これらのアプリケーションは、Oracle Internet Directory 内でこの情報が変更されていないかどうかをチェックする。

プロビジョニング・エージェント（Provisioning Agent）

Oracle 固有のプロビジョニング・イベントを外部 / サード・パーティ・アプリケーション固有のイベントに変換するアプリケーションまたはプロセス。

プロファイル（Profile）

「ディレクトリ統合プロファイル」を参照。

米国連邦情報処理標準（Federal Information Processing Standards: FIPS）

米国商務省の国立標準技術研究所（NIST）によって制定された情報処理標準。

平文（Plaintext）

暗号化技術を使用して暗号文に変換する前の読取り可能データ。または、復号化技術を使用して暗号文から変換した読取り可能データ。

変更ログ（Change Logs）

ディレクトリ・サーバーの変更を記録するデータベース。

ポリシー優先順位（Policy Precedence）

Oracle Application Server Certificate Authority（OCA）では、ポリシーのメイン・ページに表示される。この順序で、ポリシーが受信リクエストに適用される。OCA のポリシー・プロセッサ・モジュールがポリシーを解析する際には、ポリシー・リストの最上部に表示されているポリシーがリクエストに最初に適用される。ポリシー・リストの最下部に表示されているポリシーが最後に適用され、他のポリシーよりも優先される。受信リクエストに適用されるのは有効なポリシーのみ。

マスター・サイト（Master Site）

レプリケーションで、LDAP レプリケーションに参加する、**マスター定義サイト**以外のサイト。

マスター定義サイト（Master Definition Site: MDS）

レプリケーションで、管理者が構成スクリプトを実行する Oracle Internet Directory データベース。

マッピング・ルール・ファイル（Mapping Rules File）

Oracle Directory Integration Platform 環境で、Oracle Internet Directory の属性と**接続ディレクトリ**の属性間のマッピングを指定するファイル。

マルチマスター・レプリケーション（Multimaster Replication）

peer-to-peer または *n* 方向レプリケーションとも呼ばれる。対等に動作する複数のサイトがレプリケート・データ・グループを管理できるようにする、レプリケーションの 1 タイプ。マルチマスター・レプリケーション環境では、各ノードはサプライヤ・ノードであると同時にコンシューマ・ノードでもあり、各ノード上でディレクトリ全体がレプリケートされる。

メタディレクトリ（Metadirectory）

すべての企業ディレクトリ間の情報を共有し、これらを 1 つの仮想ディレクトリに統合するディレクトリ・ソリューション。管理を一元化し、管理コストを削減する。ディレクトリ間のデータを同期化し、企業全体にわたってデータが最新の一貫したものであるようにする。

メッセージ・ダイジェスト（Message Digest）

ハッシュ関数の結果。

関連項目：「ハッシュ」

メッセージ認証（Message Authentication）

特定のメッセージが特定のエンティティのものであるかを検証するプロセス。

関連項目：「**認証**」

メッセージ認証コード（Message Authentication Code: MAC）

特定のデータ・ブロックへの 2 ステップ・プロセスの適用結果。第 1 ステップでは、**ハッシュ関数**の結果を取得する。第 2 ステップでは、**秘密鍵**を使用してこの結果を暗号化する。MAC を使用すると、特定のデータ・ブロックのソースであることを認証できる。

ユーザー検索ベース（User Search Base）

Oracle Internet Directory のデフォルトの**ディレクトリ情報ツリー**において、すべてのユーザーが配置されている ID 管理レルムの中のノード。

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 OracleAS Single Sign-On Java モジュール。これにより、ニックネームは認証モジュールに渡され、認証モジュールはこのニックネームを使用してユーザーの証明書をディレクトリから取得する。

猶予期間ログイン（Grace Login）

パスワードの有効期限前の指定された期間内に行われるログイン。

読取り可能データ（readable data）

暗号化技術を使用して暗号文に変換する前のデータ。または、復号化技術を使用して暗号文から変換したデータ。

リバティ・アライアンス（Liberty Alliance）

リバティ・アライアンス・プロジェクトは、世界中の 150 社を超える会社、非営利組織および政府機関で構成されるアライアンスである。このコンソーシアムは、現行および新興のすべてのネットワーク・デバイスをサポートするフェデレーテッド・ネットワーク識別情報用のオープン規格を制定することに取り組んでいる。リバティ・アライアンスは、**フェデレーテッド ID 管理**用のオープン技術規格、プライバシ、ビジネス・ガイドラインを定義および推進する唯一の国際団体である。

リモート・マスター・サイト（Remote Master Site: RMS）

レプリケーション環境では、**Oracle Database アドバンスト・レプリケーション**に参加する、**マスター定義サイト**以外のサイトを示す。

リレーショナル・データベース（Relational Database）

構造化されたデータのコレクションで、同じ列セットが含まれる 1 つ以上の行で構成された表に格納されている。Oracle では、複数の表の中のデータ同士を非常に簡単にリンクできる。これがリレーショナル・データベース管理システム（RDBMS）の特徴である。データは複数の表に格納され、表間のリレーションシップを定義できる。リンクは、両方の表に共通する 1 つ以上のフィールドに基づく。

ルート CA（root CA）

ルート**認証局**は、階層的な**公開鍵インフラストラクチャ**において、セキュリティ・ドメインに対して最も信頼されるデータとして機能する**公開鍵**を持つ認証局。

ルート DSE（Root DSE）

「**ルート・ディレクトリ固有エントリ**」を参照。

ルート Oracle コンテキスト（Root Oracle Context）

Oracle Identity Management インフラストラクチャで、インフラストラクチャ内のデフォルトの ID 管理レルムに対するポインタが含まれる、Oracle Internet Directory のエントリ。ID 管理レルムの単純名を指定したときにそのレルムをロケーティングする方法に関する情報も含まれている。

ルート・ディレクトリ固有エントリ（Root Directory-Specific Entry: DSE）

ディレクトリに対する操作情報が格納されたエントリ。情報は複数の属性に格納される。

レガシー・アプリケーション（Legacy Application）

認証を OracleAS Single Sign-On Server に委任するように変更できない旧型アプリケーション。**外部アプリケーション**とも呼ばれる。

レジストリ・エントリ（Registry Entry）

ディレクトリ・サーバー・インスタンスと呼ばれる、起動された個々の Oracle Internet Directory Server の実行時情報が含まれるエントリ。ディレクトリ自体に格納され、対応するディレクトリ・サーバー・インスタンスが停止するまで削除されない。

レスポンス時間（Response Time）

リクエストの送信からレスポンスの完了までの時間。

レプリカ（Replica）

単一サーバー内に含まれる**ネーミング・コンテキスト**の各コピー。

レプリケーション承諾（Replication Agreement）

ディレクトリ・レプリケーション・グループ内のディレクトリ・サーバー間のレプリケーション・リレーションシップを示す特別なディレクトリ・エントリ。

レルム（Realm）

「**ID 管理レルム**」を参照。

レルム検索ベース（Realm Search Base）

すべての **ID 管理レルム**が含まれる**ディレクトリ情報ツリー**内のエントリを識別する**ルート Oracle コンテキスト**の属性。単純なレルム名をディレクトリ内の対応エントリにマッピングするのに使用される。

ロード・バランサ（Load Balancer）

大量のロードやフェイルオーバーに対応して、複数のサーバー間で接続リクエストを平準化するハードウェア・デバイスおよびソフトウェア。このようなハードウェア・デバイスとしては BigIP、Alteon、Local Director がよく知られている。ロード・バランス・ソフトウェアの例としては Oracle Application Server Web Cache がある。

論理ホスト（Logical Host）

Oracle Application Server Cold Failover Cluster（Identity Management）で、1 つ以上のディスク・グループとホスト名および IP アドレスのペアから構成される。クラスタ内の物理ホストにマップされる。この物理ホストは、論理ホストのホスト名および IP アドレスになりすます。

索引

数字

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

の

は

ひ

ふ

へ

ほ

み

む

め

も

ゆ

よ

り

る

れ

ろ

わ