Oracle8*i* Advanced Security

管理者ガイド

リリース 8.1

ORACLE®

Oracle8*i* Advanced Security 管理者ガイド リリース 8.1

部品番号 : A62778-1

第 1 版 : 1999 年 5 月

原本名 : Oracle Advanced Security Administratior's Guide, Release 8.1.5

原本部品番号 : A67766-01

原本著者 : Richard Smith

原本協力者 : Gilbert Gonzalez, Laura Ferrer, Patricia Markee, Kendall Scott, Sandy Venning, Rick Wong, Pierre Baudin, Kristy Browder, Quan Dinh, Pramodini Gattu, Shuvayu Kanjilal, Van Le, Andy Philips, Ramana Rao, Vipin Samar, Debbie Steiner, Juliet Tran, Rick Wessman

グラフィック・デザイナ : Valarie Moore

Printed in Japan.

目次

3 RADIUS 認証の構成

6 SecurID 認証の構成

7 Identix Biometric 認証の構成

8 DCE GSSAPI 認証の構成

9 SSL 認証の構成

A 暗号化パラメータとチェックサム・パラメータ

B 認証パラメータ

C RADIUS による認証デバイスの統合

はじめに

Oracle Advanced Security は、Net8 ネットワークのセキュリティと認証機能を強化し、分散コンピューティング環境（DCE）との統合を実現します。このマニュアルでは、Oracle Advanced Security のすべての機能を総合的に説明します。

ここでは、次のトピックについて説明します。

このマニュアルの内容

このマニュアルでは、既存の Net8 ネットワークで Oracle Advanced Security を使用する場合の一般的な構成方法について説明します。特定のプラットフォームに Oracle Advanced Security をインストールし、構成する方法を説明したマニュアルとともに使用します。

Oracle Advanced Security は、他の Oracle ネットワーク製品とともにインストールして構成し、すべてを同時に構成することも、既存のネットワークに Oracle Advanced Security を追加することもできます。

このマニュアルの構成

このマニュアルは次の 2 つに分かれています。

- 第 I 部 : 「Oracle Advanced Security 機能」
- 第 II 部 : 「Oracle Advanced Security および Oracle DCE Integration」

それぞれの部で、Oracle Advanced Security の各機能について説明しています。

第 I 部 : Oracle Advanced Security 機能

第 1 章の「Oracle Advanced Security の概要」－この章では、Oracle Advanced Security のセキュリティ機能と Single sign-on 機能の概要について説明します。この章では次の機能について説明します。

- ネットワーク・セキュリティ
- データ暗号化
- データの整合性チェック
- トークン認証
- Single sign-on

注意 : これらの機能は、以前に Secure Network Services と Oracle Advanced Networking Option としてパッケージされていたものです。

この章では、このリリースで使用可能な認証機構についても簡単に説明します。

第 2 章の「暗号化とチェックサムの構成」－この章では、既存の Net8 リリース 8.1.5 ネットワークで暗号化とチェックサムを構成する方法について説明します。

第 3 章の「RADIUS 認証の構成」－この章では、RADIUS（Remote Authentication Dial-In User Service）を使用する Oracle の構成方法について説明します。Oracle 環境内での RADIUS の動作、RADIUS 認証とアカウントを使用可能にする方法、サード・パーティ・ベ

ンダーがカスタマイズできる要求 - 応答ユーザー・インタフェースの概要について説明します。

第 4 章の「CyberSafe 認証の構成」－この章では、CyberSafe を使用する Oracle の構成方法を説明し、Oracle ユーザーを認証する CyberSafe の構成手順について簡単に説明します。

第 5 章の「Kerberos 認証の構成」－この章では、MIT Kerberos を使用する Oracle の構成方法を説明し、Oracle ユーザーを認証する Kerberos の構成手順について簡単に説明します。

第 6 章の「SecurID 認証の構成」－この章では、Oracle Server および Oracle クライアントで使用する SecurID 認証アダプタの構成方法を説明します。この章では、SecurID を使用するシステムの要件と既知の制限事項、および SecurID 認証アダプタを構成する際に発生する問題の解決方法も説明します。

注意： Oracle Advanced Security のエラー・メッセージに関する詳細は、『Oracle Network 製品トラブルシューティング・ガイド』を参照してください。

第 7 章の「Identix Biometric 認証の構成」－この章では、Oracle Biometric 認証アダプタの構成方法と使用方法について説明します。この認証アダプタによって、Identix 指紋認証デバイスが使用可能になります。

第 8 章の「DCE GSSAPI 認証の構成」－この章では、Oracle DCE GSSAPI 認証アダプタの構成方法を説明します。この認証アダプタを使用すると、ネットワーク内で他の DCE サービスを使用しなくても、DCE 認証を利用できます。

第 9 章の「SSL 認証の構成」－この章では、Oracle Advanced Security の SSL 機能について説明します。SSL の構成方法と、Oracle Wallet Manager を使用した Wallet と Trustpoint を管理する方法について説明します。

第 10 章の「認証方式の選択と組合せ」－この章では、別の認証サービスを構成してあってもそれを使用せずに、ユーザー名 / パスワードによる従来の方法での認証を使用する方法について説明します。また、Oracle Advanced Security を使用して、1 つまたは複数の認証サービスを使用するネットワークを構成する方法、およびクライアント上またはサーバー上で複数の認証サービスをセットアップする方法についても説明します。

第 II 部 : Oracle Advanced Security と Oracle DCE Integration

第 11 章の「Oracle DCE Integration の概要」－この章では、OSF の DCE と Oracle の DCE Integration について簡単に説明します。

第 12 章の「Oracle DCE Integration を使用する DCE の構成」－この章では、Oracle DCE Integration を使用する DCE の構成手順について説明します。また、DCE CDS ネーム・アダプタの構成方法も説明します。

第 13 章の「Oracle DCE Integration を使用する Oracle の構成」－この章では、クライアントとサーバーが DCE 環境の Oracle Server にアクセスできるように、SQL*Net または Net8

の構成ファイルに追加する必要がある DCE パラメータについて説明します。また、外部ロールにマップする DCE グループをセットアップするなど、Oracle サーバー上で必要な構成作業についても説明します。DCE CDS ネーム・アダプタを使用するクライアントの構成方法も説明します。

第 14 章の「DCE 環境の Oracle データベースに接続」－この章では、DCE 環境の Oracle データベースに接続する方法について説明します。

第 15 章の「DCE 環境と非 DCE 環境の相互運用性」－この章では、非 DCE 環境のクライアントが、TCP/IP などの別のプロトコルを使用して Oracle データベースにアクセスする方法について説明します。

付録

付録 A の「暗号化パラメータとチェックサム・パラメータ」－この付録では、Oracle Advanced Security の暗号化とチェックサムの設定パラメータの一覧を示し、説明します。

付録 B の「認証パラメータ」－この付録では、Oracle Advanced Security の認証設定ファイル・パラメータの一覧を示し、説明します。

付録 C の「RADIUS による認証デバイスの統合」－この付録では、RADIUS 要求 - 応答認証で使用されているグラフィカル・ユーザー・インタフェースを認証デバイスのサード・パーティ・ベンダーがカスタマイズする方法について説明します。

表記規則

このマニュアルでは次の構文規則を採用しています。

イタリック体	イタリック体は、コマンド構文内のパラメータ、変数、式を、適切な値で置き換える必要があることを示しています。
クーリエ・フォント	クーリエ・フォントは、コンピュータが表示する内容を示しています。 **注意 :** コマンド内の単語をより明確に区切るために、特定の語を山カッコで囲む場合もあります（`<pin><passcode>` など）。
太字	次の場合に太字を使用します。 ■ 用語集で定義されている用語 ■ 表記通りに入力する必要のある文字 **注意 :** コマンド内の単語をより明確に区切るために、特定の語を山カッコで囲む場合もあります（`<pin><passcode>` など）。
句読点	カッコと縦線以外の句読点は、表記通りに入力する必要があります。

[ ]	大カッコを使用して、オプションの項目を囲んでいます。大カッコは入力しません。
( )	カッコを使用して、接続記述子におけるすべての SQL*Net と Net8 のキーワード値ペアを囲んでいます。`(KEYWORD=value)` というように、カッコを接続記述子の一部として入力する必要があります。
|	縦線を使用して、複数のオプションから選択できる項目を示しています。縦線で区切られたオプションの中から 1 つの項目を入力する必要があります。縦線は入力しません。
大文字	テキスト内の大文字は、コマンド名とパラメータを示します。

関連マニュアル

Oracle Advanced Security ソフトウェアを特定のプラットフォームにインストールして構成するには、Oracle が提供するプラットフォーム固有のマニュアルを参照してください。

また、複数のプラットフォームに適用される Oracle ネットワーク製品に関する詳細は、次のマニュアルを参照してください。

- 『Oracle8*i* Net8 管理者ガイド』
- 『Oracle8*i* 分散システム』

ロールと権限については、次のマニュアルを参照してください。

- 『Oracle8*i* 管理者ガイド』

セキュリティと Single sign-on 機能については、サードパーティ・ベンダーが提供する次のマニュアルを参照してください。

- 『RADIUS 管理者ガイド』
- Security Dynamics の『ACE/Server Installation Manual, release 1.3』
- Security Dynamics の『ACE/Server Version 1.3 Administration Manual』
- 『ACE/Server Version 2.0 Client for UNIX』
- 『CyberSafe Challenger Release Notes, release 5.2.6』
- 『CyberSafe Challenger Administrator's Guide, release 5.2.6』
- 『CyberSafe Challenger Navigator Administrator's Guide, release 5.2.6』
- 『CyberSafe Challenger UNIX User's Guide, release 5.2.6』
- 『CyberSafe Challenger Windows and Windows NT User's Guide, release 5.2.6』

MIT Kerberos については、次のマニュアルを参照してください。

- CyberSafe Challenger 関連マニュアル
- Kerberos V5 ソース配布から Kerberos を構築してインストールする方法を説明した資料
- http://www.cygnus.com/ で提供される CNS（Cygnus Network Security）マニュアル

OSF 分散コンピューティング環境（DCE）に関する詳細は、Prentice Hall 社が出版している次の OSF マニュアルを参照してください。

- 『OSF DCE User's Guide and Reference』
- 『OSF DCE Application Development Guide』
- 『OSF DCE Application Development Reference』
- 『OSF DCE Administration Guide』
- 『OSF DCE Administration Reference』
- 『OSF DCE Porting and Testing Guide』
- 『Application Environment Specification/Distributed Computing』
- 『OSF DCE Technical Supplement』

Identix 製品については、次の Identix マニュアルを参照してください。

クライアント側

- 『Identix TouchNet II User's Guide』

サーバー側

- 『Identix TouchNet II System Administrator's Guide』

第 I 部

Oracle Advanced Security 機能

このマニュアルの第 1 部では、既存の Net8 リリース 8.1.5 のネットワークに、セキュリティと認証機能を組み込む方法について説明します。Oracle Advanced Security のインストール方法と構成方法については、ポート固有のマニュアルも参照してください。

『Oracle8*i* Advanced Security 管理者ガイド』では、次の各章で Oracle Advanced Security のセキュリティ関連機能を総合的に説明します。

- 第 1 章の「Oracle Advanced Security の概要」
- 第 2 章の「暗号化とチェックサムの構成」
- 第 3 章の「RADIUS 認証の構成」
- 第 4 章の「CyberSafe 認証の構成」
- 第 5 章の「Kerberos 認証の構成」
- 第 6 章の「SecurID 認証の構成」
- 第 7 章の「Identix Biometric 認証の構成」
- 第 8 章の「DCE GSSAPI 認証の構成」
- 第 9 章の「SSL 認証の構成」
- 第 10 章の「認証方式の選択と組合せ」

DCE Integration の詳細情報： 第 II 部「Oracle Advanced Security および Oracle DCE Integration」を参照してください。

1

Oracle Advanced Security の概要

この章では、Oracle Advanced Security **暗号化（encryption）**、**チェックサム（checksumming）**および**認証（authentication）**の各機能の概要を説明します。Net8 を使用するネットワーク製品（Oracle8*i*、Designer 2000、Developer 2000、および Net8 をサポートするその他の Oracle 製品またはサードパーティ製品など）で、これらの機能を利用できます。

この章は次の項で構成されています。

Oracle Advanced Security について

Oracle Advanced Security（以前の Secure Network Services と Oracle Advanced Networking Option）の総合的なセキュリティ機能により、企業のネットワークを保護し、企業ネットワークをインターネットに安全に展開できます。Oracle Advanced Security では、単一のソースによってネットワークの暗号化と認証の解決策、Single sign-on サービスとセキュリティ・プロトコルの統合が提供されます。業界標準を組み込むことにより、Oracle ネットワークと Oracle ネットワークの外部まで、他に類のないセキュリティが実現されます。

分散環境でのネットワーク・セキュリティ

世界中の企業は、Net8 と Oracle8*i* を使用した分散データベースとクライアント / サーバー・アプリケーションを、記録的な数で全国規模または世界規模に配備しています。分散コンピューティングの普及にともなって、企業はますます多くの情報をコンピュータに格納するようになりました。従業員レコード、財務レコード、製品テスト情報、その他の機密データまたは重要なデータが、ファイル棚からファイル構造へと移されています。コンピュータに格納される重要なデータまたは機密データの量が増加したことにより、データが危険にさらされる可能性が高まりました。

これらの環境でデータの分散化が進んだため、セキュリティの面においても重大な危機が訪れています。

- データ改ざん－分散環境になったことで、サイト間で移動するデータを悪意のある第 3 者が実際に改ざんして、コンピュータ犯罪を犯す可能性も考えられます。
- 傍受とデータの盗難－インターネットや広域ネットワーク（WAN）環境では、公共通信事業者と私設ネットワーク所有者が、安全性に欠ける陸上回線、障害を受けやすいマイクロ波と衛星リンク、または多数のサーバーをネットワークの一部で使用しているので、貴重なデータが利害関係者にのぞかれる可能性があります。ビルまたはキャンパス内のローカル・エリア・ネットワーク（LAN）環境では、物理配線にアクセスできる内部の者が、他人のデータを見ることができます。
- ユーザー ID の偽造－分散環境では、識別情報を偽造して機密情報や重要な情報にアクセスできる危険性が高まっています。クライアント B からサーバー A に接続しているユーザー Smith が、Smith 本人であるという保証はあるでしょうか。

  さらに、分散環境では、犯罪者が接続を奪い取る可能性があります。クライアント B とサーバー A が本当にクライアント B およびサーバー A であるという保証はあるでしょうか。サーバー A の人事システムからサーバー B の給与支払いシステムに転送中のトランザクションが傍受されて、サーバー B として偽装する端末に送られる可能性があります。
- 多数のパスワード管理－分散システムでは、ユーザーが使用するさまざまなアプリケーションやサービスに対して、ユーザーが複数のパスワードを記憶する必要があります。たとえば、開発者がワークステーションで開発中のアプリケーションにアクセスし、ミニコンピュータ上では本番システムにアクセスし、文書作成用に PC を利用し、テスト、バグの報告、構成管理などの目的で何台かのミニコンピュータまたはワークステーショ

ンを使用します。これらアカウントとパスワードをすべて管理する作業は複雑で、時間がかかります。

通常、ユーザーは次に示す 2 つの方法で複数のアカウントに応答します。

- ユーザーが自分自身のパスワードを選択できる場合は、すべてのマシンで共通のパスワードを使用することが考えられます。この方法では、パスワードが見破られた場合の危険が増大します。または、1 つのパスワードがわかれば容易に推測できるような類似したパスワードを使用することが考えられます。
- 複雑なパスワードを使用するユーザーは、パスワードを書き留めておくことがあり、忘れてしまうこともあります。

この場合も、パスワードの機密性が損なわれ、サービスの可用性が大幅に低下します。

Oracle Advanced Security の機能

Oracle Advanced Security では、分散環境のセキュリティを上に示した脅威から守ります。特に、Oracle Advanced Security では次の機能を備えており、それぞれを以下に説明しています。

- データの整合性－転送中にデータが変更されないようにする
- データ・プライバシ－転送中のデータの機密性を保つ
- 認証ユーザー、ホスト、クライアントの個別性を正しく確実に識別し、複数のパスワードを使用しなくて済むように Single sign-on 機能を提供する
- 認可－オブジェクトまたはオブジェクト・セットにアクセスする際に、ユーザー、プログラム、プロセスに適切なアクセス権が与えられるようにする

データの整合性

転送中のデータが変更、削除または再生されていないことを保証するために、Oracle Advanced Security では暗号論的に安全なメッセージ・ダイジェストを、MD5 アルゴリズムを使用した暗号チェックサムによってオプションで生成し、ネットワーク上で送信される各パケットにそのメッセージ・ダイジェストを組み込みます。

さらに、Oracle Advanced Security の SSL 機能によって SHA（Secure Hash Algorithm）を使用することもできます。SHA は MD5 に比べて少し遅くなりますが、長いメッセージ・ダイジェストを作成できるので、強引な衝突や反転攻撃をさらに効果的に防御できます。

データ・プライバシ

Oracle Advanced Security では、RSA と DES 暗号化によってデータ・プライバシを保証します。

- RSA 暗号化－ RSA Data Security RC4 暗号化アルゴリズムを使用した暗号化モジュール。ランダムに生成される秘密鍵をすべてのセッションで使用することによって、すべてのネットワーク・トラフィック（すべてのデータ値、SQL 文、ストアド・プロシージャの

コールと結果を含む）を完全に保護しています。クライアント、サーバーまたはその両者が暗号化モジュールの使用を要求して、データを保護することができます。Oracle の最適化された処理系によって、パフォーマンスへの影響を最小限に抑えて高度なセキュリティが実現されています。RC4 アルゴリズムでは、40 ビット、56 ビット、128 ビットの暗号キーを利用できます。

Oracle Advanced Security に実装されている 40 ビットの RSA RC4 は、暗号化製品に関する米国政府輸出ガイドラインの要件を満たしているので、オラクル社は輸出用バージョンの媒体を作成し、数カ国を除くすべての国に輸出しています。このため、ほとんどの企業はこのソフトウェアを使用して世界中で安全に業務を遂行することができます。

- DES（Data Encryption Standard）暗号化－金融をはじめとする多数の機関で必要とされる米国のデータ暗号化標準。Oracle Advanced Security for Domestic Use では国内使用向けに、最適化された 56 ビット・キーの標準の DES 暗号化アルゴリズムを用意しています。現行の米国政府輸出制限のため、標準の DES を使用することができるのは、米国とカナダのユーザーのみに制限されています。米国とカナダ以外の国では、輸出バージョンの Oracle Advanced Security for Export Use に用意された DES40 を使用することができます。DES40 は、標準の DES 暗号化アルゴリズムと国際的な 40 ビット・キーを組み合せたバージョンです。ネットワーク暗号化に使用するアルゴリズムをユーザーの構成オプションとして選択できるので、データ転送の種類に応じてさまざまなレベルのセキュリティとパフォーマンスを実現できます。

詳細情報： 暗号化とチェックサムの詳細は、第 2 章の「暗号化とチェックサムの構成」と付録 A の「暗号化パラメータとチェックサム・パラメータ」を参照してください。

認証

分散環境では、ユーザーの識別情報を確立することも重要です。これを確立しないと、ユーザーごとの権限の制限に確実性がなくなります。Oracle Advanced Security リリース 8.1.5 では、Kerberos および CyberSafe TrustBroker（Kerberos ベースの認証サーバー）、SecurID、Identix TouchNet II、RADIUS などのサードパーティ認証サービスをサポートする Oracle 認証アダプタによって、この認証機能を提供しています。この章の次項以降でこれらのアダプタについて説明します。

集中認証サービス Oracle Advanced Security 認証方式の多くで集中認証サービスを使用しています。集中認証サービスにより、分散環境でのユーザー、クライアント、サーバーの識別情報における確実性が高まります。ネットワークのすべてのメンバー（クライアント対サーバー、サーバー対サーバー、ユーザー対クライアント、ユーザー対サーバー）の認証を集中化することにより、ネットワーク上で個別性を偽っているノードの脅威に効果的に対応できます。

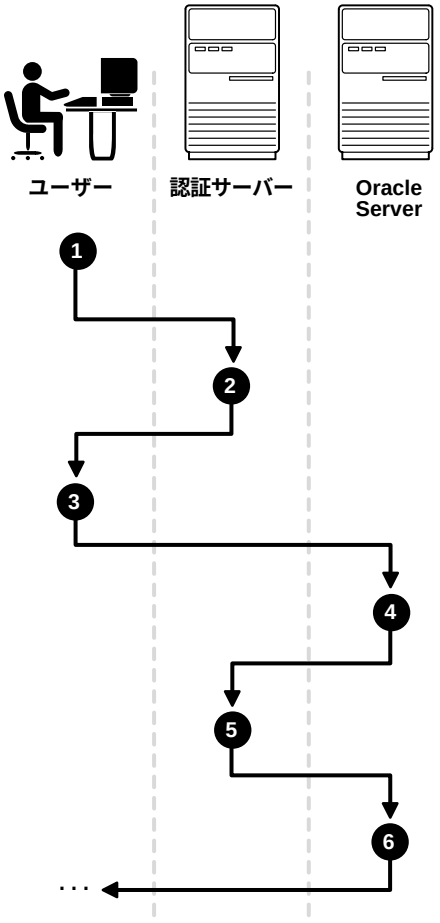
集中認証サービスでは、ユーザーの Single sign-on を使用することもできます。Single sign-on によって、ユーザーは 1 つのパスワードで複数のアカウントとアプリケーションに

アクセスできるようになるので複数のパスワードを使用する必要がなくなり、システム管理者はユーザーのアカウントとパスワードを容易に管理できます。

注意： オラクル社では集中認証サーバーは提供していません。他のベンダーのセキュリティ・サービスや、CyberSafe など、サードパーティ製の Kerberos ベースのサーバーによって認証サービスをサポートしています。Oracle Advanced Security でサポートしている認証方式の一覧と簡単な説明は、1-7 ページの「サポートされる認証方式」を参照してください。

集中認証サービスの動作 図 1-1 に、集中ネットワーク認証サービスの一般的な動作を示します。

図 1-1 ネットワーク認証サービスでのユーザーの認証方法



1. ユーザー（クライアント）が認証サービスを要求して、トークンまたはパスワードなどの自己識別情報を提供します。
2. 認証サーバーはユーザーを認証してから、クライアントにチケットまたは資格証明を戻します。このチケットの有効期限が指定されている場合もあります。
3. クライアントがこれらの資格証明を受け取り、Oracle Server に資格証明を渡してデータベース接続などのサービスを要求します。
4. サーバーは資格証明の有効性を検証するために、資格証明を認証サーバーに戻します。
5. 認証サーバーは資格証明を承諾すると、Oracle Server にその旨を通知します。
6. Oracle Server はユーザーから要求された作業を実行します。資格証明が承諾されない場合は、サーバーがサービスを拒否します。

サポートされる認証方式 Oracle Advanced Security では次の認証方式をサポートしています。

SSL － SSL（Secure Sockets Layer）はネットワーク接続を保護するための業界標準のプロトコルです。SSL では認証、暗号化、データの整合性が実現されます。

Oracle Advanced Security の SSL 機能を使用して、クライアントとサーバー間で安全に通信できます。特に、次の認証を行う場合に SSL を使用します。

- 1 つ以上の Oracle Server に対するクライアントまたはサーバー
- クライアントに対する Oracle Server

SSL 機能は SSL のみでも使用することができますが、Oracle Advanced Security でサポートされている他の認証方式とともに使用することもできます。たとえば、SSL の暗号化と Kerberos の認証方式を組み合わせて使用することができます。

SSL は、サーバーのみを認証するように構成するか、またはクライアントとサーバーの両方を認証するように構成できます。

RADIUS － RADIUS（Remote Authentication Dial-In User Service）はクライアント / サーバー・セキュリティ・プロトコルであり、リモート認証とリモート・アクセスを実現するものとして、もっとも広く知られています。Oracle Advanced Security では、RADIUS プロトコルをサポートする認証方式を使用できるようにするため、この新生の標準をクライアント / サーバー・ネットワーク環境で使用しています。RADIUS はトークン・カードやスマートカードなど、各種の認証方式と組み合わせて使用することができます。

Kerberos と CyberSafe － Oracle Advanced Security がサポートする Kerberos と CyberSafe によって、Oracle 環境で Single sign-on と集中認証サービスを利用できます。Kerberos は、共有シークレットを利用する信頼性の高いサードパーティ認証システムです。Kerberos はサードパーティの安全性を前提としています。Kerberos は、Single sign-on 機能、パスワード集中格納、データベース・リンク認証、拡張 PC セキュリティを提供します。Kerberos の認証と Kerberos ベースの認証サーバーである CyberSafe TrustBroker によって実現されます。

注意： Kerberos 用の Oracle 認証は、データベース・リンク認証（「代理認証」ともいう）を提供しています。CyberSafe と SecurID は、代理認証をサポートしていません。

スマートカード（RADIUS 準拠）－この認証方式ではクレジット・カードに似たハードウェア・デバイスを使用します。メモリとプロセッサが搭載されており、クライアント・ワークステーションにあるスマートカード・リーダーで読み込みます。

スマートカードには次の利点があります。

- セキュリティの強化－スマートカードは、認証の持つ 2 つの要素によって保証されています。スマートカードはロックすることができ、そのロックを解除できるのは、カードの所有者であり、正確な PIN を知っている人のみです。

- パフォーマンスの向上－精巧なスマートカードにはハードウェア・ベースの暗号化チップが組み込まれており、ソフトウェア・ベースの暗号化に比べてスループットがよくなります。スマートカードにはユーザー名を格納することができます。
- 任意のワークステーションからのアクセス可能性－ユーザーは、カードを読み取るハードウェア・デバイスにスマートカードを挿入し、PIN など、カードで必要な認証情報を入力するのみでログインできます。ユーザーが正しい認証情報を入力したあとで他の認証情報が必要になった場合、それはスマートカードによって生成され入力されます。

トークン・カード（SecurID および RADIUS 準拠）－トークン・カードは、いくつかの異なったメカニズムによって使いやすさを向上させます。一部のトークン・カードは、認証サービスと同期化されているワンタイム・パスワードを動的に表示します。サーバーは認証サービスと連絡を取り合うことによって、トークン・カードが提供するパスワードをいつでも検証できます。トークン・カードの中にはキーパッドを備えるものがあり、要求 - 応答に基づいて操作します。この場合、サーバーから要求（番号）が提供され、その番号をユーザーがトークン・カードに入力します。トークン・カードは応答として、要求から暗号的に導出される別の番号を提供し、それをユーザーがサーバーに渡します。

トークン・カードには次の利点があります。

- 使いやすさ－ユーザーは複数のパスワードではなく個人の識別番号（PIN）のみを覚えておくだけで済みます。
- パスワード管理の容易性－複数のパスワードは必要なく、トークン・カード 1 つだけで済みます。
- パスワードの安全性の向上－犯罪者はトークン・カードおよびトークン・カードを操作するのに必要な PIN がなければユーザーとして偽装できません。
- アカウントの向上－トークン・カードによって認証メカニズムが強化されます。

SecurID または RADIUS によって SecurID トークンを使用することができます。

Bull ISM － ISM（Integrated System Management）は Bull Worldwide Information Systems 提供の管理ツールで、システム管理者が各種管理作業を行うことができます。この認証方式は AIX プラットフォームのみで使用できます。詳細は AIX 固有のマニュアルを参照してください。

Biometric Authentication（Identix）－ Identix Biometric Authentication はクライアントと Oracle Server の両方で使用して、認証サーバーとクライアントの間で生物学的認証データをやりとりします。

認可

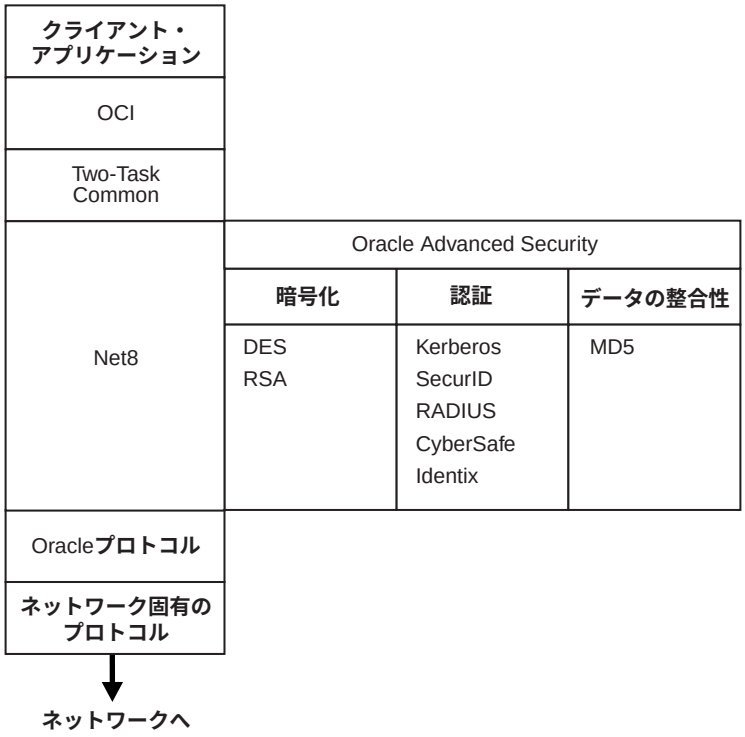
Oracle8*i* の標準機能であるユーザー認証は、Oracle Advanced Security でサポートされる認証方式を使用して大幅に強化されています。たとえば、Solaris など、特定のプラットフォームでは、Oracle Advanced Security は DCE による認証をサポートしています。

Oracle Advanced Security のアーキテクチャ

Oracle Advanced Security は標準の Net8 Server または Net8 Client のアドオン製品です。図 1-2 に、Oracle ネットワーク環境の一般的なスタック内での Oracle Advanced Security の位置付けを示します。

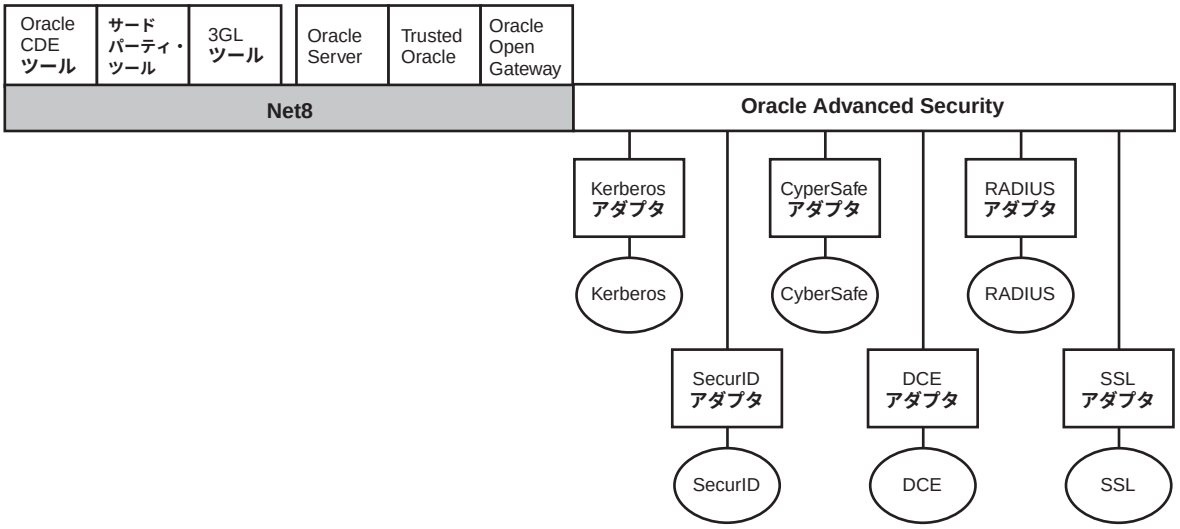
> **詳細情報：** Oracle ネットワーク環境でのスタック通信の詳細は、『Oracle8*i* Net8 管理者ガイド』を参照してください。

図 1-2 Oracle ネットワーク環境での Oracle Advanced Security



Oracle Advanced Security では、既存の Oracle プロトコル・アダプタと同様のアダプタによって認証をサポートしています。図 1-3 に示すように、認証アダプタを Net8 インタフェースの下に統合することにより、既存のアプリケーションは新しい認証システムを透過的に利用できます。既存のアプリケーションを変更する必要はありません。

図 1-3 Net8 と認証アダプタ



ネットワーク・プロトコル境界でのデータ転送の保護

Oracle Advanced Security は Oracle Connection Manager によって完全にサポートされているので、複数のネットワーク・プロトコル間で安全にデータを転送できます。たとえば、NetWare（SPX/IPX）のような LAN プロトコルを使用するクライアントは、LU6.2、TCP/IP、DECnet のような異なるネットワーク・プロトコルを使用する大型サーバーと、安全にデータを共有できます。ネットワーク・インフラストラクチャの弱点を補いながら、最大のパフォーマンスを実現するために、Connection Manager は復号化 / 再暗号化のコストと危険を回避して暗号化されたデータをプロトコル間で渡します。

システム要件

Oracle Advanced Security は標準の Net8 Server または Net8 Client のアドオン製品です。この機能を利用するには、クライアントとサーバーの両方に対してこの製品を購入する必要があり、別に費用がかかります。

Oracle Advanced Security リリース 8.1.5 では Net8 リリース 8.1.5 が必要です。

Oracle Advanced Security リリース 8.1.5 では Oracle 8*i* Enterprise Edition をサポートしています。

TrustBroker は、Oracle Advanced Security が必要なクライアントとサーバーすべてに Oracle Advanced Security をインストールします。

注意： Oracle Advanced Security リリース 8.1.5 を旧リリース（1.0 や 1.1）とともに使用しても、安全に通信が行えます。ただし、この場合は、デフォルトにより旧リリースのセキュリティ機能が使用されます。

認証方式	システム要件
SSL	Oracle Wallet Manager リリース 1.3 ベータと互換性のある Wallet。旧リリースの Oracle Wallet Manager で作成された Wallet は上位互換ではありません。
CyberSafe TrustBroker	バージョン 1.1 以降の CyberSafe GSS ランタイム・ライブラリを、Oracle クライアントを実行するマシンと Oracle Server を実行するマシンの両方にインストールする必要があります。 リリース 1.2 以降の CyberSafe TrustBroker を、認証サーバーを実行する物理的に安全なマシンにインストールする必要があります。 リリース 1.2 以降の CyberSafe TrustBroker Client を、Oracle クライアントを実行するマシンにインストールする必要があります。
Kerberos	MIT Kerberos バージョン 5、リリース 1.0。 Kerberos 認証サーバーを、物理的に安全なマシンにインストールする必要があります。
SecurID	認証サーバーで動作するバージョン 1.2.4 以降の ACE/Server。
Identix Biometric	それぞれの Biometric Manager ステーションと Biometric Manager クライアントに、Identix ハードウェアとドライバをインストールする必要があります。
RADIUS	Internet Engineering Task Force（IETF）RFC #2138、*Remote Authentication Dial In User Service（RADIUS）*および RFC #2139 *RADIUS Accounting* の標準に準拠する RADIUS サーバー。 要求 - 応答認証を使用可能にする場合は、JavaSoft の Java Development Kit リリース 1.1 で指定されている Java Native Interface をサポートするプラットフォームで RADIUS を実行する必要があります。

ネットワーク認証における Oracle 構成

この項では、ネットワーク認証用に Oracle を構成する際に設定するパラメータについて説明します。この項では、特に、次の作業について説明します。

- SQLNET.ORA での SQLNET.AUTHENTICATION_SERVICES パラメータの設定
- REMOTE_OS_AUTHENT が TRUE に設定されていないことを確認

- OS_AUTHENT_PREFIX を NULL 値に設定

  詳細情報： 特定の認証方式を構成する際の詳細は、その方式に対応した章を参照してください。

SQLNET.ORA での SQLNET.AUTHENTICATION_SERVICES パラメータの設定

クライアントとサーバーで Oracle 認証方式を使用するためには、次のパラメータが sqlnet.ora 内に存在する必要があります。

```
SQLNET.AUTHENTICATION_SERVICES=(oracle_authentication_method)
```

たとえば、Kerberos 認証を使用するすべてのクライアントとサーバーの sqlnet.ora ファイルで、次のパラメータが設定されている必要があります。

```
SQLNET.AUTHENTICATION_SERVICES=(KERBEROS5)
```

REMOTE_OS_AUTHENT が TRUE に設定されていないことを確認

注意： REMOTE_OS_AUTHENT を TRUE に設定すると、非保護プロトコル（TCP など）を使用するユーザーがオペレーティング・システム許可ログイン（以前の OPS$ ログイン）を実行できるので、セキュリティに欠陥が生じます。

Oracle 認証方式を構成するときは、データベース・インスタンス用の初期化ファイルに、次のパラメータを追加することを強くお薦めします。

```
REMOTE_OS_AUTHENT=FALSE
```

REMOTE_OS_AUTHENT を FALSE に設定した場合に、サーバーがクライアントの要求した認証方式を提供できないと、認証サービスの折衝が失敗して、接続が終了します。

次のパラメータがクライアント側またはサーバー側の sqlnet.ora ファイルで設定されているとします。

```
SQLNET.AUTHENTICATION_SERVICES=(NONE)
```

この場合、データベースはユーザー名とパスワードを使用してユーザーのログインを許可しようとします。しかし、REMOTE_OS_AUTHENT を FALSE に設定してある場合は、接続に失敗します。

OS_AUTHENT_PREFIX を NULL 値に設定

認証サービスでは長いユーザー名を使用できますが、Oracle ユーザー名は 30 文字に制限されています。したがって、データベース・インスタンス用の init.ora ファイルで、OS_AUTHENT_PREFIX パラメータを NULL 値に設定することを強くお薦めします。

```
OS_AUTHENT_PREFIX=""
```

注意： OS_AUTHENT_PREFIX のデフォルト値は OPS$ ですが、このパラメータは任意の文字列に設定できます。

注意： データベースで OS_AUTHENT_PREFIX がすでに NULL（""）以外の値に設定されている場合は、それを変更しないでください。変更すると、外部的に識別される作成済みのユーザーが Oracle Server に接続できなくなります。

ユーザーを作成するには、SQL*Plus を起動し、次のように入力します。

```
SQL> CREATE USER os_authent_prefix username IDENTIFIED EXTERNALLY;
```

OS_AUTHENT_PREFIX が NULL 値（""）に設定されているときは、次のコマンドを使用して「king」ユーザーを作成します。

```
SQL> CREATE USER king IDENTIFIED EXTERNALLY;
```

この方法でユーザーを作成すると、外部的に識別されるユーザーに対して、異なるユーザー名を管理する必要がありません。

注意： この方法は、すべての Oracle 認証方式で使用する Oracle ユーザーを作成する場合に適用されます。

詳細情報： 『Oracle8*i* 管理者ガイド』と『Oracle8*i* 分散システム』を参照してください。

サポートされていない Oracle 製品

Oracle Advanced Security でデータを安全に転送するには、Net8 が必要です。このため、Oracle の統合会計アプリケーション、人事管理アプリケーション、生産管理アプリケーションの一部を Windows プラットフォームで実行するときは、Oracle Advanced Security の認証機能を今のところ使用することができません。これらの製品で Oracle Display Manager

（ODM）を使用する部分は、現在 ODM で Net8 が使用されていないため、Oracle Advanced Security を利用できません。

2

暗号化とチェックサムの構成

この章では、次のトピックについて説明します。

- Oracle Advanced Security での暗号化
- Oracle Advanced Security でのチェックサム
- Diffie-Hellman ベースのキー管理
- 暗号化とチェックサムの構成

Oracle Advanced Security での暗号化

この項では、Oracle Advanced Security の米国内向けバージョンと輸出用バージョンで使用されている各種暗号化アルゴリズムについて説明し比較します。

米国内向けバージョンと輸出用バージョン

暗号化技術に関する輸出制限のため、Oracle Advanced Security には米国内向けバージョンと輸出用バージョンがあります。

米国内向けバージョンに含まれるもの	輸出用バージョンに含まれるもの
Diffie-Hellman キー折衝アルゴリズム	Diffie-Hellman キー折衝アルゴリズム
MD5 メッセージ・ダイジェスト・アルゴリズム	MD5 メッセージ・ダイジェスト・アルゴリズム
次の暗号化アルゴリズム（以下で説明） ■ DES40 ■ DES ■ RC4_40 ■ RC4_56 ■ RC4_128	次の暗号化アルゴリズム（以下で説明） ■ DES40 ■ RC4_40

特定の状況では、56 ビット暗号化バージョンまたは米国内向けバージョンを輸出するのに必要な特別なライセンスを取得できます。通常は、米国企業の完全所有子会社がこのライセンスを取得できます。特別なライセンスは、銀行が輸出用バージョンに DES を組み込むために取得できます。輸出および輸入に関する条例は国によって異なり、時おり変更される場合があるので、各地域における現行の規制を確認する必要があります。

サポートされる暗号化アルゴリズム

この項では、次の暗号化アルゴリズムとその使用方法について説明し比較します。

- DES アルゴリズムによる標準ベースの暗号化
- 国際用途向けに提供された DES40 アルゴリズム
- 非常に安全で高速な RSA RC4 アルゴリズム
- 米国内の顧客が使用できる RC4_56 と RC4_128
- 米国とカナダ以外の顧客が使用できる RC4_40
- Triple-DES を提供する SSL

DES アルゴリズムによる標準ベースの暗号化

米国内向けバージョンの Oracle Advanced Security には、特殊な暗号化を必要とするユーザー用に DES（データ暗号化標準）アルゴリズムが用意されています。DES は長年に渡って米国政府の暗号化標準として利用され、金融業界では利用が義務付けられることもあります。今日の大半の特殊化した銀行システムでは、大規模な国際金融取引を保護するためのアルゴリズムとして DES が使用されています。Oracle Advanced Security では、特別なプログラムを作成しなくても、この高度なセキュリティ・システムを使用してあらゆる種類のアプリケーションを保護することができます。

安全性の高い暗号システムでは、秘密の復号化キーを使用しなければ、暗号文（暗号化されたメッセージ）から平文（暗号化されていないメッセージ）を復元できません。「対称型暗号システム」では、1 つのキーが暗号化キーおよび復号化キーとして機能します。DES はシークレット・キーを使用する対称型暗号システムです。対称型暗号システムでは、メッセージを暗号化および復号化するためのシークレット・キーを、送信側と受信側が認識していなければなりません。DES は世界中で最も有名で広く使用されている暗号システムです。

国際用途向けに提供された DES40 アルゴリズム

全世界で使用できる DES40 アルゴリズムは、シークレット・キーを事前処理して 40 の実効キー・ビットを提供する DES のバージョンです。DES40 は、米国とカナダ以外の地域で DES ベースの暗号化アルゴリズムを使用するユーザーのために設計されました。DES40 によって、貿易関係の顧客は地理的な条件に左右されずにアルゴリズムを選択できるようになりました。

非常に安全で高速な RSA RC4 アルゴリズム

RSA Data Security 社が開発した RC4 アルゴリズムは、データを高速で暗号化するアルゴリズムとして、事実上の国際標準の地位を急速に確立しました。暗号化の研究者は RC4 アルゴリズムを「解読」しようとしていますが、今日までにわかっている唯一の解読方法でも、強引な系統的推測の域を脱していません。このような方法では、通常は暗号を解読できません。RC4 は DES の数倍の速度で動作するストリーム暗号なので、大量のデータ転送でさえもパフォーマンスへの影響を最小限に抑えて暗号化することができます。

米国内の顧客が使用できる RC4_56 と RC4_128

RC4 は可変キー長のストリーム暗号です。米国内向けバージョンの Oracle Advanced Security リリース 8.1.5 は、56 ビット・キーと 128 ビット・キーの RC4 を実装しています。このため、同じアルゴリズムの他のキー長の場合と比べて、パフォーマンスを犠牲にしないで強力な暗号化を実現できます。

米国とカナダ以外の顧客が使用できる RC4_40

オラクル社は、キー・サイズが 40 ビットの RC4 データ暗号化アルゴリズムを、他の Oracle 製品が使用可能なほぼすべての国に輸出するための特殊なライセンスを取得しました。これによって、国際的企業は高速で強力な暗号化を使用して安全にすべての業務を遂行できるようになりました。

Triple-DES を提供する SSL

Oracle Advanced Security の SSL 機能では Triple-DES を使用することができます。この暗号化方式では、入力データは 3 回暗号化され、暗号化はさまざまな方法で実行できます。通信チャネルの速度にもよりますが、Triple-DES の短所としては、通常の DES に比べてコンピュータのパワーを必要とすることです。

詳細情報： 第 9 章の「SSL 認証の構成」を参照してください。

Oracle Advanced Security でのチェックサム

ネットワーク・データの暗号化よってデータのプライバシが守られるので、無許可の人物はネットワーク上で転送中のプレーンテキスト・データを見ることはできません。Oracle Advanced Security では、この他に 2 つのタイプの攻撃（データ変更攻撃と再生攻撃）からデータを保護することもできます。

データ変更攻撃では、ネットワーク上で転送中のデータを無許可の人物が傍受して、そのデータの一部を変更してから再転送します。この種の攻撃の例として、銀行取引データの金額を変更する攻撃があります。

再生攻撃では、有効データの全体がネットワーク上に反復的に送られます。この種の攻撃の例として、有効な銀行口座の転送トランザクションを繰り返す攻撃があります。

Oracle Advanced Security は、キーで順序付けられた MD5 メッセージ・ダイジェスト・アルゴリズムを使用して、これらの攻撃からデータを保護します。この保護機能は暗号化機能とは別に起動されます。

Diffie-Hellman ベースのキー管理

暗号データの秘密は、通信の当事者間で共有されるシークレット・キーの存在に依存しています。このようなシークレット・キーを提供および維持することを、「キー管理」といいます。マルチユーザー環境では、キーを安全に配布するのが困難です。この問題を解決するために、公開鍵による暗号化が開発されました。Oracle Advanced Security は公開鍵に基づく Diffie-Hellman キー折衝アルゴリズムを使用して、暗号化と暗号チェックサムに使用するキーを安全に配布しています。

暗号化を使用して暗号データを保護するときは、キーを頻繁に変更して、キーの安全性が損なわれた場合の影響を最小限に抑える必要があります。このため、Oracle Advanced Security では、キー管理機能によってセッションごとにセッション・キーを変更します。

サイト固有の拡張型 Diffie-Hellman 暗号化の概要

Oracle Advanced Security では、Diffie-Hellman キー折衝アルゴリズムを組み込んで、暗号化と暗号チェックサムの両方で使用するキーを選択します。

キーは接続の両端のみで共有される秘密です。キーがなければ、暗号メッセージを復号化したり、暗号チェックサム・メッセージをわからないように改ざんするのが非常に困難です。

拡張型の認証キー・フォールドイン暗号化の概要

拡張型の認証キー・フォールドイン暗号化を使用する目的は、Diffie-Hellman キー折衝に対する「第 3 者の攻撃」を打ち破ることです。この暗号化では、共有シークレット（クライアントとサーバーの両者のみが認識している秘密）を、Diffie-Hellman によって折衝される最初のセッション・キーと組み合せることによって、セッション・キーの安全性を大幅に強化しています。

クライアントとサーバーは、Diffie-Hellman によって生成されるセッション・キーを使用して通信を開始します。クライアントサーバーに対してが自己識別した時点で、その両者のみが認識できる共有シークレットが生成されます。Oracle Advanced Security は、共有シークレットと Diffie-Hellman セッション・キーを組み合せて、より強力なセッション・キーを生成します。このセッション・キーは、共有シークレットを知らない第 3 者の攻撃を排除します。

構成を必要としない認証キー・フォールドイン機能

拡張型の認証キー・フォールドイン暗号化機能は、Oracle Advanced Security に含まれているので、システム管理者またはネットワーク管理者による構成作業は必要ありません。

暗号化とチェックサムの構成

構成の説明は、Net8 ネットワーク・ソフトウェアがインストール済みで稼働していることを想定しています。

ネットワーク管理者は、暗号化とチェックサムの構成パラメータを設定する必要があります。

暗号化とチェックサムを使用するクライアントとサーバー上のプロファイル（sqlnet.ora）には、次項以降で説明するパラメータの一部またはすべてが含まれていなければなりません。

暗号化とチェックサムをアクティブにする方法

すべてのネットワーク接続で、接続の両端（クライアントとサーバー）が複数の暗号化アルゴリズムと複数の暗号チェックサム・アルゴリズムをサポートできます。接続が確立されるときに、sqlnet.ora ファイルで指定されているアルゴリズムに基づいて、サーバーがどのアルゴリズムを使用するかを決定します。

サーバーは、サーバー自身が使用可能にしたアルゴリズムと、クライアントが使用可能にしたアルゴリズムの間で一致するアルゴリズムを探すときに、サーバー自身のリストとクライアントのリストの両方に含まれるアルゴリズムの中で最初のアルゴリズムを選択します。接続の片側がアルゴリズムのリストを指定してない場合は、そちら側にインストールされているすべてのアルゴリズムが使用可能になります。

暗号化パラメータとチェックサム・パラメータを定義するには、ネットワーク上のクライアントとサーバーの sqlnet.ora ファイルを変更します。

詳細情報： 付録 A の「暗号化パラメータとチェックサム・パラメータ」を参照してください。

暗号化とチェックサムの折衝

暗号化またはチェックサムをアクティブにするかどうかを折衝するには、Oracle Advanced Security の 4 つの構成パラメータに対して次に説明する 4 つの値を指定します。

- ACCEPTED
- REJECTED
- REQUESTED
- REQUIRED

これらの 4 つのパラメータのデフォルト値は ACCEPTED です。

ACCEPTED

接続先が希望する場合にセキュリティ・サービスをオンにします。

接続元がセキュリティ・サービスを希望しなくても、接続先が REQUIRED または REQUESTED でセキュリティ・サービスを要求すると、セキュリティ・サービスが使用できます。接続先のパラメータが REQUIRED または REQUESTED に設定されていて、一致するアルゴリズムが見つかると、エラーは発生しないで、セキュリティ・サービスがオンのまま接続が継続されます。接続先のパラメータが REQUIRED に設定されていて、一致するアルゴリズムが見つからないと、エラー・メッセージ ORA-12650 で接続が終了します。

接続先が REQUESTED に設定されていて、一致するアルゴリズムが見つからない場合、または接続先が ACCEPTED または REJECTED に設定されている場合は、エラーは発生しないで、セキュリティ・サービスがオフのまま接続が継続されます。

REJECTED

接続先が希望してもセキュリティ・サービスをオンにしません。

接続元がセキュリティ・サービスの使用禁止を指定します。接続先が REQUIRED を指定すると、エラー・メッセージ ORA-12650 で接続が終了します。接続先のパラメータが REQUESTED または ACCEPTED、REJECTED に設定されている場合は、エラーが発生しないで、セキュリティ・サービスが使用禁止のまま接続が継続されます。

REQUESTED

接続先がセキュリティ・サービスを使用可能に設定してある場合に、セキュリティ・サービスをオンにします。

接続元の指定では、セキュリティ・サービスを希望するけれど、そのサービスは必須ではありません。接続先が ACCEPTED または REQUESTED、REQUIRED を指定すると、セキュリティ・サービスがオンになります。接続先が使用可能にしたアルゴリズムと一致するアルゴリズムが見つからないと、セキュリティ・サービスがオンになりません。

接続先が REQUIRED を指定して、一致するアルゴリズムが見つからない場合は、接続が失敗します。

REQUIRED

セキュリティ・サービスをオンにするか、接続を確立しません。

接続元がセキュリティ・サービスをアクティブにすると指定します。接続先が REJECTED を指定した場合、または接続先と互換性のあるアルゴリズムが見つからない場合は、接続が失敗します。

次の表に、クライアントとサーバーの構成パラメータの組合せに応じて、セキュリティ・サービスがオンになるかどうかを示します。サーバーまたはクライアントが REQUIRED を指定した場合は、共通のアルゴリズムが存在しないと接続が失敗します。サーバーもクライアントも REQUIRED を指定しないで、セキュリティ・サービスがオンになっている場合は、共通のサービス・アルゴリズムが存在しないとサービスがオフになります。

クライアント

サーバー	Accepted	Rejected	Requested	Required
Accepted	OFF	OFF	ON	ON
Rejected	OFF	OFF	OFF	接続が失敗する
Requested	ON	OFF	ON	ON
Required	ON	接続が失敗する	ON	ON

暗号化パラメータとチェックサム・パラメータの設定

詳細情報： 各パラメータの説明と暗号化とチェックサムを使用したサンプル構成ファイルの説明は、付録 A の「暗号化パラメータとチェックサム・パラメータ」を参照してください。

構成の詳細は、Oracle Net8 Assistant ヘルプ・システムを参照してください。

暗号化パラメータまたはチェックサム・パラメータの設定を入力または変更するには、テキスト・エディタで sqlnet.ora ファイルを変更するか、Oracle Net8 Assistant を使用します。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ー *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

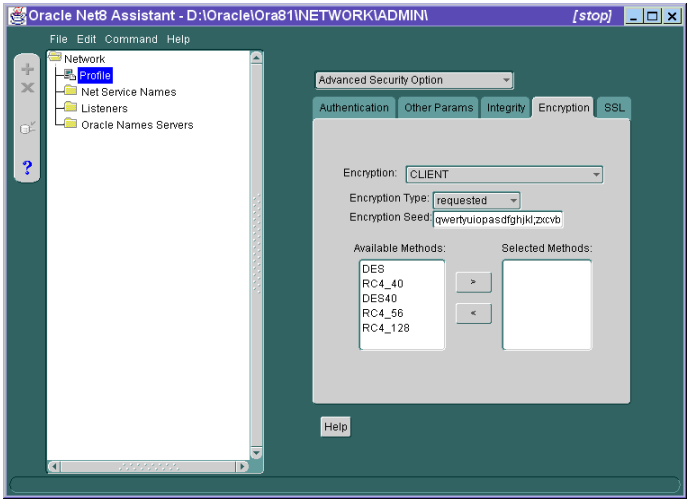
Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

クライアントとサーバーでの暗号化の構成

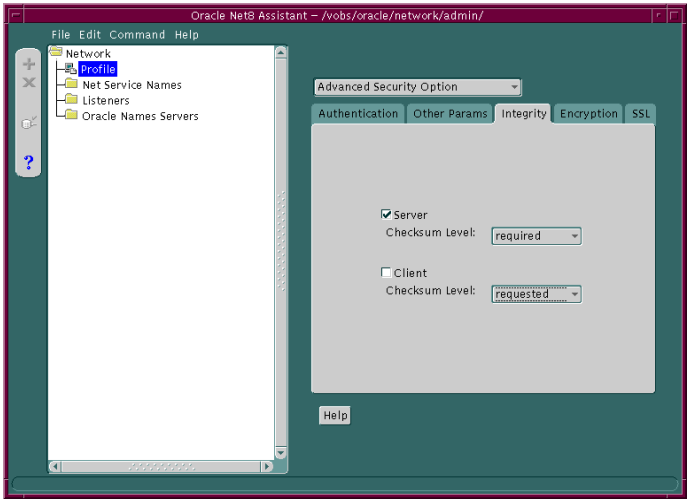
図 2-1 Oracle Net8 Assistant を使用した暗号化の設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
2-10 ページの図 2-1 を参照してください。 **1.** 「Encryption」タブを選択します。 **2.** 構成中のマシンに従って、「Encryption」リストの「CLIENT」または「SERVER」を選択してください。 **3.** 「Encryption Type」リストで「REQUESTED」、「REQUIRED」、「ACCEPTED」、「REJECTED」のいずれかを選択します。 **4.** 「Encryption Seed」ボックスで、10 ～ 70 文字の文字をランダムに入力します。 **注意 :** クライアントの暗号化シードはサーバーの暗号化シードとは別のものにします。 **5.** 「Available Methods」リストで暗号化メソッドを選択します。次に、右矢印ボタン「>」をクリックして「Selected Methods」リストに移動します。追加するメソッドすべてに対して同じ作業を繰り返します。	サーバー上で次のパラメータを設定します。 SQLNET.ENCRYPTION_SERVER = [*accepted* | *rejected* | *requested* | *required*] SQLNET.ENCRYPTION_TYPES_SERVER = (*valid_encryption_algorithm* [,*valid_encryption_algorithm*]) SQLNET.CRYPTO_SEED = "10 ～ 70 文字のランダム文字 " **注意 :** サーバーの暗号化シードはクライアントの暗号化シードとは別のものにします。 クライアント上で次のパラメータを設定します。 SQLNET.ENCRYPTION_CLIENT = [*accepted* | *rejected* | *requested* | *required*] SQLNET.ENCRYPTION_TYPES_CLIENT = (*valid_encryption_algorithm* [,*valid_encryption_algorithm*]) SQLNET.CRYPTO_SEED = "10 ～ 70 文字のランダム文字 " **注意 :** クライアントの暗号化シードはサーバーの暗号化シードとは別のものにします。 **有効な暗号化アルゴリズム :** A-3 ページの「暗号化パラメータとチェックサム・パラメータ」を参照してください。

クライアントとサーバーでのチェックサムの構成

図 2-2 Oracle Net8 Assistant を使用したチェックサムの設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 2-2 を参照してください。 1. 「Integrity」タブを選択します。 2. 「Server」ラジオ・ボタンを選択してサーバーのチェックサムを構成します。 3. 「Checksum Level」ドロップダウン・リスト・ボックスをクリックして、サーバーのチェックサム・レベルを指定する 4 つの値（REQUIRED、REQUESTED、ACCEPTED、REJECTED）のいずれか 1 つを選択します。 4. 「Client」ラジオ・ボタンを選択してクライアントのチェックサムを構成します。 5. 「Client Checksum Level」ドロップダウン・リスト・ボックスをクリックして、クライアントのチェックサム・レベルを指定する 4 つの値（REQUIRED、REQUESTED、ACCEPTED、REJECTED）のいずれか 1 つを選択します。	サーバー上で次のパラメータを設定します。 SQLNET.CRYPTO_CHECKSUM_SERVER = [*accepted* | *rejected* | *requested* | *required*] SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (*crypto_checksum_algorithm*) クライアント上で次のパラメータを設定します。 SQLNET.CRYPTO_CHECKSUM_CLIENT = [*accepted* | *rejected* | *requested* | *required*] SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (*crypto_checksum_algorithm*) **注意 :** 現行のリリースでは、RSA Data Security の MD5 アルゴリズムのみが暗号チェックサム・アルゴリズムとしてサポートされています。

3

RADIUS 認証の構成

この章では、RADIUS（Remote Authentication Dial-In User Service）を使用する Oracle8*i* の構成方法について説明します。

この章では、次のトピックについて説明します。

RADIUS の概要

RADIUS（Remote Authentication Dial-In User Service）はクライアント / サーバー・セキュリティ・プロトコルであり、リモート認証とリモート・アクセスを実現するものとして、もっとも広く知られています。Oracle Advanced Security では、この新生の標準をクライアント / サーバー・ネットワーク環境で使用しています。

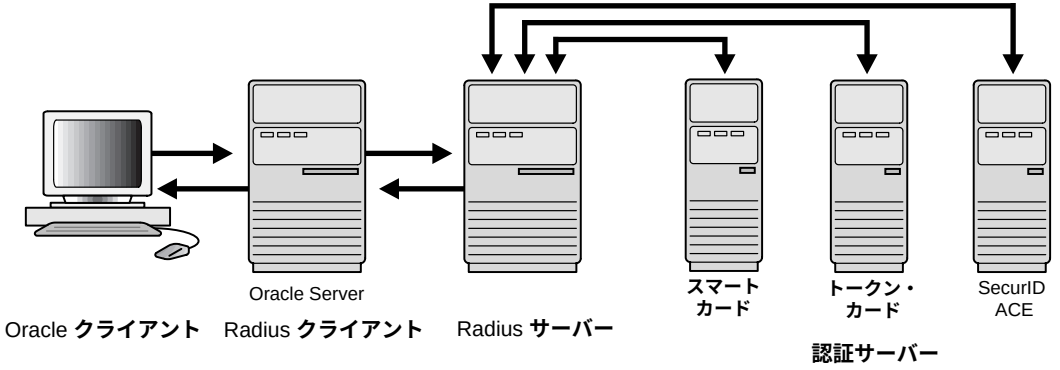
トークン・カードやスマートカードなど、RADIUS 標準をサポートする認証方式をネットワークで使用できるようにするには、RADIUS アダプタをインストールして構成するのみです。さらに、RADIUS を使用すると、Oracle クライアントまたは Oracle Server を変更することなく、認証方式を変更できます。

ユーザーの立場で見ると、認証プロセス全体が連続して透過的に行われます。ユーザーが Oracle Server へのアクセスを要求すると、RADIUS クライアントとして動作する Oracle Server が RADIUS サーバーに通知します。RADIUS サーバーは次のように動作します。

- ユーザーのセキュリティ情報を検索する
- 適切な認証サーバーと Oracle Server の間で認証と認可情報を渡す
- ユーザーのログオンの時間、頻度、接続時間などの情報を RADIUS アカウント機能によってログに記録する

Oracle 環境での RADIUS

図 3-1 Oracle 環境での RADIUS



Oracle 環境（図 3-1）では、Oracle Server は RADIUS クライアントとして動作し、Oracle クライアントと RADIUS サーバーの間で情報を渡します。同様に、RADIUS サーバーは Oracle Server と適切な認証サーバーの間で情報を渡します。転送中の認証情報を保護するため、RADIUS ではこの情報をハッシュ値に変換します。

Oracle クライアント、Oracle Server/RADIUS クライアント、RADIUS サーバー、認証サーバーの 4 つの構成要素は、同じマシンにおくことも、別のマシンにおくこともできます。Oracle クライアントと Oracle Server が同じマシンにある場合、同じ sqlnet.ora ファイルが共有されます。

> **詳細情報：** sqlnet.ora ファイルの詳細は、『Oracle8*i* Net8 管理者ガイド』を参照してください。

次の表に、各構成要素と、構成要素に格納される情報を示します。

構成要素	格納される情報
Oracle クライアント	RADIUS による通信の構成設定
Oracle Server/ RADIUS クライアント	Oracle クライアントと RADIUS サーバーの間で情報を渡すための構成設定 シークレット・キー・ファイル
RADIUS サーバー	全ユーザーの認証と認可情報 各クライアントの名前または IP アドレス 各クライアントの共有シークレット すでに認証されているユーザーが再接続せずに別のログイン・オプションを選択できる数無制限のメニュー・ファイル
認証サーバー	パスコードや PIN など、使用中の認証方式に対応するユーザー認証情報

RADIUS 認証モード

ユーザー認証には次の 2 通りあります。

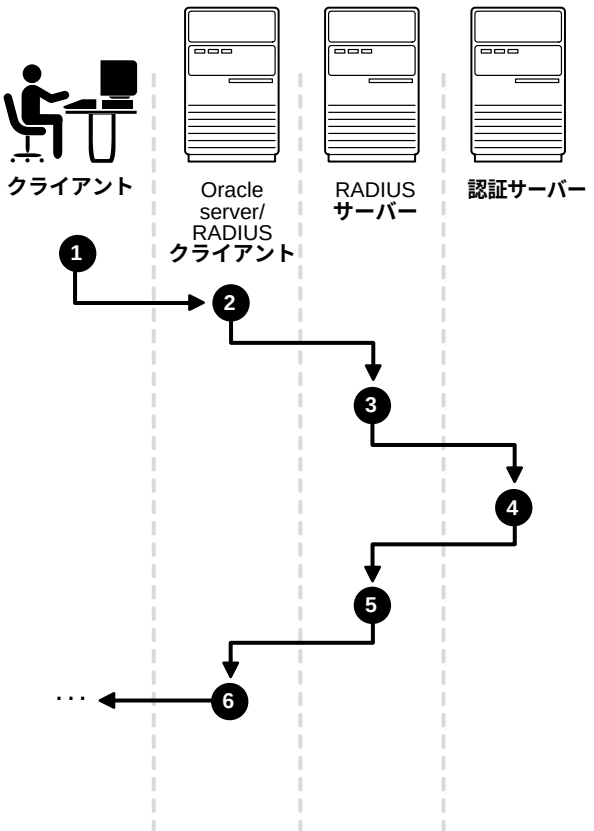
- 同期認証モード
- 要求 - 応答（非同期）認証モード

同期認証モード

同期モードの RADIUS では、パスワード、SecurID トークン・カード、スマートカードなど、各種の認証方式を使用することができます。

図 3-2 に、同期認証モードのシーケンスを示します。

図 3-2 同期認証シーケンス



1. ユーザーは接続文字列、パスコード、またはその他の値を入力してログインします。クライアント・マシンは、このデータを Oracle Server に渡します。
2. RADIUS クライアントとして動作している Oracle Server は、Oracle クライアントからのデータを RADIUS サーバーに渡します。
3. RADIUS サーバーはデータを検証するため、適切な認証サーバー（スマートカード、SecurID ACE、ActivCard など）に渡します。
4. 認証サーバーはアクセス受け入れメッセージまたはアクセス拒否メッセージを RADIUS サーバーに返します。
5. RADIUS サーバーは、この応答を Oracle Server/RADIUS クライアントに渡します。
6. Oracle Server/RADIUS クライアントは、この応答を Oracle クライアントに渡します。

例 : SecurID トークン・カードによる同期認証

SecurID 認証では、各ユーザーがトークン・カードを持ち、カードに表示される動的番号は 60 秒ごとに変わります。ユーザーが Oracle Server/RADIUS クライアントへのアクセスを得るには、パスコードとして、個人の識別番号（PIN）と SecurID カードに現在表示されている動的番号を入力します。Oracle Server/RADIUS クライアントは、この認証情報を Oracle クライアントから RADIUS サーバーに渡します。次に、RADIUS サーバーが、認証情報を検証するため、認証サーバーに渡します。認証サーバー（Security Dynamics ACE/Server）によってユーザーが確認されると、「受け入れ」パケットが RADIUS サーバーに送られます。この情報は RADIUS サーバーから Oracle Server/RADIUS クライアントに渡り、次に、Oracle クライアントに渡ります。これでユーザーが認可され、適切な表やアプリケーションにアクセスできるようになります。

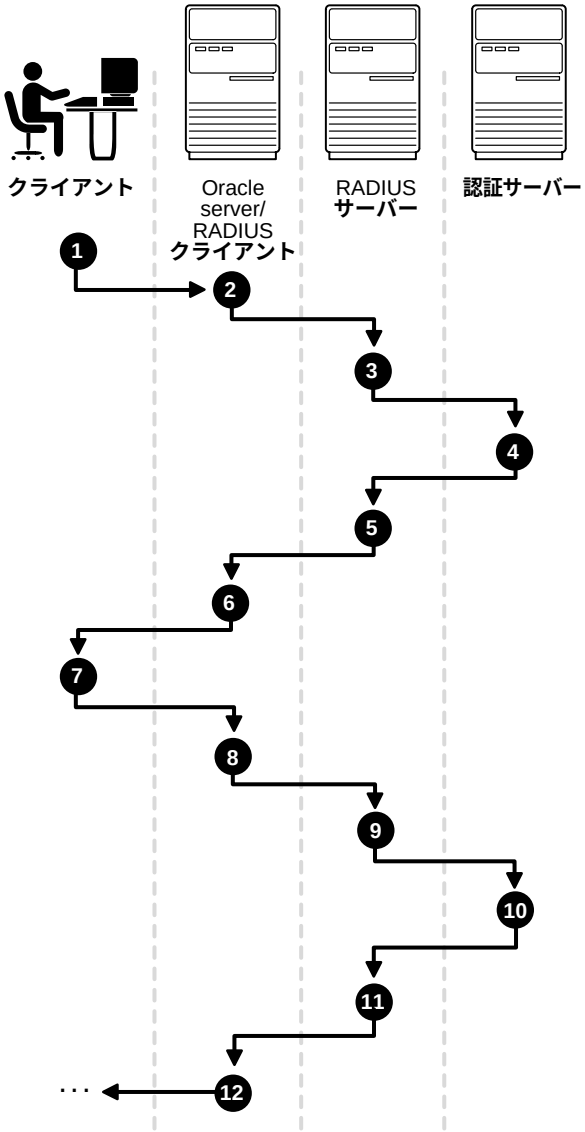
詳細情報 : SecurID トークン・カードの詳細は、1-6 ページの「サポートされる認証方式」と第 6 章の「SecurID 認証の構成」を参照してください。SecurID ベンダーから提供されるマニュアルも参照してください。

要求 - 応答（非同期）認証モード

図 3-3 に、要求 - 応答、非同期認証のシーケンスを示します。

注意 : システムで非同期モードを使用している場合は、ユーザーは SQL*Plus CONNECT 文字列でユーザー名とパスワードを入力する必要がありません。そのかわりに、プロセスの後半で、グラフィカル・ユーザー・インタフェースを使用して入力します。

図 3-3 非同期認証シーケンス



1. ユーザーは Oracle Server への接続を要求します。クライアント・マシンは、このデータを Oracle Server に渡します。
2. RADIUS クライアントとして動作している Oracle Server は、Oracle クライアントからのデータを RADIUS サーバーに渡します。
3. RADIUS サーバーは、適切な認証サーバー（スマートカード、SecurID ACE、ActivCard など）に渡します。
4. 認証サーバーはランダム番号などの要求を RADIUS サーバーに返します。
5. RADIUS サーバーは、この要求を Oracle Server/RADIUS クライアントに送ります。
6. Oracle Server/RADIUS クライアントは、この要求を Oracle クライアントに送ります。グラフィカル・インタフェースを使用してユーザーに要求が表示されます。
7. ユーザーは要求に対する応答を入力します。たとえば、ユーザーが受信した要求をトークン・カードに入力して応答を作ります。次に、トークン・カードによって動的パスワードが生成され、ユーザーはその動的パスワードをグラフィカル・インタフェースに入力します。Oracle クライアントは、ユーザーの応答を Oracle Server/RADIUS クライアントに渡します。
8. 次に、RADIUS クライアントが、ユーザーの応答を RADIUS サーバーに送ります。
9. RADIUS サーバーは、ユーザーの応答を検証するため、適切な認証サーバーに渡します。
10. 認証サーバーはアクセス受け入れメッセージまたはアクセス拒否メッセージを RADIUS サーバーに返します。
11. RADIUS サーバーは、この応答を Oracle Server/RADIUS クライアントに渡します。
12. Oracle Server/RADIUS クライアントは、この応答を Oracle クライアントに渡します。

例 : スマートカードによる非同期認証

スマートカード認証では、ユーザーはスマートカード（情報格納用の IC が組み込まれたクレジットカードに似たプラスティック製のカード）をカード読取り用のハードウェア・デバイスに挿入してログインします。Oracle クライアントは、スマートカードに格納されているログイン情報を、Oracle Server/RADIUS クライアントと RADIUS サーバーを経由して認証サーバーに送ります。認証サーバーは、RADIUS サーバーと Oracle Server/RADIUS クライアントを経由して、要求を返送し、ユーザーに認証情報を入力するよう指示します。この認証情報には、PIN やスマートカードに格納されている他の認証情報を使用することができます。

Oracle クライアントは、Oracle Server/RADIUS クライアントと RADIUS サーバーを経由して、ユーザーの応答を認証サーバーに送ります。ユーザーが入力した番号が有効であれば、認証サーバーは RADIUS サーバーと Oracle Server/RADIUS クライアントを経由して、「受け入れ」パケットを Oracle クライアントに返します。これでユーザーが認証され、適切な表やアプリケーションへのアクセスが認可されます。ユーザーが入力した情報が正しくない場合は、認証サーバーはユーザーのアクセスを拒否するメッセージを返します。

例 : ActivCard トークンによる非同期認証

ActivCard トークンの 1 つに、キーパッドを装備した、動的パスワードを表示できる携帯式のデバイスがあります。Oracle Server へのアクセスを要求するため、ユーザーはパスワードを入力し、その情報は Oracle Server/RADIUS クライアントと RADIUS サーバーを経由して、適切な認証サーバーに渡ります。認証サーバーは、RADIUS サーバーと Oracle Server/RADIUS クライアントを経由して、要求を返します。ユーザーが要求をトークンに入力すると、ユーザーが応答として返送する番号がトークンに表示されます。

Oracle クライアントは、Oracle Server/RADIUS クライアントと RADIUS サーバーを経由して、ユーザーの応答を認証サーバーに送ります。ユーザーが入力した番号が有効であれば、認証サーバーは RADIUS サーバーと Oracle Server/RADIUS クライアントを経由して、「受け入れ」パケットを Oracle クライアントに返します。これでユーザーが認証され、適切な表やアプリケーションへのアクセスが認可されます。ユーザーが入力した応答が正しくない場合は、認証サーバーはユーザーのアクセスを拒否するメッセージを返します。

RADIUS 認証とアカウントの使用

RADIUS 認証とアカウントを使用可能にするには、次の作業を行います。各作業については以下で説明しています。

手順 1: Oracle Server と Oracle クライアントへの RADIUS のインストール

Oracle8*i* の標準インストレーションでは、Oracle Advanced Security とともに RADIUS アダプタもインストールされます。

> **詳細情報：** Oracle Advanced Security と RADIUS アダプタのインストールについては、Oracle8*i* のプラットフォーム固有のインストレーション・マニュアルを参照してください。

手順 2: RADIUS 認証の構成

この項では、次のトピックについて説明します。

- Oracle クライアントでの RADIUS 基本構成－ Oracle クライアント用の最小構成設定。
- Oracle Server での RADIUS 基本構成－ Oracle Server 用の最小構成設定。
- その他の RADIUS 機能の構成－ RADIUS を強化する各種機能の構成設定。次のパラメータを設定できます。
  - プライマリ RADIUS サーバーのリスニング・ポート
  - プライマリ RADIUS サーバーに対する Oracle Server の応答待ち時間
  - プライマリ RADIUS サーバーに対する Oracle Server のメッセージ再送回数
  - 要求 - 応答の使用可能 / 使用禁止の切り替え
  - Oracle Server 上のシークレット・キーの場所
  - 代替 RADIUS サーバー

特に示されていない限り、これらの構成作業を行うには、Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して sqlnet.ora ファイルを変更します。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ー *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

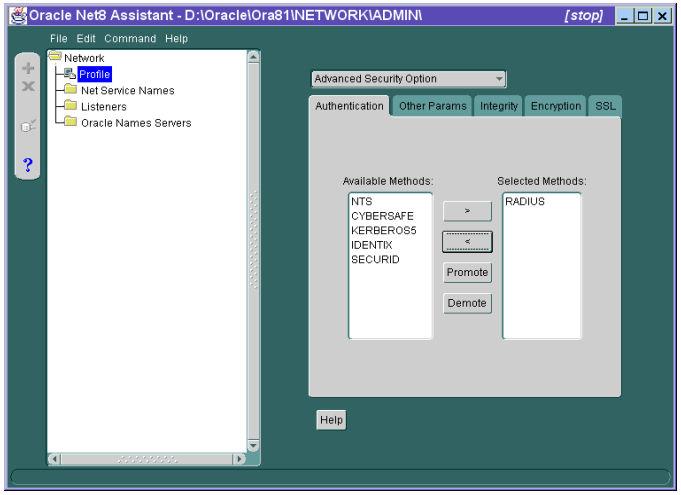
Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

Oracle クライアントでの RADIUS 基本構成

SQLNET.AUTHENTICATION_SERVICES パラメータを設定します。

図 3-4 Oracle Net8 Assistant を使用した認証サービス・パラメータの設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-4 を参照してください。 1. 「Authentication」タブを選択します。 2. 「Available Methods」リストで、「RADIUS」を選択します。 3. 次に、右矢印ボタン「>」をクリックして、「RADIUS」を「Selected Methods」リストに移動します。他に使用するメソッドがあれば同じ方法で移動します。 4. 選択したメソッドを使用優先順位の高い順に並べます。「Selected Methods」リストでメソッドを選択し、「Promote」または「Demote」をクリックして並べ替えます。たとえば、最初に使用するサービスを RADIUS にするには、リストの先頭に移動します。	次のパラメータを設定します。 SQLNET.AUTHENTICATION_SERVICES=(*RADIUS*)

Oracle Server での RADIUS 基本構成

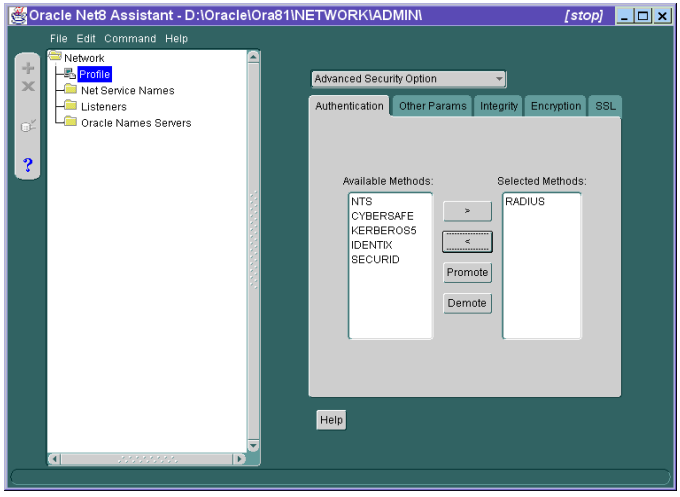
次の作業を行います。各作業については以下で説明しています。

- 認証サービス・パラメータの設定
- プライマリ RADIUS サーバー・ホスト名パラメータの設定
- Oracle Server 初期化パラメータの設定
- SQLNET.ORA への classpath パラメータの追加

認証サービス・パラメータの設定

認証メソッドは SQLNET.AUTHENTICATION_SERVICES パラメータで設定します。

図 3-5 Oracle Net8 Assistant を使用した認証サービス・パラメータの設定

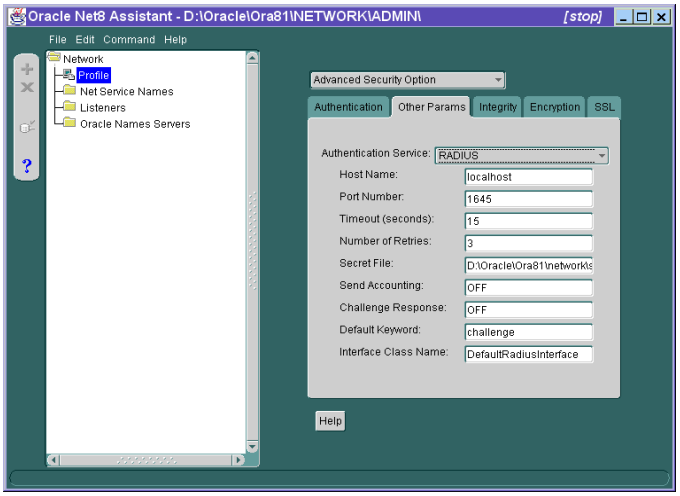


Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-5 を参照してください。 1. 「Authentication」タブを選択します。 2. 「Available Methods」リストで、「RADIUS」を選択します。 3. 次に、右矢印ボタン「>」をクリックして、「RADIUS」を「Selected Methods」リストに移動します。 4. 選択したメソッドを使用優先順位の高い順に並べます。「Selected Methods」リストでメソッドを選択し、「Promote」または「Demote」をクリックして並べ替えます。たとえば、最初に使用するサービスを RADIUS にするには、リストの先頭に移動します。	次のパラメータを設定します。 SQLNET.AUTHENTICATION_SERVICES=(*RADIUS*)

プライマリ RADIUS サーバー・ホスト名パラメータの設定

プライマリ RADIUS サーバーの場所は SQLNET.RADIUS_AUTHENTICATION パラメータで設定します。デフォルトはローカル・ホストです。

図 3-6 Oracle Net8 Assistant を使用したプライマリ RADIUS サーバー・ホスト名パラメータの設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-6 を参照してください。 1. 「Other Params」タブをクリックします。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. 「Host Name」ボックスのデフォルトは localhost です。このデフォルトをそのまま使用するか、プライマリ RADIUS サーバーのホスト名を入力します。	次のパラメータを設定します。 SQLNET.RADIUS_AUTHENTICATION= (RADIUS サーバーのホスト名または IP アドレス)

Oracle Server 初期化パラメータの設定

ディレクトリ $ORACLE_BASE¥ADMIN¥DB_NAME¥PFILE にあるファイル init<*sid*>.ora を構成します。このファイルで、次の値を指定します。

```
REMOTE_OS_AUTHENT=FALSE
OS_AUTHENT_PREFIX=""
```

注意： REMOTE_OS_AUTHENT を TRUE に設定すると、非保護プロトコル（TCP など）を使用するユーザーがオペレーティング・システム許可ログイン（以前の OPS$ ログイン）を実行できるので、セキュリティに欠陥が生じます。

詳細情報： Oracle Server での初期化パラメータ設定の詳細は、『Oracle8*i* リファレンス・マニュアル』と『Oracle8*i* 管理者ガイド』を参照してください。

SQLNET.ORA への classpath パラメータの追加

要求 - 応答認証モードを使用する場合、RADIUS では Java ベースのグラフィカル・インタフェースを表示してパスワードを最初に要求し、ユーザーがトークン・カードから取得する動的パスワードなど、他の追加情報を要求します。そのグラフィカル・インタフェースの Java クラスのパスを設定するには、sqlnet.ora ファイルに SQLNET.RADIUS_CLASSPATH パラメータを追加します。

テキスト・エディタを使用して、次のパラメータを sqlnet.ora ファイルに追加します。

```
SQLNET.RADIUS_CLASSPATH=path/netradius.jar:path/ewt-opt-3_1_8_1.zip
```

たとえば、次のとおりです。

```
SQLNET.RADIUS_CLASSPATH=/ohome/network_src/jlib/
                        netradius.jar:/ohome/network_src/jlib
                        /ewt-opt-3_1_8_1.zip
```

その他の RADIUS 機能の構成

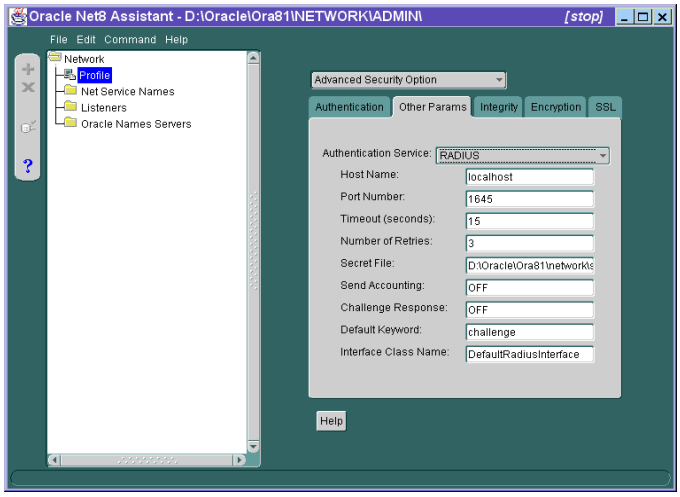
次の RADIUS 機能を構成するには、Oracle Net8 Assistant を使用するか、sqlnet.ora ファイルを変更します。

- プライマリ RADIUS サーバーのリスニング・ポートの設定
- プライマリ RADIUS サーバーに対する Oracle Server の応答待ち時間の設定
- プライマリ RADIUS サーバーに対する Oracle Server のメッセージ再送回数の設定
- 要求 - 応答の構成
- Oracle Server 上のシークレット・キーの場所の設定
- 代替 RADIUS サーバーのパラメータの設定

プライマリ RADIUS サーバーのリスニング・ポートの設定

SQLNET.RADIUS_AUTHENTICATION_PORT パラメータを設定します。デフォルトは 1645 です。

図 3-7 Oracle Net8 Assistant を使用したプライマリ RADIUS サーバーのリスニング・ポートの設定

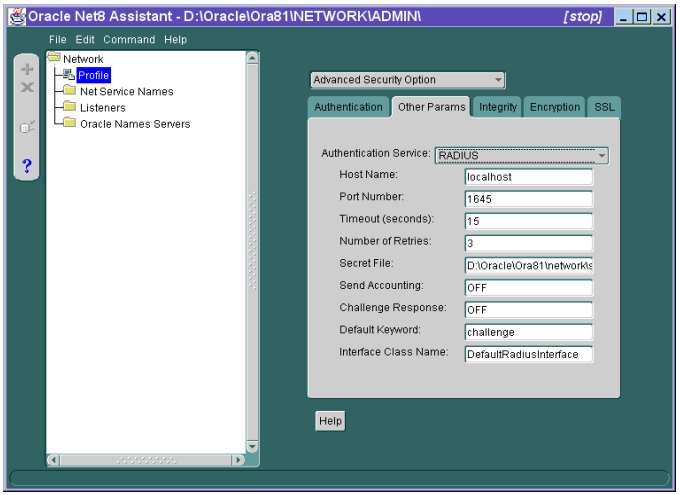


Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-7 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. 「Port Number」ボックスのデフォルトは 1645 です。このデフォルトをそのまま使用するか、プライマリ RADIUS サーバーのリスニング・ポート番号を入力します。	次のパラメータを設定します。 SQLNET.RADIUS_AUTHENTICATION_PORT=(*1645*)

プライマリ RADIUS サーバーに対する Oracle Server の応答待ち時間の設定

SQLNET.RADIUS_AUTHENTICATION_TIMEOUT パラメータを設定します。

図 3-8 Oracle Net8 Assistant を使用したプライマリ RADIUS サーバーに対する Oracle Server の応答待ち時間の構成

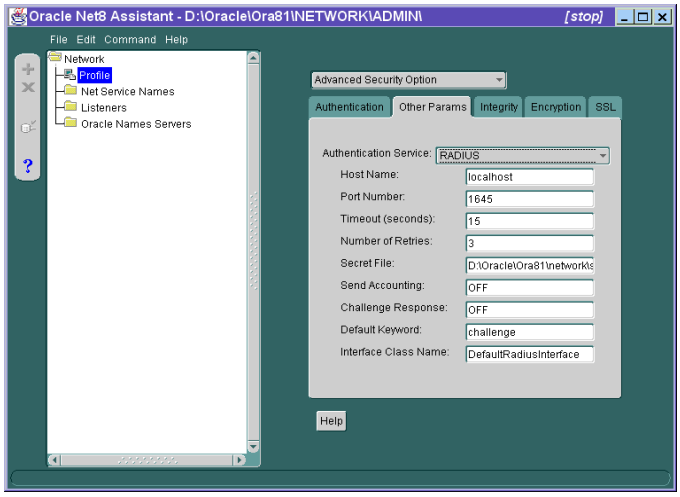


Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-8 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. 「Timeout（seconds）」ボックスのデフォルトは 15 秒です。このデフォルトをそのまま使用するか、プライマリ RADIUS サーバーに対する Oracle Server の応答待ち時間を秒単位で入力します。	次のパラメータを設定します。 SQLNET.RADIUS_AUTHENTICATION_TIMEOUT=(応答待ち時間（秒単位）)

プライマリ RADIUS サーバーに対する Oracle Server のメッセージ再送回数の設定

SQLNET.RADIUS_AUTHENTICATION_RETRIES パラメータを設定します。デフォルトは 3 です。

図 3-9 Oracle Net8 Assistant を使用したプライマリ RADIUS サーバーに対する Oracle Server のメッセージ再送回数の設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-9 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. 「Number of Retries」ボックスのデフォルトは 3 です。このデフォルトをそのまま使用するか、プライマリ RADIUS サーバーに対する Oracle Server のメッセージ再送回数を入力します。	次のパラメータを設定します。 SQLNET.RADIUS_AUTHENTICATION_RETRIES=(RADIUS サーバーへの再送回数)

詳細情報： RADIUS アカウントの構成の詳細は、3-27 ページの「手順 5: RADIUS アカウントの構成」を参照してください。

Oracle Server 上のシークレット・キーの場所の設定

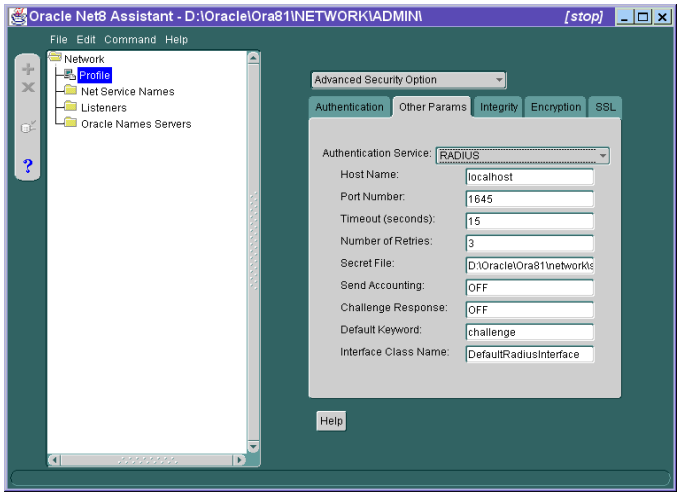
SQLNET.RADIUS_SECRET パラメータを設定します。

注意： このパラメータはシークレット・キーの場所を設定します。シークレット・キーそのものを指定するものではありません。

詳細情報： シークレット・キーの指定の詳細は、3-30 ページの「手順 9: Oracle Server での RADIUS シークレット・キーの指定」を参照してください。

注意： 安全上の理由により、このファイルをルート・アクセスのみに変更することをお薦めします。

図 3-10 Oracle Net8 Assistant を使用した Oracle Server 上のシークレット・キーの場所の設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-10 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. 「Secret File」ボックスにシークレット・キー・ファイルのパス名を入力します。	次のパラメータを設定します。 SQLNET.RADIUS_SECRET=(パス /RADIUS.KEY)

要求 - 応答の構成

要求 - 応答（非同期）モードでは、グラフィカル・インタフェースを表示してパスワードを最初に要求し、ユーザーがトークン・カードから取得する動的パスワードなど、他の追加情報を要求します。RADIUS アダプタを使用している場合は、Java ベースによるプラットフォームに適したインタフェースが使用されます。

注意： 認証デバイスのサードパーティ・ベンダーは、そのデバイスに適したグラフィカル・ユーザー・インタフェースにカスタマイズする必要があります。たとえば、スマートカードのベンダーは、Oracle クライアントがスマートカードから動的パスワードなどのデータを読み取ることができるように、Java インタフェースをカスタマイズする必要があります。次に、スマートカードが要求を受け取ると、PIN などの追加情報をユーザーに入力させて応答します。

詳細情報： 要求 - 応答ユーザー・インタフェースのカスタマイズの方法は、付録 C の「RADIUS による認証デバイスの統合」を参照してください。

要求 - 応答を構成するには、次の作業を行います。各作業は以下で説明しています。

- 環境変数 JAVA_HOME の設定
- 設定パラメータの設定

環境変数 JAVA_HOME の設定　この環境変数を使用して、Oracle クライアントを実行するシステムの JRE または JDK のある場所を設定します。

UNIX の場合

コマンド・プロンプトで、次のように入力します。

```
Unix% setenv JAVA_HOME /usr/local/packages/jre1.1.7B
```

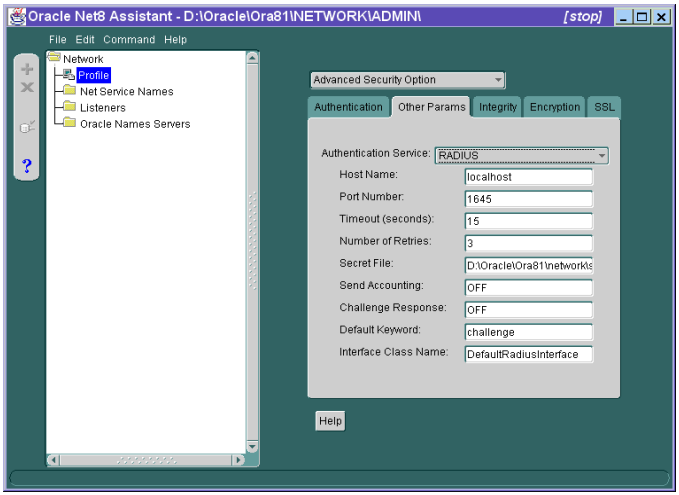
Windows NT の場合

1. 「スタート」ボタン ->「設定」->「コントロール パネル」->「システム」->「環境」の順にクリックします。
2. 変数 JAVA_HOME に c:¥java¥jre1.1.7B を設定します。

設定パラメータの設定　以下の説明に従って、sqlnet.ora ファイルに次の 3 つのパラメータを設定します。

- SQLNET.RADIUS_CHALLENGE_RESPONSE
- SQLNET.RADIUS_CHALLENGE_KEYWORD
- SQLNET.RADIUS_AUTHENTICATION_INTERFACE

図 3-11 Oracle Net8 Assistant を使用した要求 - 応答の構成



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-11 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. 「Challenge Response」ボックスのデフォルトは OFF です。このデフォルトをそのまま使用するか、要求 - 応答を使用可能にする場合は ON を入力します。 4. 「Default Keyword」[1] ボックスのデフォルトは challenge です。このデフォルトをそのまま使用するか、RADIUS サーバーから要求を求める場合はキーワードを入力します。 5. 「Interface Class Name」ボックスのデフォルトは DefaultRadiusInterface です。このデフォルトをそのまま使用するか、Oracle クライアントと RADIUS サーバ間の要求 - 応答変換を処理するために作成したクラスの名前を入力します。	次のパラメータを設定します。 SQLNET.RADIUS_CHALLENGE_RESPONSE=([*ON* | *OFF*]) SQLNET.RADIUS_CHALLENGE_KEYWORD=(*KEYWORD*) SQLNET.RADIUS_AUTHENTICATION_INTERFACE=(package_name にピリオド（.）ではなくスラッシュ（/）を続け、radius_interface_name を続ける) たとえば、次のとおりです。 SQLNET.RADIUS_AUTHENTICATION_INTERFACE=vendor/net/ActivCardRadiusInterface

[1] キーワード機能は Oracle が提供するもので、すべての RADIUS サーバーでサポートされているとは限りません。この機能は、RADIUS サーバーでサポートされている場合にのみ使用することができます。

キーワードを設定すると、ユーザーはパスワードを使用せずに識別情報を検証されるようになります。ユーザーがパスワードを入力しなかった場合は、ここで設定したキーワードが RADIUS サーバーに渡り、RADIUS サーバーから運転免許証の番号や誕生日などの要求が返されます。ユーザーがパスワードを入力した場合は、RADIUS サーバーの構成によって、要求が返される場合と返されない場合があります。

代替 RADIUS サーバーのパラメータの設定

代替 RADIUS サーバーを使用する場合は、テキスト・エディタを使用して sqlnet.ora ファイルに次のパラメータを設定します。

```
SQLNET.RADIUS_ALTERNATE=(HOSTNAME OR IP ADDRESS OF ALTERNATE RADIUS SERVER)

SQLNET.RADIUS_ALTERNATE_PORT=(1645)

SQLNET.RADIUS_ALTERNATE_TIMEOUT=(NUMBER OF SECONDS TO WAIT FOR RESPONSE)
SQLNET.RADIUS_ALTERNATE_RETRIES=(NUMBER OF TIMES TO RE-SEND TO RADIUS SERVER)
```

手順 3: RADIUS サーバー・データベースへの RADIUS クライアント名の追加

Oracle Server が RADIUS クライアントになります。3-2 ページの図 3-1 を参照してください。

Livingston RADIUS サーバー、バージョン 2.0 への RADIUS クライアント名の追加

注意： Internet Engineering Task Force（IETF）RFC #2138、*Remote Authentication Dial In User Service（RADIUS）*および RFC #2139 *RADIUS Accounting* の標準に準拠する RADIUS サーバーを使用することができます。RADIUS サーバーにはいろいろな種類があるため、固有の相互運用要件がないか、RADIUS サーバーのマニュアルで確認しておく必要があります。

RADIUS サーバーの clients ファイルには、各 RADIUS クライアントの名前または IP アドレスと共有シークレットが格納されます。このファイルのパス名は /etc/raddb/clients です。

Livingston RADIUS サーバー 2.0 データベースへの RADIUS クライアント名の追加

1. テキスト・エディタを使用して clients ファイルを開きます。次のテキストと表が表示されます。

```
@ (#) clients 1.1 2/21/96 Copyright 1991 Livingston Enterprises Inc

This file contains a list of clients which are allowed to make
authentication requests and their encryption key. The first field is a valid
hostname. The second field (separated by blanks or tabs) is the encryption
key.

Client Name                     Key
```

2. CLIENT NAME 列にクライアントの名前または IP アドレスを入力します。KEY 列に共有シークレットを入力します。

注意： CLIENT NAME 列に入力する値は、クライアントの名前または IP アドレスに関わらず、RADIUS サーバーによって異なります。RADIUS のマニュアルを参照してください。

3. clients ファイルを保存して閉じます。

   詳細情報： RADIUS サーバーの管理マニュアルを参照してください。

手順 4: ユーザーの作成とアクセス権の付与

1. Oracle Server の外部で認証されるユーザーを作成し、アクセス権を付与します。

   SQL*Plus を起動して、次のコマンドを入力します。

   ```
   SQL> CONNECT system/manager@database_name;
   SQL> CREATE USER username IDENTIFIED EXTERNALLY;
   SQL> GRANT CREATE SESSION TO USER username;
   SQL> EXIT
   ```

   Windows NT プラットフォームの場合は、Oracle Enterprise Manager の Security Manager ツールを使用することもできます。

   詳細情報： 『Oracle8*i* 管理者ガイド』と『Oracle8*i* 分散システム』を参照してください。

2. RADIUS サーバの users ファイルにも同じユーザーを入力します。

   詳細情報： RADIUS サーバーの管理マニュアルを参照してください。

手順 5: RADIUS アカウントの構成

RADIUS アカウントでは、Oracle Server へのアクセス情報を記録し、RADIUS アカウント・サーバーのファイルに格納します。この機能は、RADIUS サーバーと認証サーバーの両方でサポートされている場合にのみ使用することができます。

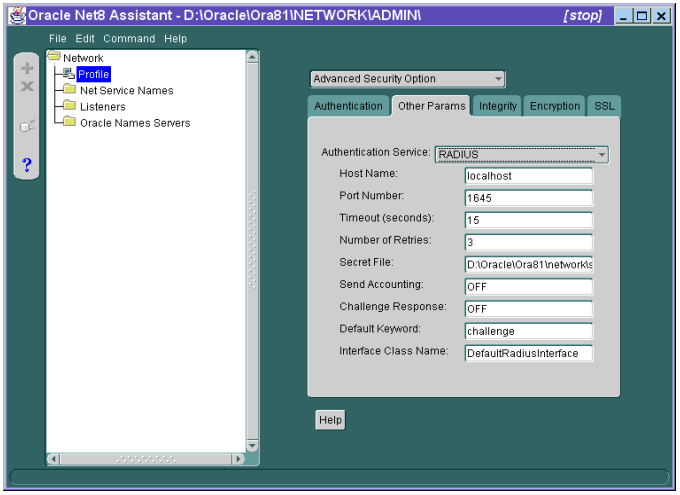
RADIUS アカウントを使用可能または使用禁止にするには、次の手順で行います。

- Oracle Server での RADIUS アカウントの設定
- RADIUS アカウント・サーバーの構成

Oracle Server での RADIUS アカウントの設定

Oracle Server の SQLNET.RADIUS_SEND_ACCOUNTING パラメータを設定します。

図 3-12 Oracle Net8 Assistant を使用した RADIUS アカウントの設定



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 3-12 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「RADIUS」を選択します。 3. アカウントを使用可能にするには、「Send Accounting」ボックスに ON を入力し、使用禁止にするには OFF を入力します。デフォルトは OFF です。	次のパラメータを設定します。 SQLNET.RADIUS_SEND_ACCOUNTING= *ON*

RADIUS アカウント・サーバーの構成

RADIUS アカウントは、RADIUS 認証サーバーと同じホストまたは別のホストにあるアカウント・サーバーから成ります。

詳細情報： RADIUS アカウントの構成の詳細は、RADIUS サーバーの管理マニュアルを参照してください。

手順 6: RADIUS とともに使用する認証サーバーの構成

詳細情報： 認証サーバーの構成の詳細は、認証サーバーのマニュアルを参照してください。xvii ページの「関連マニュアル」に使用可能なリソースの一覧があります。

手順 7: 認証サーバーとともに使用する RADIUS サーバーの構成

詳細情報： RADIUS サーバーのマニュアルを参照してください。

手順 8: ロールの作成とロール権限の付与

RADIUS サーバーでベンダー・タイプ属性をサポートしている場合は、ロールを RADIUS サーバーに格納して管理することができます。RADIUS を使用した `CONNECT` 要求があると、Oracle Server がロールをダウンロードします。

この機能を使用するには、Oracle Server と RADIUS サーバーの両方でロールを構成します。

Oracle Server でのロールの構成

1. テキスト・エディタを使用して、Oracle Server の init.ora ファイルに初期化パラメータ `OS_ROLES` を設定します。
2. Oracle Server を停止して再起動します。
3. `IDENTIFIED EXTERNALLY` 構文を使用して、RADIUS サーバーで管理する各ロールを Oracle Server に作成します。

詳細情報： 『Oracle8*i* 管理者ガイド』を参照してください。

RADIUS サーバーでのロールの構成

次の書式でロール名を作成します。

```
ORA_DatabaseName.DatabaseDomainName_RoleName
```

パラメータ	説明
DatabaseName	ロールを作成する Oracle Server の名前。db_name 初期化パラメータと同じ値です。
DatabaseDomainName	Oracle Server が属するドメインの名前。db_domain 初期化パラメータと同じ値です。
RoleName	Oracle Server に作成したロールの名前。

たとえば、次のとおりです。

```
ORA_JULIETDB.US.ORACLE.COM_MANAGER
```

詳細情報： RADIUS サーバーの管理マニュアルを参照してください。

手順 9: Oracle Server での RADIUS シークレット・キーの指定

次の作業を行います。

1. RADIUS サーバーから RADIUS シークレット・キーを取得します。RADIUS サーバーの管理者によって各 RADIUS クライアントの共有シークレット・キーが作成されます。'test123' のような単純な場合もあります。
2. Oracle Server に、ディレクトリ $ORACLE_HOME/SECURITY を作成します。
3. RADIUS サーバーからの共有シークレットを格納する radius.key ファイルを作成します。このファイルを、上で作成したディレクトリ $ORACLE_HOME/SECURITY に置きます。
4. 共有シークレット・キーをコピーし、このキーのみを、Oracle Server に作成した radius.key ファイルに貼り付けます。

   詳細情報： シークレット・キーの取得の詳細は、RADIUS サーバーの管理マニュアルを参照してください。

テキスト・エディタを使用して、`$ORACLE_HOME/SECURITY` にある radius.key ファイルを開きます。RADIUS シークレット・キーを入力し、ファイルを保存します。

注意： 安全上の理由により、このファイルをルート・アクセスのみに変更することをお薦めします。

データベースへのログイン

同期認証モードを使用している場合は SQL*Plus を起動して、プロンプトで次のように入力します。

```
CONNECT username/password@database_alias
```

このコマンドでログインできるのは、要求 - 応答が OFF の場合のみです。

要求 - 応答（非同期）モードを使用している場合は SQL*Plus を起動して、プロンプトで次のように入力します。

```
CONNECT/@database_alias
```

このコマンドでログインできるのは、要求 - 応答が ON の場合のみです。

4

CyberSafe 認証の構成

この章では、CyberSafe を使用する Oracle の構成方法を説明し、Oracle ユーザーを認証する CyberSafe の構成手順について簡単に説明します。

この章では、次のトピックについて説明します。

CyberSafe 認証の使用

CyberSafe 認証を使用可能にするには、次の作業を行います。各作業の詳細は以下で説明しています。

注意： これらの作業を以下に示す順序で実行する必要があります。

手順 1: CyberSafe サーバーをインストール

認証サーバーとして動作するマシンにインストールします。

詳細情報： このマニュアルの「はじめに」の xvii ページの「関連マニュアル」に示した CyberSafe マニュアルを参照してください。

手順 2: CyberSafe TrustBroker クライアントをインストール

Oracle Server と Oracle クライアントを実行するマシンにインストールします。

詳細情報： このマニュアルの「はじめに」の xvii ページの「関連マニュアル」に示した CyberSafe マニュアルを参照してください。

手順 3: CyberSafe Application Security Toolkit をインストール

クライアントとサーバーの両方にインストールします。

詳細情報： このマニュアルの「はじめに」の xvii ページの「関連マニュアル」に示した CyberSafe マニュアルを参照してください。

手順 4: Oracle Server のサービス・プリンシパルを構成

Oracle Server でクライアントの識別情報を検証するには、CyberSafe TrustBroker Master Server を稼働するマシン上で、Oracle Server のサービス・プリンシパルを構成する必要があります。必要に応じて、レルムを構成する必要があります。

プリンシパルの名前を次の書式で指定する必要があります。

```
kservice/kinstance@REALM
```

kservice	Oracle サービスを表す文字列。これは、データベース・サービス名と同じでも異なっていてもかまいません
kinstance	通常は、Oracle が稼働しているマシンの完全修飾名
REALM	サーバーのドメイン

注意： kservice では大文字と小文字を区別します。REALM は必ず大文字で入力します。

注意： この項で説明するユーティリティ名は、実際に実行するプログラムです。しかし、CyberSafe ユーザー名「cyberuser」とレルム「SOMECO.COM」は例にすぎないので、実際の名前はこれとは異なります。

たとえば、kservice が「oracle」で、Oracle が稼働しているマシンの完全修飾名が「dbserver.someco.com」で、レルムが「SOMECO.COM」の場合は、プリンシパル名は次のようになります。

```
oracle/dbserver.someco.com@SOMECO.COM
```

注意： 通常は、DNS ドメイン名をレルムの名前として使用します。

kdb5_edit をルートとして実行しサービス・プリンシパルを作成します。

```
# cd /krb5/admin
# ./kdb5_edit
```

「oracle/dbserver.someco.com@SOMECO.COM」というプリンシパルを、CyberSafe が認識するサービス・プリンシパルのリストに追加するには、kdb5_edit から次のように入力します。

```
kdb5_edit:  ark oracle/dbserver.someco.com@SOMECO.COM
```

手順 5: CyberSafe からのサービス表を抽出

CyberSafe からサービス表を抽出して、それを Oracle Server マシンと CyberSafe TrustBroker クライアント・マシンの両方にコピーする必要があります。たとえば、dbserver.someco.com のサービス表を抽出するには、kdb5_edit から次のように入力します。

```
kdb5_edit:  xst dbserver.someco.com oracle
'oracle/dbserver.someco.com@SOMECO.COM' added to keytab
'WRFILE:dbserver.someco.com-new-srvtab'
kdb5_edit:  exit
# /krb5/bin/klist -k -t dbserver.someco.com-new-srvtab
```

注意： *xst* を使用するときに REALM（上の例では、SOMECO.COM）を入力しないと、kdb5_edit が現行ホストのレルムを使用して、それを前述のようにコマンド出力に表示します。

サービス表を抽出したら、そのテーブルに古いエントリと新しいエントリがあることを確認します。新しいエントリがサービス表にない場合、または新しいエントリを追加する必要がある場合は、kdb5_edit を使用してエントリを追加します。

ここで、CyberSafe のサービス表を CyberSafe TrustBroker クライアント・マシンに移動する必要があります。サービス表が CyberSafe クライアントと同じマシン上にある場合は、（次に示すようなコマンドを使用して）それを移動するだけでかまいません。CyberSafe

Challenger クライアントと異なるマシンにサービス表がある場合は、FTP のようなプログラムを使用してファイルを転送する必要があります。たとえば、次のように入力してサービス表を移動します。

```
# mv dbserver.someco.com-new-srvtab /krb5/v5srvtab
```

FTP を使用するときは、ファイルをバイナリ・モードで転送してください。

Oracle Server がサービス表を読み取れるようにする

Oracle Server 実行可能プログラムの所有者がサービス表（上の例では、krb5/v5srvtab）を読み取れるようにします。ファイル所有者を Oracle ユーザーに設定するか、Oracle が属しているグループに対してファイルを読取り可能にします。ファイルをすべてのユーザーに対して読取り可能にしないでください（安全性が損なわれるため）。

手順 6: Oracle Server をインストール

CyberSafe TrustBroker クライアントを実行しているマシンと同じマシンにインストールします。

> **詳細情報：** プラットフォーム固有の Oracle8*i* インストレーション・マニュアルを参照してください。

手順 7: Oracle Advanced Security と CyberSafe アダプタをインストール

Oracle8*i* の標準インストレーションでは、Oracle Advanced Security とともに CyberSafe アダプタもインストールされます。Oracle Universal Installer によってインストレーション・プロセス全体がガイドされます。

> **詳細情報：** プラットフォーム固有の Oracle インストレーション・マニュアルを参照してください。

手順 8: サーバーとクライアント上で Net8 と Oracle を構成

> **詳細情報：** 詳細は、オペレーティング・システム固有のマニュアルを参照してください。

手順 9: CyberSafe 認証を構成

Oracle Server と Oracle クライアントの sqlnet.ora ファイルで特定のパラメータを設定する必要があります。以下に、次の作業について説明します。

- クライアントとサーバーでの認証サービスの構成
- クライアントとサーバーでの CyberSafe 認証サービス・パラメータの構成

- INIT.ORA パラメータの設定

sqlnet.ora ファイルは Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して変更します。以下にその方法を説明しています。init.ora ファイルは、テキスト・エディタで変更します。

> **詳細情報：** Oracle Net8 Assistant のオンライン・ヘルプを参照してください。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ー *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

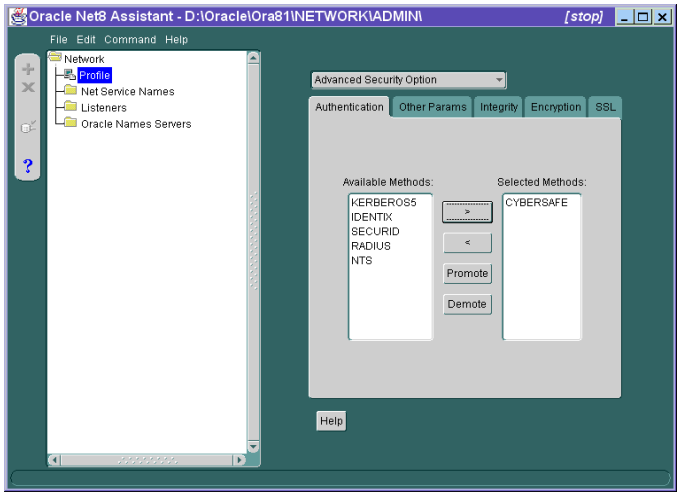
Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

クライアントとサーバーでの認証サービスの構成

SQLNET.AUTHENTICATION_SERVICES パラメータを設定します。

図 4-1 Oracle Net8 Assistant を使用した認証の構成

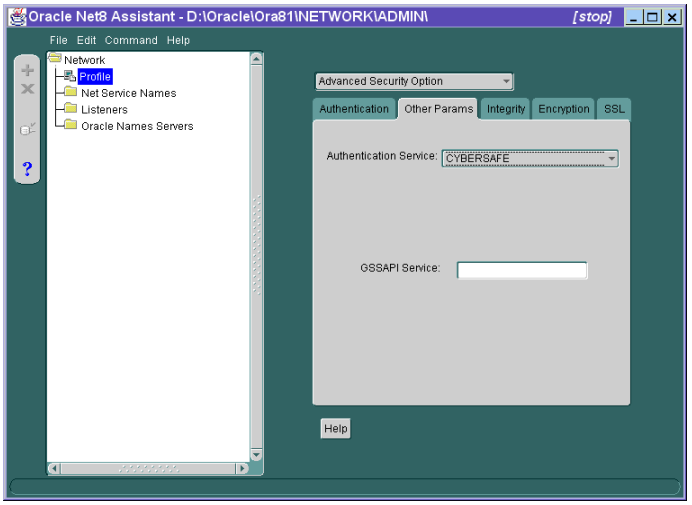


Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 4-1 を参照してください。 1. 「Authentication」タブを選択します。 2. 「Available Methods」リストで、「CyberSafe」を選択します。 3. 「>」ボタンをクリックして、サービスを「Selected Methods」リストに移動します。他に使用するメソッドがあれば同じ方法で移動します。 4. 選択したメソッドを使用優先順位の高い順に並べます。メソッドを選択し、「Promote」または「Demote」をクリックして並べ替えます。たとえば、CyberSafe サービスを最初に使用する場合は、CyberSafe をリストの先頭に置きます。	次のパラメータを設定します。 SQLNET.AUTHENTICATION_SERVICES=(*CYBERSAFE*)

クライアントとサーバーでの CyberSafe 認証サービス・パラメータの構成

SQLNET.AUTHENTICATION_GSSAPI_SERVICE パラメータを設定します。

図 4-2 Oracle Net8 Assistant を使用した認証サービス・パラメータの構成



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 4-2 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」リストで、「CYBERSAFE」を選択します。 3. GSSAPI サービスの名前を次の書式で入力します。 `oracle/`*`dbserver.someco.com`* *`@SOMECO.COM`*	次のパラメータを設定します。 SQLNET.AUTHENTICATION_GSSAPI_SERVICE=*KSERVICE/KINSTANCE@REALM* **注意：** 4-3 ページの「手順 4: Oracle Server のサービス・プリンシパルを構成」で説明している書式でプリンシパル名を追加する必要があります。

INIT.ORA パラメータの設定

データベース・インスタンス用の init<*sid*>.ora ファイルに、次のパラメータを追加することを強くお薦めします。

```
REMOTE_OS_AUTHENT=FALSE
```

sid はデータベース・システム識別子です。

注意： REMOTE_OS_AUTHENT を TRUE に設定すると、非保護プロトコル（TCP など）を使用するユーザーがオペレーティング・システム許可ログイン（以前の OPS$ ログイン）を実行できるので、セキュリティに欠陥が生じます。

CyberSafe ユーザー名には長い名前を使用できますが、Oracle ユーザー名は 30 字に制限されているので、OS_AUTHENT_PREFIX の値として次に示す NULL 値を使用することを強くお薦めします。

```
OS_AUTHENT_PREFIX=""
```

構成ファイルを変更したら、変更内容を有効にするために Oracle Server を再起動します

詳細情報： Oracle Server マシン再起動する方法については、オペレーティング・システム固有のマニュアルと『Oracle8*i* 管理者ガイド』を参照してください。

手順 10: 認証サーバー上で CyberSafe ユーザーを作成

CyberSafe で Oracle ユーザーを認証するには、管理ツールがインストールされている CyberSafe 認証サーバーでユーザーを作成する必要があります。次の手順では、レルムがすでに存在することを前提としています。

詳細情報： レルムの作成の詳細は、このマニュアルの「はじめに」の xvii ページの「関連マニュアル」を参照してください。

注意： この項で説明するユーティリティ名は、実際に実行するプログラムです。しかし、CyberSafe ユーザー名「cyberuser」とレルム「SOMECO.COM」は例にすぎないので、実際の名前はシステムによって異なります。

認証サーバー上で /krb5/admin/kdb5_edit をルートとして実行し、新しい CyberSafe ユーザー（"cyberuser"）を作成します。次のように入力します。

1. # kdb5_edit
2. kdb5_edit: ank cyberuser
3. Enter password: < パスワードは画面に表示されません >
4. Re-enter password for verification: < パスワードは画面に表示されません >
5. kdb5_edit: quit

手順 11: 外部的に認証される Oracle ユーザーを Oracle Server 上で作成

SQL*Plus を実行して Oracle ユーザーを作成するために、Oracle Server マシンで次のコマンドを実行します。

```
SQL> CONNECT INTERNAL;
SQL> CREATE USER "USNERNAME" IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO "USERNAME";
```

この例では、OS_AUTHENT_PREFIX を次のように設定します。

```
""
```

注意： Oracle ユーザーを作成するときは、次の例に示すように名前を大文字で入力して二重引用符で囲む必要があります。

次の例では、OS_AUTHENT_PREFIX を "" に設定しています。

```
SQL> CREATE USER "JDOE" IDENTIFIED EXTERNALLY
SQL> GRANT CREATE SESSION TO "JDOE"
```

詳細情報：『Oracle8*i* 管理者ガイド』を参照してください。

手順 12: Kerberos/Oracle ユーザー用の初期チケットを取得

ユーザーがデータベースと接続するには、クライアント上で kinit を実行して**初期チケット（initial ticket）**を取得する必要があります。

```
% kinit (user name)
Password for CYBERUSER@US.ORACLE.COM:
<password not echoed to screen>
```

クライアント上で klist を使用して資格証明を表示

ユーザーはクライアント上で klist を実行して、現在所有しているチケットを表示する必要があります。

```
% klist
```

作成日	有効期限	サービス
11-Aug-95 16:29:51	12-Aug-95 00:29:21	krbtgt/SOMECO.COM@SOMECO.COM
11-Aug-95 16:29:51	12-Aug-95 00:29:21	oracledbserver.someco.com@SOMECO.COM

手順 13: CyberSafe によって認証された Oracle Server に接続

kinit を実行して初期チケットを取得したら、ユーザー名またはパスワードを使用しないで Oracle Server に接続できます。次のようなコマンドを入力します。

```
%  sqlplus /@net_service_name
```

net_service_name は Net8 サービス名です。

たとえば、次のとおりです。

```
% sqlplus /@npddoc_db
```

詳細情報： 第 1 章の「Oracle Advanced Security の概要」と『Oracle8*i* 分散システム』を参照してください。

CyberSafe 認証アダプタの構成に関するトラブルシューティング

ここでは、構成に関する一般的な問題とその解決方法について説明します。

kinit を使用してチケット付与チケットを取得できない場合

- krb.conf を調べて、デフォルトのレルムが適切であるかどうかを確認します。
- レルムに指定されているホスト上で TrustBroker Master Server が稼働しているかどうかを確認します。
- Master Server にユーザー・プリンシパルのエントリがあること、およびパスワードが一致しているかどうかを確認します。
- krb.conf ファイルと krb.realms ファイルが Oracle で読取り可能になっているかどうかを確認します。

初期チケットがあるけれど、接続できない場合

- 接続を試みた後で、サービス・チケットをチェックします。
- サーバー側の sqlnet.ora ファイルに、CyberSafe Master Server が認識するサービスに対応するサービス名があるかどうかをチェックします。
- 関係するすべてのマシン上で、クロックのずれが数分以内であるかどうかをチェックします。

サービス・チケットがあるけれど接続できない場合

- クライアントとサーバー上でクロックをチェックします。
- v5srvtab ファイルが適切な場所に存在し、Oracle で読取り可能なっているかどうかをチェックします。
- サーバー側のプロファイル（sqlnet.ora）で指定されているサービスに対して、v5srvtab ファイルが生成されているかどうかをチェックします。

何も問題はないけれど、別の問合せが失敗する場合

- 初期チケットが転送可能であるかどうかをチェックします（kinit -f を実行して、初期チケットを取得してなければなりません）。
- 資格証明の有効期限をチェックします。
- 資格証明の有効期限が切れている場合は、接続を閉じ kinit を実行して新しい初期チケットを取得します。

5

Kerberos 認証の構成

この章では、Kerberos 認証を使用する Oracle の構成方法と、Oracle ユーザーを認証する Kerberos の構成方法について説明します。

この章では、次のトピックについて説明します。

- Kerberos 認証の使用
- Kerberos 認証アダプタで使用するユーティリティ
- Kerberos 認証の構成に関するトラブルシューティング

Kerberos 認証の使用

Kerberos 認証を使用可能にするには、次の作業を行います。各作業の詳細は以下で説明しています。

次の作業をこの順序に従って実行する必要があります。

手順 1: Kerberos をインストール

認証サーバーとして動作するマシンにインストールします

> **詳細情報：** マシンへの Kerberos のインストール方法は、このマニュアルの「はじめに」の xvii ページの「関連マニュアル」を参照してください。

手順 2: Oracle Server のサービス・プリンシパルを構成

Kerberos を使用して自己を認証するクライアントの識別情報を Oracle Server が検証するには、まず Oracle のサービス・プリンシパルを作成する必要があります。

プリンシパルの名前を次の書式で指定する必要があります。

```
kservice/kinstance@REALM
```

kservice	Oracle サービスを表す文字列。これは、データベース・サービス名と同じでも異なっていてもかまいません。この文字列では、大文字と小文字を区別します。
kinstance	通常は、Oracle が稼働しているマシンの完全修飾名。
REALM	サーバーのドメイン。必ず大文字で入力します。

注意： この項で説明するユーティリティ名は、実際に実行するプログラムです。しかし、Kerberos ユーザー名「krbuser」とレルム「SOMECO.COM」は例にすぎないので、実際の名前はシステムによって異なります。

たとえば、kservice が「oracle」で、Oracle が稼働しているマシンの完全修飾名が「dbserver.someco.com」で、レルムが「SOMECO.COM」の場合は、プリンシパル名は次のようになります。

```
oracle/dbserver.someco.com@SOMECO.COM
```

通常は、DNS ドメイン名をレルムの名前として使用します。

サービス・プリンシパルを作成するには、kdb5_edit を実行します。次に示すのは、UNIX の場合の例です。

```
# cd /krb5/admin
# ./kdb5_edit
```

「oracle/dbserver.someco.com@SOMECO.COM」というプリンシパルを、Kerberos が認識するサービス・プリンシパルのリストに追加するには、次のように入力します。

```
kdb5_edit:ark oracle/dbserver.someco.com@SOMECO.COM
```

手順 3: Kerberos からのサービス表を抽出

Kerberos からサービス表を抽出して、それを Oracle Server マシンと Kerberos クライアント・マシンにコピーする必要があります。

たとえば、dbserver.someco.com のサービス表を抽出するには、次のように入力します。

```
kdb5_edit:  xst dbserver.someco.com oracle
'oracle/dbserver.someco.com@SOMECO.COM' added to keytab
'WRFILE:dbserver.someco.com-new-srvtab'
kdb5_edit:  exit
oklist -k -t dbserver.someco.com-new-srvtab
```

サービス表を抽出したら、サービス表に古いエントリと新しいエントリがあることを確認します。それらがサービス表内にない場合、または追加する必要がある場合は、kdb5_edit を使用してエントリを追加します。

xst を使用するときにレルム（SOMECO.COM など）を入力しないと、kdb5_edit が現行ホストのレルムを使用して、それを前述のようにコマンド出力に表示します。

kerberos サービス表が Kerberos クライアント・マシンと同じマシン上にある場合は、それを移動するだけでかまいません。サービス表が Kerberos クライアントと異なるマシン上に

ある場合は、バイナリ FTP のようなプログラムを使用してファイルを転送する必要があります。次に示すのは、UNIX の場合の例です。

```
# mv dbserver.someco.com-new-srvtab /etc/v5srvtab
```

サービス・ファイルのデフォルト名は /etc/v5srvtab です。これ以外の名前を使用する場合は、デフォルト名をその名前で置き換える必要があります。

Oracle Server がサービス表を読み取れるようにする

Oracle Server 実行可能プログラムの所有者がサービス表（前述の例では、/etc/v5srvtab）を読み取れるようにする必要があります。このためには、ファイル所有者を Oracle ユーザーに設定するか、ファイルを Oracle が属しているグループに対して読取り可能にします。

注意： ファイルをすべてのユーザーに対して読取り可能にしてはいけません。このようにすると、安全性が損なわれます。

手順 4: Oracle Server と Oracle クライアントをインストール

詳細情報： 詳細は、オペレーティング・システム固有のマニュアルを参照してください。

手順 5: Net8 をインストール

Oracle Server マシンと Oracle クライアント・マシンにインストールします。

詳細情報： Net8 のインストレーション・マニュアルを参照してください。

手順 6: Net8 と Oracle を構成

Oracle Server と Oracle クライアントの両方で行います。

> **詳細情報：** 詳細は、オペレーティング・システム固有のマニュアルと『Net8 管理者ガイド』を参照してください。

手順 7: Kerberos 認証を構成

Oracle Server と Oracle クライアントの sqlnet.ora ファイルで特定のパラメータを設定する必要があります。以下に、次の作業について説明します。

- クライアントとサーバーでの認証サービスの構成
- Oracle Server と Oracle クライアントでの認証パラメータの構成

> **詳細情報：** Oracle Net8 Assistant による Kerberos 認証の詳細は、Oracle Net8 Assistant のオンライン・ヘルプを参照してください。

特に示されていない限り、Kerberos 認証を構成するには、Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して sqlnet.ora ファイルを変更します。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ― *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

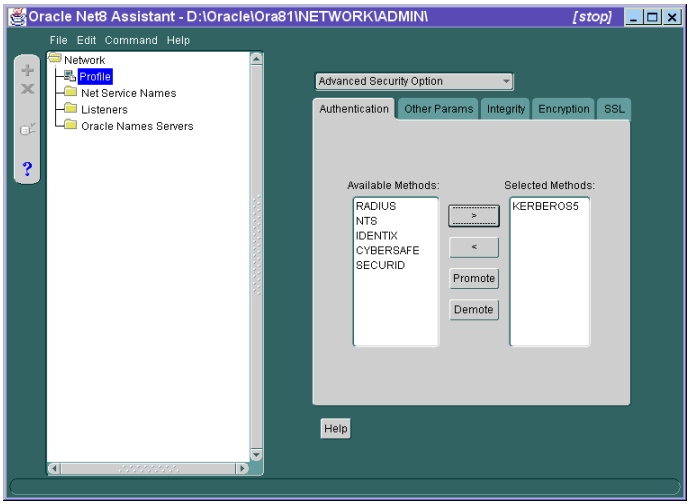
Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

クライアントとサーバーでの認証サービスの構成

SQLNET.AUTHENTICATION_SERVICES パラメータを設定します。

図 5-1 Oracle Net8 Assistant を使用した認証の構成

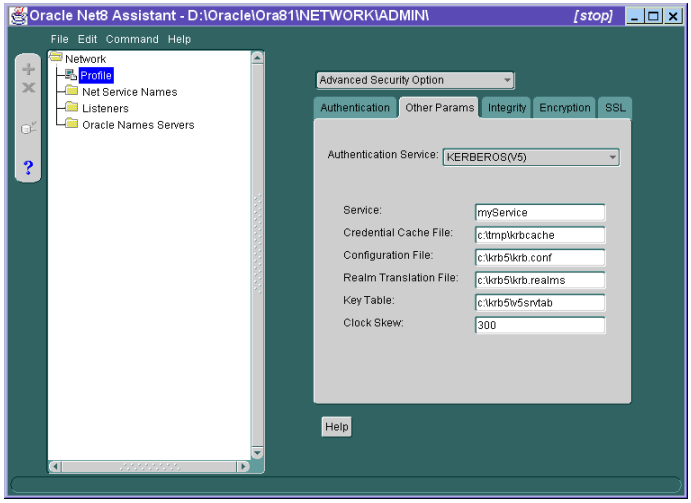


Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 5-1 を参照してください。 1. 「Authentication」タブを選択します。 2. 「Available Services」リストで KERBEROS5 を選択します。 3. 「>」ボタンをクリックして、サービスを「Selected Services」リストに移動します。他に移動するメソッドがあれば同じ方法で移動します。 4. 選択したサービスを使用優先順位の高い順に並べます。サービスをクリックして選択してから、「Promote」ボタンまたは「Demote」ボタンをクリックして、リスト内でサービスを並べ替えます。たとえば、KERBEROS5 サービスを最初に使用する場合は、KERBEROS5 をリストの先頭に置きます。	次のパラメータを設定します。 SQLNET.AUTHENTICATION_SERVICES=(*KERBEROS5*)

Oracle Server と Oracle クライアントでの認証パラメータの構成

SQLNET.AUTHENTICATION_KERBEROS5_SERVICE パラメータを設定します。この項で説明する各種オプション・パラメータを設定する場合もあります。

図 5-2 Oracle Net8 Assistant を使用した認証パラメータの構成



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 5-2 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Service」テキストボックスに kerberos と入力します。**注意 :** このパラメータの値は必ず指定してください。指定すると、他のテキスト・ボックスに入力できるようにになります。 次のパラメータの値を指定することもできます。 ■ 資格証明キャッシュ・ファイル ■ 構成ファイル ■ レルム変換ファイル ■ キー・テーブル ■ クロックのずれ	次のパラメータを設定する必要があります。 SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=*kservice* **注意 :** 前述のパラメータは、Oracle が Kerberos サービス・チケットを取得する際に使用するサービスの名前を指定します。サービス名の kservice を別の値で置き換える必要があります。 **注意 :** パラメータ SQLNET.AUTHENTICATION_KERBEROS5_SERVICE で渡す値では大文字と小文字を区別します。必ず小文字で指定します。 次のパラメータを設定することもできます。詳細は、5-9 ページの「オプションの SQLNET.ORA パラメータ」の項で説明しています。 ■ SQLNET.KERBEROS5_CC_NAME ■ SQLNET.KERBEROS5_CONF ■ SQLNET.KERBEROS5_REALMS ■ SQLNET.KERBEROS5_KEYTAB ■ SQLNET.KERBEROS5_CLOCKSKEW

INIT.ORA パラメータの設定

テキスト・エディタを使用して、データベース・インスタンス用の init.ora ファイルに、次のパラメータを追加します。

```
REMOTE_OS_AUTHENT=FALSE
```

注意 : REMOTE_OS_AUTHENT を TRUE に設定すると、非保護プロトコル（TCP など）を使用するユーザーがオペレーティング・システム許可ログイン（以前は、OPS$ ログインといいました）を実行できるので、セキュリティに欠陥が生じます。

Kerberos ユーザー名には長い名前を使用できますが、Oracle ユーザー名は 30 字に制限されているので、OS_AUTHENT_PREFIX の値として次に示す NULL 値を使用することを強くお薦めします。

```
OS_AUTHENT_PREFIX=""
```

OS_AUTHENT_PREFIX を NULL 値に設定すると、デフォルト値の OPS$ が上書きされます。

オプションの SQLNET.ORA パラメータ

前述の必須パラメータの他に、以下に示すオプション・パラメータをクライアントまたはサーバー上で設定できます。

パラメータ : SQLNET.KERBEROS5_CC_NAME=*pathname_to_credentials_cache_file*

説明 : このパラメータは、Kerberos 資格証明キャッシュ（CC）ファイルの完全パス名を指定します。デフォルト値はオペレーティング・システムによって異なります。UNIX では、/tmp/krb5cc_user id がデフォルトです。たとえば、次のとおりです。

```
SQLNET.KERBEROS5_CC_NAME=/usr/tmp/krbcache
```

注意 : KRB5CCNAME 環境変数を使用して、このパラメータを設定することもできます。

sqlnet.ora ファイルで設定する SQLNET.KERBEROS5_CC_NAME パラメータの値は、KRB5CCNAME 環境変数で設定する値より優先します。

パラメータ : SQLNET.KERBEROS5_CLOCKSKEW=*number_of_seconds_accepted_as_network_delay*

説明 : このパラメータは、Kerberos 資格証明の有効期限が切れるまでの時間を秒数で指定します。資格証明がクライアントまたはサーバーによって実際に受け取られるときに、このパラメータが使用されます。また、再生攻撃を受けないように資格証明を格納する必要があるかどうかを Oracle Server が判断するときも、このパラメータが使用されます。デフォルトは 300 秒です。たとえば、次のとおりです。

```
SQLNET.KERBEROS5_CLOCKSKEW=1200
```

パラメータ : SQLNET.KERBEROS5_CONF=*pathname_to_Kerberos_configuration_file*

説明 : このパラメータは、Kerberos 構成ファイルの完全パス名を指定します。構成ファイルにはデフォルトの KDC（キー配布センター）のレルムが含まれていて、レルムを KDC ホストにマップします。デフォルトはオペレーティング・システムによって異なります。UNIX では、/krb5/krb.conf がデフォルトです。たとえば、次のとおりです。

```
SQLNET.KERBEROS5_CONF=/krb/krb.conf
```

パラメータ : SQLNET.KERBEROS5_KEYTAB=
pathname_to_Kerberos_principal/key_table

説明 : このパラメータは、Kerberos プリンシパル / シークレット・キー・マッピング・ファイルの完全パス名を指定します。Oracle Server がキーを抽出して、クライアントから送られる認証情報を復号化するときに、このパラメータが使用されます。デフォルトはオペレーティング・システムによって異なります。UNIX では、/etc/v5srvtab がデフォルトです。たとえば、次のとおりです。

```
SQLNET.KERBEROS5_KEYTAB=/etc/v5srvtab
```

パラメータ : SQLNET.KERBEROS5_REALMS=
pathname_to_Kerberos_realm_translation_file

説明 : このパラメータは、Kerberos レルム変換ファイルの完全パス名を指定します。変換ファイルを使用して、ホスト名またはドメイン名をレルムにマップします。デフォルトはオペレーティング・システムによって異なります。UNIX では、/etc/krb.realms です。たとえば、次のとおりです。

```
SQLNET.KERBEROS5_REALMS=/krb5/krb.realms
```

手順 8: Kerberos ユーザーを作成

Kerberos で認証できる Oracle ユーザーを作成するには、管理ツールがインストールされている Kerberos 認証サーバー上で次の作業を実行します。

ここでは、すでにレルムが存在していることを想定しています。

> **詳細情報：** このマニュアルの「はじめに」の xvii ページの「関連マニュアル」を参照してください。

> **注意：** この項で説明するユーティリティ名は、実際に実行するプログラムです。しかし、Kerberos ユーザー名「krbuser」とレルム「SOMECO.COM」は例にすぎないので、実際の名前はシステムによって異なります。

/krb5/admin/kdb5_edit をルートとして実行し、新しい Kerberos ユーザー（"krbuser" など）を作成します。次に示すのは、UNIX の場合の例です。

```
# ./kdb5_edit
kdb5_edit: ank krbuser
Enter password:  <password not echoed to screen>
Re-enter password for verification:  <password...>
kdb5_edit: quit
```

手順 9: 外部的に認証される Oracle ユーザーを作成

SQL*Plus を Oracle Server 上で実行して、Kerberos ユーザーに対応する Oracle ユーザーを作成します。次の例では、OS_AUTHENT_PREFIX を "" に設定しています。

> **注意：** Oracle ユーザー名は、大文字で入力して二重引用符で囲む必要があります。たとえば、"KRBUSER@SOMECO.COM" のようにします。

```
SQL> CONNECT INTERNAL;
SQL> CREATE USER "KRBUSER@SOMECO.COM" IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO "KRBUSER@SOMECO.COM";
```

手順 10: Kerberos/Oracle ユーザー用の初期チケットを取得

データベースに接続する前に、キー配布センター（KDC）に**初期チケット（initial ticket）**を要求する必要があります。クライアントで、次のコマンドを実行します。

```
okinit (user name)
```

> **詳細情報：** okinit の使用方法は、5-13 ページの「Kerberos 認証アダプタで使用するユーティリティ」を参照してください。

データベースと接続するときに、データベース・リンクの後に次のような参照が続く場合を考えます。

```
sqlplus /@oracle
```

このときは、転送可能フラグ（-f オプション）を使用する必要があります。okinit -f を実行すると、データベース・リンクで使用できる資格証明が使用可能になります。次のコマンドを実行する前に、Oracle クライアント上に移動する必要があります。

```
% okinit -f
Password for krbuser@SOMECO.COM:<password not echoed to screen>
```

> **詳細情報：** okinit の詳細は、5-13 ページの「okinit を使用して初期チケットを取得」を参照してください。

Kerberos 認証アダプタで使用するユーティリティ

次に示す 3 つのユーティリティが Oracle Kerberos 認証アダプタとともに出荷されます。これらのコマンドを実行する前に、Oracle クライアント上に移動する必要があります。

コマンド	説明
okinit	初期チケットを取得するユーティリティ
oklist	現在所有しているチケットのリストを表示するユーティリティ
okdstry	すべてのチケットを資格証明キャッシュから削除するユーティリティ

これらのユーティリティは、Kerberos 認証アダプタがインストールされた Oracle クライアントを実行しているユーザーのためのユーティリティです。

UNIX のみ： Kerberos バージョン 4 は Solaris とともに出荷されます。誤ってバージョン 4 のユーティリティを使用しないように、パス内に Kerberos バージョン 5 のユーティリティがあることを確認してください。

okinit を使用して初期チケットを取得

okinit を使用して Kerberos チケットを取得しキャッシュに書き込みます。通常は、okinit を使用してチケット付与チケットを取得し、ユーザーが入力したパスワードを使用してキー配布センター（KDC）から送られる資格証明を復号化します。チケット付与チケットはユーザーの証明キャッシュに格納されます。okinit では次のオプションを選択できます。

オプション	説明
`-f`	転送可能なチケット付与チケットを要求します。データベース・リンクをたどる場合は、このオプションが必要です。
`-l`	チケット付与チケットを含むすべてのチケットの存続期間を指定します。デフォルトで、チケット付与チケットの有効期間は 8 時間ですが、それより長い時間または短い時間も指定できます。KDC はこのオプションを無視したり、各サイトで指定できる時間を制限することができます。数字と、「w」（週）、「d」（日）、「h」（時間）、「m」（分）、「s」（秒）の修飾文字からなる文字列で、存続期間を指定します。 たとえば、次のように指定します。 `okinit -l 2wld6h20m30s` この場合、チケット付与チケットの存続期間は 2 週間と 1 日と 6 時間 20 分 30 秒です。

オプション	説明
-c	代替資格証明キャッシュを指定します。UNIX では、/tmp/krb5cc_<*uid*> がデフォルトです。sqlnet.ora ファイルで SQLNET.KERBEROS5_CC_NAME パラメータを使用して、代替資格証明キャッシュを指定することもできます。
-?	コマンド行オプションのリストを表示します。

oklist を使用して資格証明を表示

ユーザーは oklist を実行して、所有しているチケットのリストを表示できます。表示フラグ・オプション（-f）を使用して、追加情報を表示します。

```
% oklist -f
27-Jul-1995 21:57:51   28-Jul-1995 05:58:14
krbtgt/SOMECO.COM@SOMECO.COM
Flags: FI
```

オプション	説明
-f	資格証明のフラグを表示します。Oracle で重要なフラグは「I」（資格証明がチケット付与チケット）、「F」（資格証明が転送可能なチケット）および「f」（資格証明が転送済みチケット）です。
-c	代替資格証明キャッシュを指定します。UNIX では、/tmp/krb5cc_<*uid*> がデフォルトです。sqlnet.ora ファイルで SQLNET.KERBEROS5_CC_NAME パラメータを使用して代替資格証明キャッシュを指定することもできます。
-k	UNIX でサービス表（デフォルトは /etc/v5srvtab）内のエントリを一覧表示します。sqlnet.ora ファイルで SQLNET.KERBEROS5_KEYTAB パラメータを使用して、代替サービス表を指定することもできます。

okdstry を使用してキャッシュ・ファイルから資格証明を削除

okdstry を使用して資格証明キャッシュ・ファイルから資格証明を削除します。

```
$ okdstry -f
```

オプション	説明
-f	代替資格証明キャッシュを指定します。UNIX では、/tmp/krb5cc_<*uid*> がデフォルトです。プロファイル（sqlnet.ora）で SQLNET.KERBEROS5_CC_NAME パラメータを使用して、代替資格証明キャッシュを指定することもできます。

Kerberos によって認証された Oracle Server に接続

これで、ユーザー名またはパスワードを使用しないで Oracle Server に接続できます。次のようなコマンドを入力します。

```
$ sqlplus /@net_service_name
```

net_service_name は Net8 サービス名です。たとえば、次のとおりです。

```
$ sqlplus /@oracle_dbname
```

詳細情報： 外部認証の詳細は、第 1 章の「Oracle Advanced Security の概要」と『Oracle8*i* 分散システム』を参照してください。

Kerberos 認証の構成に関するトラブルシューティング

この項では、構成に関する一般的な問題とその解決方法について説明します。

okinit を使用してチケット付与チケットを取得できない場合

- krb.conf を調べて、デフォルトのレルムが適切であるかどうかを確認します。
- レルムに対して指定されているホスト上で、KDC が稼働しているかどうかを確認します。
- KDC にユーザー・プリンシパルのエントリがあること、およびパスワードが一致しているかどうかを確認します。
- krb.conf ファイルと krb.realms ファイルが Oracle で読取り可能になっているかどうかを確認します。

初期チケットがあるけれど、接続できない場合

- 接続を試みた後で、サービス・チケットをチェックします。
- サーバー側の sqlnet.ora ファイルに、Kerberos が認識するサービスに対応するサービス名があるかどうかをチェックします。
- 関係するすべてのマシン上で、クロックのずれが数分以内であるかどうかをチェックします（または、sqlnet.ora ファイルの sqlnet.kerberos5_clockskew パラメータを変更します）。

サービス・チケットがあるけれど接続できない場合

- クライアントとサーバー上でクロックをチェックします。
- v5srvtab ファイルが適切な場所に存在し、Oracle で読取り可能なっているかどうかをチェックします（sqlnet.ora パラメータを思い出してください）。
- サーバー側の sqlnet.ora ファイルで指定されているサービスに対して、v5srvtab ファイルが生成されているかどうかをチェックします。

何も問題はないけれど、別の問合せが失敗する場合

- 初期チケットが転送可能であるかどうかをチェックします（okinit -f を実行して、初期チケットを取得してなければなりません）。
- 資格証明の有効期限をチェックします。
- 資格証明の有効期限が切れている場合は、接続をクローズし okinit を実行して新しい初期チケットを取得します。

6

SecurID 認証の構成

この章では、SecurID 認証を構成し、それを Oracle Server と Oracle クライアントで使用する方法について説明します。この章では、読者が Security Dynamics の ACE/Server に精通していること、および ACE/Server がインストールされて稼働していることを想定しています。

> **詳細情報：** このマニュアルの「はじめに」の xvii ページの「関連マニュアル」を参照してください。

この章では、次のトピックについて説明します。

- システム要件
- 既知の制限事項
- SecurID 認証の使用
- SecurID 認証のためのユーザーを作成
- SecurID 認証の構成に関するトラブルシューティング
- SecurID 認証の使用

システム要件

Oracle Advanced Security リリース 8.1.5 に含まれている SecurID 認証を使用するには、次の製品が必要です。

- Net8
- Oracle 8.0.3 以降のリリース
- ACE/Server 1.2.4 以降のリリース
- Oracle は ACE/Server と通信する必要があるので、Oracle Server マシンが UDP/IP プロトコルと TCP/IP プロトコルをサポートしている必要があります。クライアントが SQL*Net または Net8 を使用して Oracle と接続しても、Oracle は UDP を使用して ACE/Server と接続する必要があります。

既知の制限事項

SecurID カード・コードは一度しか使用できないため、SecurID 認証はデータベース・リンク（「代理認証」とも言う）をサポートしていません。

SecurID 認証を使用するときは、パスワードの暗号化が使用禁止になります。つまり、SecurID カード・コード（標準カードを使用する場合は、PIN）がわかりやすいテキストで Oracle Server に送信されるということです。このため、セキュリティの問題が生じます。したがって、Oracle Server に送信される PIN が暗号化されるように、Oracle Advanced Security の暗号化をオンにすることをお薦めします。

> **詳細情報：** 暗号化をオンにする方法については、第 2 章の「暗号化とチェックサムの構成」を参照してください。

SecurID 認証の使用

SecurID 認証を使用可能にするには、次の作業を行います。各作業の詳細は以下で説明しています。

手順 1: Oracle を SecurID クライアントとして登録（ACE/Server リリース 1.2.4）

Oracle Server が常駐しているマシンを、SecurID クライアントとして ACE サーバーに登録します。この登録を行うには、Security Dynamics の sdadmin ツールを使用します。クライアントを作成するには、「Client」メニューから、「Create Client」（ACE/Server 1.2.4 の場合) または「Add Client」（ACE/Server 2.0 の場合）を選択します。

詳細は、『Security Dynamics ACE/Server Instruction Manual, version 1.2.4』、または『Security Dynamics ACE/Server version 2.0 Administration Manual』を参照してください。

手順 2: Oracle Advanced Security をインストール

Oracle Installer を使用して、Oracle8*i* の標準インストレーションで、Oracle Server と Oracle クライアントに Oracle Advanced Security をインストールします。

> **詳細情報：** プラットフォーム固有のインストレーション・マニュアルを参照してください。

手順 3: Oracle が適切な UDP ポートを見つけられるようにする（ACE/Server リリース 1.2.4）

最初に、ACE/Server、Oracle Server、Oracle Advanced Security がインストールされていることを確認します。

Oracle Server が ACE/Server と通信するのに必要な UDP ポートを見つけられるようにします。通常、これらのポート番号は、サービスと呼ばれるファイルに格納されています。UNIX オペレーティング・システムでは、通常、このファイルが /etc ディレクトリにあります。NIS（ネットワーク情報サービス）をネーム・サービスとして使用している場合は、サービス・マップに SecurID の正しいエントリが入っていることを確認します。

注意： Security Dynamics の Kitconts ツール（ACE/Server 1.2.4 の場合）または sdinfo ツール（ACE/Server 2.0 の場合）を実行して、ACE サーバーが使用しているポートを確認できます。

手順 4: Oracle を SecurID クライアントとして構成

Windows NT および Windows 95/98 プラットフォーム

SecurID 管理者から次のものを入手する必要があります。

- ルート・ドライブ ¥VAR¥ACE にある SDCONF.REC ファイル
- Windows NT のサービス・ファイルにあるポート番号とサービス名

UNIX プラットフォームおよび ACE/Server リリース 1.2.4

> **ACE/Server リリース 2.0 の場合：** 6-5 ページの「UNIX プラットフォームおよび ACE/Server リリース 2.0」を参照してください。

Oracle Server マシンに SecurID 構成ファイルをインストールします。他の任意の SecurID クライアントまたは ACE/Server を稼働しているマシンから、SecurID 構成ファイルを取得できます。

通常、これらのファイルは /var/ace に格納されています。Oracle Server マシン上でこのディレクトリを作成し、構成ファイルをそのディレクトリにコピーします。少なくとも、sdconf.rec ファイルは必要です。構成ファイルは、Oracle および標準の SecurID ツールによって使用されます。SecurID のツールは setuid root を実行するので、/var/ace ディレクトリおよびこのディレクトリ内のファイルに対するアクセス許可に関して、問題が生じる場合があります。Oracle 実行可能ファイルの所有者（「oracle8」ユーザーなど）が、/var/ace ディレクトリ内のファイルをすべて読み取ることができ、このディレクトリ内で新しいファイルを作成できるかどうか確認してください。

注意： Oracle setuid root を実行して、この問題を解決しようとしてはいけません。この方法は不要であるだけでなく、危険でもあります。

セキュリティを損なわないでこの問題を解決する方法が 2 つあります。どちらの方法でも問題を解決できますが、第 1 の方法をお薦めします。どちらの方法でも、Oracle で SecurID 認証を使用できます。また、SecurID の他のツールを引き続き使用することもできます。

第 1 の方法

Oracle 実行可能ファイルの所有者は、/var/ace ディレクトリおよびそのディレクトリ内のファイルも所有している必要があります。たとえば、Oracle 実行可能ファイルの所有者が「oracle8」ユーザーの場合は、次の手順をルートとして実行します。

```
# chown oracle8 /var/ace
# chmod 0770 /var/ace
# chown oracle8 /var/ace/*
# chmod 0660 /var/ace/*
```

第 2 の方法

この方法では、ルートに /var/ace ディレクトリとそのディレクトリ内のファイルを所有させますが、Oracle グループに読取りアクセスと書込みアクセスを許可します。Oracle グループが「dba」の場合は、次の手順をルートとして実行する必要があります。

```
# chown root /var/ace
# chmod 0770 /var/ace
# chgrp dba /var/ace
# chown root /var/ace/*
# chmod 0660 /var/ace/*
# chgrp dba /var/ace/*
```

UNIX プラットフォームおよび ACE/Server リリース 2.0

次の点に注意してください。

- VAR_ACE 環境変数はサポートされていません。構成データを /var/ace ディレクトリに格納する必要があります。これ以外の場所に ACE 構成データを格納してある場合は、次のコマンドを使用してシンボリック・リンクを作成する必要があります。

  ```
  # ln -s $VAR_ACE /var/ace
  ```

- Oracle は ACE 構成データを読み書きできなければなりません。このデータは /var/ace ディレクトリ（上記のシンボリック・リンクを使用する場合は、$VAR_ACE）に格納されています。

Oracle が構成データを読み取れるかどうかは、ACE クライアント・ソフトウェアを Oracle Server にどのようにインストールしたかによって決まります。ACE クライアント・ソフトウェアのインストール中に、どの管理者が構成ファイルを所有する必要があるか指定できます。

注意： 次に示す第 1 の方法と第 2 の方法のどちらを使用する場合でも、Oracle をルートとしてインストールしないでください。

第 1 の方法

ルートが ACE サーバーの構成データ・ファイルを所有している場合は、Oracle 実行可能ファイルの所有者がこれらのファイルを読み書きできるように、UNIX ファイルに対する許可を変更する必要があります。たとえば、次のコマンドを実行して、Oracle がファイルにアクセスできるようにし、setuid root を実行するすべての Security Dynamics ツールもファイルにアクセスできるようにします。

```
# chown oracle8 /var/ace
# chown oracle8 /var/ace/*
# chmod 0770 /var/ace
# chmod 0660 /var/ace/*
```

環境変数 VAR_ACE が /var/ace 以外の場所に設定されている場合は、次のコマンドを実行する必要があります。

```
# ln -s $VAR_ACE /var/ace
# chown oracle8 $VAR_ACE
# chown oracle8 $VAR_ACE/*
# chmod 0770 $VAR_ACE
# chmod 0660 $VAR_ACE/*
```

第 2 の方法

ACE ファイルの所有者がルートでない場合は、次に示す 2 つの方法があります。

- ACE クライアントまたは ACE サーバーおよび Oracle を、同じ UNIX アカウントでインストールします（ACE ソフトウェアをルートとしてインストールする必要がありますが、どの管理者をファイルの所有者にするかを指定できます。Oracle 実行可能ファイルの所有者と同じユーザー（通常は「Oracle8」）を指定します）。
- Oracle 実行可能ファイルの所有者を ACE 管理者のグループに追加します。

注意： Oracle 実行可能ファイルの所有者は、DBA グループのメンバーでなければなりません。そうでないと、データベースを制御できません。

変更内容を有効にするために、次の操作を実行します。

1. ログアウトしてから、Oracle 所有者として再びログインします。
2. ネットワーク・リスナーを再起動します。
3. Oracle Server を再起動します。

手順 5: SecurID 認証を構成

SecurID 認証を構成するには、Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して sqlnet.ora ファイルを変更します。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ― *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

Oracle Net8 Assistant による変更内容の保存

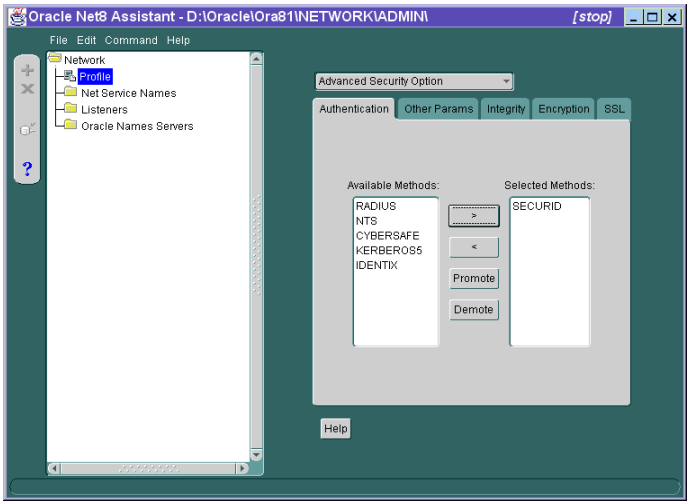
メニュー・バーの「File」->「Save Network Configuration」をクリックします。

各パラメータの設定方法を以下に示します。

クライアントとサーバーでの認証方式の構成

SQLNET.AUTHENTICATION_SERVICES パラメータを設定します。

図 6-1 Oracle Net8 Assistant を使用した認証の構成



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
1. 「Authentication」タブを選択します。 2. 「Available Methods」リストで「SECURID」を選択します。 3. 「>」ボタンをクリックして、メソッドを「Selected Methods」リストに移動します。他に使用するメソッドがあれば同じ方法で移動します。 4. 選択したメソッドを使用優先順位の高い順に並べます。リストでメソッドを選択し、「Promote」または「Demote」をクリックして並べ替えます。たとえば、SECURID メソッドを最初に使用する場合は、SECURID をリストの先頭に置きます。	次のパラメータを設定します。 `SQLNET.AUTHENTICATION_SERVICES=(`*`SECURID`*`)`

SecurID 認証のためのユーザーを作成

次の手順に従って、SecurID 認証のためのユーザーを作成します。

- 手順 1: Security Dynamics の sdadmin プログラムによる個人へのカードの割り当て
- 手順 2: このユーザーの Oracle Server アカウントを作成
- 手順 3: データベース権限をユーザーに付与

手順 1: Security Dynamics の sdadmin プログラムによる個人へのカードの割り当て

新しいユーザーを作成するときに、sdadmin ツールがログイン名を尋ねてきたら、後で Oracle ユーザーを作成するときに使用する名前を入力します。

> **詳細情報：** このマニュアルの「はじめに」の xiv ページの「関連マニュアル」に示した Security Dynamics のマニュアルを参照してください。

ユーザーが Oracle ツールを使用してカードの PIN を新規に指定できるようにしたい場合は、ユーザー自身の PIN を作成可能にするオプションを選択します。このオプションを選択しない場合は、カードが新規 PIN モードのときに、ユーザーが Security Dynamics のツールを使用して PIN を生成する必要があります。Oracle Server 上でユーザーをアクティブにします（Oracle Server は、すでに SecurID クライアントとして登録されている必要があります）。

手順 2: このユーザーの Oracle Server アカウントを作成

このアカウントを作成するには、「Create User」データベース・ロールを持つユーザーとして接続した SQL*Plus を使用します。次の構文を使用してアカウントを作成します。

```
SQL> CONNECT system/manager
SQL> CREATE USER os_authent_prefix username IDENTIFIED EXTERNALLY
```

OS_AUTHENT_PREFIX は、（init.ora ファイルなどに存在する）Oracle Server 初期化パラメータです。OS_AUTHENT_PREFIX のデフォルト値は OPS$ です。ユーザー名は、前述の手順 1 でカードに割り当てた名前と同じである必要があります。

注意： ユーザー名は長くてかまいませんが、Oracle ユーザー名は 30 字に制限されているので、次に示すように OS_AUTHENT_PREFIX を NULL 値に設定することを強くお薦めします。

```
OS_AUTHENT_PREFIX=""
```

この時点では、Oracle ユーザー（*username*）はまだ存在することはできません。

たとえば、カードをユーザー「king」に割り当て、OS_AUTHENT_PREFIX を NULL 値（""）に設定したと想定します。この時点で、次の構文を使用して、Oracle ユーザー・アカウントを作成する必要があります。

```
SQL> CREATE USER king IDENTIFIED EXTERNALLY;
```

手順 3: データベース権限をユーザーに付与

このユーザーにデータベース権限を付与することができます。ユーザーは少なくとも「セッション作成」権限を持つ必要があります。

```
SQL> GRANT CREATE SESSION TO king;
```

これで、ユーザー「king」が適切な SecurID カードを使用して Oracle に接続できます。

> **詳細情報：** SecurID 認証をインストールし構成した後で Oracle Server にログインする方法については、6-13 ページの「Oracle Server へのログイン」を参照してください。

SecurID 認証の構成に関するトラブルシューティング

SecurID 認証の構成中に問題が発生した場合は、次の点を確認してください。

- サービス・マップに、Security Dynamics ACE サーバーのエントリがなければなりません。通常、サービス名は securid ですが、SecurID 管理者が任意の名前を選択できます。

  SecurID の kitconts ツール（ACE/Server 1.2.4 の場合）または sdinfo ツール（ACE/Server 2.0 の場合）を使用して、認証サービスの名前、および SecurID が使用するポート番号を確認します。これらのポート番号が、/etc/services ファイルに格納されているポート番号（NIS を使用している場合は、サービス・マップ）と一致しているかどうかを確認します。

  ACE/Server リリース 1.2.4 のみ : /var/ace/sdconf.rec ファイルが、Oracle Server を稼働しているマシンに存在しているかどうか確認します。また、Oracle プロセスが /var/ace ディレクトリを読み書きできるように、/var/ace/sdconf.rec ファイルと /var/ace ディレクトリに対する許可が設定されているかどうかを確認します。

  ACE/Server リリース 2.0 のみ : ACE 構成データが、/var/ace ディレクトリにあるかどうか確認します。VAR_ACE 環境変数を使用することはできません。Oracle 実行可能ファイルの所有者が、このディレクトリ内のファイルを読み書きできるかどうかも確認してください。

- Oracle Server マシンが SecurID クライアントとして登録されているかどうかをチェックします。これをチェックするには、Security Dynamics の sdadmin ツールを使用します。

- Oracle に接続しようとするユーザーは、直接ユーザーまたはユーザー・グループのメンバーとして、Oracle Server 上でアクティブである必要があります。SecurID の sdadmin ツールを使用して、これをチェックします。

- Security Dynamics には、問題の検出に役立ついくつかのロギング機能が組み込まれています。sdadmin を使用して、最近のシステム・アクティビティ（障害のために失敗した認証など）のログを見ることができます。また、sdlogmon を使用して、同様のログ・リストを取得することもできます。

- Oracle 側の SQLNET.ORA ファイルに次の行を追加して、トレース機能をオンにします。

  ```
  trace_level_server = admin
  ```

  クライアント側でトレース機能をオンにしても、有益な情報はあまり得られません。これは、Oracle Server と ACE サーバーのすべてのやりとりが、SQL*Net 接続または Net8 接続の Oracle Server 側で行われるからです。チェックが完了したら、トレース機能をオフにしてください。

- ユーザーが適切な接頭辞（デフォルトは OPS$）を持つ外部識別ユーザーとして、Oracle データベース内で作成されているかどうか確認します。「System」として接続して、次のように入力して、

  ```
  SQL> SELECT * FROM all_users;
  ```

データベース・ユーザーの一覧リストを表示します。

- 非外部識別ユーザーとして Oracle に接続すると、SecurID ログ・ファイルが警告を表示します。たとえば、次のように入力して「System」として接続するとします。

```
sqlplus system/manager@oracle_dbname
```

SecurID ログ・ファイルが次の警告を表示します。

```
03/24/95   10:04  User not on client machinename
```

これはエラーではありません。Oracle クライアントと Oracle Server は、SQLNET.ORA ファイルに SQLNET.AUTHENTICATION_SERVICES 行があったため SecurID を使用するかどうか折衝したので、Oracle は ACE/Server に「System」を検証するように指示します。検証が失敗すると、Oracle がパスワードを内部的に検証します。パスワードが有効であれば、接続できます。

警告メッセージを表示しないようにするには、SecurID 認証を使用禁止にする以外にありません。使用禁止にするには、Oracle クライアント上の sqlnet.ora ファイルを次のように変更します。

```
SQLNET.AUTHENTICATION_SERVICES=(NONE)
```

このパラメータをこのように設定すると、SecurID 認証アダプタが使用禁止になります。これ以降は、SecurID カードを使用して Oracle に接続できません。

SecurID 認証の使用

この項では、SecurID 認証を Oracle クライアント・ツールで使用する方法について説明します。ここでは、読者が SecurID の概念に精通していること、および SecurID 認証を使用するために Oracle が構成されていることを想定しています。

この項では、次のトピックについて説明します。

- Oracle Server へのログイン
- 新しい PIN を SecurID カードに割り当てる
- SecurID カードが「次コード」モードで動作している場合のログイン方法

> **詳細情報：** 6-7 ページの「手順 5: SecurID 認証を構成」を参照してください。このマニュアルの「はじめに」の xvii ページの「関連マニュアル」も参照してください。

SecurID 認証を使用してパスワードを検証する前に、次の作業が完了していることを確認します。

- SecurID 認証アダプタをインストールして、SQL*Net 構成または Net8 構成にリンクしてあること
- ACE/Server を使用できるように Oracle を構成してあること（つまり、Oracle を SecurID クライアントとして構成してあること）
- データベース・パスワードを SecurID 認証サーバーで検証できるように、クライアントとサーバー上で必要なパラメータを設定してあること
- 6-7 ページの「手順 5: SecurID 認証を構成」の説明に従って、SecurID 認証で使用するユーザーを構成してあること

Oracle Server へのログイン

SecurID 認証を使用すると、SecurID カードで生成した PASSCODE で Oracle Server にログインできます。PASSCODE は、Oracle 接続文の中のパスワードと置き替わります。

SecurID カードには、次の 2 つのタイプがあります。

- 標準（モデル SD200）
- PINPAD（モデル SD520）

カードのタイプに応じて、PIN を次のように入力します。

- カードに直接入力する

または

- Oracle 接続文の一部として入力する

標準カードを使用

標準カードを使用して、PASSCODE を生成し表示します。Oracle にログインするときは、次の構文を使用して自分のユーザー名と PIN、および現行の PASSCODE を指定する必要があります。

```
sqlplus username/<pin><passcode>@net_service_name
```

たとえば、カードがユーザー「king」に割り当てられていて、PIN が「3511」で、カードが「698244」という番号を表示した場合は、次のように SQL*Plus を使用して Oracle にログインします。

```
% sqlplus king/3511698244@oracle_database
```

または

```
% sqlplus king@oracle_database
% enter password: 3511698244
```

注意： Security Dynamics のツールは、PIN と PASSCODE を区切る記号として次の文字をサポートしています。

"" <tab> ¥ / ; :

しかし、Oracle はこれらの文字を区切り記号として解釈しないので、これらの文字を使用しないでください。

PINPAD カードを使用

PINPAD カードを使用する場合は、最初に、自分の PIN をカードに入力して、新しい PASSCODE を生成する必要があります。次に示す構文でこの PASSCODE を使用して、Oracle に接続します。

```
sqlplus username/passcode@net_service_name
```

たとえば、カードがユーザー「king」に割り当てられている場合は、最初に、PINPAD カードに PIN を入力して PASSCODE を生成します（この方法については、Security Dynamics のマニュアルを参照してください）。PASSCODE として「698244」が生成された場合は、次のように SQL*Plus を使用して Oracle に接続します。

```
% sqlplus king/698244@oracle_dbname
```

新しい PIN を SecurID カードに割り当てる

初めてログインする場合、または管理者が新規 PIN モードにカードを設定している場合は、PIN をカードに割り当てる必要があります。Oracle に接続しようとして次のエラー・メッセージが表示された場合に、この作業を行う必要があります。

```
ORA-12681 "Login failed: the SecurID card does not have a pincode yet"
```

特殊な構文を使用して Oracle Server に接続することで、PIN をカードに割り当てることができます。まず、PIN を選択します。通常、PIN の長さは 4 ～ 8 桁です。所有している SecurID カードのタイプによっては、文字を使用できる場合もあります。

古い PIN をクリアした場合

Oracle データベースに接続している間に、次の構文を使用します。

```
sqlplus username/+<new_pin>+<tokencode>@oracle_dbname
```

> **注意：** PIN をカードに割り当てようとしていることを Oracle に伝えるために、接続文字列に 2 つの「+」文字を追加する必要があります。これらの文字は、新しい PIN と PASSCODE と区切る役割も果たします。
>
> また、PIN と PASSCODE の組合せを二重引用符で囲む必要があります。SQL*Plus などの Oracle ツールは、正符号（+）の直前までにパスワード文字列（PIN/PASSCODE）を切りつめます。パスワード文字列（PIN/ パスコード) を二重引用符（"") で囲むことによって、パスワード文字列が切り捨てられるのを防止できます。

tokencode の部分には、SecurID カードの LCD に現在表示されているカード・コードを入力します。PINPAD カードを所有している場合は、PIN をカードに入力しません。

たとえば、カードがユーザー「king」に割り当てられていて、新しい PIN が「45618」で、SecurID カードに「564728」という番号が表示されている場合は、次のように入力します。

```
% sqlplus king/'"+45618+564728"'@oracle_dbname
```

古い PIN をクリアしていない場合

データベースに接続している間に、次の構文を使用します。行わない場合は、管理者が新しい PIN を選択する必要があります。

```
sqlplus username/+<new_pin>+<old_pin><tokencode>@oracle_dbname
```

tokencode の部分には、SecurID カードの LCD に現在表示されているカード・コードを入力します。PINPAD カードを所有している場合は、PIN をカードに入力しません。

新しい PIN が受け入れられると、Oracle に接続されます。次に Oracle に接続するときは、「Oracle Server へのログイン」で説明した手順で行います。新しい PIN が拒否されると、次のエラー・メッセージが表示されます。

```
ORA-12688 "Login failed: the SecurID server rejected the new pincode"
```

PIN が拒否される理由

- 新しい PIN の長さが 4 文字未満か 8 文字を超えている。
- PIN に無効な文字が含まれている。有効な文字は数字です。一部の SecurID カードでは、「a」～「z」の文字も有効です。
- ユーザーが独自の PIN を作成できない。自分自身の PIN を作成できるように、Security Dynamics ACE/Server が構成されていません。この場合は、Security Dynamics ツールを使用して、カード用に新しい PIN を生成する必要があります。

SecurID カードが「次コード」モードで動作している場合のログイン方法

追加の安全保護対策として、ログインしようとしているユーザーに次のカード・コードを入力するように ACE/Server が指示して、そのユーザーが実際にカードを所有しているかどうかを確認する場合があります。これは、Oracle にログインしようとして次のエラー・メッセージが表示される場合です。

```
ORA-12682, "Login failed: the SecurID card is in next PRN mode"
```

次に Oracle にログインするときは、次の 2 つのカード・コードを指定する必要があります。Oracle にログインするときに使用する構文は、SecurID カードのタイプ（標準カードまたは PINPAD カード）によって異なります。

標準カードでのログイン

標準カードでログインするときは、次の項目を指定します。

1. 自分の PIN
2. 現行のカード・コード
3. 「+」文字と次のカード・コード

前述の手順 1、2、3 によって、パスワードが置き替えられます。「+」文字は、最初のカード・コード（PASSCODE）と 2 番目のカード・コードを区切る重要な文字です。次の構文を使用します。

```
sqlplus <username>/ "<pincode><passcode>+<next passcode>"@<net_service_name>
```

注意： PIN/PASSCODE/ 次の PASSCODE の組合せを二重引用符で囲む必要があります。SQL*Plus のような Oracle ツールは、正符号（+）の直前までにパスワード組合せを切りつめてしまいます。PIN と PASSCODE を二重引用符（""）で囲むことによって、パスワード組合せが切りつめられるのを防止できます。

たとえば、カードがユーザー「king」に割り当てられていて、PIN が「3511」で、カードの最初の番号が「698244」で、次の番号が「563866」の場合は、次のように入力します。

```
% sqlplus king/"3511698244+563866"@oracle_database
```

これによって、Oracle Server に接続され、カードが通常モードに戻ります。次に Oracle Server にログインするときは、6-13 ページの「Oracle Server へのログイン」で説明した手順を使用します。

PINPAD カードでのログイン

PINPAD カードを所有している場合は、次の手順で Oracle Server にログインします。

1. 自分の PIN をカードに入力して最初の PASSCODE を生成します。
2. P を押してカードのメモリーをクリアしてから、次の PASSCODE が生成されるのを待ちます。
3. これらの 2 つの PASSCODE を「+」文字で区切って、Oracle Server にログインします。次の構文を使用します。

   ```
   sqlplus <username>/ "<first passcode>+<second passcode>"@net_service_name
   ```

たとえば、カードがユーザー「king」に割り当てられている場合は、次の手順でログインします。

1. PINPAD カードに PIN を入力して PASSCODE（「231003」など）を生成します。
2. カードのメモリーをクリアします。次に表示される番号が「831234」だとします。
3. 手順 1 と 2 で生成した 2 つの PASSCODE を次のように入力してログインします。

   ```
   % sqlplus king/"231003+831234"@oracle_dbname
   ```

これによって Oracle Server に接続し、カードが通常モードに戻ります。次に Oracle にログインするときは、6-13 ページの「Oracle Server へのログイン」で説明した手順を使用します。

7

Identix Biometric 認証の構成

この章では、Identix Biometric 認証を使用する Oracle の構成方法について説明します。次のトピックについて説明します。

概要

Biometric Authentication Service は、Identix Biometric 認証アダプタを使用して、改ざん防止のためにユーザーを生体的に認証します。これは、秘密鍵 MD5 ハッシング機能、および生体的に識別したユーザーの集中管理、生体的に識別したユーザーを認証するデータベース・サーバーの集中管理によって提供されます。

この項では、クライアント / サーバー環境での Biometric Authentication Service の動作について説明します。

図 7-1　一般的な Biometric Authentication Service の構成

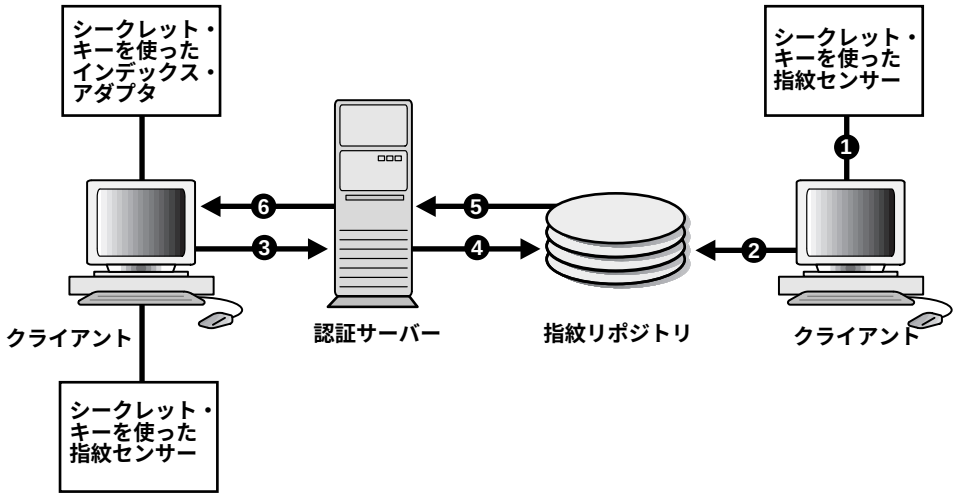


図 7-1 に Biometric Authentication Service の構成要素と構成を示します。

- 指紋リポジトリを担当する管理者は、複数のユーザーの指紋テンプレートを登録し、指紋サーバーに認証用のデータを提供するすべてのデータベースに対して DEFAULT ポリシーを定義します。
- Fingerprint Security Service Administrator は、デスクトップ指紋スキャナを使用してユーザーの指紋を読み取り、テンプレートに変換して、測定精度とともに Oracle Biometric Authentication Service に送ります。Oracle Biometric Authentication Service は、送られた指紋を指紋リポジトリ（Oracle データベース）に格納します。指紋の測定精度は、格納済みの指紋テンプレートと認証用にスキャンされたユーザーの指紋を比較するときの信頼度を示す指標となります。登録データの品質は、0 ～ 100% のスコアで表されます。たとえば、ユーザー登録データの品質が 72% というように表されます。
- Fingerprint Security Service Administrator は、生体的に識別されたユーザーを認証するすべてのデータベース・サーバーに対して、DEFAULT と呼ばれる 1 つのセキュリティ・ポリシーも定義します。セキュリティ・ポリシーは、そのデータベース・サー

バーからデータを提供されるすべてのクライアントに適用されます。セキュリティ・ポリシーには、シークレット・キーと 3 つのタイプの指紋しきい値レベル（検証、虚偽の指、ハイ・セキュリティ）が含まれています。

- クライアント側では、認証が行われる前に、Fingerprint Security Service Administrator が各クライアントの指紋センサーにシークレット・キーを格納します。指紋センサーに格納されたシークレット・キーは、セキュリティ・ポリシーに格納されているシークレット・キーと照合されます。
- クライアント側では、ユーザーの認証要求に応じて、データベース・サーバーが指紋サーバーの DEFAULT セキュリティ・ポリシーから取得した一連の値をクライアントに適用します。次に示す 3 つのしきい値レベルがあります。
  - 検証しきい値
  - 虚偽の指しきい値
  - ハイ・セキュリティしきい値

  これらのしきい値レベルの詳細は、Identix のマニュアルを参照してください。
- クライアント側では、Biometric Authentication Service がユーザーの指紋テンプレートとしきい値をセンサーに渡します。次に、ユーザーの指紋がスキャンされ、その検証結果、指紋テンプレート、シークレット・キー、およびしきい値を使用してハッシュが生成されます。このハッシュがサーバー側のアダプタに送られ、サーバー側のアダプタで生成されたハッシュと比較されます。

Biometric Authentication Service のアーキテクチャ

Biometric Authentication Service は、次のモジュールで構成されています。

- Biometric Manager。管理者はこのモジュールを使用して、セキュリティ・ポリシーと指紋を入力します。このマニュアルでは、これ以降、Biometric Manager のことを単にマネージャともいいます。
- Biometric Authentication Server（指紋リポジトリ）。このリポジトリに、セキュリティ・ポリシーと指紋テンプレートが格納されます。本番 Oracle データベース・サーバーを認証用に構成したバージョンです。このマニュアルでは、これ以降、Biometric Authentication Server を単に認証サーバーともいいます。
- Identix 認証アダプタ。クライアント側とデータベース・サーバー側の両方でこの認証アダプタを使用して、認証サーバーとクライアントが生体的認証データをやり取りして、データベース・ユーザーを認証します。

マネージャとクライアント側のアダプタが、Identix 製品（TouchNet II ソフトウェア・ライブラリ、TouchNet II ハードウェア・インタフェース、TouchNet II デスクトップ・センサー、TouchNet III ソフトウェア・ライブラリ、TouchNet III デスクトップ・センサー）とのインタフェースになります。

詳細情報： Identix 製品を説明する Identix マニュアルの一覧は、このマニュアルの「はじめに」の xvii ページの「関連マニュアル」を参照してください。

管理アーキテクチャ

Fingerprint Security Server Administrator は、マネージャを使用してユーザーの指紋を走査し、指紋の精度を測定し、データベース・サーバーのセキュリティ・ポリシーを確立します。マネージャはこの情報を認証サーバーに送信して、リポジトリにデータを格納します。

管理者または信用できる人が Identix TouchNet II ソフトウェアまたは Identix TouchNet III ソフトウェアを使用して、シークレット・キーを TouchNet II デバイスまたは TouchNet III デバイスに格納します。このキーが DEFAULT セキュリティ・ポリシーに格納されているキーと一致しなければ、認証が行われません。

認証アーキテクチャ

システムを使用するユーザーは、TouchNet II または TouchNet III デスクトップ・センサーに指紋を登録する必要があります。クライアント側のアダプタは、認証要求をサーバー側のアダプタに送ります。サーバー側のアダプタは、認証サーバーに格納されている登録済み指紋を使用して指紋を比較します。クライアントから認証要求が行われるたびに、認証サーバーがユーザーの指紋とデータベース・サーバーのセキュリティ・ポリシーを取り出し、サーバー側のアダプタを通じてクライアント側のアダプタに送り返します。

ユーザーから認証要求が行われると、Oracle Advanced Security Identix 認証アダプタ（クライアント側）が要求を Biometric Authentication Adapter（サーバー側）に送ります。サーバー側のアダプタは認証サーバーでユーザーの指紋を検索して、認証サーバーが、格納済みの指紋とセキュリティ・ポリシーを戻します。

アダプタ（クライアント側）は、セキュリティ・ポリシーに含まれているしきい値レベル値と TouchNet II ソフトウェア・ライブラリを使用して、TouchNet II デスクトップ・センサー上でしきい値を設定します。次に、TouchNet II デスクトップ・センサーにユーザーの指を置くように指示します。クライアント上とデータベース・サーバー上のアダプタは協力して、ユーザーの指紋、シークレット・キー、しきい値レベルを、管理者が認証サーバー・リポジトリに入力したセキュリティ・ポリシーと比較します。このデータが一致している場合は、ユーザーが認証されます。

前提条件

- マネージャ PC として動作する Windows NT マシンで、リリース 2.0 以降の Oracle Enterprise Manager が稼働している必要があります。
- クライアント PC として動作する Windows NT マシンまたは Windows 95 マシンで、Net8 が稼働している必要があります。

- 認証サーバーと各データベース・サーバーで、Oracle8 リリース 8.0.3 以降または Oracle8*i* が稼働している必要があります。
- Oracle Advanced Security をインストールする前に、それぞれの Windows NT クライアントと Windows 95 クライアントで、Net8 がデータベース・サーバーと接続されているかどうかを確認する必要があります。

TouchSAFE II Encrypt Device Driver for Windows NT のインストール

Biometric Manager をインストールすると、必要な TouchNet II ソフトウェアが自動的にインストールされ、デバイスが必要に応じて自動的に構成されます。

Biometrics Manager のインストール中、Identix TouchSafe II Device Driver をインストーラでセットアップしないように選択できます。その場合は次の手順で手動で構成します。

1. ディレクトリ $ORACLE_HOME¥IDENTIX に移動します。
   - デフォルト IO ポート番号 280 とデフォルトの Windows NT ディレクトリを使用している場合は、手順 4 に進みます。
   - デフォルト IO ポート番号 280 を使用していない場合は、手順 2 に進みます。
   - デフォルトの Windows NT ディレクトリが C:¥WINNT35¥SYSTEM32¥DRIVERS でない場合は、手順 3 に進みます。
2. ETSIINT.INI の IoPortAddress パラメータを、現在の TouchSafe II Encrypt I/O ポート設定に変更します。たとえば、次のとおりです。

   ```
   IoPortAddress = REG_DWORD 0x00000360  for I/O port 0x360
   ```

3. ETSIINT.BAT の Windows NT ディレクトリの設定値を、現在の Windows NT ディレクトリに変更します。

   たとえば、次のとおりです。

   ```
   copy etsiint.sys c:¥winnt¥system32¥drivers
   -> copy etsiint.sys path¥drivers
   ```

4. バッチ・ファイル ETSIINT.BAT を実行します。
5. Identix デモ・プログラムの SetKey ユーティリティを使用して、ハッシュ・キーを 16 進で設定します。たとえば、キーに C001BABY を設定します（この値は使用しないでください）。ハッシュ・キーが DEFAULT セキュリティ・ポリシーで設定されているものと完全に一致するようにします。
6. システムを再起動して、デバイス・ドライバを有効にします。
7. 再起動したあと、デバイス・コントロール・パネルでデバイス・ドライバが有効になっていることを確認します。デバイス ETSIINT はすでに起動されている必要があります。

Biometric Manager PC

マネージャ PC 上で、次の作業を行います。

1. Oracle Server と Oracle クライアントの両方に Oracle Enterprise Manager をインストールします。
2. Identix ハードウェアと Identix ドライバ・ファームウェアをインストールして、Identix の変数とデバイスを構成します。

   詳細情報： Identix Readme ファイルを参照してください。

3. Identix TouchNet II (Encrypt) 2.0 または TouchNet III をインストールしテストします。

   詳細情報： 7-5 ページの「TouchSAFE II Encrypt Device Driver for Windows NT のインストール」とプラットフォーム固有のインストレーション・マニュアルを参照してください。

Identix マニュアルの指示に従って、モジュールが Identix デモ用プログラムで機能するかどうかを確認します。このデモ用プログラムが PC で動作しなければ、他の Oracle 製品を PC にロードできません。詳細は、Identix Readme ファイルを参照してください。

クライアント PC

各クライアント PC 上で、次の作業を行います。

1. Identix ハードウェアと Identix ドライバ・ファームウェアをインストールして、Identix の変数とデバイスを構成します。詳細は、Identix Readme ファイルを参照してください。
2. Identix TouchNet II (Encrypt) 2.0 または TouchNet III をインストールしテストします。Identix マニュアルの指示に従って、モジュールが Identix デモ用プログラムで機能するかどうかを確認します。このデモ用プログラムが PC で動作しなければ、他の Oracle 製品を PC にロードできません。

   詳細情報： 7-5 ページの「TouchSAFE II Encrypt Device Driver for Windows NT のインストール」とプラットフォーム固有のインストレーション・マニュアルを参照してください。

3. Oracle Advanced Security Identix 認証アダプタをインストールします。

   詳細情報： プラットフォーム固有のマニュアルを参照してください。Identix Readme ファイルも参照してください。

データベース・サーバー

Biometric サービスを使用してユーザーを認証するそれぞれの本番データベース上に、Biometric 認証アダプタをインストールする必要があります。プラットフォーム固有のマニュアルの指示に従って、Biometric 認証アダプタをインストールします。

注意： 指紋リポジトリを格納しているデータベースにはアダプタはインストールしないでください。

Biometric Authentication Service

Biometric Authentication Service は、ユーザー情報と指紋情報を格納するデータベースです。このデータベースには、バージョン 8.0.3 以降の任意の Oracle 本番データベースを使用することができます。このデータベースは、セキュリティとアクセスが厳密に管理された信頼できるシステムでなければなりません。このデータベースにはアダプタをインストールしません。

Biometric 認証の使用

Biometric Authentication Service を構成するには、次の作業を行います。各作業の詳細は以下で説明しています。

手順 1: 認証サーバーとして機能するデータベース・サーバーを構成

1. SYSTEM/MANAGER として（または、任意のシステム・パスワードを使用して）、データベース・サーバーに接続します。
2. 次のように接続してテストします。

```
ofm_admin/ofm_admin
```

手順 2: Identix を構成

Identix 認証を構成するには、次の手順で行います。各作業は以下で説明しています。

- Oracle Server と Oracle クライアントでの認証メソッドの構成
- クライアントとサーバーでの指紋サーバー名の構成
- ユーザー名、パスワード、指紋メソッドの構成
- INIT.ORA ファイルの構成
- ORACLE.INI ファイルの構成

特に示されていない限り、Identix 認証を構成するには、Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して sqlnet.ora ファイルを変更します。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ー *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

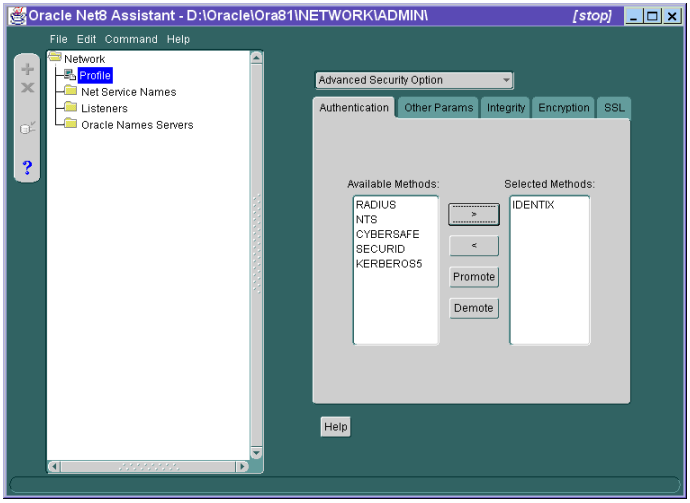
Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

Oracle Server と Oracle クライアントでの認証メソッドの構成

SQLNET.AUTHENTICATION_SERVICES パラメータを設定します。

図 7-2 Oracle Net8 Assistant を使用した認証の構成

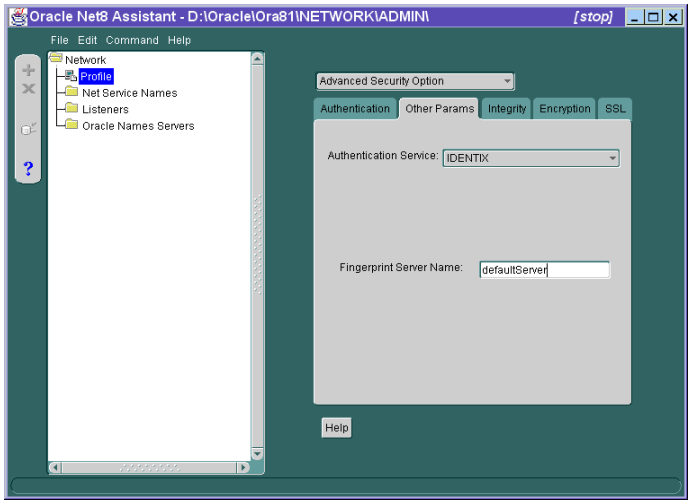


Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 7-2 を参照してください。 1. 「Authentication」タブを選択します。 2. 「Available Methods」リストで、「Identix」を選択します。 3. 「>」ボタンをクリックして、メソッドを「Selected Methods」リストに移動します。他に使用するメソッドがあれば同じ方法で移動します。 4. 選択したメソッドを使用優先順位の高い順に並べます。リストでメソッドを選択し、「Promote」または「Demote」をクリックして並べ替えます。たとえば、Identix メソッドを最初に使用する場合は、Identix をリストの先頭に置きます。	次のパラメータを設定します。 `SQLNET.AUTHENTICATION_SERVICES=(`*IDENTIX*`)`

クライアントとサーバーでの指紋サーバー名の構成

SQLNET.IDENTIX_FINGERPRINT_DATABASE パラメータを設定します。

図 7-3 Oracle Net8 Assistant を使用した指紋サーバー名の構成



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 7-3 を参照してください。 1. 「Other Params」タブを選択します。 2. 「Authentication Service」ドロップダウン・リスト・ボックスをクリックして、「IDENTIX」を選択します。 3. 「Fingerprint Server Name」ボックスに指紋サーバーの名前を入力します。	次のパラメータを設定します。 `SQLNET.IDENTIX_FINGERPRINT_DATABASE=` *service_name* service_name は認証サーバーの名前です。

ユーザー名、パスワード、指紋メソッドの構成

テキスト・エディタを使用して、次のパラメータを sqlnet.ora ファイルに設定します。

```
sqlnet.identix_fingerprint_database_user= ofm_client
sqlnet.identix_fingerprint_database_password= ofm_client
sqlnet.identix_fingerprint_method= oracle
```

username は定式ユーザー名 ofm_client で、password は定式パスワード ofm_client です。

注意： サンプル・ディレクトリに、これらのパラメータの設定方法を示すファイルが入っています。

注意： ユーザー名とパスワードの ofm_client を設定するには、NAUICAT.SQL を実行します。ofm_client を変更してはいけません。

INIT.ORA ファイルの構成

テキスト・エディタを使用して、次のパラメータを初期化ファイル（init.ora）に設定します。

```
REMOTE_OS_AUTHENT = false
OS_AUTHENT_PREFIX = ""
```

注意： データベース・サーバー上のローカル・ネーム構成ファイル（tnsnames.ora）に、指紋リポジトリのサービス名が入っている必要があります。それらが同じデータベース上にある場合は、次のパラメータでサービス名を使用します。

```
(security=(authentication_service=none))
```

ORACLE.INI ファイルの構成

oracle.ini ファイルの Oracle セクションに、テキスト・エディタを使用して USERNAME パラメータを指定します。このパラメータによって、クライアントがデータベースに接続するときに使用するデータベース・ユーザーの名前を設定します。

手順 3: 指紋リポジトリ・サーバーのネット・サービス名の設定

詳細情報： 『Oracle8*i* Net8 管理者ガイド』を参照してください。

手順 4: データベース・サーバーのアドレスがクライアントにアクセス可能なことを確認

詳細情報：『Oracle8*i* Net8 管理者ガイド』を参照してください。

手順 5: マネージャ PC を構成

認証サーバーに接続できるように、マネージャ PC にネット・サービス名を構成します。

詳細情報：『Oracle8*i* Net8 管理者ガイド』を参照してください。

Biometric Authentication Service の管理

Biometric Manager を使用して Biometric Authentication Service を管理します。

詳細情報： Identix のマニュアルを参照してください。

各クライアント上でのハッシュキーの作成

Identix Setkey ユーティリティを使用して、各クライアント上で 16 進のハッシュキー（FF30EE など）を作成します。ハッシュキーはすべてのクライアントで共通するキーであり、DEFAULT ポリシー・ハッシュキーと一致する必要があります。このキーの範囲は 1 ～ 32 の 16 進数字です。

Biometric 認証のユーザーの作成

1. クライアント上で、Windows NT User Manager を使用してユーザー名を作成します（このユーザー名は、次の手順で使用するユーザー名と同じでなければなりません）。
2. データベース・サーバー上で、データベースを再起動し、ユーザーの Oracle Server アカウントを作成します。ユーザー作成データベース・ロールを持つユーザーとして接続されている Oracle Enterprise Manager または SQL*Plus を使用している場合は、SQL*Plus を使用します。次の構文を使用してアカウントを作成します。

```
SQL> CONNECT system/manager
SQL> CREATE USER os_authent_prefix username IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO username
```

3. OS_AUTHENT_PREFIX は Oracle Server 初期化パラメータです。OS_AUTHENT_PREFIX のデフォルト値は OPS$ です。この手順で指定するユーザー名は、クライアントで作成したユーザー名と一致する必要があります。os_authent_prefix をリセットする場合は、データベースを停止して再起動する必要があります。

注意： Oracle ユーザー名は 30 字に制限されていて、ユーザー名には長い名前を使用できるので、次のように os_authent_prefix を NULL 値に設定することを強くお薦めします。

```
OS_AUTHENT_PREFIX=""
```

注意： ユーザー名が付いた Oracle ユーザーが存在することはできません。

例

ユーザー「king」を作成して、OS_AUTHENT_PREFIX を NULL 値（""）に設定する場合は、SQL*Plus を使用して次の構文で Oracle ユーザー・アカウントを作成する必要があります。

```
SQL> CREATE USER king IDENTIFIED EXTERNALLY;
```

ユーザーに少なくとも「セッション作成」権限を付与する必要があります。

```
SQL> GRANT CREATE SESSION TO king;
```

Biometric Manager を使用して、ユーザーを Biometric Authentication Service に登録します。

これで、ユーザー「king」を Oracle で生体的に認証できます。

詳細情報： 外部的に認証されるユーザーの作成については、『Oracle8*i* 管理者ガイド』と『Oracle8*i* 分散システム』を参照してください。

Biometric 認証がインストールされ構成されたあとにデータベース・サーバーにログインする方法は、7-15 ページの「Biometric Authentication Service でユーザーを認証」を参照してください。

クライアントにシークレット・キーを格納する方法は、Identix マニュアルを参照してください。

Biometric Authentication Service でユーザーを認証

ユーザーを認証するには、Biometric Authentication Service のインストールと構成が完了し、7-13 ページの「Biometric Authentication Service の管理」で説明した手順を実行しておく必要があります。

Biometric Authentication Service によるユーザーの認証

1. データベース管理者によって割り当てられたユーザー名でログオンします。
2. TouchNet II を使用している場合は、システム環境変数を設定します。次の変数は、TouchNet II ファームウェアの 10 ポート設定に基づいています。

   ```
   ETSII_IOPORT = 0X280
   ```

   注意： TouchNet III デバイスでは、環境変数 ETSII_IOPORT は使用しません。そのかわりに、tn3com.ini ファイルを使用してポートとボー・レートを設定します。

3. SQL*Plus を起動します。
4. SQL*Plus のプロンプトが表示されたら、データベース・サーバーの名前を入力します。

   ```
   SQL>connect /@net_service_name
   ```

   net_service_name がデータベース・サーバーの名前です。
5. 「Net8 Native Authentication」ダイアログ・ボックスが表示されたことを示すビープ音が鳴るまで待ちます。

   注意： システムによっては、現行ウィンドウの後ろにダイアログ・ボックスが表示される場合があります。ダイアログ・ボックスが表示されると、ビープ音が鳴ります。

6. 「Net8 Native Authentication」ダイアログ・ボックス内で「OK」をクリックします。
7. デスクトップ指紋センサーの上に指を置くように指示するメッセージが表示されたら、認証サーバー・リポジトリに入力した指と同じ指をセンサー上に置きます。
8. プロンプトが表示されたら指を離します。認証が成功したかどうかを示す別のプロンプトが表示されます。

認証に失敗し、「Access Denied」のメッセージが表示された場合
次のいずれかの方法を試してみます。

- 認証プロセスを再開します。

  詳細情報： 7-15 ページの「Biometric Authentication Service でユーザーを認証」を参照してください。

- セキュリティ管理者にしきい値を 80 まで下げてもらいます。
- セキュリティ管理者に再登録を依頼します。

  詳細情報： それぞれの作業手順については、Biometric Manager のオンライン・ヘルプを参照してください。

トラブルシューティング

Biometric 認証のインストール中または使用中に問題が発生した場合は、次の項目をチェックしてください。

- Identix Set Key ユーティリティのハッシュ・キーが、Biometric Manager の DEFAULT ポリシー・ハッシュ・キーと一致しているかどうかを確認します。
- NT ユーザー名は、データベース・サーバー内の外部識別ユーザー名、および Biometric Manager でユーザーを追加するときに使用したユーザー名と一致している必要があります。
- ドメイン名は一貫している必要があります。たとえば、ローカル名構成ファイル（tnsnames.ora）でサービス名の拡張子として .world を使用している場合は、プロファイル（sqlnet.ora）のサービス名にこの命名規則が反映されている必要があります。たとえば、次のとおりです。

```
TNSNAMES.ORA
biometrics.world = (DESCRIPTION =
                     (ADDRESS_LIST =
                      (ADDRESS =
                        ...
SQLNET.ORA
sqlnet.identix_fingerprint_database=biometrics.world
```

- 1 台のデータベースを、生体的認証サービスと本番データベースの両方に使用することができます。しかし、このような使用方法はお薦めしません。データベースをこのように使用する場合は、サーバー上および各 PC クライアント上のローカル名構成フィールド（TNSNAMES.ORA）に次の行のコードを追加してください。

```
(connect_data =
    (service_name = service_name)
    (security = (Authentication_service = NONE))
```

8

DCE GSSAPI 認証の構成

DCE GSSAPI 認証を使用すると、Oracle DCE Integration 製品の他の部分を使用しなくても DCE 認証サービスを利用できます。

この章では、DCE GSSAPI 認証の構成方法と使用方法について説明します。

注意： プラットフォームの Oracle Advanced Security リリース 8.1.5 で Oracle DCE Integration がサポートされているかどうかを、プラットフォーム固有のインストレーション・マニュアルで確認してください。

注意： すでに Oracle DCE Integration を使用している場合は、DCE GSSAPI 認証アダプタを使用する必要はありません。第 2 部「Oracle Advanced Security および Oracle DCE Integration」で説明するように、Oracle DCE Integration 製品には、DCE 認証機能が用意されています。

注意： この章は、読者が DCE の用語を十分理解していることを前提としています。DCE の詳細は、次のものを参照してください。

- このマニュアルの第 2 部「Oracle Advanced Security および Oracle DCE Integration」
- オペレーティング・システム固有の DCE 管理マニュアル
- このマニュアルの「はじめに」の「関連マニュアル」に示したマニュアルを参照してください。

DCE GSSAPI 認証の構成

DCE GSSAPI 認証を構成するには、次の作業を行います。各作業は以下で説明しています。

手順 1: DCE プリンシパルの作成

Oracle Server が認証の妥当性を検査する際に使用する DCE プリンシパルを作成するには、下の**太字**で示したコマンドを入力します。ここでは、Oracle Server のプリンシパル名を「oracle_server」と想定しています。データベース・サーバー上で次のコマンドを入力します。

```
% su
  password:    (root password is not echoed)
# dce_login cell_admin cell_admin_password
# rgy_edit
Current site is: registry server at
    /.../cellname/subsys/dce/sec/master
rgy_edit=> do p
Domain changed to: principal
rgy_edit=> add oracle_server
rgy_edit=> do a
Domain changed to: account
rgy_edit=> add oracle_server -g none -o none -pw oracle_server_
password -mp cell_admin_password
rgy_edit=> ktadd -p oracle_server -pw oracle_server_password
rgy_edit=> quit
bye
```

手順 2: 新しい DCE プリンシパルの構成と DCE GSSAPI 認証のオン

ここでは、Oracle Server のプリンシパル名を「oracle_server」と想定しています。

次の行を sqlnet.ora ファイルに追加します

```
SQLNET.AUTHENTICATION_GSSAPI_SERVICE=/.../cellname/oracle_server
SQLNET.AUTHENTICATION_SERVICES=(DCEGSSAPI)
```

注意： 前述の例で使用している Oracle Server のプリンシパル名は、セル名が含まれる完全修飾名で入力する必要があります。

手順 3: 認証時に使用するデータベース・アカウントのセットアップ

Oracle クライアントがデータベースに接続する際に使用する DCE プリンシパルを作成します。ここでは、Oracle クライアントのプリンシパル名を「oracle」と想定しています。

```
% dce_login cell_admin cell_admin_password
% rgy_edit
Current site is : registry server at /.../cellname/subsys/dce/sec/master
rgy_edit=> do p
Domain changed to: principal
rgy_edit=> add oracle
rgy_edit=> do a
Domain changed to: account
rgy_edit=> add oracle -g none -o none -pw oracle_client_password -mp
cell_admin_password
rgy_edit=> quit
bye
```

Oracle データベース・ユーザー・アカウントを作成します。以下の命令は、SQL*Plus を使用してアカウントを作成する方法を示しています。

```
SQL> connect internal
Connected
SQL> create user "/.../CELLNAME/ORACLE" identified externally;
Statement processed.
SQL> grant connect to "/.../CELLNAME/ORACLE";
Statement processed.
SQL> exit
```

注意： Oracle クライアントのプリンシパル名を、大文字の完全修飾名（完全なセル指定を含む）で入力し、引用符で囲む必要があります。

手順 4: DCE GSSAPI 認証を使用して Oracle Server に接続

ここでは、Oracle Server のプリンシパル名が「oracle_server」で、Oracle クライアントのプリンシパル名が「oracle」で、データベース・サービス名が「sales」と想定しています。

1. DCE 認証がオペレーティング・システム認証にカプセル化されていない場合は、次の構文を使用してログインします。

   ```
   % dce_login oracle_client_principal oracle_client_password
   ```

   たとえば、次のとおりです。

   ```
   % dce_login oracle oraclnt
   ```

2. DCE GSSAPI 認証を使用して Oracle データベースに接続します。

   ```
   % SQLPLUS /@<database_service_name>
   ```

   たとえば、次のとおりです。

   ```
   % SQLPLUS /@sales
   ```

9

SSL 認証の構成

この章では、次のトピックについて説明します。

Oracle 環境での SSL

SSL（セキュア・ソケット・レイヤー）は、ネットワーク接続を保護するために Netscape Communications Corporation が開発した業界標準プロトコルです。SSL では公開鍵インフラストラクチャ（PKI）を使用して、認証、暗号化、データの整合性を実現します。

この項では、次のトピックについて説明します。

SSL の機能

SSL 機能を組み込むことにより、Oracle Advanced Security での暗号化のサポートが拡張され、SSL 標準に基づく公開鍵認証が実現されます。

Oracle Advanced Security の SSL 機能を使用して、クライアントとサーバー間で安全に通信できます。特に、次の認証を行う場合に SSL を使用します。

- 1 つ以上の Oracle Server に対するクライアントまたはサーバー
- クライアントに対する Oracle Server

SSL 機能は SSL のみでも使用することができますが、Oracle Advanced Security でサポートされている他の認証方式とともに使用することもできます。たとえば、SSL の暗号化と Kerberos の認証を組み合わせて使用することができます。

> **詳細情報 :** 認証方式の詳細は、第 1 章の「Oracle Advanced Security の概要」を参照してください。

次の 3 つの認証モードのうちの 1 つで SSL を使用することができます。次のいずれかを行う必要があります。

- サーバーのみがクライアントに対して認証を行う
- クライアントとサーバーの両方がお互いに対して認証を行う
- クライアントとサーバーの両方がお互いに対して認証を行わない

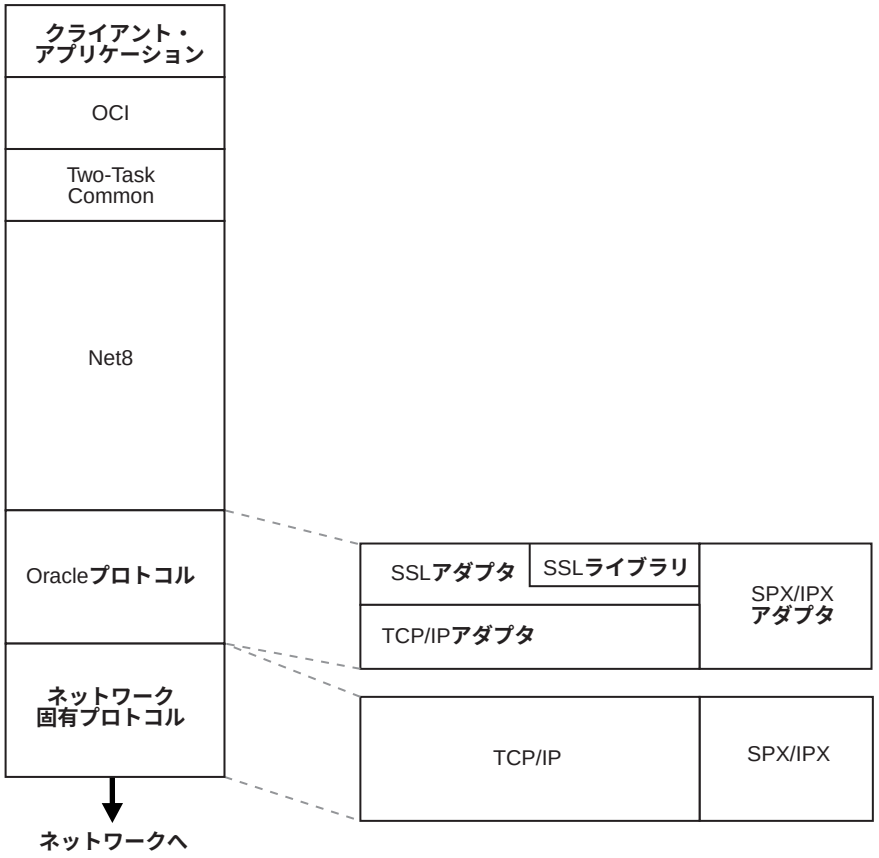
SSL 認証を無効にして、SSL の暗号化機能のみを使用することもできます。

> **詳細情報 :** SSL の詳細な説明は、IETF（Internet Engineering Task Force）のドキュメント『SSL Protocol バージョン 3.0』を参照してください。
>
> 重要なセキュリティの概念と用語は、用語集を参照してください。

Oracle 環境での SSL のアーキテクチャ

図 9-1 に示すように、Oracle 環境では、SSL は TCP/IP を使用して Oracle プロトコル・レイヤーで動作します。

図 9-1 Oracle 環境での SSL のアーキテクチャ



Oracle 環境での SSL の構成要素

Oracle 環境での SSL の構成要素には次のものがあります。それぞれについて以下で説明しています。

- 証明書
- 認証局（CA）

- Wallet

証明書

証明書によって、エンティティの識別情報が正しいことが保証され、公開鍵がそのエンティティに実際に属することが保証されます。エンティティの公開鍵が信頼できる識別情報である認証局（CA）によって署名されたときに、証明書が作成されます。この項で詳細に説明します。

証明書にはエンティティの名前、公開鍵、シリアル番号、有効期限が含まれます。証明書に関連する権限についての情報が含まれる場合もあります。さらに、発行元の CA についての情報が含まれます。

エンティティが自分自身の証明書を CA から受け取ったとき、または他のエンティティから証明書を受け取ったとき、エンティティでは証明書が**信頼できる証明書（trusted certificate）**であることを確認し、信頼できる認証局から発行された証明書であることを確認します。証明書が有効であるのは有効期間中です。

認証局（CA）

ユーザー、データベース、管理者、クライアント、サーバーなどの他のエンティティが本当に本人であるかどうかは、信頼できるサード・パーティによって証明されます。認証局では、ユーザーの識別情報を確認し、証明書を付与して、認証局の秘密鍵で署名します。

証明書を発行する際に必要になる個人情報は、CA ごとに異なる場合があります。ユーザーの運転免許証を必要とする場合や、公証によって証明書を要求する必要がある場合、証明書を要求している人物の指紋を必要とする場合などがあります。

認証局では、認証局の公開鍵を含んだ自分自身の証明書を発行します。各ネットワーク・エンティティには、信頼できる CA の証明書の一覧があります。当該のエンティティでは、他のエンティティと通信を開始する前に、相手側エンティティの証明書の署名が信頼できる CA からのものかどうかをこの一覧を使用して確認します。

ネットワーク・エンティティでは、同じ CA または別の CA から証明書を取得できます。

注意： Oracle Advanced Security では、VeriSign 証明書セットがインストールされます。

証明書を追加する方法は、9-31 ページの「手順 5: Wallet の新規作成」を参照してください。

信頼できる証明書を追加する方法は、9-38 ページの「手順 7: 新規の信頼できる証明書の追加」を参照してください。

Wallet

鍵や証明書、信頼できる証明書など、SSL で必要な認証データは Wallet として保存、管理されます。Oracle 環境で SSL を使用するシステムには、X509 バージョン 3 の証明書、秘密鍵および信頼できる証明書の一覧を持つ Wallet があります。

セキュリティ管理者は、Oracle Wallet Manager を使用してサーバーのセキュリティ資格証明を管理します。Wallet の所有者は、クライアントのセキュリティ資格証明を管理するのに Oracle Wallet Manager を使用します。Oracle Wallet Manager は、特に次の場合に使用します。

- 公開鍵と秘密鍵のペアを生成し、認証局に提出する証明書要求を作成する
- 識別情報の証明書をインストールする
- 識別情報の信頼できる証明書を構成する

注意： Oracle Advanced Security リリース 8.1.5 をインストールすると、Oracle Wallet Manager リリース 1.3 ベータもインストールされます。

詳細情報： Oracle Wallet Manager の詳細は、9-29 ページの「手順 4: Oracle Wallet Manager の起動」から始まる項を参照してください。9-42 ページの「Wallet の管理」も参照してください。

Oracle 環境での SSL の動作 : SSL ハンドシェイク

> **詳細情報 :** SSL の詳細な説明は、IETF（Internet Engineering Task Force）のドキュメント『SSL Protocol バージョン 3.0』を参照してください。

クライアントとサーバーの間で通信を開始するとき、次の 3 つの重要な処理を含む SSL ハンドシェイクが実行されます。

- クライアントとサーバーで使用する **Cipher Suite** を確立します。
- サーバーはサーバーの証明書をクライアントに送信します。クライアントは、サーバーの証明書が信頼できる CA によって署名されたものかどうかを確認します。

  クライアントの認証が必要な場合は、同様に、クライアントがクライアントの証明書をサーバーに送信します。サーバーは、クライアントの証明書が信頼できる CA によって署名されたものかどうかを確認します。
- クライアントとサーバーは、公開鍵暗号を使用して鍵情報を交換し、それぞれこの鍵情報からセッション・キーを生成します。これ以降、クライアントとサーバー間のすべての通信は、セッション・キーのセットと折衝された Cipher Suite を使用して暗号化され復号化されます。

Oracle 環境での認証は、次の 3 つの基本手順からなります。

1. ユーザーが SSL を使用してサーバーに対して Net8 接続を開始する。
2. SSL によってクライアントとサーバー間のハンドシェイクが実行される。
3. ハンドシェイクに成功した場合は、ユーザーがデータベースにアクセスするのに適切な**権限**を持っていることをサーバーが確認する。

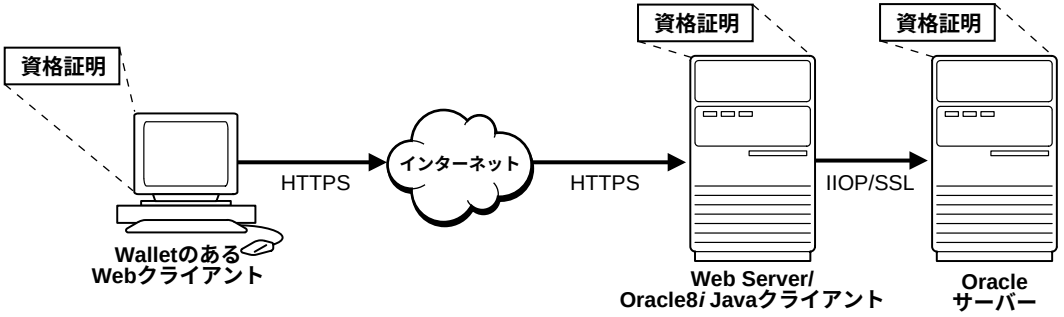
Oracle 環境外での SSL

Oracle Advanced Security の SSL 機能を使用して、非 Oracle クライアントと Oracle Server 間を安全に接続できます。たとえば、SSL を使用して、Oracle ネットワークの外部のクライアントが Oracle ネットワーク内の認可データに安全にアクセスできます。

図 9-2 は、SSL を使用して Oracle エンティティと非 Oracle エンティティの間を安全に接続する例を示したもので、インターネットと Oracle Server の間を接続しています。この例では、Web サーバーが Oracle8*i* Java クライアントとして実行されています。Web サーバーは **HTTPS**（SSL で保護された HTTP）によってメッセージを受信し、サーブレットは **IIOP**/SSL（SSL で保護された IIOP）によって Oracle Server に **CORBA** 要求を送信します。この例では、Web サーバーは、Web クライアントの証明書ではなく、サーバー自身の証明書を Oracle Server に渡しています。

> **詳細情報 :** IIOP/SSL の使用方法と構成方法は、『Oracle8*i* Enterprise JavaBeans と CORBA 開発者ガイド』を参照してください。

図 9-2 インターネットから Oracle Server への接続



SSL と他の認証方式の併用

SSL 機能と、Kerberos、SecurID、Identix など、Oracle Advanced Security でサポートされている他の認証方式を併用できます。

> **詳細情報：** 認証方式の詳細は、第 1 章の「Oracle Advanced Security の概要」を参照してください。

この項では、次のトピックについて説明します。

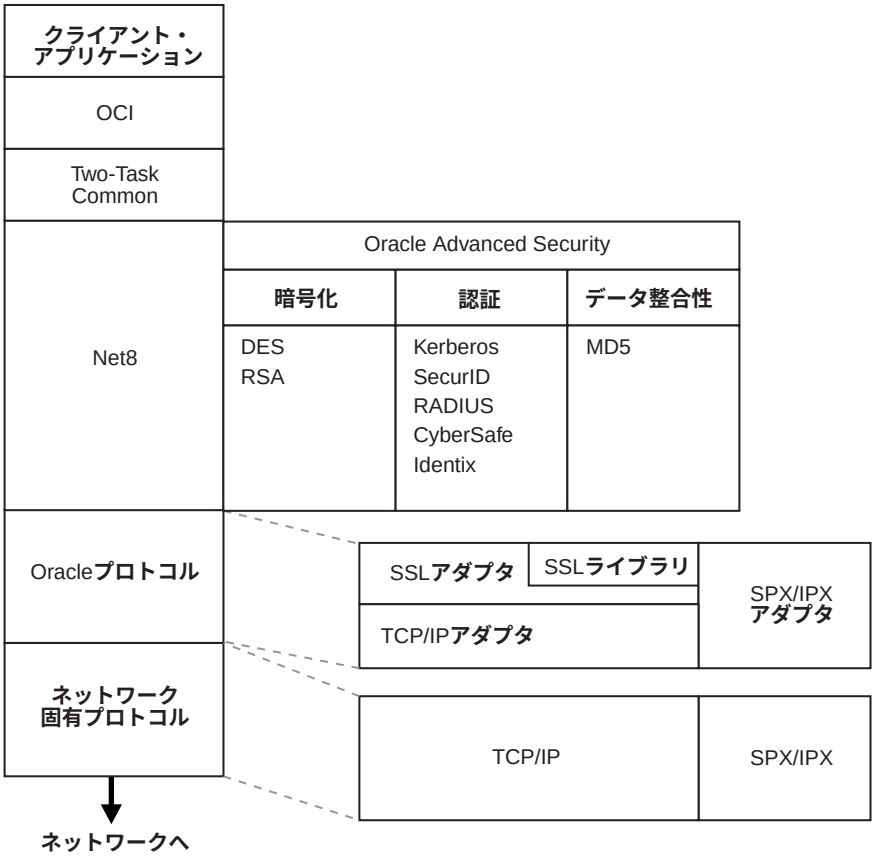
- 他の認証方式と併用する場合の SSL のアーキテクチャ
- 例 : SSL と他の認証方式の併用

他の認証方式と併用する場合の SSL のアーキテクチャ

図 9-3 に示すように、Oracle Advanced Security は、トランスポート・レイヤーで TCP/IP を使用する SSL の上部にあるセッション・レイヤーで動作します。

> **詳細情報：** Oracle ネットワーク環境でのスタック通信の詳細は、『Oracle8*i* Net8 管理者ガイド』を参照してください。

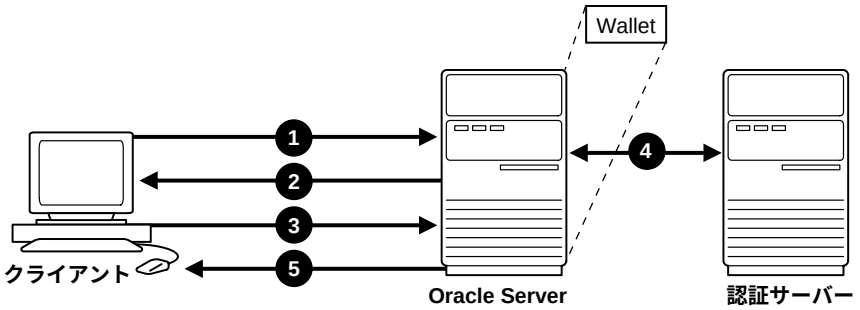
図 9-3 SSL と Oracle Advanced Security の関係



例 : SSL と他の認証方式の併用

図 9-4 に、Oracle Advanced Security でサポートされている認証方式と SSL を併用する例を示します。この例では、サーバー認証で SSL を使用し、クライアント認証では Kerberos、SecurID、Identix など、Oracle Advanced Security でサポートされている認証方式を使用しています。

図 9-4 例 : SSL と他の Oracle Advanced Security 認証方式との関係



1. クライアントが Oracle Server に接続を要求します。
2. SSL がハンドシェイクを実行します。このハンドシェイク中、サーバーはクライアントに対して認証し、クライアントとサーバーは使用する Cipher Suite を確立します。9-6 ページの「Oracle 環境での SSL の動作 : SSL ハンドシェイク」を参照してください。
3. SSL ハンドシェイクが正常に完了すると、ユーザーがデータベースへのアクセスを要求します。
4. Oracle Server が認証サーバーとユーザーの認証情報を交換します。
5. 認証サーバーの確認を待って、Oracle Server がユーザーにアクセス権と認証を付与します。

注意 : SSL の暗号化と Oracle Advanced Security の他の認証方式を併用できます。この場合、二重暗号化を禁止している政府条例に準拠するため、非 SSL 暗号化を無効にする必要があります。非 SSL 暗号化を無効にしないと接続できません。

Oracle Advanced Security で暗号化を無効にする方法は、2-7 ページの「暗号化とチェックサムの折衝」を参照してください。

SSL 認証は Oracle Advanced Security 暗号化と併用できません。

SSL を使用する上での問題

SSL は、CERN 代理サーバーのような従来のアプリケーション・レベルのファイアウォールによって代理することはできません。

SSL では、権限とロールの割り当てを行う認可は行われません。これらは、Oracle Server によって Oracle8*i* で実現されます。

SSL では認証と暗号化を行うため、パフォーマンスの面で標準の **Net8** TCP/IP トランスポートよりも遅くなります。

Oracle Advanced Security の SSL 機能は、Oracle8*i* 以前のバージョンの Oracle では動作しません。

9-2 ページで説明されている SSL 認証モードでは、それぞれで一意の設定ファイルが必要になります。これらの一意の設定については、9-11 ページの「SSL を使用可能にする」の項で説明しています。

SSL を使用可能にする

SSL を使用可能にするには、次の手順で行います。各手順の詳細は以下のページで説明しています。

手順 1: Oracle Advanced Security と Oracle Wallet Manager のインストール

クライアントとサーバーの両方で行います。

Oracle Advanced Security をインストールすると、Oracle Universal Installer によって SSL と Oracle Wallet Manager の両方がシステムに追加されます。

> **詳細情報：** プラットフォーム固有の Oracle8*i* インストレーション・ガイドを参照してください。

手順 2: クライアントの SSL の構成

クライアントの SSL を構成するには、次の手順で行います。各手順の詳細は以下に説明しています。

- SSL をまだ構成していない場合は、クライアント構成パラメータを指定
- Oracle Wallet の場所の設定
- SSL Cipher Suite の設定（オプション）
- 必要な SSL バージョンの設定（オプション）
- SSL を認証サービスとして設定（オプション）
- "SSL 付き TCP/IP" をネット・サービス名として選択

パラメータを構成するには、次の 2 通りあります。

- 静的－ sqlnet.ora にパラメータを設定します。Oracle Wallet の場所を設定し、他のパラメータのデフォルトの設定を変更するには、Oracle Net8 Assistant（図 9-5）を使用するか、テキスト・エディタで sqlnet.ora ファイルを編集します。
- 動的－ Net8 アドレスのセキュリティ・サブセクションにパラメータを設定します。

> **詳細情報：** 動的パラメータ名は、B-7 ページの「SSL を使用するクライアントとサーバーのパラメータ」を参照してください。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle － *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」>「Save Network Configuration」をクリックします。

SSL をまだ構成していない場合は、クライアント構成パラメータを指定

Oracle Net8 Assistant を使用している場合にのみ行う必要があります。

図 9-5 Oracle Net8 Assistant を使用したクライアント構成パラメータの指定

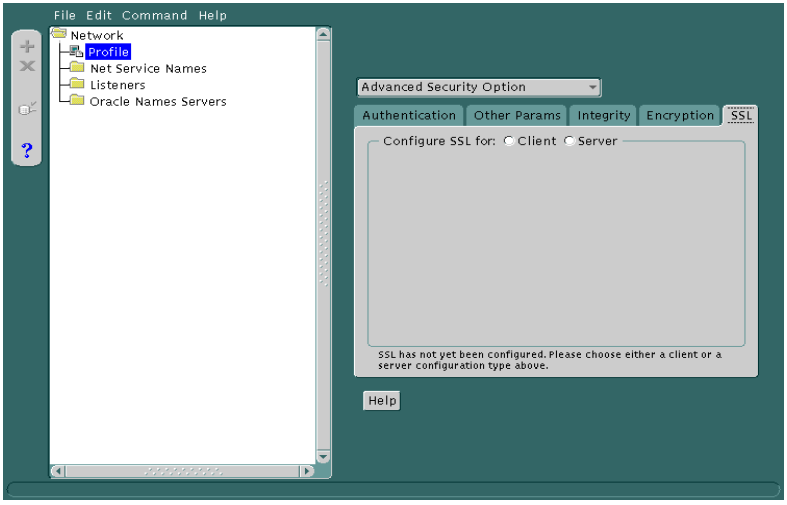
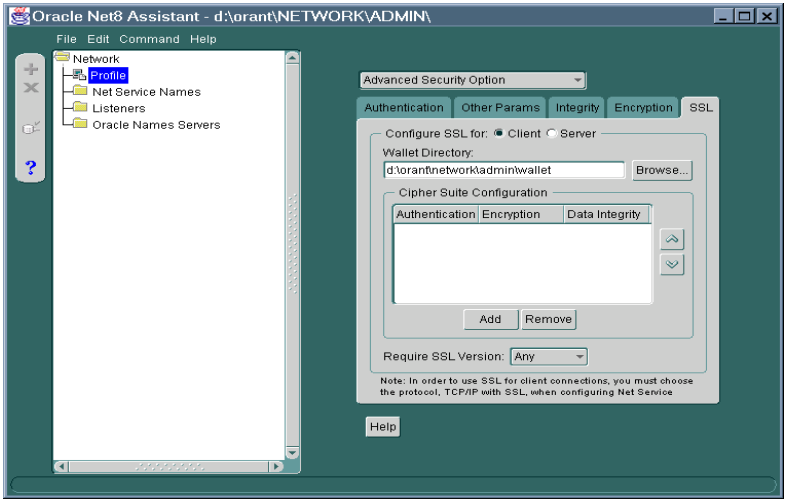


図 9-5 を参照してください。

1. 右側のペインで「SSL」タブを選択します。
2. 「SSL」タブ・ページの「Configure SSL」で「Client」ラジオ・ボタンを選択します。「SSL」タブ・ページでクライアントを適切に構成できるようになります（9-14 ページの図 9-6）。

図 9-6 Oracle Net8 Assistant のクライアント構成用の「SSL」タブ・ページ



Oracle Wallet の場所の設定

OSS.SOURCE.MY_WALLET パラメータを設定します。このパラメータのデフォルトはありません。

Oracle Net8 Assistant を使用	SQLNET.ORA を変更

図 9-6 を参照してください。
1. 「SSL」タブ・ページの上部にある「Configure SSL」で「Client」ラジオ・ボタンが選択されていることを確認します。
2. 「Wallet Directory」ボックスに Oracle Wallet のディレクトリを入力します。ファイル・システムを検索するには、「Browse」ボタンをクリックします。
注意 : ここで入力したディレクトリと同じディレクトリを、後述の 9-31 ページの「手順 5: Wallet の新規作成」でも入力する必要があります。
	次のパラメータを設定します。
	`oss.source.my_wallet =`
	`(SOURCE=`
	`(METHOD=File)`
	`(METHOD_DATA=`
	`(DIRECTORY=<`*`your_wallet_location`*`>)`
	`)`
	`)`

SSL Cipher Suite の設定（オプション）

Cipher Suite は、ネットワークのエンティティ間でメッセージ交換するのに使用する認証、暗号化、データ整合性アルゴリズムを 1 組にしたものです。SSL ハンドシェイク時に、2 つのエンティティ間で折衝し、メッセージを送受信するときに使用する Cipher Suite を確認します。

SSL で使用する Cipher Suite は SSL_CIPHER_SUITES パラメータで設定します。

Oracle Advanced Security をインストールすると、いくつかの SSL Cipher Suite がデフォルトで設定されます。1 つ以上の Cipher Suite を手動で設定すると、インストール中に設定された他のデフォルトの Cipher Suite より優先されます。たとえば、Oracle Net8 Assistant を使用して Cipher Suite SSL_RSA_WITH_RC4_128_SHA を追加すると、デフォルトで設定された他のすべての Cipher Suite は無視されます。

Cipher Suite は優先順位を設定できます。クライアントとサーバーで使用する Cipher Suite について折衝するとき、設定した優先順位に従って行われます。Cipher Suite の優先順位を設定するとき、次の点を考慮します。

- セキュリティのレベル。たとえば、Triple-DES 暗号化は DES よりも強力です。
- パフォーマンスへの影響。たとえば、Triple-DES 暗号化は DES よりも時間がかかります。
- 管理要件。クライアント用に選択された Cipher Suite は、サーバーで必要とされる Cipher Suite と互換性がある必要があります。たとえば、Oracle コール・インタフェース（OCI）ユーザーの場合、サーバーではクライアント自身が認証を行う必要があります。この場合、認証の交換ができない Diffie-Hellman 匿名認証を使用した Cipher Suite は使用できません。反対に、Enterprise Java Beans（EJB）ユーザーの場合は、サーバーでクライアント自身が認証を行う必要はありません。この場合は、Diffie-Hellman 匿名認証を使用できます。

通常、Cipher Suite の優先順位は強力なものから順に設定します。

次の 2 つの表は、Oracle Advanced Security の米国内向けバージョンと輸出バージョンでサポートされる SSL Cipher Suite の一覧です。これらの Cipher Suite は、Oracle Advanced Security をインストールしたときにデフォルトで設定されます。表には、各 Cipher Suite で使用される認証、暗号化、データ整合性の種類も併せて記載しています。

表 9-1 米国内向けバージョンの Oracle Advanced Security の SSL Cipher Suite

Cipher Suite	認証	暗号化	データの整合性
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES EDE CBC	SHA
SSL_RSA_WITH_RC4_128_SHA	RSA	RC4 128	SHA
SSL_RSA_WITH_RC4_128_MD5	RSA	RC4 128	MD5
SSL_RSA_WITH_DES_CBC_SHA	RSA	DES CBC	SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	DH 匿名	3DES EDE CBC	SHA
SSL_DH_anon_WITH_RC4_128_MD5	DH 匿名	RC4 128	MD5
SSL_DH_anon_WITH_DES_CBC_SHA	DH 匿名	DES CBC	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4 40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40 CBC	SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	DH 匿名	RC4 40	MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	DH 匿名	DES40 CBC	SHA

表 9-2 輸出バージョンの Oracle Advanced Security の SSL Cipher Suite

Cipher Suite	認証	暗号化	データの整合性
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4 40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40 CBC	SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	DH 匿名	RC4 40	MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	DH 匿名	DES40 CBC	SHA

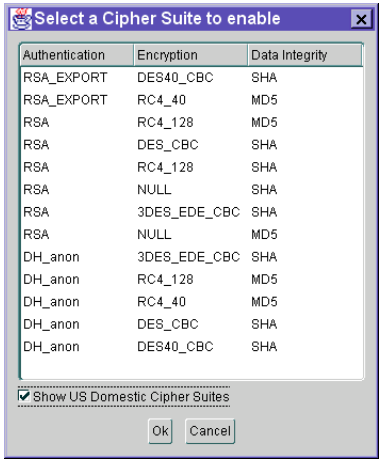
注意： SSL を Oracle Advanced Security でサポートされている他の認証方式と併用する場合は、二重暗号化を禁止している政府条例に準拠するため、非 SSL 暗号化を無効にする必要があります。非 SSL 暗号化を無効にしないと接続できません。

Oracle Advanced Security で暗号化を無効にする方法は、2-7 ページの「暗号化とチェックサムの折衝」を参照してください。

Oracle Net8 Assistant を使用	SQLNET.ORA を変更

9-14 ページの図 9-6 を参照してください。
1. 「SSL」タブ・ページの上部にある「Configure SSL」で「Client」ラジオ・ボタンが選択されていることを確認します。
2. 「Add」ボタンをクリックします。2 つ目のダイアログ・ボックス（図 9-7）に使用可能な Cipher Suite の一覧が表示されます。
3. 一覧に Suite を追加するには、追加する Suite をこの 2 つ目のダイアログ・ボックスで選択して、「OK」をクリックします。メインの「Oracle Net8 Assistant」ダイアログ・ボックスの「Cipher Suite Configuration」ウィンドウに Cipher Suite が表示されます。
4. Cipher Suite の優先順位を設定するには、「Promote」ボタンと「Demote」ボタンを使用します。ここで設定した順位が、クライアントが他のエンティティと使用する Cipher Suite を折衝するときの順位になります。
	Cipher Suite の優先順位の一覧を示すサーバーの sqlnet.ora ファイルに次のパラメータを設定します。
	`SSL_CIPHER_SUITES=`
	`(`*`SSL cipher suite1`* `[,`*`SSL cipher suite2`*`])`

図 9-7 Oracle Net8 Assistant の 2 つ目のダイアログ・ボックス : Cipher Suite の選択



必要な SSL バージョンの設定（オプション）

SSL_VERSION パラメータを設定します。このパラメータによって、クライアントの通信先になるマシンで実行する必要のある SSL のバージョンが決まります。これらのマシンでは、SSL 3.0、既存のバージョンまたは将来のバージョンの SSL を使用する必要があります。このパラメータのデフォルト設定は sqlnet.ora では "0" で、Oracle Net8 Assistant では " あらゆるバージョン " です。

Oracle Net8 Assistant を使用	SQLNET.ORA を変更
9-14 ページの図 9-6 を参照してください。 **1.** 「SSL」タブ・ページの上部にある「Configure SSL」で「Client」ラジオ・ボタンが選択されていることを確認します。 **2.** 「Require SSL Version」スクロール・ボックスのデフォルトは「Any」です。このデフォルトをそのまま使用するか、施行する SSL のバージョンを選択します。	次のパラメータを設定します。 `SSL_VERSION={ 0 | 3.0 }`

SSL を認証サービスとして設定（オプション）

SSL 認証サービスは、SQLNET.AUTHENTICATION_SERVICES パラメータで設定します。

このパラメータを設定する必要があるのは、次の 2 つの条件が両方とも当てはまるときのみです。

- SSL 認証を Oracle Advanced Security でサポートされる他の認証方式と併用するとき。たとえば、サーバーがクライアントに対して認証するときに SSL を使用し、クライアントがサーバーに対して認証するときは Kerberos または SecurID を使用するとき。

  および

- Oracle Net8 Assistant を使用して構成していないとき。

上の 2 つの条件が両方とも当てはまる場合は、テキスト・エディタを使用して、sqlnet.ora ファイルのこのパラメータに TCPS を追加します。たとえば、次のとおりです。

```
SQLNET.AUTHENTICATION_SERVICES = (BEQ,
                                 TCPS,
                                 identix,
                                 securid)
```

上の条件の片方または両方とも当てはまらない場合は、このパラメータを設定する必要はありません。

"SSL 付き TCP/IP" をネット・サービス名として選択

クライアントはリスナーの場所とともに構成する必要があります。SSL 接続では、リスナーのアドレスには SSL 付き TCP/IP プロトコルを使用する必要があります。

> **詳細情報：** Oracle Net8 Assistant のオンライン・ヘルプと『Oracle8*i* Net8 管理者ガイド』を参照してください。

手順 3: サーバーの SSL の構成

インストール中、Oracle Wallet の場所を除いて、Oracle Server と Oracle クライアントのすべての SSL パラメータにデフォルトが設定されます。サーバーの SSL を構成するには、次の手順で行います。各手順の詳細は以下に説明しています。

- SSL をまだ構成していない場合は、サーバー構成を指定
- Oracle Wallet の場所の設定
- SSL Cipher Suite の設定（オプション）
- 必要な SSL バージョンの設定（オプション）
- SSL クライアント認証の設定（オプション）
- SSL を認証サービスとして設定（オプション）
- "SSL 付き TCP/IP" をリスニング終点として選択

Oracle クライアントの場合と同じように、Oracle Server のパラメータを構成するには、次の 2 通りあります。

- 静的― sqlnet.ora にパラメータを設定します。Oracle Wallet の場所を設定し、他のパラメータのデフォルトの設定を変更するには、Oracle Net8 Assistant を使用するか、テキスト・エディタで sqlnet.ora ファイルを編集します。
- 動的― Net8 アドレスのセキュリティ・サブセクションにパラメータを設定します。

> **詳細情報：** 動的パラメータ名は、B-7 ページの「SSL を使用するクライアントとサーバーのパラメータ」を参照してください。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle － *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

SSL をまだ構成していない場合は、サーバー構成を指定

Oracle Net8 Assistant を使用している場合にのみ行う必要があります。

図 9-8 Oracle Net8 Assistant を使用したサーバー構成の指定

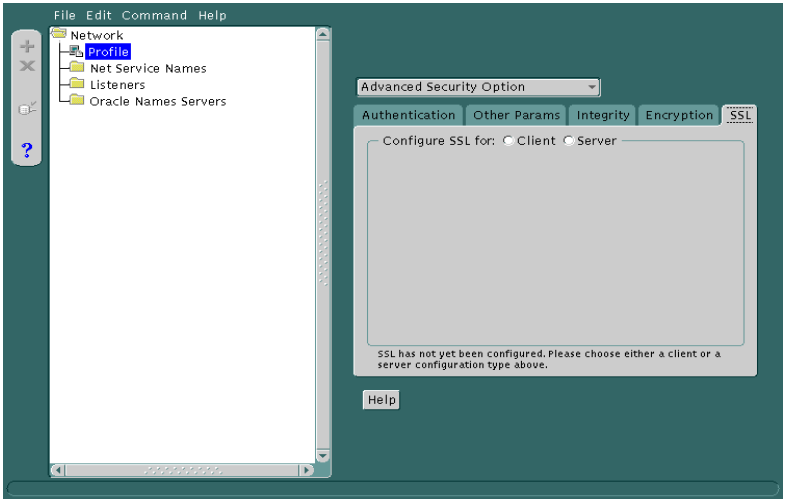
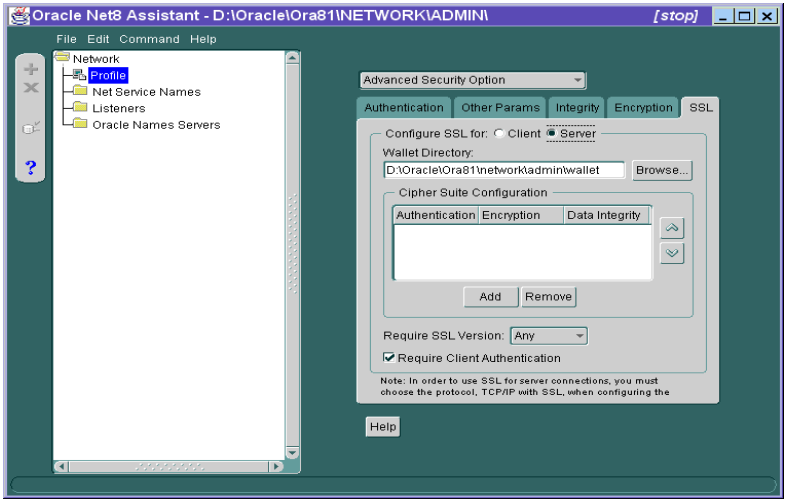


図 9-8 を参照してください。

1. 右側のペインで「SSL」タブを選択します。
2. 「SSL」タブ・ページの「Configure SSL」で「Server」ラジオ・ボタンを選択します。「SSL」タブ・ページでサーバーを適切に構成できるようになります（9-22 ページの図 9-9）。

図 9-9 Oracle Net8 Assistant のサーバー構成用の「SSL」タブ・ページ



Oracle Wallet の場所の設定

OSS.SOURCE.MY_WALLET パラメータを設定します。このパラメータのデフォルトはありません。

注意： クライアントとサーバーを構成する際、Oracle Wallet の場所を設定する機会が 2 回あります。**2 回とも、必ず同じ場所を入力してください。**

- この項では、Wallet の場所を設定するのに、Oracle Net8 Assistant を使用するか、または sqlnet.ora ファイルを変更します。
- 9-31 ページの「手順 5: Wallet の新規作成」では、Oracle Wallet Manager を使用します。

Oracle Net8 Assistant を使用	SQLNET.ORA を変更

9-22 ページの図 9-9 を参照してください。
1. 「SSL」タブ・ページの上部にある「Configure SSL」で「Server」ラジオ・ボタンが選択されていることを確認します。
2. 「Wallet Directory」ボックスに Oracle Wallet のディレクトリを入力します。Browse ファイル・システムを検索するには、「Browse」ボタンをクリックします。
注意 : ここで入力したディレクトリと同じディレクトリを、後述の 9-31 ページの「手順 5: Wallet の新規作成」でも入力する必要があります。
	次のパラメータを設定します。
	`oss.source.my_wallet =`
	`(SOURCE=`
	`(METHOD=File)`
	`(METHOD_DATA=`
	`(DIRECTORY=your wallet location)`
	`)`
	`)`

SSL Cipher Suite の設定（オプション）

SSL で使用する Cipher Suite は SSL_CIPHER_SUITES パラメータで設定します。

Oracle Advanced Security をインストールすると、いくつかの SSL Cipher Suite がデフォルトで設定されます。1 つ以上の Cipher Suite を手動で設定すると、インストール中に設定された他のデフォルトの Cipher Suite より優先されます。たとえば、Oracle Net8 Assistant を使用して Cipher Suite SSL_RSA_WITH_RC4_128_SHA を追加すると、デフォルトで設定された他のすべての Cipher Suite は取り消されます。

Cipher Suite は優先順位を設定できます。サーバーとクライアントで使用する Cipher Suite について折衝するとき、設定した優先順位に従って行われます。

Cipher Suite の優先順位を設定するとき、次の点を考慮します。

- セキュリティのレベル。たとえば、Triple-DES 暗号化は DES よりも強力です。2-4 ページの「Triple-DES を提供する SSL」を参照してください。
- パフォーマンスへの影響。たとえば、Triple-DES 暗号化は DES よりも時間がかかります。
- 管理要件。サーバーに選択された Cipher Suite は、クライアントで必要とされる Cipher Suite と互換性がある必要があります。たとえば、Oracle コール・インタフェース（OCI）ユーザーの場合、サーバーではクライアント自身が認証を行う必要があります。この場合、認証の交換ができない Diffie-Hellman 匿名認証を使用した Cipher Suite は使用できません。反対に、Enterprise Java Beans（EJB）ユーザーの場合は、サーバーでクライアント自身が認証を行う必要はありません。この場合は、Diffie-Hellman 匿名認証を使用できます。

> **注意：** Oracle Advanced Security のバージョン 8.1.5 では、Diffie-Hellman 匿名認証を使用した Cipher Suite をサーバーで設定した場合は、クライアントにも同じ Cipher Suite を設定する必要があります。同じにしないと接続できません。
>
> Diffie-Hellman 匿名認証を使用した Cipher Suite を使用する場合は、SSL_CLIENT_AUTHENTICATION パラメータに FALSE を設定する必要があります。9-27 ページの「SSL クライアント認証の設定（オプション）」を参照してください。

通常、Cipher Suite の優先順位は強力なものから順に設定します。

次の 2 つの表は、Oracle Advanced Security の米国内向けバージョンと輸出バージョンでサポートされる SSL Cipher Suite の一覧です。表には、各 Cipher Suite で使用される認証、暗号化、データ整合性の種類も併せて記載しています。

表 9-3 米国内向けバージョンの Oracle Advanced Security の SSL Cipher Suite

Cipher Suite	認証	暗号化	データの整合性
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES EDE CBC	SHA
SSL_RSA_WITH_RC4_128_SHA	RSA	RC4 128	SHA
SSL_RSA_WITH_RC4_128_MD5	RSA	RC4 128	MD5
SSL_RSA_WITH_DES_CBC_SHA	RSA	DES CBC	SHA
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	DH 匿名	3DES EDE CBC	SHA
SSL_DH_anon_WITH_RC4_128_MD5	DH 匿名	RC4 128	MD5
SSL_DH_anon_WITH_DES_CBC_SHA	DH 匿名	DES CBC	SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4 40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40 CBC	SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	DH 匿名	RC4 40	MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	DH 匿名	DES40 CBC	SHA

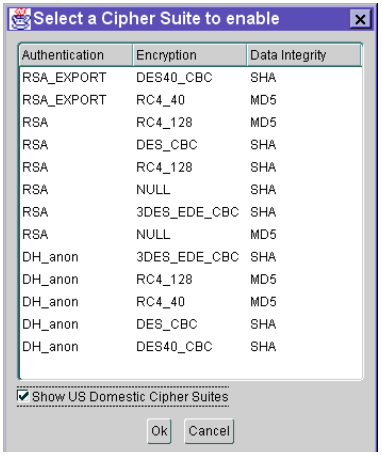
表 9-4 輸出バージョンの Oracle Advanced Security の SSL Cipher Suite

Cipher Suite	認証	暗号化	データの整合性
SSL_RSA_EXPORT_WITH_RC4_40_MD5	RSA	RC4 40	MD5
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA	DES40 CBC	SHA
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5	DH 匿名	RC4 40	MD5
SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA	DH 匿名	DES40 CBC	SHA

Oracle Net8 Assistant を使用	SQLNET.ORA を変更

9-22 ページの図 9-9 を参照してください。
1. 「SSL」タブ・ページの上部にある「Configure SSL」で「Server」ラジオ・ボタンが選択されていることを確認します。
2. 「Add」ボタンをクリックします。2 つ目のダイアログ・ボックス（図 9-10）に使用可能な Cipher Suite の一覧が表示されます。
3. 一覧に Suite を追加するには、追加する Suite をこの 2 つ目のダイアログ・ボックスで選択して、「OK」をクリックします。メインの「Oracle Net8 Assistant」ダイアログ・ボックスの「Cipher Suite Configuration」ウィンドウに Cipher Suite が表示されます。
4. Cipher Suite の優先順位を設定するには、「Promote」ボタンと「Demote」ボタンを使用します。ここで設定した順位が、サーバーが他のエンティティと使用する Cipher Suite を折衝するときの順位になります。
	Cipher Suite の優先順位の一覧を示すサーバーの sqlnet.ora ファイルに次のパラメータを設定します。
	`SSL_CIPHER_SUITES=`
	`(SSL cipher suite1 [,SSL`
	`cipher suite2])`

図 9-10 Oracle Net8 Assistant の 2 つ目のダイアログ・ボックス : Cipher Suite の選択



必要な SSL バージョンの設定（オプション）

SSL_VERSION パラメータを設定します。このパラメータによって、サーバーの通信先になるマシンで実行する必要のある SSL のバージョンが決まります。これらのマシンでは、SSL 3.0、既存のバージョンまたは将来のバージョンの SSL を使用する必要があります。

このパラメータのデフォルト設定は sqlnet.ora では "0" で、Oracle Net8 Assistant では " あらゆるバージョン " です。デフォルト値では、旧バージョンの SSL を使用したクライアントが最新バージョンの SSL を使用したサーバーと通信できる設定になっており、この設定を使用することをお薦めします。

Oracle Net8 Assistant を使用	SQLNET.ORA を変更
9-22 ページの図 9-9 を参照してください。 1. 「SSL」タブ・ページの上部にある「Configure SSL」で「Server」ラジオ・ボタンが選択されていることを確認します。 2. 「Require SSL Version」リスト・ボックスのデフォルトは「Any」です。このデフォルトをそのまま使用するか、施行する SSL のバージョンを選択します。	次のパラメータを設定します。 `SSL_VERSION={ 0 | 3.0 }`

SSL クライアント認証の設定（オプション）

クライアント認証で SSL を使用するかどうかは SSL_CLIENT_AUTHENTICATION パラメータで制御します。デフォルト値は TRUE です。

Diffie-Hellman 匿名認証（DH_anon）を含む Cipher Suite を使用する場合は、このパラメータに FALSE を設定する必要があります。また、サーバーに対してクライアントが認証するときに、Kerberos や Identix など、Oracle Advanced Security でサポートされている非 SSL 認証方式を使用する場合にも、このパラメータに FALSE を設定する必要があります。

Oracle Net8 Assistant を使用	SQLNET.ORA を変更
9-22 ページの図 9-9 を参照してください。 1. 「SSL」タブ・ページの上部にある「Configure SSL」で「Server」ラジオ・ボタンが選択されていることを確認します。 2. デフォルトでは、「Require Client Authentication」チェック・ボックスが選択されています。このデフォルトをそのまま使用するか、クライアント認証が必要ない場合は、このチェック・ボックスの選択を解除します。	次のパラメータを設定します。 `SSL_CLIENT_AUTHENTICATION={ TRUE | FALSE }`

SSL を認証サービスとして設定（オプション）

SSL 認証サービスは、SQLNET.AUTHENTICATION_SERVICES パラメータで設定します。

このパラメータを設定する必要があるのは、次の 2 つの条件が両方とも当てはまるときのみです。

- SSL 認証を Oracle Advanced Security でサポートされる他の認証方式と併用するとき。たとえば、サーバーがクライアントに対して認証するときに SSL を使用し、クライアントがサーバーに対して認証するときは Kerberos または SecurID を使用するとき。

  および

- Oracle Net8 Assistant を使用して構成していないとき。

上の 2 つの条件が両方とも当てはまる場合は、テキスト・エディタを使用して、sqlnet.ora ファイルのこのパラメータに TCPS を追加します。たとえば、次のとおりです。

```
SQLNET.AUTHENTICATION_SERVICES = (BEQ, TCPS,
                                  selected_method_1,
                                 selected_method_2)
```

上の条件の片方または両方とも当てはまらない場合は、このパラメータを設定する必要はありません。

"SSL 付き TCP/IP" をリスニング終点として選択

クライアントの接続で SSL をアクティブにするには、listener.ora のリスニング終点として、SSL 付き TCP/IP プロトコルを選択する必要があります。データベースの Java オプションに IIOP クライアントが接続している場合は、ポート番号が 2482 であることを確認します。

詳細情報：『Oracle8*i* Net8 管理者ガイド』を参照してください。

手順 4: Oracle Wallet Manager の起動

次の場合に、クライアントとサーバーの両方で Oracle Wallet Manager を使用します。

- Wallet の作成
- 認証局からの証明書の要求と、その証明書の Wallet へのインストール
- オプションで新規**信頼できる証明書（trusted certificate）**の追加
- Wallet の保存

> **注意：** クライアント認証が必要ない場合でも、サーバーとクライアントの両方に、信頼できる証明書の一覧とともに Wallet を作成する必要があります。

Oracle Wallet Manager の起動方法は、システムによって異なります。

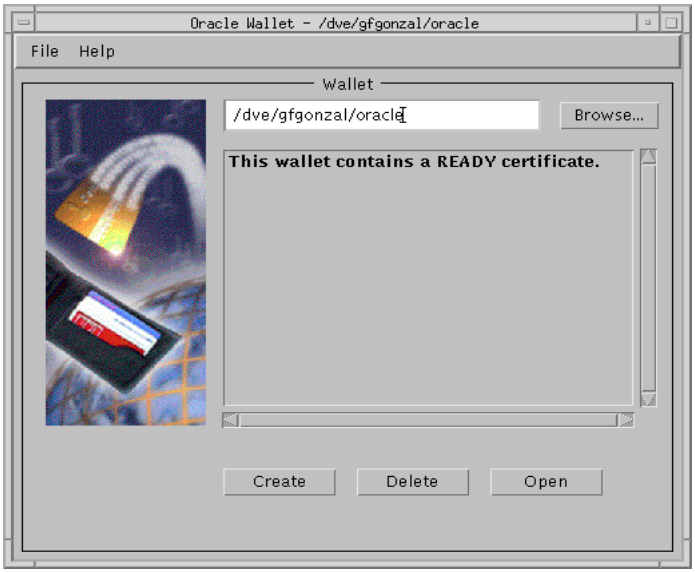
Windows NT

Windows NT で Oracle Wallet Manager を起動するには、「スタート」->「プログラム」->「Oracle — *HOME_NAME*」->「Network Administration」->「Wallet Manager」の順にクリックします。コマンド・プロンプトで、**`wmtgui`** と入力しても起動できます。Oracle Wallet Manager の「Oracle Wallet」ダイアログ・ボックス（図 9-11）が表示されます。

Solaris

Oracle Wallet Manager を起動するには、コマンド行で **`wmtgui`** と入力します。Oracle Wallet Manager の「Oracle Wallet」ダイアログ・ボックス（図 9-11）が表示されます。

図 9-11 Oracle Wallet Manager



このダイアログ・ボックスには、デフォルトの Wallet の場所、Wallet に格納されている証明書のバージョン、および Wallet の状態が EMPTY、REQUESTED、READY で表示されます。次の表に、ダイアログ・ボックスのフィールドとボタンの説明を示します。

フィールド名	説明
Wallet の場所のテキスト・ボックス	デフォルトの Wallet ファイルの場所を表示します。別の場所にある Wallet を指定するには「Browse」ボタンをクリックします。
「Help」->「Wallet Information」	使用中の Oracle Wallet Manager のバージョンと、Wallet に証明書がインストールされている場合は、その証明書の状態を表示します。

ボタン名	機能
「Create」	Wallet を新規作成します。
「Delete」	このダイアログ・ボックスに表示されている Wallet を削除します。
「Open」	このダイアログ・ボックスに表示されている Wallet をオープンします。

手順 5: Wallet の新規作成

次の手順に従って Wallet を新規作成します。ここでは、Oracle Wallet Manager がすでに起動されており、最初のダイアログ・ボックスが表示されていることを前提としています（図 9-11）。

1. 「Create」をクリックして、Wallet を新規作成します。

   「New Wallet Identity」ダイアログ・ボックス（図 9-12）が表示されます。

図 9-12 「New Wallet Identity」ダイアログ・ボックス

2. 証明書で使用する識別情報を入力して、「OK」をクリックします。

   Single sign-on を使用している場合は、このダイアログ・ボックスのフィールドと、そのフィールドに入力した値を書き留めておきます。後でグローバルなユーザーを作成するときに、この情報が必要になります。9-40 ページの「手順 10: グローバルな証明書によって Oracle Server に認証されるユーザーの作成」を参照してください。

   「New Wallet」ダイアログ・ボックス（図 9-13）で、新規 Wallet を格納するファイル・システムのディレクトリを指定します。

注意： Oracle Wallet の場所を設定する機会は 2 回あります。**2 回とも、必ず同じ場所を入力してください。**

- ここでは、Oracle Wallet Manager を使用します。
- 構成のはじめの段階では、Oracle Net8 Assistant を使用したか、または sqlnet.ora ファイルを変更しました。現在構成しているマシンによって、9-12 ページの「手順 2: クライアントの SSL の構成」または 9-19 ページの「手順 3: サーバーの SSL の構成」を参照してください。

図 9-13 Wallet ファイルの場所の指定

3. 新規 Wallet ファイルの場所を入力します。別のディレクトリにある Wallet を検索する場合は、「Browse」をクリックします。最初のダイアログ・ボックスに戻る場合は「Cancel」をクリックし、続ける場合は「Next」をクリックします。「New Wallet password」ダイアログ・ボックスが表示されます。

図 9-14 新規 Wallet のパスワードの入力

4. 「Enter Password」フィールドにパスワードを入力し、同じパスワードを「Verify Password」フィールドにもう一度入力します。

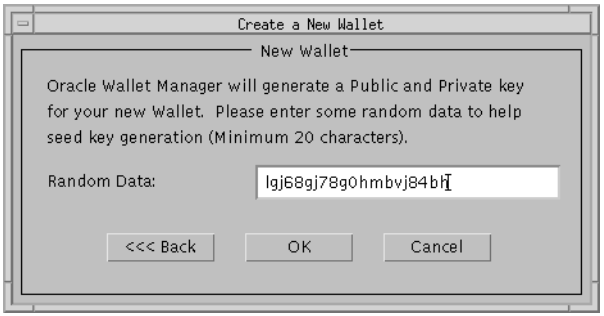
注意：「Enter Password」テキスト・ボックスと「Verify Password」テキスト・ボックスに入力したパスワードが同じでない場合、「Error」ダイアログ・ボックスが表示されます。「OK」をクリックして「New Wallet password」ダイアログ・ボックスに戻り、「Enter Password」テキスト・ボックスに再度パスワードを入力し、「Verify Password」テキスト・ボックスにも確認用に入力します。

---

5. 「Next」をクリックして続けます。

「New Wallet」ダイアログ・ボックス（図 9-15）が表示されます。

図 9-15 「New Wallet」ダイアログ・ボックス



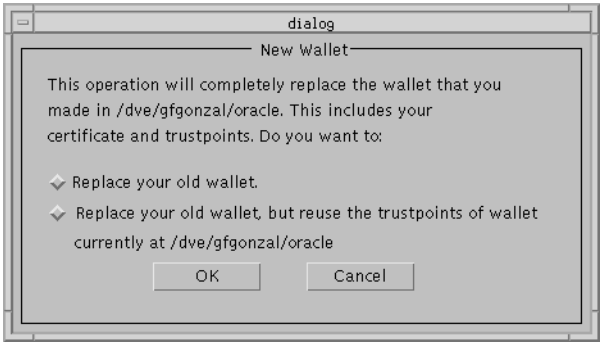
6. 最低 20 文字のランダム文字列をフィールドに入力します。この文字列が公開鍵と秘密鍵を生成するときのシードになります。「OK」をクリックします。

   デフォルトのファイルの場所にすでに存在する Wallet、証明書および信頼できる証明書が新規 Wallet によって上書きされるという内容のメッセージが「New Wallet」ダイアログ・ボックス（図 9-16）に表示されます。このメッセージは、デフォルトの場所にすでに Wallet が存在するときに表示されます。

図 9-16 「New Wallet」ダイアログ・ボックスに表示されたメッセージ

7. 「OK」をクリックします。「Replace Wallet」ダイアログ・ボックス（図 9-17）が表示されます。

図 9-17 「Replace Wallet」ダイアログ・ボックス



8. 証明書と信頼できる証明書を含むすべての Wallet を置き換える場合は「Replace your old wallet」ラジオ・ボタンをクリックします。Wallet を置き換える場合で前の Wallet の信頼できる証明書を再使用する場合は「Replace your old wallet, but reuse...」ラジオ・ボタンをクリックします。最初のダイアログ・ボックスに戻る場合は「Cancel」をクリックし、続ける場合は「OK」をクリックします。

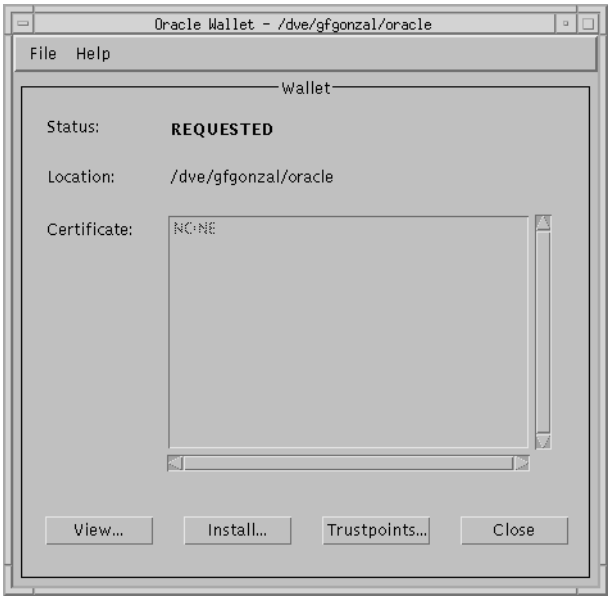
   ダイアログ・ボックス（図 9-18）に証明書要求ファイルの場所が表示されます。このファイルが認証局に送るファイルです。

図 9-18 証明書要求の場所

9. 証明書要求を表示する場合は「View」をクリックし、表示しない場合は「Close」をクリックします。

   状態が「REQUESTED」、証明書が「NONE」の「Oracle Wallet」ダイアログ・ボックス（図 9-19）が表示されます。

図 9-19 証明書要求が表示されている新規 Wallet



手順 6: 新規 Wallet への証明書のインストール

証明書要求を認証局に送ったあとは、署名済みの証明書が含まれた電子メールが戻ってくるのを待ちます。認証局によって異なりますが、certificate.txt のような認証ファイルが返送されてきます。次のいずれかの方法で、新規 Wallet に証明書をインストールします。

- オプション 1: ファイルからの証明書のインストール
- オプション 2: 電子メール本文からの証明書のインストール

オプション 1: ファイルからの証明書のインストール

1. 認証局から受け取ったファイルをオープンし、認証テキストの場所を指定します。証明書の内容は、通常、Begin Certificate と End Certificate で区切られています。
2. 「Oracle Wallet」ダイアログ・ボックスの「Install」をクリックします（図 9-19）。

   「Install a new Certificate」ダイアログ・ボックス（図 9-20）が表示されます。
3. 「Browse」をクリックします。

   ディレクトリ・ダイアログ・ボックスが表示されます。このダイアログ・ボックスを使用して、certificate.txt ファイルの場所を指定します（認証局によって、ファイル名は異なる場合があります）。

4. ファイル名を選択し、「Open」をクリックします。証明ファイルの内容がダイアログ・ボックスに表示されます（図 9-20）。

図 9-20 ウィンドウに表示された証明書のテキスト

5. 「OK」をクリックします。

   「Oracle Wallet」ダイアログ・ボックスに戻ります。状態が「READY」に変わります。

オプション 2: 電子メール本文からの証明書のインストール

1. 認証局から受信した電子メールをオープンします。
2. 電子メール本文から証明書テキストを選択してコピーします。
3. 「Install a new Certificate」ダイアログ・ボックスの「Paste」をクリックします。証明書テキストがこのダイアログ・ボックスに貼り付けられます（図 9-20）。
4. 「OK」をクリックします。
5. 「Oracle Wallet」ダイアログ・ボックスに戻ります。状態が「READY」に変わります。

手順 7: 新規の信頼できる証明書の追加

信頼できる証明書は、信頼レベルの認可を受けたサード・パーティ識別情報です。信頼できる証明書は Wallet 内に含まれます。信頼できる証明書は、エンティティが本人であるという識別情報の確認が行われるときに使用されます。信頼できる証明書は Trustpoint とも呼びます。

Oracle Wallet Manager をインストールすると、VeriSign からの信頼できる証明書のデフォルト・セットがデフォルト Wallet にインストールされます。信頼できる証明書を管理するには Oracle Wallet Manager を使用します。新規の信頼できる証明書の追加、既存の信頼できる証明書情報の表示、信頼できる証明書の削除を行うことができます。

信頼できる証明書の一覧にない CA から発行された証明書を使用する場合は、その CA を一覧に追加する必要があります。CA の証明書がルート CA によって署名されている場合は、証明書を 1 つずつ追加して、**証明書連鎖（certificate chain）**全体を一覧に追加する必要があります。

> **詳細情報：** 信頼できる証明書を追加、表示、管理する方法は、9-45 ページの「信頼できる証明書の管理」を参照してください。

Wallet をファイル・システムに作成すると、その Wallet の場所をアプリケーションで特定できるように構成すれば、SSL を使用してアプリケーションを起動することができます。

手順 8: 変更内容の Wallet への保存

「Oracle Wallet」ダイアログ・ボックスで「File」->「Save」をクリックし、変更内容を Wallet に保存します。

手順 9: Single sign-on 機能での自動ログイン Wallet の作成

Wallet をオープンするたびにユーザーにパスワードを入力させるのではなく、SSL の Single sign-on 機能を使用する場合は、9-31 ページの「手順 5: Wallet の新規作成」で作成した Wallet から自動ログイン Wallet を作成する必要があります。自動ログイン Wallet を作成するには、Oracle Wallet Manager のコマンド行バージョンを使用します。

自動ログイン Wallet の作成

1. sqlnet.ora ファイルに次の行があることを確認します。

```
oss.source.my_wallet =
(SOURCE=
  (METHOD=File)
  (METHOD_DATA=
    (DIRECTORY=your wallet location)
  )
)
```

2. 次の環境変数を設定します。

```
setenv TNS_ADMIN your_sqlnet.ora_file
```

3. コマンド・プロンプトで次のコマンドを入力して、Oracle Wallet Manager のコマンド行バージョンを起動します。

```
owmcmd -f
```

たとえば、次のとおりです。

```
/vobs/oracle/network/bin/owmcmd -f
```

Oracle Wallet Manager のコマンド行バージョンにより、ユーザーのパスワードが求められます。

9-31 ページの「手順 5: Wallet の新規作成」で作成したときに入力したパスワードを入力します。

4. Oracle Wallet Manager により、**Wallet Resource Locator** の入力が求められます。

5. Wallet Resource Locator を入力します。

cwallet.sso という名前で自動ログイン Wallet が作成され、指定した Wallet Resource Locator に配置されます。最初の Wallet がローカル・マシンではなくディレクトリ・サーバーに格納されている場合は、その Wallet がディレクトリ・サーバーからダウンロードされ、それを使用して自動ログイン Wallet が作成されます。そして、その自動ログイン Wallet が指定した Wallet Resource Locator に配置されます。

手順 10: グローバルな証明書によって Oracle Server に認証されるユーザーの作成

企業のディレクトリ・サービスを使用する場合、Oracle Enterprise Manager の Security Manager ツールを使用するか、次のコマンドを入力して、各ローカル・データベースにグローバル・ユーザーを作成します。

```
CONNECT system/manager@database_name;
CREATE USER username IDENTIFIED GLOBALLY AS 'external_name'
```

external_name は、ユーザーの完全な識別名と一致する必要があります。

注意： ディレクトリ・サーバーを使用する場合は、ディレクトリの識別名が Oracle Wallet のものと一致することを確認します。

識別名 識別名は、ユーザーを一意に識別する最大 6 つの情報フィールドから成ります。各フィールドは次のとおりです。

- Common Name (CN)
- Location (L)
- State (ST)
- Organizational Unit (OU)
- Organization (O)
- Country (C)

識別名は、最も細分化されたものから順に左から並べられます。

```
CN=user, L=location, ST=state, OU=unit, O=organization, C=country
```

たとえば、次の属性のユーザーがいるとします。

- Common Name: Tom Jones
- Location: HQ
- State: California
- Organizational Unit: Information Technologies
- Organization: Acme Corporation
- Country: US

このユーザーの完全識別名は次のようになります。

```
CN=Tom Jones, L=HQ, ST=CA, OU=Information Technologies, O=Acme Corporation, C=US
```

したがって、次の文で Tom Jones の新規アカウントを作成できます。

```
CREATE USER tjones IDENTIFIED GLOBALLY AS "CN=Tom Jones, L=HQ, ST=CA,
OU=Information Technologies, O=Acme Corporation, C=US"
```

Oracle Wallet 所有者の完全識別名の取得　9-31 ページの「手順 5: Wallet の新規作成」の「Create a New Wallet」ダイアログ・ボックスで入力した値を参照してください。まず、ダイアログ・ボックスの下部にある「Common Name」フィールドに入力した値を書き留めます。次に、その上の「Organizational Unit」フィールドに入力した値を書き留めます。続いてその上のフィールドの値を書き留めていき、すべてのフィールドの値を書き留めます。上で説明した識別名の書式になるように注意してください。

詳細情報：『Oracle8*i* 管理者ガイド』を参照してください。

管理作業

Oracle Advanced Security の SSL 機能を構成した場合は、その時々に従っていくつかの作業を行う必要があります。この項では、次の作業内容について説明します。

- Wallet の管理
- 信頼できる証明書の管理

Wallet の管理

既存の Wallet のオープン、表示、変更、および Wallet の新規作成を行うには、Oracle Wallet Manager を使用します。

この項では、次の作業について説明します。

- 既存 Wallet のオープン
- Wallet の内容の表示
- Wallet のリモート・ノードへのコピー

> **詳細情報：** Oracle Wallet Manager の起動については、9-29 ページの「手順 4: Oracle Wallet Manager の起動」を参照してください。
>
> Wallet の新規作成については、9-31 ページの「手順 5: Wallet の新規作成」を参照してください。
>
> 新規 Wallet への証明書のインストールについては、9-36 ページの「手順 6: 新規 Wallet への証明書のインストール」を参照してください。

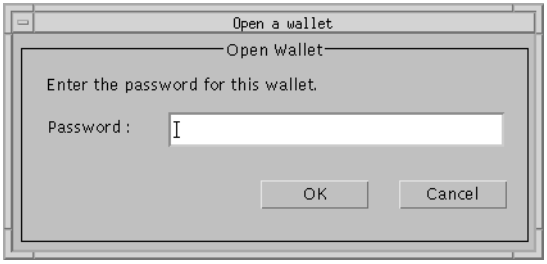
既存 Wallet のオープン

Wallet 所有者がデフォルト Wallet をオープンするには、Oracle Wallet Manager を使用します。デフォルト Wallet は「Oracle Wallet」ダイアログ・ボックスに表示されます。Wallet 所有者は、Wallet をオープンするのに必要な **Wallet Resource Locator**（WRL）と正しいパスワードを指定する必要があります。

1. 「Oracle Wallet」ダイアログ・ボックスの「Open」をクリックします。

   「Open a Wallet」ダイアログ・ボックス（図 9-21）が表示されます。

図 9-21 「Open a Wallet」ダイアログ・ボックス

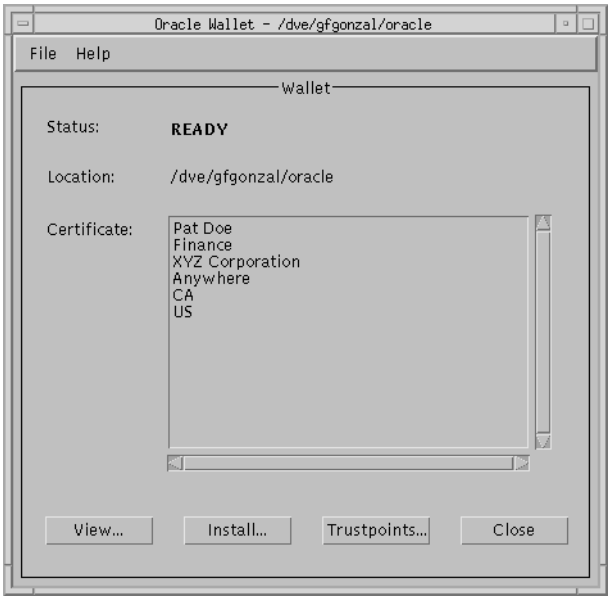


2. パスワードを入力します。「Oracle Wallet」ダイアログ・ボックスに戻る場合は「Cancel」をクリックし、続ける場合は「OK」をクリックします。

   「Oracle Wallet」ダイアログ・ボックス（図 9-22）が表示されます。

注意： 正しいパスワードが入力されなかった場合は、「Failed to Open wallet!」というタイトルのエラー・ダイアログ・ボックスが表示されます。「OK」をクリックして、「Oracle Wallet」ダイアログ・ボックスに戻ります。パスワードを確認して、再度実行します。

図 9-22 「Oracle Wallet」ダイアログ・ボックスのデフォルトの Wallet



Wallet の内容の表示

Wallet の内容を表示、変更するには、「Oracle Wallet」ダイアログ・ボックスを使用します。このダイアログ・ボックスには、次のフィールドとボタンがあります。

フィールド名	説明
「Status」	Wallet の状態を表示します。EMPTY、REQUESTED、READY の 3 つの状態があります。EMPTY 状態は、要求されている証明書またはインストールされている証明書が Wallet にないことを表します。REQUESTED 状態は、Wallet の証明書要求が生成されたことを表します。READY 状態は、証明書があることを表します。
「Location」	Wallet が格納されているディレクトリを表示します。
「Certificate」	Wallet にインストールされている証明書の識別情報の名前を表示します。

ボタン名	機能
「View」	インストールされている証明書を表示します。
「Install」	新規証明書を Wallet にインストールします。
「Trustpoints」	Wallet にインストールされている信頼できる証明書を表示し管理します。
「Close」	「Oracle Wallet」ダイアログ・ボックスに戻ります。

Wallet のリモート・ノードへのコピー

複製されたサーバーを使用している場合は、各ノードに同じ Wallet がある必要があります。

信頼できる証明書の管理

Wallet の信頼できる証明書は Oracle Wallet Manager を使用して管理します。新規の信頼できる証明書の追加、既存の信頼できる証明書の表示、信頼できる証明書の削除を行うことができます。Oracle Wallet Manager をインストールすると、4 つの信頼できる証明書のデフォルト・セットがデフォルト Wallet にインストールされます。

この項では、次の作業について説明します。

- 新規の信頼できる証明書の追加
- 既存の信頼できる証明書情報の表示
- 信頼できる証明書の削除
- Wallet の既存 WRL（Wallet Resource Locator）への保存

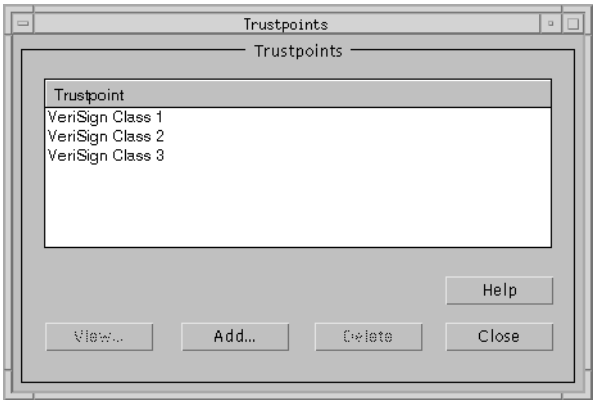
新規の信頼できる証明書の追加

新規の信頼できる証明書を Wallet に追加するには、次の手順で行います。

1. 「Oracle Wallet」ダイアログ・ボックスの「Trustpoint」をクリックします（9-44 ページの図 9-22）。

   「Trustpoints」ダイアログ・ボックス（9-46 ページの図 9-23）が表示されます。

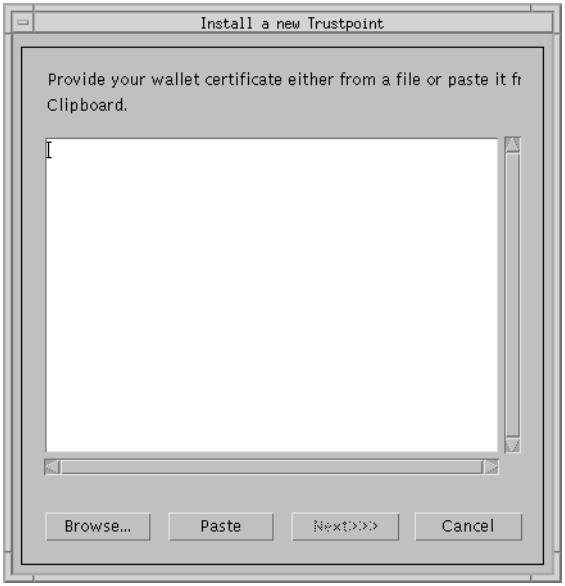
図 9-23 「Trustpoints」ダイアログ・ボックス



2. 「Add」をクリックします。

   「Install a New Trustpoint」ダイアログ・ボックス（図 9-24）が表示されます。このダイアログ・ボックスに、信頼できる証明書を貼り付けます。

図 9-24 「Install a New Trustpoint」ダイアログ・ボックス

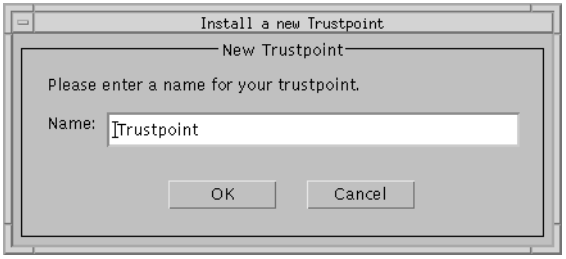


3. 「Paste」をクリックします。証明書テキストがダイアログ・ボックス本体に表示されます。

4. 「Next」をクリックします。

   「New Trustpoint」ダイアログ・ボックス（図 9-25）が表示されます。

図 9-25 「New Trustpoint」ダイアログ・ボックス



5. 信頼できる証明書の別名を入力します。名前には任意の英数字が使用できますが、空白は使用できません。
6. 前のダイアログ・ボックスに戻る場合は「Cancel」をクリックし、続ける場合は「OK」をクリックします。

   作成した信頼できる証明書が「Trustpoints」ダイアログ・ボックス（9-46 ページの図 9-23）の信頼できる証明書の一覧に追加されます。
7. 「Close」をクリックして「Oracle Wallet」ダイアログ・ボックス（9-44 ページの図 9-22）に戻ります。

既存の信頼できる証明書情報の表示

「Trustpoints」ダイアログ・ボックスを使用して信頼できる証明書の詳細情報を表示するには、次の手順で行います。

1. 詳細情報を表示する信頼できる証明書の名前をクリックします。
2. 「View」をクリックします。

   「Trustpoint Certificate」ダイアログ・ボックス（9-48 ページの図 9-26）が表示されます。

図 9-26 「Trustpoint Certificate」ダイアログ・ボックス

3. Wallet にインストールされている信頼できる証明書の情報を確認します。この情報には、証明書の識別情報と発行者が含まれます。
4. Wallet の信頼できる証明書の X.509 v3 証明書拡張情報を表示するには「Extensions」をクリックし、「Trustpoints」ダイアログ・ボックスに戻るには「Close」をクリックします。

信頼できる証明書の削除

信頼できる証明書の信用が損なわれた場合には、Oracle Wallet Manager を使用して削除できます。「Trustpoints」ダイアログ・ボックス（9-46 ページの図 9-23）を使用して信頼できる証明書を削除するには、次の手順で行います。

1. 「Trustpoint」列に表示されている信頼できる証明書の名前をクリックし、信頼できる証明書を選択します。
2. 「Delete」をクリックします。

   ダイアログ・ボックスに「Do you really want to delete this trusted certificate?」というメッセージが表示されます。

3. 信頼できる証明書を削除する場合は「Yes」をクリックします。

   「Trustpoints」ダイアログ・ボックスに戻ります。信頼できる証明書の一覧には、今削除した信頼できる証明書は表示されません。

   「No」をクリックすると、同じように「Trustpoints」ダイアログ・ボックスに戻りますが、信頼できる証明書の一覧には、選択した信頼できる証明書は表示されます。

4. 「Close」をクリックして「Oracle Wallet」ダイアログ・ボックスに戻ります。

Wallet の既存 WRL（Wallet Resource Locator）への保存

「Oracle Wallet」ダイアログ・ボックスで「File」->「Save」をクリックし、変更内容を Wallet に保存します。

データベースへのログイン

SSL 認証を使用している場合は SQL*Plus を起動して、プロンプトで次のように入力します。

```
CONNECT/@database_alias
```

SSL 認証を使用していない場合は SQL*Plus を起動して、プロンプトで次のように入力します。

```
CONNECT username/password@database_alias
```

10

認証方式の選択と組合せ

この章では、別の認証方式を構成してあってもそれを使用せずに、ユーザー名 / パスワードによる従来の方法での認証を使用する方法について説明します。また、Oracle Advanced Security を使用して、1 つまたは複数の認証方式を使用するネットワークを構成する方法、およびクライアント上またはサーバー上で複数の認証方式をセットアップする方法についても説明します。

この章では、次のトピックについて説明します。

ユーザー名とパスワードによる接続

ユーザー名とパスワードを使用して Oracle Server に接続する場合、Oracle Advanced Security 認証方式が構成されている場合は、後者を使用禁止にします。

詳細情報： 10-3 ページの「Oracle Advanced Security 認証を使用禁止にする」を参照してください。

Oracle Net8 Assistant の使用

このグラフィカル・インタフェース・ツールを使用して、sqlnet.ora ファイルと他の Oracle8*i* 構成ファイルのパラメータを簡単に設定できます。

Oracle Net8 Assistant の起動

- UNIX では、$ORACLE_HOME/bin でスクリプト netasst を実行します。
- Windows プラットフォームでは、「スタート」ボタン ->「プログラム」->「Oracle ー *HOME_NAME*」->「Network Administration」->「Net8 Assistant」の順にクリックします。

Oracle Net8 Assistant を使用した Oracle Advanced Security の構成

Oracle Net8 Assistant の左側のペインで「Profile」フォルダをクリックします。次に、右側のペインの上端にあるドロップ・ダウン・リスト・ボックスで「Advanced Security」を選択します。Oracle Advanced Security のタブ・ページが表示されます。

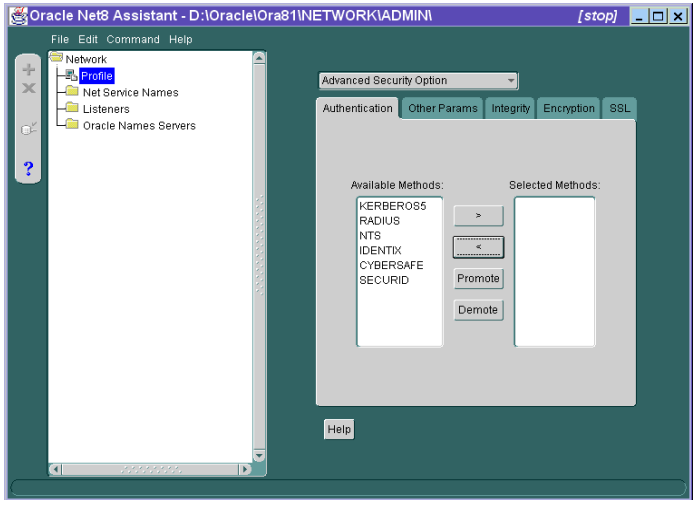
Oracle Net8 Assistant による変更内容の保存

メニュー・バーの「File」->「Save Network Configuration」をクリックします。

Oracle Advanced Security 認証を使用禁止にする

Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して sqlnet.ora ファイルを変更します。

図 10-1 Oracle Net8 Assistant を使用して認証を使用禁止にする



Oracle Net8 Assistant を使用	SQLNET.ORA を変更
図 10-1 を参照してください。 1. 「Authentication」タブをクリックします。 2. 「Selected Methods」でメソッドを選択し、左矢印ボタン「<」をクリックして、「Available Methods」に移動します。 3. 「Selected Methods」からすべてのメソッドが削除されるまで繰り返します。	次のパラメータを設定します。 `SQLNET.AUTHENTICATION_SERVICES = (NONE)`

ユーザーは、次に示すユーザー名 / パスワードの書式でデータベースに接続できます。

```
% sqlplus username/password@net_service_name
```

たとえば、次のとおりです。

```
% sqlplus scott/tiger@emp
```

複数の認証メソッドを使用する Oracle の構成

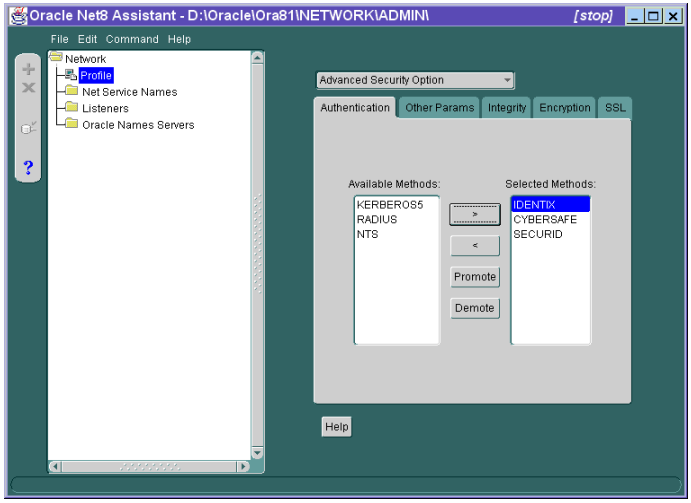
多くのネットワークは、1 つのセキュリティ・サーバー上で複数の認証メソッドを使用しています。このため、Oracle Advanced Security では、Oracle クライアントが特定の認証方式を使用し、Oracle Server が任意の方式を受け入れられるようにネットワークを構成することができます。

この項では、複数の認証方式を使用する Oracle Server と Oracle クライアントのセットアップ方法について説明します。

クライアント・マシンとサーバー・マシンの両方に複数の認証方式をセットアップするには、Oracle Net8 Assistant を使用するか、テキスト・エディタを使用して sqlnet.ora ファイルを変更します。

次に示す手順は、クライアントとサーバーの両方に適用できます。

図 10-2 Oracle Net8 Assistant を使用した複数メソッドの構成



Oracle Net8 Assistant を使用	SQLNET.ORA を変更

図 10-2 を参照してください。
1. 「Authentication」タブを選択します。
2. 「Available Methods」リストでメソッドを選択します。
3. 右矢印ボタン「>」をクリックして、選択したメソッドを「Selected Methods」リストに移動します。
4. 必要なすべてのメソッドが「Selected Methods」に追加されるまで繰り返します。
5. メソッドをクリックし、「Promote」ボタンまたは「Demote」ボタンをクリックして、使用優先順位の高い順に認証方式を並べ替えます。
「Selected Methods」リストの先頭に置いたメソッドで、認証が開始されます。
	次のパラメータを設定します。
	`SQLNET.AUTHENTICATION_SERVICES=(`*`RADIUS`* `|` *`CYBERSAFE`* `|` *`KERBEROS`* `|` *`SECURID`* `|` *`IDENTIX`*`)`
	必要なすべてのメソッドが追加されるまで、確認証方式の名前を入力します。
	例 :
	`SQLNET.AUTHENTICATION_SERVICES =(SECURID,CYBERSAFE)`

第 II 部

Oracle Advanced Security および Oracle DCE Integration

注意： プラットフォームの Oracle Advanced Security リリース 8.1.5 で Oracle DCE Integration がサポートされているかどうかを、プラットフォーム固有のインストレーション・マニュアルで確認してください。

次の章では、Oracle 分散コンピューティング環境（DCE）Integration について説明しています。

- 第 11 章の「Oracle DCE Integration の概要」
- 第 12 章の「Oracle DCE Integration を使用する DCE の構成」
- 第 13 章の「Oracle DCE Integration を使用する Oracle の構成」
- 第 14 章の「DCE 環境の Oracle データベースに接続」
- 第 15 章の「DCE 環境と非 DCE 環境の相互運用性」

11

Oracle DCE Integration の概要

この章では、分散コンピューティング環境（DCE）と Oracle DCE Integration 製品について簡単に説明します。

> **詳細情報：** 詳細は、このマニュアルの「はじめに」に示した xvii ページの「関連マニュアル」を参照してください。

この章では、次のトピックについて説明します。

- システム要件
- 下位互換性
- 分散コンピューティング環境（DCE）の概要
- Oracle DCE Integration の概要

システム要件

Oracle DCE Integration を使用するには、Net8 と Oracle8*i* が必要です。Oracle DCE Integration を使用すると、Oracle アプリケーションと Oracle Tools から DCE 環境の Oracle8*i* サーバーにアクセスできます。

注意： Oracle DCE Integration は、オープン・ソフトウェア・ファウンデーション（OSF）の DCE バージョン 1.0 または 1.1 をベースにした製品で、OSF が今後発表する DCE と互換性を保ちます。

OSF は、もう 1 つの標準グループである X/Open と合併して Open Group を設立しました。このグループが引き続き DCE をサポートする計画です。

下位互換性

DCE Integration 2.3.2 以降のリリースを稼働している Oracle Server は、SQL*Net/DCE 2.1.6 または 2.2.3 を稼働しているクライアントと下位互換性があります。ただし、2.1.6 を稼働しているクライアントは、外部ロールを利用できません。

DCE Integration 2.3.2 以降のリリースを稼働しているクライアントは、SQL*Net/DCE 2.1.6 または 2.2.3 を稼働しているサーバーに接続できません。DCE Integration 2.3.2 以降のリリースを稼働しているクライアントがデータベースに接続するには、2.3.2 以降のリリースを稼働しているサーバーが必要です。

分散コンピューティング環境（DCE）の概要

オープン・ソフトウェア・ファウンデーション（OSF）の分散コンピューティング環境（DCE）は、複数のシステムで機能して分散環境を提供する一連の統合ネットワーク・サービスです。ネットワーク・サービスには、リモート・プロシージャ・コール（RPC）、ディレクトリ・サービス、セキュリティ・サービス、スレッド、分散ファイル・サービス、ディスクレス・サポート、分散タイム・サービスなどがあります。

DCE は、分散アプリケーションとオペレーティング・システム / ネットワーク・サービスの間に存在するミドルウェアであり、クライアント / サーバー・モデルをベースにしています。ユーザーは DCE が提供するサービスとツールを使用して、異機種環境で動作する分散アプリケーションを作成および使用、管理できます。

詳細情報： このマニュアルの「はじめに」に示した xvii ページの「関連マニュアル」を参照してください。

Oracle DCE Integration の概要

Oracle DCE Integration を使用すると、Oracle Tools と Oracle Applications から DCE 環境の Oracle8*i* サーバーにアクセスすることができます。

Oracle DCE Integration の構成要素

Oracle の DCE Integration 製品は DCE Communication/Security および DCE CDS Native Naming から成ります。

DCE Communication/Security

DCE Communication/Security には、次のものが含まれます。

- **認証された RPC** － Oracle DCE Integration は、複数ベンダー間での相互運用性を実現するトランスポート・メカニズムとして、認証されたリモート・プロシージャ・コール（RPC）を採用しています。RPC は他の DCE サービス（ディレクトリ・サービスやセキュリティ・サービスなど）を使用して、位置の透過性と安全な分散コンピューティングも実現します。
- **統合セキュリティと Single sign-on** － Oracle DCE Integration は DCE セキュリティ・サービスと連携して、DCE セル内のセキュリティを確立します。このため、DCE にログオンしたユーザーは、ユーザー名またはパスワードを指定しなくても、任意の Oracle データベースに安全にアクセスできます。これをデータベースへの外部認証といったり、*single sign-on* という場合もあります。DCE 認証サービスを使用しないクライアントとサーバーは、Oracle パスワードを指定することによって、DCE セキュリティが確立されているシステムにアクセスできます。
- **データのプライバシと整合性**－ Oracle DCE Integration は、DCE が提供する複数のレベルのセキュリティを使用して、データの確実性とプライバシおよび整合性を保証しています。たとえば、ユーザーは接続ごとに「保護なし」から「完全な暗号化」までのさまざまなレベルを選択して、転送中のデータが変更されないようにすることができます。

注意： ネットワーク内で DCE を使用しない部分では、Oracle Advanced Security に用意された他のセキュリティ・サービスと認証サービスを使用することができます。（以前は Secure Network Service で提供されていた）これらのサービスは、SQL*Net 2.1 以降のリリースまたは Net8 で機能します。これらのサービスは、非 DCE 環境でメッセージ整合性サービスとデータ暗号化サービスを提供します。これらのサービスによって、ネットワーク接続の始点または終点に関係なく、すべてのネットワーク・トラフィックが許可なしに表示または変更されるのを防止できます。

詳細情報： このマニュアルの第 1 部「Oracle Advanced Security 機能」を参照してください。

DCE CDS 固有のネーム

DCE CDS Native Naming コンポーネントには命名機能と位置透過性の機能があります。

DCE Integration は Oracle8*i* 接続記述子を DCE セル・ディレクトリ・サービス（CDS）に登録して、DCE 環境内のどこからでも接続記述子に透過的にアクセスできるようにします。

ユーザーは使い慣れた Oracle サービス名で、DCE 環境内の Oracle データベース・サーバーに接続できます。

DCE セル・ディレクトリ・サービスは、ネットワークに存在するオブジェクトの名前、アドレスおよび属性を登録する分散型の複製リポジトリ・サービスです。サーバーがオブジェクトの名前とアドレス情報をセル・ディレクトリ・サービス（CDS）に登録するので、Oracle クライアントは位置に依存しないで Oracle8*i* サーバーに接続できます。クライアントの構成に変更を加えずに、サービスを再配置できます。Oracle ユーティリティを使用して、Oracle サービス名（および、対応する接続記述子）を CDS にロードします。Oracle サービス名を CDS にロードしたら、標準 DCE ツールを使用して集中管理された Oracle 接続識別子を表示できます。

サービスの位置が複数のセルにまたがっている場合は、次のサービスを使用することができます。

- DCE グローバル・ディレクトリ・サービス（GDS）
- インターネット・ドメイン・ネーム・サービス

詳細情報： DCE CDS Native Naming の詳細は、次の章またはマニュアルを参照してください。

- CDS ネーミングを使用する DCE の構成については、第 12 章の「Oracle DCE Integration を使用する DCE の構成」を参照
- CDS を使用する Oracle クライアントと Oracle Server の構成については、第 13 章の「Oracle DCE Integration を使用する Oracle の構成」を参照
- Oracle Native Naming と他の Oracle ネーム・サービスの連携については、『Oracle8*i* Net8 管理者ガイド』を参照

DCE の柔軟な配置方法

Oracle Advanced Security では、DCE のサービス使用方法を柔軟に選択できます。次のオプションを選択できます。

- DCE Integration 全体を環境に配置して、このマニュアルの第 2 部で説明するすべての DCE Secure Core サービス（RPC、ディレクトリ、セキュリティ、スレッド）と統合することができます。
- DCE CDS 固有のネーム・アダプタと、TCP/IP のような従来型のプロトコル・アダプタを使用できれば、DCE のディレクトリ・サービスのみを使用することができます。CDS 固有のネーム・アダプタの構成については、このマニュアルの第 12 章の「Oracle DCE Integration を使用する DCE の構成」と第 13 章の「Oracle DCE Integration を使用する Oracle の構成」で説明します。

  詳細情報： Oracle 固有のネーム・アダプタと他の Oracle ネーム・サービスの連携については、『Oracle8*i* Net8 管理者ガイド』を参照してください。

- このマニュアルの第 8 章の「DCE GSSAPI 認証の構成」で説明した DCE GSSAPI 認証方式を使用すると、DCE の認証サービスのみを使用することができます。この場合は OSF DCE 1.1 が必要です。

このリリースにおける制限事項

- DCE プロトコルを使用するリスナー・アドレスは、各ノードで 1 つしか認められていません。
- データベース・リンクで接続するには、ユーザー名とパスワードを指定する必要があります。
- このリリースの DCE Integration アダプタは、Oracle MultiProtocol Interchange をサポートしていません。
- このリリースは Oracle マルチスレッド・サーバー（MTS）で動作しません。

12

Oracle DCE Integration を使用する DCE の構成

この章では、Oracle DCE Integration を正しくインストールした後で、DCE Integration を使用できるように DCE を構成する手順について説明します。

> **詳細情報：** 詳細は、このマニュアルの「はじめに」に示した xvii ページの「関連マニュアル」を参照してください。

DCE Integration を使用する DCE の構成

DCE Integration を使用する DCE の構成手順を、次のようにまとめることができます。この手順では、DCE セルが構成済みで、マシンがそのセルの一部であると想定しています。

DCE セル管理者として、次の作業を実行する必要があります。

手順 1: 新しいプリンシパルとアカウントの作成

手順 2: サーバーのキーをキータブ・ファイルにインストール

手順 3: Oracle DCE Integration で使用する DCE CDS を構成

手順 1: 新しいプリンシパルとアカウントの作成

最初に、次のような手順を使用してサーバー・プリンシパルを追加します。

```
% dce_login cell_admin password
% rgy_edit
Current site is: registry server at
  /.../cell1/subsys/dce/sec/master
rgy_edit=>do p
Domain changed to: principal
rgy_edit=> add oracle
rgy_edit=> do a
Domain changed to: account
rgy_edit=> add oracle -g none -o none -pw oracle_password
  -mp cell_admin_password
rgy_edit=> quit
bye
```

これで、"oracle" という DCE プリンシパルが作成されました。このプリンシパルには、"*password*" というパスワードを持つアカウントが対応しています。このアカウントはどの DCE グループまたは DCE プロファイルにも属していません。

DCE Integration をインストールした後で、この手順を一度だけ実行します。また、このプロシージャは、クライアントに対してではなく、Oracle データベース・サーバーに対して実行します。

手順 2: サーバーのキーをキータブ・ファイルにインストール

この段階的な手順では、サーバーのキーをキータブ・ファイル（dcepa.key）にインストールします。このキータブ・ファイルには、Net8 リスナーが起動するプリンシパルのパスワードが入っています。Net8 リスナーはこのファイルを読み取って、リスナー自身を DCE に対して認証します。DCE Integration をインストールした後で、この手順を一度だけ実行します。また、このプロシージャは、クライアントに対してではなく、Oracle データベース・サーバーに対して実行します。

注意： $ORACLE_HOME 変数を適切な完全パス名で置き替えてください。存在していないディレクトリを指定する場合は、コマンドを実行する前にそのディレクトリを作成する必要があります。次のように入力してディレクトリを作成します。

```
mkdir $ORACLE_HOME/dcepa
mkdir $ORACLE_HOME/dcepa/admin
```

次のコマンドを実行してキータブ・ファイルを生成します。

```
% dce_login cell_admin password
% rgy_edit
Current site is: registry server at /.../cell1/subsys/dce/sec/master
rgy_edit=> ktadd -p oracle -pw Oracle_password -f
$ORACLE_HOME/dcepa/admin/dcepa.key
rgy_edit=>quit
bye
```

手順 3: Oracle DCE Integration で使用する DCE CDS を構成

/.:/subsys/oracle/names ディレクトリに、Net8 サービス名を接続記述子にマップするオブジェクトが入っています。CDS ネーム・アダプタがこの接続記述子を使用します。

/.:/subsys/oracle/service_registry ディレクトリにも、DCE アドレス内のサービス名をネットワーク終点にマップするオブジェクトが入っています。DCE プロトコル・アダプタのクライアントとサーバーが、このネットワーク終点を使用します。

CDS 名前領域に Oracle ディレクトリを作成する

DCE Integration Adapter を初めてセルにインストールした後で、この作業を実行する必要があります。

```
% dce_login cell_admin
Enter Password:(password not displayed)

$ cdscp
cdscp> create dir /.:/subsys/oracle
```

```
cdscp> create dir /.:/subsys/oracle/names
cdscp> create dir /.:/subsys/oracle/service_registry
cdscp> exit
```

注意： これらのディレクトリをすべての CDS レプリカ上で作成します。

CDS 名前領域でのオブジェクト作成権限をサーバーに付与する

次の手順を実行して、oracle プリンシパルを cds-server グループに追加します。

```
$ dce_login cell_admin
Enter Password:    (password not displayed)
$ rgy_edit
rgy_edit=> domain group
Domain changed to: group
rgy_edit=> member subsys/dce/cds-server -a oracle
rgy_edit=> exit
```

Oracle サービス名を CDS にロードする

詳細情報： クライアントの構成方法の詳細は、13-13 ページの「DCE CDS ネームを使用するクライアントの構成」を参照してください。

Oracle サービス名を CDS にロードする方法については、13-15 ページの「Oracle 接続記述子を CDS にロードするのに必要な TNSNAMES.ORA ファイルを作成」を参照してください。

13

Oracle DCE Integration を使用する Oracle の構成

この章では、Oracle DCE Integration をインストールした後で、DCE Integration を使用できるように Oracle と Net8 を構成する方法について説明します。次の各項で、サーバーとクライアントで設定する必要があるパラメータについて説明します。

- DCE アドレス・パラメータ
- サーバーの構成
- 外部的に認証されるアカウントの作成と命名
- DCE Integration の外部ロールの設定
- クライアントの構成
- DCE CDS ネームを使用するクライアントの構成

DCE アドレス・パラメータ

listener.ora 構成ファイルと tnsnames.ora 構成ファイルの DCE アドレスは、DCE パラメータによって定義されます。これらのパラメータは、以下で説明する必須フィールドとオプション・フィールドで構成されています。

```
ADDRESS=(PROTOCOL=DCE)
        (SERVER_PRINCIPAL=server_name)
        (CELL_NAME=cell_name)
        (SERVICE=dce_service_name))
```

各構成要素は次のとおりです。

PROTOCOL	DCE RPC プロトコルを識別する必須フィールドです。
SERVER_PRINCIPAL	サーバーの必須フィールドで、クライアントのオプション・フィールドです。サーバーはこのプリンシパルでサーバー自身を DCE に対して認証します。このフィールドは、リスナー構成ファイル（listener.ora）の必須フィールドで、サーバーが起動する際のプリンシパルを指定します。このフィールドは、ローカル名構成ファイル（tnsnames.ora）のオプション・フィールドで、クライアントが接続する必要があるサーバーのプリンシパルを指定します。このフィールドを指定しないと、1 方向の認証が使用されます。この場合、クライアントはサーバーのプリンシパルを意に介しません。
CELL_NAME	オプション・パラメータです。このパラメータを設定して、データベースの DCE セル名を指定します。このパラメータを設定しないと、セル名はデフォルトのローカル・セルになります（これは、単一セル環境で役立ちます）。また、次に説明する SERVICE パラメータでサービスの完全パス（セル名を含むパス）を指定すれば、CELL_NAME パラメータを設定する必要はありません。
SERVICE	サーバーとクライアントの両方で必須フィールドです。サーバーでは、CDS に登録されているサービスを指定します。クライアントでは、CDS に Oracle DCE サーバーの場所を問い合せるときに使用するサービス名を指定します。サービス名を CDS に格納するときのデフォルト・ディレクトリは、/.../cell_name/subsys/oracle/service_registry です。このサービス名で、CDS 内の完全パスを指定できます。

サービスを次のように指定します。

```
SERVICE=/.../cell_name/subsys/oracle/service_registry/dce_service_name
```

次のように指定することもできます。

SERVICE=*dce_service_name*

CELL_NAME=cell_name も指定されている場合です。

もう 1 つの方法として、SERVICE=dce_service_name と指定することもできます。この場合、セル名はデフォルトのローカル・セルになります。しかし、この方法でサービス名を指定できるのは、1 つのセル内で作業をしているときのみです。

注意： SERVICE フィールドで指定する dce_service_name は、Net8 が使用するサービス名と同じでも違っていてもかまいません。Net8 が使用するサービス名は、ローカル名構成ファイル（tnsnames.ora）内の接続記述子にマップされます。dce_service_name は、接続記述子内のアドレス部です。

注意： このリリースの DCE Integration では、listener.ora、sqlnet.ora、tnsnames.ora、protocol.ora の各構成ファイルは、$ORACLE_HOME/network/admin ディレクトリにあります。init<*sid*>.ora ファイルは、$ORACLE_HOME/dbs ディレクトリにあります。

サーバーの構成

DCE Integration を使用するサーバーを構成するには、13-2 ページの「DCE アドレス・パラメータ」と次項以降で説明するように、Net8 ファイルで DCE のアドレス情報とパラメータ情報を設定する必要があります。

注意： Oracle Net8 Assistant を使用して必要な構成ファイルを作成します。構成ファイルの詳細は、『Oracle8*i* Net8 管理者ガイド』を参照してください。

サーバーを構成するには、次の前提条件を満たしている必要があります。

- すべてのサーバーに対して、リスナー構成ファイル（listener.ora）で DCE のアドレス情報を設定する必要があります。
- 分散環境内で他のサーバーにデータベース・リンク接続する必要があるサーバーに対して、プロファイル（sqlnet.ora）と protocol.ora ファイルを構成する必要があります。

LISTENER.ORA パラメータ

データベース・サーバーが DCE 環境で Net8 クライアントからの接続を受け入れるには、サーバー・プラットフォーム上で Net8 リスナーがアクティブになっていなければなりません。リスナーは、リスナー構成ファイル（listener.ora）で定義されているネットワーク・アドレス上で接続をリスニングします。

SERVER_PRINCIPAL パラメータは、リスナーが動作する DCE プリンシパルを指定します。次のサンプルでは、リスナーが「oracle」プリンシパルで動作しています。

LISTENER.ORA ファイルで設定する DCE アドレスのサンプル

次に示すのは、listener.ora ファイルで設定する DCE アドレスのサンプルです。

```
LSNR_DCE=
  (ADDRESS=
      (PROTOCOL=DCE)
      (SERVER_PRINCIPAL=oracle)
      (CELL_NAME=cell1)
      (SERVICE=dce_svc))
SID_LIST_LSNR_DCE=
      (SID_DESC=
      (SID_NAME=ORASID)
       (ORACLE_HOME=/private/oracle7))
```

外部的に認証されるアカウントの作成と命名

DCE 認証を使用して Oracle データベースにログオンするには、「外部的に認証される」データベース・アカウントを作成する必要があります。

> **詳細情報：** 外部認証の詳細は、『Oracle8*i* 分散システム』を参照してください。

次の手順に従って、安全性の高い外部認証を使用可能にします。

1. init<*sid*>.ora ファイルに次の行があるかどうか確認します。

   ```
   REMOTE_OS_AUTHENT=FALSE
   OS_AUTHENT_PREFIX=""
   ```

2. DCE に対するマルチスレッド・サーバー（MTS）のエントリが、init<*sid*>.ora ファイルに存在しないことを確認します。たとえば、次のようなエントリがあってはいけません。

   ```
   mts_dispatchers="dce, 3"
   ```

3. DBA グループのメンバーとしてログインしていることを確認します。データベース・インスタンスを再起動して、変更内容を有効にします。
4. SQL*Plus プロンプトでユーザーを定義します。その前に、現在またはこれ以降に、Oracle データベースにセルの境界を超えてアクセスできるマルチセル DCE 環境で作業をするかどうかを判断します。ユーザーの定義方法は、ユーザーが 1 つのセル内でデータベースに接続するか、セルの境界を超えて接続するかによって異なります。

注意： この後に示す権限は最小限必要な権限です。実際に必要な権限は、インスタンスまたはアプリケーション（あるいはその両方）によって異なります。

ユーザーがローカル・セル内で接続する場合は、次の書式を使用します。

```
SQL> CREATE USER server_principal IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO server_principal;
```

たとえば、次のとおりです。

```
SQL> CREATE USER oracle IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO oracle;
```

注意： CELL_NAME/SERVER_PRINCIPAL 文字列の長さは、全体で 15 字以内でなければなりません。

たとえば、次のとおりです。

```
SQL> CREATE USER "CELL1/ORACLE" IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO "CELL1/ORACLE";
```

複数のセルにまたがってデータベースに接続する場合は、cell_name と server_principal の両方を指定します。

```
SQL> CREATE USER "CELL_NAME/SERVER_PRINCIPAL" IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO "CELL_NAME/SERVER_PRINCIPAL";
```

注意： スラッシュは予約文字なので、外部的に識別されるアカウントの名前を二重引用符で囲む必要があります。また、アカウント（ユーザー）名を二重引用符で囲む場合は、アカウント（ユーザー）名を大文字で入力する必要があります。

たとえば、次のとおりです。

```
SQL> CREATE USER "CELL1/ORACLE" IDENTIFIED EXTERNALLY;
SQL> GRANT CREATE SESSION TO "CELL1/ORACLE";
```

注意： 前述の書式を使用するときは、protocol.ora ファイルで次のパラメータを FALSE に設定します。

```
dce.local_cell_usernames=false
```

注意： この方法で作成した Oracle アカウントを参照するときは、スキーマ / アカウントを適切な書式で指定する必要があります。たとえば、別のアカウントの表にアクセスを要求する場合について考えてみます。ローカル・セル内で作成した別のアカウントの表を参照するときは、次のようなコマンドを使用します。

```
SQL> SELECT * FROM oracle.emp
```

複数のセルにまたがる接続用に作成した別のアカウントの表にアクセスしたいときは、次のようなコマンドを使用します。

```
SQL> SELECT * FROM "CELL1/ORACLE".emp
```

DCE Integration の外部ロールの設定

この項では、DCE Integration の外部ロールを設定する手順と、DCE 資格証明で SYSOPER または SYSDBA として Oracle データベースに接続する方法を説明します。

DCE Integration の外部ロールの設定

1. 次のパラメータを init<*sid*>.ora に設定します。

   ```
   OS_ROLES=TRUE
   ```

   次に、データベースを再起動します。

2. Oracle ロールにマップする DCE グループが、次の構文になっているかどうかを確認します。

   ```
   ORA_<global_name>_<role>[_[a][d]]
   ```

   各構成要素は次のとおりです。

ORA	このグループを Oracle 用に使用することを指定
<GLOBAL_NAME>	データベースのグローバル名
<ROLE>	データ・ディクショナリで定義されているロール名

A	ユーザーがこのロールの admin 権限を持つことを示すオプション文字
D	接続時にデフォルトでロールを使用可能にすることを示すオプション文字

注意： 外部ロールの詳細は、『Oracle8*i* 管理者ガイド』を参照してください。

3. DCE が `dce_login` コマンドと `klist` コマンドを実行して、DCE グループのメンバーであるユーザーを認証します（`dce_login` コマンドと `klist` コマンドのサンプル出力を次に示します）。

注意： DCE グループは、手順 2 に示した構文で指定されていなければなりません。

```
% dce_login oracle
Enter Password:
% klist
DCE Identity Information:
        Warning: Identity information is not certified
        Global Principal: /.../ilab1/oracle
        Cell:      001c3f90-01f5-1f72-ba65-02608c2c84f3 /.../ilab1
        Principal: 00000068-0568-2f72-bd00-02608c2c84f3 oracle
        Group:     0000000c-01f5-2f72-ba01-02608c2c84f3 none
        Local Groups:
      0000000c-01f5-2f72-ba01-02608c2c84f3 none
      0000006a-0204-2f72-b901-02608c2c84f3 subsys/dce/cds-server
      00000078-daf4-2fe1-a201-02608c2c84f3 ora_dce222_dba
      00000084-89c8-2fe8-a201-02608c2c84f3 ora_dce222_connect_d
      00000087-8a13-2fe8-a201-02608c2c84f3 ora_dce222_resource_d
      00000080-f681-2fe1-a201-02608c2c84f3 ora_dce222_role1_ad
.
.
.
```

4. 通常の方法でデータベースに接続します。

   次のサンプル出力は、DCE グループにマップされた外部ロール（DBA、CONNECT、RESOURCE、ROLE1）のリストを示しています。

```
SQL> SELECT * FROM session_roles;

ROLE
------------------------------
CONNECT
RESOURCE
ROLE1

SQL> SET ROLE all;

Role set.

SQL> SELECT * FROM session_roles;

ROLE
------------------------------
DBA
EXP_FULL_DATABASE
IMP_FULL_DATABASE
CONNECT
RESOURCE
ROLE1

6 rows selected.

SQL> EXIT
```

DCE で SYSDBA または SYSOPER として Oracle データベースに接続

DCE 資格証明で SYSOPER または SYSDBA として Oracle データベースに接続するには、次の手順で行います。

1. Oracle DBA ロールと OPERATOR ロールにマップする DCE グループを作成します。DCE グループ名は、13-6 ページの「DCE Integration の外部ロールの設定」で説明している構文に準拠している必要があります。外部的に認証されるユーザー「oracle」をグループのメンバーとして追加します。

```
$ dce_login cell_admin <cell_admin password>
$rgy_edit
rgy_edit=> domain group
DOmain changed to: group
rgy_edit=> add ora_dce222_dba_ad
```

```
rgy_edit=> add ora_dce222_operator_ad
rgy_edit=> member ora_dce222_dba_ad -a oracle
rgy_edit=> member ora_dce222_operator_ad -a oracle
```

2. GLOBAL_NAME パラメータを DCE アドレスに追加するか、TNS サービス名をローカル構成ファイル TNSNAMES.ORA に追加します。

```
ORADCE=
    (ADDRESS=
               (PROTOCOL=DCE)
               (SERVER_PRINCIPAL=oracle)
               (CELL_NAME=cell1)
               (SERVICE=dce_svc))
 (CONNECT_DATA=
              (SID=ORASID)
              (GLOBAL_NAME=dce222)))
```

3. 13-4 ページの「外部的に認証されるアカウントの作成と命名」で説明している方法で、データベース・ユーザー「oracle」を作成します。

4. 外部的に認証されるユーザーの DCE 資格証明を取得します。

```
$ dce_login oracle <oracle password>
$klist
DCE Identity Information:
        Warning: Identity information is not certified
        Global Principal: /.../dce.dlsun685.us.oracle.com/oracle
        Cell:      00af8052-7e94-11d2-b261-9019b88baa77
/.../dce.dlsun685.us.ora
cle.com
        Principal: 0000006d-88b9-21d2-9300-9019b88baa77 oracle
        Group:     0000000c-7e94-21d2-b201-9019b88baa77 none
        Local Groups:
                0000000c-7e94-21d2-b201-9019b88baa77 none
                0000006a-7e94-21d2-ad01-9019b88baa77 subsys/dce/cds-server
                00000076-8b53-21d2-9301-9019b88baa77 ora_dce222_dba_ad
                00000077-8b53-21d2-9301-9019b88baa77 ora_dce222_operator_ad

Identity Info Expires: 1998-12-04-10:28:22
Account Expires:       never
Passwd Expires:        never

Kerberos Ticket Information:
Ticket cache: /opt/dcelocal/var/security/creds/dcecred_43ae2600
Default principal: oracle@dce.dlsun685.us.oracle.com
Server: krbtgt/dce.dlsun685.us.oracle.com@dce.dlsun685.us.oracle.com
        valid 1998-12-04-00:28:22 to 1998-12-04-10:28:22
Server: dce-rgy@dce.dlsun685.us.oracle.com
```

```
        valid 1998-12-04-00:28:22 to 1998-12-04-10:28:22
Server: dce-ptgt@dce.dlsun685.us.oracle.com
        valid 1998-12-04-00:28:26 to 1998-12-04-02:28:26
Client: dce-ptgt@dce.dlsun685.us.oracle.com     Server:
krbtgt/dce.dlsun685.us.o
racle.com@dce.dlsun685.us.oracle.com
        valid 1998-12-04-00:28:26 to 1998-12-04-02:28:26
Client: dce-ptgt@dce.dlsun685.us.oracle.com     Server:
dce-rgy@dce.dlsun685.us.
oracle.com
        valid 1998-12-04-00:28:27 to 1998-12-04-02:28:26
```

注意： リスト出力は、Oracle の DCE グループのメンバーシップです。

5. Oracle データベースに SYSBDA または SYSOPER として接続します。たとえば、次のように指定します。

```
SQL> connect /@oradce as SYSDBA
```

クライアントの構成

DCE Integration を使用するクライアントを構成するには、以下の説明に従って、次の Net8 ファイルで DCE のアドレス情報とパラメータ情報を構成する必要があります。

- protocol.ora
- sqlnet.ora

通常は、CDS を使用して名前を解決します。したがって、名前とアドレスを CDS にロードする場合を除いて、ローカル名構成ファイル（tnsnames.ora）は使用しません。

詳細情報： 13-13 ページの「DCE CDS ネームを使用するクライアントの構成」を参照してください。

PROTOCOL.ORA ファイルのパラメータ

4 つの DCE パラメータが protocol.ora ファイルにあります。これらのパラメータは、他のプロトコルに関連するパラメータと区別するために「DCE」で始まります。これら 4 つのパラメータでデフォルト値を使用する場合は、protocol.ora ファイルを構成する必要がありません。これらのパラメータとその現行デフォルト値を次に示します。

- DCE.AUTHENTICATION=*dce_secret*
- DCE.PROTECTION=*pkt_integ*
- DCE.TNS_ADDRESS_OID=1.3.22.1.5.1

- DCE.LOCAL_CELL_USERNAMES=TRUE

> **注意：** DCE.LOCAL_CELL_USERNAMES のデフォルトは TRUE です（DCE Integration リリース 2.1.6 では、FALSE に設定されていました）。

構成パラメータでは大文字と小文字を区別しないので、大文字または小文字のどちらで入力してもかまいません。

> **注意：** DCE.AUTHENTICATION エントリを指定しないと、デフォルトのセル内認証レベルが使用されます。
>
> DCE.AUTHENTICATION エントリを指定しないと、デフォルトのセル内認証レベルが使用されます。

DCE.AUTHENTICATION －このパラメータはオプションです。このパラメータは、それぞれの DCE RPC で使用する認証値を指定します。クライアント側の DCE_AUTHENTICATION の値は、サーバー側の DEC_AUTHENTICATION の値と同じでなければなりません。次の値を選択できます。

- *NONE:* 認証なし
- *DCE_SECRET:* DCE 共用シークレット・キー認証（Kerberos）
- *DCE_SECRET:* デフォルトの認証レベル
- *DEFAULT:* セルのデフォルト

> **注意：** このパラメータでは、DCE_SECRET を指定するようお薦めします。

DCE.PROTECTION －これはオプション・フィールドです。このパラメータは、転送データの整合性に対する保護レベルを指定します。クライアント側で指定する DCE_PROTECTION のレベルは、サーバー側で指定する DCE_PROTECTION のレベル以上でなければなりません。次の値を選択できます。

- *NONE:* 現行の接続でデータの整合性を保護しません。
- *DEFAULT:* デフォルトのセル内保護レベルを使用します。
- *CONNECT:* クライアントがサーバーと関係を確立するときのみ、データの整合性を保護します。
- *CALL:* サーバーが要求を受け取る各リモート・プロシージャ・コールの最初のみ、データの整合性を保護します。

- *PKT:* すべてのデータを所定のクライアントから受け取られることを保証します。
- *PKT_INTEG:* クライアントとサーバーの間で転送されるデータが変更されていないことを保証します。
- *PRIVACY:* 上記のすべてのレベルで指定した保護を実行し、それぞれのリモート・プロシージャ・コールの引数値とすべてのユーザー・データを暗号化します。

DCE.TNS_ADDRESS_OID －これは、DCE.TNS_ADDRESS_OID のデフォルト（下に示す値）にかわる値を指定するオプション・パラメータです。

```
DCE.TNS_ADDRESS_OID=1.3.22.1.x.x
```

詳細情報： このパラメータを指定する必要があるかどうかの判断基準、およびこのパラメータの指定方法については、13-14 ページの「CDS 属性ファイルを変更して CDS を再起動する」を参照してください。

DCE.LOCAL_CELL_USERNAMES －このオプション・パラメータは、プリンシパル名（username）を、セル名とともにまたはセル名なしで指定するときに使用する書式を定義します。

注意： このパラメータで指定する値は、ユーザーが複数のセルにまたがって接続するかどうかによって異なります。複数のセルにまたがって接続する場合は、異なるセル内のユーザーを一意な名前にするかどうかによって、このパラメータの値が決まります。

次の値を選択できます。

TRUE: これがデフォルト値です。CELL_NAME を指定せずに SERVER_PRINCIPAL 書式のみを使用する場合は、TRUE を選択します。たとえば、この書式を使用して次のようにユーザーを指定します。

```
oracle
```

ユーザーが 1 つのセル内で接続を行う場合、または異なるセル内のユーザーを一意な名前にする命名規則をネットワークで採用している場合は、TRUE が適しています。

FALSE: CELLNAME/SERVER_PRINCIPAL 書式を使用するときは、FALSE を選択します。たとえば、この書式を使用して次のようにユーザーを指定します。

```
CELL1/ORACLE
```

ユーザーが複数のセルにまたがって接続を行い、異なるセル内のユーザー名が重複してもよい場合は、この値が適しています。

DCE CDS ネームを使用するクライアントの構成

通常、クライアントは CDS を使用して Oracle サービス名をアドレスに解決します。以下で説明する手順に従って CDS を構成します。

名前の検索で CDS を使用する

名前を解決するときに CDS を使用するには、CDS を使用するすべてのクライアントとサーバーに DCE Integration CDS ネーム・アダプタをインストールする必要があります。また、DCE Integration が使用する CDS 名前領域を構成しておく必要があります

> **詳細情報：** CDS ネーム・アダプタをインストールして構成する方法は、DCE Integration のインストレーションの説明と、12-3 ページの「手順 3: Oracle DCE Integration で使用する DCE CDS を構成」を参照してください。

たとえば、「ORADCE」のようなサービス名とそのネットワーク・アドレスを、DCE の CDS に格納できます。

通常、ユーザーは使い慣れた Oracle サービス名で Oracle サービスに接続できます（ドメインがない場合、またはデータベースがユーザーのデフォルト・ドメインにある場合）。たとえば、次のように入力します。

```
sqlplus /@ORADCE
```

この例では、DCE の外部認証アカウントを使用していることを想定しています。

CDS にアクセスできないときは、別の名前解決サービスとしてローカル名構成ファイル（tnsnames.ora）を使用することができます。このファイルを使用するには、すべての Oracle Server の名前とアドレスをローカル名構成ファイル（tnsnames.ora）で指定する必要があります。

CDS 属性ファイルを変更して CDS を再起動する

CDS ネームを使用するすべての DCE マシン上で、CDS 属性 TNS_Address のオブジェクト ID を CDS 属性ファイルに追加します（オブジェクト ID は、すべてのマシンで同じでなければなりません）。

1. /opt/dcelocal/etc/cds_attributes ファイルに、次に示す書式の行を追加します。

   ```
   1.3.22.1.5.1    TNS_Address    char
   ```

   TNS_Address のデフォルト OID（オブジェクト識別子）の値（1.3.22.1.5.1）がすでに cds_attributes ファイルに存在している場合は、使用中でない OID の値を指定する必要があります。

   > **注意：** DCE 命名規則では、TNS_Address 属性値（1.3.22.1.x.y）の最初の 4 桁が固定されています。

   OID のデフォルト値を使用できない場合は、クライアント上の protocol.ora ファイルで OID を指定する必要があります。

   デフォルト（1.3.22.1.5.1）以外の値を指定しなければならなかった場合は、次のパラメータを protocol.ora ファイルに追加する必要があります。

   ```
   DCE.TNS_ADDRESS_OID=1.3.22.1.x.y
   ```

   > **注意：** cds_attributes ファイルで指定する OID の値は、protocol.ora ファイルの DCE.TNS_ADDRESS_OID パラメータで指定した値と一致する必要があります。

2. マシン上で CDS を再起動します（CDS を再起動するためのコマンドは、プラットフォームによって異なります。たとえば、IBM AIX では、`smit` コマンドを使用して CDS を再起動します）。IBM AIX では、次の手順で CDS を再起動します。
   1. 「smit DCE」と入力します。
   2. 「Restart DCE/CDS Daemons」を選択します。
   3. 「List」を選択します。
   4. 使用可能な CDS デーモンをすべて選択します。

Oracle 接続記述子を CDS にロードするのに必要な TNSNAMES.ORA ファイルを作成

Oracle サービス名とアドレスを CDS にロードするために、サービス名（または別名）とアドレスが入っているローカル名構成ファイル（tnsnames.ora）を作成または修正します。サンプルのローカル名構成ファイル（tnsnames.ora）を次に示します。ローカル名構成ファイル（tnsnames.ora）を使用して、サービス名を Net8 で使用するアドレスにマップします。

この項では、tnsnames.ora ファイルに含める必要があるパラメータについて説明します。tnsnames.ora ファイルには、ネットワーク内の宛先または終点の接続記述子にマップされる Oracle サービス名のリストが入っています。下の例の DCE アドレスは、Oracle サービス名が「ORADCE」の Oracle Server のネットワーク・アドレスを示しています。この DCE アドレスを使用して、CDS ディレクトリ /.../*cell_name*/subsys/oracle/names に「DCE_SVC」として登録されているサービスに接続します。

```
ORADCE=(DESCRIPTION=
        (ADDRESS=
         (PROTOCOL=DCE)
       (SERVER_PRINCIPAL=oracle)
        (CELL_NAME=cell1)
        (SERVICE=DCE_SVC))
(CONNECT_DATA=
    (SID=ORASID)))
```

注意： この例では、Oracle サービス名と DCE サービス名が異なっていますが、同じサービス名を使用する場合もよくあります。

キーワード値ペア「PROTOCOL=DCE」は必須フィールドです。このキーワード値ペアは、リスナー構成ファイル（listener.ora）のアドレス・セクションと、ローカル名構成ファイル（tnsnames.ora）のアドレス・セクションにあります。両方の場所で、この値ペアが同じでなければなりません。

DCE パラメータ SERVER_PRINCIPAL は、ローカル名構成ファイル（tnsnames.ora）のオプション・パラメータです。

DCE パラメータ SERVICE は必須パラメータです。DCE パラメータの値（SERVICE=*dce_service_name*）は、リスナー構成ファイル（listener.ora）とローカル名構成ファイル（tnsnames.ora）で同じものにしてください。

Oracle パラメータ SID は必須パラメータです。このパラメータで Oracle システム ID を指定します。SID の値はノード上で一意でなければなりません。SID は完全なローカル・パラメータであり、DCE CDS では使用しません。

詳細情報： ローカル名構成ファイル（tnsnames.ora）の詳細は、『Oracle8*i* Net8 管理者ガイド』を参照してください。

Oracle 接続記述子の CDS へのロード

Oracle DCE Integration には、接続記述子を CDS にロードするためのユーティリティ「tnnfg」があります。

Oracle サービス名または別名を CDS にロードするには、次の手順を実行します。

```
% dce_login cell_admin
% tnnfg dceload full_pathname_to_TNSNAMES.ORA

% Enter Password:(password will not display)
```

注意： 上記のコマンドでは、tnsnames.ora ファイルの完全パス名を入力する必要があります。

また、sqlnet.ora ファイルが tnsnames.ora ファイルと同じディレクトリにあることも確認してください。

この手順によって、tnsnames.ora ファイル内のサービス名が DCE の CDS にロードされます。

注意： tnsnames.ora ファイルで新しいサービス名とアドレスを構成すると、tnnfg が新しいサービス名とアドレスを CDS に追加します。

特定のサービス名に対するアドレスを変更すると、tnnfg が特定のサービス名に対するアドレスを更新します。

TNSNAMES.ORA ファイルの削除または改名

SQL*Net 2.2 以前のリリースを使用している場合は、tnsnames.ora ファイルを DCE の CDS にロードした後で、そのファイル名を別の名前（tnsnames.bak など）に変更するか、ファイルを削除することをお薦めします。こうしないと、サービス名をアドレスに解決するときに、CDS ではなく tnsnames.ora ファイルが検索される場合があります。

SQL*Net 2.3 または Net8 を使用している場合は、CDS が使用不能になった場合のバックアップとして tnsnames.ora ファイルを残しておくことができます。tnsnames.ora ではなく CDS が正しく検索されるように、13-17 ページの「CDS で名前が解決されるように SQLNET.ORA ファイルのパラメータを変更」の説明に従って、プロファイル（sqlnet.ora）の NAMES.DIRECTORY_PATH パラメータを設定します。

CDS で名前が解決されるように SQLNET.ORA ファイルのパラメータを変更

プロファイル（sqlnet.ora）に含める必要があるパラメータは、SQL*Net または Net8 のバージョンによって異なります。

SQL*Net 2.3 以降のリリースと Net8

DCE CDS ネームを使用するクライアントまたはサーバーに対して、管理者は次の作業を行う必要があります。

- CDS ネーム・アダプタがそのノード上にインストールされていることを確認する。
- 次のパラメータを sqlnet.ora ファイルに追加する。

```
NAMES.DIRECTORY_PATH=(dce, tnsnames, onames)
```

このパラメータの値として最初にリストされている名前解決サービスが使用されます。このサービスがなんらかの理由で使用できない場合は、次の名前解決サービスが使用されます。

DCE の Oracle Server に接続

詳細情報： DCE 環境の Oracle データベースに接続する方法については、第 14 章の「DCE 環境の Oracle データベースに接続」を参照してください。

14

DCE 環境の Oracle データベースに接続

この章では、DCE 環境の Oracle データベースに接続する方法について説明します。Oracle データベースに接続するには、Oracle DCE Integration をインストールし、Oracle DCE Integration を使用できるように DCE と Oracle を構成しておく必要があります。

この章では、次のトピックについて説明します。

ネットワーク・リスナーの起動

次の手順に従って Net8 リスナーを起動します。

1. リスナーを起動するには、次のコマンドを入力します。

```
% dce_login principal_name password
%  lsnrctl start listener_name
```

たとえば、listener.ora ファイルで設定されている LSNR_DCE がリスナー名の場合は、次のように入力してリスナーを起動します。

```
% dce_login oracle orapwd
% lsnrctl start LSNR_DCE
```

サーバーのバインディング・ハンドラが rpcd に登録されていることを確認するために、次のように入力します。

```
% rpccp show mapping
```

表示される画面で、リスナー・アドレスの一部として dce_service_name が含まれている行を探します。

2. サービスが作成済みであるかどうか確認するために、次のように入力して dce_service_name を検索します。

```
% cdscp show object "/.:/subsys/oracle/service_registry/dce_service_name"
```

たとえば、次のとおりです。

```
% cdscp show object "/.:/subsys/oracle/service_registry/dce_svc"
```

リスナーが終点として選択した CDS 名前領域内のマッピングが表示されます。たとえば、次のとおりです。

```
              SHOW
            OBJECT    /.../subsys/oracle/service_registry/dce_svc
               AT   1995-05-15-17:10:52
RPC_ClassVersion = 0100
         CDS_CTS = 1995-05-16-00:05:01.221106100/aa-00-04-00-3e-8c
         CDS_UTS = 1995-05-16-00:05:01.443343100/aa-00-04-00-3e-8c
       CDS_Class = RPC_Server
CDS_ClassVersion = 1.0
      CDS_Towers = :
           Tower = ncacn_ip_tcp:144.25.23.57[]
```

DCE 環境の Oracle データベース・サーバーに接続

DCE 環境の Oracle Server に接続するには、次のいずれかの手順で行います。

1. 外部的に識別されるアカウントをセットアップすると、ユーザー名 / パスワード情報を入力しなくても、DCE 認証を利用して Oracle にログインすることができます。次のようなコマンドで DCE にログインするのみで、この Single sign-on 機能を使用することができます。

   ```
   % dce_login principal_name password
   ```

   たとえば、次のとおりです。

   ```
   % dce_login oracle orapwd
   ```

   注意： **dce_login** コマンドを入力する必要があるのは一度だけです。すでに DCE にログインしている場合は、再びログインする必要はありません。

   これで、ユーザー名またはパスワードを使用しないで Oracle Server に接続できます。次のようなコマンドを入力します。

   ```
   % sqlplus /@net_service_name
   ```

   net_service_name はデータベース・サービス名です。

   たとえば、次のとおりです。

   ```
   % sqlplus /@ORADCE
   ```

   詳細情報： 『Oracle8*i* 分散システム』を参照してください。

2. クライアントからユーザー名 / パスワードを使用して接続できます。

   ```
   % sqlplus username/password@net_service_name
   ```

   net_service_name は Net8 サービス名です。

   たとえば、次のとおりです。

   ```
   % sqlplus scott/tiger@ORADCE
   ```

15

DCE 環境と非 DCE 環境の相互運用性

この章では、非 DCE 環境のクライアントが DCE 環境の Oracle Server に接続する方法、および CDS にアクセスできるときにローカル名構成ファイル（tnsnames.ora）を使用して名前を検索する方法について説明します。

この章では、次のトピックについて説明します。

非 DCE 環境のクライアントから DCE 環境の Oracle Server に接続

クライアントは DCE と CDS にアクセスできなくても、TCP/IP またはその他のプロトコルを使用して、DCE の Oracle Server に接続できます（リスナーを適切に構成してある場合）。サーバー上の listener.ora ファイルでリスナーを構成してある場合は（次項のサンプル listener.ora ファイルを参照）、非 DCE 環境のクライアントが Oracle および Net8 の通常の手順を使用して、DCE の Oracle Server に接続できます。

注意： この場合、クライアントは DCE のセキュリティ機能を利用できません。また、サービス名が検索されてネットワーク・アドレスに解決されるときに、CDS ネーム・サーバーではなく、クライアント上の tnsnames.ora ファイルが使用されます。

詳細情報： サンプルファイルについては、15-2 ページの「LISTENER.ORA」と 15-4 ページの「TNSNAMES.ORA」を参照してください。

非 DCE 環境のクライアントが DCE 環境の Oracle データベース・サーバーに接続する場合に構成する必要がある listener.ora ファイルと tnsnames.ora ファイルのサンプルについて、次項以降で説明します。

サンプル・パラメータ・ファイル

クライアント / サーバー間で正しく通信を行うためには、少なくとも 2 つの Oracle パラメータ・ファイルが必要です。任意のテキスト・エディタを使用して、これらのファイルを作成および変更できます。次の 2 つのファイルです。

- LISTENER.ORA
- TNSNAMES.ORA

LISTENER.ORA

このファイルはリスナー・ノード上にあります。このファイルは、リスナー特性およびリスニング場所のアドレスを定義します。

次の例では、各要素を別々の行に置いてあるので、ファイルの構造を容易に理解できます。この書式を使用することをお薦めします。listener.ora ファイルを手作業で編集する場合は、各要素を別々の行に置く必要はありません。ただし、適切なカッコをすべて含めるようにし、次の行に要素が続く場合は字下げするよう注意してください。

この例では、一方のリスナーで UNIX オペレーティング・システムと TCP/IP プロトコルを想定し、別のリスナーで DCE プロトコルを想定しています。1 つのリスナーが複数のアドレスを持つこともできます。たとえば、サーバー・ノード上の異なるデータベース・インスタンスに対して 2 つのリスナーを定義するかわりに、両方のデータベース・インスタンスに対して 1 つのリスナーを定義して、TCP/IP と DCE でリスニングすることができます。ただし、別々のリスナーを定義した方がパフォーマンスは向上します。

```
LSNR_TCP=
      (ADDRESS_LIST=
          (ADDRESS=
                 (PROTOCOL=IPC)
                 (KEY=DB1)
          )
          (ADDRESS=
                 (PROTOCOL=tcp)
                 (HOST=rose)
                 (PORT=1521)
          ))

  SID_LIST_LSNR_TCP=
         (SID_DESC=
                (SID_NAME=ORASID)
                (ORACLE_HOME=/usr/jprod/oracle7)
         )
LSNR_DCE=
  (ADDRESS=
     (PROTOCOL=DCE)
     (SERVER_PRINCIPAL=oracle)
     (CELL_NAME=cell1)
     (SERVICE=dce_svc))
   SID_LIST_LSNR_DCE=
     (SID_DESC=
       (SID_NAME=ORASID)
       (ORACLE_HOME=/usr/prod/oracle8))
```

```
#For all listeners, the following parameters list sample
#default values.

PASSWORDS_LISTENER=
STARTUP_WAIT_TIME_LISTENER=0
CONNECT_TIMEOUT_LISTENER=10
TRACE_LEVEL_LISTENER=OFF
TRACE_DIRECTORY_LISTENER=/usr/prod/oracle7/neatwork/trace
TRACE File_LISTENER=listener.trc
LOG_DIRECTORY_LISTENER=/usr/prod/oracle7/network/log
LOG_FILE_LISTENER=listener.log
```

TNSNAMES.ORA

このファイルは、クライアント・ノード上とサーバー・ノード上の両方にあります。このファイルには、ネットワーク上のすべてのサービスのサービス名とアドレスのリストが入っています。

次に示す tnsnames.ora ファイルは、TCP/IP アドレスが入っている接続記述子に ORATCP サービス名をマップし、DCE アドレスが入っている接続記述子に ORADCE サービス名をマップします。

```
ORATCP = (DESCRIPTION=
          (ADDRESS=
            (PROTOCOL=TCP)
            (HOST=rose)
            (PORT=1521)
           )
           (CONNECT_DATA=
             (SID=DB1)
           )
          )
ORADCE=(DESCRIPTION=
         (ADDRESS=
           (PROTOCOL=DCE)
           (SERVER_PRINCIPAL=oracle)
           (CELL_NAME=cell1)
           (SERVICE=dce_svc)
          )
          (CONNECT_DATA=
                 (SID=ORASID)
          )
          )
```

DB1 データベースにアクセスする場合は、次のように ORATCP を使用して適切な接続記述子を識別します。たとえば、次のとおりです。

```
SQLPLUS SCOTT/TIGER@ORATCP
```

CDS にアクセスできないときに、TNSNAMES.ORA を使用して名前を検索

通常は、CDS によって名前がネットワーク・アドレスに解決されます。（固有のネーム・アダプタと関連して）tnsnames.ora を使用する主な目的は、Oracle サービス名とネットワーク・アドレスを CDS にロードすることですが、CDS にアクセスできない場合は、予備用の名前解決サービスとして tnsnames.ora を使用することができます。

SQL*Net 2.2 以前のリリース

tnsnames.ora を使用して名前を検索し解決するには、クライアント上の sqlnet.ora ファイルから「固有名」パラメータを削除（またはコメント・アウト）します。行をコメント・アウトするには、次のように各行の先頭に # を追加します。たとえば、次のとおりです。

```
#native_names.use_native=true
#native_names.directory_path=(dce)
```

SQL*Net リリース 2.3 と Net8

クライアント上の sqlnet.ora ファイルで NAMES.DIRECTORY_PATH パラメータの値として tnsnames を指定してある場合は、DCE CDS が使用不能なときに tnsnames.ora を使用して名前を検索し解決することができます。たとえば、次のとおりです。

```
names.directory_path=(dce, tnsnames)
```

このパラメータでは、複数の名前解決方法を指定できます。指定した順序で名前解決方法が使用されます。上の例では、最初に dce が使用され、dce が失敗すると tnsnames が使用されます。

A

暗号化パラメータとチェックサム・パラメータ

この付録では、Oracle Advanced Security でサポートされる暗号化とチェックサム・パラメータの一覧を示し、説明します。第 2 章の「暗号化とチェックサムの構成」の説明に従ってネットワークを構成した後で生成される sqlnet.ora ファイルの例を紹介します。

この付録では、次のトピックについて説明します。

- SQLNET.ORA ファイルのサンプル
- 暗号化パラメータとチェックサム・パラメータ

SQLNET.ORA ファイルのサンプル

この項では、特性が類似している一連のクライアントとサーバーに対して生成される sqlnet.ora 構成ファイルの例を紹介します。このサンプル sqlnet.ora ファイルには、Oracle Advanced Security の暗号化とチェックサム・パラメータの例があります。

```
# SQLNET.ORA Configuration File:/private/users/oracle7/sqlnet.ora
# Generated by Oracle Net8 Assistant

SQLNET_CRYPTO_CHECKSUM_TYPE_SERVER = MD5

OSS.SOURCE.MY_WALLET =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = /private/users/oracle7/ano814/8.1.4/network/admin/wallet)
    )
  )

SQLNET.AUTHENTICATION_SERVICES= (BEQ, SECURID)

SQLNET.CRYPTO_CHECKSUM_CLIENT = requested

SQLNET.ENCRYPTION_TYPES_SERVER= (RC4_40, DES40)

SQLNET.ENCRYPTION_TYPES_CLIENT= (RC4_40, DES40)

SSL_VERSION = Any

SQLNET_CRYPTO_CHECKSUM_TYPE_CLIENT = MD5

SQLNET.EXPIRE_TIME = 0

SQLNET.ENCRYPTION_SERVER = requested

SQLNET.ENCRYPTION_CLIENT = requested

SQLNET.CRYPTO_CHECKSUM_SERVER = requested

SQLNET.CRYPTO_SEED = qwertyuiopasdfghjkl;zxcvbnm
```

次の点に注意してください。

- サーバー暗号化またはクライアント暗号化、サーバー・チェックサム、クライアント・チェックサムの値を指定しないと、それぞれに対応する構成パラメータが sqlnet.ora ファイルに設定されません。ただし、Oracle Advanced Security はデフォルト値の ACCEPTED をとります。
- サーバー暗号化またはクライアント暗号化、サーバー・チェックサム、クライアント・チェックサムの各ページで、暗号化アルゴリズムまたはチェックサム・アルゴリズムを指定しないと、接続のサーバー側は、クライアント側のインストール済みアルゴリズム・リストとサーバー自身のインストール済みアルゴリズム・リストの両方に含まれるアルゴリズムの中で、サーバー側のリストで最初に現れるアルゴリズムが使用されます。
- 暗号化とチェックサムは互いに独立して機能します。チェックサムをオフにして暗号化をオンにしたり、暗号化をオフにしてチェックサムをオンにすることができます。

暗号化パラメータとチェックサム・パラメータ

暗号化とチェックサムを使用可能にするには、次に示す 9 個のパラメータを使用します。これらのパラメータについて次項以降で説明します。

- サーバーの暗号化レベル設定
- クライアントの暗号化レベル設定
- サーバーの暗号化アルゴリズム・リスト
- クライアントの暗号化アルゴリズム・リスト
- サーバーのチェックサム・レベル設定
- クライアントのチェックサム・レベル設定
- サーバーのチェックサム・アルゴリズム・リスト
- クライアントのチェックサム・アルゴリズム・リスト
- クライアント暗号化プロファイル

> **詳細情報：** 2-7 ページの「暗号化とチェックサムの折衝」を参照してください。

サーバーの暗号化レベル設定

用途 : このパラメータで、クライアント（またはクライアントとして動作するサーバー）がこのサーバーに接続するときの希望の動作を指定します。サーバーの動作は、接続先で設定されている SQLNET.ENCRYPTION_CLIENT によって多少変化します。

構文 : SQLNET.ENCRYPTION_SERVER = *valid_value*

指定できる値 : ACCEPTED、REJECTED、REQUESTED、REQUIRED

デフォルト値 : ACCEPTED

クライアントの暗号化レベル設定

用途 : このパラメータで、このクライアント（またはクライアントとして動作するこのサーバー）がサーバーと接続するときの希望の動作を指定します。クライアントの動作は、接続先で設定されている SQLNET.ENCRYPTION_SERVER によって多少変化します。

構文 : SQLNET.ENCRYPTION_CLIENT = *valid_value*

指定できる値 : ACCEPTED、REJECTED、REQUESTED、REQUIRED

デフォルト値 : ACCEPTED

サーバーの暗号化アルゴリズム・リスト

用途 : このパラメータで、このサーバーがサーバーとして動作するときに使用することができる暗号化アルゴリズムのリストを希望する使用順で指定します。使用優先順位の最も高いアルゴリズムを最初に指定します。このリストを使用して、接続先と相互に受入れ可能なアルゴリズムを折衝します。一致するアルゴリズムが見つかるまで、サーバー側の各アルゴリズムがクライアント側のアルゴリズム・リストと照合されます。インストールされていないアルゴリズムをこのサーバー側で指定すると、エラー・メッセージ ORA-12650 で接続が終了します。

構文 : SQLNET.ENCRYPTION_TYPES_SERVER = (*valid_encryption_algorithm [,valid_encryption_algorithm]*)

指定できる値 : RC4_40 －米国内向けと輸出用の RSA RC4（40 ビット・キー・サイズ）

RC4_56 －米国内向けのみの RSA RC4（56 ビット・キー・サイズ）

RC4_128 －米国内向けのみの RSA RC4（128 ビット・キー・サイズ）

DES －米国内向けのみの標準 DES（56 ビット・キー・サイズ）

DES40 －米国内向けと輸出用の DES40（40 ビット・キー・サイズ）

デフォルト値 : sqlnet.ora ファイルでアルゴリズムが定義されていない場合は、すべてのインストール済みアルゴリズムが折衝で使用されます。

使用するときの注意 : **米国内向けバージョン**－米国内向けバージョンを使用している場合は、5 つのアルゴリズム（RC4_40、RC4_56、RC4_128、DES、DES40）がすべてインストールされています。アルゴリズムを指定しないと、インストール済みのアルゴリズムが上記の順序で使用されて、接続先と相互に受け入れ可能なアルゴリズムを折衝します。

輸出用バージョン－輸出用バージョンを使用している場合は、2 つのアルゴリズム（RC4_40 と DES40）がインストールされています。アルゴリズムを指定しないと、インストール済みのアルゴリズムが上記の順序で使用されて、相互に受け入れ可能なアルゴリズムを折衝します。

複数の暗号化アルゴリズム、つまり、アルゴリズム名の 1 つの値またはリストを指定できます。たとえば、次に示す暗号化パラメータはどちらも有効です。

SQLNET.ENCRYPTION_TYPES_SERVER=(*RC4_40*)

SQLNET.ENCRYPTION_TYPES_SERVER=(*DES,RC4_56,RC4_128,DES40*)

クライアントの暗号化アルゴリズム・リスト

用途 : このパラメータで、このクライアント（または、クライアントとして動作するこのサーバー）がサーバーと接続するときに使用することができる暗号化アルゴリズムのリストを指定します。このリストを使用して、接続先と相互に受入れ可能なアルゴリズムを折衝します。パラメータを任意の順序で指定できます。インストールされていないアルゴリズムをこのサーバー側で指定すると、エラー・メッセージ ORA-12650 で接続が終了します。

構文 : `SQLNET.ENCRYPTION_TYPES_CLIENT = (`*valid_encryption_algorithm [,valid_encryption_algorithm]*`)`

指定できる値 : RC4_40 －米国内向けと輸出用の RSA RC4（40 ビット・キー・サイズ）

RC4_56 －米国内向けのみの RSA RC4（56 ビット・キー・サイズ）

RC4_128 －米国内向けのみの RSA RC4（128 ビット・キー・サイズ）

DES －米国内向けのみの標準 DES（56 ビット・キー・サイズ）

DES40 －米国内向けと輸出用の DES40（40 ビット・キー・サイズ）

デフォルト値 : sqlnet.ora ファイルでアルゴリズムが定義されていない場合は、すべてのインストール済みアルゴリズムが折衝で使用されます。

使用するときの注意 : **米国内向けバージョン**－米国内向けバージョンを使用している場合は、5 つのアルゴリズム（RC4_40、RC4_56、RC4_128、DES、DES40）がすべてインストールされています。sqlnet.ora ファイルでアルゴリズムが定義されていない場合は、インストール済みのアルゴリズムが上記の順序で使用されて、接続先と相互に受入れ可能なアルゴリズムを折衝します。

輸出用バージョン－輸出用バージョンを使用している場合は、RC4_40 と DES40 の 2 つのアルゴリズムがインストールされています。sqlnet.ora ファイルでアルゴリズムが定義されていない場合は、インストール済みのアルゴリズムが上記の順序で使用されて、相互に受入れ可能なアルゴリズムを折衝します。

複数の暗号化アルゴリズム、つまり、アルゴリズム名の 1 つの値またはリストを指定できます。たとえば、次に示す暗号化パラメータはどちらも有効です。

SQLNET.ENCRYPTION_TYPES_CLIENT=(*DES,DES40,RC4_56,RC4_40*)

SQLNET.ENCRYPTION_TYPES_CLIENT=(*RC4_40*)

サーバーのチェックサム・レベル設定

用途 : このパラメータで、クライアント（またはクライアントとして動作する別のサーバー）がこのサーバーと接続するときの希望のチェックサム動作を指定します。このパラメータで指定するチェックサム動作は、接続先で設定されている SQLNET.CRYPTO_CHECKSUM_CLIENT によって多少変化します。

構文 : SQLNET.CRYPTO_CHECKSUM_SERVER = valid_value

指定できる値 : ACCEPTED、REJECTED、REQUESTED、REQUIRED

デフォルト値 : ACCEPTED

クライアントのチェックサム・レベル設定

用途 : このパラメータで、このクライアント（または、クライアントとして動作するこのサーバー）がサーバーと接続するときの希望のチェックサム動作を指定します。このパラメータで指定するチェックサム動作は、接続先で設定されている SQLNET.CRYPTO_CHECKSUM_SERVER によって多少変化します。

構文 : SQLNET.CRYPTO_CHECKSUM_CLIENT = *valid_value*

指定できる値 : ACCEPTED、REJECTED、REQUESTED、REQUIRED

デフォルト値 : ACCEPTED

サーバーのチェックサム・アルゴリズム・リスト

用途 : このパラメータで、このサーバーがクライアントまたは別のサーバーに対するサーバーとして動作するときに使用することができるチェックサム・アルゴリズムのリストを指定します。使用優先順位の最も高いアルゴリズムを最初に指定します。このリストを使用して、リモート端末と相互に受入れ可能なアルゴリズムを折衝します。一致するアルゴリズムが見つかるまで、サーバー側の各アルゴリズムがクライアント側のアルゴリズム・リストと照合されます。最初に見つかった一致アルゴリズムが使用されます。このサーバー側にインストールされていないアルゴリズムを指定すると、エラー・メッセージ ORA-12650 で接続が終了します。

構文 : SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER = (*crypto_checksum_algorithm*)

指定できる値 : 現行のリリースでは、RSA Data Security の MD5 アルゴリズムのみが暗号チェックサム・アルゴリズムとしてサポートされています。

デフォルト値 : MD5（現時点で指定できる唯一の値）

クライアントのチェックサム・アルゴリズム・リスト

用途 : このパラメータで、このクライアント（またはクライアントとして動作するこのサーバー）がサーバーと接続するときに使用することができるチェックサム・アルゴリズムのリストを指定します。このリストを使用して、リモート端末と相互に受入れ可能なアルゴリズムを折衝します。リスト内のアルゴリズムの順序は、特に意味がありません。こちら側にインストールされていないアルゴリズムを指定すると、エラー・メッセージ ORA-12650 で接続が終了します。

構文 : SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT = (*crypto_checksum_algorithm*)

指定できる値 : 現行のリリースでは、RSA Data Security の MD5 アルゴリズムのみが暗号チェックサム・アルゴリズムとしてサポートされています。

デフォルト値 : MD5（現時点で指定できる唯一の値）

クライアント暗号化プロファイル

SQLNET.CRYPTO_SEED = "*10-70 random characters*"

このパラメータの値として入力する文字を使用して、暗号キーが生成されます。このフィールドにランダムな文字を入力するほど、強力なキーが生成されます。このパラメータを設定するには、前述の文にランダムな文字を 10 〜 70 文字入力します。

注意 : 生成されるキーがランダムで強力になるように、できるだけ多くの文字（最大 70 文字まで）を入力することをお薦めします。

暗号化またはチェックサムをオンにするときは、このパラメータが必ずその sqlnet.ora ファイルに存在している必要があります。

B

認証パラメータ

この付録では、CyberSafe、Kerberos、SecurID、RADIUS、または SSL の各認証を使用するときに、必要なプロファイル（sqlnet.ora）とデータベース初期化ファイル（init.ora）を含む構成ファイルのサンプルを紹介します。この付録は、次の項で構成されています。

- CyberSafe 認証を使用したクライアントとサーバーのパラメータ
- Kerberos 認証を使用するクライアントとサーバーのパラメータ
- SecurID 認証を使用するクライアントとサーバーのパラメータ
- RADIUS 認証を使用するクライアントとサーバーのパラメータ
- SSL を使用するクライアントとサーバーのパラメータ

CyberSafe 認証を使用したクライアントとサーバーのパラメータ

CyberSafe を使用するクライアントとサーバーの構成ファイルには、次のパラメータを挿入します。

SQLNET.ORA パラメータ

```
SQLNET.AUTHENTICATION_SERVICES=(cybersafe)
SQLNET.AUTHENTICATION_GSSAPI_SERVICE=oracle/dbserver.someco.com@SOMECO.COM
```

INIT.ORA パラメータ

```
REMOTE_OS_AUTHENT=FALSE
OS_AUTHENT_PREFIX=""
```

Kerberos 認証を使用するクライアントとサーバーのパラメータ

Kerberos を使用するクライアントとサーバーの構成ファイルには、次のパラメータを挿入します。

SQLNET.ORA パラメータ

```
SQLNET.AUTHENTICATION_SERVICES=(KERBEROS5)
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.KERBEROS5_CC_NAME=/usr/tmp/DCE-CC
SQLNET.KERBEROS5_CLOCKSKEW=1200
SQLNET.KERBEROS5_CONF=/krb5/krb.conf
SQLNET.KERBEROS5_REALMS=/krb5/krb.realms
SQLNET.KERBEROS5_KEYTAB=/krb5/v5srvtab
```

INIT.ORA パラメータ

```
REMOTE_OS_AUTHENT=FALSE
OS_AUTHENT_PREFIX=""
```

SecurID 認証を使用するクライアントとサーバーのパラメータ

SecurID を使用するクライアントとサーバーの構成ファイルには、次のパラメータを挿入します。

SQLNET.ORA パラメータ

```
SQLNET.AUTHENTICATION_SERVICES=(securid)
```

INIT.ORA パラメータ

```
REMOTE_OS_AUTHENT=FALSE
OS_AUTHENT_PREFIX=""
```

RADIUS 認証を使用するクライアントとサーバーのパラメータ

RADIUS を使用するクライアントとサーバーの構成ファイルに挿入するパラメータを次の表に示します。

SQLNET.ORA パラメータ

SQLNET.RADIUS_AUTHENTICATION

説明　プライマリ RADIUS サーバーの場所を設定するには、ホスト名またはドット付き 10 進数を使用した書式で指定します。RADIUS サーバーが Oracle Server 以外のマシンにあるときは、そのマシンのホスト名または IP アドレスを指定する必要があります。

デフォルト　`localhost`

SQLNET.RADIUS_AUTHENTICATION_PORT

説明　プライマリ RADIUS サーバーのリスニング・ポートを設定します。

デフォルト　`1645`

SQLNET.RADIUS_AUTHENTICATION_TIMEOUT

説明　応答待ち時間を設定します。

デフォルト　5

SQLNET.RADIUS_AUTHENTICATION_RETRIES

説明　再送回数を設定します。

デフォルト　3

SQLNET.RADIUS_SEND_ACCOUNTING

説明　アカウントの ON/OFF を設定します。アカウントを使用可能にすると、パケットはリスニング・ポート +1 のアクティブ RADIUS サーバーに送られます。デフォルト・ポートは 1646 です。この機能をオンにする必要があるのは、RADIUS サーバーでアカウントをサポートしている場合で、システムにログインしたユーザーのログイン回数を記録する場合のみです。

デフォルト　`OFF`

SQLNET.RADIUS_ALTERNATE

説明　プライマリ RADIUS サーバーが使用できない場合に使用する代替 RADIUS サーバーの場所を設定します。この機能のデフォルトは OFF です。フォールト・トレラントのためにセカンダリ RADIUS サーバーをセットアップする場合は、セカンダリ RADIUS サーバーのあるホストのホスト名または IP アドレスを指定する必要があります。

デフォルト　NONE

SQLNET.RADIUS_ALTERNATE_PORT

説明　代替 RADIUS サーバーのリスニング・ポートを設定します。

デフォルト　1645

SQLNET.RADIUS_ALTERNATE_TIMEOUT

説明　応答待ち時間を設定します。

デフォルト　5

SQLNET.RADIUS_ALTERNATE_RETRIES

説明　メッセージ再送回数を設定します。

デフォルト　3

SQLNET.RADIUS_CHALLENGE_RESPONSE

説明　要求 - 応答の ON/OFF を切り替えます。

デフォルト　OFF

SQLNET.RADIUS_CHALLENGE_KEYWORD

説明　RADIUS サーバーからの要求を求めるキーワードを設定します。クライアント側のユーザーはパスワードを入力しません。

デフォルト　challenge

SQLNET.RADIUS_AUTHENTICATION_INTERFACE

説明　RADIUS が要求 - 応答（非同期）モードのときに、グラフィカル・ユーザー・インタフェースを持つ Java クラスの名前を設定します。

デフォルト　DefaultRadiusInterface

SQLNET.RADIUS_CLASSPATH

説明	要求 - 応答認証モードを使用する場合、RADIUS では Java ベースのグラフィカル・インタフェースを表示してパスワードを最初に要求し、ユーザーがトークン・カードから取得する動的パスワードなど、他の追加情報を要求します。そのグラフィカル・インタフェースの Java クラスのパスを設定するには、sqlnet.ora ファイルに SQLNET.RADIUS_CLASSPATH パラメータを追加します。
デフォルト	デフォルトはありません。このパラメータを sqlnet.ora ファイルに追加する必要があります。

INIT.ORA パラメータ

```
REMOTE_OS_AUTHENT=FALSE
OS_AUTHENT_PREFIX=""
```

SSL を使用するクライアントとサーバーのパラメータ

パラメータを構成するには、次の 2 通りあります。

- 静的− sqlnet.ora のパラメータの名前
- 動的− Net8 アドレスのセキュリティ・サブセクションで使用するパラメータの名前

認証

パラメータ名（静的）:	SQLNET.AUTHENTICATION_SERVICES
パラメータ名（動的）:	AUTHENTICATION
パラメータ・タイプ:	文字列 LIST
パラメータ・クラス:	静的
指定できる値:	使用可能な認証サービスのリストに **TCPS** を追加します。
デフォルト値:	デフォルト値はありません。
説明:	ユーザーが使用する認証サービスを制御します。 **注意:** 動的バージョンでは 1 種類の設定のみサポートされます。
既存または新規のパラメータ	既存
構文（静的）:	SQLNET.AUTHENTICATION_SERVICES = (TCPS, selected_method_1, selected_method_2)
例（静的）:	SQLNET.AUTHENTICATION_SERVICES = (TCPS, cybersafe, securid
構文（動的）:	AUTHENTICATION = *string*
例（動的）:	AUTHENTICATION = (TCPS)

Cipher Suite

パラメータ名（静的）:	SSL_CIPHER_SUITES
パラメータ名（動的）:	SSL_CIPHER_SUITES
パラメータ・タイプ:	文字列 LIST
パラメータ・クラス:	静的
指定できる値:	既知の SSL Cipher Suite
デフォルト値:	デフォルトはありません。
説明:	SSL で使用する暗号化とデータ整合性の組み合わせを制御します。
既存または新規のパラメータ	新規
構文（静的）:	SSL_CIPHER_SUITES=(*SSL cipher suite1* [, *SSL cipher suite2*, ... *SSL cipher suiteN*])
例（静的）:	SSL_CIPHER_SUITES=(SSL_DH_DSS_WITH_DES_CBC_SHA)
構文（動的）:	SSL_CIPHER_SUITES=(*SSL cipher suite1* [, *SSL cipher suite2*, ... *SSL cipher suiteN*])
例（動的）:	SSL_CIPHER_SUITES=(SSL_DH_DSS_WITH_DES_CBC_SHA)

サポートされている SSL Cipher Suite

- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

SSL バージョン

パラメータ名（静的）:	SSL_VERSION
パラメータ名（動的）:	SSL_VERSION
パラメータ・タイプ:	文字列
パラメータ・クラス:	静的
指定できる値:	SSL で有効な任意のバージョン（0, 3.0）
デフォルト値:	"0"
説明:	SSL 接続のバージョンを強制実行します。
既存または新規のパラメータ	新規
構文（静的）:	SSL_VERSION=*version*
例（静的）:	SSL_VERSION=3.0
構文（静的）:	SSL_VERSION=*version*
例（動的）:	SSL_VERSION=3.0

SSL クライアント認証

パラメータ名（静的）:	SSL_CLIENT_AUTHENTICATION
パラメータ名（動的）:	SSL_CLIENT_AUTHENTICATION
パラメータ・タイプ:	ブール値
パラメータ・クラス:	静的
指定できる値:	TRUE/FALSE
デフォルト値:	TRUE
説明:	サーバーに加えて、クライアントを SSL で認証するかどうかを制御します。
既存または新規のパラメータ	新規
構文（静的）:	SSL_CLIENT_AUTHENTICATION={*TRUE* | *FALSE*}
例（静的）:	SSL_CLIENT_AUTHENTICATION=FALSE
構文（動的）:	SSL_CLIENT_AUTHENTICATION={*TRUE* | *FALSE*}
例（動的）:	SSL_CLIENT_AUTHENTICATION=FALSE

Wallet の場所

プロセス空間にセキュリティ資格証明をロードするため、Wallet にアクセスする必要のあるアプリケーションでは、読み込む Wallet の場所をパラメータ・ファイルに指定する必要があります。静的構成のパラメータの構文は次のとおりです。

```
oss.source.my_wallet =
(SOURCE=
  (METHOD=File)
  (METHOD_DATA=
    (DIRECTORY=your wallet location)
      )
    )
```

パラメータを動的に指定するには、次のようにします。

```
MY_WALLET_DIRECTORY = your wallet dir
```

デフォルトの Wallet の場所は $HOME/oracle ディレクトリです。

C

RADIUS による認証デバイスの統合

この付録では、認証デバイスのサードパーティ・ベンダーが、その認証デバイスに合わせて RADIUS 要求 - 応答ユーザー・インタフェースをカスタマイズする方法について説明します。

詳細情報： 第 3 章の「RADIUS 認証の構成」を参照してください。

この付録では、次のトピックについて説明します。

- RADIUS 要求 - 応答ユーザー・インタフェースについて
- 要求 - 応答ユーザー・インタフェースのカスタマイズ

RADIUS 要求 - 応答ユーザー・インタフェースについて

RADIUS 標準をサポートする認証デバイスをセットアップして、Oracle ユーザーを認証できます。認証デバイスで要求 - 応答認証モードを使用する場合、グラフィカル・インタフェースを表示してパスワードを最初に要求し、ユーザーがトークン・カードから取得する動的パスワードなど、他の追加情報を要求します。Java ベースによるプラットフォームから独立したインタフェースが使用されます。

認証デバイスのサードパーティ・ベンダーは、そのデバイスに適したグラフィカル・ユーザー・インタフェースにカスタマイズする必要があります。たとえば、スマートカードのベンダーは、スマートカード・リーダーに要求を発行するように、Oracle クライアントをカスタマイズします。次に、スマートカードが要求を受け取ると、PIN などの追加情報をユーザーに入力させて応答します。

Oracle では、このインタフェース用に Java インタフェース・クラスを開発しました。JavaSoft の Java Development Kit リリース 1.1 で指定されている Java Native Interface を使用して C コードで記述されたメソッドのセットです。このコードは以下に示していますが、システム固有です。ディレクトリ $ORACLE_HOME/network/security/classes の OracleRadiusInterface ファイルにあります。

要求 - 応答ユーザー・インタフェースのカスタマイズ

このインタフェースをカスタマイズするには、独自のクラスを作成して、Oracle クライアントと RADIUS サーバーの間の要求 - 応答変換を処理する必要があります。次に sqlnet.ora ファイルを開いて、SQLNET.RADIUS_AUTHENTICATION_INTERFACE パラメータを検索し、クラス名 DefaultRadiusInterface を、作成したクラス名に置き換えます。この変更を sqlnet.ora ファイルで行うと、認証プロセスを処理するために、このクラスが Oracle クライアントにロードされます。

サードパーティは、ORACLE.NET.RADIUS パッケージにある Oracle RADIUS Interface を実装する必要があります。

```
public interface OracleRadiusInterface {
  public void radiusRequest();
  public void radiusChallenge(String challenge);
  public String getUserName();
  public String getPassword();
  public String getResponse();
  }
```

パラメータ	説明
radiusRequest	通常、ユーザーに対してユーザー名とパスワードを入力するようプロンプトを表示し、これらの値を getUserName と getPassword で取得する。
getUserName	ユーザーが入力したユーザー名を取得する。このメソッドが空の文字列を返したときは、ユーザーが操作をキャンセルしようとしていることを意味します。ユーザーは、認証に失敗したというメッセージを受け取ります。
getPassword	ユーザーが入力したパスワードを取得する。getUserName が有効な文字列を返した場合に、getPassword が空の文字列を返したときは、「要求キーワード」がサーバーからのパスワードとして受け継がれます。ユーザーがパスワードを入力した場合、要求はサーバーから返される場合と返されない場合があります。
radiusChallenge	ユーザーに付加情報を入力させるための RADIUS サーバーから送られた要求を表示する。
getResponse	ユーザーが入力した応答を取得する。このメソッドが有効な応答を返した場合は、新規の Access-Request パケットの User-Password 属性にその情報が入力されます。空の文字列が返された場合は、対応する値を返して、両サイドでの処理が停止されます。

用語集

Cipher Suite

SSL で、ネットワークのノード間でメッセージ交換するのに使用する認証、暗号化、データ整合性アルゴリズムのセット。SSL ハンドシェイク時に、2 つのノード間で折衝し、メッセージを送受信するときに使用する Cipher Suite を確認する。

CORBA

Common Object Request Broker Architecture（CORBA）。オブジェクトと呼ばれるプログラムが、それが記述されているプログラミング言語や動作するオペレーティング・システムに関係なく、お互いにやりとりできるようになるアーキテクチャ。CORBA は OMG（Object Management Group）として知られる業界のコンソーシアムで開発されたアーキテクチャである。

DES

米国データ暗号化標準。

HTTP

ワールド・ワイド・ウェブでファイル（テキスト、グラフィック・イメージ、サウンド、ビデオ、他のマルチメディア・ファイル）を交換する際の規則セット。TCP/IP プロトコルがインターネットでの情報交換の基礎的なプロトコルであるのに対して、HTTP はアプリケーション・プロトコルである。

HTTPS

標準の HTTP アプリケーション・レイヤーのサブレイヤーとして SSL（Secure Sockets Layer）を使用したプロトコル。

IIOP

Internet Inter-ORB Protocol（IIOP）。OMG（Object Management Group）で開発されたプロトコルで、ワールド・ワイド・ウェブで CORBA ソリューションをインプリメントするプロ

トコル。IIOP では、テキストの転送のみがサポートされる HTTP とは異なり、ブラウザとサーバーで整数、配列、その他の複雑なオブジェクトを交換できる。

KDC/TGS

キー配布センター / チケット付与サービスの略。KDC は、Kerberos 認証でユーザー・プリンシパルのリストを管理する。ユーザーは kinit プログラムを実行して KDC とコンタクトをとり、**初期チケット（initial ticket）**を取得する。チケット付与サービスはサービス・プリンシパルのリストを管理する。チケット付与サービスなどを提供するサーバーにユーザーが自己認証しようとするときに、チケット付与サービスとコンタクトをとる。

KDC/TGS は、安全性の高いホスト上で稼働する必要がある信頼度の高いサードパーティで、チケット付与チケットとサービス・チケットを作成する。通常、KDC と TGS は同じエンティティである。

Kerberos

分散環境のセキュリティ強化を図るためにマサチューセッツ工科大学での Athena プロジェクトで開発されたネットワーク認証サービス。Kerberos は共有シークレットに依存し、サードパーティの安全性を前提とした信頼度の高いサードパーティ認証システムである。Kerberos には、Single sing-on 機能とデータベース・リンク認証機能（MIT Kerberos のみ）があり、パスワードを集中的に記憶できるため、PC のセキュリティを向上できる。

kinstance

サービスのインスタンシエーションまたは位置。kinstance として任意の文字列を指定できるが、通常はサービスのホスト・マシン名を指定する。

kservice

Kerberos サービス・オブジェクトを表す任意の名前。

MD5

ファイルの内容から一意の 128 ビット暗号化メッセージ・ダイジェスト値を生成して、データの整合性を保証するアルゴリズム。ファイル内の 1 ビットが変更されただけでも、ファイルの MD5 チェックサムが変更される。オリジナル・ファイルと同じ結果を MD5 が生成するようにファイルを偽造することはほぼ不可能である。

Net8

Oracle Server または Designer/2000 などの Oracle Tools を稼働する複数のコンピュータが、サードパーティ・ネットワークを通じてデータを交換できるようにする Oracle 製品。Net8 は分散処理と分散データベース機能をサポートしている。Net8 は通信プロトコルに依存しない「オープン・システム」である。ユーザーは Net8 を多くのネットワーク環境のインタフェースとして使用できる。

Secure Hash Algorithm（SHA）

264 ビット長未満のメッセージを扱い、160 ビット・メッセージ・ダイジェストを作成するアルゴリズム。SHA は MD5 に比べて少し遅くなるが、長いメッセージ・ダイジェストを作成できるので、強引な衝突や反転攻撃をさらに効果的に防御できる。

SHA

「**Secure Hash Algorithm（SHA）**」を参照。

Trustpoint

「**信頼できる証明書（trusted certificate）**」を参照。

Wallet

個々のエンティティのセキュリティ資格証明を保存、管理するのに使用する抽象化。各種暗号化サービスで使用する資格証明の保存と取得を行う。Wallet Resource Locator（WRL）によって Wallet の場所を特定するのに必要なすべての情報が提供される。

Wallet Resource Locator

特定の Wallet の場所を特定するのに必要なすべての情報を提供するディレクトリ・パス。

WRL

「**Wallet Resource Locator**」を参照。

X.509

公開鍵は各種データ形式で署名できる。ISO の X.509 形式は、その一般的な形式の 1 つ。

暗号化（encryption）

メッセージの内容を隠すためのメッセージ隠蔽プロセス。

暗号化（cryptography）

シークレット・コードの書き込みと復号化処理。これによりメッセージが保護される。

機密保護（confidentiality）

暗号化の機能。機密保護によって、メッセージの本来の受信人のみがメッセージをみる（暗号文を復号化する）ことができる。

クライアント（client）

サービスを利用する側。クライアントはユーザーであったり、データベース・リンク中にユーザーとして機能するプロセス（代理ともいう）であったりする。

公開鍵暗号（public-key encryption）

送信側でメッセージを受信側の公開鍵で暗号化するプロセス。受信側に配信されると、受信側の秘密鍵でメッセージが復号化される。

公開鍵 / 秘密鍵ペア（public/private key pair）

数学的に関連付けられた 2 つの数値のセットで、一方を公開鍵といい、一方を秘密鍵という。公開鍵は、通常、広い範囲で使用することができるが、秘密鍵は所有者のみが使用できる。公開鍵で暗号化されたデータは、それに対応する秘密鍵で復号化でき、秘密鍵で暗号化されたデータは、それに対応する公開鍵で復号化できる。ただし、公開鍵で暗号化されたデータは同じ公開鍵で復号化することはできない。

サーバー（server）

サービスの提供側。

サービス（service）

クライアントが使用するネットワーク資源（Oracle データベース・サーバーなど）。

サービス・チケット（service ticket）

クライアントを認証する際に使用する信頼度の高い情報。初期チケットとも呼ばれるチケット付与チケットを取得するには、kinit プログラムを直接または間接的に実行し、パスワードを入力する。チケット付与チケットは、クライアントがサービス・チケットを要求するときに使用される。「サービス・チケット」は、クライアントがサービスへの認証を受けるときに使用される。

サービス表

Kerberos 認証では、サービス表は、*kinstance* 上に存在するサービス・プリンシパルのリスト。Oracle で Kerberos を使用する前に、サービス表を Kerberos から抽出して Oracle Server マシンにコピーする必要がある。

サービス・プリンシパル（service principal）

「**プリンシパル（principal）**」を参照。

サービス名（service name）

Kerberos ベースの認証で使用するサービス・プリンシパルの **kservice** 部分。

識別情報（identity）

エンティティの公開鍵と他の公開情報の組合せ。公開情報には、電子メールのアドレスなど、ユーザー認証データが含まれる。

証明書（certificate）

証明書は、エンティティの公開鍵が信頼できる識別情報である認証局（CA）によって署名されたときに作成される。証明書によって、エンティティの情報が正しいことが保証され、公開鍵がそのエンティティに実際に属することが保証される。

証明書にはエンティティの名前、認証情報、および公開鍵が含まれる。また、証明書に関連する権利、ユーザーおよび権限についてのシリアル番号、有効期限、その他の情報が含まれる場合もある。さらに、発行元の認証局についての情報も含まれる。

証明書連鎖（certificate chain）

エンドユーザーまたはサブスクライバの証明書と、その認証局の証明書を含む指定順の証明書リスト。

初期チケット（initial ticket）

Kerberos 認証では、初期チケットまたはチケット付与チケット（TGT）によって、その他のサービス・チケットの要求権利を持つユーザーであることが証明される。初期チケットがなければ、他のチケットは取得できない。初期チケットは、kinit プログラムを実行し、パスワードを入力することで取得できる。

信頼できる証明書（trusted certificate）

信頼レベルの認可を受けたサード・パーティ識別情報。信頼できる証明書は、エンティティが本人であるという識別情報の確認が行われるときに使用される。通常、信頼できる認証局を信頼できる認証という。

スマートカード（smartcard）

ユーザー名やパスワードなどの情報を格納するための IC が組み込まれた（クレジット・カードに似た）プラスティック製のカード。スマートカードはクライアントまたはサーバーにあるハードウェア・デバイスで読み取る。

スマートカードは、ワンタイム・パスワードとして使用することができるランダム数字を生成できる。この場合、スマート・カードは、サーバー上のサービスと同期化されているので、サーバーはスマート・カードによって生成されるパスワードと同じパスワードを要求する。

整合性（integrity）

受信したメッセージの内容が、送信前のメッセージ内容と変更されていないことの保証。

セッション・キー（session key）

2 つ以上のパーティ（通常は、クライアントとサーバー）によって共有されるキー。

チェックサム（checksumming）

メッセージ・パケットに含まれているデータに基づいてメッセージ・パケットの値を計算し、その値をデータとともに渡して、データが改ざんされていないことを証明するメカニズム。データ受信側は暗号チェックサムを再計算して、それをデータとともに送られた暗号チェックサムと比較する。これらの暗号チェックサムが一致している場合は、データが転送中に改ざんされなかったことを「高い確率で」証明できる。暗号チェックサムの重要な特性は、悪意のある傍受者が秘密鍵を知らない限り、有効なチェックサムを持つメッセージを再構築できる可能性がほとんどないことである。

チケット（ticket）

所有者を識別するのに役立つ情報。「**サービス・チケット（service ticket）**」を参照。

デジタル署名（digital signature）

デジタル署名は、送信者の秘密鍵によって送信者のメッセージを署名するのに公開鍵アルゴリズムが使用されているときに作成される。デジタル署名によって、文書が信頼できるものであること、別のエンティティで偽造されていないこと、変更されていないこと、送信者によって拒否されないことが保証される。

トークン・カード（token card）

ユーザーが容易に認証サービスを利用できるように、数種類のメカニズムを提供するデバイス。一部のトークン・カードは、認証サービスと同期化されているワンタイム・パスワードを提供する。サーバーは認証サービスと連絡を取り合うことによって、トークン・カードが提供するパスワードをいつでも検証できる。要求 - 応答に基づいて機能するトークン・カードもある。この場合は、サーバーが要求（番号）を提供し、ユーザーがその番号をトークン・カードに入力する。そして、トークン・カードは別の番号（最初の番号から暗号的に導出される番号）を提供し、それをユーザーがサーバーに渡す。

認可（authorization）

ユーザーまたはプログラム、プロセスに、オブジェクトへのアクセスを許可すること。Oracle では、ロール・メカニズムに基づいて認可が行われる。1 人のユーザーまたはユーザー・グループに、1 つのロールまたは一連のロールを付与することができる。また、ロールに他のロールを付与することもできる。

認証（authentication）

コンピュータ・システム内でユーザーまたはデバイス、その他のエンティティの識別情報を検証するプロセス。通常このプロセスは、システム内の資源に対するアクセスを許可するための前提条件として実行される。

認証局（certificate authority）

ユーザー、データベース、管理者、クライアント、サーバーなどの他のエンティティが本当に本人であるかどうかを証明する信頼できるサード・パーティ。ユーザーを証明するとき、認証局では、最初にユーザーが証明書失効リスト（CRL）にないことを確認してからユーザーの識別情報を検証し、認証局の公開鍵で署名して証明書を付与する。認証局には、認証局が発行する認証局独自の証明書と公開鍵がある。サーバーとクライアントではこれらを使用して、認証局が作成した署名を検証する。認証局は証明書サービスを行う外部の会社であったり、企業の MIS 部門などの内部組織である場合がある。

ネットワーク認証サービス（network authentication service）

分散環境で、クライアントをサーバーに対して、サーバーをサーバーに対して、またはユーザーをクライアントとサーバーに対して認証する方法。ネットワーク認証サービスは、ユーザーに関する情報、ユーザーがアクセスするさまざまなサーバー上のサービスに関する情報、およびネットワーク上のクライアントとサーバーに関する情報を格納するためのリポジトリである。認証サーバーは物理的に異なるマシンであったり、システム内で別のサーバー上に置かれる機能であったりする。可用性を向上させるために、認証サービスを複製して 1 点障害を回避できる場合がある。

復号化

暗号化されたメッセージの内容（暗号文）を、元の読取り可能な書式（平文）に戻す変換プロセス。

プリンシパル（principal）

kservice/kinstance@REALM からなる Kerberos オブジェクト。*kservice*、*kinstance* および*レルム*も参照。一意に識別されるクライアントまたはサーバー。

メッセージ・ダイジェスト（message digest）

「**チェックサム（checksumming）**」を参照。

メッセージ認証コード（message authentication code）

データ認証コード（DAC）ともいう。秘密鍵を追加した**チェックサム（checksumming）**。鍵を持つ人のみが暗号化チェックサムを検証できる。

レルム（realm）

Kerberos オブジェクト。1 つのキー配布センター / チケット付与サービス（KDC/TGS）の元で動作する一連のクライアントとサーバー。異なるレルムに存在する同じ名前を持つ *kservices* は一意である。

索引

T

W

X

あ

い

か

き

く

け

こ

さ

し

す

せ

ち

て