

Oracle Direct Seminar



ORACLE®

**意外と簡単!? Oracle Database 11g
- セキュリティ編 -**

日本オラクル株式会社

Oracle Direct

Agenda

- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

Agenda

- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

はじめに

近年では、データベースに高い安全性を
求められるようになっています

なぜ高い安全性が求められるようになったのか？

- データベースには非常に重要な情報が格納されています
(銀行のATM、クレジットカード情報など)
- 近年情報漏えい問題が話題となっています

データベースはセキュアなデータベースとして
構成されている必要があります

セキュアなデータベースとは？

- 情報漏えいに対応できる高度なセキュリティ設定
- 悪意のある処理を抑止するための監査やログの保存



本日のゴールとシステム構成

• 本日のゴール

セキュリティを高めるために実現できる基本的な設定ができるようになる

データベース・システムでの考慮
すべきセキュリティを高めるための
施策を大きく5つに分けて、
こちらの観点から解説します

- データベースの初期構成
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他

• システム構成

オペレーティング・システム: Microsoft Windows 2003 + Service Pack1

RDBMS: Oracle Database 11g Release 1 Enterprise Edition for Windows

ORACLE®

Agenda

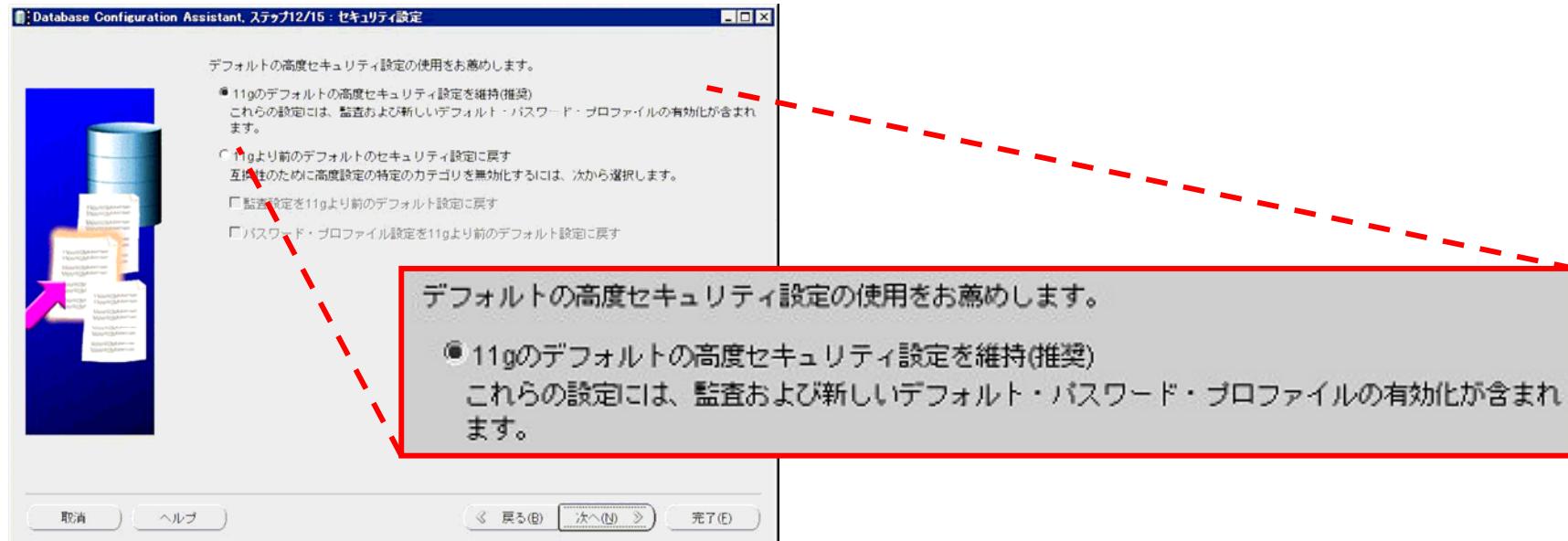
- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

初期状態からセキュアなデータベース

- Database Configuration Assistant(DBCA)にて
データベースの構成を行う際のセキュリティ設定画面



具体的に初期設定される内容

- 標準監査の有効化
- デフォルト・プロファイルのパスワード制限の強化
- PUBLICロールからのCREATE EXTERNAL JOB権限の削除

ORACLE®

Agenda

- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

認証の管理

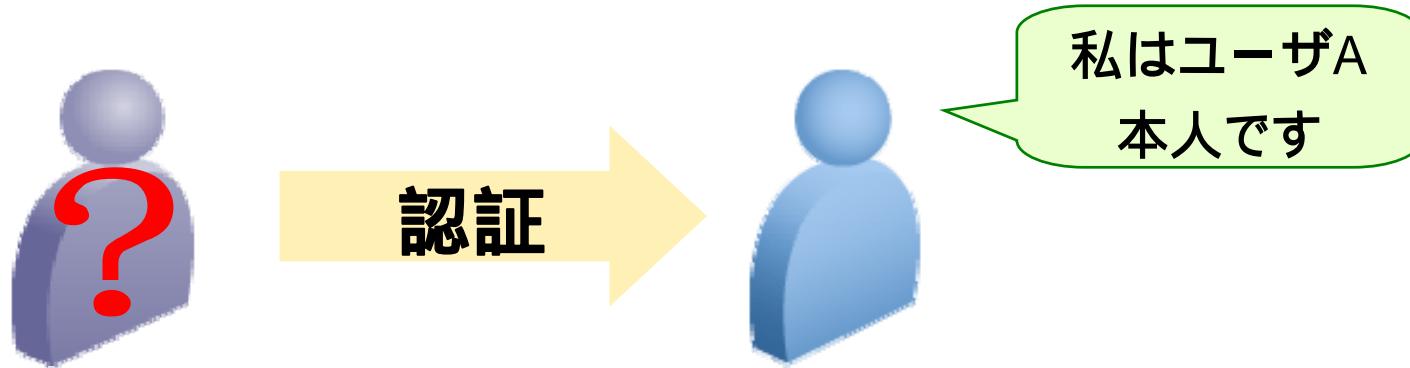
- ユーザー・アカウントの管理
 - 認証とは？
 - データベース・ユーザーとは？
 - **EM** ユーザー・アカウントの表示
- 不要なユーザーを利用可能な状態にしない
 - **EM** データベース・ユーザーのロックを解除しよう
 - **EM** データベース・ユーザーをロックしよう
- パスワードの変更
 - **EM** データベース・ユーザのパスワードを変更しよう
- パスワードの管理
 - プロファイルとは？
 - **EM** 新しいプロファイルの作成
 - **EM** 新しいプロファイルの割り当て

Enterprise Manager
を使った設定方法を
解説します

ORACLE®

認証とは？

- 認証とは、ユーザがデータベースにログインする時に、「ユーザが誰か」を特定するためのものです



Oracleには次の認証方法が用意されています

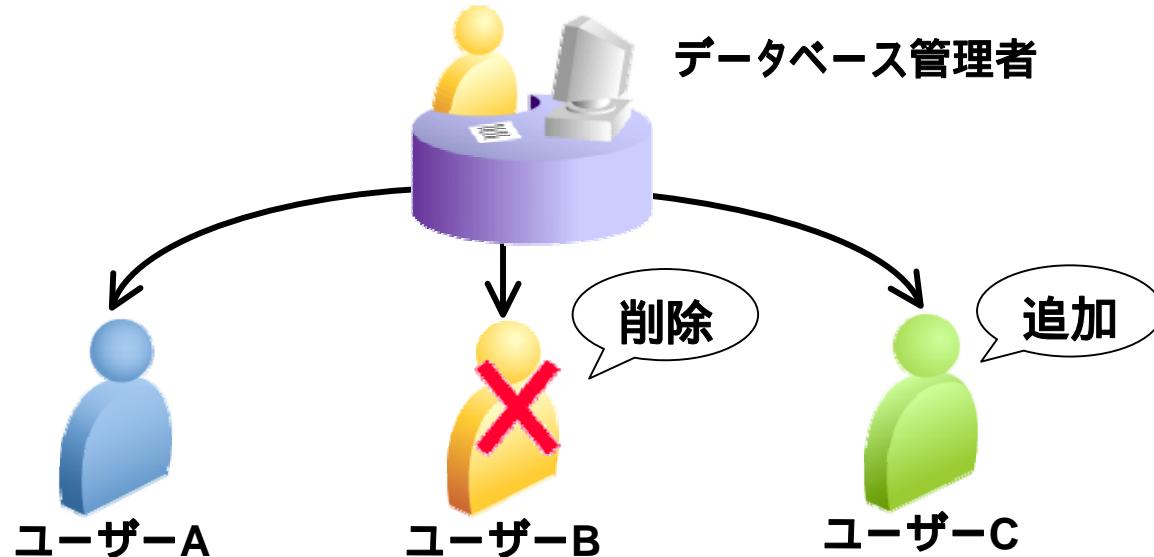
- データベースによるパスワード認証: ログイン時にパスワードを入力する方法
- 外部認証: OSまたはネットワークシステムを利用
- グローバル認証: ディレクトリ・サービスを利用



ORACLE

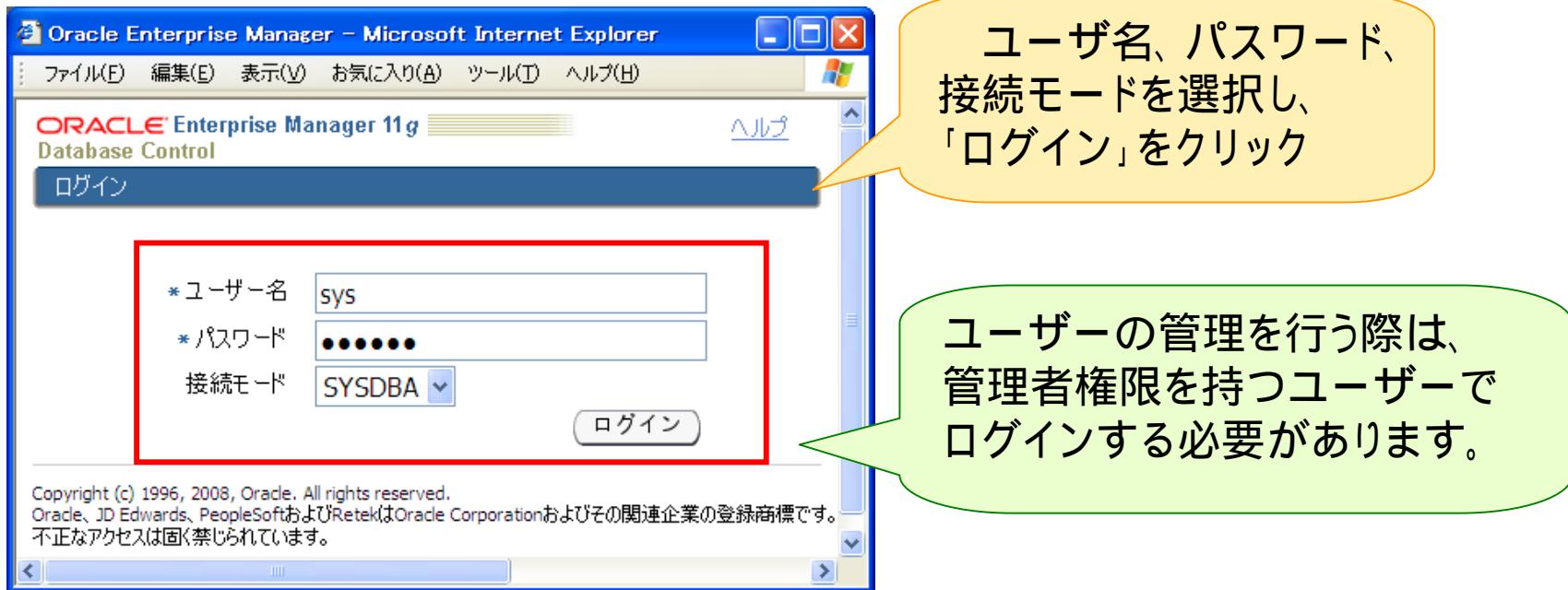
■ データベース・ユーザーとは

- ・データベース・ユーザーとは、データベース内に接続するためのアカウントのことです



セキュリティを高めるためにデータベース管理者は、
ユーザー・アカウントを適切に作成・管理する必要があります

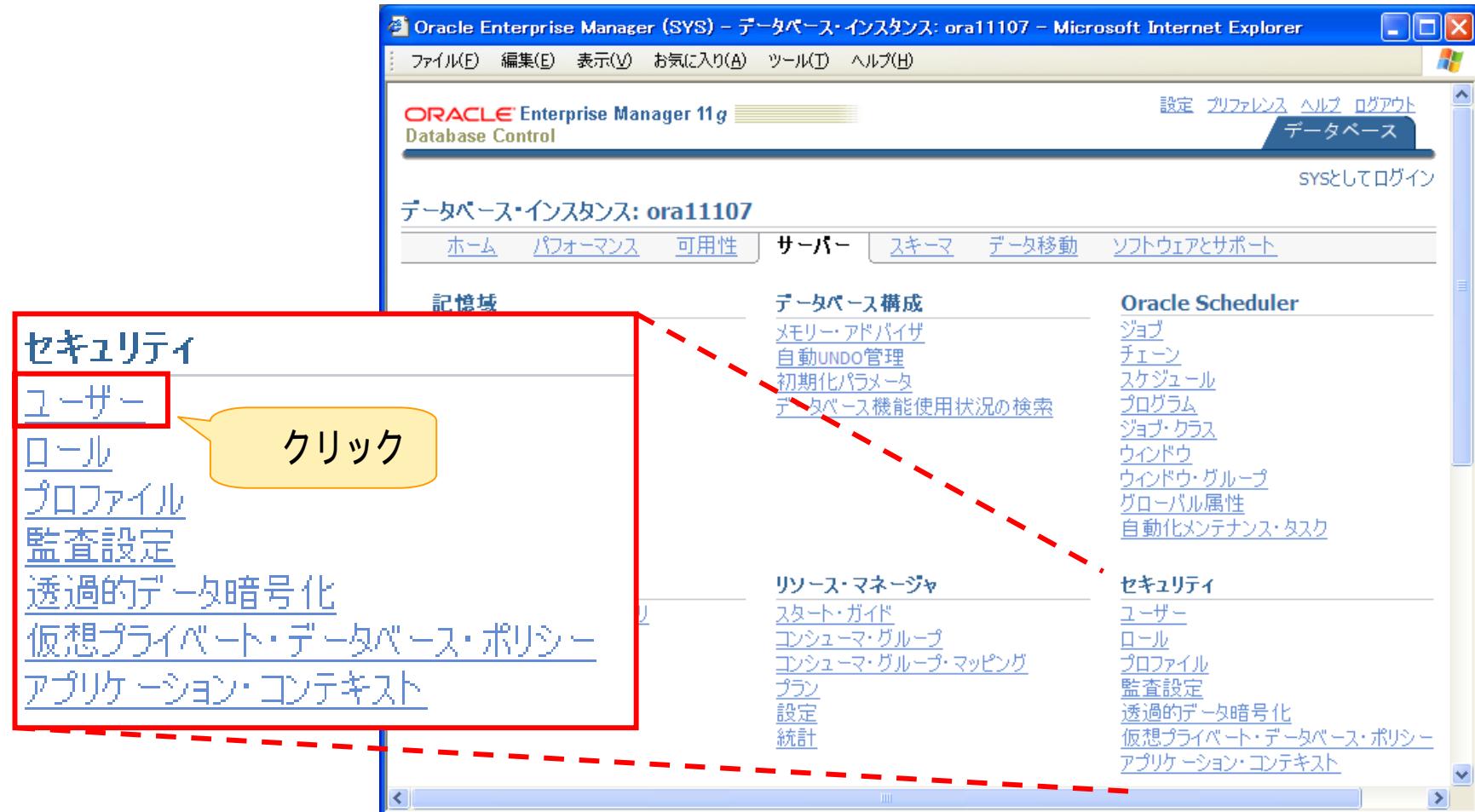
ユーザー・アカウントの管理



データベース作成時に次のユーザー・アカウントが作成されます

- **SYS**: データベースの管理ユーザ(全ての管理作業)
- **SYSTEM**: データベースの管理ユーザ(データベースの起動・停止以外の管理作業)
- **SYSMAN, DBSNMP, サンプル・スキーマ・ユーザー(HR,OE,SHなど)**

ユーザーアカウントを表示します



ユーザーアカウントの表示画面

The screenshot shows the Oracle Enterprise Manager 11g Database Control interface for managing users. The title bar reads "Oracle Enterprise Manager (SYS) - ユーザー - Microsoft Internet Explorer". The menu bar includes "ファイル(F)", "編集(E)", "表示(V)", "お気に入り(A)", "ツール(T)", and "ヘルプ(H)". The top navigation bar says "ORACLE Enterprise Manager 11g Database Control" and "データベース". A green callout bubble points to the "データベース" button. The main content area is titled "ユーザー" (User). It features a search bar with "オブジェクト・タイプ: ユーザー" and a search input field. Below the search is a "検索" section with a note about filtering results. A "オブジェクト名" input field and a "実行" button are present. A "選択モード" dropdown is set to "単一". At the bottom, there's a toolbar with buttons for "編集", "ビュー", "削除", "アクション", "類似作成", "実行", "前へ", "1-25 / 38", and "次の13行". A table lists user accounts with columns: 選択 (Select), ユーザー名 (User Name), アカウント・ステータス (Account Status), 有効期限 (Effective Date), デフォルト表領域 (Default Table Space), 一時表領域 (Temporary Table Space), プロファイル (Profile), and 作成 (Create). The table rows show the following data:

選択	ユーザー名	アカウント・ステータス	有効期限	デフォルト表領域	一時表領域	プロファイル	作成
<input checked="" type="radio"/>	ANONYMOUS	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 6:58:43 JST
<input type="radio"/>	APEX_PUBLIC_USER	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	USERS	TEMP	DEFAULT	2008/10/01 7:32:04 JST
<input type="radio"/>	CTXSYS	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 6:57:44 JST
<input type="radio"/>	DBSNMP	OPEN	2009/08/12 15:44:41 JST	SYSAUX	TEMP	MONITORING_PROFILE	2008/10/01 6:44:53 JST
<input type="radio"/>	DIP	EXPIRED & LOCKED		USERS	TEMP	DEFAULT	2008/10/01 6:34:00 JST
<input type="radio"/>	EXFSYS	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 6:57:18 JST

この画面から、ユーザー
アカウントの管理作業を
行っていただけます

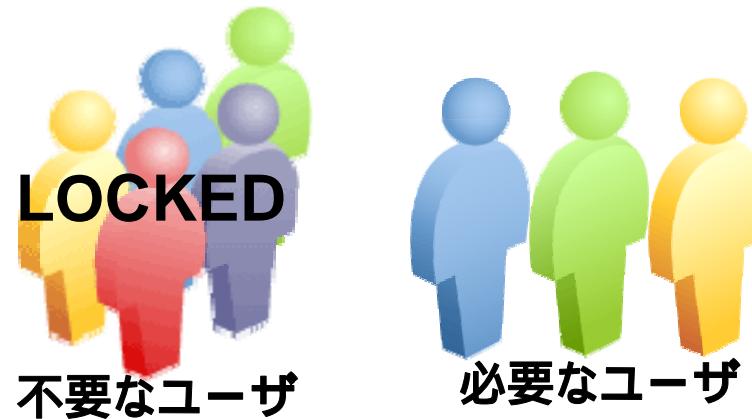
- アカウントのロック解除
- アカウントのロック
- パスワードの変更

ORACLE®

不要なユーザーを利用可能な状態にしない

- Oracleデータベースの作成時には、内部的作業をするユーザーやサンプル用のユーザーが作成され、不正アクセスを防ぐため、これらの多くのユーザーはロックされています
- セキュリティを向上させるために、必要性の無いユーザーはログインできないようにロックしておくべきです

セキュリティを向上
不正アクセスを防止



続いてユーザーのロックの解除とロックの方法を確認してみましょう

ORACLE

ユーザーHRのロックを解除します

The screenshot shows the Oracle Enterprise Manager interface for managing users. A yellow callout points to the 'Actions' dropdown menu in the toolbar, with the text: 'アクションリストから「ユーザーのロックの解除」を選択し、「実行」をクリック'. Another yellow callout points to the 'User Name' column, with the text: 'ロックを解除したいアカウントを選択'. A third yellow callout points to the 'HR' row, which is highlighted with a red border, with the text: 'ユーザーHRのロックが解除されました'. To the right, a confirmation dialog box titled '確認' (Confirmation) asks 'ロック解除 USER HRが必要ですか。' (Do you want to unlock user HR?). The 'はい' (Yes) button is highlighted with a red border and has the text 'クリック' (Click) above it.

Oracle Enterprise Manager (SYS) - ユーザー - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)

選択モード 単一

選択	ユーザー名	状態	最終更新日時	領域	一時表領域	プロファイル	作成
<input type="radio"/>	ANONYMOUS	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 6:58:43 JST
<input type="radio"/>	APEX PUBLIC USER	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 7:32:04 JST
<input type="radio"/>	CTXSYS	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 6:57:44 JST
<input type="radio"/>	DBSNMP	OPEN	2009/08/12 15:44:41 JST	SYSAUX	TEMP	MONITORING_PROFILE	2008/10/01
<input type="radio"/>	DIP	EXPIRED &		USERS	TEMP		
<input type="radio"/>	EE			SYSAUX	TEMP		
<input type="radio"/>	EJ			SYSAUX	TEMP		
<input checked="" type="radio"/>	HR	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	USERS	TEMP		
<input type="radio"/>	MDDATA	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	USERS	TEMP		

確認 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 > ユーザー > データベース SYSとしてログイン

確認

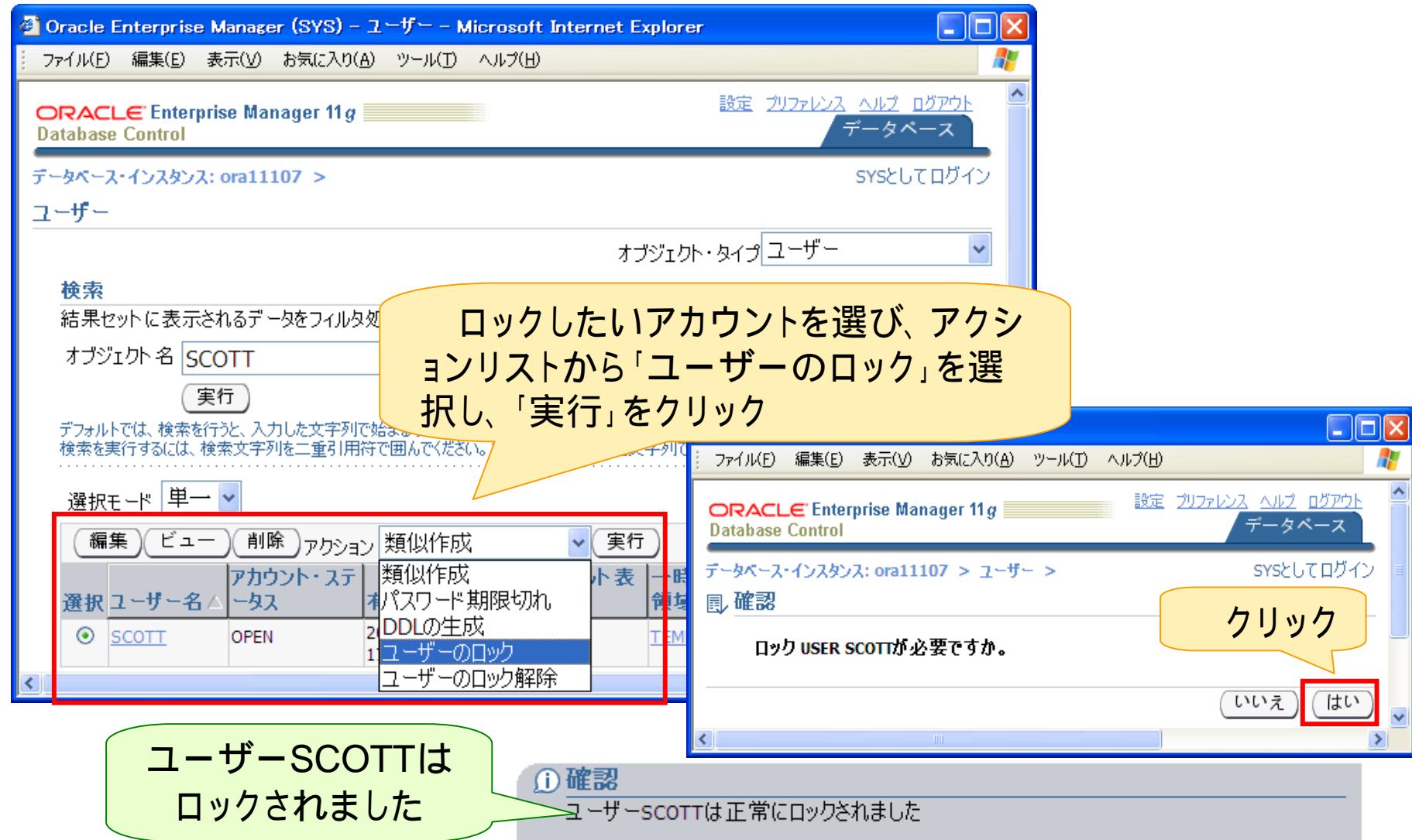
ロック解除 USER HRが必要ですか。

いいえ はい

確認

ユーザーHRは正常にロック解除されました

ユーザーSCOTTのアカウントをロックします



ORACLE

■ パスワードの変更について

- アカウント・ステータスがEXPIRED(パスワード期限切れ状態)の場合、ユーザーは次回ログイン時にパスワードを変更するよう求められます

選択	ユーザー名 △	アカウント・ステータス
	HR	EXPIRED

パスワード期限切れ状態

データベース作成時に同一のパスワードを使用するように設定している場合にも、適切にパスワードを変更しておくことをお勧めします

パスワードを変更したいユーザーを選択します

Oracle Enterprise Manager (SYS) - ユーザー - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 >

ユーザー

オブジェクト・タイプ: ユーザー

検索: オブジェクト名 S

実行

選択モード: 単一

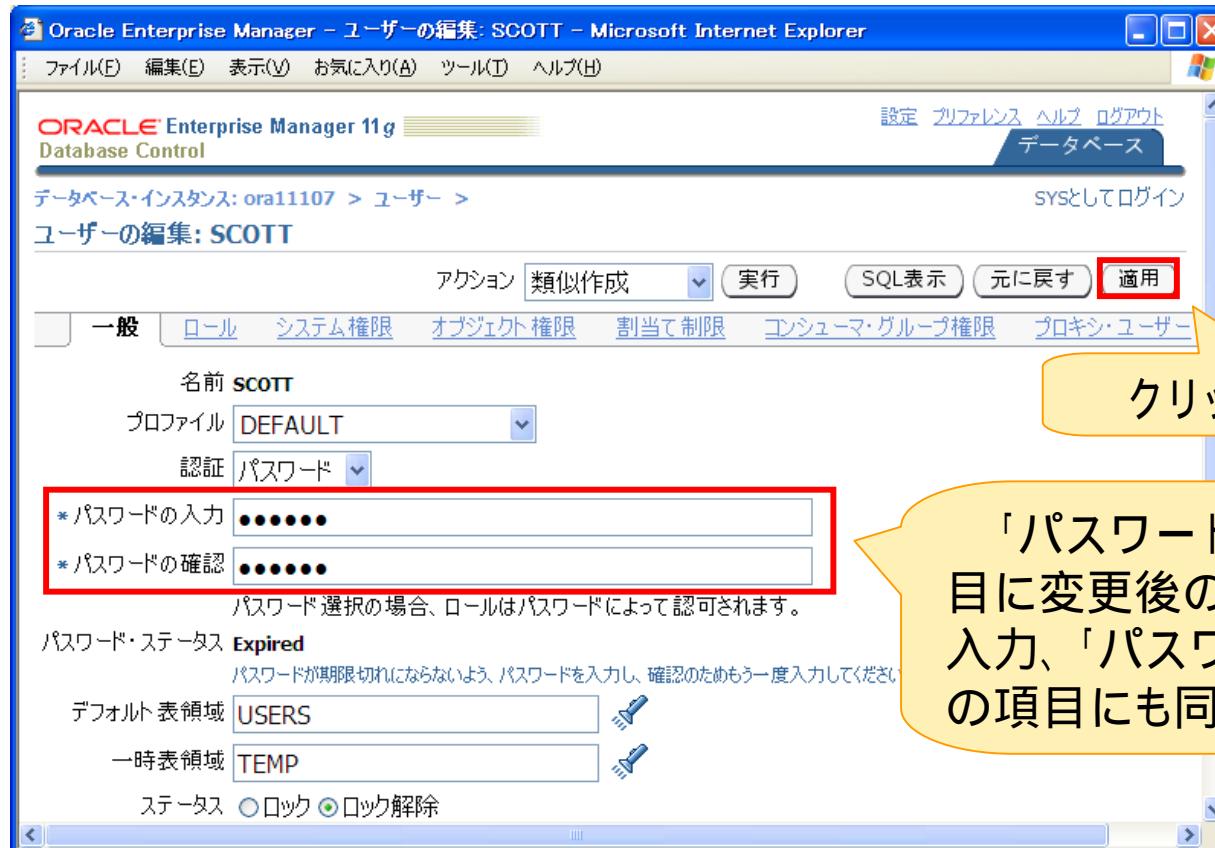
編集 (選択済み) ビュー 削除 アクション 類似作成 実行

選択ユーザー名	アカウント・ステータス	有効期限	デフォルト表領域	一時表領域	プロファイル	作成
SCOTT	EXPIRED	2009/03/24 13:59:32 JST	USERS	TEMP	DEFAULT	2008/10/01 7:57:40 JST
SI_INFORMTN_SCHEMA	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYSAUX	TEMP	DEFAULT	2008/10/01 7:03:11 JST
SPATIAL_CSW_ADMIN_USR	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	USERS	TEMP	DEFAULT	2008/10/01 7:19:34 JST
SPATIAL_WFS_ADMIN_USR	EXPIRED & LOCKED	2009/02/13 14:21:42 JST	USERS	TEMP	DEFAULT	2008/10/01 7:19:25 JST
SYS	OPEN	2009/08/12 14:21:07 JST	SYSTEM	TEMP	DEFAULT	2008/10/01 6:31:51 JST
SYSMAN	OPEN	2009/08/12 16:18:46 JST	SYSAUX	TEMP	DEFAULT	2009/02/13 16:18:46 JST
SYSTEM	OPEN	2009/08/12 14:21:07 JST	SYSTEM	TEMP	DEFAULT	2008/10/01 6:31:51 JST

パスワードを変更
したいアカウントを選
び、「編集」をクリック

ORACLE®

新しいパスワードを入力します



ユーザーSCOTTのパスワードが変更されました

更新メッセージ

ユーザー SCOTTは正常に変更されました

ORACLE

■ プロファイルとは？

- プロファイルとは、システム・リソースおよびパスワードの制限の設定をまとめたものです
- ユーザーは一度に1つのプロファイルのみを割り当てられます



プロファイル

- リソース使用量の制限
- アカウント・ステータスおよびパスワードの有効期限の管理

- データベースにはデフォルトのプロファイルが存在しており、ユーザー作成時に個別にプロファイルを指定しない限りは、DEFAULTプロファイルの内容が適用される仕組みとなっています

ORACLE®

アカウント・ステータスおよびパスワードの有効期限の管理について



アカウント・ステータス

- 特定のユーザーが、ある回数以上データベースへの接続に失敗した場合にそのユーザーをロックする設定ができます
- 11gのDEFAULTプロファイルでは、10回ログインに失敗すると、ユーザー・アカウントが1日ロックされます(初期状態)



パスワードの管理

- パスワードに有効期限をつけて、同じパスワードを使いつづけないように設定できます
- 11gのDEFAULT プロファイルでは、ユーザー・アカウントのパスワードは180日で自動的に期限切れとなります(初期状態)

ORACLE®

新しいプロファイルを作成します

- このセクションでは、「意外と簡単!?データベース設定編」で作成したORADIRECTを使用します



ORADIRECT

ユーザー情報の入力内容

項目名	入力内容
名前	ORADIRECT
プロファイル	DEFAULT
認証	パスワード
期限切れパスワード	チェックしない
デフォルト表領域	USERS
一時表領域	TEMP
ステータス	ロック解除

ORADIRECTプロファイルを作成します

The screenshot shows two windows of Oracle Enterprise Manager 11g. The left window displays the main navigation menu with various database management options like 'データベース構成' (Database Configuration), 'データベース監査' (Database Audit), and 'データベース統計' (Database Statistics). The right window is a detailed view of the 'セキュリティ' (Security) section under 'データベース' (Database). A red box highlights the 'プロファイル' (Profile) link, which is also pointed to by a yellow speech bubble containing the word 'クリック' (Click). Below it, other security-related links are listed: '監査設定' (Audit Settings), '透過的データ暗号化' (Transparent Data Encryption), '仮想プライベート・データベース・ポリシー' (Virtual Private Database Policy), and 'アプリケーション・コンテキスト' (Application Context). A dashed red arrow points from the 'セキュリティ' section to the right window. The right window itself has a title bar 'Oracle Enterprise Manager (SYS) - プロファイル - Microsoft Internet Explorer'. It shows a search bar with 'オブジェクト・タイプ: プロファイル' (Object Type: Profile) and a search input field. A yellow speech bubble with 'クリック' points to the '実行' (Execute) button. Below the search area is a table titled '選択 プロファイル' (Selected Profile) with three rows: 'DEFAULT' (selected with a radio button), 'MONITORING PROFILE', and 'WKSYS PROF'. The table includes columns for '接続時間(分)' (Connection Time (min)) and '同時セッション' (Simultaneous Sessions). A red box highlights the '作成' (Create) button at the bottom right of the table.

プロファイル作成時の「一般」タブの画面

- この画面では、リソース使用量の制限について設定できます

CPU:

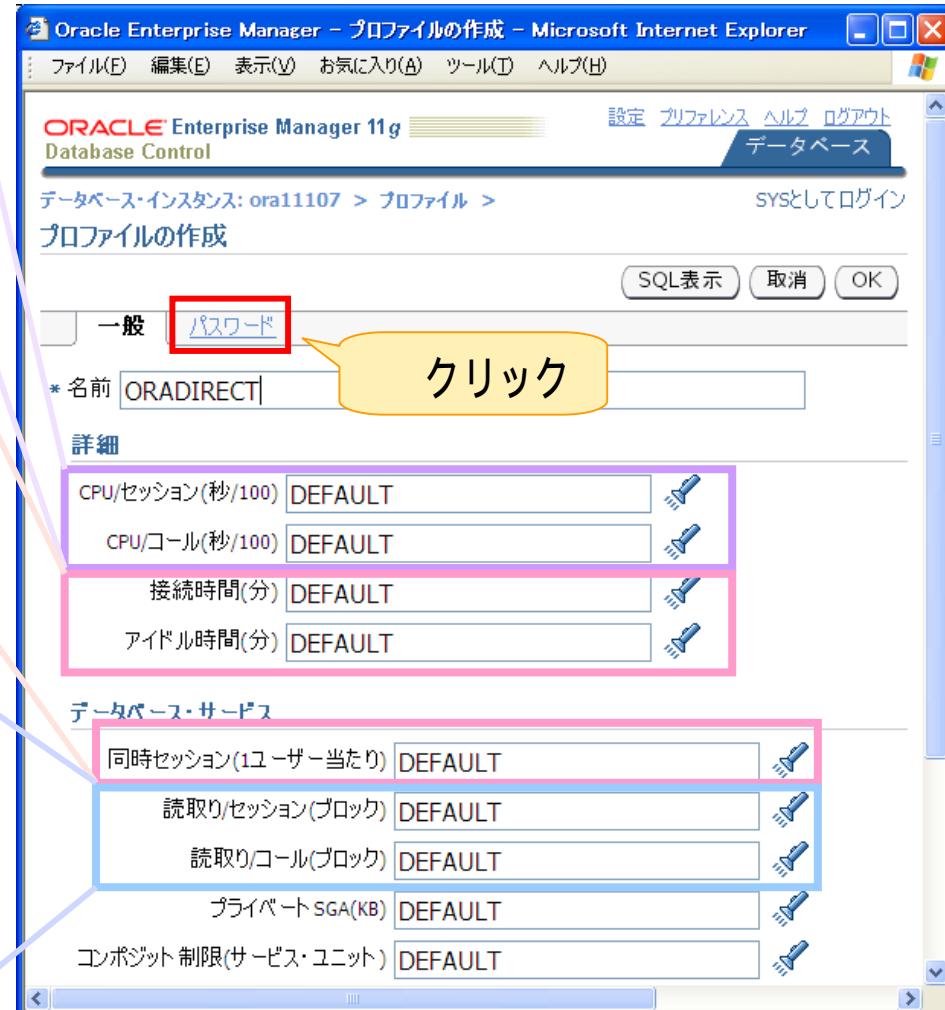
CPUリソースは、セッションごと
またはコールごとに制限できます

ネットワーク/メモリー:

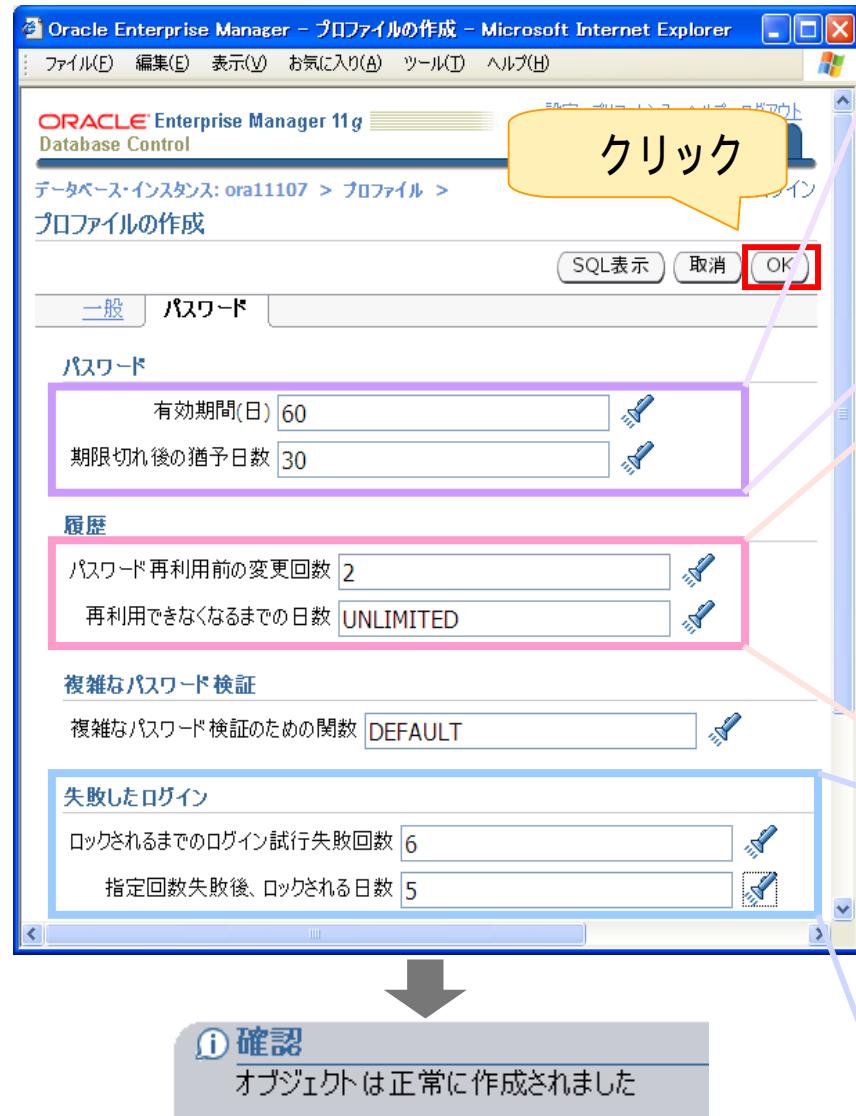
接続時間やアイドル時間、
同時セッションなどを設定できます

ディスクI/O:

セッションごとまたはコールごとの
レベルでユーザが読み取ることが
できるデータ量を制限できます



パスワードについての内容を入力します



有効期限(日) : 60

設定したパスワードは60 日間使用可能

期限切れ後の猶予日数 30

有効期限が切れた後、

30日間は同じパスワードを使用可能

パスワード再利用前の変更回数 : 2

2 度異なるパスワードに変更されてからでないと、

同じパスワードは使用できません

再利用できなくなるまでの日数 : 180

パスワード履歴を保持する期間

ロックされるまでのログイン試行失敗回数 : 6

6回ログインを失敗するとユーザーがロックされます

指定回数失敗後、ロックされる日数 : 5

ロックされた後で5 日間経過するとロック解除されます

ORACLE

新しいプロファイルをORADIRECTユーザーに割り当てます

The image shows two screenshots of the Oracle Enterprise Manager interface. The left screenshot displays the main navigation menu with various database management options like Performance, Configuration, Scheduler, and Security. A red dashed arrow points from the 'Security' link in the left sidebar to the right screenshot. The right screenshot shows the 'User' management page where the 'ORADIRECT' user has been selected and the 'Edit' button is highlighted. A yellow callout box on the right side provides instructions: 'ユーザー一覧の中から「ORADIRECT」を選択し、「編集」をクリック' (Select 'ORADIRECT' from the user list and click 'Edit').

Oracle Enterprise Manager (SYS) - データベース・インスタンス: ora11107 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107

セキュリティ

ユーザー

ロール

プロファイル

監査設定

透過的データ暗号化

仮想プライベート・データベース・ポリシー

アプリケーション・コンテキスト

Oracle Enterprise Manager (SYS) - ユーザー - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 >

ユーザー

オブジェクト・タイプ ユーザー

検索

結果セットに表示されるデータをフィルタ処理するには、オブジェクト名を入力します。

オブジェクト名 ORADIRECT

実行

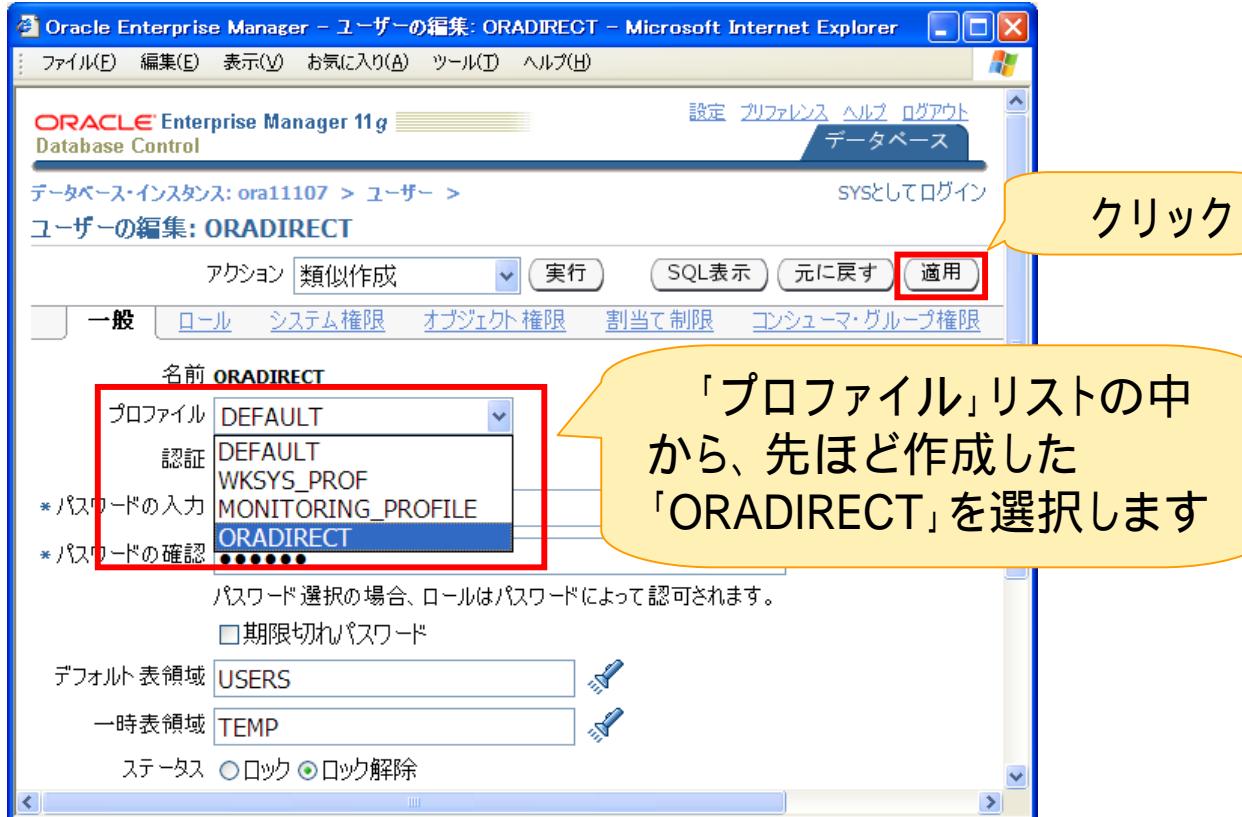
デフォルトでは、検索を行うと、入力した文字列で始まるすべて大文字の一一致結果が戻されます。完全一致検索または大文字/小文字を区別する検索を実行するには、検索文字列を二重引用符で囲んでください。二重引用符で囲んだ文字列では、ワイルドカード記号(%)を使用できます。

選択モード 単一

編集 ビュー 削除 アクション 類似作成 実行

選択	ユーザー名	アカウント・ステータス	有効期限	デフォルト表領域	一時表領域	プロファイル	作成
<input checked="" type="radio"/>	ORADIRECT	OPEN	2009/09/20 15:50:31 JST	USERS	TEMP	DEFAULT	2009/02/24 16:42:03 JST

ORADIRECTユーザーに割り当てるプロファイルを選択します



① 更新メッセージ

ユーザー ORADIRECTは正常に変更されました

ORACLE

Agenda

- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

権限の管理

- 権限の種類
- 権限の付与
- 権限の許可、拒否、取り消し
 - **EM** EMによる権限の割り当て
- ユーザー定義のデータベースロール
 - **EM** ユーザー定義ロールを作成する
- ロールによる権限管理の簡素化
 - **EM** ユーザーにロールを割り当てる
- Publicロール

Enterprise Manager
を使った設定方法を
解説します

権限とは

権限とは、主にSQL の実行やオブジェクトへのアクセスを行える権利のことです



たとえば、次のような処理を行う権利を権限と呼びます

- データベースへの接続(セッションの作成)
- 表の作成
- 他のユーザーの表からの行の選択
- 他のユーザーのストアド・プロシージャの実行

セキュリティを高く維持するためには、常に必要
最低限の権限を付与するようにしてください

権限の種類とロール

- ・権限は大きく分けて次の2つに分類されます

システム権限

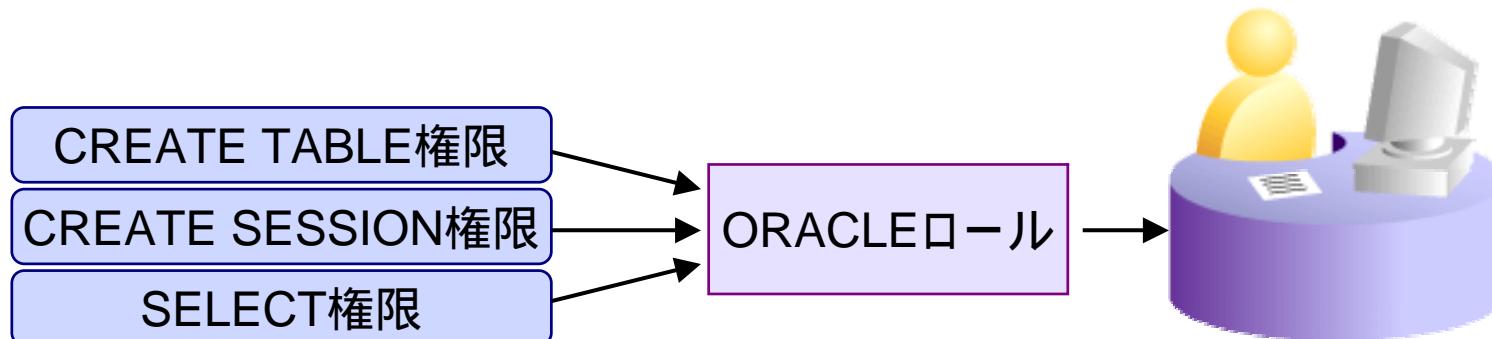
特定のアクションを実行する権限、
特定のタイプのオブジェクトに対する
アクションを実行する権限のことです
例: CREATE SESSION権限、
CREATE TABLE権限

オブジェクト権限

他のユーザの表などに対して特
定のアクションを実行する権限の
ことです
例: GRANT SELECT ON 表名
TO ユーザ名 ;

- ・権限をまとめ、1つのグループにしたもの **ロール**といいます

ロールとは、特定の権限の集合を持つユーザーの論理グループのことです

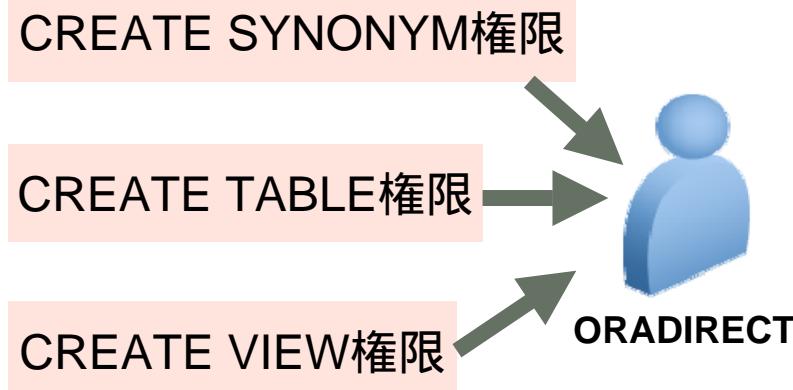


権限の付与

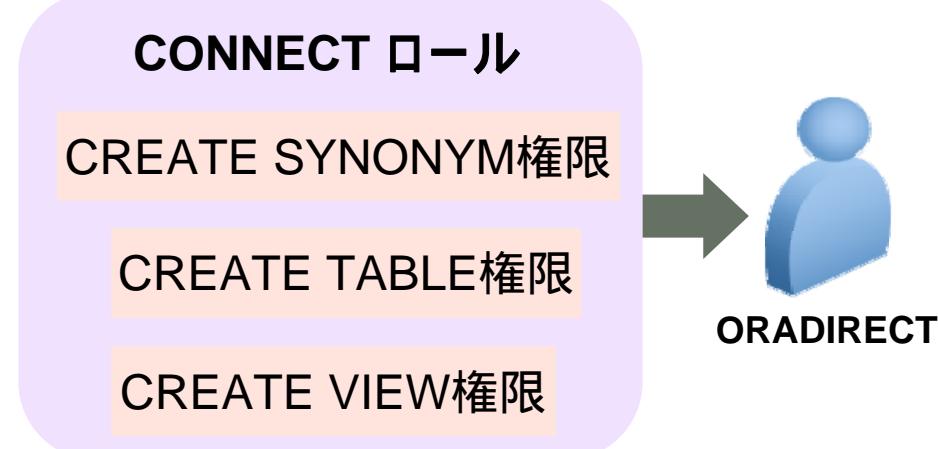
- 権限を付与するには、2つの方法があります
 - 直接ユーザーに対して権限を付与する方法
 - 権限をロール(名前つきの権限グループ)に付与したあとで、このロールをユーザーに付与する方法

例えばORADIRECTユーザに表、ビュー、シンニムを作成する権限を付与したい場合

直接、権限を付与する方法



ロールを付与する方法



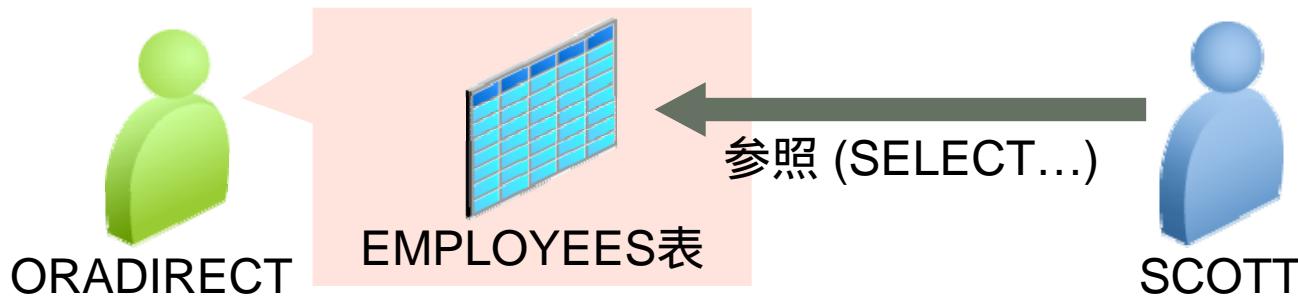
ロールを使用すると、一括して権限の管理が行えるため効率的です

権限の管理

- 権限の種類
- 権限の付与
- 権限の許可、拒否、取り消し
 - EM EMによる権限の割り当て
- ユーザー定義のデータベースロール
 - EM ユーザー定義ロールを作成する
- ロールによる権限管理の簡素化
 - EM ユーザーにロールを割り当てる
- PUBLICロール

Enterprise Manager
を使った設定方法を
解説します

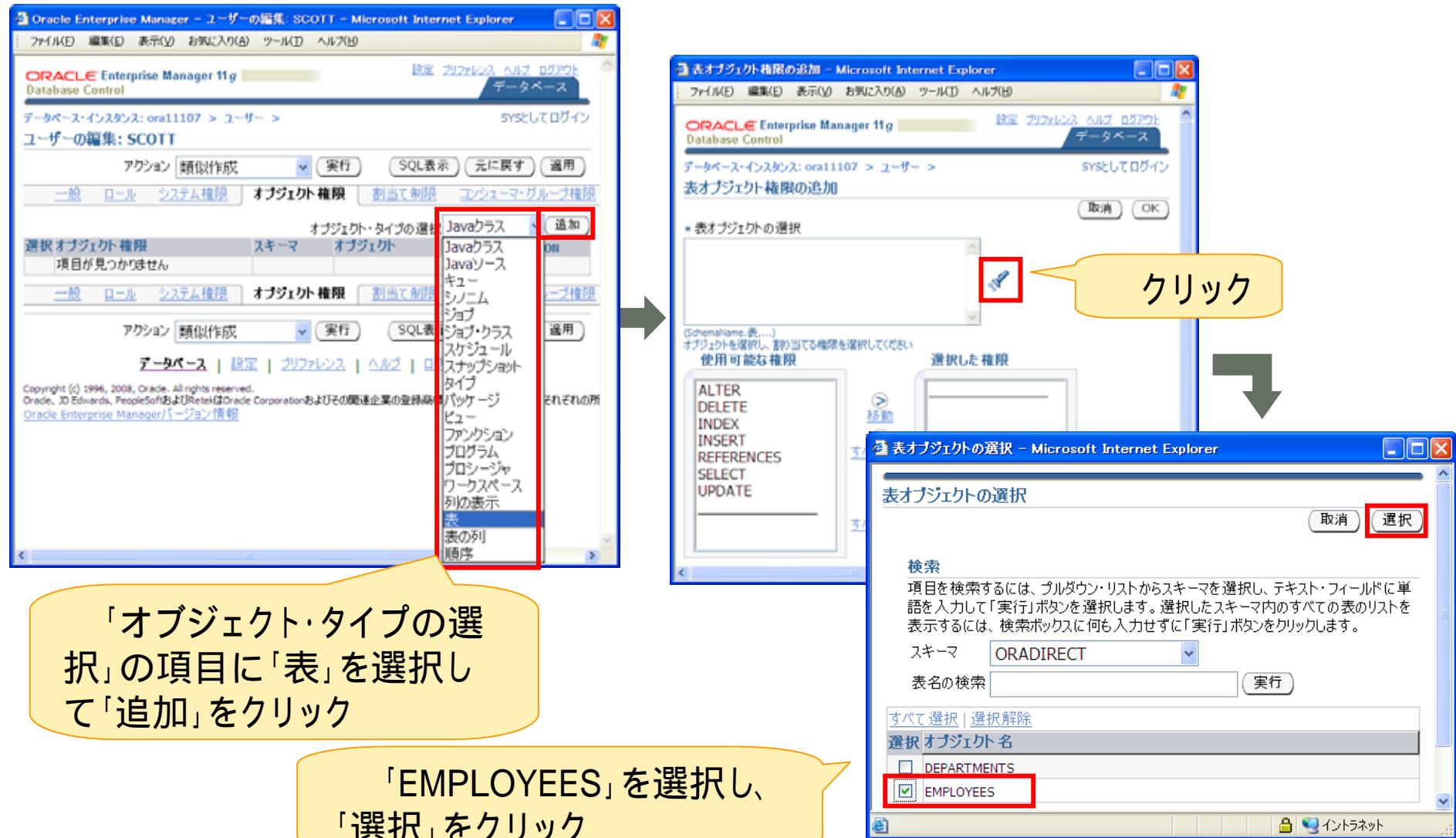
SCOTTユーザーにORADIRECTスキーマのEMPLOYEES表のSELECT権限を割り当てます



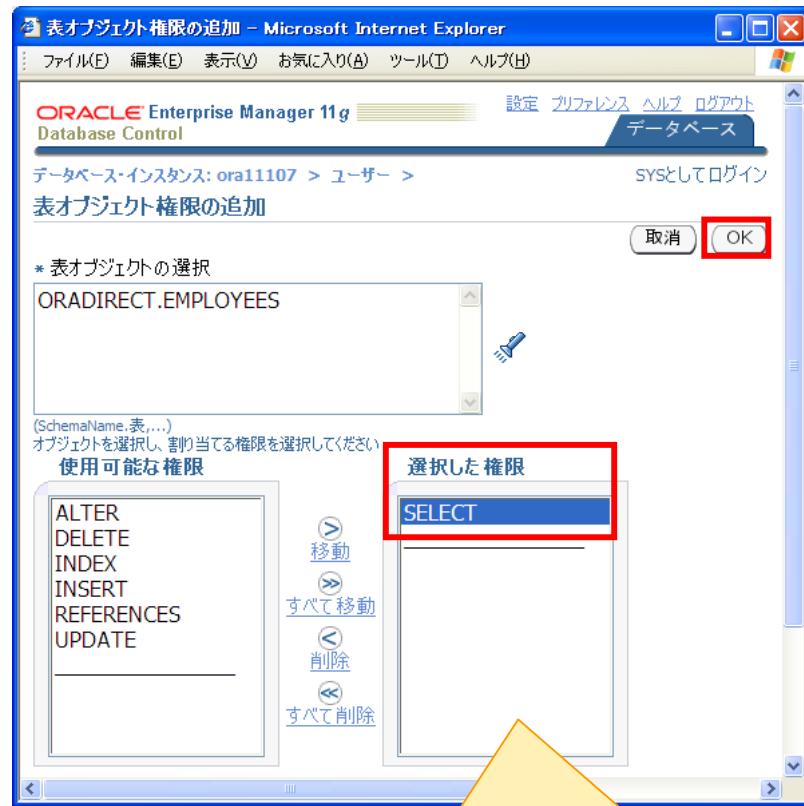
This screenshot shows the Oracle Enterprise Manager interface for managing users. In the search bar, the user name 'SCOTT' is entered. A yellow callout box highlights this entry with the text: 'ユーザ名「SCOTT」を選択し、「編集」をクリック'. Below the search bar, there is a toolbar with buttons for '選択', '編集' (highlighted with a red box), '削除', 'アクション', '類似作成', and '実行'. The main table displays user information for 'SCOTT', including status 'OPEN', creation date '2009/09/22 13:13:29 JST', and default tablespace 'USERS'. The '編集' button is highlighted with a red box.

This screenshot shows the 'Edit User' dialog in Oracle Enterprise Manager for the user 'SCOTT'. The 'オブジェクト権限' (Object Privileges) tab is selected. A yellow callout box highlights the 'オブジェクト権限' tab with the text: 'クリック'. The dialog shows fields for '名前' (Name: SCOTT), 'プロファイル' (Profile: DEFAULT), and '認証' (Authentication: パスワード). It also includes fields for password input and confirmation, and dropdowns for default and temporary tablespaces ('DEFAULT' and 'TEMP'). The bottom section contains checkboxes for '期限切れパスワード' (Expired Password) and 'ステータス' (Status: ロック or ロック解除).

オブジェクト・タイプと表オブジェクトを設定します



特定の表オブジェクト権限を選択し、権限を設定します



選択した権限に「SELECT」
を追加し、「OK」をクリック



権限にはOPTIONを
指定できます

① 更新メッセージ

ユーザー SCOTTは正常に変更されました

ORACLE

OPTIONが指定されている権限について

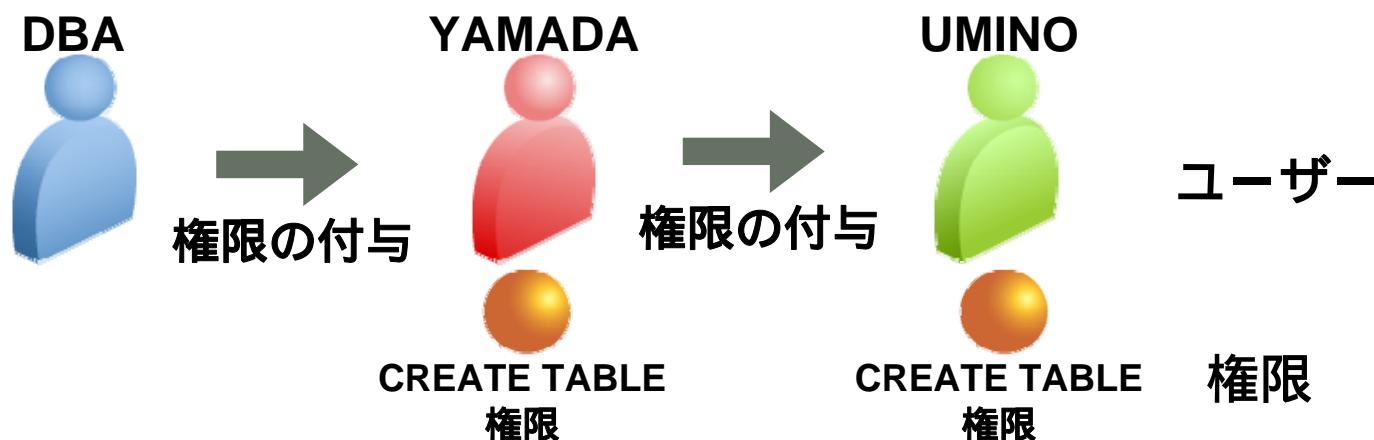
- ・システム権限

ADMIN OPTION: そのシステム権限を他のユーザーに付与できるようになります

- ・オブジェクト権限

GRANT OPTION: そのオブジェクト権限を他のユーザーに付与できるようになります

例えば、CREATE TABLE権限をADMIN OPTION付きで付与する場合



ユーザー定義のロールを作成します



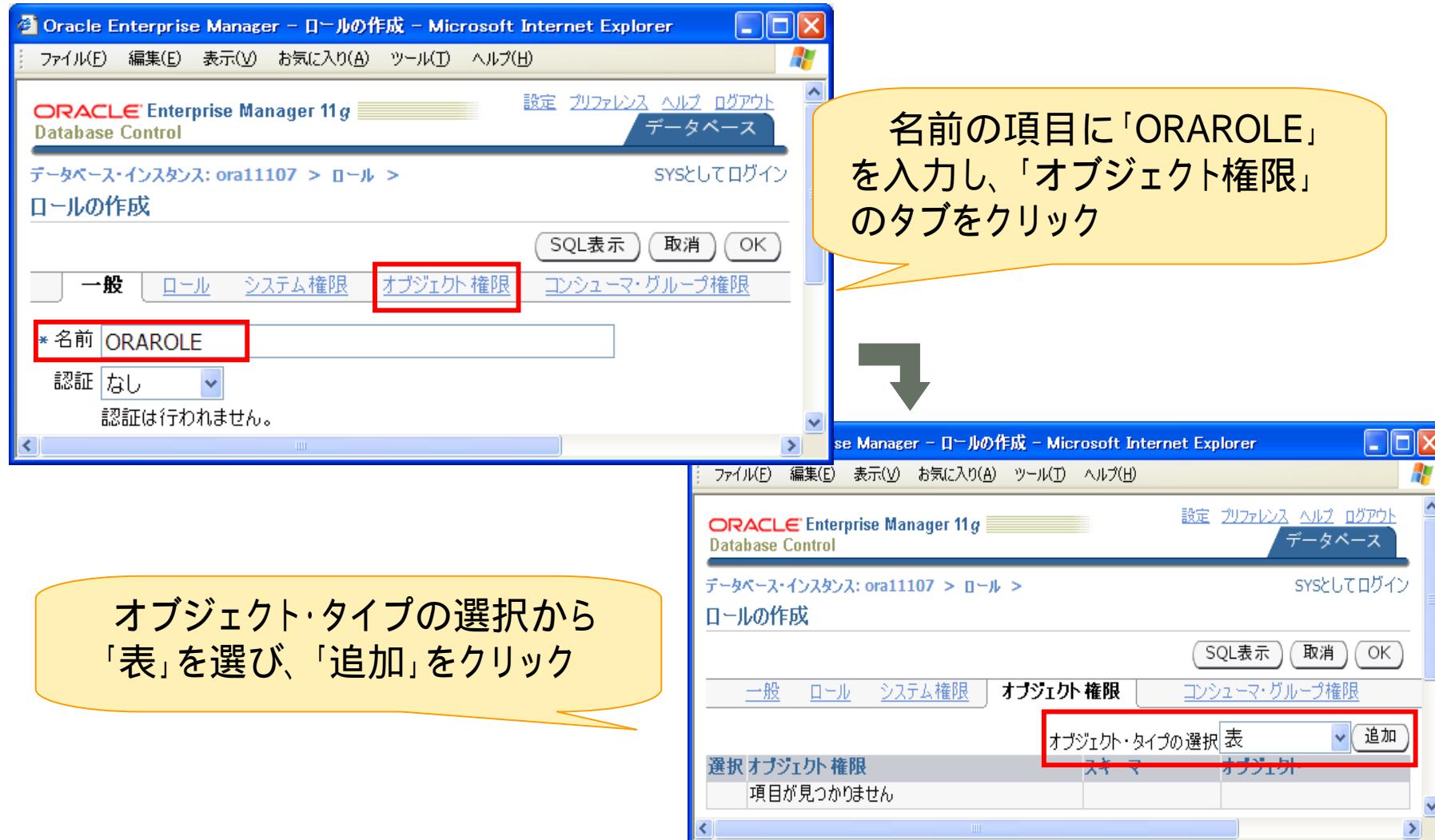
セキュリティ
ユーザー
ロール **クリック**
プロファイル
監査設定
透過的データ暗号化
仮想プライベート・データベース・ポリシー
アプリケーション・コンテキスト

ロールとは、特定の権限の集合を持つ
ユーザーの論理グループのことです

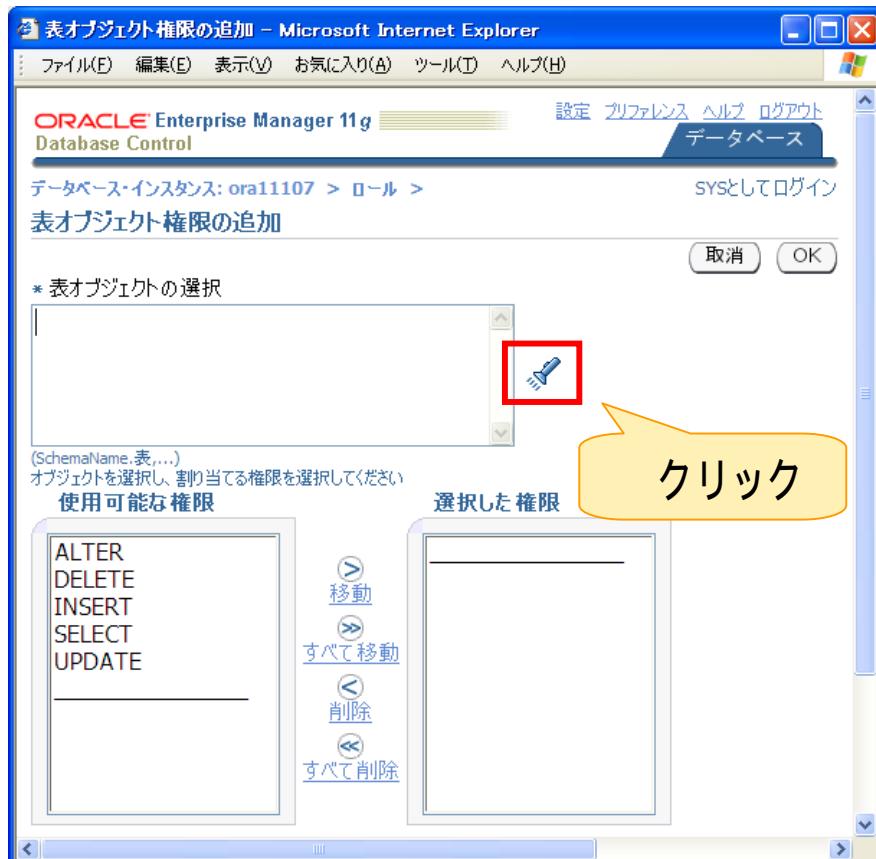
選択	ロール	認証
<input checked="" type="radio"/>	AQ_ADMINISTRATOR_ROLE	NO
<input type="radio"/>	AQ_USER_ROLE	NO
<input type="radio"/>	AUTHENTICATEDUSER	NO
<input type="radio"/>	CONNECT	NO
<input type="radio"/>	CSW_USR_ROLE	YES
<input type="radio"/>	CTXAPP	NO

ORACLE®

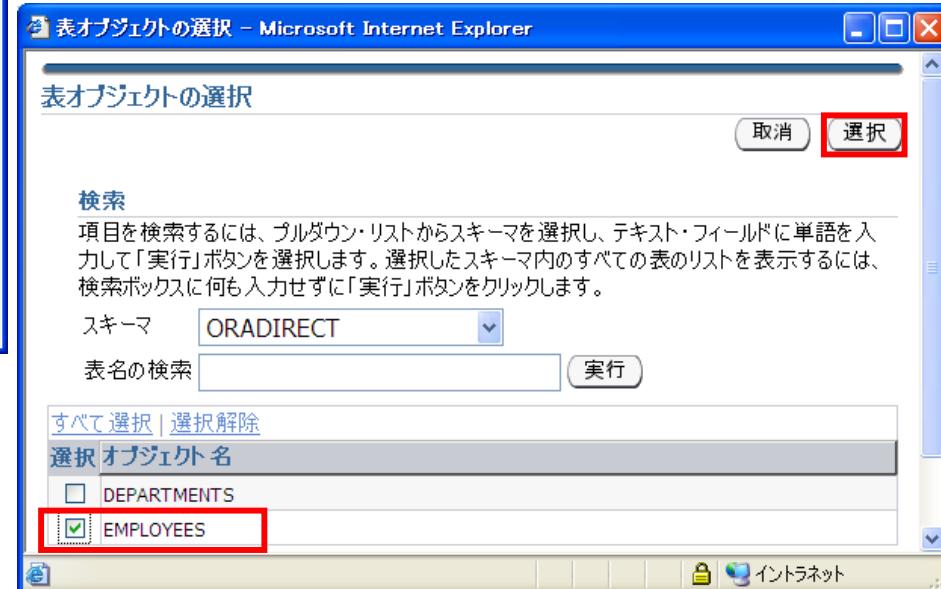
ロール名とオブジェクト・タイプを設定します



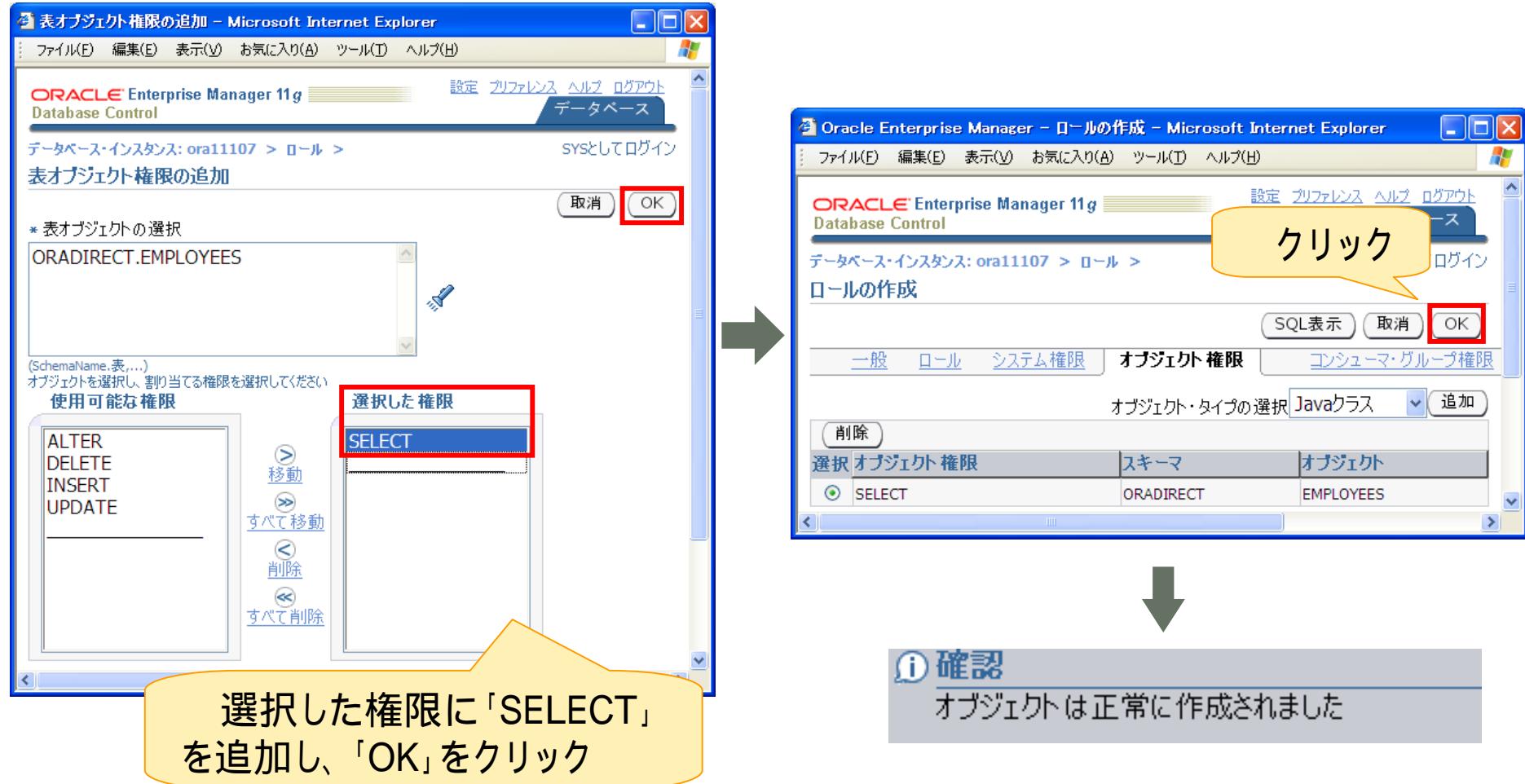
表オブジェクトを設定します



ORADIRECTスキーマの
EMPLOYEES表を選択し、
「選択」をクリック



ロールにORADIRECTスキーマのEMPLOYEES表へのSELECT権限を設定します

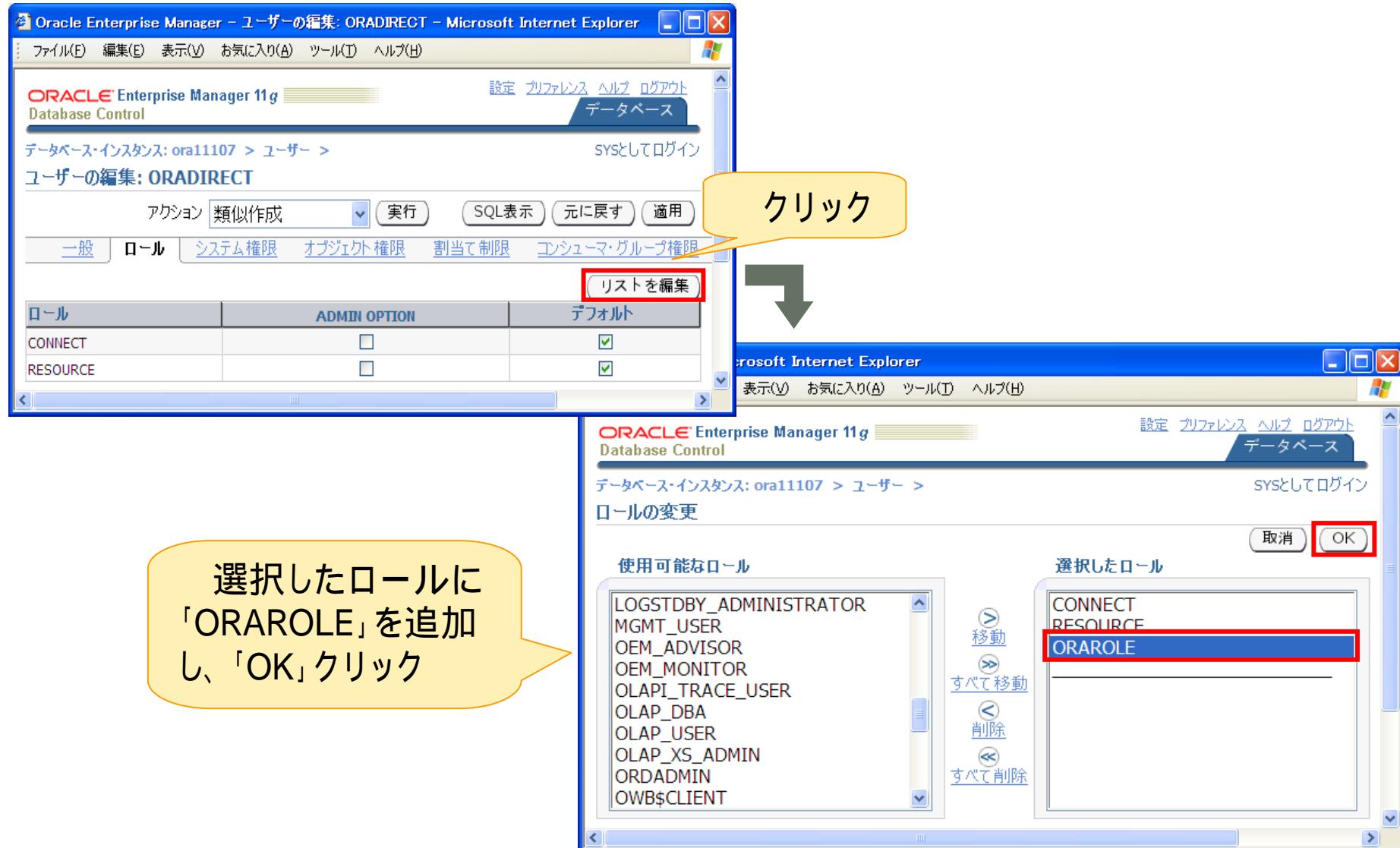


ORACLE®

作成したロールをユーザに割り当てます



割り当てるロールを選択します



「ORAROLE」ロールの付与を適用します

The screenshot shows the Oracle Enterprise Manager interface for editing a user. The title bar reads "Oracle Enterprise Manager - ユーザーの編集: ORADIRECT - Microsoft Internet Explorer". The main content area is titled "ORACLE Enterprise Manager 11g Database Control" and shows the path "データベース・インスタンス: ora11107 > ユーザー > ユーザーの編集: ORADIRECT". The "Role" tab is selected. A yellow callout bubble with the text "クリック" (Click) points to the "Apply" button. Below the table, a large downward-pointing arrow indicates the next step. A message box at the bottom right contains the text "① 更新メッセージ" and "ユーザー ORADIRECTは正常に変更されました".

ロール	ADMIN OPTION	デフォルト
CONNECT	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ORAROLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
RESOURCE	<input type="checkbox"/>	<input checked="" type="checkbox"/>

ORACLE

PUBLICに付与された権限について

PUBLIC に権限を付与すると

- ・全ユーザー(新規ユーザーも含む)が、その権限を行使することができます
- ・権限を取り消す場合、PUBLIC で取り消す必要があります

例:CREATE TABLE権限をPUBLICに付与する場合

```
GRANT CREATE TABLE TO PUBLIC;
```

すべてのユーザが、表を作成できるようになります

PUBLIC への権限付与は、すべてのユーザーへ影響を与えるので十分に注意を払い、必要最低限の権限とすることをおすすめします



Agenda

- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

外部からのアクセス

- リスナーの役割
- リスナーを監視と管理制限
 - **EM** : リスナーの状態を確認する
 - **EM** : リスナーにパスワードを設定する

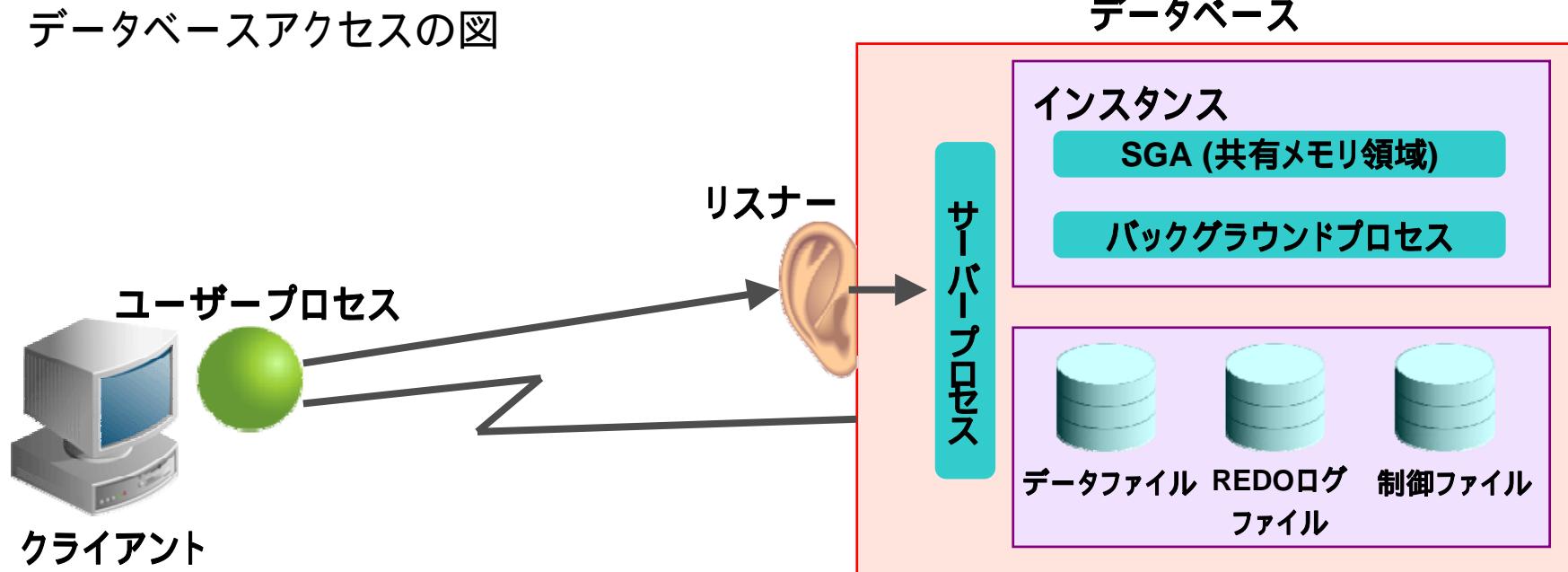
Enterprise Manager
を使った設定方法を
解説します



リスナーの役割

- ・リスナーとは、データベースがクライアントからの初期接続要求を受け付けるデータベース・サーバー側のプロセスです
- ・リスナーは、クライアントからの要求を受け取ったあとデータベースへ要求を引き渡します

データベースアクセスの図



リスナーの状況を確認します

The screenshot shows two Oracle Enterprise Manager windows. The left window displays the 'Listener Control' page for database instance ora11107. It shows the listener is running (稼働中) since March 31, 2009, at 11:32:47 JST. The right window shows detailed information about the listener, including its version (11.1.0.7.0), address (jpdel15dc.jp.oracle.com), and port (1521). A red box highlights the 'Listener' section in the left window, and a yellow box with the text 'クリック' (Click) points to the 'Edit' button in the right window. A green callout bubble on the right side states: 'リスナーの情報(リスナーのバージョン、NETアドレス、起動時間など)が表示され、停止する事もできます' (Listener information (listener's version, NET address, start time, etc.) is displayed, and it can also be stopped).

リスナーの情報(リスナーのバージョン、NETアドレス、起動時間など)が表示され、停止する事もできます

クリック

リスナー: LISTENER_jpdel15dc.jp.oracle.com

リスナー・プロセスの動作およびアイデンティティは、リスニング・エンドポイント（「ホスト および ポート」）のみではなく、リスナー・プロセスの起動に使用された「リスナー・パラメータ・ファイル」（listener.ora）によっても定義されます。「リスナー・パラメータ・ファイル」では、リスニング・エンドポイントの他にも、ログ・レベルやトレース・レベル、ログ・トレース・ディレクトリなどを指定しているため、EMTで「リスナー・ターゲット」を一意に識別するためにリスナー・パラメータ・ファイルの場所は必須です。

クリック

すべてのプロパティの表示

リスナー: LISTENER_jpdel15dc.jp.oracle.com

ステータス 稼働中
稼働開始 2009/03/31 11時32分47秒 JST
インスタンス名 ora11107
バージョン 11.1.0.7.0
ホスト jpdel15dc.jp.oracle.com
リスナー LISTENER_jpdel15dc.jp.oracle.com

編集 停止 ブラックアウト

ステータス 稼働中
可用性(%) 0
(過去2時間)
別名 LIS11107
バージョン 11.1.0.7.0
Oracleホーム D:\Oracle\product\11.1.0\db_1
Netアドレス (ADDRESS=(PROTOCOL=TCP)
(HOST= jpdel15dc.jp.oracle.com)
(PORT=1521))
LISTENER.ORAの場所 D:\Oracle\product\11.1.0\db_1
¥network\\$admin
開始時間 2009/04/02 14:35:24
ホスト jpdel15dc.jp.oracle.com

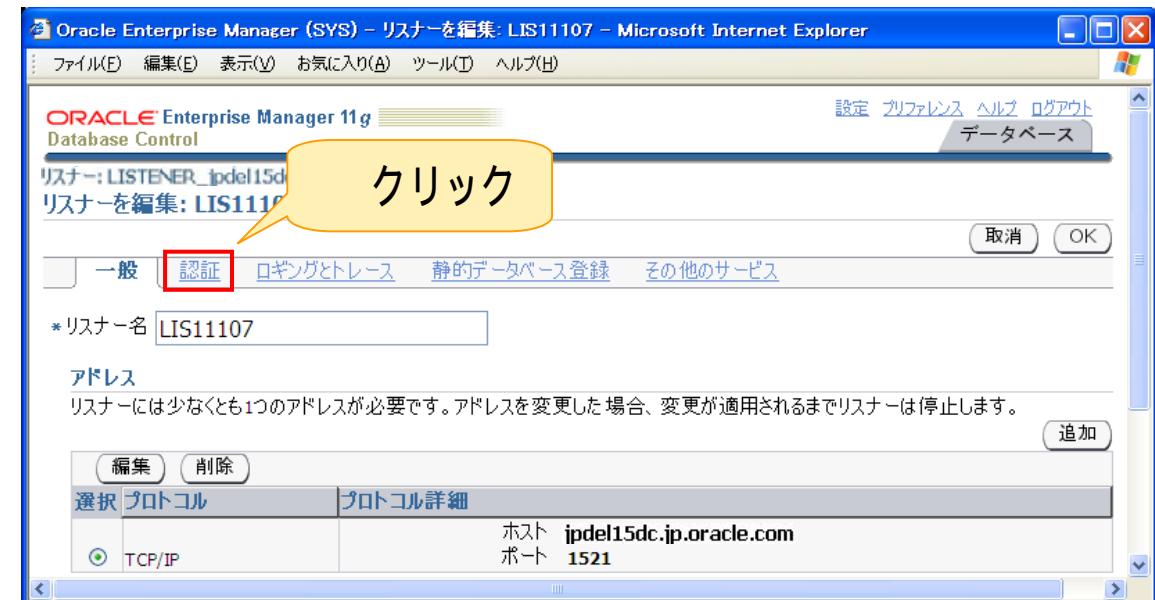
TNS ping(ミリ秒) ✓ 20
確立された接続数/分 0
拒否された接続数/分 0

ORACLE®

リスナーにパスワードを設定します

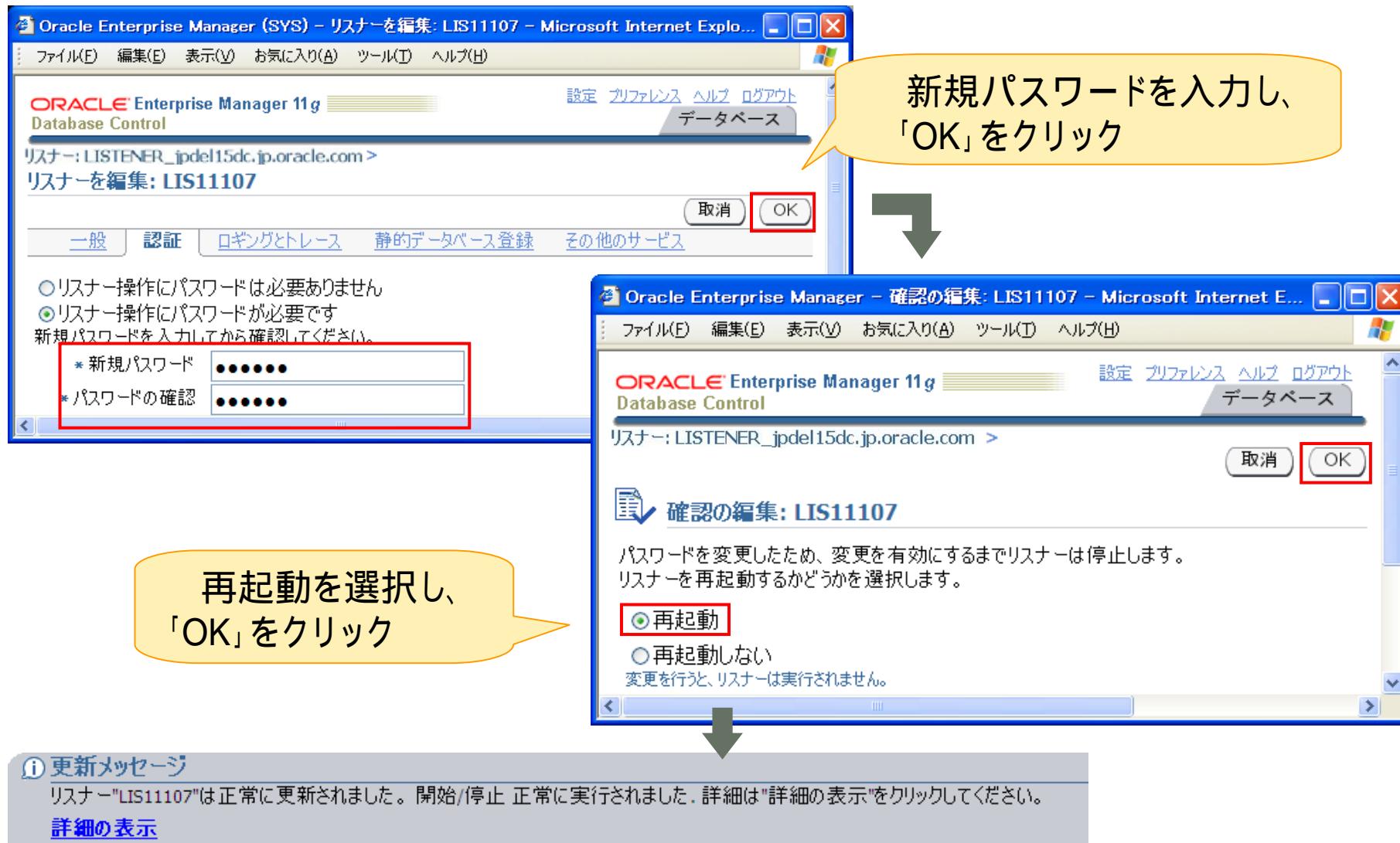


サーバーOSのユーザー名とパスワードを入力し、「ログイン」をクリック



ORACLE

リスナーにパスワードを設定します



ORACLE®

Agenda

- はじめに
- 初期状態からセキュアなデータベース
- 認証の管理
- 権限の管理
- 外部からのアクセス
- その他のセキュリティトピックス
- おわりに



ORACLE®

ビューを使用したアクセス制御

- ・ ビューとは1つ以上の表から選択されたデータを表現したものです
- ・ ビュー内には実際のデータは持ちません

従業員表

EMP_ID	EMP_NAME	SALARY
100	YAMADA	6000
101	KAWADA	5500
102	UMINO	4000
103	TSUTIYA	3000

SALARY列は一般ユーザにはアクセスさせたくない

ビュー

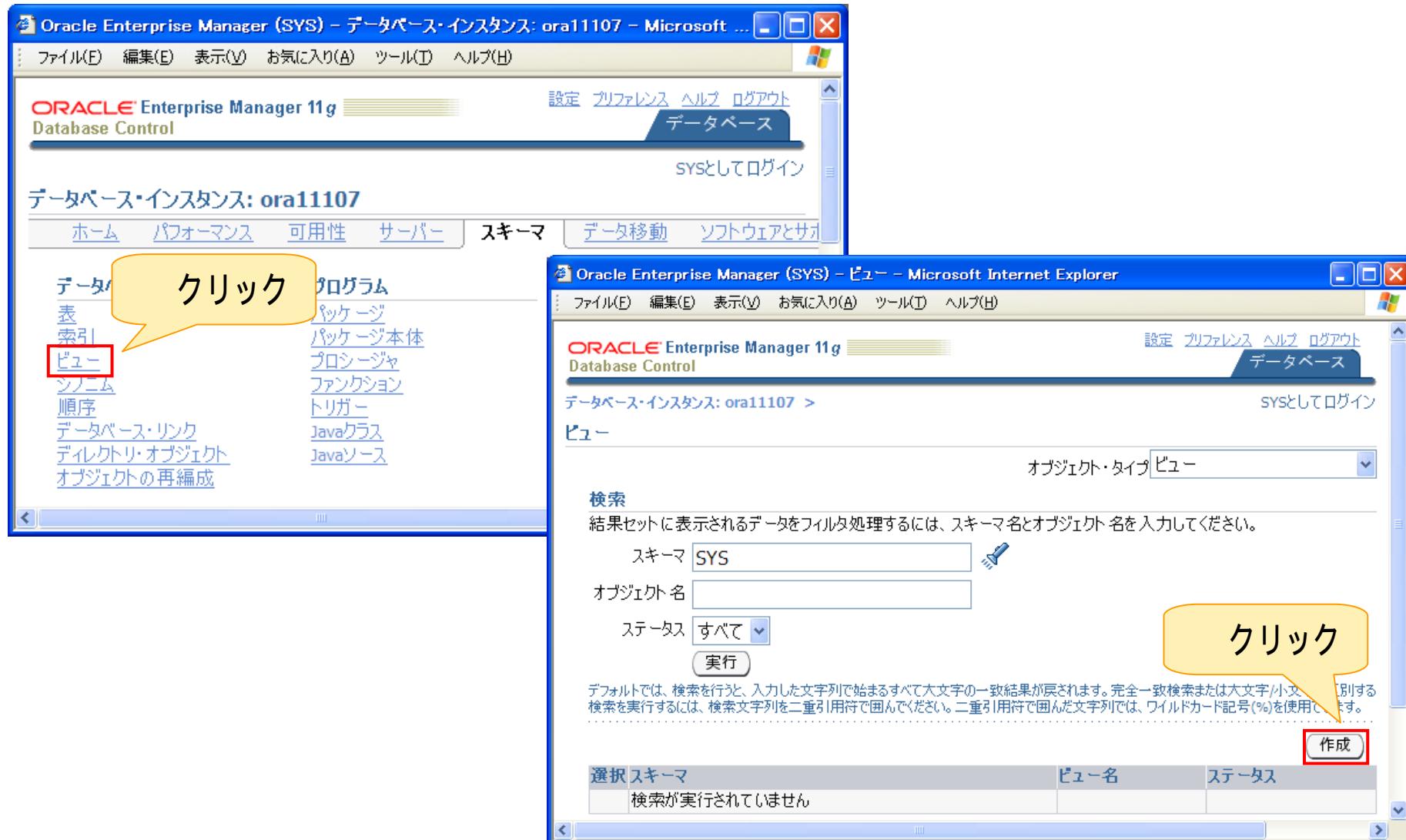
EMP_ID	EMP_NAME
100	YAMADA
101	KAWADA
102	UMINO
103	TSUTIYA

EMP_ID列とEMP_NAME列のみを含んだビューを作成し、ユーザーにはこのビューの参照権限のみを付与

ビューを使えば、実表へのアクセスを禁止しながら必要最低限の情報を参照させることができます

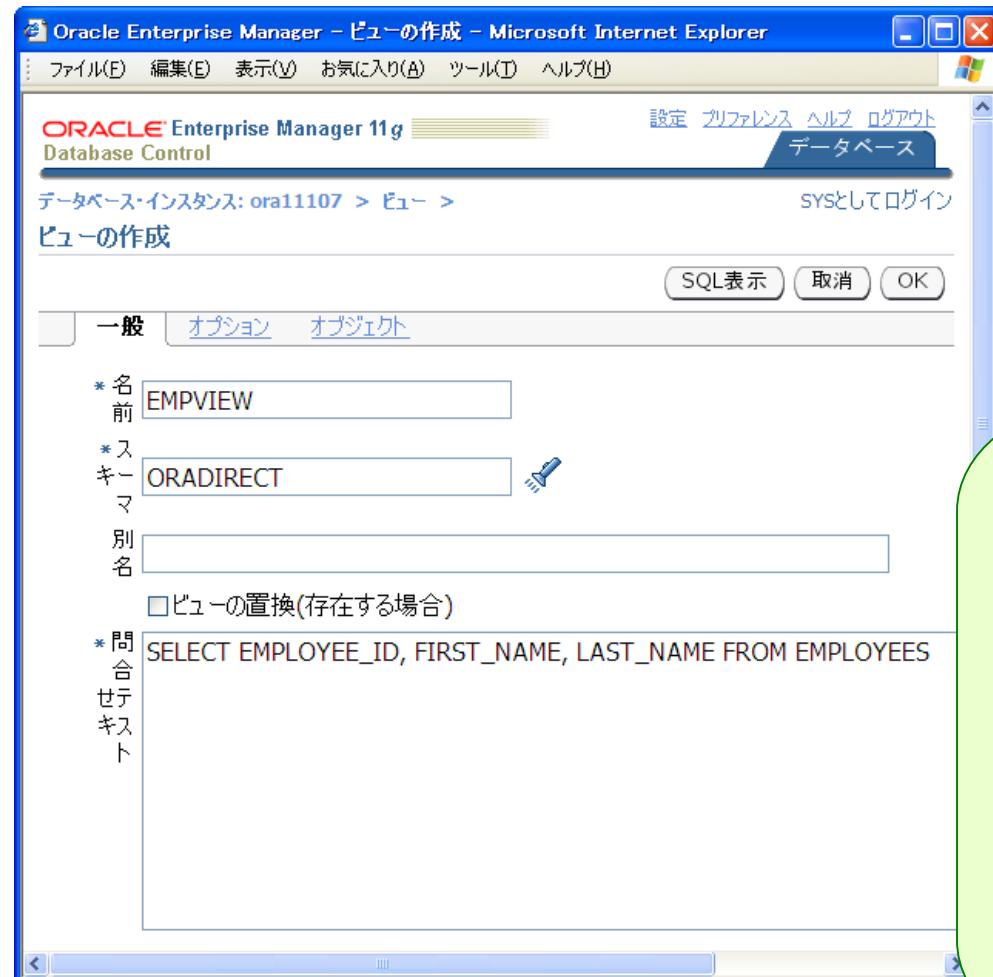
ORACLE®

EMPVIEWビューを作成します



ORACLE®

作成するビューの設定内容を入力します

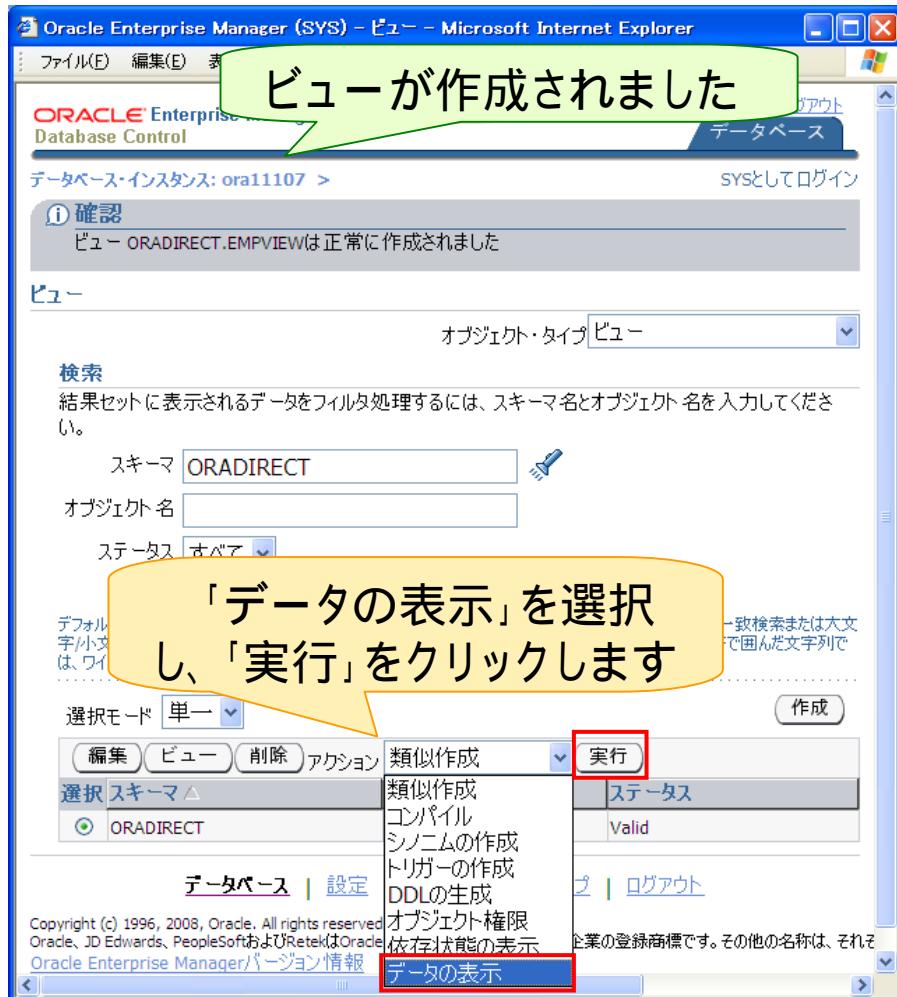


名前、スキーマ、問い合わせテキストを記述し、「OK」をクリックします

設定項目	設定内容
名前	EMPVIEW
スキーマ	ORADIRECT
問い合わせテキスト	SELECT EMPLOYEE_ID, FIRST_NAME, LAST_NAME FROM EMPLOYEES

ORACLE

作成したビューのデータを確認します



ビューのデータを表示できます

The screenshot shows the Oracle Enterprise Manager interface with a green callout bubble in the top right corner saying "ビューのデータを表示できます" (View data can be displayed). The main window displays the results of the query: SELECT "EMPLOYEE_ID", "FIRST_NAME", "LAST_NAME" FROM "ORADIRECT"."EMPVIEW". The results are listed in a table:

EMPLOYEE_ID	FIRST_NAME	LAST_NAME
100	Steven	King
101	Neena	Kochhar
102	Lex	De Haan
103	Alexander	Hunold
104	Bruce	Ernst
105	David	Austin
106	Valli	Pataballa
107	Diana	Lorentz
108	Nancy	Greenberg
109	Daniel	Faviet
110	John	Chen
111	Ismael	Sciarras
112	Jose Manuel	Urman
113	Luis	Popp
114	Den	Raphaely
115	Alexander	Khoo
116	Shelli	Baida
117	Sigal	Tobias

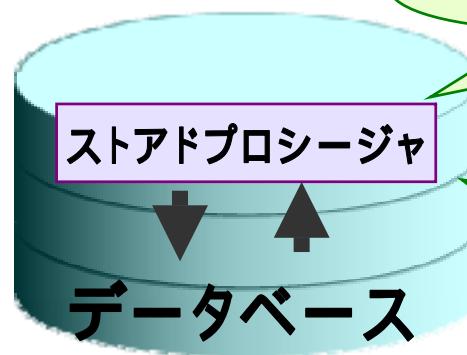
ストアド・プロシージャを使用したセキュリティ管理

- ストアド・プロシージャを使うと、業務運用に応じた柔軟な権限制限を実現することができます

EMPLOYEES表

EMPLOYEE_NAME	ADDRESS	SALARY
...

人事部門 担当者 →



EMPLOYEES表のEMPLOYEE_NAMEとADDRESSのみを、勤務時間内のみに更新を許可するプロシージャ

プロシージャのみに権限を付与
(担当者単位には権限を付与せずに)

人事部門の担当者が権限を使用できるのはプロシージャのコンテキスト内のみになり、EMPLOYEES表を直接更新することはできなくなります

初期化パラメータ

代表的な2つのセキュリティ関連の初期化パラメータ

- O7_DICTIONARY_ACCESSIBILITY (11gのデフォルト値はFALSEです)
 - このパラメータは、システム権限を制限します
 - FALSE に設定: データ・ディクショナリを保護します
 - TRUE に設定: SYS スキーマ内のオブジェクトへのアクセスが可能になります
(ANY 権限を持つ不正なユーザーがデータ・ディクショナリ表
にアクセスし、変更する危険性があります)
- REMOTE_OS_AUTHENT (11gのデフォルト値はFALSEです)
 - OS のユーザー名によるユーザー認証が行われるようになり、
これによって全てのクライアントを暗黙的に許可するようになります
 - 全てのクライアントが信頼できる環境にある場合を除いては
FALSE に設定することをおすすめします

セキュリティ関連のその他のパラメータについては、「2 日でセキュリティ・ガイド」の各章末を参考にしてください

http://otndnld.oracle.co.jp/document/products/oracle11g/111/doc_dvd/server.111/E05781-03/toc.htm



おわりに

1. 初期状態からセキュアなデータベース

構築直後から高いセキュリティを保つ

4. 外部からのアクセス

リスナーにパスワード設定可能

2. 認証の管理

不要なユーザを使用可能にしない

3. 権限の管理

必要最低限の権限のみを付与する

5. その他のセキュリティトピックス

ビューとストアドプロシージャでセキュリティ強化





年末ダイセミ受講感謝キャンペーン

Oracle Direct Seminarを御愛護頂き、誠にありがとうございます。感謝の気持ちを込めまして、**合計100名様**にWendy2010年版カレンダーをプレゼントいたします。11月・12月に開催のダイセミを2つ以上受講頂いた方が対象です。是非皆様奮ってご応募下さい!!

プレゼントの送付先は、セミナ登録時にご登録されている貴社住所宛てに送付させて頂きます。お客様の登録情報に、a.貴社名、b.部署名、c.役職名、d.住所が正しく登録されていることをご確認ください。a,b,c,dの情報が**正しく登録されていない場合はご応募が無効となります**のでご注意下さい。お客様情報の変更はこちらから実施頂けます。

<http://www.oracle.com/technology/global/jp/membership/index.html>

応募方法



ORD_SEMINAR_JP@ORACLE.COM

[タイトル]年末カレンダー応募

[必要情報]

- 1、ご登録の氏名
- 2、ご登録の貴社名、所属部署名
- 3、受講された2009年11月・12月開催のセミナタイトル
- 4、現在ご検討中のシステムについてなど、Oracle Directに相談されたいことなどございましたら記載ください。

必要情報を明記のうえ、メールでご応募ください。当選者の発表は発送をもってかえさせて頂きます。



ORACLE

OTN×ダイセミ でスキルアップ!!



- ・技術的な内容について疑問点を解消したい！
- ・一般的なその解決方法などを知りたい！
- ・セミナ資料など技術コンテンツがほしい！

Oracle Technology Network(OTN)を御活用下さい。

<http://otn.oracle.co.jp/forum/index.jspa?categoryId=2>

セミナーに関連する技術的なご質問は、OTN掲示版の
「データベース一般」へ

OTN掲示版は、基本的にOracleユーザー有志からの回答となるため100%回答があるとは限りません。

ただ、過去の履歴を見ると、質問の大多数に関してなんらかの回答が書き込まれております。

<http://www.oracle.com/technology/global/jp/ondemand/otn-seminar/index.html>

過去のセミナ資料、動画コンテンツはOTNの
「OTNコンテンツ オン デマンド」へ

セミナ事務局にダイセミ資料を請求頂いても、お受けできない可能性がございますので予めご了承ください。
ダイセミ資料はOTNコンテンツ オン デマンドか、セミナ実施時間内にダウンロード頂くようお願い致します。

ORACLE®

ITプロジェクト全般に渡る無償支援サービス Oracle Direct Conciergeサービスメニュー

システム運用状況の診断

- [パフォーマンス・クリニック・サービス](#)
- [システム・セキュリティ診断サービス](#)
- [データ管理最適化サービス](#)

構築

設計

運用

IT企画

経営企画

システム構築時の道案内

- [Access / SQL Serverからの移行](#)
- [MySQL / PostgreSQLからの移行](#)
- [Oracle Database バージョンアップ支援](#)
- [Oracle Developer Webアップグレード](#)
- [システム連携アセスメントサービス](#)

業務改善計画の作成支援

- [業務診断サービス](#)
- [BIアセスメントサービス](#)

システム企画の作成支援

- [業務診断サービス](#)
- [BIアセスメントサービス](#)

RFP / 提案書の作成支援

- [BIアセスメントサービス](#)
- [メインフレーム資産活用相談サービス](#)
- [仮想化アセスメントサービス](#)
- [Oracle Database 構成相談サービス](#)
- [Oracle Database 高可用性クリニック](#)

ORACLE®



あなたにいちばん近いオラクル

Oracle Direct

まずはお問合せください

Oracle Direct

検索

システムの検討・構築から運用まで、ITプロジェクト全般の相談窓口としてご支援いたします。

システム構成やライセンス/購入方法などお気軽にお問い合わせ下さい。

Web問い合わせフォーム

専用お問い合わせフォームにてご相談内容を承ります。

http://www.oracle.co.jp/inq_pl/INQUIRY/quest?rid=28

フォームの入力には、Oracle Direct Seminar申込時と同じ
ログインが必要となります。

こちらから詳細確認のお電話を差し上げる場合がありますので、ご登録さ
れている連絡先が最新のものになっているか、ご確認下さい。

フリーダイヤル

0120 - 155 - 096

月曜~金曜 9:00~12:00、13:00~18:00

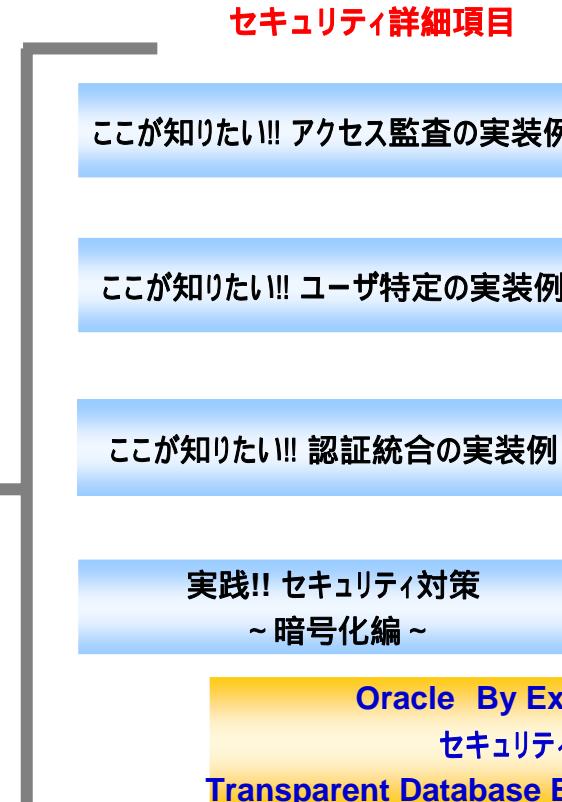
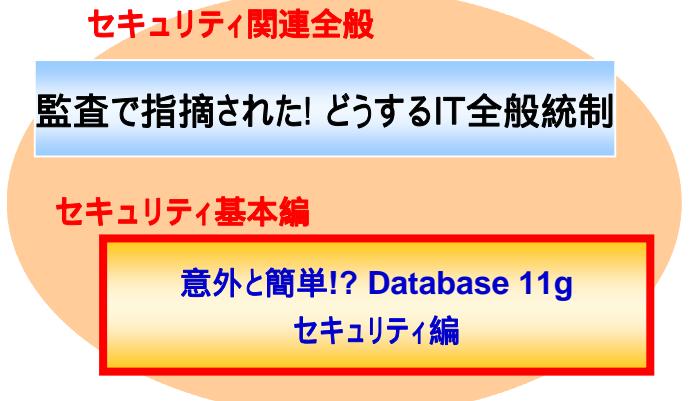
(祝日および年末年始除く)

ORACLE®

Oracle Direct Seminar コースフロー セキュリティ編

Oracle Direct Seminar

OTNコンテンツ



OTN(Oracle Technology Network) 無料技術情報公開サイト。

・意外と簡単!? シリーズ:スキルアップ講座:初心者向け講座

<http://www.oracle.com/technology/global/jp/columns/index.html>

ORACLE®



日本オラクル株式会社 無断転載を禁ず

この文書はあくまでも参考資料であり、掲載されている情報は予告なしに変更されることがあります。

日本オラクル社は本書の内容についていかなる保証もいたしません。また、本書の内容に関連したいかなる損害についても責任を負いかねます。

Oracle、PeopleSoft、JD Edwards、及びSiebelは、米国オラクル・コーポレーション及びその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標の可能性があります。