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

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

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をできるようになる

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

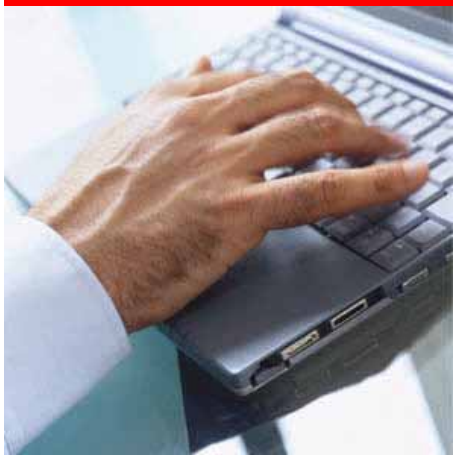
- **データベースの初期構成**
- **認証の管理**
- **権限の管理**
- **外部からのアクセス**
- **その他**

- **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

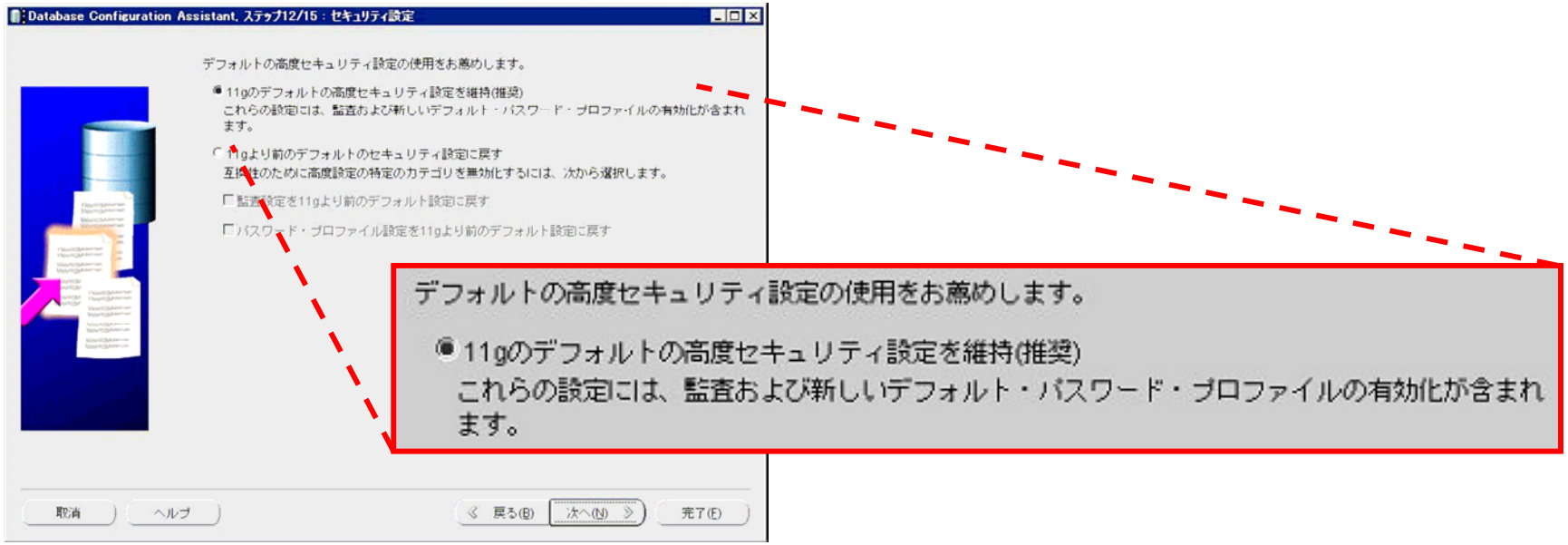
Agenda



- 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

初期状態からセキュアなデータベース

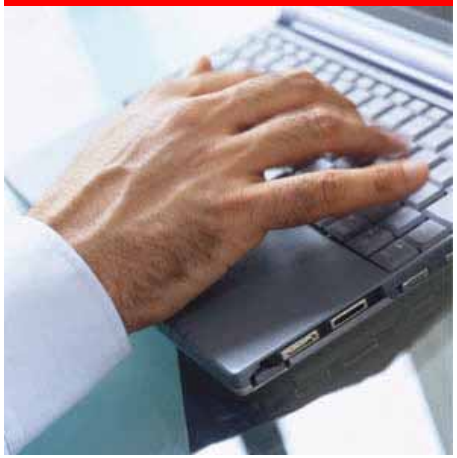
- Database Configuration Assistant(DBCA)にて
  データベースの構成を行う際のセキュリティ設定画面



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

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

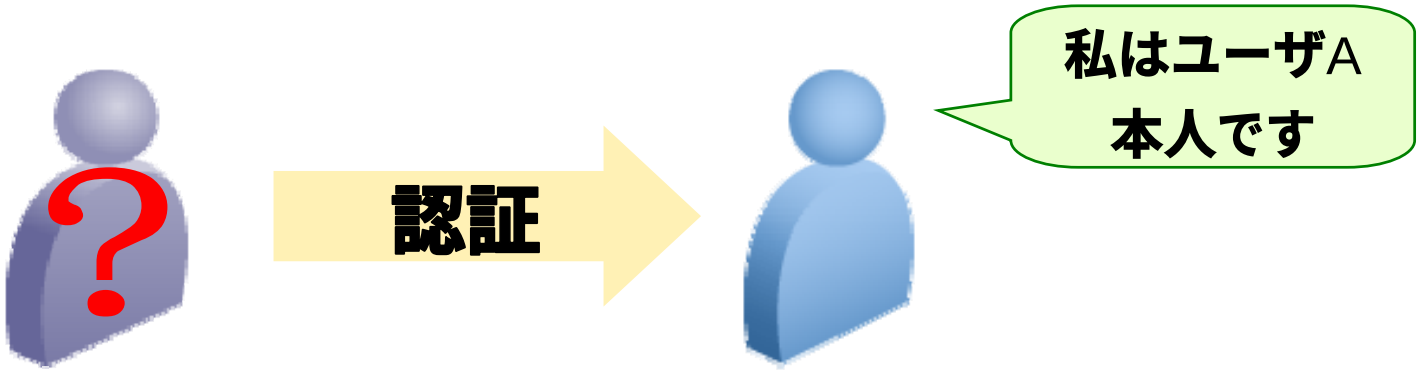
認証の管理

- 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

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

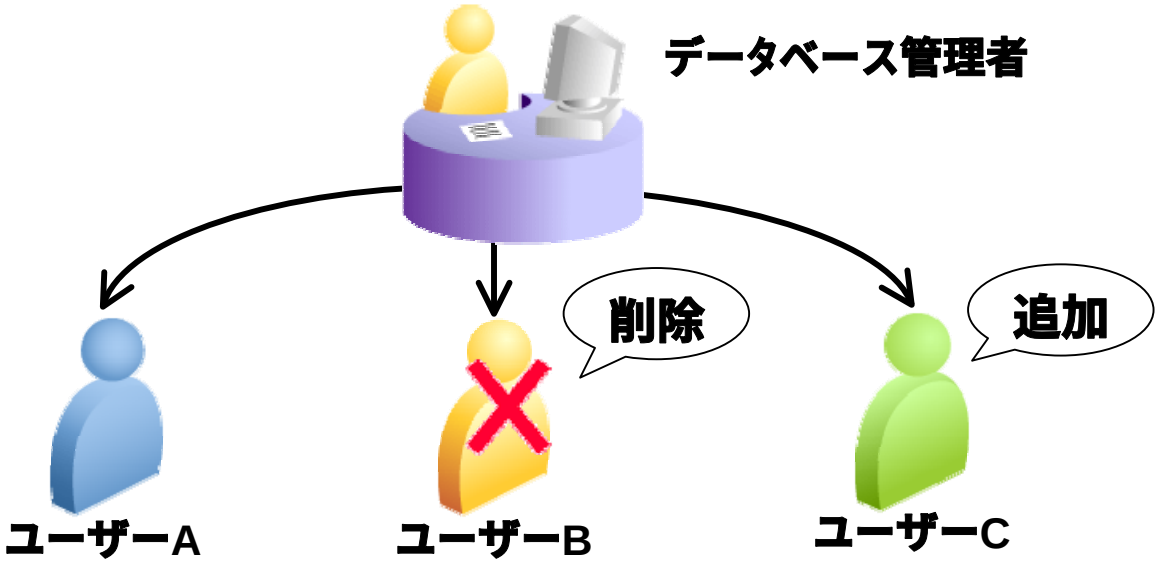


Oracleには次の認証方法が用意されています

- 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

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

①ユーザ名、パスワード、接続モードを選択し、「ログイン」をクリック

ユーザーの管理を行う際は、管理者権限を持つユーザーでログインする必要があります。

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

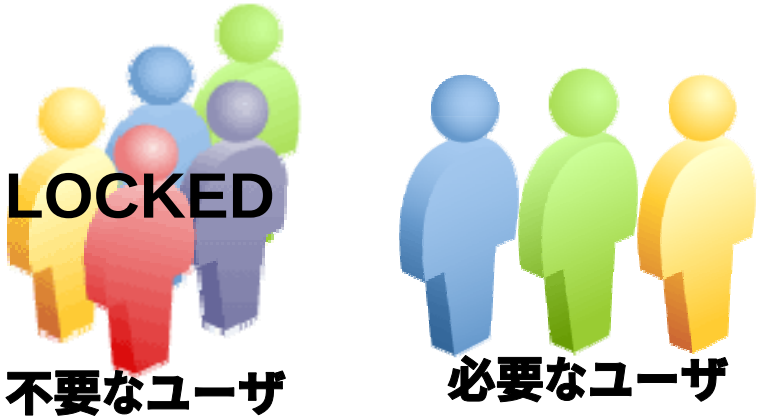
この画面から、ユーザーアカウントの管理作業を行っていただけます

- 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

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やサンプル用のユーザが作成され、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

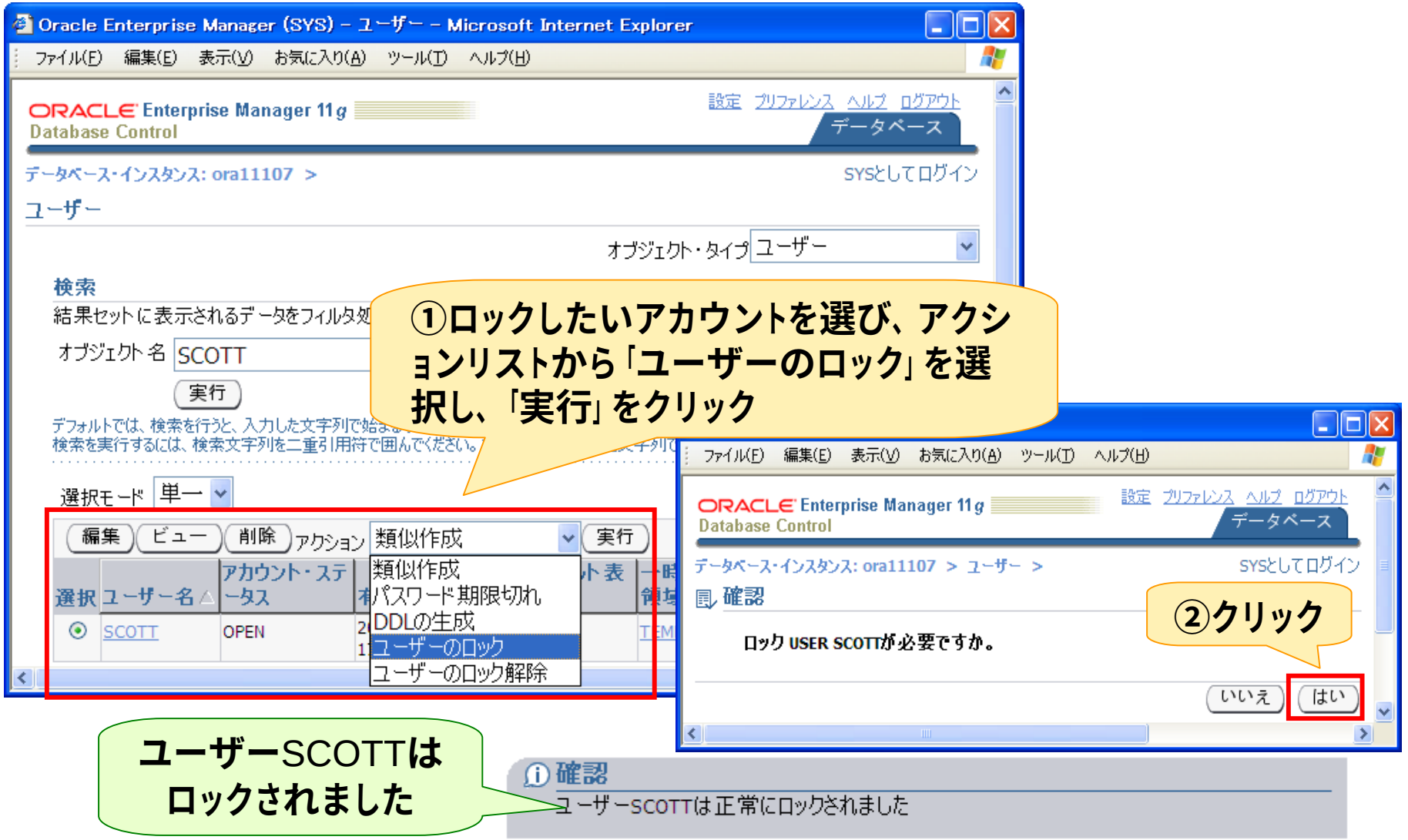
ユーザーHRのロックを解除します

ユーザーHRのロックが解除されました

確認

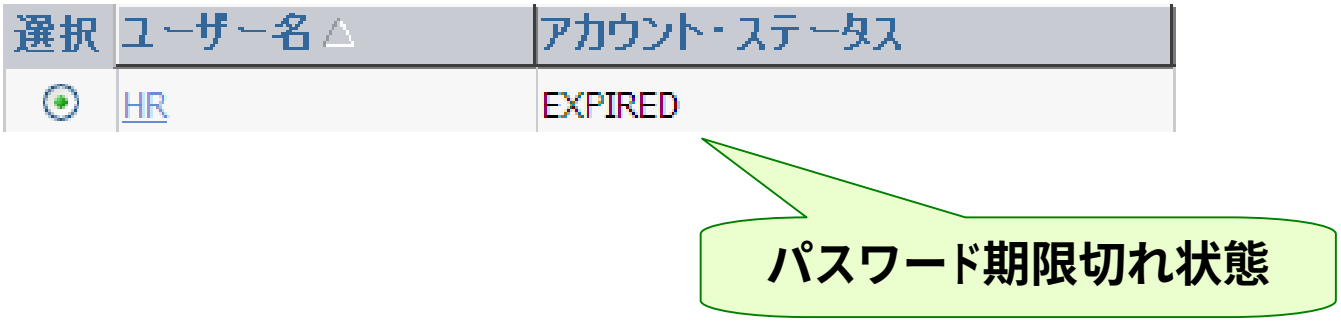
ユーザーHRは正常にロック解除されました

ユーザーSCOTTのアカウントをロックします



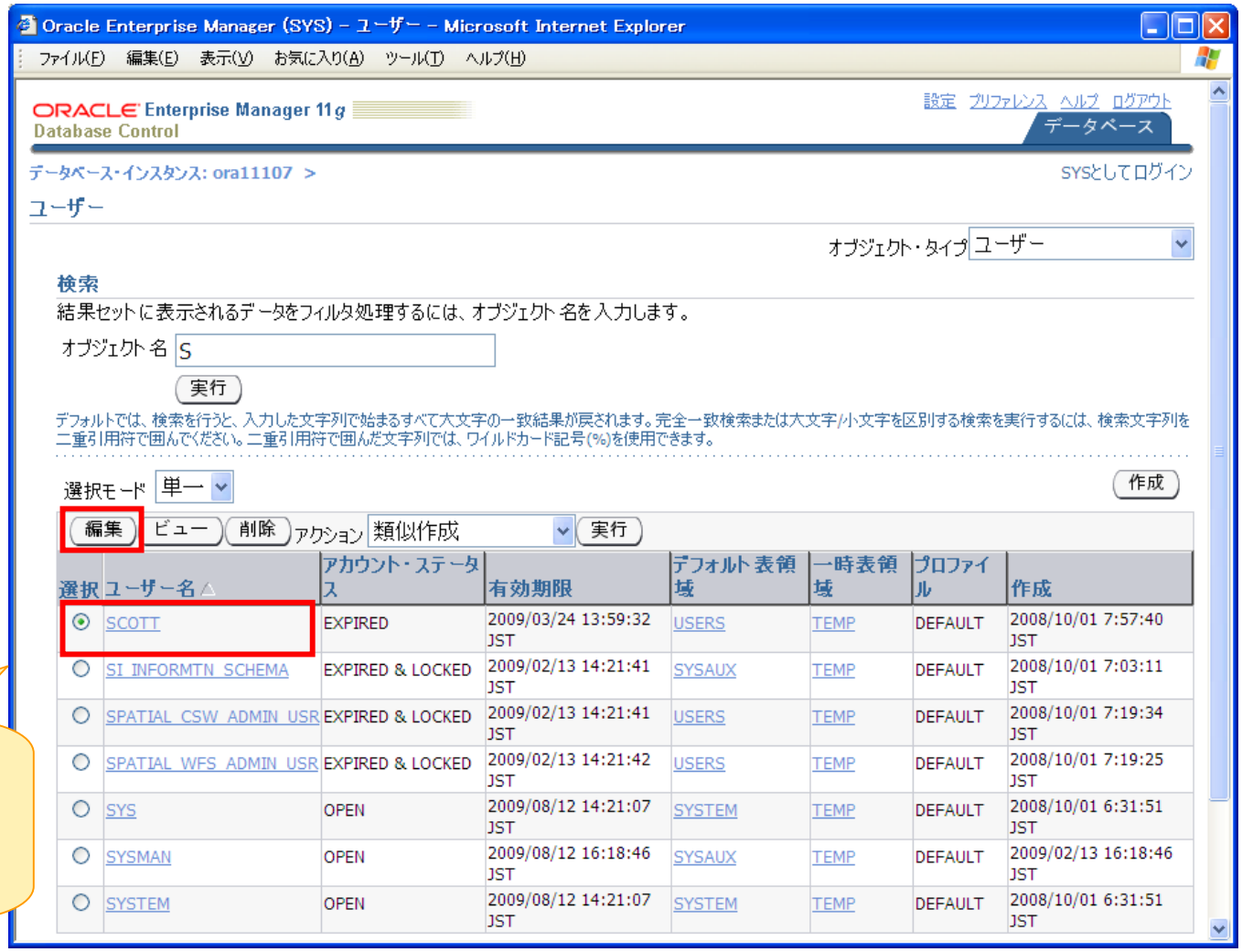
パスワードの変更について

- 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



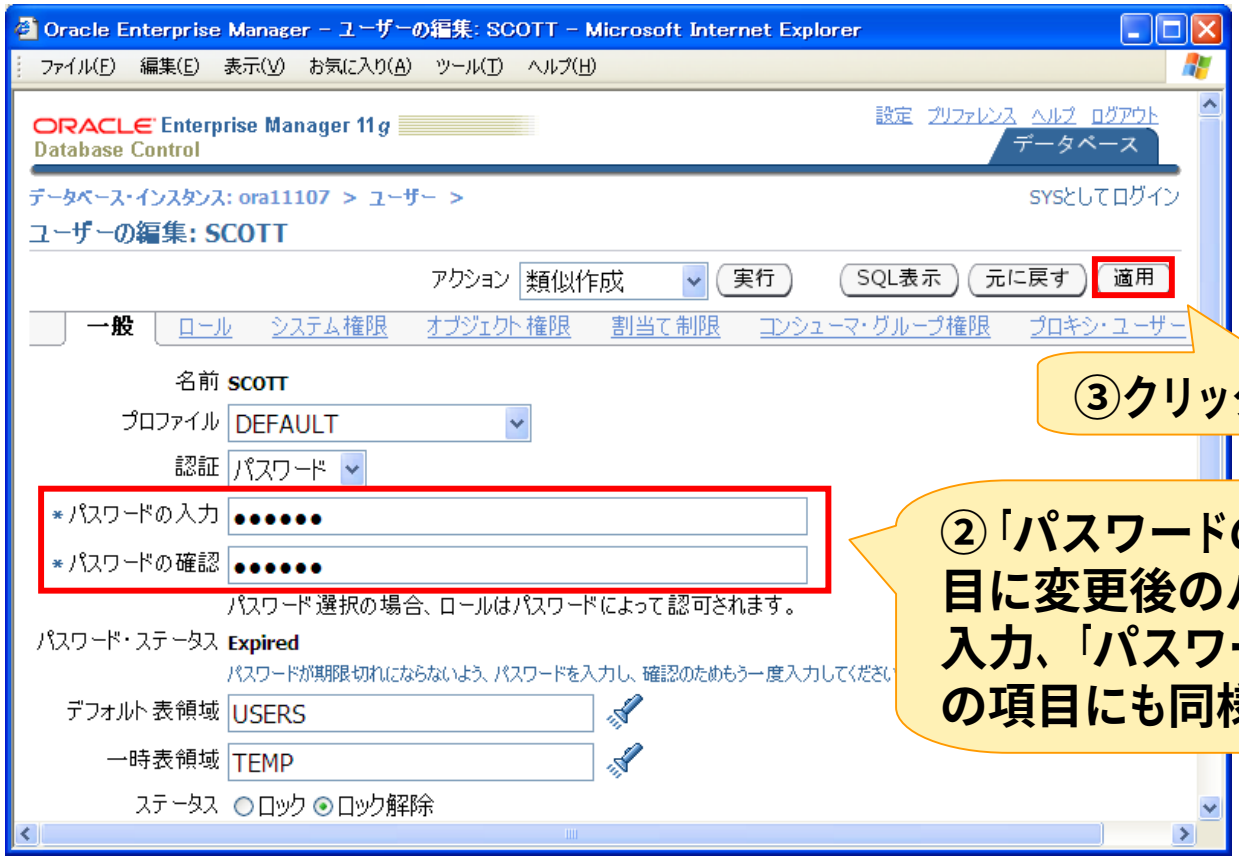
データベース作成時に同一のパスワードを使用するように設定している場合にも、適切にパスワードを変更しておくことをお勧めします

パスワードを変更したいユーザーを選択します

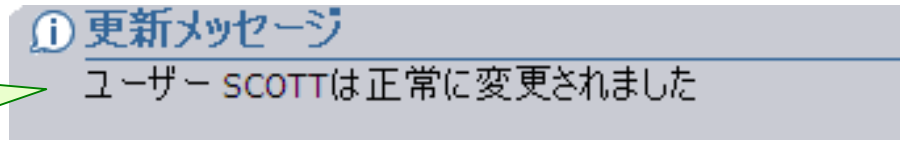


①パスワードを変更したいアカウントを選び、「編集」をクリック

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



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

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)

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

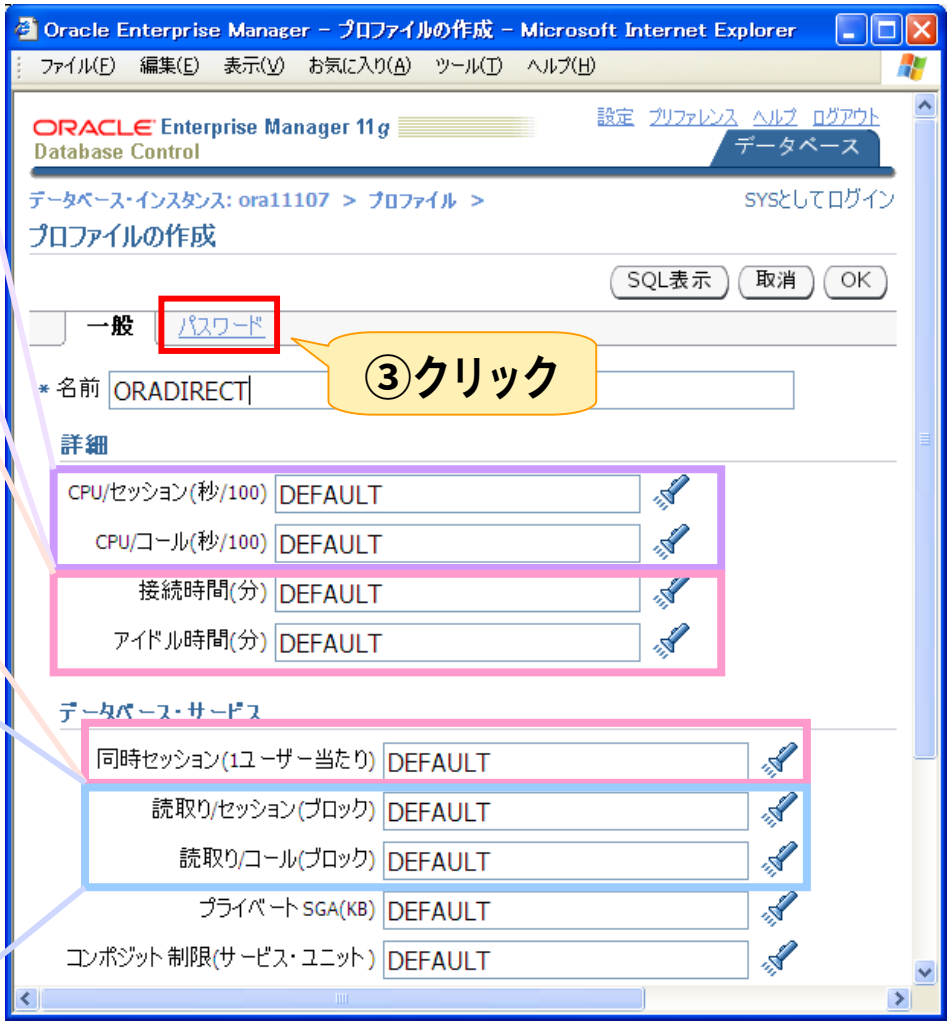
プロファイル作成時の「一般」タブの画面

- 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

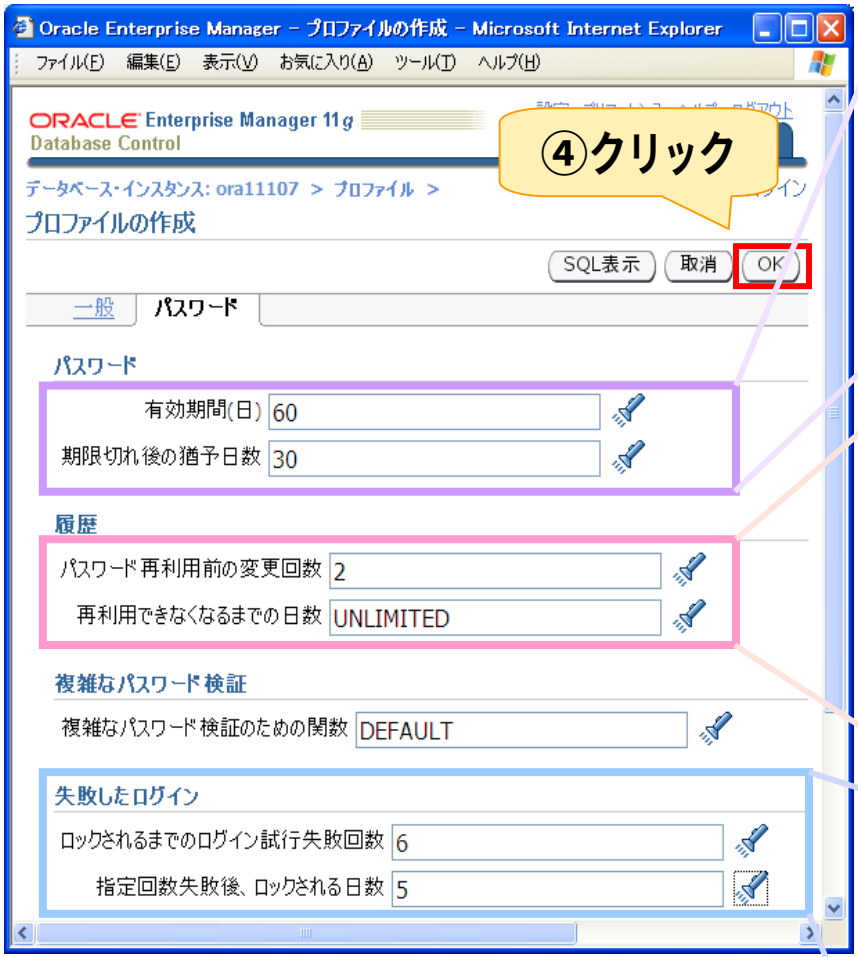
CPU:
CPUリソースは、セッションごと
またはコールごとに制限できます

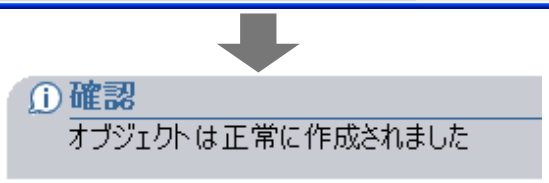
ネットワーク/メモリー:
接続時間やアイドル時間、
同時セッションなどを設定できます

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



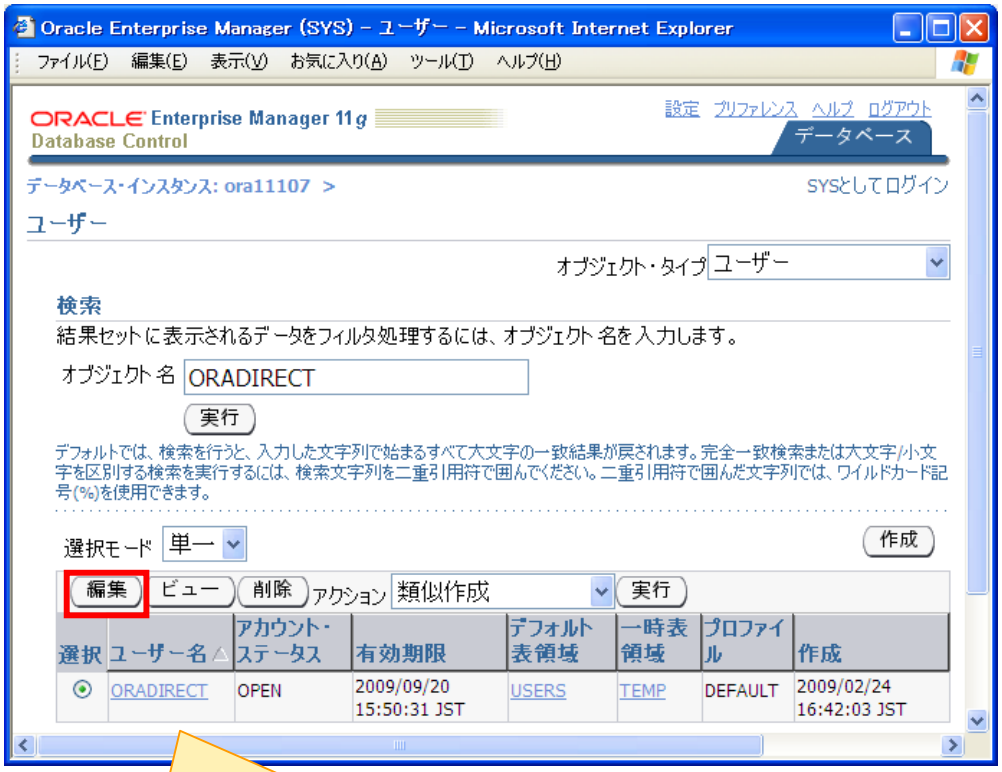


有効期限（日）：60
設定したパスワードは60 日間使用可能
期限切れ後の猶予日数 30
有効期限が切れた後、
30日間は同じパスワードを使用可能

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

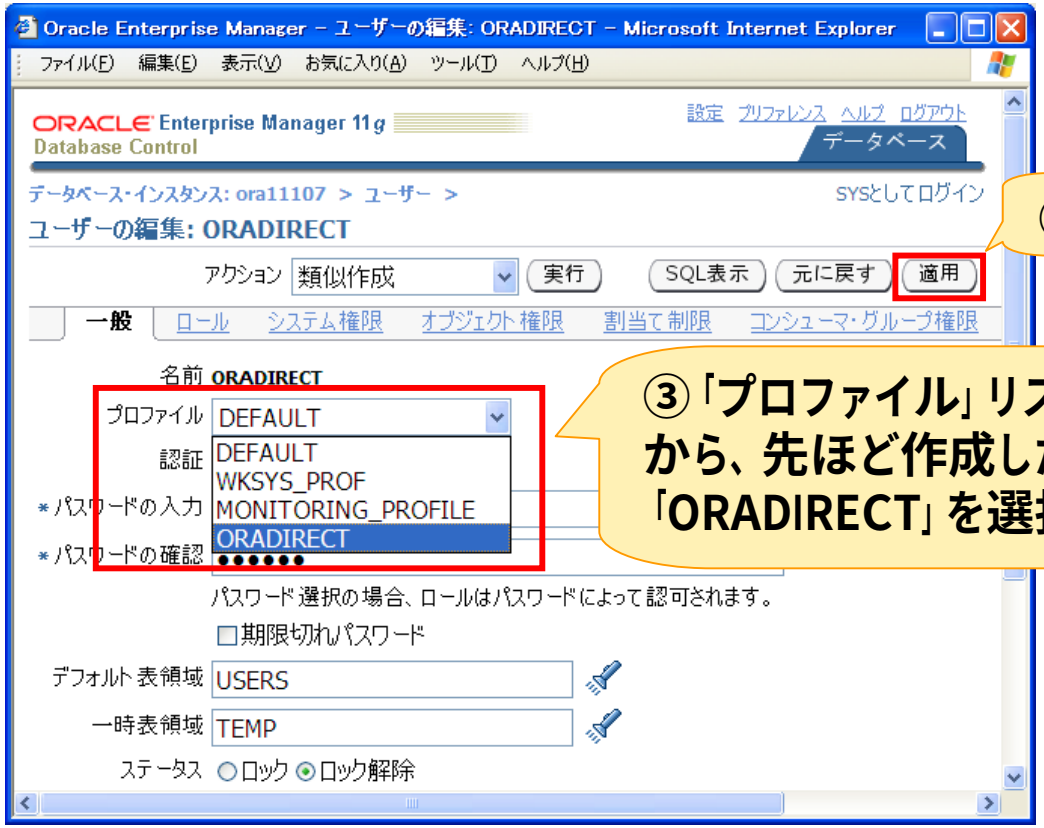
ロックされるまでのログイン試行失敗回数：6
6回ログインを失敗するとユーザーがロックされます
指定回数失敗後、ロックされる日数：5
ロックされた後で5 日間経過するとロック解除されます

新しいプロファイルをORADIRECTユーザーに割り当てます



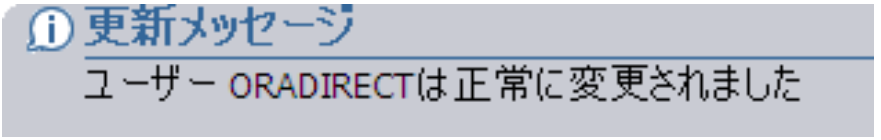
②ユーザー一覧の中から「ORADIRECT」を選択し、「編集」をクリック

ORADIRECTユーザーに割り当てるプロファイルを選択します

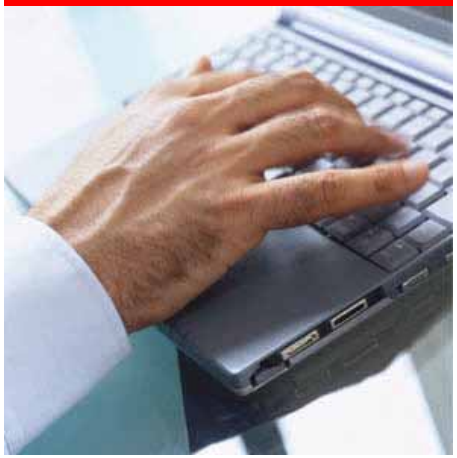


④クリック

③「プロファイル」リストの中から、先ほど作成した「ORADIRECT」を選択します



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

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

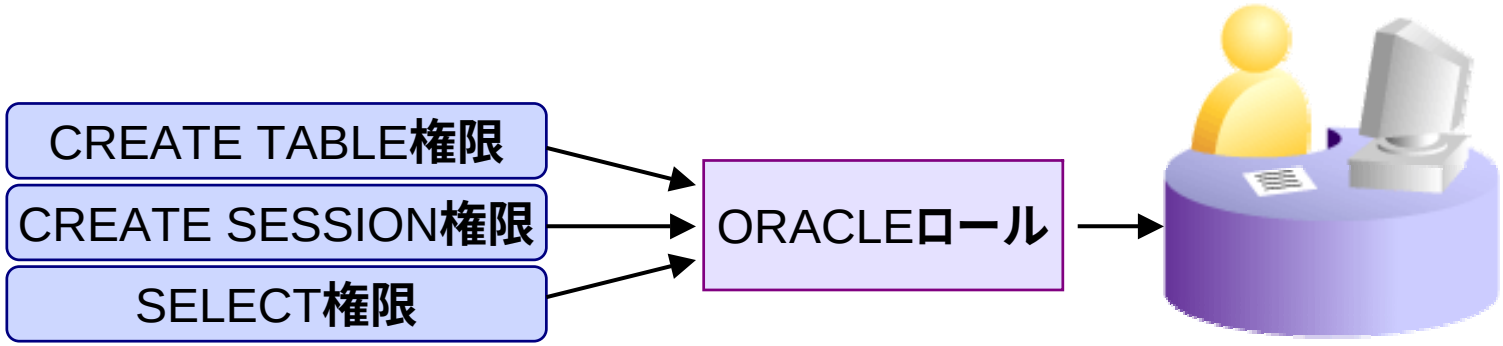
オブジェクト権限

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を**ロール**といいます

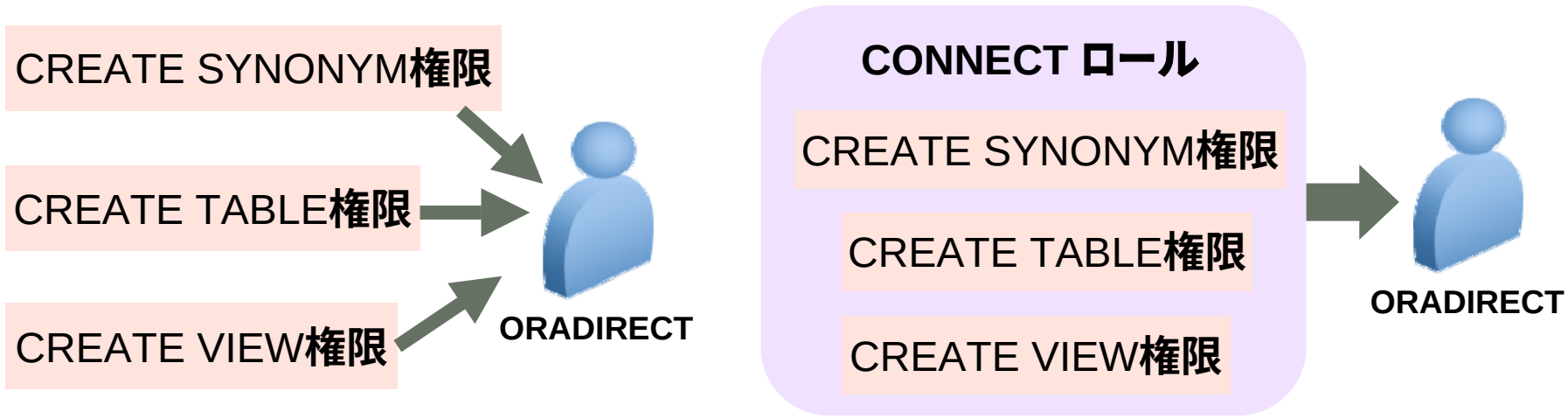
ロールとは、特定の権限の集合を持つユーザーの論理グループのことです



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、シノニムを作成する権限を付与したい場合



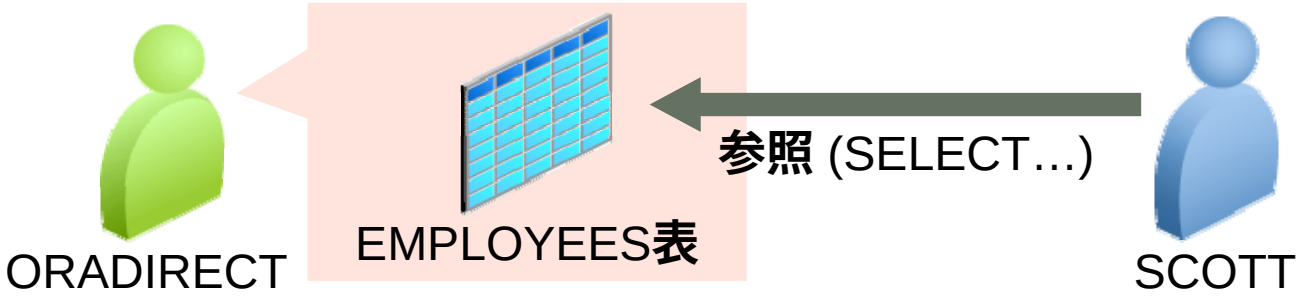
ロールを使用すると、一括して権限の管理が行えるため効率的です

権限の管理

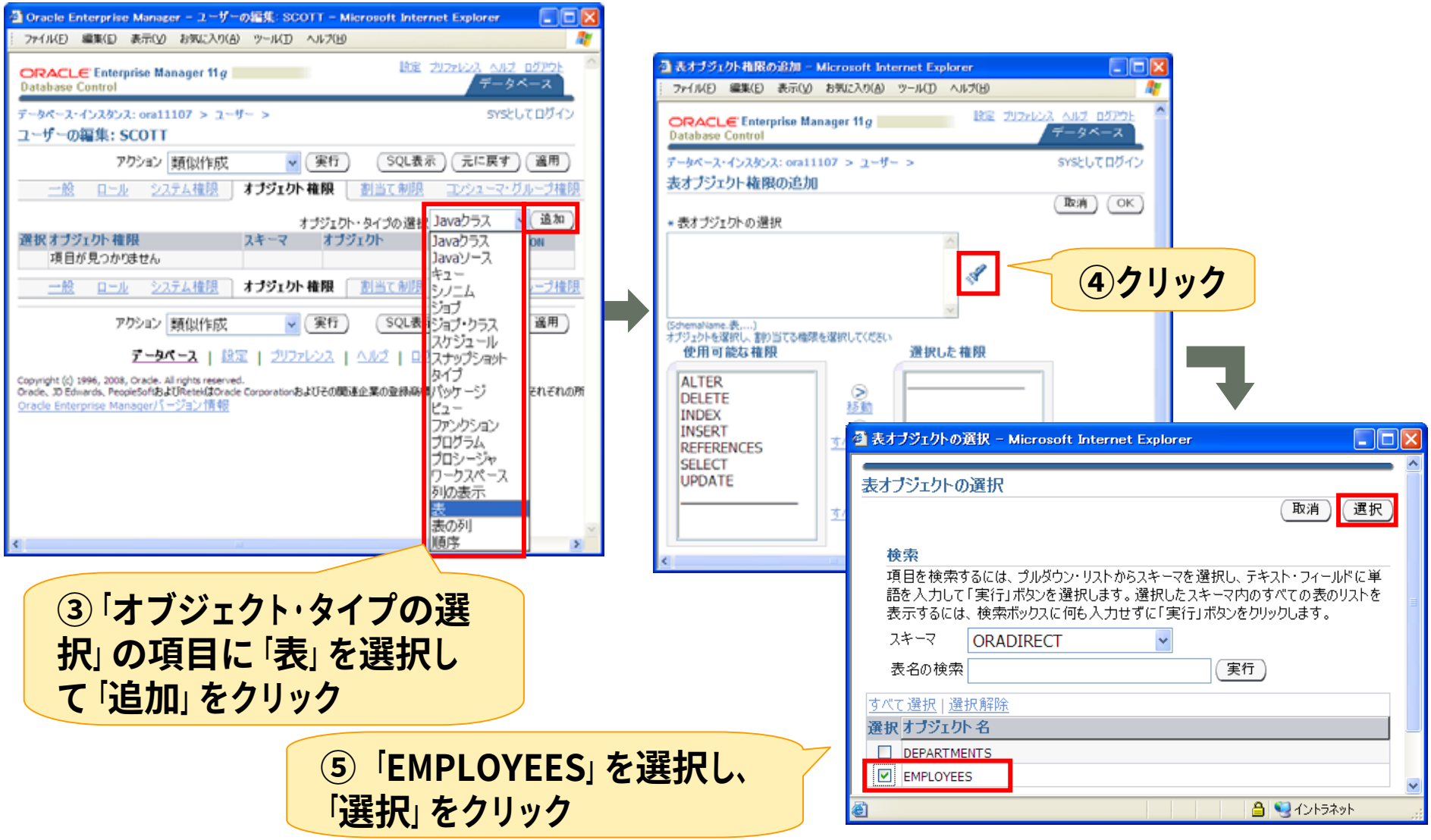
- 権限の種類
- 権限の付与
- 権限の許可、拒否、取り消し
  - EM EMによる権限の割り当て
- ユーザー定義のデータベースロール
  - EM ユーザー定義ロールを作成する
- ロールによる権限管理の簡素化
  - EM ユーザーにロールを割り当てる
- PUBLICロール

Enterprise Manager
を使った設定方法を
解説します

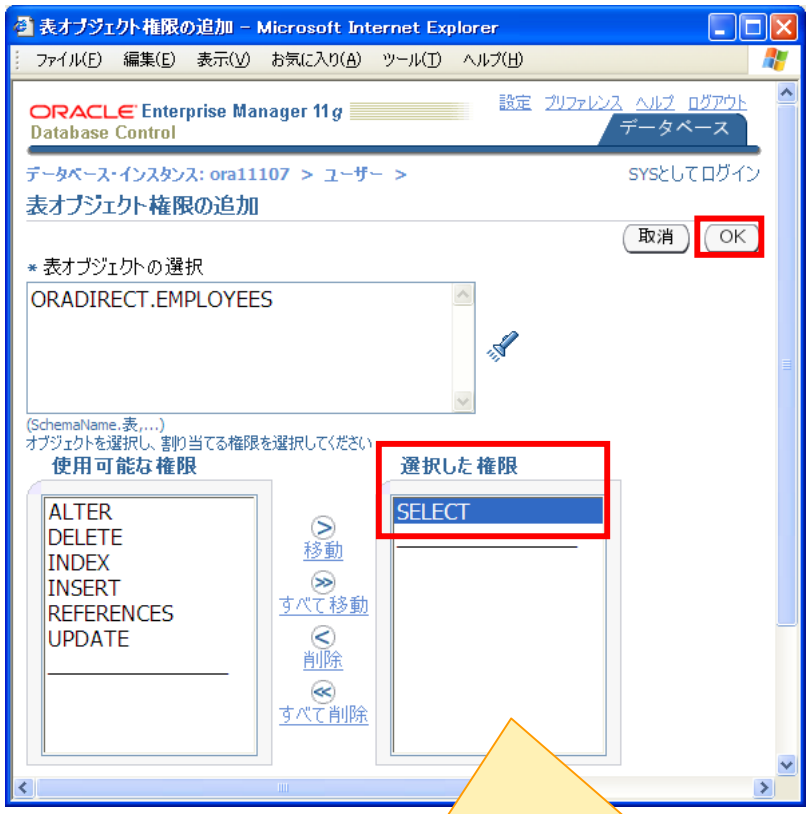
SCOTTユーザーにORADIRECTスキーマのEMPLOYEES表のSELECT権限を割り当てます



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



⑥ 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

OPTIONが指定されている権限について

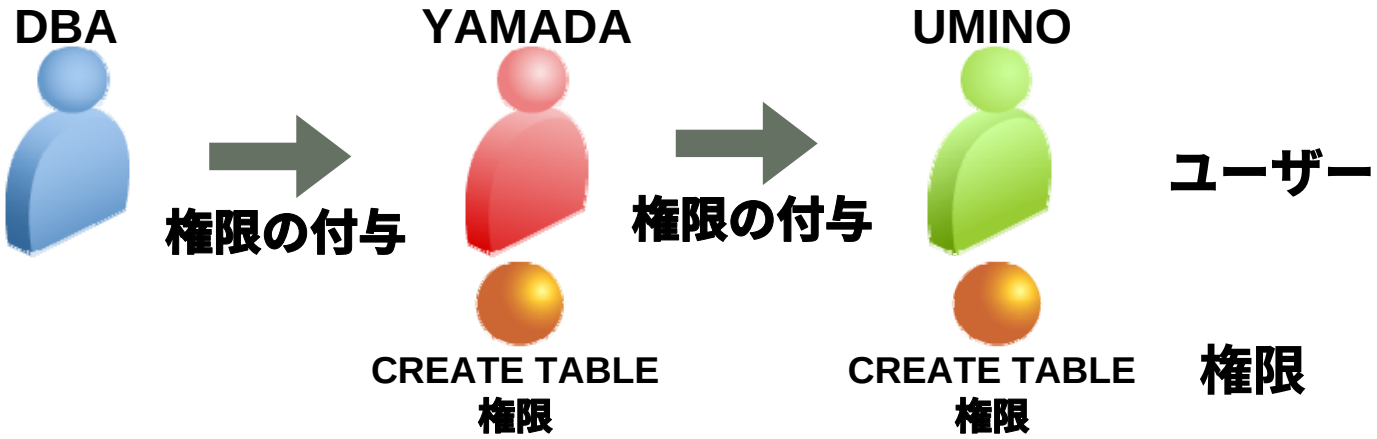
- **システム権限**

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**

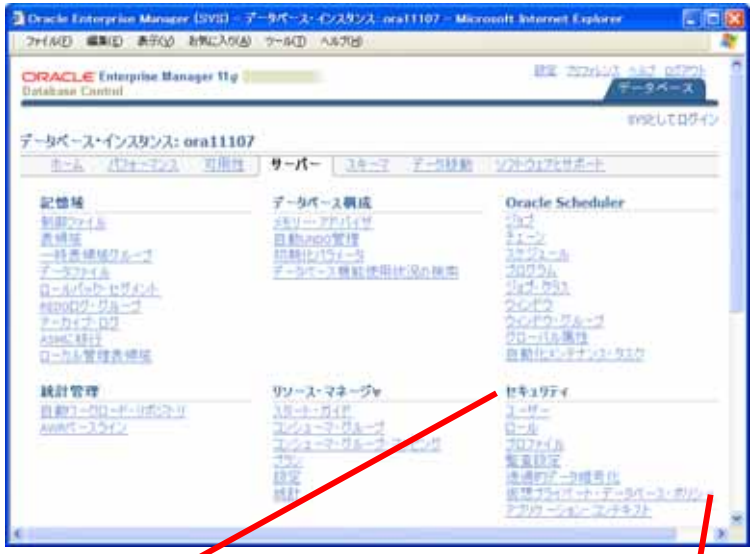
- **オブジェクト権限**

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**



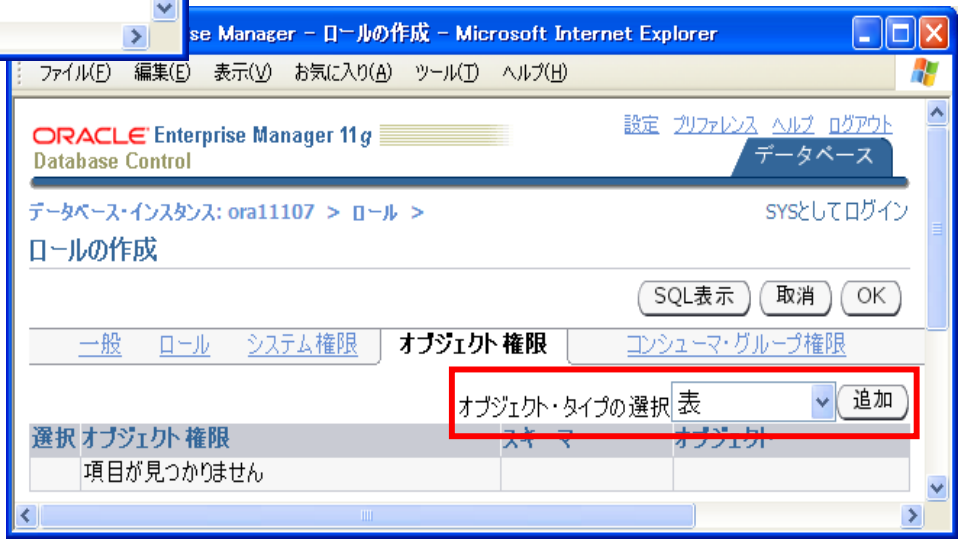
ユーザー定義のロールを作成します



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

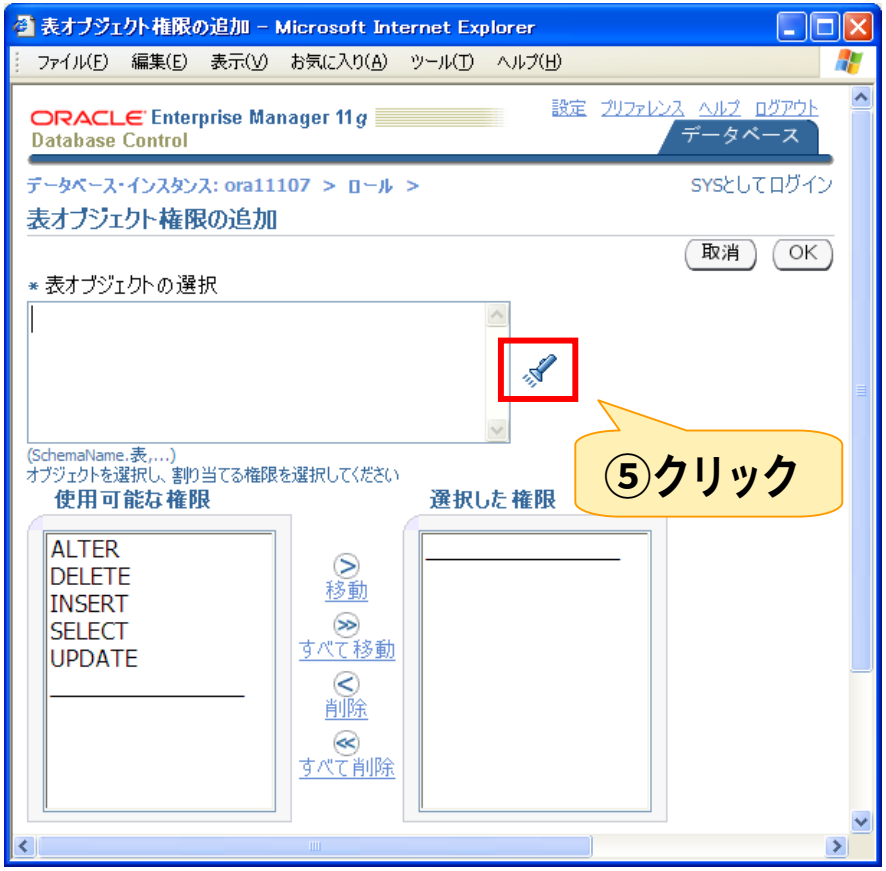
ロール名とオブジェクト・タイプを設定します

③名前の項目に「ORAROLE」を入力し、「オブジェクト権限」のタブをクリック



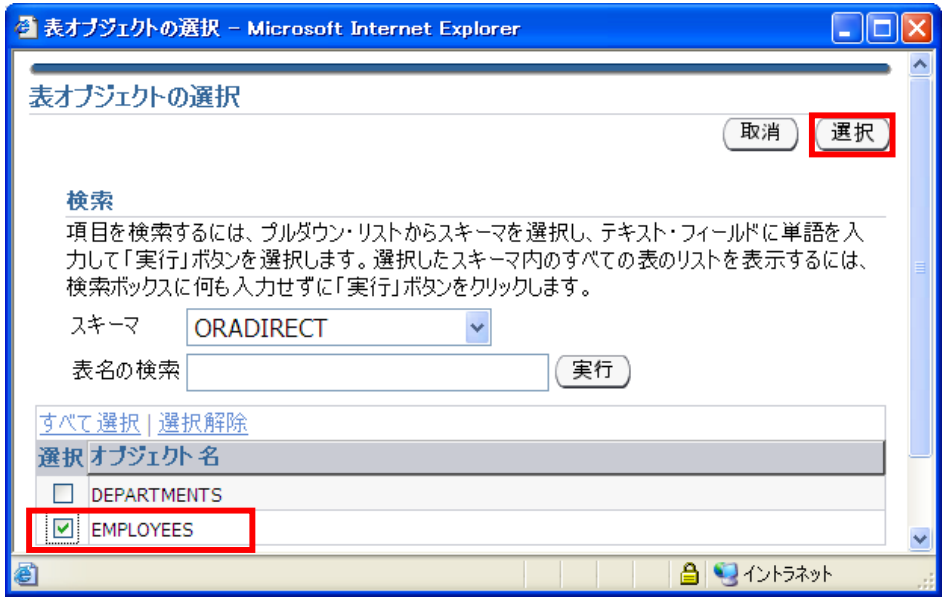
④オブジェクト・タイプの選択から「表」を選び、「追加」をクリック

表オブジェクトを設定します

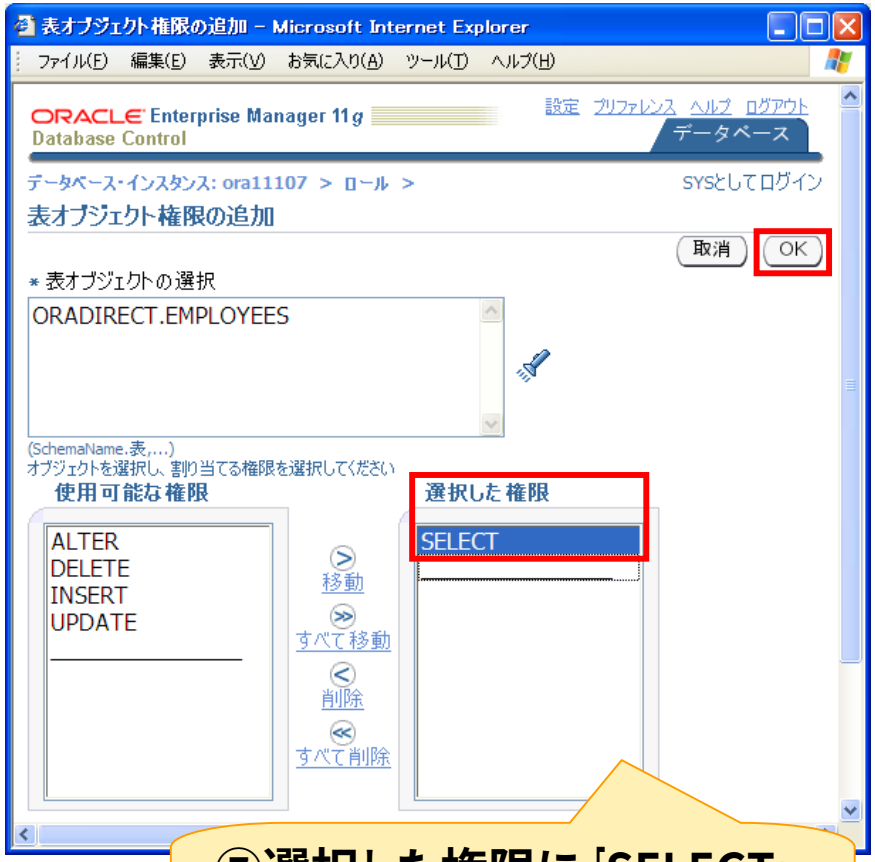


⑤クリック

⑥ORADITECT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

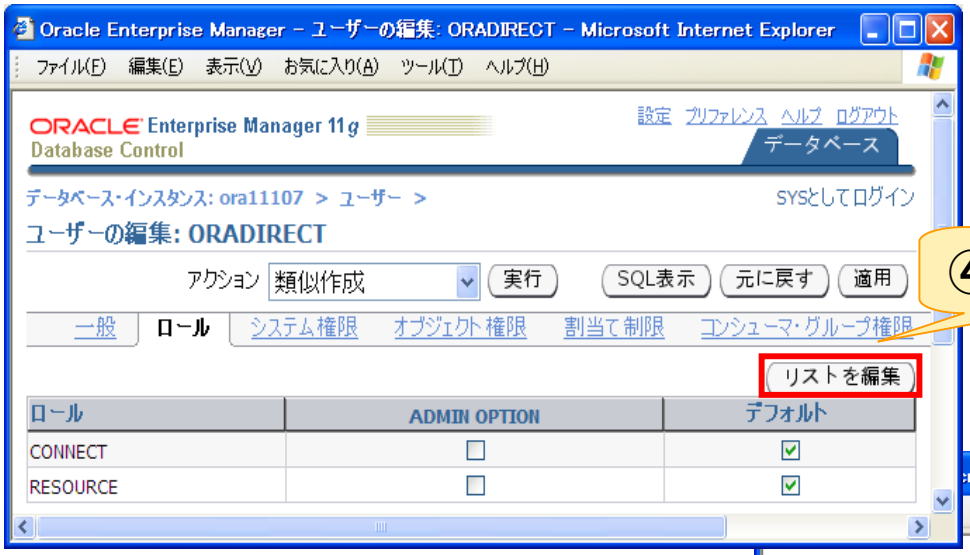


⑦選択した権限に「SELECT」を追加し、「OK」をクリック

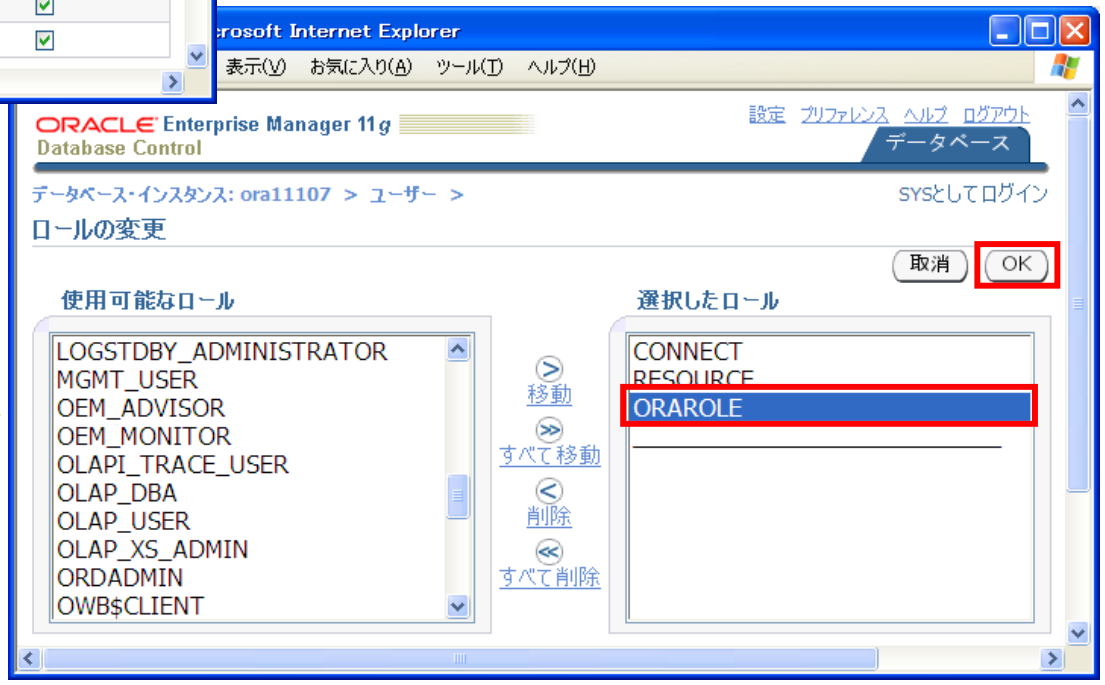
確認
オブジェクトは正常に作成されました

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



④クリック



⑤選択したロールに「ORAROLE」を追加し、「OK」クリック

「ORAROLE」ロールの付与を適用します

⑥クリック

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

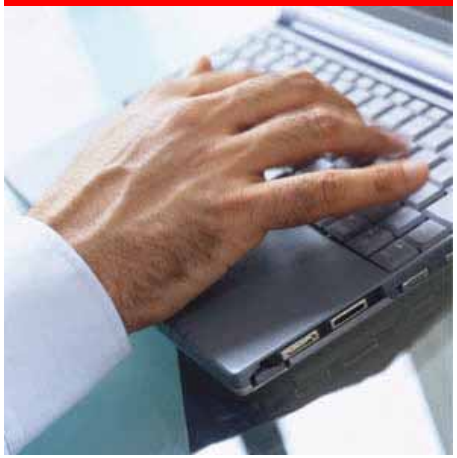
例：CREATE TABLE権限をPUBLICに付与する場合

```
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

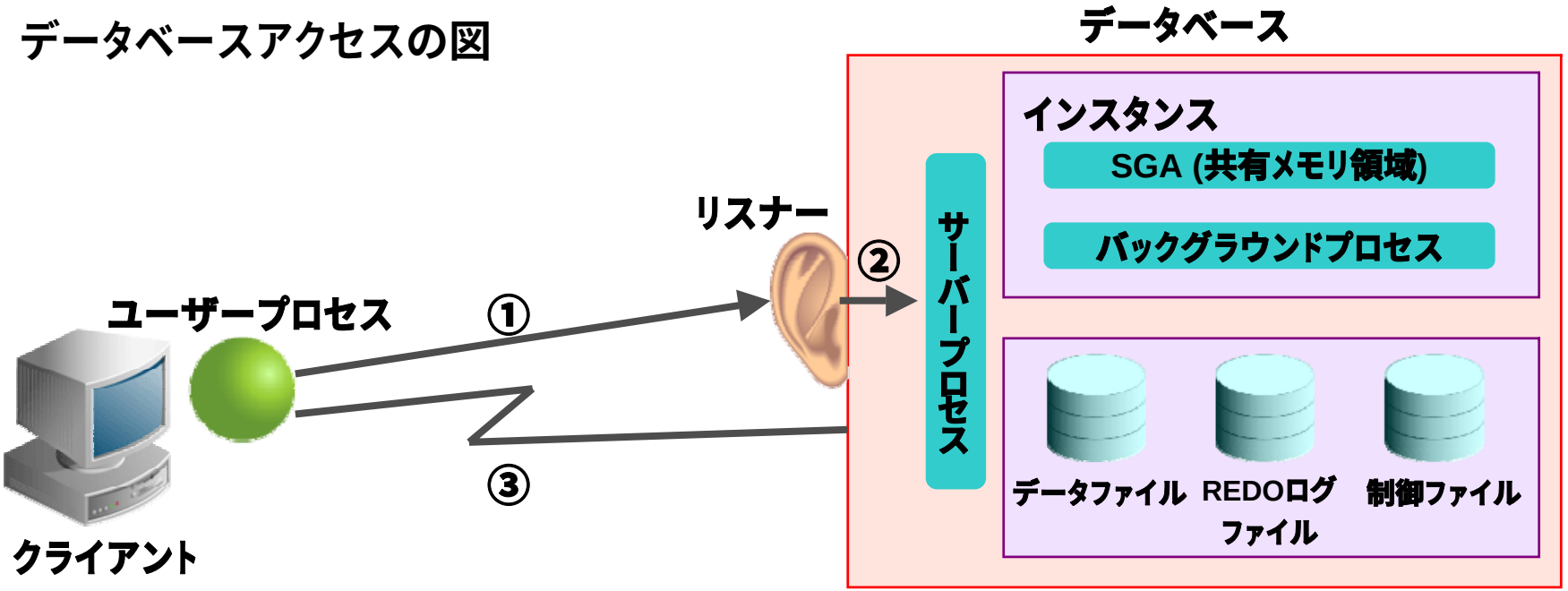
外部からのアクセス

- 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

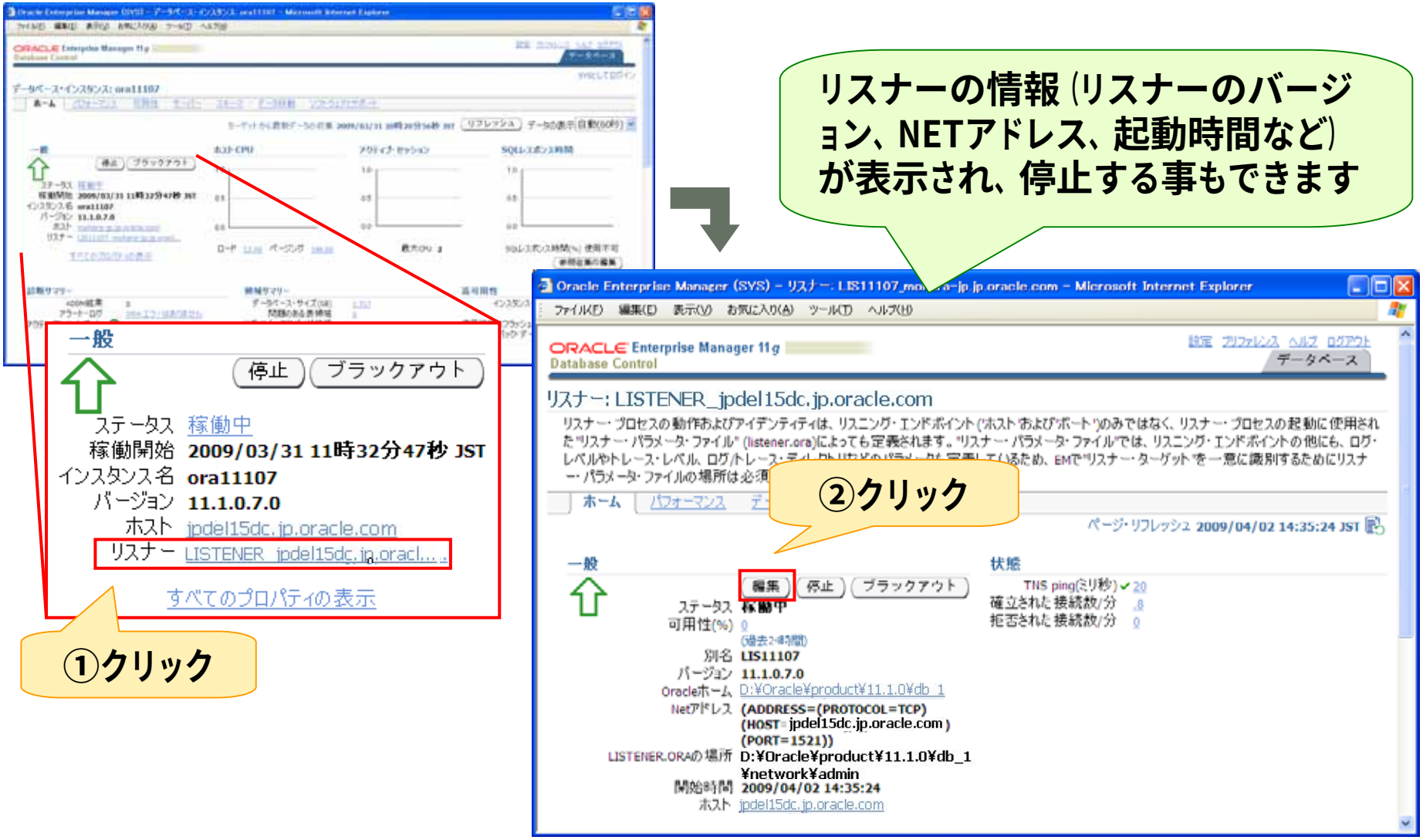
Enterprise Manager
を使った設定方法を
解説します

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

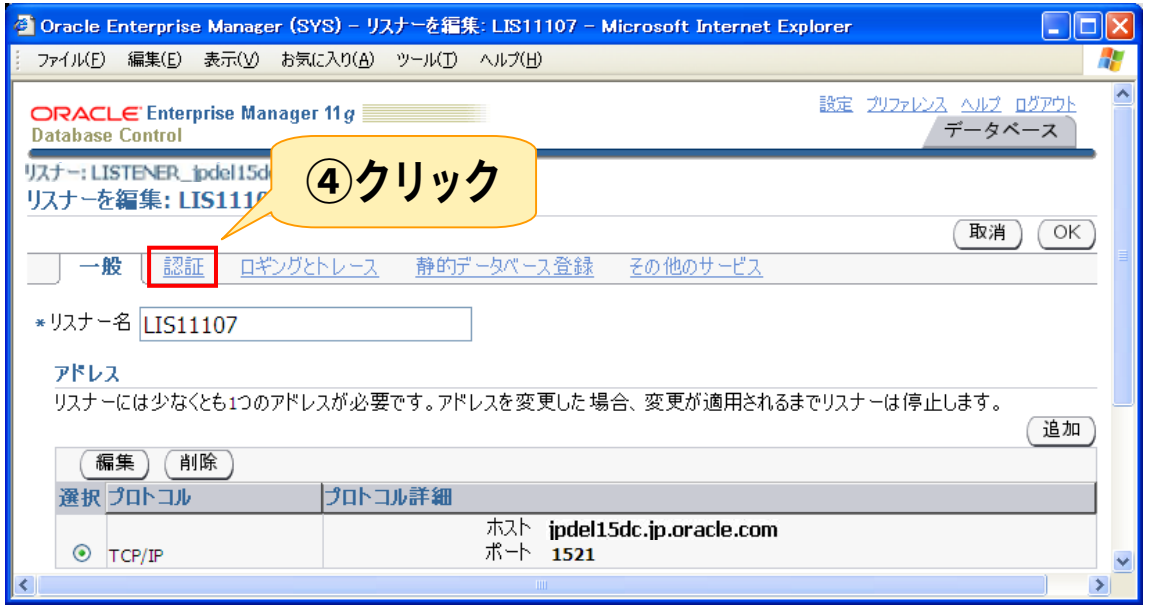


リスナーの状況を確認します

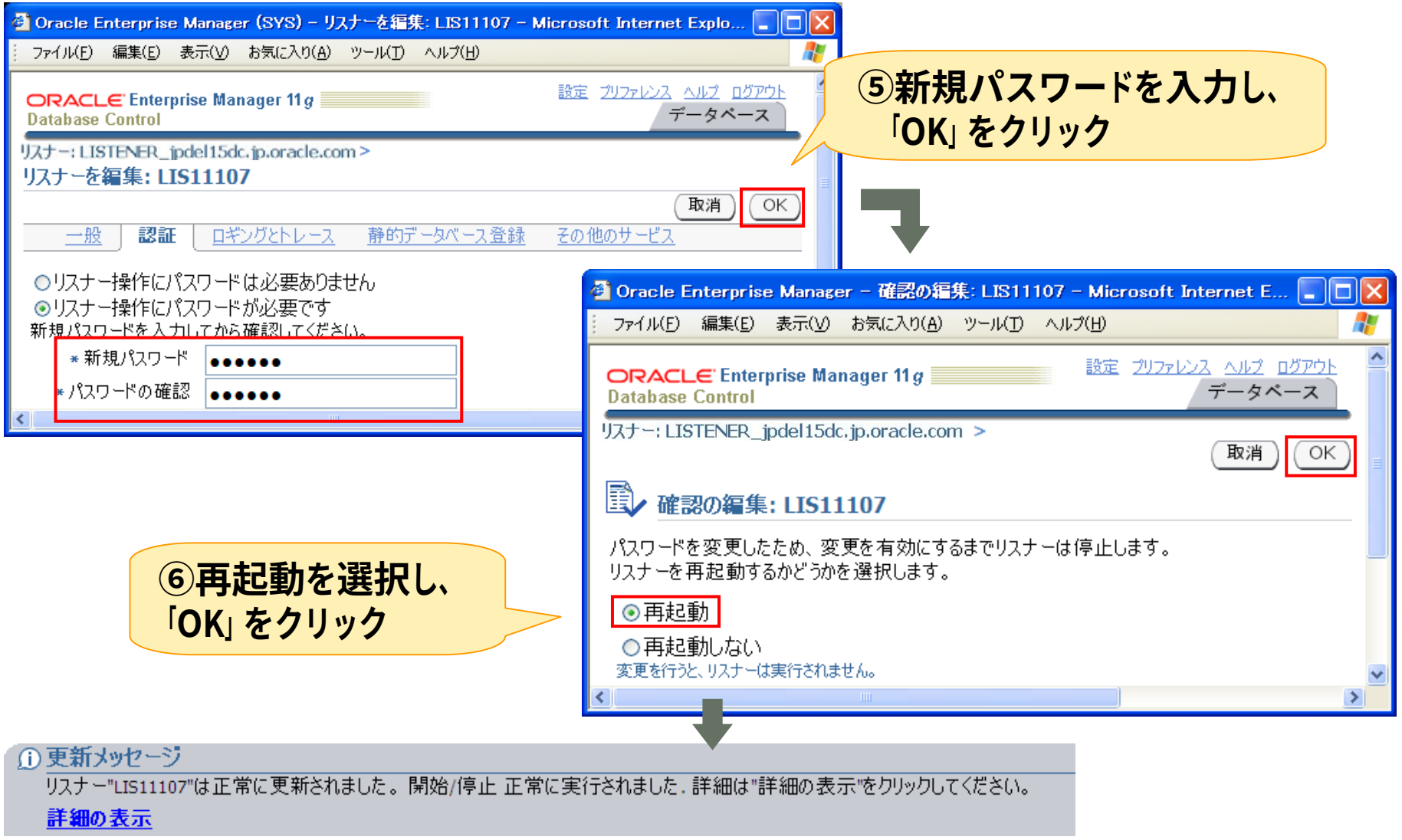


リスナーにパスワードを設定します

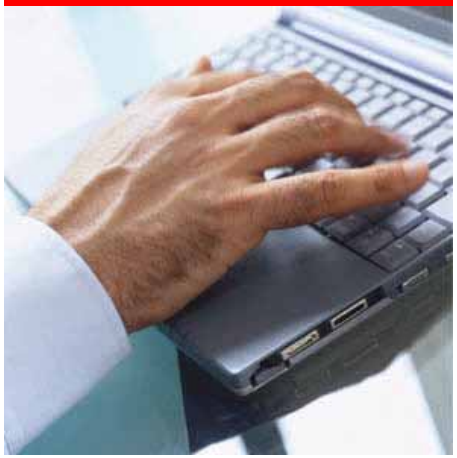
③サーバーOSのユーザー名とパスワードを入力し、「ログイン」をクリック



リスナーにパスワードを設定します



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

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

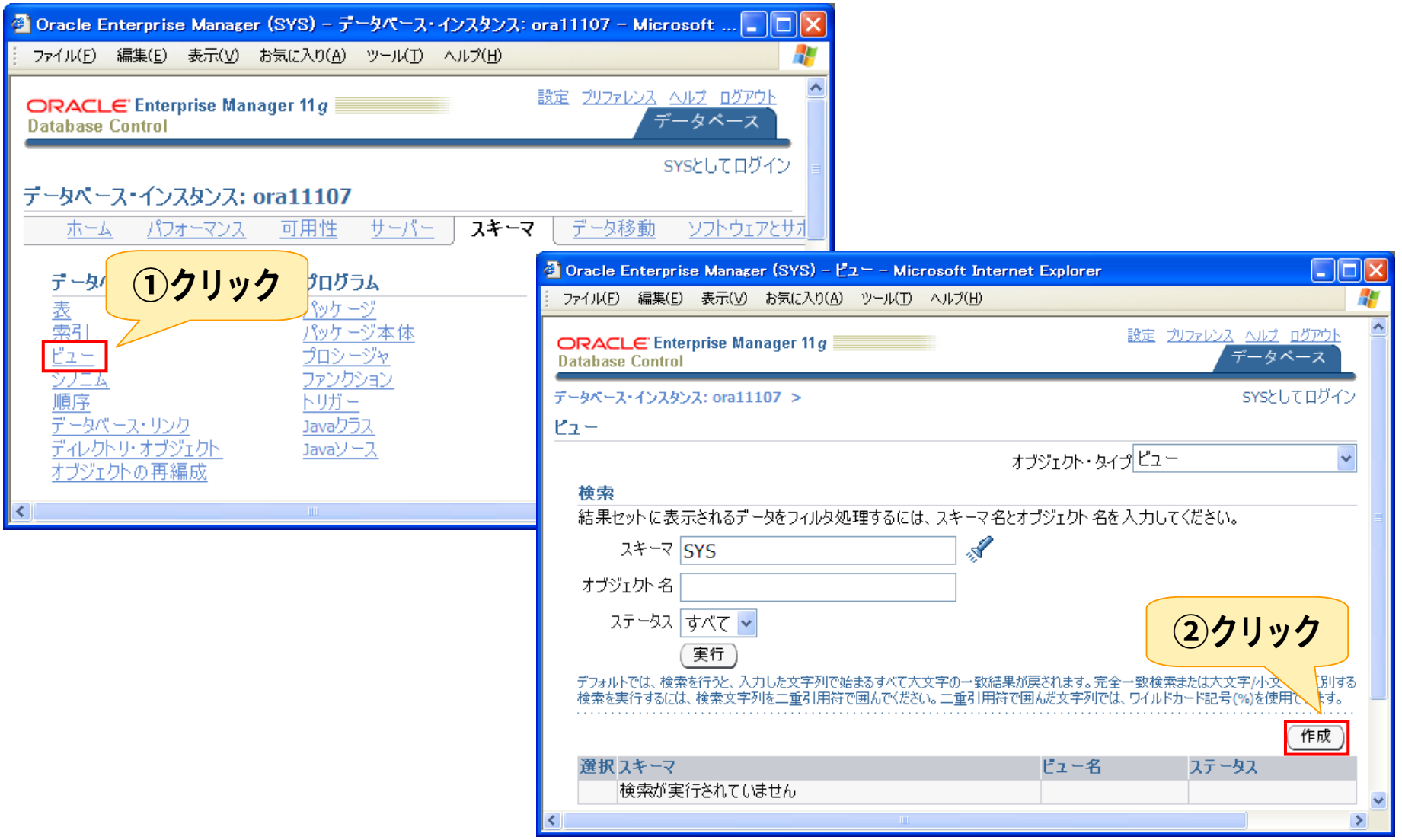
ビュー

EMP_ID	EMP_NAME
100	YAMADA
101	KAWADA
102	UMINO
103	TSUTIYA

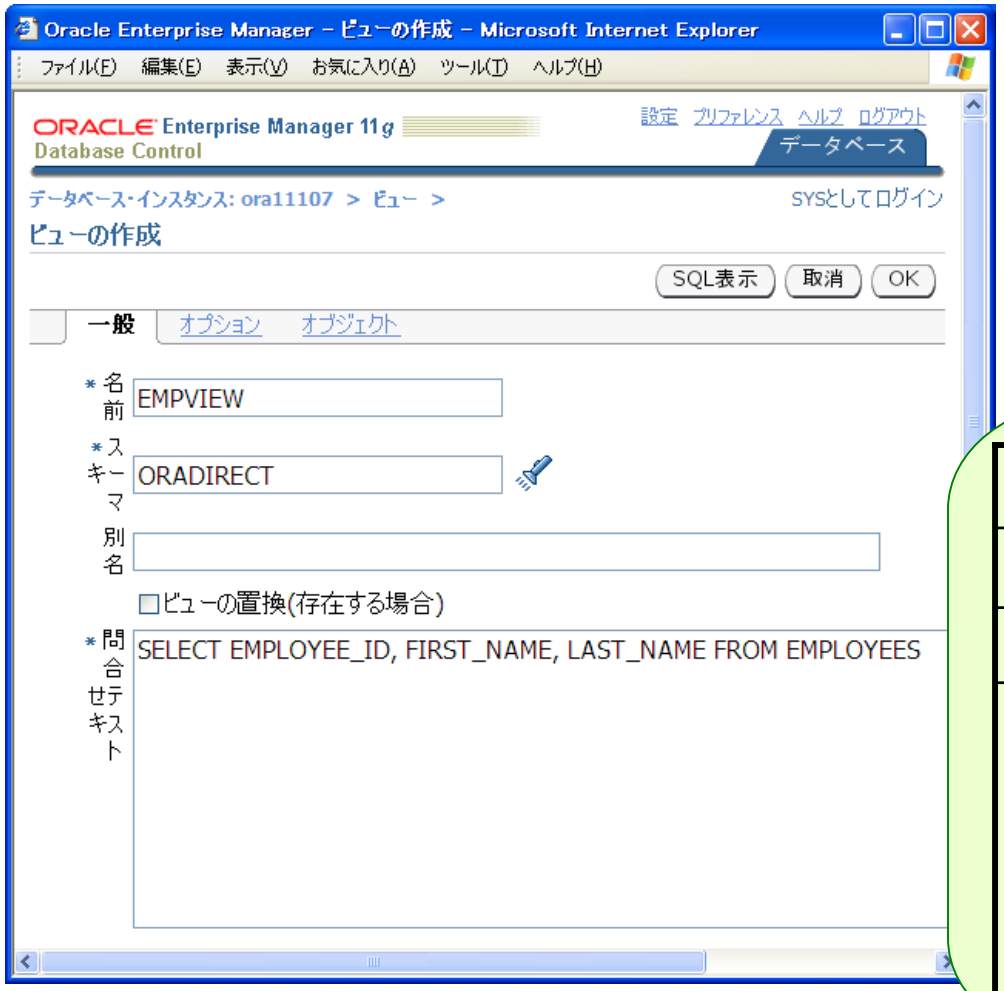
EMP_ID列とEMP_NAME列のみを含んだビューを作成し、ユーザーにはこのビューの参照権限のみを付与

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

EMPVIEWビューを作成します



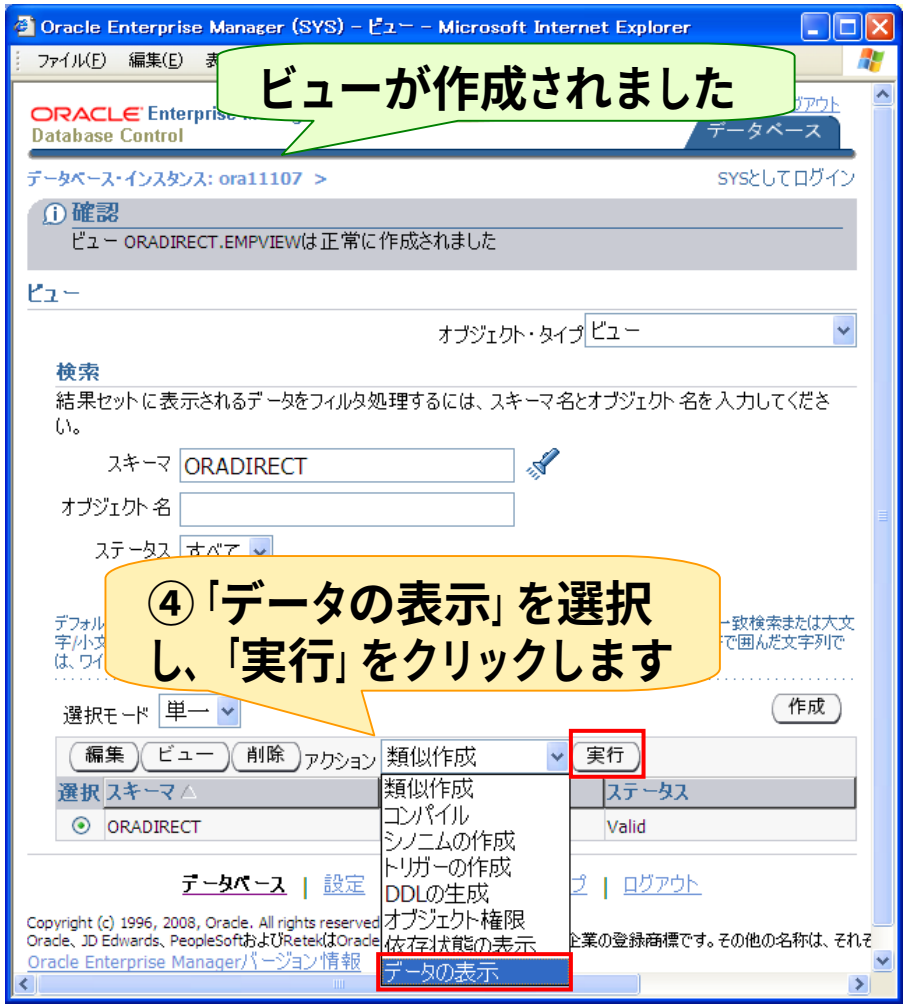
作成するビューの設定内容を入力します



③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

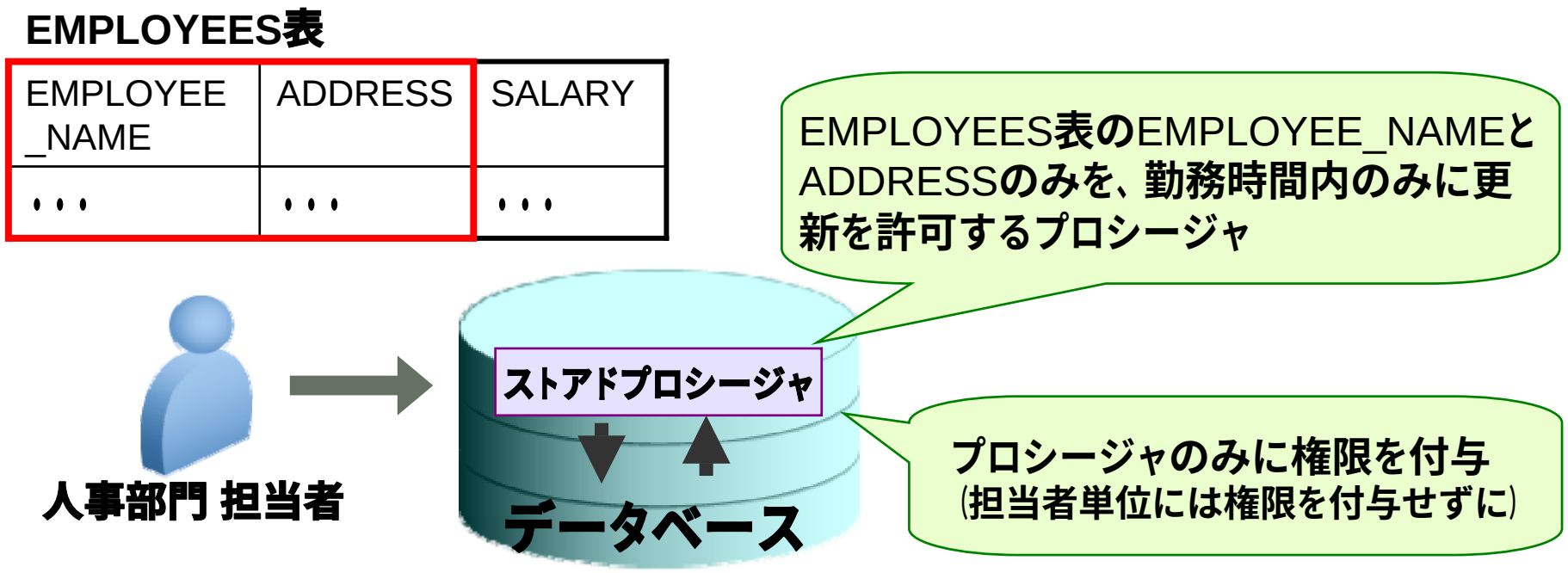
作成したビューのデータを確認します



ビューのデータを表示できます

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



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

2. 認証の管理

不要なユーザを使用可能にしない

4. 外部からのアクセス

リスナーにパスワード設定可能

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

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

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

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

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

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

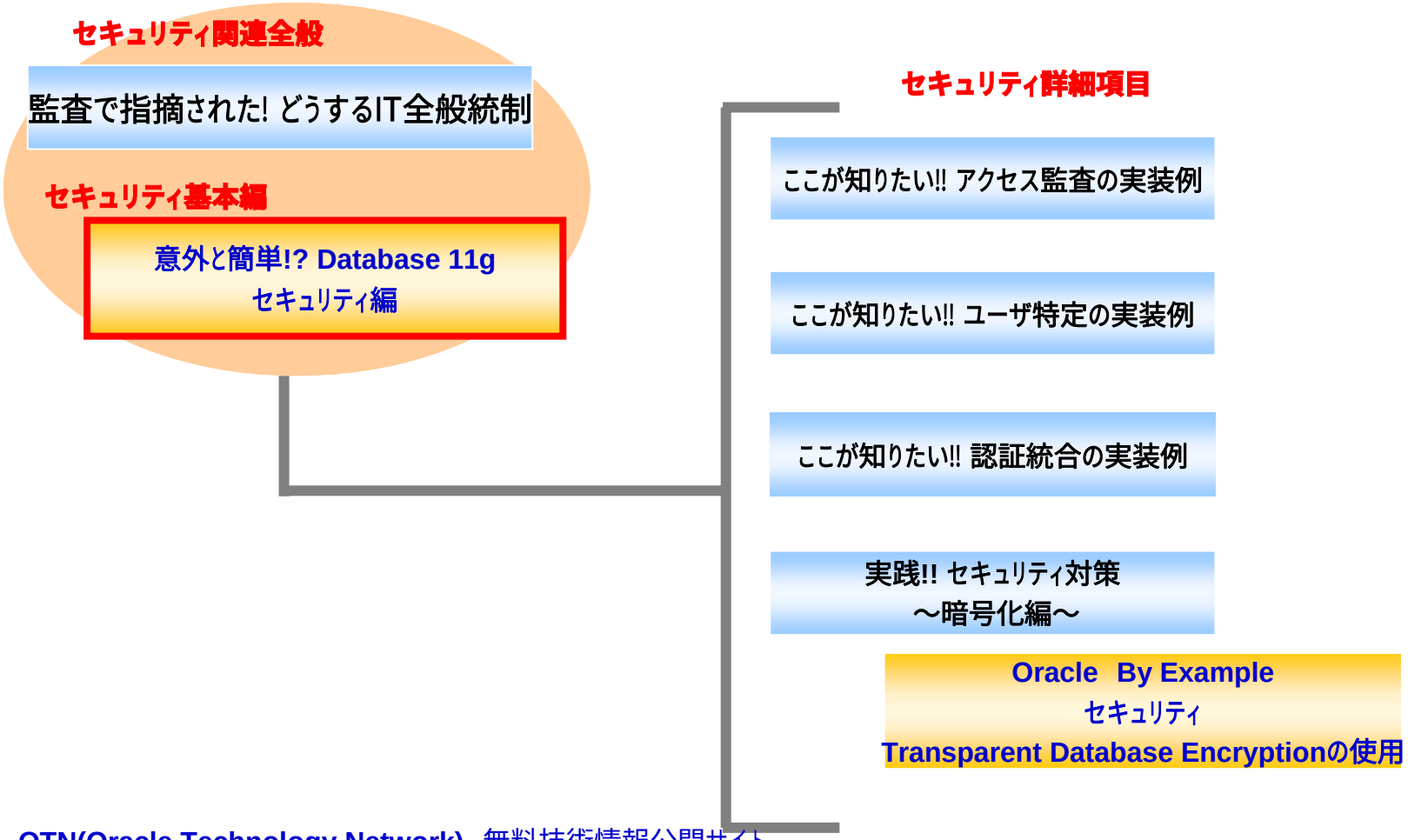
（祝日および年末年始除く）

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