

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きます

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

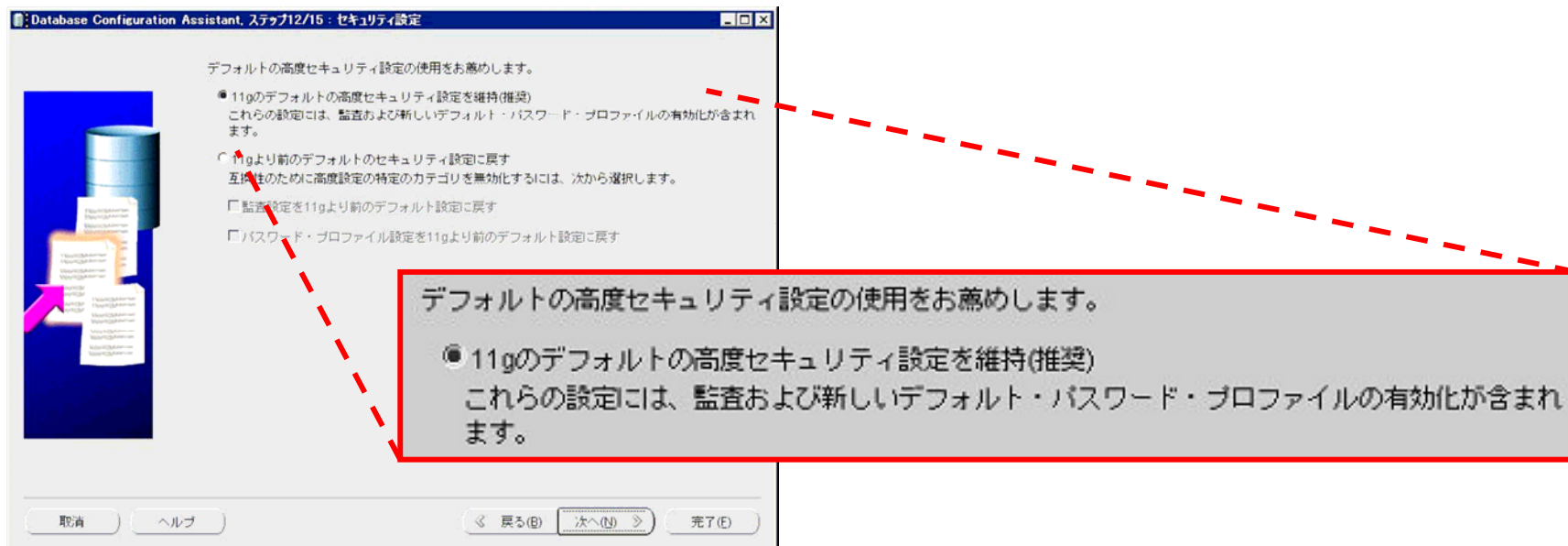
Agenda

- 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



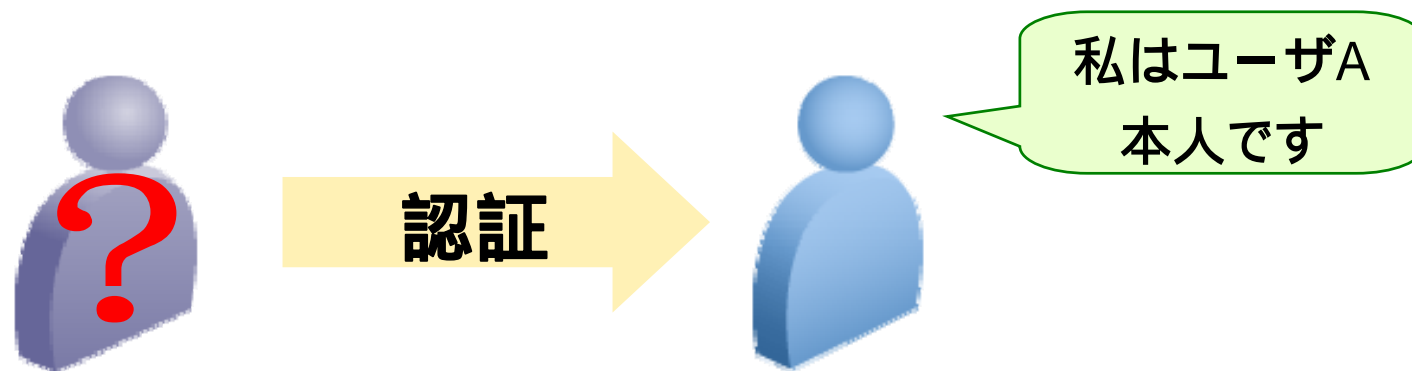
認証の管理

- 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

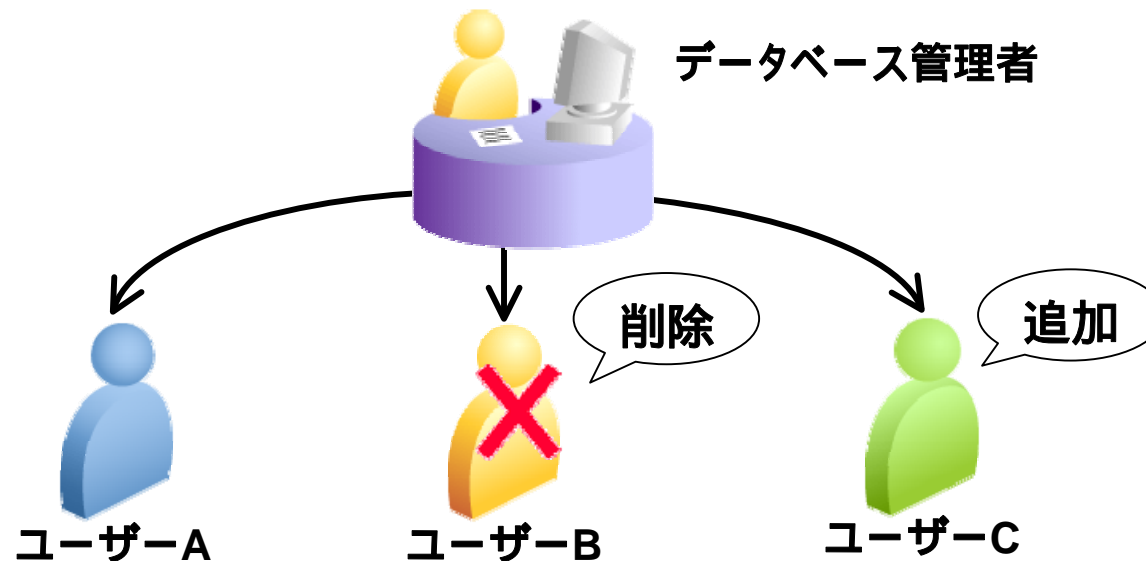
- データベースによるパスワード認証: ログイン時にパスワードを入力する方法
- 外部認証: OSまたはネットワークシステムを利用
- グローバル認証: ディレクトリ・サービスを利用



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

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

The screenshot shows the Oracle Enterprise Manager 11g Database Control interface in a Microsoft Internet Explorer browser window. The title bar reads "Oracle Enterprise Manager (SYS) - データベース・インスタンス: ora11107 - Microsoft Internet Explorer". The main header includes "ORACLE Enterprise Manager 11g Database Control" and navigation links like "設定", "プリファレンス", "ヘルプ", "ログアウト", and "データベース". Below the header, there's a section for "データベース・インスタンス: ora11107" with tabs for "ホーム", "パフォーマンス", "可用性", "サーバー", "スキーマ", "データ移動", and "ソフトウェアとサポート". The "サーバー" tab is selected. On the left, a "記憶域" (Memory) section is visible. The main content area is divided into three columns: "データベース構成" (Database Configuration), "Oracle Scheduler", and "リソース・マネージャ" (Resource Manager). The "セキュリティ" (Security) link is highlighted in the left sidebar, and a red dashed line points from it to the "ユーザー" (Users) link in the "セキュリティ" section of the main content area. A yellow callout bubble with the text "クリック" (Click) points to the "ユーザー" link.

セキュリティ

- ユーザー** (クリック)
- 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

データベース構成

- メモリー・アドバイザー
- 自動UNDO管理
- 初期化パラメータ
- データベース機能使用状況の検索

Oracle Scheduler

- ジョブ
- チェーン
- スケジュール
- プログラム
- ジョブ・クラス
- ウィンドウ
- ウィンドウ・グループ
- グローバル属性
- 自動化メンテナンス・タスク

リソース・マネージャ

- スタート・ガイド
- コンシューマ・グループ
- コンシューマ・グループ・マッピング
- プラン
- 設定
- 統計

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

ユーザーアカウントの表示画面



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

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

ORACLE Enterprise Manager 11g
Database Control

データベース・インスタンス: ora11107 > SYSとしてログ

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

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 作成

編集 ビュー 削除 アクション 類似作成 実行 前へ 1-25 / 38 次の13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"/>	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

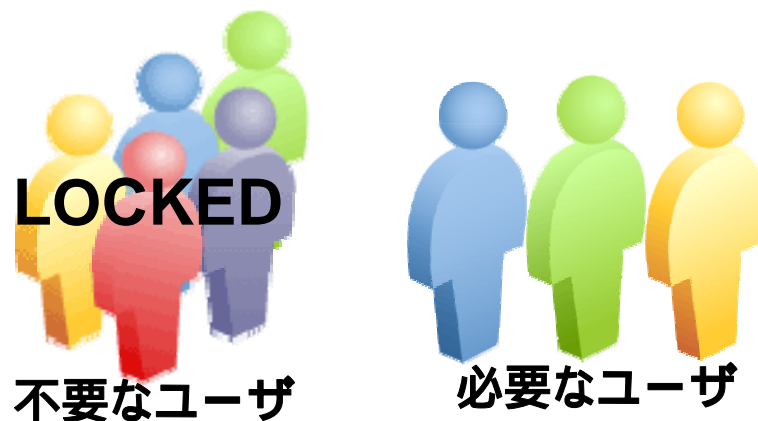
この画面から、ユーザーアカウントの管理作業を行っていただけます

- 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

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

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

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

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

ロックを解除したいアカウントを選択

選択	ユーザー名	アクション	類似作成	デフォルト表領域	一時表領域	プロファイル	作成
<input type="radio"/>	ANONYMOUS	EXPIRE	類似作成	SYSAUX	TEMP	DEFAULT	2008/10/01 6:58:43 JST
<input type="radio"/>	APEX_PUBLIC_USER	LOCK	パスワード期限切れ	USERS	TEMP	DEFAULT	2008/10/01 7:32:04 JST
<input type="radio"/>	CTXSYS	DDLの生成	ユーザーのロック	USERS	TEMP	DEFAULT	2008/10/01 6:57:44 JST
<input type="radio"/>	DBSNMP	ユーザーのロック解除		USERS	TEMP	MONITORING_PROFILE	2008/10/01
<input type="radio"/>	DIP	LOCKED		USERS	TEMP		
<input type="radio"/>	E	EXPIRED & LOCKED		SYSAUX	TEMP		
<input type="radio"/>	E	EXPIRED & LOCKED		SYSAUX	TEMP		
<input type="radio"/>	FLWS_FI	EXPIRED & LOCKED		SYSAUX	TEMP		
<input checked="" type="radio"/>	HR	EXPIRED & LOCKED		USERS	TEMP		
<input type="radio"/>	MDDATA	EXPIRED & LOCKED		USERS	TEMP		

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

確認 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース

データベース-インスタンス: ora11107 > ユーザー > 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

クリック

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HRのロックが解除されました

ユーザーSCOTTのアカウントをロックします

Oracle 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

オブジェクト名: SCOTT

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オブジェクトを検索します。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。

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	類似作成	パスワード期限切れ	ト表
	SCOTT	OPEN	DDLの生成	ユーザーのロック	一時領域
			ユーザーのロック解除		

ロックしたいアカウントを選び、アクションリストから「ユーザーのロック」を選択し、「実行」をクリック

クリック

ロック USER SCOTTが必要ですか。

いいえ はい

確認

ユーザーSCOTTは正常にロックされました

ユーザーSCOTTはロックされました

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に求められます

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 > SYSとしてログイン

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: S

実行

選択モード: 単一

作成

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"/>	SCOTT	EXPIRED	2009/03/24 13:59:32 JST	USERS	TEMP	DEFAULT	2008/10/01 7:57:40 JST
<input type="radio"/>	SI_INFORMTN_SCHEMA	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	SYS_AUX	TEMP	DEFAULT	2008/10/01 7:03:11 JST
<input type="radio"/>	SPATIAL_CSW_ADMIN_USR	EXPIRED & LOCKED	2009/02/13 14:21:41 JST	USERS	TEMP	DEFAULT	2008/10/01 7:19:34 JST
<input type="radio"/>	SPATIAL_WFS_ADMIN_USR	EXPIRED & LOCKED	2009/02/13 14:21:42 JST	USERS	TEMP	DEFAULT	2008/10/01 7:19:25 JST
<input type="radio"/>	SYS	OPEN	2009/08/12 14:21:07 JST	SYSTEM	TEMP	DEFAULT	2008/10/01 6:31:51 JST
<input type="radio"/>	SYSMAN	OPEN	2009/08/12 16:18:46 JST	SYS_AUX	TEMP	DEFAULT	2009/02/13 16:18:46 JST
<input type="radio"/>	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

新しいパスワードを入力します

Oracle Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 > ユーザー > ユーザーの編集: SCOTT

アクション: 類似作成 | 実行 | SQL表示 | 元に戻す | 適用

一般 | ロール | システム権限 | オブジェクト権限 | 割当て制限 | コンシューマ・グループ権限 | プロキシ・ユーザー

名前: SCOTT
プロファイル: DEFAULT
認証: パスワード

* パスワードの入力:
* パスワードの確認:

パスワード・ステータス: Expired
パスワードが期限切れにならないよう、パスワードを入力し、確認のためもう一度入力してください。

デフォルト表領域: USERS
一時表領域: TEMP

ステータス: ☐ ロック ☒ ロック解除

ユーザーSCOTTのパスワードが変更されました

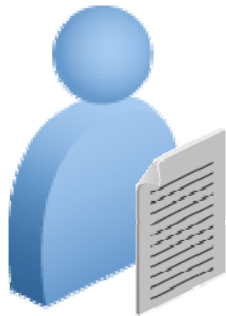
更新メッセージ

ユーザー SCOTTは正常に変更されました

ORACLE

プロフィールとは？

- 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



プロフィール

- 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

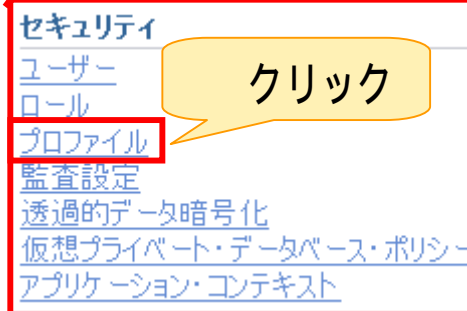
ユーザー情報の入力内容

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

ORADIRECTプロフィールを作成します



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

Oracle Enterprise Manager 11g - プロファイルの作成 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 > プロファイル > プロファイルの作成

SQL表示 取消 OK

一般 **パスワード** クリック

* 名前 ORADIRECT

詳細

CPU/セッション(秒/100)	DEFAULT	🔧
CPU/コール(秒/100)	DEFAULT	🔧
接続時間(分)	DEFAULT	🔧
アイドル時間(分)	DEFAULT	🔧

データベース・サードス

同時セッション(1ユーザーあたり)	DEFAULT	🔧
読取り/セッション(ブロック)	DEFAULT	🔧
読取り/コール(ブロック)	DEFAULT	🔧
プライベート SGA(KB)	DEFAULT	🔧
コンポジット 制限(サービス・ユニット)	DEFAULT	🔧

パスワードについての内容を入力します

Oracle Enterprise Manager 11g
Database Control
データベース・インスタンス: ora11107 > プロファイル > プロファイルの作成

SQL表示 取消 OK

一般 パスワード

パスワード

有効期間(日) 60

期限切れ後の猶予日数 30

履歴

パスワード再利用前の変更回数 2

再利用できなくなるまでの日数 UNLIMITED

複雑なパスワード検証

複雑なパスワード検証のための関数 DEFAULT

失敗したログイン

ロックされるまでのログイン試行失敗回数 6

指定回数失敗後、ロックされる日数 5

確認

オブジェクトは正常に作成されました

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

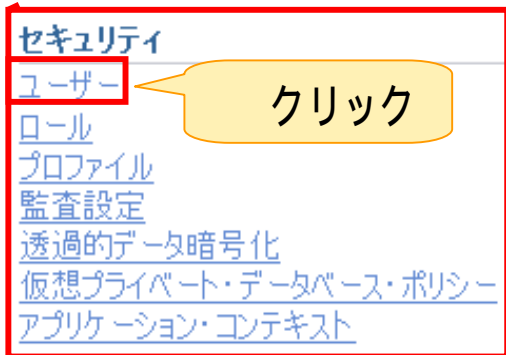
ロックされるまでのログイン試行失敗回数 : 6

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



ORACLE®

ORADIRECTユーザーに割り当てるプロファイルを選択します

Oracle Enterprise Manager 11g Database Control

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

アクション: 類似作成 [実行] [SQL表示] [元に戻す] [適用]

一般 [ロール] [システム権限] [オブジェクト権限] [割当て制限] [コンシューマ・グループ権限]

名前: ORADIRECT

プロファイル: DEFAULT

認証: DEFAULT, WKSYS_PROF, MONITORING_PROFILE, ORADIRECT

* パスワードの入力:

* パスワードの確認:

パスワード選択の場合、ロールはパスワードによって認可されます。

☐ 期限切れパスワード

デフォルト表領域: USERS

一時表領域: TEMP

ステータス: ☐ ロック ☒ ロック解除

クリック

「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

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



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

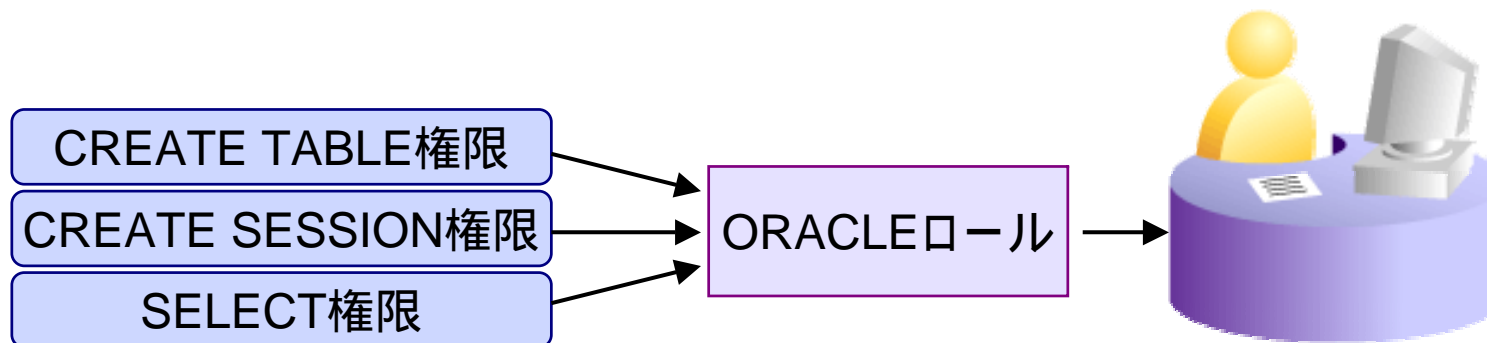
オブジェクト権限

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

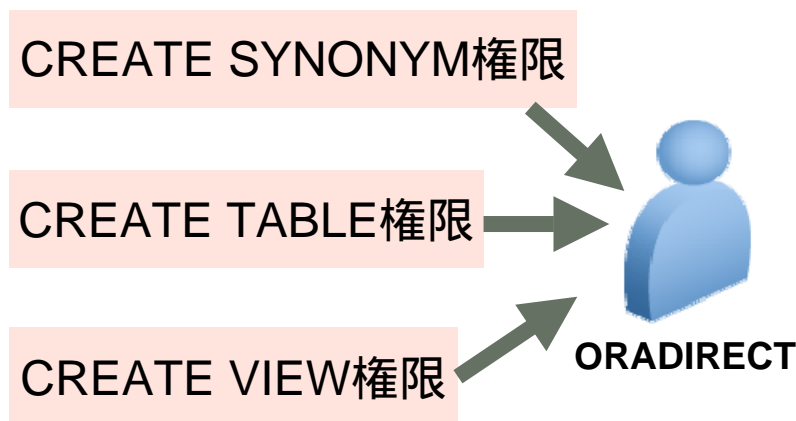


権限の付与

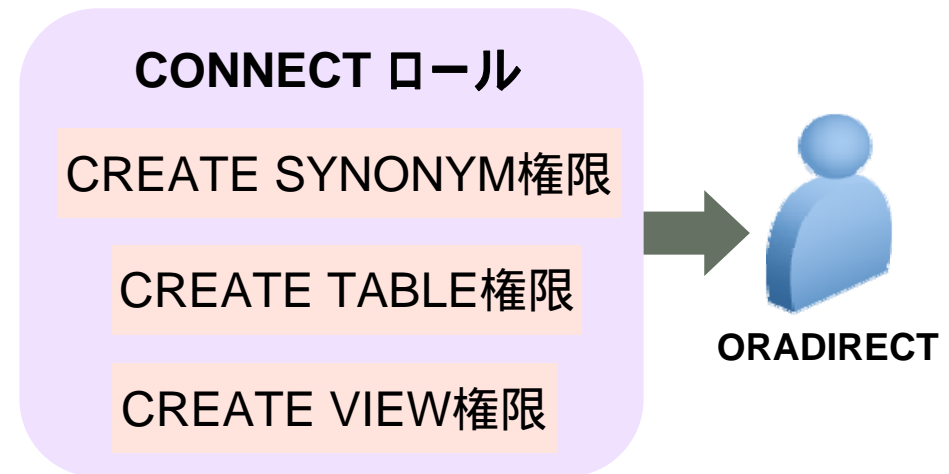
- 権限を付与するには、2 つの方法があります
 - 直接ユーザーに対して権限を付与する方法
 - 権限をロール(名前付きの権限グループ)に付与したあとで、このロールをユーザーに付与する方法

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

直接、権限を付与する方法



ロールを付与する方法



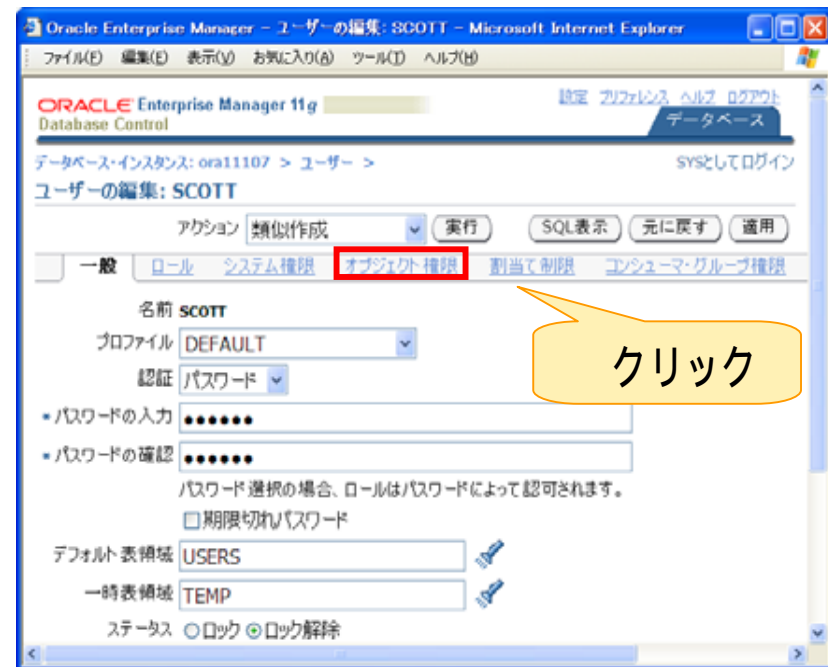
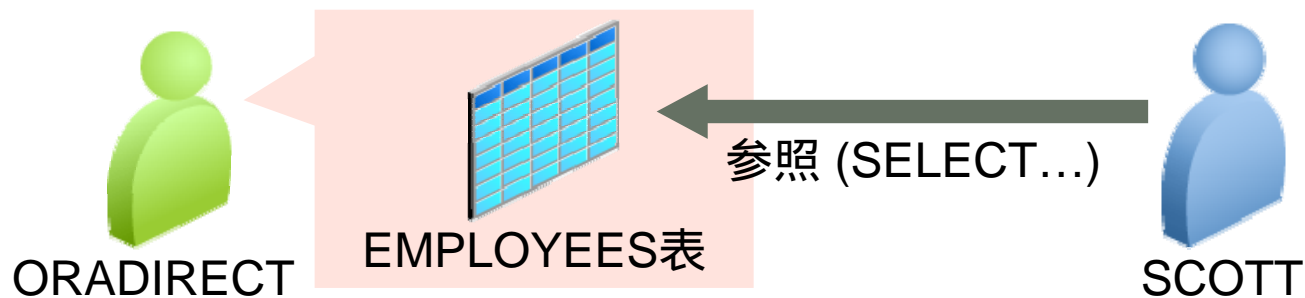
ロールを使用すると、一括して権限の管理が行えるため効率的です

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

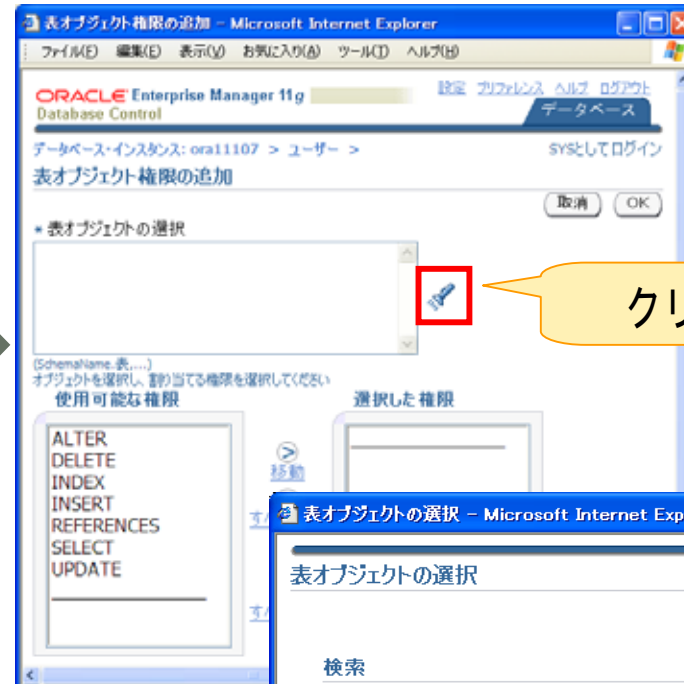


オブジェクト・タイプと表オブジェクトを設定します

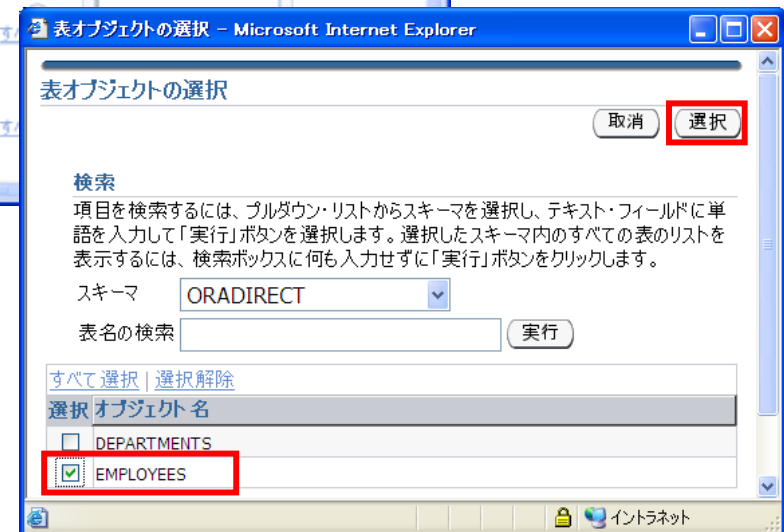


「オブジェクト・タイプの選択」の項目に「表」を選択して「追加」をクリック

「EMPLOYEES」を選択し、「選択」をクリック

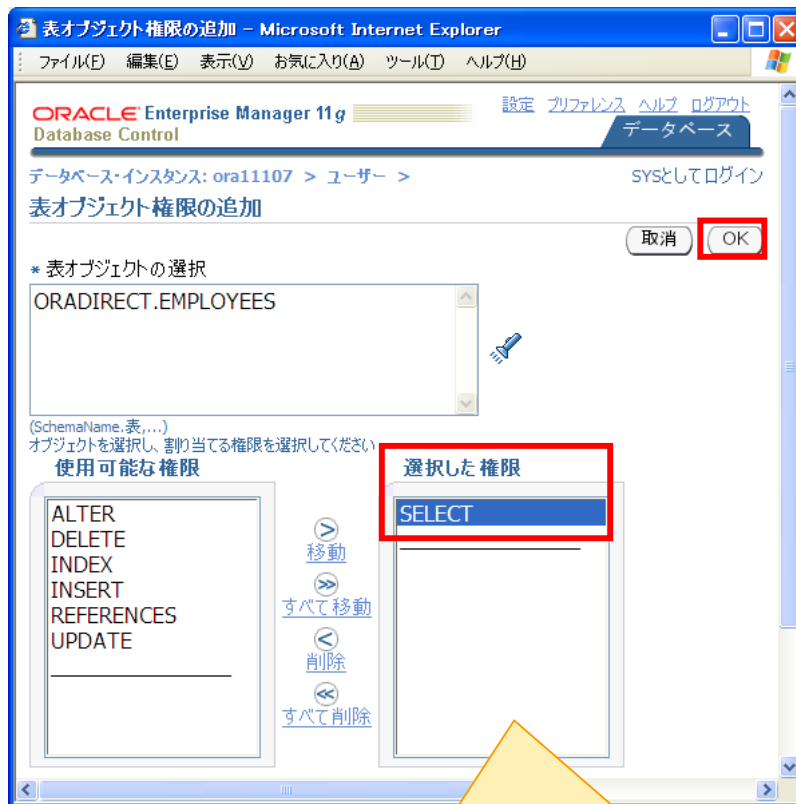


クリック



ORACLE

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



更新メッセージ

ユーザー SCOTTは正常に変更されました

OPTIONが指定されている権限について

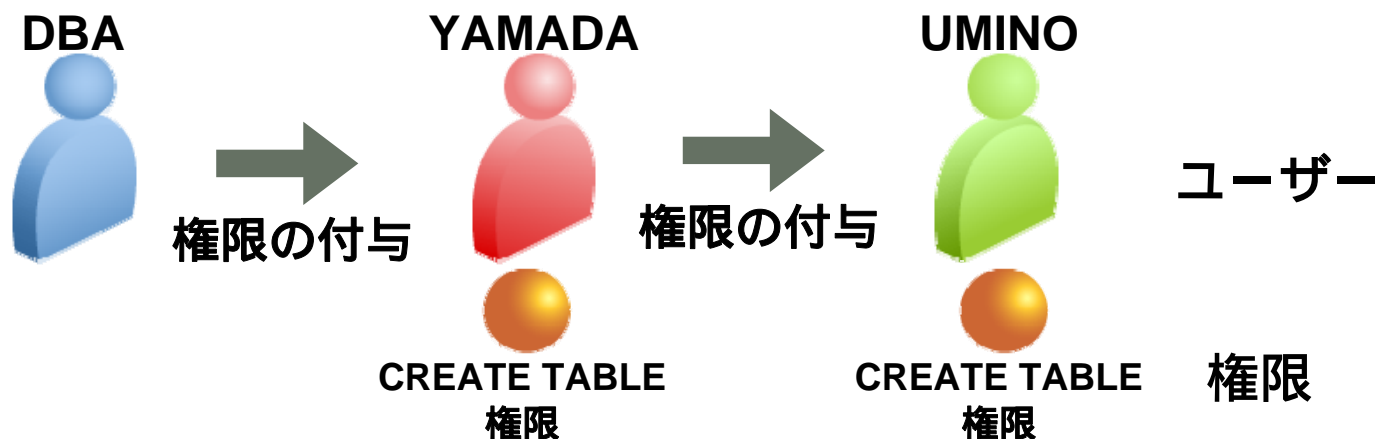
- システム権限

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



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

クリック



クリック

ORACLE

ロール名とオブジェクト・タイプを設定します

Oracle Enterprise Manager 11g - ロールの作成 - Microsoft Internet Explorer

Database Control

データベース・インスタンス: ora11107 > ロール > SYSとしてログイン

ロールの作成

SQL表示 取消 OK

一般 **ロール** システム権限 **オブジェクト権限** コンシューマ・グループ権限

* 名前 **ORAROLE**

認証 なし

認証は行われません。

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



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

Oracle Enterprise Manager 11g - ロールの作成 - Microsoft Internet Explorer

Database Control

データベース・インスタンス: ora11107 > ロール > SYSとしてログイン

ロールの作成

SQL表示 取消 OK

一般 **ロール** システム権限 **オブジェクト権限** コンシューマ・グループ権限

オブジェクト・タイプの選択 **表** **追加**

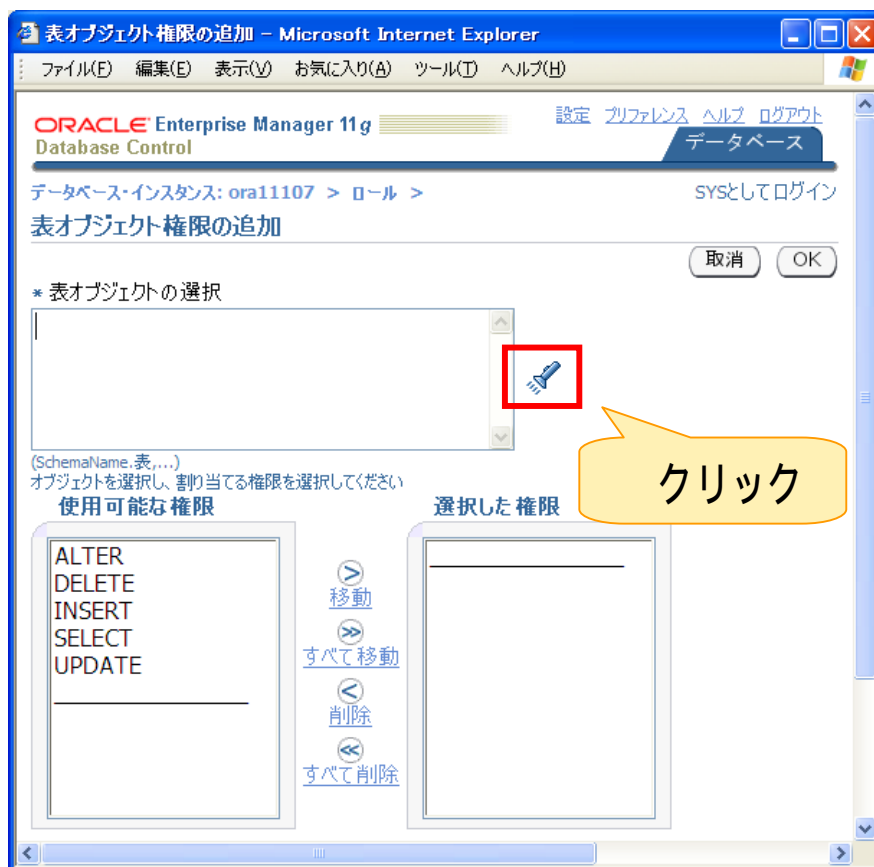
選択 オブジェクト権限

スキマ オブジェクト

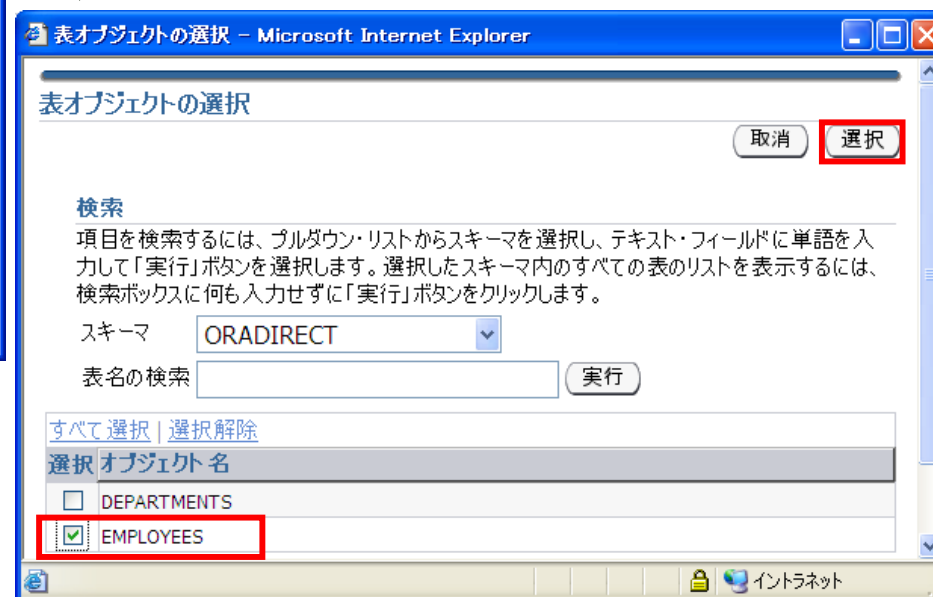
項目が見つかりません

ORACLE

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



ORACLE

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

表オブジェクト権限の追加 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 > ロール > 表オブジェクト権限の追加

* 表オブジェクトの選択
ORADIRECT.EMPLOYEES

使用可能な権限
ALTER
DELETE
INSERT
UPDATE

選択した権限
SELECT

OK

選択した権限に「SELECT」を追加し、「OK」をクリック

Oracle Enterprise Manager - ロールの作成 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

データベース・インスタンス: ora11107 > ロール > ロールの作成

SQL表示 取消 OK

一般 ロール システム権限 オブジェクト権限 コンシューマ・グループ権限

オブジェクト・タイプの選択 Javaクラス 追加

削除

選択	オブジェクト権限	スキーマ	オブジェクト
<input checked="" type="radio"/>	SELECT	ORADIRECT	EMPLOYEES

クリック

確認

オブジェクトは正常に作成されました

ORACLE



割り当てるロールを選択します

Oracle Enterprise Manager 11g
Database Control
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

アクション: 類似作成 [実行] [SQL表示] [元に戻す] [適用]

一般 **ロール** システム権限 オブジェクト権限 割当て制限 コンシューマ・グループ権限

リストを編集

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

クリック

選択したロールに「ORAROLE」を追加し、「OK」クリック

Oracle Enterprise Manager 11g
Database Control
データベース・インスタンス: ora11107 > ユーザー >
ロールの変更

使用可能なロール

- LOGSTDBY_ADMINISTRATOR
- MGMT_USER
- OEM_ADVISOR
- OEM_MONITOR
- OLAPI_TRACE_USER
- OLAP_DBA
- OLAP_USER
- OLAP_XS_ADMIN
- ORDADMIN
- OWB\$CLIENT

移動
すべて移動
削除
すべて削除

選択したロール

- CONNECT
- RESOURCE
- ORAROLE**

取消 OK

「ORAROLE」ロールの付与を適用します



クリック

更新メッセージ
ユーザー ORADIRECTは正常に変更されました

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

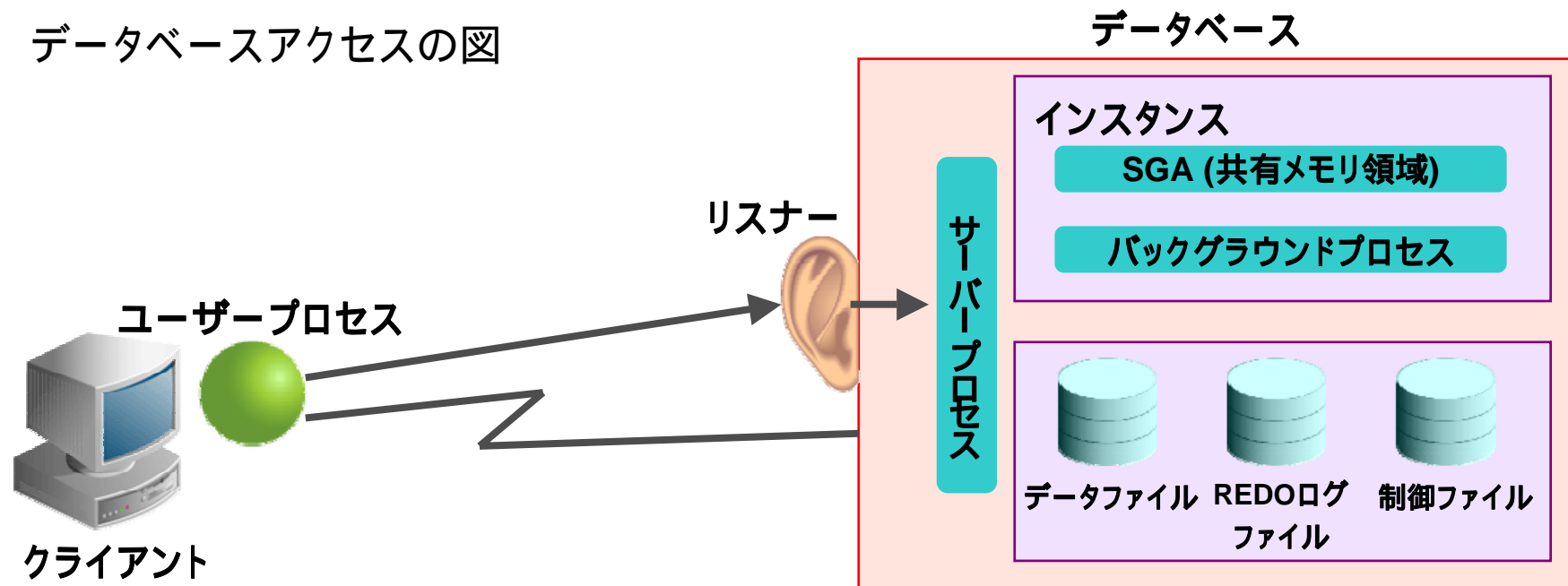
- リスナーの役割
- リスナーを監視と管理制限
 - **EM** :リスナーの状態を確認する
 - **EM** :リスナーにパスワードを設定する

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

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



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

クリック

ORACLE

リスナーにパスワードを設定します

Oracle Enterprise Manager (SYS) - Net Services管理: ホストのログイン - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

Net Services管理: ホストのログイン

ホスト: jpdcl15dc.jp.oracle.com

Oracleホーム: D:\Oracle\product\11.1.0\db_1

* ユーザー名: Administrator

* パスワード: ●●●●●●●●

☐ 優先資格証明として保存

取消 ログイン

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 Enterprise Manager (SYS) - リスナーを編集: LIS11107 - Microsoft Internet Explorer

ORACLE Enterprise Manager 11g Database Control

リスナー: LISTENER_jpdcl15dc

リスナーを編集: LIS11107

一般 **認証** ログインとトレース 静的データベース登録 その他のサービス

* リスナー名: LIS11107

アドレス
リスナーには少なくとも1つのアドレスが必要です。アドレスを変更した場合、変更が適用されるまでリスナーは停止します。

編集 削除

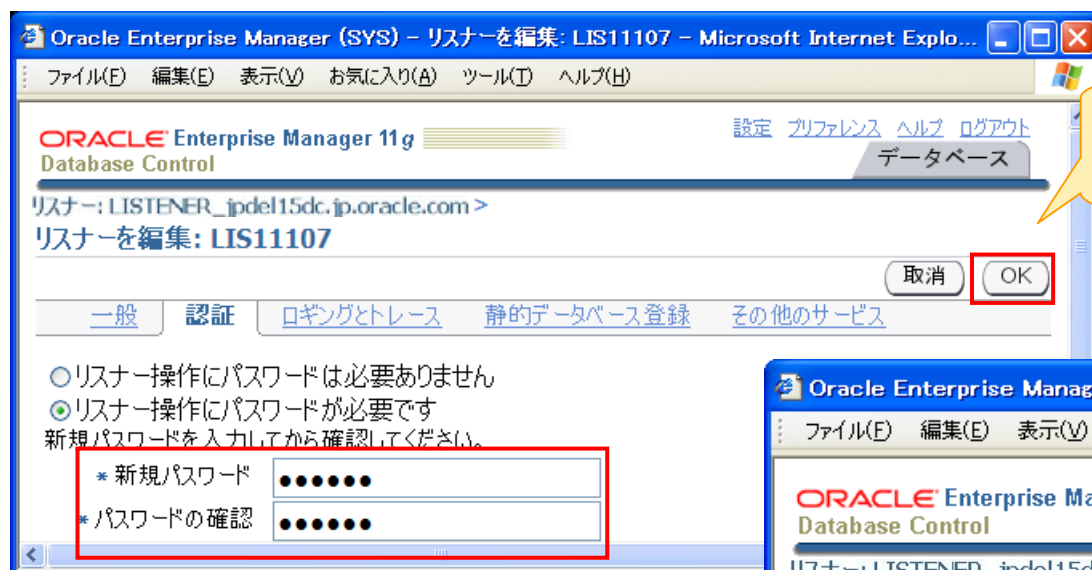
選択	プロトコル	プロトコル詳細
<input checked="" type="radio"/>	TCP/IP	ホスト: jpdcl15dc.jp.oracle.com ポート: 1521

追加

クリック

ORACLE

リスナーにパスワードを設定します



新規パスワードを入力し、
「OK」をクリック



再起動を選択し、
「OK」をクリック

更新メッセージ

リスナー" LIS11107"は正常に更新されました。開始/停止 正常に実行されました。詳細は"詳細の表示"をクリックしてください。

[詳細の表示](#)

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

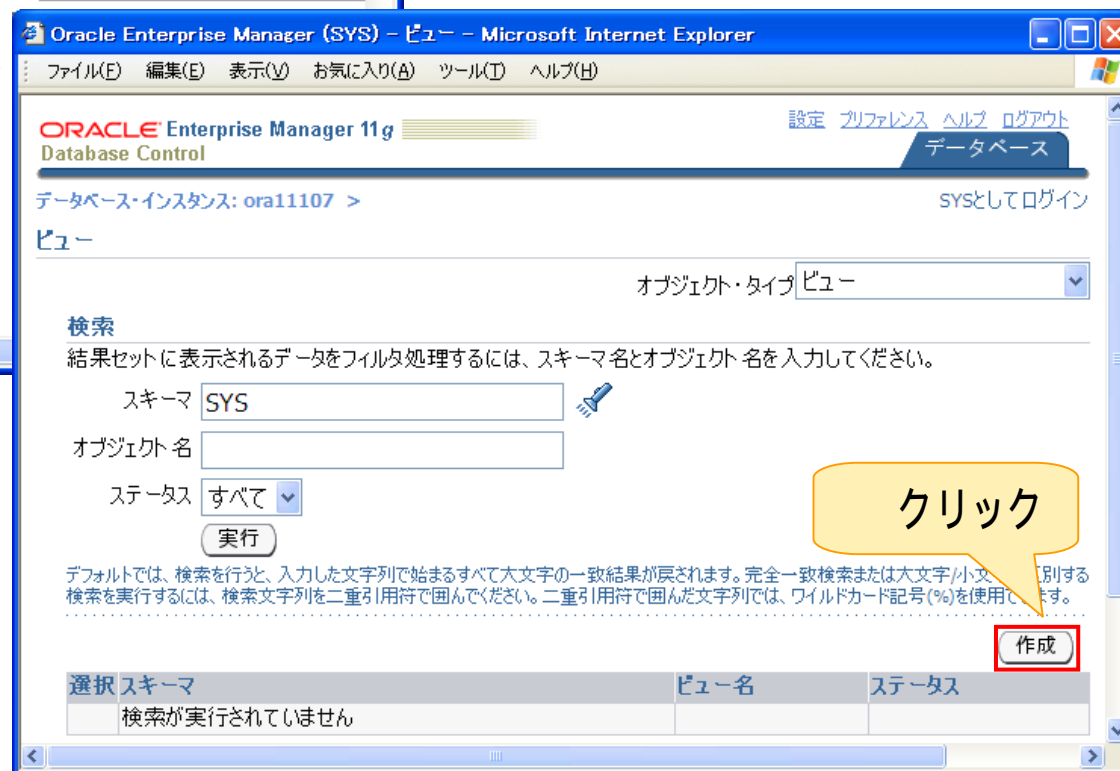
ビュー

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



ORACLE

作成するビューの設定内容を入力します

Oracle Enterprise Manager 11g Database Control
データベース-インスタンス: ora11107 > ビュー > ビューの作成

SQL表示 取消 OK

一般 オプション オブジェクト

* 名前: EMPVIEW

* スキーマ: ORADIRECT

別名:

☐ ビューの置換(存在する場合)

* 問い合わせテキスト: SELECT EMPLOYEE_ID, FIRST_NAME, LAST_NAME FROM EMPLOYEES

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

ビューが作成されました

ビュー ORADIRECT.EMPVIEWは正常に作成されました

ビュー

オブジェクト・タイプ ビュー

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、スキーマ名とオブジェクト名を入力してください。

スキーマ ORADIRECT

オブジェクト名

ステータス オブジェクト

「データの表示」を選択し、「実行」をクリックします

選択モード 単一

編集 ビュー 削除 アクション

類似作成

類似作成
コンパイル
シノニムの作成
トリガーの作成
DDLの生成
オブジェクト権限
依存状態の表示
データの表示

実行

ステータス

Valid

データベース | 設定

Copyright (c) 1996, 2008, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoftおよびRetekはOracle
Oracle Enterprise Managerバージョン情報

ビューのデータを表示できます

ビューのデータの表示: ORADIRECT.EMPVIEW

問合せ

```
SELECT "EMPLOYEE_ID", "FIRST_NAME", "LAST_NAME"
FROM "ORADIRECT"."EMPVIEW"
```

結果

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	Sciarra
112	Jose Manuel	Urman
113	Luis	Popp
114	Den	Raphaely
115	Alexander	Khoo
116	Shelli	Baida
117	Sinal	Tobias

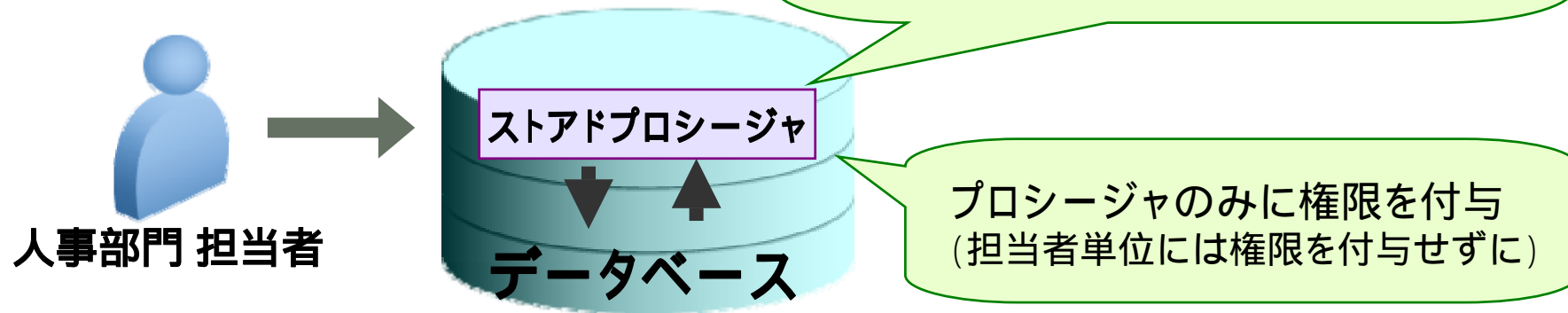
ストアド・プロシージャを使用したセキュリティ管理

- 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制限を実現することができます

EMPLOYEES表

EMPLOYEE_NAME	ADDRESS	SALARY
...

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



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

ORACLE

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、 세미나登録時にご登録されている貴社住所宛てに送付させていただきます。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ください。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



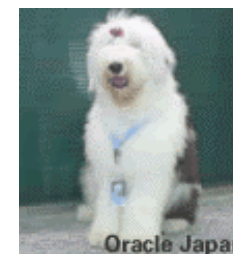
ORD_SEMINAR_JP@ORACLE.COM

【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 세미나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いただきます。



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！
- ・ 세미나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>

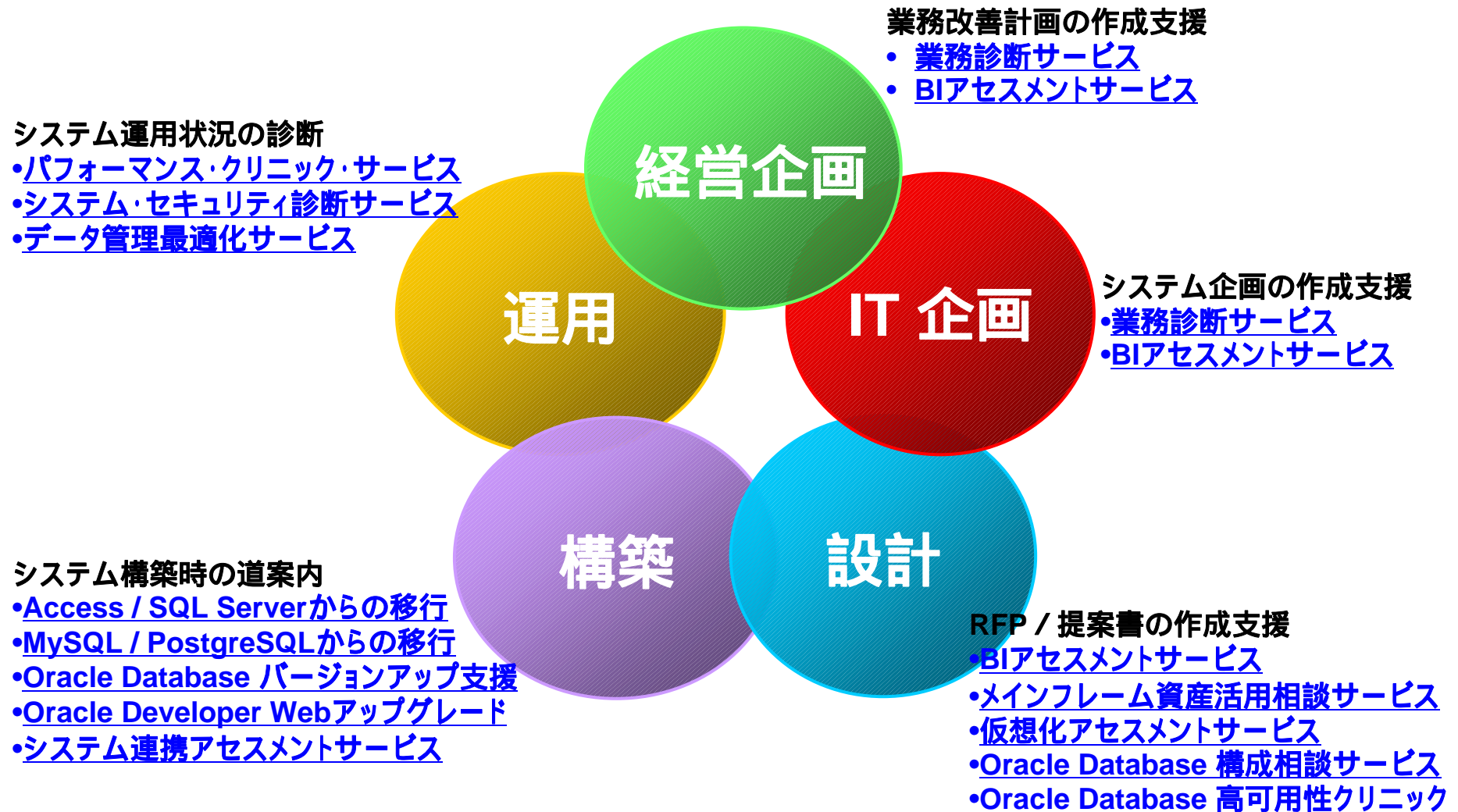
過去の 세미나資料、動画コンテンツはOTNの
「OTNコンテンツ オン デマンド」へ

세미나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、 세미나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



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

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

セキュリティ関連全般

監査で指摘された! どうするIT全般統制

セキュリティ基本編

意外と簡単!? Database 11g
セキュリティ編

セキュリティ詳細項目

ここが知りたい!! アクセス監査の実装例

ここが知りたい!! ユーザ特定の実装例

ここが知りたい!! 認証統合の実装例

実践!! セキュリティ対策
～ 暗号化編 ～

Oracle By Example

セキュリティ

Transparent Database Encryptionの使用

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関し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