

Oracle Direct Seminar



ORACLE®

Oracle on Windows ～セキュリティ編～

日本オラクル株式会社

Oracle Direct

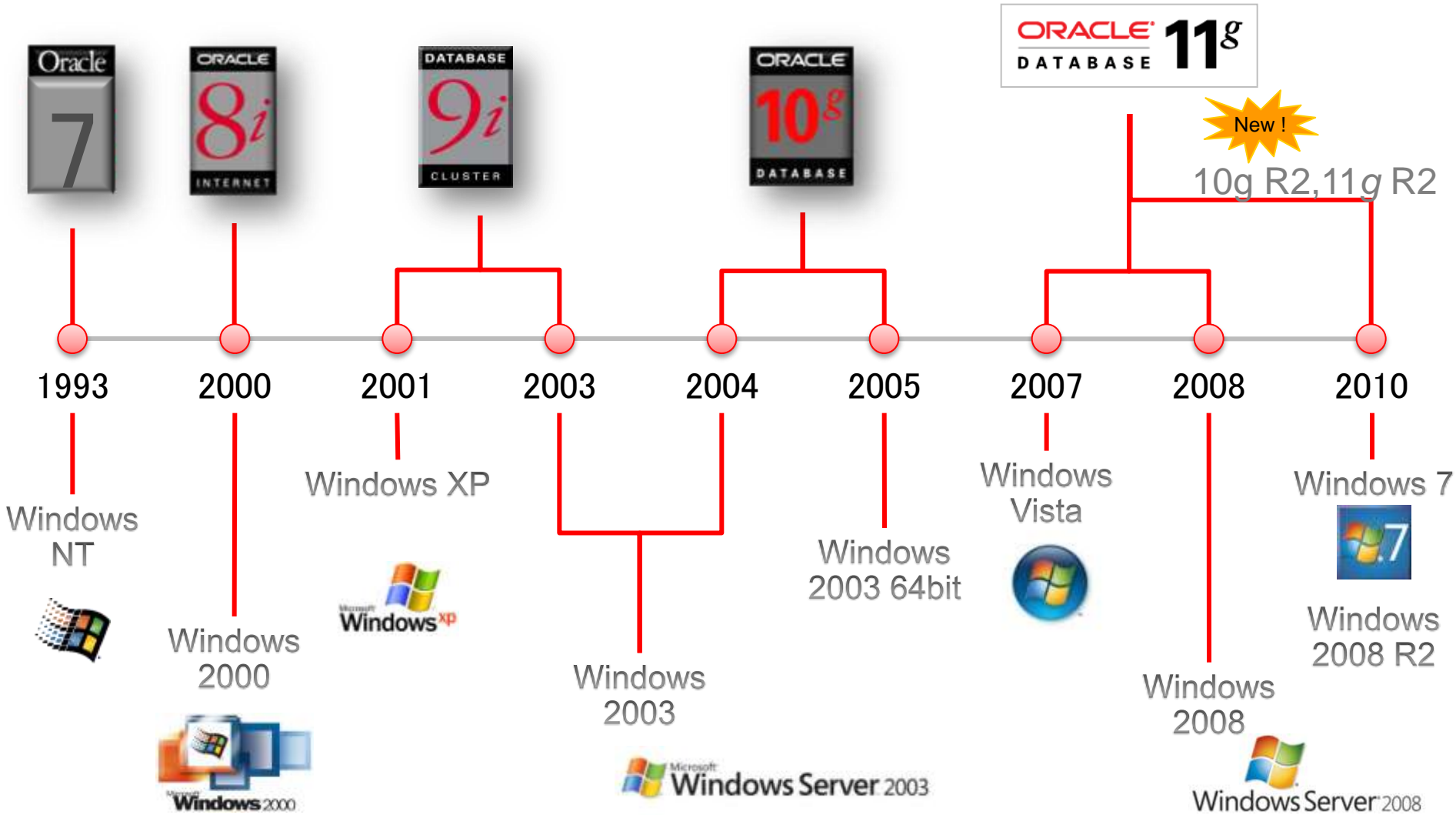


Agenda

- **Windows ServerとOracle Databaseについて**
- 最低限知っておいてほしい、セキュリティ面でのポイント
 - Windowsユーザー向け
 - .NET開発者向け

Windows 2008 R2 / Windows 7 に対応！

Oracle Database 10g Release2, 11g Release 2 に対応



Windows (x86) サポート状況

Operating System	9i R2	10g R1	10g R2	11g R1	11gR2
Windows 2000	○	○	○	○	-
Windows XP Professional	○	○	○	○	○
Windows Server 2003	○	○	○	○	○
Windows Server 2003 R2	○	○	○	○	○
Windows Vista	-	-	○	○	○
Windows Server 2008	-	-	○	○	○
Windows Server 2008 R2	-	-	-	-	-
Windows 7	-	-	○	-	○

Windows (x64) サポート状況

Operating System	9i R2	10g R1	10g R2	11g R1	11g R2
Windows XP	-	-	○	○	○
Windows Server 2003	-	-	○	○	○
Windows Server 2003 R2	-	-	○	○	○
Windows Vista	-	-	○	○	○
Windows Server 2008	-	-	○	○	○
Windows Server 2008 R2	-	-	○	-	○
Windows 7	-	-	○	-	○

11g R2 on Windows 対応OS一覧

<注意> RAC,ASMを利用する場合には**64bit**のOSを選択

対応OS一覧		DB11.2		Client11.2		Grid Infra11.2	
		32bit	64bit	32bit	64bit	32bit	64bit
Microsoft Windows Server 2008 R2	64bit	-	○	○	○	-	○ (*1)
Microsoft Windows Server 2008	32bit	○	-	○	-	×	-
	64bit	-	○	○	○	-	○ (*1)
Microsoft Windows Server 2003 R2	32bit	○	-	○	-	×	-
	64bit	-	○	○	○	-	○
Microsoft Windows Server 2003	32bit	○	-	○	-	×	-
	64bit	-	○	○	○	-	○
Microsoft Windows 7	32bit	○	-	○	-	×	-
	64bit	-	○	○	○	-	×
Microsoft Windows Vista	32bit	○	-	○	-	×	-
	64bit	-	○	○	○	-	×
Microsoft Windows XP	32bit	○	-	○	-	×	-
	64bit	-	○	○	○	-	×

*1 ACFSは Windows Server 2003 x64, Windows Server 2003 R2 x64のみの提供

Oracle Databaseのインストール

- 「意外と簡単!?!」シリーズでインストール方法を詳細解説



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

Oracle Database 11g R2 for Windows

- Oracle Database 11g R2 ダウンロード
 - <http://www.oracle.com/technology/global/jp/software/products/database/index.html>
- Oracle Database 11g R2 マニュアル
 - <http://www.oracle.com/technology/global/jp/documentation/database.html>
- 【チュートリアル】意外と簡単!? Oracle Database 11g Release2 - Windows版「データベース構築編」
 - <http://www.oracle.com/technology/global/jp/columns/easy/index.html>

11g R2 on Windows Install Tips

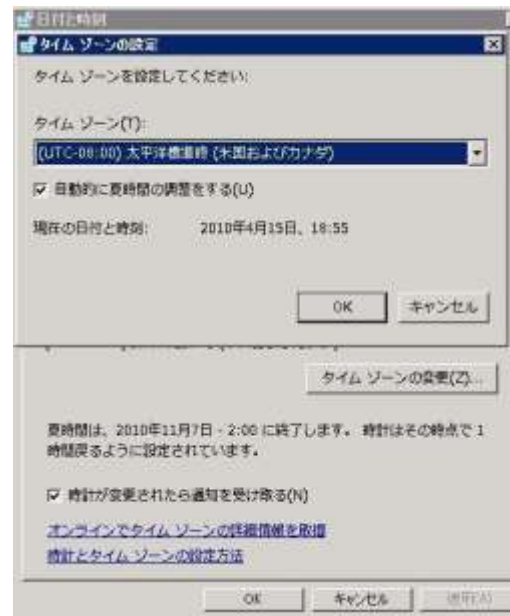
- OTN-Jからダウンロードできます。
- <http://www.oracle.com/technology/global/jp/software/products/database/index.html>



ダウンロード後、2つのzipファイル内のdatabaseディレクトリが統合されるよう、同一ディレクトリに解凍

11g R2 on Windows Install Tips

- タイムゾーンの設定を「太平洋標準時」に変更
- 「自動的に夏時間の調整をする」にチェック
- 再度東京のタイムゾーンに変更します。



上記手順を行わないと、Oracle Databaseの運用管理ツールである、Enterprise Managerの起動に失敗する場合があります

Agenda

- Windows ServerとOracle Databaseについて
- **最低限知っておいてほしい、セキュリティ面でのポイント**
 - **Windowsユーザー向け**
 - **.NET開発者向け**

Windows 向け Oracle Database の機能

- Windows サービスとの統合



- Active Directory との統合
- COM+サービス(MTS) との統合
- MSFC(MSCS) との統合



- VSSライター対応

- NAS でのパフォーマンス向上



- Oracle Database 11g Direct NFS Client

- .NET + Oracle Database の親和性

- データベースへの高速アクセス / Oracle Data Provider for .NET
- 開発生産性の向上 / Oracle Developer Tools for Visual Studio .NET
- 開発言語の統一 / Oracle Database Extensions for .NET

認証: ユーザーの管理

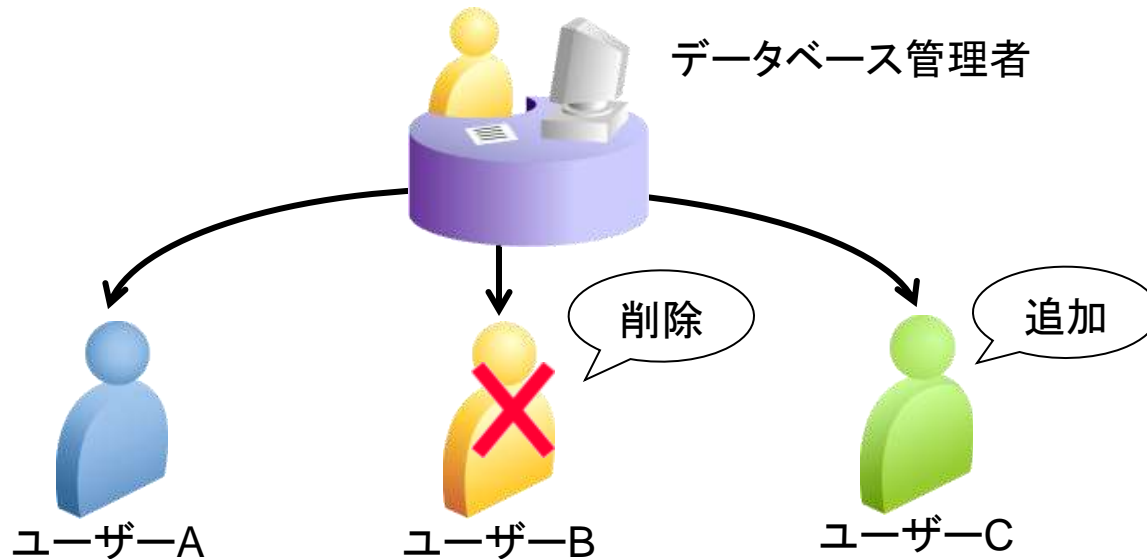


※Windows におけるユーザー認証の詳細については、以下のマニュアルをご覧ください

<http://otndnld.oracle.co.jp/document/products/oracle11g/111/windows/E05885-05/authen.htm#i1007802>

データベース・ユーザーとは

- データベース・ユーザー：
データベース内に接続するためのアカウント



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

Oracle Enterprise Manager によるセキュリティ管理 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

ORACLE Enterprise Manager 11g Database Control

データベース > 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

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

アクション 類似作成 前へ 1-25 / 38 次へ 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

ユーザーアカウントの
管理作業を実行

- ・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

ユーザー管理のポイント(1)

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に、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きましょう

セキュリティを向上
不正アクセスを防止



不要なユーザー



必要なユーザー

ユーザー管理のポイント(2)

プロファイルを利用してセキュリティを強化

- ・ 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。

Windows 固有のユーザー管理 ポイント(1)

Windows認証

- Oracle Databaseでは、データベース・ユーザーの認証にWindowsのユーザー・ログオン資格証明を使用できます。これには次の利点があります。

Windows認証の利点

- ユーザー名またはパスワードを入力しなくても、Oracle Databaseに接続できます。
- ユーザー・パスワードまたはロールの情報をOracle Databaseに格納して管理する必要がなくなります。



Windows 固有のユーザー管理 ポイント(1)

Windows認証

- Windows認証を利用するには、クライアントとデータベース・サーバーの両方で、次のファイル内のパラメータ SQLNET.AUTHENTICATION_SERVICESにntsを含む必要があります。



SQLNET.ORA

•SQLNET.AUTHENTICATION_SERVICES= (NTS)

ORACLE_BASE¥ORACLE_HOME¥network¥admin¥sqlnet.ora

Windows 固有のユーザー管理 ポイント(1)

Windows認証

- Oracle Databaseでは、データベース・ユーザーの認証にWindowsのユーザー・ログオン資格証明を使用できます。これには次の利点があります。

Windows認証の利点

- ユーザー名またはパスワードを入力しなくても、Oracle Databaseに接続できます。
- ユーザー・パスワードまたはロールの情報をOracle Databaseに格納して管理する必要がなくなります。



Windows 固有のユーザー管理 ポイント(1)

Windows認証

- Windows認証を利用するには、クライアントとデータベース・サーバーの両方で、次のファイル内のパラメータ SQLNET.AUTHENTICATION_SERVICESにntsを含む必要があります。



SQLNET.ORA

•SQLNET.AUTHENTICATION_SERVICES= (NTS)

ORACLE_BASE¥ORACLE_HOME¥network¥admin¥sqlnet.ora

Windows 固有のユーザー管理 ポイント(2)

Oracle ネット・サービス・ディレクトリ・ネーミング機能

- Oracle ネット・サービス・ディレクトリ・ネーミング機能の提供
 - tnsnames.ora ファイルのクライアント配布が不要
 - 中央管理による運用管理コストの削減
 - Active Directory との認証統合

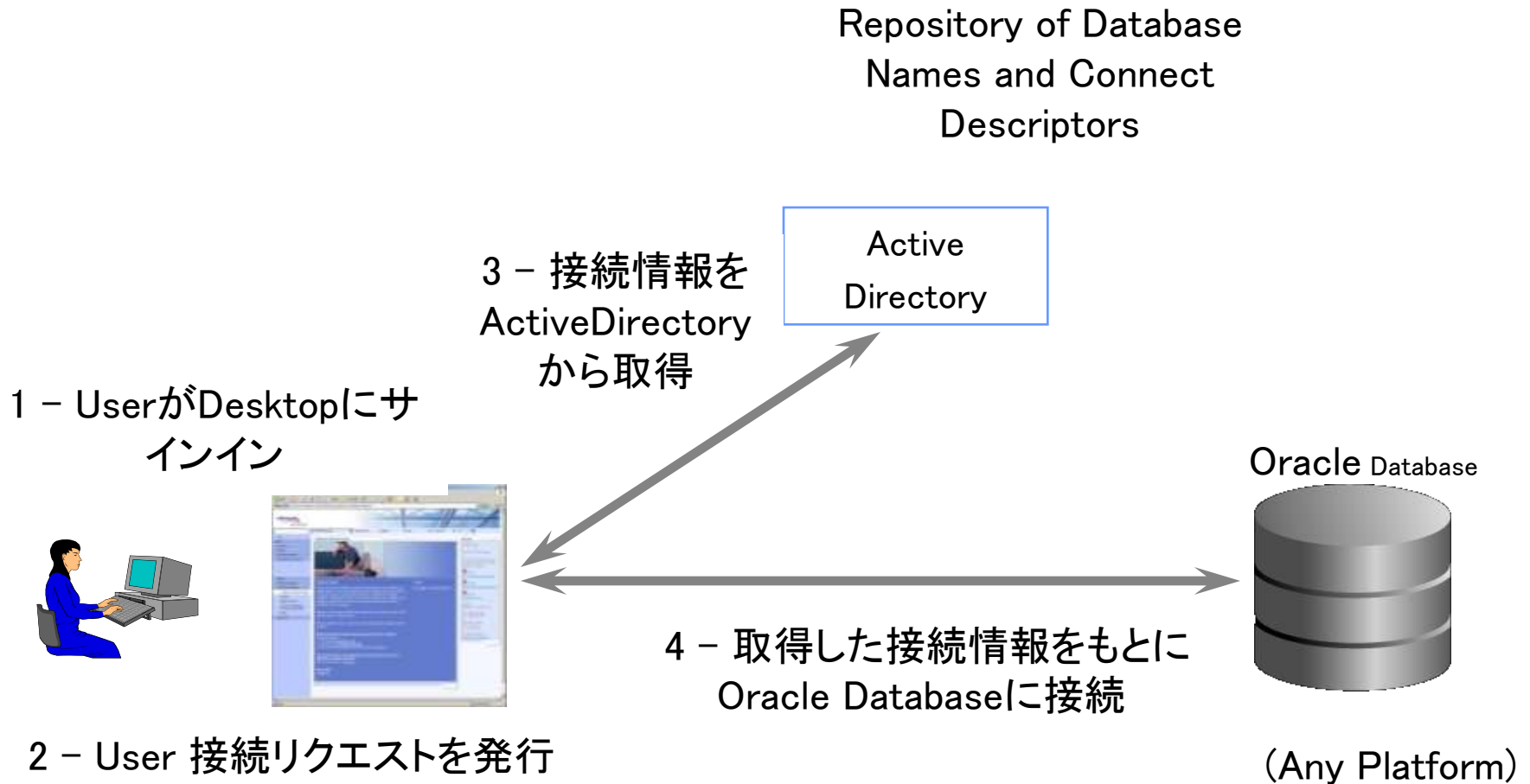
詳細な設定方法は、以下を参照してください。

Oracle Database プラットフォーム・ガイド 11g リリース 1 (11.1) for Microsoft Windows

– 13 Microsoft Active Directory との Oracle Database の使用

Windows 固有のユーザー管理 ポイント(2)

Oracle ネット・サービス・ディレクトリ・ネーミング機能



考慮すべきその他のセキュリティ関連項目

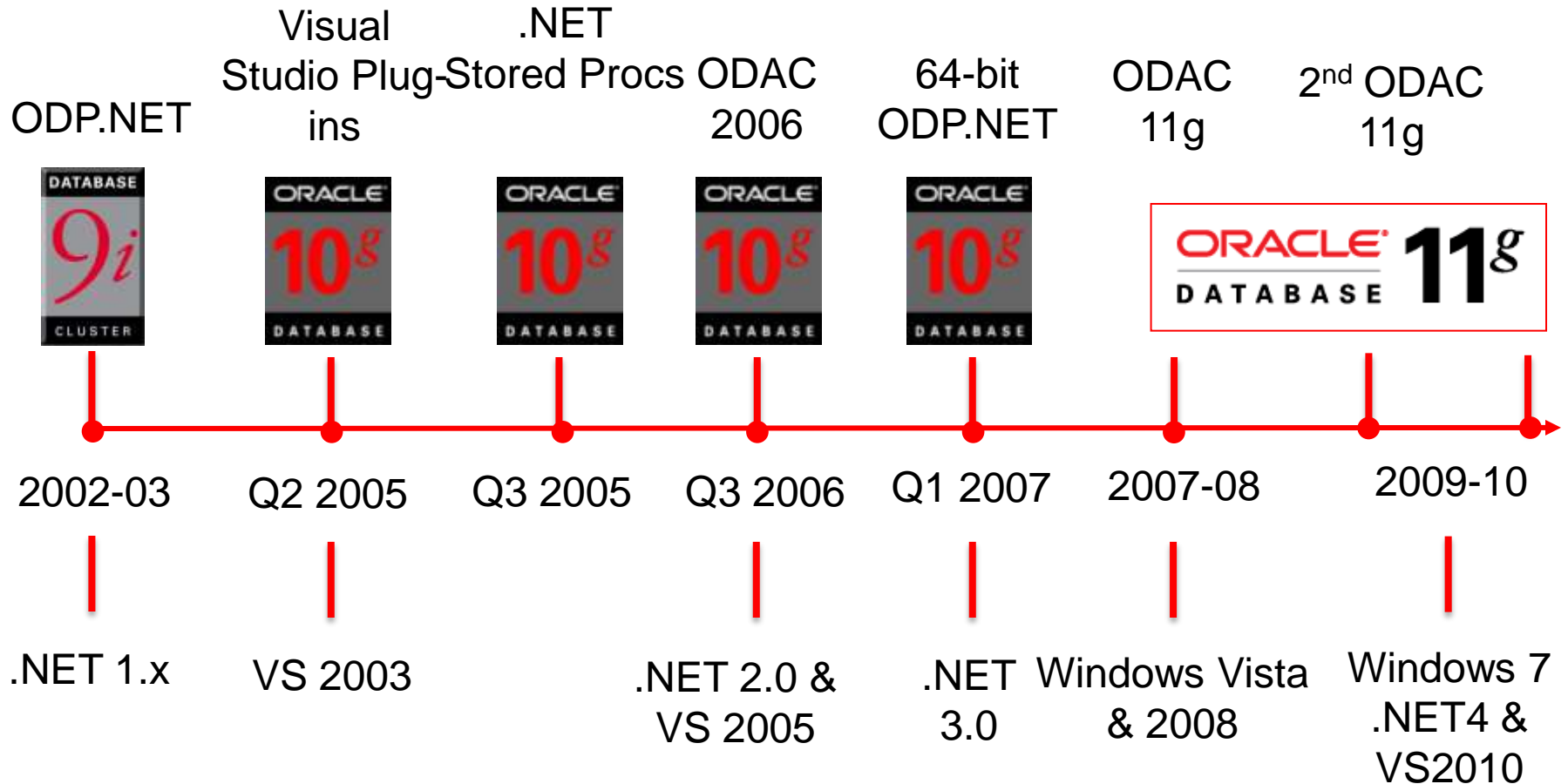
Oracle Databaseプラットフォーム・ガイド

- Windowsでのインストール後の構成タスク
 - Windowsファイアウォール
 - デフォルト・アカウントのパスワードのリセット
 - NTFSファイル・システムとWindowsレジストリの権限
 - Windowsでのスケジューラの外部ジョブ・サポートの構成
- <http://otndnld.oracle.co.jp/document/products/oracle11g/111/windows/E05885-05/config.htm#i1008781>

Agenda

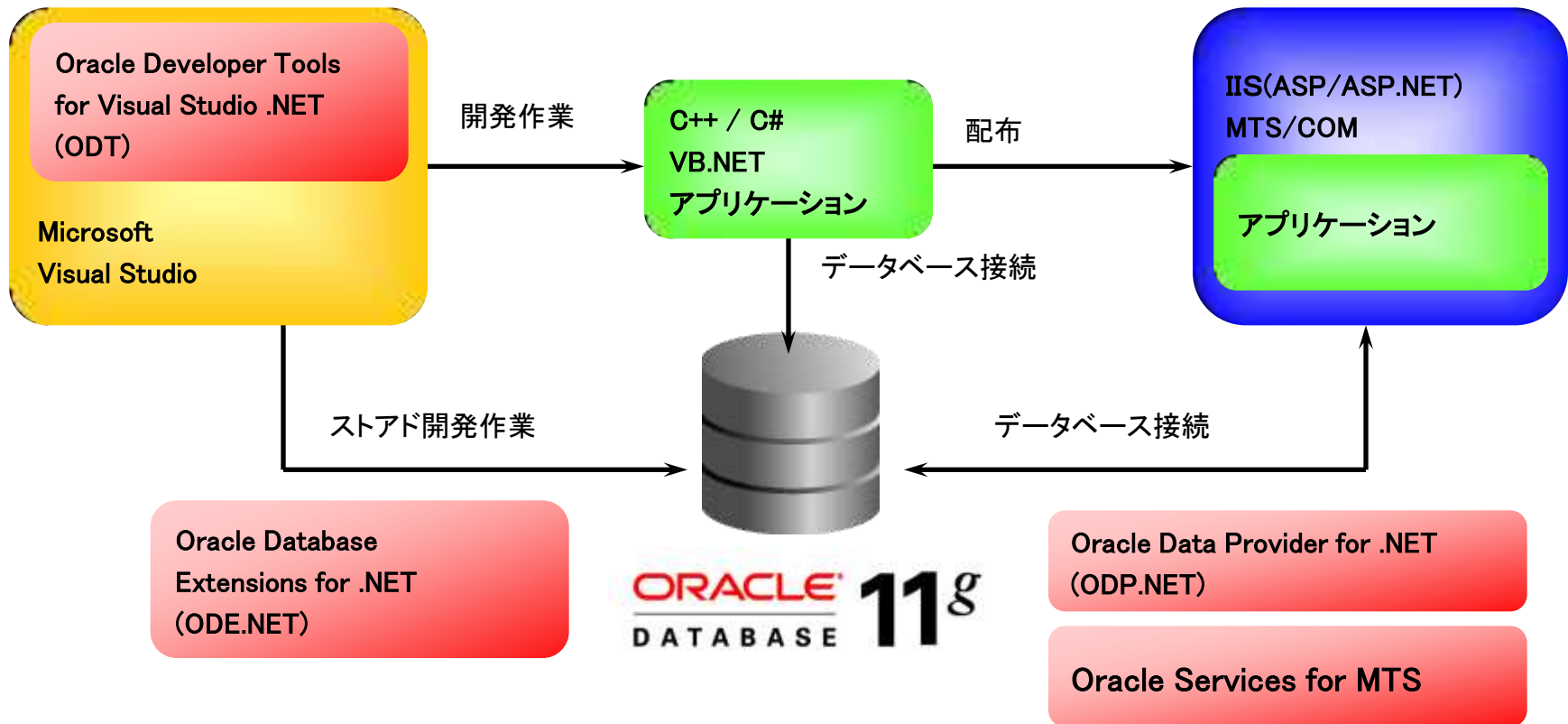
- Windows ServerとOracle Databaseについて
- **最低限知っておいてほしい、セキュリティ面でのポイント**
 - Windowsユーザー向け
 - **.NET開発者向け**

最新の.NET環境にいち早く対応



充実した開発ツール

- Visual Studio とも完全統合



Visual Studio 2005, 2008, 2010 および .NET Framework 2.0/3.x/4.0 に対応

ORACLE

.NET + Oracleでしか出来ない一押し機能 — セキュリティ —

.NET 関連のセキュリティ機能

Windows Native認証を利用したユーザー認証

```
Dim cnn As New OracleConnection  
  
cnn.ConnectionString = "User Id=/;Data Source=orcl;DBA Privilege=SYSDBA" ——— ①  
cnn.Open()  
  
MsgBox("Connect OK!!")  
cnn.Close()
```

- ①ConnectionString属性のUser Idを / に設定することにより、データベース・ユーザーの認証にWindowsユーザー・ログイン資格証明を使用できます。また、DBA Privilege属性を介してSYSDBA権限またはSYSOPER権限のいずれかを使用してOracleデータベースに接続

ODP.NET 11.1.0以上では、OS認証でも接続プーリングが有効

.NET 関連のセキュリティ機能

Client識別子の利用

```
Dim cnn As New OracleConnection

cnn.ConnectionString = "User Id=Scott;Password=Tiger;Data Source=orcl"
cnn.ClientId = "Hiroshi.Ota" —— ①
cnn.Open()

' -- SQL発行

cnn.Close()
```

- ① ClientIdプロパティに文字列をセットすることで、そのセッションに固有の名前を付けることが可能。通常、3層アプリケーションではアプリケーションからデータベースへの接続は同一のスキーマ(データベースのユーザー)を使用することが多いが、どのユーザーが接続しているのか把握できない。ClientIdを使用すると、クライアントの識別子を簡単にセットすることができるため、セキュリティの問題を解決する1つの方法となる。

.NET 関連のセキュリティ機能

パスワードの期限切れ

```
Dim cnn As New OracleConnection
cnn.ConnectionString = "User Id=scott;Password=tiger;Data Source=orcl"
Try
    cnn.Open()
Catch
    cnn.OpenWithNewPassword("panther") ——— ①
End Try
```

- ① Oracleユーザーのパスワードが期限切れだった場合、新しいパスワードで接続をオープンすることが可能

.NET 関連のセキュリティ機能

Proxy認証を利用したユーザー認証

```
Dim conn As New OracleConnection( _  
    "User Id=user1;Password=xxxx;Proxy User Id=proxyuser;" + _  
    "Proxy password=xxxxxxxxxx;Data Source=orcl")  
conn.Open()  
conn.close()
```

プロキシ認証を行うための接続文字列

上記のサンプルコードを実行する前に、プロキシ認証を行うためのユーザーを作成します

```
CREATE USER user1 IDENTIFIED BY oracle;  
GRANT CONNECT, RESOURCE TO user1;  
GRANT SELECT ON proxyuser.table1 TO user1;  
ALTER USER user1 GRANT CONNECT THROUGH proxyuser;
```


.NET 関連のセキュリティ機能

ODAC 11.1.0 新機能 Oracle Providers for ASP.NET

- ASP.NET 2.0/4.0に対応する以下の Provider を新たに提供
 - メンバーシップ・プロバイダ
 - ロール・プロバイダ
 - サイト・マップ・プロバイダ
 - セッション・ステート・プロバイダ
 - プロファイル・プロバイダ
 - Webイベント・プロバイダ
 - Webパーツ・パーソナライズ・プロバイダ
 - キャッシュ依存性プロバイダ



OTNセミナー オンデマンド コンテンツ

ダイセミで実施された技術コンテンツを動画で配信中!!
ダイセミのライブ感はそのままに、お好きな時間で受講頂けます。

最新のコンテンツ

 <p>エンジニアのための ITIL実践術 再生時間: 60分</p>	 <p>ここからはじめよう Oracle PL/SQL入門 再生時間: 60分</p>	 <p>実践!!高可用システム構築 -RAC基本 再生時間: 60分</p>	 <p>お悩み解決! Oracle のサイジング 再生時間: 60分</p>
--	--	---	--

Database

 <p>今さら聞けない!?バックアップ・リカバリ入 再生時間: 60分</p>	 <p>意外と簡単!? Oracle Database 11g -セ 再生時間: 60分</p>	 <p>実践!!バックアップ・リカバリ 再生時間: 60分</p>	 <p>意外と簡単!? Oracle Database 11g -デ 再生時間: 60分</p>
--	---	--	--

>> もっと見る

twitter

最新情報つぶやき中

oracletechnetjp

- ・人気コンテンツは?
- ・お勧め情報
- ・公開予告 など

OTN オンデマンド

検索

※掲載のコンテンツ内容は予告なく変更になる可能性があります。
期間限定での配信コンテンツも含まれております。お早めにダウンロード頂くことをお勧めいたします。

ORACLE

Oracle エンジニアのための技術情報サイト オラクルエンジニア通信

<http://blogs.oracle.com/oracle4engineer/>

twitter

最新情報つぶやき中
oracletechnetjp

- 技術資料
- ダイセミの過去資料や製品ホワイトペーパー、スキルアップ資料などを多様な方法で検索できます
- キーワード検索、レベル別、カテゴリ別、製品・機能別
 - コラム
- オラクル製品に関する技術コラムを毎週お届けします
- 決してニッチではなく、誰もが明日から使える技術の「あ、そうだったんだ！」をお届けします



こんな資料が人気です

- ✓ 6ヶ月連続で「**RAC/ASMインストール資料**」が第一位。根強い人気のチュートリアル系コンテンツですが、**レプリケーション**解説資料が上位に挙がってきました。
- ✓ **.NetやWindowsサーバー**ならではの**機能**を集めた特集ページも好評です。

オラクルエンジニア通信



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

■ パフォーマンス診断サービス

- Webシステム ボトルネック診断サービス **NEW**
- データベースパフォーマンス 診断サービス

■ 移行支援サービス

- SQL Serverからの移行支援サービス
 - DB2からの移行支援サービス
 - Sybaseからの移行支援サービス
 - MySQLからの移行支援サービス
- Postgre SQLからの移行支援サービス
 - Accessからの移行支援サービス
- Oracle Application ServerからWeblogicへ移行支援サービス **NEW**

■ システム構成診断サービス

- Oracle Database構成相談サービス
 - サーバー統合支援サービス
 - 仮想化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
 - BI EEアセスメントサービス
 - 簡易業務診断サービス

■ バージョンアップ支援サービス

- Oracle Databaseバージョンアップ支援サービス
- Weblogic Serverバージョンアップ支援サービス **NEW**
- Oracle Developer/2000(Froms/Reports) Webアップグレード相談サービス

オラクル社のエンジニアが 直接ご支援します
お気軽にご活用ください!

オラクル 無償支援

検索

ORACLE



1日5組限定!

製品無償評価サービス

提供シナリオ

- ・データベースチューニング
- ・無停止アップグレード
- ・アプリケーション性能・負荷検証
- ・Webシステム障害解析

製品をインストールせず無償で体験いただけます

選べるサービスご提供方法

- ・弊社が用意したサーバー環境で、インターネット越しにお客様自身が製品を体感
- ・Web会議システムを通し、弊社エンジニアがデモンストレーションを実施

URL : <http://www.oracle.com/jp/direct/services/didemo-195748-ja.html>

Web問い合わせフォーム

お問い合わせフォームにて「製品評価サービス希望」と明記し、送信ください

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

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

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®

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す。