Oracle Direct Seminar

ORACLE®

30分で理解する！！

Oracle Database + Active Directory ベストプラクティス

日本オラクル株式会社

Oracle Direct

Oracle Direct Seminar

アジェンダ

- Active Directoryとは
- Active DirectoryとOracle Databaseの連携
- Active DirectoryとOracle Databaseを組み合わせた効率的な運用

無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle Database 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

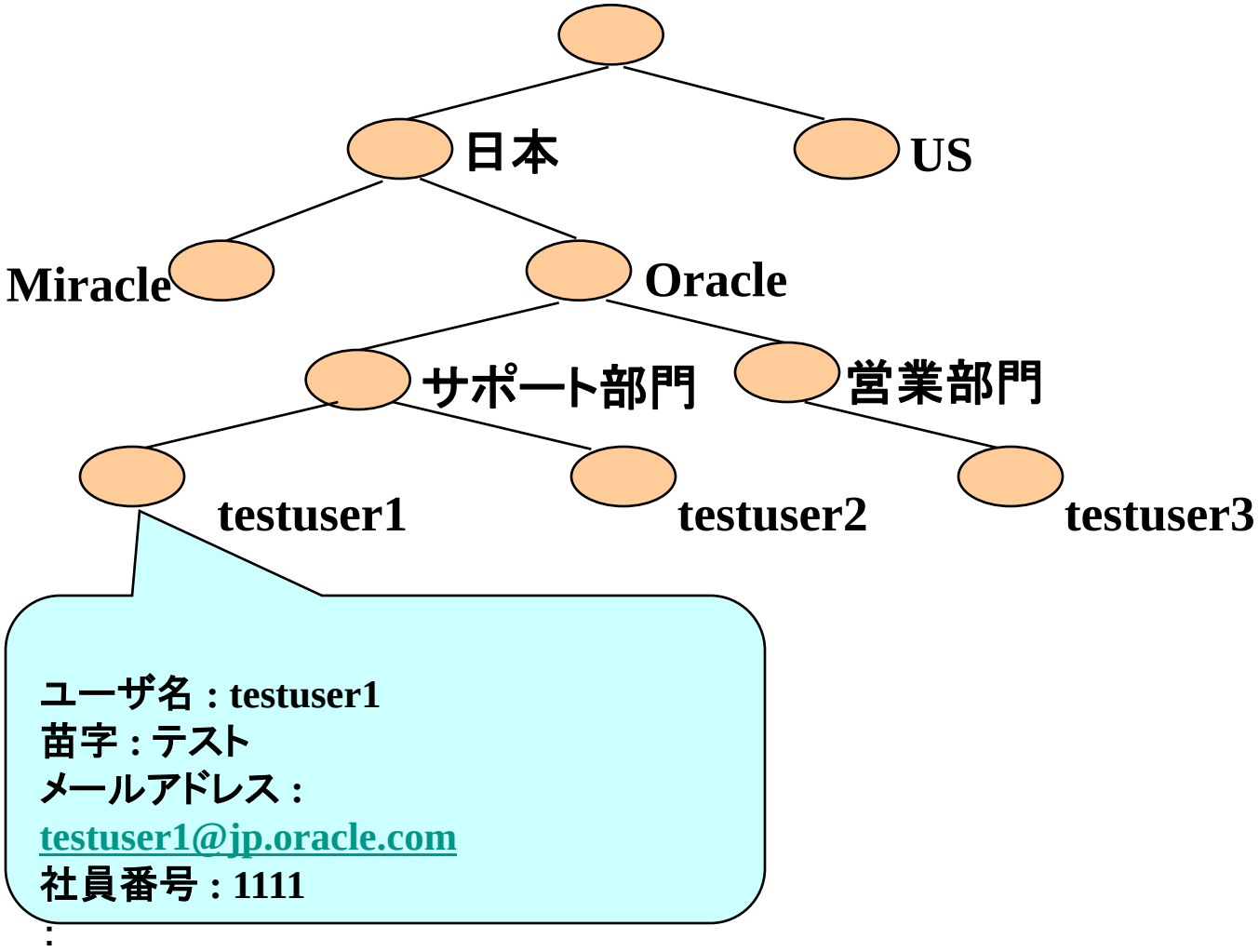
Microsoft Active Directoryとは

- 特徴
  - ユーザアカウントや共有プリンタなどのネットワークリソース管理を行うための「ディレクトリ・サービス」機能。
  - 「ディレクトリ・サービス」とは、ネットワークリソースやそれらが対応する場所を特定するデータベース。
  - Windows　2000からサポート
- 長所
  - PCログインと同時にドメインへのログインも同時に行われるためWindows共有リソース（共有フォルダなど）へのアクセスにパスワードを必要としない

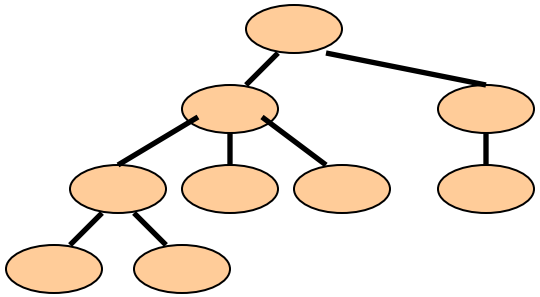
ディレクトリとは

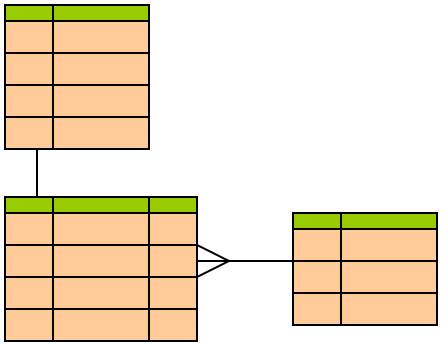
- 階層型データベース
- 元々は「住所氏名録」やビルの「住民案内板」の意味
- データ単位を「オブジェクト」として扱う
- X.500 シリーズ

ディレクトリとは – 構成要素



ディレクトリとは – RDB との比較





	ディレクトリ	RDBMS
データ表現	オブジェクトの階層構造	表の集合
データ間の構造	属性値を持つオブジェクトとその階層構造	データ同士の関連を扱う
検索・更新	静的なデータの検索に最適化	トランザクションサポートとそれを生かした検索・更新処理
プロトコル	標準プロトコル	独自プロトコル
格納データ	人、組織、ネットワーク機器、資源、セキュリティ情報	ビジネスデータ（商品情報、在庫情報、受注情報、人事情報　等）

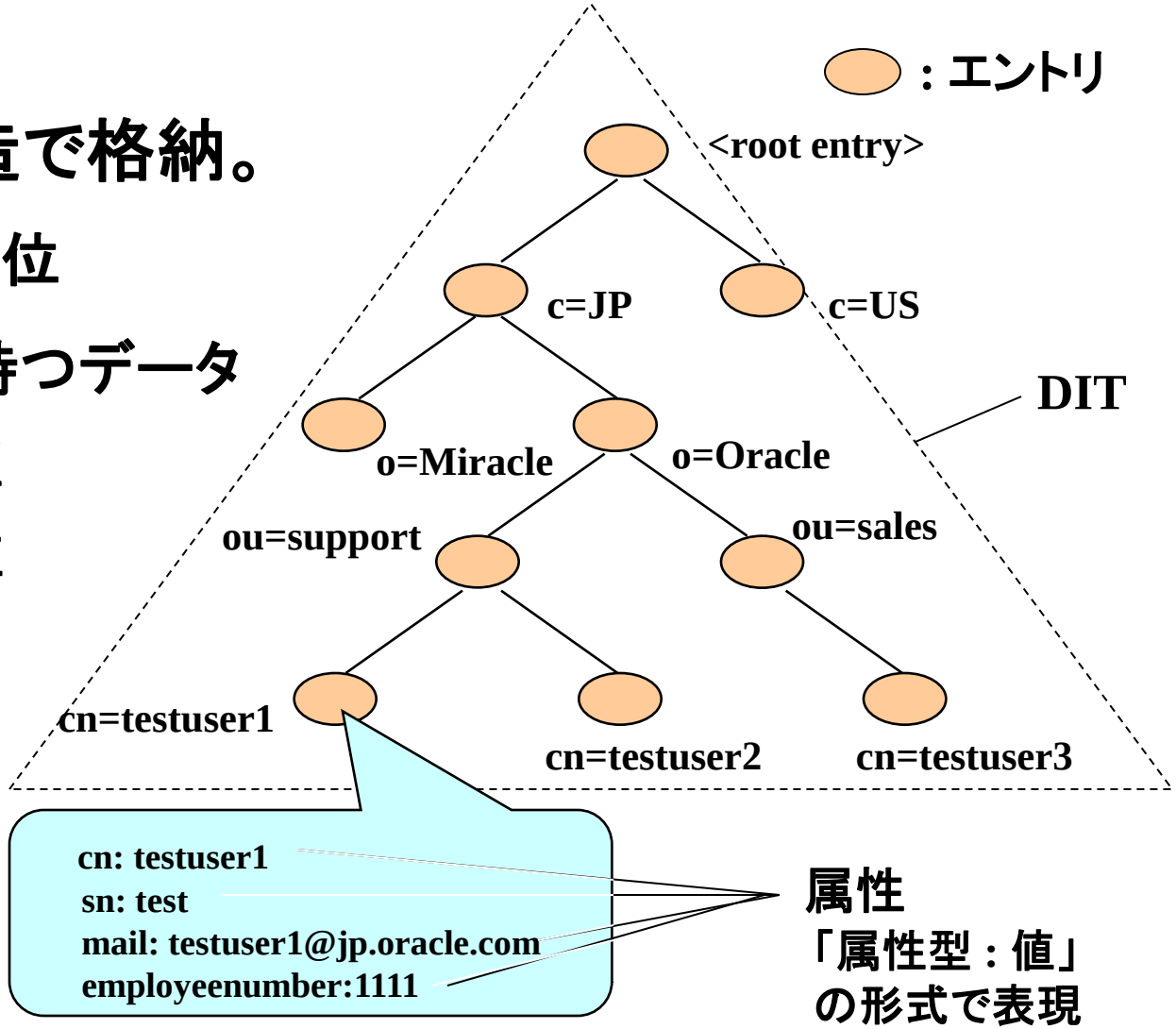
LDAPとは

- 軽量化されたディレクトリアクセスプロトコル
  (Lightweight Directory Access Protocol)
- 一般的なプロトコル(RFCで規定)
  - Active Directory
  - Oracle Internet Directory
  - Sun One Directory Server
  - Novell NDS
  - Open LDAP etc…

データ構造

データはツリー構造で格納。

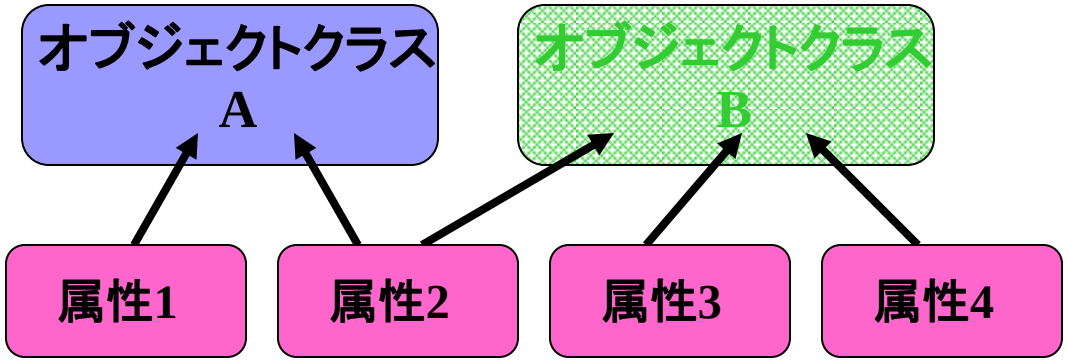
- エントリ：データの単位
- 属性：各エントリの持つデータ
  - 属性型：データの型
  - 属性値：データの値



エントリと属性

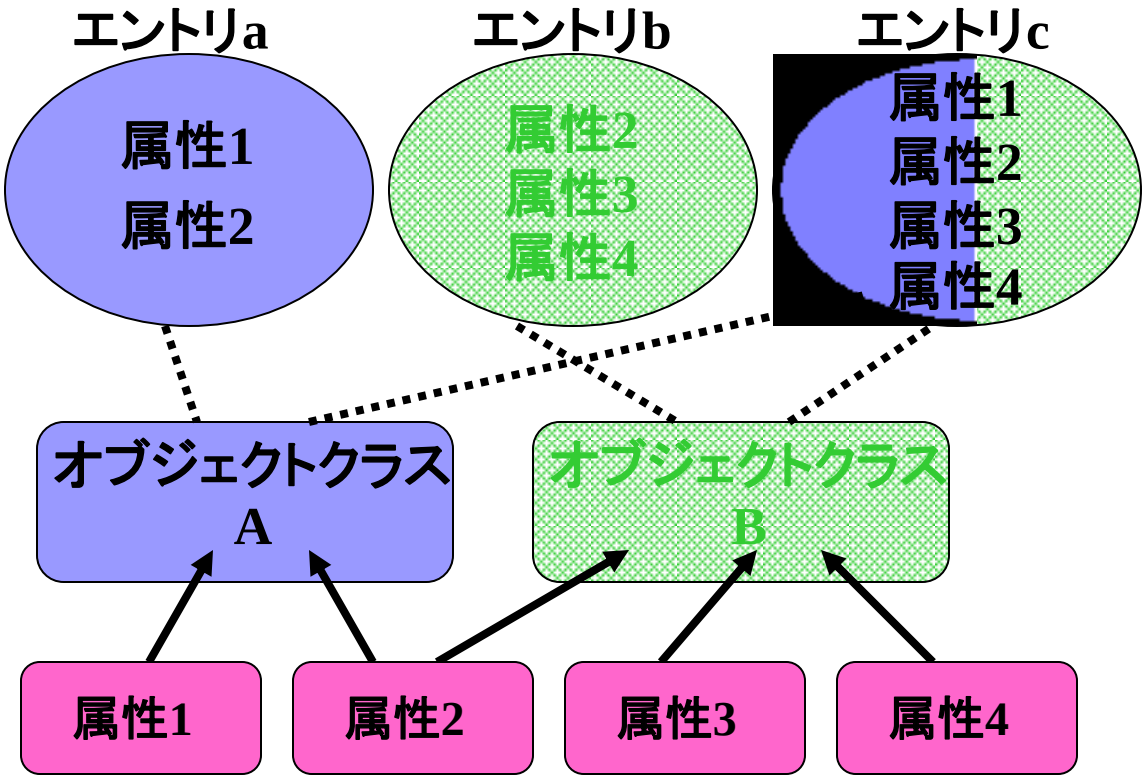
エントリで設定される属性は、そのエントリがどのオブジェクトクラスに属しているかにより決まる

オブジェクトクラス：
エントリの集まり



エントリと属性

エントリで設定される属性は、そのエントリがどのオブジェクトクラスに属しているかにより決まる



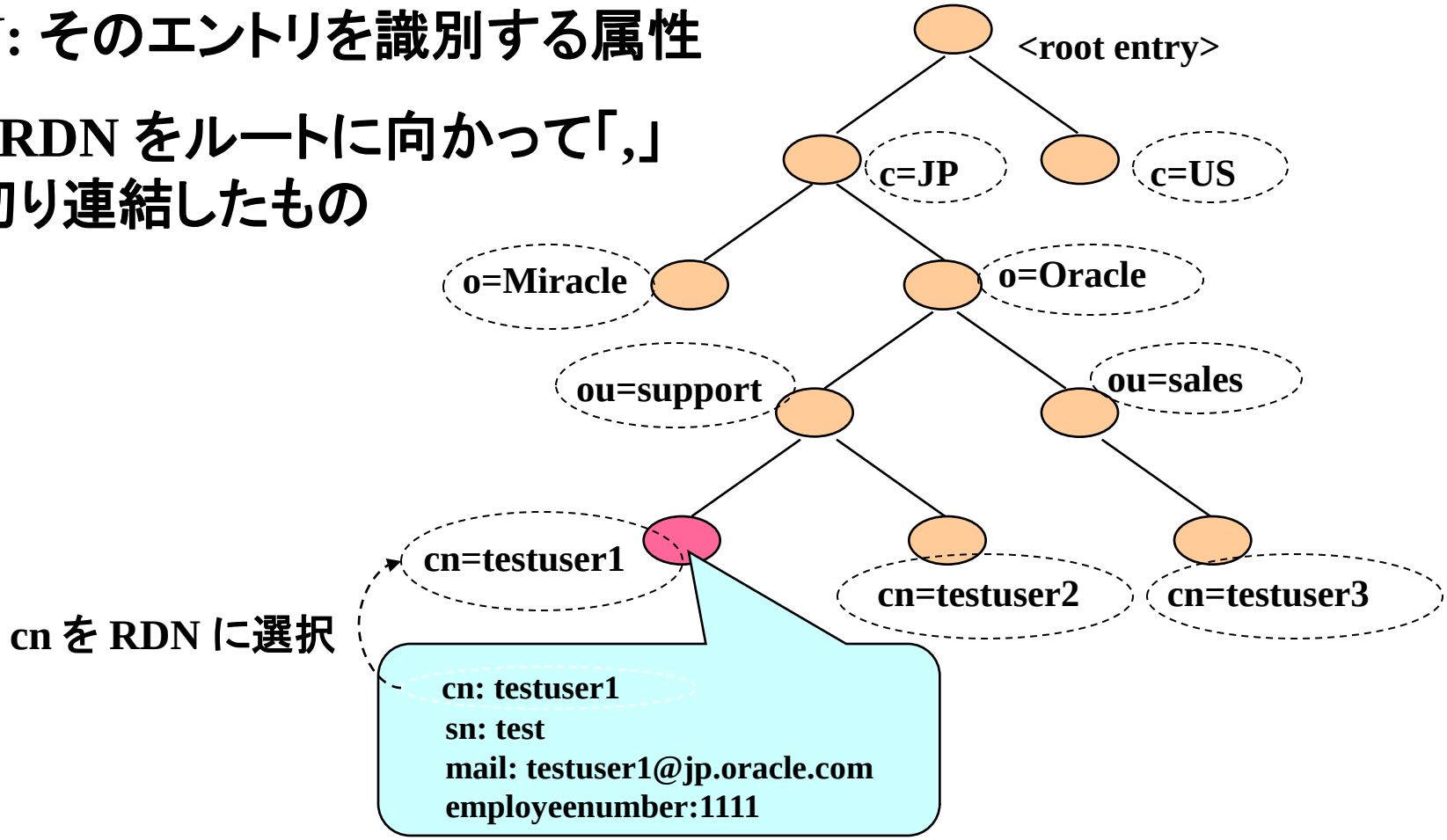
・オブジェクトクラスA に属しているエントリで設定可能な属性 = 属性1,2

・オブジェクトクラスB に属しているエントリで設定可能な属性 = 属性2,3,4

・オブジェクトクラスA,B ともに属しているエンとりで設定可能な属性 = 属性1,2,3,4

エントリの識別

- RDN: そのエントリを識別する属性
- DN: RDN をルートに向かって「,」で区切り連結したもの



● の DN は cn=testuser1,ou=support,o=Oracle,c=JP

アジェンダ

- Active Directoryとは
- Active DirectoryとOracle Databaseの連携
- Active DirectoryとOracle Databaseを組み合わせた効率的な運用

無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle Database 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

Active Directory + Oracle Database

- Active Directoryによる名前解決
  - 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(11g)
- Single Sign On
  - Windows ネイティブ 認証
  - Kerberos 認証

Active Directoryによる名前解決

Active Directoryによる名前解決

Overview

- 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(11g)
- Windowsツールとの統合
  - AD Userとコンピュータの管理
  - Oracle DB Configuration Assistant, Net Configuration Assistant and Net Manager

Active Directoryによる名前解決

Client OS	Server OS	AD	OID	Comments
Windows	Windows	Yes	Yes	
Windows	Any	Yes	Yes	Tools for registering Net Service in AD must be run on Windows
Linux/Unix	Any	No	Yes	AD Integration solutions can help

Active Directoryによる名前解決
Configuration/Administration

1 –Administrator による**Active Directory**のスキーマ変更

2 – NetCAによるスキーマ登録

5 – NetCAによる **Directory Naming** と **Directory Usage (AD)** の設定

Windows Environment

3 – NetCAによる**Naming Context** の作成

4 - DBCA or Net Managerによるデータベースの登録

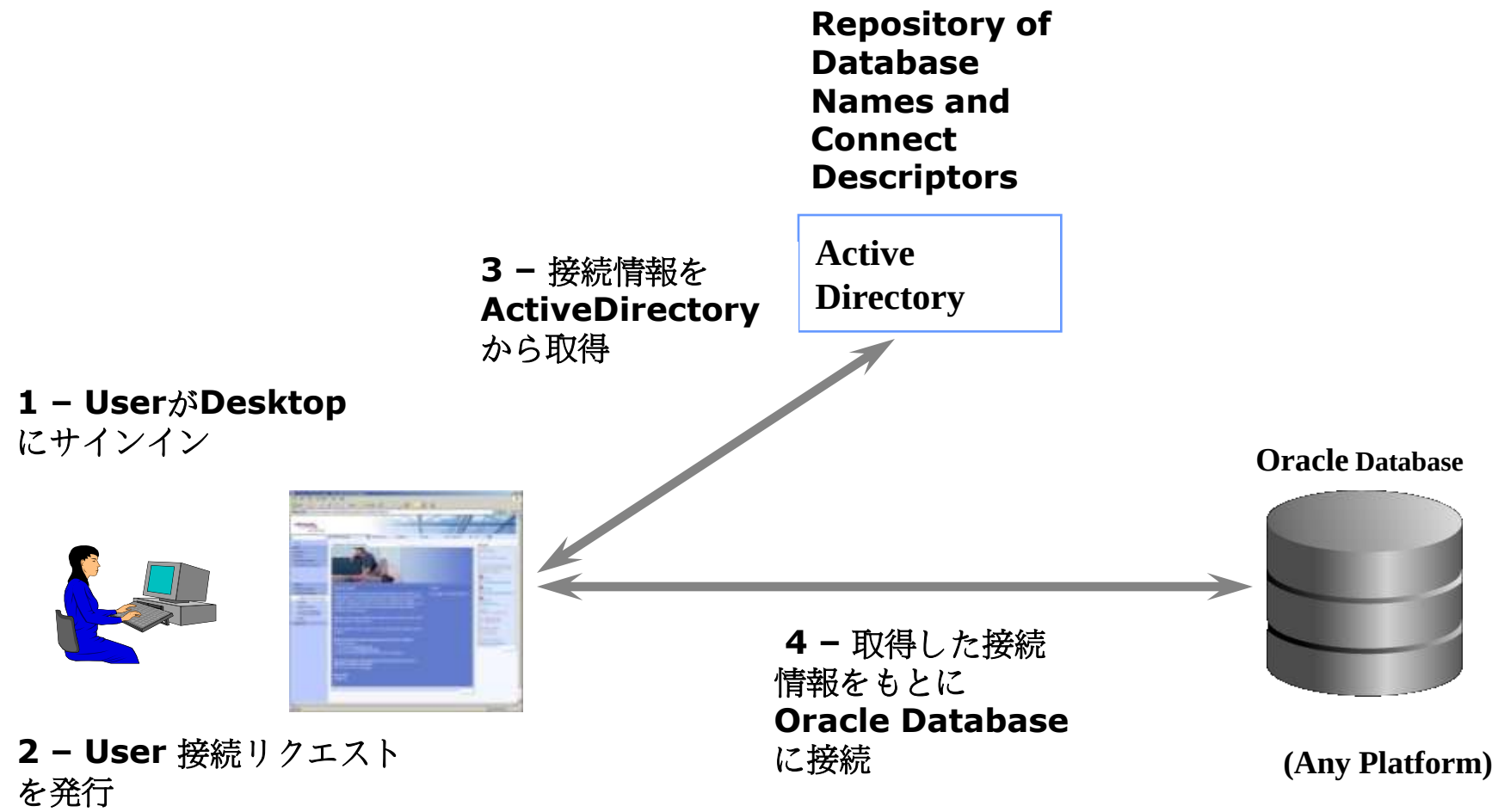
Active Directory

Repository of Database Names and Connect Descriptors

Client Systems

Active Directoryによる名前解決

Run-time



Active Directoryによる名前解決
Summary

1. NetCA - Active Directory スキーマの変更
2. NetCA - Naming Contextの生成
3. DBCA (Net Manager) - Acitive Directoryにデータベースの登録
4. NetCA - Directory Naming と Directory Usage (AD) と修正
5. SQLNET.ORA の編集（11g client）
   NAMES.LDAP_AUTHENTICATE_BIND=Yes

To support pre-11g clients

1. anonymous bind の有効化（in AD）
2. ACLs for Oracle Naming Context と Database/Net Services objects
   anonymous ユーザがアクセスできるように変更

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

Single Sign-On

Single Sign-On

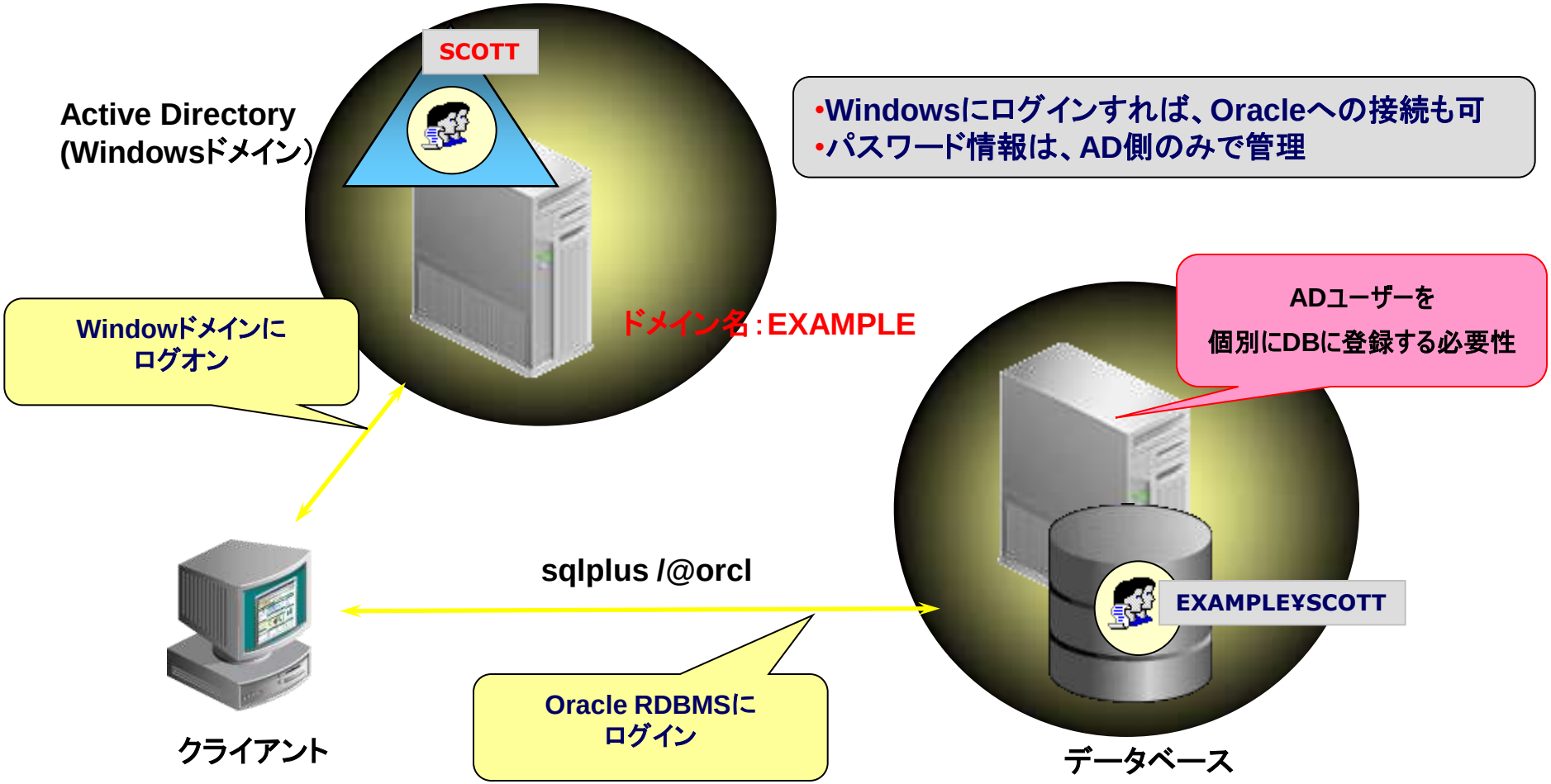
Authentication	Client OS	Server OS	Comments
Windows ネイティブ認証	Windows	Windows	•全てのEditionで利用可能 •暗黙的にMS KDCを利用 •外部認証メカニズム •Enterprise User Security は未サポート
Kerberos 認証	Any	Any	•EE and ASO option が必要 •MS KDC をサポート •外部認証メカニズム •Enterprise User Security をサポート

Windows ネイティブ 認証

Basics

- ORA_DBA: SYSDBA 権限
- ORA_OPER: SYSOPER権限
- External user を Oracle DBに作成する必要があります。
  - create user “Sales¥frank” identified externally;
- Windows groups can be used to assign roles (*os_roles* が trueの場合)
  - create role sales identified externally;

Windows ネイティブ認証の概要



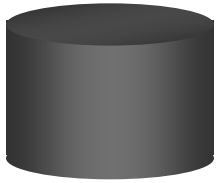
Windowsにログインすれば、Oracleへの接続時に、ユーザーID/パスワードは不要

Windows ネイティブ認証の動作

1 - UserがDesktopにサインイン

2 – UserがOracleにサインインを実施

Active Directory/KDC



3 – セキュリティプロトコルで通信を行い**security tokens**の交換

4 – 外部ユーザーとして認証

5 –Windows Group membershipsの検索 **(os_roles** が **true**の場合**)**

6 – データベースのロールかグループメンバーシップに基づきロールの割り振り **(based on os_roles)**

Windows ネイティブ 認証

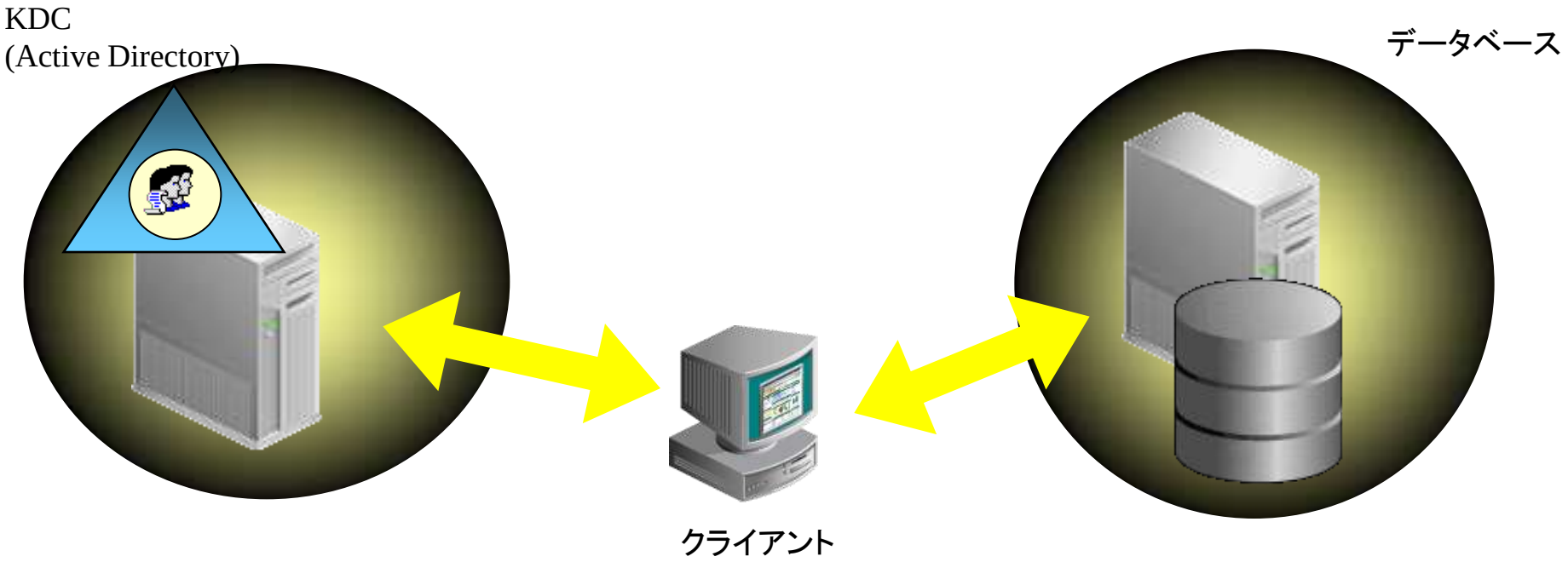
Configuration

- init.oraに *os_authent_prefix* to “” を設定
- *sqlnet.authentication_services* NTS を sqlnet.oraにセット (default設定)
- *os_roles* to true を init.ora に設定

  （Windows Group Membership for role authorizationを使用したい場合）

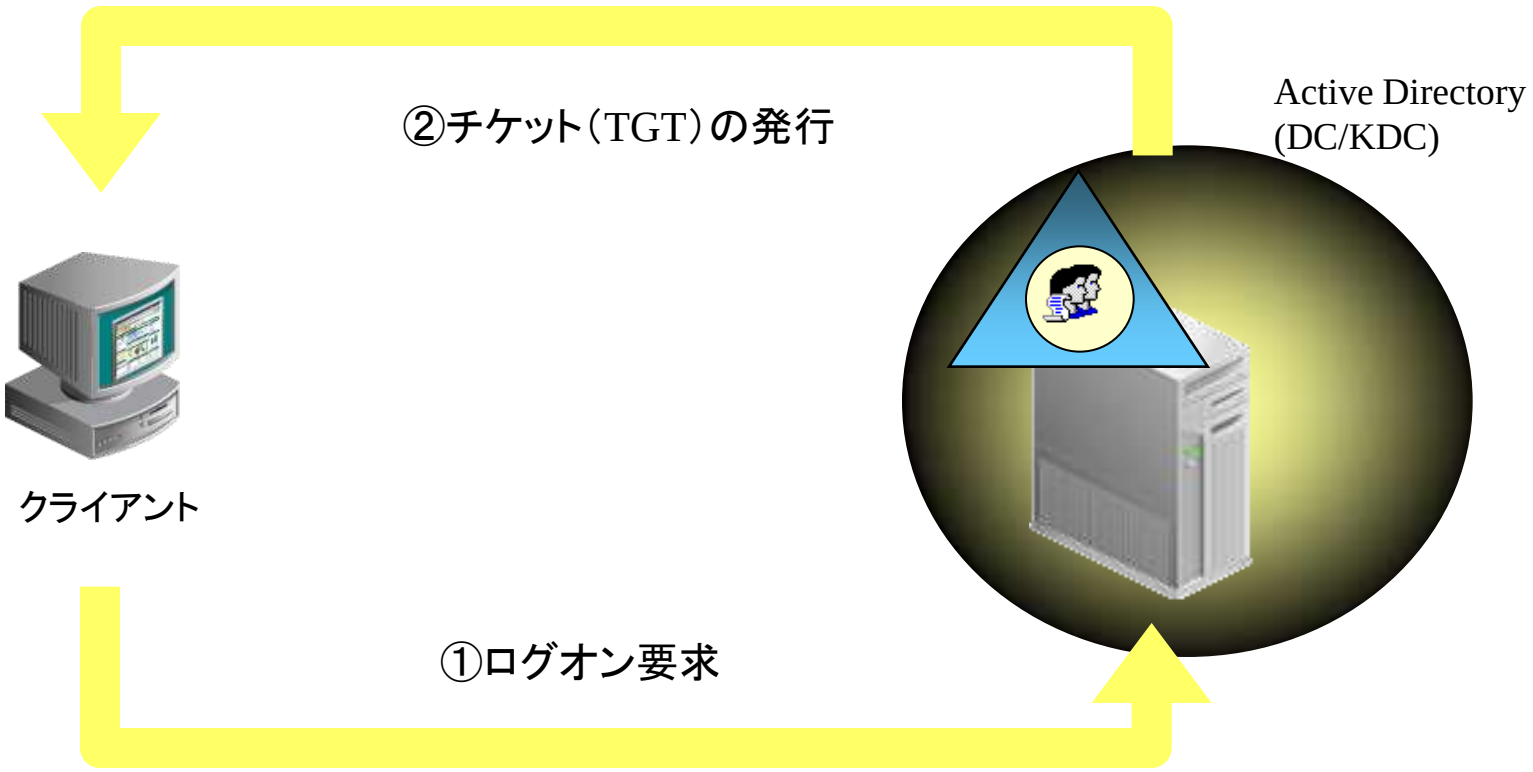
Kerberos 認証

Windows以外のプラットフォームでOracleが稼動している場合は、Kerberos アダプタを使用してActive Directoryと認証を統合することが可能です。



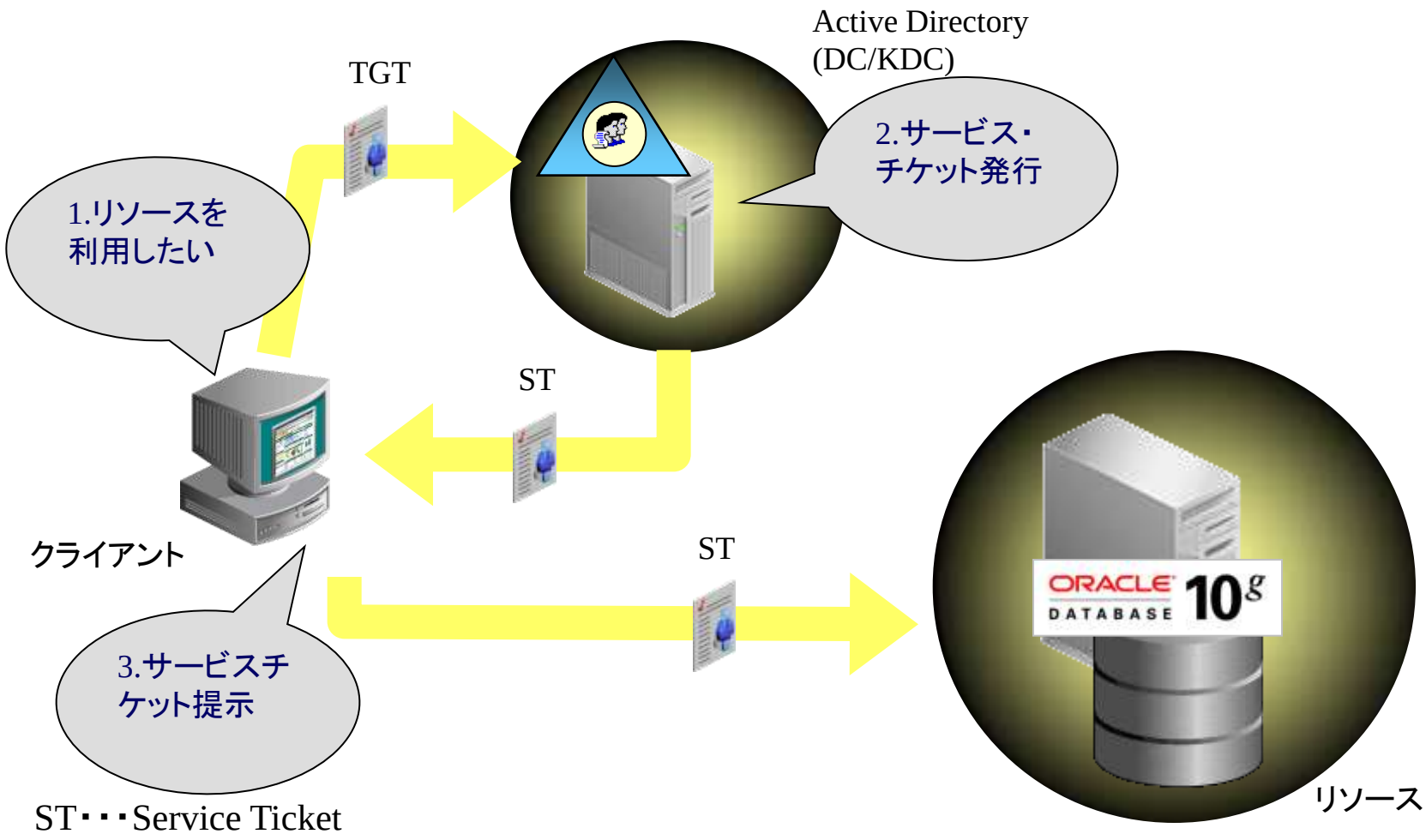
1. もちろん、AD以外のKDC(Key Distribution Center)サーバーでもこの機能は利用可能です
2. Kerberos認証アダプタの機能を利用するには、Advanced Security Optionが必要です

Kerberosによる認証の仕組み(1/3)



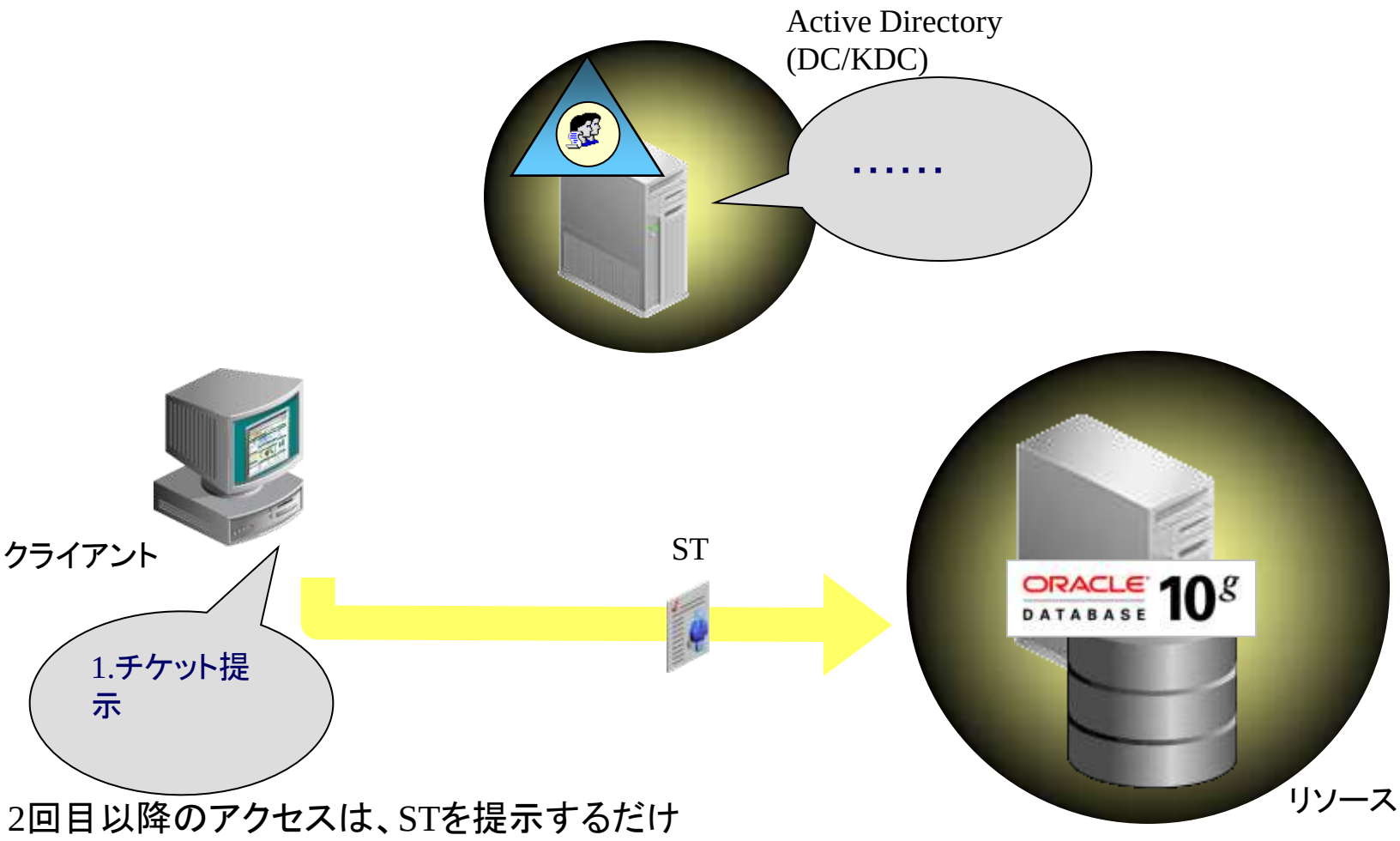
TGT・・・Ticket Granting Ticket
DC・・・Domain Controller
KDC・・・Key Distribution Center

Kerberosによる認証の仕組み(2/3)



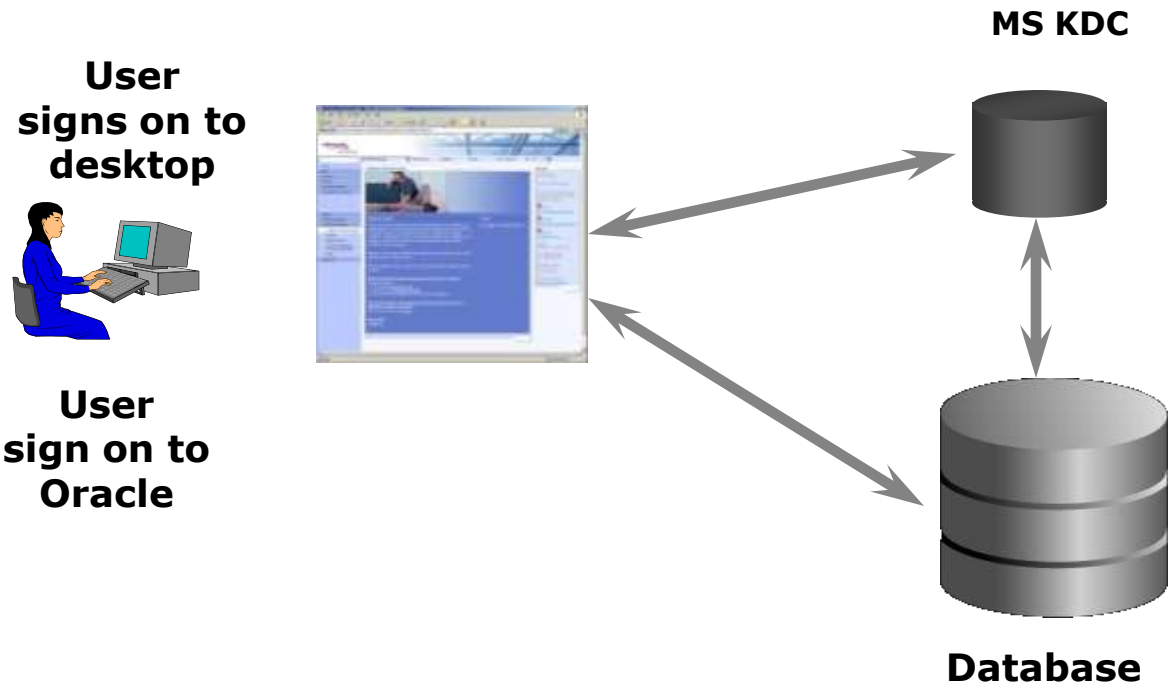
ST・・・Service Ticket

Kerberosによる認証の仕組み(3/3)



2回目以降のアクセスは、STを提示するだけ

Kerberos 認証の動作



外部ユーザーとして認証

Example:

```
SQL> CREATE USER KRBUSER IDENTIFIED EXTERNALLY AS
'KerberosUser@SOMEORGANIZATION.COM';
SQL> Grant connect, resource to KRBUSER;
```

アジェンダ

- Active Directoryとは
- Active DirectoryとOracle Databaseの連携
- Active DirectoryとOracle Databaseを組み合わせた効率的な運用

無償技術サービスOracle Direct Concierge

・SQL Serverからの移行アセスメント
・MySQLからの移行相談
・PostgreSQLからの移行相談
・Accessからの移行アセスメント
・Oracle Database バージョンアップ支援
・Oracle Developer/2000 Webアップグレード相談
・パフォーマンス・クリニック
・Oracle Database 構成相談
・Oracle Database 高可用性診断
・システム連携アセスメント
・システムセキュリティ診断
・簡易業務診断
・メインフレーム資産活用

http://www.oracle.com/lang/jp/direct/services.html

.NET アプリケーションでのセキュリティについて

- OS 認証利用時もコネクションプールが利用可能

- ASP.NET Membership ,Role Providerのサポート

オペレーティング・システム認証と特権接続

ODP.NET ONLY

```
Dim conn As New OracleConnection

conn.ConnectionString = "User Id=/;Data Source=orcl;DBA Privilege=SYSDBA"
conn.Open()

MsgBox("Connect OK!!")
cnn.Close()
```

①

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できます。

Oracle 11gでは、OS認証での接続もコネクションプールが有効

大量Oracle Clientの効率的な配布

- 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
- Oracle Clientの効率的な配布
  - Oracle Instant Clientを利用したOracle Clientの配布

クライアントの配布を簡単に
Instant Client

- OCI-、OCCI-、Pro*C、ODBC- 、JDBCアプリケーション
- Oracle Client のインストールが不要
- 非常にシンプルな配布
  - OTNよりダウンロード
  - ターゲットとなるクライアントにコピーするだけ
  - 環境変数のセット（PATH/LD_LIBRARY_PATH 、TNS_ADMIN）
- 以下のURLよりダウンロード可能
  http://www.oracle.com/technology/global/jp/tech/oci/instantclient/instantclient.html

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。

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 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/

- 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

オラクルエンジニア通信

<u>先月はこんな資料が人気でした</u>

- ✓ Oracle Database 11gR2 RAC インストレーション・ガイド ASM 版 Microsoft Windows x86-64
- ✓ Oracle Database 11gR2 旧バージョンからのアップグレード

オラクル クルクルキャンペーン

あのOracle Database Enterprise Editionが超おトク!!

おトクな買い方
オラクル5年分

- ライセンス使用期間　を5年間に設定
- 初期のライセンスコストがなんと67%OFF　！
- テクニカル・サポート価格も53%OFF　！

Oracle Databaseの
ライセンス価格を大幅に抑えて
ご導入いただけます

多くのお客様でサーバー使用期間とされる
5年間にライセンス期間を限定
- 期間途中で永久ライセンスへ差額移行
- 5年後に新規ライセンスを購入し継続利用
- 5年後に新システムへデータを移行

Enterprise Editionはここが違う!!
- 圧倒的なパフォーマンス!
- データベース管理がカンタン!
- データベースを止めなくていい!
- もちろん障害対策も万全!

この機能でこの価格
ライセンスパック

- Oracle Databaseの機能を存分に使える!
- 2ノードRAC構成も可能!
- サーバー構成によって計4種類のパックから選べる!

詳しくはコチラ
http://www.oracle.co.jp/campaign/kurukuru/index.html

Oracle Direct 0120-155-096

お問い合わせフォーム
http://www.oracle.co.jp/inq_pl/INQUIRY/quest?rid=28

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

OTN×ダイセミ　でスキルアップ!!

・一般的な技術問題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

一般的技術問題解決にはOTN掲示版の
「データベース一般」をご活用ください

※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セミナー　オンデマンド コンテンツ」へ

※ダイセミ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。

以上の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。