5.1 Active Directoryオブジェクトの概要

5.1.1　オブジェクトの種類と属性

Active Directoryでは，オブジェクトと属性の関係でデータを扱うことを第4章で説明しました．ディレクトリサービスとして組織内の「個人」に関わる情報を格納するActive Directoryでは，主に**表5.1**のようなオブジェクトを作成することができます．

表5.1　オブジェクトの種類と利用目的

オブジェクトの種類	利用目的
ユーザーオブジェクト	従業員がログオンを行うために必要な情報を格納したオブジェクト．
コンピュータオブジェクト	従業員が利用するコンピュータの情報を格納したオブジェクト．
組織単位オブジェクト グループオブジェクト	作成したユーザーやコンピュータをまとめておくためのオブジェクト．

これらのオブジェクトを作成すると，オブジェクトの種類に合わせた「属性」を設定することができます．例えば，ユーザーオブジェクトの場合，ログオン認証を行うために利用されるので，パスワードの情報が入っていなければ正しいパスワードを確認することができません．そのため，ユーザーオブジェクトにはパスワードが属性として設定することができます．一方，ユーザーをまとめることを目的に用意されているグループオブジェクトの場合，グループを使ってログオン認証することはありません．そのため，グループにパスワードの属性を設定することはできません．しかし，グループオブジェクトがまとめているユーザーの一覧を属性と設定することができます．

5.1.2　Active Directoryオブジェクトの参照

ユーザーやグループなど，AD DSの管理でよく利用するオブジェクトを参照する場合，Active Directoryユーザーとコンピュータを使います．

1「サーバーマネージャ」の左ペインから「役割」−「Active Directoryドメインサービス」−「Active Directoryユーザーとコンピュータ」の順に選択し，ドメイン名をクリックします（図5.1）．

Active Directoryユーザーとコンピュータの画面で，ドメイン内に作成されているオブジェクトの一覧を確認することができます．

2「Active Directoryユーザーとコンピュータ」が選択されているサーバーマネージャ

のウィンドウで，「表示」メニューの「拡張機能」を選択します．

デフォルトでは表示されていなかったコンテナが表示されます(**図5.2**)．

図5.1　Active Directoryユーザーとコンピュータ

図5.2　拡張機能をクリックしたあとのActive Directoryユーザーとコンピュータ

注意

このあとの操作では，拡張機能が有効になっている状態でないと確認できない情報があるので，拡張機能を有効にしたままの状態にしてください．

5.1.3　識別名

識別名とは，LDAPのディレクトリサービスにアクセスするときに使われるもので，特定のActive Directoryオブジェクトを指し示すときに使用する指定方法です．具体的にどのような場面で利用するかは後述しますが，ここではどのような使い方をするかについて説明します．

識別名は，オブジェクトの名前，コンテナの名前，ドメインの名前の順で指定し，それぞれの名前は**表5.2**のような指定方法をとります．

表5.2　識別名の指定

指定方法	対象
CN=	ユーザー，グループ，コンピュータ，コンテナなど
OU=	組織単位
DC=	ドメイン

以上を踏まえて，識別名を記述すると，次のようになります．

【例1】example.comドメインのUsersコンテナにあるAdministratorユーザー

```
CN=Administrator,CN=Users,DC=example,DC=com
```

【例2】osaka.example.comドメインのDomain Controllers組織単位にあるChildDCコンピュータ

```
CN=ChildDC,OU=Domain Controllers,DC=osaka,DC=example,DC=com
```

ドメイン名を指定するときには，ドットで区切られた名前ごとにDC=で記述します．また，コンテナオブジェクトでも，コンテナの場合はCN=と指定するのに対し，組織単位の場合はOU=と指定する点に注意します．

5.2 組織単位オブジェクト

5.2.1 組織単位オブジェクトの概要

組織単位オブジェクト（組織単位）はActive Directoryのオブジェクトをグループ化するためのオブジェクトとして用意されています．厳密に言うと，Active Directoryのオブジェクトをグループ化するためのオブジェクトとして，「コンテナオブジェクト」と呼ばれるオブジェクトが用意されており，その一部として組織単位があります．

コンテナオブジェクトは，オブジェクトの「入れ物」として利用されるのに対し，組織単位は「入れ物」としての機能に加えて次のことが可能です．

・特定の組織単位だけでの管理が可能な「部門管理者」の設定．
・グループポリシーを割り当てる単位．

組織単位とOU

組織単位は英語でOrganization Unitと書くことから，略して「OU」と呼ぶ場合があります．

5.2.2 組織単位の作成

組織単位を作成する方法について説明します．ここでは，ドメインの直下にSalesという名前の組織単位を作成します．

操作

1「サーバーマネージャ」の左ペインから「役割」−「Active Directoryドメインサービス」−「Active Directoryユーザーとコンピュータ」の順に選択します．

2「Active Directoryユーザーとコンピュータ」のドメイン名を右クリックし，「新規作成」−「組織単位(OU)」の順にクリックします．

3「新しいオブジェクト - 組織単位(OU)」ダイアログボックスが表示されます(図5.3)．

組織単位の名前を指定します．名前に「Sales」と入力して，[OK]ボタンをクリックします．

4作成した組織単位はActive Directoryユーザーとコンピュータで確認することができます(図5.4)．

図5.3 「新しいオブジェクト - 組織単位(OU)」ダイアログボックス

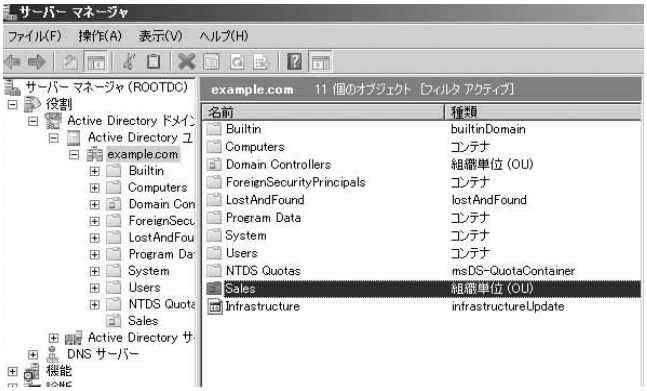

図5.4　作成された「Sales」組織単位

5.2.3　組織単位の削除

組織単位を削除する場合，Delキーで削除しようとするとエラーが表示されます．これは，組織単位がかんたんに削除されないように保護されているためです．組織単位を作成するときに，**図5.3**で「間違って削除されないようにコンテナを保護する」にチェックを付けておくと保護対象となります．

それでは，保護対象となっている組織単位の削除方法を説明します．

操作

1「Active Directoryユーザーとコンピュータ」で，削除する組織単位を右クリックし，「プロパティ」を選択します．

ここでは，5.2.2項の手順で作成した「Sales」組織単位を右クリックして「プロパティ」を選択します．

2「Salesのプロパティ」ダイアログボックスで，「オブジェクト」タブを選択します(図5.5)．

「誤って削除されないようにオブジェクトを保護する」のチェックをはずし，組織単位が削除可能な状態にします．