4.1 Active Directoryとは

Active Directoryは組織のネットワーク環境において，ユーザー等のID管理と，ファイル共有などのリソースへのアクセス管理を行うための機能を提供するサービス群です．Active Directoryはこれまでにもユーザー認証の機能として利用されてきましたが，近年セキュリティや内部統制，そして管理性能に対するニーズの高まりから，Active Directoryに対して求められる役割が単なるユーザー認証から，より効率的なID管理やアクセス管理へとシフトしてきました．そうした時代のニーズに対応できるよう，第1章でも述べたように，Active Directoryは五つのサービスから構成され，それぞれのサービスが連携を図りながらIDとアクセス管理が実現できます(**図4.1**)．

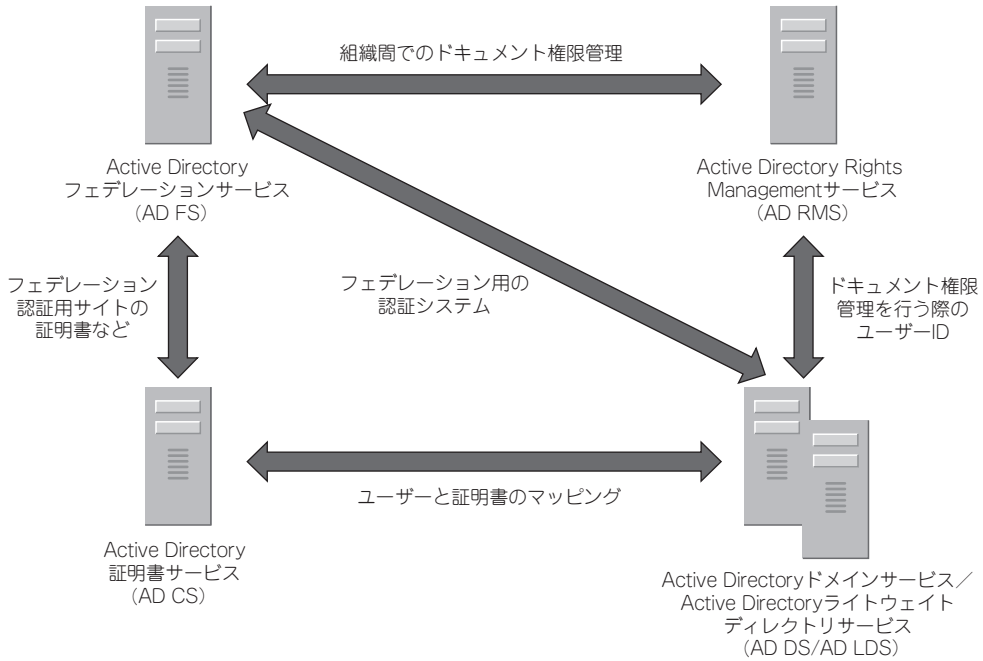

図4.1　Active Directoryサービス群の連携機能

この章では，Active Directoryサービス群の中から，Active Directoryドメインサービス(AD DS)について取り上げ，組織のネットワークでドメインを構築，運用管理する方法について解説します．

4.2 Active Directoryドメインサービスの構成要素

4.2.1　認証と承認

認証と承認は，ネットワーク内のリソースを適切なユーザーだけに利用させるようにするために欠かせないサービスです．認証とは，ネットワークを利用するユーザーの本人確認を行うサービスです．一般的には，ユーザー名とパスワードを入力することにより，認証を実現させます．ユーザー名に対するパスワードが正しいものであるかについては，認証用のデータベースに問い合わせることで確認します．

一方，承認は認証を済ませたユーザーがファイル共有などのリソースにアクセスする際，共有にアクセスするためのアクセス許可があるか確認するサービスです．承認は認証が既に済んでいることが前提で行われます．

次節で述べるドメインとワークグループは，いずれも認証と承認のサービスを提供する機能であり，どちらを利用するかによって認証用のデータベースの保存先が異なるなどの違いがあります．

4.2.2　ドメインとワークグループ

Active Directoryドメインサービス（AD DS）は文字通り，ドメインの機能を提供するサービスです．ドメインとは，Windowsネットワークの管理単位であり，一元的な管理が可能な範囲を指します．ドメインを構築すると，Active Directoryデータベースが生成され，このデータベースに，認証用の情報が格納されます．こうして，ドメインは自分のデータベースを利用して一元的な管理を実現させることにより，管理者の作業に対する重複をなくし，管理負担を抑えています．

また，ユーザーはドメインへのログオンを1回だけ行うことにより，ドメイン内のリソースへアクセスすることが可能となります（**図4.2**）．このように，1回のログオン操作によって，複数のリソースにアクセスできるような機能を「シングルサインオン」といいます．AD DSはドメイン内においてシングルサインオンを実現しています．

ドメインにはドメイン名と呼ばれる名前を付ける必要があります．ドメイン名には，DNSの名前付け規則を採用しており，`example.com`のようにドットで区切られた名前を付けなければなりません．

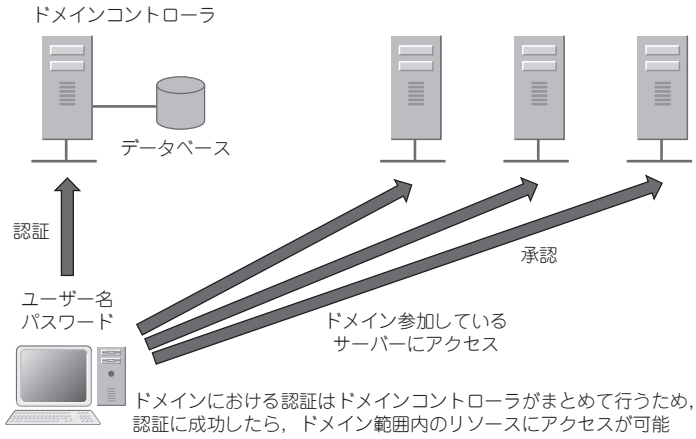

図4.2　ドメインの認証と承認

一方，ワークグループはドメインのように認証用データベースを集中管理することはなく，個々のコンピュータでその情報を持ちます．そのため，一度のログオン操作によってアクセスできる範囲は自分のコンピュータのみとなり，ほかのコンピュータのリソースにアクセスするときは，ほかのコンピュータで有効な認証情報を改めて入力しなければなりません(**図4.3**)．ワークグループはサーバーを利用することなくネットワークを構成することができますが，コンピュータの台数が増えると認証を行わなければならない回数も増えるため，ある程度の規模以上のネットワークにおいては適切ではありません．

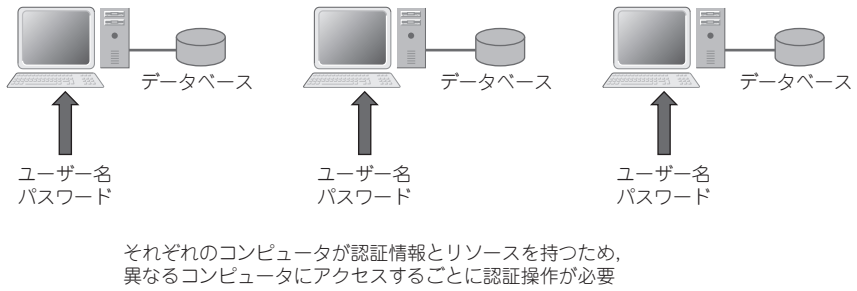

図4.3　ワークグループの認証と承認

4.2.3　ドメインツリー

Active Directoryドメインは「信頼」と呼ばれる設定を行うことにより，特定のドメインにログオンしたユーザーは，ログオンしたドメインだけでなく，信頼が設定されたもう一つのドメインにアクセスすることも可能となります．信頼を設定するにはいくつかの方法がありますが，Active Directoryドメインをインストールするタイミングで設

定する信頼の種類にドメインツリーがあります．

ドメインツリーに参加するドメインは連続した名前空間をもちます．**図4.4**を例にとればルートドメインがexample.comその下のサブドメイン名がosaka.example.comとnagoya.example.comとなります．親ドメインの先頭にサブドメインのドメイン名＋ドット「.」を追加しています．さらに孫ドメインにも同様の規則で名前付けしてsales.nagoya.example.comとします．

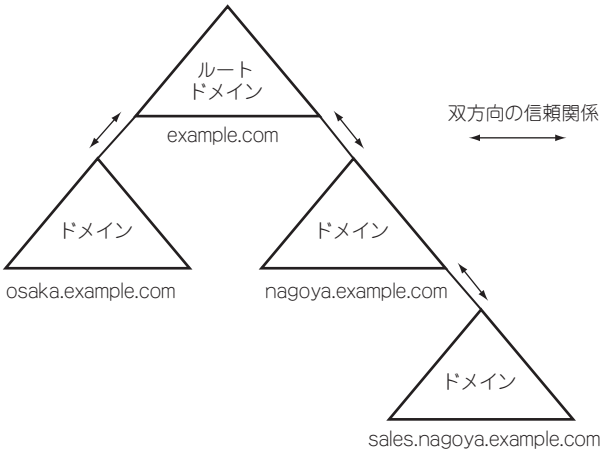

図4.4　ドメインツリーの例

ドメインツリー内に複数のドメインが構成される場合，最初にインストールされたドメインを「ツリールートドメイン」と呼びます．また，ドメインツリー内で，example.comドメインに対して，osaka.example.comドメインが実装された場合，example.comドメインを親ドメイン，osaka.example.comドメインを子ドメインと呼びます．信頼については4.4節を参照してください．

4.2.4　フォレスト

フォレストは，一つ以上のドメインツリーから構成されるドメインの集合体で，Active Directoryドメインをインストールするタイミングで設定する信頼の種類です．フォレストは最初のドメインをインストールするタイミングで定義されるため，2番目以降のドメインをインストール場合，既存のフォレストに参加するようにインストールすることで複数のドメインが一つのフォレストとして構成されるようになります(**図4.5**)．

同じフォレストとして構成されたドメインどうしは，スキーマやグローバルカタログを共有します(スキーマについては4.3.7項，グローバルカタログについては4.3.6項で解説します)．