ワークグループとドメインネットワーク

ネットワーク上に複数のコンピュータが存在すると、アクセスしたい相手を示すために名前を付ける必要がある。つまり、ネットワーク上に接続されているコンピュータにそれぞれ名前をつけて区別するという必要がある。コンピュータに名前を付けることで、どのコンピュータにアクセスしたいのかがはっきりとわかる。しかし、多くのコンピュータがつながっていた場合は、その名前を探すのに時間もかかり非常に不便であり効率もよくない。そこで、ネットワークをグループ分けする方法があげられる。

ネットワークのグループ管理には、大きく分けてワークグループで管理する方法とドメインで管理する２つの方法があり、その方法について詳しく述べていきたい。

Ⅰ　ワークグループ

ネットワークで作業を行うコンピュータに、ワークグループ名をつけてクルーピングすることで、管理をしやすくしようというのがワークグループの考え方である。

１　ワークグループの特徴

（１）独立した SAM（Security Account Manager）データベースをもつ

それぞれのコンピュータごとに専用の SAM データベースを持ち、ユーザアカウントやグループアカウント情報を構成していく。すなわち、所属するコンピュータが独立した存在として、それぞれが資源の管理を行う。各コンピュータの管理をユーザが担当するために、ネットワーク管理者が不要である。

（２）分散型のリソース管理を行う

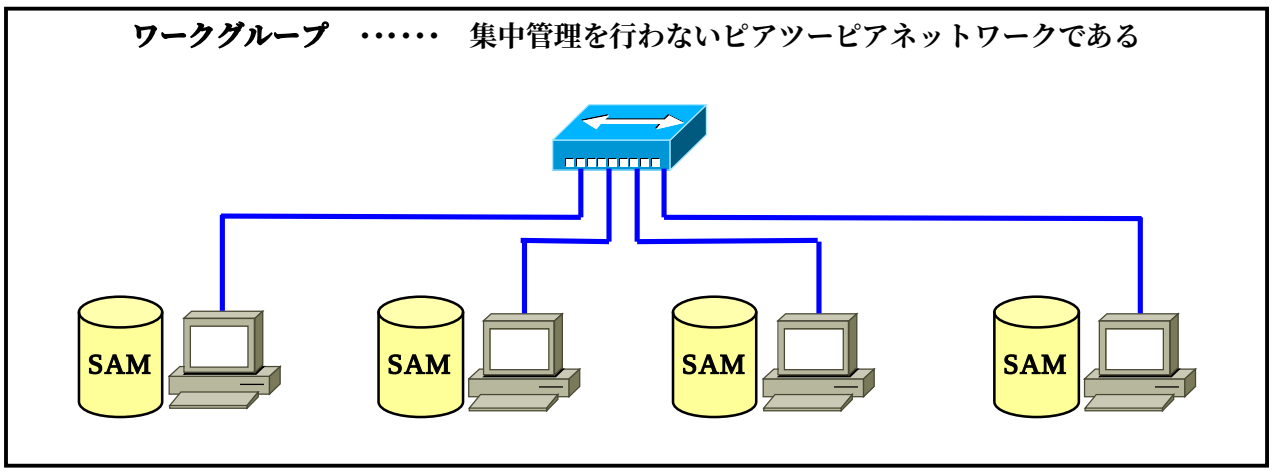
リソース管理やユーザ認証は、それぞれのコンピュータごとで実行される。

（３）容易で低コストな構築

ワークグループ環境では、サーバを必要とせずクライアントコンピュータだけで構築が可能である。また、構築も容易かつ安価でできる。

（４）小規模環境向け

分散型のリソース管理を行うため、ユーザ数やクライアントコンピュータの数が増加すると管理がだんだんと困難になる可能性がある。よって、ワークグループに属するコンピュータを同じ設定にするには、全てのコンピュータを設定しなければならなく、変更が生じたら全てのコンピュータに同じ設定を行わなければならない。



Ⅱ　ドメイン管理

ドメイン管理はユーザを一元管理するために専用のサーバが必要となる。ドメインを設定することにより、ネットワークのユーザアカウントやセキュリティの原則を一元的に管理することができ、個々のコンピュータでこれらの管理を行う方法（ワークグループ）に比べて、ネットワーク管理の効率化が図れる。

ネットワークに接続しているそれぞれのユーザは一度認証を受けると、どのコンピュータへアクセスしてもパスワードを要求されることなく作業を続けることができる。

しかもユーザ管理を一元化しているため、ユーザの権限変更等が非常に簡単になり、信頼性も高まる。

1　ドメインの特徴

(1) ドメイン情報を保持する Active Directory データベース

ドメインの情報を保持するためにアクティブディレクトリが必要である。

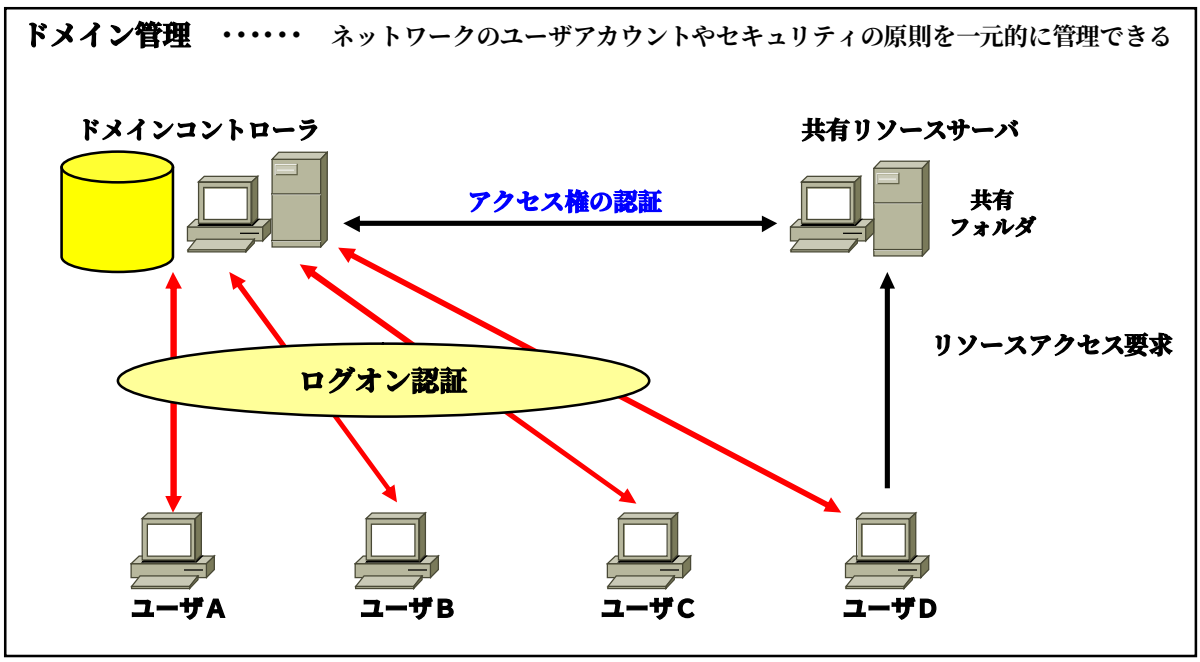
(2) リソースやアカウントの集中管理

リソースやアカウントを集中管理することが可能である。

(3) 高い拡張性

(4) Windows 2000 Server 以上の製品が必要

ドメイン環境を構築するためには、ドメインコントローラというアクティブディレクトリデータベースを保持するコンピュータが必要になる。そのためには、1 台以上の Windows 2000 Server 以上のサーバが必要となる。また、ドメイン環境を構築することによって、大規模なネットワークも容易に管理作業を行うことができる。それ以外にも、アクティブディレクトリのグループポリシーなどの機能を使用した一元管理、およびセキュリティ設定やアプリケーションの配布といった作業が簡単に行える。



ドメイン内のユーザアカウントを一元管理

2　ドメインの管理

（1）ドメインコントローラ

ドメインコントローラは、Windows 2000 Server 等を使用してドメインを構成する際に、ドメイン内にユーザアカウントデータベースを一元的に保持する役割を果たす。

（2）ユーザ登録

ドメインが構築されている環境では、ネットワーク上の資源を利用したいユーザは、ドメインコントローラにユーザ登録をしなければならない。登録される内容は、ユーザアカウントとパスワードなどである。ユーザがドメインに参加しているコンピュータにログオンしたい場合は、ログオン画面でユーザ名とパスワード、参加するドメインを入力する。入力された情報は、参加を希望するドメイン内のドメインコントローラに受け渡され、認証を受けドメインに参加することができる。

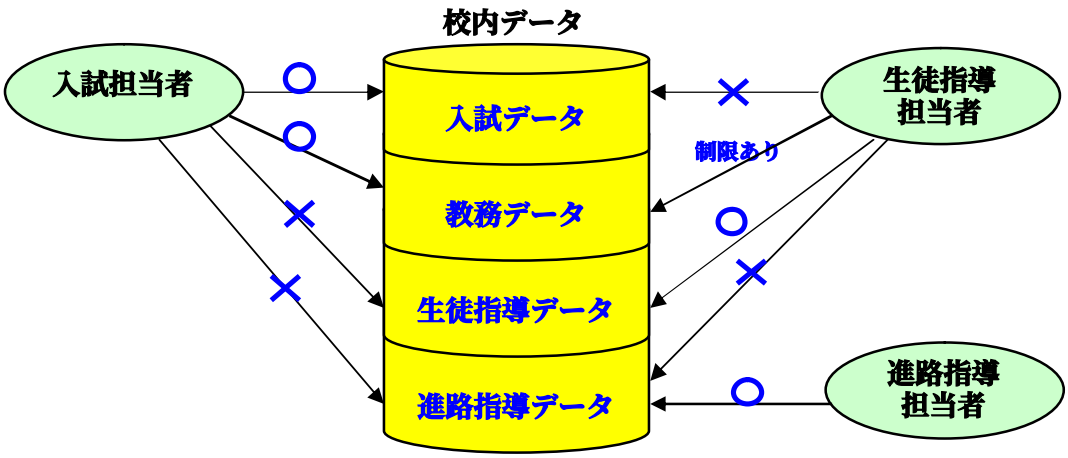
共有リソースを使用する場合には、ユーザ名やパスワードはリソースを管理するサーバに渡されるが、そのユーザに許可されているリソースのアクセス権の認証はドメインコントローラに受け渡され認証が行われる。

（3）ユーザグループ

Windows 2000 Server では、通常ユーザをクループに分け、そのグループに権限を与えることにより、グループに属するユーザは同一の権限を持つことができる。ユーザごとに異なる権限を与えることもできるが、管理上の面からグループを設定する方が効率的である。

（4）アクセス権の設定

個人またはグループに対して、ファイルやフォルダごとにアクセス権を設定することにより、利用できる権限のレベルを変えることができる。これにより、権利のないユーザに対して不用意に情報を与えてしまうことを防ぐことができる。



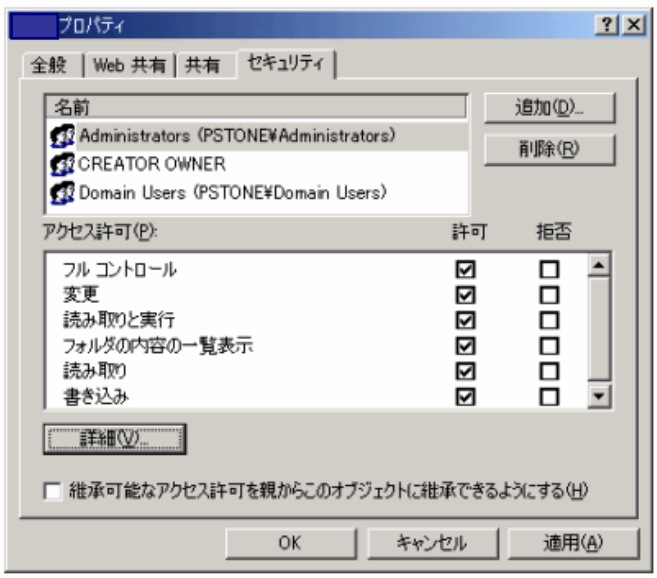
（5）サーバ上でのアクセス権設定

Windows 2000 Server の場合、右図（アクセス許可欄）を用いて設定を行う。

Windows のファイルシステムには、

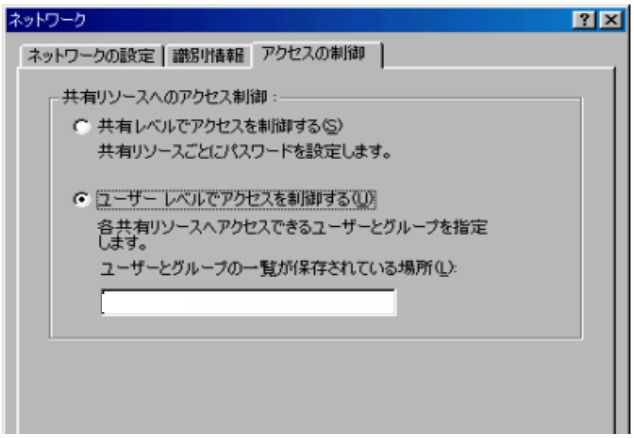
- FAT（File Allocation Table）
- FAT32
- NTFS（NT File System）

の３種類がある。



（6）クライアントでのアクセス権設定

クライアントのＰＣにもアクセス権を設定することができる。ドメインに参加している場合には、ドメインコントローラ内のユーザアカウントの単位でアクセス権を設定することができる。



Ⅲ　校内ネットワークの管理形態の移行（ワークグループからドメイン管理へ）

現在、本校のネットワーク管理形態はワークグループで管理しており、教員用と生徒用にそれぞれ「NT-DOMAIN」と「NT-SERVER」というグループ名を付けている。このようにすればコンピュータの数が多くても比較的運用しやすくなる。

しかし、このような場合、それぞれのコンピュータはワークグループ名で単純にグループ分けされているだけで、それぞれのコンピュータは独立した動きをしている。コンピュータが独立した動きをしているとコンピュータＡがコンピュータＢにアクセスしようとした場合、コンピュータＢはユーザ名とパスワードを要求する。その逆も同様で、それぞれのコンピュータが独立してユーザを管理しているため、このような煩雑な作業が発生する。

そこで、本校のネットワークの管理形態についてはドメイン管理に移行する必要がある。ただ単にパソコンの接続台数が多いからという理由ではなく、セキュリティ面の強化のためにもドメインで管理を行った方がより安全で信頼性も高まる。

それでは、どのようなグループを作り、どのような管理が望ましいのか、以下に説明していく。

１　ドメイン名とユーザグループ（一例）

教員用

ドメイン名	グループ名	校務分掌等	係り	アクセス権
教　員	admin	―	ネットワーク管理者	フルアクセス
	kanri	管理職	―	管理職用
	kyomu	教務部	教務主任	教務主任・教務全般・入試・成績データ・個人用
			入試係	教務全般・入試・成績データ・個人用
			成　績	教務全般・成績・個人用
			時間割	教務全般・個人用
	seito	生徒指導部	生徒指導主事	生徒指導主事・生徒指導全般・個人用
			生徒会・その他	生徒指導全般・個人用
	shinro	進路指導部	進路指導主事	進路指導主事・進路指導全般・個人用
			進学・就職・その他	進路指導全般・個人用
	kojin	教員用	全教員用	個人用

※グループ・フォルダレベルで制限をかける。

生徒用

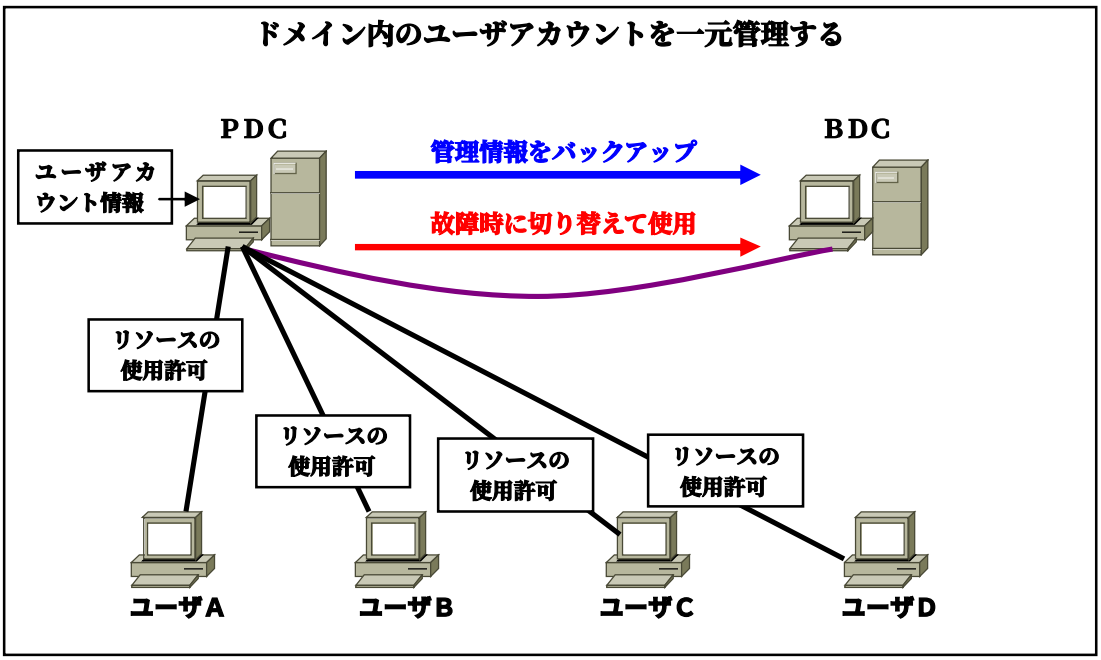
ドメイン名	グループ名	アクセス権	ドメイン名	グループ名	アクセス権
生　徒	multi	マルチ生徒用	生　徒	paso2	パソ２生徒用
	paso1	パソ１生徒用		prog	プログ生徒用

2　ドメイン管理の欠点に対する手立て

ドメインで管理することにより、一元化による管理作業工程最小化による管理コストの削減や作業工程の増大による人為的ミスが解消できる。しかし、集中型システムではドメインコントローラの故障、あるいはドメインコントローラの故障や通信不能時に、クライアントのコンピュータが使用できなくなるという欠点がある。

そこで、現在本校では教員用ファイルサーバとして Windows NT Server 、生徒用として Windows 2000 Server を使用している。稼動していないサーバが２台（Windows 2003 Server）あり、その２台についてユーザアカウントを管理するＰＤＣ（プライマリドメインコントローラ）とＰＤＣに障害が発生した場合にＰＤＣに代わってユーザアカウントの管理をするＢＤＣ（バックアップドメインコントローラ）

を設定するように考えている。こうすることにより、クライアントはＰＤＣもしくはＢＤＣの認証（リソースの使用許可）を受けてログオンすることになる。



Ⅳ　クライアントの設定

コンピュータの管理者の権限を持つユーザとして、Windows XP Professional にログオンする。

1　[スタート] ボタンをクリックし、[マイ コンピュータ] を右クリック。

2　[プロパティ] をクリックする。

3　[コンピュータ名] のタブで、[変更] ボタンをクリックする。

4　[ドメイン] をクリックし、使用しているコンピュータが所属するドメインの名前を入力し、次に [OK] をクリックする。（ドメイン名が不明の場合は、ネットワーク管理者に問い合わせること）

5　画面の表示に従い、ドメイン ユーザ名とパスワードを入力し、[OK] をクリックする。

完了したら、[OK] をクリックし、再度 [OK] をクリックして、[プロパティ] ウィンドウを閉じる。

6　コンピュータはドメインに加わり、ドメインへの参加を通知するメッセージが表示される。

新しい設定が適用されるようにするためにコンピュータを再起動し、ユーザ名とパスワードを入力してドメインにログオンする。