福井大学大学院工学研究科　研究報告　第56巻2008年3月
Mem. Grad. Eng. Univ. Fukui, Vol.56(March 2008)

管理者の負担軽減のためのLDAPを用いた研究室内LANの構築
– 小倉研究室内LAN構築 –

瀧澤　崇*　小倉　久和*　黒岩　丈介*　小高　知宏**　白井　治彦††

Establish Laboratory LAN Based on LDAP for the Purpose of Reducing Network Administrative Task
- LAN Establishing in Ogura Laboratory -

Takashi TAKIZAWA, *Jousuke KUROIWA, *Haruhiko SHIRAI, *
Tomohiro ODAKA, *and Hisakazu OGURA*

(Received January 31, 2008)

In this paper, we report the process in constructing our laboratory LAN, which enables us to share user's information and network recources. In our laboratory, three types of operating system(OS), Linux, Windows and Mac, are employed on computers, being difficult to administrate users's information through all the computers. In order to overcome the difficulty, we employed LDAP protocol, which provides directory service. In collaborating with LDAP and the other services, it is possible to unify the management of user's information, for instances, 'Login Shell', 'User Password', 'Mail Address', 'Mount Map' and so on. Finally, the management of user's information becomes simple.

Key words : LocalAreaNetwork(LAN), LDAP, User Administration, Network Security

1. はじめに

本稿では，研究室内LANの構築について報告する．近年，組織内でLANを構築する事例が増えているが，本研究室も例外ではない．LANを導入するメリットはいくつかある．一つ目は情報の共有である．LAN内で各PCに保存されている実験データや研究資料を簡単に共有でき，作業効率が上がる．また研究室内の連絡もLANで行うことが可能であり，本研究室においても実際に研究室内でのコミュニケーション促進を目的とした支援システムを開発し運用している[1]．また，各PCに分散されたデータを共有するだけではなく，データを一ヶ所にまとめて利用するということも可能になる．もう一つは，ネットワークリソースの共有である．LANを構築することによって，LAN内に存在するPCだけでなく，ネットワークに接続されたプリンタやスキャナを共有することや，複数のPCで外部への接続回線を共有できる．これらが，LAN構築の大きなメリットといえる．特に，本研究室の研究は，そのほとんど実験環境としてPCを用いるので，LAN構築のメリットは非常に大きい．

LANは非常に有用であるが，ネットワークを構築すると，それを管理する人間が必要となる．例えば外部ネットワークに接続できない，研究室内のサービスが利用できなくなったなどの各種トラブルシューティングだ

* 大学院工学研究科知能システム工学専攻
** 大学院工学研究科原子力エネルギー工学専攻
†† 工学部技術部
* Human and Artificial Intelligent Systems Couse, Graduate School of Engineering
** Nuclear Power and Energy Safety Engineering Couse, Graduate School of Engineering
†† Technical Support Division

けではなく，ネットワークやそのサービスを日常から監視し，不具合や異常の兆候があれば異常が発生する前に対処することも求められる．トラブル以外にも，ネットワークを利用するユーザーの管理や新しいネットワーク機器導入の検討なども必要で，これらの仕事が管理者にとって大きな負担となる．本研究室のネットワークは50台以上のPCで構成されているため，ネットワークの管理は容易ではない．

その他，本研究室独自ともいえる問題もある．本研究室はLinux・Windows・MacOSが混在する混在環境である．前述のとおり，日々の研究をPCで進めるため，トラブルが発生した場合を考えて，同じOS同士では，最低限同じ実験環境で且つ研究室の全メンバーが利用できる状態である必要がある．その際，問題となる1つがユーザー管理である．ユーザー管理や重要なデータの管理などは，ユーザーの人数や管理対象の数に比例して負担が大きくなる．そこで，本研究室ではLDAPというプロトコルを採用した．LDAPはネットワーク上にディレクトリサービスを提供するプロトコルである．これを用いることで，ネットワーク上の資源とその属性を定義して一纏めにすることが可能である．LDAPは他のアプリケーションとの連携も容易である．メールサービスを提供するためのPostfixを例とすると，LDAPを用いて，ユーザー管理やネットワークリソースの管理を一元化し，リソースの管理の負担を減らすことが可能となる．

その他にも，LANではいくつか注意すべき点がある．LANは外部ネットワークに接続するため，セキュリティに気を配らなくてはならない．外部からの侵入を許してしまうとデータの消失や，侵入されたサーバーを他のネットワークへの踏み台とされ，別のネットワークへも影響を及ぼすこととなってしまう．メールサーバを運用する場合スパムメールの問題は避けることができない．大量に送信されてくるスパムメールはディスクを圧迫するだけではなく，ウィルスメールを含むこともある．メールサーバについても，場合によってはスパムメールの中継点とされてしまうこともあるため注意しなくてはならないなどの諸般の問題がある．

この様に，LAN構築には計画時に考えるべき事項と実際に運用し始めてから起こる問題と両方を考慮する必要がある．本稿では，LDAPを用いたユーザー管理を中心に，研究室内LANの構築過程について報告する．その際，考えられるトラブルをできるだけ回避してトラブル時にも被害を最小限にでき，できるだけ管理者の負担とならないようなLANを設計し構築した．

2. ネットワークの概要

2.1 研究室LANの必要要件

今節では，研究室内LANにおける必要要件について述べる．研究室内にはデスクトップPC，ノートPCが約７０台，その他プリンタなどのネットワーク機器があり，それら全てを研究室内LANに接続する．そして，研究室に所属するユーザは研究室内の一部サーバー群を除いた全てのマシンを利用できる必要がある．当研究室の研究テーマはそのほとんど実験環境としてPCを用いるものであるため，PCが故障した場合においてもデータがあれば別のPCにて実験をすることが可能である．そのため，ユーザーは研究室内全てのPCにログインすることができ，ログインしたPCにおいて自分の研究データ等を利用できるということが，ユーザーが研究を進めていく上で非常に有用であり，これが最重要要件であると考える．また，このような構成にすることによって，学生が卒業・修了した後にその研究データを管理し，継続研究では次の学生に伝えるということが容易になる．その条件を満たすために，全ユーザーのアカウントを一元管理するためのアカウント管理サーバーや，各ユーザーの研究データを保存するためのファイルサーバーが必要となる．

その他，研究室に所属するユーザーにメールサービスを提供するためのSMTPサーバーや，外部に研究室の情報を発信するためのWEBサーバー，日常でユーザーが利用，管理を行うクライアントPCを管理するためのDHCPサーバー，研究室内LANと外部ネットワークとの入り口に配置し，セキュリティを高めるためにFireWallを設置したゲートウェイマシン等もそれぞれ必要である．

また，研究データを含めた各種バックアップも必要である．特に，ファイルサーバでは研究データを管理するため，そのファイルサーバ自体に何かしらのトラブルが発生したときに，そこに保存されている研究データを利用できなくなったり，研究データ自体を失ってしまうということも考えられる．そこで，前述のサーバー群を中心に，バックアップを作成するための体制を整える必要もある．

まとめると，本研究室での必要要件は以下の通りである．

- 環境に依存しないユーザー管理

- データを集中管理するファイルサーバ
- DHCP サーバ，DNS サーバ
- メールサーバ
- Web サーバ
- ネットワークセキュリティの確保
- 定期的なバックアップ体制

特にユーザー管理，ファイルサーバは本研究室独自の要件と言える．これらを満たすネットワークを計画，構築していく．

2.2 ユーザー管理構築の方針

前節で述べた要件を満たすネットワークを構築する上で，解決しなくてはならない問題がある．一つ目は研究室内には多数の PC があるが，全てが同一の環境というわけではなく，Windows/MacOS/Linux という複数の OS が混在しているという点である．研究テーマによっては，「Linux では可能だが，Windows では難しい」というものや，その逆となるものもある．そのため，研究室内のクライアント PC の環境を同一にすることは難しく，どうしても混在環境となってしまう．これより，前述のような「全ユーザーが研究室内の全クライアントマシンへログイン可能」という要件を満たすことは非常に困難になると考えた．各サーバー，クライアントそれぞれにユーザー情報を持たせるという解決策も考えられるが，研究室のような多くの PC マシンを管理しなくてはならない状況では，非常に大きな負担となる上，ユーザー情報が分散してしまうために全体を管理することが困難となる．OS 毎にユーザー管理をし，各 OS 用のアカウントサーバーを用意したとしても，全クライアントが個別に管理する場合ほどではないが，同じ状況が発生すると考えられる．

また，ユーザー管理が必要なのはログイン時だけではなく，メールの送受信やファイルサーバーを利用する場合にもアカウントによる制限が必要である．特にファイルサーバにおいては，ユーザー管理だけではなくサーバーに保存されている研究データを異なる OS でも自由に読み書きすることができ，違うマシンを利用した場合においてもユーザーが普段使っているような環境を再現できるような状態にする必要がある．もちろん，これらのサービス毎にユーザー管理することも可能であるが，やはりユーザー情報が分散し管理の負担が増大する．

そこでこれらの問題点を解決するために，LDAP を用いてユーザー情報を一元管理する方法を採用した．LDAP とはディレクトリサービスにアクセスするためのプロトコルで，LDAP を用いるネットワークの管理方法は近年各所で採用され，広がりつつある方法である．

3. ディレクトリサービスと LDAP の概要

LDAP は，"Lightweight Directory Access Protocol" の略である．RFC1777 等で定義されているインターネット標準のプロトコルで，TCP/IP 上にディレクトリサービスを提供するためのプロトコルである [2]．ディレクトリサービスとは，ネットワーク上に存在する資源とその属性とを記憶して，容易に検索できるようにまとめたものである．ここで言う資源とは，ネットワークを利用するユーザや組織に関する情報や，利用可能なサーバと提供しているサービス，プリンタやスキャナなどのネットワークを介して利用できる機器等のことを指す．

LDAP は，もともと X.500 ディレクトリアクセスプロトコル (DAP) を改良して作られたプロトコルである．このプロトコルは，世界中の情報を集めたディレクトリサービスを実現しようとするものであったが，そのために非常に多くのコンピュータリソースを必要としたために普及しなかった．これに対して，LDAP は，TCP/IP 上で軽快に動作することを目的として作成されたディレクトリサービスである．軽快でありながら，X.500 が提供する多くの重要な機能の多くを引き継いでいる．

LDAP にはもともと人名録や住所録という意味合いがあるため，様々なデータを保管しておき，それを調べるために利用される場合が多い．つまりデータベースの一種として考えることもできる．しかし，人名やメールアドレスなどは頻繁には変更されないデータであり，それらを大量に保管してその中から一定の条件で検索を行うという利用方法が多い．LDAP はリレーショナルデータベースではなく，トランザクションの概念も持たないため，動的で複雑なデータを扱う分野では不向きである．データの相関関係ではなく，物 (オブジェクト) を管理しようとする．そのため，本研究室のように，ユーザーのアカウント管理に使うというような利用方法には向いていると考えられる．

LDAP を利用する理由として，様々なアプリケーションとの連携が可能という点が挙げられる．LDAP は他アプリケーションとの連携を目標の一つにしており，現在では多くのアプリケーションが LDAP をサポートしている．これらのアプリケーションでは，LDAP をユーザーの認証情報の管理に利用することが多い．ユーザー

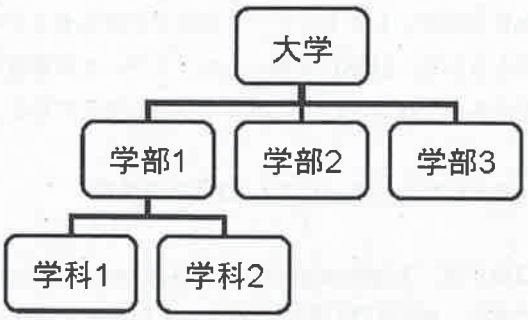

図 1　LDAP ツリーのイメージ

名とパスワードを必要とするシステムは非常に多いが，それらを用途毎に記憶することが困難であると同時に，対象が多いと定期的なパスワード変更などが困難になる．LDAP を用いることによってそれらの一元管理が可能になる．

LDAP では，データの管理単位をエントリと呼び，そのデータに関する様々な情報を登録することができ，属性という単位で管理する．図 1 は，LDAP ツリーのイメージである．例えば，”福井大学” というエントリに対して，”所在地” という属性があれば属性値は” 福井県福井市” となる．これらのエントリは，ディレクトリインフォメーションツリーと呼ばれる階層構造で管理される．大学を例にとると，大学の中に学部という階層があり，それぞれの下に学科やコースといった階層が存在し，さらにその下に学年という階層がある．学生個人のデータは，これらの階層を使って管理される．

各階層のエントリの管理には，階層の中で他の項目と識別するために利用する一意の識別名 (Relative Distinguished Name, RDN) を定義する．そして，ツリー中のエントリは各階層の RDN を連結したもので識別する．

以上が，LDAP の概要である．本研究室では，LDAP の特徴である「ユーザーアカウント管理に向いている」という特性と，様々なアプリケーションとの連携が可能という点に着目し，管理システム中心部に LDAP を採用した．また，一言に LDAP といっても多くの製品があるが，本研究室では OpenLDAP[3] を採用した．OpenLDAP はフリーの LDAP サーバーで，多くの Linux ディストリビューションで採用されているため，様々な解説書もあり，導入が簡単であるという利点がある．

表 1　posixAccount クラス

属性	解説
cn	一般名称
uid	ユーザ名
uidNumber	ユーザ番号
gidNumber	グループ番号
homeDirectory	ホームディレクトリ
userPassword	ログインパスワード
loginShell	ログインシェル

表 2　inetOrgPerson クラス

属性	解説
displayName	表示名
mail	メールアドレス

4. LDAP を用いたネットワーク

4.1 Linux アカウント管理

LDAP を導入する準備として，LDAP ツリーを設計する．本研究室では，主に Linux のログインアカウント管理に用いる．LDAP には，オブジェクトクラスというエントリに登録されるべき属性に関する取り決めが存在する．様々なオブジェクトクラスが存在し，複数のオブジェクトクラスを一つのエントリに関連付けることも可能である．Linux のログインユーザを管理するために”People” という識別名を定義し，エントリを追加していく．エントリのオブジェクトクラスには表 1 のような posixAccount クラスを用いた．

posixAccount クラスには Linux のログイン時に必要な情報に関する属性が定義されている．これらの属性は，Linux においてアカウントの詳細が記述されている /etc/passwd ファイルと同じ内容である．posixAccount クラスは単独で使用することができないため，同時に inetOrgPerson クラスを定義する．これはインターネット上で組織に所属する個人を管理するためのオブジェクトクラスである．このオブジェクトクラスには必ず使用しなくてはならない必須属性はなく，すべてオプション属性として定義されている．ここでは利用した属性についてだけ表 2 に示す．

inetOrgPerson クラスは，LDAP をアドレス帳として利用するような場合に必要な属性は定義されているが，

表3 posixGroup クラス

属性	解説
cn	一般名称
gidNumber	グループ ID
memberUid	グループのメンバー

表4 他アプリケーションとの連携

サービス	アプリケーション cc
メールユーザの管理	postfix, courier-imap
Windows ユーザの管理	samba
NFS マウントマップの管理	autofs

Linux のユーザー管理とは直接関係ない．"mail" 属性については，後述するメールサービスでの認証に利用する．

ユーザーアカウントと同様，ユーザーグループについても LDAP にて管理する．グループの管理には表 3 の posixGroup クラスを利用する．グループはユーザーアカウントに関連付けるのではなく，ユーザーアカウントとは別の識別名を持つ．そして，"memberUid" 属性の属性値がグループに所属するユーザーのアカウントとなるように定義する．

4.2 メールサーバとの連携

LDAP を他アプリケーションと連携させることで，複数サービスの集中管理が可能となる．本研究室では，以下のサービスと LDAP を連携させる．

初めに，メールサーバについて述べる．メールサーバと LDAP を連携させることによって，メールを利用するユーザー情報も Linux ユーザー情報と統合して管理することが可能となる．本研究室では，SMTP サーバーに Postfix，IMAP サーバーに courier-imap を採用した．両アプリケーションとも，LDAP と連携が可能である．メールサーバには大きく分けて POP サーバーと IMAP サーバーの 2 つがあるが，メールをサーバー上のメールボックスで管理できる IMAP を選択し，メールボックス形式は Maildir 形式を選択した．Maildir 形式ではメール一通二体して一つのファイルを作成してメールを管理するため，IMAP サーバーと合わせることによってメールを失う危険性を大幅に軽減できると考えた．courier-imap では，実際に IMAP の処理を行うプログラムとユーザー認証を行うプログラムは分離している．認証に LDAP を利用する場合でも，特定のオブジェクトクラスを前提としておらず，posixAccount 等のオブジェクトクラスで構成されたユーザーアカウント情報を利用することができる．そこで，本研究室では，inetOrgPerson に含まれる "mail" という属性の属性値を IMAP サーバーへのログイン ID とした．これにより，IMAP サーバー認証のために新たな属性を定義する必要がなくなる．courier-imap の認証部はこのユーザー ID を元に LDAP を検索し，パスワード/ユーザー番号/グループ番号/Maildir を引き出す．

Postfix では，検索テーブルやメール配送の多くの機能で LDAP と連携可能である．そのため，システムユーザーメールユーザーとを完全に分離し，メールの仮想ユーザーを作成することが可能である．今回はメールの仮想ユーザーを利用していないが，今後システムを変更する場合を考慮して Postfix を利用することとした．

4.3 Linux 以外でのユーザー管理

前述した通り，本研究室は様々な OS が混在する環境である．前節までに Linux でのユーザー管理について述べたが，Windows ではまた別のユーザー管理が必要となる．通常，それぞれの PC にて管理することが多いが，これではユーザー情報を持つマシンが分散してしまい管理者にとって負担となる．そこで，本研究室では Samba[4] を用いる．Windows ではファイル共有に Common Internet File System(CIFS) を利用しているが，Samba はそれを Linux で実現するアプリケーションである [5]．これを利用することで，Linux-Windows 間のファイル共有を実現するだけではなく Windows のドメインコントローラを構築することができ，Linux でも Windows ユーザーを管理することが可能になる．しかし普通に管理した場合，結局 Linux のユーザーとドメインコントローラのユーザーが別になってしまう．この問題を，Samba と LDAP の連携で解決する．

LDAP には表 5 にのような SambaSamAccess というオブジェクトクラスが用意されている．sambaSamAccess クラスには，ユーザー ID やパスワード以外にも登録されているユーザーのアクセス権の制御・ホームディレクトリへのパス・ネットワークドライブ名等を定義するための属性が用意されている．これを Linux ユーザーの管理で用いた poxixAccount と併用して，ユーザー管理を一元化した．また，samba で用いるホームディレクトリを Linux のホームディレクトリと同

表5　sambaSamAccess クラス

属性	解説
sambaSID	一般名称
sambaAcctFlags	ユーザーに関するフラグ
sambaHomeDrive	ドライブ名
sambaHomePath	ホームディレクトリのパス
sambaLMPassword	Lan Manager 用パスワード
sambaNTPassword	NT パスワード
sambaProfilePath	プロファイルへのパス

一にすることで，ユーザーが Windows にログインする場合でも自分のホームディレクトリを簡単に参照・利用できるようにした．さらに，ホームディレクトリにプロファイルが存在すれば，ユーザーは Linux の個人設定だけではなく，Windows の個人設定についても同じホームディレクトリで保存・管理が可能となる．これらによって，ユーザーは環境を気にすることなく複数のマシンにログインしての作業が可能になり，Windows でないと動かないアプリケーションなども気にすることなく利用できる．管理者側から見てもユーザー情報が一つにまとまるメリットは非常に大きい．

4.4　Autofs との連携

本研究室では，ユーザーのホームディレクトリの実体はファイルサーバーに存在し，クライアントマシンにログインする際に NFS によってホームディレクトリを各クライアントにマウントする．そのマウントには Autofs というアプリケーションを利用する．ファイルシステムを自動的に任意の位置にマウントする automount デーモンというプログラムがあるが，Autofs はそれを制御するためのプログラムである．Autofs を用いると，ユーザーがディレクトリにアクセスしようとした時だけファイルシステムをマウントし，一定時間が経過すると自動的にアンマウントを行うようになる．これを NFS で利用することで，ユーザーの実験データ等を一つのファイルサーバにまとめることができる．しかし，ファイルサーバの異常等でサーバを変更したり，ユーザーのホームディレクトリの位置を変えたい場合等に，全クライアントマシンの設定を変更する必要がある．これはクライアントマシンの台数が増えれば増えるほど管理者の負担になってしまう．そこで，Autofs と LDAP を連携させることによって，この問題を解消する．

通常 Autofs のマウントマップは各クライアントマシンが管理する．しかし，このマウントマップを LDAP で管理することで，クライアントマシンは図 2 のように LDAP を参照してマウントポイント等の情報を引き出し，実際のマウントを行う．このようにしてマウントマップを一ヶ所で管理することが可能になり，ファイルサーバーの変更等の場合でも，管理者は一つのマウントマップを変更することで対応可能となる．

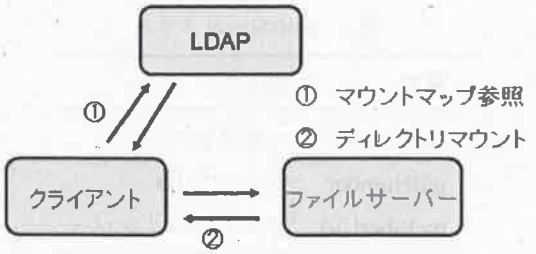

図2　LDAP ツリーのイメージ

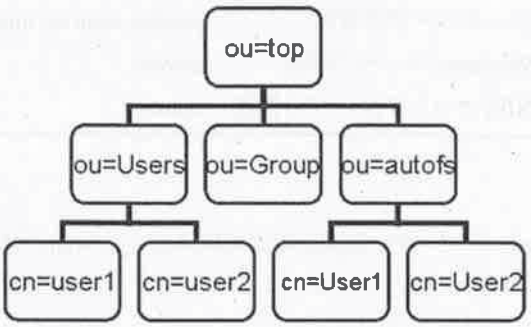

図3　本研究室での LDAP ツリー

以上が，本研究室で構築する LDAP ツリーの概要である．これを元に構築した LDAP ツリーが図 3 である．

トップドメインの下の階層に"Users","Groups","autofs" という RDN が存在し，その下に各種エントリが属するという形になる．"Users" に含まれるエントリには，Linux でのユーザー情報，Windows ドメインでのユーザー情報，メールアドレスやフルネーム等の個人情報についての属性が定義されている．"Group" では，Linux でのグループや研究室で新たに定義したグループのエントリが登録され，それぞれグループのメンバーに関する属性が定義されている．そして"autofs" は，各ユーザー毎にエントリを作り，エントリには各ユーザーのマウントポイントが定義されている．クライアントマシンはこのツリーから必要な情報を引き出す．

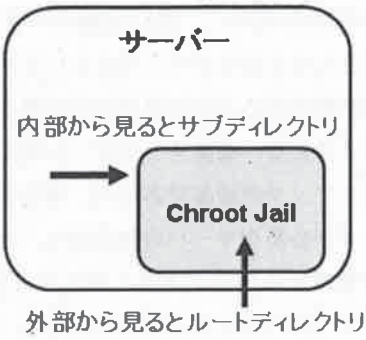

図4　Chroot Jail

5.　平時の管理

ネットワークを構築する時のことだけでなく，構築後のことも考慮しなくてはならない．今節ではネットワーク構築後のセキュリティやバックアップについて述べる．

5.1　ネットワークセキュリティ

ネットワークを構築する際，当然セキュリティについても考慮しなくてはならない．特に，メールや研究室のWebサイトなどは外部ネットワークとの接触があるので注意が必要である．今節では，それらのセキュリティについて述べる．

初めにWebについて述べる．本研究室でも研究室Webサイトを公開したり研究室メンバー個人のWebサイトを公開することが可能になっている．実験等を行う場合もあるので，ここでは基本的にCGIの制限などはしていない．場合によっては，ユーザーが作ったCGIに潜むセキュリティホールからサーバー本体の情報を見られてしまったり，何かしらのトラブルによってサーバー自体のroot権限を奪われてしまうということも考慮しなくてはならない．そこで，本研究室ではWebサーバーを"Chroot Jail"という領域の内部で動作させることとした．Chroot Jailとは表4のように，システム内のサブディレクトリを仮想的なルートディレクトリとして見せかけるものである．

これにより，Webサーバーや CGIのセキュリティホールを通過して侵入されても侵入者からはサブディレクトリがルートディレクトリに見えるため，侵入者を"檻(Jail)"に閉じ込めることが可能になり，被害を最小限に食い止めることができる．

次にメールについて述べる．メールでは2つの点について考慮しなくてはならない．一つ目はウィルスメールの予防，もう一つは迷惑メールの処分である．もしウィルスメールを受信して間違って開いてしまった場合，研究室内LANに接続するマシン全てに影響を及ぼす恐れがある．迷惑メールについても，ひとつひとつのサイズはそれほどでもないが，大量に受信するとそれだけでディスク容量を圧迫する恐れもある．本研究室ではIMAPサーバーを採用しており，メールは各ユーザーのホームディレクトリに一ファイルづつ保存されるため，ディスクを圧迫した場合他のユーザーにも迷惑がかかる．そこで本研究室では表6のアプリケーションを用いてこれらを対策することとした．

表6　スパム・ウイルスメール対策

アプリケーション	説明
glaylisting	一時的な受信拒否
spamassassin	スパムメールチェック
clamAV	ウイルスメール対策

まず，送られてきたメールはglaylistingにより，そのホストから初めて送られてきたかどうかを確かめ，初めての場合は一度受信を拒否する．この対策はSMTPサーバーの性質によるものである．SMTPサーバーは一度送信が失敗するともう一度再送する．しかし，スパムメールのホストは再送を行わないという性質があるため，これによっていくつかのスパムメールは拒否できる．このglaylistingを通過したメールは，clamAVに送られてウイルスメールかどうかチェックされる．clamAVは多くのLinuxディストリビューションで採用されているウイルスチェックソフトで，スキャンが高速である点が優れている．このフィルタを通過すると，最後にspamassassinによってスパムかどうかを確かめられる．spamassassinでは，そのメールの送り元ホストから以前スパムメールが届いたことがあるか，NGワードが含まれているか等を点数化し，一定以上の点数となったらそれをスパムと判断する．スパムと判断されたメールの行方に関してはメールサーバの管理者が設定することができるが，本研究室ではメールタイトルに"SPAM"と付与するだけとした．スパムメールをサーバで拒否または削除してしまった場合，万が一必要なメールでスパムと判断されたときにユーザーに届かない恐れがあるからである．タイトルにスパムであるという情報を付与することでユーザー自身で最後の確認ができたり，本当に必要な

ければメールクライアントソフトでブロックすることもできる．また，spamassassin はスパム学習機能も備えている．そこで，各ユーザーのメールボックスにスパム専用のディレクトリを作り，スパムと判断された場合自動的にそこに移動するようにした．これにより，スパム学習をメールユーザー全員のスパムボックスで行うことが可能となる．これにより，スパムメール・ウイルスメールは概ねブロックすることができる．

5.2 バックアップ

研究室内 LAN を運用する上で，バックアップ体制は非常に重要である．例えば LDAP サーバーにトラブルがあった場合，研究室のユーザーはどのマシンにも一般ユーザーでのログインができなくなってしまう．また，研究室では，各ユーザーのホームディレクトリや研究室 OB のディレクトリをファイルサーバーにて一括管理している．もしファイルサーバーでトラブルがあった場合は，中に保存されている研究データやメールなどを失ってしまう．本研究室では，主要サーバのバックアップ機を準備し，一定時期にメインサーバと同期をとるようにした．同期で利用するのは Unix コマンドの ssh コマンドと rsync である．rsync とはファイル同期アプリケーションの一つで，ディレクトリ間の同期を行うことができ，ネットワークでの利用もできる．また rsync は新旧ディレクトリ間の差分をとって同期を行うので，比較的高速なバックアップが可能な点で優れている．本研究室では，ssh 用の公開鍵と秘密鍵のペアを作り，それぞれのサーバーに置くことで，バックアップ機へのユーザーパスワードの入力なしでのログインを可能にし，Linux に標準で用意されている cron コマンドで同期を自動化した．これにより，管理者が同期を忘れるということを防ぎ，どちらのサーバも常に最新の状態を保つことができる．サーバー群に何かトラブルが発生した場合，最終的にはメインサーバとバックアップサーバを入れ替えることで通常のサービスを提供することができる．

6. 考察

本研究室のネットワーク構築の際に，各種サービスのバックエンドとして LDAP を用いることで，ユーザーアカウントなどの様々なデータを一ヶ所にて集中管理できるようになった．またユーザーの実験データや個人のメールなどもファイルサーバで管理することで，各種データの保存性を高めた．特に実験データは研究室にとって財産とも言えるもので，それを一ヶ所で集中管理することで継続研究において研究の引き継ぎも非常に容易にできると考える．重要データも一ヶ所で保存しているためバックアップが重要であるが，集中管理によってバックアップが必要なサーバの数が減り，それを自動化することで管理者の負担を大きく減らすことができた．外部メディアへのバックアップについても一台のファイルサーバから外部メディアへのバックアップだけでいいので，複数台から外部メディアへバックアップしなくてはならない場合よりも作業を簡略化できる．研究室内のデータをできるだけ集中して管理することで，ある程度大きなネットワークにおいても管理者の負担を大きく減らすことができる．

今後の課題として，各種管理ツールの導入を検討する必要がある．現在ユーザー管理は全て管理者で行っているが，これによって管理者でしなくてもいい作業が増えていると考える．例えば，ユーザーのログインシェルの変更はその一つである．ユーザーがログインシェルを変更したいとしても，現在の状態では全て管理者に依頼する必要があり，気軽に変更ができないユーザー側にとっても，仕事が増える管理者にとっても得策であるとは言い難い．研究室内で利用する PC についても同様で，その時使用していた PC と交換して新しい PC を利用しようとしても，管理者に依頼が必要となってしまう．ユーザーは必ず一つ以上の PC を利用しているため，一人一台は無条件に許可という方法をとっても問題ないはずである．しかし，管理ツールを導入することでこれらを解決できる．ユーザー情報の変更等，管理者が行っている作業の一部をユーザーができるようになれば管理者の負担はさらに減少するだろうと考える．

7. まとめ

本稿では小倉研究室の研究室内 LAN の構築について，主に LDAP を用いたユーザー管理を中心に述べた．また，LAN を運営する際の平時の管理についても，起こりうる例を挙げてその解決方法について述べた．本稿では LDAP を主にユーザー管理で用いたが，その他ネットワーク上に存在する様々な情報を整理して管理することも可能である．前節まで述べたとおり，ネットワーク管理者にかかる負担は大きい．しかしその負担を減らすことで設定ミスなどを減らし，ネットワーク自体の堅牢性も高まると考える．今後も負担減少と堅牢性の強化につ

いては検討していく.

参考文献

[1] 山上浩司: 工学部教育支援システムの開発 -研究室配属及び研究室内活動の支援を目指して-, 福井大学平成 18 年度卒業論文,2007.02.

[2] デージネット: 入門 LDAP/OpenLDAP ディレクトリサービス導入・運用ガイド, 秀和システム (2007)

[3] OpenLDAP: http://www.openldap.org

[4] Samba: http://www.samba.org

[5] 武田安真: 徹底解説 Samba LDAP サーバ構築 (2004).