東京家政学院筑波女子大紀要第２集　83～88ページ　　1998年

＜研究ノート＞

UNIXを使ったインターネット接続

山野井　一夫

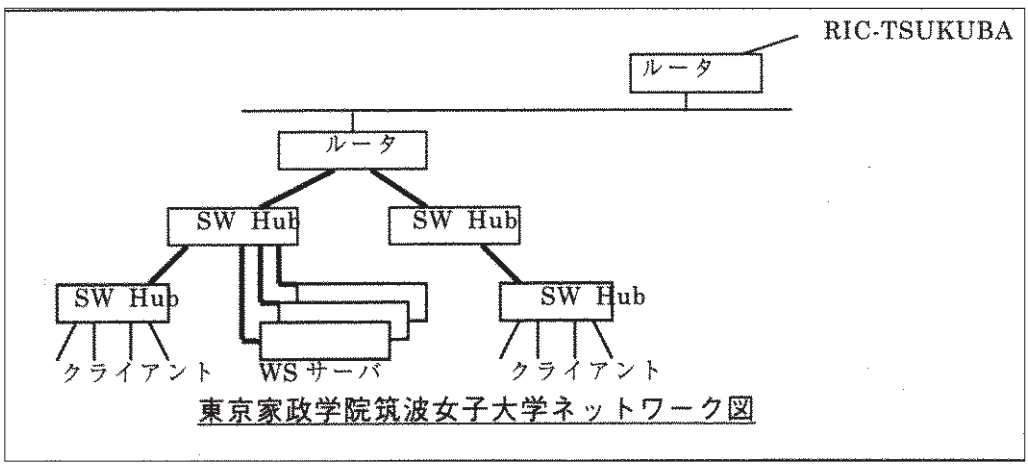
The Environment of INTERNET for UNIX Workstation

Kazuo YAMANOI

１　はじめに

本学は、平成５年度から学内ＬＡＮの導入が始まり、インターネットに接続されている図書館情報大学とＵＵＣＰ（電話回線を使ったコンピュータ間通信）による電子メール利用を行って来た。その後、平成６年度にはRIC-TSUKUBAとの64Kbps専用回線によるインターネット利用を本導入し、学生に電子メール（通信メディア）を使った教育利用を行っている。平成8年度からは、インターネット接続を64Kbpsから512Kbps専用回線に速度ＵＰし、WWWを使った教育（ホームページを使った情報の発信とインターネットからの情報収集）利用を推し進めている。

ネットワーク環境は、大きく学内ＬＡＮとインターネット接続に分けて構築している。学内利用は、専門知識の少ない教員・学生にも容易に活用できるように、WindowsNTをベースに学内サーバを構築した。学内の利用者



東京家政学院筑波大学ネットワーク図

は日頃から慣れ親しんだWindows95、Windows NT、Machintoshを使って、電子メール、ホームページ作成等を行っている。

インターネットへの接続は、ドメイン名とＩＰアドレスを定義するドメインネームサーバ（ＤＮＳ）、電子メールサーバ、Ｗｅｂサーバ、Ｐｒｏｘｙサーバ等の設置などが必要であり、動作の安定しているＵＮＩＸマシン（ＷＳ：ワークステーション）を用いて行っている。

このインターネット接続は、①増え続けるクラッカー対策、②著作権や機密を含むと思われる学内情報の隠蔽、③授業でのアクセス集中をさけるためのシステムの負荷分散④キャッシュサーバによるＷｅｂ情報収集の高速化⑤Ｗｅｂサーバ等の利用環境の向上を目的にシステムを幾つかのマシンに分散してサーバを構築している。

本紀要では、このＷＳをベースにしたインターネット関連のサーバシステム構築と概要について述べる。

２　システム構成

本学の学内ＬＡＮは、バックボーンを100 BaseT×２（国際学部＋図書館用、短期大学部用）で構築し、学内専用ルータでバックボーン間と外部とを接続している。各バックボーンには100Base-TのスイッチングHubを置き、利用の高いサーバ群は100BaseTで接続し、利用者のクライアントは100BaseT-10 BaseTのスイッチングHub、10BaseTHubを経由して、コンピュータ教室やすべての一般教室のネットワークコンセントに繋がっている。本学では、利用者がネットワークを、どこからでも接続できるインフラ、構内ＬＡＮを本年度から整備している。

インターネット接続では、インターネット接続用のＷＳを３台用意し、それぞれの目的に合わせて次のように配置している。

WS1: 学外用サーバ１（Ｓ－４／２０Ｈ）
　　プライマリィＤＮＳ
　　プライマリィＳＭＴＰサーバ
　　仮想Ｗｅｂサーバ
　　キャッシュサーバ
WS2: 学外用サーバ２（Ｓ－４／５）
　　セカンダリィＤＮＳ
　　セカンダリィＳＭＴＰサーバ
WS3: 学内用サーバ（Ｓ－７／３００Ｕ）
　　ＤＮＳ
　　ＳＭＴＰサーバ
　　仮想Ｗｅｂサーバ
　　キャッシュサーバ
　　Ｗｅｂサーバ

その他のサーバと呼ばれるものは、学内用として、WindowsNTをベースに電子メールシステム、Ｗｅｂサーバ、ＤＨＣＰサーバ、ファイルサーバ、プリントサーバやライブカメラなどが学部ごとに用意され接続されている。

３　ＤＮＳの二重化

インターネットは、あらゆるジャンルの人が生活する公共の世界規模ネットワークであり、犯罪天国ともいわれているほど何をされるかわからない世界である。本学も外部からのハッカーと思われる人間からftp、telnet、smtpやWebを使った侵入を試みる形跡があとをたたない。これらすべてを防ごうとすればFirewallシステムと呼ばれる防御システムを導入すればよいのだが金銭的面や、システムが大規模になるにつれてトラフィック増大によるFirewallの信頼性の不安があり、導入は先送りになっている。

本学では、幾つかのハッカー対策の一つとしてＤＮＳを学内用と学外用の２つにするを考え、幾分かの防御に役立っている。このＤＮＳを２つに分けることより学外から必要のないマシン名を削除することができる。学外

用のＤＮＳには必要最低限の情報を載せて、ＩＰアドレスの逆引きなどを利用してマシンをある程度特定できないようにしているである。学内用は、利用しやすいようにすべての情報を現在載せており、WS1、WS2、WS3を含めて学内のマシンはすべて学内用ＤＮＳを使っている。

ＤＮＳを学内用と学外用に二重化するには、２つのＤＮＳを置き、学内用ＤＮＳのキャッシュに学外用ＤＮＳを設定すれば簡単にできる。ここで忘れてはいけないのは重複する学内のＤＮＳへのドメイン登録も必ず２つのＤＮＳで定義しなければならないことだ。なぜなら２つのＤＮＳは、どちらも自分がkasei.ac.jpのドメインと認識しているからである。

ＤＮＳでマシン名を隠蔽したシステムへの侵入の試みは現在ないが、本格的なハッカー（破壊活動を目的とするクラッカーと呼ばれる人種）の侵入を考えると、まだセキュリティ問題が解決されたわけではない。

幾つかのサイトでは、pingコマンドによるマシンの応答を遮断する方法を導入しており、マシンの存在も外部からは判断しにくくする防御を行っているところが増えているようである。

４　仮想Ｗｅｂサーバ

学内で稼動しているＷｅｂサーバには、WindowsNTで構築した国際学部用Ｗｅｂサーバ、短期大学部用Ｗｅｂサーバ、Ｗｅｂサーバ機能を持ったライブカメラ、学生のCGI実習用Ｗｅｂサーバ、あとUNIXシステム上で動いている卒業生が作成した過去のＷｅｂ情報を入れておくＷｅｂサーバ（WS3）、図書館専用Ｗｅｂサーバなどがある。Windows NT上で動く電子メールシステム（Post Ofice）もＷｅｂで簡単に管理でき、ライブカメラ（AXIS製）もＷｅｂで設定可能できる。

本学では、ライブカメラの利用統計を取りたくても取れない問題や、増えるＷｅｂサーバの名前を覚えきれない、学内の機密情報を外部に出したくないなどを解決するために、delegate(電子総合研究所で作成)を使って１つの仮想Ｗｅｂサーバhttp://www. kasei.ac.jpとして構築し、運用している。利用者からは、すべてがこのwww.kasei.ac.jpというマシンの下にあるように錯覚して見えるのである。

利用者は、このdelegateを経由し実Ｗｅｂサーバをアクセスする。また、実Ｗｅｂサーバのポート番号を８０から他の番号にすることにより、ハッカーの侵入阻止にも完全ではないが多少役立っている。

また、ライブカメラの場合、delegateでMOUNT=”/camera/1/[fh]*　http://ライブカメラ:ポート/*”と仮想化の定義をすることにより、先頭がfかhでないものはアクセスできなくし、ライブカメラの設定機能を完全に隠蔽した。この方法で、他の実Ｗｅｂサーバについても、ハッカーに狙われやすい情報はすべて隠蔽している。

仮想Ｗｅｂサーバは、学内用と学外用を起動することにより、同じＵＲＬでも重要な学内情報は仮想化する先を変更して外部から覗くこができないように実Ｗｅｂサーバに割り付けている。この仮想Ｗｅｂサーバとして使っているdelegateは、独自の機能でアクセス元により仮想化を変更できる機能をもっているが、後に述べるキャッシュサーバとの組み合わせを考慮して、別々の異なったマシンで運用している。この異なったマシンでの運用は、負荷の分散と利用統計を学外者と区別してとれる効果がある。

学内専用と学外者用Ｗｅｂサーバの構築に踏み切った理由は、学内機密情報の隠蔽が最大の目的である。近年、検索エンジンシステムがＷｅｂ内をしらみつぶしに情報を読み取り、検索データベースに登録を行っている、この検索ロボットソフト（芋蔓式に次々とリ

ンクを元に情報を読み取る）が毎日のようにやってくる。これらの検索ロボットによって秘密情報も簡単に外に漏れてしまう。検索ロボットの検索範囲をrobots. txtで記述しておけばよいのだが，考慮していない検索ロボットもあるために信用できないと考えて、本学では仮想Ｗｅｂサーバを二重化し運用することにした。

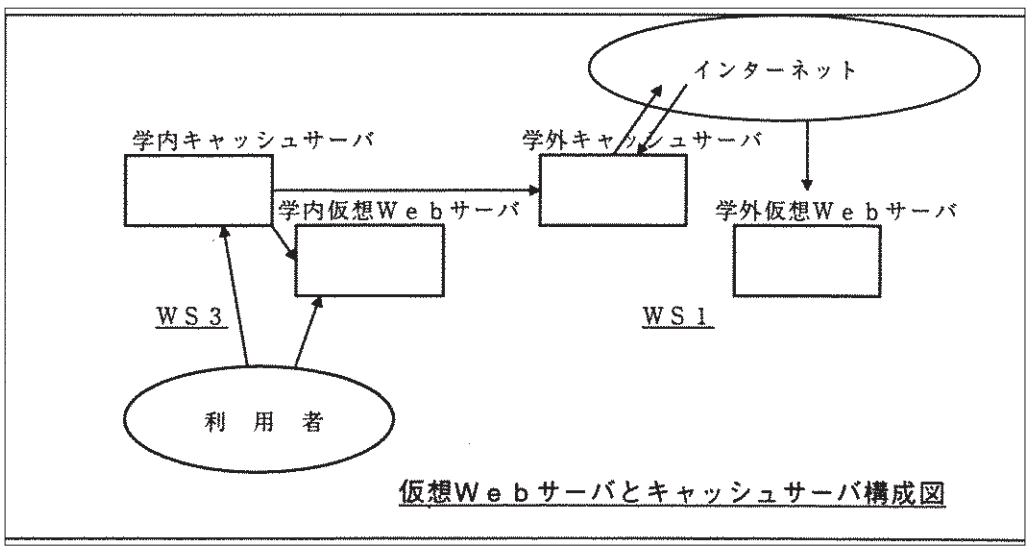
５　電子メールサーバ

本学では利用環境の向上を考えて中継用の電子メールサーバ（SMTPサーバ）を複数設置している。外部からの電子メールはWS1かWS2に一時蓄積され、学内利用者が使うWindowsNT上の電子メールサーバに送られる。この時、ＤＮＳのMXレコードの情報を読み取れないか無視をしている学外の電子メールシステムから、直接WindowsNTの電子メールシステムに送り付けてくるものが多くある。電子メールの履歴を集中管理する上で問題となるためにＤＮＳによって電子メールシステム名を隠蔽し、ＵＮＩＸ上のＳＭＴＰサーバを必ず経由するようにしている。

もう１つの問題が外部への電子メールを送る場合である。緊急の電子メールを送るユーザからの意見で、相手マシンがダウンしている場合１時間置きに７日の再送期間が過ぎて遅れなかったでは困るとの申し出があり、本学では外部からの受信用ＳＭＴＰサーバ２台と内部から外部への送信用ＳＭＴＰサーバを置くことにより可能にしている。外部送信用ＳＭＴＰサーバはWS3に置き、学内の電子メールサーバからの外部送信は常にWS3に送る。このWS3は、相手電子メールシステムが２分間隔で20分応答がないと電子メールは送信者に戻されるように設定されている。

６　Proxyサーバ

Proxyサーバは、Ｗｅｂサーバをブラウザ（本学はNetscapeを利用）で多数の人が直接見に行くと通信回線のトラフィックが当然増大する。学校の授業中、みんなでブラウザを使った場合、ネットワークがストップ状態になりかねない。Proxyサーバは、このトラフ



仮想Ｗｅｂサーバとキャッシュサーバ構成図

ィックを軽減するための技術であり、ブラウザがProxyサーバを経由して相手のＷｅｂサーバを見に行くようにしたものである。この時、Proxyサーバは読み込んだ情報をディスクにキャッシュして、次回に同じ情報を要求されたらキャッシュした情報を返す。

本学は、当初CERNのhttpdをProxyサーバとして運用してきた。しかし、運用に伴い次のような問題が発生してきた。

① 学生が手入力でURLを入れた場合、間違ったURLのサイト名がディスクのキャッシュに残ってしまう。特に漢字で入力された場合、コード系が違うため、UNIXからキャッシュが確認できない、このようなごみの名前を消すのが困難になった。

② キャッシュの一段目のディレクトリィはＷｅｂサイト名になるために、数が増えるにつれて、ディスクのアクセス効率が徐々に悪化してきた。

③ 昨年度冬ごろからネットワークの混雑（SINETの国外線とWIDEとの線）が原因で、途中までしか読み込まれていないディスクのキャッシュが発見され、増大している。これにより利用者からＷｅｂの情報を見るのが困難になってきた。

④ Ｗｅｂサイトからの読み込みの途中で死んでしまったProxyサーバの分身がゾンビのように増加しており、夜中に起動し直す必要がでてきた。これもネットワークの混雑が原因と考えている。

原因の多くがインターネットの混雑で、セッションの時間切れで相手から切断、もしくは混雑によってセッションが切断されたものと考える。

この問題を解決するために平成９年からProxyサーバを電子総合研究所のdelegateに変更を行った。変更により、①の問題、③の問題、④の問題は解決されたが②の問題であるキャッシュが増大した場合の速度低下の問題が残った。

さらに問題を解決するために平成９年度４月からProxyサーバを今度はキャッシュサーバSquidに変更した。Squidは、キャッシュをディレクトリィ名でＵＲＬサイトを管理しないためにキャッシュ量による速度低下の問題は解消した。この他、Squidの導入により次にあげる効果も得ることができた。

① sibling（兄弟）と呼ばれるSquidサーバ同士の接続により、外のSquidサーバのキャッシュを利用することによりキャッシュされているＵＲＬのアクセス速度が上がった。

② ドメイン別にparent（親）の設定ができ、外の親Squidサーバを経由してＷｅｂ情報を見に行けるようになった。この機能で適切な親を選ぶことによって、幾つかのＷｅｂサイトについては高速に情報を収集することが可能になった。

③ ディスクキャッシュ容量を指定することにより古いキャッシュをシステムが自動で削除できるようになり、残りディスク容量に関するメインテナンス面で容易になった。

7　tcp_wrapperの導入

インターネットのサイトには、狙われる物がうちのサイトにはないからと安易に考えているところがあるが間違いである。踏み台と呼ばれる接続先をごまかす為の繋ぎにされないよう、本学もハッカーの侵入には特に注意している。

ハッカーは、外部から特定のサービスをねらって侵入を試みるが、すべてのサービスを止めるわけにはいかない。多くの不必要なサービス（rshやrloginなど）は止めても、メインテナンス用に必要とおもわれるサービスは止められない。

インターネットの利用で問題になるハッカーを防ぐために、本学ではtcp_wrapperと呼ばれるソフトウエアをすべてのＷＳにインスト

ールしている。ソフトウエアはアクセスしてきたＩＰアドレス、ドメイン名を元に利用制限するためのソフトウエアである。侵入の試みがあった場合には管理者に侵入元とサービス名を電子メールで通知する。現在は、１月に10件ほどの不法なアクセスが電子メールで届くが、マシンに侵入された形跡は今のところない。

８　ま と め

筆者は、インターネットとの接続にあたり、より高効率な利用環境の整備、インターネットからの侵入者対策、Ｗｅｂの学内情報の隠蔽、そして利用しやすい環境をめざして学内のネットワーク構築をしてきたことを中間報告する。

本学のネットワーク整備にあたり、多くの方々に御協力をいただいたことをこの場を借りて深く感謝いたします。