【論文】

VPNを用いた分離したネットワークの統一

本田　貢†　松本勝哉††

Integration of Physically Separated Sub-networks by use of VPN

Mitsugu HONDA†　Katsuya MATSUMOTO††

Abstract: The depletion problem of IP address is going on in order to widely use of the INTERNET in these ten years. One of the simple solution of this problems in the small local area network is to use the private address that we don't need to connect directly to global world. But it appears difficult management of physically separated sub networks. In this paper we show the way how to integrate the physically separated sub-networks by use of VPN. And we also present the effective machine monitoring by free softwares.

Keywords: VPN, sub-network, integration

1　はじめに

年々インターネットの使用量は増えグローバルIPアドレスの枯渇問題が出てきた。現在インターネットで主に使われているインターネットプロトコルはIPv4と呼ばれる方式で、32ビットのアドレス長を持ち、約43億台のコンピュータにアドレスを振り分けることができるが、増え続けるインターネット人口に耐えきれなくなってきている。

松本研究室でもPCの増加に伴って研究室に割り振られたグローバルIPの不足や、8号館7階ネットワークへの通信データ量の増大という問題から研究室内をサブネット化することになった。このようにすることによって使用するグローバルIPの数が減り、8号館7階ネットワークへのデータ量も少なくなった。さらに、ネットワークの通信速度を増しセキュリティレベルも高めることができた。しかし、松本研究室のように院生室と学部生室が物理的に離れている場合には、サブネットが分離してしまい、通常の接続法では直接通信することができない。そのため相互に利用するサーバ、例えばファイルサーバなどはグローバルネット上におかなければならず、セキュリティ面での問題となっていた。

本研究ではVPNを応用して2つの離れたサブネットワーク同士を仮想的に1つのネットワークとグローバルネットワーク上においてあるサーバをサブネット内に入れ、研究室内のセキュリティの向上を図る。また、サブネット上にあるプリンターなどの機器の共有も行い、導入したVPN環境をシステム管理まで含めて有効的に使える環境改善を試みることにした。

2　研究室内LAN

2.1　サブネット化前の研究室内LAN

サブネットとは、大きなネットワークを小さなネットワークに分割して管理する際の管理単位となる小さなネットワークのことである。学内の主幹ネットワークの中に電気情報工学科のネットワークがあり、さらにその中で分割されて各研究室で管理することとなる。この研究室単位で管理する小さなネットワークがサブネットということになる。学科ネットワークを例にすると次の図2-1のように

†　工学研究科電気工学専攻2年
††電気情報工学科

なる。

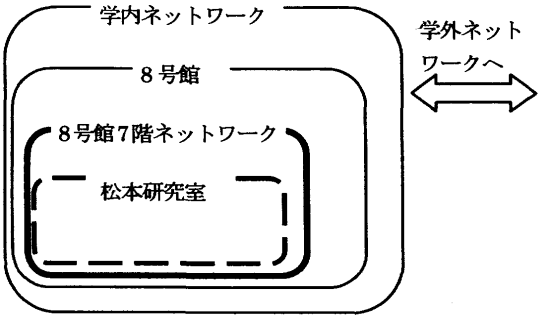

図 2-1 学内ネットワークとの関係

図 2-2 はサブネット化前の研究室内ネットワークである。学部生室には複数の PC があり、それぞれがグローバル IP アドレスを持っている。院生室も学部生室と同様な状況で PC がありその中にファイルサーバが置かれている。この構成では、8 号館 7 階のネットワーク上のトラフィックが増大し、通信が混雑した場合、学部生室と院生室間の通信が影響を受け、ファイルサーバとのデータ送受信に支障をきたす可能性があった。また、ブロードキャストなどによって必要のない無駄なパケットが流出し、8 号館 7 階のネットワーク上に無駄なトラフィックを増大させていた。

さらに、PC の増加によって、研究室ごとに与えられたグローバル IP アドレスが不足して、インターネットに接続できない PC がでてきたことや、どの PC にファイルを保存したのか等の問題が発生してきたので、研究室内のネットワーク及び PC の管理が重要になってきた。

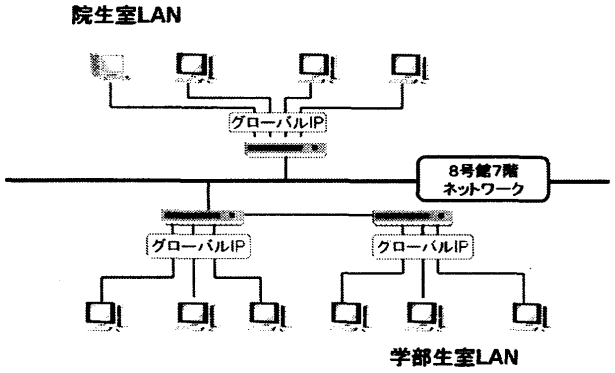

図 2-2 サブネット化前の研究室内ネットワーク

2.2 サブネット化後の研究室内 LAN

研究室内のサブネット化を行うことによって、2.1 で挙げられていた問題を改善できる。

サブネット化されたネットワークは、松本研究室学部生内にあるサーバ機 Blue で管理されている。OS が Red Hat Linux9.0 であるのは、オープンソースという理由からである。また、ファイルサーバは Blue 内に構築されているので、Blue の下に配置された各 PC は、8 号館 7 階のネットワークを介さずにファイルサーバに接続することが可能となった。

サブネット化のほかに、研究室から松本研究室のホームページを配信するという試みから Web サーバを構築することとなり、院生室内にあるサーバ機 Brazil に導入された。

その後、他の研究課題との関係で Blue のファイルサーバ機能を他のファイルサーバ専用機に移すことになり、サーバ機は院生室と学部生室両方からアクセスできるようにと 8 号館 7 階のネットワーク上に設置した。この環境の研究室内 LAN を図 2-3 に示す。

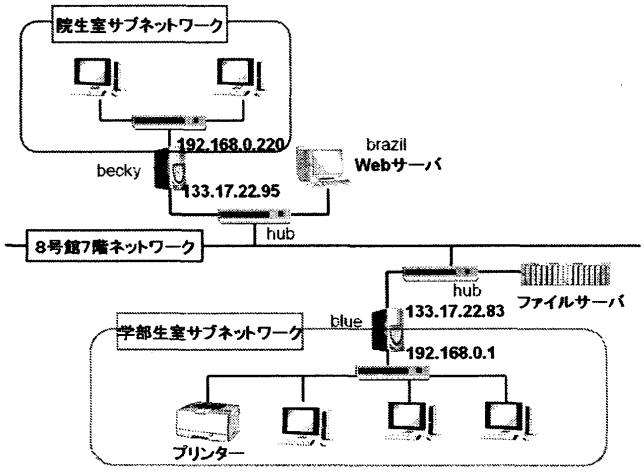

図 2-3 サブネット化後の研究室内 LAN

2.3 VPN でネットワークを 1 つに

ファイルサーバの安全性を考えればサブネット内に入れることが好ましい。外部ネットワークからサブネット内のサーバにアクセスするためにはルーティングという手法がある。しかし、ルーティングは利用するサービスごとに設定が必要であり、ルーティングするサービスが増えるほどより複雑な設定が必要となってしまう。

そこで、図 2-4 のように学部生室側のサブネットと院生室側のサブネットを VPN で繋げて仮想的にひとつのネットワークとする方法を探った。ルーティングと違い VPN はサービスがどのポートを利用しているのか意識する必要がないため、複雑なルーティングは無用である。また、VPN によってサブネット間の通信が暗号化されることにより、サブネット内のサーバの管理を安全に行うことも可能になる。VPN については後の章で説明する。

3 Virtual Private Network

3.1 VPN暗号化通信[1]

現在インターネットを利用する上でセキュリティのことを考慮しないわけにはいかないほどインターネットの危険度が増してきている。

遠隔地からインターネットを使って安全に学内、または組織内にアクセスをしたり、企業の支部同士を繋ぎ安全に通信したりするには専用通信回線が必要であった。この専用通信回線とは特定の 2 点間の通信を提供するサービスであり、一般的に使われている公共通信回線網が何らかの障害により通信ができないような場合でも確保しなければならない通信や、改ざん・盗聴を防がなければならない重要な情報を通信する際などのセキュリティを確保する回線である。この専用通信回線を確保する以外にも Web ベースでの暗号化接続を提供する SSL(Secure Sockets Layer)を使った手法などが取られていた。

しかし、専用通信回線を使った通信は非常に経費がかかり、SSL を使った通信は利用するアプリケーションに制限があり、ユーザはより安価でよりアプリケーションの自由度の高い通信環境を求めた。そうした環境に対して、VPN は有効な手段であり急速に広まっていった。

3.2 VPN とは

VPN とは Virtual Private Network の略称で、図 3-1 のように、公衆回線上に仮想的な専用線を作る仕組みである。公衆回線とは、一般電話網やインターネットに代表される公衆回線網のことである。

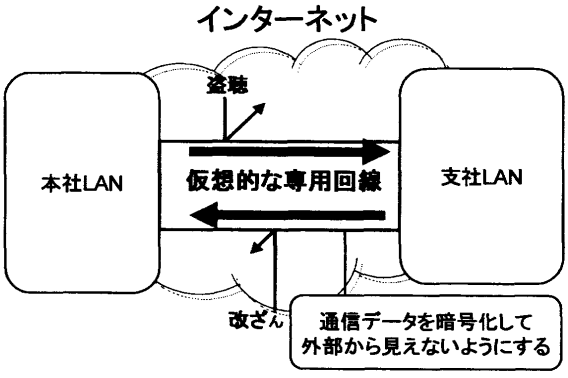

図 3-1 VPN の概念図

専用通信回線は公共の回線を通らず直接拠点同士を繋げることができるため安全性は高いが、接続地点間の距離と通信速度に応じて通信料がかかる。利用状況によって異なるが公衆回線に比べてはるかに利用料がかかる。VPN は公衆回線を介して、私的な LAN 同士および私的な LAN と端末機器が相互通信するため仮想的な専用線を作り、その専用線を使って通信することで LAN 同士を繋げる。私的な LAN とは学校内のネットワークや会社の社内ネットワークなどの私有回線網のことである。

VPN を構築するにも、ハードウェアで実現する方法やソフトウェアで実現する方法、更には専用回線を通して実現する方法やインターネット回線を通して実現する方法などさまざまな方法がある。

3.3 プロバイダ VPN[2][3]

プロバイダ VPN とは専用線を確保するのではなく、インターネット回線を提供するプロバイダ内ネットワークを利用した VPN である。

・IP-VPN

IP-VPN はユーザのネットワーク同士をプロバイダ内の IP-VPN 網で接続する VPN である。パケットは IP-VPN 網の入り口で MPLS(Multi Protocol Label Switching)という規格に沿って目的のネットワークに向けて転送される。

・広域イーサネット

広域イーサネットは規模の大きな LAN でも使われる VLAN を使った VPN のことである。IP-VPN と違い通信をレイヤ 2 で行っているため、IP や TCP などのプロトコルを気にせずに通信を行うことができる。

近年では IP-VPN と広域イーサネットを組み合わせて WAN を構築する複合型 VPN サービスが提供されるようになってきた。

3.4 インターネット VPN

ここまでの VPN サービスは通信事業者が保有している独自のネットワーク内を通して離れた LAN 同士を結び合わせるという特徴を持っていた、インターネット VPN は公共の回線であるインターネットを仮想的に専用線として使うことにより安価に VPN サービスを構築することができる。インターネット VPN は安価ではあるが通信事業者が提供する VPN サービスに比べると通信速度が遅く、また通信速度が一定でなく帯域が確保できないなどの特徴がある。インターネット VPN にはさまざまなタイプがある。

4 ネットワークの改善

4.1 VPN 導入前のサブネット環境

VPN 導入前のサブネット環境は図 2-3 のようになっており、以下の様な問題がある。

・ ファイルサーバがグローバルネットワーク上にある

学部生室サブネットと院生室サブネットの両方から使えるようにするためグローバルネットワーク上に置いてあるが、どこからでもアクセスできてしまうのでセキュリティ面に不安が残る。

・ 管理が分散している

サブネットワークが2つに分かれているので、互いの内部にあるマシン同士をつなげようとするとルーティング設定が複雑になってしまう。また、ゲートウェイが 2 つあるので両方共にファイアウォール設定などしなければならなくなっており管理しにくい。

以上の問題点を解決するためには、両サブネットが同じネットワーク範囲内に存在すればよく、対策として以下の方法が考えられる。

・ 学部生室サブネット以外を無線化する

学部生室内に無線LANアクセスポイントを設置すれば、クライアントが物理的に離れた位置にあっても、学部生室サブネットのネットワークに属することになる。無線 LAN は有線 LAN に比べて通信速度に劣るが、通常の通信だと問題はない。

・ VPN 接続を利用する

学部生室サブネットと院生室サブネットをVPN接続で繋げる。VPN には様々な種類があるが、その中でもレイヤ2トンネルを作成するタイプのVPN接続を利用すれば、2 つのサブネット間の通信はどんなプロトコルでも通過できるようになる。つまり、仮想的に 2 つの離れたサブネットを同一ネットワークとして扱うことも可能になる。

前者の方法だと、院生室サブネットのマシンが全て無線に対応しなければならず、コストがかかってしまう。そこで、後者のVPN接続を利用する方法で院生室サブネットと学部生室サブネットを仮想的に同一ネットワークにすることにした。

しかし、新しく PC を用意するのでは無線 LAN 導入するよりもコストがかかってしまうため、研究室内で既に使われていない PC を VPN サーバ、現状の院生室サブネットのルータをそのままVPNクライアントにすることにした。2つのサブネットを VPN 接続で繋げたネットワークを図 4-1 に示す。このネットワークは、既存のネットワークの構成を変更する必要がなく、VPN サーバを学部生室サブネットに設置するだけでよい。なお、学部生室のルータ機の blue が 2 つのネットワークのルーティング設定と DHCP による IP アドレス配布を担っている。

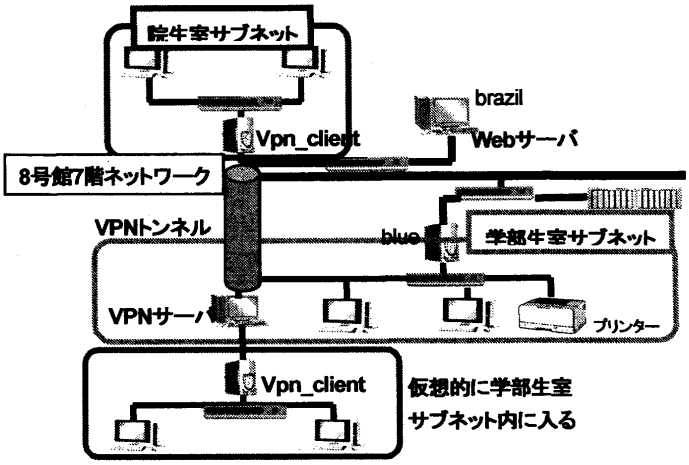

図 4-1 VPN 導入後のネットワーク

4.3 VPN 環境の構築

このVPN環境を構築するにはレイヤ2トンネルを作成できるVPNアプリケーションを選ぶ必要がある。そこで、IPsec よりも容易に使用できる OpenVPN というアプリケーションを使った。OpenVPN については次に説明をする。

4.3.1 OpenVPN[4]

OpenVPN とは GPL ライセンスに帰属し、オープンソースプロジェクトで開発されており、無料で入手することができるソフトウェアである。標準では通信の暗号化に OpenSSL を利用し、仮想ネットワークデバイスを使用したレイヤ2、レイヤ3レベルでのVPN通信を可能にする。OpenVPN の特徴は通信に TCP/UDP を選択することが可能で柔軟なネットワーク設定を行うことができる点や、他の SSL-VPN サービスと異なり VPN サーバにアクセスするためにクライアントソフトを使用する点である。接続にクライアントソフトを必要とすることにより、他の SSL-VPN サービスにある SSL に対応したアプリケーション(例えば Web ブラウザなど)のみ接続できるという制約が取り払われ、基本的にどんなプロトコルでもネットワーク上を通信することが可能となる。また、Windows、Linux、Solaris、MacOS など複数の OS 用にパッケージが提供されているのも特徴のひとつである。

4.3.2 OpenVPN の動作

OpenVPN は使用する用途に応じて設定を変更する必要がある。OpenVPN で構築できる VPN の構成は以下の2種類の方法がある。

・ルーティングモード

ルーティングモードはVPN接続がレイヤ3で行われて

いる。ルーティングモードでは、VPN サーバと VPN クライアントが既存のネットワークと異なるネットワークを構築する。VPN クライアントの IP アドレスは VPN サーバから割り当てられる IP アドレスになる。そして、そのアドレスは既存のネットワークと同じネットワークアドレスを割り当てることができない。つまり、VPN クライアントは既存のネットワークのマシンへ接続することができない。接続するためには VPN サーバに適切なルーティングルールを加える必要がある。

・ブリッジモード
ブリッジモードは VPN 接続がレイヤ 2 で行われている。ブリッジモードでは VPN クライアントは、VPN サーバのネットワークに追加される形でネットワークを構成する。VPN クライアントは既存のネットワークの IP アドレス構成を引き継ぐので VPN クライアントは既存のネットワークのマシンへ直接通信することができる。

4.4 VPN 環境の構築

VPN 環境を構築するマシン環境として VPN サーバ、VPN クライアント共に Linux ディストリビューションの 1 つである ubuntu を利用した。

また、本研究では VPN サーバは学部生室サブネット内にあるので、このままではサブネット外部のマシンからは直接接続することができない。そこで、学部生室サブネットのルータである blue にルーティングルールを付け加えることによって外部からの通信を直接 VPN サーバに繋げられるようにする。
VPN 環境の構築の流れは以下通りとなる。

・OpenVPN インストール
・ブリッジ接続の設定
・VPN サーバの設定
・VPN クライアントの設定
・ルーティングルールの追加
・VPN 接続の確認

4.4.1 Ubuntu[5]

Ubuntu は Linux ディストリビューションの 1 つである。Debian GNU/Linux をベースとしているが、より使いやすさや、定期的なリリース、インストールの容易さを重要視している。Ubuntu の特徴は「インストールすればすぐに使える」という点である。そのため、多様なアプリケーションがパッケージとして提供されており、コマンド 1 つで容易にダウンロードとインストールを行うことができる。

また、フリーな OS はセキュリティフィクスやバグフィックスの提供などシステムの安定性に関わる部分もボランティアベースで開発されているが、Ubuntu は Canonical Ltd という企業が行っているため、安定した品質を保たれている。

4.4.2 OpenVPN のインストール

OpenVPN のパッケージは OpenVPN の Web サイトのダウンロードページから入手することができる。Debian 系 Linux の場合、APT パッケージに含まれているため apt-get コマンドや Synaptic パッケージマネージャーを使用することで簡単にインストールすることができる。その他の Linux の場合でも簡単にインストールできるように作られている。

本研究では、VPN 環境をブリッジモードで構築するので、Linux でブリッジ接続を提供する bridge-utils と、証明書と認証鍵を作成することが可能な OpenSSL を追加でインストールした。

4.4.3 VPN サーバの設定

この章では、学部生サブネットと院生室サブネットとのつながりのみを重視しているので TCP・UDP のプロトコルの選択、暗号強度の設定、暗号アルゴリズムの選択などは初期のままで設定を行っている。

VPN サーバの設定で必要な項目は以下の通りになる

・使用するポート番号
・TCP/UDP の選択
・Tap/Tun デバイスの選択
・使用する仮想インターフェースの名前
・CA 証明書、サーバ証明書、サーバ秘密鍵、DH 鍵のパス指定
・ブリッジモードで起動させるための設定
・クライアントにサーバ側ネットワークを知らせる
・クライアント側の通信を全て VPN サーバ経由にさせる
・クライアント同士の通信を可能にする
・暗号化方式の選択
・動作時ログのパス指定

上記の通り OpenVPN サーバは仮想インターフェース、証明書と暗号鍵を必要とする。仮想インターフェースの生成は OpenVPN 本体に実装されておりサーバ起動時に自動的に作られる。証明書と暗号鍵については認証局と暗号鍵を生成するためのスクリプト群が用意されており、それを利用することで容易に証明書と認証鍵を作ることが可能である。

ブリッジモードはVPNサーバで設定するだけでは使用することができない。VPN サーバを立ち上げる前に、仮想インターフェースと物理インターフェースをブリッジ接続する必要がある。事前に作成したブリッジインターフェースを利用してOpenVPNはVPN接続を実現している。

また、クライアント側の通信を全てVPNサーバ経由にさせているのは、ネットワーク内部の通信の出入り口を1箇所とするためである。もし、この設定をしなければ院生室サブネット側の通信は、学部生室サブネット内のマシンにアクセスする時のみVPN通信をし、それ以外の通信は院生室サブネットのルータから出て行くようになる。このように、同一ネットワークでありながら、出て行く経路が2つあるとネットワーク経路の混乱をまねく可能性がある。

したがって、出入り口を1つとすることにより、ファイアウォールやルーティングの設定を一元化することができる。

4.4.4 ブリッジ接続

ブリッジ接続とは、2つのネットワーク間を直接接続する方法である。本来は「ブリッジ」とはメディアの異なるネットワーク同士を接続するための装置の名称だったが、OpenVPN では 2 つのネットワークの間を直接接続することを指す。

LAN 同士のブリッジ接続は、HUB のカスケード接続によく似ている。カスケード接続とは、2 台の HUB によって構成されている別々の 2 つの LAN を、クロスケーブルまたはカスケードポートによって LAN ケーブルで接続することにより、2 つの LAN が 1 つの同じ LAN として通信することができるようにする接続方法で、中規模・大規模な LAN では必ず利用されている。

4.4.5 VPN クライアントの設定

この設定は院生室サブネットの出入り口であるルータ機に対して行う。ルータ機以下のサブネットの通信を全てVPN サーバ経由で流すので、仮想インターフェースとサブネット側物理インターフェースをブリッジ接続する必要がある。VPN クライアントの設定の手順は以下のとおりになる。

- VPN サーバの IP アドレスまたはホスト名を指定
- Tap/Tun デバイスの選択(ブリッジモードならば tap)
- TCP/UDP の選択(サーバ側の設定と同じ)
- 使用するポート番号の指定(サーバ側の設定と同じ)
- CA 証明書、サーバ証明書、サーバ秘密鍵のパス指定
- 暗号化方式の選択(サーバ側の設定と同じ)

以上のように、設定のほとんどはVPN サーバ側の設定に合わせる形となっている。もし、設定がかみ合っていないならば当然のようにVPN 接続はできない。しかし、クライアント自体は正常に起動しているのでVPN接続できない場合は VPN クライアント、VPN サーバ両方のログを見てどこに原因があるのか特定する必要がある。本論文中の Vpn_cliant の動作を次の図 4-2 に示す。

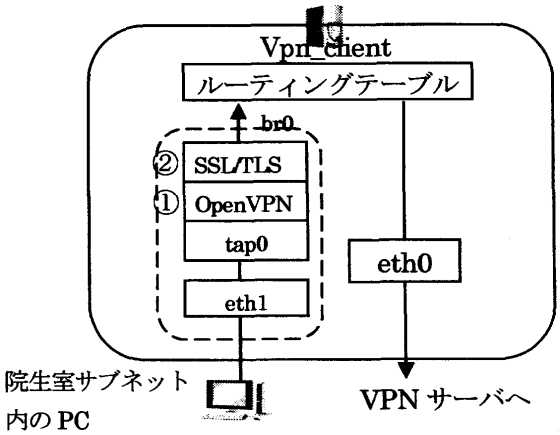

図 4-2 VPN クライアントの動作

また、VPN クライアントの働きにより転送されるパケットの内容がどのように変化していくかを次の図 4-3 に示す。

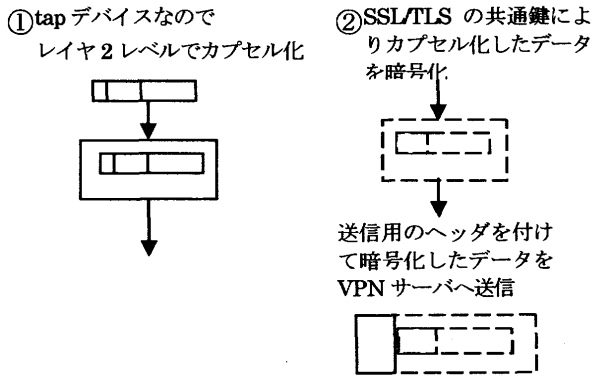

図 4-3 パケットのカプセル化

4.5 VPN 環境のメリット・デメリット

本研究で構築した VPN 環境を導入し、利用する上でのメリット・デメリットを以下に示す。

メリット

・セキュリティの向上

VPN 環境において最大の長所はやはりこの点である。

異なるサブネット間を通信する場合、パケットは通常の通信とほぼ同じ経路を取るが、通常の通信と違い暗号化されていることが大きい。これにより、通信を傍受されても中身を見ることが難しくなる。

・マシンを置く場所を選ばない

学部生室は現在サーバがある部屋ということで年中空調が入っている。ネットワークが同一で使えるようになると、管理上の都合により現在院生部屋においてある一部のサーバを学部生室の中に入れることができ、マシンにとってよい環境で動かすことができるようになる。

・ネットワーク管理が容易になる

本研究のVPN環境は、院生側サブネットの通信が全て学部生側サブネットのゲートウェイを通る。このことにより、ファイアウォールやルーティングの設定を学部生側ルータで一意的に設定することが可能となる。

デメリット

・通信速度の低下

これは通常より経路が多くなってしまったためと、通信する際に暗号化などさまざまな処理をしているためである。また、追加のヘッダをつけるためにデータ部分が少なくなってしまうのも要因の1つである。

・ネットワーク環境の安定性の低下

サブネット同士が独立していた時は、片方のルータが落ちても、もう片方のネットワークは動いたままであった。VPN環境の場合、VPN環境を保つためには学部生室サブネットのルータ、VPNサーバ、VPNクライアントの3台が同時に不備なく動いていないといけない。どれか1つのマシンが止まってしまうとVPN環境が保てなくなってしまう。

5 マシンの監視

ネットワーク環境は常に安定して使えることが重要だと考えられる。そこで、VPNサーバとVPNクライアントの2台のマシンの状態を監視することで異常の発生を速やかに察知できるようにする。今回、ハードウェアの監視を行うにあたりmuninというソフトウェアを使った。

5.1 munin

muninはPCのハードウェアの状態をグラフ化表示するためのソフトウェアである。同様のソフトウェアにネットワークのトラフィック監視などに用いられているMRTGなどがある。MRTGはSNMP(Simple Network Management Protocol)というネットワーク上の通信機器を監視するプロトコルを利用し、ハードウェア情報を集め、それをグラフ化表示するソフトウェアである。muninはSNMPを使わず、Linuxのハードウェア情報を集めているprocファイルシステムを参照することでハードウェア情報を集めグラフ化する。

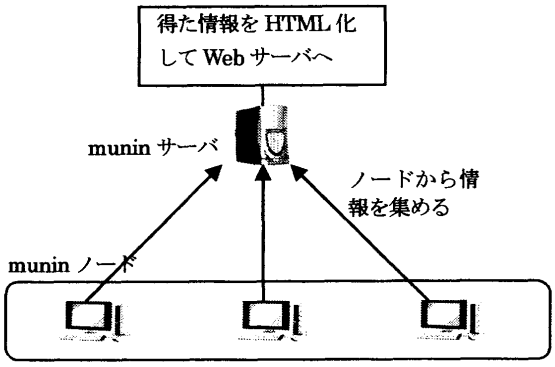

図5-1 muninの動作

procはLinuxシステムなどのUnixシステム以外、Windowsシステムなどprocが導入されていないマシンの情報を得ることはできない。muninにはその様な場合のためにSNMP経由で情報を得るための機能が備わっている。また、グラフ化したい情報を増やす場合にも簡単に追加できるプラグインが用意されている。

図5-1に示すように、muninはmuninサーバとmuninノードの2つのパッケージから成り立っている。ノードはハードウェア情報を集めるマシンにインストールして常時起動した状態にする。サーバは一定の時間ごとにノードへ問い合わせをし、ノードからハードウェア情報を受け取って、その情報を元にグラフ化する。そのグラフ化された情報はHTMLテキストとしてWebサーバによって配信され、ユーザはグラフを閲覧することによりマシンの状態を知ることができる。

5.2 procファイルシステム[6]

procは、プロセスやメモリなどのLinuxシステム上のリソース関連情報を、あたかもファイルであるかのように配置した仮想的なファイルシステムである。仮想的とはいえ、通常のファイルと同様にアクセスできる。

procには、プロセス関連情報やメモリ関連情報などが、ファイルとして配置されており、CPUの情報やメモリの情報などのファイルの値は、情報を必要とするアプリケーションなどから直接参照されている。procに含まれる主なファイルは表5-1のようになっている。

表 5-1 proc に含まれるファイル

ファイル名	意味
cpuinfo	CPU情報
meminfo	メモリ情報
net	ネットワークに関する設定
swap	スワップの利用情報

5.3 munin の実装

今回 munin は VPN 環境を維持するために必要な VPN サーバと VPN クライアントを監視の対象として実装した。

munin の動作はマシンスペックを必要としないため、munin サーバを VPN クライアントに導入し自らと VPN サーバを監視させるよう設定した。今回は、使い古したマシンを再利用する形で VPN 環境を構成している、そのマシンの中でも HDD は特に故障しやすい部分である。そのため HDD 情報を参照するプラグインを導入した。

munin により生成されたグラフの一例を次の図 5-2 に示す。

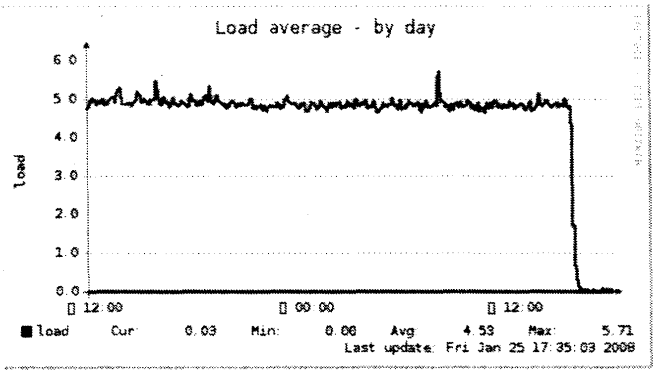

図 5-2 munin が生成したグラフ

6 おわりに

本論文では、研究室ネットワークの特徴を活かしたまま、安全で管理しやすいネットワーク環境の改善を試みた。VPN 接続を利用することにより目的は十分に達成された。

サブネットワークの独立化に代表される研究室内ネットワーク環境を改善する研究は数年来継続して行われてきた。その中で共通して、サブネットワークが院生室と学部生室 2 つに分かれてしまっていることが問題となっていた。部屋をまたいで通信を行う場合には使用するアプリケーションごと、マシンごとに、ルーティングルールを書き換えなければならなかった。

本研究により 2 つのサブネットが 1 つにまとめられたことにより、ルーティングルールを追加することなく離れたサブネットのマシン同士が通信できるようになった。また、ルーティングと違いサブネット間の通信が全て暗号化されているため安全性も高まっている。このため、研究室内にある各種サーバの管理やサブネットマシン間のファイル交換などがより安全に行えるようになった。

これで本研究を終えるが、今後の検討課題として以下のことがあげられる。

・ 復旧に関して、VPN サーバ又はクライアントを再起動することにより VPN 環境の復旧ができるようになっているが、人の手を使わず自動で復旧できるよう設定をする必要がある。

以上のことをやり遂げることにより VPN 環境はより安定し、より扱いやすくなると考えられる。

参考文献

[1]株式会社アスキー：アスキービジネス
http://ascii-business.com/vpn/vpn2-1.html
「VPN の基礎知識」
(2008-1)

[2]株式会社リクルート：キーマンズネット
http://www.keyman.or.jp/search/network2/30001597_1.html
「IP-VPN」
(2008-1)

[3]株式会社リクルート：キーマンズネット
http://www.keyman.or.jp/3w/prd/97/30001597/
「広域イーサネット」
(2008-1)

[4]株式会社アイティーブースト：スタックアスタリスク
http://www.stackasterisk.jp/tech/systemConstruction/openVpn01_01.jsp
「OpenVPN で構築するリモートアクセス環境」

[5]ウィキメディア財団：Wikipedia
http://ja.wikipedia.org/wiki/Ubuntu
「Ubuntu」

[6]株式会社日経 PB 社:ITpro
http://itpro.nikkeibp.co.jp/article/Keyword/20071214/289515/
「/proc とは」