学外から使う，学内 LAN

技術センター　情報メディア教育研究センター部門
吉田 朋彦

1. はじめに

広島大学情報メディア教育研究センターでは，学生，教職員 2 万人を超える構成員に対してアカウントを発行し，メールサービスをはじめとして種々の情報ネットワーク環境を提供している．また同時に 3 箇所の主要キャンパスを中心にすべての地区に学内 LAN を敷設し，運用している．

本学では，学生の履修登録から教員の出張処理にいたるまで，多くの手続きがオンラインで行われており，近年では各家庭にも高速なインターネット常時接続環境が普及してきたこともあいまって，家庭や出張先など，構成員は場所や時間を問わず，学内 LAN を利用する必要性に迫られてきている．しかし，このような手続きに関してはセキュリティ上の問題から，アクセスが学内に限定されているものがほとんどである．

このような問題に対応するため，本センターでは学外ネットワークに接続した状態でも広島大学の LAN との間に仮想プライベートネットワークを構築し学内にいるのと同等の利用環境を提供する「VPN サービス」を行っている．

本稿では，本学の学内 LAN の概要を解説するとともに，誰でも簡単に利用できる VPN サービスについて説明する．

2. HINET の構成

本学の主要キャンパスは，広島市内の 2 箇所と東広島市の 3 箇所に分かれており，両市は３０Km 以上離れている．この 3 キャンパス間に本学所有の専用光ファイバーを敷設し，3 地区間それぞれについて 1 Gbps の回線 2 本づつで接続している．

キャンパス内は，それぞれ 1 箇所に基幹 L3 スイッチを設置し，キャンパス内の主要な建屋に L2 スイッチを配置し，L３基幹スイッチから１Gbps の光ファイバーを敷設している．（図１）

キャンパス間については，国道２号線沿いにある，国土交通省の情報ボックスを借用し，専用光ファイバーケーブル（１００芯）を敷設してある．一部，広島市内については，（株）NTT 西日本所有の管路を借用している区間もある．（図２）

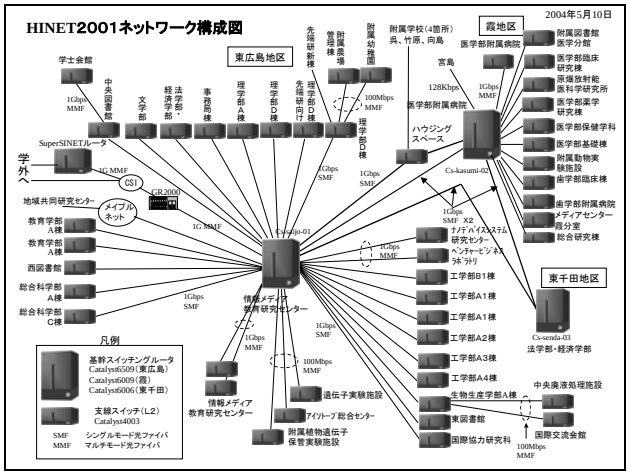
次に，学内ネットワークの論理構成についてであるが，本学では，133.41.0.0/16 のネットワークを利用しており，それを/24 でサブネット化して学内に配布している．学内の各サーバでは，このアドレスからのアクセスを学内と判別するのが一般的である．（図３）

３．学外からのアクセス

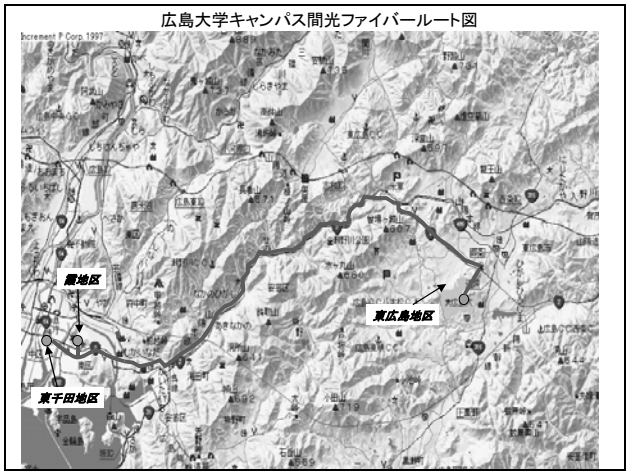
本センターでは，かねてより学外からのアクセス，とりわけ自宅からの利用については整備を進めてきており，ダイヤルアップサーバはもちろん，（株）NTT 西日本のフレッツ接続からも直接本学に接続できるようになっている．

ダイヤルアップやフレッツ接続であればクライアントに学内アドレスが割り当てられ，学内と同等の利用が可能になるが，逆に言えばその二つの方法に制限されることになり，好ましいとはいえない．

VPN サービスを利用すれば，基本的にインターネット接続環境さえあれば本学との間に仮想的なトンネリングが構築されるため，他の組織や一般プロバイダに接続した状態でも，本学の学内アドレスを割り当てることが可能になる．（図４，５）



（図１）



（図２）

広島大学のネットワークアドレス

- インターネットアドレス
  - IPアドレスでの通信（Ipv4）
- 133.41.0.0 /16 のネットワーク
  - 133.41.0.0 ～ 133.41.255.255 の範囲のIPアドレスが利用可能
- 133.41.0.0 /24 で利用
  - サブネット化
  - （例）133.41.10.0 ～ 133.41.10.255
- 学内からのアクセスかどうかの判断

（図３）

学外からのネットワーク利用

	利用できる場所	特徴	学内扱い
広島大学へダイアルアップ	どこでも 電話は必要	短時間の接続向け	○
広島大学へフレッツ接続	広島県内	家庭でじっくり NTT西との契約	○
上記以外 他の大学、ホテルのLAN YahooBB、その他プロバイダなど	いろいろあります	出先で便利	× VPNの利用で○

※メールだけなら、Webメール、携帯メールも便利

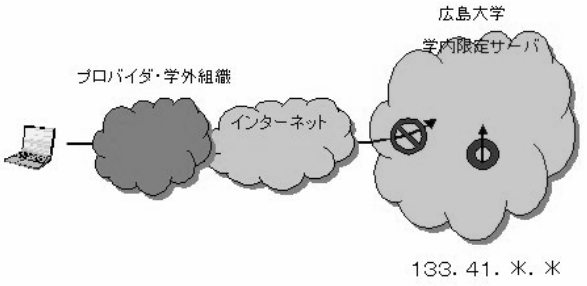
（図４）

VPNサービスとは？

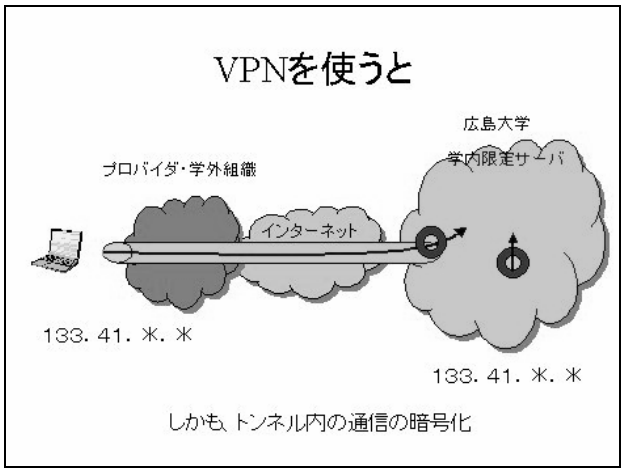
- 一般プロバイダや、他の組織につないだパソコンに「学内IP」を与える
  - 学内限定ページをみる
  - 大学のメールの送受信
    - もみじ
    - 電子ジャーナル（附属図書館・要確認）
    - メディアセンターのメールサービス
- 仮想的な、閉じた（大学の）、ネットワーク

（図５）

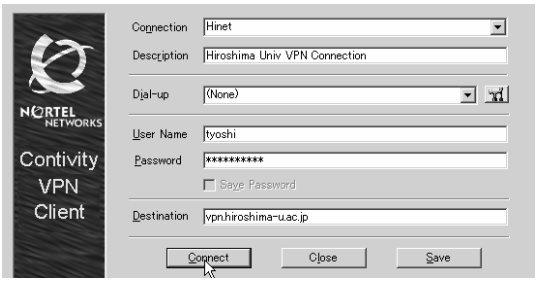
学外からのアクセス環境



（図６）



（図７）



（図８）

４．VPN の仕組み

VPN の概念について簡単に説明しておこう．学外の組織や一般プロバイダに接続したクライアントでは，当然のことであるが広島大学の IP アドレスが付与されず，そこから本学にアクセスすると学内からのアクセスとはみなされず，学内限定サーバの利用はできない．（図６）

そこで，クライアント PC に VPN ソフトをインストールし，対応する本学側の VPN サーバに接続し，仮想的なトンネルセッションを張ることにより，本学の IP アドレスが付与され，広島大学へアクセスする場合に限り，VPN セッションの通信路を利用する仕組みになっている．

同時に，この仮想通信路では Ipsec により通信が暗号化されるので，セキュリティ面でもある程度保障されることになる．（図７）

５．VPN サービスの利用方法と注意点

VPN サービスを利用するためには，利用するクライアント PC に VPN ソフトウエアをインストールする必要がある．

以下の情報メディア教育研究センターのサイトからダウンロードできるが，ダウンロードには本センターのアカウントとパスワードの認証が必要になっている．

http://www.media.hiroshima-u.ac.jp/

また，VPN セッションを確立する際にも，本センターのアカウントとパスワードの認証が必要になっている．

図８に VPN クライアントソフトの起動画面を示す

最後に，VPN サービスの利用上の注意点を挙げておく．

- ブロードバンドルータなどを介して NAT をしている場合
- ＠FreeD などのパケット通信型の PHS 接続

などの場合は注意が必要である．

前者の場合，デフォルトでは IPSec が通らないことが多いので，明示的に IPSec パススルーを設定する必要がある．

後者の場合，無通信で通信セッションを切断されていることがあるので，VPN も切れてしまい，再接続を要求されることがある．このような場合は通信を持続させるようなソフトウエアを別途作動させる必要があるが，通信帯域を圧迫しないような注意も必要になり，やや高度な使い方を強いられる．

６．まとめ

大学の重要な情報は学内限定アクセスになっていることが多い．しかしながら，家庭や出張先でもアクセスの必要性は生じる．

学外の組織や，家庭のプロバイダに接続した状態でも，広島大学の学内から利用しているのと同等の利用ができる VPN サービスは，セキュリティレベルも高く大学のユビキタスネットワークの拡充に非常に有効である．

接続している組織のネットワーク環境によって若干の制約はあるが，ぜひ有効に活用すべきサービスである．