インターネットからのキャンパスネットワークの安全なアクセス

2001MT088 千賀 健太郎
指導教員　後藤 邦夫

1　はじめに

現在、LAN 内のコンピュータをネットワークの外から安全に使用するための暗号化 VPN(Virtual Private Network) は企業や大学において必要不可欠なものに成りつつある．しかし VPN を使用することで利用が不便になるサービスが発生する，スループット低下，VPN 利用ユーザ管理などの新たな問題が発生する．本研究では暗号化 VPN を使用して大学ネットワークをインターネットから安全に利用するためのユーザ毎の利用サービス設定，アクセス制限とスループット測定をおこない，改良した VPN が大学での VPN 利用として有用であるという提案をする．

まず企業と大学での VPN 利用の特徴と大学で VPN を利用するユーザに対する制限事項をまとめる．そして自宅の端末や大学から貸与されたノート PC を用いて学外から大学ネットワークに VPN 接続する利用モデルとし，VPN ソフトウェアに OpenVPN[1] を使用する．

OpenVPN の問題点は VPN に必要な機能であるユーザ管理機能が実装されていないためにユーザ毎の利用サービス設定やアクセス制限が出来ないことである．これを解決するために OpenVPN ゲートウェイに利用者リストを用いたユーザ管理機能を追加し，上記の問題を解決する．また実際に大学において利用出来るか調べるためにさまざまなネットワーク環境で性能測定をおこなう．

2　学外からの安全な利用方法

一般的な大学での利用の特色として VPN 利用者は学生，教員，職員の 3 グループに分けられる．そして利用者，特に学生は卒業，休学，退学など異動が多いので年度途中での利用一時停止が出来るようにしたい．本研究では VPN から LAN を利用する際には利用頻度の高さやセキュリティを考慮し HTTP，HTTPS，HTTP PROXY，SMTP，POP3，SSH，FTP を各ユーザが利用すること，NAT によるグローバルアドレス変換は教員と職員のみに対してのみおこなうこと，各ユーザごとに決められたサーバのみ接続可能とすることを前提とする．これらを実現するために利用者リストをゲートウェイに実装して管理する．実現例として上記の 3 グループでアクセス制限を区別し，ユーザ名とユーザのグループを記載した利用者リストによりユーザ毎のアクセス権とユーザの VPN 利用の一時停止を実現する．

本研究で前提とする利用モデルは自宅の端末や貸与ノート PC を自宅等で使い VPN で大学内専用のホストにログインし，学内専用サービスを利用するものである．使用する暗号化トンネリングを選択するため IPsec，SSL-VPN[2]，SoftEther[3]，OpenVPN の特徴と長所，短所を比較し表 1 にまとめる．

表 1　各 VPN の長所、短所

IPsec	長所： ネットワーク層で動作するため TCP や UDP などの上位のプロトコルのアプリケーションを意識しなくてよい．IPv6 では標準. 短所：カーネルレベルでの実装なのでインストールが困難.
SSL-VPN	長所：さまざまな VPN ルータがあるので利用用途に合わせて選択できる. 短所：同時セッション数の多い VPN ルータ，大学などの利用者が多い場合のライセンス費用が高価である．TCP over TCP 問題がある.
SoftEther	長所：簡単に VPN を構築できる. 短所：事実上対応している OS は Windows のみ．TCP over TCP 問題がある.
OpenVPN	長所：NAT 使用環境でも問題無く使用できる．TLS 認証を用いた強力なクライアント管理が可能．ほとんどの OS にて動作可能. 短所：ユーザ管理機能が実装されていない.

IPsec はインストールが困難である．SSL-VPN や SoftEther は VPN 自体が TCP 上で動作する．その上に TCP を使うアプリケーションを通しパケットの損失やタイムアウトが起こると通信速度が極端に低下する TCP over TCP 問題が発生する．SoftEther の対応 OS は事実上 Windows のみである．OpenVPN には通信相手の情報を引き出す外部コマンド起動機能はあるが接続してきたクライアント管理機能は無い．また認証方法と暗号化方式について IPsec，SoftEther，OpenVPN を表 2 にまとめる．

表 2　認証，暗号化方式の比較

トンネリング	認証方式と方法	暗号化方式
IPsec	パケットに EPS でデータ付加し認証	IPsec
SoftEther	仮想 HUB でアカウントとパスワード認証	SSL
OpenVPN	無し	SSL

暗号化方式はどのトンネリングも同じような方式が使用でき，暗号の強度も十分である．また IPsec の ESP 認証はカーネル実装しないといけない，アカウントパスワード方式はパスワードが流出すると不正に利用される危険がある．

ソフトウェアのインストール，利用可能 OS，コスト，ユーザ管理機能等を比較した結果，OpenVPN にユーザ管理機能を追加したものが本研究の利用モデルと合致することから本研究では OpenVPN を採用した．

3　ユーザ管理機能の追加

OpenVPN にユーザ管理機能を追加してユーザ毎のサービスの設定やアクセス制限を可能にする．本研究では TLS 認証を使用するのでユーザの公開鍵中の common name にユーザごとに異なる値を設定し，それを OpenVPN ゲートウェイで抽出し利用者リストと比較することでユーザの管理機能を実現する．また利用者リ

ストに所属グループを記述することで各グループに許可されたサービス設定やアクセス制限を実現する．具体的には OpenVPN の外部コマンド起動オプションである tls-verify, client-connect, up を利用する．tls-verify では接続クライアントの common name と利用者リストを比較し接続の続行または拒否をする．client-connect では接続クライアントの VPN で使用する仮想 IP アドレスと common name を読み込み，クライアントがどのグループかを調べる．そして up で client-connect で読み込んだ仮想 IP アドレスと利用者リストから得たユーザグループを使い iptables によってサービス設定やアクセス制限をおこなう．上記のユーザ管理機能を実装した OpenVPN の処理の流れを図 1 に示す．

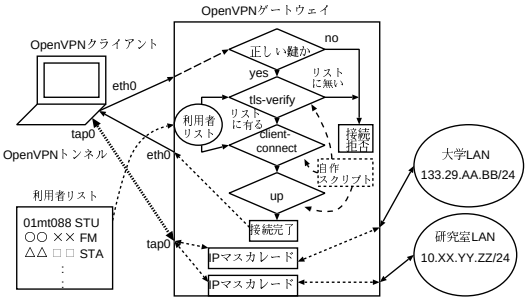

図 1　ユーザ管理機能付き OpenVPN の処理の流れ

図 1 のユーザ管理機能を実際に実験環境で実現でき，ユーザ管理機能の問題が解決出来たことで本研究の利用モデルに適したトンネリングが得られた．改良を加えた認証方式を利用することでカーネル実装しないといけない IPsec の ESP 認証やアカウントパスワード方式より簡単に高いセキュリティを確保できると言える．また登録ユーザリストを使用することで利用の一時停止が簡単におこなえることも本研究の成果である．

4　通信速度の測定

本研究で用いる OpenVPN が実際に大学ネットワークで使用出来るか調べるために通信速度の測定をした．測定はクライアントがサーバから FTP で圧縮の無いファイルをダウンロードし，ファイルサイズをダウンロード時間で割ってスループットを導く．実験で使用するネットワークは OpenVPN サーバに複数のクライアントをルータで接続したものを用いた．サーバの CPU は Intel Celeron500MHz，OS は Vine Linux 2.6r4，メモリは 128MBytes，カーネルは 2.4.22 を使用した．OpenVPN の LZO 圧縮使用時のスループットは使用しない場合の約 1.2 倍となったので実験は LZO 圧縮を有効にしておこなう．スループット測定は VPN 未使用状態，100BASE-TX 環境 VPN 使用状態，実験ネットワークに 10M ハブを繋いで 10BASE-T 環境とした VPN 使用状態での測定を 1 クライアントで，複数同時サーバ利用状態での測定を 2〜4 クライアントでおこなった．試行回数は複数同時利用は各ファイル 5 回その他は各 20 回で測定した．複数クライアントの実験結果は 1 クライアントあたりの平均値にクライアント数をかけた値である．実験結果の平均値をそのファイルサイズでのスループットとした．実験結果を図 2 に示す．

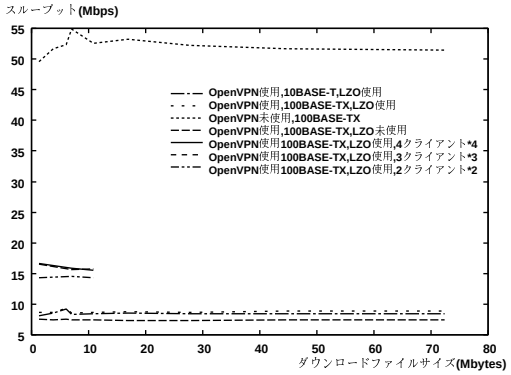

図 2　スループット測定結果

100Base-TX 環境の場合 OpenVPN を使用すると圧縮が有効でも 1 クライアントのスループットは OpenVPN を使用しない時のスループット 52Mbps を大きく下回り 8.8Mbps となった．しかしクライアント数を増やした実験での全クライアントの合計スループットは約 16Mbps となることや 10Base-T で実験でもほぼ同じ結果が得られたことから OpenVPN の処理速度がスループットの上限を決めると言える．結果よりサーバやクライアントの CPU の処理速度が速ければスループットも上がる可能性がある．

5　おわりに

本研究ではインターネットからの安全な LAN の利用法を考え，OpenVPN にユーザ管理機能を追加しユーザ毎のアクセス制限が出来るようにした．また様々なネットワーク環境での性能評価をおこない，サーバの CPU を性能の良いものにすれば本研究で提案したネットワークでの利用も可能だという結果が得られた．OpenVPN サーバの CPU を変えての性能評価や IPsec や SSL-VPN などの他のトンネリングと性能の比較が今後の課題である．

参考文献

[1] James Yonan：OpenVPN, http://openvpn.sourceforge.net/(2004)

[2] **鈴木淳也**：@IT トレンド解説 http://www.atmarkit.co.jp/fnetwork/trend/20030725/sslvpn.html(2003)

[3] **登大遊**：SoftEther.com, http://www.softether.com/jp/(2004)