多段のファイアウォールを越える PPP/PPTP 中継システムの実装と評価

齋藤彰一[†] 泉裕[††]
上原哲太郎[†] 國枝義敏[†]

VPN（Virtual Private Network）は，エクストラネットの構築のため，あるいはユーザがインターネットから安全にリモートシステムにアクセスするため広く用いられている．ある組織において，管理を部署ごとに分散させる必要から LAN 内にファイアウォールが階層的に構成される場合がある．このような場合，あるユーザが組織外から自分の所属部署にアクセスするには，複数の VPN ゲートウェイを経由する必要がある．しかし，一部のオペレーティングシステムに，同時に複数の VPN 接続を構成できないものがある．そこで我々は，単一の VPN 接続を用いて，複数の VPN ゲートウェイを介して目的の VPN サーバに接続可能な VPN 中継システムを提案する．本論文では，既存の VPN クライアントと VPN サーバにいっさいの変更を加えずに，PPTP を用いて中継システムを実現する方法について述べる．本システムの性能評価において，イーサネットによる 4 段中継の場合で，約 10 Mbps の転送性能を示した．

Implementation of Relaying PPP/PPTP Connection over Multi-step Firewalls and Its Evaluation

Shoichi Saito,[†] Yutaka Izumi,[††] Tetsutaro Uehara[†] and Yoshitoshi Kunieda[†]

VPN (Virtual Private Network) is commonly used to build extranets and to allow users to access from the Internet to remote systems securely. There are some organizations of which LAN is constructed with layered firewall systems to deploy the network administration to each division. In such organizations, when a member wants to access to his division's network from the outside of the organization, he needs to connect the VPN server via multiple VPN gateways. Unfortunately, there are some major operating systems which cannot establish multiple VPN connections at the same time. Therefore, we propose a VPN relay system which can connect a VPN server via multiple VPN gateways with single VPN connection. This paper describes an implementation of the VPN relay system using PPTP without any modifications to VPN client systems and VPN servers. According to the performance evaluation, when data were transfered via 4 VPN gateways, the system achieved a throughput of about 10 Mbps.

1. はじめに

VPN（Virtual Private Network）は，ある組織において離れた事業所を結ぶエクストラネットの構築や，利用者の組織外からのリモートアクセスにおける認証や通信の暗号化に用いられている．ある組織内で管理主体が部署単位などに分散されている場合，関係部署以外からのアクセスを制限するために，組織の LAN 内においても VPN が利用される場合がある．この場合の例を**図 1** に示す．このような組織においては，出張などで組織外から組織内の部署（たとえば研究部）にアクセスするには，組織全体の VPN ゲートウェイと部署（以降，セキュリティポリシーや運用ポリシーが同じ組織を **VPN ドメイン**という）の VPN ゲートウェイを経由する必要がある．しかし，一部のオペレーティングシステム（Operating System，以下 OS という）では，同時に複数の VPN 接続を構成できない．このため，管理者による VPN ゲートウェイの設置と運用に支障がでる場合がある．我々は，VPN ドメインが階層的に配置された組織向けに，複数の VPN ゲートウェイを介して目的の VPN ゲートウェイ（以下，**VPN サーバ**という）に接続可能な VPN 中継シ

† 和歌山大学システム工学部
Faculty of Systems Engineering, Wakayama University
†† 和歌山大学システム情報学センター
Center for Information Science, Wakayama University

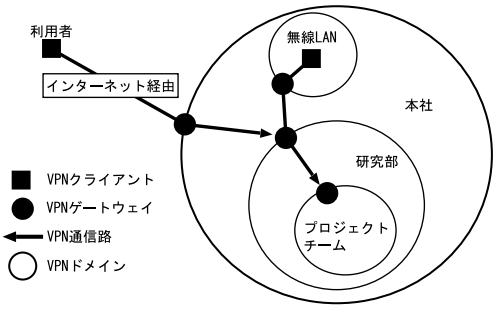

図 1 VPN ドメイン間の接続
Fig. 1 Inter VPN-domain connections.

ステムを提案する．本論文では，本中継システムを，既存の利用者端末（以下，**VPN クライアント**という）と VPN サーバにいっさいの変更を加えずに実現し，可能な限りのセキュリティを保証する方法について述べる．

本 VPN 中継システムは，最も利用者の多い OS である Windows に標準搭載されている VPN プロトコルである PPTP [1]の中継を実現する．VPN クライアントに新たなプログラムを導入したり，新規プロトコルを構築したりした場合には，一般の利用者の端末への導入に多くの時間と利用者サポートなどの人的コストを要すると考えられる．これらのコストを最小限にするためには，標準搭載されたプロトコルを基盤にし，VPN クライアントを変更しないことが必要である．

PPTP は，PPP [2]を IP 上で転送する通信路を実現するプロトコルである．利用者認証や暗号化などは PPP を用いて行うために，PPTP にはそれらの機能はない．本中継システムにおいても，利用者認証と通信の暗号化と IP アドレスの交渉などは PPP の機能を利用もしくは改良することで実現している．

しかし，本システムは VPN クライアントを変更しないことを第 1 目標としたため，本中継システムでは，VPN 通信路を中継する VPN ゲートウェイにおいて，管理者による盗聴となりすましが可能である．このため，各 VPN ゲートウェイの管理者を完全に信用できない組織は，本システムの対象とはならない．VPN ゲートウェイ管理者が信頼できるという前提の下，少数の VPN ゲートウェイの保守と少ない導入コストで，多数の利用者向けの VPN サービスを必要とする組織が本システムの対象である．

以下，2 章では，既存の VPN システムの概要について述べ，本システムにおいて採用する VPN プロトコルについて述べる．また，VPN 通信路の中継方式について検討する．3 章では，中継による多段 PPTP 通信路構築の実現方法について述べる．4 章で，Linux を用いた実装の詳細を示しその性能評価について述べ，本システムの有効性を示す．

表 1 VPN の実現方法
Table 1 Implementation method of VPN.

SSH	遠隔ログインやポート転送
Socks	代理サーバ
IPsec	ネットワーク層による実現．
PPTP	データリンク層による実現．PPP によって暗号化と認証が行われる．
L2TP	データリンク層による実現．IPsec によって暗号化が行われる．
MPLS	タグスイッチにより実現．専用線を使用するために暗号化機構が不要である．

2. 既存の VPN システムと中継方式

本章では，既存の VPN システムの特徴を述べて，本システムで利用する VPN プロトコルを検討する．さらに，これまでに提案されている VPN 通信路の中継方式を検討し，本システムで採用する中継方式を検討する．

2.1 既存の VPN システムの概要

既存の VPN システムには複数の実現方法がある．**表 1** にその特徴を示す．SSH [3]と Socks [4]は，トランスポート層より上位の層によって VPN 通信路を実現している．そのために，すべての IP パケットを転送するような利用には向いていない．さらに，多くの OS では標準実装されておらず，システムを別途導入する必要があるために，VPN 通信路を構築するためには利用される例は少ない．一方，IPsec [5]と PPTP と L2TP [6]は，ネットワーク層より下層で VPN 通信路を実現する．よって，利用者はその存在を意識する必要がない．これらは，Microsoft 社製の Windows に標準実装されているために利用者が多いと思われる．Windows で利用可能な VPN プロトコルとしては，Windows 98 および Millennium Edition では PPTP が，Windows 2000 および XP では PPTP に加えて L2TP と IPsec がある．また，携帯端末の OS である Pocket PC 2002 では PPTP の利用が可能である．PPTP は，これらの中では最も古くに制定されたプロトコルであり，各種 Windows のほかに Linux でも利用可能であることから利用者が多いといえる．最後の MPLS [7]は，各 IP パケットにタグを付けることによりその通信路を制御するものである．一般にルータ間で利用され，利用者の PC などから直接利用することはない．我々は，クライアントシステムの変更なしに VPN を利用するという本システムの目的を考慮し，利用者の数とその存在を意識する必要がない点から，

PPTP を VPN のプロトコルとする．

2.2 VPN 通信路の中継方式

階層的に配置された複数の VPN ドメインについて，その外部から内側の VPN ドメインに対して VPN 通信路を構築する方式について述べる．まず，ファイアウォールの設定で関係するパケットを通過させる方式との比較について述べる．次に，複数の VPN ゲートウェイを経由して多段の VPN 通信路を構成する方式について述べる．最後に，既存の中継方式との比較について述べる．

2.2.1 ファイアウォールの通過方式との比較

多段 VPN 通信路を構成する方式とファイアウォールにおいてパケットを通過させる方式との比較について述べる．たとえば図 1 の場合に，組織内の VPN ドメイン（たとえば研究部）に組織外から VPN 接続を確立するためには，2 つの方法がある．1 つ目の方法は，ファイアウォールの設定において VPN 接続で用いるプロトコルを通過可能にする方法である．2 つ目の方法は，目的の VPN ドメインに至るまでのすべての VPN ゲートウェイを経由する VPN 通信路を構築する方法である．1 つ目の方法の利点は，その設定や管理が容易なことである．また，VPN を多段構成にする必要がないことから，経路途中における利用者管理が不要な点である．しかし，欠点として，ファイアウォールの通過を許可するか否かの判断を，利用者ごとに行うことが難しいことがあげられる．このために，組織全体の VPN ドメインへの接続許可を持たなくても，組織内の VPN ドメインへの接続許可のみで，組織全体のファイアウォールを通過できることになる．したがって，この方法では，組織全体のネットワークを利用（通過を含む）する者をすべて認証することはできない．

一方，2 つ目の方法では，VPN ドメインごとに，VPN ドメインへの接続の可否の判断を利用者単位で行うことが可能である．さらに，VPN ゲートウェイの設定によって，VPN ドメイン外からの利用者に暗号化通信を強制することができることも，2 つ目の方法の利点である．

以上から，1 つ目の方法は，専用線を用いた組織間接続など，利用者個人の認証の必要がない場合に有効である．2 つ目の方法は，利用者個人による組織外や無線 LAN からのリモートアクセスに対して有効である．本中継システムはリモートアクセスを対象としていることから，2 つ目の方式が必要である．

2.2.2 多段 VPN 通信路の構成方式

複数の VPN ゲートウェイによる VPN 通信路の構成方式を，文献 9) では 3 種類に分類している☆（**図 2**, **図 3**, **図 4** 参照）．各方式の問題点を以下に示す．

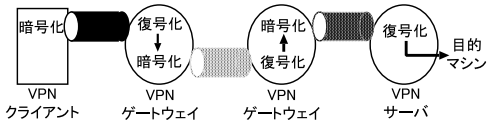

図 2 文献 9) による多段 VPN 通信路の構成（1）
Fig. 2 VPN link (1) in Ref. 9).

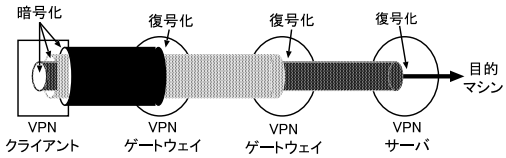

図 3 文献 9) による多段 VPN 通信路の構成（2）
Fig. 3 VPN link (2) in Ref. 9).

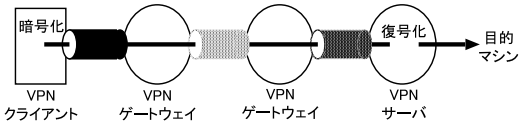

図 4 文献 9) による多段 VPN 通信路の構成（3）
Fig. 4 VPN link (3) in Ref. 9).

構成（1） VPN ゲートウェイにおいて復号化と暗号化が繰り返し行われる．復号後から再暗号化されるまでの間は，通信が平文で行われるため，VPN ゲートウェイの管理者に通信内容を盗聴される可能性がある．

構成（2） VPN クライアントが必要な暗号化をすべて行うために，VPN クライアントの負荷が大きくなる．また，パケットのカプセル化が入れ子構造になるために，一度にデータを運べるサイズが，1 回のカプセル化と比較して小さくなる．この結果，通信スループットが低下する場合がある．

構成（3） 通信路における認証と暗号化の区間が異なるために，既存のソフトウェアだけでは対応できない．

さらに，構成（1）と（2）に共通の問題点として，VPN ゲートウェイの数に比例して暗号化と復号化のオーバヘッドが増加する点がある．

構成（3）を PPTP に適用する場合には，各 VPN ゲートウェイ間に PPTP 通信路を構成し，それらを経由した PPP 通信路を構成する方式となる．しかし，利用者認証を PPP に依存する PPTP では，PPTP 通

☆ 文献 9) は，階層的なセキュリティドメイン（本論文でいう VPN ドメイン）における Socks ベースによる中継方式を示しているが，VPN リンク（本論文でいう VPN 通信路）の多段構成の方式は VPN 一般にいえる．

信路の構成の段階で利用者情報を得ることができない．したがって，PPTP のみでは，各 VPN ゲートウェイにおいて認証することができない．そのため，PPTP で構成（3）を実現するためには，PPTP に利用者情報と認証機構を付加する拡張が必要である．本システムでは，クライアントシステムを変更することなく中継を実現することが目的の 1 つであるので，PPTP を用いて構成（3）を実現することは不適当である．

構成（1）と（2）を比較すると，構成（2）は VPN クライアントによる暗号化の負荷が構成（1）より大きい．さらに，Windows 98 など複数の VPN 通信路を構成できない OS では，構成（2）を実現することができない．一方，構成（1）は，VPN クライアントを変更することなく使用でき，さらに，VPN クライアントの負荷が少ないといえる．しかし，構成（1）の問題点として，VPN ゲートウェイの管理者による盗聴の可能性がある．このために，構成（1）を採用するには，一般利用者のログイン制限などとともに，VPN ゲートウェイの管理者は「盗聴などを行わなず，また侵入などの不慮の事態を備えることができる，十分に信用に足る者であること」が必要条件となる．また，不正な侵入に対する予防策として，復号化と暗号化を 1 つのプロセス内で行うことが考えられる．いったんは復号化することから，完全なセキュリティを確保することはできないが，盗聴を困難にすることは可能である．なお，この機構の実現は今後の課題である．したがって,「完全なセキュリティを持たない VPN を利用者に使用させない」というポリシーを持つ組織は，構成（1）によるシステムを利用すべきではない．しかし,「小数の VPN ゲートウェイの保守と少ない導入コスト（新たなソフトウェアの導入なし）で，多数の一般利用者向けの VPN を実現する」ことを求める組織には，現実的な解決策を提供可能である．以上から，我々は，構成（1）を本システムの中継方式の構成とする．

2.2.3 既存の中継システムとの比較

文献 9) のシステムは，VPN クライアントからの既存の VPN プロトコルによる接続をプロトコル変換することで，SOCKS ベースの多段 VPN 通信路を実現した方式である．多段通信路の構成は構成（3）である．このシステムは SOCKS による中継で各段に仮想パスを構成し，VPN クライアントと VPN サーバ間に直接の VPN リンクを実現する．このために，中継ゲートウェイにおける盗聴はできない．これは，本論文のシステムと比較した場合の利点である．一方，本論文で提案するシステムと比較した場合の欠点には以下の項目がある．1) ソフトウェアの追加が必要である．このシステムでは，VPN クライアントとなるマシンにイニシエータという代理ゲートウェイを導入する必要がある．2) SOCKS によるサポートが必要である．このシステムのベースとなる SOCKS は，Windows 98 や Pocket PC において利用する PPTP に必要なプロトコルである GRE[10] をサポートしてない．したがって，PPTP を利用できないと思われる☆．3) 利用者ごとの中継先の指定ができない．このシステムでは VPN サーバの IP アドレスにより中継先を特定している．これには，すべての VPN サーバが異なる IP アドレスを持っているという前提が必要である．VPN サーバがプライベートアドレスを利用した場合は，この前提は一般に成立しない．本論文のシステムでは，利用者ごとに中継先を決定する方式を採用している（詳細は 3.2.1 項で述べる）．

3. 多段 PPP/PPTP 通信路

本章では，中継方式に構成（1）を用いて PPTP を中継する方法について詳細に述べる．まず，本中継システムを使用するために必要な準備と利用者登録について述べる．次に，PPP を利用した実現手順について述べる．

3.1 中継システムの準備

PPP/PPTP 通信路を中継するために必要となる機器は，中継用の VPN ゲートウェイ，クライアント接続用の VPN クライアントと VPN ドメインのファイアウォールとなる VPN サーバである．これらの中で，VPN クライアントと VPN サーバは，既存のシステムをそのまま利用可能である．特にネットワーク管理者が用意しなければならない機器は，VPN ゲートウェイである．VPN ゲートウェイは，中継を行うための改良が加えられたものが必要である．改良点については，3.3 節以降で述べる．なお，VPN ゲートウェイは VPN サーバとしての機能を有しているので，VPN ゲートウェイと VPN サーバを兼ねることが可能である．

VPN サーバ管理者は，VPN 接続に対して VPN クライアントと VPN サーバが使用する IP アドレスの組を発行できるようにシステムを設定する．これは，IP アドレスの交渉を容易にするための本システムの制限である．詳細は 3.3 節以降で述べる．

☆ 文献 9) ではプロトコル変換の詳細について述べられていないため，PPTP を中継可能か否かは不明である．しかし，SOCKS を用いることから，中継可能なプロトコルは SOCKS に依存すると思われる．

3.2 中継システムの利用者登録

3.2.1 中継先リスト

利用者は，事前に，中継に利用するVPNゲートウェイの**中継先リスト**に，利用者名とパスワードと，次段のVPNゲートウェイと利用者名とパスワードを登録する必要がある．これは，PPPによる暗号化のためにMSCHAP-v2[11]が必要であり，MSCHAP-v2を使用するためには事前に利用者名とパスワードの登録が必要なためである．この利用者名とパスワードは，直接接続するVPNゲートウェイ（とVPNサーバ）のみで利用するため，全VPNゲートウェイで統一する必要はない．直接接続する2台が共有することで十分である．また，1人の利用者が複数の中継先を利用する場合には，中継先ごとに次段のVPNゲートウェイと利用者名とパスワードを中継先リストに登録する必要がある．中継先の登録は，利用者ごとに利用可能なVPNゲートウェイが異なる場合があるためと，中継先を動的に決定することが困難なためである．なお，動的な経路制御やRADIUS[12),13)]などを利用した中継先の確定は今後の課題である．

多数の利用者が複数の中継先を登録する場合に，利用者名の決定方法，次段の利用者名の衝突，中継先リストの増大，登録業務などの管理コストの増加が問題となる．以下，これらの問題の解決方針について述べる．利用者名の決定方法は，中継用利用者名を「利用者名@識別子」として，利用者名の部分はVPNドメインに利用登録されている利用者名をそのまま利用する．これにより，中継用利用者名と実際の利用者の対応を容易にとれるようにする．利用者の登録業務については，SSLを用いたWWWによる登録ページを設けることで自動化が可能である．最後に，次段の利用者名の衝突と中継先リストの増大については今後の課題であるが，中継先VPNゲートウェイごとに中継先リストを設けることで衝突の回避と負荷分散を図ることが可能である．さらなる対策が必要な場合には，データベースシステムの活用を検討する必要がある．

3.2.2 利用者の認証方式

中継先リストへの事前登録によって，VPNゲートウェイの管理者は利用者のパスワードを容易に知ることができる．これを利用して利用者になりすまし，次段のVPNゲートウェイに接続することが可能となる．

この問題は2.2.2項で述べたVPNゲートウェイ管理者の条件に反する．しかし，不正侵入への予防策として以下の解決策が考えられ，本システムに実装する予定である．MSCHAP-v2によるパスワードは通信路確立にのみ使用し，実際にパケット転送を可能にするためには別の認証を行う方法である．たとえば文献14)で述べられている方式のように，各VPNゲートウェイにおいてWWWによる認証とパケット転送の可否を組み合わせることで，MSCHAP-v2とは異なる利用者情報（VPNゲートウェイ管理者以外が管理している利用者情報）による認証が可能である．この方式を本システムに適用する場合の手順を述べる．1) VPNクライアントとVPNサーバ間で接続を確立する．その際，各VPNゲートウェイにおいて次のaの経路設定を行わずに，bの経路設定を行う．1-a) PPP/PPTP通信路のためのポリシールーティングの設定（詳細は次節で述べる）を行わない．1-b) PPP/PPTP通信路から出力されるパケットは，自VPNゲートウェイのWWWサーバ向け以外を破棄する．2) WWWによる認証を実行し，その成功によりパケット破棄設定の解除とポリシールーティングの設定を行い，パケットの転送を可能とする．以上の手順により，VPNサーバからのIPアドレスの取得と，WWWによる認証前のパケット転送の禁止を両立することができる．この方式の利点は，VPNクライアントに新たなソフトウェアを追加することなく実現可能なことである．また欠点は，VPNサーバにも同様の設定が必要な点である．

3.3 中継方式

中継を行わない場合のPPP/PPTP通信路を**図5**に示す．これは，VPNサーバが接続してきたVPNクライアントに，アドレスを割り当てる様子を表した図である．これを，VPNクライアントとVPNサーバを変更せずに多段中継に変更した様子を**図6**に示す．VPNクライアントとVPNサーバは図5と同じだが，2台のVPNゲートウェイが挿入されている．ここでPPP/PPTP通信路を構成するためには，3つの

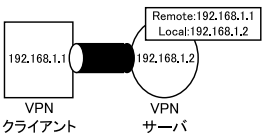

図5 中継のないPPP/PPTP通信路の構成
Fig. 5 VPN connection without relay.

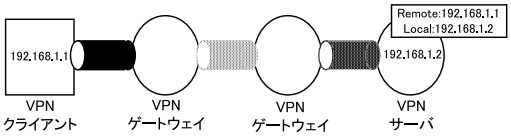

図6 多段VPN通信路の構成のイメージ
Fig. 6 Image of multi-step VPN connection.

問題がある．1つ目はクライアント側の IP アドレスを VPN クライアントに伝える方法，2つ目は各 VPN ゲートウェイ内で通信路間のパケットを交換する方法，3つ目は各 VPN ゲートウェイが使用する IP アドレスの決定方法である．以下，これらの問題点の解決策について述べる．

1つ目の問題点について，一般に PPP における IP アドレスは，PPP の中の IPCP[15]を用いて，VPN サーバと VPN クライアントの交渉によって決定される．VPN クライアントと VPN サーバのプログラムを変更しないためには，IPCP を用いて IP アドレスを VPN クライアントに伝える必要がある．本システムでは次の方法によってこの問題を解決した．VPN ゲートウェイは，VPN クライアントとして振る舞うことで VPN サーバと IPCP による交渉を行う．続いて，ここで得た IP アドレスの組（サーバ側とクライアント側）を用いて，今度は VPN サーバとして振る舞うことで VPN クライアントと IPCP による交渉を行う．これを，本当の VPN クライアントに到達するまで繰り返し実行する．以上により，1つ目の問題点を解決した．この方法の利点は，IPCP にいっさいの変更を加えず実現できることである．さらに，VPN ゲートウェイは，接続相手が本当の VPN サーバや VPN クライアントか，また VPN ゲートウェイかを意識する必要がない点である．

次に，2 つ目の問題点について述べる．一般に PPP/PPTP 通信路から入力したパケットは，宛先 IP アドレスに基づいて経路制御が行われる．その結果，適切なネットワークインタフェースより出力される．しかし，VPN ゲートウェイでは，一方の PPP/PPTP 通信路から入力されたパケットは，ペアとなる通信路にすべて出力されなければならない．本システムでは，これをポリシールーティングの機能を利用して解決した．本システムで用いるポリシールーティングは，VPN サーバ側と VPN クライアント側に生成されるインタフェースデバイス（Linux の場合 `ppp0` や `ppp1` に相当する）間のパケットを相互に通過させ，他のインタフェースデバイス（Linux の場合 `eth0` などに相当する）には入出力しないポリシーである．さらに，このポリシーは，他のインタフェースデバイスを用いて入出力されるパケットには影響を与えないように適用する．Linux の場合の設定例を**図 7** に示す．この設定は利用者や中継先に関係のない単一のポリシーであり，管理者が利用者や中継先ごとに個別に設定する必要はない．これにより PPP/PPTP 通信路のパケットを，他のパケットの経路制御に影響を与えることなく，

```
/sbin/ip route add default dev ppp1 table 1
/sbin/ip rule add dev ppp0 table 1
```

図 7 ポリシールーティングの設定例
Fig. 7 Exsample of policy routing.

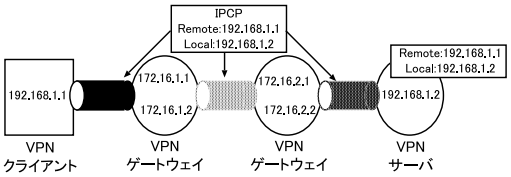

図 8 多段 PPP/PPTP 通信路の構成
Fig. 8 Multi-step VPN connection.

ペアとなる VPN サーバと VPN クライアント間で送受信することが可能となる．

最後に3つ目の問題点の解決策について述べる．各 VPN ゲートウェイにおける PPP/PPTP 通信路の IP アドレスは，他に存在しないユニークなアドレスを使用することで十分である．他で使用されている IP アドレスを与えた場合は，当然であるが，当該 IP アドレスに送られるパケットがすべてその VPN ゲートウェイによって処理されて目的のマシンに到達しない．一般にはプライベートアドレスを用いることができるが，組織内で当該プライベートアドレスを使用していないことを確認する必要がある．逆の視点から述べると，本方式による通信路は VPN ゲートウェイ以外の IP アドレスの影響を受けない．そのため，VPN 通信路の途中にある VPN ドメインにおいて使用されるプライベートアドレスが重なっていた場合にも，その影響を受けることなく多段通信路を構成することが可能である．これにより，本システムを利用するために，既存のネットワークの設定変更が必要ない．これは，本方式の利点といえる．以上の方法によって最終的に得られる PPP/PPTP 通信路の構成を**図 8** に示す．

3.4 実現の手順

3.4.1 接 続 手 順

PPP/PPTP 通信路の中継の接続手順を**図 9** に示す．以下に，接続手順の詳細について述べる．なお，図 9 と以下の説明は中継段数が 1 段の場合であるが，段数が増加した場合でも同一の方法で接続可能である．

(1) VPN クライアントは，最寄りの VPN ゲートウェイに接続要求し，PPTP 通信路を確立する．
(2) 確立した PPTP 通信路上で PPP による認証を行う．
(3) PPP 認証が成立した場合，VPN ゲートウェイは「利用者名に@を含むか否か」により，「当該

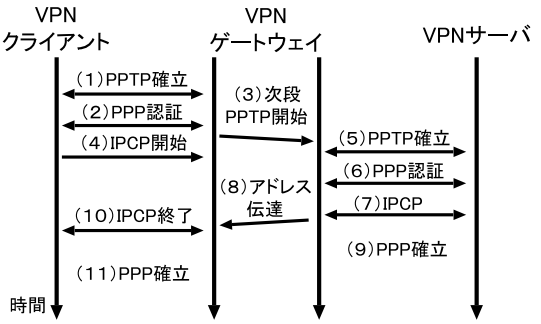

図 9 多段 PPP/PPTP 通信路の確立手順
Fig. 9 Process of setup multi-step PPP/PPTP connection.

利用者が中継を必要とするか否か」を判断する．中継が必要な場合は，次段の PPTP 通信路の構成を開始する．

(4) VPN クライアントは，認証後に IPCP により IP アドレスの交渉を開始する．しかし，接続先の VPN ゲートウェイは即座には応答しない．そのために，IPCP は応答待ちの状態となる．

(5) VPN ゲートウェイが接続要求した次段の PPTP 通信路が確立する．

(6) (2) と同様に，確立した PPTP 通信路上で PPP による認証を行う．

(7) 認証後，IPCP により IP アドレスを交渉する．この場合は，交渉相手が VPN サーバであることから，IPCP は待ち状態になることなく交渉が行われる．

(8) IPCP による交渉によって得た IP アドレスの組を，待ち状態にある初段の PPP/PPTP 通信路に送る．同時にポリシールーティングの設定を行う．

(9) 次段の PPP 通信路が確立し，通信が可能となる．

(10) 次段の IPCP から得た IP アドレスの組により，(4) で応答待ちになっていた初段の IPCP による交渉を行う．

(11) IPCP の交渉が終了後，PPP 通信路が確立して初段の通信が可能となる．これによって，VPN クライアントから VPN サーバに至る通信路が確立する．

3.4.2 切断手順

通常の切断処理は，OS もしくは PPP/PPTP の制御プロセスによって自動的に検知されて，当該 PPP/PPTP 通信路が VPN マシンから削除される．しかし，本システムは PPP/PPTP 通信路が多段構成となっていることから，ある PPP/PPTP 通信路が切断された場合には，関連するすべての PPP/PPTP 通信路を切断する必要がある．関連する PPP/PPTP 通信路を切断するために，VPN ゲートウェイでは，そのペアとなる PPP/PPTP 通信路を制御する PPP プロセスにシグナルを送り，実行を停止させる．PPP プロセスの停止は，PPP/PPTP の制御メッセージにより「通信路が切断した」として，さらにその接続相手に伝えられる．以降，VPN サーバと VPN クライアントに伝わるまで，連続的に PPP プロセスの停止と PPP/PPTP 通信路の切断が行われる．以上の手順により，PPP/PPTP 通信路の一カ所でも切断した場合，関連するすべての PPP/PPTP 通信路が OS または制御プロセスによって連鎖的に切断される．

4. 実装と評価

本章では，多段 PPTP/PPP 通信路の Linux における実装の詳細と，その性能評価について述べる．本システムの評価には，多段 PPP/PPTP 通信路におけるスループットとログインに要する時間を，中継段数とクライアント OS を変えて測定した．

4.1 実装方法

VPN ゲートウェイの実装には，Kondara[16] で使用されている PPP デーモンに MPPE パッチ[17] を適用したもの（以下，PPPD という）と，PPTP 通信路の構成に PoPToP[18] を PPTP のサーバとして，linux-pptp クライアント[17]（以下，PPTP クライアントという）をクライアントとして使用した．また，ポリシールーティングには，iproute2+tc[19] を使用した．

実装は，PPPD のソースプログラム中で IPCP を制御する `ipcp.c` に変更を加えることで行った．さらに，PPPD が実行する外部スクリプトとして，認証成功時に実行する `auth-up` と，IPCP 完了後に実行する `ip-up`，IPCP 切断後に実行する `ip-down` の 3 種類を作成した．

`ipcp.c` に加えた変更は大きく分けて 2 つである．1 つ目は，1 台の VPN ゲートウェイの中でペアとなる 2 つの PPPD 間で IP アドレスを伝達する手段である．これは，UNIX ドメインによる通信コードの追加により実現した．2 つ目は，PPP/PPTP 通信路のインタフェースアドレスを独自に設定するためのコードの追加である．これにより，VPN サーバから VPN クライアントに至るすべての VPN ゲートウェイに，VPN サーバが割り当てた IP アドレスの組を伝えることが可能となる．次に，各スクリプトの処理について述べる．`auth-up` スクリプトでは，次段の VPN ゲートウェイを中継先リストから検索し，PPTP クライアントを実行する．`ip-up` スクリプトでは，ペアとなる

表 2 実験環境
Table 2 Evaluate environment.

	VPN クライアント	VPN ゲートウェイ	VPN サーバ	FTP サーバ
CPU	Celeron 500 MHz	Pentium III 800 MHz	Celeron 700 MHz	Pentium III 1 GHz
Memory	256 MB	512 MB	384 MB	384 MB
Network	100BASE-TX IEEE–802.11b	100BASE-TX	100BASE-TX	100BASE-TX
OS	Windows 98SE Windows XP(Pro) Linux 2.4.4	Linux 2.4.4	Windows 2000 Server	Linux 2.4.4

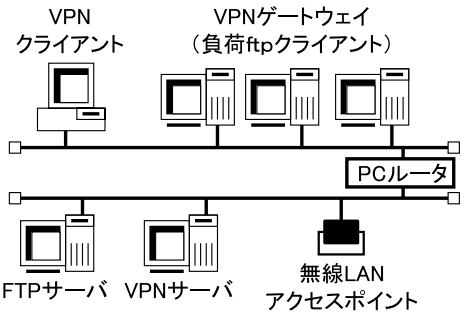

図 10 実験ネットワーク
Fig. 10 Network of evaluation.

PPP/PPTP 通信路へのポリシールーティングを設定する（図 7 参照）．`ip-down` スクリプトでは，`ip-up` スクリプトで設定したポリシールーティングの削除と，ペアとなる PPPD を終了させる．PPPD を終了させることで，PPP/PPTP 通信路がクローズ状態となり，連鎖的に各 VPN マシンの PPPD と PPTPD の実行を終了させることが可能である．以上により，PPP/PPTP 通信路の中継を可能とした．

4.2 性能評価

4.2.1 実験環境

実験環境を**図 10** に示す．また，各マシンのスペックを**表 2** に示す．実験内容は，多段接続に要する負荷を測定する意味から，次の 2 つとする．

- スループット
- ログインに要する時間

それぞれ，VPN クライアントの OS（3 種類）と中継の段数（中継なしから 4 段まで）を変更して測定する．なお，スループットではイーサネットと無線 LAN☆を用いて測定した．また，ログインに要する時間では他のトラフィックがない場合と ftp による負荷がある場合について測定した．

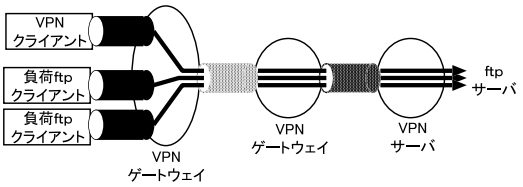

図 11 負荷を与えてのログイン実験
Fig. 11 Login evaluation with ftp-sessions.

スループットの測定は，通信路を構成後に FTP サーバから VPN クライアントにファイル☆☆を転送して行った．比較のために VPN を使用せずに直接接続した場合も測定した．スループットの値は，各 OS 付属の ftp コマンドの出力値を用いた．それぞれの OS で連続して 10 回の転送を行い，その平均値を求めた．また，実験環境における暗号化は，接続相手に関係なく MPPE[20]による暗号化を行うが，Windows 98SE と接続する場合のみ 40 ビットの MPPE を用い，それ以外の接続においては 128 ビットの MPPE を用いる．

ログインの所要時間は，Windows 98SE では接続のログから，Linux は syslog の出力結果から求めた．Windows XP は，クライアント側に接続のログを得ることができなかったために測定していない．それぞれの OS で 3 回のログインを行い，その平均値を求めた．また，他の PPP/PPTP 通信路のトラフィックがログイン時間に与える影響を調べた．負荷となる ftp 接続は，複数の ftp クライアントから，VPN クライアントが利用する VPN ゲートウェイと VPN サーバに 1 本または 2 本を接続した（**図 11** 参照）．なお，3.2.2 項で述べた WWW による VPN ゲートウェイごとの認証は行っていない．また，Windows98SE では「ネットワークへのログオン」を off に設定している．

4.2.2 実験結果

イーサネットによるスループットの測定結果を**表 3**

☆ アクセスポイントにエレコム社製 LD-WL11/AP を，無線 LAN カードにエレコム社製 LD-WL11/PCC をそれぞれ用いた．

☆☆ Linux のカーネルファイル（/boot/linuz-2.4.4-46k，884300 バイト）を用いた．

表 3 イーサネットによるスループット（Mbps）
Table 3 Through put by Ethernet (Mbps).

OS	VPN なし	中継なし	中継段数			
			1 段	2 段	3 段	4 段
98SE	11.10	1.40	1.54	1.53	1.52	–
XP	78.62	15.05	12.57	10.85	10.19	9.53
Linux	75.42	21.70	16.27	14.19	13.15	13.15

表 4 無線 LAN（IEEE 802.11b）によるスループット（Mbps）
Table 4 Through put by IEEE 802.11b (Mbps).

OS	VPN なし	中継なし	中継段数			
			1 段	2 段	3 段	4 段
98SE	1.28	1.50	1.52	1.50	1.40	–
XP	0.69	1.40	1.35	1.26	1.24	1.28

表 5 ログインの所用時間（秒）
Table 5 Process time for login (sec).

OS	負荷 ftp 接続数	中継なし	中継段数			
			1 段	2 段	3 段	4 段
98SE	0	3.1	9.2	13.3	17.1	–
	1 接続	3.1	5.3	8.4	11.6	14.7
	2 接続	3.1	5.3	8.7	11.3	14.7
Linux	0	6.0	10.3	14.6	18.3	20.6
	1 接続	6.6	7.0	9.3	12.0	15.3
	2 接続	6.3	6.3	10.0	12.3	15.6

に，無線 LAN によるスループットの測定結果を**表 4** に，ログインの所用時間の測定結果を**表 5** にそれぞれ示す．イーサネットによるスループットの測定結果から，Windows 98SE の結果が約 1.4 Mbps と低い値となった．他の OS と同一マシンによる測定であることから，Windows 98SE のネットワーク関係の実装に依存する結果と考えられる．一方，中継の影響による速度低下は現れていない．これは，約 1.4 Mbps という低いスループットのため，VPN ゲートウェイの処理能力で十分に復号化／暗号化が可能だったためと思われる．Windows XP と Linux の結果では，段数の増加によりスループットの低下が見られる．これは，10 Mbps 以上の転送速度により，VPN ゲートウェイの処理能力では十分な復号化と暗号化の速度が得られなかったためと考えられる．次に，無線 LAN によるスループットでは，約 1.0 Mbps から約 1.4 Mbps の結果となった．この結果でも，低いスループットのために中継による転送速度の低下は現れていない．イーサネットの場合の結果と異なり，Windows XP による結果が Windows 98SE による結果よりも低速であった．同一マシンによる測定であることから，無線 LAN のデバイスドライバによる影響と考えられる．また，VPN を利用した場合の結果が使用しない場合の結果よりも高速であったが，原因は不明である．これらの結果が示す値は，現在普及している無線 LAN や ADSL 環境では，実用上問題ない速度といえる．

他のトラフィックによる負荷がない場合のログインの所要時間の結果は，OS に関係なくほぼ同じ時間を要する結果となった．中継が 1 段増加するにつれて，約 4 秒の増加が見られる．Windows 98SE では，4 段の中継でのログインが，タイムアウトのためにできなかった．したがって，この実験結果では，Windows 98SE をクライアントとした場合は，中継段数は最大 3 段となる．Linux と Windows XP では 4 段でのログインも可能であった．これは，当然ながら，ログインタイムアウト値に依存する結果である☆．次に，ftp による負荷を与えた場合の結果は，負荷を与えない場合よりも短時間でログイン可能であった．これは，PPTP に定められている，2 台のマシン間の 1 つの接続で複数の PPP/PPTP 通信路を扱う call id と呼ばれる規格が有効に働いた結果である☆☆．call id により，新規の PPP/PPTP 通信路を開設する場合よりも，短時間で通信路を開設できたと考えられられる．また，負荷となる ftp の数を増やした場合でも，ログイン時間に変化は見られなかった．以上から，他のトラフィックがログイン時間に与える影響は少ないといえる．

5. おわりに

本論文では，VPN クライアントと VPN サーバにいっさいの変更を加えることなく，複数の VPN ゲートウェイを介した多段 PPP/PPTP 通信路を実現する方法について述べた．本システムにより，異なる運用ポリシーによる複数の VPN ドメインが運用されている場合でも，利用者は目的の VPN サーバに対して VPN 通信路を構築することが可能となった．問題点として，VPN ゲートウェイによるセキュリティの確保が完全でないことがあげられる．しかし，Windows 98 や Pocket PC などの複数の VPN 通信路を構成できない OS においても，VPN クライアントを変更することなく多段 VPN を構成できるようになった．本学においては，本システムを一般利用無線 LAN のゲートウェイとして設置する予定であり，現在利用者を限定しての運用を行っている．

今後の課題としては，VPN ゲートウェイ内のセキュリティの低下を防ぐさらなる方法の検討である．さら

☆ 当然ながら，インターネットを介した場合などは，この最大段数が小さくなる場合がある．

☆☆ 本実験で使用した PoPToP と linux-pptp クライアントは call id の扱いが不完全であったため，call id を扱うことができるように修正を加えた．

に，VPNゲートウェイの利用者のパスワード管理や，VPN通信路の動的経路の実現がある．

参考文献

1) Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and Zorn, G.: Point-to-Point Tunneling Protocol, RFC2637 (1999).
2) Simpson, W.: The Point-to-Point Protocol (PPP), RFC1661 (1994).
3) SSH Comunications Security. http://www.ssh.com/
4) Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D. and Jones, L.: SOCKS Protocol Version 5, RFC1928 (1996).
5) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC2401 (1998).
6) Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and Palter, B.: Layer Two Tunneling Protocol "L2TP", RFC2661 (1999).
7) Rosen, E., Viswanathan, A. and Callon, R.: Multiprotocol Label Switching Architecture, RFC3031 (2001).
8) Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.J. and Lear, E.: Address Allocation for Private Internets, RFC1918 (1996).
9) 岡山聖彦，山井成良，石橋勇人，安部広多，松浦敏雄：代理ゲートウェイを用いたSOCKSベースの階層化VPN構成法，情報処理学会論文誌，Vol.42, No.12, pp.2860–2868 (2001).
10) Hanks, S., Li, T., Farinacci, D. and Traina, P.: Generic Routing Encapsulation (GRE), RFC1701 (1994).
11) Zorn, G.: Microsoft PPP CHAP Extensions, Version 2, RFC2759 (2000).
12) Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC2865 (2000).
13) Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and Goyret, I.: RADIUS Attributes for Tunnel Protocol Support, RFC2868 (2000).
14) 渡辺義明，渡辺健次，江藤博文，只木進一：利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，Vol.42, No.12, pp.2802–2809 (2001).
15) McGregor, G.: The PPP Internet Protocol Control Protocol (IPCP), RFC1332 (1992).
16) Kondara Project: Kondara MNU/Linux Official Web Site. http://www.kondara.org/
17) PPTP Client Project. http://pptpclient.sourceforge.net/
18) Djamaludin, D.: Poptop—The PPTP Server for Linux. http://www.poptop.org/
19) Kuznetsov, A.. ftp://ftp.inr.ac.ru/ip-routing/
20) Pall, G. and Zorn, G.: Microsoft Point-To-Point Encryption (MPPE) Protocol, RFC3078 (2001).

(平成14年3月28日受付)
(平成14年9月 5 日採録)

齋藤 彰一（正会員）

1993年立命館大学理工学部情報工学科卒業．1995年同大学大学院博士前期課程修了．1998年同大学院博士後期課程単位習得満期退学．同年和歌山大学システム工学部情報通信システム学科助手，現在に至る．オペレーティングシステム，分散並列処理，インターネット等の研究に従事．博士（工学）．日本ソフトウェア科学会，ACM，IEEE-CS各会員．

泉 裕

1993年和歌山大学教育学部情報科学学科卒業．1995年奈良先端科学技術大学院大学博士前期課程修了．1998年同大学院大学博士後期課程単位習得満期退学．同年和歌山大学システム情報学センター助手，現在に至る．ネットワークアーキテクチャ，ネットワーク管理，インターネットセキュリティ等の研究に従事．修士（工学），ISOC会員．

上原哲太郎（正会員）

1990年京都大学工学部情報工学科卒業．1992年同大学大学院修士課程修了．1995年同大学院博士後期課程研究指導認定退学．同年同大学院工学研究科助手．1996年和歌山大学情報処理センター講師．1997年同大学システム情報学センター講師．2000年同大学システム工学部情報通信システム学科講師，現在に至る．自動並列化コンパイラ，分散並列処理，システム運用技術，インターネットセキュリティ等の研究に従事．京都大学博士（工学）．日本ソフトウェア科学会，CIEC各会員．

國枝　義敏（正会員）

1980 年京都大学工学部情報工学科卒業．1982 年同大学大学院修士課程修了．同年京都大学工学部情報工学科助手．1991 年同助教授．1996 年和歌山大学システム工学部情報通信システム学科教授，現在に至る．工学博士．主として，計算機ソフトウェア，システムプログラム，言語処理系，超高速計算等の分野に関する研究に従事．電子情報通信学会，ACM，IEEE-CS 各会員．