# 特定のユーザーだけが利用可能な仮想プライベートネットワーク

宇崎 央泰† 千葉 滋† 光来 健一††
†東京工業大学情報理工学研究科数理・計算科学専攻
††NTT 未来ねっと研究所

仮想プライベートネットワーク（VPN）は、二つのホスト間に仮想的な一本の回線を引くための技術といえる。この VPN を構築する場合、構築時にユーザー認証は行われるが、その後は認証が行われない。したがって、ホスト上にいるすべてのユーザーが VPN を利用できてしまう。複数のユーザーが存在するサーバーなどから VPN を構築した場合、他のユーザーが勝手に VPN 上のホストにアクセスできるため危険である。ユーザー専用の VPN を構築するために、我々は VPN にユーザーの概念を取り入れたパーソナル VPN を提案する。パーソナル VPN は、OS が VPN を利用するユーザーを制限することで実現する.

## 1 はじめに

盗聴や改ざんなどの危険などのあるパブリックなネットワークを経由した場合でも、暗号化などを利用し、通信を保護することにより専用線を仮想的に構築することができる。このような技術またはこの技術を用いて構築したネットワークを仮想プライベートネットワーク（Virtual Private Network：VPN）という。コストのかかる専用線を引いてプライベートネットワークを構築する代わりに、インターネットを経由した VPN を構築することで、安価にプライベートネットワークを構築することができる。また、インターネットを利用して構築するネットワークであるため、インターネットに接続できる環境にあればどこからでもプライベートネットワークが構築可能であり、柔軟性が高い。

しかし、VPN はホスト間に安全な回線を仮想的に作ることを目的としているので、ホスト上のどのユーザーが VPN を利用するかということは考えられていない。そのため、VPN を構築すると VPN のホスト上のどのユーザーもこの VPN を自由に利用できる。ホスト上のユーザーが常に一人である場合は問題ないが、複数のユーザーが同時に利用するサーバーなどから VPN を構築した場合、あるユーザーが構築した VPN を他のユーザーが勝手に利用し、VPN を構築しているホストにアクセスすることが考えられる（図 1)。

そこで、我々は、特定のユーザーだけが利用可能なパーソナル VPN を提案する。パーソナル VPN とは、VPN にユーザーの概念を取り入れ、OS によるアクセス制御を働かせることのできるようにした VPN である。通常、あるユーザーが計算機の資源を利用しようとする場合は OS によるアクセス制御が行われる。パーソナル VPN も資源の一つと考え、パーソナル VPN を利用しようとするユーザーは OS によるアクセス制御を受けるようする。

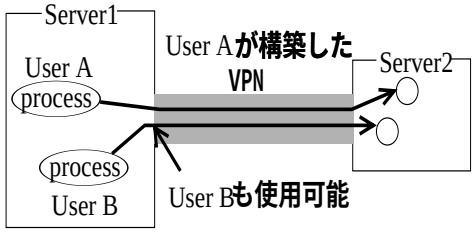


図 1: 他のユーザーが VPN を使用

## 2 パーソナル VPN

パーソナル VPN とは、ユーザーの概念を取り入れ、特定のユーザーだけが利用できるようにした VPN のことである。VPN を構築するときにユーザー認証を行うことができ、VPN を構築した後も、OS がこの VPN を利用しようとするユーザーの認証を行う。

パーソナル VPN は連結の機能を持つ。ゲートウェイなどの中継ホストでパーソナル VPN の連結を行うことで、ファイアーウォールなどのために直接通信できないホスト間にパーソナル VPN を構築することができる。

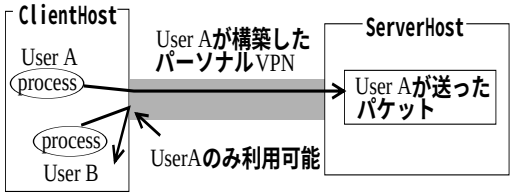


図 2: 特定ユーザーのみ利用可能

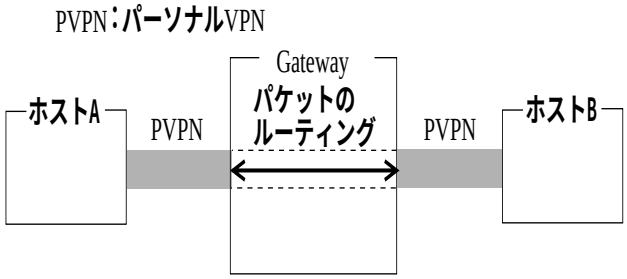


図 3: パーソナル VPN の連結

### 2.1 ユーザー認証

パーソナル VPN のユーザー認証には、パーソナル VPN 構築時に行うユーザー認証とパーソナル VPN 構築後に行うユーザー認証がある。

パーソナル VPN 構築時に行うユーザー認証は、サーバーホストがパーソナル VPN を構築しようとするユーザーの認証を行う。それ以後、サーバーホストの OS は、このパーソナル VPN を通ってくるパケットは認証したユーザーからのものであるとして扱う。認証したユーザーからのパケットとして扱ってよいことは、次のクライアントホストで行われるパーソナル VPN 利用時のユーザー認証により保証される（図 2)。

クライアントホストでは、パーソナル VPN を利用するユーザーを制限するため、パケットを送信したユーザーの UID を調べ、パケットの認証を行う。クライアントホストの OS は、パケットの送信を監視し、パーソナル VPN を構築したユーザーが送信したパケットはパーソナル VPN を通るようにする。こうすることで、パーソナル VPN を通ってくるパケットを送信したユーザーは、パーソナル VPN 構築時のユーザーであることが保証される。

パーソナル VPN を利用して行われる通信は、外部からの通信である場合が多い。パーソナル VPN の機能をもった OS では、パーソナル VPN を通しての通信には外部からの通信であるとして、認証したユーザーのもつ権限に何らかの制限（たとえば root 権限を持つことはできないようにするといったことなど）を加えることも可能である。

### 2.2 パーソナル VPN の連結

パーソナル VPN は、連結の機能を持つ。連結は直接通信できないホスト間にパーソナル VPN を構築するときに利用する。パーソナル VPN の連結は、連結を行うゲートウェイなどの中継ホストが、一方のパーソナル VPN を通ってきたパケットをもう一方のパーソナル VPN にルーティングすることで実現する (図 3)。

ゲートウェイにおけるファイアウォールやプライベート IP アドレスなどのために、パーソナル VPN を構築したいホスト同士が直接通信できない場合がある。NAPT（Network Address Port Translation）を使えば、プライベート IP アドレスをもつホストからグローバル IP を持つホストに対してコネクションを確立できるが、その逆は一般にはできない。互いのホストがグローバル IP アドレスを持っていても、ゲートウェイのファイアウォールでフィルタリングされると、通信できない。特定の IP アドレスは通過させるように設定すれば通信可能だが、その IP アドレスを持つホストからしか利用できなくなってしまう。

ゲートウェイなどの中継ホストの OS がパーソナル VPN に対応した OS ならば、中継ホストにパーソナル VPN の連結をしてもらうことで、直接通信できないホスト間にパーソナル VPN を構築することができる。

例えば、図 3 において、ホスト A のユーザーがホスト B との間にパーソナル VPN を構築しようとする場合、ホスト A はまず Gateway との間にパーソナル VPN を構築する。その後、Gateway がホスト B との間にパーソナル VPN を構築し、これら 2 つのパーソナル VPN 間のパケットのルーティングを行う。ここで、Gateway がホスト B との間にパーソナル VPN を構築しようとするとき、ホスト B はユーザー認証のネゴシエーションを Gateway に対して送ることになる。Gateway にホスト A のユーザーのプライベートキーを置いておけば Gateway が認証を行えるが、プライベートキーは、本人だけが所有すべきであると考える。そこで、ホスト B が Gateway に送るネゴシエーションをホスト A にフォワードし、

ホスト A で認証を行うようにする。

パーソナル VPN の連結を行った場合、実際には中継ホストの両端に 2 つの暗号化通信路が作成される。したがって、中継ホストは通信を解析できるのでログを取ったり、フィルタリングを行うことも可能である。しかし、中継ホストが復号化を行って解析を行う場合、負荷がかかり通信速度が低下する可能性がある。通信の解析をする必要がないときは、2 つの暗号化通信路で同じセッションキーを利用することで、中継ホストは復号化を行わずにルーティングを行うことも可能である（文献 [6] より引用）。

## 3 実装

我々は、パーソナル VPN を構築するために必要な機能の一部を Linux 上に実装した。実装した機能は、パケットを送信したユーザーを調べ、そのユーザーが VPN を作成したユーザーであった場合、パケットをその VPN に流すようにしたことである。

VPN の構築には、文献 [6] のカーネルレベル SSL を利用した。カーネルレベル SSL とは OpenSSL[4] を Linux カーネル内で動かせるようにしたものである。

### 3.1 パーソナル VPN の構築

パーソナル VPN を構築するホスト上にはパーソナル VPN を作成するサーバープロセスが動いており、ユーザーはこのプロセスにパーソナル VPN の構築を依頼する。依頼を受けたサーバープロセスは、SSL 暗号化通信路を作成する。このとき、サーバープロセスは set_tunnel_uid システムコールを呼び出し、この SSL 暗号化通信路を利用できるユーザーの UID を socket 構造体に書き込む。

パーソナル VPN 構築相手のホストが行うユーザー認証は、RSA ユーザー認証により行う。

### 3.2 パケットの認証

パケットが送信される前に、パケットを送信しようとするユーザーのチェックを行い、VPN に特定のユーザーのパケットを流すことができるようにした。

パケット自体にはユーザーの情報は含まれてないので、パケット送信ユーザーを調べるためにはパケットを作成した socket を所有するユーザーを調べる必要がある。これはパケットを管理する sk_buff 構造体から sock 構造体、socket 構造体、inode 構造体までたどり、inode 構造体のメンバ変数を調べることで行う。その後、パーソナル VPN を使用可能なユーザーかどうかチェックを行い、もし使用可能ユーザーであったらパケットのあて先アドレスをチェックし、どのパーソナル VPN に流すか、あるいはパーソナル VPN に流すべきパケットではないのかを決める。

これらの操作をすべてのパケットに対して行わなければならない。パケットの送信は大量に行われるので、ひとつのパケットにかける処理を減らしたい。このために、socket 構造体に次の 2 つを追加した。1 つはパーソナル VPN を通過させるパケットかどうかをチェックするための flag で、もう 1 つはパーソナル VPN へのポインタである。

flag が 0 ならば通常の送信を行い、1 ならばパーソナル VPN へのポインタを利用して、パケットをパーソナル VPN へ送るようにすることで、パケットの認証にかかるステップを減らすことができる。

## 4 実験

我々は、本稿で提案したパーソナル VPN の実装を考えるにあたり、まず予備実装として、カーネルの改変をせずにユーザレベルで実装をおこなった。本章では、この実装を使って測定したオーバヘッドを示す。

実験に使用したマシンは、クライアントマシンが Pentium 400MHz、Memory384MB、サーバーマシンが AthlonXP1800+、Memory640MB で、100Mbps のイーサネットで繋いだ。ベンチマークソフトは WebStone を使用した。

クライアントマシンからサーバーマシンの web サーバーにアクセスをしたときのスループットおよび平均レスポンスタイムを、以下の 3 つの場合について計測した。

1. クライアントマシンから直接サーバーマシンの web サーバーにアクセスする。
2. パーソナル VPN を通してアクセスする。ただしデータの暗号化は行わない。
3. パーソナル VPN を通してアクセスする。データの暗号化を行う。

WebStone が利用するファイルは、0byte、1Kbyte、10Kbyte、100Kbyte、1Mbyte の 5 種類のサイズのものを使用した。実験結果を表 1 と表 2 に示す。

データのサイズが小さいときには、通常の通信速度とくらべ数百倍のパフォーマンスの差がある。こ

表 1: スループット (Kbytes/sec)

| file size(KB) | 0 | 1 | 10 | 100 | 1,000 |
|---|---|---|---|---|---|
| normal | 170 | 710 | 3,200 | 8,400 | 8,500 |
| noencrypt | 1.5 | 6.1 | 260 | 650 | 820 |
| encrypt | 0.4 | 2.2 | 30 | 260 | 630 |

表 2: 平均レスポンスタイム (msec)

| file size(KB) | 0 | 1 | 10 | 100 | 1,000 |
|---|---|---|---|---|---|
| normal | 1.9 | 1.9 | 3.3 | 12 | 120 |
| noencrypt | 210 | 220 | 40 | 160 | 1,300 |
| encryptencrypt | 760 | 610 | 340 | 390 | 1,700 |

れはパケットの再送が頻繁に発生してしまったためである。データサイズを大きくとると、再送はほとんど発生しなくなった。その場合でも通常の通信速度と比べ、10 倍以上の差が出る。

予備実装の実験結果から、ユーザーレベルでパーソナル VPN を実装した場合、性能が非常に悪くなることがわかった。これは、パケットをアプリケーションとの間でやり取りするときのオーバーヘッドと、パケットの送信ユーザーを調べるのに proc ファイルシステムを利用したことによるオーバーヘッドが大きかったためと考える。

本稿では、パーソナル VPN の性能を改善するためにカーネルレベルで実装する方法を採用した。

## 5 関連研究

IPSec[3] では、暗号化、カプセル化の処理を IP レベルで行い、ホストごとにセキュリティを確保することを目的としている。IP レベルで暗号化、カプセル化を行うので、上位のアプリケーションはこれらのことを特別に意識する必要はない。VPN 構築時にユーザー認証を行うことができるが、その後、VPN はどのユーザーも利用できる。

データリンクレベルの VPN には、L2TP[2] や PPTP[1] などがある。これらは PPP プロトコルをベースとしており、ユーザー認証も PPP 認証によって行われるが、やはり VPN 構築後はどのユーザーも利用できてしまう。

より上位の層のプロトコルを利用する場合、たとえば SSL を利用した VPN では、クライアントとサーバーの間に VPN を構築できるが、アプリケーションが対応する必要があり、汎用的でない。

## 6 まめと今後の課題

本稿では仮想プライベートネットワークにユーザーの概念を取り入れたパーソナル VPN を提案した。OS がパーソナル VPN 利用ユーザーのチェックを行うことで、特定のユーザーだけが利用できるようにする。パーソナル PVN を連結することで、直接通信できないホスト間にパーソナル PVN を構築することができる。

我々は、パーソナル VPN の一部の機能を実装し、VPN を作成したユーザーが送信するパケットのみを VPN に流せるようにした。

今後の課題は、サーバーホスト側でのパケットの処理、パーソナル PVN の連結など、まだ実現できていない機能を実装することである。

### 参考文献

[1] amzeh, K. Pall, G. Verthein, W. Taarud, J. Little, W. and Zoron, G. Point-to-Point Tunneling Protocol(PPTP), Request For Comments2637(1999).

[2] ownsky, W. Valencia, A. Rubens, J. Pall, G. Zorn, G. and Palter, B. Layer 2 Tunneling Protocol "L2TP", Request For Comments(Standards Track)2661(1999).

[3] ent, S. and Atkinson, R. Security Architecture for the Internet Protocol, Request For Comments(Standards Track)2401(1998).

[4] roject,T.O.:OpenSSLProject,http://www.openssl.org/.

[5] Beck, M. Bohme, H. Dziadzka, M. Kunitz, U. and Verworner, D. Linux カーネルインターナル, ピアソンエデュケーション (1999).

[6] 光来健一, 千葉滋, インターネットにおけるパーソナルネットワークの構築. *SIG notes of Information Processing Sciety of Japan(2001-OS-88)*, pp. 83–90(2001).

[7] 廣津登志夫, 福田健介, 明石修, 佐藤孝治, 山崎憲一, 菅原俊治. 仮想データリンクを用いた多重通信クラスに関する一考察, 第 3 回インターネットテクノロジーワークショップ（WIT2000)(2000)

[8] 是友春樹, マルチメディア通信研究会. ポイント図解式 VPN/VLAN 教科書, アスキー出版局.