PU-M2006-0003

TinyVPN とブリッジ接続によるリモートアクセス方法

Version 1.8

シモウサ・システムズ

目次

はじめに（リモートアクセスとは）

この文書では TinyVPN と Windows のブリッジ接続機能を併用したリモートアクセス方法を説明します。

LAN と VPN を接続させるコンピュータでは Windows XP 以降の OS に付属するブリッジ接続機能が必要になりますのでご注意下さい。

TinyVPN の仮想 LAN と本物の LAN を Windows のブリッジ接続機能を用いて束ねることで、社内 LAN に対し、外出先からアクセスする事が可能になります。これにより、外出先からもノート PC 等を用いて社内 LAN 上にある他の PC を始め、プリンタ、ファイルサーバ、ネットワークカメラ等に自由にアクセス出来るようになります。

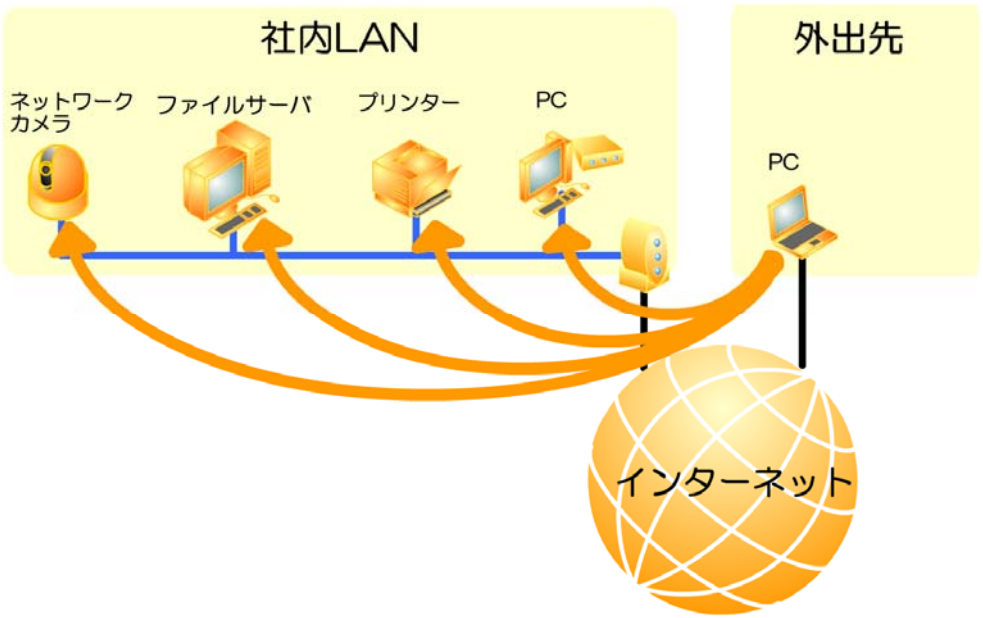

図1. 概要図

IP アドレスに関する注意点

TinyVPN とブリッジ接続機能を併用して外出先の PC から社内 LAN にアクセスする環境を構築する際に気を付けなければならないのは、外出先の PC には最終的に外出先環境用のネットワークアダプタと社内 LAN 用の仮想ネットワークアダプタという2つのネットワークアダプタが作成されるので、これらが同じ IP アドレス体系にならないようにしなければならない点です。

これは外出先 PC がモデム等を使って直接インターネットに接続されている場合は問題ありませんが、外出先 PC も何らかの LAN 環境上にあり、そのサイトのルータを経由している場合に注意が必要です。

例えば、社内 LAN の IP アドレスが 192.168.1.x で 外出先 LAN の IP アドレスも 192.168.1.x である場合、外出先 PC は自分が送信したい相手がどちらの LAN にいるのか分からなくなり、混乱してしまいます。

これを避ける為には社内 LAN もしくは外出先 LAN の IP アドレスを変更する事が望ましいですが、大掛かりな作業になる事から、この文書で説明する手段とは違う手段を検討する必要があります。

以下のページではリモートアクセス環境構築のための具体的な手順を説明します。

前提となる回線構成

まず、ここではリモートアクセス環境構築前の回線構成について説明します。

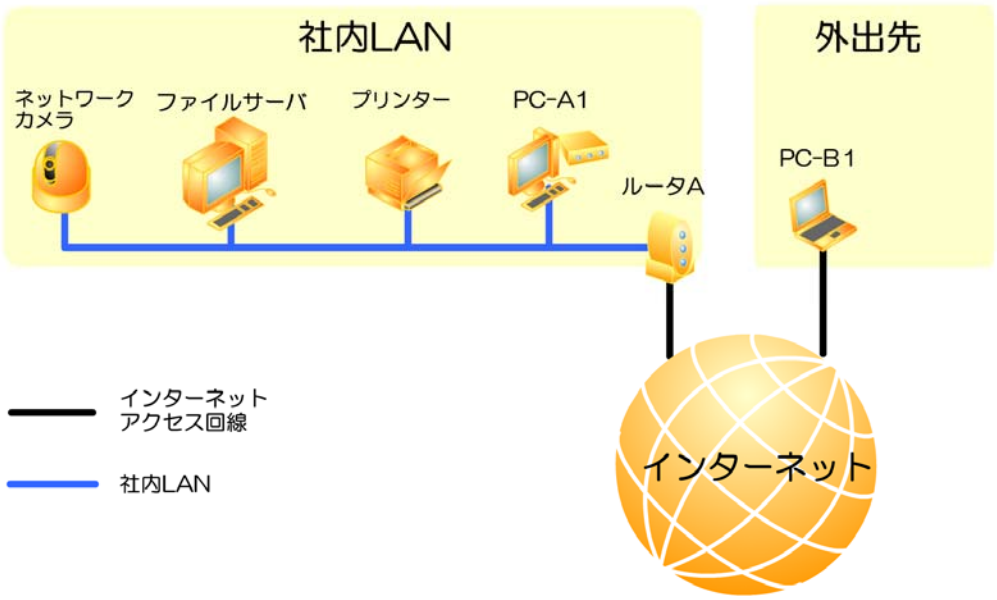

図2. 回線構成

社内には社内 LAN が敷かれており、そこには上図のとおり PC-A1やプリンタなど様々なネットワーク機器が接続されています。

一方で外出先の PC-B1は ADSL モデムにてインターネットに直接接続しています。(つまり、PC-B1はグローバル IP アドレスを持っています)

以下の事を計画しています。

1. 仮想ハブは PC-A1にて稼動させる
2. 仮想ネットワークアダプタは PC-A1、PC-B1にて稼動させる

以上から、TinyVPN をインストールするのは PC-A1と PC-B1の 2 台となります。

1. PC-A1 の仮想ハブ設定

社内 LAN の PC-A1に TinyVPN をインストールし、以下の設定で仮想ハブを1つ追加します。以下、説明上仮想ハブの待受ポート番号を 9999 とします。

[基本設定]
ハブ名称:これは任意に決定して下さい
待受ポート番号:9999
認証機能:ON
DHCP に関して:関与しない

[アカウント設定]
社内 LAN から接続する PC-A1 用と、外出先から接続する PC-B1 用の合計 2 つのアカウントを作成します。

2. PC-A1 の仮想ネットワークアダプタを仮想ハブに接続する

仮想ハブを設置した PC-A1 に、以下の設定で仮想ネットワークアダプタを1つ追加します。

[仮想ハブへの接続設定]
ホスト名もしくは IP アドレス: localhost
Port 番号: 9999
この仮想ハブは認証が必要: チェックする (仮想ハブで設定した通り、認証情報を設定する)

[暗号化設定]
通信を暗号化する: チェックする
暗号化キー: 任意の暗号化キーを設定する

[このネットワークアダプタの設定値]
IP アドレスを自動的に取得する: チェックしない
IP アドレス: 192.168.200.1
サブネットマスク: 255.255.255.0
デフォルトゲートウェイ: 設定しない (空欄のまま)

次の DNS サーバのアドレスを使う: チェックする
優先 DNS サーバ: 設定しない (空欄のまま)
代替 DNS サーバ: 設定しない (空欄のまま)

[ルーティング設定]
「なにもしない」を選択する

> ここでは仮想ネットワークアダプタに 192.168.200.1 という IP アドレスを割当てていますが、これはダミーとして設定するだけで、実際にはブリッジ接続設定をする時点で意味がなくなります。

3. PC-A1 のネットワークアダプタをブリッジ接続する

この時点で、PC-A1 には本物のネットワークアダプタと、TinyVPN の仮想ネットワークアダプタの2つが存在しています。

オフィス A 側の LAN のデータを仮想 LAN にも転送出来る様にするため、PC-A1 の2つのネットワークアダプタをブリッジ接続にします。

まず、「スタートメニュー」から「コントロールパネル」を開き、「ネットワークとインターネット接続」を選択します。
そして、「ネットワーク接続」というメニューを選ぶとネットワークアダプタの一覧画面が表示されます。

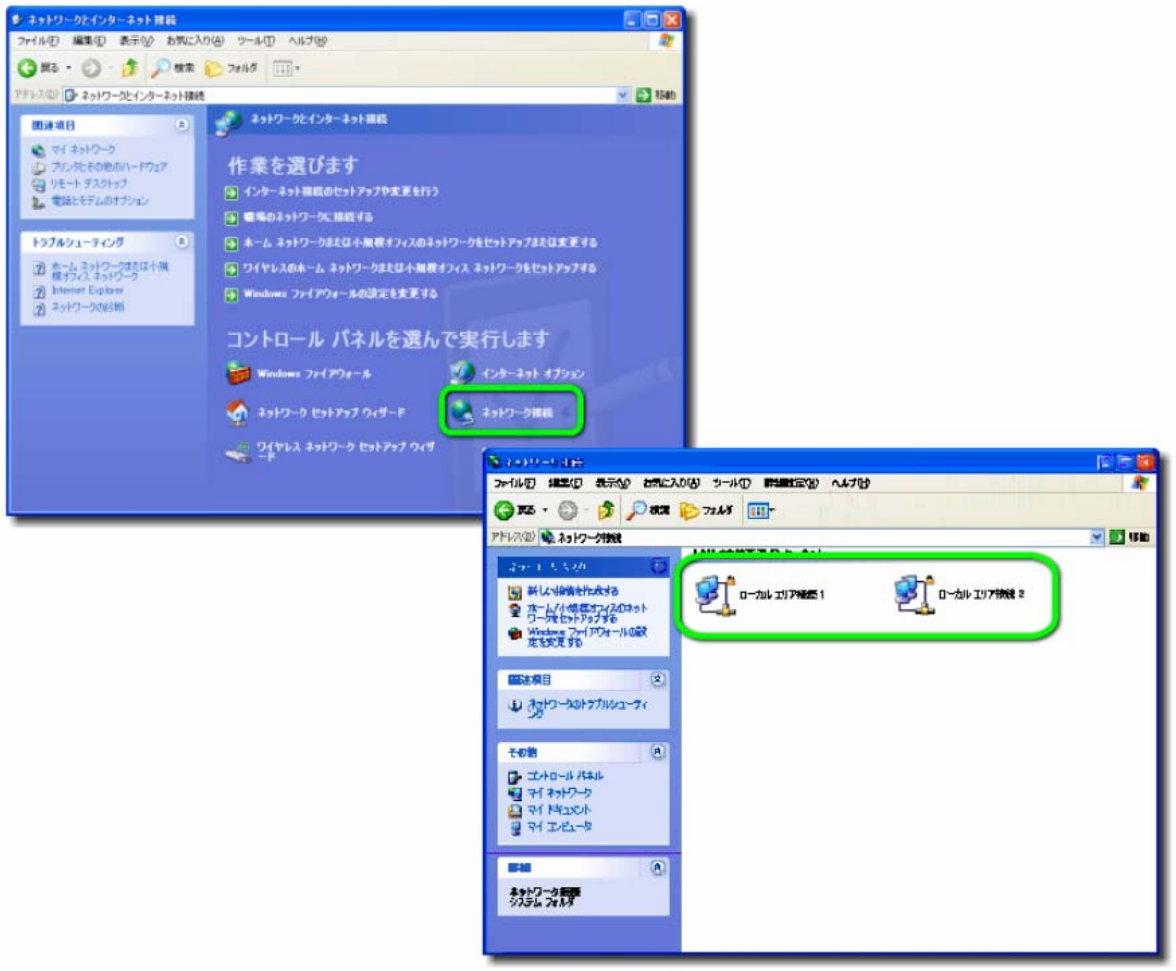

図3. ネットワークアダプタの一覧表示

そして、2つのネットワークアダプタを選択し、右クリックしてコンテキストメニューを表示させると「ブリッジ接続」という選択肢がありますので、これを選択します。

「Ctrl」を押しながら選択することで、複数選択することができます。

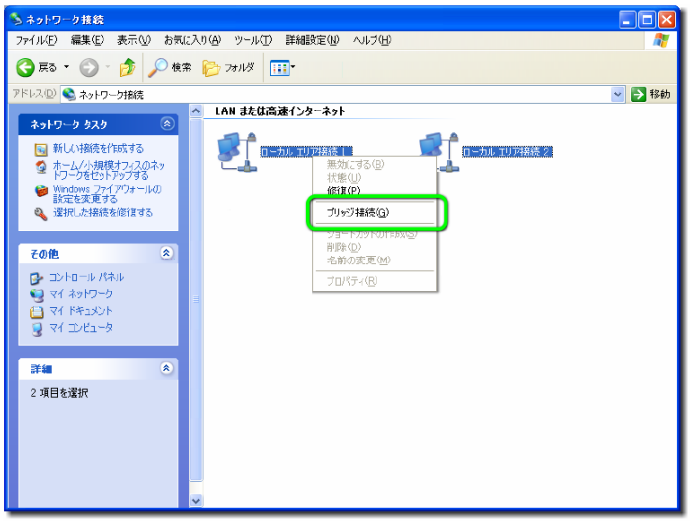

図4. ブリッジ接続の設定

これでブリッジ接続により、オフィス A の本物の LAN と仮想 LAN の相互接続が可能になります。

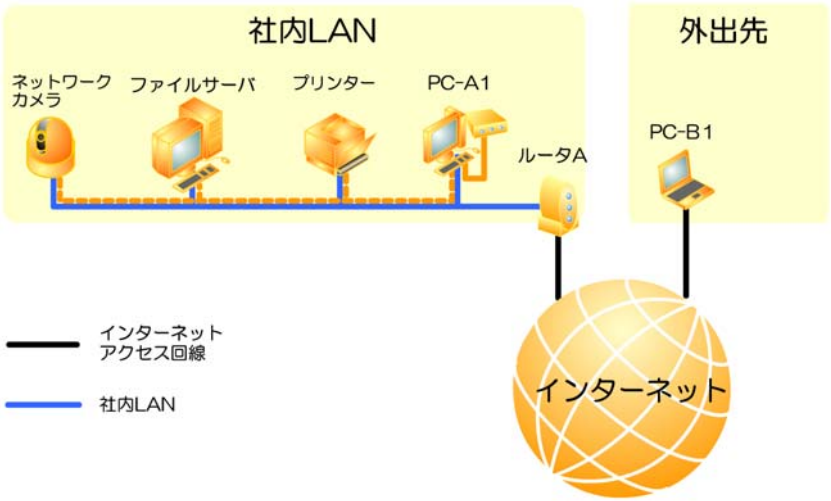

図5. オフィス A のブリッジ接続完成図

ブリッジ接続を設定すると、本物のネットワークアダプタと仮想ネットワークアダプタは「ネットワークブリッジ」という物の傘下に入り、以降はこの「ネットワークブリッジ」が IP アドレスを持ち通信を行います。 その為、この時点で PC-A1 を固定 IP アドレスとして再度設定する為に「ネットワークブリッジ」に対して以下の様に設定を施す必要があります。
（ブリッジ接続された後は「ネットワークブリッジ」の傘下にいるネットワークアダプタの IP アドレスは意味を持ちません）

[IP アドレス]	192.168.1.2 ～ 192.168.1.9 のうちのどれか
[サブネットマスク]	255.255.255.0
[デフォルトゲートウェイ]	192.168.1.1
[優先 DNS サーバ]	192.168.1.1
[代替 DNS サーバ]	<空欄のまま>

以上の設定でインターネット上のドメイン名がうまく解決できない場合は［優先 DNS サーバ］と［代替 DNS サーバ］を ISP が指定する IP アドレスに変更してください。

4. ルータ A の静的 NAT 設定

注意事項
PC-A1 の「ネットワークブリッジ」に割当てる IP アドレスは手動で設定してください。（固定 IP アドレスとする）
その際の設定値は以下の通りです。

[IP アドレス]	192.168.1.2 ～ 192.168.1.9 のうちのどれか
[サブネットマスク]	255.255.255.0
[デフォルトゲートウェイ]	192.168.1.1
[優先 DNS サーバ]	192.168.1.1
[代替 DNS サーバ]	<空欄のまま>

以上の設定でインターネット上のドメイン名がうまく解決できない場合は［優先 DNS サーバ］と［代替 DNS サーバ］を ISP が指定する IP アドレスに変更してください。

オフィス B からオフィス A の PC-A1 上で稼動する仮想ハブに接続するためには、オフィス A の入り口にあるルータ A に対して静的 NAT の設定をしなければなりません。この設定の名称はルータのメーカーにより様々ですが、例として以下の名称があります。

1. アドレス変換（BUFFALO）
2. 静的マスカレード（YAMAHA）
3. 静的 NAT（NEC）

概念としてはルータがインターネット側に1つしか持っていない IP アドレスに対して、別のサイトからパケットが届いた場合に LAN 側の特定の PC に転送する設定の事です。

ここでは、オフィス B からオフィス A に対して TCP ポート 9999 宛ての TCP パケットが届いた場合に PC-A1 の TCP ポート 9999 に転送する事が設定の趣旨です。

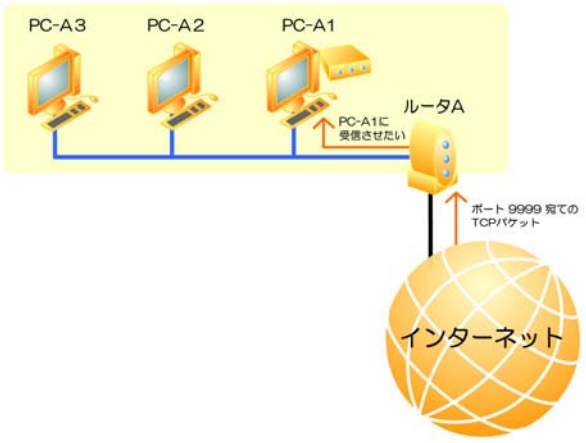

図6. 静的 NAT

TinyVPN2.8.6 以降の仮想ハブには「静的 NAT 設定機能」がついております。ルータが UPnP に対応した製品である場合、仮想ハブ管理パネルから簡単にルータの静的 NAT 設定ができるので便利です

5. PC-B1 の仮想ネットワークアダプタを仮想ハブに接続する

いよいよ、外出先にある PC-B1から社内 LAN にある仮想ハブに接続します。
まず。外出先の PC-B1に TinyVPN をインストールし、以下の設定で仮想ネットワークアダプタを1つ追加します。

[仮想ハブへの接続設定]
ホスト名もしくは IP アドレス: <社内 LAN のインターネット側アドレス>
Port 番号: 9999
この仮想ハブは認証が必要: チェックする (仮想ハブで設定した通り、認証情報を設定する)

[暗号化設定]
通信を暗号化する: チェックする
暗号化キー: PC-A1 と同じ暗号化キーを設定する

[このネットワークアダプタの設定値]
IP アドレスを自動的に取得する: チェックする
デフォルトゲートウェイ: 設定しない (空欄のまま)

次の DNS サーバのアドレスを使う: チェックする
優先 DNS サーバ: 設定しない (空欄のまま)
代替 DNS サーバ: 設定しない (空欄のまま)

[ルーティング設定]
「なにもしない」を選択する

※ルーティング設定の応用に関しては、別途「TinyVPN によるルーティング設定」をご参照ください。2010 年 7 月 27 日現在、
この文書は、下記 URL よりダウンロード可能となっております。

http://www.shimousa.com/tv/pdf/routing_with_tinyvpn.pdf

これで、外出先にある PC-B1 は社内 LAN に参加出来る様になります。
(PC-B1の仮想ネットワークアダプタには社内 LAN のルータ A から IP アドレスが振られます)

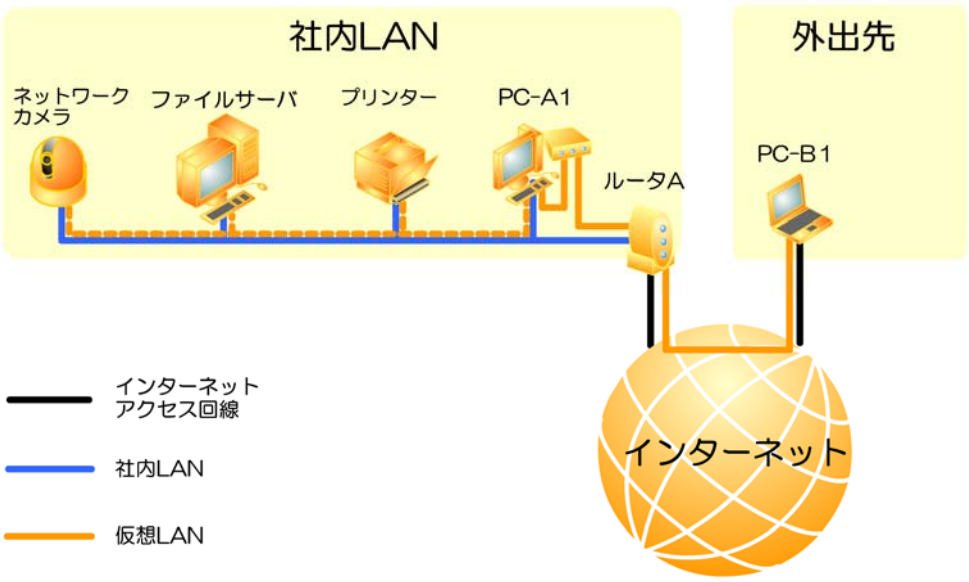

図7. リモートアクセス環境の完成

おわりに （リモートアクセスでの注意事項）

リモートアクセス環境の説明としてこの文書では外出先のインターネットアクセス回線を ADSL と仮定しました。
ADSL の場合、回線契約上、ほとんどのものがデータ量や接続時間に関係ない固定料金制のサービスですので、心配ありませんが、これがアナログ回線であったり、PHS、携帯電話を経由したサービスの場合の多くはデータ量や接続時間に比例した従量料金制のサービスですので、十分ご注意ください。