



PU-M2006-0004

TinyVPNとブリッジ接続機能による LAN の統合方法

Version 1.7

シモウサ・システムズ

目次

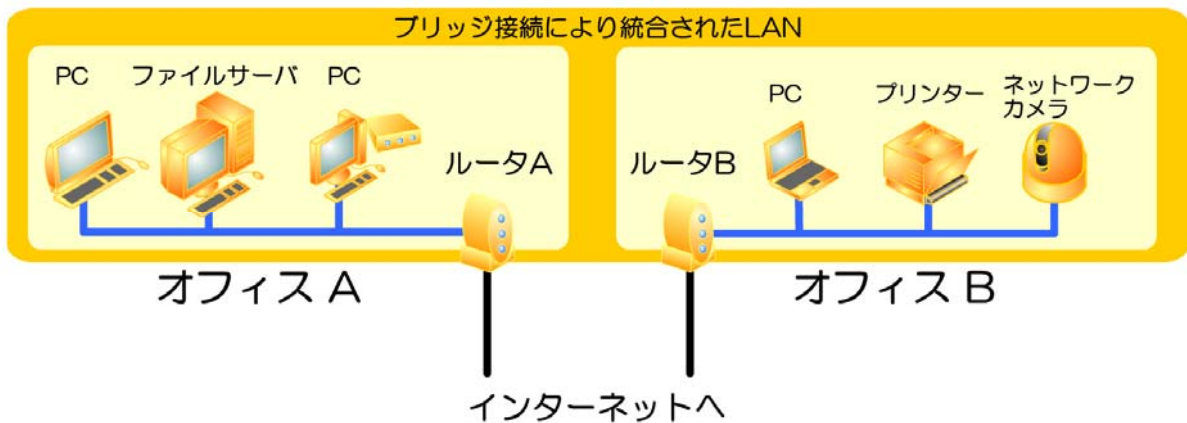
はじめに (LAN の統合とは)	3
1. オフィスA とオフィスB のIP アドレス見直し.....	4
2. ルータA のDHCP 設定	6
3. ルータB のDHCP 設定	6
4. PC-A1 の仮想ハブ設定.....	6
5. PC-A1 の仮想ネットワークアダプタを仮想ハブに接続する.....	7
6. ルータA の静的NAT設定	8
7. PC-B1 の仮想ネットワークアダプタを仮想ハブに接続する.....	9
8. PC-A1 のネットワークアダプタをブリッジ接続する.....	10
9. PC-B1のネットワークアダプタをブリッジ接続する	12
おわりに (統合されたLAN での注意事項).....	13

はじめに (LAN の統合とは)

この文書では TinyVPN と Windows のブリッジ接続機能を併用した LAN の統合方法を説明します。

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ください。

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、2箇所以上のオフィスにある LAN 同士をあたかも1つの LAN である様に統合する事が可能になります。これにより、仮想ネットワークアダプタを稼働させている PC 以外にも、プリンタ、ファイルサーバ、ネットワークカメラなども仮想 LAN を通じて通信する事が可能になります。



以下のページでは LAN を統合するための具体的な手順を説明します。

1. オフィスA とオフィスB のIP アドレス見直し

TinyVPN と Windows のブリッジ接続機能を利用して2つのオフィスの LAN を統合する場合、2つのオフィスは同じネットワークアドレスにて運用しなければなりません。

ネットワークアドレスとは1つの LAN セグメントで使用されている IP アドレスを表現するアドレス表記の事です。

電話番号のしくみを例にとると、「0312345678」という電話番号を見た際に私たちが考えるのは最初の「03」は東京の市外局番で、東京の場合市内局番は 4 桁なので市内局番が「1234」で回線番号が「5678」という事です。ただし、電話番号の場合は上記の番号を表記上「03-1234-5678」と表現するため、しくみを知らない人でもどれが局番でどれが回線番号なのか把握できます。

一方 IP アドレスは「xxx.xxx.xxx.xxx」と表記されるのですが、この中に実はネットワークアドレスとホストアドレスという2つの要素が組み込まれています。これは電話番号という市内局番と回線番号と同じような概念です。(市外局番は無いと考えると) しかし、ピリオドで区切って「192.168.1.1」等と表記されますが、これはネットワークアドレスとホストアドレスを区切っている訳ではありません。IP アドレスは 4 バイトの整数値である為、これを 1 バイトずつ 10 進法で表現し、それぞれをピリオドで区切って表記しているだけなのです。

LAN で通常使われるプライベート IP アドレスのうち、ネットワークアドレスとホストアドレスを分ける方法は原則的にアドレスの 1 バイト目(一番左)の番号の範囲によって以下の様に決まります。

< クラス A > 10.0.0.0 ~ 10.255.255.255 のアドレス

クラス A の場合、ネットワークアドレスは先頭 1 バイトで、ホストアドレスは残りの 3 バイトとなります。

クラス A では1つの LAN セグメントに最大で 16,581,373 台の端末が接続できます。

アドレス体系の例としては以下の様になります。

ネットワークアドレス	10.0.0.0
端末アドレス	10.0.0.1 ~ 10.255.255.254
ブロードキャストアドレス	10.255.255.255

(ホストアドレス部分が全て 0 の場合はネットワークアドレスを指し、全て 255 の場合はブロードキャストアドレスという全端末宛のアドレスを指します)

< クラス B > 172.16.0.0 ~ 172.31.255.255 のアドレス

クラス B の場合、ネットワークアドレスは先頭 2 バイトで、ホストアドレスは残りの 2 バイトとなります。

クラス B では1つの LAN セグメントに最大で 65,534 台の端末が接続できます。

アドレス体系の例としては以下の様になります。

ネットワークアドレス	172.16.0.0
端末アドレス	172.16.0.1 ~ 172.16.255.254
ブロードキャストアドレス	172.16.255.25

< クラス C > 192.168.0.0 ~ 192.168.255.255 のアドレス

クラス C の場合、ネットワークアドレスは先頭 3 バイトで、ホストアドレスは残りの 1 バイトとなります。

クラス C では1つの LAN セグメントに最大で 254 台の端末が接続できます。

アドレス体系の例としては以下の様になります。

ネットワークアドレス	192.168.0.0
端末アドレス	192.168.0.1 ~ 192.168.0.254
ブロードキャストアドレス	192.168.0.255

市販されている多くのルータでは DHCP サーバ機能のデフォルトとして、クラス C のアドレスを割当てる設定になっている物が多いのですが、TinyVPN を使って LAN セグメントを統合する場合には1つのネットワーク(LAN セグメント)に存在する端末数が増える事から、クラス C のアドレスでは端末台数に見合わなくなる事も想定されます。そういった場合はクラス B など、より多くの端末を接続できるアドレス体系にすると良いでしょう。

一方、万が一インターネット回線の切断・輻輳等の理由で VPN 回線が切断された際にも、それぞれのオフィス内での通信は行える様に考える必要があります。この為、下図の様なオフィス構成を考えた場合には以下のポイントを押さえる必要があります。

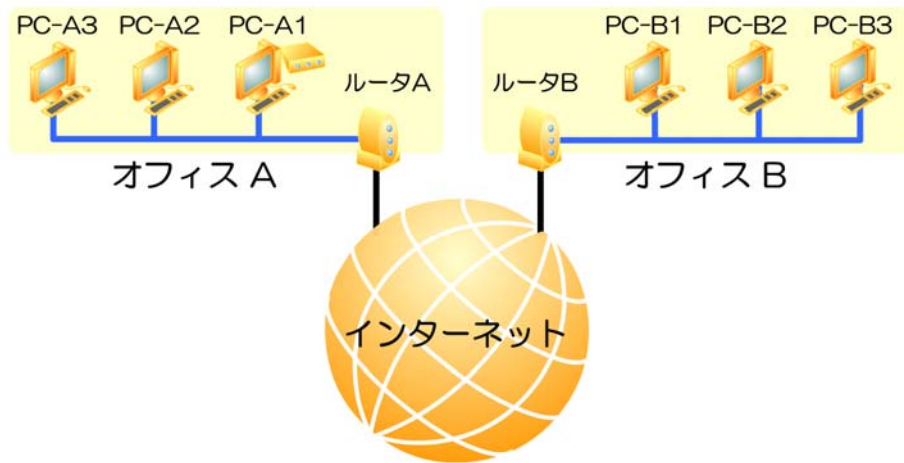


図1. オフィス構成図

1. ルータ A、ルータ B ともに DHCP サーバとして稼働させる
2. ルータ A とルータ B が同じ IP アドレスを割当てないように、それぞれの割当範囲を分けておく

例えばネットワークアドレスとして、192.168.1.0 (192.168.1.1 ~ 192.168.1.254) を使用する場合は以下のアドレス割当が良いでしょう。

ルータ A:

ルータ自身の IP アドレス: 192.168.1.1
DHCP 割当範囲: 192.168.1.10 ~ 192.168.1.127

ルータ B:

ルータ自身の IP アドレス: 192.168.1.128
DHCP 割当範囲: 192.168.1.137 ~ 192.168.1.254

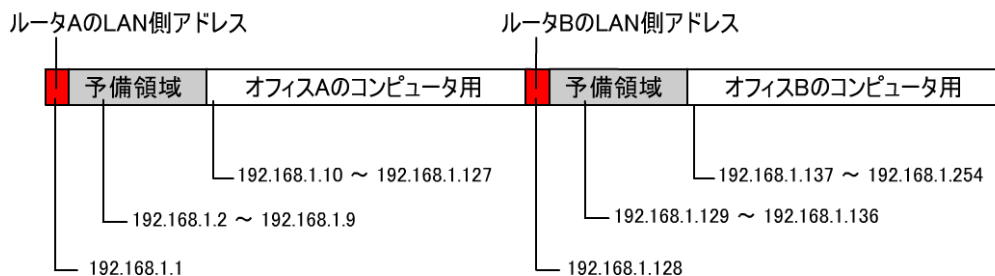


図 2. IP アドレスの割当範囲

(ここでの予備領域は固定 IP で運用したいサーバ・コンピュータ等の為に空けてある領域です)

なお、運用するコンピュータの数が 254 台を超えそうな場合はクラス A やクラス B の IP アドレスを割当てる様に設計すると良いでしょう。

2. ルータA のDHCP 設定

前項「オフィス A とオフィス B の IP アドレス見直し」にて設計した IP アドレスをクライアントに割り当てるためにオフィス A に設置されているルータ A の DHCP 設定を変更します。

細かい設定方法は各ルータ製品により異なりますので、ここでは説明を割愛します。

3. ルータB のDHCP 設定

前項「オフィス A とオフィス B の IP アドレス見直し」にて設計した IP アドレスをクライアントに割り当てるためにオフィス B に設置されているルータ B の DHCP 設定を変更します。

細かい設定方法は各ルータ製品により異なりますので、ここでは説明を割愛します。

4. PC-A1 の仮想ハブ設定

オフィス A 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:DHCP パケットをブロックする

[アカウント設定]

オフィス A から接続する PC-A1 用と、オフィス B 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。

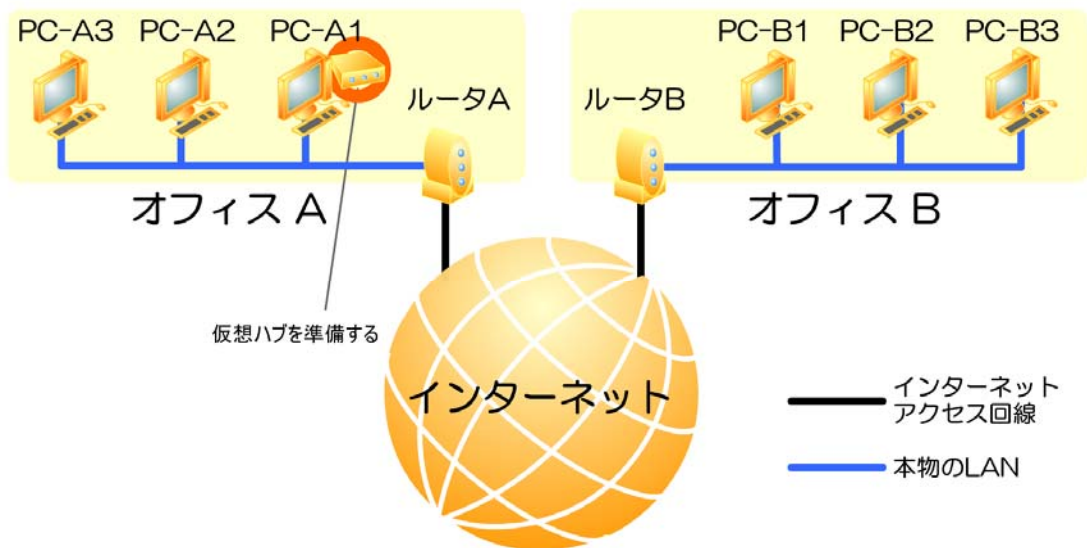


図3. 仮想ハブの準備

5. 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

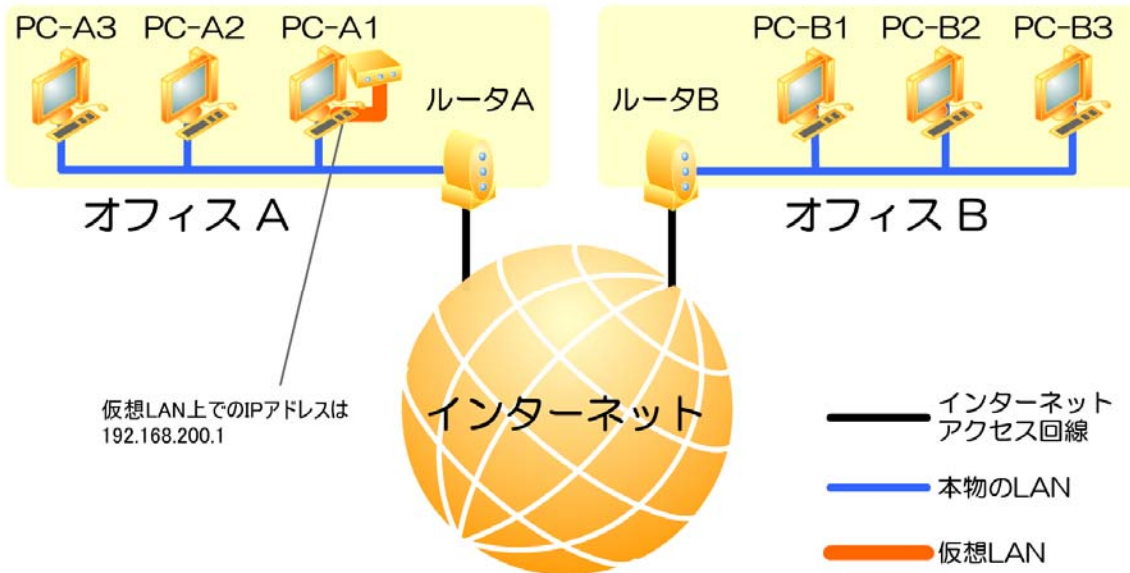


図4. PC-A1 の接続

6. ルータA の静的NAT設定

注意事項

PC-A1 の本物のネットワークアダプタに割り当てる 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。

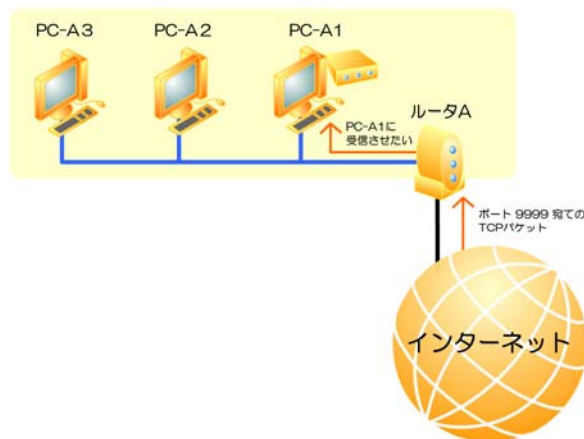


図5. 静的 NAT

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

7. 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、オフィス B にある PC-B1 からオフィス A にある仮想ハブに接続します。

まず、オフィス B 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: <オフィス A 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: チェックしない

IP アドレス: 192.168.200.2

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

これで、オフィス B の中にある PC-B1 はオフィス A の PC-A1 と仮想 LAN を通じて通信できるようになります。

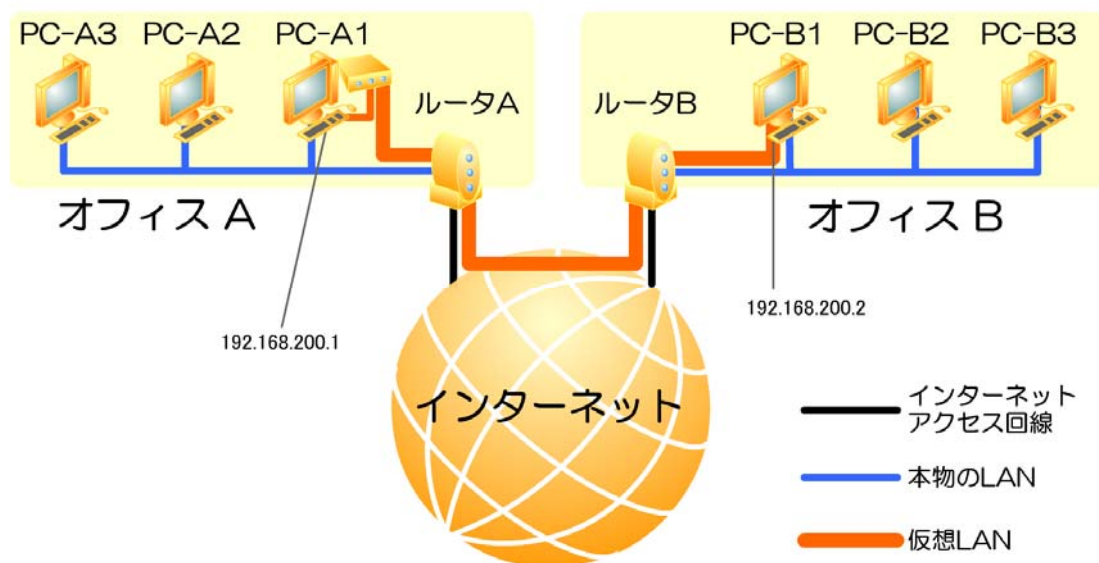


図6. PC-B1の接続

8. 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。

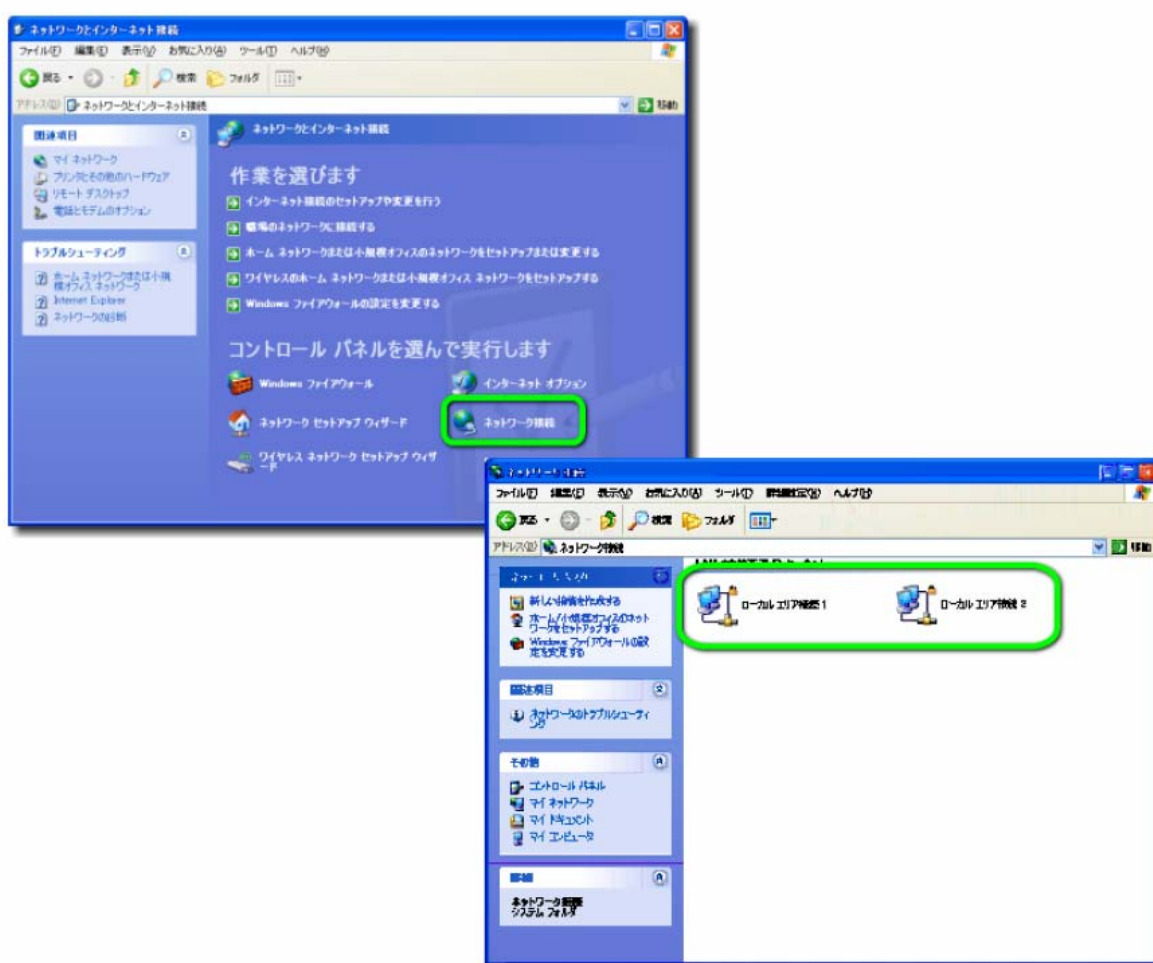


図7. ネットワークアダプタの一覧表示

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。

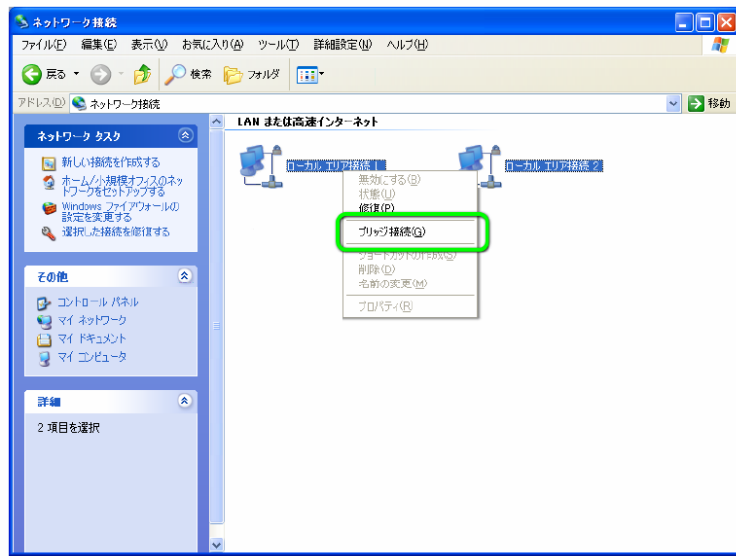


図8. ブリッジ接続の設定

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。

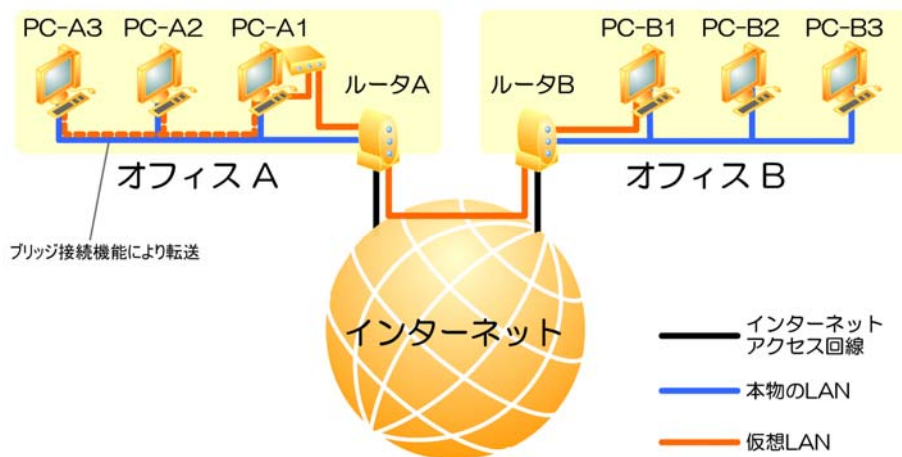


図9. オフィス A のブリッジ接続完成図

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。

9. PC-B1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-B1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 B 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-B1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。

細かい設定方法は「8. PC-A1 のネットワークアダプタをブリッジ接続する」で説明した方法と同じなのでここでは割愛します。

これで、2つのオフィスの LAN は1つの LAN セグメントとして統合されます。

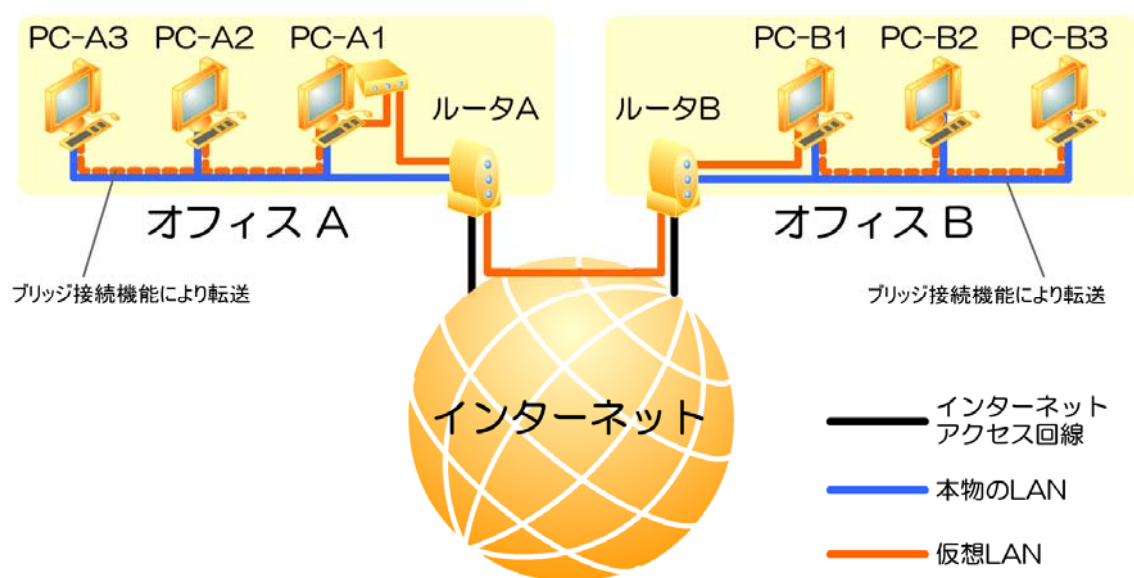


図10. 統合された LAN

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。その為、今まで仮想 LAN で使われていた 192.168.200.1 および 192.168.200.2 は意味がなくなります。

その代わりに、オフィス A やオフィス B で使われている 192.168.1.xxx の LAN に流れるデータは仮想 LAN を通じて相手方のオフィスの LAN に中継されるようになります。

おわりに（統合されたLAN での注意事項）

LAN が統合されるとオフィス A の PC とオフィス B の PC が自由に通信出来るようになりますが注意しなければならぬ事もいくつかあります。

ここでは統合された LAN を利用する際には以下の点にご注意ください。

1. 一つの LAN に DHCP が2台ある形であるため、稀に別のオフィスのルータからアドレスが振られる点
2. インターネット自体の接続が切れる等の障害発生時にお互いのオフィス間の通信も出来なくなる点
3. 仮想ハブや仮想ネットワークアダプタを停止させた場合はそれぞれのオフィス内だけの通信しか出来ない点