

BA8000 Pro  
静的IPマスカレード/マルチNAT  
設定ガイド

BA8000 Pro  
株式会社NTT-ME

はじめに

・本ガイドはBA8000 Proの静的IPマスカレードおよびマルチNAT機能の設定方法を説明したものです。

更新履歴

修正初版 2002 年 12 月 24 日

## BA8000 Proの静的フィルタIPマスカレード/マルチNAT機能について

### 1. グローバルIPアドレス1個のサービスを使用する場合:

通常のインターネット接続(Webサイトの閲覧等)ではLAN側のパソコンのWAN側への通信要求から通信が開始されるため、WAN側からの応答パケットに対しNAT/IPマスカレード(NAPT)により転送先ローカルIPアドレスを指定することができます。しかし以下のケースでは通信がWAN側から(BA8000 ProのWAN側ポートに設定したグローバルIPアドレスに対する通信要求として)開始されるため、BA8000 Proに静的IPマスカレードまたはマルチNATを設定し、転送先のローカルIPアドレスの指定を行う必要があります。

LAN側にインターネットに公開するサーバを設置する場合

ネットワークゲーム、コミュニケーション系のアプリケーション(チャット等)を使用する場合

静的IPマスカレードとマルチNATの動作の違いは以下の通りです。

#### 静的IPマスカレード機能:

BA8000 ProのWAN側IPアドレス宛に来る転送先LAN側ホストが不明なパケットのうち、特定のプロトコル/ポートのパケットをあらかじめ設定したローカルIPアドレスのホスト宛に転送する機能

#### マルチNAT機能:

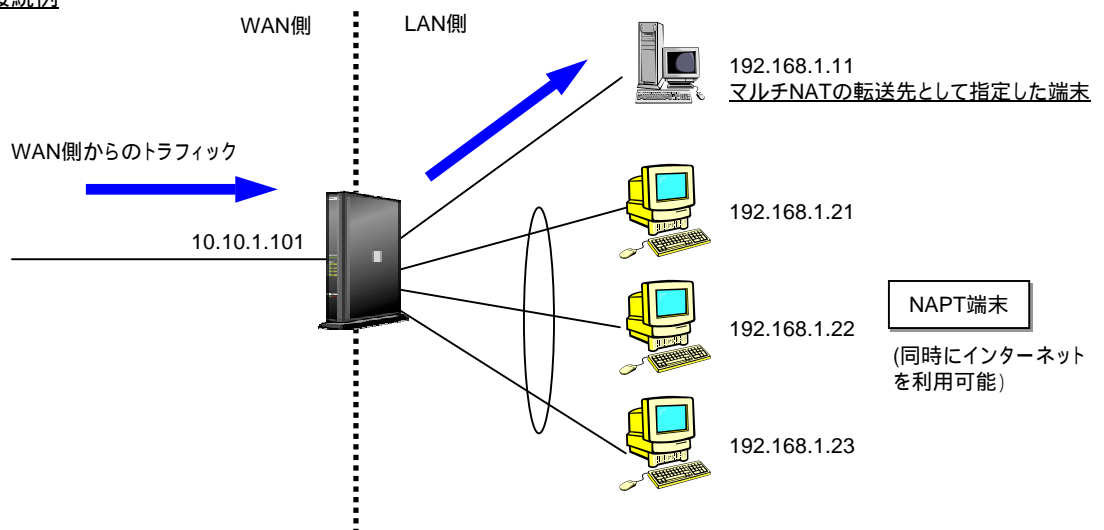
BA8000 ProのWAN側IPアドレス宛に来る転送先LAN側ホストが不明なすべてのパケットをあらかじめ設定したローカルIPアドレスのホスト宛に転送する機能

従って、アプリケーションで使用するプロトコル/ポートが不明な場合はとりあえずマルチNAT機能を使用して下さい。静的IPマスカレード機能を使用する場合はマルチNATを使用する場合と比較して以下のメリットがあります。

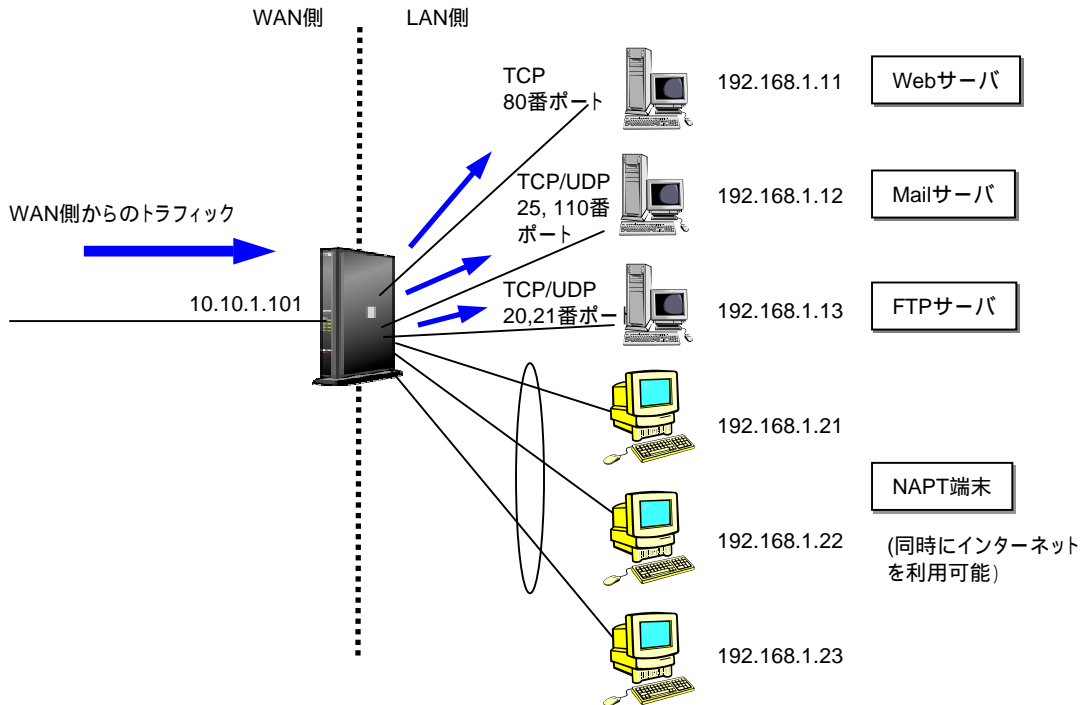
必要最小限のポートを開けることにより、マルチNATを使用する場合と比較してセキュリティレベルが向上します。

使用するポートごとに転送先ローカルIPアドレスを指定できるため、アプリケーションの異なる複数の端末/サーバを同時に使用可能です。

#### マルチNATによる接続例



## 静的IPマスカレードによる接続例



## 2. 複数のグローバルIPアドレス(LAN型PPPoE接続等)のサービスを使用する場合:

静的IPマスカレードとマルチNATの動作の違いは以下の通りです。

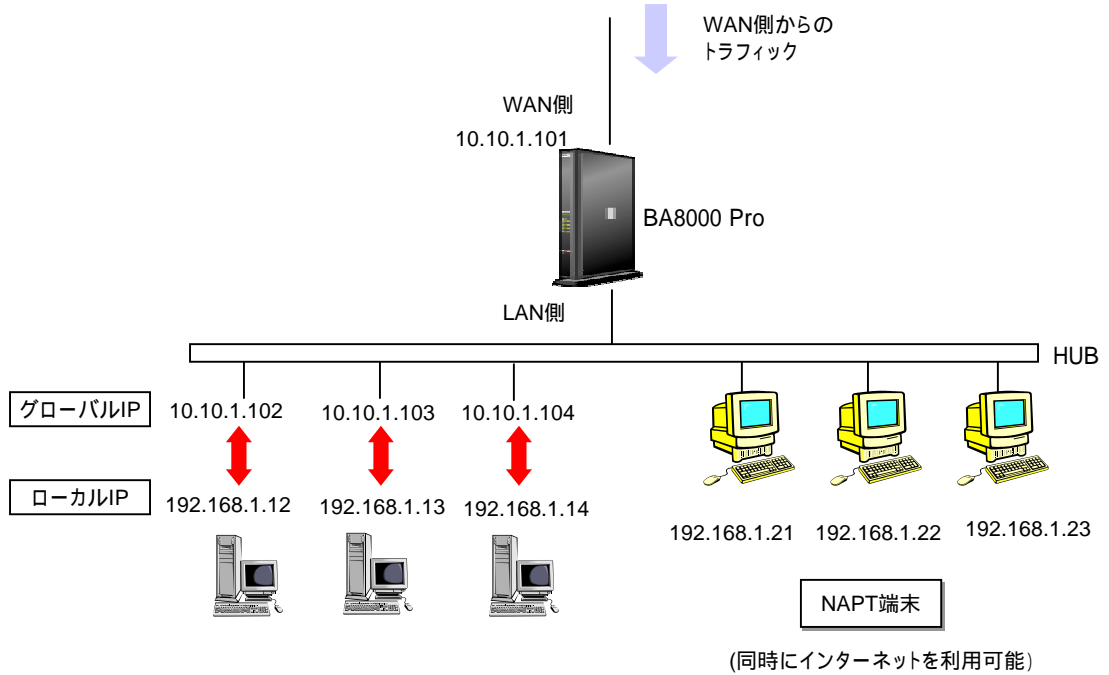
### 静的IPマスカレード:

BA8000 ProのWAN側IPアドレス以外のグローバルIPアドレス宛に来る特定のIPアドレス/プロトコル/ポート宛のパケットをあらかじめ設定したローカルIPアドレスのホスト宛に転送する機能です。また、BA8000 ProのWAN側に設定したグローバルIPアドレス宛に来る転送先LAN側ホストが不明なパケットのうち、特定のプロトコル/ポートのパケットをあらかじめ設定したローカルIPアドレスのホスト宛に転送することも可能です。

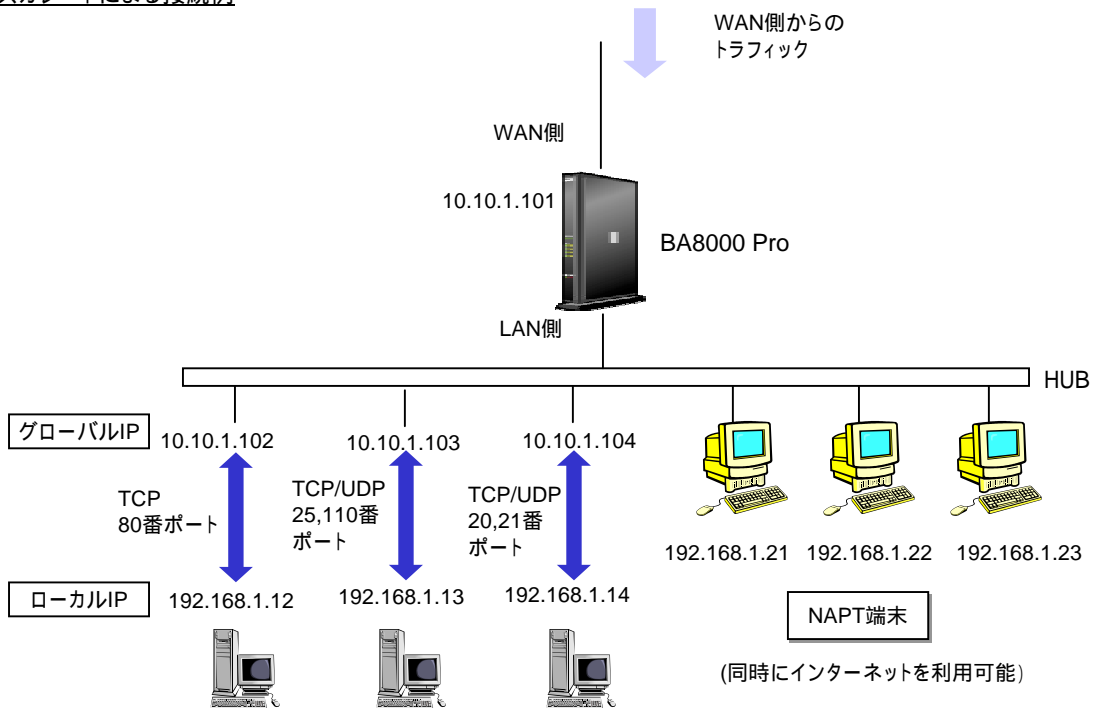
### マルチNAT:

BA8000 ProのWAN側IPアドレス以外のグローバルIPアドレス宛に来るパケットをあらかじめ設定したローカルIPアドレスのホスト宛に転送する機能です。また、BA8000 ProのWAN側に設定したグローバルIPアドレス宛に来る転送先LAN側ホストが不明なパケットをあらかじめ設定したローカルIPアドレスのホスト宛に転送することも可能です。

マルチNATによる接続例

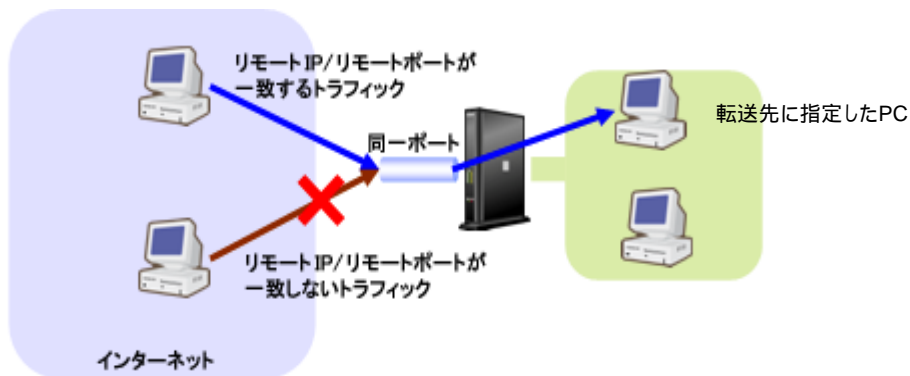


静的IPマスカレードによる接続例



## BA8000 Proの静的IPマスカレード機能の特徴

静的マスカレードを利用すると、設定したWAN側ポート宛のトラフィックを無条件にLAN側に転送してしまい、セキュリティが高いとはいえません。これに対し本製品は、「リモートIPアドレス」「リモートポート」のパラメータを追加し、同じポート番号宛に来るトラフィックでも、あらかじめ設定したインターネット上のIPアドレス(リモートIPアドレス)や送信元ポート番号(リモートポート)以外から来るトラフィックはLAN側に転送しません。特定の相手や、特定の送信元ポートからの通信に対してのみポートを空けることができ、よりセキュリティの高い静的マスカレードを実現することができます。



### 静的IPマスカレード/マルチNAT機能利用上の注意

- ・マルチNATで転送先に設定したローカルIPアドレスのホストはインターネット側から直接参照可能となりますのでご注意ください。使用するプロトコル、ポートが判明している場合はセキュリティの観点から静的IPマスカレードをご利用されることをお奨めします。また、送信元IPアドレス、ポートを指定できる場合は「リモートIPアドレス」、「リモートポート」の設定を行い、指定アドレス以外からのトラフィックを転送しないようにしてください。
- ・静的IPマスカレードで転送先に設定したローカルIPアドレスのホストは設定したプロトコル/ポートを通じてインターネット側から直接参照可能となりますのでご注意ください。送信元IPアドレス、ポートを指定できる場合は「リモートIPアドレス」、「リモートポート」の設定を行い、指定アドレス以外からのトラフィックを転送しないようにしてください。
- ・静的IPマスカレード/マルチNATを使用した際に他のNAPT端末は通常のインターネット接続が可能です。
- ・使用するプロトコル/ポートが異なる場合には1つのグローバルIPアドレスに対してプロトコル/ポート/転送先ローカルIPアドレスの異なる複数の静的IPマスカレードのエントリを設定することができます。
- ・コミュニケーション系のアプリケーションによってはパケットのヘッダ部だけでなくデータ内部にIPアドレス情報を埋め込む場合があります。この場合は静的IPマスカレード/マルチNATで転送先のローカルIPアドレスを指定してもご利用いただけない場合がありますのでご注意ください。

- ・MSN Messengerをご利用の場合はWindows 95/98/NT/2000でご使用の場合マルチNATの設定を行ってください。Windows Meでご使用の場合UPnPを有効にすれば自動的に静的IPマスカレードの設定を行い、かつ複数台のWindows Me端末で同時にご利用いただくことができます。詳しくはUniversal Plug&Play (UPnP) 利用ガイドをご覧ください。
- ・Windows Messengerをご使用の場合UPnPを有効にすれば自動的に静的IPマスカレードの設定を行い、かつ複数台のWindows XP端末で同時にご利用いただくことができます。詳しくはUniversal Plug&Play (UPnP) 利用ガイドをご覧ください。
- ・Windows XP またはWindows Me端末でUPnPを有効にしている場合、UPnPによるポートマッピングが静的IPマスカレードテーブルの設定に対して優先的に働きます。ポートマッピングの状態は[メンテナンス]-[モニタ]にてご確認ください。
- ・複数グローバルIPアドレスのサービスで静的IPマスカレード/マルチNATで転送先を指定したグローバルIPアドレスは「DMZネットワーク」の設定は行わないようにしてください。  
(詳細は「LAN型PPPoE接続ガイド」を参照ください)
- ・マルチNAT, 静的IPマスカレードで転送先に設定したローカルIPアドレスのサーバに対してはNAPT端末からグローバルIPアドレスまたはドメイン名でアクセスすることができませんのでご注意ください。

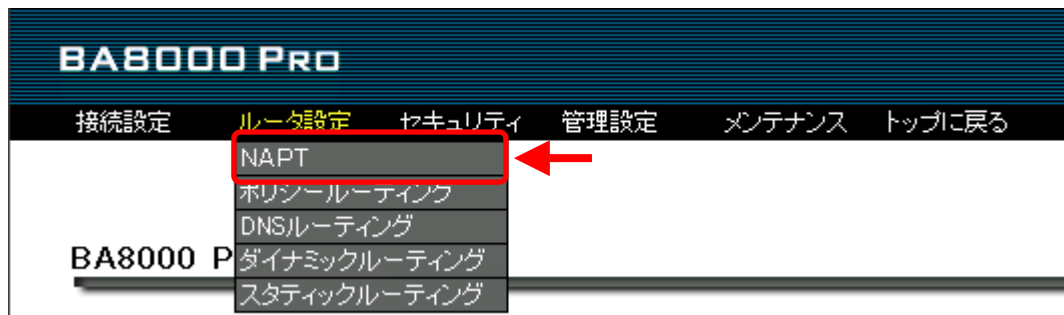
グローバルIPアドレス1個のサービスを使用する場合	ローカルIPアドレスのクライアントからLAN内のサーバにグローバルアドレスまたはドメイン名で <u>アクセスできません。</u>	
複数グローバルIPアドレスのサービスを使用する場合	サーバにグローバルアドレスを割り当てた場合	ローカルIPアドレスのクライアントからLAN内のサーバにグローバルアドレスまたはドメイン名で <u>アクセスできます。</u> (*)
	サーバに静的IPマスカレード/マルチNATとして転送先に指定したローカルIPアドレスを割り当てた場合	ローカルIPアドレスのクライアントからLAN内のサーバにグローバルアドレスまたはドメイン名で <u>アクセスできません。</u>

\*工場出荷時の設定でプライマリLAN(lan0)とセカンダリLAN(lan1)間の通信は遮断されています。  
lan0, lan1間の静的フィルタで透過のエントリを設定してください。

- ・PPTPパススルー、L2TPパススルー、IPsecパススルーを利用する場合、これらを利用するLAN側ホストに対して、マルチNATの設定(プロトコルが「すべて(\*)」の静的マスカレード)を行ってください。

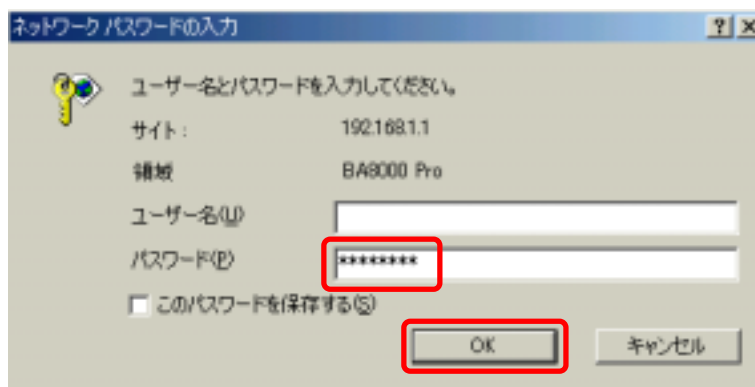
## 静的マスカレード設定手順

1. WebブラウザのURL欄に「http://192.168.1.1/」と入力し「Enter」キーを押します。  
BA8000 Pro設定画面のトップページが表示されますので**[ルータ設定]**の**[NAPT]**を選択して下さい。



ユーザ名/パスワード入力画面が表示されます。パスワード欄に「password」を入力し**[OK]**ボタンをクリックします。

上記は工場出荷時のパスワードです。パスワードを変更している場合は設定してあるパスワードを入力してください。



2. 静的IPマスカレードを設定するアカウントを選択してください。NAPTが有効になっていることを確認してください。(工場出荷時の設定は有効です)

## NAPT

アドレス変換の設定を行います。それぞれのアカウントで設定してください。

アカウント選択	plala ▼
NAPT	有効 ▼

3. [静的マスカレード]画面で[静的マスカレードの追加]をクリックしてください。

## 静的マスカレード



マルチNAT機能やローカルサーバ機能の設定を行います。

ID	プロトコル	リモートIPアドレス	リモートポート	外部IPアドレス	外部ポート	内部IPアドレス	内部ポート	修/削
----	-------	------------	---------	----------	-------	----------	-------	-----

静的マスカレードの追加

設定

やり直し

4. [静的マスカレードの追加/修正]画面で各項目に入力し[設定]をクリックしてください。

## 静的マスカレードの追加/修正

静的マスカレードを追加/修正します。

静的マスカレードID	64
プロトコル	tcp
リモートIPアドレス	*
リモートポート	*
外部IPアドレス	WAN側ポートIPアドレス
外部IPアドレス入力	192 . 168 . 10 . 1
外部ポート	80
内部IPアドレス	192 . 168 . 1 . 20
内部ポート	外部ポート番号と同じ
内部ポート指定	

設定

戻る

## 静的マスカレードID

設定したい静的マスカレードエントリに、番号を付けます。エントリ間で対象とするトラフィックが重複する場合、小さいIDのエントリが優先されますので、注意してください

### プロトコル

インターネットからLAN側への通信を許可するプロトコルを表示します。

- \* : すべてのプロトコルが対象となります。 は入力しないでください。
- icmp : icmp (pingなど) が対象となります。 は入力しないでください。
- tcp : tcpが対象となります。 も入力してください。
- udp : udpが対象となります。 も入力してください。
- tcp&udp : tcpとudpの両方が対象となります。 も入力してください。

### リモートIPアドレス

設定したい静的マスカレードエントリの対象となるトラフィックの、送信元IPアドレス (WAN側ホストのIPアドレス) を入力します。指定なし、特定アドレス指定、ネットワークアドレス指定、範囲指定、列挙指定が可能です。

送信元IPアドレス(例)	説明
*	すべてのIPアドレス
192.168.1.3	特定のホストアドレス
192.168.1.0/24	ネットワークアドレス(24ビットマスク)
192.168.1.3-192.168.1.33	範囲指定 スペース無しでハイフン“-”区切り
192.168.1.3, 192.168.1.8	列挙指定 スペース無しで“,”区切り(3つまで)*

### リモートポート

**[プロトコル]**が「tcp」、「udp」または「tcp&udp」の場合に、設定したい静的マスカレードエントリの対象となるトラフィックの、送信元ポート(WAN側ホストからの送信元ポート)を入力します。指定なし、特定アドレス指定、範囲指定、列挙指定が可能です。

送信元ポート(例)	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“-”区切り
80,8080	列挙指定 スペース無しで“,”区切り(3つまで)*

## 外部IPアドレス

静的IPマスカレード/マルチNATでインターネットからLAN側端末への通信を許可する際のインターネット側からみた送信先IPアドレス(公開アドレス)を選択します。

グローバルIPアドレス1個のサービスの場合	「WAN側ポートIPアドレス」を選択してください
複数グローバルIPアドレスのサービスで BA8000 ProのWAN側IPアドレスで公開する場合	「WAN側ポートIPアドレス」を選択してください
複数グローバルIPアドレスのサービスで BA8000 ProのWAN側IPアドレスで以外で公開する場合	「指定」を選択してください

### 外部IPアドレス入力

**[外部IPアドレス]**で「指定」を選択した場合にインターネットに公開したいグローバルIPアドレス(BA8000 ProのWAN側IPアドレス以外のアドレス)を入力します。

### 外部ポート

**[プロトコル]**欄でtcp, udpまたはtcp&udpを選択している場合にインターネット側から見た送信先ポート番号(公開ポート番号)を入力します。ネットワークゲームや公開サーバで利用するプロトコルのポート番号を入力してください。マルチNATを使用する場合は「\*」のままで結構です。

例: wwwサーバを公開するにはプロトコルに「tcp」、送信先ポートに「80」を選択

送信元ポート(例)	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“-”区切り
80,8080	列挙指定 スペース無しで“,”区切り(3つまで) *

### 内部IPアドレス

上記**[外部IPアドレス]**宛の packets がBA5000 ProのWAN側ポートから送られてきた場合にそれが転送されるべきLAN側ホストのIPアドレスを入力します。ここに入力されたIPアドレスのホストが公開インターネットサーバまたはネットワークゲームをプレイするパソコンになります。

### 内部ポート

**[プロトコル]**欄でtcp, udpまたはtcp&udpを選択している場合に**[内部IPアドレス]**で指定したパソコンがそのパケットを受け入れるポート番号を選択します。通常は「外部ポート番号と同じ」にしてください。WAN側の待ち受けポートと転送先(LAN上)のパソコンの待ち受けポートを異なる番号にしたい場合のみ「指定」を選択して以下の**[内部ポート指定]**欄に入力して下さい。

### 内部ポート指定

**[内部ポート]**欄で「指定」を選択している場合にここに転送先(LAN上)のパソコンの待ち受けポートを入力してください。

5. 設定内容を確認して **[設定]** ボタンをクリックしてください。

## 静的マスカレード



マルチNAT機能やローカルサーバ機能の設定を行います。

ID	プロトコル	リモート IPアドレス	リモート ポート	外部 IPアドレス	外部 ポート	内部 IPアドレス	内部 ポート	修/削
64	tcp	*	*	192.168.10.1	80	192.168.1.20	80	修正 削除

静的マスカレードの追加

**設定**

やり直し

## 端末のローカルIPアドレスの設定

静的IPマスカレード/マルチNAT機能を使用する場合、転送先として指定したローカルIPアドレスを端末に固定設定する必要があります。これには以下の3つの方法があります。

BA8000 ProのDHCPサーバ機能をOFFにして端末にローカルIPアドレスを固定設定する方法

**[接続設定]-[LAN設定]**で「DHCPサーバ機能」を「無効」に設定してください。

端末にはローカルIPアドレスの他DNSアドレスも設定してください。

BA8000 ProのProxy DNSを有効にした場合 BA8000 ProのLAN側ポートのアドレス

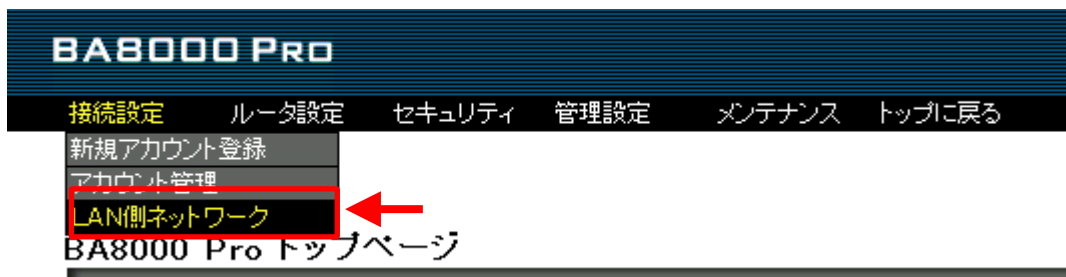
BA8000 ProのProxy DNSを無効にした場合 プロバイダのDNSアドレス

BA8000 ProのDHCPサーバ機能のDHCPスコープテーブルの範囲外のローカルIPアドレスを端末に固定設定する方法

BA8000 ProのDHCPサーバ機能の「DHCP固定アドレステーブル」の設定を行う方法

下記の手順に従ってください。

1. 画面上部の**[接続設定]**メニューから**[LAN設定]**を選択します。



2. 「DHCP固定IPアドレステーブル」で**[固定割り当ての追加]**ボタンをクリックして下さい。

## DHCP固定IPアドレス ?

DHCPサーバ機能を使って、特定ホストに対し常に同じIPアドレスを割り当てる設定を行います。



3. 「固定IP割り当ての追加/修正」で割り当てるホストアドレスと端末のMACアドレスを投入して**[設定]**ボタンをクリックして下さい。

## 固定IP割り当ての追加/修正

DHCP固定IP割り当てを追加/修正します。

固定割り当てIPアドレス	<input type="text" value="20"/>
パソコンのMACアドレス	<input type="text" value="00"/> : <input type="text" value="80"/> : <input type="text" value="98"/> : <input type="text" value="E8"/> : <input type="text" value="26"/> : <input type="text" value="32"/>

4. 「DHCP固定IPアドレステーブル」に追加されたことを確認して**[設定]**ボタンをクリックして再起動してください。

## DHCP固定IPアドレス



DHCPサーバ機能を使って、特定ホストに対し常に同じIPアドレスを割り当てる設定を行います。

固定割り当てIPアドレス	パソコンのMACアドレス	修/削
192.168.1.20	00-80-98-e8-26-32	<input type="button" value="修正"/> <input type="button" value="削除"/>
<input type="button" value="固定割り当ての追加"/>		

## 静的IPマスカレード/マルチNAT機能の設定例

### [設定例1]

グローバルIPアドレス1個のサービスで

tcpの80番ポート宛のトラフィック 192.168.1.11へ

tcp&udpの20,21番ポート宛のトラフィック 192.168.1.12へ

それ以外の(転送先不明の)トラフィック 192.168.1.13へ

それぞれ転送する設定

ID	プロトコル	リモートIPアドレス	リモートポート	外部IPアドレス	外部IPアドレス入力	外部ポート	内部IPアドレス	内部ポート	内部ポート指定
62	tcp	*	*	WAN側 ポートIPアドレス	*	80	192.168.1.11	外部ポート 番号と同じ	*
63	tcp&udp	*	*	WAN側 ポートIPアドレス	*	20,21	192.168.1.12	外部ポート 番号と同じ	*
64	*	*	*	WAN側 ポートIPアドレス	*	*	192.168.1.13	外部ポート 番号と同じ	*

### [設定例2]

複数グローバルIPアドレスのサービスで

10.10.1.102宛のトラフィック 192.168.1.12へ

10.10.1.103宛のトラフィック 192.168.1.13へ

ルータのWAN側ポートIPアドレス(10.10.1.101)宛のtcp80番ポート宛のトラフィック

192.168.1.14へ

それぞれ転送する設定

ID	プロトコル	リモートIPアドレス	リモートポート	外部IPアドレス	外部IPアドレス入力	外部ポート	内部IPアドレス	内部ポート	内部ポート指定
62	*	*	*	指定	10.10.1.102	*	192.168.1.12	外部ポート 番号と同じ	*
63	*	*	*	指定	10.10.1.103	*	192.168.1.13	外部ポート 番号と同じ	*
64	tcp	*	*	WAN側 ポートIPアドレス	*	80	192.168.1.14	外部ポート 番号と同じ	*

[設定例3]

複数グローバルIPアドレスのサービスで

10.10.1.102宛のtcp&udp20,21番ポート宛トラフィック 192.168.1.12へ  
 10.10.1.103宛のtcp&udp25,110番ポート宛トラフィック 192.168.1.13へ  
 ルータのWAN側ポートIPアドレス(10.10.1.101)宛のtcp80番ポート宛のトラフィック 192.168.1.14へ

それぞれ転送する設定

ID	プロトコル	リモートIPアドレス	リモートポート	外部IPアドレス	外部IPアドレス入力	外部ポート	内部IPアドレス	内部ポート	内部ポート指定
62	tcp&udp	*	*	指定	10.10.1.102	20,21	192.168.1.12	外部ポート番号と同じ	*
63	tcp&udp	*	*	指定	10.10.1.103	25,110	192.168.1.13	外部ポート番号と同じ	*
64	tcp	*	*	WAN側ポートIPアドレス	*	80	192.168.1.14	外部ポート番号と同じ	*

[設定例4]

複数グローバルIPアドレスのサービスで

10.10.10.101から10.10.1.102宛のtcp&udp20,21番ポート宛トラフィック 192.168.1.12へ  
 転送する設定

ID	プロトコル	リモートIPアドレス	リモートポート	外部IPアドレス	外部IPアドレス入力	外部ポート	内部IPアドレス	内部ポート	内部ポート指定
62	tcp&udp	10.10.10.101	20,21	指定	10.10.1.102	20,21	192.168.1.12	外部ポート番号と同じ	*

[付録] tcp, udpで使用するポート番号一覧

ポート番号	説明
20	Ftp (Default Data)
21	Ftp (Control)
23	telnet
25	smtp
53	dns
70	gopher
79	finger
80	http
110	pop3
113	ident
119	nntp
123	ntp
194	irc
443	https