

BA8000 Pro  
DNSルーティング利用ガイド

BA8000 Pro  
株式会社NTT-ME

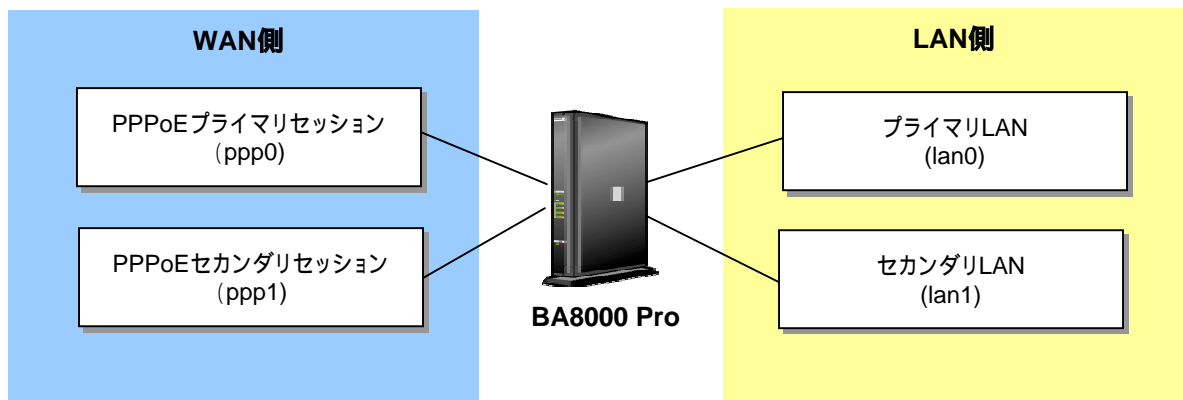
## はじめに

- ・本ガイドはBA8000 ProのDNSルーティング機能について解説したものです。

更新履歴      修正初版   2002 年 12 月 24 日

## BA8000 Proのルーティング機能について

BA8000 ProではPPPoEマルチセッション接続時には以下のような論理的なインターフェースを有します。このインターフェース間のルーティングを行う機能としてスタティックルーティング機能、ダイナミックルーティング機能に加えてポリシールーティング機能を搭載しています。



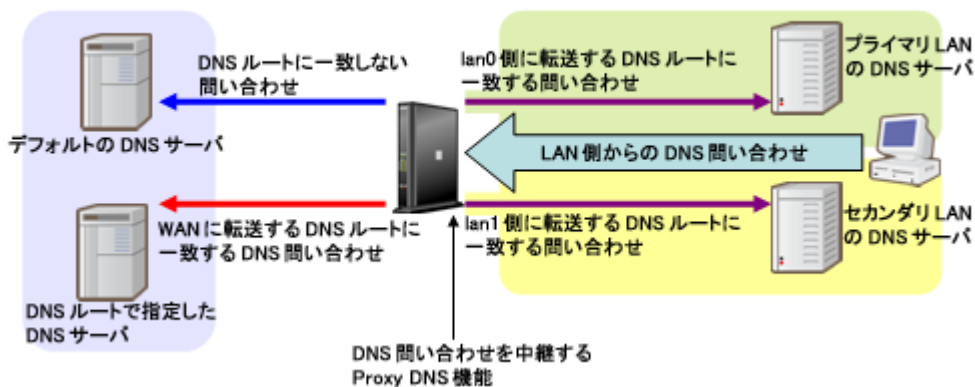
PPPoEマルチセッションを利用する際には本製品のポリシールーティング機能を利用して送信先アドレス、ポート、送信元アドレス、ポート、プロトコルなどのパラメータを指定することにより、デフォルトルートを使用しない(即ちセカンダリセッションを使用する)ルーティングのルールを設定することができます。(指定がない場合はプライマリセッションに転送されます)

詳細は「BA8000 Proポリシールート設定ガイド」を参照してください

しかしながら、通常のネット利用においてはURLなどのドメイン(ホスト)名をDNSでアドレス解決して初めて宛先アドレスを知ることができます。解決したアドレスを一つ一つポリシールートに設定することも可能ですが、特定ドメインに対するIPアドレスは変化する可能性があり、この方法は実用的ではありません。そこでBA8000 Proでは特定のDNS問い合わせを指定したDNSサーバに転送する「DNSルーティング機能」を搭載しています。

本製品のDNSルーティング機能は以下のパラメータを設定することが可能です。

- 送信元IPアドレス : どのホストからのDNS問い合わせを対象とするか
- クエリタイプ : a/mx/ns/cname/ptrなどのクエリタイプ
- クエリ : どのようなクエリを対象とするか
- インターフェース : 上記で指定したDNS問い合わせをどのインターフェースに転送するか
- DNSアドレス : 上記インターフェース上のどのDNSサーバに転送するか

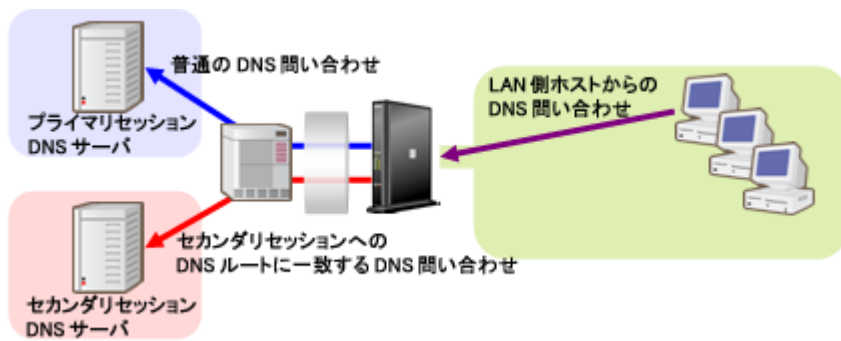


## DNSルーティング機能とポリシールーティング機能の連携

ここで注意すべき点は、ポリシールーティングとDNSルーティングは基本的に別個の機能として働くことです。すなわち、「www.ntt-me.co.jpのDNS問い合わせはセカンダリセッションのDNSサーバに転送する」と設定した場合にDNS問い合わせ自身はセカンダリセッション上のDNSサーバで解決しますが、アドレス解決後の「www.ntt-me.co.jp」宛の通信トラフィックはデフォルトルートであるプライマリセッションに転送されてしまいます。「www.ntt-me.co.jp」宛のDNS問い合わせだけでなく、アドレス解決後の「www.ntt-me.co.jp」宛の通信も、セカンダリセッションを利用したい場合は、DNSルーティングとポリシールーティングの連携を設定しなければなりません。

具体的には、ポリシールーティングの設定において、「宛先」を送信先IPアドレスで指定する代わりに、DNSルーティングのID番号を入力します。この設定を行うことで本製品は、LAN側ホストからの「www.ntt-me.co.jp」のDNS問い合わせ(アドレス解決)をセカンダリセッション上のDNSサーバに転送するとともに、DNSサーバからの回答(www.ntt-me.co.jpのIPアドレス)を問い合わせたLAN側ホストに教えるだけでなく、当該ポリシールートの送信先IPアドレスとして一時的に記憶します。その後、LAN側ホストから「www.ntt-me.co.jp」のIPアドレス宛の通信が来ると、記憶しているIPアドレスと照合し、セカンダリセッションに転送します。

さらに注意点として、DNS問い合わせを転送するという性格上、DNSルーティングを利用するためには、LAN側ホストが本製品のProxy DNS機能を利用する必要があります。すなわち、LAN側ホストのIP設定を本製品のDHCPサーバ機能によって自動構成するか、もしくは本製品のLAN側IPアドレスをLAN側ホストのDNSサーバアドレスとして手動登録しておく必要があります。



## DNSルーティングの設定例

**[設定例1]** フレッツスクウェア上のサイトのDNS問い合わせをセカンダリセッションに転送する。

送信元アドレス: \*  
クエリタイプ: **すべて、またはa**  
クエリ: **.flets**  
インターフェース: セカンダリセッションのアカウント  
DNSアドレス: 指定せず

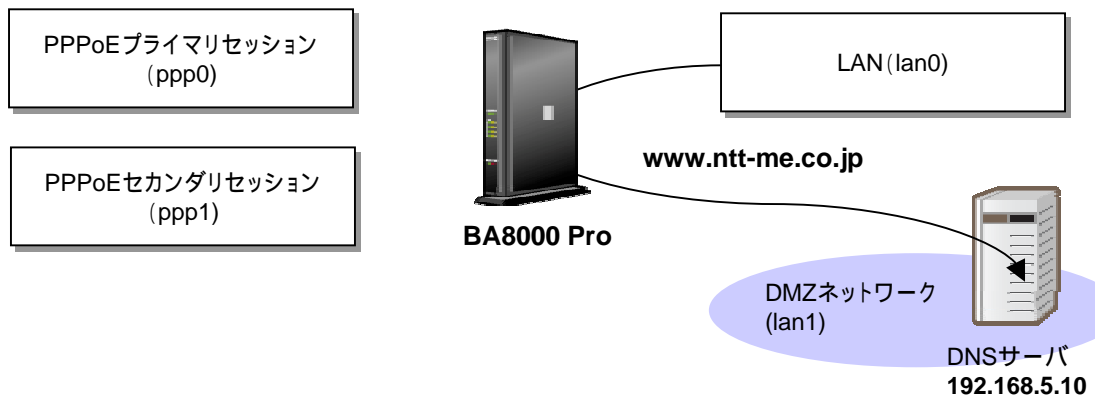


対象DNS問い合わせのみセカンダリへ、その他はプライマリへ

**[設定例2]** [www.ntt-me.co.jp](http://www.ntt-me.co.jp)をLAN側内のDMZネットワークに設置したDNSサーバに問い合わせたい場合

送信元アドレス: \*  
クエリタイプ: **すべて、またはa**  
クエリ: **www.ntt-me.co.jp**  
インターフェース: **lan1**  
DNSアドレス: **192.168.5.10**

lan0 - lan1間の通信はデフォルト設定で遮断されているため透過の静的フィルタエントリを追加する必要があります。



[設定例3] [www.ntt-me.co.jp](http://www.ntt-me.co.jp)をLAN側ユーザに見せたくない場合

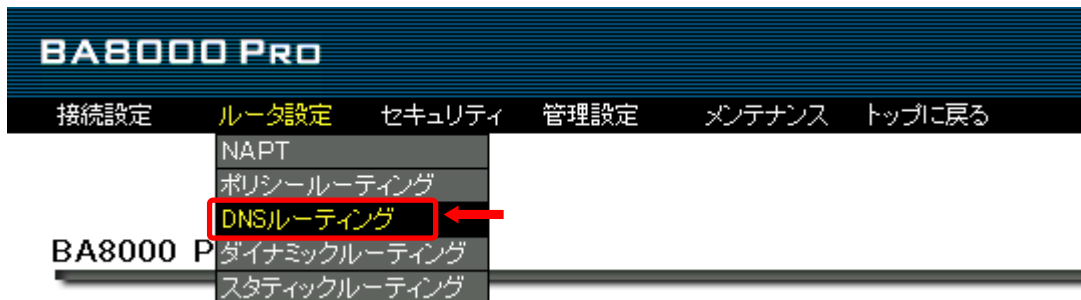
送信元アドレス:	*
クエリタイプ:	すべて、またはa
クエリ:	<a href="http://www.ntt-me.co.jp">www.ntt-me.co.jp</a>
インターフェース:	破棄
DNSアドレス:	指定せず

この使い方でURLフィルタ代わりに使うことができます



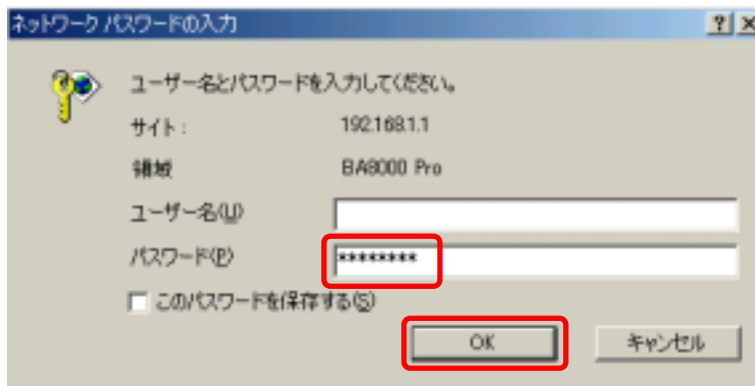
## ポリシールーティング設定手順

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[DNSルーティング]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. DNSルーティング設定画面で **[DNSルートの追加]** をクリックします。

## DNSルーティング



特定のDNSクエリの経路を指定します。

### 注意:

DNSルーティング機能は、以下のいずれかの場合にのみ機能します。

- Proxy DNS機能有効、且つ本製品のDHCPサーバ機能を利用
- Proxy DNS機能有効、且つパソコンのDNSサーバIPアドレス設定が本製品のLAN側ポートIPアドレス

ID	送信元 IPアドレス	クエリ タイプ	クエリ	インター フェイス	DNS アドレス	修/削
<b>DNSルートの追加</b>						
設定						
やり直し						

3. **[DNSルートの追加/修正]**の各項目を設定してポリシールートのエントリを作成してください。最後に**[設定]** ボタンを押してください。

## DNSルートの追加/修正



DNSルートの追加/修正を行います。

DNSルートID	32
送信元アドレス	*
クエリタイプ	すべて(ptr以外)
DNSクエリ	flets
インターフェイス	Flets
DNSサーバアドレス	0 . 0 . 0 . 0

設定	戻る
----	----

## DNSルートID

設定したいDNSルートに、番号を付けます。ルート間で対象とするトラフィックに重複がある場合、小さいIDのルートが優先されます。半角数字 1～32

### 送信元IPアドレス

設定したいDNSルートが対象とするDNS問い合わせの、送信元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。(半角文字で入力し、スペースを入れないください)

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)*

### クエリタイプ

設定したいDNSルートが対象とするDNS問い合わせの、レコードタイプを選択します。

#### すべて(ptr以外)

以下の[DNSクエリ]に入力された文字列をクエリとする、ptrを除くすべてのレコードタイプを対象とします。

#### a

以下の[DNSクエリ]に入力された文字列をクエリとする、Aタイプレコードを対象とします。

#### mx

以下の[DNSクエリ]に入力された文字列をクエリとする、MXタイプレコードを対象とします。

#### ns

以下の[DNSクエリ]に入力された文字列をクエリとする、NSタイプレコードを対象とします。

#### cname

以下の[DNSクエリ]に入力された文字列をクエリとする、CNAMEタイプレコードを対象とします。

#### ptr

以下の[DNSクエリ]に入力されたIPアドレスをクエリとする、ptrタイプレコードを対象とします

## DNSクエリ

[クエリタイプ]での選択に従って、設定したいDNSルートが対象とするDNS問い合わせの、DNSクエリ内容を入力します。入力できる文字列は選択したクエリタイプによって異なります。

### ptr以外のクエリタイプの場合:

ドメイン名またはホスト名を入力します。ホスト、サブドメイン、デフォルトドメインまで含んだ完全修飾ドメイン名(FQDN)で指定するか、連続性のあるドメイン名で指定してください。

入力例	説明
.jp	トップレベルドメインのみ指定。日本(jp)ドメインに属するすべてを対象とする。“.”を付けなければならない。
.co.jp	セカンダリレベルドメインまで指定「co.jp」ドメインに属するすべてを対象とする。“.”を付けなければならない。
ntt-me.co.jp	「ntt-me.co.jp」のみを対象とする。「www.ntt-me.co.jp」などサブドメインやホストは対象外
www.ntt-me.co.jp	「www.ntt-me.co.jp」のみを対象とする。「host.www.ntt-me.co.jp」など、下位サブドメインやホストは対象外。
.www.ntt-me.co.jp	「host.www.ntt-me.co.jp」など、下位サブドメインやホストを対象とする。「 <a href="http://www.ntt-me.co.jp">www.ntt-me.co.jp</a> 」は対象外
www.*.co.jp	ワイルドカードを使用。「www.yahoo.co.jp」などを対象とする。

### ptrタイプの場合:

ptrは逆引きであるため、IPアドレスで指定する必要があります。指定無し、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。  
(半角文字で入力し、スペースを入れないください)

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)*

## インターフェイス

設定したいポリシールート対象トラフィックの出力先になる、インターフェイスを選択します。

- ・ WAN側への転送の場合：「アカウント名」を選択します。
  - ・ プライマリLANネットワーク側への転送の場合：「LAN0」を選択します。
  - ・ セカンダリLAN (DMZ) ネットワーク側への転送の場合：「LAN1」を選択します。
  - ・ 特に指定しなくても良い場合：「自動」を選択します。
- 送信先IPアドレスのサブネットと、本製品のいずれかのインターフェイスの属するサブネットが同一の場合のみ、これを選択することができます。

## DNSアドレス

設定したいDNSルートが対象とするDNS問い合わせの、送信先DNSサーバのIPアドレスを入力します。上記インターフェイスで選択した接続アカウントのデフォルトDNSサーバを利用する場合は、入力する必要はありません

4. 設定内容を確認の上**[設定]**ボタンをクリックください。

## DNSルーティング



特定のDNSクエリの経路を指定します。

### 注意:

DNSルーティング機能は、以下のいずれかの場合にのみ機能します。

- Proxy DNS機能有効、且つ本製品のDHCPサーバ機能を利用
- Proxy DNS機能有効、且つパソコンのDNSサーバIPアドレス設定が本製品のLAN側ポートIPアドレス

ID	送信元 IPアドレス	クエリ タイプ	クエリ	インター フェイス	DNS アドレス	修/削
32	*	すべて(ptr以外)	.flets	Flets	0.0.0.0	<a href="#">修正</a> <a href="#">削除</a>

DNSルートの追加

**設定**

やり直し

## DNSルーティング機能をご利用いただく上での注意事項

- ・PPPoEマルチセッションを利用する場合や、DNSルーティングを利用する場合は、必ずProxy DNS機能を利用してください。
- ・ProxyDNS機能は、プライマリLANネットワークだけでなく、セカンダリLANネットワーク(DMZ除く)に対しても機能します。したがって、プライマリLANネットワーク上のホストのDNSサーバアドレスはプライマリLAN IPアドレス、セカンダリLANネットワーク上のホストのDNSサーバアドレスはセカンダリLAN IPアドレスになります。
- ・セカンダリLANがDMZネットワークである(DMZネットワークを利用している)場合、セカンダリLAN IPアドレスはProxy DNSとして機能しません。したがって、DMZネットワーク上のホストは、DNSルーティング機能を利用することはできません。
- ・本製品のDHCPサーバ機能はプライマリLANネットワークのみ有効です。したがってセカンダリLANネットワーク上のホストのIPアドレス設定、DNSサーバアドレス設定は手動で行う必要があります。
- ・「インターフェース」に「破棄」を設定したエントリを投入することによりURLフィルタとして使用することができます。