

## <設定例> DMZ ポートを利用して自宅サーバをインターネットに公開したい

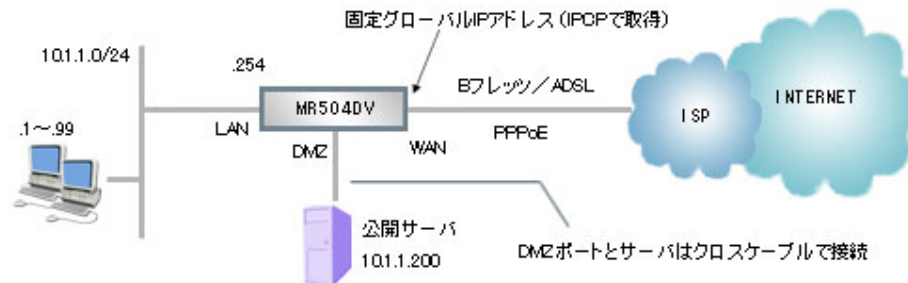
公開サーバで使用するアプリケーションのポートの数が多い場合や、ポート番号が動的に変化する場合などは DMZ ポートの活用が有効です。

ここでは、MR504DV を使って、DMZ ポートに接続したサーバをインターネットに公開する際の設定例を示します。

(MR404DV で構成する場合も同じ設定になります)

特定の条件に一致しないインターネット側からのすべてのアクセスを、DMZ 上の公開サーバへ転送させます。

外部からアクセスするために、WAN 側に固定のグローバル IP アドレスが1つ必要です。



### 設定概要

#### ・PPPoE クライアント設定

ISP から指定されたインターネット接続用アカウントをルータに設定します。

ユーザ ID: abcde@sogen.com

パスワード: abcde123

#### ・IP アドレス設定

ルータの LAN 側ネットワークアドレス: 10.1.1.0/24

ルータの IP アドレス: 10.1.1.254/24

WAN 側の IP アドレス (グローバル IP アドレス) は IPCP で取得するため、明示的に設定しません

#### ・DHCP サーバ機能

LAN 内のクライアントに IP アドレス、デフォルトゲートウェイ、DNS アドレスの情報を配布します。

配布する IP アドレス範囲: 10.1.1.1 ~ 10.1.1.99

デフォルトゲートウェイ、DNS アドレスはルータの IP アドレスが通知されます

#### ・DMZ ポート設定

DMZ 利用を有効にし、DMZ ポートに接続するホスト(サーバ)の IP アドレスを定義します。

DMZ に接続するサーバの IP アドレス: 10.1.1.200/24

また、インターネットからサーバへのアクセスを許可するための IP フィルタリング設定を行います。

(補足)

LAN のクライアントがインターネットへ接続できるようにするための NAPT (IP マスカレード) 機能については、本製品では工場出荷時の状態で有効になっていますので、改めて設定する必要はありません。

### 設定

```
ip address 10.1.1.254/24
ip dhcp address 10.1.1.1/99
ip dhcp server on
dmz port on
ip dmzhost address 10.1.1.200
ip filter 1 pass in * 10.1.1.200/32 * wanany
remote 0 name INTERNET
remote 0 mode terminal
remote 0 ppp ipcp address on
```

```
remote 0 ppp ipcp dns on
remote 0 dos mode on
remote 0 dos log on
remote 0 mss mode on
remote 0 mss size 1414
remote 0 mtu 1454
remote 0 send id abcde@sogen.com
remote 0 send password abcde123
remote 0 disconnect idle 0
remote 0 pppoe keepalive on
remote 0 pppoe always on
ip route 0.0.0.0/0/7 remote 0 auto
```

#### 解説

ip address 10.1.1.254/24

ルータの LAN 側 IP アドレスを 10.1.1.254/24 に設定します。

ip dhcp address 10.1.1.1/99

ip dhcp server on

DHCP で配布するアドレス範囲を 10.1.1.1 ~ 10.1.1.99 に設定し、DHCP サーバ機能を有効にします。

dmz port on

ip dmzhost address 10.1.1.200

DMZ ポート利用を有効にし、接続するホスト(公開サーバ)の IP アドレスを指定します。

ip filter 1 pass in \* 10.1.1.200/32 \* wanany

インターネット側から公開サーバへのアクセスを許可するためのフィルタ設定を行います。

本例ではすべてのプロトコルによる外部からのアクセスが許可されますが、フィルタを変えることによってプロトコルを制限することも可能です。

たとえば DMZ に Web サーバを置いて、外部からのアクセスは http(TCP:80)と https(TCP:443)だけを許可したいというような場合は、次のフィルタを設定します。

ip filter 1 pass in \* 10.1.1.200/32 tcp \* 80 wanany

ip filter 2 pass in \* 10.1.1.200/32 tcp \* 443 wanany

ip filter 3 reject in \* 10.1.1.200/32 \* wanany

remote 0 name INTERNET

ISP との接続を接続相手番号 0(remote 0)として定義します。名称を「INTERNET」とします。

remote 0 mode terminal

ISP と端末型接続します。

(デフォルト設定値のため、コンフィグには表示されません)

remote 0 ppp ipcp address on

remote 0 ppp ipcp dns on

PPPoE 接続時、IPCP で WAN 側の IP アドレスおよび DNS アドレスを取得します。

(デフォルト設定値のため、コンフィグには表示されません)

remote 0 dos mode on

remote 0 dos log on

DoS 攻撃防御機能、DoS 攻撃に関するログ出力を有効にします。

(デフォルト設定値のため、コンフィグには表示されません)

remote 0 mss mode on  
remote 0 mss size 1414  
remote 0 mtu 1454

NTT 東西のフレッツサービスをご利用の場合、MTU=1454 / MSS=1414 に設定します。  
(デフォルト設定値のため、コンフィグには表示されません)

remote 0 send id abcde@sogen.com  
remote 0 send password abcde123

ISP から指定されたインターネット接続用アカウント(ユーザ ID、パスワード)を設定します。

remote 0 disconnect idle 0                   ... (1)  
remote 0 pppoe keepalive on               ... (2)  
remote 0 pppoe always on                 ... (3)

インターネットに常時接続するためのオプション機能です。

(1) 回線自動切断タイマを 0 秒(無効)にします。

(2)(3) ルータ起動時に自動的に PPPoE 接続を行い、また何らかの原因で回線が切断された際には定期的に再接続を試みます。

ip route 0.0.0.0/0/7 remote 0 auto

ルータのデフォルトルートを remote 0 に設定します。