

IPv6 で DNS

IPv6 で DNS サーバの構成

DNS サーバ

Windows Server 2003 のドメイン ネーム システム (DNS) サーバを使用して、ホスト名を IPv6 アドレスに解決することができる。IPv6 ホストに DNS サーバのアドレスを構成すると、ホストはサーバに DNS 名クエリを送信して解決する。Windows Server 2003 の DNS サーバは IPv4 と IPv6 双方に同時に対応可能である。ここでは、DNS サーバサービスのインストールはすでに済ませてあるとする。DNS サーバサービスのインストールは、「コントロールパネル」の「アプリケーションの追加と削除」から行う。

DNS クライアントとサーバ間の通信を可能にする

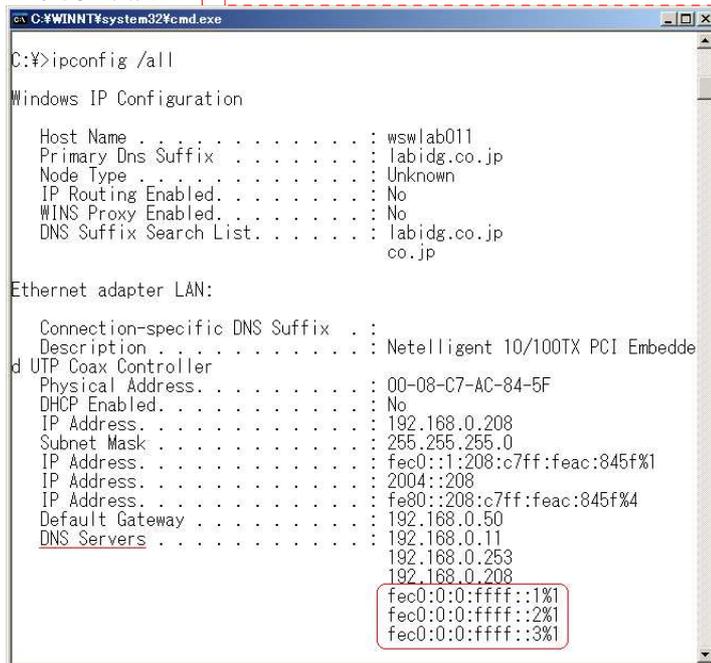
DNS クライアントとサーバ間の通信を可能にするには、

- DNS サーバに、すべての IPv6 クライアントに自動的に構成されている 3 つの既定の DNS サーバ IPv6 アドレスのいずれかを構成するか、
- クライアントに DNS サーバの IPv6 アドレスを構成する。

DNS サーバに、IPv6 クライアント コンピュータで既定で利用可能になっている 3 つの IPv6 アドレスのいずれかを構成するには、netsh interface ipv6 add address コマンドを使用する。IPv6 クライアントに自動的に構成されている 3 つの既定の DNS サーバアドレスは、

- FEC0:0:0:FFFF::1
- FEC0:0:0:FFFF::2
- FEC0:0:0:FFFF::3

である。<画面 36>



```
C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : wswlab011
Primary Dns Suffix . . . . . : labidg.co.jp
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : labidg.co.jp
                                   co.jp

Ethernet adapter LAN:

   Connection-specific DNS Suffix . . :
   Description . . . . . : Netelligent 10/100TX PCI Embedde
   d UTP Coax Controller
   Physical Address. . . . . : 00-08-C7-AC-84-5F
   DHCP Enabled. . . . . : No
   IP Address. . . . . : 192.168.0.208
   Subnet Mask . . . . . : 255.255.255.0
   IP Address. . . . . : fec0::1:208:c7ff:feac:845f%1
   IP Address. . . . . : 2004::208
   IP Address. . . . . : fe80::208:c7ff:feac:845f%4
   Default Gateway . . . . . : 192.168.0.50
   DNS Servers . . . . . : 192.168.0.11
                           192.168.0.253
                           192.168.0.208
                           fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
```

コメント [W1]: このアドレスが DNS サーバとして自動設定されているアドレスである、と明示するために、画面 36-2 を用意しています。

DNS サーバが IPv6 クライアントとは異なるサブネット上にある場合は、DNS サーバのサブネット上で利用可能な任意の IPv6 ルータに、DNS サーバへの静的ルートを構成する。

明示的に DNS サーバの IPv6 アドレスをクライアントに構成すれば、FEC0:0:0:FFFF::1 といったアドレスを DNS サーバに設定する必要はない。明示的に DNS サーバの IPv6 アドレスをクライアントに構成する方法は後で述べる。

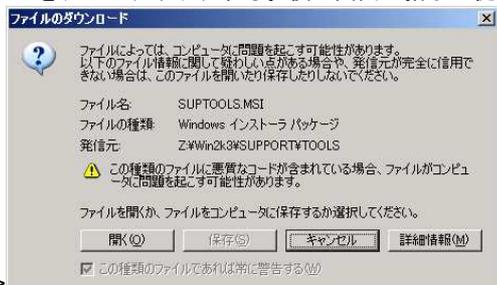
DNS サーバが IPv6 上でリッスンするように構成する

Windows 2003 Server の DNS サービスは、デフォルトでは IPv4 クエリパケットのみしか受け付けない。IPv6 の名前解決も、IPv4 のクエリパケットに対して IPv4 のアンサーパケットで AAAA レコードを返す。もちろん DNS サーバが IPv6 を介して DNS 名の登録および解決要求をリッスンするように構成できる。DNS サーバが IPv4 と IPv6 の両方をリッスンするように構成すると、

- IPv6 では機能するが、IPv4 では機能しないデバイスが、DNS サーバで機能する。
- IPv4 と IPv6 の両方を使用するように構成されたコンピュータやその他のデバイスが、既定で IPv6 を使用する。(最初に IPv6 でクエリを出し名前解決を試みる。解決できないと次に IPv4 でクエリを出し解決を試みる。)

DNS サーバが IPv6 を介してリッスンするように構成するには、次の操作を行う。

1. Windows サポート ツールをインストールする。それには、Windows の CD-ROM を CD-ROM ドライブに挿入し、¥Support¥Tools フォルダに移動する。
2. suptools.msi をダブルクリックする。後は画面の指示に従う。



<画面 37>



<画面 38>



<画面 39>

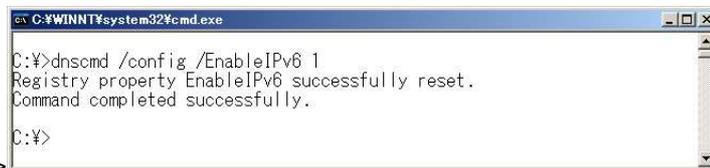


<画面 40>

3. サポートツールが完了したら、コマンド プロンプトを開く。
4. 次のコマンドを入力する。

```
dnscmd /config /EnableIPv6 1
```

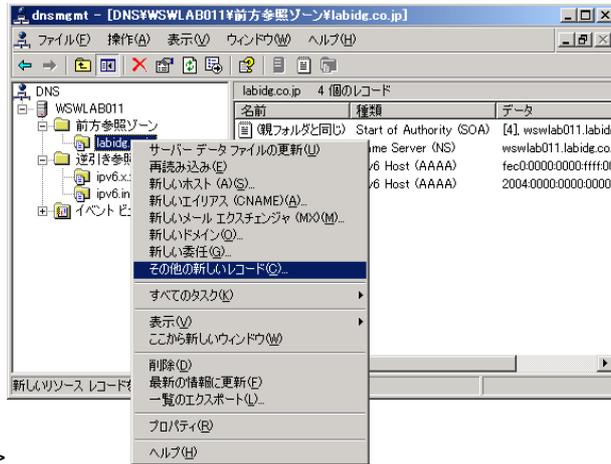
上記コマンドは、サポートツールをインストールしないと実行できない。



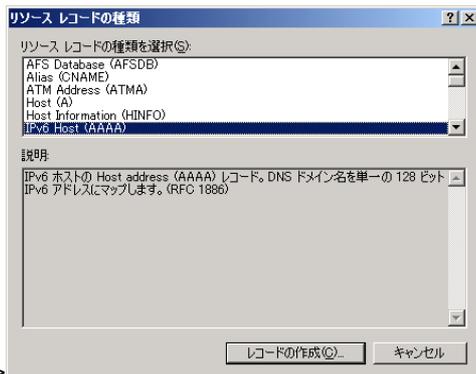
<画面 41>

5. DNS サーバサービスを再起動する。

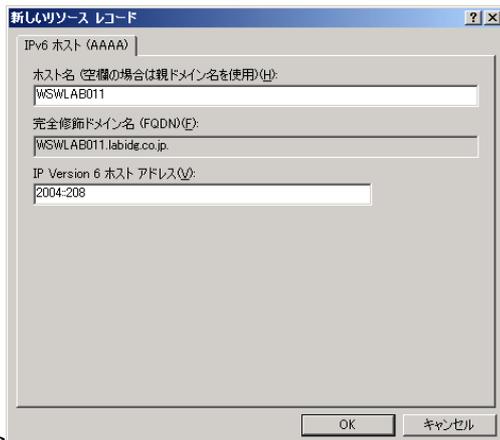
DNS サーバへの IPv6 正引きエントリを追加するには、DNS サーバ管理コンソール(dnsmgmt.msc)を起動して、前方参照ゾーンのプライマリゾーンに AAAA レコードを追加する。



<画面 42>



<画面 43>



<画面 44>

※ 残念ながら逆引きエントリは、筆者にはわからぬ。Technet のページ http://www.microsoft.com/japan/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_DNS_und_ReverseLookup.asp には、IPv6 の逆引きも可能な記述があるが、具体的な設定方法の記載がない。どなたか Windows Server で逆引き参照ゾーンを構成する方法をご存知であれば、連絡してほしい。

BIND9.2 や 9.3 で逆引き参照ゾーンを構成する方法は、@IT > Linux Square > IPv6 対応 DNS サーバの実現

<http://www.atmarkit.co.jp/flinux/rensai/bind912/bind912a.html>

などに記述もあり、筆者も構築実績がある。しかしテキストファイルなので、初心者には敷居が高い。IPv4 の BIND を設定した経験があれば面倒だが簡単だ。

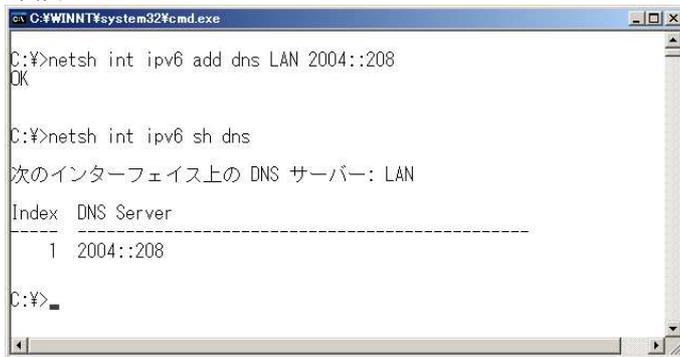
IPv6 で DNS クライアントの構成

クライアントに DNS サーバの IPv6 アドレスを構成するには、

- ① クライアントがネットワークにログオンするたびに実行される ログオンスクリプト、または、
- ② 各クライアントコンピュータ、

で、netsh interface ipv6 add dns コマンドを使用する。ログオンスクリプトは Microsoft TechNet での記述であるが、筆者が実験した環境では、再起動しても DNS サーバのエントリは消去されない。あくまでも何千台もあるクライアントコンピュータに対して管理者が一台ずつローカル設定するようなナンセンスを否定する記述だと思われる。

<画面 45>



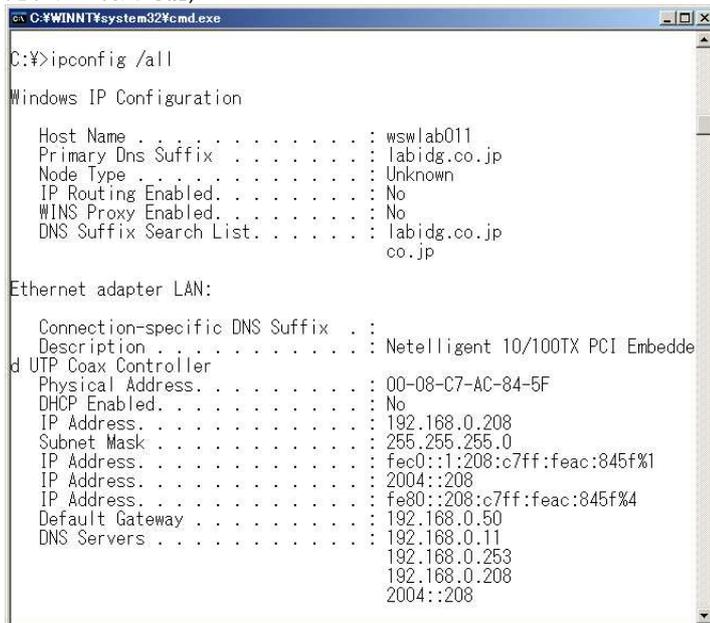
```
C:\>netsh int ipv6 add dns LAN 2004::208
OK

C:\>netsh int ipv6 sh dns
次のインターフェイス上の DNS サーバー: LAN

Index  DNS Server
-----
1      2004::208

C:\>
```

クライアントコンピュータに netsh interface ipv6 add dns コマンドを実行すると、IPv6 を enable にしたときから既定で DNS サーバのアドレスとして自動設定されている 3 つの IPv6 アドレスは disable となる。(ipconfig /all で確認できる。<画面 46>netsh interface ipv6 add dns コマンドで明示的に静的設定すれば利用可能)



```
C:\>ipconfig /all

Windows IP Configuration

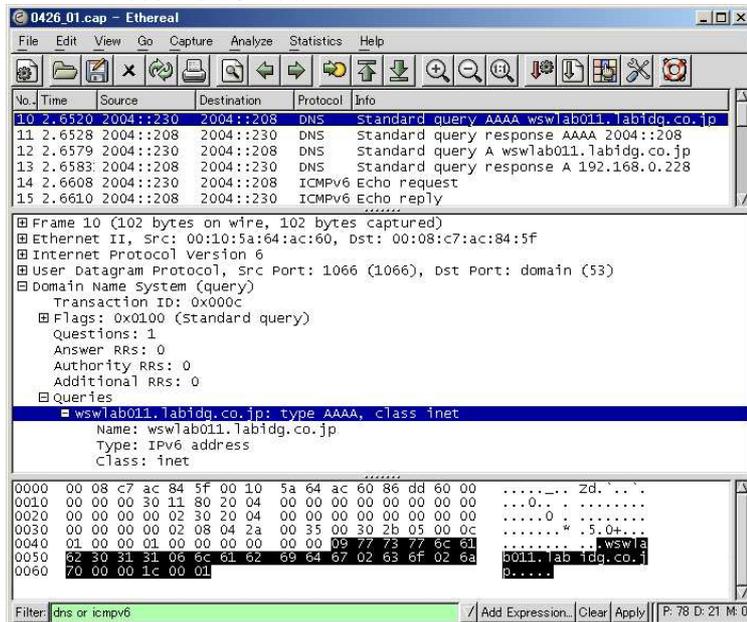
Host Name . . . . . : wswlab011
Primary Dns Suffix . . . . . : labidg.co.jp
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : labidg.co.jp
                                   co.jp

Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : 
   Description . . . . . : Netelligent 10/100TX PCI Embedded UTP Coax Controller
   Physical Address. . . . . : 00-08-C7-AC-84-5F
   DHCP Enabled. . . . . : No
   IP Address. . . . . : 192.168.0.208
   Subnet Mask . . . . . : 255.255.255.0
   IP Address. . . . . : fec0::1:208:c7ff:feac:845f%1
   IP Address. . . . . : 2004::208
   IP Address. . . . . : fe80::208:c7ff:feac:845f%4
   Default Gateway . . . . . : 192.168.0.50
   DNS Servers . . . . . : 192.168.0.11
                           192.168.0.253
                           192.168.0.208
                           2004::208
```

Windows Server 2003 で DNS クライアント

Windows Server 2003 を DNS クライアントとして構成すると、IPv6 パケットで AAAA レコードに対する name クエリを DNS サーバに対して送出する。回答が返ってくる・来ないにかかわらず、次に IPv6 パケットで A レコードに対する name クエリを送出する。この様子は Microsoft Network モニタや Ethereal で確認できる。<画面 47>



Windows Server 2003 の DNS でも、BIND9 でも、IPv4・IPv6 双方のクエリに対応している。Windows Server 2003 で DNS クライアントを構成すると、いずれの DNS サーバからも IPv6 のクエリに対して IPv6 で応答がある。

Windows Xp で DNS クライアント(IPv4 でのみクエリを送出)

残念ながら、Windows Xp はデフォルトでは IPv6 のパケットで DNS クエリを送出しない。IPv4 パケットで AAAA レコードを尋ねるクエリを送出し、回答を得てからリモートホストに IPv6 で通信する。

Microsoft Technet などでは SP1 を適用した Windows Xp は、Windows Server 2003 相当の netsh の機能となるという記述を見かけるが、netsh interface ipv6 add dns コマンドで IPv6 の DNS サーバを指定しても機能しない。そもそも、Windows Xp は IPv6 で DNS クエリを投げられないのである。(コマンド操作そのものは受け付けられ、ipconfig /all や netsh interface ipv6 show dns コマンドなどでも設定を確認できる。しかし、ホスト名で ping を実行しても名前解決しない。<画面 48>network モニタ等で計測しても、クエリそのものを送出していないことが判る。IPv6 アドレスでの ping は成功する。)

Windows Xp で IPv6 クエリを投げるには、次に紹介する nameproxy のような Add-on ソフトを利用する。

```
C:\WINDOWS\System32\cmd.exe
C:\>netsh int ipv6 sh dns
No entries were found.

C:\>netsh int ipv6 add dns LAN 2004::208
OK

C:\>netsh int ipv6 sh dns
DNS Servers on Interface: LAN
-----
Index  DNS Server
-----
1     2004::208

C:\>ping wswlab011.labidg.co.jp
Ping request could not find host wswlab011.labidg.co.jp. Please check the name and try again.

C:\>ver
Microsoft Windows XP [Version 5.1.2600]

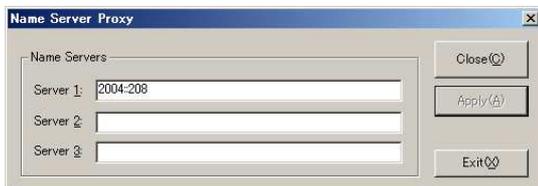
C:\>
```

Nameproxy

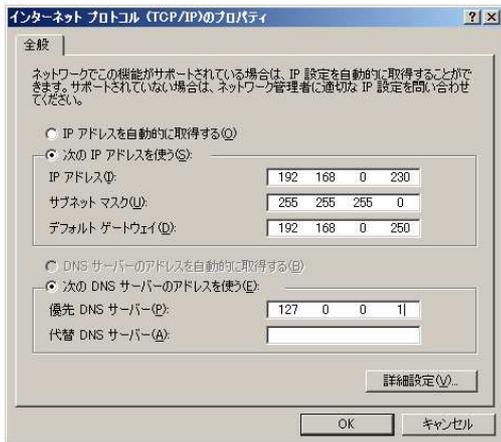
IPv6Style(http://www.ipv6style.jp/jp/statistics/ipv6win/20030120_p.shtml)でも紹介している IPv6 で DNS をひきに行くプロキシである。残念ながら現在、このページで紹介しているリンク先は別コンテンツになっており、ダウンロードできない。しかも IPv6Style で紹介している IPv6 対応ソフトウェア一覧 (Windows) の最新版 <http://www.ipv6style.jp/jp/statistics/ipv6win/index.shtml> から消えてしまっている。しかし、検索サイトで nameproxy を引くと、いくつかのサイトが引っかかるので、参照してほしい。

- どこまで IPv6 で生活できるか [Windows XP] <http://www.tumori.nu/IPv6/windowsxp.html>
- Windows での IPv6 DNS Query <http://chivas.jp/IPv6/dnsquery.html>

nameproxy は IPv4 クエリを IPv6 クエリに変換する。使用方法は簡単である。nameproxy の DNS サーバ欄に IPv6 の DNS サーバを追加するだけである。 <画面 49>

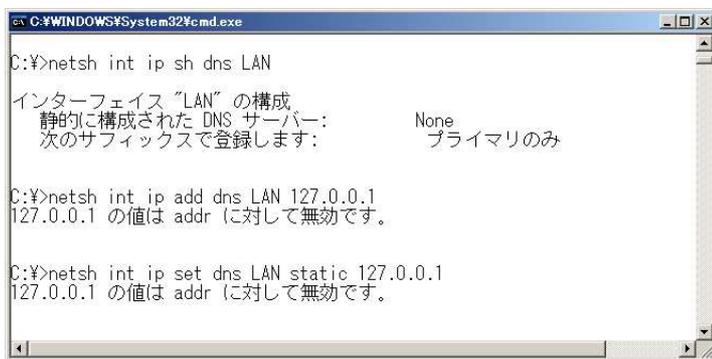


ネットワーク上の Windows Xp は、nameproxy が動作している Windows PC を DNS サーバとして設定すればよい。(ここが Proxy たる所以だ。) nameproxy が動作している Windows Xp は TCP/IP の設定画面で自分自身を DNS サーバとして設定すればよい。 <画面 50>

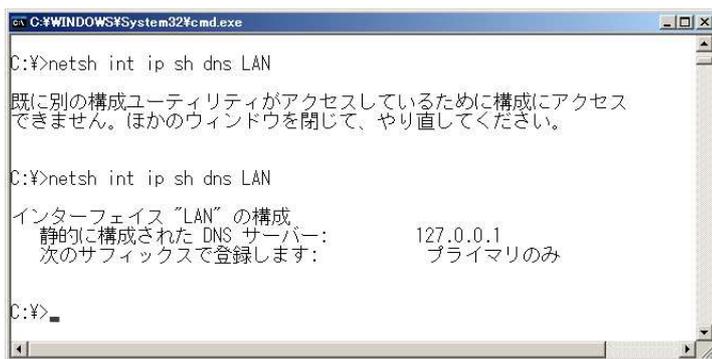


DNS サーバのエントリとして 127.0.0.1 が設定できるのは、Windows Xp 以降の OS である。しかし、
netsh interface ip add dns intfacename 127.0.0.1 コマンド
や

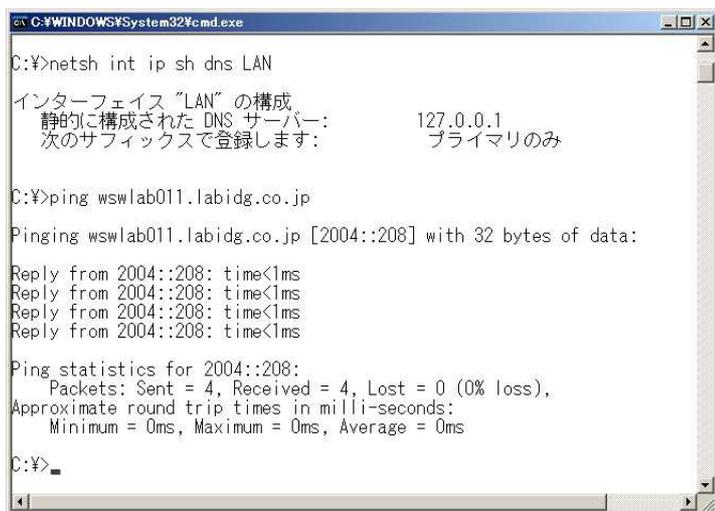
netsh interface ip set dns intfacename static 127.0.0.1 コマンド
は機能しない。設定内容を表示しても設定されていないことが確認できる。<画面 51>



ここだけは Gui の「マイネットワーク」の「プロパティ」の「TCP/IP 設定画面」に頼る。設定後は
netsh interface ip show dns コマンドで確認できるが、このとき、マイネットワークのプロパティの設
定画面が閉じていないとエラーが出る。プロパティの設定画面を閉じるとコマンドで確認可能だ。<画
面 52>



FQDN で ping を実行すると、名前解決が成功している。<画面 53>



```
C:\WINDOWS\system32\cmd.exe
C:\>netsh int ip sh dns LAN
インターフェイス "LAN" の構成
  静的に構成された DNS サーバー:      127.0.0.1
  次のサフィックスで登録します:      プライマリのみ

C:\>ping wswlab011.labidg.co.jp
Pinging wswlab011.labidg.co.jp [2004::208] with 32 bytes of data:
Reply from 2004::208: time<1ms
Reply from 2004::208: time<1ms
Reply from 2004::208: time<1ms
Reply from 2004::208: time<1ms

Ping statistics for 2004::208:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

IPv6 で IIS(HTTP サーバ)の構成

Internet Information Server

Windows Server 2003 で HTTP サーバを構成するには、さまざまな HTTP サーバーアプリケーションが公開されているが、ここでは標準の IIS(Internet Information Service)を利用する。今回は IIS のインストール・設定については触れない。

IPv6 での制限事項

MSDN のドキュメントでも Windows server 2003 はネイティブに IPv6 に対応していると書かれているが、IPv4 で使用できる機能すべてが IPv6 でも可能ということではない。IPv4 では物理サーバー一台に複数 IP アドレスを設定して仮想サイトを構築し、複数台の HTTP サーバとして利用できた。しかし、残念ながら IPv6 では仮想サイトを複数構築しても、IP アドレスがひとつしか与えられないので、ひとつのサイトのみを IPv6 の HTTP サイトとして公開できる。

アドレス設定

IIS を IPv6 アドレスで利用するに当たって、IPv4 と異なるところは一ヶ所、IPv6 アドレスで利用するサイトのアドレス設定のみである。IPv4 環境で IIS を運用する場合、IP アドレスを複数用意することで、一台の物理サーバで複数の web サイトが構築できた。FQDN も複数付与可能である。しかし、IPv6 では IP アドレスがひとつしか与えられない。仮想サイトを複数構築しても、そのうち IPv6 でアクセス可能なサイトはひとつのみとなる。なぜならば、標準のインターネットインフォメーションサービスマネージャーでは、IPv6 のアドレスを任意の仮想 web サイトに設定できないからである。IPv6 アドレスでアクセスさせたい web サイトの IP アドレス設定は、(未使用の IP アドレスすべて)という設定にする。<画面 54>



どうやら、明示的に IPv4 のアドレスを設定すると、IPv6 のアドレスでアクセスできなくなるらしい。<画面 55>

```

C:\W\NT\system32\cmd.exe
C:\>netstat -n -p TCPv6 -a

Active Connections

Proto Local Address          Foreign Address        State                   Count
TCP   [::]:53                [::]:0                LISTENING               0
TCP   [::]:80                [::]:0                LISTENING               0
TCP   [::]:135               [::]:0                LISTENING               0
TCP   [::]:443               [::]:0                LISTENING               0
TCP   [::]:445               [::]:0                LISTENING               0
TCP   [::]:1025              [::]:0                LISTENING               0
TCP   [::]:1026              [::]:0                LISTENING               0
TCP   [::]:1027              [::]:0                LISTENING               0
TCP   [::]:1030              [::]:0                LISTENING               0
TCP   [::]:1034              [::]:0                LISTENING               0
TCP   [::]:1035              [::]:0                LISTENING               0
TCP   [::]:1036              [::]:0                LISTENING               0
TCP   [::]:1038              [::]:0                LISTENING               0
TCP   [::]:2169              [::]:0                LISTENING               0
TCP   [::]:445               [::]:1034             ESTABLISHED             0
TCP   [::]:1034              [::]:445             ESTABLISHED             0
TCP   [2004::208]:53        [::]:0                LISTENING               0
TCP   [fe80::1%1]:53        [::]:0                LISTENING               0
TCP   [fe80::208:c7ff:feac:845f%4]:53 [::]:0                LISTENING               0
TCP   [fec0::1:208:c7ff:feac:845f%1]:53 [::]:0                LISTENING               0

```

これまでの設定で IIS を IPv6 で公開する準備はできた。IPv4 との相違は、アドレスの設定のみである。イントラネット上に既に IPv4 で公開している IIS があれば、必要ならばアドレスの設定を変更するだけで、IPv6 対応にできる。

IPv6 での web ブラウズ

次に HOSTS ファイル、もしくは、DNS サーバに web サーバのエントリを作り、ホスト名で web サーバにアクセスできるようにする。

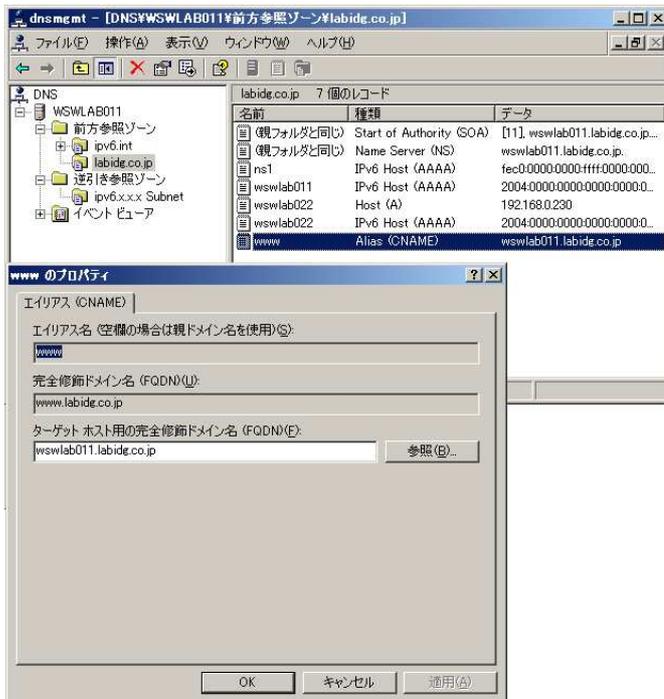
HOSTS ファイルは、%systemroot%\system32\drivers\etc に存在する。コマンドプロンプトもしくは「ファイル名を指定して実行」から、notepad %systemroot%\system32\drivers\etc\HOSTS で編集可能だ。

```

hosts - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97   rhino.acme.com   # source server
#       38.25.63.10  x.acme.com       # x client host
#
127.0.0.1           localhost
2004::208           www.labidg.co.jp

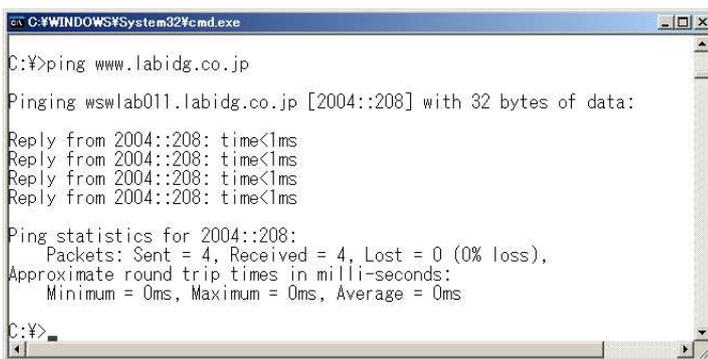
```

<画面 56>



<画面 57>

作成したエントリで名前解決ができているかどうかを、ping で確認してみる<画面 58>



疎通確認ができれば、「ファイル名を指定して実行」に `http://www.labidg.co.jp/` と入力して実行する。)



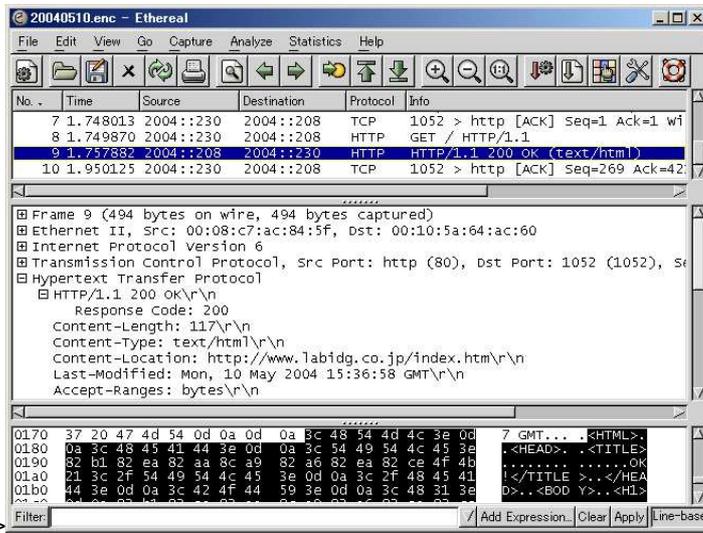
<画面 59>

web ブラウザで表示できれば OK だ。(確認用のページは前もって用意しておくこと



<画面 60>

Ethereal でキャプチャしてみた。IPv6 でアクセスしていることがわかる。



<画面 61>

Windows Xp の IPv6 で ping が失敗するときは…

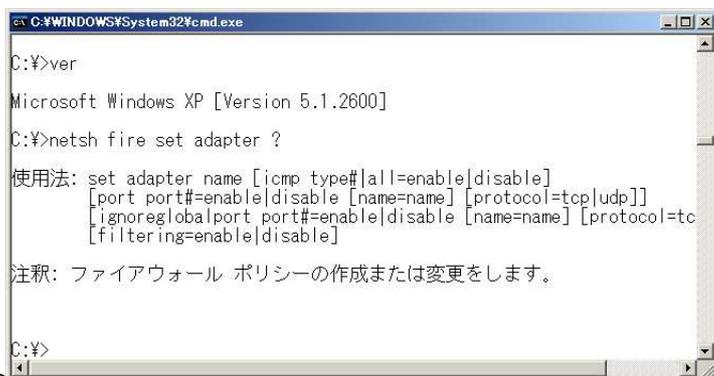
firewall 設定

Windows Update と service Pack

2003 年の 7 月に脆弱性として *Microsoft* が発表していたにもかかわらず、一ヵ月後の 8 月に MSBlaster が大発生した。このことを教訓として *Microsoft* はデフォルトセキュアの一環で、IPv6 の Firewall をデフォルト ON に設定した。Windows Update をまめに適用していると、filtering 設定だけでなく ICMP 設定がデフォルトでかかるようになる。Windows Xp を 2004 年 04 月 14 日現在の最新状態にすると、次のコマンドを実行して設定変更しないと ping が失敗する。

- netsh firewall set adapter LAN filtering=disable
- netsh firewall set adapter LAN icmp all=enable

まずは、? で訊いてみると良い。



```
C:\WINDOWS\System32\cmd.exe
C:\>ver
Microsoft Windows XP [Version 5.1.2600]
C:\>netsh fire set adapter ?
使用法: set adapter name [icmp type#[all=enable|disable]
[port port#=enable|disable [name=name] [protocol=tcp|udp]]
[ignoreglobalport port#=enable|disable [name=name] [protocol=tc
[filtering=enable|disable]
注釈: ファイアウォール ポリシーの作成または変更をします。
C:\>
```

<画面 62>

```

C:\>netsh fire sh adapter

-----
AdapterFriendlyName      IPV6FilteringEnabled
-----
Teredo Tunneling Pseudo-Interface   はい
LAN                                  はい
6to4 Pseudo-Interface              はい
Automatic Tunneling Pseudo-Interface はい

C:\>netsh fire sh adapter LAN

Description      EffectivePort  Protocol
-----
Description      OpenPort      Protocol
-----
Description      IgnoredGlobalPort Protocol
-----

Description      ICMPTypeNo  Enabled
-----
到達不可能な送信宛先を許可する          1          いいえ
送信パケットが大きすぎることを許可する  2          いいえ
送信時間の超過を許可する                3          いいえ
送信するパラメータの問題を許可する      4          いいえ
着信エコー要求を許可する                128        いいえ
リダイレクトを許可する                  137        いいえ

C:\>

```

<画面 63>

```

C:\>netsh fire set adapter LAN filtering=disable

C:\>netsh fire set adapter LAN icmp all=enable

C:\>netsh fire sh adapter

-----
AdapterFriendlyName      IPV6FilteringEnabled
-----
Teredo Tunneling Pseudo-Interface   はい
LAN                                  いいえ
6to4 Pseudo-Interface              はい
Automatic Tunneling Pseudo-Interface はい

C:\>netsh fire sh adapter LAN

Description      EffectivePort  Protocol
-----
Description      OpenPort      Protocol
-----
Description      IgnoredGlobalPort Protocol
-----

Description      ICMPTypeNo  Enabled
-----
到達不可能な送信宛先を許可する          1          はい
送信パケットが大きすぎることを許可する  2          はい
送信時間の超過を許可する                3          はい
送信するパラメータの問題を許可する      4          はい
着信エコー要求を許可する                128        はい
リダイレクトを許可する                  137        はい

C:\>

```

<画面 64>

icmp に関しては、パッチ適用のタイミングもあるのだろうが、デフォルトで enable の場合もあるようだ。もし ping その他の通信に失敗するようであれば、この firewall filtering 設定を確認してみよう。

Windows Xp の IPv6 で ping が失敗するときは… (2)

設定してはいけないインターフェース ID

2000:111:fe40:0:ffff::45fc (例)

IPv6 は通常、64bit のプリフェックスで皆さんの前に姿をあらわす。プリフェックスとはネットワーク ID のことだ。IPv6 アドレスは 128bit だから、残りの 64bit がインターフェース ID となる。ネットワーク設計者やネットワーク管理者ならば、通常はこの 64bit のインターフェース ID に重複のない数値をアドレスとして自由に設計できるはずである。しかし、64bit のインターフェース ID の先頭の 16bit を全て ffff とし、次の 32bit を 0000:0000 とすると、Windows では通信出来ない。

この 64bit のインターフェース ID の先頭の 16bit を全て ffff とし、次の 32bit を 0000:0000 とするアドレスを持った TCP/IP ホストに対して、Windows PC が ping を実行する様を、Ethereal などのネットワークモニターで計測すると、reply が届いているにもかかわらず、Windows はこれを無視し、Request time out を表示する。

逆に、64bit のインターフェース ID の先頭の 16bit を全て ffff とし、次の 32bit を 0000:0000 とするアドレスを持った TCP/IP ホストから、Windows PC に対して ping を実行する様を、Ethereal などのネットワークモニターで計測すると、request が届いているにもかかわらず、Windows はこれを無視する。

Windows PC に 64bit のインターフェース ID の先頭の 16bit を全て ffff とし、次の 32bit を 0000:0000 とするアドレスを設定し、自分自身に対して ping を実行しても、Request time out を表示する。

他の OS ではどうかというと、一般的な IPv6 対応のルータや Linux や Unix 互換のコンピュータなどのネットワーク機器では、インターフェース ID の先頭の 16bit を全て ffff とし、次の 32bit を 0000:0000 としても、問題なく使用できる。なぜか、Windows だけダメである。

```
netsh int ipv6 add address intfacename xxxx:xxxx:xxxx:xxxx:ffff::xxxx
```

この設定をして、己自身やリモート PC から、このアドレスに対して ping してみたい。必ずや失敗するはずである。<画面 65>

コメント [W2]: 操作内容と評価を説明するために、画面 65-2 を用意しています。

```
C:\WINDOWS\system32\cmd.exe
C:\>netsh int ipv6 add ad LAN 2000::230
OK
C:\>netsh int ipv6 add ad LAN 2000::ffff:100:1:230
OK
C:\>netsh int ipv6 add ad LAN 2000:100:0:1:ffff::230
OK
C:\>netsh int ipv6 sh ad LAN nor
Querying active state...

Interface 4: LAN
-----
Addr Type DAD State Valid Life Pref. Life Address
-----
Manual Preferred infinite infinite 2000::ffff:100:1:230
Manual Preferred infinite infinite 2000:100:0:1:ffff::230
Manual Preferred infinite infinite 2000::230
Temporary Preferred 6d13h29m7s 13h29m30s 2004::cff:6eb:4e13:d933
Public Preferred infinite infinite 2004::210:5aff:fe64:ac60
Public Preferred infinite infinite fe80::1:210:5aff:fe64:ac60
Link Preferred infinite infinite fe80::210:5aff:fe64:ac60
No entries were found.

C:\>ping fe80::210:5aff:fe64:ac60
Pinging fe80::210:5aff:fe64:ac60 with 32 bytes of data:
Reply from fe80::210:5aff:fe64:ac60: time<1ms
Reply from fe80::210:5aff:fe64:ac60: time<1ms
Reply from fe80::210:5aff:fe64:ac60: time<1ms
Reply from fe80::210:5aff:fe64:ac60: time<1ms
Ping statistics for fe80::210:5aff:fe64:ac60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2000::230
Pinging 2000::230 with 32 bytes of data:
Reply from 2000::230: time<1ms
Reply from 2000::230: time<1ms
Reply from 2000::230: time<1ms
Reply from 2000::230: time<1ms
Ping statistics for 2000::230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2000::ffff:100:1:230
Pinging 2000::ffff:100:1:230 with 32 bytes of data:
Reply from 2000::ffff:100:1:230: time<1ms
Reply from 2000::ffff:100:1:230: time<1ms
Reply from 2000::ffff:100:1:230: time<1ms
Reply from 2000::ffff:100:1:230: time<1ms
Ping statistics for 2000::ffff:100:1:230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 2000:100:0:1:ffff::230
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 2000:100:0:1:ffff::230:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

アドレスを追加

アドレス状態を確認

追加したアドレス2000::230にping

追加したアドレス2000::ffff100:1:230にping

追加したアドレス2000:100:0:1:ffff::230にping

Replyがない

リンクローカルアドレスでは成功する。2000::230 は OK、2004::ffff:100:1:230 でも OK だ。
2000:100:0:1:ffff::230 では失敗する。

今回使用した IPv6 アドレスについて

本記事で使用したアドレスはグローバルアドレスの範囲にある。本来ならば ISP から割り振られるアドレスである。アドレスの重複を避ける為にも、グローバルな範囲のアドレスを勝手に使用してインターネットに接続するようなことがあってはならない。本記事執筆時は、あくまで実験室内に閉じられた環境でインターネットに接続はしていない環境である。

IPv4 のプライベートアドレスのように使用できるアドレスが IPv6 にも存在する。それは FEC0::1 から始まるのサイトローカルアドレスである。各サイト内で一意になるように設定する。

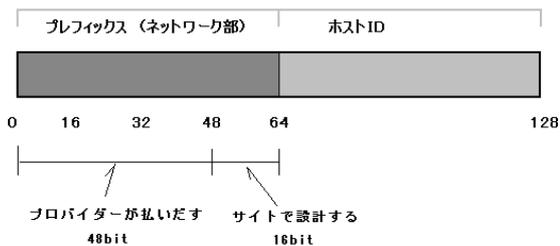
しかし、IPv6 のアドレスは全 IP ホストにグローバルユニキャストアドレスを割り振ることができるのがメリットである。そうするとサイトローカルアドレスがどの程度利用されるかは、まったく予想がつかない。

実際、IETF では、

- ① 「サイト」の定義のむずかしさ、
- ② 2つの「サイト」の境界ルーターの扱い、
- ③ NAT 利用の問題

という理由から、廃止されることがほぼ決定している。そしてそのための RFC も改定作業中らしい。また、プロバイダーに接続前に使う等の用途のために、グローバルにユニークな新サイトローカルアドレスが検討中らしい。

少なくとも ISP は、ユーザーがネットワークの場合グローバルアドレスを 48bit で払い出し、サイトの管理者はさらに 16bit を設計し、/64 でホストにアドレスを設定する。<画像 2> ISP はホストに対しては 64bit で払い出す。グローバルアドレスで通信可能ならば、サイトローカルをわざわざ使用する意味はない。



ISP が払い出す 48 のアドレスもさらに上位の組織が管理している。IPv6 アドレス空間の割り当ては <http://www.iana.org/assignments/ipv6-address-space> を参照すること。また TLA … Top Level Aggregation については、<http://www.iana.org/assignments/ipv6-tla-assignments> を参照すること。アドレスポリシーについては、<http://www.iana.org/ipaddress/ipv6-allocation-policy-26jun02> を参照すること。ISP がどのアドレスを受け持っているかは、<http://www.ripe.net/cgi-bin/ipv6alloc> を参照すること。