

BackOffice 原稿(2回目)

「入門・ビギナーのためのネットワークトラブル対策」

奥川博司

今回は前回に続いて、Windows NT が標準で備えているネットワーク系のコマンドラインユーティリティの中から ipconfig、route、nslookup、netstat という4つのコマンドについて説明していきたいと思います。

ipconfig

ipconfig コマンドは、IP Configuration を縮めたもので TCP/IP に関連したネットワークの設定値の表示および、DHCP によって構成されている設定内容の解除や再割り当てなどを行うことができます。

オプションを設定せずに実行した場合は、現在の IP アドレスやサブネットマスク、ゲートウェアアドレスを簡潔に表示しますが、ipconfig /all というように all オプションを付けて実行することで詳細な設定内容を表示することができます。(ネットワークコントロールパネルの TCP/IP のプロパティを参照することでも確認できますが、ipconfig コマンドでは一度に全ての情報を表示できるので便利です。また ipconfig /all >memo.txt とすれば設定値をファイルに保存することもできます) 実行画面を図1に示します。

```

C:\WINNT\system32\CMD.EXE
Microsoft (R) Windows NT (R)
(C) Copyright 1985-1996 Microsoft Corp.

O:\WINNT\system32>ipconfig /all

Windows NT IP Configuration

Host Name . . . . . : jinro.tcs.sirius.co.jp
DNS Servers . . . . . : 202.232.2.38
                   : 202.232.2.39
Node Type . . . . . : Hybrid
NetBIOS Scope ID. . . . . :
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
NetBIOS Resolution Uses DNS : No

Ethernet adapter E190x1:

Description . . . . . : 3Com 3C90x Ethernet Adapter
Physical Address. . . . . : 00-60-97-7F-91-59
DHCP Enabled. . . . . : No
IP Address. . . . . : 10.40.40.1
Subnet Mask . . . . . : 255.0.0.0
Default Gateway . . . . . : 10.0.0.100
Primary WINS Server . . . . . : 10.0.0.8

O:\WINNT\system32>
  
```

図1 .ipconfigの実行画面

表示されている項目を簡単に説明していきます。

Windows NT IP Configuration

Host Name:ホスト名

DNS Server : DNS サーバのアドレス

Node Type: ノードタイプ(どのようなタイプがあるかは表1を参照)

NetBIOS Scope ID:NetBIOS スコープ ID

IP Routing Enabled:IP ルーティングが有効かどうか

WINS Proxy Enabled:WINS の代理サーバ機能が有効かどうか

NetBIOS Resolution Use DNS : Windows の名前解決に DNS を使うかどうか

Ethernet adapter

Description: ネットワークアダプタの説明

Physical Address: ネットワークカードの MAC アドレス

DHCP Enabled:DHCP が有効かどうか

IP Address:IP アドレス

Subnet Mask: サブネットマスク

Default Gateway: デフォルトゲートウェイ

Primary WINS Server: プライマリ WINS サーバの IP アドレス

DHCP を有効にしている場合には、このほかに DHCP サーバのアドレスや、DHCP サーバより割り当てられた IP アドレスのリース権取得日(Lease Obtained)やリース権期限(Lease Expires)なども表示されます。

このように ipconfig コマンドの利点はネットワークに関係する諸設定を一度に参照できる点にあります。うまくサーバに接続できない場合などにサブネットアドレスの値が間違っていたりすることがあるので、このコマンドを利用して正しく設定されているかどうかを確認してみてください。

Windows 95には、ipconfig というコマンドは用意されていませんが代わりに winipcfg という GUI 版のツールがあります。Windows 98では、ipconfig、winipcfg 共に用意されています。winipcfg の実行画面を図2に示します。

表1 .NetBIOSのノードタイプ一覧

タイプ	説明
Broadcast	b ノード 名前登録、名前解決にブロードキャストを使用
Peer-Peer	p ノード 名前登録、名前解決に NetBIOS ネームサーバへのポイントツーポイントの名前紹介を使用
Mixed	m ノード 名前登録、名前解決にまずブロードキャストを使用。ブロードキャストによる名前解決で応答が無かったときは NetBIOS ネームサーバを使用
Hybrid	h ノード 名前登録、名前解決にまず NetBIOS ネームサーバを使用。失敗した場合はブロードキャストを使用

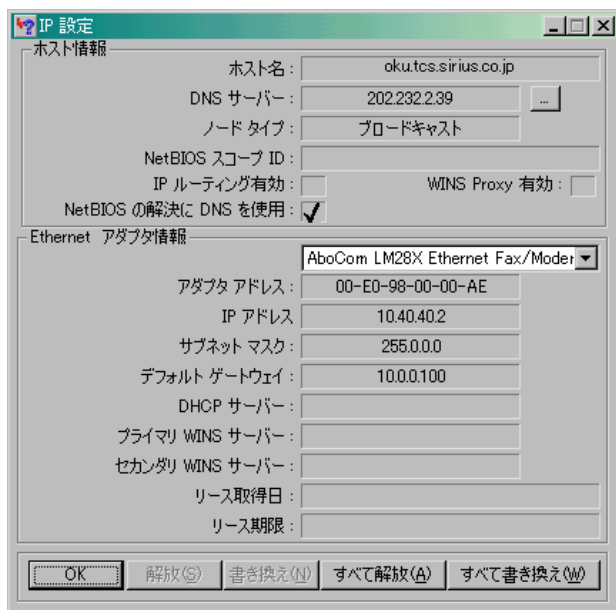


図 2 .winipcfgの実行画面

サブネットアドレスの設定間違いについて

サブネットアドレスを間違えている場合でも相手も特定されている(既に相手の IP アドレスがわかっている)ときは、通信が可能なのですが、ブロードキャストにて名前解決を行う場合などサブネットマスクが間違っていると送られてきたブロードキャストパケットを正しくブロードキャストパケットとして認識できなったり、ブロードキャストパケットを送信しても他のマシンはそれをブロードキャストとして認識してくれないことがあるので注意が必要です。

例えば、正しいサブネットマスクが 255.0.0.0 のネットワークにて 255.255.255.0 という設定されているマシンがいるとそのマシンはブロードキャストパケットして(仮にそのマシンの IP アドレスが 10.40.40.1 とすると) 10.40.40.255 というあて先のパケットを送信しますが、正しく設定されているマシンにとっては 10.255.255.255 というアドレスが正しいブロードキャストパケットとなるので、10.40.40.255 というアドレスでは、無視されてしまったりします。この場合はその端末が通信できないだけでなく、役に立たないパケットが送信されているためネットワーク全体に対して悪影響を与えていることにもなってしまいます。

route

route コマンドは、TCP/IP のルーティングテーブルの表示や変更などを行うために使用します。小規模なネットワークの場合はほとんど利用する機会はありませんが、サブネットによって分割されたネットワークや Windows NT Server でルーティングを行う場合には知っておいたほうが良いでしょう。

ルーティングテーブルを表示するためには route print と入力します。実行画面を図 3 に示します。

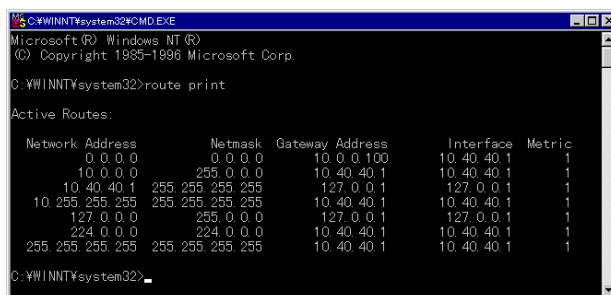


図 3 . route コマンドの実行画面

ルーティングテーブルの表示では、ネットワークアドレス (Network Address) と、ネットマスク (Netmask) を組み合わせることであて先の範囲を表しています。見方はビットで見た場合 1 が立っていると一致している必要があり、0 では一致していなくてよいことになっています。例えば一番上の行にある 0.0.0.0 と 0.0.0.0 の組み合わせでは全てのネットマスクが 0 ですので、0~255.0~255.0~255.0 という風に全てのあて先を含むこととなり他のアドレステーブルによって解決されなかったあて先の場合には、この行で設定されているゲートウェイアドレス (Gateway Address) である 10.0.0.100 に向かって送信されることになります。

次の行では 10.0.0.0 と 255.0.0.0 の組み合わせですので、最初の 10 は、一致している必要がありますつまり 10.0~255.0~255.0~255 の範囲に含まれるあて先へのパケットは 10.40.40.1 に向かって送信されるわけです。

ゲートウェイアドレスには、ローカルネットワークカードあるいは、ローカルサブネット上のゲートウェイが指定されます。前出の例で言うと 10.0.0.100 はローカルサブネット上のゲートウェイ、10.40.40.1 はローカルネットワークカードです。

4 列目に表示されている インターフェイス (Interface) は、ゲートウェイアドレスにパケットを送信する際に経由するネットワークカードのアドレスです。

ネットワークカードを一枚しか挿していないにも関わらず 2 つのアドレスが表示されていますが、127.0.0.1 はソフトウェアループバックを表す特殊なネットワークアドレスです。

5 列目に表示されている メトリック (Metric) は、あて先であるアドレスに到達するために越えるルータの数 (ホップ数) です。外部に接続しているルータなどでルーティングテーブルを参照した場合は 2 以上のメトリックを見ることができるとありますが、LAN にて通常使用しているマシンではデフォルトゲートウェイさえ指定しておけば事が足りるためメトリックは 1 のみの場合がほとんどです。このメトリックは効率のよいルートを決断するために使用されます。

ルーティングテーブルにルートを追加したり削除する場合は add や delete といったオプションを使用します。利用する機会は通常は無いと思いますので、ここでは説明を省略しますが必要に応じてヘルプなどを参照してください。

nslookup

nslookup コマンドは、DNS サーバに問い合わせることで、DNS によって管理されている様々な情報を表示することができます。DNS サーバの設定を行った後の動作確認や、名前解決が正常にできなくなった場合に原因を調べるため いわば DNS サーバの動作をデバッグするためなどに用いられます。このコマンドは多くのパラメータオプションが用意されているため使い方が難しく感じられるかもしれませんがここではより多くの情報を指定した DNS サーバから得て表示するオプションでの利用例を示します。

nslookup -querytype=ANY cqpub.co.jp

という風に、問い合わせ種別(QueryType)として全てのデータタイプ(ANY)を指定し その後ろにサーバ名を書いて実行します。

複数のサーバの情報を問い合わせたい場合は、対話モードを利用すると便利です。

オプションを指定せずに nslookup と入力して実行すれば '>' というプロンプトが表示される対話モードとなりますので set querytype=ANY として問い合わせ種別を設定したのち '>' のところで サーバ名を入力すれば問い合わせが実行されます。対話モードを終了するには '>' にて exit を入力するか、[Ctrl]+[C] を押してください。

実行画面を図 4 に示します。

```

C:\WINNT\system32\CMD.EXE - nslookup
C:\WINNT\system32>nslookup -querytype=ANY cqpub.co.jp
Server: ns4.iij.ad.jp
Address: 202.232.2.38

Non-authoritative answer:
cqpub.co.jp
  primary name server = keikasun.cqpub.co.jp
  responsible mail addr = yoshida.hibika.iinc.or.jp
  serial = 1998051801
  refresh = 10800 (3 hours)
  retry = 3600 (1 hour)
  expire = 3600000 (41 days 16 hours)
  default TTL = 86400 (1 day)
cqpub.co.jp MX preference = 20, mail exchanger = BSD1.cqpub.co.jp
cqpub.co.jp MX preference = 10, mail exchanger = exchange.cqpub.co.jp
cqpub.co.jp nameserver = keikasun.cqpub.co.jp
cqpub.co.jp nameserver = ns.tokyonet.ad.jp
cqpub.co.jp nameserver = soho-ocn.cqpub.co.jp

cqpub.co.jp nameserver = keikasun.cqpub.co.jp
cqpub.co.jp nameserver = ns.tokyonet.ad.jp
cqpub.co.jp nameserver = soho-ocn.cqpub.co.jp
BSD1.cqpub.co.jp internet address = 202.218.30.80
exchange.cqpub.co.jp internet address = 202.218.30.17
keikasun.cqpub.co.jp internet address = 202.218.30.25
ns.tokyonet.ad.jp internet address = 202.239.61.61

C:\WINNT\system32>nslookup
Default Server: ns4.iij.ad.jp
Address: 202.232.2.38

> set querytype=ANY
> cqpub.co.jp
  
```

図 4. nslookup コマンドの実行画面

全てのデータタイプを設定した場合 図 4 のように、プライマリネームサーバやメールサーバのアドレス 公開されているホスト名および IP アドレスなどを表示することができます。

このコマンドは Windows 95/98 には用意されていません。

netstat

netstat コマンドは、TCP/IP の通信に関する統計情報や接続情報などを表示することができます。netstat としてオプションを指定せずに実行した場合は、そのコマンドを実行したマシンからサーバに接続している情報(クライアント接続)について表示することができます、サーバ接続も含めて表示したい場合は netstat -a という風に -a オプションを指定して実行します。実行画面を図 5 に示します。

```

C:\WINNT\system32\CMD.EXE
C:\WINNT\system32>netstat

Active Connections

Proto Local Address Foreign Address State
TCP jinro:1580 VODKA:nbsession ESTABLISHED
TCP jinro:1025 localhost:1026 ESTABLISHED
TCP jinro:1026 localhost:1025 ESTABLISHED

C:\WINNT\system32>netstat -a

Active Connections

Proto Local Address Foreign Address State
TCP jinro:1026 0.0.0.0:0 LISTENING
TCP jinro:telnet 0.0.0.0:0 LISTENING
TCP jinro:smtp 0.0.0.0:0 LISTENING
TCP jinro:pop3 0.0.0.0:0 LISTENING
TCP jinro:135 0.0.0.0:0 LISTENING
TCP jinro:135 0.0.0.0:0 LISTENING
TCP jinro:1580 0.0.0.0:0 LISTENING
TCP jinro:1580 VODKA:nbsession ESTABLISHED
TCP jinro:137 0.0.0.0:0 LISTENING
TCP jinro:138 0.0.0.0:0 LISTENING
TCP jinro:nbsession 0.0.0.0:0 LISTENING
TCP jinro:1025 0.0.0.0:0 LISTENING
TCP jinro:1025 localhost:1026 ESTABLISHED
TCP jinro:1026 localhost:1025 ESTABLISHED
UDP jinro:1573 *.*
UDP jinro:135 *.*
UDP jinro:nbname *.*
UDP jinro:nbdatagram *.*

C:\WINNT\system32>
  
```

図 5. netstat コマンドの実行画面

一列目から順にその意味を説明していくと、Proto は接続に使用されているプロトコルが表示されています。2 列目の Local Address には、ローカルコンピュータの名前(名前が解決できなかったり -n オプションが指定されている場合は IP アドレス)^{*1} と サービス名(あるいはポート番号)^{*2}、3 列目の Foreign Address には、接続されているリモートコンピュータの名前(あるいは IP アドレス)と ポート名(あるいはポート番号)が、4 列目の State には TCP 接続の状態が表示されています。TCP 接続状態には表 2 に示すようなものがあります。

画面中央付近の Local Address に表示されている telnet や smtp、pop3 などのサービスがクライアントからの接続待機状態(LISTENING)になっておりサーバとして正常に動作しているのを見て取ることができます。

なお、ポート番号が 1024 ~ 5000 のものはサーバへの接続が確立された後の通信のために一時的利用されているケースが多いため利用されているポート番号自体にはあまり意味はありません

*1 IP アドレスの名前解決には DNS や %SystemRoot%\System32\Drivers\Etc\Hosts ファイルが使用されます

*2 ポート番号からのサービス名の解決には %SystemRoot%\System32\Drivers\Etc\Services ファイルが参照されます。このファイルを編集しておくことでなるべく多くのポート番号をポート名にて表示することが可能になるので分かり易い表示結果を得ることも可能です

ん。

Web サーバにアクセスしているときに、netstat コマンドを実行すれば多くの接続が表示されるので直感的にこのコマンドの利用例が分かると思います。この場合 Foreign Address の項目に 接続先のアドレスと WWW のポート番号である 80 が表示されていることと思います。

また、サーバの電源をオフにする前などに netstat コマンドを実行することで接続中のクライアントが存在するかどうかを調べるといった使い方もできます。

netstat コマンドには他にも ルーティングテーブルを表示する -r オプションや、プロトコル毎のパケットの送受信量やエラー数などの統計情報を表示する -s オプションなどもあります、

netstat -s の実行画面を図 6 に示しておきます。

表 2 . TCP接続の状態一覧

状態	説明
CLOSED	切断状態
LISTENING	接続要求待ち
SYN_SENT	接続要求送信
SYN_RECEIVED	接続要求受信
ESTABLISHED	接続状態
FIN_WAIT_1	切断要求待ち 1
FIN_WAIT_2	切断要求待ち 2
CLOSE_WAIT	切断待ち状態
CLOSING	切断中
LAST_ACK	最終応答待ち
TIME_WAIT	時間待ち

```

C:\WINNT\system32\CMD.EXE
C:\WINNT\system32>netstat -s

IP Statistics
Packets Received           = 47118
Received Header Errors     = 30
Received Address Errors    = 0
Datagrams Forwarded        = 0
Unknown Protocols Received = 0
Received Packets Discarded = 0
Received Packets Delivered  = 47088
Output Requests            = 16669
Routing Discards           = 0
Discarded Output Packets    = 0
Output Packet No Route     = 0
Reassembly Required        = 0
Reassembly Successful      = 0
Reassembly Failures        = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created          = 0

ICMP Statistics
                Received  Sent
Messages         148    177
Errors             1      0
Destination Unreachable 66      0
Time Exceeded     0      0
Parameter Problems  0      0
Source Quenches   0      0
Redirects          0      0
Echoes            2     175
Echo Replies      79      2
Timestamps        0      0
Timestamp Replies  0      0
Address Masks     0      0
Address Mask Replies  0      0

TCP Statistics
Active Opens      = 154
Passive Opens     = 6
Failed Connection Attempts = 1
Reset Connections = 77
Current Connections = 3
Segments Received = 12917
Segments Sent     = 13913
Segments Retransmitted = 5

UDP Statistics
Datagrams Received = 28116
No Ports           = 6053
Receive Errors     = 0
Datagrams Sent     = 2574

```

図 6 . netstat コマンドの実行画面

__ ipconfig

この診断コマンドは、現在の TCP/IP ネットワーク構成値をすべて表示します。特に、このコマンドを DHCP を実行するシステムで使えば、DHCP を使用して構成した TCP/IP 構成値がどれであるかを突き止めることができます。

```
ipconfig [/all | /renew [アダプタ] | /release [アダプタ]]
```

パラメータ

all

構成値をすべてを表示します。このスイッチがないと、ipconfig が表示するのは、各ネットワークカードの IP アドレス、サブネットマスク、およびデフォルトゲートウェイの値のみです。

```
/renew [アダプタ]
```

DHCP 構成パラメータを更新します。このオプションは、DHCP Client サービスを実行するシステムでのみ使用できます。アダプタ名を指定するために、パラメータなしで ipconfig を使ったとき表示されるアダプタ名を入力します。

```
/release [アダプタ]
```

現在の DHCP 構成を解除します。このオプションは、ローカルシステム上で TCP/IP を使用不能にし、DHCP クライアント上でのみ使用できるようにします。アダプタ名を指定するために、

パラメータなしでipconfigを使ったとき表示されるアダプタ名を入力します。

パラメータを指定しないと、ipconfigユーティリティは、ユーザーに対し、IPアドレスとサブネット マスクを含むすべての現在のTCP/IP構成値を表示します。特に、このユーティリティをDHCPを実行するシステムで使えば、DHCPを使用して構成した値がどれであるかを突き止めることができます。

__ Route

ネットワーク ルーティング テーブルを取り扱います。このコマンドはTCP/IPプロトコルがインストールされている場合のみ有効です。

```
route [-f] [-p] [コマンド [送信先] [maskサブネットマスク]
[ゲートウェイ] [metricコストメトリック]]
```

パラメータ

-f

すべてのゲートウェイ エントリのルーティング テーブルを消去します。コマンドとともにこのパラメータを指定すると、テーブルが消去されてからそのコマンドが実行されます。

-p

addコマンドとともに使用すると、システムの起動を繰り返してもルート (経路) が変わらないようにします。既定の設定では、ルートはシステムが再起動すると変わることがあります。printコマンドとともに使用すると、ルートが変わらないように登録されたルートの一覧を出力します。その他のコマンドは、指定しても無視されます。

コマンド

次の 4 つのコマンドから 1 つ指定します。

コマンド 目的

print ルートを出力します。

add ルートを追加します。

delete ルートを削除します。

change 既存のルートを修正します。

送信先

コマンドの送信先となるコンピュータを指定します。

maskサブネットマスク

このルート エントリと関連付けられるサブネット マスクを指定します。指定されない場合、255.255.255.255 が使われます。

ゲートウェイ

ゲートウェイを指定します。

送信先またはゲートウェイに使うすべてのシンボリック名は、それぞれネットワークおよびコンピュータ名データベース ファイルNETWORKSおよびHOSTSの中で検索されます。コマンドがprintまたはdeleteであれば、送信先とゲートウェイにワイルドカードを使用するか、またはゲートウェイ引数を省略できます。

metricコストメトリック

最も高速で、信頼性が高く、コストの低いルートを算出するのに使われるコストメトリック整数 (1 から 9999 の範囲) を指定します。

__ Nslookup

この診断ツールは、DNS (ドメイン ネーム システム) ネーム サーバーからの情報を表示します。このツールを使うには、DNSの働きを理解している必要があります。このコマンドは、TCP/IPプロトコルがインストールされている場合のみ利用できます。

```
nslookup [-オプション...] [対象コンピュータ] [- [サーバー]]
```

モード

Nslookupには、対話型モードと非対話型モードの 2 つのモードがあります。

問い合わせるデータが 1 つだけの場合は、非対話型モードを使います。第 1 の引数には、照合したい対象のコンピュータの名前またはIPアドレスを指定します。第 2 引数には、DNSネーム サーバーの名前またはIPアドレスを指定します。第 2 引数を省略すると、既定 (デフォルト) のDNSネーム サーバーが使われます。

複数の情報を問い合わせる場合は、対話型モードを使います。第 1 引数にはハイフン (-) を指定し、第 2 引数にはDNSネーム サーバーの名前またはIPアドレスを指定します。または、両方の引数を省略します (既定のDNSネーム サーバーが使われます)。

パラメータ

-オプション...

コマンドラインのオプションとして、1 つまたは複数の

nslookupコマンドを指定します。コマンドの一覧については、Nslookupコマンドを参照してください。それぞれのオプションは、ハイフン (-) とコマンド名からなります。場合によっては、コマンド名の後に等号 (=) と値が続きます。たとえば、既定の問い合わせの種類をホスト (コンピュータ) 情報に変更し、初期タイムアウトを 10 秒に変更するには、次のように入力します。

```
nslookup -querytype=hinfo -timeout=10
```

コマンドラインの長さは、256 文字未満でなければなりません。

対象コンピュータ

現在の既定のサーバーまたは指定したサーバーを使って、対象コンピュータについての情報を照合します。対象コンピュータにIPアドレスを指定し、問い合わせの種類にAまたはPTRを指定すると、コンピュータの名前が返されます。対象コンピュータにコンピュータ名を指定し、その後にピリオドを付けなかった場合は、コンピュータ名に既定のDNSドメイン名が付加されます (この動作は、setオプションdomains、srchlist、

defname、およびsearchの状態によって異なります)。現在のDNSドメイン内にはないコンピュータを照合するには、名前にピリオドを付加します。

対象コンピュータ名の代わりにハイフン (-) を指定すると、コマンドプロンプトはnslookupの対話型モードに変わります。

サーバー

DNSネームサーバーとして、このサーバーを使います。このパラメータを省略すると、既定のDNSネームサーバーが使われます。

__ Netstat

プロトコルの統計情報と現在のTCP/IPネットワーク接続を表示します。このコマンドはTCP/IPプロトコルがインストールされている場合のみ有効です。

netstat [-a] [-e] [-n] [-s] [-p プロトコル] [-r

] [間隔]

パラメータ

-a

すべての接続および聴取 (listening) ポートを表示します。通常は、サーバー接続を表示しません。

-e

イーサネットの統計情報を表示します。このパラメータは-sオプションと組み合わせられます。

-n

アドレスとポート番号を数値書式で (名前を検索しようとせずに) 表示します。

-s

プロトコルごとの統計情報を表示します。既定の設定では、TCP、UDP、ICMP、およびIPに関する統計情報を表示します。-pオプションを使うと、既定のサブネットを指定できます。

-pプロトコル

指定したプロトコルの接続を表示します。プロトコルとしてtcpまたはudpを指定できます。-sオプションとともに使って、プロトコルごとの統計情報を表示する場合は、プロトコルとしてtcp、udp、icmp、またはipを指定できます。

-r

ルーティングテーブルの内容を表示します。

間隔

指定した秒間隔で、選択した統計情報を再表示します。統計情報の再表示を停止するには、Ctrl + Cキーを押します。このパラメータが省略されると、netstatは、現在の構成情報を一度だけ印刷します。

__ 参考文献

Microsoft Windows NT 4.0 Server ネットワーキングガイド アスキー出版局
OPEN DESIGN No.3 CQ 出版社
Windows NT ヘルプファイル