Part 1 ネットワークトラブルの原因究明と解決に大活躍！ 厳選！ 使える 基本コマンド&モニタツール

Part1では、トラブルシューティングに必須の基本コマンドとネットワークモニタについて解説する。5つの基本コマンドの目的や利用法を習得すれば、原因不明のネットワークトラブルが発生しても、その究明や解決に向けて、冷静な対応ができるようになるだろう。なお、Part1でのコマンド解説は概要だけにとどめるので、具体的な活用法については、Part2の実践事例と絡めてマスターしてもらいたい。

Network Command 1

TCP/IPの設定情報を調べる

ipconfig

例えば、ローカルのPCから社内イントラネットのWebコンテンツを表示できないトラブルが発生した場合、Webブラウザの設定で解決を図ることが多いだろう。しかし、それではトラブルを解決できず、また、その原因もわからない場合、どのように対処すればよいだろうか。

まずは、「ipconfig」コマンドで、TCP/IPの設定を確認することから始める。ipconfigは、WindowsのTCP/IP設定を確認するコマンドで、ネットワークトラブルが発生したら、最初に使用する（画面1）。これは、自分のPCのTCP/IP設定がまちがっている可能性をあらかじめ排除しておくためだ。ipconfigを実行して、Webコンテンツを表示できない原因、つまり、ターゲットPCと通信できない原因がTCP/IP設定にあると判明したら、それを修正すればよい。

また、リモートネットワークとの通信に障害がある場合、デフォルトゲートウェイの設定も障害の可能性として考慮する。デフォルトゲートウェイが設定されていなかったり、無効な値が設定されていると、そのローカルPCが所属するネットワーク内部でしか通信できない。そのため、同じくipconfigでデフォルトゲートウェイのIPアドレスを確認しておく。さらに、ipconfigの「/all」オプションを使えば、DNS（Domain Name System）サーバのIPアドレスも表示できる。利用するDNSサーバのIPアドレスが正しいかどうかも、ここで確認しておく。

当然のことだが、あるホストのIPアドレスが、ほかのホストのIPアドレスと重複すると、通信できない。たとえこちらからのパケットが目的のあて先に届いても、同一のアドレスを持つどちらのホストにリプライすればよいのか判断できないからである。そのため、TCP/IPのネットワークでは、IPアドレスが重複すると、同一アドレスを持つホストどうしだけではなく、ほかのホスト間でも通信できなくなる。ipconfigを実行して、既存のホストとIPアドレスが重複していないことも確認しよう。

また、ほかのPCと通信できない原因として、DHCP（Dynamic Host Configuration Protocol）クライアントがIPアドレスを取得できないケースが考えられる。Windows2000以降では、この現象が発生すると、「APIPA（Automatic Private IP Addressing）」機能が働き、「169.254.X.X」というアドレスが表示される（以前のWindowsでは「0.0.0.0」）。この場合、「ipconfig /renew」を実行して、DHCPクライアントにIPアドレスを取得させる。なお、NIC（Network Interface Card）のドライバやPCの種類によっては、あらかじめ「ipconfig /release」を実行しておかないと、「ipconfig /renew」が実行できないケースもあるので注意する。「ipconfig /renew」を実行しても、IPアドレスが取得できない場合は、NICやケーブルなどのネットワーク媒体に不具合がないかを疑ってみよう。

以上のように、TCP/IP設定のまちがいを修正し、ネットワーク媒体にも不具合が見当たらないのに、ターゲットPCとの通信が回復できなければ、さらにほかの原因を探ってみる。

画面1●「ipconfig /?」で使用可能なオプションを確認できる。これはOSにより異なる

Network Command 2

リモートホストとの通信を調べる

ping

ipconfigを使って、ローカルPCのTCP/IP設定には、問題ないことが判明した。ところがまだ、社内イントラネットのWebサイトが閲覧できない。ここではTCP/IPの設定以外にも、次のようなものがトラブルの原因として想定できる。

❶Webサーバが停止している。
❷プロキシを利用している場合、プロキシサーバが停止している。
❸ホスト名を使用して接続を試みている場合、DNSサーバが停止している。または、DNSサーバにWebサーバの登録がない。
❹Webサーバ、プロキシサーバ、DNSサーバは正常稼働しているが、経路上のどこかで接続が途切れている。

それでは、これらの想定できる原因のうち、実際にはどこで障害が発生しているのだろうか。障害発生個所を探るのために使用するのが、リモートホストとの通信状況を確認する「ping」コマンドである（画面2）。pingは、次のStepを踏んで実行する。

Step1
ping 127.0.0.1

まずは、pingを使って、自分のPCの「TCP/IPコンポーネント」が正しく構成されているかどうかを確認しよう。TCP/IPのコンポーネントに異常があるとリプライを受け取れない。解決法としては、TCP/IPプロトコルを再インストールする必要がある。OSによっては、TCP/IPの再インストールは、OS自体の再インストールを意味する。なお、ここで使用するIPアドレス「127.0.0.1」は、ネットワークカードなどのループバックインタフェースに割り当てられた自分自身を表すアドレスで、「ping localhost」を実行しても、同じリプライを受け取ることができる。

画面2●　「ping /?」で使用可能なオプションを確認できる。これもOSにより異なる

Step2
ping 自分のIPアドレス

Step1で、ループバックアドレスへのpingが成功すれば、次に、ipconfigで調べた自分自身のIPアドレスにpingを実行する。ここでリプライを受け取れない場合、NICの実装に失敗している可能性がある。対策としては、NICのドライバを再インストールするか、NIC自体を交換する必要がある。

Step3
ping デフォルトゲートウェイのIPアドレス

リモートネットワークとの通信障害を確認するには、デフォルトゲートウェイのIPアドレスを使ってpingを実行する。このpingに失敗する場合は、トラブルの原因がデフォルトゲートウェイにあると推測できる。しかし、pingでは、デフォルトゲートウェイが停止しているのか、インタフェースがダウンしているのか、この切り分けができない。また、リモートネットワーク側のインタフェースがダウンしていても、デフォルトゲートウェイからのリプライがある。そのため、リプライがあっても、「デフォルトゲートウェイは正常に稼働している」と判断してはいけない。これは、次のStep4で確認する。なお、実際には、デフォルトゲートウェイがローカルホストと異なるスイッチやハブに接続されていることを考慮して、pingを実行する。

Step4
ping リモートネットワークの任意ホストのIPアドレス
ping リモートホストのIPアドレス

リモートネットワークに所属する任意のホストにpingを実行すると、そのネットワークまでのルーティングに成功しているかどうかを判定できる。リプライがない場合、リモートネットワークまでの経路上、どこまで通信が届いているかを確認する（Network Command3の「tracert」参照）。pingでもtracertでも、「Request time out」が表示される場合、そのルータ、もしくはそのルータと直前のルータ間の経路に障害がある。また、「Destination host unreachable」が表示される場合は、その直前のルータが持つルーティング情報と、あて先に近い側のイ

ンタフェースをトラブルの原因として調べてみる（画面3、図1）。

リモートネットワークまでの経路上に障害がなければ、通信したいあて先のIPアドレスを指定して、pingを実行する。これでリプライが得られない場合、リモートホスト自体に障害が発生している可能性が高い。

Step5
ping リモートホスト名

次に、IPアドレスではなくコンピュータ名やホスト名でpingを実行する。リプライがあれば、名前解決が成功していると判断できる。もし、名前解決に失敗する場合は、DNSサーバに対して、これまでのpingによる障害調査のステップを実行してみる。名前解決も、プロキシサーバとの通信にも問題がないのに、Webサイトを閲覧できない場合は、Webサーバのアプリケーションの動作を確認する。これはpingでは判定できない。コントロールパネルの「管理ツール」から「コンピュータの管理」を開くと、リモートでサービスの起動を確認できる。

画面3●　例として、リモートホスト「192.60.230.24」にpingとtracertを実行すると、障害が発生している経路上のホストから「Destination host unreachable」がリプライされる

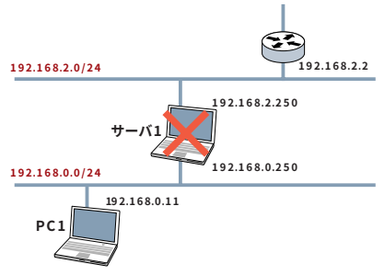


図1●　画面3のコマンド実行例からは、「192.168.0.250」のサーバ1で障害が発生していることがわかる

Network Command 3

ネットワーク経路を調査する
tracert

あて先ホストまでの経路を調査するためのコマンドである（画面4）。通過するネットワークルータまでのpingを3回実行しているのとほぼ同様の動作をする。使用している「ICMP（Internet Control Message Protocol）」というプロトコルも、pingと同じだ。経路上のルータが正確なルーティング情報を持ち、正常な動作をしていれば、所用時間がリプライされる。リプライがない場合は、そのルータが障害の原因と考えられる。しかし、セキュリティ上の理由で、ICMPをリプライしないように設定されているホストも存在する。そのため、リプライがないからといって、障害が発生しているとは限らない。

画面4●　「tracert -?」で使用可能なオプションを確認できる

Network Command 4

ルーティング情報を設定する
route

ネットワークアドレスが異なるネットワークへパケットを転送するのが「ルーティング」である。単なる同じネットワーク内でのパケットの転送は「スイッチング」という。ルータが一方のネットワークから受け取ったパケットの転送先は、TCP/IPホストの

ルーティング情報（ルーティングテーブル）によって判断される。このルーティング情報を表示・設定するのが、「route」コマンドである（画面5、画面6）。ルーティング情報を表示するだけなら、「netstat -r」でも同じ内容を確認できる。

すべてのTCP/IPホストは、ルータとして構成しなくても、ルーティングテーブルを持っている。ルーティングテーブルでは、例えば「『0.0.0.0/0』のネットワークへ接続するために、『192.168.0.250』のホストを経由する」という情報が保持されている。「0.0.0.0/0」で表されるネットワークは、「世の中すべてのネットワークアドレス」を意味する。つまり、このルーティングテーブルでは、リモートネットワークへのすべての接続で、「192.168.0.250」がゲートウェイの役割を果たしている。

図2で考えると、PC1から見て、ルータ1のホスト「192.168.0.250」が「デフォルトゲートウェイ」になる。ここで、「add」オプションを使用すると、PC1のルーティングテーブルにルーティング情報を追加できる。例えば、PC3が存在する「192.168.200.0/24」のネットワークへ接続するのに、ルータ2の「192.168.0.3」を経由させたい場合、次のコマンドを入力すればよい（画面7）。

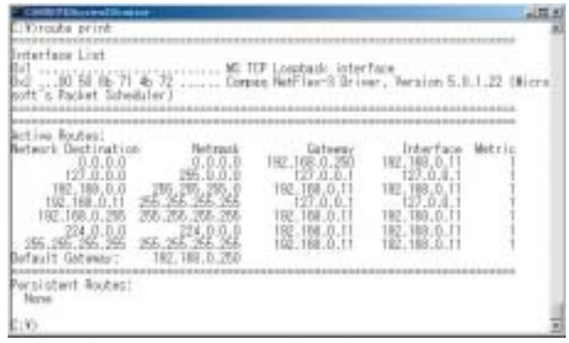
route add 192.168.200.0 mask 255.255.255.0 192.168.0.3

また、PC3でも同様に、次の❶❷のようにルーティング情報を設定する。これは、PC1からのパケットがPC3に届いても、PC3がリプライ先をわかっていなければ、通信できないからだ。

❶「192.168.0.0/24」のネットワークへは、「192.168.200.3」のホストを経由する。
❷「192.168.200.3」をデフォルトゲートウェイとして、「すべてのリモートネットワークへの出入り口に「192.168.200.3」を利用する。

通常、デフォルトゲートウェイには、すべてのリモートネットワークあてのトラフィックが集中する。ところが、routeで明示的に任意のリモートネットワークへのルーティング情報を設定した場合、この経路がデフォルトゲートウェイに優先して機能する。一方、図2のPC3のように、自分が所属するネットワークから、ほかのネットワークへのデフォルトゲートウェイが1か所だけに限定される場合、任意のルーティング情報をrouteで追加する必要はない。なお、ほかのネットワークへのルーティング情報がルーティングテーブルに保持されていないと、通信はネットワークアドレスが同じホストだけに限定される。

画面5●　「route -?」で使用可能なオプションを確認できる



画面6●　「route print」でルーティング情報を表示できる

画面7●　図2のPC1がPC3のネットワーク「192.168.200.0/24」へ接続する際、ルータ2のホスト「192.168.0.3」を経由させるには、「route add」でルーティング情報を追加する

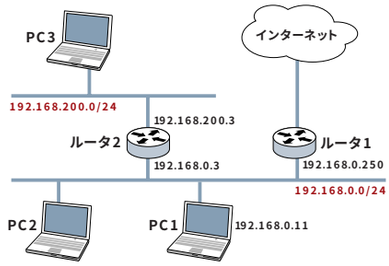


図2●　PC1がインターネットに接続するためのデフォルトゲートウェイは、ルータ1の「192.168.0.250」である

Windowsをルータとして使う

Windowsはルータとして利用可能である。複数のNICを実装したり、1つのNICにネットワークアドレスが異なる複数のIPアドレスを設定したりして、それぞれのインタフェース間でルーティングを有効にすればよい。PCに複数のNICを実装すると、そのインタフェースの属しているネットワークすべてのルーティング情報が自動で追加される（画面8）。図3を例にして考えてみよう。サーバ1には2枚のNICが実装されていて、NICにはそれぞれ次のようなIPアドレスが設定されいる。

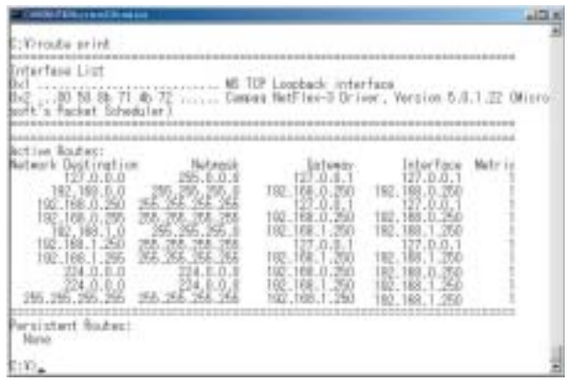
192.168.0.250/24
192.168.0.251/24

ところが、図3ではサーバ1でルーティングを有効にしても、PC1とPC2は通信できない。物理的に異なるネットワークセグメントを構成しても、PC1とPC2が所属するネットワークアドレスが「192.168.0.X」と同じなので、ルーティングの対象にならないからである。また、PC1とPC2でそれぞれ次のコマンドを実行しても、通信できない。

PC1
route add 192.168.0.253 mask 255.255.255.255 192.168.0.250
PC2
route add 192.168.0.11 mask 255.255.255.255 192.168.0.251

そこでPC1とPC2の通信を可能にするためには、図4のように、PC2が所属するネットワークのアドレスを変更する。このとき、サーバ1のホストアドレスは「192.168.1.251」のままでもかまわないが、複数のネットワークに所属しているルータの場合、ホストアドレス部分に同じ値を使用したほうが、記憶まちがいが少ない。

ルータを構成するときは、その両側のネットワークに異なるアドレスが設定されるように注意しよう。



画面8●　PCに複数のNICを実装すると、それぞれのインタフェースが属しているネットワークすべてのルーティング情報が追加される。画面例では、「192.168.0.0」と「192.168.1.0」

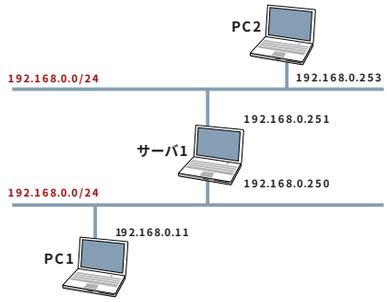


図3●　サーバ1の両側に同じネットワークアドレスが設定されているので、PC1とPC2は通信できない。ちなみに、サーバ1はそれぞれPC1とPC2とは通信可能

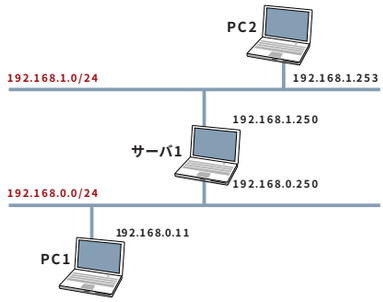


図4●　サーバ1の両側に異なるネットワークアドレスが設定されているので、PC1とPC2は通信できる

Network Command 5

DNSサーバの登録情報を確認する

nslookup

「nslookup」コマンドは、DNSサーバに登録されているデータベースの内容を確認したいときに利用する（画面9）。DNSサーバに名前解決クエリーが届いていると、回答を得られる。ただし、DNSサーバの持つゾーンファイル情報を表示するだけなので、nslookupで任意ホストのエントリを確認できても、ローカルホストがそのゾーンファイル情報を持っているDNSを利用できるとはかぎらない。

ローカルホストが名前解決で利用するDNSサーバのIPアドレ

スは、「ipconfig /all」で確認する。DNSサーバに対してpingが届けば、nslookupでもDNSサーバと通信できる。nslookupは、デフォルトで「ipconfig /all」で確認したDNSサーバにクエリーを要求する。

DNSサーバの仕組みとして、自分が解決できないクエリーをほかのDNSサーバで解決するようになっている。その名前解決の結果を一定時間キャッシュとして保持して、その間はあたかも自分が持っている情報のように名前解決に使用する。この情報は、nslookupのクエリーで確認できる（画面10）。

画面9●　ヘルプの指示どおりに「nslookup /?」を実行すると、「/?」そのものをクエリーしてしまう。使用可能なオプションを確認するには、あらかじめ「nslook」を起動してから、「?」を入力する必要がある

画面10●　「wwww.idg.co.jp」のIPアドレスをクエリーする

パケット解析ツール

トラブルの原因究明に必須！
ネットワークモニタ

Windows2000 Server/Sever2003には、ネットワーク上のパケットをキャプチャして解析する「ネットワークモニタ」が装備されている（画面11）。フィルタリング機能を利用して目的のトラフィックだけを表示できるなど、トラブルシューティングには欠かせないツールだ。また、Systems Management Server（SMS）には、ルータを検索したり、名前からIPアドレスを解決したりできるなど、より高機能なネットワークモニタが装備されている。

最近では、無償のパケットキャプチャツール「Ethereal」もよく使われる。ネットワークモニタと同等の表示が可能で、ネットワークモニタでキャプチャしたファイルの読み込みもできる。Windowsのネットワーク管理者は、ネットワークモニタとEtherealの2つを用意しておけば、どちらかのツールでしか計測表示できないトラフィックにも対応できる。

画面11●　ネットワークモニタでキャプチャしたトラフィックを解析する。ICMPだけを表示するようにフィルタリングを実行している

Column

記述方法が統一されていないWindowsコマンドに悩む

通常、名称が同じコマンドにもかかわらず、収録しているOSやリリース時期が異なると、実行結果やプログラム動作、オプションなどが変化するものだ。しかし、マイクロソフトのOSは、UNIX互換OSに比べると、ばらつきがとても多い。例えば、UNIX互換OSでは、引数（オプション）記号に「-」「--」を使い、コマンドと引数の間はスペースで区切る。だが、マイクロソフトOSの引数記号には、「-」と「/」の2つが存在し、両方使えるコマンドもあれば、どちらか一方だけしか使えないコマンドもある。さらに、コマンドと引数の間は、スペースで区切ったり区切らなかったり、Windowsの中で統一が図られていない。　Windows 2000以降のOSでは、スペースで区切らなくても使えるコマンドが多いようだ。Windows2000以前のOS操作に慣れていない管理者は、スペースで区切らずに入力して「実行できない」と悩む前に、スペースを入れる書式を心がけたい。引数記号については、マイクロソフトに統一を心がけるように望みたい。