Part 2 どんな障害にも慌てない問題解決力を鍛える こうしてトラブルに打ち勝つ! 実践事例編

トラブルが発生したら、すぐにその原因を探り出し、正常な状態に復旧する必要がある。Part 1 ではトラブルシューティングを行うための基本コマンドやツールの利用法を学んだ。今度は、それを実践で使えるようにしたい。実際の現場では、コマンドを組み合わせたり、いくつもの現象から問題点を導き出す推理力が求められる。紹介する7つの事例は、読者の環境とは必ずしも同じではないだろうが、解決に至るまでのプロセスを学んでもらいたい。

トラブル事例 1

デフォルトゲートウェイの設定が消失!
リモートネットワークに接続できない

現象▶ サーバの遠隔操作ができなくなった　コマンド▶ ipconfig　route　ping

サーバルームへの入室権限がない

事例の1つ目は、Windows系のプログラマーが常駐する現場でのトラブルを紹介したい。Windowsのインストールとプログラミングは得意でも、「ネットワークはよくわからない」というメンバーが中心の会社だったので、Windows系ネットワークエンジニアの筆者が、1か月の常駐サポートを要請された。サポート業務が中心なので、トラブルが起きないかぎりは、時間を持てあます仕事になるはずだった。しかし現実には、トラブルが起きない状況というのはまれだろう。

まず、この会社のネットワーク構成図を確認してもらいたい(図5)。PC1の所属するネットワーク(192.168.220.0/24)から、ほかのネットワークへの出入り口は、ルータ2(192.168.220.1)だけである。そのため、PC1の所属するネットワーク上のホストは、ルータ2がデフォルトゲートウェイに設定されている。一方、サーバセグメントに所属するサーバ1とサーバ2は、ルータ1(192.168.0.250)がデフォルトゲートウェイに設定されている。サーバセグメントは、物理的に離れた鍵のかかるサーバルームに設置され、ローカルでの直接操作が必要ないかぎり、PC1の所属するのネットワークから、「ターミナルサービス」を使ってリモート操作していた。ところがあるとき突然、PC1の所属するネットワークからサーバ2にアクセスできなくなるトラブルが発生した。

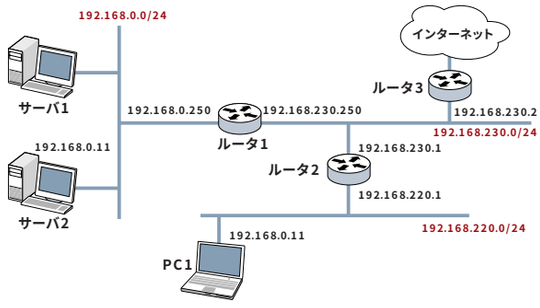


図5●　社内LAN(PC1)とサーバセグメント(サーバ1、サーバ2)、また、これらのセグメントとインターネットを結ぶ「ルータセグメント」で構成されている

そのほかの障害状況も確認すると、PC1の所属するネットワークからサーバ1には、アクセスできることがわかった。また、サーバセグメントのローカルで操作すると、サーバ1からサーバ2に対して、また逆にサーバ2からサーバ1にアクセスできるようだ。そのため、PC1の所属するネットワークからサーバセグメントまでの経路上に障害はなく、サーバ2が問題なく稼働していることも判明した。どうやら障害は、「192.168.0.0/24」のネットワーク内で、しかもサーバ2で起きているようだ。このようなケースでは、できるだけ障害の発生ポイントに近づいて、原因の切り分けや究明を図りたい。ところが筆者は、サーバルームへの入室権限を持ってなかったので、別の方法で解決を試みることにした。

多段階接続でアクセスする

最初に、ターミナルサービスのリモートデスクトップで、サーバ1にアクセスして、さらにターミナルサービスでサーバ2にアクセスする。直接アクセスできるホストを通して、直接アクセスできないホストに間接的(多段階)に接続する方法だ。その後、サーバ2のデスクトップにログオンしたら、コマンドプロンプトを起動して、ipconfigを実行する。その結果、デフォルト

ゲートウェイが設定されていないことが判明した(画面12)。何らかの操作中に、誤ってデフォルトゲートウェイを削除する設定が行われたのだろう。

つまり、このトラブルは、パケットがPC1からサーバ2まで届いているが、サーバ2にデフォルトゲートウェイが設定されていないので、リプライができない状態なのである。トラブルシューティングとしては、routeを実行して、サーバ2にデフォルトゲートウェイを追加設定すればよい(画面13)。

```
route -p add 0.0.0.0 mask 0.0.0.0 192.168.0.250
```

このコマンドでサーバ2にデフォルトゲートウェイを設定するだけでトラブルを解決できる。それは、サーバ2の所属するネットワークから、ほかのネットワークへの出入り口がルータ1に限られ、ルータ1とルータ2が、それぞれ次のようなルーティング情報を持っているからだ。

画面12●　ipconfigを実行すると、デフォルトゲートウェイが設定されていないことが判明した

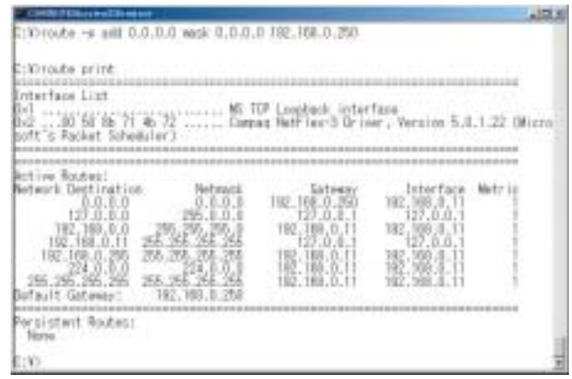
ルータ1

ルータ2が「192.168.220.0/24」への接続経路である

ルータ2

ルータ1が「192.168.0.0/24」への接続経路である

このルーティング情報のおかげで、サーバ2もPC1もそれぞれのデフォルトゲートウェイであるルータ1とルータ2にパケットの転送を任せれば、通信が可能になる。つまり、あるホストのネットワークへの出入り口(デフォルトゲートウェイ)が、1か所に限定されるときは、そのデフォルトゲートウェイを設定するだけで、リモートネットワークと通信できるようになるのだ。



画面13●　routeを実行して、サーバ2にデフォルトゲートウェイを追加設定する

トラブル事例 2

リモートサーバへの接続でタイムアウトが発生！

ネットワークが遅延する

現象▶ リダイレクトでパケット量が激増　　コマンド▶ ping

複数の出入り口が存在

事例1と同じ会社で遭遇したトラブルである。今度は別のネットワークで、「サーバへの通信に時間がかかりすぎて困る」という苦情がきた(図6)。実際、社内LAN上のPC1から、サーバセグメントにpingを実行すると、たびたびタイムアウトする。

まず、このネットワークで注意したいのは、サーバセグメントがインターネットと社内LANの2つの出入り口を持っている点だ。それぞれのサーバは、Webサービスやメールサービスでインターネットと通信している。一方、同時に社内LAN側にもサービスを提供している。つまり、2つのゲートウェイを持っているのだ。このように、ほかのネットワークへの出入り口が複

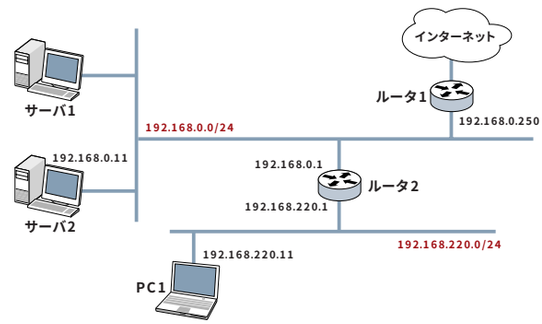


図6●　サーバセグメントから、ほかのネットワークへの出入り口(ルータ)が複数あるケースのトラブル事例。ネットワークの遅延はどこで生じているのだろうか

数ある場合、属するホストにデフォルトゲートウェイを設定するだけでは不十分だ。デフォルトゲートウェイ以外にも、ルーティング情報を設定する必要がある。

このネットワークで言えば、PC1の所属するネットワークは、ルータ2がデフォルトゲートウェイとして設定されている。一方、サーバ1とサーバ2のデフォルトゲートウェイには、ルータ1が設定され、「ルータ2を経由して社内LAN（192.168.220.0/24）にたどりつく」というルーティング情報が追加で設定されている。もちろん、ルータ2をデフォルトゲートウェイに設定しても、社内LANと通信できる。しかし、インターネット上のネットワークと通信するときは、「その経路はルータ1を通過する」というルーティング情報を追加する必要がある。これから通信する可能性のあるインターネット上のホストとネットワークを事前にルーティングテーブルに設定するのは現実的ではない。やはり、ルータ1をデフォルトゲートウェイにして、「ルータ2を経由して社内LAN（192.168.220.0/24）にたどりつく」というルーティング情報を追加するのが正しい方法だ。実際、当初はそう設定されていた。

ネットワークが混雑する理由

ところが、調べてみると、サーバ側のホストに追加するべきこのルーティング情報が消失していたのである。さらに不自然なのは、それでもサーバが社内LANのネットワークと通信できてしまう点だ。

どうして通信できるのだろうか。それは、「ルータ2が社内LAN（192.168.220.0/24）への経路情報を持っている」とルータ1が把握しているからだ。そうでなければ、PC1のネットワークからインターネットとの通信はできない。つまり、PC1がインターネット上のホストに送ったパケットのリプライが戻るには、ルータ1がルータ2の経路情報を知っている必要がある。逆に、ルータ2はルータ1がインターネットへの出入り口であることを知っている。ルータ2にとって、ルータ1がデフォルトゲートウェイなのだ。そのため、サーバ1とサーバ2のデフォルトゲートウェイがルータ1に設定され、ルーティング情報が消失している状況でも、PC1がサーバ2と通信できる。この場合、トラフィックは次のように流れる。

❶PC1からのパケットはルータ2を経由する。
❷ルータ2は、サーバ2の所属するネットワークにもインタフェースを持っているので、PC1からのパケットはサーバ1に届く。
❸サーバ2は、リプライをデフォルトゲートウェイのルータ1に転送する。
❹ルータ1は、社内LAN（192.168.220.0/24）のネットワークへの経路情報がルータ2にあることを知っている。そのため、ルータ2にパケットを転送する。
❺ルータ2は、パケットを社内LAN（192.168.220.0/24）のネットワークに転送する。

この場合、サーバ2からのパケットは直接ルータ2を経由せず、ルータ1を1回経由するので、パケットのTTL（Time To Live）値は1つ消費する。さらに、「❸サーバ2からルータ1」「❹ルータ1からルータ2」のように、同じパケットが同一セグメントに2回出現するので、「社内LAN（192.168.220.0/24）のネットワークへは、ルータ2を経由する」というルーティング情報をサーバ2が消失していない場合に比べると、ネットワークは2倍混雑する（図7）。ネットワークが混雑すれば、ホストは届かなかったパケットを再送しようとして、いっそうネットワークを混雑させる悪循環となる。この現象が「サーバへの通信が遅い」という苦情につながったのだ。解決策としては、消失したルーティング情報を次のコマンドを使って再度設定すればよい。

```
route -p add 192.168.220.0 mask 255.255.255.0 192.168.0.1
```

なお、ルータ1が同一ネットワーク内で行う転送動作を「リダイレクト」という。リダイレクトは、ネットワークの遅延を引き起こす原因となるので避けるほうが望ましい。しかし、サーバ2の運用中に何らかのミス操作によって、ルータ2を経由して社内LANに接続するルーティング情報を失ってしまっても、サーバ2とPC1の通信は確保される。つまり、冗長性を持つという利点もある。同様に、サーバ2がルータ2をデフォルトゲートウェイとしても、ルータ2がルータ1へリダイレクトを行うので、サーバ2はインターネット上の任意ホストとの通信が可能になる。

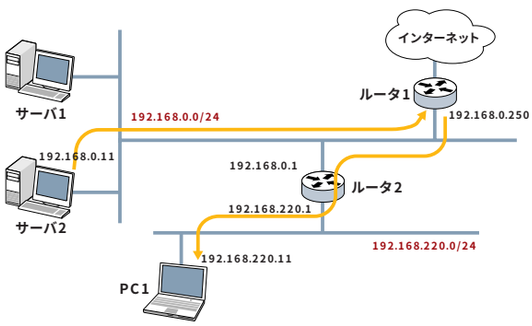


図7●　同じパケットの通信が2回出現するリダイレクトが行われると、ネットワークは2倍混雑して、遅延を生じる

トラブル事例 3

ブロードバンドルータにアクセスできなくなった！

ネットワーク構成の変更でWeb閲覧が不可能に

現象▶ デフォルトゲートウェイが更新されない　コマンド▶ ping　trace

ルータを増やしたり、減らしたり

ネットワークの構成変更を行うと、OSや機器の設定をやり残して、トラブルを招くケースがある。特に運用を一気に開始すると、設定忘れやまちがいの場所がわからなくなるので、復旧に時間がかかってしまう。これを防止するには、変更を1つ済ませるたびに動作確認を行い、そこまでの設定で正常に動作することを確認してから、次の設定に移るのが基本だ。

事例3では、社内LANとブロードバンドルータとの間に新しいルータセグメントを設けて、LANを追加したときのトラブルを紹介しよう。筆者はルータを2台用意して、既存のブロードバンドルータのLAN側のIPアドレスを変更して、ルータセグメントだけを構成した（図8、図9）。

新しいネットワークのブロードバンドルータから見て、以前所属していた「192.168.220.0/24」に対しては、ルータ2（192.168.230.1）を通して、トラフィックが流れることになる。また、「192.168.200.0/24」に対しても、以前は、ルータ1（192.168.220.100）にトラフィックを流していたが、これからは、ルータ2「192.168.230.1」に投げることになる。そこで筆者は、ブロードバンドルータが持つルーティングテーブルを次のように変更した

旧ネットワーク

❶「192.168.200.0/24」には、ルータ1（192.168.220.100）を経由。

新ネットワーク

❶「192.168.220.0/24」には、ルータ2（192.168.230.1）を経由。

❷「192.168.200.0/24」には、ルータ2（192.168.230.1）を経由。

また、ルータ1（192.168.220.100）では、以前と同じ「192.168.220.1」がデフォルトゲートウェイなので、設定の変更は必要ない。一方、「192.168.230.1」と「192.168.220.1」というアドレスを持つルータ2は、次のルーティングテーブルを設定する。

❶デフォルトゲートウェイは、ブロードバンドルータ（192.168.230.2）。

❷「192.168.200.0/24」には、ルータ1（192.168.220.100）を経由。

こうして、ネットワークの「192.168.230.0/24」を構築できた。無事に動作確認も終えたが、諸事情により、元のネットワークに戻すはめになってしまったのだ。

そこで、「192.168.230.0/24」をなくし、「192.168.220.0/24」にブロードバンドルータを接続して、「192.168.220.1」というアドレスに戻すことにした（図10）。ところが、ネットワークを元どおりにしたあと、「192.168.200.0/24」のPC2からWebサイトを閲覧できない状況に陥ってしまった。試しに、PC1を「192.168.220.0/24」に接続したところ、問題なくWebサイトを閲覧できる。どこにトラブルの原因があるのだろうか。早速トラブルシューティングの開始である。

まず、PC1のルーティングテーブルには、デフォルトゲート

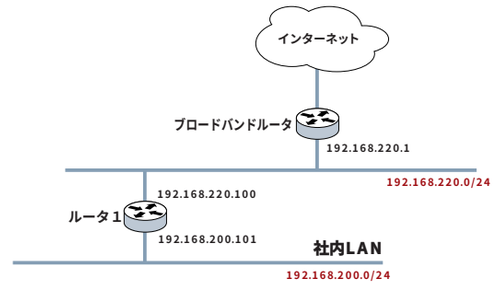


図8●　構成変更前のネットワーク。社内LANとブロードバンドルータまでに、ルータを1つ経由する

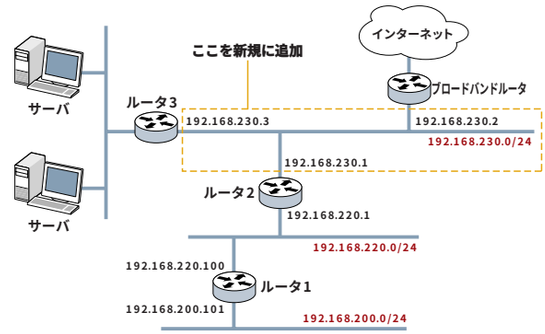


図9●　構成変更後のネットワーク。図8のブロードバンドルータの内側にルータだけのネットワークを増設して、サーバセグメントを接続する。ブロードバンドルータのLAN側アドレスは、図8の「192.168.220.1」から「192.168.230.2」に変更する

ウェイとしてブロードバンドルータ「192.168.220.1」が設定されている。このことから、ブロードバンドルータは正常に動作していると判断した。

次に、PC2を利用して、「192.168.200.0/24」から「192.168.220.0/24」への出口となるルータ1（192.168.200.101）とブロードバンドルータ（192.168.220.1）に対して、pingを実行すると、次のような結果を得られた。

❶PC2から「192.168.200.101」　ping成功。
❷PC2から「192.168.220.1」　ping失敗。

同様にtraceを実行すると、pingの結果と同じく、「192.168.200.101」へは到達できているようで、次の結果を得られた。

❶PC2から「192.168.200.101」　tracert成功。
❷PC2から「192.168.220.1」　tracert失敗。

ここで、PC1に『192.168.200.0/24』へのネットワークには、『192.168.220.100』を経由する」というルーティング情報を追加してみた。

```
route add 192.168.200.0 mask 255.255.255.0 192.168.220.100
```

すると、「PC1からPC2」「PC2からPC1」それぞれのpingに成功した。ブロードバンドルータと同様、ルータ1も正常に動作していると判断できる。さらに、routeでPC1のルーティングテーブルを確認すると、次の結果を得られた

❶デフォルトゲートウェイは、ブロードバンドルータ（192.168.220.1）。
❷「192.168.200.0/24」には、「192.168.220.100」を経由。

同様に、PC2のルーティングテーブルは次のとおりだった。

❶デフォルトゲートウェイは、ルータ1（192.168.200.101）。

IPアドレスが自動消去せず…

PC2は、接続できないブロードバンドルータと同じネットワークに属しているPC1には接続できる。そのため、ルータ1だけでなく、PC1もPC2も正常なルーティングテーブルを持ち、動作していると判断した。

それでは、「192.168.200.0/24」上のPC2がインターネットに接続できない原因はどこにあるのだろう。残されたトラブル発生源として疑わしいのは、ブロードバンドルータのルーティングテーブルである。実際、ブロードバンドルータのルーティングテーブルを確認すると、次のような結果が得られた。

❶「192.168.220.0/24」には、「192.168.230.1」を経由
❷「192.168.200.0/24」には、「192.168.230.1」を経由

読者はお気づきになっただろうか。筆者がうっかりしていたのだ。「192.168.230.1」は、新しいネットワークを構築したときに、ルータ2に設定したIPアドレスである（図9参照）。つまり、ネットワーク構成を元に戻したときに、ブロードバンドルータのルーティングテーブルを戻し忘れていた。「192.168.200.0/24」上のPC2からの通信は、ブロードバンドルータに届いているのに、ブロードバンドルータはそのリプライを「192.168.230.1」という存在しないIPアドレスに対して送っていたのである。

今回のトラブルは次のコマンドで、ブロードバンドルータのルーティングテーブルを変更して、一件落着となった。

```
route delete 192.168.220.0
route delete 192.168.200.0
route -p add 192.168.200.0 mask 255.255.255.0 192.168.220.100
```

ブロードバンドルータやCiscoなどのハードウェアルータ、もしくはPCなど、TCP/IPホストであれば、ルーティングテーブルを持っている。通常はインタフェースが所属するネットワーク上のルータ（ゲートウェイ）のIPアドレスを、ゲートウェイアドレスとして設定する。ところが、TCP/IPホストの中には、リモートネットワーク上のルータをゲートウェイとして設定できるOSもある（Windowsは不可）。

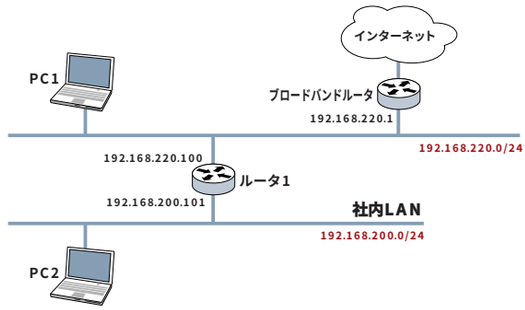


図10●　ネットワークを元どおりに戻したつもりが、社内LAN（192.168.200.0/24）から、インターネットに接続できなくなるトラブルが発生した

一方、リモートネットワーク上のルータをゲートウェイとして設定できないOSでは、インタフェースのIPアドレスを別のネットワークに所属するIPアドレスに変更した場合、それ以前にゲートウェイアドレスとして設定していたルータのIPアドレスが自動的に消去されることが多い。今回利用していたブロードバンドルータは、リモートネットワーク上のルータをゲートウェイとして設定できるにもかかわらず、以前の設定が残ってしまった。現実には存在しないゲートウェイのIPアドレスに対してパケットを送っていたのだ。もっとも、インタフェースのIPアドレス変更でルーティング情報が消去される場合でも、ルーティング情報の追加は必要である。

トラブル事例 4

ネットワークの構成変更で接続不可能に
ルーティング情報の設定ミス

現象▶ ルーティング機能が正常に働かない　コマンド▶ ping　route

事務所移転が引き金となって

オンラインショップを営む会社（社員数約20名）から引き受けた案件にまつわるトラブル事例を紹介しよう。この会社では、事業所の移転に伴い、サーバを外部ホスティングから自前で立ち上げることになった。そのため、筆者は「メールサーバ」「DNSサーバ」「Webサーバ」を含むネットワークの構築を依頼された。具体的には、移転前の事務所内でサーバをインストールしたあと、移転先のアドレスを使って「ドメイン名」「ホスト名」「IPアドレス」を設定し、動作確認までを筆者が行う。移転当日の作業にはかかわらなくてもよいが、このとき移転日まで3日しか残されていなかった。

まずは、新事業所で構築されるネットワークを確認しよう（図11）。サーバOSとアプリケーションは顧客から指定されていたので、筆者はWindows2000を使ってルータ1を構成するところから始めた。Windows2000のインストールは無事に終わったので、今度はインターネットに接続して「Windows Update」を適用したい。この会社のシステム管理者に、使用可能なネットワークアドレスを確認すると、教えられたのは「192.168.1.0/24」である。また、ルータ1のホストアドレスとして、移転後に使用する「192.168.1.250」を現時点で利用できるという。そこで、ルータ3の「192.168.1.2」をデフォルトゲートウェイとするように設定した。

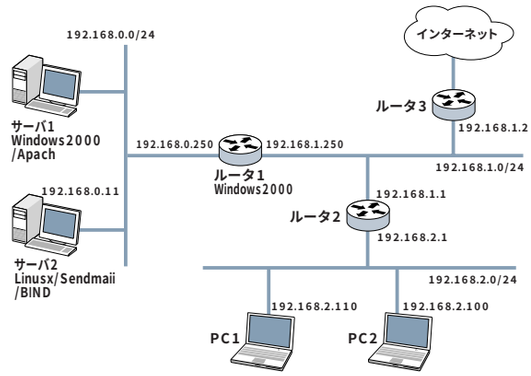


図11●　移転先のネットワーク構成

次に、サーバ2の設定に取りかかる。Linuxとメールサーバ（Sendmail）やDNSサーバ（BIND）は、雑誌付録のCD-ROMのからインストールできる。しかし、セキュリティ上の観点から、最新の実行ファイルとパッチを使うのが理想的だ。筆者は、雑誌付録CD-ROMから、最低限の環境だけをインストールして、残りはインターネット上からダウンロードして適用することにした。

サーバ2をインターネットに接続させるには、ルータ1をデフォルトゲートウェイとして構成する。ルータ1はルータ3をデフォルトゲートウェイとしている。さらに、ルータ3はサーバ2が所属する「192.168.0.0/24」へのルーティング情報を持っている必要がある。ルータ3がこのルーティング情報を持っていないと、サーバ2からインターネット上のホストにパケットが届いても、そのホストからのリプライを送るあて先がわからず、通信は成功しない。

そこで、ルータ3に「192.168.0.0/24」へのルーティング情報を設定するように、この会社の管理者にお願いすると、すでに設定されているという。安心してサーバ2からWebサイトの閲覧を試みたところ、なぜかこれが失敗するのだ。ルータ1として構成したWindows2000で確認すると、ルータ3へのpingも、インターネットへの通信も成功している。また、サーバセグメントのネットワーク内でも、ルータ1とサーバの通信は成功している。

トラブルがさらなるトラブルを招く

筆者は、このトラブルの原因がルータ1の設定ミスにあると考えた。そこで、ルータ1のルーティング機能と「192.168.0.250」の

インタフェース機能（NIC）を無効化したあと、「192.168.0.0/24」のブロードキャストアドレスである「192.168.0.255」に対して、サーバ1からpingを試すことにした。ブロードキャストアドレスとは、そのネットワーク上の全ホストを表し、これを使えば、1回のpingでホストの有無を確認できる。今は、NICを無効にしたルータに対してpingを実行するので、もちろんリプライはないはずである。

ところが、驚いたことにリプライがあったのだ。疑問に感じた筆者が管理者に確認すると、現在の社内LANで使用していることが判明した。つまり、「192.168.0.0/24」というネットワークが重複して存在しているのだ。サーバ2からインターネットに通信できないのは当然である（図12）。

早速、トラブルシューティングの開始である。現在のネットワーク構成で、ルータ3は「ルータ2が『192.168.0.0/24』への経路を知っている」というルーティング情報を持つ。そこで、ルータ3のルーティング情報を「『192.168.0.0/24』にはルータ1が接続している」という内容に書き換えたい。ところが、ルーティング情報を変更すると、新事務所に移転するまでのあいだ、社内LANからはリモートネットワークと通信ができなくなってしまう。

このようなトラブルケースでは、移転前に現在の社内LANのネットワークアドレスを変更することで対応できるが、管理者によれば、この方法は避けたいという。そこで、ほかの選択肢には、次の2つがある。

❶移転先で使用するアドレス計画を変更する。
❷移転前の段階では、計画しているアドレスを使用しないで、現在のネットワークでも利用できるアドレスを使う。DNSのゾーンファイルやconfファイルの設定ファイルは、移転前と移転後の2とおりを用意しておく

❶の方法では移転後に、設定ファイルを変更する手間はかからない。一方、❷の方法では、移転後に設定ファイルを入れ替えたり、PCのIPアドレスを変更したりする作業が生じるが、20台程度のPCなら、時間はかからないだろう。しかし、SendmailやBINDの環境では技術的なスキルが要求される。筆者は移転後の作業にはかかわらない契約なので、顧客だけで作業するのは少々不安だ。今回は、アドレス計画を変更したくない顧客側の意向で、❷の方法を採用することになった。

とりあえずは、図13のようなネットワークを構築して、メールの送受信や転送などの動作確認も無事に終了した。しかし、念のため、移転後のアドレスを使って動作確認をしておきたい。そこで、PC1を「192.168.1.0/24」に移動して、IPアドレスも設定変更し、デフォルトゲートウェイをルート3に設定した。さらに、サーバ1とサーバ2も「192.168.0.0/24」のネットワークに戻して、アドレス構成を再設定した（図14）。

当然のこと、ルータ3の設定は変更できないので、サーバ1とサーバ2は、インターネットに接続はできないが、ルータ1を介してPC1には接続できるはずである。ところが、ルータ1は正常動作しているにもかかわらず、接続できない。そこで筆者はPC1のルーティング情報を「route print」で確認してみることにした（画面14）。ここでは、「『192.168.0.0/24』のネットワークへはルータ1を経由する」と情報が設定されている必要がある。しかし、実際には設定されていなかったのだ。

これでは通信できなくて当然である。サーバ1やサーバ2からのパケットがPC1に届いていても、PC1は「192.168.0.0/24」への経路を知らないので、リプライのしようがない。次のように「route add」を実行して、ルーティング情報を追加した。

```
route add 192.168.0.0 mask 255.255.255.0 192.168.1.250
```

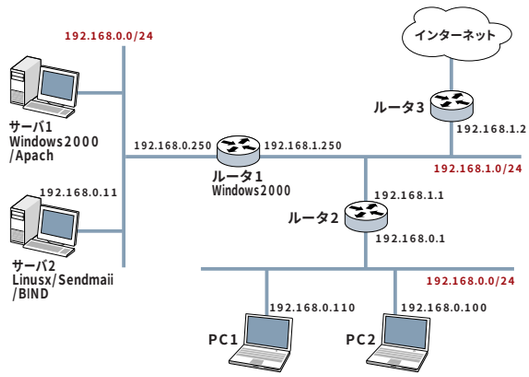


図12●　現在（移転前）のネットワーク構成

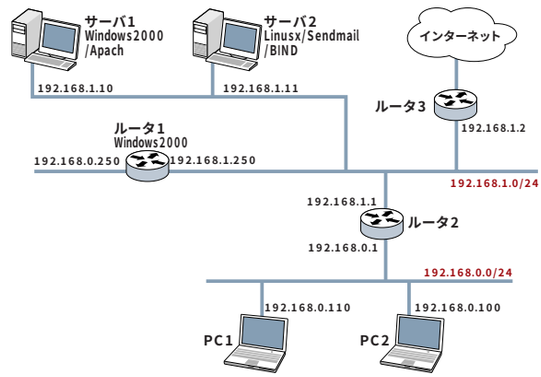


図13●　暫定のネットワーク構成。サーバセグメントからインターネットに接続できるようになった

こうすることで移転後のアドレス環境でも、動作することが確認できた。再度、現在のネットワーク構成でも動作するアドレス環境に戻して、今回の仕事を終了した。ネットワークの構成変更はくれぐれも慎重に行いたい。

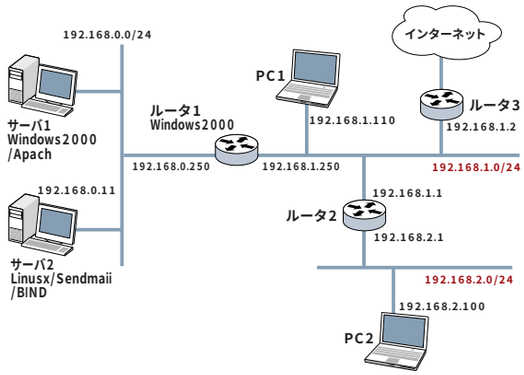
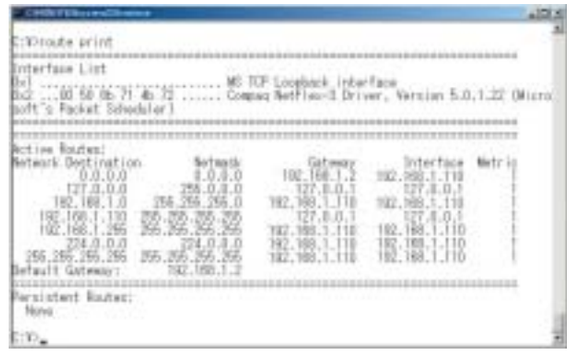


図14●　移転後のアドレスを使って動作確認を行うため、PC1を移動する



画面14●　「route print」の実行結果。PC1は「192.168.0.0/24へのルーティング情報を持っていない

トラブル事例 5

ADSL開通でブロードバンドルータを新規導入！

ローカルDNSで名前解決に失敗する

現象▶ ハードウェアに致命的な障害が発生　　コマンド▶ route　ping　tracert　ネットワークモニタ

ルータ交換でアクセス不可能に

3年ほど前、自宅にADSLを導入したときに遭遇したトラブルを紹介したい。開通工事が無事に終了したので、筆者は購入したばかりのブロードバンドルータを使って、ネットワークの構成に取りかかった(図15)。

通常、DNSサーバをローカルに立てないで、ブロードバンドルータのDNS転送機能を利用する。しかし、筆者はローカルにDNSサーバを用意して使っている。ルータ1には、Windows 2000がインストールされ、ネットワーク上の全ホストの名前解決は、「192.168.0.251」のDNSサーバを利用する。DNSサーバは、インターネット上の「root.server」や「gtld.server」に反復クエリーを実行して、任意のホスト名を解決する。

ブロードバンドルータの位置には、もともとISDNダイヤルアップルータがあった。ISDNダイヤルアップルータをそっくりそのままADSL用のブロードバンドルータに置き換えれば、ネットワークの変更点は少なくて済む。

まずは、ブロードバンドルータにデフォルトで設定されている「192.168.0.1」を変更する。「192.168.1.250」のIPアドレスを持つルータ1のインタフェースに「192.168.0.2」を一時的に付与した。この間、「192.168.0.0/24」のネットワークは、「192.168.1.0/24」のネットワークと一時的に通信できなくなる。続いて、ルータ1からブロードバンドルータに接続して、LAN側のIPアドレスを変更した。変更後は、ルータ1のNICから一時的に付与したIPアドレス「192.168.0.2」を削除した。このように、Windowsで構成されたルータのNICは、IPアドレスを自由に変更できるので便利だ。

ブロードバンドルータには、ISPとの接続情報を設定する前にセキュリティを考慮して、フィルタ設定をしておく。そして、ルータ1が接続されているもう1つのネットワーク「192.168.0.0/24」のルーティング情報をブロードバンドルータに設定すれば、す

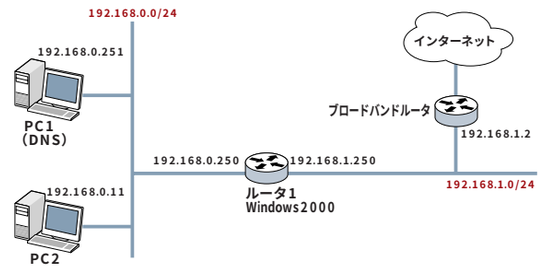


図15●　ADSL開通と同時にブロードバンドルータを導入した自宅のネットワーク構成

ぐに使用できるはずだ。ルータ1では、次のようにルーティング情報を設定した。

```
route -p add 0.0.0.0 mask 0.0.0.0 192.168.1.2
```

つまり、自分で解決できないルーティングは、すべてブロードバンドルータに任せることにしたのだ。ところが、いざ「192.168.0.0/24」のネットワークからインターネット上のWebサイトにアクセスしても、閲覧ができないのだ。

トラブルシューティングの開始である。まずは、ルータ1からブロードバンドルータのIPアドレスに対して、pingを実行してみると、正常なリプライがある。続いて、インターネット上の任意のホストに対して、FQDN（Fully Qualified Domain Name）でpingを実行すると、リプライが戻らない。ところが、同じくIPアドレスでpingを実行すると、リプライがある。どうやらDNSの名前解決で失敗しているようだと筆者は判断した。

そこで、ルータ1からブロードバンドルータに接続する。ISPのサーバから振られたWAN側インタフェースのIPアドレスと、ISPのDNSサーバのIPアドレスを確認するためである（画面15）。

筆者が利用しているISPでは、ローカルPCのIPアドレスとISPのDNSサーバのIPアドレスも自動配布する。このような場合、ブロードバンドルータをDHCPクライアントとして設定すれば、ISPを通してインターネット上の任意のホストと通信できる。実際、ルータ1からISPのDNSサーバのIPアドレスに対して、pingを実行すると、リプライがある。つまり、DNSサーバには到達できている。それではどこで、名前解決に失敗しているのだろうか。

ISPのDNSサーバのホスト名は、ブロードバンドルータに振られたIPアドレス情報からは判断できないので、tracertを使うことにした。筆者は通常、tracertのリプライ結果だけを知りたいので、「-d」オプションを実行する。こうすれば、経路上のルータのホスト名解決を行わない。今回は逆に、「-d」オプションなしで、「tracert <ISPのDNSサーバのIPアドレス>」を実行した。しかし、ホスト名は解決されない。

画面15●　ISPが配布するIPアドレス情報の一例

続いて、ノートブックPC（PC3）を「192.168.1.0/24」のネットワークに接続した（図16）。ここでは、デフォルトゲートウェイをブロードバンドルータのIPアドレスに設定する。また、DNSサーバのIPアドレスは、LAN内にあるローカルDNSサーバを利用せず、ISPが提供するDNSサーバのIPアドレスに設定する。その結果、インターネット上の任意のWebサイトを閲覧できるし、pingも成功した。ISPのDNSサーバのIPアドレスに対して、tracertを実行しても、ホスト名を解決した。さらに、ブロードバンドルータのDNS転送機能を試すと、ブロードバンドルータのLAN側のIPアドレスをDNSサーバのように利用でき、こちらもWebサイトの閲覧とpingは成功した。

ブロードバンドルータのDNS転送機能とは、クライアントPCの名前解決クエリーをブロードバンドルータがDNSサーバのごとく解決する機能である。ブロードバンドルータは、DNSサーバではないので、自分では名前解決を行わない。しかし、ブロードバンドルータに設定されているDNSサーバのアドレスにクエリーを転送して回答を得る。その回答は、クエリーを発信したクライアントに転送される。つまり、クライアントはブロードバンドルータをDNSサーバーとして利用できるのだ。ほとんどの一般家庭用ブロードバンドルータに実装されている。Windows2000/XP/2003でも、インターネット接続共有やNATを構成すると、DNS転送機能が利用できる。

リモートへのルーティング機能が無効

上述の原因調査からは、LANに設置されているローカルDNSサーバが名前解決に失敗していることが判明した。しかし、ブロードバンドルータ導入してもネットワーク上の変更点はない。IPアドレスも以前のままである。どのような理由があるのだろうか。

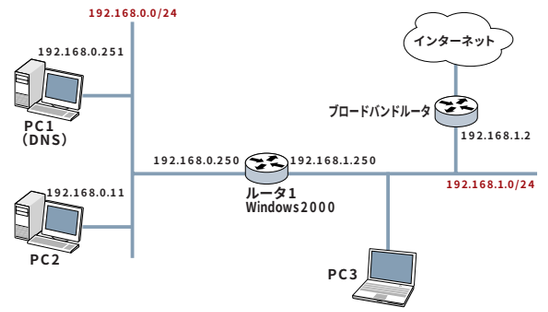


図16●　ルータセグメントにPC3を接続して、ブロードバンドルータとPC1・PC2との接続を確認する

この原因調査のため、ローカルDNSサーバがある「192.168.0.0/24」上のPCから、インターネット上の任意のホスト（例えばISPのDNSサーバ）に対して、pingを実行してみた。すると、リプライがない。さらには、ブロードバンドルータに対して、pingを実行しても、成功しないのである。どうやらブロードバンドルータに原因があるらしい。つまり、ルータ1からは、ブロードバンドルータに接続できるが、DNSサーバのPC1からは、ブロードバンドルータに接続できないのである。ルータ1のルーティングが機能しなくなったのだろうか。

ルータ1の正常なルーティング機能を確かめるには、PC3を利用する。PC3で次のrouteを実行して、「『192.168.0.0/24』への経路はルータ1が知っている」という情報を設定した。

```
route add 192.168.0.0 mask 255.255.255.0 192.168.1.250
```

設定後に、PC3からPC1へpingを実行するとリプライがある。また、PC1からPC3へも同様にリプライがある。ルータ1は、ルータとして機能していることは証明できた。そこで次に、これまで使用していたISDNダイヤルアップルータを接続して、LAN側IPアドレスに「192.168.1.3」を設定した（図17）。

当然、ISDNルータには「『192.168.0.0/24』への経路は、ルータ1が知っている」という情報を設定した。ここで、「192.168.0.0/24」に所属するPC1とPC2からISDNダイヤルアップルータに対して、pingを実行するとリプライがある。「192.168.0.0/24」から、ISDNルータへの通信が成功することを確認してから、インターネットへの出口経路を変更してみることにした。まず、ルータ1でブロードバンドルータをデフォルトゲートウェイとするルーティング情報を削除する。続いて、ISDNダイヤルアップルータをデフォルトゲートウェイとするルーティング情報を設定した。次のコマンドを使う。

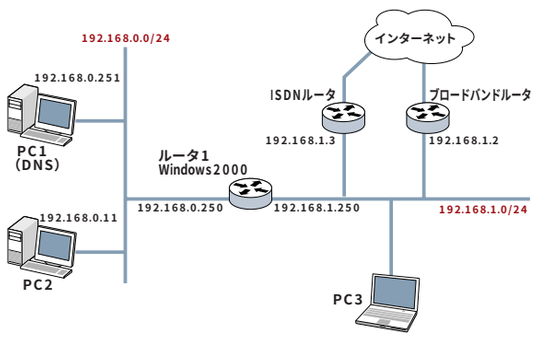


図17●　これまで利用していたISDNダイアルアップルータを、再度インターネット接続に利用する

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.3
```

これでルータ1は、インターネットへの経路をブロードバンドルータからISDNルータに変更する。「192.168.0.0/24」からインターネットへの通信トラフィックもISDNルータを経由する。「192.168.0.0/24」からインターネット上の任意ホストへ通信してみると成功する。Webサイトも閲覧できるし、pingも成功する。つまり、ISDNルータならば通信でき、ブロードバンドルータでは通信できないのだ。ブロードバンドルータと接続され、同じセグメントにあるホストは、ブロードバンドルータと通信できるし、インターネットへも通信可能だ。一方、ルータ1を介して接続するホストは、ブロードバンドルータと接続できない。リモートセグメントのホストが、ブロードバンドルータと同じセグメントにいる別のホストに対して、pingを実行するとリプライがあるのに、ブロードバンドルータに対してのpingではリプライがない。どうやらブロードバンドルータに設定したリモートセグメント「192.168.0.0/24」への静的ルーティング設定が機能していないようだ。

サポートセンターに電話すると…

この現象を確認するのに適しているのが、Windowsのネットワークモニタである。ルータ1の「192.168.1.250」のインタフェースで起動し、「192.168.1.0/24」のネットワークセグメントのトラフィックをキャプチャする。無関係なトラフィックは非表示にして、pingが利用しているICMPだけを表示する。その結果、PC1からブロードバンドルータへのpingは、「192.168.1.0/24」のネットワークに届いてはいるが、リプライがない。PC1やPC2からISDNルータへのpingには、「192.168.1.0/24」のネットワークに届いているだけでなく、リプライも表示されている。これでブロードバンドルータの静的ルーティング設定が機能していないことが判明した。しかし、この理由は筆者にもわからない。

ブロードバンドルータのメーカーに連絡を取ると、「ブロードバンドルータとネットワーク上のPCは、IPアドレスがバッティングしていないでしょうか？」など初歩的なことを質問され、「筆者の設定がまちがっている」という。

そこで、筆者が実施した検証内容やネットワーク構成図、そのほかネットワークモニタのキャプチャファイルを送付した。メーカー側でも、ブロードバンドルータのLANポートにPCを直接つなぐ構成ではなく、ほかのルータを接続してリモートネットワークから通信を試みる実験を行ったようだ。結果は、筆者の環境と同様、リモートネットワークへのリプライはなかった。この原因は、ファームウェアのバグにあるという。本来LAN側

に送出するはずのフレームをWAN側に送出してしまうという。その後リリースされた修正ファームウェアを適用したが、LAN側ポートに設定した静的ルーティングは有効に機能しないままだったので、結局返品するはめになった。

実は、この製品の不具合は、あまり話題にならなかった。それは、このブロードバンドルータが一般家庭向けの製品だからだろう。企業ユーザーであれば、LAN側ポートと同じセグメントに、1つだけのネットワークを構成する例はあまりない。さらに、その先にリモートネットワークを接続するためのルータが何台も存在する大きな構成をとる。DNSサーバもLAN内に設置される。トラフィックも大容量になるから、ブロードバンドルータではなく、高価なルータを使用する。しかし、個人ユーザーがブロードバンドルータのLAN側セグメントにルータを設置することは少ないだろう。DNSサーバも、ブロードバンドルータのDNS転送機能やISPのものが利用される。筆者が経験したようなトラブルに遭遇する機会はあまりないと思われるが、トラブルシューティングの過程では、ハードウェア障害も見過ごしてはいけない。

イベント開催中に突然つながらなくなった!

公衆無線LANサービスで認証エラー

現象▶ 二重ログインでアクセスできない

モバイルPCのスタンバイ状態

「HOTSPOT」(NTTコミュニケーションズ)や「Mフレッツ」(NTT東西)、「FREESPOT」(FREESPOT協議会)などが提供する公衆無線LANサービスが広がりを見せている。また、「CPU」「チップセット」「内蔵無線LANカード」を組み合わせたインテルのCentrino搭載PCも次々と発売され、公共施設やファーストフード店などで無線LANが気軽に利用できるになった。事例6では、筆者が公衆無線LANサービスを無料体験してもらう12日間のイベントに携わったときのトラブルを紹介する。

通常、公衆無線LANサービスを利用するには、IDとパスワードを使ってログインする。一方、公衆無線LANサービスのユーザーは、PCの利用を中断する際、その後すぐに利用できるように、液晶パネルのフタだけを閉じてスタンバイ状態にしていることが多い。このスタンバイ状態は、通常の有線LAN環境であれば、ネットワークからの切断を意味する。

ところが、無線LAN環境ではたびたび電波が途切れる「瞬断」が発生する。そのため、明示的にログアウトされないかぎり、しばらくはログイン状態が継続される必要がある。つまり、公衆無線LANサービスを提供する側では、スタンバイ状態のPCでもログイン中として認識しているのだ。ただし、「タイムアウト」が設定され、信号が途絶してから一定時間が経過すると自動ログアウトされるようになっている。明示的なログアウトがない場合でも、別の地域に移動したユーザーの二重ログインを回避するのが目的だ。

明示的にログアウトしないと…

今回の無料体験イベントでは、10台のノートブックPCを持ち込み、初日に全PCが公衆無線LANサービスでインターネットに接続できることを確認した。さて、初日のイベントが終了したところで、公衆無線LANサービスからは明示的にログアウトせず、OSを終了させた。翌朝の接続設定の手間を省くためである。実際、利用した公衆無線LANサービスは、タイムアウト時間が比較的長く設定されているようで、2日目にノートブックPCの電源を入れると、ログインされた状態が続き、IDとパスワードを入力しないでもインターネットに接続できた。利用した無線LANサービスのタイムアウトまでの時間は、PCの電源を落としたイベント終了の18時から翌朝9時までの15時間以上に設定されていると判断した。

ところが、この方法がトラブルを招くことになる。3日目の朝一番にPCを起動すると、初日にIDとパスワードを入力した「ログイン画面」が再び表示されたのだ。ログインを試みると、「認証エラー」という理由で、公衆無線LANサービスに接続できない。もちろん、IDとパスワードは前日のまま変更していない。そのほかの理由も思い当たらないので、公衆無線LANサービス自体の障害を疑って、サービス提供会社に電話で確認してみた。その結果、「二重ログイン状態が原因で、接続が拒否されている」と回答されたのだ。

すでにログインしているIDを利用して、別のPCからログインすると「二重ログイン」になるのは理解できる。一方、今回の公衆無線LANサービスでは、PCとIDの組み合わせを変更していない。そのため、明示的にログアウトしない場合でも、二重ログインとして扱われないはずだろう。ところが、ほとんどのPCで、二重ログイン状態によるログイン拒否が発生してしまった。また、すべてのPCは同じ時間帯で利用しているにもかかわらず、一部のPCは正常に接続できている。この理由もわからない。

結局、今回のトラブルは、毎日終了時に明示的にログアウトして、再ログインすれば、簡単に解決できることが判明した。筆者は、さらに使い勝手をよくするため、無線LANサービスの提供会社に全PCのMACアドレスを登録してもらい、イベント期間中は明示的にログイン／ログアウトしなくても、利用できるようにしてもらった。しかし、この対策法は、イベントのように公衆無線LANサービスを毎日、同じPCで利用するケースでしか活用できない。しかも、一般利用者の場合、公衆無線LANサービスの提供会社に、MACアドレスの登録を依頼することはないだろう。公衆無線LANサービスでは、あくまで契約者のIDが認証に利用される。同じような現象に遭遇したら、明示的なログイン／ログアウトを試してもらいたい。

トラブル事例 7

有名ポータルサイトは閲覧できるのに…

公衆無線LANサービスでDNS名前解決ができない

現象▶ 一部のWebサイトが404エラーを表示　コマンド▶ ipconfig　ping　nslookup　tracert

PHSからは閲覧できるのはなぜ？

事例6で紹介した公衆無線LANサービスの無料体験イベントでは、もう1つ別のトラブルが発生した。イベントの3日目に一部のWebサイトが閲覧できなくなってしまったのだ。イベント会場からのアクセス数が多い人気ポータルサイトは閲覧できるが、たまにしかアクセスのないWebサイトが閲覧できない現象である。閲覧できないWebサイトでは、「404エラー」が表示される。このトラブルが発生した当初、筆者はWebサーバがメンテナンス中でダウンしているのだろうと対策を取らなかったが、複数のWebサイトが閲覧できない状況が続くと、別のトラブルが原因である可能性が高い。

トラブルシューティングの開始である。まずは、PHSでISPにダイヤルアップ接続を行い、公衆無線LANサービスで閲覧できないWebサイトにアクセスを試みた。すると、これが問題なく閲覧できるのである。さらに近くにあったISDN公衆電話（グレー電話）で、同様に試みたところ、これもまた閲覧できるのである。この結果、現在利用している公衆無線LANサービスとインターネットまでの経路上に障害が起きている可能性があると判断した。

そこで、「ipconfig /all」でTCP/IP設定の確認を行う。今回の公衆無線LANサービスでは、DHCPでIPアドレスを付与しているので、次の3点を確認すればよい。

❶IPアドレス（APIPA機能が動作していないことを確認）
❷デフォルトゲートウェイのIPアドレス
❸DNSサーバのIPアドレス

この調査の結果、DHCPサーバからIPアドレスは付与されており、APIPAのIPアドレスではないことも判明した。デフォルトゲートウェイも正常である。また、イベント参加者の多くが閲覧する有名ポータルサイトには正常にアクセスできる状況から、ローカルネットワークからリモートネットワークへの経路も保たれていると考えてよい。もっとも、一部にせよインターネット上のWebサイトは閲覧できているので、APIPAのアドレスが付いていることはまずない。APIPAのIPアドレスの場合、ルータは越えられないからだ。

続いて、404エラーが表示されるWebサーバのIPアドレスにpingを実行するとリプライがあった。これは、PHSで接続したときに解決したホスト名とIPアドレスの対応結果を基にしている。この結果、IPアドレスでは通信できるので、Webサーバは起動しており、そこまでの経路も落ちていないことがわかった。

キャッシュの存在に気が付く

筆者は、DNSの名前解決で失敗している可能性を疑った。名前解決のクエリーがDNSサーバへ到着していないかもしれないのだ。通常、IEなどのブラウザのアドレス欄に、IPアドレスを入力するのは、ホスト名がないなど、特別の事情があるときにかぎる。PCどうしは、IPアドレスで相手を特定するが、人がインターネット上のホストと通信するときは、ホスト名で通信する。その際、DNSによってホスト名とIPアドレスの対応付けが解決される。これがうまくできないと通信は成功しない。IPアドレスのpingに対してリプライがあっても、ホスト名のpingでは、名前解決のプロセスで失敗していると通信も失敗する。

実際、イベント会場のクライアントPCが公衆無線LANサービスで利用する2台のDNSサーバに、pingを実行してもリプライは1台からしかない。nslookupで接続できるDNSサーバも1台だけである。また、イベント会場で閲覧可能な人気ポータルサイトのホスト名でDNSサーバにクエリーを投げると、次のような文字列のリプライがあった（画面16）。

Non-authoritative answer:

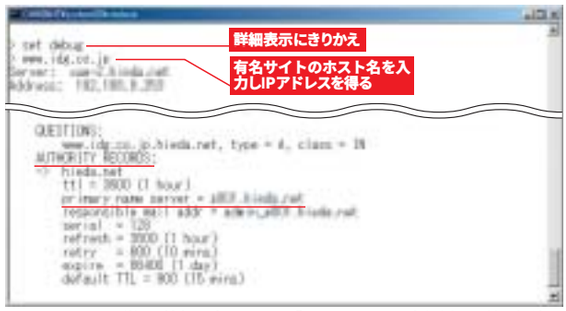
この文字列は、以前に解決したクエリー結果のキャッシュによって、今回のクエリーを解決したという意味を表す。通常なら、閲覧できないWebサイトのクエリーでは、「timeout」と表示される。さらに、詳細な情報を表示させるために「set debug」を実行して、クエリーを投げる（画面17）。ここでは、rootを表す「.」を付けないで、「AUTHORITY RECORDS:」を表示させる。その結果、pingでリプライがないほうのDNSサーバが、AUTHORITY RECORDSの「primary name server」に設定されていることがわかった。

ローカルネットワーク上に複数のDNSが存在する場合、インターネット上の名前解決を行うDNSサーバを1台に設定するのはよくあるケースだ。名前解決のトラフィックを削減するのが目的である。このとき、インターネット上へ解決クエリーを要求するDNSサーバに対して、ほかのDNSサーバが解決クエリー要求をする動作を「フォワーダ」という。

今回のネットワークでは、クライアントPCから通信できるDNSサーバ（セカンダリDNSサーバ）の「フォワーダ」先として、もう1台のDNSサーバが設定されていた。つまり、クライアントPCから通信できるDNSサーバが解決できないホスト名は、フォワーダ設定されている「primary name server」が解決しなければならない。

しかし、この「primary name server」は、クライアントPCからのpingとnslookupコマンドにリプライがない。そのため、このDNSサーバに障害があるか、DNSサーバまでの経路上に障害があるのではないかと推測できる。

画面16●　まだ閲覧できる人気ポータルサイトのホスト名でDNSサーバにクエリーを投げるとリプライがある



画面17●　より詳細な情報を表示できる「set debug」の実行例。以前に解決したクエリーをキャッシュとして保持する時間もわかる

有名ポータルサイトのWebサイトだけが閲覧できるのは、クライアントPCから通信できるDNSサーバが以前に解決したクエリー結果のキャッシュを持っているからだろう。一方、キャッシュを持っていないWebサイトは、クエリーを解決できていない。

「primary name server」のIPアドレスをインターネット上のwhoisサービスで確認すると、この公衆無線LANサービスを提供する会社が用意したものではなく、ISP-Aのサーバである。クライアントPCから通信できるDNSサーバは、この会社で用意していることもわかった（図18）。

続けて、クライアントPCから接続可能なインターネット上の任意のサーバに対して、tracertを実行すると、ISP-Aとは別のISP-Bを経由してインターネット上に出た。どうやら、DNSクエリーのトラフィックはフォワーダ先であるISP-AのDNSサーバを経由して、そのほかのトラフィックはISP-Bを経由するように設定されている。

再度、PHSからダイヤルアップでインターネットに接続して、ISP-AにあるDNSサーバに、pingとnslookupでアクセスしてみると、これが問題なくリプライされたのである。この結果、公衆無線LANサービスが利用しているISP-AのDNSサーバまでの経路上に何らかの障害があると予測できる。

ここから先のトラブルシューティングは、公衆無線LANサービスを設置している会社の担当者に頼らなければならない。今までの調査から判明したことを伝えると、どうやら思い当たる節があるらしい。担当者の説明によれば、この会社とISP-A間で使用している帯域は、DNSサーバへのホスト名解決トラフィックのために、飽和状態になっていて、ホスト名解決に失敗する現象は以前から発生していたという。そこで今回の対処法として、ローカルネットワークとISP-Aとの間にある複数の回線の中から、帯域に余裕のある回線を使用して、名前解決を行うように切り替えた。この対処のあとは、404エラーが表示されていたWebサイトも閲覧できるようになった。

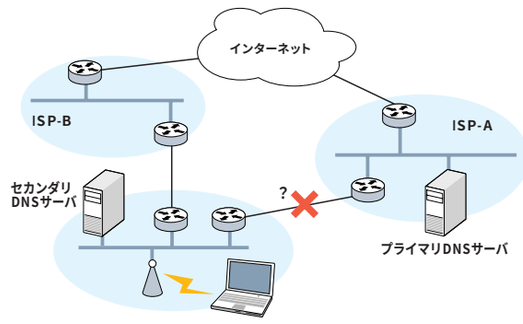


図18●　イベント会場からインターネットまでのネットワーク構成。プライマリDNSサーバはISP-A、セカンダリDNSサーバはイベント会場内に設置されている