# ネットワークトラブルシューティングと<br>トラブルに強いネットワークの構築

岡本 久典（(株）NTT データ）

近藤 邦明（(株）インターネットイニシアティブ）

1998 年 12 月 15 日

Internet Week 98　国立京都国際会館

（社）日本ネットワークインフォメーションセンター編

# 目次

# 1　概要

このチュートリアルでは、次の内容を取り上げます。

- ネットワークの障害と概要
- 実際の障害に対応するプロセスモデル
- 障害に強いネットワークを構築するポイントと実例
- ケーススタディ

# 2　ネットワーク障害の概要

## 2.1 ネットワーク障害の種類と概要

ネットワークの障害には様々なものがありますが､次のように対応するネットワークレイヤに分類して把握すると分かりやすくなります。

- 回線障害　　レイヤ 1
- ネットワーク機器障害　　レイヤ 2
- ルーティング障害　　レイヤ 3
- サーバ機器障害　　レイヤ 3、4、5
- アプリケーション障害　　レイヤ 5、6、7
- 情報伝達ミスなど人為的障害　　レイヤ 8（?）

図に示したように、それぞれの障害は、レイヤをまたがることがあります。そのために、自動的な監視ではなく、人手による監視と対応が必要となります。

## 2.2 回線障害

レイヤ 1 にあたる回線障害には、次のようなものがあります。

- 専用線交換機の異常
- 回線提供業者の設定ミス
- 回線設定業者と回線利用者の情報伝達ミス
- 回線利用者の機器トラブル

これらの障害の特徴は、回線利用者によってコントロールできる部分が少ない点にあります。

## 2.3 ネットワーク機器障害

レイヤ 2 にあたるネットワーク機器障害は、まず最初に疑うべき障害です。この障害には次のようなものがあります。

- ハブ、ルータの故障～電源障害もある
- ケーブルの損傷～実効速度の大幅な低下などで現れる

これらの障害が発生した場合、ネットワークが分断されたり、ネットワーク全体が停止してしまったりすることがあります。

## 2.4 ルーティング障害

レイヤ 3 にあたるルーティング障害には、次のようなものがあります。

- ルータ・ソフトウェアのバグ～バグ情報をチェック
- ルータの設定ミス
- 外部からの不正経路情報
- 外部からの不正アクセス

これらの障害が発生した場合、パケット伝送の一部や全体に障害が発生します。過負荷によって、ルータが制御不能となることもあります。

## 2.5 サーバ機器障害

レイヤ３～５の広範囲に現れるサーバ機器障害には、次のようなものがあります。

- ディスク容量あふれ～ログファイルなど
- サーバのカーネルの不具合～コンフィギュレーションのミス
- 外部からの不正アクセス

これらの障害が発生した場合の影響範囲は狭く、サーバ機器自体へのアクセスが不能となることが考えられます。

## 2.6 アプリケーション障害

レイヤ５～７の広範囲に現れるアプリケーション障害は、アプリケーション毎に機能が閉じているのが特徴です。この種の障害には、次のようなものがあります。

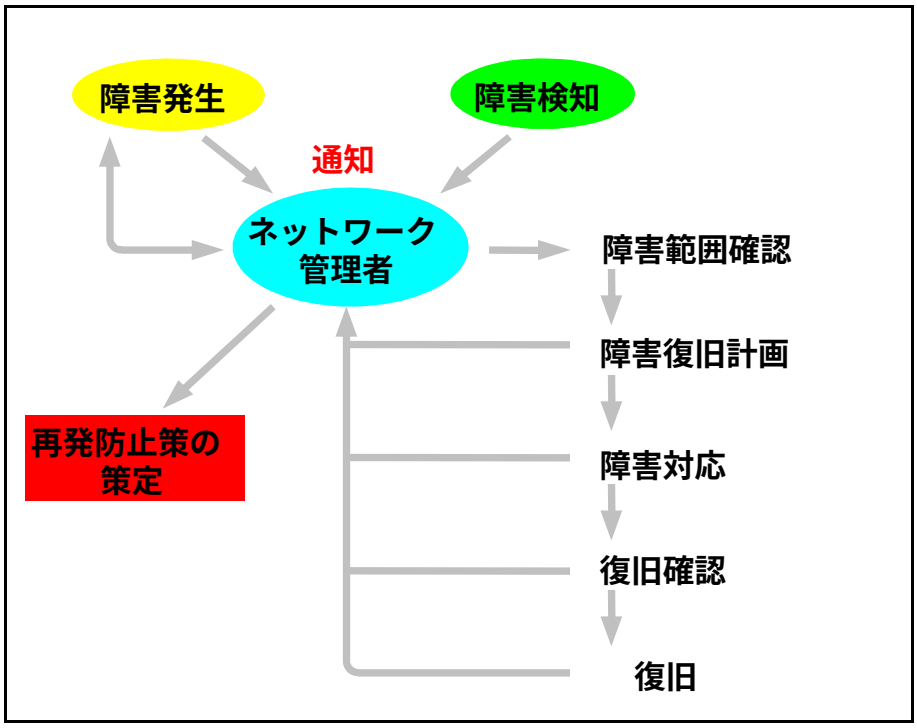
- アプリケーションのバグ
- アプリケーションの設定ミス
- アプリケーションが停止している
- 外部からの不正アクセス

これらの障害の特徴は、サーバ自体にはアクセスできるものの、目的のプロトコルによるアクセスが不能になることです。

このように障害の種類と症状は様々ですので、ユーザからのクレームだけでは、症状や原因を追及することが困難です。障害をレイヤ毎に分けて分析するのが、原因追及の近道です。

# 3　障害対応のプロセスモデル

障害が発生した場合の対応方法は、障害発見から、完全な復旧と再発防止策に至るまでのプロセスモデルとして定義すると良いでしょう。




すなわち、次の 3 つのステップに分けられます。

1. 障害の発見と確認
2. 障害への対応と経過の報告（記録）
3. 復旧の報告と再発防止策の策定

## 3.1 障害の発見と確認

まず、障害情報をいかに収得するかが問題となります。ユーザからのクレームで障害の発生を知る場合は、問い合わせる情報を定型化しておくと便利です。たとえば、ソースホストとディスティネーションホスト、利用したプロトコル、障害発生時のネットワークの状況などです。

続いて、障害による影響範囲を確認します。障害が発生した時のネットワーク状況～アプリケーションの稼働状況や、他の障害が発生していないかを確認します。さらに、ネットワーク機器に関連するログが記録されていないかを確認すると良いでしょう。この時、IP だけではなく他のプロトコルも使用している場合には、そのプロトコルの稼働状況が重要なヒントとなる場合があります。

得た情報を元に、障害が発生しているレイヤを「推測」します。特に、レイヤ 3（IP 層）より上か下かを確認することが有用です。ping が通ればレイヤ 3 以上であることが疑われますし、通らなければレイヤ 3 以下であることが疑われます。さらに、telnet で目的ホストの該当ポートにアクセスして、アプリケーションの動作を確認することが有用です。

## 3.2 障害への対応と報告（ログ）

実際に障害が発生していることが確認できたならば、影響範囲や詳細な症状、および復旧予定時刻などをユーザに通知します。もちろん、通常の動作であれば、その旨を通知することも必要です。ユーザに報告しない場合であっても、記録をログとして保存することは有用でしょう。

障害への実際の対応として、次のようなものが挙げられます。

- ハードウェア障害
  →機器の交換
- 特定パケットの障害
  →ファームウェアのアップデート
  →バグ情報の確認
  →ソフトウェアのアップデート
- ネットワーク構成の変化による障害〜機器やトラフィックの増加時に障害が発生することが多い
  →ネットワーク構成の変更
  →回線の増強
  →インタフェースの交換

障害への対策を施したならば、復旧したことを確認しなければなりません。対策後のネットワークの状態について、しばらくの間様子を見ること、障害を意味するログを確認すること、利用者に確認すること、などが必要です。

## 3.3 復旧の報告と再発防止策の策定

障害から復旧した場合、特に原因が人為的ミスであった場合には、障害を記録しておくことが必要です。障害の時間帯、箇所、機器名、障害の状態、復旧方法などを記録しておくことが、今後のノウハウの蓄積になります。また、すぐに復旧しなかった場合〜回線容量不足など〜には、考えられる対応策を記録しておきます。

さらに、障害の発生を防ぐために、原因を明確にして、あくまでも現実的な範囲内で再発防止の対策を講じることが必要です。現実性のない対策案は意味がありません。

# 4　障害の発見と切り分け

障害を発見する方法は、次の 3 つに大きく分けられます。

- 管理ツールなどによる～作り込むことが可能
- ユーザからの不具合連絡
- 通信先（他 ISP や通信相手企業）からの不具合連絡

ISPか企業ネットワークかによりますが､基本的な流れは同じと思われます。

発見した障害の原因を切り分けるには､ユーザから通知してもらう情報を定型化しておくことが役に立ちます。また、過去の障害履歴を残しておけば、それを検索することも有用でしょう。その後、障害レイヤを推定し、障害箇所を特定します。障害箇所の特定には、ping、traceroute、telnet などのツールや、ネットワーク機器のログ情報が極めて有用です。

# 5　障害に強いネットワーク

では、ここから、実際に障害に強いネットワークを構築するために、設計の段階から考慮しなければならない点をまとめてみましょう。

## 5.1 電源

電源に関する問題はあまり考慮されない場合が多いのですが､実は非常に重要です。ネットワークを敷設する際には、多くの機器を設置しますので、フロア毎に必要となる電源容量を計算しなければなりません。

必要な電源容量は、機器によって表記が異なることに注意して、VA を単位として計算を行います。一般に誤解されているようですが、
「$W = V \times A \times \cos\theta$」であり、コンピュータ機器の場合には、
$\theta = 30 \sim 60$ になりますから、W よりも VA の方が大きくなるのです。

また､電源容量を計算する場合には､電源投入直後に大きな電力が消費されることに注意します。通常時の電力で計算すると、全機器が一斉に立ち上がるときに電力が不足しますから､全館停電後､機器が一斉に自動再起動した場合などに、問題が発生することになります。

電源ユニットを 2 つ持っている機器の場合､障害時には 1 つの電源ユニットにかかる負荷が倍になることにも注意が必要でしょう｡複数の電源ユニットを持つ機器では、それぞれの電源ユニット毎に、異なるブレーカーに繋がったコンセントから電源を供給することが重要です。1 カ所の障害で、両方が同時に使用不可能とならない配線を考察し､それぞれのラックに 2 系統の電源を引き込むと良いでしょう。

コンピュータやネットワーク機器は､スイッチング電源を使用しているために､筐体自体をアースに落とす必要があります｡特に多くの機器を､アース線のあるケーブルで接続する場合（シリアル､パラレル､CRT など）には､電位差が累積されないように､筐体を共通するアースに取るべきです｡3 ピンのアース付きコンセントがあるならば､2 ピンのコンセントに変換するアダプタを使わないようにします｡

## 5.2 ケーブル

ケーブルには様々な種類があります｡ネットワーク用のケーブルの種類毎に､特徴をまとめておきましょう｡

### 5.2.1 ツイストペアケーブル

現在､よく使われているツイストペアケーブルは､撚り対線によってノイズの飛び込みを軽減しているもので､クロストークとノイズに対する性能によって､カテゴリ 3 ～ 5 までが決められており､それぞれに上限の伝送速度が決められています｡

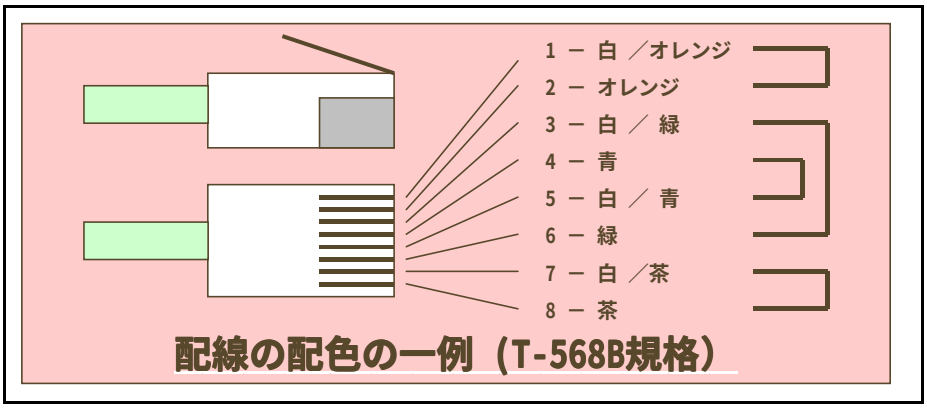
- カテゴリ 3　～ 10Mbps
- カテゴリ 4　～ 20Mbps
- カテゴリ 5　～ 100Mbps
- エンハンスド・カテゴリ 5　～ 1Gbps（?）

カテゴリ 5 では､コネクタにケーブルを差し込むときに､撚り対をほぐす長さも決まっているので（～ 13mm）注意しましょう｡

ツイストペアケーブル用のコネクタには､次の 3 種類があります｡

- RJ11　6 極　電話用
- RJ45　8 極　LAN/ISDN 用
- RJ48　8 極突部有り　ISDN 新規格用（INS1500）

なお、それぞれのピンに接続するケーブル内部の色は、次のように決められているので、ケーブルを自作する場合などには、規格に沿って統一しておきましょう。




ツイストペアケーブルには、撚り対と被覆との間のシールドの有無によって、Un-shielded Twist Pair（UTP）と、Shilede Twist Pair（STP）に分けられます。100Mbps を超えると、ツイストペアケーブル自体から雑音が発生しますから、ノイズ規制の厳しいドイツや病院では STP が使われます。STP ケーブルは、コネクタも UTP とは異なります。

また、ツイストケーブル内部のケーブルが単線であるか撚り線であるかという違いもあります。自作する場合には内部のケーブルが単線のものの方が楽ですが、撚り線であるものの方がケーブルが柔らかいのでパッチケーブルなどには利用しやすいでしょう。コネクタによっては、単線のみ、あるいは撚り線のみしか使えないものがありますので、注意が必要です。

### 5.2.2 同軸ケーブル

ネットワークで使用する同軸ケーブルは、インピーダンスの違いによって 2 種類に分けられます。

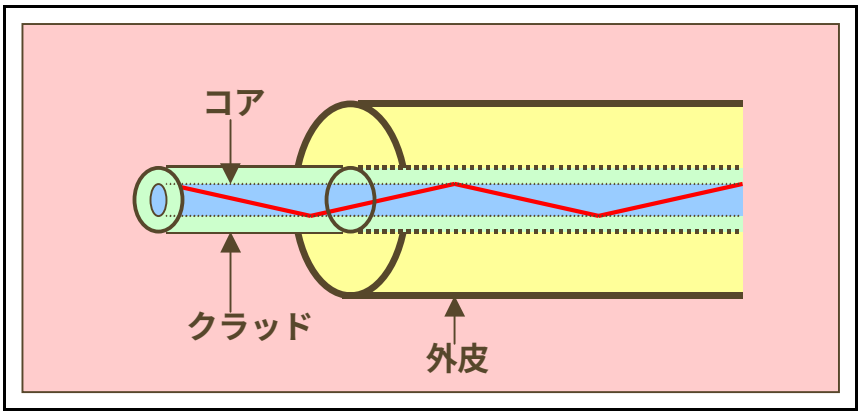
- 50Ω
  - 主に LAN 用（10BASE-2 など）
  - JIS 規格：3D2V
  - 米軍規格：RG-58A/U
- 75Ω
  - WAN 用（T3、DS3 など）
  - JIS 規格：3C2V
  - 米軍規格：RG-59A/U

コネクタとして、BNC が主に使用されます。

### 5.2.3 光ファイバ

ネットワークの高速化に伴って、光ファイバに注目が集まっています。

光ファイバの基本的な構造を示します。入力された光は、クラッド内を反射しながら進んでいきます。




ネットワークに使用される光ファイバは、クラッド径が 125μm のものが使われており、コア径によって何種類かに分かれています。シングルモードファイバでは、コア径が 10μm 以下のものが使われています。マルチモードファイバには、コア径が 50μm のものと 62.5μm のものがあり、米国では 62.5μm のものが、日本では両方が使われています。

光ファイバの特性は、波長・伝送損失・伝送帯域などで表されます。最近、よく使用されているのは 50μm のダブルウィンドウ（850nm と 1300nm）のものが、ギガビットイーサネットの登場などによって主流になりつつあります。シングルモードファイバでは、複数の波長を使用する WDM に使用できるものが主流になると思われます。

光ファイバで使用するコネクタには、次のような種類があります。

- SC
  プラスチックの角形モールドタイプ。2 つが連結した SC-Dual というものもあります。ATM や 100BASE-FX などで使用されます。
- ST
  1 芯毎に金属製の爪でツイストロックするタイプのものです。ATM や 100BASE-FX などで使用されます。
- MIC
  2 芯が 1 セットになっているプラスチックモールドタイプのもので、主にマルチモードファイバで使用します。FDDI でケーブルの種類を見分けやすいように、A/B/M の形状が違います。主に FDDI で使用されます。

- FC
  1 芯毎にツイストロックするタイプのもので、ST コネクタと似ています。10BASE-FL などで使用されます。

逆に、ネットワーク種別からコネクタを分類すると、FDDI では MIC コネクタが、その他のネットワークでは SC コネクタ（新しいもの）と ST コネクタ（古いもの）が使われます。10BASE-FL では FC コネクタが主に使用されます。

## 5.3 ケーブリングの注意

障害に強いネットワークを実現するためには、問題のあるネットワークの部位を見つけるのが容易であることが必要です。

各ケーブルに起点と終点、ID、ケーブル長を明示したタグを付けておくことが有効です。ケーブル種別や、ネットワーク毎に、ケーブルやコネクタの色を変えるのも有効でしょう。なお、ケーブルを延ばす時には、ねじれが発生しないように注意して、ケーブル同士が絡み合わないようにします。

### 5.3.1 ツイストペアケーブル固有の注意点

ツイストペアケーブルの場合は、電源からのノイズを避けるために、電源ケーブルなどと平行するケーブリングを行わないことが注意点として挙げられます。特に、フリーアクセスのフロアでは、支柱 1 本程度の空間を開けるようにします。

また、ツイストペアケーブルには、ケーブルを折り曲げたり、ねじったりすると伝送距離が短くなり、エラー率が高くなるという特徴があります。最低でも、折り曲げ半径 10cm は取るようにしましょう。

### 5.3.2 同軸ケーブル固有の注意点

同軸ケーブルの場合は、個々の機材に合った、起点から終点まで同じインピーダンスのケーブルを使用することが注意点として挙げられます。インピーダンスが異なるケーブルを接続すると、反射波によって波形が乱れるのです。同軸ケーブルに使用するコネクタ類にもインピーダンスがあるので、注意しましょう。

### 5.3.3 光ファイバ固有の問題点

光ファイバの場合は、光ファイバが折れることを避けること、および内周と外周で反射率が変わるのを防ぐために、最小折り曲げ半径を最低でも 10cm 程度とすることが、注意点として挙げられます。

また、マルチモードファイバの場合には、ケーブルの混用に気を付けてください。混用すると反射波によってトラブルの元となります。もっとも、光ファイバはネットワーク全体で統一する必要はなく、機器間が 1 種類のファイバで接続されていれば十分です。

なお、光ファイバの敷設時には、ケプラーコートされた折れにくいケーブルを使用したり、保護用パイプやリボンケーブルなどを使用したりして、ファイバを保護しておくと良いでしょう。

## 5.4 LAN

最近の LAN において、ネットワーク種別毎に障害が発生しやすい箇所について説明しますので、設計の際に参考にしてください。

代表的なネットワーク種別は、次のように分類できます。

- イーサネット系
  - 10BASE-2、5、FL、T
  - 100BASE-TX、FX
  - 1000BASE-SX、LX、T
- xDDI 系
  - FDDI（ファイバ）
  - CDDI（銅線）
- その他
  - Token Ring
  - ATM
  - FiberChannerl

最近よく見かけるトラブル例を、ネットワーク種別毎に紹介していきましょう。

- 10BASE-5 （ThickEthernet）
  トランシーバを同軸ケーブルにタップして接続するため、接触が悪くなって、障害が発生するケースが増えています。
- 10BASE-2 (ThinEthernet)
  相次ぐ機器増設で全長が 200m を超えた場合、経年変化によってコネクタの接触不良が起こった場合などに、特定の端末からしか接続できないというケースがあります。
  古い機器の場合には、電源やトランシーバに使われているコンデンサの経年劣化が原因であることが見受けられますし、埃の堆積などにも注意が必要です。

- 10BASE-T
  MAU（Media Access Unit）の SQE（Heart Beat）が enable となっており、Heart Beat 信号をコリジンと誤認してパフォーマンスが落ちている場合があります。また、最近はスイッチの登場により問題なくなりつつありますが、ハブの最大段数（4 段）が守られていない場合もあります。

- 100BASE-TX
  10Mbps と 100Mbps 自動識別、全二重と半二重の自動識別がうまく動作しない場合があります。条件が分かっているのであれば、できるだけ固定の設定を行うことをお勧めします。

- FDDI
  FDDI は Dual Ring を使用しているため、1 カ所で障害が起きていてもネットワークが正常に使用できます。このため、障害に気づきにくい場合があります。常に、両ポートのステータスを確認するようにします。台数が多くなると、リングのトポロジーが分かりにくいのも問題の1つでしょう。

- Gigabit Ethernet
  マルチモードファイバでも、コア径によって伝送距離は異なります。また、パケットフレームのエンコーディング方法、プリアンサンブルのビット長などについて、規格の変更により複数の方法が混在しています。新しい機器では大丈夫ですが、古い機器を混在して使用している場合には、気を付ける必要があるでしょう。

ネットワーク種別にかかわらず、よく見かけるトラブルとして、ARP テーブルのキャッシュ情報がうまく更新されないことが挙げられます。特にスイッチング機器では、MAC アドレスの学習とタイムアウトに癖があることがあります。

## 5.5 LAN の歴史

ここで、LAN の歴史について少し振り返っておきましょう。現在の潮流を一言で言うと、「シェアードネットワークからスイッチネットワークへの移行期」となります。この流れを理解した上で、次世代のネットワークを設計することが必要です。

- 第 1 期（～ 1992 年）
  10BASE-5/2 がバックボーンであり、ブリッジによる接続が主だった時期です。

- 第 2 期（1992 ～ 1993 年）
  10BASE-T が登場し、フロア内での端末接続にハブを用いることが主だった時期です。ブリッジやルータによって、ネットワークをセグメントに分けて管理することが行われるようになりました。

- 第 3 期（1993 ～ 1995 年）
  ルータのポート単価が安価になり、同一フロア内で複数のセグメントを持つようになりました。バックボーンが 10Mbps で足りない場合には、FDDI でルータ間を接続するようにもなりました。ルータがそれなりに使われるようになってきた時期とも言えるでしょう。
- 第 4 期（1995 ～ 1997 年）
  スイッチが登場し、トポロジーをそのままにパフォーマンスを向上させる方策が取れるようになりました。LAN 間接続には、100BASE-TX や CDDI、100M VG-AnyLAN などの 100Mbps ネットワークが使用されるようになりました。ルータではなく、スイッチとハブでネットワークを構成するようになった時期とも言えるでしょう。
- 第 5 期（1997 年～）
  100BASE を使用した高速バックボーンと、スイッチが全盛になっています。バックボーンには、GigabitEthernet や 100Mbps を束ねて使う EtherChannel の技術も使われています。レイヤ 3 スイッチによって、ルータではなく、物理チップによってルーティングを行い、高速なネットワークが実現されています。

## 5.6 WAN

WAN 用に NTT が提供しているサービスを、まず列挙しましょう。

- 専用線
  - HSD（ハイスーパーデジタル）専用線
  - DA（デジタルアクセス）専用線（30km まで）
  - DR（デジタルリーチ）専用線（同一県内）
  - ATM メガリンク
  - 音声帯域専用線（3.4KHz）
- 準専用線
  - スーパーリレー FR
  - スーパーリレー CR
- ISDN
  - INS64
  - INS1500

中でも、Ethernet と ATM を直接接続する機器の登場と、容量当たりのコストの面から、長距離では ATM の利用が増えているようです。

NTT の提供するサービス以外のものでは、構内自設線として構内モデムを用いた回線があります。最近では HDSL を用いて 4 芯のケーブルで最高 2Mbps 程度の速度が出るようになっています。また、衛星回線や、CATV を WAN のアクセス回線として使用することもあります。

WAN 回線に障害が発生した場合、NTT に連絡して DSU 間の折り返し試験を行ってもらうのが最初の一歩となります。折り返し試験に問題がない場合は、機器の故障である場合がほとんどですが、DSU の T 点側インタフェースの故障の可能性もあるので注意が必要です。まずはルータのシリアルインタフェースを別のものに交換してみます。稀に、ケーブルの緩みなどで、一部の信号線だけが不通となっていることもありますので、ケーブルやコネクタにも注意してください。

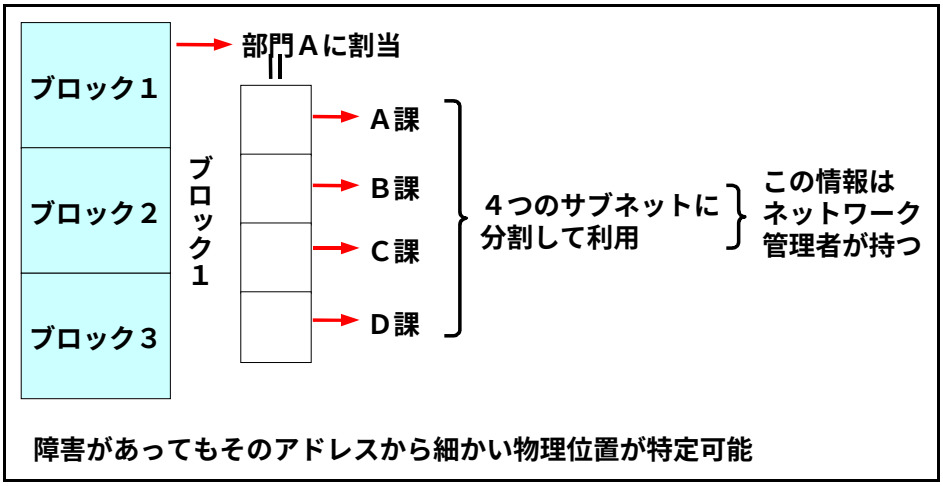
実際にあった例として、NEC 製の TA で、相手が別のメーカー製の場合にエラーとなったケースがありました。この原因としては、スクランブルが ON になっていたこと、およびオール 0 ないしオール 1 のデータを SVA/BSVA として誤検出していたことがありました。NEC のように、ホームページなどで情報を公開してくれるメーカーでは、使っている機器の情報を常にチェックすると良いでしょう。

また、ATM メガリンクで、光のレベルが高いために通信がうまく行えないケースもありました。10db のアッテネータをルータの受信側に入れれば良いのですが、緊急時にはケーブルを半差しにすることでしのぐことも可能です。

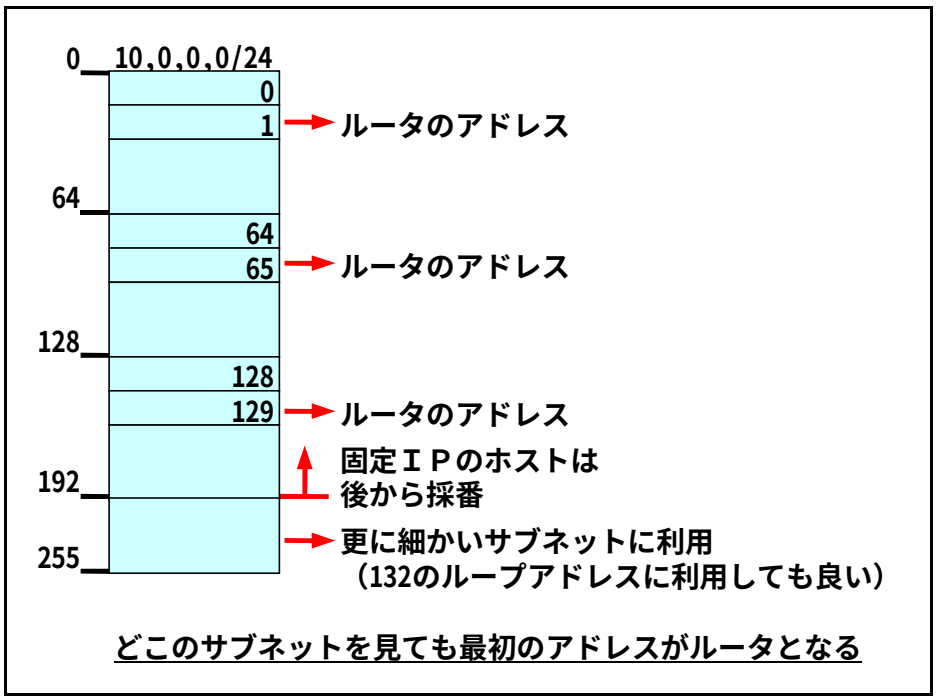
# 6　アドレッシング

## 6.1　アドレスの採番

障害に強いネットワークを構築するには、障害を発見しやすく、メンテナンスしやすいアドレスの採番方法を採る必要があります。つまり、アドレスのブロックでネットワークの物理的なエリアを特定できるように採番しておけば、障害が起きたときにアドレスを見てどの部署であるかが分かるのです。



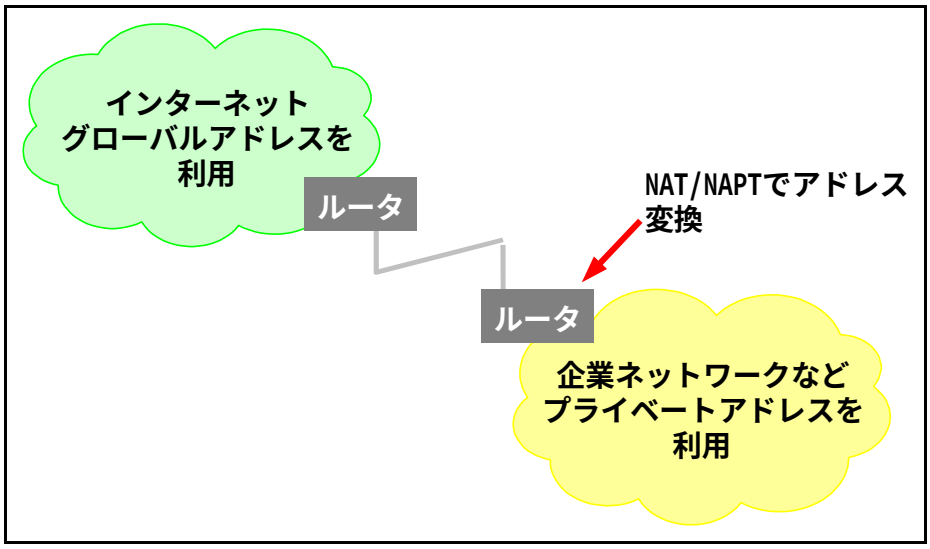

あるいは、ルータや重要なサーバに、サブネット内で常に一定のアドレスを与えるように採番しておけば、障害が起きたサブネットにおけるルータをすぐに探し出すことができます。



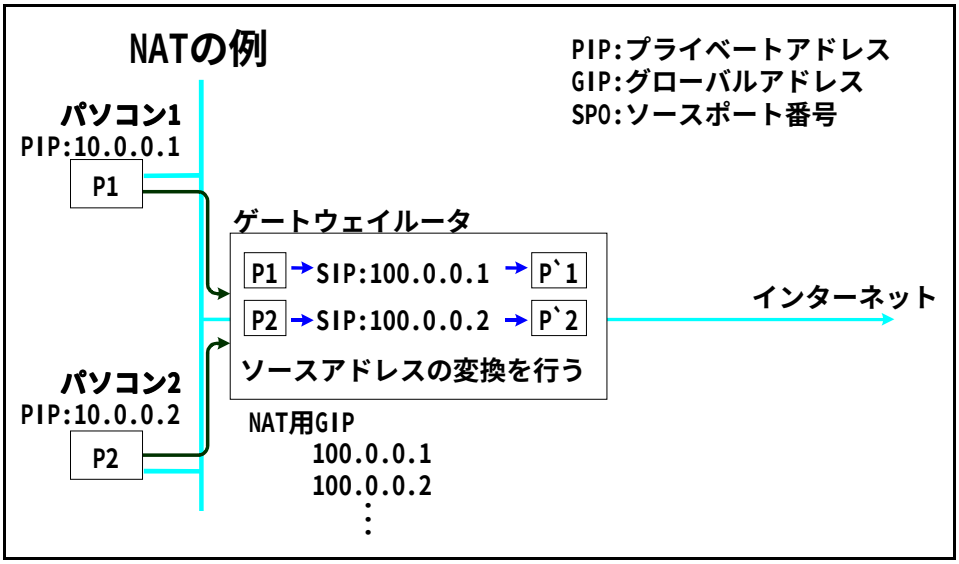
## 6.2 アドレス変換

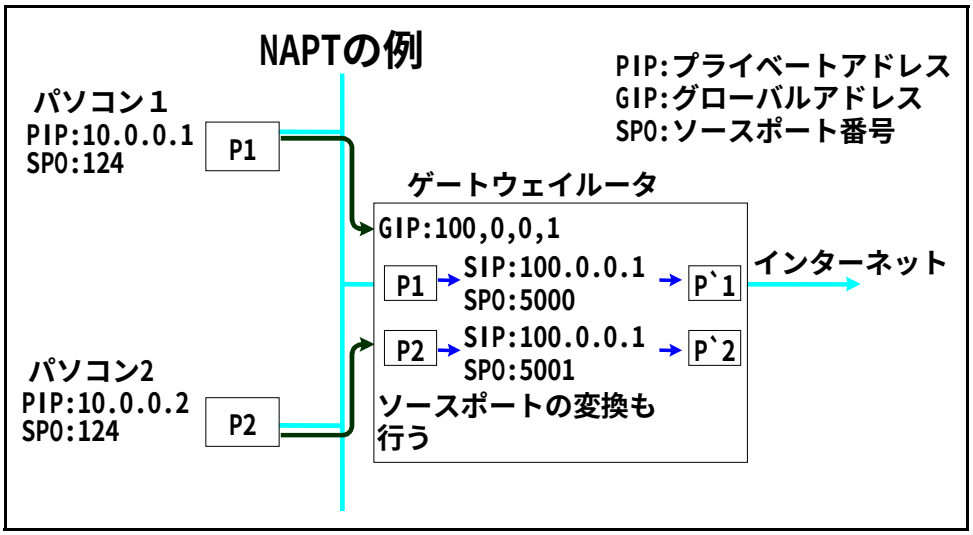
IP アドレスには、世界中で一意に決定できる番号が割り当てられるグローバルアドレスと、閉じたネットワーク空間で利用するプライベートアドレスがあります。イントラネットなどの企業ネットワークでは、プライベートアドレスを使用するのが一般的です。

少ないグローバルアドレスを効率よく利用するために、NAT や NATP（Masquerade）と呼ばれるしくみが使われます。




アドレス変換時に、NAT では 1 つのグローバルアドレスに 1 つのプライベートアドレスを割り当ててソースポートを変更しないのに対して、NAPT ではソースポートを適当に変換する点が異なります。このため、NAPT では、複数台の機器で 1 つのグローバルアドレスを利用することが可能になります。


NATの例
PIP:プライベートアドレス
GIP:グローバルアドレス
SPO:ソースポート番号
パソコン1
PIP:10.0.0.1
P1
ゲートウェイルータ
P1
SIP:100.0.0.1
P`1
P2
SIP:100.0.0.2
P`2
インターネット
ソースアドレスの変換を行う
パソコン2
PIP:10.0.0.2
P2
NAT用GIP
100.0.0.1
100.0.0.2


NAPTの例
PIP:プライベートアドレス
GIP:グローバルアドレス
SPO:ソースポート番号
パソコン１
PIP:10.0.0.1
SPO:124
P1
ゲートウェイルータ
GIP:100,0,0,1
P1
SIP:100.0.0.1
SPO:5000
P`1
インターネット
P2
SIP:100.0.0.1
SPO:5001
P`2
パソコン2
PIP:10.0.0.2
SPO:124
P2
ソースポートの変換も
行う

# 7 ルーティング

ネットワークのトラブルとして、ルーティングにまつわるトラブルは非常に多いと思われます。まず、ルーティングプロトコルの種類を列挙して、それぞれにおける注意点を述べていきましょう

- RIP
  小規模なイントラネットなどで使用されるプロトコルです。Valiable Length SubnetMask（VLSM）に対応できないため、大規模なネットワークでは使用されません。
- RIPv2
  RIP のプロトコルをそのまま VLSM 対応したもので、実装が簡単で、安価な機器にも実装しやすいという特徴があります。ただし、30 秒に 1 回全てのルーティング情報を隣接するルータに配信するという特徴から、大規模ネットワークでスケールする技術ではありませんし、障害時の即応性が低いという問題があります。
- OSPF （Version 2）
  OSPF はある程度大規模なネットワークにも対応可能なルーティングプロトコルであり、ISP 内部のルーティングなどに使用されています。ルーティングアップデートが起こらないと、10 秒に 1 回の Hello パケットで隣接ルータの生存を確認し、40 秒間 Hello パケットを受信できなければ、そこからのルーティング情報を削除します。これにより、大規模ネットワークにおいても、トラフィック上の問題とはなりません。

OSPF を使用する場合には、エリア 0 を中心として各エリアが接続するトポロジーとすることに注意します。LAN においては、OSPF はマルチキャストを使用しますので、スイッチの設定によっては OSPF ルーティングパケットが通らないことにも注意します。

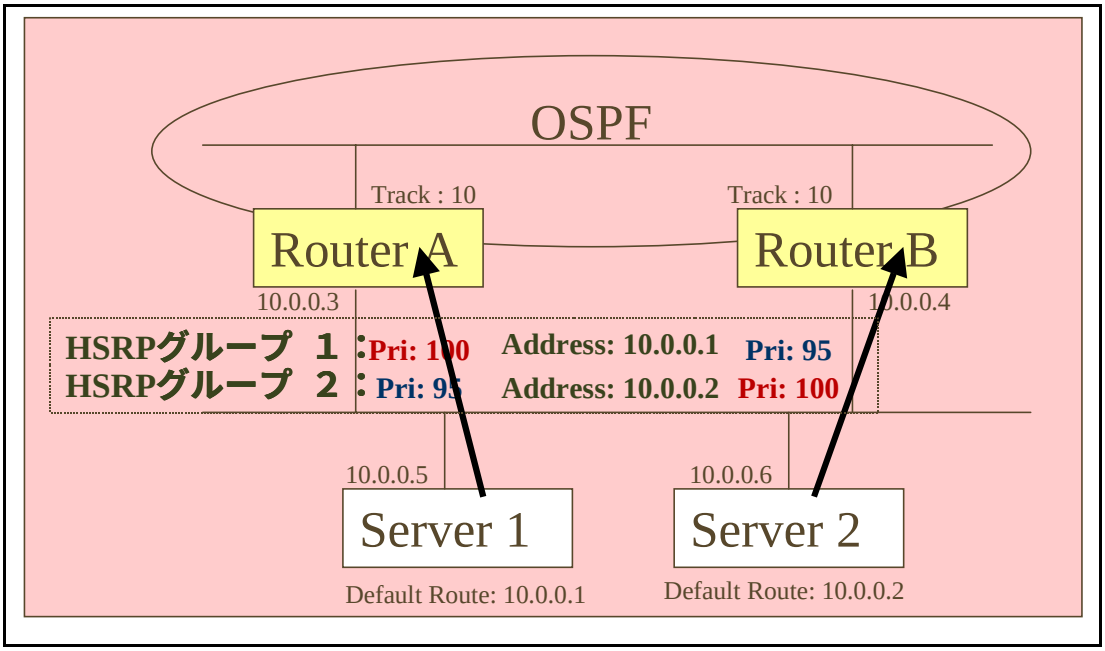
また、OSPF には、Disignated Router/Backup Disignated Router（DR/BDR）と呼ばれる問題が発生することがあります。OSPF では、セグメント毎に DR ルータ／ BRD ルータを選出して、それらが自分で構築したルーティングデータベースを他のルータに配布するというしくみを取っています。DR/BDR ルータが、着信したルーティング情報にフィルタリングを行っている場合、フィルタを通過したルーティング情報しか配らないため、ネットワークのルーティング情報に不整合が発生することがあります。DR/BDR ルータには計算能力も要求されますので、DR/BDR になれるルータを、設定によって制限しておくのが好ましいでしょう。

ルータの機種によっては、複数のプロセスで OSPF を実行できるものがあり、ルーティングが混ざって欲しくないネットワークで限定した、ルーティング情報だけを相互にやりとりしたい場合などに有効です。ただし、この場合、ルーティング情報をクリアすると、ルーティング情報が流れなくなってしまうことがあります。

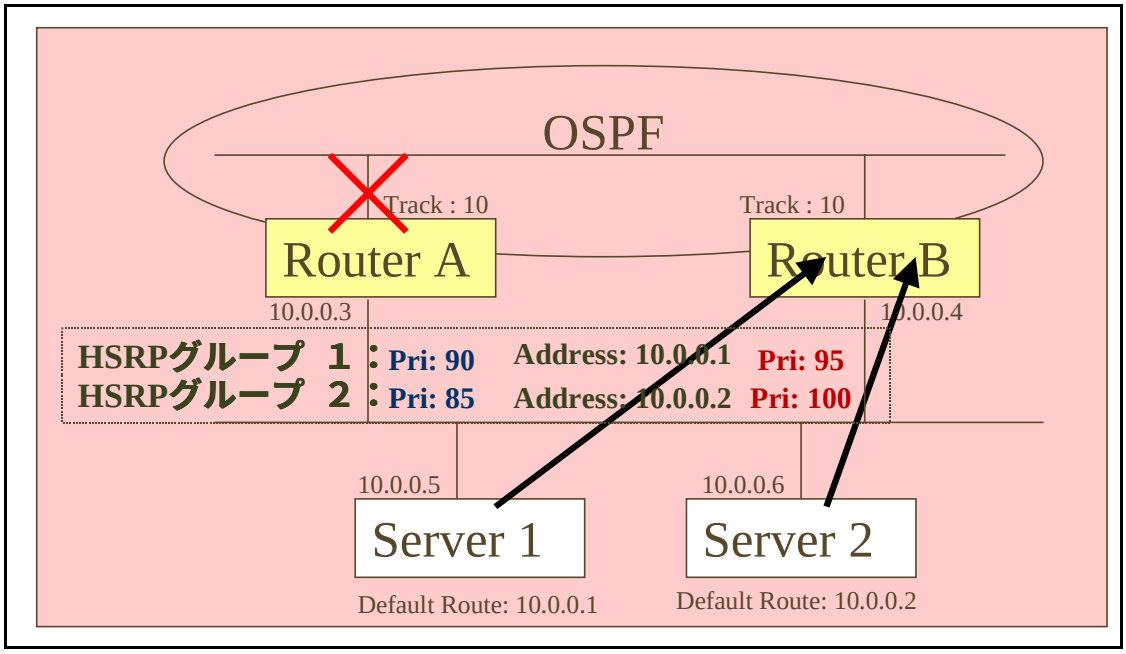
OSPF ではそれぞれのネットワーク機器がルータ ID を持ちます。デフォルトでは、アクティブなアドレスのうちで、最も大きなものをルータ ID として使用しますので、機器やネットワークの切り替えの場合に、ルータ ID になっているインタフェースからケーブルを抜くと、トラブルが発生することがあります。ローカルループバックアドレスを設定しておけば、それがOSPF のルータ ID となりますので、このようなトラブルを未然に防ぐことが可能となります。また、ループバックアドレスを設定すると、特定インタフェースがダウンした場合にも、ループバックアドレスを使ってルータ自体にアクセスすることが可能になるというメリットもあります。ただし、そのループバックアドレスが/32 のホスト情報としてルーティングテーブルに追加されますので、台数が多い場合には問題となることもあるでしょう。

## 7.1 Hot standby routing protolcol（HSRP）

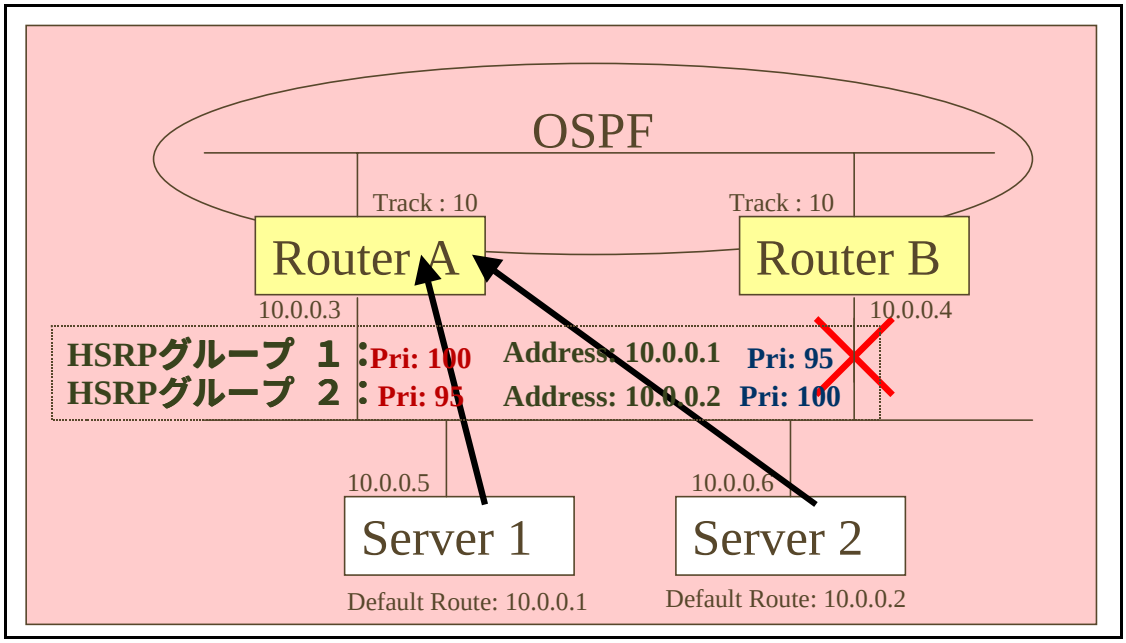
ネットワークの障害を最小限に抑えるためには、Hot Standby Routing Protocol（HSRP）と呼ばれる技術が有効です。HSRP とは、仮想的な 1 つの IP アドレスに対して、プライオリティを付けた複数の MAC アドレスを対応づけておき、障害時に MAC アドレスの割り当てを変えることで、耐障害性を高める技術です。




上図では、HSRP グループ 1 として、仮想 IP アドレス 10.0.0.1 に、ルータ A の MAC アドレス（プライオリティ 100）と、ルータ B の MAC アドレス（プライオリティ 95）が対応づけられています。同様に、HSRP グループ 2 として、仮想 IP アドレス 10.0.0.2 に、ルータ A の MAC アドレス（プライオリティ 95）と、ルータ B の MAC アドレス（プライオリティ 100）が対応づけられています。通常は、仮想 IP アドレスに割り当てられた MAC アドレスの内、最もプライオリティが高いものが採用され、10.0.0.1 に宛てたパケットは RouterA に、10.0.0.2 に宛てられたパケットは RouterB に送られます。Server1 はデフォールトルートとして、10.0.0.1 を、Server2 は同じく 10.0.0.2 を持っていますから、ServerA からのパケットは RouterA に、ServerB からのパケットは RouterB に向かいます。このように、複数の HSRP グループをうまく定義すると、ルータ間の負荷分散を図ることもできるわけです。




HSRP では、Track 指定したインタフェースがダウンすると、指定した値を HSRP グループのプライオリティから減算します。RouterA のインタフェースがダウンすると、HSRP グループ 1 における RouterA のプライオリティが 90 に、グループ 2 における RouterA のプライオリティが 85 に減少します。これにより、HSRP グループ 1 では、RouterB のプライオリティが RouterA よりも高くなるため、10.0.0.1 に宛てたパケットは RouterB に向かいます。すなわち、ServerA からのパケットも、RouterB に向かうことになります。




また、HSRP では、アクティブルータを keepalive パケットで監視しており、タイムアウトが発生すると、次にプライオリティが高いルータをアクティブにします。RouterB のサーバ側インタフェースがダウンした場合、このしくみによって HSRP グループ 2 のアクティブルータが RouterB から RouterA に変更され、10.0.0.2 に宛てたパケットは RouterA に向かいます。すなわち、ServerB からのパケットも RouterA に向かうことになります。

HSRP では、複数のグループを同一インタフェイスで使用することが可能ですが、ルータの機種によって使用できるグループ数が制限される場合があります。なお、HSRP を設定するインタフェースでは、パケットリダイレクトが起こるとまずいので、IP リダイレクトを禁止しておく必要があります。

# 8 ネットワーク障害監視

まず、ネットワークを監視する意味を考えてみましょう。ここでは、トラブル（障害）をできるだけ発生させないために、監視を行うことを考えます。それは、常にネットワークの健康状態を知っておくことに他なりません。それによって、ネットワーク拡張の予測をたてることも可能になりますし、アタックを早期に発見することも可能になります。

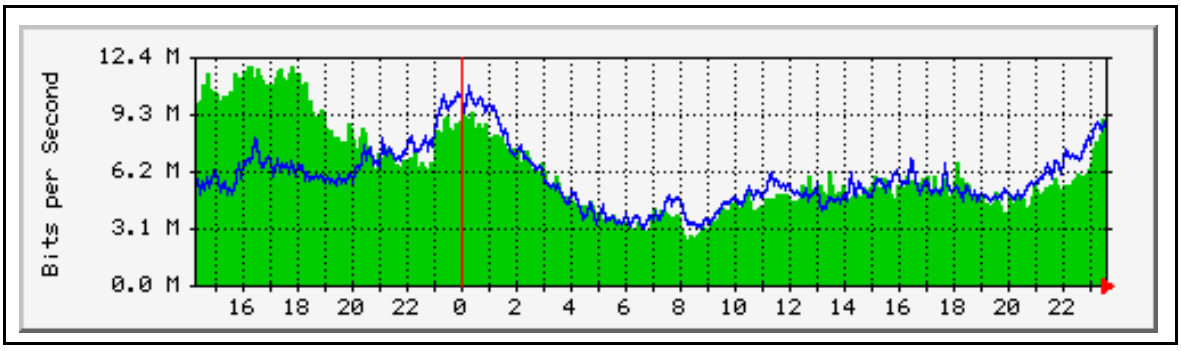
ネットワークを監視する場合には、現存の監視ツールを有効に利用して、現在のトラフィックパターンを周知しておくことが必要です。トラフィックパターンが変化したならば、ネットワークの何かが変わったということですから、トラブルが起こった時にその「変わったこと」からさまざまな推測が行えます。

パターンを把握するためにも、収得可能なログはできる限り残すように設定しておきましょう。また、ネットワークの管理担当者を明確にしておくこと、不要な機器はネットワークに接続せずに、試験などは専用のセグメントで行うことなども重要です。

## 8.1 監視のためのツール

ネットワーク監視のために有効なツールをいくつか紹介していきましょう。

- Multi Router Traffic Grapher （MRTG）
  計測したトラフィック量や、ディスクの空き容量などをグラフ化するためのツールです。*http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html* から入手できます。

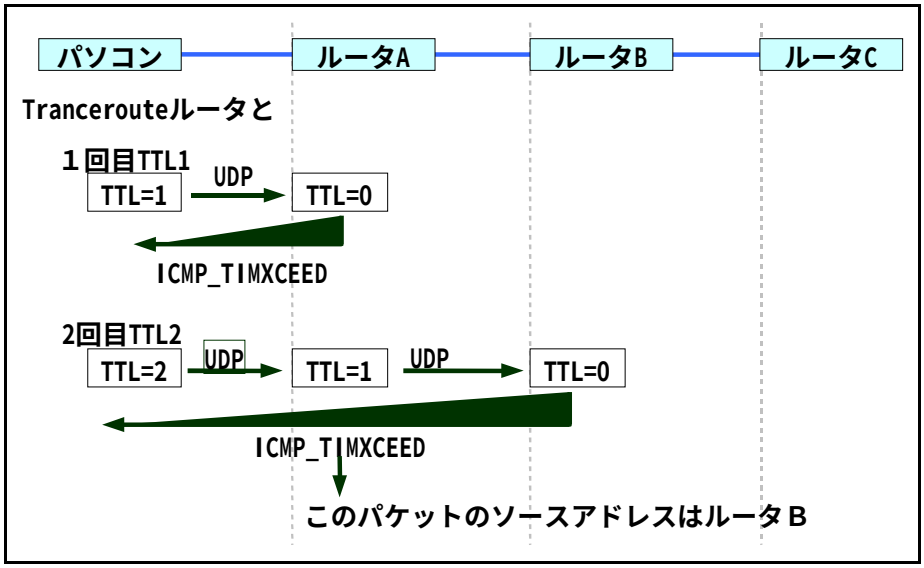



- ping
  ECMP_ECHO パケットを利用して、ターゲットホストまでの
  RTT（RoundTrip Time）の参考値を知るためのツールです。このツールによる RTT はあくまでも参考値であることに注意してください。

  ping では、ローカルホストが ICMP_ECHO パケットの中に送出時刻を収納して送出し、ターゲットホストが、その時刻情報を含む ICMP_ECHOREPLY パケットを返送します。ping で表示される RTT は、ICMP_ECHOREPLY の到着時刻と、その中に含まれる時刻情報の差分ですから、それぞれのパケットを送受信する時間と、パケットを生成・解析する時間を含むことになります。つまり、厳密な意味での RTT ～ネットワーク上をパケットが流れている時間よりも、長い時間が表示されます。

  なお、UNIX 版と Windows ではオプションが異なりますので注意してください。

- traceroute
  UDP パケットをディスティネーションホストに宛てて送り出し、その TTL を 1 つずつ順に増やしていき、その応答となる ICMP パケットによってルートを検出するツールです。パケットの流れは行きと帰りで異なる場合も多いのですが、このツールは行きのルートを検出します。なお、途中のルータに負荷がかかっている場合には、表示される TTL 値は全くあてになりません。




- telnet
  サーバが稼働していることを確認するために使用します。ポート番号を指定することで、任意の TCP サービスの稼働状態を調べることができます。

- Sniffer
  LAN/WAN/ATM 対応のアナライザで、OSI7 層までのネットワーク障害をリアルタイムに検出し、解析することが可能な製品です。簡易版がソフトウェアとして販売もされています。*http://www.toyo.co.jp/sinfer/*

- TTCP
  目的のサーバで稼働する TTCP サーバに向けて、TCP パケットをバースト的に送出し、ホスト間のパケットロスや伝達時間などを計測するツールです。ネットワークにかなりの負荷をかけますので、空いている時間を狙って実行しましょう。ソースは ftp://ftp.iij.ad.jp/pub/network/ttcp/ttcp.c にありますが、公式サポートサイトではありません。

- Pathchar
  ICMP_ECHO と ICMP_ECHOREPLY の応答時間のゆらぎを分析して（未確認）、目的のホストまでの回線残容量を測定するツールです。ネットワークにかなりの負荷をかける上に、実行に長い時間がかかるため、あまり使用することはありません。*http://www.caida.org/Pathchar/*

- ucd-snmp
  SNMP エージェントを含むさまざまな SNMP ツールのパッケージです。コマンド形式になっているため応用範囲が広範ですが、SNMP に対する知識が必要です。*http://www.ece.ucdavis.edu/ucd-snmp/*

- ホームページからの ping や traceroute
  遠隔地のホストから ping や traceroute を実行するためのホームページは、場合によっては非常に有効です。*http://nitrous.digex.net/* や *http://neptune.dti.ad.jp/* などがあります。

- メール・Perl・携帯電話（ポケベル）
  Perl などの簡易プログラミング言語を使って、細かな監視ツールを有機的に結びつけて利用すると、自分のネットワークをきめ細かく、かつ、使いやすく監視するためのツールを作成することができます。メールや、携帯電話（ポケベル）は、障害発生を自動的に通知するための強力なツールとなります。自分なりの監視ツールを作成すると良いでしょう。

# 9 おわりに

インターネットにおける技術的事項、および、それにまつわるオペレーションに関する事項を議論・検討・紹介することにより、日本のインターネット技術者、ならびに利用者に貢献することを目的としたグループとして、JANOG があります。

このチュートリアルで紹介した内容に関する議論なども行われています。詳細は *http://www.janog.gr.jp/* を参照してください。