ネットワーク構築運用管理
～トラブルシューティング～

岡本 久典（株式会社 NTT データ）

近藤 邦昭（株式会社インターネット・イニシアティブ）

1999 年 12 月 16 日

Internet Week 99　パシフィコ横浜

（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

この講演では、ネットワーク障害を最小限にするという観点から、障害検出、回復、再発防止をプロセスモデルとして捕らえて、ネットワークを管理する方法を紹介します。また、同じ観点から、障害に強い～すなわち、障害が起きにくく、起きても回復しやすい～ネットワークの構築・運用技術を紹介していきます。

ここでは、上記の事柄を次の順に解説します。

- ネットワーク障害の分類（2 を参照）
- プロセスモデルによる障害対応（3 を参照）
- 障害に強いネットワーク（4 を参照）

2 ネットワーク障害の分類

一口にネットワーク障害と言っても様々なものがあり、その症状もさまざまです。ここでは、障害をレイヤに分けて分類し、その症状を概観してみます。

2.1 障害の種類

ユーザから見れば「繋がらない」という現象として見える障害について、「どこに問題があるのか」を明らかにしなければ、障害に対応することはできません。障害の内容を知るには、表 1 のようなレイヤに分類して考えるとよいでしょう。

表 1：障害の種類

障害の種類	レイヤ
回線障害	レイヤ 1
ネットワーク機器障害	レイヤ 1 の一部、レイヤ 2、レイヤ 3 の一部
ルーティング障害	レイヤ 3
サーバ機器障害	レイヤ 3、レイヤ 4、レイヤ 5
アプリケーション障害	レイヤ 5、レイヤ 6、レイヤ 7

また、情報伝達ミス等による障害（レイヤ 8 障害）も考えることができますが、これは人為的なものと考えられるので、ここでは触れません。

2.2 回線障害の概要

回線障害には次のようなものがあります。特徴としては、回線利用者側でコントロールできる部分が少なく、適当な機材を持ってきて適切に設定する以外の対応策はありません。

- 専用線交換機の異常

  回線に使用しているファイバが切れてしまうと言った障害もあります。

- 回線提供業者の設定ミスによるもの
- 回線提供業者との情報伝達ミス

  レイヤ 8 に属するものですが、かなりの頻度で発生します。

- 利用者側の機器トラブル

2.3 ネットワーク機器障害の概要

ネットワーク機器の障害には次のようなものがあります。

- ハブやルータ等の故障
- ハブやルータ等の電源障害

  電源電圧の変化によって、機器の動作が不安定になり、障害発見が困難な場合もあります。

- FDDI や UTP ケーブルの損傷

  特に UTP ケーブルでは、より対がほどけてしまってノイズが乗るという場合もあります。

2.4 ルーティング障害の概要

ルーティング障害には次のようなものがあります。

- ルータのバグによる障害

  特定のコマンドを実行したときに、経路情報が途絶えてしまうといった例があります。

- ルータの設定ミス
- 外部からの障害

  外部からの不正な経路情報に対する対策を施していないと、経路が消失するといった問題が発生することがあります。

- 外部からの不正アクセス

  ルータの設定を消去してしまう、動作を停止させる（リブートさせる）といった攻撃があります。

2.5 サーバ機器の障害の概要

サーバ機器の障害には次のようなものがあります。特徴としては、特定のサーバへのアクセスが不可能になるだけで、ネットワーク全体への影響が少ないことが挙げられます。

- ログファイル等によるディスク容量あふれ
- カーネルのバグ
- 外部からの不正アクセス

2.6 アプリケーション障害の概要

アプリケーションの障害には次のようなものがあります。特徴としては、サーバへは到達できるものの、特定のサービスにアクセスできないことが挙げられます。

- アプリケーションのバグ
- アプリケーションの設定ミス
- アプリケーションの停止
- 外部からの不正アクセス

3 プロセスモデルによる障害対応

障害が発生したときには、障害に対応するプロセスモデルを作成しておき、それに沿って対応を行うことが有効です。特に、障害が直った後の報告と再発防止対策を行うことが重要です。

3.1 障害対応のプロセスモデル

障害対応のプロセスは、次の 3 つのステップから成っています（図 1 も参照）。

- 障害の発見と確認
- 障害への対応とその経過の報告
- 復旧の報告と再発防止策の策定

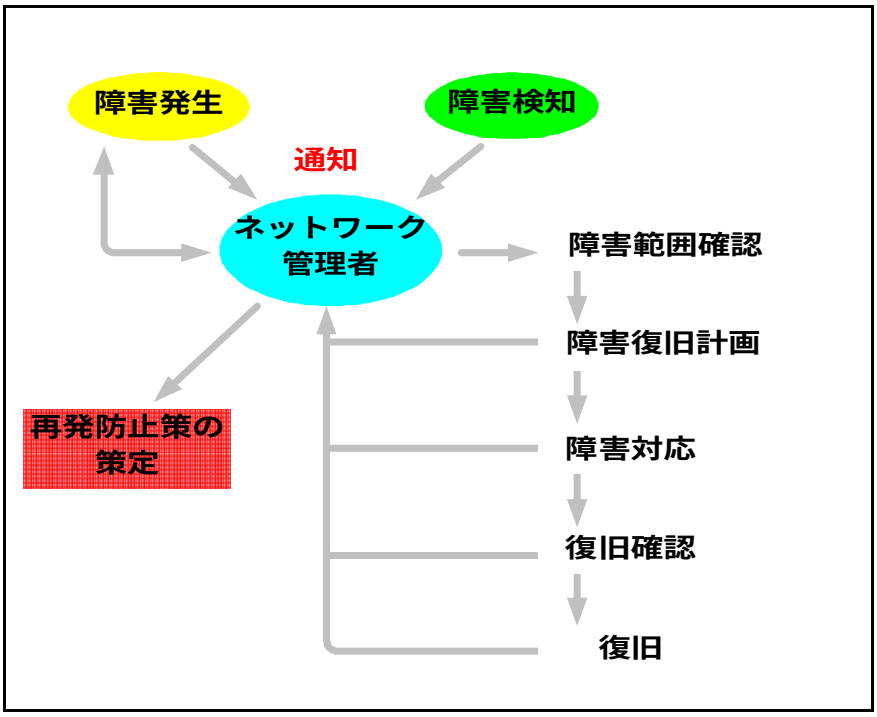

図 1：障害対応プロセス概念図

次に、それぞれのプロセスについて解説します。

3.2 障害の発生と確認

最初に、障害が発生していると知ることからプロセスは始まります。ユーザからの連絡によって知ることもありますし、ネットワーク監視ツールによって知ることもあるでしょう。監視ツールを使用している場合には、障害の発生だけではなく、常日頃の状態を知っておくことも重要です。ユーザからの情報による場合は、まずそれが障害なのか、ユーザのミスや誤解ではないのかを判断することも必要です。その上で、「どこからどこに宛てた」、「どのプロトコル」によるものなのかを確認し、不具合が発生したときのできるだけ詳しい状況を把握します。

次に、障害の影響範囲を確認します。不具合が発生したときの状況によっては、「不具合」ではなくて「正常な症状」の場合もあるでしょう。たとえば、他のアプリケーションの影響によって、別のアプリケーションの動作が通常とは異なっている場合も考えられます。ネットワーク機器のログにエラーメッセージが出ていないかを確認してみます。さらに、IP 以外のプロトコルを使用している場合には、不具合が IP ネットワークだけなのか、他のプロトコルにも障害が発生しているのか等を確認します。

ここまでで集めた情報を使って、障害が発生しているレイヤを切り分けます。IP ネットワークにおいては、レイヤ 3 が動作しているかどうかがキーになります。レイヤ 3 を境界として、対応部署が異なることもあるでしょう。ping が OK であればレイヤ 3 以上ですし、NG であればより下位のレイヤが怪しいことが多いのですが、必ずしも絶対的なものではありません。レイヤ 3 以上が怪しい場合には、traceroute で機器を特定し、telnet 等で目的ホストの該当ポートにアクセスしてみることを試してみます。ネットワーク機器のログを調査することも忘れてはいけません。

なお、ネットワーク障害は特定の場所（機材）に集中して発生する傾向がありますので、過去の障害履歴を残してある場合には、類似のものがないかどうかを確認してみると有用な場合があります。

3.3 障害への対応と報告

障害が発生していることが分かった場合には、ユーザならびに上司や同僚に、その影響範囲を連絡することが必要です。ここまでの調査で、対応方法等の目処が付いているようでしたら、たとえば、回復予定時刻を知らせる必要もあるでしょう。なお、障害ではない通常動作だった場合も、その旨を連絡することが必要です。

実際の障害対応としては、次のようなものが挙げられます。

- ハードウェアトラブル

  代行機に交換します。予備の機材を準備しておくとよいでしょう。

- 特定パケットに固有の障害

  ネットワーク機器等のバグ情報を確認し、必要があれば、ファームウェア等の交換やソフトウェアのバージョンアップを行います。

- ネットワーク構成に起因する障害

  いつの間にか一方向のトラフィックのみが増大していた場合等には、ネットワーク構成そのものが障害の原因となっている場合もあり得ます。そういった場合には、ネットワーク構成そのものの変更や、インタフェースカードの交換や、回線の増速が必要となることがあります。

対策を施した後には、しばらくの間様子を見て、障害に伴うログが表示されていないことを確認したり、利用者に復旧していることを確認したりする必要があります。

3.4 復旧の報告と再発防止策の策定

障害からの復旧が確認できたならば、必ずその障害内容（時間、場所、機器名、状態）と、行った対応策を記録しておきます。直ちに復旧することができなかった場合には、今後どうするかを記録します。

いずれの場合であっても、同じ障害を繰り返さないように、現実的な再発防止策を考察することが非常に重要です。「気を付ける」と言うだけや、非現実的な策では意味がありません。

3.5 障害の発見方法

講演者の ISP では、管理ツールによって定常的な障害検出を行っています。「欲しい情報」を取り出すためには、市販のツールはほとんど役に立たないため、フリーのものを主に使用しています。ネットワークの状態があるスレッショルドを超えると、アラートが点いたり、ポケベルや携帯を呼び出すといったツールまで用意しています。

企業ネットワークにおいては、人材的なリソースが ISP よりも少ないものと思われますので、市販の管理ツール等を使用するのもよいでしょう。

いずれの場合にも、ユーザや通信相手からの不具合連絡によって障害を知ることも多いでしょう。障害発生時に連絡を受け付ける窓口を用意して、障害発生を前提とした連絡体制を作っておくことも重要です。

4 障害に強いネットワーク

次に、観点を変えて、障害に強いネットワークを作るためのポイントを紹介していきます。ここでも、レイヤ毎にポイントを分類し、低位のレイヤから解説していきます。

4.1 電源

コンピュータを使用する場合であっても、電源について考慮されていることは意外と少ないようです。

4.1.1 電源容量の計算

誤解されがちなことに、W と VA の違いがあります。機器によって、消費電力を W で表記しているものと VA で表記しているものがありますので、UPS を使用している場合にはそれに合わせて計算するとよいでしょう。乱暴なやり方では、W < VA なので、全て VA として計算してしまえば、電力が足りないという事態は避けることができます。

また、機器は電源投入直後に急激に電力を消費することを忘れてはいけません。ハードディスクやファンのモータは、回転を始めるときに最大電流を消費するからです。電源の設計にあたっては、起動時の電力で計算を行うことが原則ですが、ぎりぎりの場合には機器を順に立ち上げるといった運用でカバーします。

4.1.2 電源の取り方

電源ユニットを 2 つ以上持っている機器の場合には、1 つの電源ユニットに障害が起きた場合に他方の消費電力が倍増することを考慮して、電源系統を別のものにしておきます。ラックに電源コンセントが 2 列付いている場合には、図 2 のようにそれぞれを別の電源系統に接続しておけば、一方の系統がダウンしても他方でカバーされます。

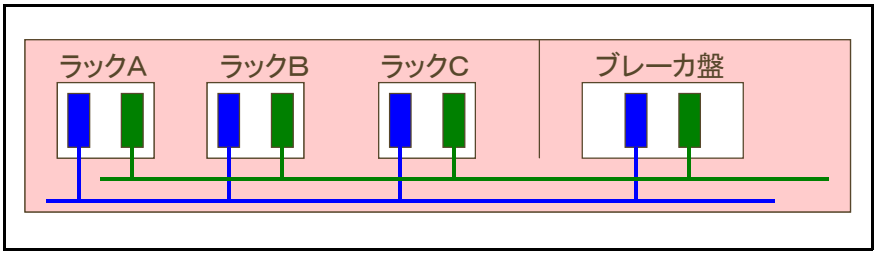

図 2：2 系統の電源ユニット構成

4.1.3 アース

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ます。スイッチング電源を使用している機器を接続する場合には、それぞれの機器の筐体をアースに落としておかないと、筐体毎に電位が違うために、最悪の場合は機器の破損に繋がります。

日本ではそれほど普及していませんが、アース付きの機器の電源は、できるだけアース付きの抜け止めタイプのコンセントを使うようにするべきでしょう。

4.2 ケーブリング

ネットワークを組む場合には、当然、機器と機器を接続するケーブルが必要です。まず、それぞれのケーブルの特徴等を説明し、続いて、障害が発生しにくいという観点から取り回しについて説明します。

全ての種類のケーブルに共通する取り回しの注意点としては、巻かれているケーブルを敷設するときにねじれが発生しないように、ケーブル自体を回転しながら伸ばしていくことが挙げられます。また、障害発生時に問題のあるケーブルを特定できるように、それぞれのケーブルに ID を付けると共に、両端にタグを付けて始点／終点を明記しておきましょう。

4.2.1 ツイストペアケーブル

名前が示すとおり、ケーブルを対にしてより合わせることでノイズの飛び込みを低減し、長距離伝送を可能にしているケーブルです。クロストーク（漏話）とノイズ耐性によって、カテゴリー 3 ～カテゴリー 7 にクラス分けされており、カテゴリー 5 以上では、コネクタ部で、より対をほぐす長さまで決められています。

ツイストペアケーブルで使用されるコネクタには、表 2 に示す種類があります。

表 2：ツイストペアケーブルで使用されるコネクタ

規格	形状	用途
RJ11	6 極	電話用
RJ45	8 極	LAN 用 /ISDN 用
RJ48	8極凸部あり	ISDN 用新規格（ピン配置も異なる）

機器によっては、形状やピン配置で RJ45 と RJ48 が混ざったようなものも存在するので、注意が必要です。なお、ケーブル内の線の色とピン配置は規格によって決まっていますので、自作するような場合には規格に従って配線を行っておくのが好ましいでしょう。

ツイストペアケーブルは、さらに UTP（Un-shielded Twist Pair）と STP（Shielded Twist Pair）に分類されます。STP は、より対線と被覆との間に同軸ケーブルと同様のシールドがあるもので、UTP よりもノイズ特性が良くなっています。そのため、ノイズに対する規制が厳しいドイツや、病院等では STP が使用されていることがあります。UTP と STP は、コネクタもそれぞれの形状が決められていますので、ケーブルに合ったものを使用します。

また、ケーブルには芯線が単線のものと、さらにより対になっているものがあります。工具で自作する場合には単線のものの方が楽ですが、パッチケーブル等では、より対線のものの方がケーブルがしなやかで扱いやすいでしょう。

ツイストペアケーブルの敷設にあたっては、電源ケーブルからノイズが飛び込むことを防ぐために、電源ケーブルに平行しないように注意します。また、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が増えるので、最小折り曲げ半径として 10cm 程度を保つようにします。

4.2.2 同軸ケーブル

一般に使用されている同軸ケーブルには、インピーダンスが 50Ω のものと 75Ω のものがあります。インピーダンスが 50Ω のものは主に LAN ケーブル（10BASE-2 等）に使われ、75Ω のものは主に WAN ケーブルに使われます。接合部で反射波が発生するので、これらを混在して使用することはできません。機器に応じたものを使用する必要があります。

同軸ケーブルを接続するコネクタ類（プラグ、ジョイント、パッチ）にも規定のインピーダンスがありますので、敷設にあたっては機器に合ったインピーダンスのものを用い、混在させないように注意します。

4.2.3 光ファイバ

光ファイバは、図 3 のようにコアとクラッドから成り、コア部に入力された光がクラッドで反射しながら進んでいくという構造になっています。

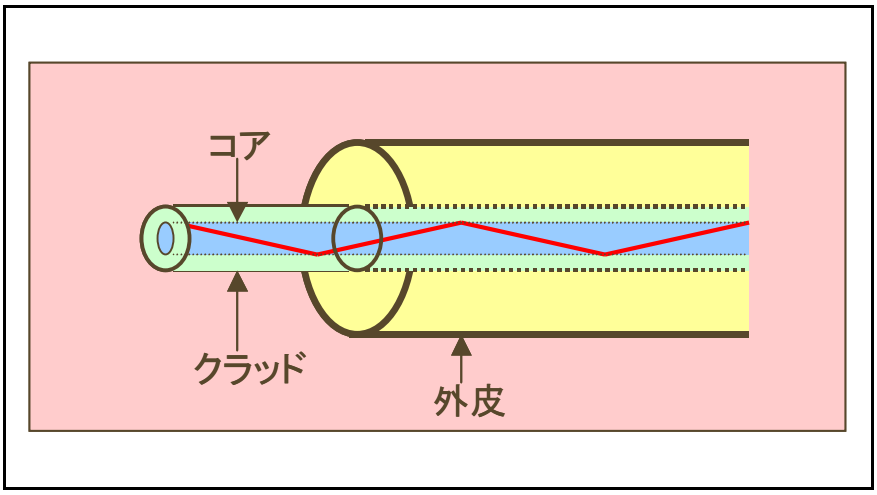

図 3：光ファイバの構造

ネットワークで使用される光ファイバには、シングルモードファイバとマルチモードファイバの 2 種類があり、それぞれにコアの径が異なるものがあります。シングルモードファイバは、WDM 装置を使った長距離広帯域伝送に主に使用されています。

LAN でよく使われるマルチモードファイバには、径が 50μm のものと 62.5μm のものがあります。また、光ファイバには、波長、伝送損失、伝送帯域等の特性があります。現在は、50μm 径で 850nm と 1300nm の波長で使用できる「ダブルウィンドウ」と呼ばれるものが主流になりつつあります。

光ファイバのコネクタには、材質や形状によって次の 4 種類がよく使われています。

- SC

  プラスチックの角形モールド。古い機材に多い。

- ST

  金属製でツイストロックするもの。新しい機材に多い。

- MIC

  2 芯が 1 セットになっているプラスチックモールド。FDDI で使用。

- MT-RJ

  2 芯が RJ 程度の大きさにまとまっているもの。今後の主流となるか。

光ファイバは折れやすいので、設置にあたっては 10cm 程度の最小曲げ半径を取るように注意します。フリーアクセスの床下に設置するような場合には、最近登場しているケプラーコートされた折れにくい光ファイバを使うか、保護用のパイプを通す、スパイラルチューブを巻くようにする等といった対策を施しておきます。また、ジョイントして延長する場合には、ファイバの径が異なるものを接続すると反射波が発生しますので、同一の特性のものを接続するようにします。

4.3 LAN のトラブル

LAN で発生するトラブルには次のようなものがあります。

- 10BASE-5（Thick Ether）

  LAN を早くから導入したところに残っており、経年変化によってトランシーバのタップ部分の接触が悪くなっていることがあります。

- 10BASE-2（Thin Ether）

  ある端末からは接続できるが、別の端末からは接続できないという症状が現れることがあります。相次ぐ機器増設で、セグメントの全長が規格の 200m を超えていることや、経年変化によるコネクタの接触不良等が原因となっていることがあります。

- 10BASE-x

  AUI に接続している MAU（Media Access Unit）の SEQ（Heart Beat）がオンになっていると、その信号をコリジョンと検出してパフォーマンスが悪化していることがあります。また、ブリッジの段数は 4 段までという規格が、いつのまにか破られていることもあります。

- 100BASE-x

  10Mbps/100Mbps の自動認識や、Half/Full Duplex の自動選択はあまりあてになりません。できるだけ固定の設定を使用するとよいでしょう。

- FDDI

  二重リング構成で障害に強いだけに、1 カ所の障害には気付きにくくなっています。日頃から両方のリングのステータスに気を付けていないと、機器増設等で 1 カ所に障害が発生したときにネットワーク全体が使用不可になってしまいます。

- ギガビット Ethernet

  ファイバのコア径によって伝送距離が異なるので気を付ける必要があります。機器によっては、パケットフレームのエンコーディング手法や、プリアンサンブルのビット長の違いによって通信ができないこともあります。

- その他（共通）

  同一のアドレスで機器の交換を行った場合に、ARP テーブルのキャッシュを更新し忘れていることがあります。特に、スイッチを使用している場合には、MAC アドレスを学習しなおさせることが必要です。

  分かりにくいトラブルを避けるために、特に必要でなければ、ルータでは次のような項目を設定しておくとよいでしょう。

  ```
  no ip redirect
  no ip proxy-arp
  no ip directed-broadcast
  ```

4.4 LAN の動向

ここで、古いネットワークや機材によるトラブルを切り分けるための知識として、LAN の変遷を簡単に振り返っておきます。この流れは、Shared なネットワークから、Switched なネットワークへの移行として捕らえることができます。

- 第 1 期（〜 1992 年）

  10BASE-5/2 が主流のネットワークで、ブリッジが時々使われており、ルータはほとんど使われていませんでした。

- 第 2 期（1992 〜 1993 年）

  10BASE-T が登場し、フロアが変わればブリッジやルータで接続することが一般的になってきました。

- 第 3 期（1993 〜 1995 年）

  ルータのポート単価が下がってきて、フロア毎にルータによってセグメントを分けることが一般的になってきました。バックボーンには、FDDI が使われることも珍しくなくなってきました。

- 第 4 期（1995 〜 1997 年）

  100BASE-TX とスイッチが登場し、トポロジーや配線を変えずにスイッチによる効率化が可能になりました。バックボーンには 100Mbps の Ethernet や FDDI が使われることが一般的になってきました。

- 第 5 期（1997 年〜）

  バックボーンには 100BASE を使用して、エッジ部には 10/100Mbps のスイッチが普通に使用されるようになりました。ルータに代わってレイヤ 3 スイッチを使いながら、論理的な VLAN を重ねてネットワークを作るのが一般的になりました。

4.5 WAN

WAN に使われる回線は、次のように分類することができます。現在では、一般的な LAN（10/100Mbps）より高速な WAN 回線も普通に利用されるようになってきています。

- 専用線
- 準専用線
- ISDN
- 構内自設網
- 衛星回線

- CATV

通信事業者が提供する WAN 回線に障害が発生した場合には、まず通信事業者に連絡して、DSU 折り返し試験を行ってもらうことになります。折り返し試験で問題が発生しない場合には、機器が故障している可能性が高いので、まず別のシリアルインタフェースに交換してみます。ケーブルのゆるみから、一部の信号だけが不通となっていることもありますので、コネクタの確認も必要です。

ネットワーク機器によっては、工場出荷の状態では他のメーカの機器と対向したときにエラーが発生することがあります。機器の設定をよく確認しましょう。

ATM メガリンクでは、光信号のレベルが高すぎてエラーとなることもあります。このような場合には、受信側に光アッテネータを入れるとよいでしょう。

4.6 アドレッシング

障害発生時に問題点の発見が行いやすいという観点から、アドレッシングの方法を説明します。これが絶対的なものではなく、基本的には各管理者のポリシーに基づくものであることに注意が必要です。

- NAT と NAPT

  アドレッシングについて説明する前に、グローバルアドレスとプライベートアドレスについて簡単におさらいしておきます。グローバルアドレスとは、一般にインターネットで使われるアドレスで、基本的に世界中で一意に決定できる番号です。対してプライベートアドレスとは、イントラネット等の閉ざされたネットワークで使われるアドレスで、インターネットに流出してはいけません。

  限られたグローバルアドレスを効率よく活用するために、NAT/NAPT と呼ばれる技術を使います。これは、1 つ以上のグローバルアドレスを、それ以上のプライベートアドレスが振られた端末で共有するためのしくみです。

  NAT 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るもので、ソースポート番号はそのままのパケットがインターネットに送出されます。対して、NAPT（Masquerade）は、ソースポートを適当に変更することによって、1 つのグローバルアドレスを複数の端末で共用することが可能です。

- アドレス採番

  障害対応の面からの最適なアドレス採番方法とは、アドレスブロックで機器の設置エリアを特定できるというように、障害発生時にその箇所が容易に特定できるものです。また、ルータ等のアドレスが容易に推測可能であることも有用です。

  たとえば、/24 のアドレスが割り当てられたならば、概念的に /26 に分割して、それぞれを部門別に割り当てて利用します。アドレスブロックの先頭にルータを置き、固定の IP アドレスを後ろから割り当てる等といった運用が考えられます。

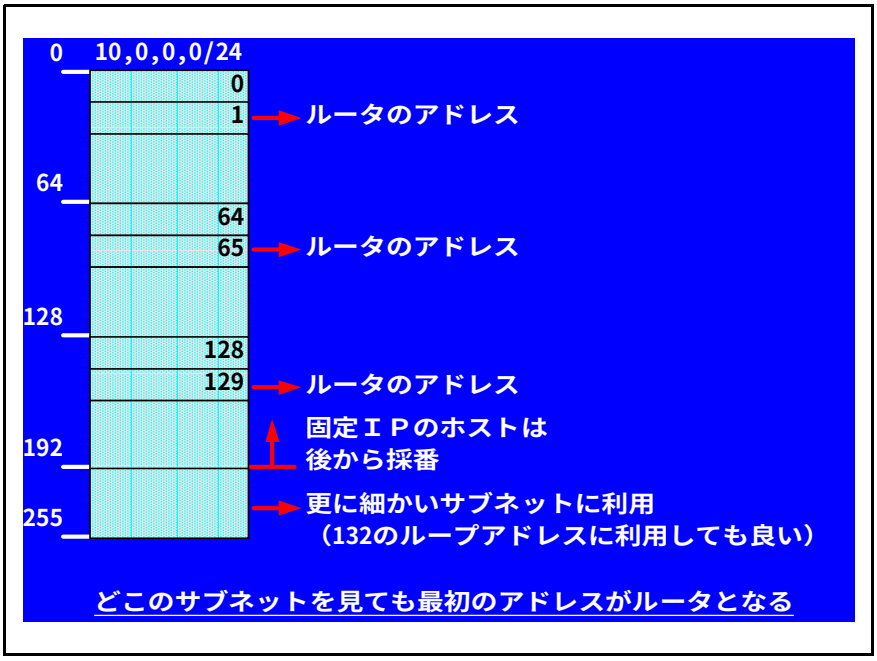

図 4：最適なアドレス採番の例

4.7 ルーティング

ネットワークが大規模になるほど、ルーティングが重要になってきます。同時に、ルーティングに関する障害は、比較的発生しやすいものです。ここでは、ルーティングプロトコルをおさらいしてから、障害に強いルーティングプロトコルとして、HSRP（Hot Standby Routing Protocol）を解説します。

- RIPv2

  古い RIPv1 プロトコルをそのまま VLSM に対応したもので、実装が簡単で安価な機材にも実装しやすいものです。ルーティングテーブルが大きくなる大規模なネットワークには向きません。また、障害発生時の即応性が低いという問題もありますが、小規模なネットワークや、部門ネットワークで利用する場合には最も手軽です。

- OSPF

  ある程度大規模なネットワークにも対応可能で、IGP（Interior Gateway Protocol：内部ルーティングプロトコル）として一般的に使用されています。ルーティングテーブルが更新されたときにのみ、ルーティング情報を配りますので、場合によっては RIPv2 を使用した方がよい場面も考えられます。また、OSPF は、LAN においてはマルチキャストを使ってルーティング情報を配りますので、スイッチ等でマルチキャストを無効にしてはいけません。

  OSPF 運用上の問題として、DR/BDR 問題と呼ばれるものがあります。OSPF では、セグメント毎に DR（Designated Router）と BDR（Backup DR）を選出し、それらがルーティング情報を他のルータに配布します。そのため、DR や BDR がルーティング情報にフィルタをかけていると、フィルタ後の情報しかそれぞれのルータには配られないという問題が起きることがあります。これを防ぐためには、DR/BDR になれるルータを限定しておくとよいでしょう。

  機種によっては、1 つのルータで複数の OSPF プロセスを動作させることが可能なものがあります。そのような機種は、ルーティング情報が混じって欲しくないネットワークの接続に使用することができます。

- OSPF の運用

  OSPF を運用する場合の Tips をいくつか示します。

  - ルーティング情報を redistribute する場合には、subnets オプションを付ける

    ルータが勝手にルーティング情報をアグリゲートしてしまうことが防げます。

  - OSPF プロセス間で redistibute するときには tag を付けておく

    tag を付けておくと、どのプロセスからのルーティング情報であるかをすぐに見分けることができます。

  - デフォルトルートは static routing でも redistribute されない

    デフォルトルートを OSPF で配布する場合には、default-information-originate を使用します。

- ルーティングループに気を付ける

  OSPF と RIPv2 を混在して使用する場合（RIPv2 を使ってルーティング情報を伝達する箇所がある場合）には、distance を調整して、ルーティングループが起きないように注意することが必要です。

- ローカルループバックアドレスを使う

  OSPF のルータでは、インタフェースのアドレスから、最も大きなアドレスをルータ ID として採用します（CISCO の場合）。そのため、インタフェースを切り替えるとルータ ID が変わってしまい、他のルータが混乱してしまうことがあります。ローカルループバックアドレスを割り当てておけば、それがルータ ID になるので、アドレスが変化してしまうことはありません。また、ループバックアドレスを割り当てると、それを「ルータそのもの」のアドレスとして利用できるので、telnet や syslog のアドレスとして便利です。ただし、この方法では、/32 のホストアドレスがルーティング情報として流れてしまうことが欠点です。

• BGP

  主にプロバイダ間で使われますので、ここでは取り上げません。

• HSRP（Hot Standby Routing Protocol）

  1 つの架空の実アドレスに対して、その MAC アドレスを動的に変更することで障害性能を上げる技術で、ダイナミックルーティングが使えない機器の負荷分散や障害回避に有効です（図 5）。

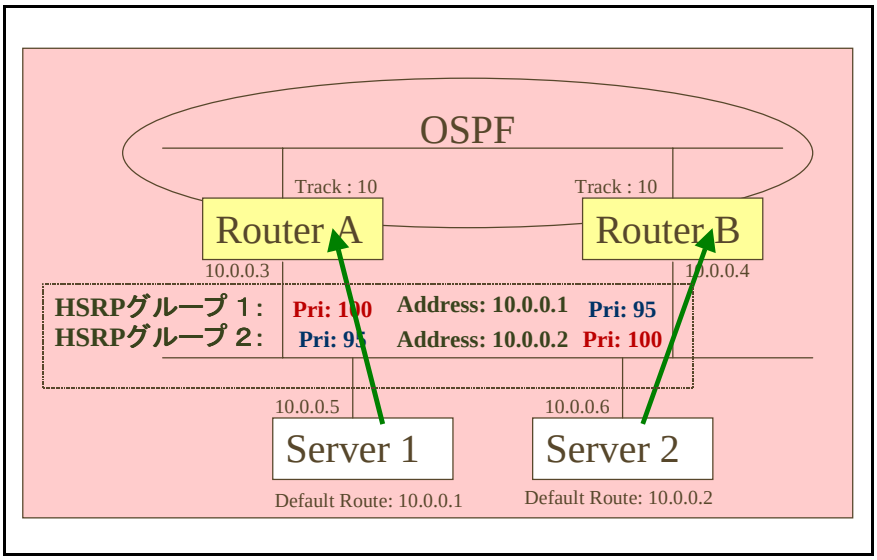

図 5：HSRP（通常時）

仮想的なアドレス、10.0.0.1 と 10.0.0.2 を HSRP グループとして定義し、ルータ毎にそれぞれの仮想的なアドレスに対するプライオリティを割り当てます。通常時は、仮想アドレスに対して、最もプライオリティの高いルータが使用されます。

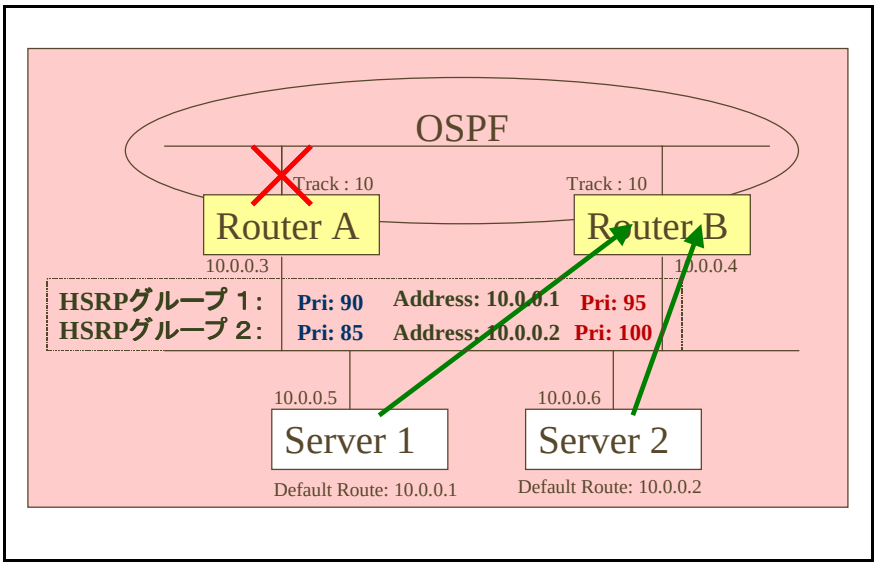

図 6：HSRP（障害発生時）

一方のルータに障害が発生すると、障害が発生したルータのプライオリティが引き下げられ、仮想的なアドレスに対応するルータが変化します。この切り替えは、仮想的なアドレスに対応する MAC アドレスを変更することで行われます（図 6）。

なお、HSRP を利用する場合には、次の点に注意が必要です。

- ルータの機種によって、扱えるグループ数に制限がある。
- パケットリダイレクトが起きないように、no ip redirect を設定する。

4.8 障害監視

障害の発生を最小限にするためには、障害が発生する前にその兆候を検出するための監視が必要です。常日頃からネットワークの健康状態を知っておくことによって、ネットワーク拡張の予測を立てられたり、アタックを見つけられたりするという長所もあります。

監視を行う上での留意点を、まず列挙しましょう。

- 既存の各種ツールを有効に利用する。
- 現在のトラフィックパターンを周知しておく。
- 各ネットワークの管理担当者を明確にしておく。
- 不要な機器はネットワークに接続しない。
- 機器の試験等は専用のセグメントで行う。
- 収得可能なログはできるだけ残しておく。

次に、障害監視に有用なツールを紹介していきます。

- MRTG（Multi Router Traffic Grapher）

  ルータのトラフィックや、サーバのディスク容量等をグラフ化して表示するツールです。同種の RRD Tool というものも登場しており、ツールを組み合わせて、より細かな監視を行うこともできます。

  http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html

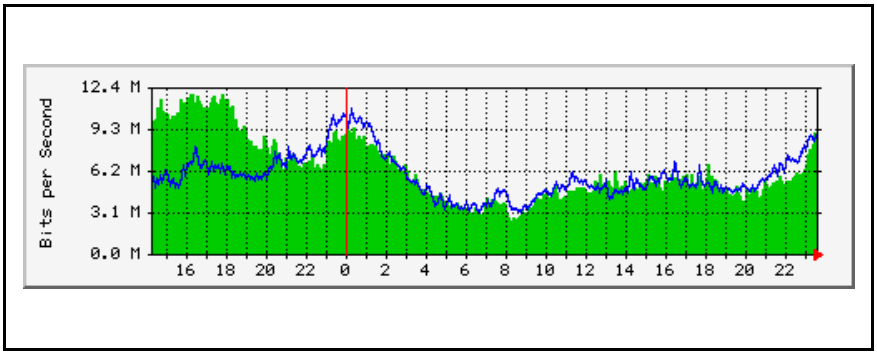

図 7：MRTG によるトラフィック値のグラフ化

- ping

  ICMP_ECHO パケットを利用して、ターゲットホストまでの RTT の参考値を得るツールです。パケットが回線を伝わる時間や、インタフェースでパケットを送受信するための時間が含まれますので、RTT の目安にしかなりません。

- traceroute

  UDP パケットの TTL を変化させ、帰りとなる ICMP パケットによって経路を確認するツールです。基本的に、パケットの流れは行きと帰りで非対称であることに注意が必要です。traceroute で確認できるのは、「行き」の経路だけです。

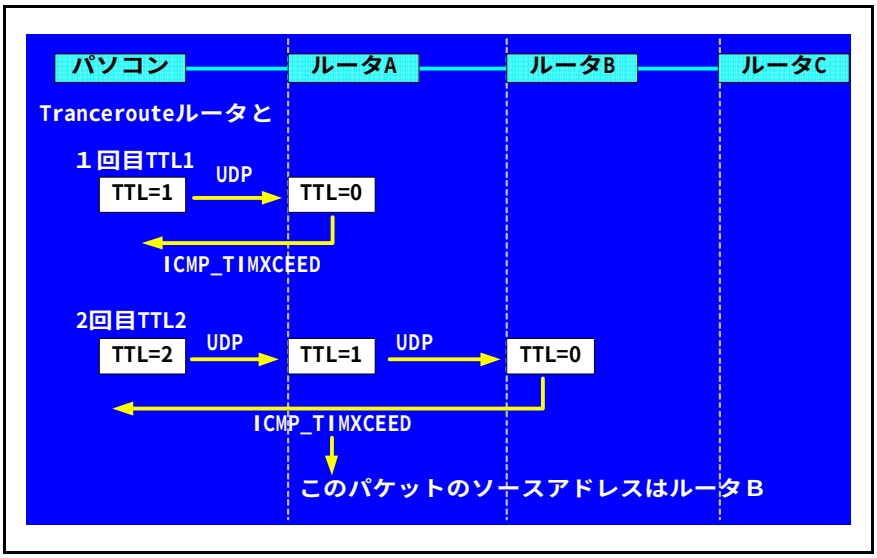

図 8：traceroute

- telnet

  サーバのサービスが稼働していることを確認するために使用できます。次のコマンドで、特定のサービスに接続することができます。

  ```
  telnet <host> <port>
  ```

- Sniffer

  LAN/WAN/ATM 対応のネットワークアナライザで、OSI7 層までのネットワーク障害をリアルタイムで検出することができます。簡易 LAN アナライザとしてソフトの販売も行われています。

  http://www.toyo.co.jp/sniffer/

- TTCP

  2 つのホスト間で TCP パケットをバースト的に送出して、ホスト間のパケットロスや伝送時間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から、利用には注意が必要です。

  ftp://ftp.iij.ad.jp/pub/network/ttcp/ttcp.c（非公式）

- Pathchar

  大量の ICMP パケットを送出し、そのジッターを計測することで、ターゲット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ますし、うまく動作しないこともあります。最近はあまり使われません。

  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。応用範囲が広い点が特徴ですが、SNMP に関する知識が必要です。

  http://www.ece.ucdavis.edu/ucd-snmp/

- BGPView

  BGP-4 の経路監視を行うツールです。現在は α バージョンです。

  http://www.kk.iij4u.or.jp/~kuniaki/bgpview/

- Web ページ

  Web ページから ping や traceroute できるサイトがあり、場合によっては有用です。

  http://nitrous.digex.net

  http://neptune.dti.ad.jp 等

- cflowd

  AS 番号毎にフロー情報を取って、トラフィックを検出することができるツールです。

  http://www.caida.org/Tools/Cflowd/

- その他

  Perl 等の簡易プログラミング言語を使って、細かい監視ツールを有機的に結びつけて利用することで、きめ細かく、かつ利用しやすい監視ツールを構築できます。さらに、メールや携帯電話を有機的に組み合わせれば、検出した障害を直ちに担当者に連絡するツールとすることもできます。