ネットワーク管理と監視フリーソフトの利用法

佐藤 友治（(株）インターネット総合研究所）
矢萩 茂樹（インテリジェント・テレコム（株））

1999 年 12 月 15 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、ネットワーク管理、および監視フリーソフトの利用方法について説明します。

まず、コンピュータネットワークの設計・運用に関する考え方を説明しますので、それによってネットワーク管理の手がかりを掴んでください。その後で、ネットワーク管理に利用できるフリーソフトを紹介します。そして、フリーソフトを使ったネットワーク管理について示します。

2 ネットワーク管理の基礎知識

2.1 ネットワーク管理の歴史

最初に、ネットワーク管理の歴史を振り返っておきましょう。

- 10 年前まで

  メインフレームやミニコンを使った、階層構造のネットワークでした。

- 1980 年代末

  UNIX の普及が始まり、NFS によるディスクや、NIS によるアカウントの共有が一般的になってきました。

- 1990 年代

  UNIX 等のサーバに加えて、ルータ等のネットワーク機器の管理を行う必要が出てきて、ネットワーク管理者の仕事が急増してきました。

- 現在

  UNIX からパーソナルコンピュータまで、多彩なシステムが管理対象となりました。これに伴って、管理対象機器が急増し、ネットワークサービスを把握しておく必要性が高まっただけではなく、そのユーザが技術的な知識を持っていないことを前提とした管理業務が必要とされています。現在、考えなければいけない管理作業には、次のようなものがあります。

  - 共有資源の管理（DNS やメール）
  - ネットワークサービスの管理（外部コネクティビティを含む）
  - セキュリティ管理
  - ユーザ環境の整備
  - ユーザ教育と啓発

2.2 ネットワーク管理の目的

ネットワークを管理する目的は、おおむね次のようにまとめられるでしょう。

- 機器の稼働状況を把握

  スレッシュホールドとして定義した事象を、視覚的・聴覚的に通知するアラーム処理を行うと、異常を早期に発見できます。

- 個人の生産性とコストの制御

  企業においては、コストを抑えつつ、その生産性を確認することが目的の 1 つです。

- ネットワークの規模と複雑さの管理

  ネットワークの規模を常に把握しておかないと、トラブルシューティングに対応することができません。

2.3 ネットワークの規模

ネットワークの規模によって、管理すべき内容や、対象となる機器・技術が異なります。ここでは、ネットワークの規模と、そこで使われる技術についてまとめてみましょう。

- SOHO

  数台のマシンを単一セグメントに接続したネットワークで、ダイヤルアップや 128Kbps まで程度の専用線でインターネットに接続します。ここでは、DHCP や PPP といった技術が使われます。

- キャンパスネットワーク

  大学等の同一敷地内に敷設される比較的フラットなネットワークで、バックボーン部とリーフ部に分けて管理することができます。バックボーンには、ファーストイーサネットや ATM、ギガビット・イーサネット等が使用されています。ここでは、経路制御に OSPF が使われることがあります。

- エンタープライズネットワーク

  企業のネットワークでは、ファイアウォール、アカウンティングの管理等、セキュリティ管理がかなりの比重を占めることになります。ここでは、外部との接続にあたっての NAT、VLAN による論理階層的なネットワークといった技術が使われます。

- サービスプロバイダ

  接続サービスを提供するための認証とアカウンティング、バックボーンを維持するための高速ネットワークや経路制御、経路やサーバの負荷分散といった技術が使われます。

2.4 ネットワーク管理のポイント

ネットワーク管理にあたって、考えておかなければならないポイントには次のようなものがあります。

- トータルコストの低減を目指す。

  人件費が一番高いことを念頭において、管理者を集約して置くことを考えるべきでしょう。

- 単純なネットワーク構成を目指す。

  ネットワーク構築・運用のスタート時から、管理・監視を行うことを前提として、階層的なネットワーク構成を目指すべきでしょう。

- 信頼できるデータ伝送を確保する。

  ネットワークの内部で管理を行うのか、管理用に別のネットワークを作るのかを考えておきます。初期投資はかさみますが、監視専用のネットワークで重要なサーバやリンクだけでも見ることができると、障害時に役立つでしょう。

- 手に余る管理は目指さない。

  組織や上司に管理できる範囲を理解してもらい、適切な権限委譲が行われることが重要です。

- 正常時の状況を把握する。

  ネットワーク設計書に基づき、現在のネットワークの状況を常に把握しておくことが極めて重要です。特に、最近では VLAN が複雑に組み合わさる等、物理構成図を見ただけでは分かりづらいネットワークが多くなっていますから、ドキュメント化してそれを把握しておくことが必要です。また、機器購入による拡張や変更を履歴として記録しておくことも重要です。

- 健康管理を行う。

  ネットワーク管理専用の機材を導入した場合には、それらがきちんと動作していることを定期的に検査しなければなりません。いざと言うときに動作しないものでは、管理の役に立ちません。

2.5 ネットワークの管理ポリシー

ネットワーク管理を行うにあたっては、あらかじめ次のような点における管理ポリシーを定め、それぞれの責任範囲を決めておくことが重要です。

- 管理対象は何か。
- どのような管理作業を行うか。
- 担当者と責任者は誰か。
- 障害発生時にはどのような手順で対応するか。
- ユーザの責任範囲はどこまでか。
- 管理に付随する作業（作業報告書等）は何か。

2.6 ネットワークの監視

ネットワークの動きを理解するために、リアルタイムの監視ツールや、オフラインによるレポート等を使用して、次のような項目を調査すると良いでしょう。

- トラフィックフロー
- 利用度（現在のもの / 過去のもの）
- 利用の傾向（いつ頃どこで）
- アクティビティの監視

かつては、主に内部ネットワークのトラフィックを監視することが多かったのですが、最近ではインターネットへのトラフィックを監視し、維持することが重要になっていると思われます。

なお、ネットワーク監視を行う場合には、監視基点を定めて、Inside と Outgoing の区別を付けやすいように気を付けます。ポリシーを決めておかないと、監視地点毎にトラフィックの向きが逆順になる等、混乱の原因となってしまいます。

2.7 何を監視するか

監視の概要を理解したところで、具体的に何を監視すべきかを、機器毎に見ていきましょう。

- ルータ、スイッチ

  インタフェース毎のトラフィック、パケットロスやコリジョンの頻度を監視します。ネットワークの混雑度が分かったならば、それを基にして、トラフィックを運ぶ経路としてふさわしいものを考察します。スイッチやルータを導入した方が良いのか、冗長な経路があるならばどれを使うのが効率的か、ルーティングプロトコルを使用するのが良いか否か等といった判断を行います。

- サーバ

  インタフェースや、ディスク容量、CPU の稼働状況を監視するだけではなく､ユーザ数やトランザクション数､稼働しているアプリケーション等も監視すべきでしょう。また、サービス毎のトランザクション数やエラー状況を調べることも必要です。

  さらに、セキュリティ対策を施したならば、その稼働状況の監視も必要です。ファイアウォールを導入しても、その管理が必要なことを忘れがちです。

監視対象を決めて、運用を始めたならば、それぞれの機器が正常に動作していること、ボトルネックとなっている箇所が無いこと等を常に監視し続けることになります。

2.8　ネットワーク管理システム

ネットワーク管理を行うシステムを概念的に表すと、図１ のようになります。

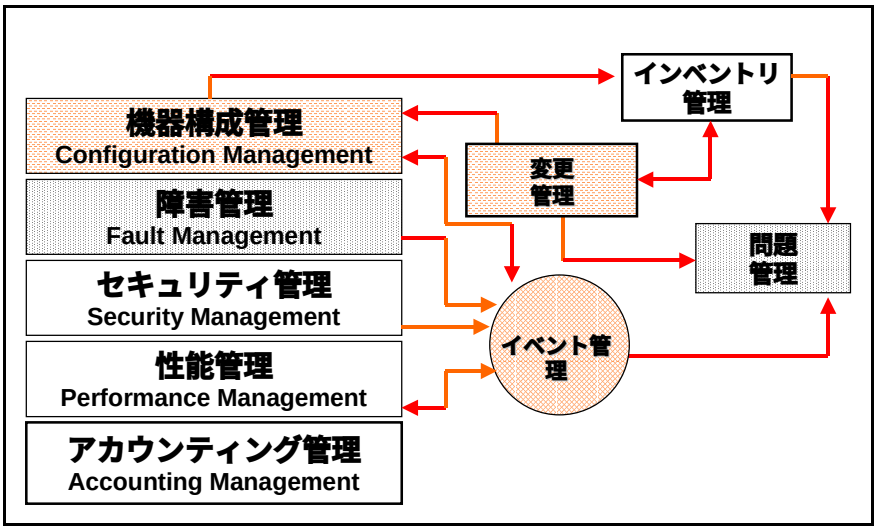


図１：ネットワーク管理構造

中でも重要なのは、「障害管理」と「機器構成管理」の機能でしょう。

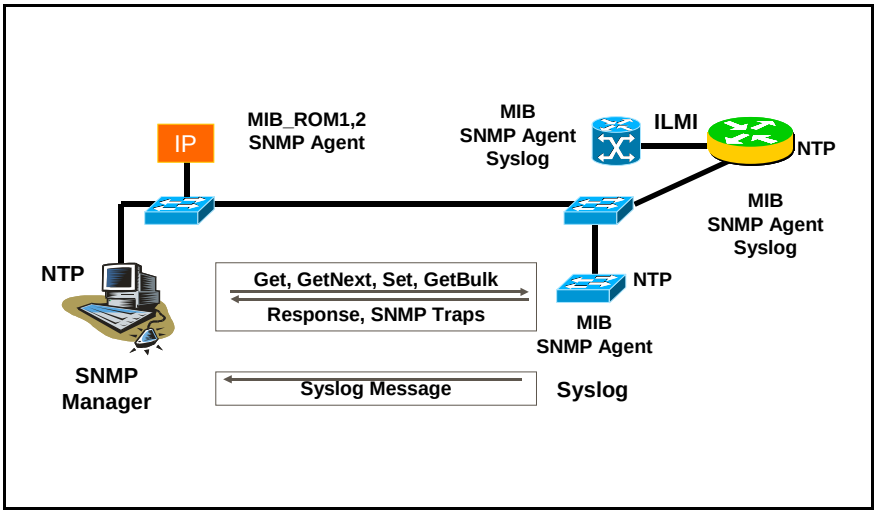


図２：ネットワークの障害管理と機器構成管理

後半で紹介していくネットワーク管理ツールでは、主に SNMP の機能を使って必要な情報を収集していきますが、IP コネクティビティそのものや、Syslog 機能、NTP（Network Time Protocol）の機能、Auto Neibor Discovery や ILMI（Integrated Local Management Interface）の機能等を利用するものもあります。

2.9 ルータの管理

ルータの管理を行うためには、そのための設定をしておく必要があります。主な設定項目を次に示します。

- Loopback インタフェースを定義

  ルータ自体を表すことになる、ループバックインタフェースを定義して、管理用の IP アドレスを割り当てます。もちろん、telnet できるポートには、パスワードをセットしておきます。

- SNMP コミュニティ

  パブリックなものには必ずReadOnly属性を付けること、逆にReadWrite属性を持つものには想像しにくいコミュニティ名を付けて、セキュリティ対策とします。もちろん、アクセスリストを設定することも大切です。

- ログ

  syslog サーバを用意して、ログを記録します。内部のネットワークで NTP を使用して、時刻を同期させておくと良いでしょう。

- SSH（Secure SHell）

  ルータにも SSH が組み込まれるようになってきています（Cisco 社、Juniper 社等）。セキュリティのために、使える場合には活用すると良いでしょう。

2.10 監視結果の通知

監視したものは、オペレータに通知しなければ意味がありません。現在では、監視結果をグラフ（Web ベース）で表示したり、メールやページャに通知したりするツールを簡単に実現できるようになっています。

2.11 ネットワーク監視のトレンド

最近のトレンドとして、SLA（Service Level Agreement）に基づくネットワークサービスを提供することが多くなると考えられます。この実現準備段階として、ping を使って、パケットロスや RTT を調べることが有効です。定常的に監視を行う場合には、ルータではなく、サーバの応答に対して使うべきでしょう。ルータに対する ping は、予想外にルータの負荷を上げてしまうことがあります。

2.12 SNMP（Simple Network Management Protocol）

SNMP の基礎的な知識を簡単にまとめておきましょう。SNMP はマネージャ（クライアント）/ エージェント（サーバ）型のプロトコルで、UDP の 161/162 番ポートを使用します。

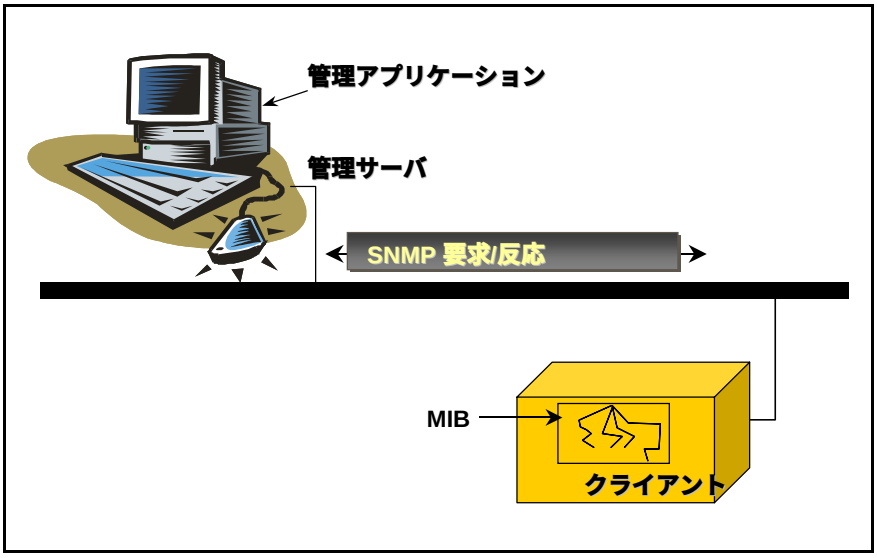


図 3：SNMP の概要

エージェントには、MIB（Management Information Base）と呼ばれるデータベースが納められており、マネージャはそれらを参照してトポロジデータベースや、モニターログを作成・管理します。MIB 情報は、マネージャからエージェントに問い合わせる場合（polling）と、事象が発生したときにエージェントからマネージャに通知する場合（trap）があります。また、マネージャからエージェントの設定を変更することもできます。

SNMP による情報収集は、マネージメントステーションから管理対象機機をポーリングすることが基本となります。このプロトコルでは、ネットワーク全体の状況を把握するのみで、どのような通信が行われているかを知ることはできません。また、UDP は再送制御を行わないため、エージェントからの情報が必ず届くとは限りません。

エージェントが保持しているMIBとは、階層的な命名体系で管理オブジェクトを定義したものです。

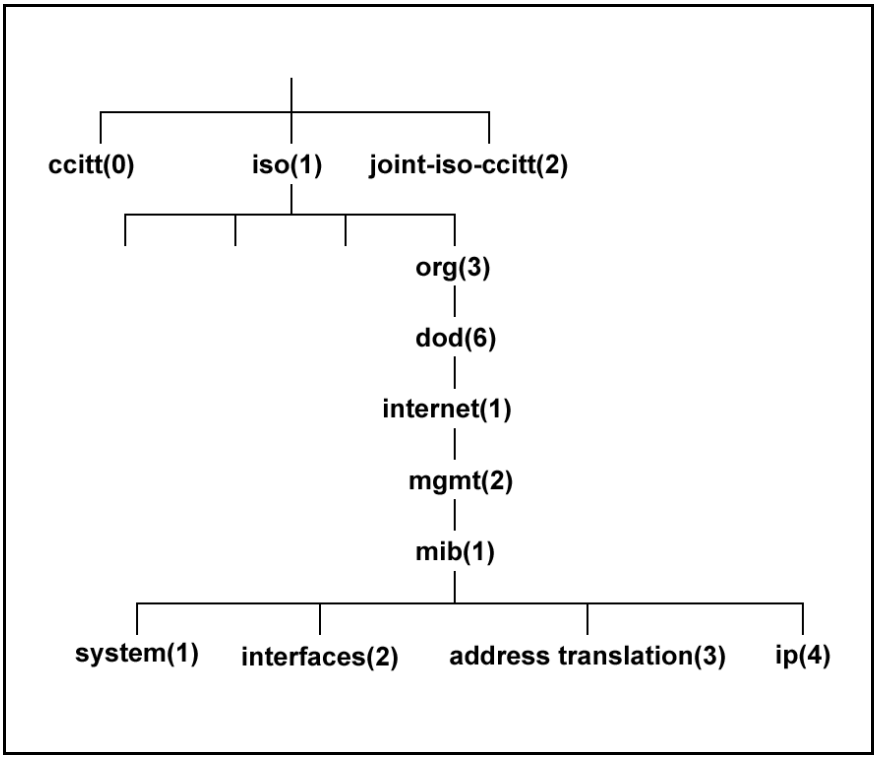


図 4：MIB の階層的命令体系

トラフィックフロー測定機構と MeterMIB（データ測定用 MIB）の実装と利用に関する実験の記録が RFC2123 に述べられています。これを使ったツールとして、NeTraMet や NeMac 等があります。

2.13 まとめ

ネットワークを管理するためには、まず、ネットワークの規模や稼働状況、ユーザの挙動等を把握することが大前提となります。その上で、効果的なポイントにおいて、フリーのツール等を使ってコネクションとトラフィックを把握して、再設計や拡張のための指針を作ります。

3 フリーソフトによるネットワーク監視

3.1 なぜフリーソフトか

ネットワーク管理ツールと呼ばれる市販製品がいくつも存在していますが、ここでは、主にフリーソフトを取り上げます。フリーソフトを利用するメリットとして、次のような項目が挙げられます。

- 小規模なネットワークでも、手軽かつ安価に監視できる。
- 実際に管理している人のノウハウが反映されている。
- 改造して利用できる（教育効果）。
- PC の低価格化と PC-UNIX の普及により導入が容易である。
- ビジュアライズが容易である（Web ブラウザの普及）。

一方、市販ツールのメリットとしては、オートコレクト等のネットワーク分析機能や、ベンダーからの情報提供が必要な VLAN への対応等が挙げられます。

現在のフリーの管理ツールは、X ベースから Web ベースに移行しつつあると言えるでしょう。Perl ベースのツールによって、グラフィカルな表示を Web 上に行うものが増えています。

すべてを 1 つで満足するツールはありませんから、適材適所のツール群を組み合わせて、簡単に監視システムを作ることが重要です。最低限 3 種のツール（状態監視、状態検知、トラフィック監視）を組み合わせ、それらを Web で統合するのが望ましいものと考えられます。

次に、ネットワークの監視・管理に役立つフリーソフトについての理解を助けるために、ネットワーク機器の監視方法、監視手段、監視システムの要件をまとめておきます。

3.2 ネットワーク機器の監視方法

ネットワーク機器を監視する方法は、次の 2 つに大別されます。

- 個別監視－クライアントベース

  監視対象となるサーバ自身で、各サービスの状態監視を行い、問題があった際にアラートをあげるものです。運用者がサーバを見て回ることが前提となるため、遠隔地にある装置の監視はできません。

- 集中監視－共通

  監視サーバを立ち上げて、監視対象の外部から監視を行うものです。個別監視の場合とは異なり、サーバのシステムダウンや、ルータやスイッチの監視も行うことが可能です。特に、集中監視によって、少ない人数で多くの機器を監視することができるのが最大のメリットです。

集中監視方法の 1 つとして、監視対象のサーバやサービスには特別なしくみを用意せずに、監視サーバからサービスポートをポーリングすることによって稼働状態を監視するものがあります。大変に手軽ですが、詳細情報を収集できない、ディスクフル等のサーバ自体の問題に対処できないという問題があります。

そこで、監視対象のサーバに、詳細情報を収集するためのプローブを組み込んでおく方法が考えられます。SNMP による監視はこの方法の代表です。詳細で高度な管理が行える反面、インストールが面倒で、プラットフォーム毎に適切なプローブを用意しなくてはならないという問題があります。

3.3 監視する手段

ネットワーク機器の稼働状態を調べるための手段として、次のようなものが考えられます。

- ICMP によるポーリング

  ping による疎通確認であり、IP ネットワークに繋がっている機材では必ず使えるのが利点です。

- TCP ポートのポーリング

  サービスポートを直接監視することで、実際にサービスが稼働しているかどうかを直接判断できます。

- SNMP によるポーリング

  標準プロトコルですから、ベンダーに関わらず様々な機器の監視に使用することができます。商用製品が多いこともメリットの 1 つでしょう。サーバには個別に SNMP デーモンを設定する必要があります。

- イベントによるトラップ

  システムの状態が変化したときに、何らかのイベントを発生させるものです。サーバによる個別状態監視はこの方法の 1 つです。また、syslog によるメッセージ伝達や、SNMP トラップによるものは、エージェント / マネージャによるイベントの処理方法です。

3.4 監視システムの要件

「ネットワークを監視する」ということをさらに分類すると、次の 3 つの切り口に分けられます。

- 現状監視（今を知る）

  ポーリング等によって、現在のシステム状態を知ることです。

- 現状検知（今を検知する）

  トラップによって、自律的なアラームを捕らえることです。

- 経過監視（これまでを見る）

  ネットワークや機器のトレンドを把握することです。

これらは、密接に関連しあった独立の事柄ですから、どれが抜けても不十分なものとなってしまいます。監視システムを構築する際には、この 3 つの切り口を念頭に置いて、監視ポイント・モジュール構成を検討する必要があります。

この他に、監視システムに求められる機能を考察してみると、次のようにまとめることができるでしょう。

- Web 画面でリモート監視・確認

  管理する人間をできるだけ集中して配置できるように、監視は 1 カ所で行い、そこから通知できることが求められます。また、監視作業は各人が作業に使っている端末だけでなく、どこにでもあり、誰もが持っているソフト（現在では Web ブラウザ）で行えることも必要です。

- E-mail で通知、ページャ呼び出し

  リモートからも、情報を収集して対応できることが求められます。トラップをメールで通知して、ページャを呼び出してくれると嬉しいでしょう。

4　ポーリングによる状態監視ツール

紹介した分類方法のうち、ポーリングによってネットワークの状態を監視し、Web ベースで見ることができるツールを紹介します。SCOTTY 等、古くからの優秀なツールもありますが、今回は「Web ブラウザで見られる」ものを取り上げました。

4.1　Big Brother

http://maclawran.ca/sean/bb-dnld/

監視・表示・通知の機能が分散している、サーバークライアント型の監視システムです。機能が分離しているので、監視サーバを分散して置きながら、表示サーバに集中して状態表示を行うといった、柔軟な運用が可能となっているのが特徴です。また、NT や NetWare 用の監視クライアントを用いれば、それらの機器の稼働状況を監視することも可能です。

Big Brother で監視できるサービスは次のとおりです。

・サービス：ping、smtp、http、pop3、dns、ftp、telnet、ssh 他

・サーバ状態（プローブが必要）：CPU、disk、processes、logs 他

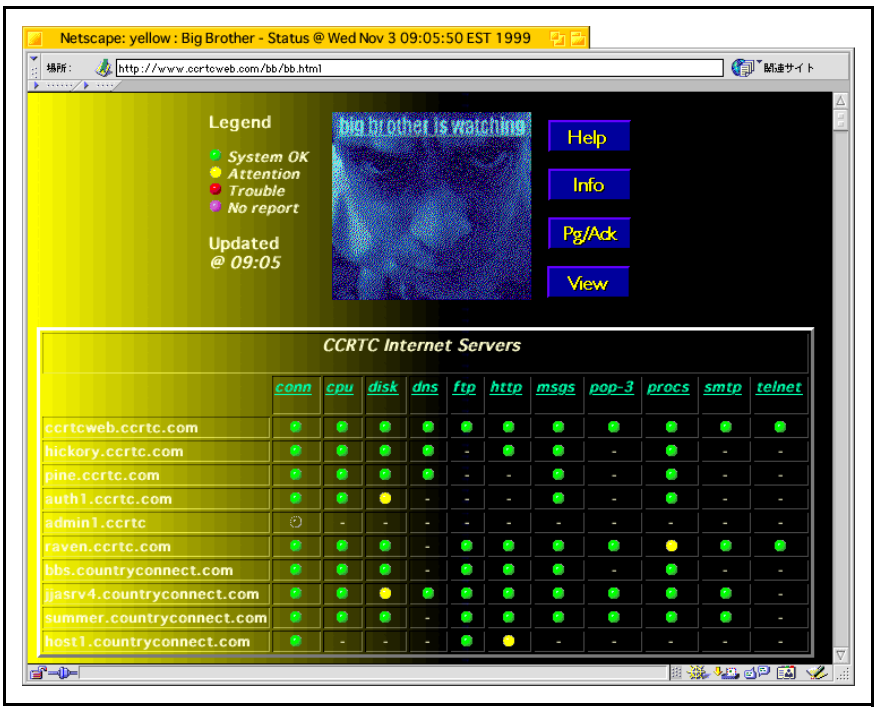


図 5：Big Brother の画面例

Big Brother を実際に使用すると、次のような点が非常に便利に感じられます。

- 監視対象をグループ化することができる。
- ホスト単位でシステムの停止時間（監視対象外時間）を指定できる。
- ホスト単位で障害通知先を変更できる。
- 簡単な障害履歴機能がある。
- 異常状態の機器のみを抽出した画面表示を行うことができる。
- 取り扱いが非常に簡単である。

このソフトは、主に次の 2 つの設定ファイルによって、動作をカスタマイズできます。

- bb-hosts

  /etc/hosts と同様のフォーマットで、ホスト毎に監視するサービスを定義します。監視サーバ、表示サーバ、通知サーバ、表示 URL、監視するサービス等をコメントとして記入します。

- bbwarnrules

  ホストグループとサービスの組み合わせ毎に、障害検出時刻や障害発生時の通知方法を定義します。

4.2 SPONG

http://www.edsgarage.com/projects/spong/

Big Brother をベースとして開発されたもので、しばらく開発が止まっていましたが、新しい開発者の元で作業が再開されています。Big Brother と同様の特徴を持っていますが、それに加えて、障害ログの管理機能が充実しています。すなわち、ホスト単位、サービス単位といった多面的なログ解析機能を備えています。

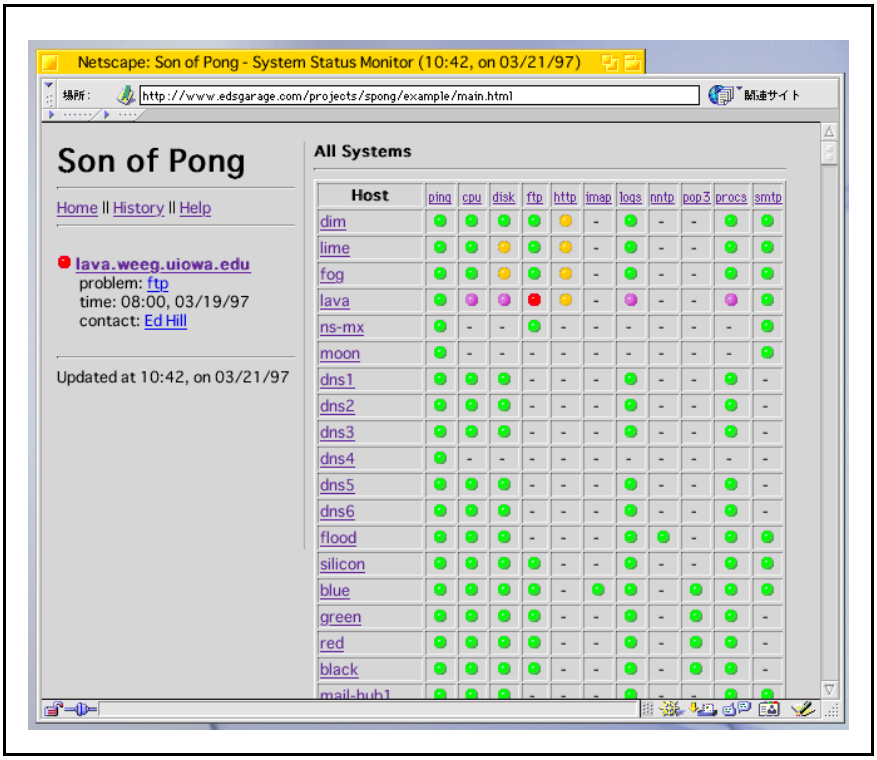


図 6：SPONG のメイン画面

このソフトの設定ファイルは、Big Brother とはかなり異なっており、Perl の定義文を並べたような感じのものとなっています。主な設定ファイルとして、ホスト毎に、監視対象とするサービスや、稼働時間、障害通知者等を定義する spon.hosts ファイルがあります。

4.3 Angel

http://www.ism.com.br/~paganini/angel

簡単な設定で使えて、表示画面がとてもきれいなツールです。Perl で記述されています。開発途上で機能的に十分ではないために、ここでは解説を省略します。

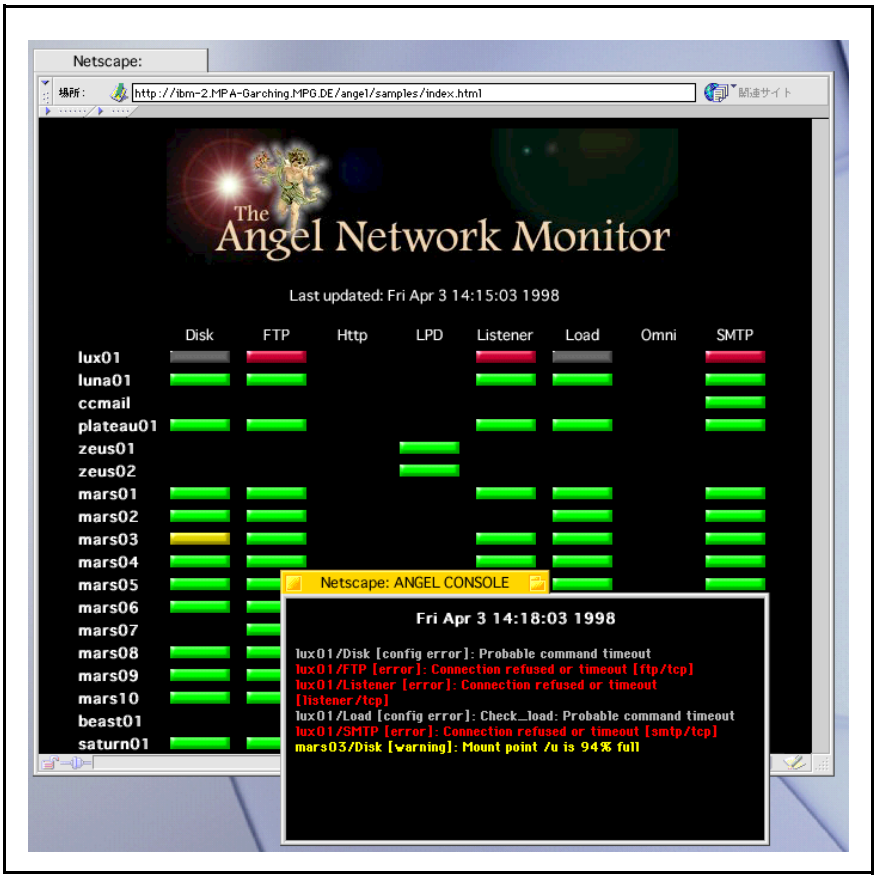


図 7：Angel の監視画面

4.4　NOCOL

http://www.netplex-tech.com/software/nocol

ICMP と TCP ポーリング以外に、CMU-SNMP パッケージの拡張版を使用して SNMP ベースでの監視を行えるほか、ネットワーク機器に直接 telnet でログインして情報を収集することもできる、極めて高機能な状態監視ツールです。稼働実績も多く、米国の ISP 等でも盛んに利用されているようです。また、同一の対象に対して、複数の通知レベルを定義することも可能となっています。

NOCOL で監視できるサービスは、次のように多岐に及びます。

ping、Ethernet 負荷、Radius、ntp、bgp ピア、RPC portmapper、
TCP ポート、syslog、UPS、SNMP 変数、DNS、メールキュー……

NOCOL は、統合的な 1 つのツールではなく、個別機能を持ったツールを組み合わせて設定・利用するタイプのツールです。そのため、設定ファイルやツールの数も極めて多く、挑戦し甲斐のあるツールであると言うことができるでしょう。

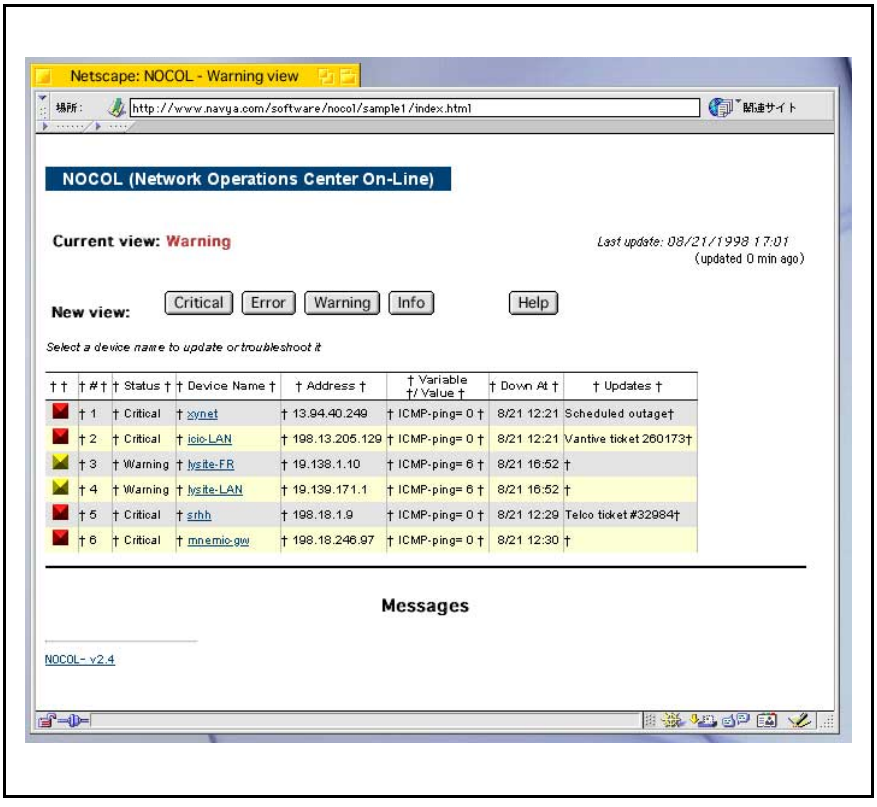


図 8：NOCOL の監視画面

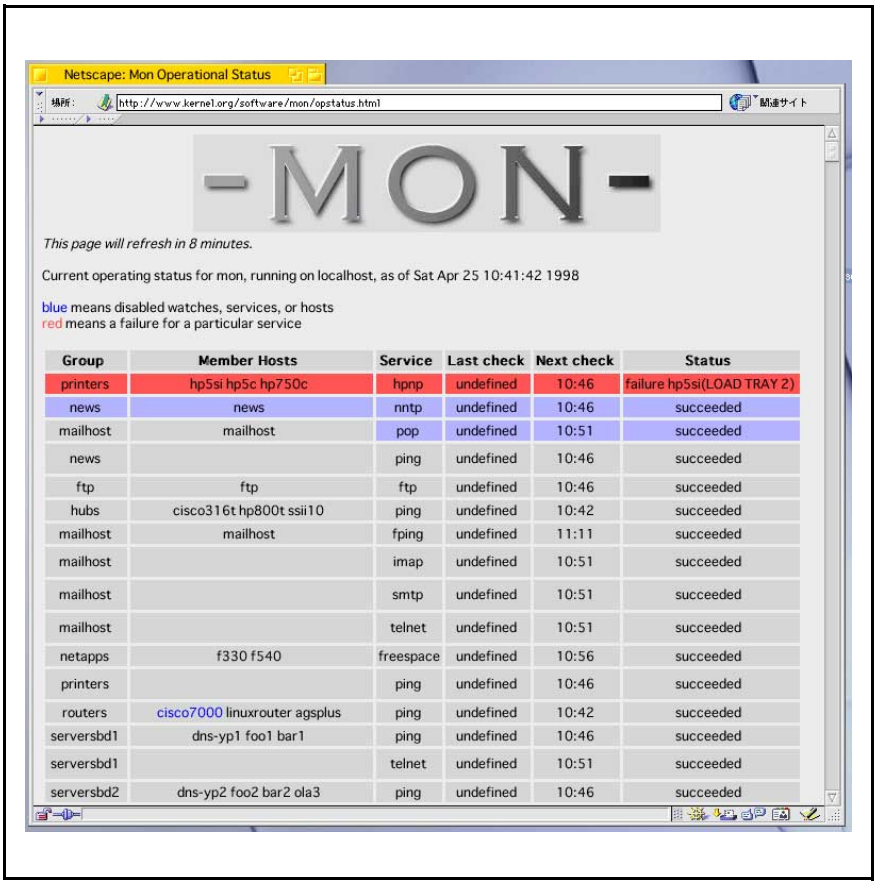
4.5 mon

http://www.kernel.org/software/mon

機能的には、Big Brother と NOCOL の中間くらいの多機能監視ツールです。このツールも UCD-SNMP パッケージをベースとしており、ICMP と TCP によるポーリング以外に、SNMP による監視を行うことができます。監視機能はかなり細かくカスタマイズすることができますが、通知機能は簡単になっています。

mon で監視できるサービスを次に示します。

ping、SMTP、telnet ftp、nntp、http、pop3、imap、
TCP ポート、ディスク容量、SNMP 変数、LDAP、DNS、モデム



Group	Member Hosts	Service	Last check	Next check	Status
printers	hp5si hp5c hp750c	hpnp	undefined	10:46	failure hp5si(LOAD TRAY 2)
news	news	nntp	undefined	10:46	succeeded
mailhost	mailhost	pop	undefined	10:51	succeeded
news		ping	undefined	10:46	succeeded
ftp	ftp	ftp	undefined	10:46	succeeded
hubs	cisco316t hp800t ssii10	ping	undefined	10:42	succeeded
mailhost	mailhost	fping	undefined	11:11	succeeded
mailhost		imap	undefined	10:51	succeeded
mailhost		smtp	undefined	10:51	succeeded
mailhost		telnet	undefined	10:51	succeeded
netapps	f330 f540	freespace	undefined	10:56	succeeded
printers		ping	undefined	10:46	succeeded
routers	cisco7000 linuxrouter agsplus	ping	undefined	10:42	succeeded
serversbd1	dns-yp1 foo1 bar1	ping	undefined	10:46	succeeded
serversbd1		telnet	undefined	10:51	succeeded
serversbd2	dns-yp2 foo2 bar2 ola3	ping	undefined	10:46	succeeded

図 9：mon の監視画面

mon の設定ファイルは、監視クラスを定義して、そこに監視対象を設定していく、一種のスクリプトのような形式になっています。

4.6 状態監視ツールのまとめ

ここで紹介したツールを、機能と使いやすさの面から分類すると、図 10 のようにまとめることができるでしょう。バランスの面から、Big Brother と SPONG がお勧めです。

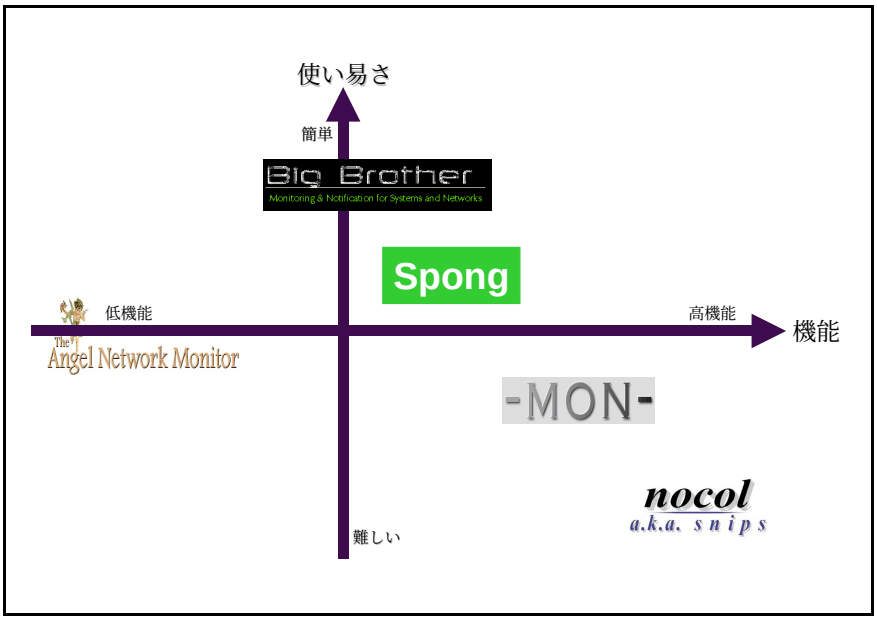


図 10：状況監視ツールのセグメント分類

5 トラップベースの状態検知ツール

次に、「今を検知する」ためのツールを紹介します。特に、SNMP のトラップを検出するためのツールは、ルータの状態を検知するために有効です。

5.1 SWATCH

http://www.engr.ucsb.edu/~eta/swatch/

ログファイルを監視して、パターンに一致したイベントが発生した場合に、アクションを起こすためのツールです。syslog を取りまとめる loghost 等で SWATCH を利用し、サーバプロセスの監視を行ったり、セキュリティ向上のために使用したりすることが多いものです。

SWATCH の設定ファイルには、検出するパターンと、それに対するアクション（コマンド）を記述していきます。UNIX マガジンの 1999 年 12 月号「ファイアウォールの作り方」にて詳細が説明されています。

5.2 UCD-SNMP パッケージ

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

様々な UNIX プラットフォームで稼働する、統合的な SNMP パッケージです。次のコマンドから成っています。

- snmpd

  SNMP のクライアント（エージェント）プログラムです。

- snmptrapd

  SNMP トラップイベントを受信して、様々なアクションを実行するクライアントプログラムです。受信したトラップイベントを、外部プログラムの標準入力として引き渡すことができますから、様々なスクリプトを作成するのに便利です。

- その他

  snmpbulkwalk、snmpget、snmpset、snmptest、snmpusm、snmpcheck、snmpgetnext、snmpstatus、snmptranslate、snmpwalk、snmpdelta、snmpnetstat、snmptable、snmptrap といった、標準的な SNMP 機能を実現するプログラムが含まれています。

なお、同種の SNMP 統合パッケージとして、CMU-SNMP パッケージがあります。ここでは、簡単さの点から UCD のものを紹介しました。

6 経過監視ツール

状態の経過を監視するためによく使用されているツールとして、MRTG（Multi Router Traffic Grapher）と PyNG（the Python Network Grapher）が挙げられます。機能的にも、普及具合からも、ここでは MRTG を主に取り上げます。

6.1 MRTG （Multi Router Traffic Grapher）

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

http://www.ceres.dti.ne.jp/~riocat/webtools/mrtg/（和文）

ほとんどの UNIX プラットフォームと Windows NT で動作し、主にネットワークトラフィックを監視するために使用される、非常に稼働実績の多いツールです。MRTG の特徴は次のとおりです。

- トラフィックだけではなく、2 系列のデータを集計して、短期・中期・長期のトレンドグラフを（Web ブラウザ上に）表示します。
- 独自に SNMP 機能を実装しているため、外部に SNMP パッケージを必要としません。
- 定期的にログをサマリーしており、ログファイルのサイズが大きくなりません。
- 設定を半自動で行うツールが付属しています。
- 日・週・月・年のデータを集計して表示します。

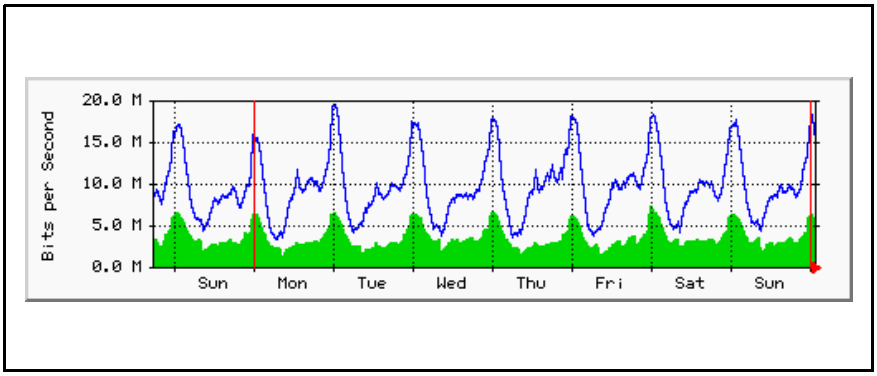


図 11：MRTG で作成したトレンドグラフ

MRTG の簡易設定ツールは、SNMP のコミュニティとターゲットを指定するだけで、機器に存在する ifInOctets や ifOutOctets を測定するための大部分の設定ファイルを自動生成する優れたツールです。syscontact や location の情報、停止しているインタフェース情報等は、コメントとして設定ファイルに書き込まれます。したがって、簡易ツールで作成した設定ファイルに WorkDir のみを指定すれば、トラフィックの測定を行うことができるようになります。

MRTG は独立したコマンドとして作成されているため、cron で定期的に起動して使用します。config ファイルの Target レコードで、インタフェースインデックスや SNMP の OID インデックス、MIB シンボル、インタフェースのアドレス等を指定します。ルータやスイッチでは、インタフェースの増減によってインタフェース番号（ifIndex）が変化するものがありますが、MRTG には、割り振られたアドレスをキーにしてデータ照会を行い、ifIndex の変化に対応する機能があります（IP アドレスによるポート指定）。

外部コマンドを実行して、その結果を集計してグラフ化することも、MRTG では可能です。外部コマンドには、各行に入力バイト数、出力バイト数、機器の稼働時間、機器の名称を出力するコマンドを指定します。

たとえば、簡単なスクリプトを作成し、ping によってパケットロスの定期的な監視を行い、ネットワークの品質を測定することもできます。

MRTG を使用する場合には、次のような点に注意します。

- データの方向性に注意する。

  対外線を出口として、そこを基準にデータの流れる方向を考えると良いでしょう。

- データの単位に注意する。

  ifInOctets や ifOutOctets は Octets 単位、回線速度は bps 単位となります。

- インタフェースアドレス指定を効果的に使う。

  ifIndex ではなく、IP アドレスによる指定を使うのが便利です。

7　今後期待するツール

7.1　NetSaint

http://www.netsaint.org/

今後期待できそうな Web ベースの監視システムで、Web ブラウザを使って管理・変更ができるのが特徴です。現在開発中であり、パッケージとしての配布は行われていません。プラグインを利用する形式となっていて、外部拡張が可能です。

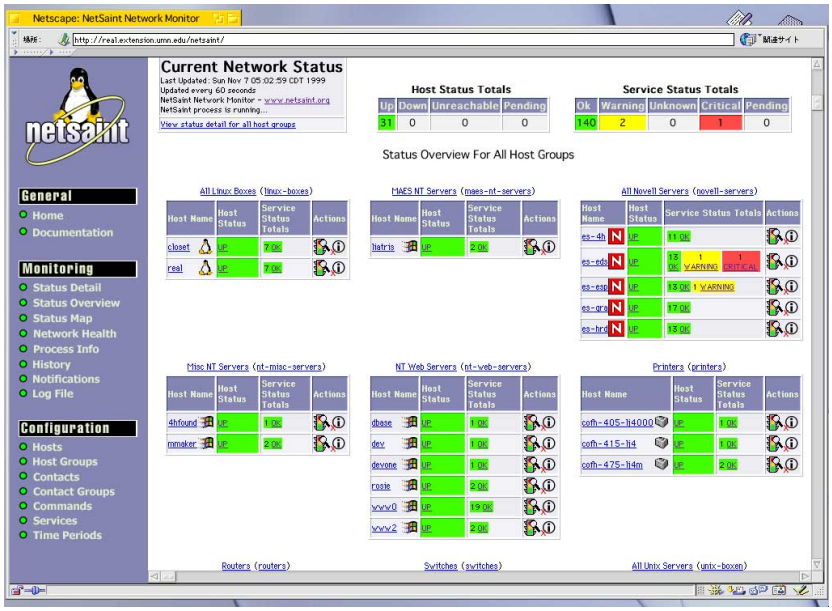


図 12：NetSaint の Summary 画面

7.2 RRDTools

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

MRTG の作者である Tobi Oetiker による後継プロジェクトで、Round Robin Database Tools が正式名です。MRTG の利点を生かしつつ、より柔軟に、より多彩な表現ができることを目標として、データベース管理とグラフ作成に特化したツールです。RRDTools だけでは Web で表示することはできませんが、Remstat や ORCA、NRG といったフロントエンドプログラムが既に開発されており、これらと RRDTools を組み合わせることにより、統合トラフィック監視システムを構築できます。

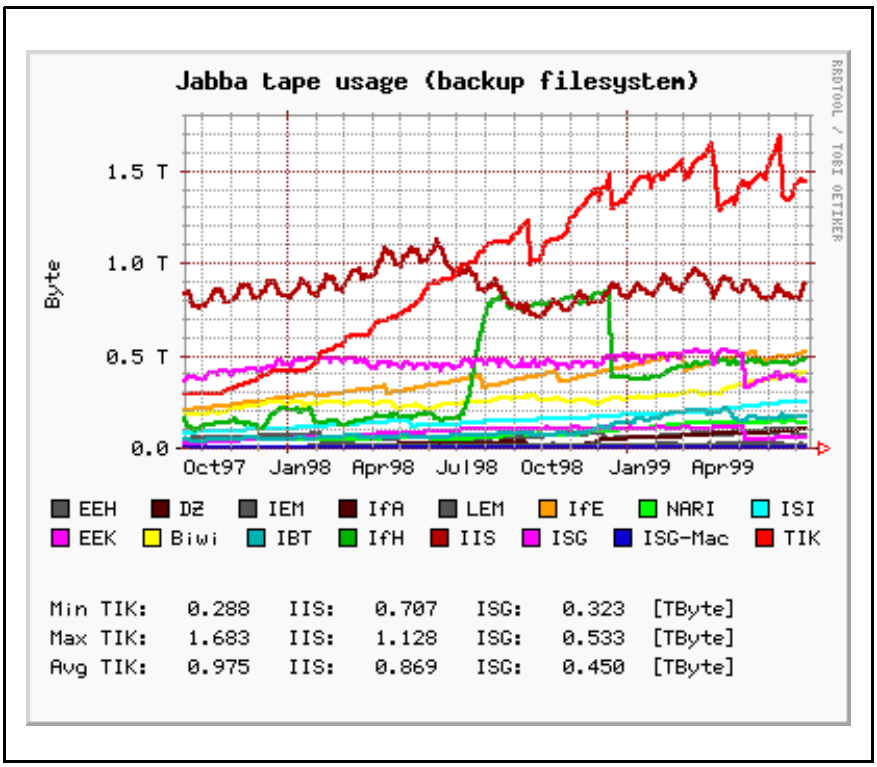


図 13：RRDTools により作成したグラフ

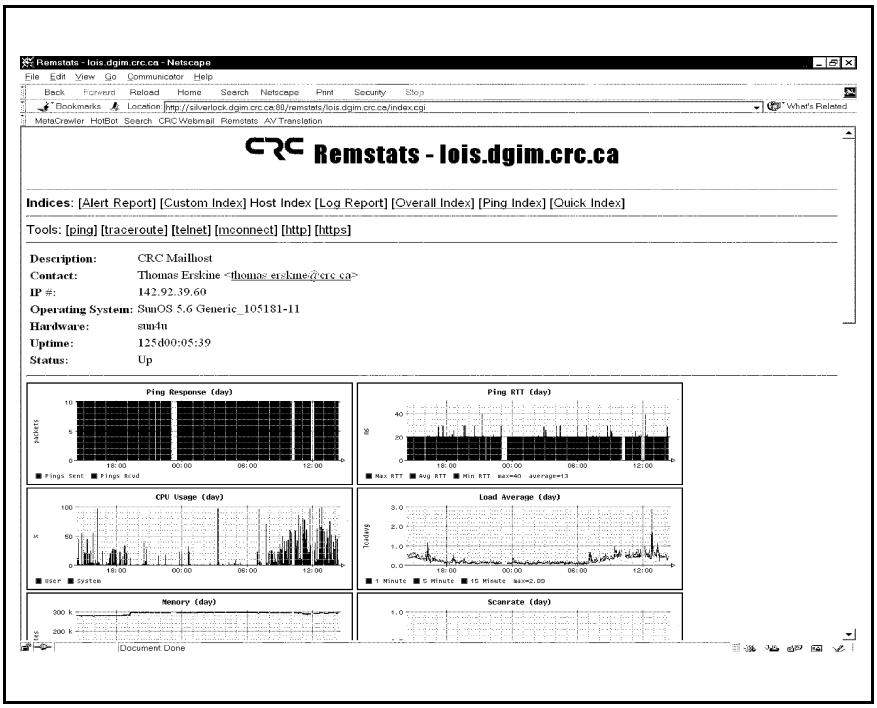


図 14：RTDTools と Remstat による表示例

8 その他のツール

Webベースではありませんが､ネットワーク管理に有効に利用できるツールを簡単に紹介しておきます。

8.1 基本コマンド

監視・設定に使う一般的なコマンドには、次のようなものがあります。これらを組み合わせて、Shell や Perl スクリプトを作成することもよくあります。

- ping
- traceroute
- nslookup
- ifconfig
- arp
- netstat
- tcpdump （snoop）

- route
- telnet （ポート番号指定）
- SNMP tools

8.2 Expect

http://expect.nist.gov/

telnet、ftp、passwd といった対話型のツールを自動化するために、便利に使用できるツールで、イベントが発生した後の調査、ログ処理の自動化等に有効です。Tcl ベースのツールですが、最近は Perl モジュールも登場しました。

8.3 Scotty

http://wwwhome.cs.utwente.nl/~schoenw/scotty/

ネットワークマップを作成する機能が充実した、Tclベースのツールです。

8.4 NFR（Network Fright Recorder）

http://www.nfr.net/

Network Fright Recorder, Inc による侵入検知システムですが、管理のためにも有用です。パケットの収集と解析を実行し、Java 対応の Web ブラウザでそれを参照することができます。

コラム：MIB-2

RF-1213 で規定される MIB-2 を簡単にまとめておきましょう。iso（1）.org（3）.dod（6）.internet（1）.mgmnt（2）.mib（1）の下にある、代表的な MIB は表 1 のとおりです。ネットワーク監視で使用するほとんどのパラメータは、system（1）と interfaces（2）の下にあります。

表 1：代表的な MIB

1	system	システムグループ
2	interfaces	インタフェースグループ
3	at	アドレス変換グループ
4	ip	IP グループ
5	icmp	ICMP グループ
6	tcp	TCP グループ
7	udp	UDP グループ
11	snmp	SNMP グループ

特に、トラフィック計測で頻繁に参照するパラメータを表 2 に示します。いずれも、iso（1）.org（3）.dod（6）.internet（1）.mgmnt（2）.mib（1）.interface（2）に属するパラメータです。

表 2：トラフィック計測で参照するパラメータ

1.3.6.1.2.1.2.2.1.1 : ifIndex	インタフェース番号
1.3.6.1.2.1.2.2.1.2 : ifDescr	インタフェース名
1.3.6.1.2.1.2.2.1.3 : ifType	メディアタイプ
1.3.6.1.2.1.2.2.1.10 : ifInOctets	入力側オクテット数
1.3.6.1.2.1.2.2.1.16 : ifOutOctets	出力側オクテット数
1.3.6.1.2.1.2.2.1.11 : ifInUcastPkts	入力ユニキャストパケット数
1.3.6.1.2.1.2.2.1.17 : ifOutUcastPkts	出力ユニキャストパケット数
1.3.6.1.2.1.2.2.1.13 : ifInDiscards	入力側破棄パケット数
1.3.6.1.2.1.2.2.1.19 : ifOutDiscards	出力側破棄パケット数
1.3.6.1.2.1.2.2.1.14 : ifInErrors	入力側エラー数
1.3.6.1.2.1.2.2.1.20 : IfOutErrors	出力側エラー数

9 Tips

最後に、ネットワーク管理に関する Tips をいくつか示しておきます。

- ツールの挙動を調べてから利用すること

  稼働中のネットワークでツールを稼働させる前に、実験用のネットワークで挙動を調べておきます。負荷の高い機器に対して、flood オプションを付けた ping や SNMP クエリーを送るだけで機器がダウンしてしまうことがあります。

- traceroute は不確かであると認識すること

  IP パケットの行きと帰りは同じ経路を通るとは限りません。traceroute では、行きの経路のみ表示されていることを認識しておく必要があります。

- 監視サーバの置き場所を考慮すること

  コアになる装置と同じセグメントに置くのが原則です。

- 監視結果の表示

  監視結果は外部に公開しないのが一般的だと思われます。結果を表示するための Web サーバでは、アクセス制限を行ったり、ポート番号を変更したりすることで外部からのアクセスを規制できます。また、Web サーバにてアクセス許可されているセグメント内のプロクシサーバは見落としがちですので、こちらでのアクセス制限には注意が必要です。

- 監視対象

  監視対象となるネットワーク機器が多くなってくると、ポーリングや統計処理にかかる時間がどんどん増えてきます。ポーリング間隔までに 1 回の計測が終わらないということもあり得ますので、適正な範囲に分割して監視を行う工夫が必要となります。

- SNMP のセキュリティ

  SNMP は便利であるだけに、セキュリティ上の問題となることもあります。SNMP ポートに対するスキャンもよく行われていることから、デフォルトのコミュニティを使用することは避けましょう。アクセス規制をかけられるクライアントでは、必ずアクセス規制を行い、アクセス規制ができないものは、プライベートアドレスを割り振ることで外部からのアクセスを規制するようにします。

- 高速インタフェース

  MIB の ifInOctets や ifOutOctets は 32 ビットの正数で定義されているために、高速なネットワークインタフェースでは、カウンタが一周してしまうことがあります。たとえば 110Mbps を超えるトラフィックがある場合には、5 分間でカウンタが一周してしまいますので、測定周期を調整することが必要となります。

- ifIndex の割り当て

  前述しましたが、インタフェースボードを増減・変更した場合には、インタフェースに割り当てられるifIndexの値が変化することがあります。インタフェースの構成を変更した場合には、監視ツールの設定も合わせて見直すようにしましょう。また、MRTG ではインタフェースに振られた IP アドレスをキーにデータ取得できます。この機能を有効利用しましょう。

- UCD-SNMP コマンド

  UCD-SNMP パッケージの最も基本的なコマンドは、次の 2 つです。まず、これらのコマンドの使い方をマスターしましょう。

  - snmpwalk

    機器からデータを収得します。

  - snmptranslate

    OID と MIB 名の対応を表示します。

10 参考文献一覧

10.1 雑誌

- UNIX MAGAZINE

  連載「Unix Communication Notes」山口　英 1998.3 ～
  「倉敷芸術科学大学のネットワーク構築」小林和真 1997.12

- OPEN DESIGN No.10

  「ネットワーク管理技術のすべて」

- Software Design 1999.9

  「フリーソフトウェアでネットワークをチェック～ trafshow, MRTG, ntop の導入」田村吉章

10.2 書籍

- "Snmp, Snmpv2, Snmpv3, and Rmon 1 and 2" -- William Stallings; 3rd edition （January 1999） Addison-Wesley Pub Co; ISBN: 0201485346
- "Practical Guide to SNMPv3 and Network Management, A" -- David Zeltserman, Dave Zeltserman; （May 4, 1999） Prentice Hall; ISBN: 0130214531
- 「SNMP バイブル - インターネット管理への実践ガイド -」William Stallings 著、大鐘久生、Addison-Wesley Publiching Company; ISBN-7952-9651-0

10.3 性能評価

- Communication Traffic Project

  http://www.mmlab.tnl.ntt.co.jp/

- Distributed Benchmark System

  http://shika.aist-nara.ac.jp/member/yukio-m/dbs/index-j.html

10.4 ネットワーク管理

http://wwwsnmp.cs.utwente.nl/Docs/software/pubdomain.html

http://netman.cit.buffalo.edu/index.html

http://www.nemoto.ecei.tohoku.ac.jp/~nitou/snmpdocs/tutorial1.html

10.5 ツール

- Angel Network Monitor

  http://ibm-2.MPA-Garching.MPG.DE/angel/

- Big Brother

  http://maclawran.ca/sean/bb-dnld/

- Expect

  http://expect.nist.gov/

- IPTraf

  http://cebu.mozcom.com/riker/iptraf/index.html

- MRTG

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

- mon

  http://www.kernel.org/software/mon

- NeTraMet

  http://www.auckland.ac.nz/net/Accounting/ntm.Release.note.html

- NetSaint

  http://www.netsaint.org/

- nocol

  http://www.netplex-tech.com/software/nocol

- ntop

  http://www-serra.unipi.it/~ntop/

- RRDTool

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

- Frontend - CRICKET

  http://www.munitions.com/~jra/cricket/

- Frontend - NRG

  http://ee-staff.ethz.ch/~oetiker/webtools/rrdtool/frontends/nrg.html

- Frontend - ORCA

  http://www.gps.caltech.edu/~blair/

- Frontend - Remstats

  http://silverlock.dgim.crc.ca/~terskine/remstats/

- SPONG

  http://www.edsgarage.com/projects/spong/

- Scotty

  http://wwwhome.cs.utwente.nl/~schoenw/scotty/

- SWATCH

  http://www.engr.ucsb.edu/~eta/swatch/

- statscout

  http://www.statscout.com

- Treno

  http://www.psc.edu/~pscnoc/treno.html

- Experimental TCP Implementations

  http://www.psc.edu/networking/tcp.html

- UCD-SNMP

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

10.6 参考 URL

- General network management portal

  http://netman.cit.buffalo.edu/index.html

- Another good network management portal

  http://compnetworking.miningco.com/msubmanage.htm?terms=network+management&cob=home&TMog=5006366091143m&Mint=56534342191358&FFV=1

- “ The Simple Times ”

  http://www.simple-times.org/pub/simpletimes/issues/

- SNMP FAQ

  http://www.cis.ohio-state.edu/hypertext/faq/usenet/snmp-faq/part1/faq.html

- Sample Cisco device security configs

  http://www.cisco.com/warp/public/700/tech_configs.html#SECURITY

- Cisco device SNMP configuration tips

  http://www.cisco.com/warp/public/490/index.shtml

10.7 組織

- IETF

  http://www.ietf.org/

- NANOG

  http://www.nanog.org/

- JANOG

  http://www.janog.gr.jp/

- CAIDA

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

  cflowd、RRD …etc

- LBNL's Network Research Group

  http://ee.lbl.gov/

  tcpdump、libpcap 、arpwatch、traceroute、pathchar

- Solaris Freeware Project

  http://sunsite.sut.ac.jp/sun/solbin/

- Fresh Meat - Linux Software Index

  http://www.freshmeat.net/