MRTG + RRDtool によるサーバ，ネットワークの監視

三重大学　総合情報処理センター
松原伸樹
matsubara@cc.mie-u.ac.jp

１．初めに

総合情報処理センターでは、日常的にネットワークトラフィックやセンター内のサーバの状況について監視しています。その際、mrtg＋RRDtool というツールを用いて、継続的に監視を行っており、障害などが発生した際に大いに役立っています。今回は、その業務の一部を紹介いたします。

２．mrtg とは

MRTG（Multi Router Traffic Grapher）とは、SNMP を使用し、各サーバ等よりデータを取得して、グラフ化するツールです。監視対象のデータは、2 年間分保存され、過去 1 日間、1 週間、1 月、1 年のグラフを生成することに使用します。

各サーバ、SW のデータをグラフ化することにより、トラブルが発生した際の原因特定がとても簡単になります。以下の図 1 は、mrtg で生成されたグラフの 1 つで、サーバの cpu 使用率を表示しているグラフなのですが、以下のように、金曜日が突出している瞬間があります。　この瞬間、トラブルが発生しており、学外⇔学外間の通信がとても遅くなっていましたが、可視化することで、CPU 使用率が急激に上昇していることがわかり、CPU 使用率を圧迫しているプロセスを探し出し、早急に原因特定することが出来ていました。

このように、サーバ、ネットワークを監視することで、トラブルを未然に防いだり、トラブルが発生してもできる限り早く解決することが総合情報処理センターにおける基本業務の一つになっています。

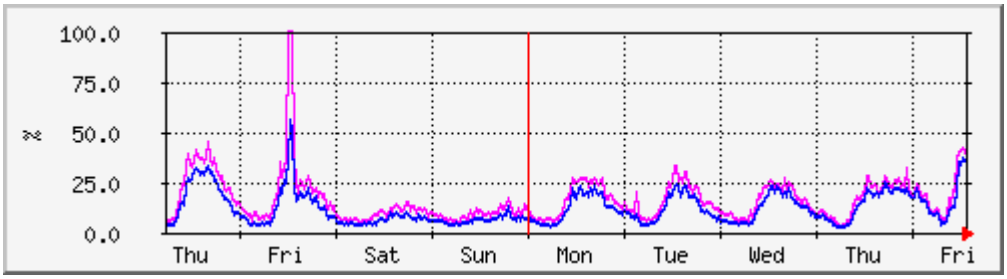

図 1. センターで監視しているサーバの Cpu 使用率

３．RRDtool とは

MRTG 標準の機能ですと、データの取得間隔が 5 分おきであり、もっと間隔を短く情報を取得しようと思っても、標準機能ではすることが出来ません。また、MRTG がグラフを生成する際にとても負荷がかかり、多くの台数を監視しようと思っても、負荷がかかりすぎて監視することが出来ません。

そこで利用されるようになったものが、RRDtool というツールです。RRDtool はデータを取得するたびに、グラフを自動生成するのではなく、一時的に RRD というデータベースにデータを保存させます。

この MRTG と、RRDtool を組み合わせることで、かなりの負荷が軽減することが可能になり、また、5 分おきにしか情報を取得できないという制限もなくなり、1 分おきや 2 分おきに情報を取得するよう変更することが出来ます。

図 2、図 3 はそれぞれ同じ性能を持った PC から、MRTG のみを使って監視した場合と、MRTG＋RRDtool を利用して監視をした場合の CPU の利用率です。MRTG のみを使った時と比べ、CPU の負荷が半分以下になっていることがわかります。少ない台数の監視の場合は、MRTG で十分ですが、多い台数の場合は、RRDtool と組み合わせる必要が生じてきます。

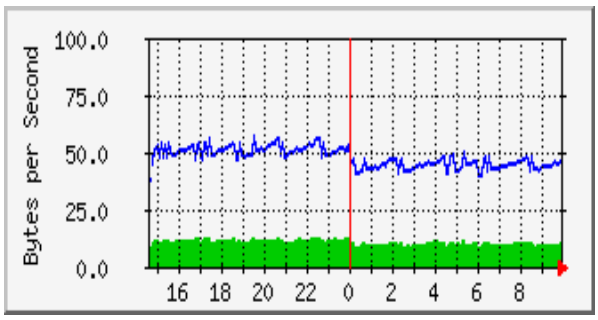

図 2 . MRTG のみで監視(5 分おき、計 375 台)

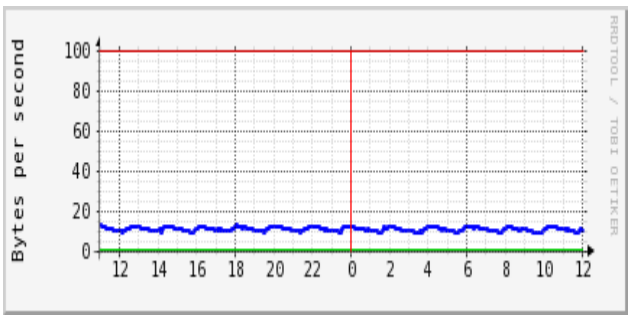

図 3. MRTG + rrdtool で監視(5 分おき、計 375 台)

４．総合情報処理センターのサーバ監視

上記 MRTG+RRDtool を用いて、総合情報処理センターで運用している各種サーバの監視を行っています。大学でサーバを運用するときに、通常のサーバ運用の場合と気を付けなければいけないことは、授業による一斉アクセスです。図 4. は Portal サーバ(moodle サーバ) 12/15 ～ 12/16 のトラフィック量の推移になります。 通常時はほとんど利用がない場合でも、授業で moodle を利用することになったときに、急激にトラフィック量が増大します。 通常のサーバの場合は、特殊なことがない限り、急激に利用量が増大するという事はあまりないのですが、大学のサーバの場合はこのようなことが日常的に生じます。　日頃 CPU 使用率やメモリの使用率が少ないからと、サーバの性能を低く見積もると、このような急激なアクセスの上昇に耐えられず、サーバダウンが生じます。

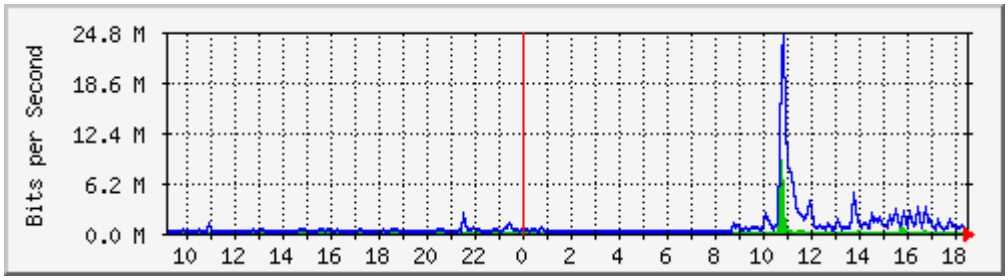

図 4. 12/15 ～ 12/16 Portal サーバ(moodle) のトラフィック量の推移

MRTG では、CPU , メモリ情報、トラフィック情報、ハードディスクの使用率などが監視できます。図 5. はセンターで管理しているサーバのハードディスクの監視状況です。普段からグラフを監視していてディスク容量が多くなってきているので、圧縮などをしたりして、以下のように推移しています。

一度一部のファイルを削除してディスクの空きが増えたと勘違いしたことも、監視をしていることにより、早めに気づくことが出来ました。

このように mrtg によりサーバ監視を行う事は、総情センターの日常業務の一つになっています。

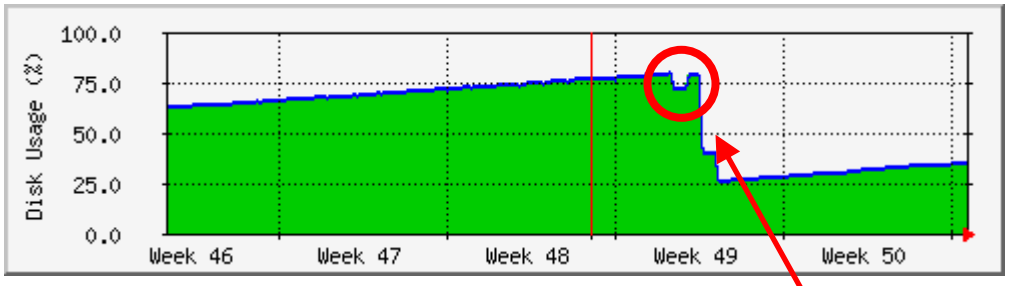

図 5. サーバのハードディスク容量の推移

ディスク容量が増えてきたのでファイルサイズが大きいファイルを削除してディスク容量を空けたのだが、間違えて自動生成されるタイプのファイルを削除していたため、翌日になって再度ファイルが自動生成されが走り、再度ディスク容量を圧迫される羽目に。

５．三重大学内のネットワーク監視

図 6. は学外⇔全学のトラフィック量の 1 日の推移です。こちらは学内制限ですが、総情センターのホームページからも閲覧が可能です。(http://www.cc.mie-u.ac.jp/cc/i/network/traffic.html) こちらは日頃から常に監視していて、学外との異常な量のトラフィックが流れた場合、攻撃を受けていないか、学内から不正な利用を行っていないかを調査しています。

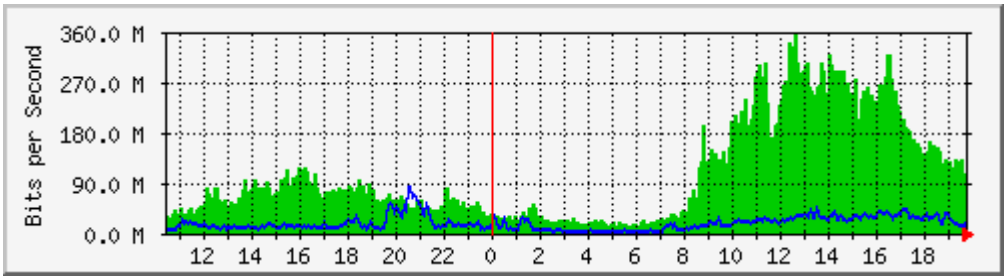

図 6. 全学のトラフィック量の 1 日の推移

図 7. はとある研究室の 1 週間のトラフィックの推移です。普段はほとんどトラフィックが流れていないのに、一時的に大量のトラフィックが流れていることがわかります。このような状況が確認された際に、どことデータをやり取りしているのか、不正な使用ではないかを適宜調査しています。

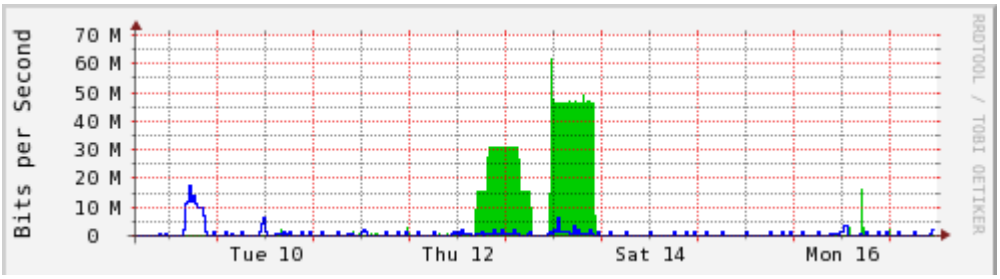

図 7. とある研究室の 1 週間のトラフィックの推移

６．MRTG の拡張

MRTG で取得できる値は、基本的には SNMP の値のみになりますが、スクリプトを組み込むことで、SNMP プロトコル以外からも取得が可能になります。

例えば、総情センターでは、学内にサイトライセンスにて、Matlab、AutoCAD、Solidworks、Mathmatica 等を提供していますが、これらのソフトは同時利用ライセンスに制限があり、同時利用制限を超えて利用しようとすると利用ができなくなります。

この値は、直接 SNMP で値を取得することはできませんが、スクリプトを使いデータを加工することで、データの取得を可能にしています。以下がそのスクリプトになります。

```
#!/bin/bash
global=`snmpwalk -v2c -c public IP アドレス 1.3.6.1.2.1.6.13.1.1 | grep -v "0\.0\.0\.0" | grep ポート番号 | wc -l`
echo $global
echo $global
echo
```

このスクリプトを、mrtg の設定ファイルに記述して、グラフを作成することで、現在のサイトライセンスソフトの利用者を、可視化することが出来るようになります。(図 8 参照)

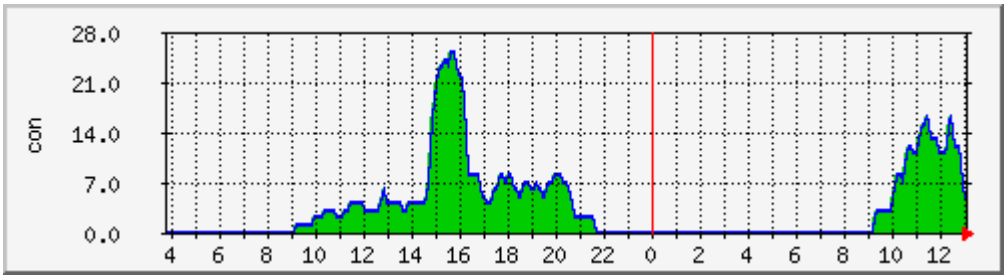

図 8. 12/17～12/18　AutoCAD の 利用者の推移

７．今後の課題

現状抱えている問題として、特定の人しか mrtg の作成及び修正をすることが出来ないという問題があります。本来でしたら、誰もが作成ができるようになることが望ましいのですが、いろいろと理由があり、できないでいるのが現状です。

また、大学内に設置している SW の数が 12/16 現在、274 個、アクセスポイントの数が、349 個、センター内のサーバの数が 50 台以上あります。機器更新のたびに、MRTG を作り直す必要があり、結構な仕事の負担となってきます。MRTG の作成の自動化をおこなえるようにするか、もしくは、どの機器のグラフ作成を行うか、厳密に選定する必要が出てきます。

監視項目が多すぎるために、グラフの作成自体は行えていても、人的要因でトラブルを見逃すという事も、どうしても発生してしまいます。MRTG には、メール通知機能もありますので、異常な値を検出した際には、グラフ化させるだけではなく、メール通知するなどの機能拡張の検討も必要になってくるかと思われます。

８．参考文献

1) http://www.mrtg.jp/doc/　mrtg ホームページ
2) http://www.mrtg.jp/doc/reference.html mrtg リファレンス
3) 横浜国立大学におけるネットワークトラフィック監視 学術情報処理研究 No.15 2011