ネットワークのトラフィックのトラブル発見及び警告通知

03H007 井上 忠昭

1　はじめに

学校や会社などでは多くのユーザーが使用する環境がある。その環境のなかで、規模によって要求されるシステムの質に違いはあるが、24 時間 365 日ノンストップで稼働することが理想である。しかし、絶対に止まらないシステムを作ることは不可能である。それに近い状態で稼働させるのが管理者の仕事である。そのためにはシステムを監視し、トラブルが発生しても、ユーザーがトラブルに気がつかないようにするのが理想である。

そこで、システム管理を手助けしてくれるのがシステム監視ツールである。一言でシステム監視ツールと言ってもいろいろなツールがあり、例えば、BigBrother や MRTG や NetSaint などがある。

本研究室では MRTG を使用してネットワークを監視しており、過去のトラフィックデータがあるので、これを利用して本研究を行う。MRTG は SNMP を使用して、ネットワークの稼働状況を監視し、ネットワーク機器の利用状況を、InPut/OutPut パケットでグラフ化ができ、Web データとして作成できる。

しかし、グラフ化できるだけでは、トラブルが発生したときに管理者がグラフを見続けていないといけませんし、見続けていないとグラフの異常な変化に気がつかない。それでは管理者の負担が大きいので、軽減できないかと考えた。

その方法としてトラフィックデータを監視し、異常を知らせるメール送るをプログラム作成作成しようと考えた。システム内容は、普段の研究室におけるルータを流れるトラフィックのデータの統計をとり、その結果を基本として、ルータのトラフィックデータを比較する。

そのなかで、差が大きすぎたり、急激なトラフィックの増大、増減などは障害が発生する前兆の可能性があるので、警告を表示するシステムを作成しようと考えた。

しかし、平日と土曜、日曜、祝日によって利用率が違うので平日と休みの日のそれぞれの統計をとる。祝日で日が決まってる日は日にちで設定し、成人の日など、曜日で決まってる祝日は、○ 月第○ 月曜日で設定を行う。設定の変更が簡単なテーブルを利用する。

2　目的

ネットワーク機器の利用状況を監視したものを MRTG でグラフ化できる。

しかし、トラブルを発見するには管理者がグラフの変化を見ていないといけない。そこでグラフの異常な変化が起きたとき、警告をメールで送信することで、グラフを見なくても発見でき、グラフを監視する負担を減らせると考えた。

3　まとめ・結果

実装し、cron コマンドを利用し、毎分 5 分ごとに監視し、異常は発見するとメールを送るプログラムを動かすことができた。

ハッピーマンデーや振替休日など、祝日判定行ない、祝日・日・土・平日で別けることができた。春分・秋分の日は計算で判定するとずれが発生する可能性があるのでテーブルを利用した。

今後の課題

- log の数値だけでは判定が難しいので、判定方法を考え直す必要がある
- 処理が遅いため、 現在より早く動くプログラムを作成する必要がある
- 負荷が大きいので、負荷が少ないシステムにする必要がある