MRTG を利用したネットワーク機器の障害検知

03H017 大西由之

1　はじめに

ネットワークシステムを快適に利用するには、システムが正常に動いていなければならない。しかし、障害が発生しないシステムを作ることは不可能である。障害が発生した場合、すぐに修復しなければ、システムの利用者に多大な被害を与えかねない。そういった状況を回避するには、障害の早期発見と、修復が重要である。そこで、システムが正常に動いているかどうかを常に監視しなければならない。しかし、人間がシステムを常時監視するのは困難である。そこで定期的にネットワークを監視するシステムが必要である。それがネットワーク監視ツールである。ネットワーク監視ツールは、様々な種類があるが、今回の研究では、研究室内でも使われている MRTG(Multi Router Traffic Grapher) というネットワーク監視ツールを利用する。

2　本システムの構成

- 日常のログデータの取得
  今回の研究に必要なネットワークのトラフィックデータのログは、h-ps011 サーバ内の MRTG のログディレクトリ内にある。このデータから最新のデータを取り出す。
- 基準となるログファイルの作成
  平日、土日祝日によってマシンの利用率が異なるため、平日、土曜、日曜祝日毎に基準値を設定し、基準値を書いたファイルを作成する。
- 比較する基準値ログファイルの選択
  現在の時刻 (JST) を取得し、曜日の判定を行う。また、祝日の判定は、あらかじめ作成しておいた祝日テーブルを読み込み、現在の日付が、祝日テーブル内にあるかを確認し、もし一致した場合は祝日と判定する。今回の研究では、日曜日と祝日は同様のファイルを使用する。
  そして、平日・土曜・日曜祝日別にファイルを選択する。
- ログファイルの比較と障害発生の判定
  選択された基準値のデータファイルと、日常のログファイルのデータを比較する。比較した結果、基準値よりも日常のログデータが大きい場合は、障害が発生したという判定をする。
- 警告メイルの送信
  障害発生の判定が出た場合、管理者へ警告メイルを送信するプログラムを作成した。
- ウェブインターフェース
  障害発生の有無を表示させるウェブインターフェースを作成した。正常に稼働している場合は緑色で表示し、障害発生の判定が出た場合は赤色で表示させた。

3　まとめ

今回の研究により、障害発生時に管理者に警告メイルの送信をすることで、いち早く障害の発生を知ることができるようになる。

また、Web ブラウザにネットワークの状態を表示することにより、ネットワークの障害を Web ブラウザから知ることが可能になり、グラフの変化を見る余裕が無いときでも Web ページを見るだけで容易にネットワークの状態を知ることが可能になる。

以上のことから、ネットワークの障害をより早く知ることができ、ネットワークを快適に利用することができる。