横浜国立大学におけるネットワークトラフィック監視

Network Traffic Monitoring in Yokohama National University

志村　俊也
Toshiya Shimura

tshimura@ynu.ac.jp

横浜国立大学　情報基盤センター

Information Technology Service Center, Yokohama National University

概要

ネットワークトラフィック監視はネットワーク運用管理の基本業務の 1 つである。本学では、MRTG と RRDtool を利用し、学内各所のネットワークトラフィックを常時監視している。監視は 5 分平均の大局的なトラフィックを MRTG で行い、5 秒平均の瞬間(短時間平均)トラフィックを RRDtool で行っている。本稿では、学内の代表的な 3 つの監視ポイントにおける、5 分平均と 5 秒平均それぞれで得られたトラフィックの特徴について報告する。

キーワード

ネットワークトラフィック監視, MRTG, RRDtool

1. はじめに

学内ネットワークのトラフィック監視はネットワーク運用管理の基本業務の 1 つである。ネットワークトラフィックの振舞いを常時把握することにより、ネットワーク異常・障害・不正利用・不正通信の検知、及びその発生箇所・原因特定を速やかに行うことができる。このため、本学では、学内各箇所のネットワークトラフィックを常時監視している。監視ポイント総数は 1141 箇所であり、学内各建物のネットワークトラフィックに関しては各フロアまでの送受信トラフィックを、サービスサーバ群に関しては、各サーバの送受信トラフィックを監視している。

トラフィック監視に利用しているのは、フリーソフトウェアの Multi Router Traffic Grapher (MRTG) と Round Robin Database Tool (RRDtool) である。 MRTG は、5 分平均のトラフィックを 1 ピクセルとして過去 400 ピクセル分(33 時間 20 分) のトラフィックを 1 つのグラフとして可視化するソフトであり、学内各所のネットワークトラフィックの約 1 日分の振舞いを一目で把握することができる。このため、ネットワーク異常・障害・不正利用・不正通信の検知、及びその発生箇所・原因特定を行う上で、この MRTG で得られた 5 分平均のグラフが非常に役に立つ。

RRDtool も MRTG 同様にトラフィックの時間的な推移を 1 つのグラフとして可視化するソフトである。RRDtool には MRTG が持つグラフ自動作成機能は搭載されていないので、利用者側でグラフ作成スクリプトを作成しなくてはならないが、取得するトラフィックの平均時間を 1 秒まで下げることができるという利点がある。

このため、MRTG では得ることができない瞬間（短時間平均）トラフィックを把握することが可能であり、MRTG 同様にトラフィック監視の強力なツールとなっている。

実際のトラフィック監視においては、1141 箇所全てに対して MRTG(5 分平均)による監視を行い、かつ、その中でも瞬間トラフィックを把握する必要がある最重要監視ポイント(SINET との接続点やコアスイッチ内の各ポート等)に対しては、MRTG に加えて RRDtool による瞬間トラフィックの監視も行なうという方法をとっている。RRDtool で監視するトラフィックの平均時間については、短く取り過ぎるとネットワーク機器が受ける SNMP アクセス負荷が大きくなり、またグラフ全体の表示時間が短くなってしまう。このため、本学では 5 秒平均の値を 1 ピクセルとして、過去 800 ピクセル分(約 1 時間) のトラフィックを 1 つのグラフとして表示するように設定している。

本稿では、最重要監視ポイントの内、代表的な 3 箇所を例に挙げて、MRTG (5 分平均)と RRDtool (5 秒平均)それぞれで監視したトラフィックの特徴について報告する。

2. トラフィック

本稿で紹介するトラフィック監視ポイントのネットワーク上の配置を図-1 に示す。

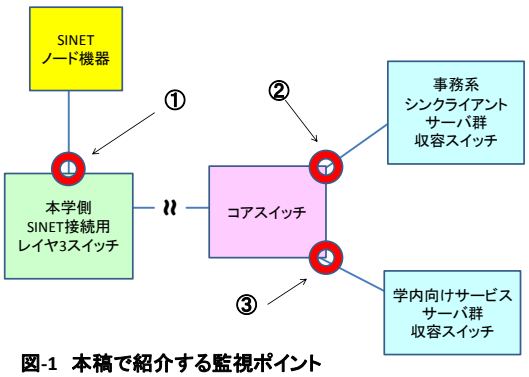

図-1 本稿で紹介する監視ポイント

図-1 中の◎で示した箇所、具体的には、

① SINET ノード機器←→本学側 SINET 接続用レイヤ 3 スイッチ
② コアスイッチ←→ 事務系シンクライアントサーバ群収容スイッチ
③ コアスイッチ←→ 学内向けサービスサーバ群収容スイッチ

の 3 箇所のトラフィックの特徴を以降の章で説明する。

なお、以降で出てくる図-2～図-4 において、MRTG のグラフの時間推移方向は、『右→ 左』であり、RRDtool のグラフの時間推移方向は、『左→右』であることを注記しておく。(MRTG と RRDtool では時間の推移方向が逆になっていることに注意して頂きたい。)

2.1. SINET ノード機器←→本学側 SINET 接続用レイヤ 3 スイッチ 間のトラフィック

本学は SINET ノード校であり、SINET 側の設備が本学情報基盤センター内に設置されている。そのため、SINET ノード機器に対して、民間のキャリア回線を使用せずに直接 1000BASE-T で接続することが可能となっている。図-2 は、『SINET ノード機器 ←→本学側 SINET 接続用レイヤ 3 スイッチ』間のトラフィックである。上が 5 分平均(MRTG) 、下が 5 秒平均(RRDtool) のトラフィックを示している。5 分平均のトラフィックは 2011 年 7 月 19 日 23 時 ～7 月 21 日午前 9 時のものである。5 秒平均によるトラフィックは、 上記の時間帯の 7 月 20 日 15 時 10 分 ～ 16 時 10 分の間の詳細トラフィックを示している。 グラフより、学内への受信トラフィックが学外への送信トラフィックよりも圧倒的に多いのがわかる。これは、通信の大部分が ウェブアクセスによる学外から学内へのデータ・コンテンツのダウンロードであることを示している。学内への受信トラフィック量は、午前 6 時前後が最少であり、その後、時間とともに増加していき、12～17 時にかけて最大となり、その後次第に減少するという振る舞いとなっている。教職員・学生が学内で行う各種業務（教育・研究・事務）とほぼ同じリズムでトラフィックが増減しているのがわかる。 MRTG(5 分平均)による監視では、トラフィックの最大値は 28MB/s (224Mbps)程度であるが 、RRDtool (5 秒平均)による監視では、それを上回る 40～50MB/s (320～400Mbps)が計測されており、SINET との接続帯域(1Gbps) が有効に活用されていることが RRDtool によって明確に示されている。

2.2. コアスイッチ ←→ 事務系シンクライアントサーバ群収容スイッチ 間のトラフィック

本学の事務系職員用 PC の大部分は、ネットブート型シンクライアント PC である。シンクライアント PC の総数は 400 台であり、 事務局庁舎、学務部庁舎、各部局の事務棟など学内各所に配置されている。ネットワーク的には、24bit のグローバルサブネット 3 個を使用し、ブートサーバと PC を同一サブネットに収容し、ブートサーバ←→PC 間通信はルーティングせずに行なえる構成

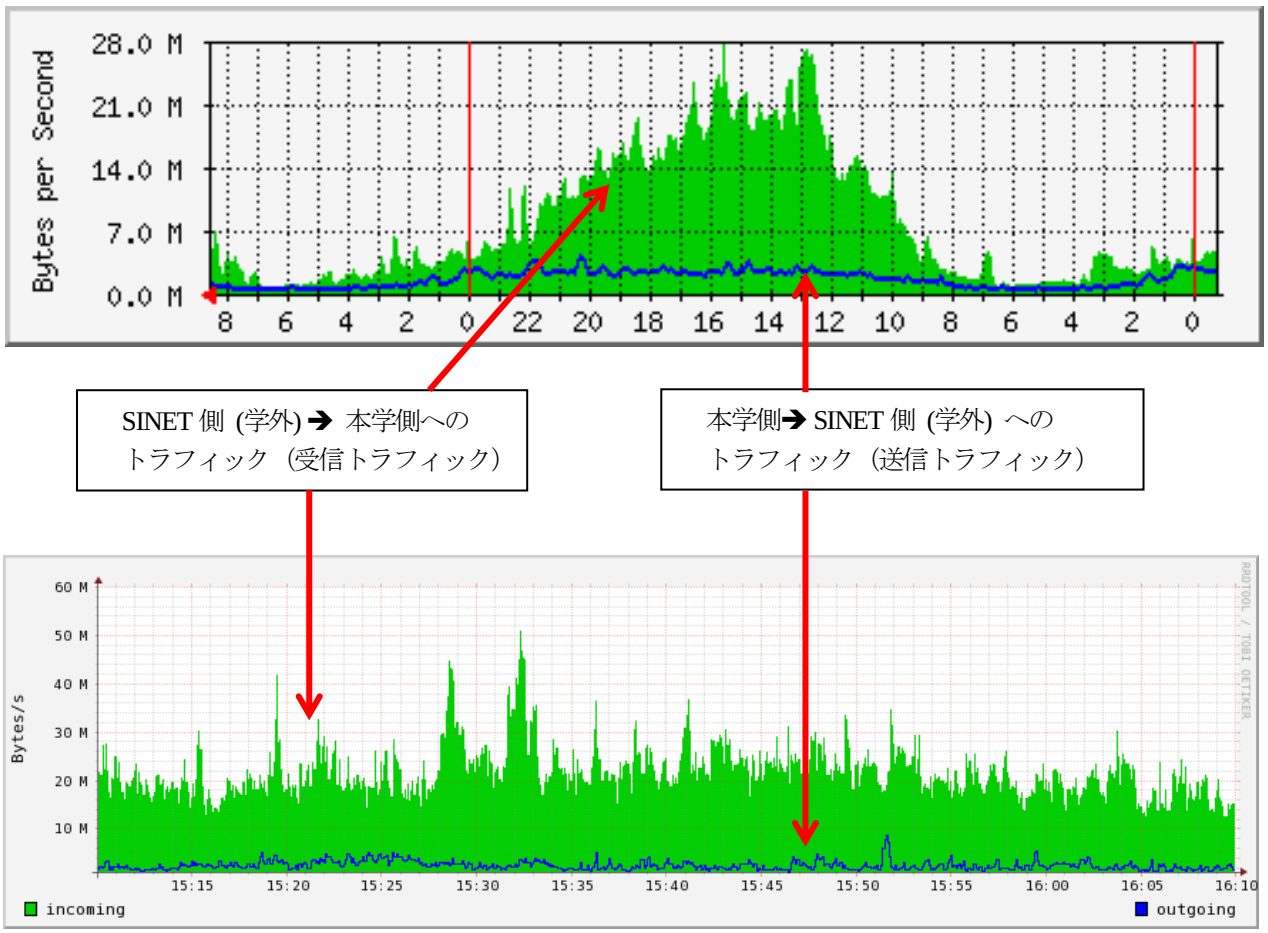

図-2　『SINET ノード機器 ←➔本学側 SINET 接続用レイヤ 3 スイッチ』間のトラフィック。
上図が 5 分平均 (MRTG) 、下図が 5 秒平均 (RRDtool) のトラフィックを示す。

としている。PC400 台の内 239 台は、毎起動時にブートサーバから OS のイメージ配信を受ける標準型ネットブートであるが、残り 161 台は、初回のイメージ配信を受けた後、利用したイメージを PC 側の内蔵 HDD にキャッシュし、2 回目以降の起動は差分イメージだけが配信される ReadCache 型ネットブートである。ブートサーバ群は、標準型 6 台と ReadCache 型 4 台で構成されている。

図-3 は標準型ネットブートのサーバ群 6 台が収容されている『シンクライアントサーバ群収容スイッチ←➔コアスイッチ』間のトラフィックを示す。上が 5 分平均 (MRTG)、下が 5 秒平均 (RRDtool) のグラフである。5 分平均のトラフィックは、2011 年 7 月 13 日 午前 6 時 ～ 7 月 14 日 15 時 のものである。5 秒平均のトラフィックは、上記の時間帯の 7 月 14 日 午前 8 時 05 分～9 時 05 分の詳細トラフィックを示している。5 分平均のグラフからわかるように、事務系職員が出勤する午前 8 時 30 分前後に『収容スイッチ➔ コアスイッチ』に対して非常に多くのトラフィックが出ている。これは、出勤した事務系職員が、自身の利用する PC を次々と起動し、ブートサーバ群から集中的に OS イメージの配信が行われるためである（配信されるイメージは PC1 台あたり約 50MB）。ブートサーバ群からのトラフィックの最大値は、MRTG の 5 分平均では約 56MB/s (448Mbps) 程度であるが、RRDtool による 5 秒平均値では、約 110MB/s (880Mbps) まで達しており、帯域上限値である 1Gbps 近くまで利用されていることがわかる。なお『コアスイッチ➔収容スイッチ』方向のトラフィックは『収容スイッチ➔ コアスイッチ』のトラフィックに比べて非常に小さいため、グラフ上には表れていない。

2.3. コアスイッチ ← ➔ 学内向けサービスサーバ群収容スイッチ間のトラフィック

学内向けサービスサーバ群収容スイッチ配下には、全学教職員・学生(約 13,000 人)を対象とした各種サービス提供サーバ群が接続されている。具体的には、DNS サーバ 4 台、認証サーバ(Active Directory, LDAP, Radius) 4 台 、

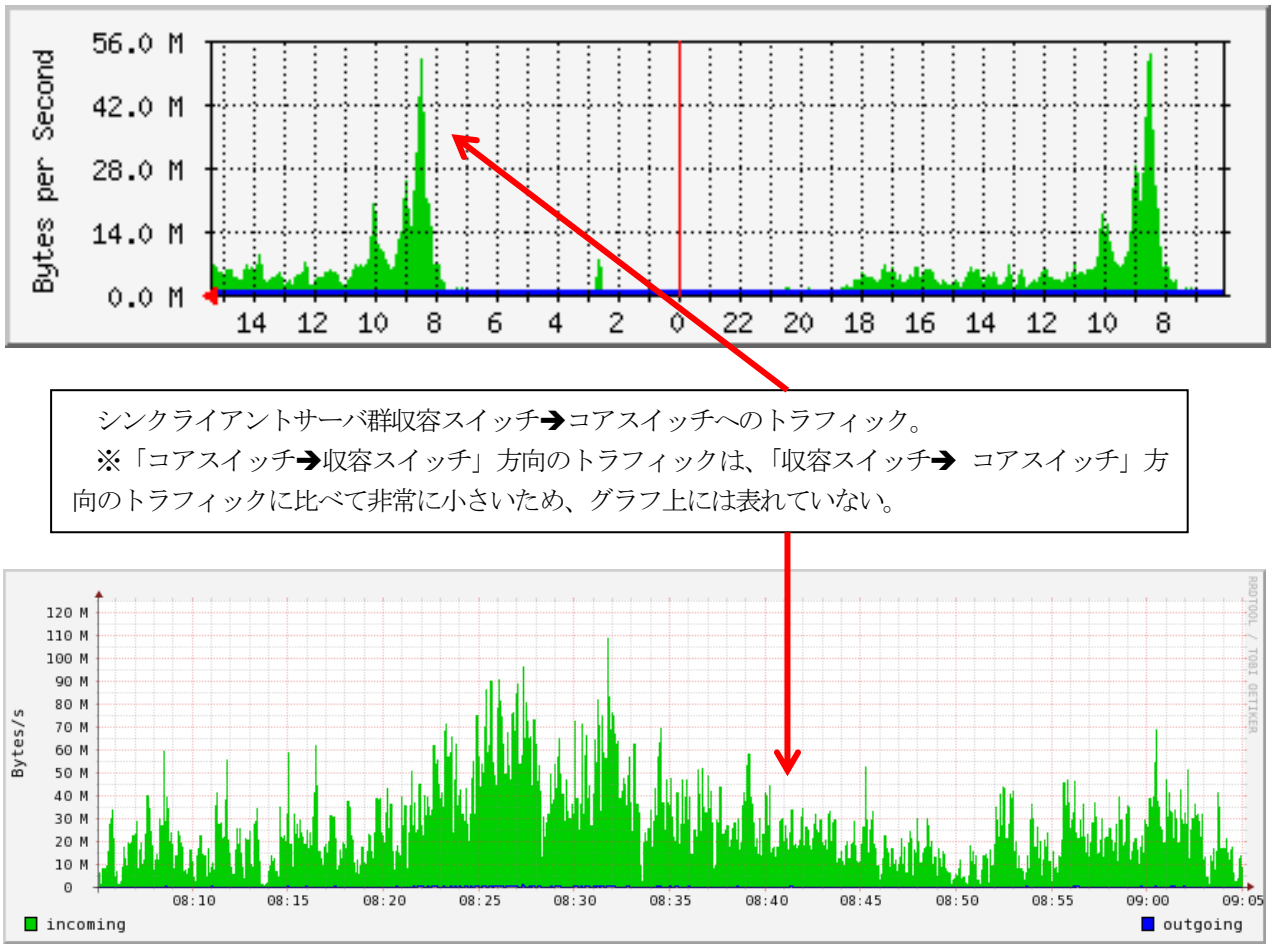

図-3　『シンクライアントサーバ群収容スイッチ➔➔ コアスイッチ』間のトラフィック。上図が 5 分平均(MRTG) 、下図が 5 秒平均 (RRDtool) のトラフィックを示す。

メールサーバ 1 台、メール中継サーバ(学外から配信されてくるメールを一旦受信し、メールサーバに受け渡すサーバ)1 台、ウェブメールサーバ 1 台 、メーリングリストサーバ 1 台である。

図-4 に示すのは、『コアスイッチ➔➔ 同サーバ群収容スイッチ』間のトラフィックである。上が 5 分平均(MRTG)、下が 5 秒平均(RRDtool)のグラフである。MRTG のトラフィックは、2011 年 7 月 25 日午前 4 時 30 分～7 月 26 日 13 時 50 分の間のトラフィックである。RRDtool によるトラフィックは、上記の時間帯の 7 月 26 日午後 12 時 45 分～13 時 45 分の間の詳細トラフィックを示している。MRTG(5 分平均)で計測した『サーバ群収容スイッチ➔ コアスイッチ』のトラフィックの振舞いとしては、午前 2 時～6 時の間は量的には非常に少なく、午前 6 時以降から徐々に増加し、業務時間帯である午前 9 時～18 時の間は、平均して 500 kB/s (4Mbps) 前後のほぼフラットな形状となり、その後徐々減少するという特徴を示している。一方、RRDtool (5 秒平均)で計測した業務時間帯のトラフィックでは、1～2MB/s (8～16Mbps) 程度のショット状のトラフィックが多数計測されており、MRTG(5 分平均)によって表示されているフラット形状とは様相が異なっていることがわかる。

MRTG(5 分平均)で計測した『サーバ群収容スイッチ➔ コアスイッチ』方向のトラフィックの内訳は、DNS サーバの寄与が 4 台で 30kB/s 程度、 メーリングリストサーバの寄与が 10kB/s 程度であり、残りの大部分がメールサーバとウェブメールサーバによるものである。認証サーバ 4 台の寄与は無視できるほど小さい。メール中継サーバは、メールサーバに対する学外からの SMTP 接続のゲートウェイサーバとして機能するため、『サーバ群収容スイッチ➔コアスイッチ』へのトラフィックには寄与しない。

『コアスイッチ➔サーバ群収容スイッチ』の業務時間時間帯のトラフィックが概ね 300kB/s 程度であるのに対して、『サーバ群収容スイッチ➔ コアスイッチ』のトラフィックが 500kB/s 程度となっているのは、『コアスイッチ➔ サーバ群収容スイッチ』の通信が、「学内 PC からメールサーバへの SMTP 接続」と「ウェブメールサーバ

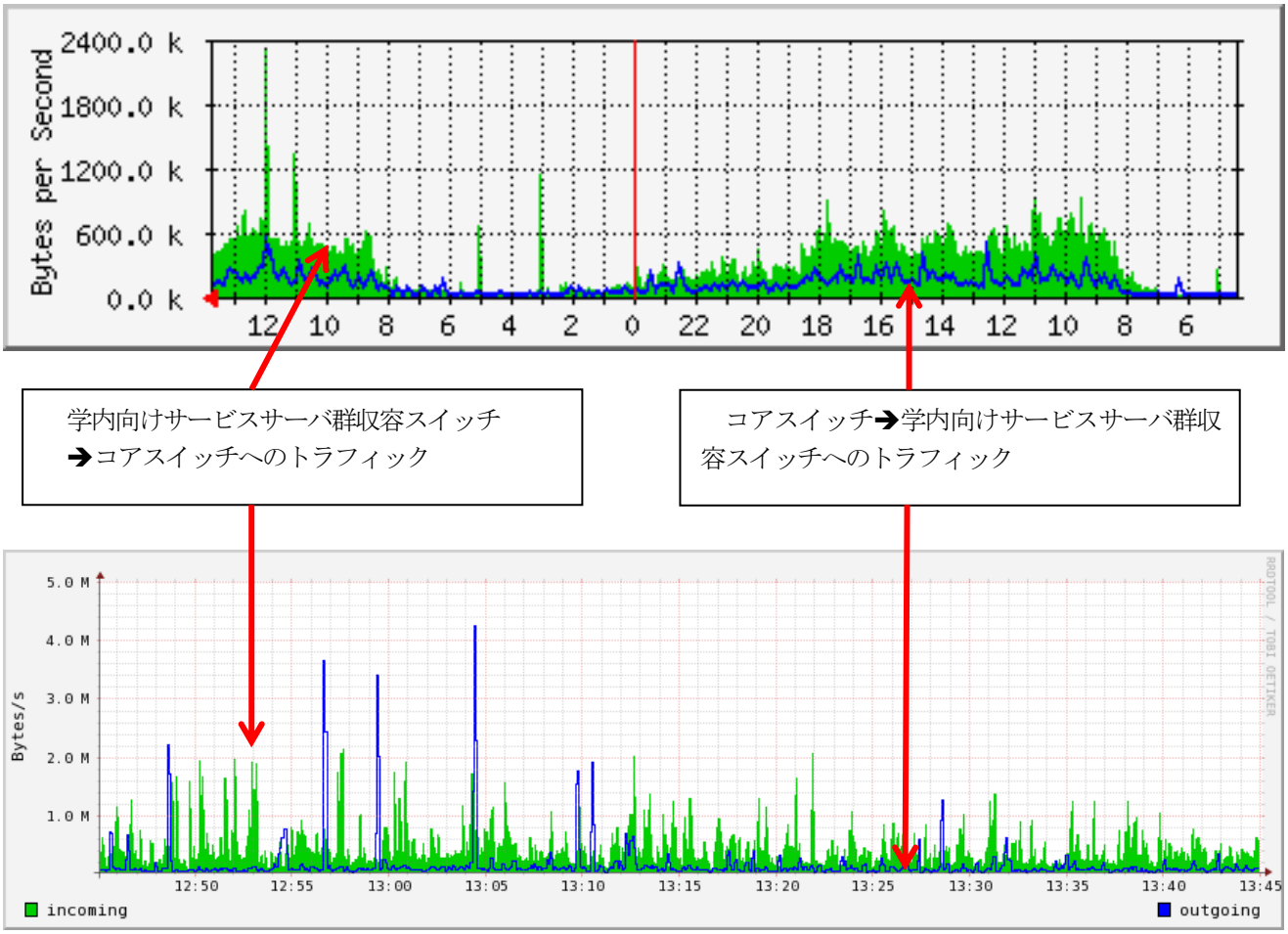

図-4 『学内向けサービスサーバ群収容スイッチ←→コアスイッチ』間のトラフィック。上図が 5 分平均 (MRTG) 、下図が 5 秒平均 (RRDtool) のトラフィックを示す。

に対する HTTPS 経由でのメール送信」によるものが主であるのに対して、『サーバ群収容スイッチ ➔ コアスイッチ』の通信は、学内 PC のウェブメールサーバに対するウェブアクセスによって発生するウェブコンテンツ（ウェブメールサーバへのログイン画面、ログイン後の受信メール一覧画面等）のダウンロードが主であることに起因する。本学では、事務系職員の場合、メールの送受信はウェブメールを利用する決まりとなっている。学生・教員の場合は、そのような制限はないが、それでも、多くの利用者がウェブメールを利用している。このため、業務時間帯のウェブメールサーバへのアクセスは大変多く、ウェブメールサーバからウェブコンテンツが頻繁にダウンロードされる。その結果として、5 分平均の MRTG のグラフにおいて、常時 500kB/s 程度のトラフィックが計測されているのである。

3. 終わりに

本稿では、本学のネットワークトラフィック監視の現状について代表的な監視ポイント 3 箇所を例に挙げて紹介した。MRTG と RRDtool の双方を利用することで、大局的(5 分平均)及び瞬間(5 秒平均)トラフィックをリアルタイムに把握できるようにしているため、学内ネットワーク管理上、非常に役に立っている。

なお、本稿では説明を省略したが、本学のネットワーク監視において、測定可能な機器に対しては、トラフィックだけでなく、CPU 使用率、メモリー使用量、接続セッション数も MRTG で監視している。また別のソフトウェアを利用して、全機器に対する死活監視も行っている。ネットワーク異常・障害の検知の際には、トラフィックだけでなく、これらの情報を総合して、発生箇所・原因の特定を行っている。本学の取り組みが他大学の参考になれば幸いである。