sFlow を利用したネットワーク監視の試み

Trial of network surveillance using sFlow

白清　学，谷内田　昌寿
Manabu Hakusei, Masatoshi Yachida

hakusei@vos.nagaokaut.ac.jp, yachida@ipc.nagaokaut.ac.jp

長岡技術科学大学 情報処理センター
Information Processing Center Nagaokauniversity of Technology

〒940-2188 新潟県長岡市上富岡町 1603-1
Kamitomioka1603-1, Nagaoka, Niigata , 940-2188　JAPAN

概要

長岡技術科学大学のキャンパスネットワークでは，これまで MRTG を用いて全学のトラフィックの動向の確認を行ってきた．ネットワーク全体のトラフィックに影響を与えるような大量データの通信については，MRTG グラフのような全体の統計情報を見ることでその有無について確認することは可能であるが，利用者や利用アプリケーションの特定には MRTG 以外の情報による詳細の把握が必要であり，調査のための時間を必要とする．このようなネットワークの利用動向をモニタリングする手法として，フロー情報を用いたネットワーク監視の手法が着目されている．これらの手法の 1 つである sFlow に対応したネットワーク機器を導入し，サンプリングされたパケットのフロー情報に基づく監視手法について試行を行った．2 台の sFlow エージェントによる出力を 1 台のコレクタで収集するシステムを構築しており，フロー情報を統計処理した後に，電子メールで通知する形態を採用している．

キーワード：学内 LAN，ネットワーク監視，sFlow，パケットサンプリング

1.はじめに

長岡技術科学大学は構成員約 2700 人の工科系単科大学であり，情報処理センター(以下，センター)を中心としてツリー状のネットワークを設置してコンピュータネットワーク利用している．本学の構成員が過不足なくネットワークを利用できるよう，Cisco 社製 Catalyst6506 の Layer3 スイッチをセンターに設置してルーティングを行い，この中央に設置されたスイッチの配下に 36 台の Layer2 スイッチを分散接続することによって基幹ネットワークを構成している．現在は，約 5500 台の IP アドレスが発行されており, これらの機器が約 50 のセグメントに分かれて接続され，キャンパスネットワークを利用している. ネットワークの監視には MRTG を使用しており,

学外接続されたセグメントにおけるネットワーク全体の受信パケットおよび送信パケットを，図 1 に示すようなグラフ化した情報を用いて視覚的に把握をすることで，キャンパスネットワーク全体の利用動向の確認を行ってきた.

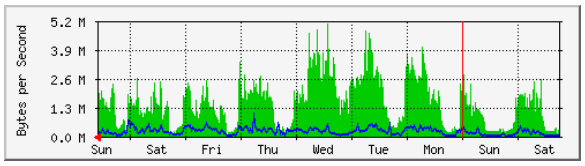

図 1 MRTG による本学のトラフィック

近年はコンピュータネットワークが普及し，一般家庭においても広く利用される状況となったことから，構成員のネットワーク利用の認識に変化が生じており，学内 LAN の環境下において，本学のネットワーク利用のガイドラインに抵触する目的外利用の通信が散見される状況となっている．これらの通信のうち，ネットワーク帯域を広く使用する通信では MRTG グラフを確認することでその問題利用の発生が視認できることから，使用者への注意喚起を行うことは可能である．しかしながら，MRTG グラフのみではその通信機器やアプリケーションを特定することはできないため，調査のために時間を費やす必要がある．一方，ネットワーク監視の手法ではフロー情報に着目したモニタリング手法が用いられるようになっている．フローベースの監視技術としては，NetFlow および sFlow[1]，さらに標準化の進められている IPFIX などの技術がある．この中で sFlow はサンプリングしたデータを扱い，かつデータのヘッダーサンプルを解析する手法であることから，エージェントにおける負荷が高くないといった利点を考慮し，sFlow に対応した情報収集を目的とするスイッチを導入するものとし，フローベースの監視技術を用いることで，従来とは異なる詳細な情報を元にネットワークを監視できるよう試行を実施することとした.

2.sFlow 対応機器の導入

2.1　システム構成

sFlow は複数のベンダーのネットワーク機器に実装される状況となっているが，仕様を規定している RFC3176[2] の公開と同時に実装を行っている FOUNDRY 製のスイッチを対象とし，対応する機器の中から FastIron LS624 を 2 台導入することとした．コレクタは sFlow を提唱した InMON 社が独自に提供している sflowtool[3]を用い，簡易にデータの取得および蓄積を行うこととした．コレクタのサーバ構成を表 1 に示す.

表 1　コレクタのサーバ構成

機種	EPSON 製 AT970
OS	FreeBSD6.3-Release
CPU	Celeron 1.6GHz
memory	1GB
HDD	160GB
collector software	sflowtool-3.12
受信ポート	6343/UDP

既設の基幹ネットワークの中央部分に接続しているサーバ 2 台に対してそれぞれ sFlow エージェントを挿入し，sFlow を用いたサンプリング収集の試行対象とした．これらのサーバは学内のパソコンに向けて，アンチウィルスソフトの定義ファイルを配布する役割を担っており，学内機器との通信が主体となるものの一定量の通信が高い頻度で発生することから試行の対象とした．コレクタは収集の影響を受けることの無いよう上流スイッチに直接接続し，エージェントからの出力パケットを速やかに取得できる構成とした(図 2)．学内 LAN を利用するユーザの PC とサーバ間の通信を sFlow エージェントによってサンプリングし，1 行ごとに出力される csv 形式のデータをコレクタで受信するものとしている.

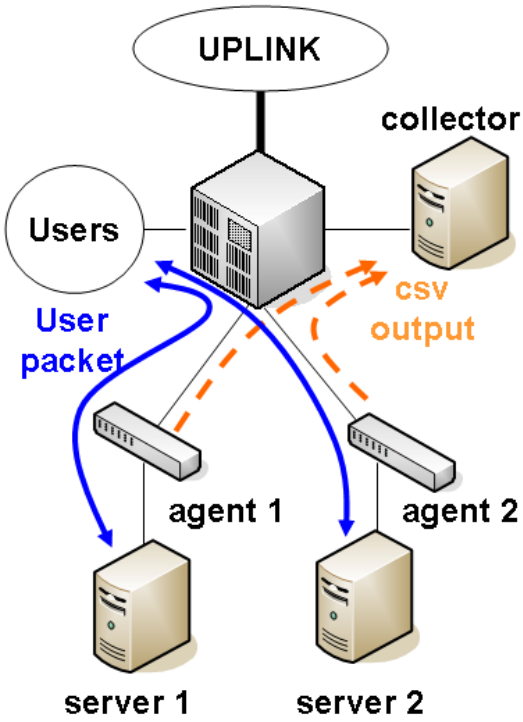

図 2 システム構成

2.2 コレクタの設定

コレクタの OS として用いた FreeBSD では sflowtool がパッケージとして用意されており，こちらをそのまま追加する形で/usr/local/bin 配下へ導入している．また，sFlow 対応のネットワーク機器は通信ポートとして UDP の 6343 番が設定されているのでデフォルト値を用いることとした．sflowtool の起動オプションでは，csv 形式，tcpdump 形式，NetFlow 形式の 3 種類に出力形式に対応しているが，文字列処理により容易に統計処理を行うことが可能な csv 形式での出力を得るため -l オプションを指定することとし，サーバ上で下記により実行している．

```
% /usr/local/bin/sflowtool -l > logfilename
```

サーバでコマンドを実行してる間，コレクタとしてエージェントからの情報を取得することが可能であり，テキスト情報として受信したデータを指定したログファイルへ格納するものとしている．

2.3 sFlow エージェントの設定

sFlow エージェントとして導入した FastIron LS624 では，ターミナルへログインした後，sflow コマンドによって sFlow に関する設定を行うことができる．図 3 にエージェントの設定例を示す．

```
telnet@FLS624 Switch#show sflow
sFlow services are enabled.
sFlow agent IP address: 133.44.XX.46
Collector IP 133.44.XX.XX, UDP 6343
Polling interval is 20 seconds.
Configured default sampling rate: 1 per 8 packets.
Actual default sampling rate: 1 per 8 packets.
626209 UDP packets exported
2158329 sFlow samples collected.
sFlow ports: ethe 0/1/9 to 0/1/10 ethe 0/1/24
Module Sampling Rates
---------------------
Port Sampling Rates
---------------------
Port=0/1/9, configured rate=8, actual rate=8
Port=0/1/10, configured rate=8, actual rate=8
Port=0/1/24, configured rate=8, actual rate=8
```

図 3　sFlow エージェント(Fast Iron LS624)の設定例

エージェントおよびコレクタの IP アドレスの設定のほか，デフォルトのサンプリングレートを設定することができる．試行のネットワーク環境では利用目的が限定された通信であることから収集が充分可能であると考え，最小値である 8(1/8 の割合でパケットを取得)を設定をしている．また，ネットワークスイッチのポートごとにサンプリングの設定を行う必要があり，スイッチの 9,10,24 の 3 箇所の接続ポートに対して最小値の 8 のサンプリングレートにて情報を収集するよう指示をしている．これらの設定によりコレクタへデータを転送することが可能となる．

2.4 sFlow エージェントの出力情報

sFlowで出力されるcsv形式の出力項目を表2に示す．エージェントではサンプリング毎に 1 行で構成した情報を出力してしているが，時刻に関する情報が含まれていないため，コレクタ側で別途考慮する必要がある．試行では，データを格納するファイル名を日時を含むものとし，おおよその時刻を把握する形としている．

表 2　sFlow エージェントの出力項目

データの種別	FLOW または CNTR
agent IP	エージェントの IP アドレス
input Port	スイッチの入力ポート
output Port	スイッチの出力ポート
in vlan	入力 VLAN
out vlan	出力 VLAN
source MAC	発信元 MAC アドレス
destination MAC	宛先 MAC アドレス
ethernet type	イーサネットタイプ
source IP	発信元 IP アドレス
destination IP	宛先 IP アドレス
IP Protocol	IP プロトコル番号
udp source port OR tcp source port OR icmp type	UDP/TCP 発信元ポート番号 または icmp タイプ
udp destination port OR tcp destination port OR icmp code	UDP/TCP 宛先ポート番号 または icmp タイプ
tcp flags	tcp フラグ
packet size	パケットサイズ
IP size	IP サイズ
sampling rate	パケット取得の割合

図 4 にエージェントからの出力例を示す．下線で示す 2 カラム目にエージェントの IP アドレスが記載されており，どちらのエージェントからの出力であるか判別が可能である．多数の項目により通信状況を把握することが

可能であるが，特に囲み線で示す発信元の IP アドレス，宛先の通信ポート，IP サイズに着目することによってサーバとのユーザのパソコンの間における通信状況を確認することとした．

```
FLOW,133.44.XX.46,24,9,0005dd------,001bfc------,0x0800,1,
1,133.44.YY.20,133.44.XX.42,6,0x00,127,1898,80,0x18,394,
380,8
FLOW,133.44.ZZ.86,1,21,0005dd------,0018f3------,0x0800,1,
1,133.44.YY.65,133.44.ZZ.102,17,0x00,31,2967,2967,0x00,4
32,418,8
```

図 4　sFlow エージェントによる csv 出力の例

3. Flow 情報の集計と通知

コレクタでは，2 台のエージェントから収集した csv 出力を元に定期的に集計処理を行っている．エージェント毎に，発信元 IP アドレス毎のパケットサイズの合計，宛先ポート番号などの情報を元に集計処理を行い，結果を電子メールで管理者へ通知している．通知の電子メールの例を図 5 に示す．

```
Subject: sflow 集計報告
To: hakusei@vos.nagaokaut.ac.jp

　このメールはシステムからの自動送信です.
sFlow agent から収集したパケットの集計結果です.

---agent1 発信元 IP 別 sizeTOP10----------
133.44.XX.42                8160464
133.44.XX..40                819507
　(中略)
---agent1 発信元ポート  TOP10----------
80                           9428
2967                         1417
　(中略)
---agent2 発信元 IP 別 sizeTOP10----------
133.44.ZZ.20                40091
133.44.ZZ.57                 7636
　(中略)
---agent2 発信元ポート  TOP10----------
2967                          232
8080                           33
　(以下，略)
```

図 5　電子メールによる集計情報の通知

パケットサイズの合計値は，サンプリングされた値であるため正確な数値を表してはいないが，サンプリングレートとの積算によりおおよその通信量を知ることができる．これらの情報を元に，大容量の通信を行っている利用者機器や利用アプリケーションの特定を定期的に把握することが可能と考えている．

4.おわりに

キャンパスネットワークを監視する手法として，サンプリングした形でパケット情報の取得を行う sFlow 技術に対応したスイッチおよびコレクタサーバを導入し，収集した結果を統計処理を行うシステムを構築し，学内向けサーバに対して試行を行った．sFlow に対応したネットワーク機器を導入する必要があるものの，収集のためのソフトウェアは無償にて公開されている sflowtool を用いることが可能であり，出力結果を集計することでネットワーク動向を確認する目的で使用することができた．

今後は，上流ネットワークとの間に対応機器を挿入することによって，学外外接続との間のトラフィックの監視体制を整えることにより，本格的な利用の実施を行いたいと考えている．膨大な学外間とのトラフィックへの対応として，コレクタのデータ保存領域の増強，サンプリングレートの調整を行う必要があるが，集計や電子メールによる通知の機能については，構築したシステムで充分な利用が可能と考えている．

現行のシステムでは定期的に収集情報を集計する形でのフロー情報の利用であるが，長期間の経時変化を調査する上でも有用な情報源と考えている．サンプリングレートの調整を行い，取得データ量を抑制した状態で収集を継続し，長期間に渡るデータを横断的に調査することで，従来とは異なる側面からネットワーク利用の動向を知ることができるものと考えている．

参考文献

[1]sFlow
http://www.sflow.org/
[2] RFC3176(日本語訳)
http://www.twise.co.jp/download/rfc3176j.txt
[3]sflowtool
http://www.inmon.com/technology/sflowTools.php