WIDEのトランジットトラフィック概要

1　2016年トラフィック概要

MAWIワーキンググループでは、トラフィックを多次元集約するagurimツール[1]を開発し、2013年2月よりWIDEのトランジット回線のトラフィックを継続的に記録している。2015年5月には、ツールをオープンソースとして公開し、同時に、IPアドレスを匿名化したWIDEのトランジット回線のトラフィックデータをWebインターフェイスでブラウズ可能にした[2]。これによって、ネットワーク運用者や研究者が、バックボーンのトラフィック状況の詳細をブラウズできるようになり、トラフィック情報の共有や研究の促進に繋がることを期待している。

agurimツールは、トラフィック量およびパケット数を使ってフローを集約する。パケットキャプチャしたデータを基に、30秒間隔で一次集約フローデータを作成、保存している。また、このデータから1時間毎に再集約したデータを、さらにこの1時間毎のデータを基に1日毎の再集約データを生成している。データの閲覧する際には、Webユーザインターフェイスから、時間粒度やフロー数を変化させて、グラフ生成を行なう。元データには、pcap、NetFlow、sFlowが利用可能である。

ここでは、2016年1年間のトラフィック概要を、公開している匿名化データを使って示す。同じ元データから、アドレスを元に集約したトラフィック量(図1)とパケット量(図3)、プロトコルを元に集約したトラフィック量(図2)とパケット量(図4)の4つのグラフに表している。いずれのグラフも粒度は1日となっている。

グラフの各集約フローのラベルは、ソース、デスティネーションIPアドレス(レンジ)と全体に対する割合に続いて、そのうちの上位サブフローのリストが示される。サブフローは、プロトコル番号、ソース、デスティネーションポート番号と、その集約フローに対する割合で表される。“*”はワイルドカード(IPv6アドレスの場合は“*::”)を示す。

2016年全体を通して、1日平均のトラフィック量は約200-600Mbps、パケット量は50-100kpps程度である。図1の6/22-23のピークは、AWSからNAISTの研究用クラスタへのダウンロードによるものである。

個別の集約フローを見ると、集約されたネットワークに加えて、いくつかのホストが識別されている。ここには、ftp.nara.wide.ad.jp、ftp.jaist.ac.jp、 pinger-j2.ant.isi.edu などが含まれる。ISIのマシンはSFCでホストしているpingerプローブである。

MAWIワーキンググループでは、今後もagurimツールを使ったトラフィック状況の把握を行なっていく予定である。

参考文献

[1] Midori Kato, Kenjiro Cho, Michio Honda, Hideyuki Tokuda. Monitoring the Dynamics of Network Traffic by Recursive Multi-dimensional Aggregation. OSDI2012 MAD Workshop. Hollywood, CA. October 2012.

[2] Agurim Web site. `http://mawi.wide.ad.jp/~agurim/about.html`

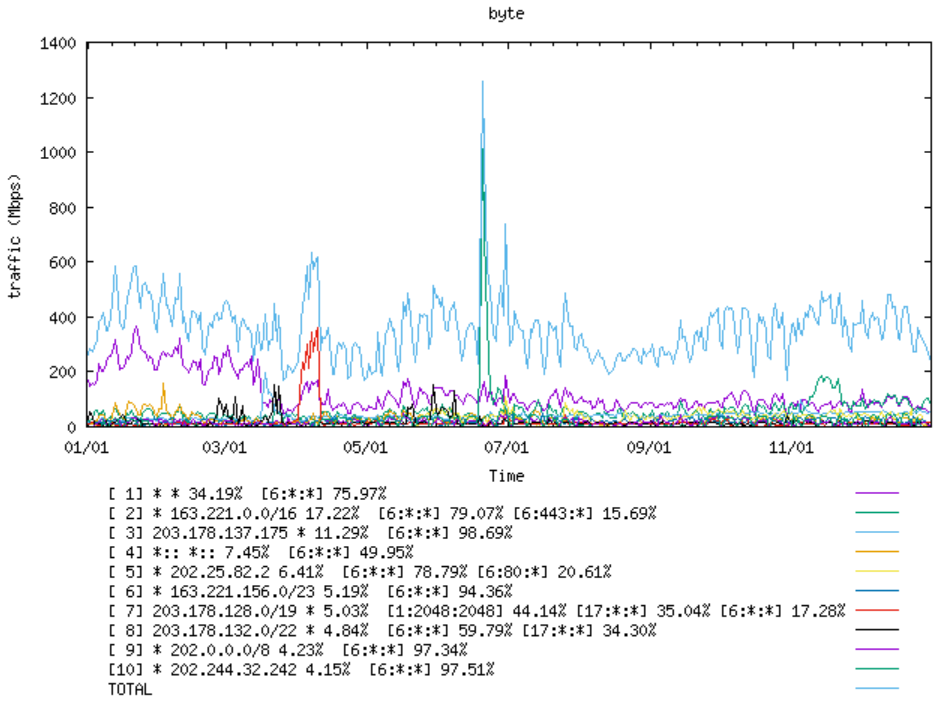

図 1: アドレス別トラフィック量 (2016 年 1 月-12 月)

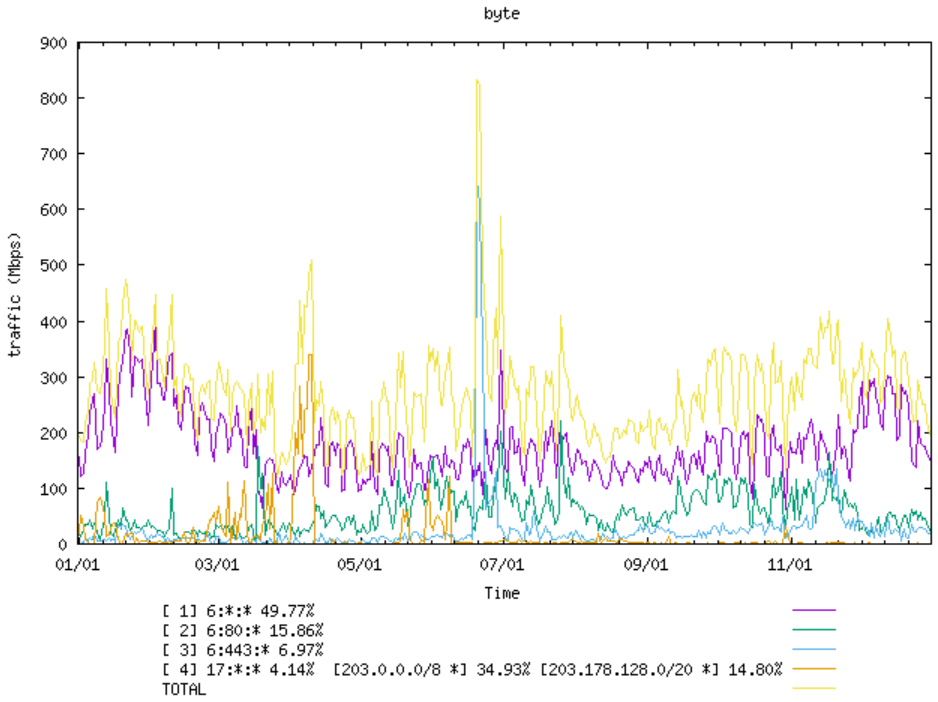

図 2: プロトコル別トラフィック量 (2016 年 1 月-12 月)

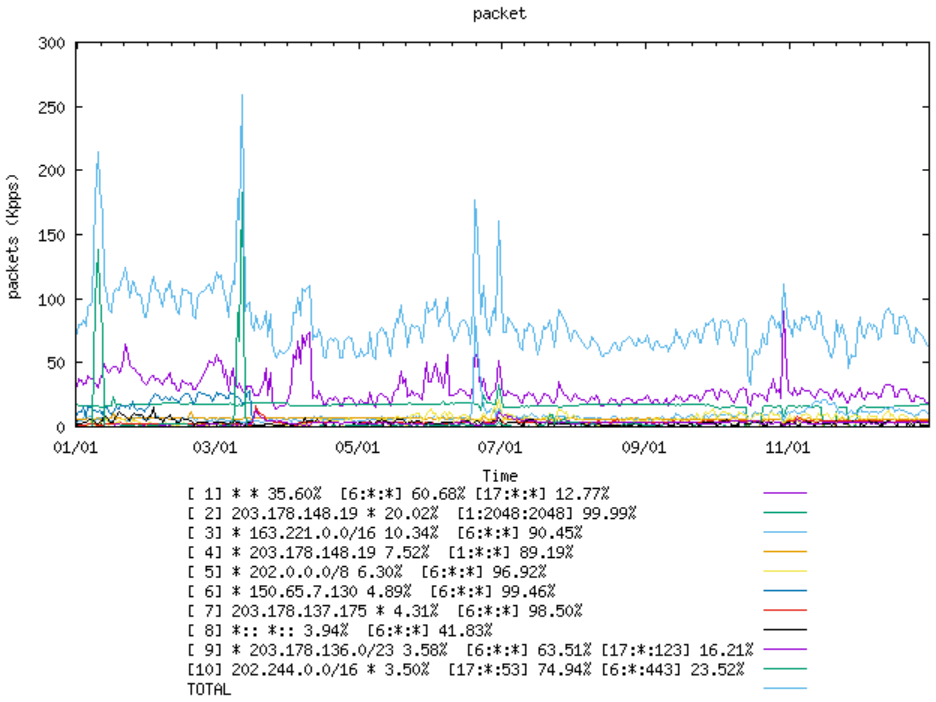

図 3: アドレス別パケット量 (2016 年 1 月-12 月)

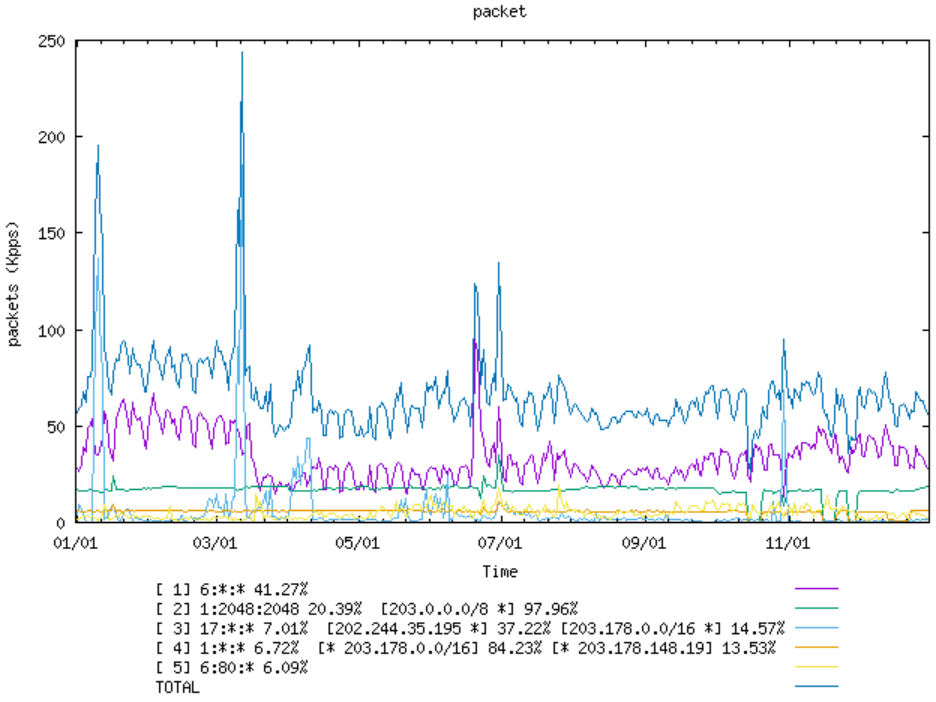

図 4: プロトコル別パケット量 (2016 年 1 月-12 月)