flow 実験チーム 2004 年 WIDE 春合宿 実験報告

藤井 聖<sato-fu@is.naist.jp>

1. 実験の主旨、期待していた成果

roft Working Group (http://www.roft.org/)(以下 roft wg) は、フローを用いたトラフィック観測システムを提案し、研究開発している。2004 年 WIDE 春合宿において、roft wg は flow 実験チームとして実験をした。当該実験では、フローと呼ばれる観測単位で合宿のネットワークトラフィックを観測することで、次の成果を目指した。

1. 得られたトラフィック情報をネットワーク管理者に提供することにより、合宿ネットワークの安定運用に貢献する。
2. 動作デモを通じて、提案システムの有用性をアピールすることで、様々な地点での計測許可をいただく。また、既存トラフィック計測ツールで困っている点や、追加機能案、改良案等を広く収集し、今後の研究開発に生かす。

2. プライバシーポリシー

ネットワークトラフィックを計測するにあたり、トラフィックに含まれる個人情報の扱いについて十分考慮する必要がある。本実験では、パケットのレイヤ 3 およびレイヤ 4 ヘッダに書かれた情報、転送パケット数、転送バイト数のみを収集し、パケットのペイロード部分に関しては一切収集していない。また、一般ユーザに対するトラフィック可視化のデモンストレーションにおいては、アドレス情報など、個人の識別に繋がる情報は全て暗号化して提供した。今回収集したトラフィックデータは研究・運用目的でのみ利用する。特に、アドレス情報などを除いた統計データは今後の合宿ネットワーク運用の資料と本報告書上および Web アプリケーション経由で公開する。

3. 実験の構成

3.1. 合宿ネットワークトポロジ

2004 年 WIDE 春合宿のネットワークは図 1 に示すように、

- noc
- wired
- wireless-1
- wireless-2

の 4 つのセグメントで構成された。noc セグメントにはいくつかのインターネットへ繋がる回線とサーバ群が配置され、その他 3 つのセグメントは一般参加者の生活用セグメントとなった。

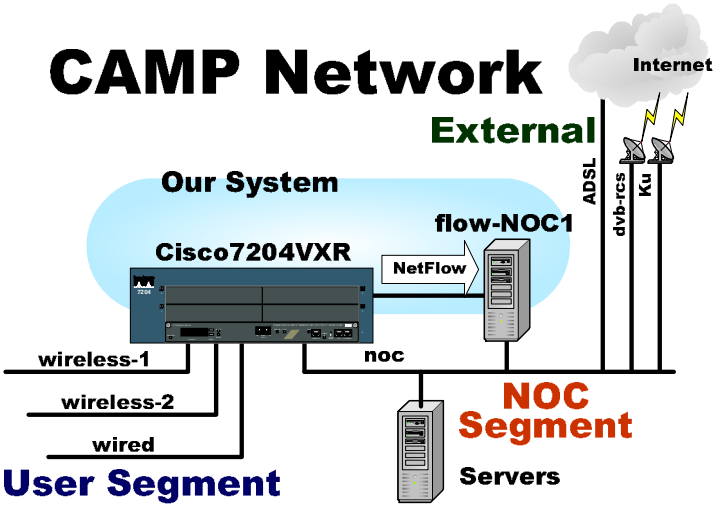

図 1. 合宿ネットワークの構成と flow 実験チーム機器の構成

3.2. flow 実験チーム、システム構成

flow 実験チームは、前節で述べた 4 つのセグメントの間に設置されたルータ、Cisco7204VXR にて計測し、各セグメント間のトラフィック、各セグメントからインターネットへと向かうトラフィックは全て観測対象とした。noc セグメントからインターネットへ向かうトラフィックも、一時 Cisco7204VXR を経由するよう設定され、観測対象となった。Cisco7204VXR で観測されたトラフィックはフローと呼ばれる単位(Cisco の定める NetFlow に基づく)で集約され、NetFlow パケットとして、フロー収集用 PC(flow-NOC1)に対して出力された。flow-NOC1 は、フローデータ用データベースサーバと可視化されたトラフィック情報を Web アプリケーション経由で提供する Web サーバを兼ねた。flow-NOC1 にて収集されたフローデータは Web アプリケーションを介して可視化されネットワーク管理者、一般参加者に提供された。

3.3. Web アプリケーションの構成

Web アプリケーションに、トラフィックを指定するための様々なパラメータを与えることで、該当するトラフィックの情報を可視化することができる。指定できるパラメータとして、日時、入力インターフェース、出力インターフェース、IP プロトコルバージョン、プロトコルタイプ、送信元ポート番号、宛先ポート番号などがある。

トラフィックの可視化方法は二種類用意した。可視化方法 A では 24 時間の時系列で転送量または転送パケット数の変化を表示する。可視化方法 B では 5 分の時間枠の中で大量のトラフィックを発生させている送信元ホストと宛先ホストを表示する。各可視化方法では、指定したパラメータに該当するトラフィックを種類ごとに分類(色分け)して表示できる。分類方法には、「送信元ポート番号や宛先ポート番号ごと」、「入力・出力インターフェースごと」、「IP プロトコルバージョンごと」、「プロトコルタイプごと」を用意した。

Web アプリケーションのトップページからパラメータと分類方法を指定することで、可視化方法 A のページへ遷移する。このページ上のトラフィック量変化のグラフから時間枠を指定することで可視化方法 B のページへ遷移する。図 1～図 4 は実際の Web アプリケーションの動作画面である。

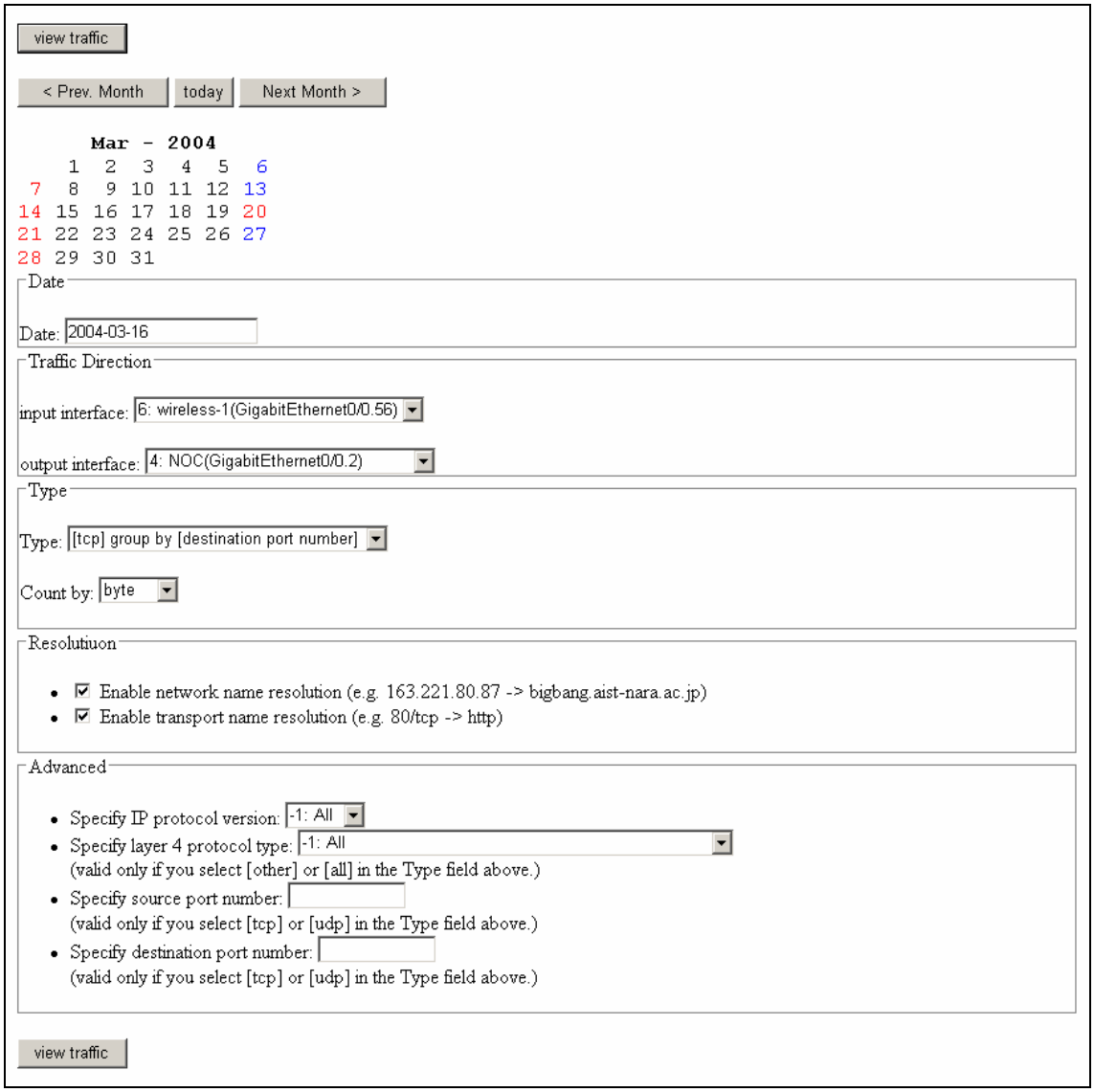

図 2. Web アプリケーショントップ画面

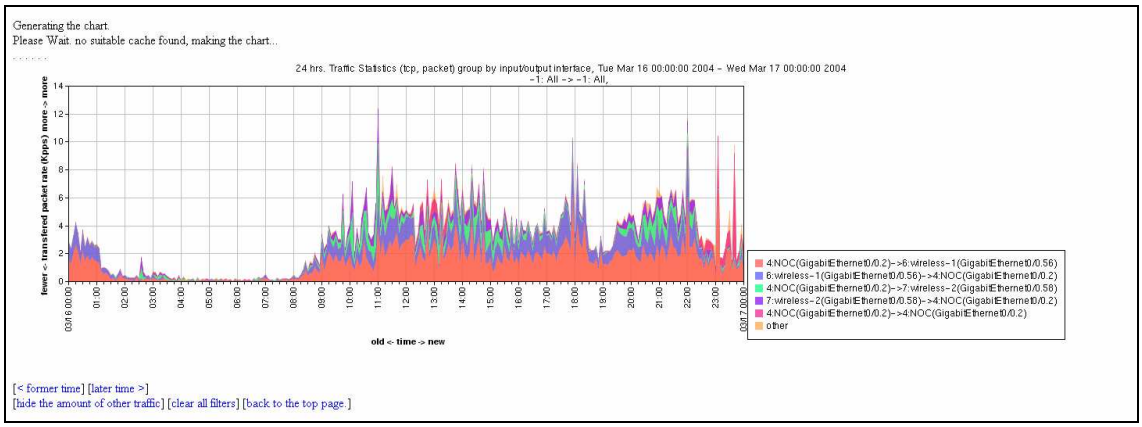

図 3. 可視化方法 A の例 – 入力・出力インターフェースごとに分類したトラフィック量変化

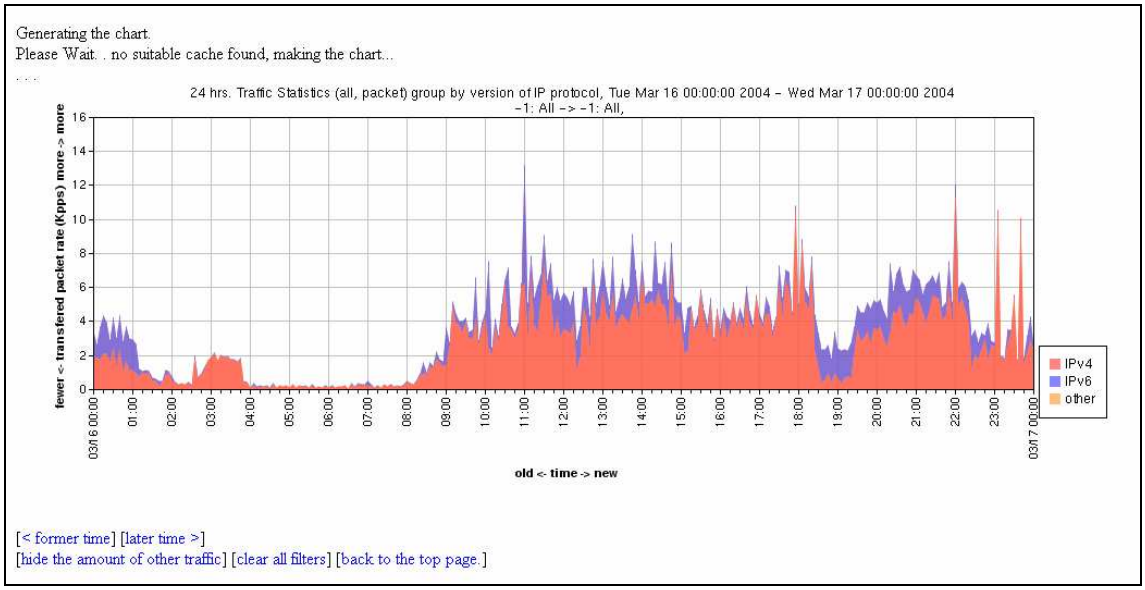

図 4. 可視化方法 A の例 – IP プロトコルバージョンごとに分類したパケット量変化

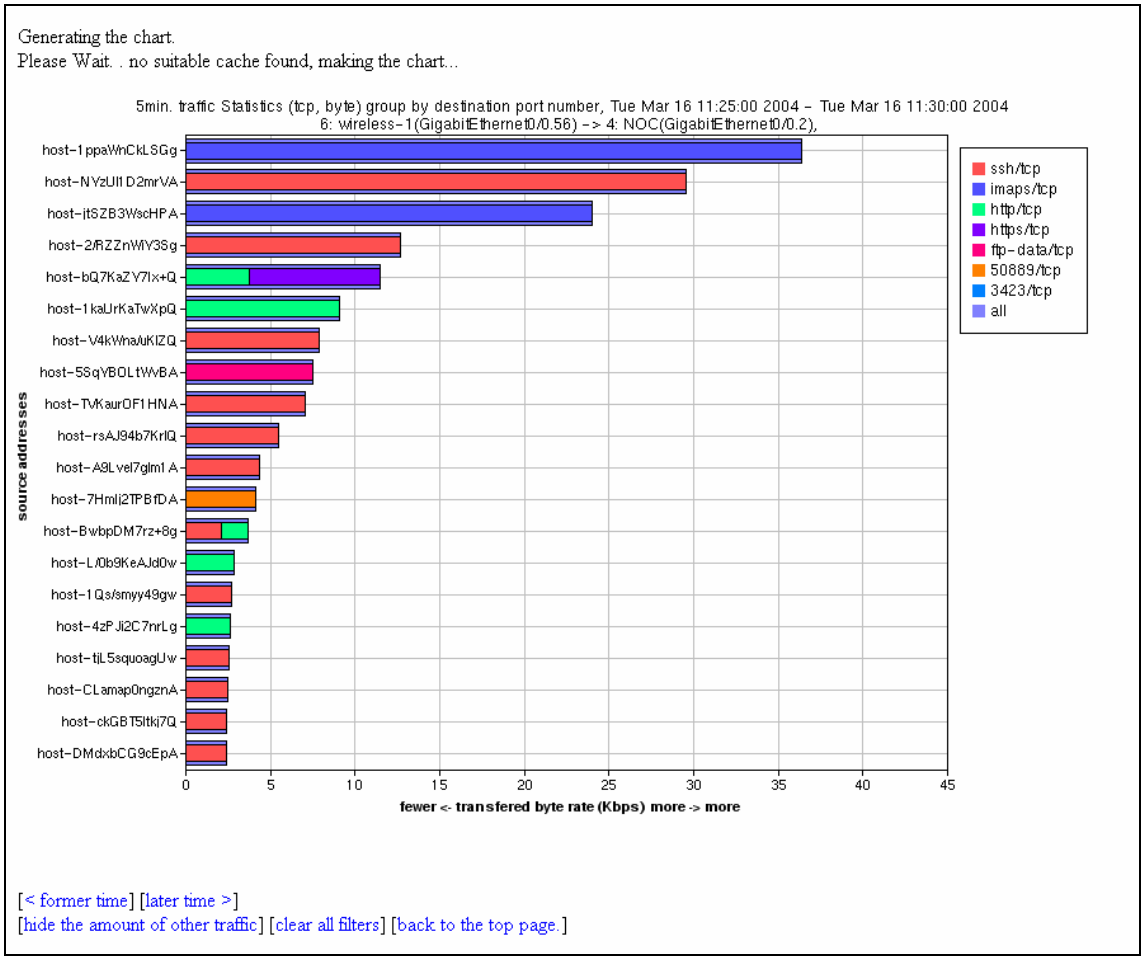

図 5. 可視化方法 B の例 – 宛先ポート番号ごとに分類したトラフィック発生量の多い送信元ホスト(ホスト名を暗号化済)

4. 実験の結果と考察、得られた知見

トラフィック計測において特に問題は発生せず、計測は成功した。実験システムの構成で問題なくトラフィックの計測が可能なことが証明された。

計測の結果、合宿の 4 日間で 58,873 件のトラフィックレコードが観測された。これは、パケット数で見ると 93,998 個、転送バイト数で見ると約 39MB 分に相当する。本実験では、サンプリングレートをパケット単位で 1/1000 とした。従って、実際に合宿期間中に Cisco7204VXR を通過したパケット数はその約 1,000 倍と推測され、約 94 メガパケット、39GB となる。平均秒間転送レートに直すと、329kpps、1.1Mbps となる。1/1000 というサンプリングレートはデータベースサーバの負荷を考慮し、Web アプリケーションが現実的な時間で処理できるレコード数から逆算した値である。

4.1. トラフィック内訳

得られたトラフィック情報の代表的な統計値を示す。

4.1.1. IP プロトコルバージョン別トラフィック量

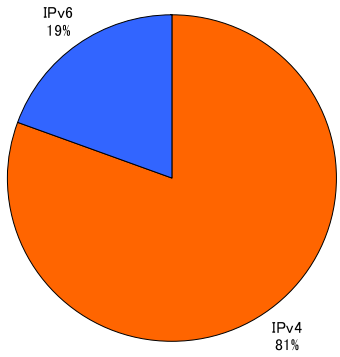

図 6. IP プロトコルバージョン別トラフィック量(パケットカウント)

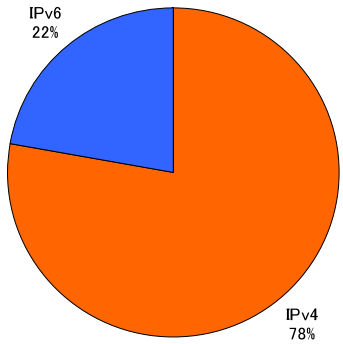

図 7. IP プロトコルバージョン別トラフィック量(転送量)

図 6,7 は全体トラフィックに対する IPv4、IPv6 それぞれの内訳を、パケットカウント単位、転送量単位で示している。IPv4 トラフィックが首位であるが、IPv6 トラフィックも 20%程度と、かなりの量を占めていることが分かる。

4.1.2. ポート番号別トラフィック量

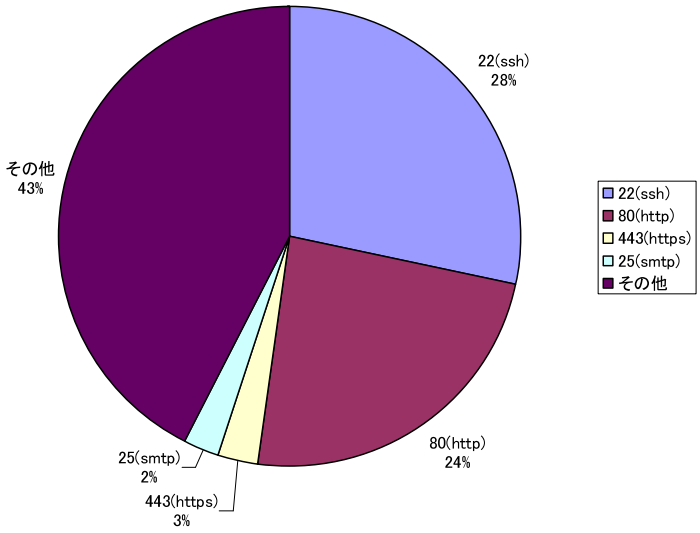

図 8. 宛先ポート番号別上り TCP トラフィック量(転送量)

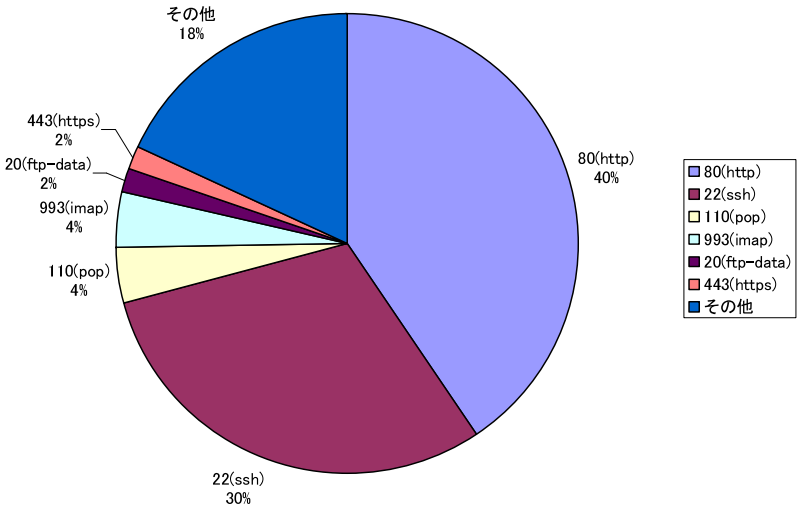

図 9. 送信元ポート番号別下り TCP トラフィック量(転送量)

図 8 は合宿内セグメントから外部(インターネット)へ向かう上り TCP トラフィックの転送量を宛先ポート番号別に示している。22(ssh)が最も多く、80(http)、443(https)、25(smtp)と続いている。ただし、当実験ではレイヤ 4 ヘッダ上のポート番号情報のみからアプリケーションを判断しており、例えばポート番号が 80(http)であるからといって、実際に http のトラフィックであるという保証はできない。

図 9 は同様に下りトラフィックの転送量を送信元ポート番号別に示している。ただしインターネットからの下りセグメントの他に、noc セグメントからユーザセグメントへの下りトラフィックも含んでいる。80(http)が最も多く、22(ssh)やメール関連と続いている。

4.1.3. プロトコル別トラフィック量

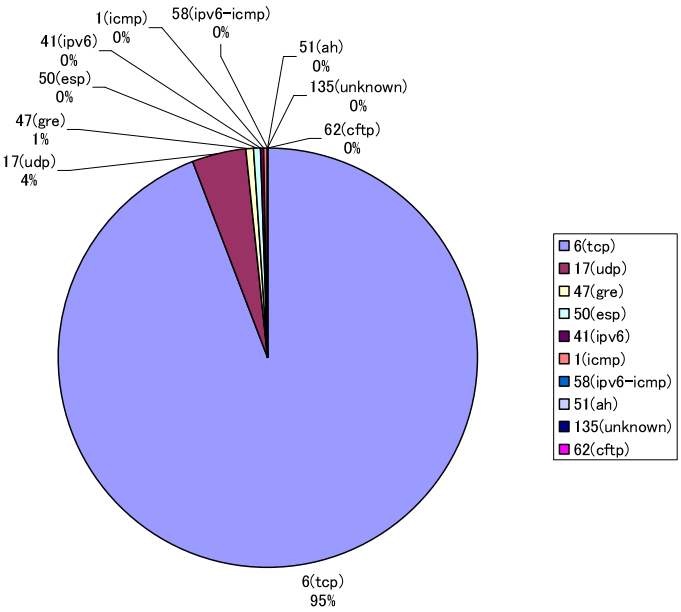

図 10. プロトコルタイプ別トラフィック量(転送量)

図 10 は全体トラフィックに対するプロトコル別のトラフィック量を示している。全体の 95%が TCP によるトラフィックであり、4%が UDP によるトラフィックである。トンネリングに使われる gre、esp、ipv6 がそれぞれ 1%以下含まれている。icmp 関連トラフィックも全体トラフィック量と比較すると 1%未満である。

4.2. ワーム検知

本実験では、ネットワークの安定運用に貢献するためにワームに感染したホストの検知も目指し

た。その方法は、ワームが原因で発生するトラフィックの特徴を利用し、該当トラフィック量の変化を監視することで、ワームに感染しているホストを特定するというものである。合宿期間中、ワームが原因で大量発生することが多い ICMP、宛先ポートが 135/tcp であるトラフィックを実験システムによって監視した。しかし、そのようなトラフィックはほぼ0であり、感染ホストも検出できなかった。合宿では、IPtraceback 実験チームも同様の目的で IDS を設置していたが、その IDS でもワームが原因と推測されるトラフィックは観測されていない。このことから、本実験でのワームの検知方法に問題があったのではなく、実際にワームに感染したホストが発生しなかったものと考える。

4.3. トラフィック量変化

ネットワークの安定運用に必要な指標として、トラフィック量の変化がある。本実験では、回線障害などを原因とする、急激なトラフィックの減少や増加を監視した。その結果、各日におけるトラフィック量の周期的な変化は観測できたが、急激な変化は観測できず、障害検知には応用できなかった。

4.4. Web アプリケーションへのアクセスとアンケート結果

アクセスログからの推定によると、合宿期間中にのべ 100 人ほどの人に本実験の Web アプリケーションを試用して頂いたようである。

アンケートのも結果には、実験自体や実験の有用性に対する否定的な意見はなく、提案システムの有用性のアピールは成功した。一方、Web インターフェースの操作性や、計測結果の応用方法に対する疑問も多く寄せられた。

5. 結論

まず、本実験の一つ目の目標である、「得られたトラフィック情報をネットワーク管理者に提供することにより、合宿ネットワークの安定運用に貢献する」という点について述べる。トラフィック情報の管理者への提供については、Webアプリケーションを通じて正常にでき、問題はなかった。しかし、今回、想定していたワームによる異常トラフィックや回線障害によるトラフィック量の急激な変化は観測できず、それらの管理者への通知もできなかった。その原因の一つは、合宿ネットワークがそもそも安定していたことが挙げられる。また、合宿期間が 4 日間と非常に短く、正常なネットワークの状態の定義が困難であったことも原因である。

次に、二つ目の目標である、「動作デモを通じて、提案システムの有用性をアピールすることで、様々な地点での計測許可をいただく。また、既存トラフィック計測ツールで困っている点や、追加機能案、改良案等を広く収集し、今後の研究開発に生かす。」という点について述べる。Web アプリケーションの動作デモは合宿参加者のおよそ 35%、100 人前後の人に閲覧して頂いた。このパーセンテージは十分とは言えず、実験に関する宣伝が不足していたと考えられる。合宿参加者用

メーリングリストやポスターなどを用いた宣伝は繁盛に行ったが、BoF 枠などを活用して、宣伝すべきであった。追加機能案や改良案も、口頭やアンケート結果を通じて頂いたが、これについてもBoF 枠を設定すべきであったと感じでいる。計測拠点の拡充については、ワーキンググループ内で具体的な計測目的と必要機器、計測担当者などの詳細がまとめきれておらず、具体的な提案に持って行くことができなかった。ワーキンググループ内でさらなる議論をし、これらの詳細を取り決める必要がある。

6. 今後の方向

実験システムの構成で問題なくトラフィックの計測が可能なことが証明され、その応用事例(Web アプリケーション)の有用性についてもアピールできた。今後、roft Working Group は、フローベース計測であることの優位性をアピールするとともに、他の応用方法も検討する必要がある。

フローベース計測であることの優位性を示すには、広帯域なネットワーク上でも低コストで計測が可能なことを示す他に、サンプリングレートの妥当性についても示す必要がある。計測データの目的に応じた妥当なサンプリングレートを検討する他、目的によってはサンプリングをせずともスケーラブルに計測が可能なシステムの検討が必要であると考えている。

計測結果の他の応用事例としては、過去のトラフィック状況を考慮した上で異常なトラフィックを自動的に検出する手法、多地点で計測することによって直接計測していない地点のトラフィックを予測する手法などを検討している。

7. 参考文献

- roft working group、 http://www.roft.org/
- 2004 年 WIDE 春合宿、flow 実験チームの Web ページ、http://cluster19.aist-nara.ac.jp/public/widecamp-04spring/
- 本報告書著者の Web ページ(flow 関連ソフトウェア、トラフィック解析例等)、http://www.aist-nara.ac.jp/~sato-fu/
- 中尾 嘉宏、許 先明、中村 豊、藤川 和利、砂原 秀樹、"自由度の高い解析可能なネットワークトラフィック計測システムの実現"、電子情報通信学会通信方式研究会、2003 年 11 月
- 藤井 聖、中尾 嘉宏、中村 豊、藤川 和利、砂原 秀樹、"フローを用いた特定トラフィック検出システムの運用"、 情報処理学会 分散システム／インターネット運用技術研究会(DSM 研究会)、2003 年 11 月
- 中尾 嘉宏、"トラフィック特徴抽出によるネットワーク運用支援手法に関する提案と評価"、奈良先端科学技術大学院大学 修士論文、2004 年 3 月
- 高橋 宏明、"トラブルシューティングの効率化を考慮したトラフィックモニタリングシステムの設計と実装"、慶應義塾大学 卒業論文、2004 年 3 月

8. Copyright Notice