第 IV 部

ネットワークトラフィック統計情報の収集と解析

第 4 部
ネットワークトラフィック統計情報の収集と解析

第 1 章　MAWI WG について

MAWI（Measurement and Analysis on the WIDE Internet）ワーキンググループは、トラフィックデータの収集と解析を研究対象とした活動を行なっている。

MAWI WG では WIDE プロジェクトの特徴を活かした研究をするため、「広域」「多地点」「長期的」の三つの項目に重点を置いたトラフィックの計測・解析を行っている。広域バックボーンでのデータ収集はバックボーンを持っている WIDE だからできる事である。分散管理されるインターネットの状態を把握するためには、多地点で観測したデータを照らし合わせることが欠かせない。また、長期的にデータを収集し蓄積するために、ワーキンググループとしての継続的な活動が役に立つ。

計測技術はほとんどの研究分野で必要となるため、MAWI ワーキンググループは WIDE 内の他のワーキンググループと連係をとりながら活動をしている。具体的には、

- グローバルな視点からの DNS の挙動解析（dns-wg と共同）
- IPv6 普及度の計測（v6fix と共同）
- ネットワークトポロジの観測（netviz-wg と共同）
- 長期的な経路変動の観測（routing-wg と共同）
- AI3 の衛星トラフィックの計測（ai3-wg と共同）

などが挙げられる。

また、国際協調として

- CAIDA（http://www.caida.org/）
- CNRS（http://www.cnrs.fr/）
- ICANN RSSAC（http://www.icann.org/committees/dns-root/）
- ISC OARC（https://oarc.isc.org/）
- USC/ISI（http://www.isi.edu）

などと共同して研究活動をしている。

第 2 章　MAWI WG 2008 年度の活動概要

今年度の報告書では、まず第 3 章において、国内 ISP 6 社と共同で行っているブロードバンドトラフィックの収集と解析活動について報告する。

次に第 4 章では、計測に関する国際協調について報告する。現在、WIDE では、CAIDA とフランスの CNRS との間で計測に関する包括的な共同研究を行なっていて、それぞれの組織と複数のテーマについて共同研究を進め、定期的なワークショップの開催や研究者交換を行なっている。

第 5 章と第 6 章で、CNRS の ENS Lyon に交換留学した東京大学の肥村洋輔君と LIP6 に交換留学した慶應義塾大学の空閑洋平君が活動を報告する。肥村君は統計的なモデルに基づく異常トラフィックの検出手法について、空閑君はトポロジ探索手法について研究を行った。このような学生の交換留学は、本人にとって貴重な経験になるのと同時に、組織間の交流を促進し相互理解を深めるので、共同研究を円滑に進めるためにも有効である。

第 7 章では、異常検出などのトラフィック解析結果を共有するためのツールについて報告する。WIDE では長年に渡ってトラフィックデータを公開し、それらのデータはさまざまな研究に利用されている。しかし、論文等で解析結果が発表されても、他の研究者が二次利用できる形になっていないので、解析結果とデータを照合したり、他の研究成果と比較したりするのは難しい。もし、解析結果をデータに関連付けてメタデータとして公開することができると、データ利用の利便性が大きく向上する。そこで、そのようなメタデータの記述のためのツールの開発を行い、データの解析結果の再利用を促進する試みを進めている。

第 3 章　ISP から見たブロードバンドトラフィックの現状と傾向

3.1 ブロードバンドトラフィック増加の影響

日本ではブロードバンドが普及し、誰もが速いインターネットを安く利用できる環境が出来てきた。特に、FTTH の普及率では日本は世界最高で、最速のブロードバンド先進国となっている。その一方で、ブロードバンド利用者のトラフィック量が急増、バックボーントラフィック全体の 2/3 を占めるまでに至り、全体のトラフィック増加を牽引している。

トラフィック量の伸び率は今後を予想する上で重要な意味を持つ。トラフィック量が年率 100%で増加を続けると 10 年で 1000 倍にもなり、その実現のためには画期的な技術的ブレークスルーが必要となる。しかし、年率 50%の増加なら 10 年で 58 倍なので、既存技術の延長で対応できる可能性が出てくる。実際に、国内のトラフィック増加率は、一時より増加速度が鈍ってきている。国内主要 IX のトラフィック量は、ブロードバンドへの移行が本格化した 2002 年には年率 4 倍もの速度で伸びていたが、ここ 5 年ぐらいは年率 50%程度の増加で安定している。この要因として、ブロードバンド普及が一巡した事や、人気コンテンツが P2P ファイル交換から事業者の動画配信サービスに移行している事が挙げられる。

3.2 協力 ISP によるトラフィック量調査

2004 年の総務省次世代 IP インフラ研究会報告書 [216] では、今後のインターネットの在り方を考える上で重要な基礎データとして、技術的かつ継続的なトラフィックデータ集計の必要性を訴えると同時に、企業機密であるトラフィックデータの集計には産官学の協力による取り組みが欠かせない事が指摘された。

これを受け 2004 年 7 月に、総務省データ通信課を事務局に、学界の研究者と国内 ISP 7 社がトラフィック量調査の取り組みを始めた。データを提供頂いている協力 ISP は、IIJ、ケイ・オプティコム、KDDI、NTT コミュニケーションズ、ソフトバンク BB、ソフトバンクテレコム、パワードコムの 7 社でスタートした。2006 年の KDDI とパワードコムの合併により、現在は 6 社 7 ネットワークとなっている。

調査の目的は、国内バックボーンにおけるトラフィック量の基礎データを開示する事によって、事実に基づいた健全なインターネットの発展に寄与する事である。

企業機密であるトラフィック情報は個別の事業者では開示が難しい。そのためデータの入手が難しく、ややともすれば、推測あるいは一部の偏ったデータをもとに議論や判断がなされかねない。そこで、産官学の連携によって、トラフィック情報の秘匿性を維持しつつ、協力 ISP 全社の合計値としてトラフィック量を公開している。集計結果は、総務省の報道資料として、また、国際会議等の場で発表され、ブロードバンド先進国である日本のバックボーンの現状を示す貴重な資料として、あるいは、競合 ISP が協調して大規模なトラフィック集計を行なった世界初の事例として、国内外から注目されている [27, 28]。

3.3 収集データ

調査を開始するにあたり、協力 ISP では、ほぼ全てのバックボーンルータのインターフェイスカウンタ値を SNMP で取得し、データを保存している事が確認できた。そこで、ルータのインターフェイスの共通分類を定義し、これらのログを集計し、個別 ISP のシェア等が分からないように合算した結果を開示する事にした。また、平均値は加算可能であるが、最大値等は加算できないため、平均値のみを扱うことにした。

測定対象は、ISP 境界を越えるトラフィックである。一般に、ISP 境界は、顧客を接続するカスタマー境界と、他の ISP と接続する外部境界に分けられる。協力 ISP と協議の結果、各社の実運用と整合するよう図 3.1 に示す以下の共通分類を定義した。

(A1) ブロードバンドカスタマートラフィック
ADSL/CATV/FTTH などのブロードバンドサービスの顧客。ここには、ブロードバンド回線利用の中小企業も含まれる。

(A2) ブロードバンド以外のカスタマートラフィック
専用線、データセンター、ダイヤルアップ利用者等のブロードバンド回線以外の顧客。なお、ここには、専用線接続の下流プロバイダも含まれているので、その下にブロードバンドカスタマーが存在する場合もある。

(B1) 主要 6 IX 外部トラフィック　国内主要 IX、つまり、JPIX、JPNAP、NSPIXP の東京および大

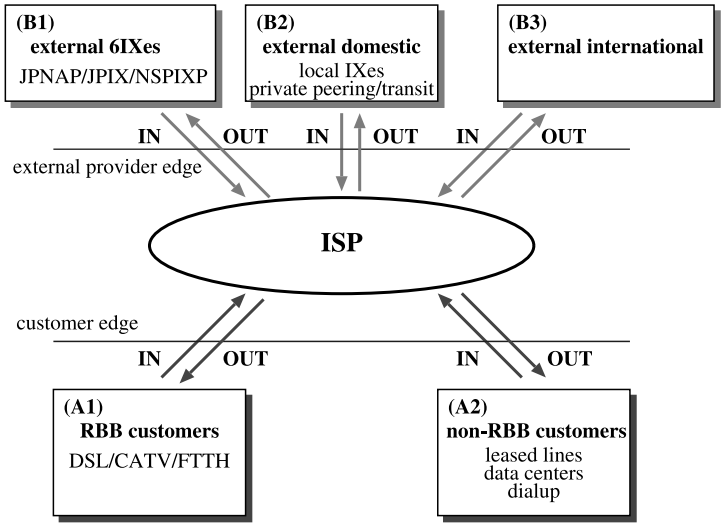


図 3.1. 定義した ISP 境界における 5 つのトラフィック分類

阪で交換される外部トラフィック。これは我々の調査結果を主要IX側での計測値と比較するため。

(B2) その他国内外部トラフィック 主要 6 IX 以外で交換される国内外部トラフィック。主に、プライベートピアリング、トランジット、ローカル IX で交換される国内外部トラフィック。ここでは、両端が国内にあるリンクを国内と定義している。したがって、グローバルな AS に国内で接続している場合も含まれる。

(B3) その他国際外部トラフィック 接続点が国外にあるような国際交換トラフィック。

なお、(A2) のブロードバンド以外のカスタマートラフィックは 4 社からしかデータが得られていない。これは、ISP のネットワーク構成によっては社内リンクと外部リンクの切り分けが難しく集計が困難なためである。その他の項目は全社からデータが提供されている。そのため、(A2) のトラフィック量を他の項目と直接比較する事はできない。

データの収集は、トラフィック分類毎に SNMP インターフェイスカウンタ値を 2 時間粒度で 1 ヶ月分収集する事にした。2 時間粒度のデータによって、各 ISP で大きなトラフィック変化があった場合にも特定が可能となる。前回の測定値や IX での測定結果と比較し、食い違いがある場合には、原因の究明を行なうようにしている。原因には、ネットワーク構成の変更、障害、SNMP データの抜け、インターフェイスグループ分けの不備等が挙げられる。トラフィック量に予想外の変化が見つかった場合には、当該 ISP に確認を依頼し、必要があればデータを再提出してもらう確認体制を取っている。

協力 ISP 側における作業工数で大きいのは、トラフィック分類毎にインターフェイスのログリストを作成、維持管理する手間である。大手 ISP ではインターフェイスログの総数は 10 万以上にのぼる。また、頻繁なネットワーク構成変更に追従する必要があるため、ログリストの維持管理にも大きな労力を要する。協力 ISP 各社には、調査の意義をご理解いただき、データ収集に協力頂いている。

集計を開始した 2004 年 9 月から 3 ヶ月間は毎月データを収集したが、データの一貫性が検証されたので、その後は年に 2 度、5 月と 11 月に計測、収集を行なうようにした。以下に示すデータは、6 社 7 ネットワーク分のデータの合算値である。なお、IN と OUT は ISP からの視点である。

3.4 計測結果

3.4.1 トラフィックの増加傾向

図 3.2 にカスタマートラフィックと外部トラフィックの増加傾向を示す。

2007 年には各項目で 19–68%の増加が観測された。ブロードバンドカスタマーに関しては、IN で年率 22%、OUT で 29%の増加となっている。

トラフィックの増加傾向として以下の点が挙げられる。

- (A1) の IN/OUT の差が開いてきた。2004 年には IN と OUT はあまり差がなかったが、2005 年

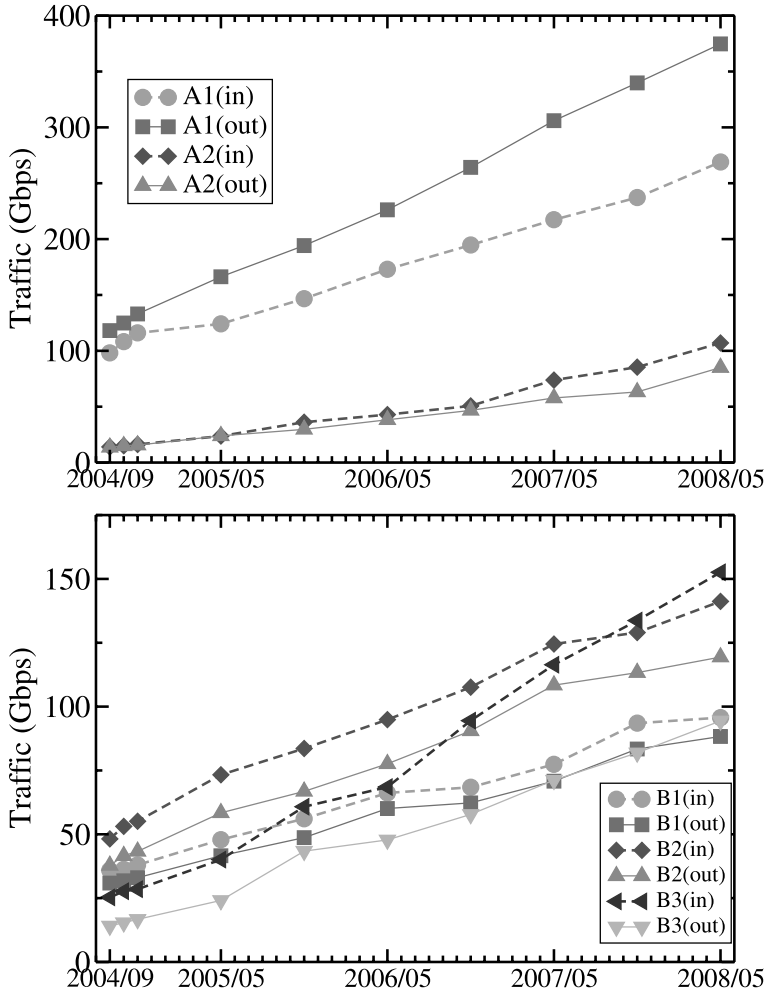


図 3.2.　トラフィックの増加傾向：カスタマートラフィック（上）と外部トラフィック（下）

表 3.1.　計測データの IX 総流入量に占める割合

	2004 年			2005 年		2006 年		2007 年		2008 年
	9 月	10 月	11 月	5 月	11 月	5 月	11 月	5 月	11 月	5 月
割合 (%)	41.5	41.9	41.6	42.0	41.4	43.1	41.5	42.4	41.8	42.6

以降の OUT（カスタマーのダウンロード）の伸びが大きい。これは、2004 年には P2P ファイル共有が支配的だったのに対し、P2P ファイル共有の伸びが鈍り、代わって Gyao、YouTube、ニコニコ動画などの映像配信のトラフィックが増えてきたためと思われる。

- (B2) が (B1) より大きく、その差が開いて来ている。これは、大手 ISP 間のプライベートピアリングが広がり、その結果、主要 IX でのパブリックピアリングからトラフィックが移動しているためだと思われる。
- 国際トラフィックの伸び率が高く、特に 2006 年以降の流入が急増している。これは、YouTube に代表される国外の人気動画サービスの影響だと思われる。

前述のように、(A2) は 4 社からしか提供されていないが、この 4 社の合計値で見ると、(A1) : (A2) はほぼ 2 : 1 となっていて、ブロードバンドカスタマーのトラフィックが全カスタマートラフィックの 2/3 を占めている。

次に、(B1) OUT と IX 側で測定した総流入量との比率を表 3.1 に示す。(B1) OUT は、IX 側の総流入量に対し、測定開始以来一貫して 42%程度のシェアがあり、整合のとれたデータ収集ができている事

が確認できる。この数字を国内総トラフィックに対する協力 ISP のシェアだと仮定すると、2008 年 5 月の国内ブロードバンドトラフィック総量は、アップロードが 631.5 Gbps（269.0/0.426）、ダウンロード 879.6 Gbps（374.7/0.426）と推定できる。

3.4.2 カスタマートラフィック

図 3.3 は 2008 年 5 月の週間カスタマートラフィックを示す。これは、6 社の DSL/CATV/FTTH カスタマーの合計値で、各曜日の同時間帯を平均した値である。休日はトラフィックパターンが異なるため、除いて集計している。

図 3.3（上）のブロードバンドカスタマーでは、一日のピークは、21:00 から 23:00 で、夕方からトラフィックが増え、深夜を過ぎるとトラフィックは急減する、週末は昼間のトラフィックが増えるなど、家庭での利用形態を反映している。また、OUT（カスタマーのダウンロード）に匹敵する量の IN トラフィックがあり、もはや家庭利用はダウンロード中心とは言えなくなっている。平均で IN 側 266 Gbps、OUT 側 370 Gbps の流量があり、そのうち 200 Gbps 以上は定常的にトラフィックがある。変動分は、利用者の操作がトリガーとなっているトラフィックと考えられ、定常部分の多くは機械的に発生されるトラフィックが占めると推測できる。

図 3.3（下）のブロードバンド以外のカスタマーでも、時間別の変動や定常部分の割合といった家庭利用の特徴が出ている事が分かる。これは、ホームユーザ向けサービスや専用線の下流にいるホームユーザの影響だと思われる。上図と比べると、昼間のトラフィック量がやや大きい程度で、従来主流だった企業や大学の就業時間のビジネストラフィック量の割合が小さくなっている事が分かる。

参考までに、図 3.4 に 2004 年 11 月のブロードバンドカスタマーの週間トラフィックを示す。2004 年には IN/OUT がほぼ対称であったのが、2008 年の図 3.3（上）では OUT が大きくなっている様子が分かる。

図 3.5 は過去 4 年間のブロードバンドカスタマーの週間トラフィックを IN 側（上）と OUT 側（下）で比較したものである。定常部分、変動部分共に増加してきている事や、OUT の伸びが大きい事が分かる。また、ピーク時間 21:00–23:00 もより明確になってきた。

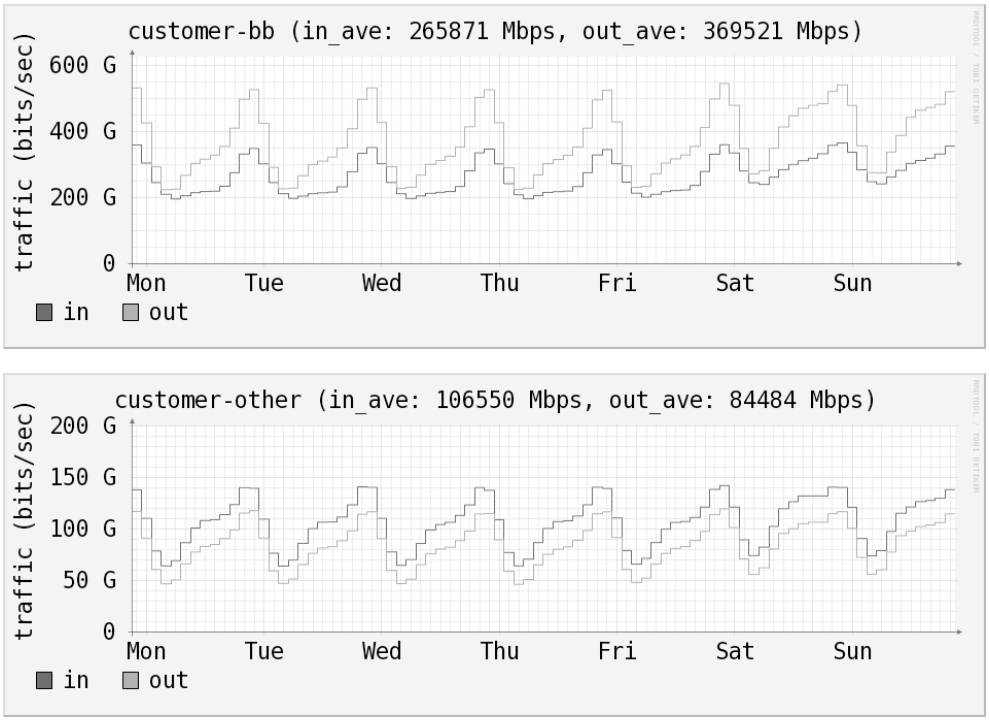


図 3.3. 2008 年 5 月の週間カスタマートラフィック：ブロードバンドカスタマー（上）とブロードバンド以外のカスタマー（下）

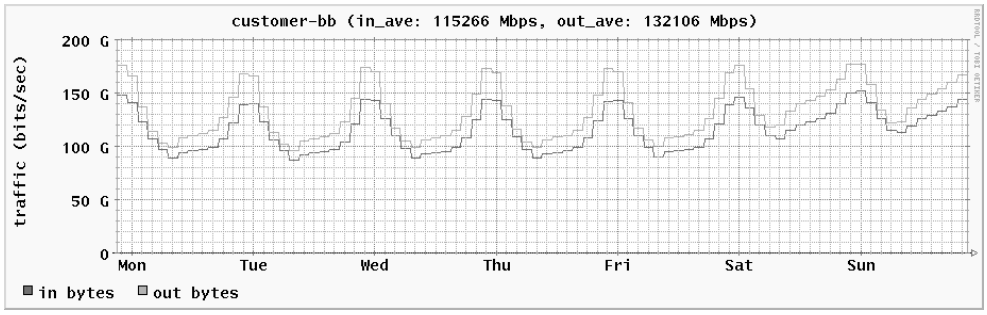


図 3.4.　2004 年 11 月のブロードバンドカスタマートラフィック

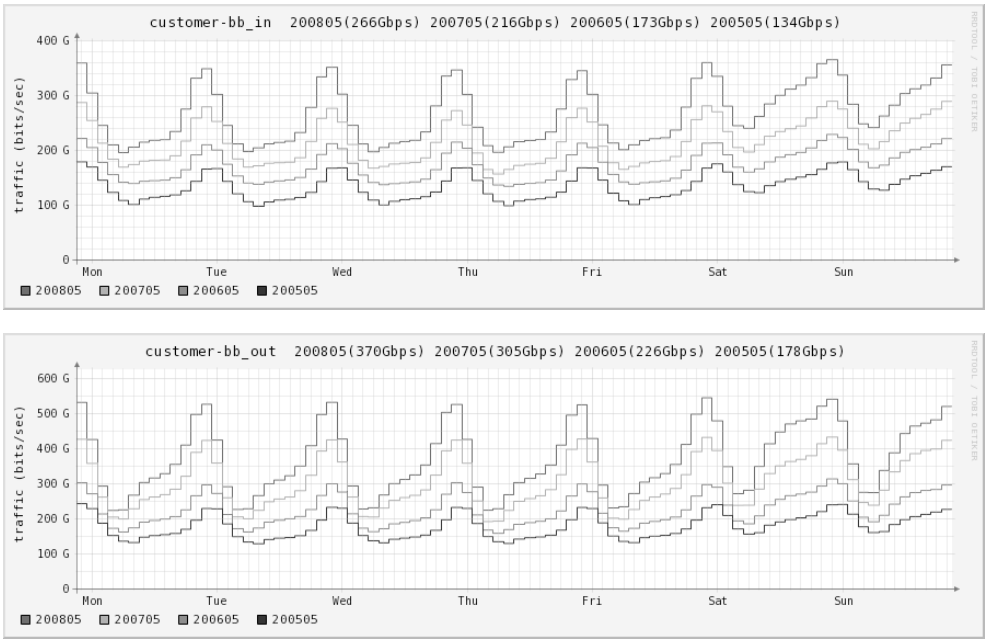


図 3.5.　過去 4 年間のブロードバンドカスタマートラフィックの増加傾向：IN（上）と OUT（下）

3.4.3 外部トラフィック

図 3.6 は 2008 年 5 月の週間外部トラフィックを示す。主要 IX トラフィック（上）とその他国内トラフィック（中）のパターンは、ブロードバンドカスタマーのそれと酷似していて、ホームユーザのトラフィックの影響を大きく受けている事が分かる。国際トラフィックに関しても、ピーク時間は同様であるが、変動部は流入が大きく、国外からのダウンロードが支配的である。

3.5 まとめ

我々は、2004 年から ISP の協力を得て、国内インターネットのトラフィック量を調査し、基礎データとして開示している。トラフィック量の増加率は、過去 4 年間は全体的に 30–40%程度で安定しているが、その中で、この 2 年間は国外からの流入トラフィックの伸びが目立つ。これらの要因として、ブロードバンド普及が一巡したことや、人気コンテンツが P2P ファイル交換から事業者の動画配信サービスに移行していることが挙げられる。

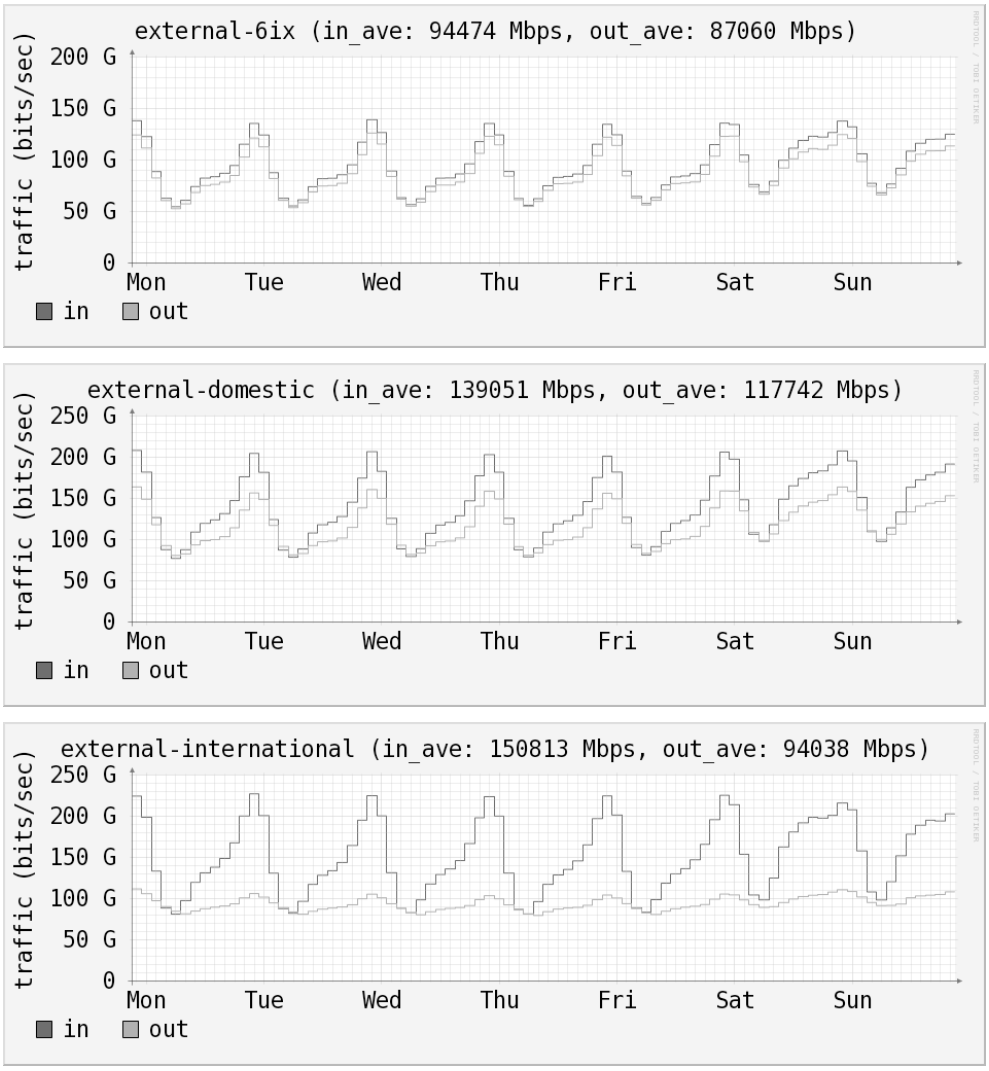


図 3.6. 2008 年 5 月の外部トラフィック：主要 6 IX（上）その他国内（中）その他国際（下）

第 4 章　計測に関する 2008 年度国際協調活動報告

4.1 はじめに

WIDE プロジェクトは多くの国際協調活動を行なっているが、近年は計測研究の重要性が増している。これは、インターネット研究において、グローバルなレベルでその挙動を把握する必要性と難しさが認識されてきたためである。

現在、WIDE では、CAIDA（the Cooperative Association for Internet Data Analysis）とフランスの CNRS（The Centre National de la Recherche Scientifique）との間で計測に関する共同研究を行なっている。

4.2 CAIDA との共同研究

CAIDA と WIDE プロジェクトは、2003 年度から計測に関する包括的な共同研究を行なっている。主なテーマは、DNS 計測、トポロジ計測、IPv6 計測、BGP 計測であり、年に 2 回程度ワークショップを開催し、相互の活動を理解し協力体制を作っている。

2008 年度には以下のワークショップを開催した。今回から韓国の CASFI チームも参加し、日米韓の連係を深め、共同研究に繋げていく予定である。

- 第 10 回 CAIDA-WIDE-CASFI 計測ワークショップ
  2008 年 8 月 15–16 日 Marina del Rey, CA

2008 年度の主な活動を以下にあげる。

- インターネット計測デーの実施
  2007 年に引続き、インターネット計測デーを 3 月に実施した。WIDE では国際線の 72 時間のパケットトレース等を収集し公開した。
- 計測データの目録化
  計測データの研究利用を促進するため、CAIDA が中心となり各組織の持つ計測データを目録化するプロジェクトを進めている。今年度は主に、2008 年 3 月のインターネット計測デーに収集したデータの目録化を行なった。
- 地理情報を考慮したトポロジ解析
  CAIDA の持つ広域 traceroute データをもとにして、WIDE が地域別の AS トポロジの解析を行なっている。
- 広域計測基盤
  主に開発途上国からの計測を行なう目的で、WIDE が小型計測箱を設置、遠隔管理する計画を進めている。

2009 年度もこれらの共同研究活動を継続する予定である。

4.3 CNRS との共同研究

2006 年より、フランスの大学連合である CNRS と WIDE は、計測とモビリティの 2 つの分野において 3 年間の共同研究を行なっている。共同研究最終年の今年は、相互の技術を組合せた研究への取り組みや、今後の共同研究に繋がる議論に重点を置いた活動を行なった。

計測グループでは、ゲームや P2P 等の新規アプリケーションやセキュリティ攻撃を計測、モデル化することをテーマとして共同研究を行なっている。より具体的には、以下のような研究活動を行なっている。

(1) アプリケーション識別

フランス側 LIP6 の Salamatian 教授のグループが開発した、パケットの先頭数十バイトの情報からアプリケーションのタイプを識別する技術を日本側のデータを使って検証を行なっている。

(2) 時系列データ解析

フランス側 ENS Lyon の Patrice Abry のグループと日本側福田准教授が、時系列トラフィックデータをモデル化し、定常時と異常時のパラメータ変化の違いに着目し、セキュリティ攻撃等を自動で検出する共同研究を行なった。次のステップとして、日本側の蓄積データに含まれる異常トラフィックの目録化に着手している。これにより既存データの研究利用の促進が期待できる。

(3) ハニーポットによるセキュリティ攻撃の検出

フランス側 LAAS Philippe Owezarski のグループのハニーポットを日本側にも設置し、日仏で同時に観測する事によって、広域に渡る攻撃を検出することや、地域差を明らかにする共同研究を実施中。双方の技術を組合せより精度を高める研究を進めている。

(4) 分散計測基盤

広域分散計測基盤について、双方で研究を進めている。

2008 年度は、10 月に東京でワークショップを開催し、研究の進捗報告や、学生交換の成果報告等を中心に発表を行ない、今後のスケジュールを確認した。また、2009 年 3 月には、本枠組で最後となるワークショップをフランス、トゥールーズで開催する予定である。

- 第 6 回 CNRS-WIDE ワークショップ
  2008 年 10 月 28–29 日 NII, Tokyo Japan.

また、2008 年度は以下の研究者交換を行なった。

- 慶應義塾大学村井研の学生空閑洋平君が 2008 年 7 月から 10 月まで LIP6 の Timur Friedman 教授の研究室を訪問。トポロジ探索手法について研究を行なった。
- 東京大学江崎研の学生肥村洋輔君が 2008 年 9 月に約 4 週間 ENS Lyon の Patrice Abry 教授の研究室を訪問。統計的なモデルに基づく異常トラフィックの検出手法について研究を行なった。
- フランス側計測グループのリーダである Kave Salamatian 教授が 8 月に約 3 週間日本に滞在して共同研究を行った。

以下はこれまでの日仏の共同執筆論文のリストである。

- Guilaume Dewaele, Kensuke Fukuda, Pierre Borgnat, Patrice Abry, Kenjiro Cho. Extracting Hidden Anomalies using Sketch and Non Gaussian Multiresolution Statistical Detection Procedures. ACM SIGCOMM2007

LSAD Workshop, Kyoto Japan. August 2007.

- Thomas Silverston, Olivier Fourmaux, Kave Salamatian, Kenjiro Cho. Measuring P2P IPTV Traffic on Both Sides of the World. CoNEXT Student Workshop, NY, NY. December 2007.
- Pierre Borgnat, Guilaume Dewaele, Kensuke Fukuda, Patrice Abry, Kenjiro Cho. Seven Years and One Day: Sketching the Evolution of Internet Traffic. To appear in IEEE INFOCOM 2009. Rio de Janeiro, Brazil. April 2009.

2008 年度は、共同研究の最終年度である。成果をまとめると同時に、今後もより活発な連係ができるような枠組を作る活動をしていく予定である。

4.4 まとめ

インターネットの計測研究では、国際的な協調による広域なデータ収集、しかも長期に渡る地道な努力が重要である。今後は、これまでに築いた関係をベースに、さらに協調の幅を広げると同時に、具体的な成果を出す努力をしていく。

第 5 章　WIDE-CNRS 間の交換留学活動報告 (1)

概要

WIDE プロジェクトおよび CNRS 間の学生交換として、東京大学大学院江崎研究室修士 1 年の肥村洋輔がÉNS Lyon に 1 ヶ月間、Patrice Abry らの下で研究活動を行った。研究内容はインターネットトラフィック分類手法の性能向上であり、この問題に対するアプローチとして、コネクションパターンを考慮した特徴量を用い、MST（Minimum Spanning Tree）クラスタリングによる分類を行った。その結果、コネクションパターンを考慮しないクラスタリングに比べて独立性の高いクラスタが得られ、また、未知のトラフィックグループを新たに発見することができ、コネクション構造を考慮した特徴量によって既存の分類手法の性能向上を行うことができた。

5.1 はじめに

WIDE プロジェクトの研究活動のひとつに、フランス国立科学センター（CNRS: Centre National de la Recherche Scientifique）との協力活動があり、その一環として両者は学生交換を行っている。本年度は、東京大学大学院江崎研究室修士 1 年の肥村洋輔が対象者の 1 人として、2008 年 9 月 1 日から 2008 年 9 月 30 日までの 1 ヶ月間、フランスのリヨンにおいて研究活動を行った。受け入れ先は、École Normale Supérieure de Lyon の Patrice Abry らの研究室である。Patrice は、同大学の Pierre Borgnat、Guillaume Dewaele とともに、WIDE プロジェクトメンバの長健二朗（IIJ 技術研究所）、福田健介（国立情報学研究所）との協力体制でインターネットトラフィック解析の研究を行っている。その中でもとくに異常トラフィック検出に焦点を当て、統計的なモデルにもとづく異常トラフィックの検出を行う手法 [38] を提案し、同手法の評価および検出トラフィックの解析を行っている。

本学生交換における研究トピックは、異常検出手法の性能評価・性能比較をさらに高精度に行うための、トラフィック分類手法に関する調査および実装・解析である。異常検出手法を評価するためには予め分類された（ラベル付けをされた）データが必要であるが、現在使用されている分類手法はポート番号および TCP フラグを用いた経験的な方法であり、総ホスト数（本レポートにおいてはホスト単位でトラフィック分類を行う）のうち 30%程度が未分類である。これらの未分類ホストは評価結果に多かれ少なかれ影響を与えるため、早急な性能向上が望まれている。この問題に対するアプローチとして、コネクションパターンを考慮した特徴量を採用し、MST にもとづくクラスタリング [197] を行うことで、新たな分類を試みた。この手法はポート番号に依存しない分類を行うため、現在使用している手法と相互に性能向上を行うことができる。結果として、コネクションパターンを考慮したトラフィック分類手法の有効性を確認することができ、既存の分類手法の性能向上を行うことができた。

5.2 成果

本研究において、分類性能向上のために 2 つの知見を利用した。それらは、(1) コネクションパターン

を考慮した特徴量および (2) MST クラスタリングである。

5.2.1 コネクションパターンを考慮した特徴量の発見

現在、提案されている統計的トラフィック分類手法が用いている多くの分類手法は、フローサイズや平均パケットサイズなどの “1 次元的” な特徴量を主に採用しているが、高い分類精度や未知トラフィックの発見などにおいて、十分な結果を出していないと考えられる。そこで、我々は “二次元的” な特徴量の発見のため、コネクションパターンを構造化して調査を行った。

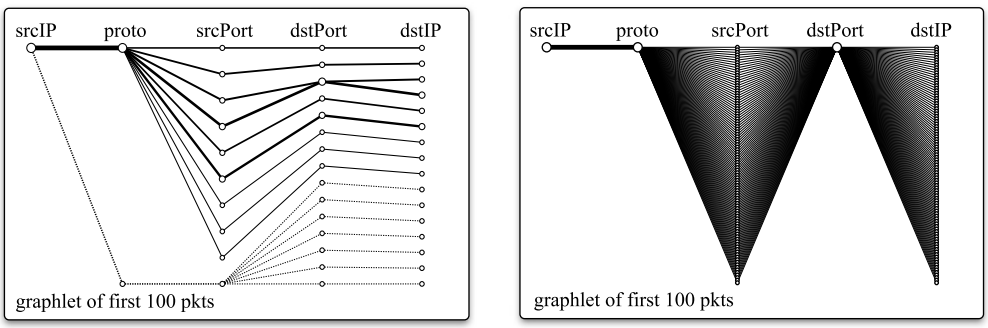
図 5.1 に構造化の例（1 つの送信元ホストに着目し、コネクションパターンの構造化を行った）を示す。ここで、srcIP は送信元 IP アドレス、proto はトランスポート層プロトコル、srcPort は送信元ポート、dstPort は宛先ポート、dstIP は宛先 IP アドレスを意味する。用いたデータは MAWI トラフィックレポジトリ [29] の 2007 年 09 月 16 日における 14:00 から 14:15 までのトラフィックであり、先頭の 100 パケット分のみを抽出して構造化および視覚化がなされている。また、付加的な情報として、線の太さおよびノードの大きさ（フローサイズ）およびフローの線種（コネクションの状態[1]）も視覚化した。ここで、図 5.1(a) におけるホスト（srcIP）は、P2P アプリケーションを用いていると考えられる。なぜならば、同ホストは 2 つのプロトコルを用い、通信相手は複数存在し、ポート番号は通信相手によって異なり、各フローはほぼ独立しているためである。一方、図 5.1(b) におけるホストは明らかに、送信元ポートを適宜変更しつつ水平ポートスキャン [116] を行っていると考えられる。

このように、各ホストのコネクションパターン構造を視覚化し調査を行った結果、コネクションパターンはホスト分類における重要な特徴量になり得ることが発見された。一方、これらの特徴は非常に直感的ではあるが、機械的分類用の特徴量としての抽出は未解決問題である。本報告書においては、機械的分類を行うための出だしとして、次の特徴量を選択する。

- (送信元ポート数)/(宛先 IP アドレス数)：この特徴量は、クライアント・サーバ型通信でのクライアントとしては 1 より非常に大きな値をとり、サーバとしては 0 に近い値をとる。一方、P2P 型通信では、1 に近い値をとると考えられる。
- (宛先ポート数)/(宛先 IP アドレス数)：この特徴量は、クライアント・サーバ型通信でのクライアントとしては 0 に近い値をとり、サーバとしては 1 より非常に大きな値をとる。一方、P2P 型通信では、1 に近い値をとると考えられる。
- (宛先 IP アドレス数)/(総パケット数)：この特徴量は、ポートスキャンであれば 1 に近い値をとり、それ以外では 0 に近い値をとると考えられる。

5.2.2 MST クラスタリング

クラスタリングは、特徴量の類似度が高いもの同士をグループに分ける操作であり、特徴の隠れた構造を発見することができる。本学生交換においては、MST（Minimum Spanning Tree）を用いるクラスタリング手法 [197] に着目した。この手法は、代表的なクラスタリング手法である K-means 法 [49] な



(a)　(b)

図 5.1.　コネクションパターン構造化の例：(a) P2P トラフィック、(b) ポートスキャン

1　実線：TCP フローである、点線：UDP フローである、破線：ICMP フローである。実際には色を用いてコネクション成立の可否などの情報も視覚化している。

どとは異なり、クラスタ内のデータ数およびクラスタの形状に依存せず、ノイズに強いロバストなクラスタリングを行う。そのため、特徴量空間に複雑な構造を持つインターネットトラフィックに対するクラスタリング手法として、本手法が適切であると考えられる。

図 5.2 に MST クラスタリングの例を示す。クラスタリングの流れは次のようになる：

(a) 特徴量空間にホストの持つ特徴量をプロットする。

(b) 全てのホストをエッジで結合する。このとき、エッジの総距離が最小かつ木にループがないように結合する。

(c) 距離が閾値以上のエッジを切断する。その結果、複数のホスト群（クラスタ）を見つけることができる。

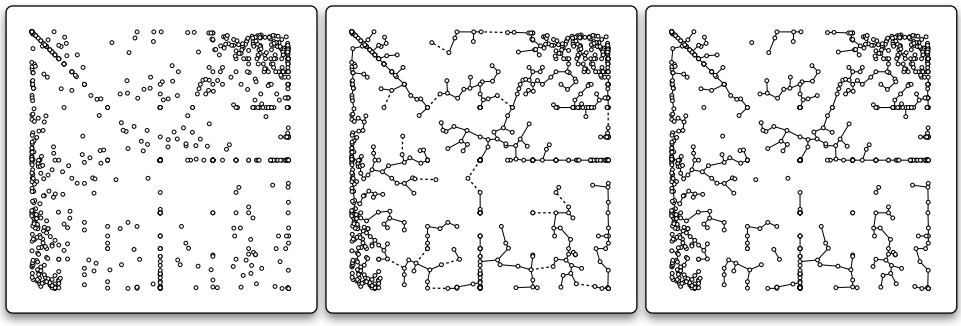
図 5.2 では 2 次元特徴量空間による例であるが、実際には以下の 8 つの特徴量を用いてクラスタリングを行った。

(1) (送信元ポート数)/(宛先 IP アドレス数)
(2) (宛先ポート数)/(宛先 IP アドレス数)
(3) (宛先 IP アドレス数)/(総パケット数)
(4) スモールサイズパケットの割合
(5) ラージサイズパケットの割合
(6) H (ミディアムサイズパケットのパケットサイズ)
(7) (H(IP[3]))/(H(IP[4]))
(8) (H(IP[2]))/(H(IP[4]))

ここで、H(x) は “変数 x の分布のエントロピー”、IP[n] は “IP アドレスの n オクテット目” を表す。また、スモールサイズパケットおよびラージサイズパケットとは、全長がそれぞれ 144 バイト未満および 1400 バイト以上のパケットを指し、ミディアムサイズパケットは先述した条件に当てはまらないパケットを指す。なお、距離としてユークリッド距離を採用するが、特徴量の値域はそれぞれ異なるため、適宜正規化を行っている。

8 次元特徴量空間におけるクラスタリング結果の一例を、表 5.1 に示す。列はポート番号にもとづく分類結果、行はクラスタリングによる分類結果である。用いたデータセットは、2007 年 9 月 16 日のデータ（15 分）である。このクラスタリングにより得られた結果は、以下の 2 点である：

- 2 手法間のクロスバリデーション：表 5.1 は、ポート番号にもとづく分類手法およびコネクションパターンにもとづく分類手法による分類結果を比較したものである。表 5.1 によると、これらの手法は概念の大きく異なる手法であるにもかかわらず、各クラスタの独立性が高いことが理解できる。これは、両手法の妥当性・信頼性を高めるだけではなく、各手法の分類ミスを検出することにおいても有効である。
- 未知トラフィックの新たな識別：ポート番号にもとづく分類手法では分類できなかったホスト（表 5.1 における未分類カテゴリのホスト）は、クラスタリングによって複数のクラスタに分かれている。未分類ホストを特徴に応じて分類することで、人間による精査を効率的にするだけではなく、同クラスタの他のカテゴリのホストとの比較により、類似したアプリケーションを判断する際に有効である。



(a) (b) (c)

図 5.2. MST クラスタリングの例：(a) 特徴量空間へのプロット、(b) MST の決定（点線は距離が一定値以上のエッジ）、(c) クラスタの決定

表 5.1.　8 特徴量によるクラスタリング結果

クラスタ No.	合計	HTTP サーバ	HTTP クライアント	SCAN	DNS	その他	未分類
1	173	0	104	0	3	5	61
2	58	0	52	0	2	2	2
3	46	0	23	0	2	4	17
4	42	0	0	0	37	1	4
5	39	37	0	0	0	0	2
6	24	0	0	0	24	0	0
7	18	0	0	18	0	0	0
8	16	0	0	12	0	2	2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

5.3 評価

コネクションパターンを考慮した特徴量 (1)、(2)、(3) を取り入れたことによるクラスタリングの有効性を示すために、これらの特徴量がある場合とない場合のクラスタリング結果を比較する。ここで、特徴量数を増加させると必ずしも精度が上がるわけではなく、逆に性能を低下させる恐れがあることに注意されたい。表 5.1 は 8 特徴量におけるクラスタリング結果、表 5.2 は上記特徴量を除いた 5 特徴量におけるクラスタリング結果である。評価に公平性を持たせるために、総クラスタ数が同程度になるようにクラスタリングを行い、ホストが多い順にクラスを並べ替えた。なお、現在は定性的な評価のみを行うこととする。なぜならば、クラスタリング評価において一般的に用いられている指標 (F 尺度、エントロピー、相互情報量など) は本結果に用いることは不適切である。これらの尺度はクラスタの独立性・完備性に主眼が置かれているが、本研究の目的は (1) 未分類ホストを分類するための解析および (2) 同カテゴリ内の新たな構造発見であるため、クラスタの独立性および完備性は必ずしも必要とならない。

表 5.1 と表 5.2 を比較した時、とくにクラスタ 2 において表 5.1 が直感的にも適切なクラスタリングが行われていることが分かる。なぜならば、表 5.2 では、HTTP クライアント、DNS サーバ、ポートスキャナという、比較的容易に分類できるホストが同一クラスタに属しているためである。また、同クラスタの未分類カテゴリを精査したところメールサーバのトラフィックが多く見られた。これら 4 種類のホストは、表 5.1 では、クラスタ 2、4、7、12 にそれぞれ表れている。これらは、コネクションパターンを考慮した特徴量を追加したことにより、分類が可能となったといえる。図 5.3 に、各ホストの代表的なコネクションパターンを示す。各トラフィックは異なるコネクション構造を持つことが明らかである。

この分類方法は、コネクションパターンを考慮するという点において BLINC[93] がとっている方法に類似している。しかし、BLINC はルールにもとづく分類方法に主眼が置かれているため、(1) ロバ

表 5.2.　5 特徴量によるクラスタリング結果

クラスタ No.	合計	HTTP サーバ	HTTP クライアント	SCAN	DNS	その他	未分類
1	243	1	134	1	10	15	82
2	146	0	39	14	46	8	39
3	55	52	0	0	0	0	3
4	20	0	0	0	0	1	19
5	17	0	0	17	0	0	0
6	17	12	0	0	0	0	5
7	16	0	4	0	0	9	3
8	9	1	1	1	6	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

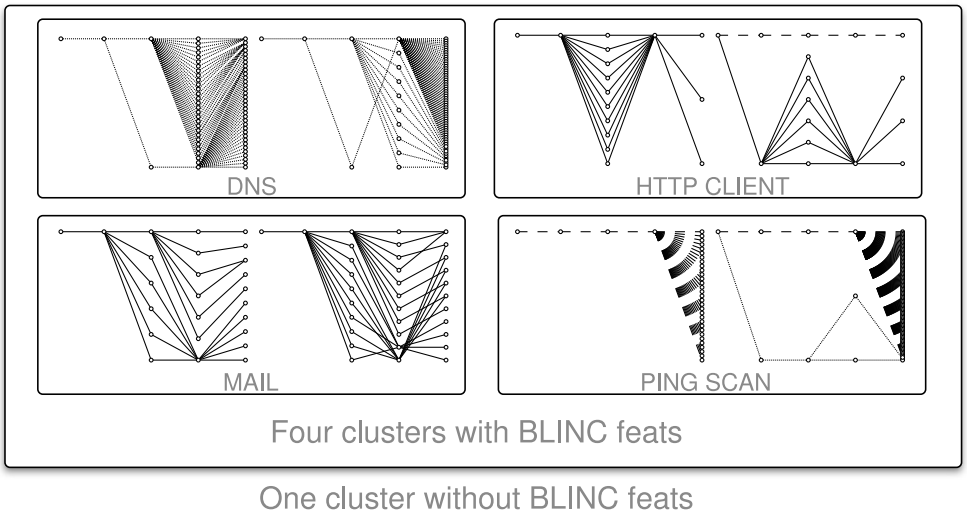


図 5.3. コネクションパターン特徴量による出現した新たなクラスタ

ストな分類および (2) 未知トラフィックの新たな識別を行うことができないと考えられる。これに対して、本手法はクラスタリングにもとづく教師なし学習を行うことで、上記二点の問題を解決できている。

5.4 今後の課題

定量的評価：本報告書において定性的評価を行った理由は、F 尺度およびエントロピーなどの広く一般的に用いられているクラスタリングの評価指標は我々の意図に即さず、本研究の評価として適切ではないためである。今後は的確な評価を与える指標を開発し、定量的評価を行う必要があると考えられる。

特徴量の再検討：今回はコネクションパターン構造を表す特徴量として、(1) 送信元ポート数と宛先ホスト数の比、(2) 宛先ポート数と宛先ホスト数の比、(3) 宛先ホスト数と総パケット数の比を用いた。これらの特徴量は統計的分類を行う上で強力であることを確認できたが、コネクションパターンを的確に記述する上では不十分である。なぜならば、フローサイズおよび TCP コネクションの成立・不成立などを考慮していないためである。今後は、これらの状態を的確に記述する特徴量の調査および分類への応用を行う必要があると考えられる。また、特徴量の正規化方法についても検討を行う必要がある。

クラスタの更なる精査：クラスタリングにより、統計的特徴の類似したホストに分類することができた。今後は、とくに未分類クラスタのホストを調査することにより、未知ホストの解明および新たな経験則の追加について研究を行う。

トラフィックデータベースの構築：トラフィック分類を行う上で発見できる多種の知見をデータベースとして体系的にまとめ、トラフィック解析に携わる研究者を主として広く公開する。

5.5 まとめ

本学生交換で行った研究活動は、インターネットトラフィック異常検出手法のより信頼性の高い評価のためのトラフィック分類手法の向上である。この問題に対するアプローチとして、(1) コネクションパターンを考慮した特徴量を発見し、(2) MST（Minimum Spanning Tree）クラスタリングによる分類を行った。その結果、コネクションパターンを考慮しないクラスタリングに比べて、独立性の高いクラスタが得られ、また、未知のトラフィックグループを新たに発見することができ、コネクション構造を考慮した特徴量の有効性を確認するとともに、分類手法の性能向上を行うことができた。

第 6 章　WIDE-CNRS 間の交換留学活動報告 (2)

6.1 概要

WIDE プロジェクトとフランス国立科学研究センター（CNRS）の間での研究協力の一環として、両組織間で人的交流・学術的交流を目的とした、学生の交換留学制度を設けている。慶應義塾大学大学院村井

研究室修士 2 年の空閑洋平は、本プログラムの交換留学生として、2008 年 7 月 20 日から 2008 年 10 月 13 日までの約 3 ヶ月間、フランスのパリで現地の研究活動に参加した。受け入れ先は、LIP6 (Laboratoire d'Informatique de Paris 6) [2] の Timur Friedman らの研究室である。滞在中は、Timur らによるインターネットトポロジの計測と解析を目的とした TopHat プロジェクトに参加し、本グループのメンバである Thomas Bourgeau と共に本システムのアーキテクチャについて、議論と実装を行った。

TopHat プロジェクト [180] は、2008 年に始まった研究プロジェクトであり、現在も基盤アーキテクチャの議論とシステムの研究開発が続いている。今後は、引き続き Timur 指導の元で TopHat の研究グループに参加していく予定であり、研究プロジェクト間の交流を続けていく。

本報告書では、はじめに第 6.2 項で滞在中参加した TopHat グループの概要を述べる。次に、第 6.3 項では、ネットワーク環境に協調したトポロジ探索手法と現在の進捗、そして、今後の作業予定を述べる。第 6.4 節では、ユーザへのトポロジ情報の提供システムについて述べる。最後に第 6.5 項では、本交換留学のまとめを述べる。

6.2 TopHat

滞在中、私は Timur らが活動している OneLab プロジェクト [137] の複数ある研究グループのうち、大規模にインターネットトポロジ情報の収集と解析、そして、収集したトポロジ情報をユーザへ提供するシステムを研究開発している TopHat のグループに参加した。OneLab は、次世代インターネットのテストベット環境構築を目的として、PlanetLab[143] の普及と高度化を進めているヨーロッパ圏の研究グループである。実際に、TopHat グループでは、PlanetLab 上に計測環境を構築し、トポロジデータの収集を開始している。

滞在時、TopHat グループでは、ネットワーク環境に協調したトポロジ探索手法の検討とユーザへのトポロジ情報の提供システムの開発を開始した状況であった。前者の計測手法については、DoubleTree[42] と呼ばれるトポロジ探索アルゴリズムを提案している。また、計測基盤のアーキテクチャは、Timur らが過去に構築したシステムである traceroute@home[179] のアーキテクチャをもとにして構築されている。本アーキテクチャは、PlanetLab 上に計測ノードを配置し、計測ノード間の情報共有に WIDE プロジェクトのメンバである益井賢次氏が研究開発している N-TAP[178] を採用している。滞在中は、TopHat のトポロジ探索手法の検討とユーザへのトポロジ情報の提供システムを担当して作業した。

6.3 トポロジ計測手法

本留学では、はじめに TopHat の計測基盤アーキテクチャの理解と議論を行った。具体的には、Timur らの論文と実際に動作している TopHat のコードを参照し、TopHat の Problem statement をまとめた。その上で、滞在中の後半では、トポロジ情報の提供システムを担当して、*StitchRoute* アルゴリズムの提案と実装を行った。

本節は、*StitchRoute* アルゴリズムを説明するために必要である TopHat の計測機能である DoubleTree アルゴリズムを述べる。*StitchRoute* については、次節で扱う。

6.3.1 DoubleTree アルゴリズム概要

TopHat はインターネット上に分散配置された PlanetLab 上のノードがそれぞれ traceroute を用いてトポロジ情報を収集し、得られた情報を統合することで、インターネット全体のトポロジ情報を探索する。このような、インターネット全体のトポロジを複数の計測ノードから分散して探索する手法は、他の研究プロジェクトでも採用されている一般的なトポロジ探索手法である。しかし、複数の計測ノードを用いた手法は、探索パケットが重複した経路や同一の宛先ノードを対象とすることで、探索途中のネットワークに対して、高負荷をかける恐れがある。また、重複して経路を探索するため、1 回のトポロジ探索により多くの時間を消費する。

図 6.1 にインターネット上のノードに対して、高負荷をかける状況を示す。左図では、同一ネットワーク上に複数存在する計測ノードからトポロジ情報を探索した結果、イントラドメインの共通する経路を重複探索している。これらの計測ノードから同一のタイミングでトポロジ探索することで、対象ルータに対して必要以上の負荷をかける恐れがある。また、右図では、分散した計測ノードから、同一の宛先ノードを対象にトポロジ探索することで、宛先ノードとその近くのネットワークを重複探索している。

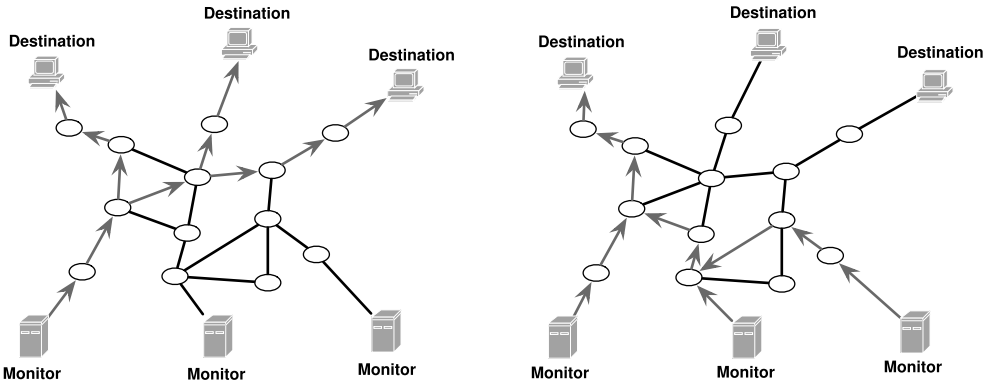


図 6.1. DoubleTree の扱うトポロジ計測時の問題点

DoubleTree は、計測ノード間で *Stop set* と呼ばれる探索した経路の情報を共有することで、このような重複経路の探索を排除する探索アルゴリズムである。それにより、大規模に展開されるインターネットのトポロジ情報を既存の手法に比べて素早く、また、探索対象のネットワークを構成するノードの負荷を削減できる。

6.3.2 DoubleTree によるトポロジ探索

DoubleTree によるトポロジ探索手法を述べる。DoubleTree では、traceroute と同じように IP パケットの TTL 値を漸増させることで、計測ノードと宛先ノード間のトポロジ情報を収集する。traceroute との違いは、計測開始時の TTL 値である。計測開始時に、TTL 値 h で計測を開始する。探索は、TTL 値を $h+1, h+2, \ldots$ と漸増させながら宛先ノードまでの経路を探索する *Forward probing* と、TTL 値を $h-1, h-2, \ldots$ と漸減させながら計測ノードまでの逆向きの経路を探索する *Backward probing* を交互におこなう。それにより、経路の中央近くから末端のノード方向へ探索していく。TTL の初期値 h の選定には、事前に計測した任意の 2 ノード間における直接応答された確率 p をもとに決定している。また、計測ノード間で探索済みのトポロジ情報を共有することで、重複した経路を探索しないよう調整する。*Forward probing* と *Backward probing* を実行する際、毎試行時に *Stop set* を参照することで、重複探索を判断する。*Forward probing* では、*Global*

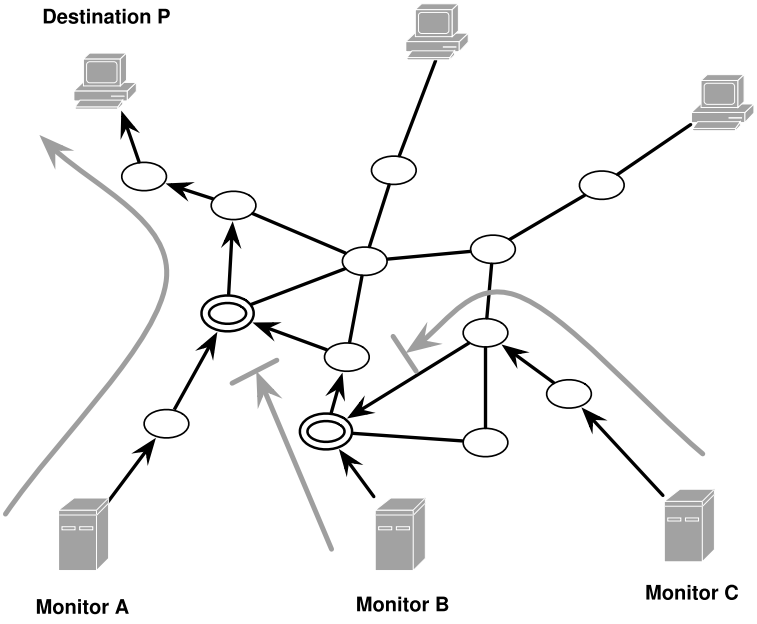


図 6.2. DoubleTree 動作概要

Stop Set と呼ばれるインタフェース IP アドレスと宛先 IP アドレス、計測ノードから成るデータを用いて判断する。*Global Stop Set* は、計測ノード間で共有される。探索は、*Forward probing* の毎試行時に *Global Stop Set* を参照する。*Global Stop Set* 内から計測ノード自身の宛先 IP アドレスと直前に発見したインタフェース IP アドレスのペアを発見した場合、探索を停止する。一方、*Backward probing* では、*Local Stop Set* と呼ばれるインタフェース IP アドレスのデータから判断する。*Local Stop Set* は、各計測ノードのみで参照され、共有しない。

図 6.2 に DoubleTree の動作概要を示す。計測ノード（Monitor）A、B、C から宛先ノード（Destination）P に対して DoubleTree を用いてトポロジ情報を収集する。TTL の初期値は $h = 2$ とする。

(1) 計測ノード A から P までの経路を探索する。A は、探索した経路情報を *Global Stop Set* として保存し、さらに A、B、C 間で共有する。

(2) 計測ノード B が宛先ノード P までの経路を探索する。B は、A と同様に TTL 値 $h = 2$ から探索を開始する。B の *Forward probing* は、探索途中で *Global Stop Set* から、すでに A が発見した重複経路部分を発見し、探索を停止される。

(3) 計測ノード C が宛先ノード P までの経路を探索する。C は、B が発見済みの経路までを探索する。

6.3.3 現状と今後

現在、TopHat グループでは、PlanetLab 上で DoubleTree を用いたトポロジの探索を開始している。今後の予定は、インターネット上の経路ループやロードバランスされた経路の検出に対応する目的で、Paris-traceroute による経路探索手法の置き換え作業を行う。

また、グループでは、DoubleTree の TTL 初期値 h の決定方法や、計測結果の提示方法についての議論を続けている。DoubleTree で発見されるトポロジの情報量は、TTL の初期値 h で大きく変動するためである。今後は、実際に TopHat システムで収集したトポロジ情報を解析することで TTL 値を検討し、計測手法を改善していく予定である。

6.4 StitchRoute

滞在中行った作業は、第 6.3 節で述べた計測手法についての議論に加え、本システムの基幹機能である任意の IP アドレス 2 点間の経路を返答する機能を検討し、実装した。以後、本機能を *StitchRoute* とよぶ。

TopHat グループでは、traceroute@home から続くトポロジ計測基盤アーキテクチャの機能をほぼ実装し、実際にトポロジ計測をはじめている。次のステップとして、TopHat グループでは、収集したトポロジ情報を一般ユーザに提供するアーキテクチャを検討している。本システムは、ユーザの XML-RPC によるリクエストに応答する手法で任意の 2 点間の IP アドレスまたは AS 番号の経路情報を提供することを考えている。

6.4.1 目的

StitchRoute の目的を述べる。本機能は、TopHat が収集した経路の断片（*piece* とよぶ）をつなぎ合わせることで、任意の 2 点間の IP アドレス間の経路を算出するものである。

用語を定義する。計測ノードから宛先ノードまでの完全な経路は、$\mathbf{r} = (r_0, r_1, r_2, \ldots, r_\ell)$ と定義する。r_0 は、ある計測ノードのソース IP アドレスであり、それぞれの値である r_i、$i > 0$ は、ホップ i ごとで発見されたインタフェース IP アドレスである。r_ℓ は、宛先 IP アドレスである。次に、*piece* は、$\mathbf{p} = (p_0, p_1, p_2, \ldots, p_\ell)$ と定義する。p_0 は、*piece* の先頭 IP アドレスであり、p_ℓ は、*piece* の末尾の IP アドレスである。p_0 と p_ℓ は、*Stop set* で経路探索が終了している可能性があるため、必ずしもそれぞれ、計測ノードと宛先ノードの IP アドレスとは限らない。この時、*StitchRoute* の目的は、ユーザのリクエスト (S, D) に対して、$\mathbf{p} = (p_0, p_1, p_2, \ldots, p_\ell)$ をつなぎ合わせ、$\mathbf{r} = ((p_{0\_0}, \ldots, p_{0\_\ell}), (p_{1\_0}, \ldots, p_{1\_\ell}), \ldots, (p_{n\_0}, \ldots, p_{n\_\ell}))$ を返答することである。S は *source*、D は destination を表す。

6.4.2 背景

StitchRoute が必要となる背景を述べる。TopHat では、DoubleTree アルゴリズムを用いて、ネットワークに協調したトポロジ探索の計測基盤を構築した。TopHat では、通常の traceroute の結果と異なり、計測した経路を断片化された状態でシステム内部で保持する。*piece* は、DoubleTree による経路探索がすでに発見した重複経路で探索を中止するために発生する。

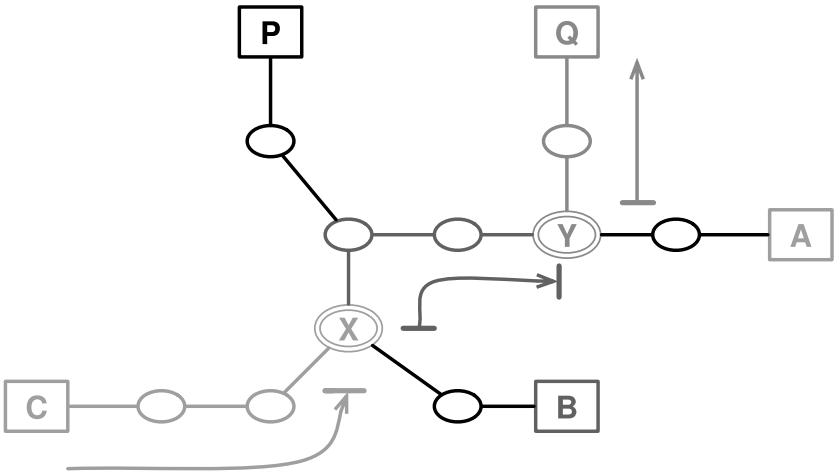


図 6.3. DoubleTree による探索経路の断片化

図 6.3 に経路が断片化される様子を示す。計測ノード A、B、C は、宛先ノード P、Q に対して初期 TTL 値 $h = 3$ で経路を探索する。はじめに P に対して経路を探索する。この時点で、各計測ノードは、*Local Stop Set* を持つ。次に、宛先ノード Q に対して経路探索する。計測ノード A は、自身の *Local Stop Set* を参照することから、YQ 間の経路で探索を終了する。計測ノード B は、自身の *Local Stop Set* と、計測ノード A と共有して得た *Global Stop Set* を参照し、XY 間の経路のみを探索する。計測ノード C は、すでに CQ 間の経路探索が終了していることから、初期探索のみ実行し、探索を終了する。本図の状況で収集したトポロジ情報から CQ 間の経路を知るには、計測ノード C が探索した CX の経路情報と計測ノード B が探索した XY の経路情報、そして計測ノード A が探索した YQ 間の経路をつなぎ合わせる必要がある。

6.4.3 piece

TopHat では、ユーザからのリクエストに応答するため、事前に計測した *pieces* を細分化した、ホップ間における IP アドレスのペアをシステムで保持する。細分化したデータ構造は、$(s_n, d_{q+1}, star)$ であり、本データを *piece* とよぶ。それぞれ、s は *source*、d を *destination*、*star* は *source* と *destination* 間において、応答パケットの返信が無かったことを意味する *no replay* の数を表す。*star* の初期値は 0 であり、dst_{q+1} が *no replay* である場合に *star* の値を漸増し、dst_{q+2} を *destination* とする。また、ロードバランスされたネットワークでは、経路探索時に、同一の TTL 値で複数 IP アドレスから返答される場合がある。このようなトポロジデータは、返答された IP アドレスの数だけ *piece* に分解する。

6.4.4 アルゴリズム

図 6.4 に *StitchRoute* アルゴリズムを示す。*StitchRoute* アルゴリズムは、*piece* をつなぎ合わせることで、経路 **r** を探索する。本手法は、traceroute によるインターネットトポロジの探索が、計測ノードを根ノードとした木構造の深さ優先探索することに注目する。TopHat 内のデータ探索には、反復深化深さ優先探索（iterative deepening depth-first search: IDSearch）を採用した。単純な深さ優先探索のみでは、経路ループがデータ内に含まれる場合に探索が終了しない恐れがある。また幅優先探索では、より多くのメモリを消費することから、探索深度を 1 から漸増させながら深さ優先探索する IDSearch を採用した。

6.4.5 今後の予定

StitchRoute は、滞在中に実装作業を行った、今後、実際に TopHat が収集したトポロジ情報を用いて、実行時間を計測する予定である。

6.5 まとめ

WIDE プロジェクトと CNRS 間の交換留学生として渡仏し、現地の研究プロジェクトに参加した。滞在中は、Timur 指導の元、インターネットトポロジの計測と解析を目的とした TopHat プロジェクトに参加し、本グループのメンバである Thomas Bourgeau

```
1: procedure StitchRoute(S, D)                          ▷ source, destination
2:     i ← 1
3:     loop
4:         F̂ ← IdSearch(i, S)
5:         if F̂ ∩ D then
6:             response                                  ▷ Output
7:         else if |F̂ ∩ B̂| > 0 then
8:             response                                  ▷ No output
9:         end if
10:        i ← i + 1
11:    end loop
12: end procedure

13: procedure IDSearch(l, P)                            ▷ limit, Path
14:    n ← |P|
15:    m ← P_ℓ
16:    L̂ ← ∅
17:    if n = l then
18:        L̂ ← L̂ ∪ {P_ℓ}
19:    else
20:        for all c ∈ Adjacent(m) do
21:            if c ∩ P = ∅ then
22:                P ← P ∪ {c}
23:                IdSearch(l, P)
24:                P ← P − {P_ℓ}
25:            end if
26:        end for
27:    end if
28: end procedure
```

図 6.4. Stitchroute algorithm

と共に本システムのアーキテクチャについて、議論と実装を行った。現地での TopHat グループに参加しての作業は、今後も続けていく予定であり、研究協力関係はこれからも継続される。

第 7 章　Meta-data format and associated tools for communicating PCAP analysis results

7.1 Background

To date, many engineers and scientists have been working on PCAP files, yet we did not have any effective means to communicate what we have found. In other words, we are still in the dark ages of data analysis in this field, since the result of analysis cannot be communicated and compared with each other.

This is typically problematic in the cyber-security context, since many scientists have been working on common datasets (e.g., the MAWI traffic archive) to locate anomalies, without being able to further validate their results with each other. Since real-world datasets do not have "correct class label" in most cases, relative comparison among multiple anomaly detection algorithms seems to be best alternative approach to improve their accuracy.

7.2 Common meta-data format for PCAP analysis

Here we consider adopting common meta-data format across different analysis techniques. If different analysis techniques can produce compatible

mark-ups against the same dataset, we can compare their results without translating or converting the mark-ups.

There are lots of potential benefits that we can obtain from common meta-data format. More specifically, there are four kinds of direct beneficiaries, as described below.

Algorithm designers will benefit from the common meta-data format since their results will be made comparable among adopting parties. In addition, they will be freed from developing in-house data format to store the analysis result. Furthermore, they will benefit from additional tools built around the common meta-data format, e.g., tools for synthesizing datasets out of known anomalies and background traffic.

Cybersecurity researchers and practitioners will benefit from the meta-data format, because they will be able to benchmark multiple anomaly detection algorithms against the same dataset, without being involved in time-consuming data conversion process. In addition, they may choose to communicate their own analysis results in the same format, giving feedback to algorithm designers.

Tool implementers will benefit from existing common meta-data definition and associated class libraries. Also, they can test their newly developed tool against existing real data.

Dataset repository maintainers will benefit from common meta-data format, since it enriches the scientific value of shared dataset repository. The common meta-data format simplifies management of secondary data. It also helps analysts to document essential information for reproducible analysis; e.g., relationship of secondary data with original PCAP data, and parameters given to particular algorithm.

7.3 ADMD schema

As a starting point of meta-data format, XML Schema for annotating the result of analysis is made available[2], which we call ADMD (Anomaly Detection Meta-Data), along with C and C++ API to annotate PCAP dataset according to the XML Schema. PCAP data analysis programs are supposed to use either C or C++ API to represent the result of analysis in the ADMD XML Schema. Data analysis programs written in other languages such as Java or Perl can also be supported through native-code wrappers.

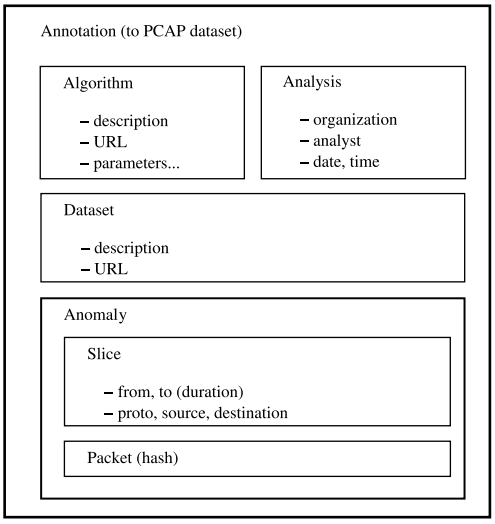


Fig. 7.1. Outline of ADMD schema

The primary focus of this XML Schema is content (annotated results) and reproducibility (algorithm description and parameters). The envelope information of each PCAP dataset, e.g., date and observation point, should be better described by CAIDA's DatCat tools. This tool focuses more on individual record or flow in PCAP datasets.

The concise XML Schema currently consists of 8 data types, in 80 lines. The data types are organized in hierarchical manner, as depicted in Figure 7.1.

7.4 PCAP manipulation and validation tools

A set of toolchain is provided to 1) manipulate PCAP datasets according to mark-ups, and 2) compare anomaly detection results. They are described in the following.

`admd_slice` takes annotated result of analysis, represented in XML, and emits matching slice of the input PCAP file into the output PCAP file.

`admd_merge` takes annotated result of analysis,

2 `http://admd.sourceforge.net/`

then injects matching slice of the second PCAP file into first PCAP file with the specified time offset, generating the output PCAP file.

`admd_validate` takes a PCAP file and a set of annotated analysis results in XML. It is intended to compare the performance of variety of algorithms.

7.5 Next steps

We have been working with algorithm designers to improve the proposed ADMD schema and toolchain. We are looking forward to see more scientists, who will benefit from public PCAP dataset and existing secondary datasets that are created through ADMD.

We are also looking into collaboration with cybersecurity researchers and practitioners by developing more operator-friendly interfaces. We already have minimal, Eclipse-based environment for editing ADMD-compliant annotations.

In near future, we will have to work with Dataset repository maintainers for general issues pertaining to archival of secondary data, e.g., naming conventions.

第 8 章　まとめ

インターネットの研究において、計測はますます重要視されてきていて、国際協調の機会も増している。そのような状況のなかで、WIDE の計測活動は、グローバルな視点を持った継続的な計測活動として国際的にも認知されてきている。2009 年度は、国際協調を実りある研究に結びつける事を目標に置いている。