第 III 部

ネットワークトラフィック統計情報の収集と解析

第 3 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 ワーキンググループについて

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 ワーキンググループでは 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 プロジェクト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 プロジェクト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 ワーキンググループと共同）
- 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 ワーキンググループと共同）
- 長期的な経路変動の観測（routeview ワーキンググループと共同）
- sFLow/NetFlow を使ったトラフィック計測（roft ワーキンググループと共同）
- AIII の衛星トラフィックの計測（ai3 ワーキンググループと共同）

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 ワーキンググループ 2006 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、例年のように集約型トラフィックプロファイラを使った国際線トラフィックの傾向を報告する。このツールは、WIDE バックボーンのトラフィックをニアリアルタイムかつ長期的にモニタリングする目的で 2001 年に開発され、それ以来利用されてきている。また、急増する分散型 DoS アタックの早期検出にも役立っている。特に、今年度は 7 月に WIDE の主要国際線および US でのトランジット AS が変更になったため、その前後のトラフィック傾向の変化を中心に報告する。

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 プロジェクトでは、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 章では、CNRS のパリ第六大学に交換留学した奈良先端科学技術大学院大学の益井君が留学中の活動について報告する。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 6 章では、ダイヤルアップを使った Root DNS サーバ群の計測について、今年度はアジア地域からの測定に的を絞って行なったので報告する。結果から、ほとんどの観測点で RTT 100 ms 以下の Root サーバが複数観測され、Root DNS サーバで採用されている BGP anycast がアジア地域で有効に機能している事が確認された。

第 3 章　WIDE 国際線のトラフィック傾向

3.1 はじめに

WIDE インターネットのような広域なネットワークを運用し続けていくためには、トラフィックモニタリングを多地点、かつ長期間行い、ネットワークの現状に適した通信機器の設置、設定を行う必要がある。

しかし、現存するネットワークモニタリングツールは長期に渡ってトラフィックの傾向を収集し続けることが難しい。

そこで、WIDE プロジェクト/mawi ワーキンググループでは収集したトラフィックを効果的に集約することによって、ネットワークの特徴を抽出することのできるトラフィックモニタリングツール AGURI[32] の設計、実装を行った。

AGURI（Aggregation-based Traffic Profiler）は、1) トラフィック中の特徴的なフロー傾向を残しつつ、2) 短期間から長期間に渡って利用可能なトラフィックモニタリングツールである。

AGURI は以下に示す 4 種類のネットワークサマリ情報を作成する。

- 送信元 IP アドレス
- 受信先 IP アドレス
- IP バージョン＋プロトコル＋送信ポート番号
- IP バージョン＋プロトコル＋受信ポート番号

この 4 種類のネットワークサマリを定期的に出力することによって、ある短時間のネットワーク状態の特徴を知ることができる。

さらに、AGURI は一度 AGURI で作成したネットワークサマリからもデータを入力することができ、複数のサマリを同時に入力することもできるので、ある短時間のサマリを組み合わせて AGURI に入力することによって、可変長の時間のネットワーク状態の特徴を知ることができる。

WIDE プロジェクトでは 2006 年 7 月に国際線の契約変更、収容変更を行なった。今年度の報告書では、国際回線の変更以前、以降のトラフィック状態の比較を行なう。

3.2 収集データ

WIDE プロジェクトで利用している 2 本の国際線のうち、1 本は他 AS と BGPpeer を張っている地点において WIDE インターネットの入り口側でデータ収集を行っている（samplepoint1）。

他の 1 本は WIDE プロジェクトの利用している国際線日本側（samplepoint2）でそれぞれデータ収集を行っている。

以下に示す 2 地点において国際線のデータを収集している。

1. samplepoint1　trans-Pacific line (18 Mbps CAR on 100 Mbps link)
2. samplepoint2　US-Japan line (100 Mbps transit)
3. samplepoint3　US-Japan line (Japan side 60 Mbps POS)

2006 年 7 月の国際線の契約変更、収容変更では、transit を 18 Mbps CAR on 100 Mbps link から、100 Mbps transit への変更が行なわれた。そのため、今年度の報告書では、samplepoint1 の 4、5、6 月のトラフィックデータと 10、11、12 月のトラフィックデータの比較を行なう。

以降、samplepoint1 における 4、5、6 月のトラフィックデータを ‘移行前データ’、samplepoint2 における 10、11、12 月のトラフィックデータを ‘移行後データ’ とする。

移行前データ、移行後データとも、IN/OUT を合計したトラフィック量を示している。

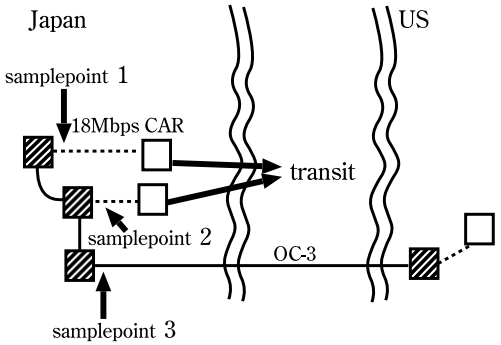

図 3.1.　データ収集地点

3.3 収集データ

移行前、移行後データを図 3.2 から図 3.9 に示す。

移行前､移行後のトラフィック総量を比較した場合、

表 3.1. トラフィック傾向一覧表

	移行前	移行後
宛先 IP アドレス	図 3.2	図 3.3
送信元 IP アドレス	図 3.4	図 3.5
宛先ポート番号	図 3.6	図 3.7
送信元ポート番号	図 3.8	図 3.9

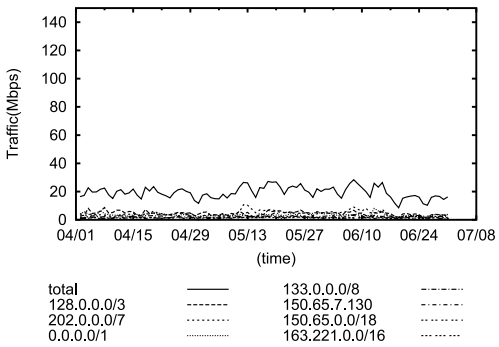

図 3.2. 移行前宛先 IP アドレス

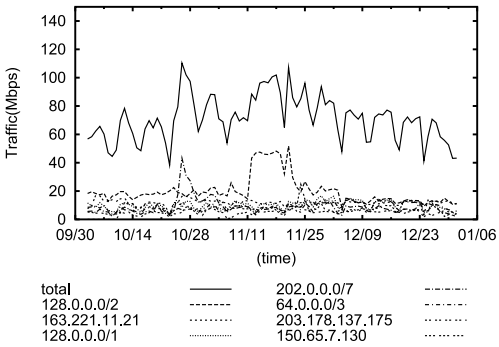

図 3.3. 移行後宛先 IP アドレス

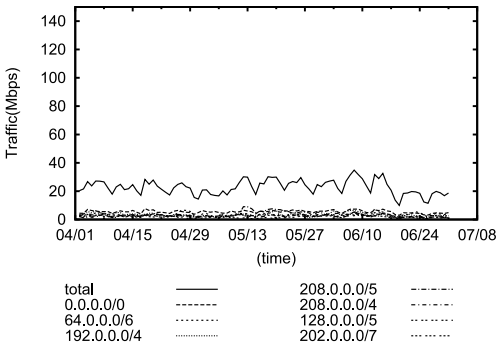

図 3.4. 移行前送信元 IP アドレス

移行前のトラフィック量は平均 28.10 Mbps であるのに対し、移行後のトラフィック量は、平均 78.32 Mbps に増加している。アドレス毎、プロトコル毎のトラフィック傾向の変化を分析した上で、移行に伴うトラフィック量の変化に関して考察を行なう。

図 3.2 から図 3.9 に示した長期的トラフィック傾

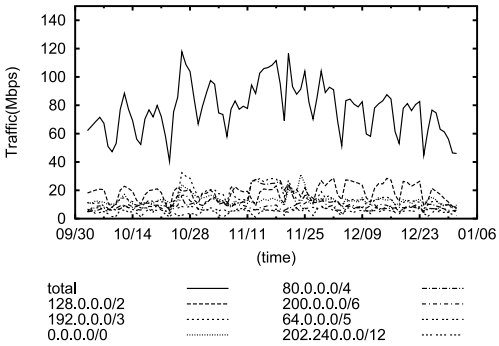

図 3.5. 移行後送信元 IP アドレス

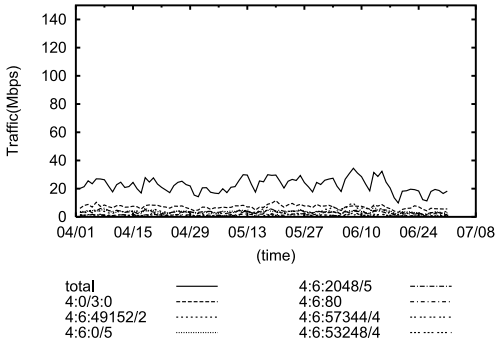

図 3.6. 移行前宛先ポート

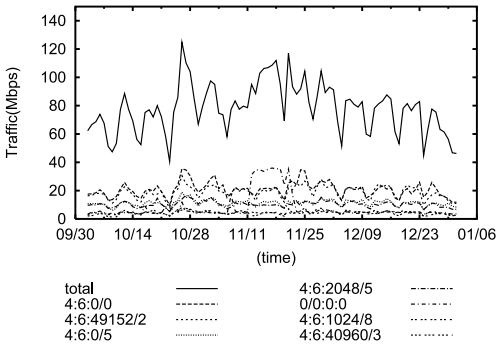

図 3.7. 移行後宛先ポート

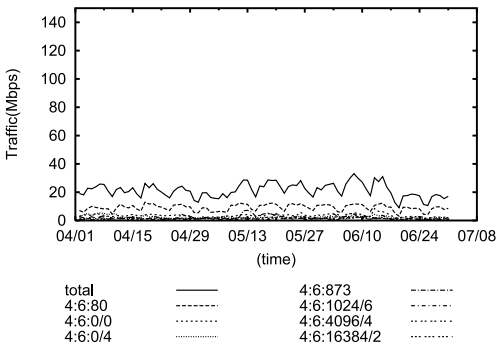

図 3.8. 移行前送信元ポート

向から抽出できた情報を表 3.2、表 3.3 に示す。

図中、表中に出て来る “4:6:80” とは IP バージョンが 4、プロトコル番号が 6（つまり TCP）、送信元ポート番号が 80（つまり HTTP）ということを示している。

ここに示した図は 2 つの情報を持っている。

- 折れ線グラフ
  回線を占めているトラフィックの属性を視覚的に見ることができる。
  今回取り上げた WIDE インターネット国際線の例では、全トラフィック量の推移と HTTP データの割合を把握できる。
- 項目
  折れ線グラフの下にリストアップされる項目数は、AGURI によって設定することができる。この項目は全トラフィック中の占有率順にリストアップされるため、回線を使用している組織や使われているアプリケーションを検知することができる。

送信元、宛先 IP アドレスからは、特定の組織の IP アドレス空間と特定のホストを検出できた。

特に 2005 年度の WIDE 報告書と比較した場合、2005 年度に観測された jaist.ac.jp を宛先としたトラフィックを引き続き抽出できた。

また、特定のホストにトラフィックが集中している様子も観察できた。抽出された ‘150.65.7.130’、‘163.221.11.21’、‘203.178.137.175’ という IP アドレスは、3 つとも WIDE プロジェクト内に設置されている公開 FTP サーバである。

送信元ポート番号からは、特定のポートを使用したアプリケーションを検出できた。

今年度も引き続き HTTP トラフィックの観測に加えて、今年度から BitTorrrent という p2p ファイル転送ツールのトラフィックを検出できた。また、2005 年度に観測された rsync トラフィックは、移行前には観測する事ができたが、移行後のデータにおいては、他のアプリケーションのトラフィック量増加に伴って割合的に減少したため、観測することができなかった。

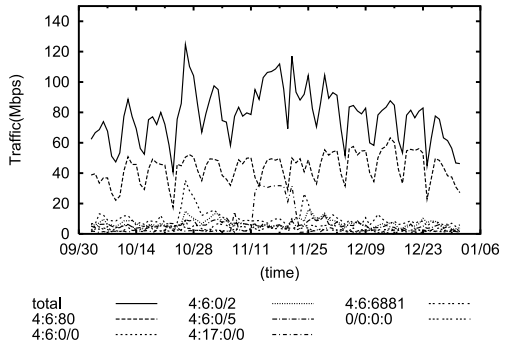

図 3.9.　移行後送信元ポート

3.4 結論

本節では、AGURI を用いた WIDE インターネット国際線のトラフィック傾向を述べた。

WIDE インターネットのような広域なネットワークを運用し続けていくためには、トラフィックモニタリングを多地点、かつ長期間行い、ネットワークの現状に適した通信機器の設置、設定を行う必要がある。

しかし、現存するネットワークモニタリングツールは長期に渡ってトラフィックの傾向を収集し続けることが難しい。

WIDE プロジェクト/mawi ワーキンググループでは収集したトラフィックを効果的に集約することによって、ネットワークの特徴を抽出することのできるトラフィックモニタリングツール AGURI を用い長

表 3.2.　識別された IP アドレス

graph	IP アドレス	hostname
図 3.2、図 3.3	150.65.7.130	ftp.jaist.ac.jp
図 3.3	163.221.11.21	mozilla-mirror.naist.jp
図 3.3	203.178.137.175	ftp.nara.wide.ad.jp

表 3.3.　識別されたポート番号

graph	ポート番号	プロトコル/アプリケーション
図 3.6、3.8、3.9	4:6:80	HTTP
図 3.8	4:6:873	rsyc
図 3.9	4:6:6881	BitTorrent

期に渡る国際線のトラフィック傾向を明らかにした。

実際に AGURI を用いて WIDE インターネット国際線でデータを収集し、対象とした国際線のトラフィックの傾向を明らかにした。

WIDE プロジェクトでは、AGURI の開発をすすめると共に、WIDE インターネットのバックボーンにおいて AGURI を運用し続けている。これらのデータは `http://mawi.wide.ad.jp/mawi/` から参照可能である。

第 4 章　計測に関する 2006 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 プロジェクトでは、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。

2006 年には以下の 2 回のワークショップを開催した。

- 第 6 回 CAIDA-WIDE 計測ワークショップ
  2006 年 3 月 17–18 日　USC/ISI
- 第 7 回 CAIDA-WIDE 計測ワークショップ
  2006 年 11 月 3–4 日　UCSD/SDSC

2006 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
  一年に一度、世界中の組織で同時に計測を行なおうという取り組みである。今回はパイロットプログラムとして、2007 年 1 月に CAIDA と WIDE プロジェクトが中心になり計測データ収集を実施した。
- 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。
- トポロジ計測ツールの開発
  scamper と呼ぶ並列 traceroute ツールの改良を継続している。
- 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 プロジェクトが地域別の 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 プロジェクトが小型計測箱を設置、遠隔管理する計画を進めている。

2007 年度もこれらの共同研究活動を継続し、研究者交換も実施する予定である。

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 プロジェクトは、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 1 年目の今年は、相互の研究を理解し交流を深めること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 など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 WIDE プロジェクトで、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、異常を自動で検出する共同研究を実施中である。

(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である。

(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。

2006 年から 2007 年にかけて 3 回のワークショップをモビリティチームと合同で開催し、各自の研究の進捗報告や、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。

- 第 1 回 CNRS-WIDE ワークショップ
  2006 年 2 月 8–10 日　慶應義塾大学三田キャンパス
- 第 2 回 CNRS-WIDE ワークショップ
  2006 年 11 月 18–19 日　パリの CNRS 本部
- 第 3 回 CNRS-WIDE ワークショップ
  2007 年 1 月 19–20 日　広島大学東千田キャンパス

また、2006 年度は以下の研究者交換を行なった。

- LIP6 の Salamatian 助教授の学生 Nageeb Earally が 2006 年 6 月から 9 月まで日本に滞在した。奈良先端科学技術大学院大学門林助教授の研究室で受け入れ、アプリケーションの自動識別に関する研究を行なった。
- 奈良先端科学技術大学院大学の学生益井賢次君が 2006 年 9 月から 12 月まで LIP6 を訪問した。分散計測基盤について研究を行なった。
- ENS Lyon の Patrice Abry の学生 Guillaume Dewaele が 2007 年 1 月から 3 週間日本に滞在した。国立情報学研究所福田助教授が受け入れ、時系列解析に関する共同研究を行なった。

2007 年度は、共同研究も 2 年目に入り、より活発な研究活動を行なって成果を出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

5.1 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。この交換留学生として、2006 年 9 月 14 日から同年 12 月 12 日にかけて約 3 ヶ月間渡仏した。受入組織は、パリ第 6 大学情報処理研究所（Laboratoire d'informatique de Paris 6; LIP6）内の Networks and Performance Analysis group（NPA）で、同組織の Kavé Salamatian 助教授を中心に受入体勢を整えていただいた。

滞在中は両組織間の研究協力関係に沿って、以下のような活動をした。まず、自身の研究活動の周知のため、CNRS に関連する研究イベントに参加し研究発表を行い、また人的交流も深めた。その上で、自身の研究に関連の深い研究者と直接議論することで、より具体的な研究協力関係の構築に努めた。

5.2 研究イベントへの参加

在仏中、いくつかの研究イベントに参加し、CNRS 関係者との交流を深めるとともに研究内容について意見を交換した。ここでは、それらのイベントの内容について報告する。

5.2.1 CNRS/INRIA/WIDE ミーティング

2006 年 9 月 18 日・19 日に、フランス・パリ市内の CNRS 本部で行われた CNRS/INRIA/WIDE ミーティングに参加した。本ミーティングには、CNRS・フランス国立情報学自動制御研究所（Institut National de Recherche en Informatique et en Automatique; INRIA）および WIDE プロジェクトのそれぞれの研究者らが参加し、Measurement と Mobility の各セッションに分かれて研究発表を行った。

このミーティングには先述の研究協力プロジェクトの関係者が多く参加することもあり、実質的に顔合わせのためのミーティングとなった。ミーティング中、CNRS 側の関係者の紹介を受けるとともに互いの研究内容について概説し合い理解を深めた。また、関連

の深い研究に携わる研究者らとは後日個別に面談し、研究協力の体制について話し合うことを約束した。

5.2.2 NPA 内での研究発表

2006 年 10 月、フランス・パリ市内の LIP6（図 5.1）で行われた NPA によるミーティングに参加し、自身の研究発表を行った。NPA は、主にネットワークトラフィックの数学的な解析手法を研究対象とするメンバーから構成される。約 10 名の NPA メンバーが参加する中で、互いの研究内容について議論した。

自身の研究 [138] の中心となるテーマが、彼らの研究対象であるトラフィック解析手法を実装するための基盤であることもあり、互いに研究内容を補完できる関係で意見交換が行われた。こちら側の研究内容に関しては、基盤技術を利用する当事者から要望や意見が得られた点で有意義であった。

図 5.1. パリ第 6 大学・LIP6

5.2.3 MetroSec Project での研究発表

MetroSec Project[141] は、ネットワークトポロジなどインターネットに関わる様々な特性を収集する手法について研究を行っている研究グループで、研究協力プロジェクトの CNRS 関係者も多く参加している。2006 年 10 月にフランス・リヨンの ENS Lyon 内で行われた MetroSec ミーティングで研究発表を行い、意見を交換した。

CNRS のコアメンバーも多く参加するミーティング内で研究発表を行いその内容を周知させるとともに、当該分野の第一線の研究者から指摘・意見をいただくことができた。

5.3 研究協力

前述の数回の研究イベントへの参加を経て、研究活動において具体的に協力していくため、自身の研究内容に関連の強い研究者と直接対話した。その上で、2 つの研究プロジェクトについて協力していくこととなった。

5.3.1 大規模トポロジ収集プロジェクト（traceroute@home）

traceroute@home Project[251] は、インターネット上に分散配置されたエンドノードが各々 IP ネットワークトポロジを収集し、得られた情報を統合することによりインターネット全体のトポロジ情報を構築することを目的としている。このプロジェクトには CNRS のメンバーである Timur Friedman 助教授も関わっており、現在も活動が続いている。traceroute@home Project の研究課題は大きく 2 つに分けられる。1 つは、大規模・広域に展開するインターネットにおいてトポロジ情報を収集するために有効な計測手法を研究することである。もう 1 つは、そのような手法を実際にインターネット上で適用できる計測基盤のアーキテクチャについての研究である。

前者の計測手法については、Doubletree[59] と呼ばれるトポロジ情報の収集手法が traceroute@home Project から提案されている。この協調計測アルゴリズムでは、各計測ノードがトポロジ情報の収集のために IP パケットの TTL 値を漸増させる手法（いわゆる traceroute の方式）を用いる。その上で、ある計測ノードは他の計測ノードが収集したトポロジ情報のグラフの中から共通部分を抽出し、自身が行うトポロジ情報の収集範囲をその共通部分に重複しないように調節する。このようにして重複したトポロジ収集活動を避けることで、収集活動に伴うネットワーク資源の消費を押さえ、トポロジ情報の収集の効率化を図っている。重複部分の開始点を示すデータセットは stop set と呼ばれ、各計測ノードが収集結果に基づいて協調して構築していく。

また、Doubletree のような協調計測アルゴリズムを適用できる計測基盤についての研究も行われている。traceroute@home v1 と呼ばれる計測基盤では、計測ノード間で片方向リング状の計測ネットワークを構築し、stop set を含むデータを回覧・修正していくことで Doubletree を実際に適用していた。この基盤の問題点として、リング状ネットワークに属するホストが 1 台でも故障すると stop set の回覧が途切れ計測ネットワークが機能しなくなる点、次第

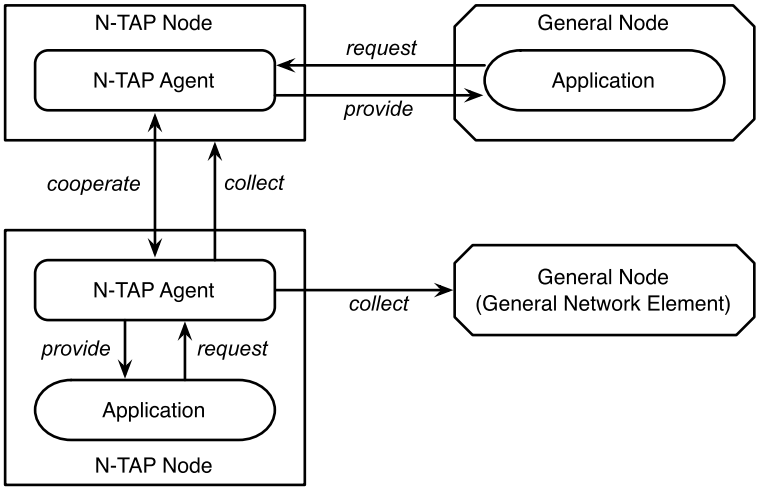

図 5.2.　N-TAP とそれを利用するアプリケーションとの関係

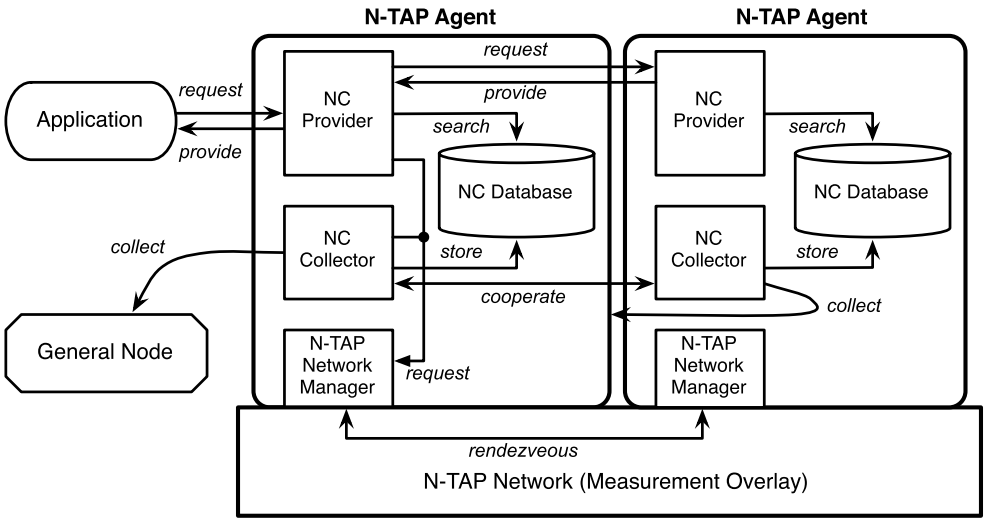

図 5.3.　N-TAP のコンポーネント間の関係

に大容量化する stop set を計測ノード間で交換する際のネットワーク負荷の高さ、リングネットワーク中の各ノードの性能が計測ネットワーク全体の性能に直接影響する点などが挙げられている。

そこで、traceroute@home v1 の改善版として traceroute@home v2 が現在策定中である。traceroute@home v2 では、分散ハッシュテーブル（Distributed Hash Table; DHT）の一実装である OpenDHT[199] ベースの共有ストレージに stop set を含むデータを蓄積することで、先述の問題の解決を図ろうとしている。共有ストレージの構成ノードは、必ずしも計測ノードである必要はない。

一方で、我々が研究・開発を進めている計測基盤 N-TAP[138] は、計測ノード間の通信と分散共有ストレージの機能を提供する、協調計測・分散計測の実現を目的とした計測基盤である。N-TAP では、計測ノード間で DHT ベースのオーバレイネットワークを構築し、その上に協調分散計測アルゴリズムで最も重要となる、共有ストレージおよび計測ノード同士のランデブーを実現する機構を備えている。図 5.2 のように、N-TAP では計測エージェントがエンドノード上で動作し、計測活動を行う。また、エージェントはアプリケーションからの要望に応じてネットワーク特性の提供も行う。図 5.3 は、N-TAP エージェントの内部コンポーネントとそれらの間の関係を示している。エージェントは、アプリケーションからの要求を受付けネットワーク特性を提供する provider、実際の収集活動を行う collector、計測オーバレイネット

ワークを構成し計測ノード間の協調活動を管理するnetwork manager、分散共有ストレージの一片となるdatabaseから構成され、それぞれが連携しつつ全体として動作する。現在、N-TAPはPlanetLab[191]をはじめとした数種のプラットフォームで動作することが確認されている。

traceroute@home v2の根幹となる機能要件は、先述したとおり規模拡張性をもった共有ストレージを用意することである。さらに、従来通り計測ノード間の通信機構も必要となる。これらの機能はN-TAP上で実現可能であると判断したため、将来の研究活動において互いに補完し合うことのできる事項があるかについて、Timur Friedman助教授と直接議論した。議論では、traceroute@home v2での要件の洗い出しとN-TAPですでに実現可能である機能の列挙を行い、traceroute@home v2がN-TAP上で実現可能であることを確認した。また、双方のシステムについての改良すべき点について議論した。ただし、traceroute@home v2の開発において、議論の時点ですでに開発者の雇用が完了している段階でその取り消しが難しい状況であったので、早急にtraceroute@homeのプラットフォームをN-TAPのみに移行することは難しいという。このような事情を考慮し、当面は独立して各々のシステムの研究・開発を続け、双方のマイルストーンに達した時点で成果を統合することで合意した。そのため、日本帰国後も互いに連絡を取り続ける体勢をとっている。現時点（2006年12月）で、双方での開発作業が続行中である。

5.3.2 TCPトラフィックの初動分析によるアプリケーション識別手法の研究

Kavé Salamatian助教授らが関わる研究の一つに、TCPトラフィックのセッション初期の傾向を分析することで、そのトラフィックがどのプロトコルに準じたものであるかを識別する手法[19]がある。TCPトラフィックに含まれるポート番号を判断基準にした従来の識別法では、通常使用されるものとは異なるポート番号で運用されているサービスに起因するトラフィックを判別することができない。また、パケットのペイロードを逐一検査してプロトコル判別を行う手法はCPU資源などの消費が大きく、大量のトラフィックの判別が必要な場合に規模拡張性がない。さらにどちらの手法も、Peer-to-Peerアプリケーションなどに起因する暗号化された任意のポート間のトラフィックについては、識別が難しい。このような従来の手法の欠点をふまえた上で、この研究はTCPトラフィックの数パケットの特性を分析することで、高速にトラフィックの識別を実現することを目的としている。

この手法では、ひとつのTCPセッションについて、その開始からの数パケットを分析対象とする。分析の指標となる項目は、トラフィックの方向（2ノード間通信であるので、2方向のいずれか）とパケットサイズである。これらの指標を用い、K平均法・ガウス混合分布などにもとづくトラフィックのクラスタリングを行ってプロトコル別に分類する。現在、この手法はEarly Application Identificationと呼ばれている。

本研究では、識別可能なトラフィックの種類の拡充を図る一方で、人間の動作により生じるトラフィックとボット（bot）のようなプログラムにより機械的に生じるトラフィックの識別が可能であるかについても、検証の課題としている。ボットを利用した、ネットワークおよびホストを対象とするDoS攻撃およびネットワークゲームにおける不正行為など、機械的に生じるトラフィックに起因するセキュリティ上・サービス展開上の問題・妨害は後を絶たない。対策の第一歩として、このようなトラフィックを識別することは重要である。本件に関して、Kavé Salamatian助教授より研究協力の要請を受け、研究へ荷担することとなった。

まず、先述の対象トラフィックの拡充という点で、ゲームトラフィックの識別を行うことになった。現時点でEarly Application Identificationが適用されたアプリケーション（プロトコル）は、NNTP・POP3・SMTP・SSH・HTTPS・POP3S・HTTP・FTP・eDonkey・Kazaaであり、ゲームトラフィックの識別は未検証である。Early Application Identificationがゲームトラフィックに対して適用可能であるかを検証するために、ゲームトラフィックを含むトラフィックデータセットを用意する必要がある。そのため、既存のネットワークゲームの調査から実験環境の構築までを引き受け、行った。現時点（2006年12月）で、ゲームサーバ環境の整備が完了し、参加者数人程度で小規模なゲームプレイを試行し、その結果を解析する体勢までが整った。

今後、フランス国内の各所から実験協力者を募り、可能であれば日本からも協力者を用意して大規模な

実験を行う。本実験では、正規のプレイヤに加えて、ボットプログラムが操作するプレイヤもゲーム内に参加させる。その上で、取得したデータセットを解析して Early Application Identification のゲームトラフィックへの適用可能性を検証するとともに、機械的に生じるトラフィックの識別手法についての検討も並行して進めていく。本実験は 2007 年 1 月に実行予定で、今後も Kavé Salamatian 助教授との協力関係のもと、ネットワークオペレーションおよびトラフィック分析の両面から共同で研究を進める。

5.4 まとめ

WIDE プロジェクトと CNRS との間の交換留学生として渡仏し、研究発表と研究者との議論を通じて、2 つの研究プロジェクトについて協力することとなった。研究協力の 1 つは、traceroute@home Project に対するネットワーク計測基盤技術の提供、もう 1 つは Early Application Identification と呼ばれる手法に関する実験協力である。これらの研究協力関係は、これからも継続される。

第 6 章　ダイヤルアップゲリラ式 dnsprobe による Root DNS サーバ群の計測 in 2006

6.1 概要

本報告書は、2006 年前半に集中的に行った dnsprobe による Root DNS サーバ群の計測結果を示す。

dnsprobe[1] とは、計測ホストから DNS サーバ群までの RTT と DNS サーバ情報を計測するツールである。各種 UNIX 系 OS ならびに Windows にて動作する。

今回の計測は、主にアジアの国々を中心に、2006 年 3 月に集中して行なった。図 6.1 に示す手法を用いて、アジア各国の ISP のアクセスポイントに国際電話をかけ、計測を行った。なお、ISP は GoRemote ローミングに参加している、各国の現地の ISP を利用した。

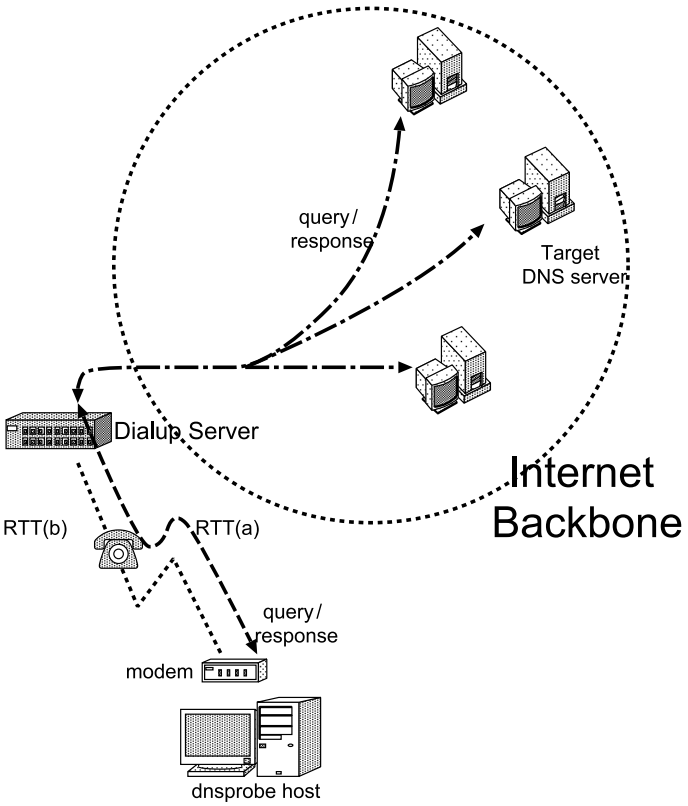

図 6.1.　ダイヤルアップによる dnsprobe 計測

1　http://mawi.wide.ad.jp/mawi/dnsprobe/

6.2 計測

本節では、計測の具体的な手法について述べる。

6.2.1 計測手法

国際電話を使ったダイヤルアップにて行った。ダイヤルアップ元は日本であり、28,800 bps のアナログモデムを利用し、1 回のダイヤルアップ時間は約 30 分で行った。この 30 分の接続時間の間、dnsprobe を利用してできる限り Root DNS サーバへの計測を行った。

また、ダイヤルアップによる RTT の増加と揺れを補正するために、図 6.1 に示す dnsprobe host から Dialup Server まで定期的に ping を行い、その RTT 結果の中間値を補正値として用いて、計測結果の補正を行った。

6.2.2 計測地点

今回の計測では、主にアジア各国を計測地点に選んだ。計測を行った国ならびに都市と回数を表 6.1 に示す。

これ以外にも、次に示す国に対してダイヤルアップを試みた。しかし、国際電話によるダイヤルアップがうまくつながらず、有効な計測結果が得られなかった。

- モンゴル
- カンボジア
- バングラディシュ
- パキスタン
- ネパール

6.2.2.1 計測結果

表 6.1 にあげた各国からの Root DNS サーバに対する計測結果を示す。各グラフは、横軸に Root DNS サーバまでの RTT を示し、1 つの CDF グラフで 1 回のダイヤルアップ結果を示す。また、CDF

表 6.1. 計測地点

国名	ダイヤルアップした都市の数	ダイヤルアップ回数
中国	5	6
香港	1	2
インド	2	3
インドネシア	4	4
韓国	2	4
マレーシア	3	4
シンガポール	1	6
スリランカ	2	5
台湾	1	1
フィリピン	5	5

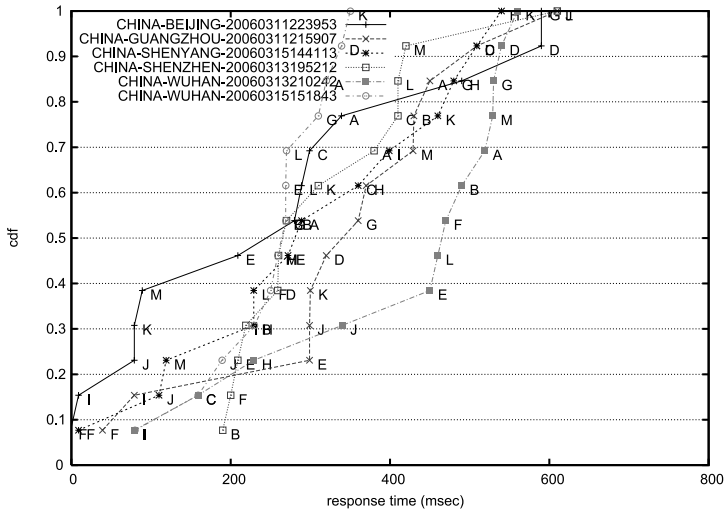

図 6.2. 中国からの計測結果

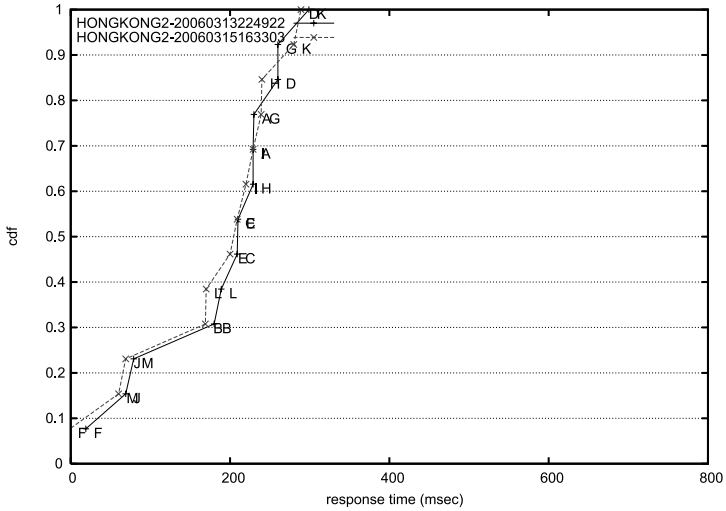

図 6.3.　香港からの計測結果

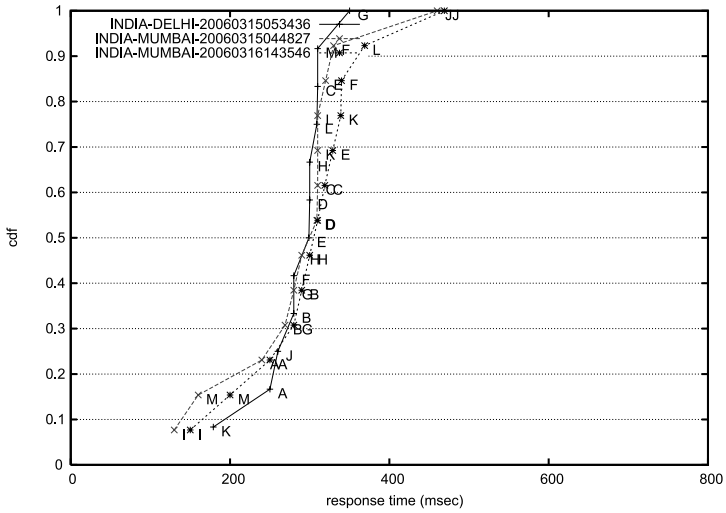

図 6.4.　インドからの計測結果

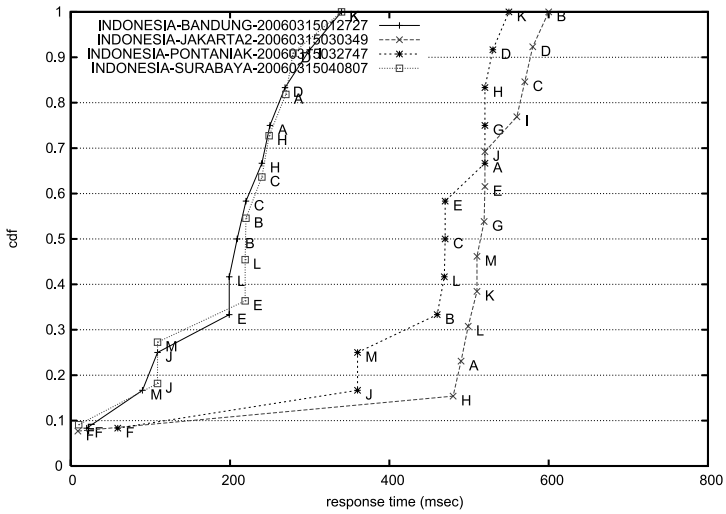

図 6.5.　インドネシアからの計測結果

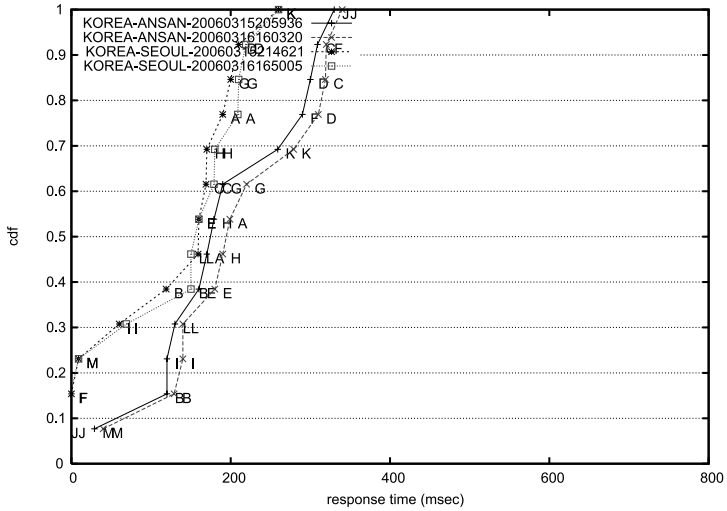

図 6.6. 韓国からの計測結果

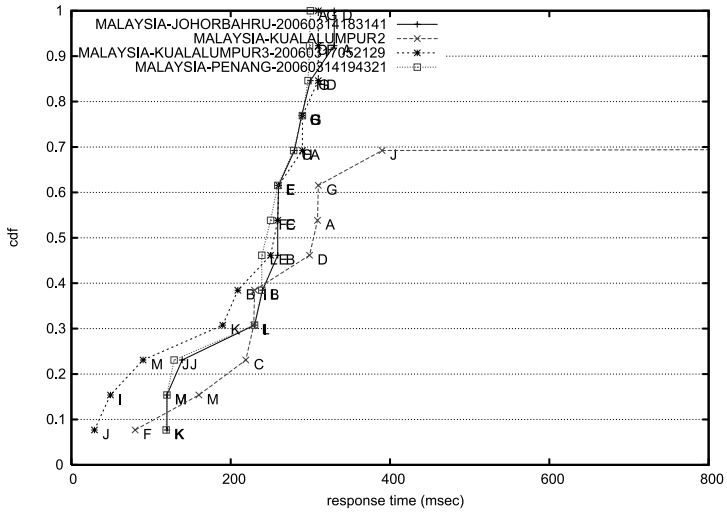

図 6.7. マレーシアからの計測結果

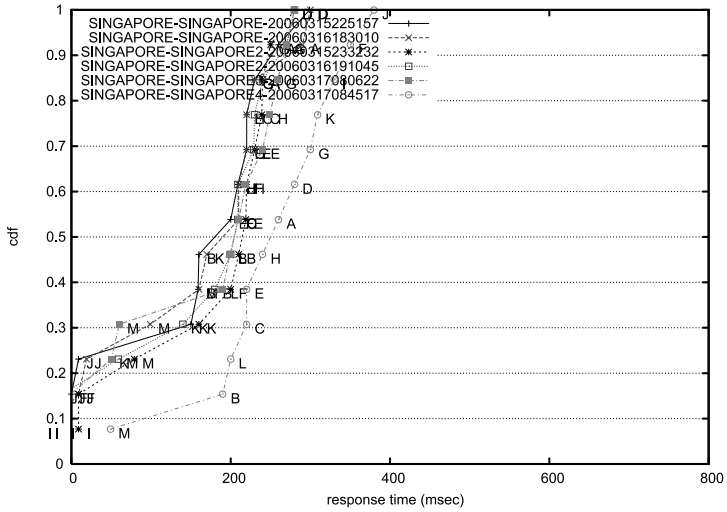

図 6.8. シンガポールからの計測結果

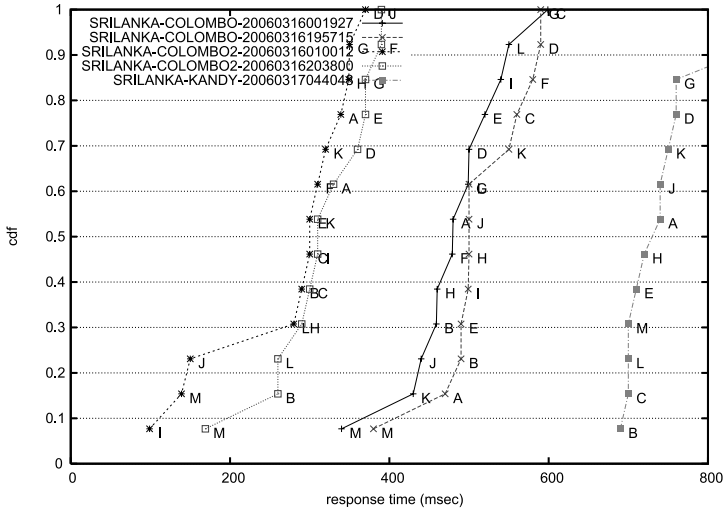

図 6.9.　スリランカからの計測結果

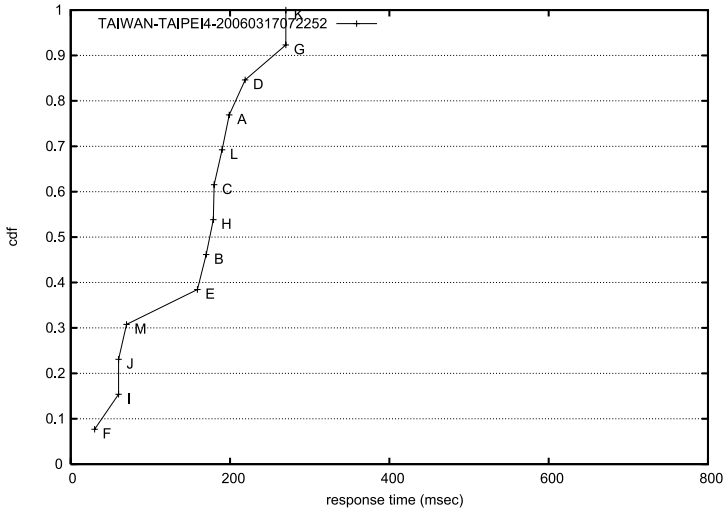

図 6.10.　台湾からの計測結果

グラフ上の A から M までのアルファベットで Root DNS サーバの種類を示す。なお、1 回のダイヤルアップにて行った複数回の dnsprobe における中間値をグラフの値として用いた。

6.3 考察

今回の計測は、アジア各国を中心に行った。その結果、有効な結果が得られた国のうち、スリランカとインドを除けば、最も RTT の小さい Root DNS サーバは 100 ms 以下で応答することがわかった。これは予想よりも良好な結果であると言える。特に、シンガポールや香港、中国、韓国の結果から見てとれるように、エニーキャストによる Root DNS サーバの運用が有効に機能していることがわかる。

第 7 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 プロジェクトの計測活動は、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。2007 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。