DNS Global Measurement

-- DNSday, InternetWeek 2004 --

長 健二朗
IIJ技術研究所/WIDEプロジェクト

グローバルなDNSの挙動

- **大規模分散運用**
  - **多様な実装、運用形態**
  - **ローカルな挙動とグローバルな挙動**
    - **見落とされがちな全体への影響**
- **キャッシュの効果**
  - **本来はグローバルな**DNS**トラフィックは少ないはず**
  - **実際にはかなりの量の本来必要のないクエリ**
    - **ルートへ来るクエリの**98% (Wessels@NANOG26)
- **サーバ選択アルゴリズムの影響**
  - **単純な最短サーバ選択法では変動に弱く、負荷分散も困難**

DNS計測の目的

- **現状の把握**
  - **タイプ別クエリの割合**
  - **メッセージサイズ**
  - **古い実装の割合、**etc
- **問題の検出**
  - LAME**デリゲーション**
  - **プライベートアドレスの**Dynamic Update
  - DNS**パケットのフィルタリング**
  - AAAA**クエリに対する誤動作、** etc
- DNS**サーバの適切な配置**
  - **可用性向上**
  - **負荷分散**
  - **応答時間改善**

WIDEプロジェクトのDNS計測活動

- DNS**サーバの運用**
  - M-root、jp**セカンダリ**、AS112**サーバ**
- **国際的な協調活動**
  - ICANN RSSAC (DNS Root Server System Advisory Committee)
    http://www.icann.org/committees/dns-root/
    - **ルートサーバシステムの計測**
  - CAIDA (Cooperative Association for Internet Data Analysis)
    http://www.caida.org/
    - DNS**計測の共同研究**
  - ISC OARC (An Operations, Analysis, and Research Center)
    https://oarc.isc.org/docs/dns-oarc-overview.html
    - **グローバル**なDNS**システムの運用と解析**
  - JPNIC
    - DNSQC**などの活動**

WIDEが関連するDNS計測ツール

- **サービスサイドでの計測**
  - **クエリ統計**: dsc (passive), dnstop (passive)
  - **クラアント分布計測**: skitter (active)
- **クライアントサイドでの計測**
  - **クエリ統計**: dnstop (passive)
  - **応答時間計測**: rootprobe (active), NeTraMet (passive)

- **今回はツールを中心に紹介**

skitter

- **作者**: Bradley Huffaker
- **大規模トポロジ探索ツール**
  - **パラレル**traceroute**を実行する**
- **ルートサーバにコロして、クライアントの分布を調べるために利用**
  - **もともと**13**個のルートサーバの再配置の検討のためのデータ**
  - BGP anycast**の普及による状況の変化**

http://www.caida.org/tools/measurement/skitter/

NeTraMet DNSモニタ (1/2)

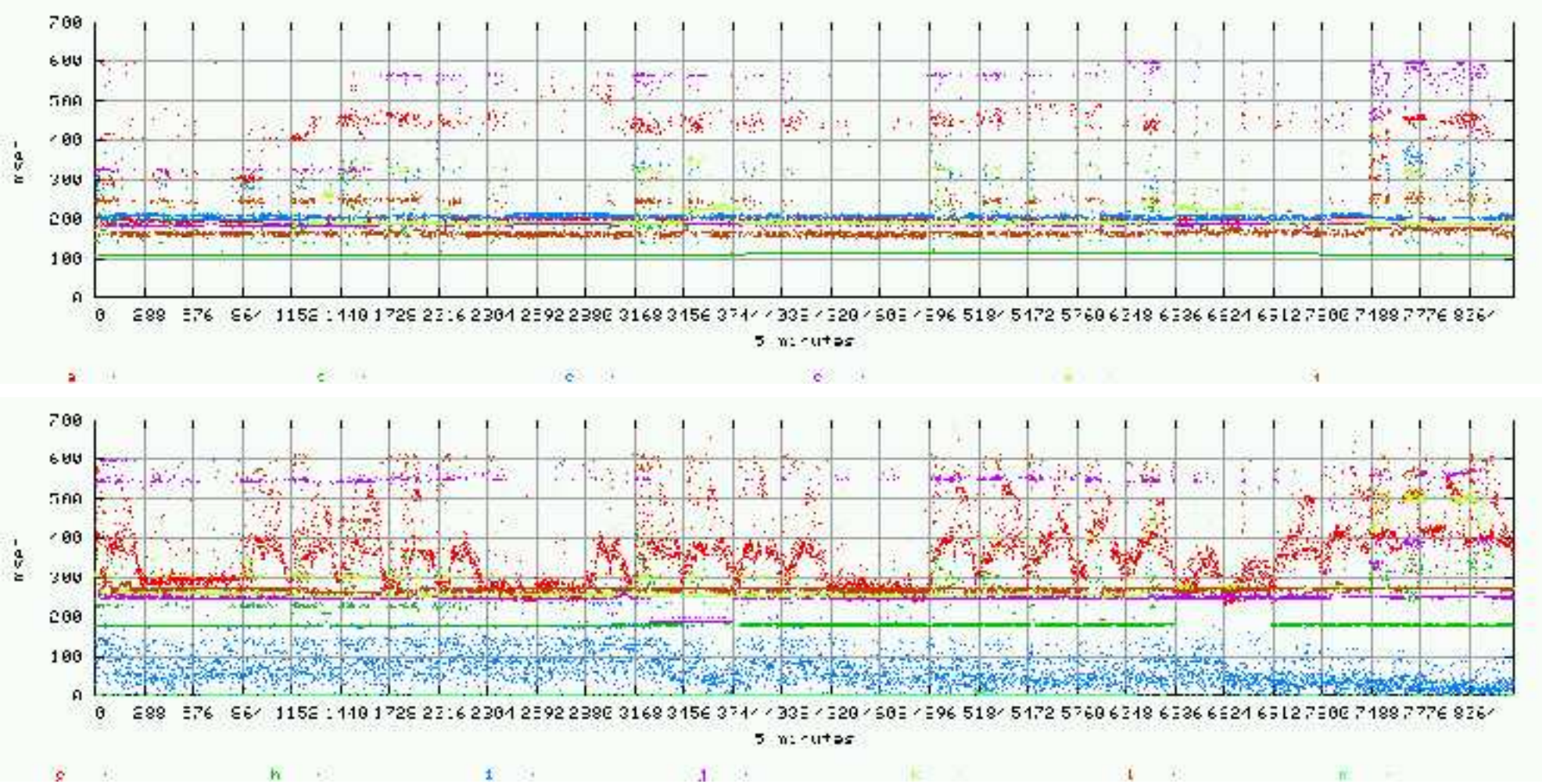
- NeTraMet
  - **作者**: Nevil Brownlee
  - **リアルタイム・フロー計測ツール**
  - RTFM (Real-Time Flow Measurement): RFC2721-2724
    - **ユーザが定義するフローテーブルのメータ** (**パッシブモニタ**)
    - SNMP**エージェントとして動作**

    http://www2.auckland.ac.nz/net/NeTraMet/
- NeTraMet**をベースに**DNS**計測用にカスタマイズ**

  http://www.caida.org/analysis/workload/netramet/dns/

NeTraMet DNSモニタ (2/2)

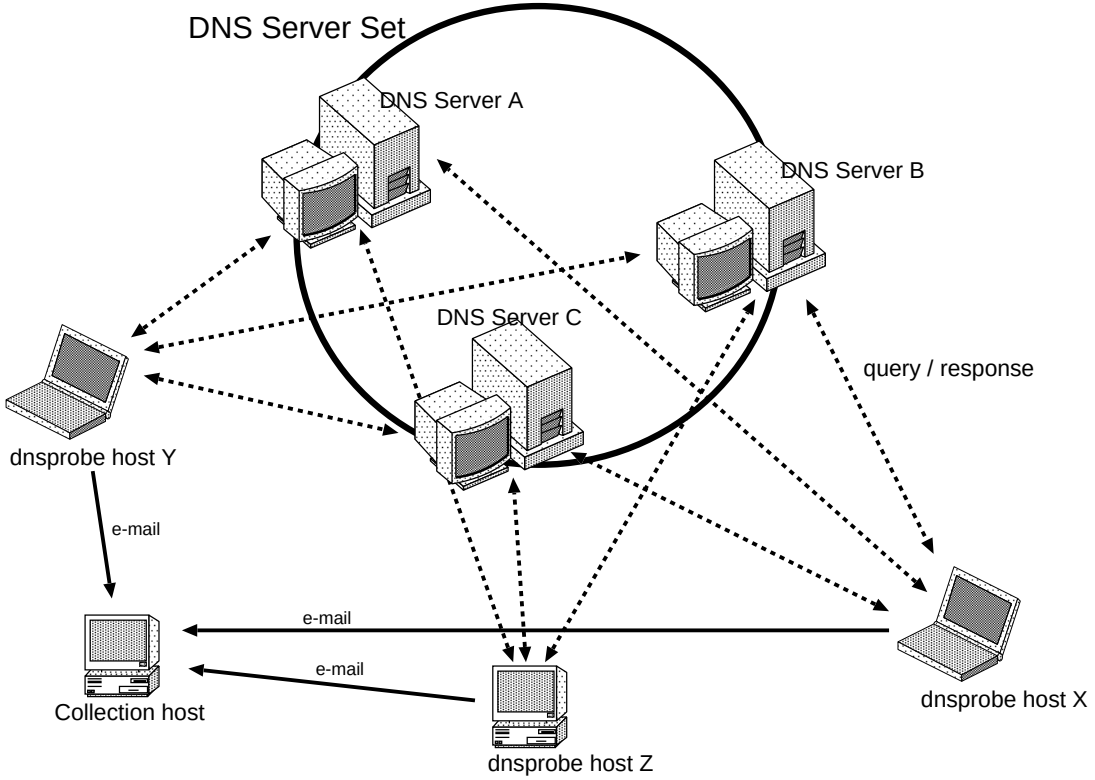
- **ルートの応答時間** (2004/10 from u-tokyo)



rootprobe (1/4)

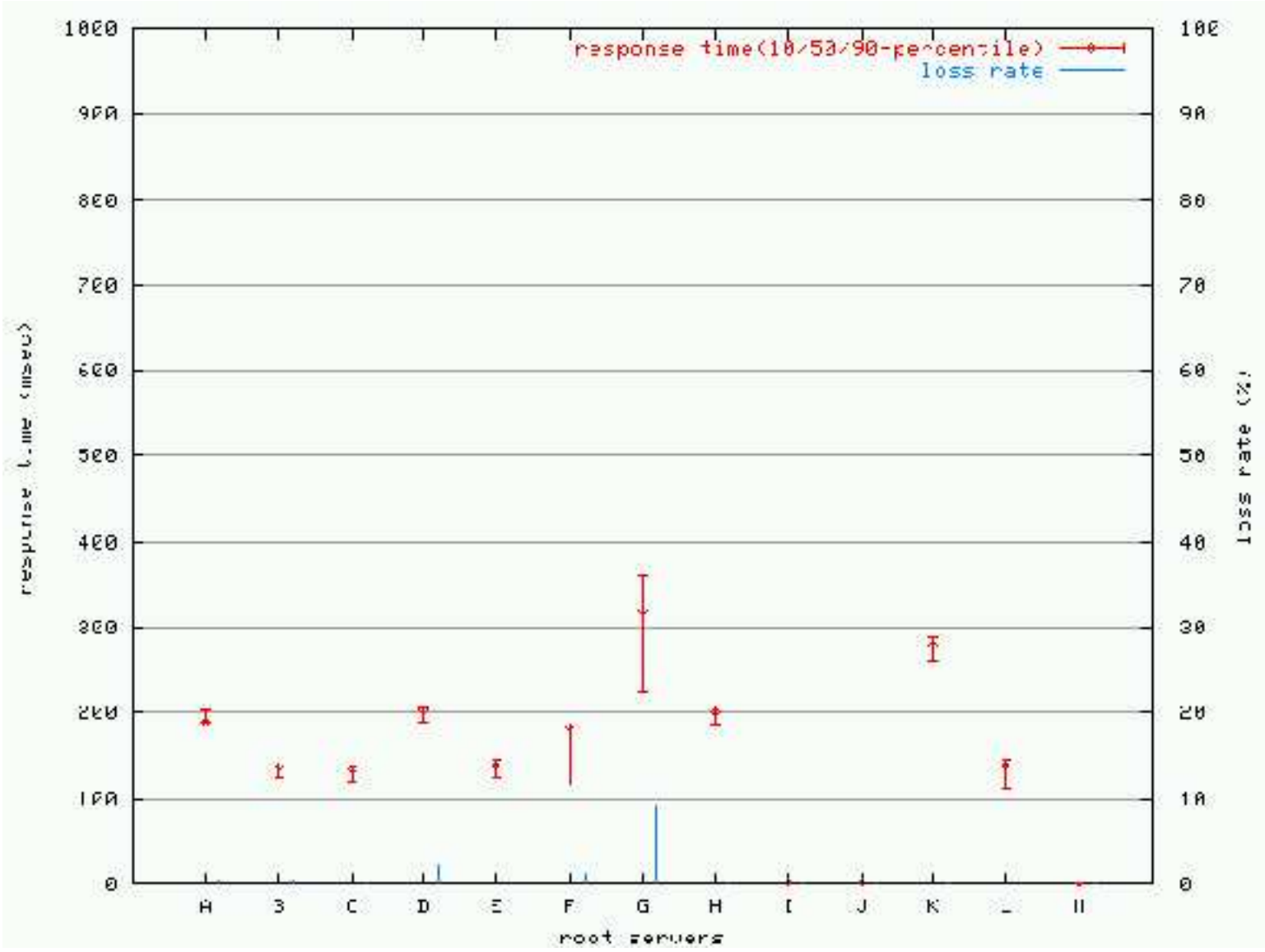
- **簡単なアクティブDNS応答時間計測ツール**
  - **ターゲットにAクエリを投げて、応答時間を収集サーバにレポート**
- **どこからでも計測可能 (パッシブ計測の欠点を補間する)**
  - **旅先で自分のノートPCから、また、ダイアルアップで世界中から計測**
- ccTDL**サーバを使ったアクセス網遅延の補正**

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



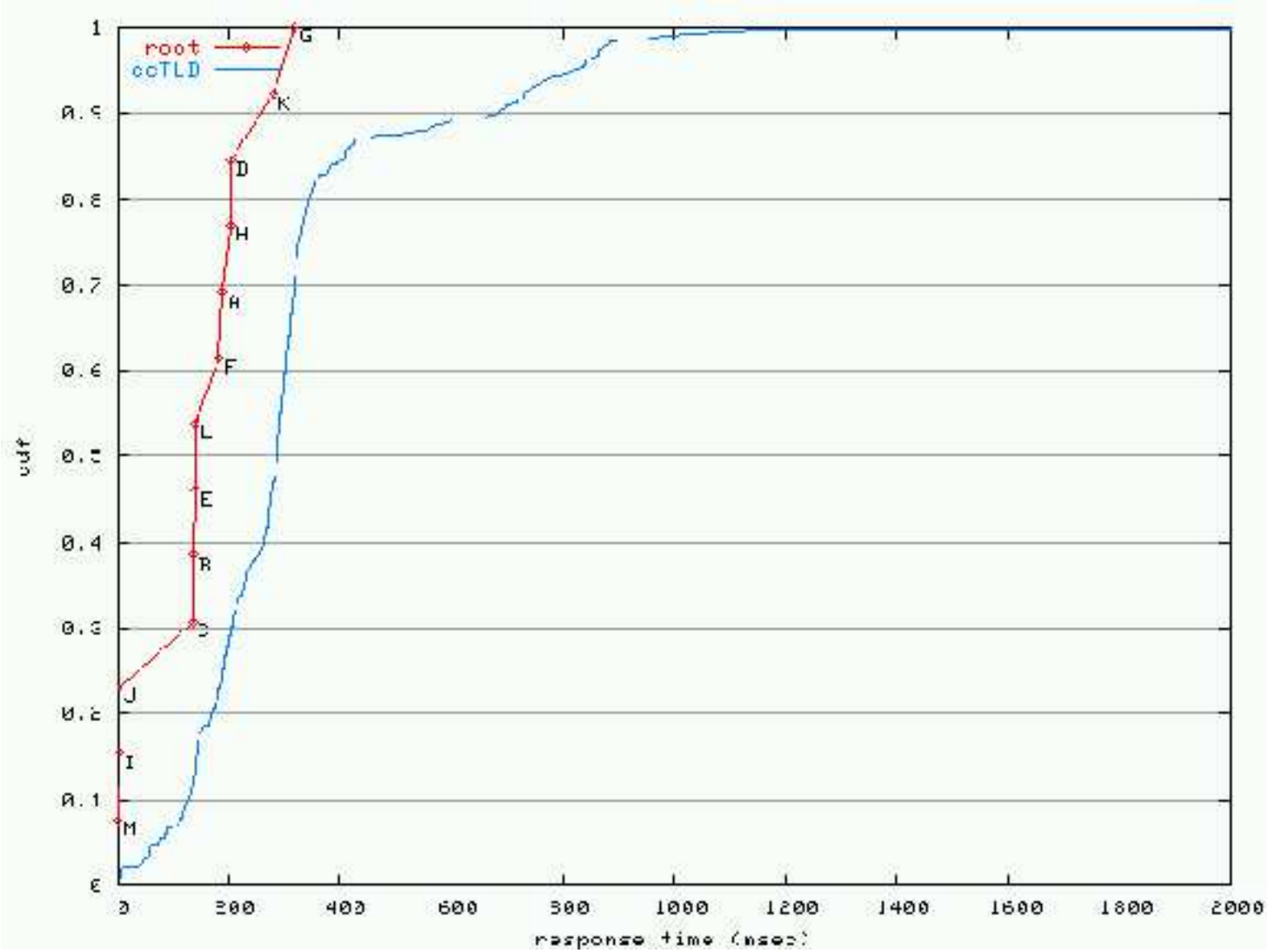
rootprobe (2/4)

- **各ルートサーバの応答時間とロス率** (2004/11/14-21 from home in tokyo)



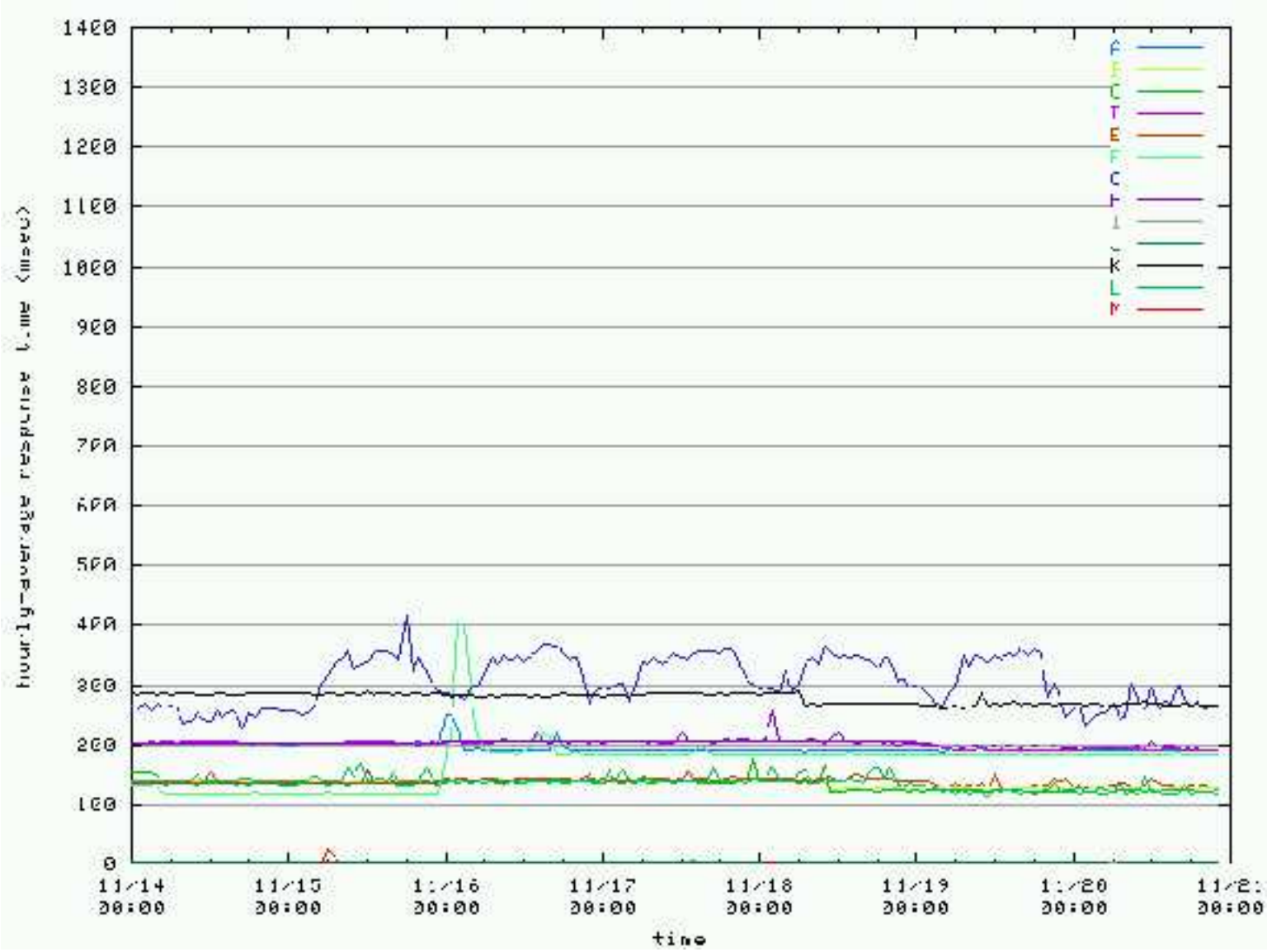
rootprobe (3/4)

- **ルートと**ccTLD**サーバの応答時間累積度分布**



rootprobe (4/4)

- ルートサーバの応答時間の時間変化



Toward Lowering the Load on Root DNS Servers

- Duane Wesselsの F-rootでのクエリ解析 @NANOG26 (2002/10)
  - **ルートに来るクエリのほとんどはゴミ**
  - 44.9% Repeated QNAME: **異なるクエリ**ID**をもつ同一クエリの繰り返し**
    - **リプライがファイアーウォールでフィルタされている**
  - 25.4% Repeated Query: **同一クエリ**ID**をもつクエリの繰り返し**
  - 12.5% Unknown TLD: **存在しない**TLD: local, localhost, domain, c
  - 7.3% A for A: **すでにアドレスに対する**A**クエリ** (WIN2K**のバグ？**)
  - 4.4% Referral Not Cached: **同一ゾーンに対するクエリの繰り返し**
  - 2.2% Legitimate: **正しいと思われるクエリ**
  - 1.9% Nonprintable in QNAME: **アスキー以外が**QNAME**に入っている**
  - 1.6% rfc1918 PTR: **プライベートアドレスの逆引き**
  - 0.0% Unused Query Class: IN, CH, HS, NONE, ANY**以外**

dnstop (1/2)

- **作者**: Duane Wessels
- pcap**を使って**DNS**メッセージをキャプチャ**
- curses**を使った**DNS**統計の表示**
  - src addr
  - dst addr
  - Query type
  - Top Level Domain
  - Second Level Domain

http://dns.measurement-factory.com/tools/dnstop/

dnstop (2/2)

- クエリタイプ別表示

Query Type	count	%
#0?	14	0.0
A?	21333	21.8
NS?	314	0.3
CNAME?	18	0.0
SOA?	388	0.4
PTR?	10564	10.8
MX?	10097	10.3
TXT?	865	0.9
AAAA?	49598	50.8
SRV?	79	0.1
A6?	3700	3.8
ANY?	671	0.7
#16443?	2	0.0
#16588?	1	0.0
#16733?	1	0.0
#16989?	1	0.0
#17063?	1	0.0
#17621?	1	0.0

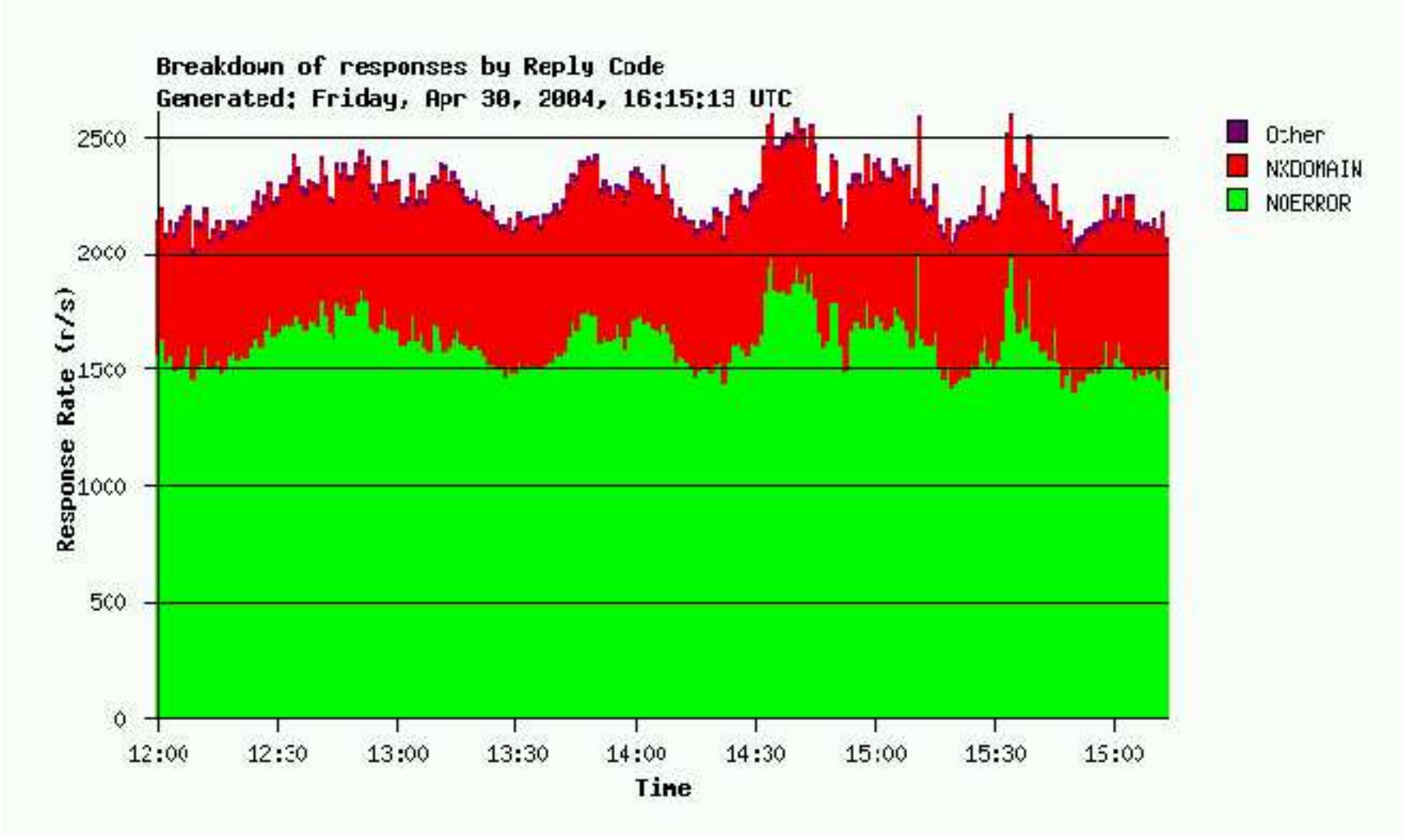
DSC: A DNS STATISTICS COLLECTOR (1/6)

- **作者**: Duane Wessels
- Collector
  - pcap**を使って**DNS**メッセージをキャプチャ**
  - **項目別の統計データを管理**
    - client addr, /24 subnet, message length
    - Opcode, Response Code, Qtype, Qclass, Qname length,
    - TLD, IDN, EDNS, DNSSEC, etc
  - 60**秒毎に統計データを**XML**形式でセーブ**
  - **フィルタの設定が可能**
    - Query Only, Reply Only, Qtype, IDN, AAAA, Query for root
- Extractors
  - **項目ごとの**XML**ファイルのパーサ**
  - **グラフ化のための中間ファイルの生成**
- Graphers
  - **中間ファイルからグラフを生成**
  - **グラフ化には**ploticus (http://ploticus.sourceforge.net/) **を利用**

    http://dns.measurement-factory.com/tools/dsc/

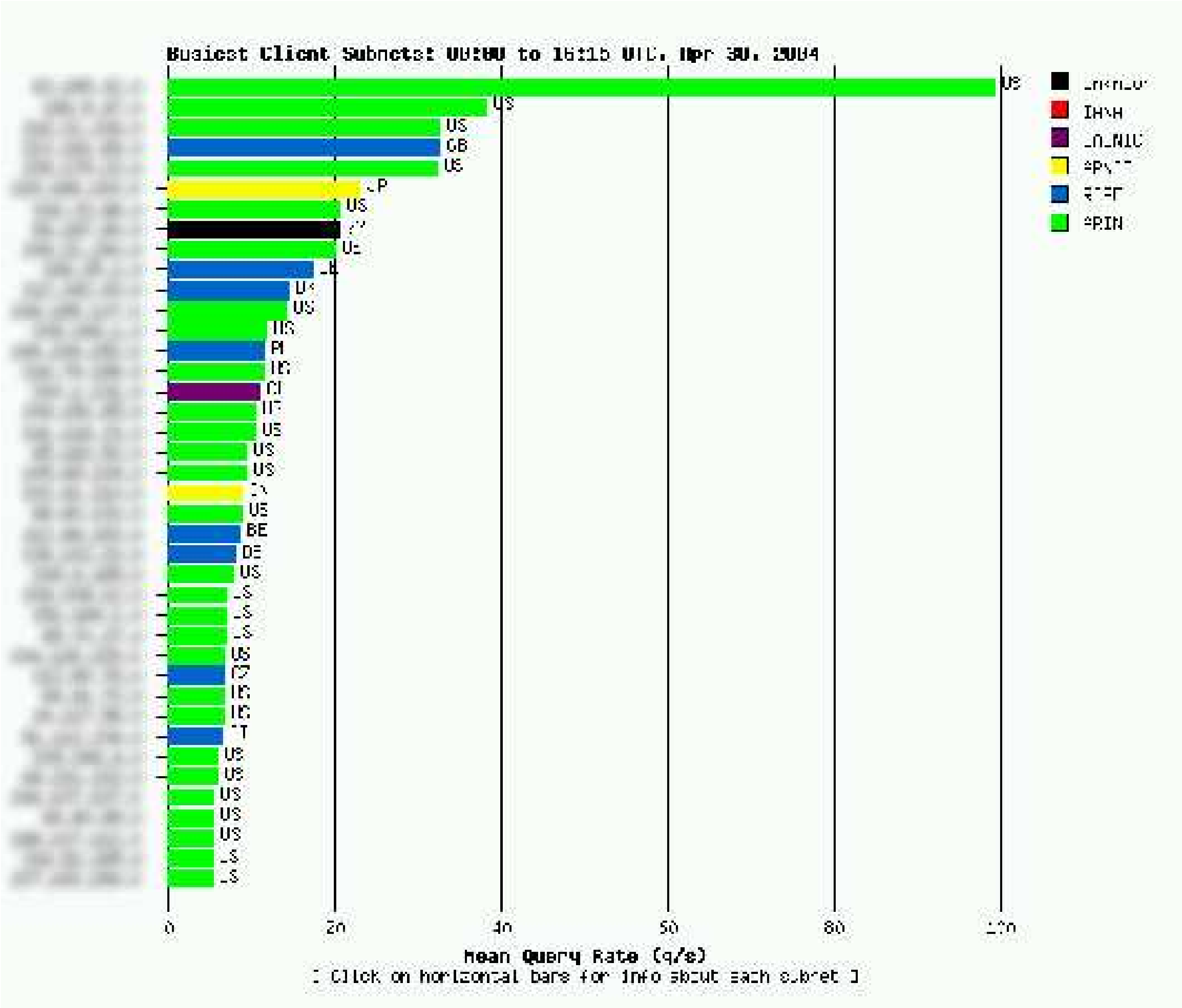
dsc (2/6)

- **リプライコード**
  - **約**1/4**は**NXDOMAIN



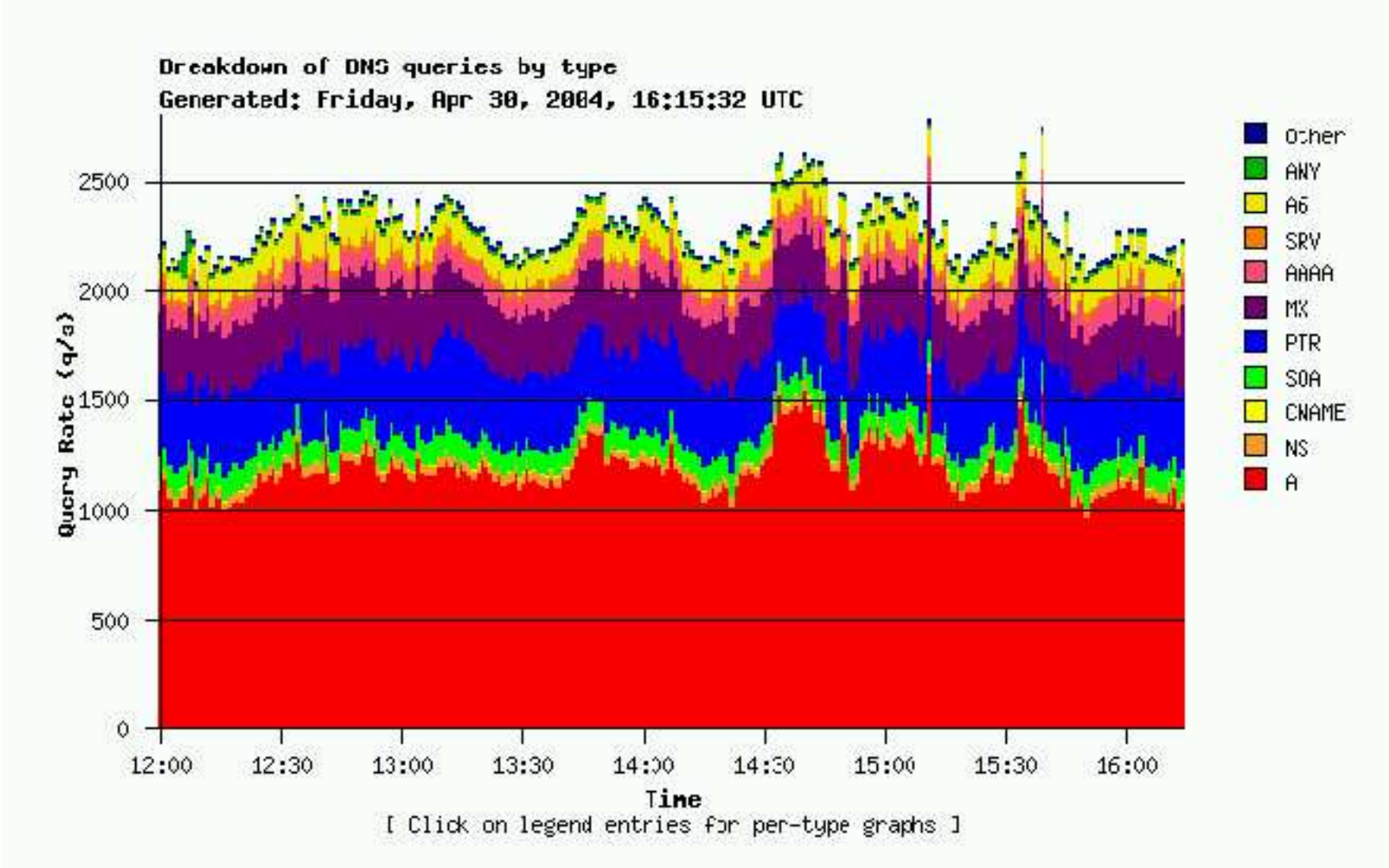
dsc (3/6)

◦ クライアント別 (地域別)



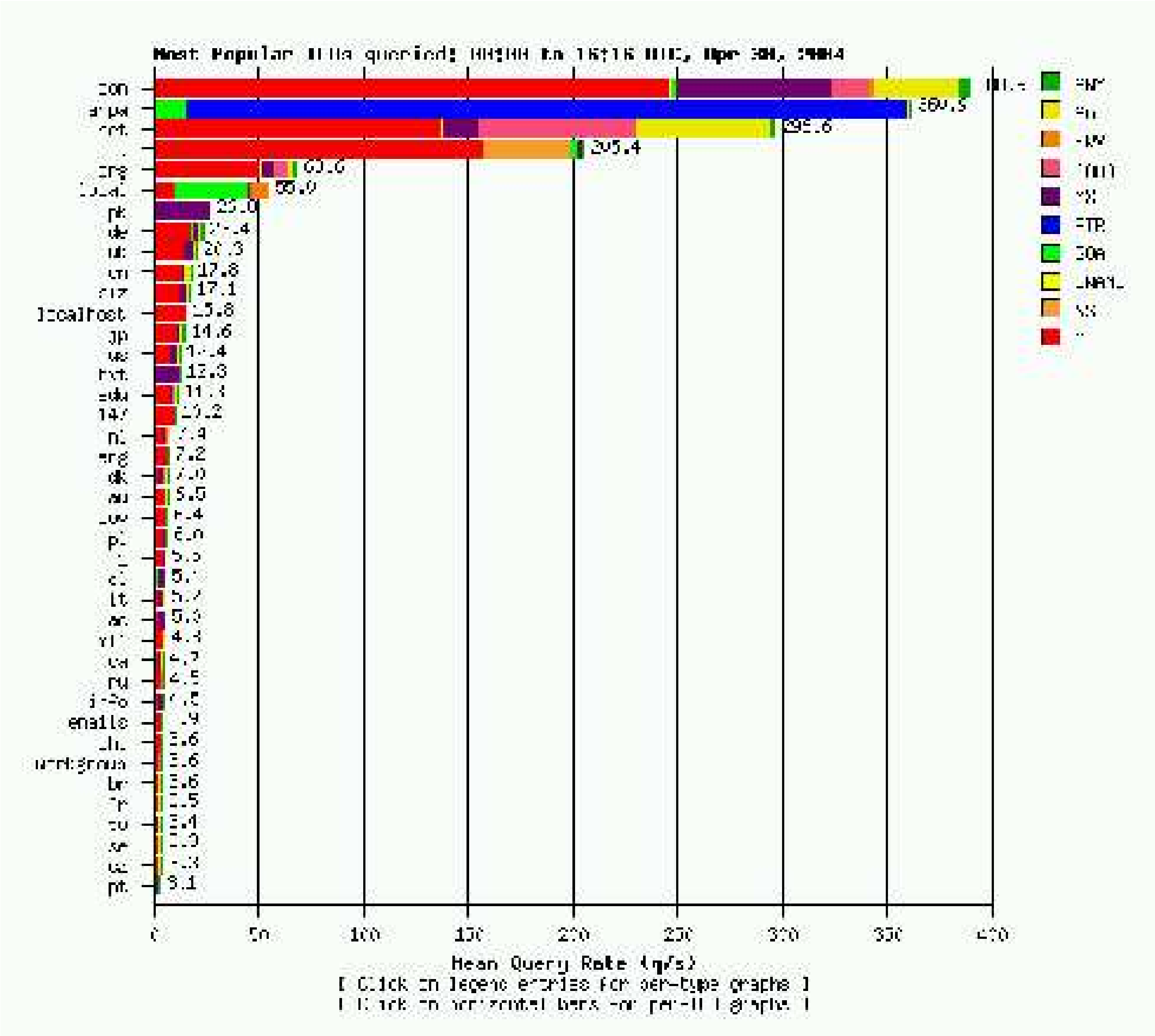
dsc (4/6)

- クエリタイプ
  - 約1/2がA



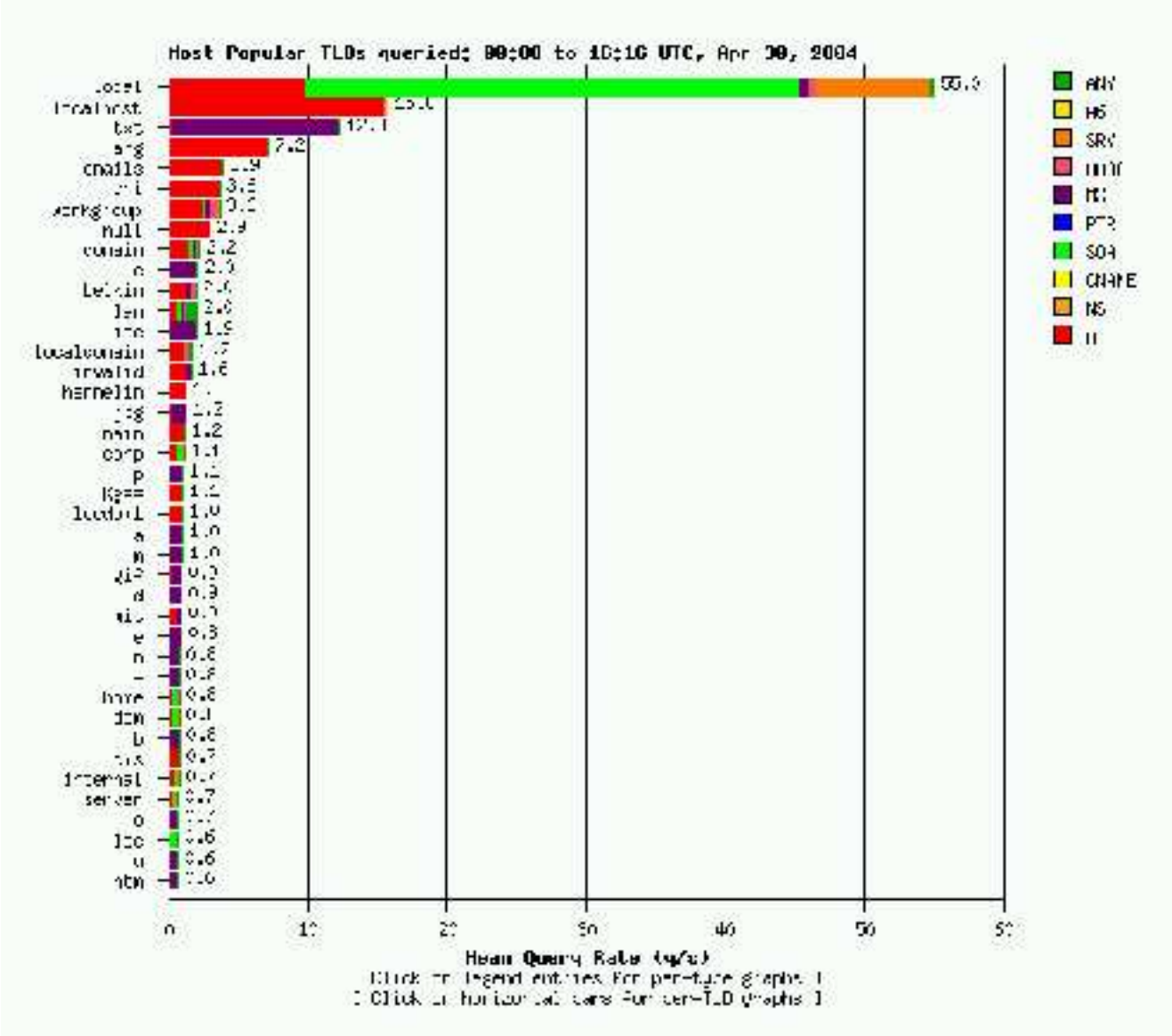
dsc (5/6)

- TLD別



dsc (6/6)

- **存在しない**TLD



その他のDNS計測ツール

- dnsmon
  - **多数のプローブから測定対象サーバの応答を継続的に記録**
    http://dnsmon.ripe.net/
- dnsreport.com
  - DNS**設定の検証サイト**
    http://www.dnsreport.com/
- checkdns.net
  - DNS**設定の検証サイト**
    http://www.checkdns.net/

まとめ

- **グローバルなDNSの挙動**
  - **ローカルな挙動とグローバルな挙動**
  - **キャッシュの効果**
  - **サーバ選択アルゴリズムの影響**
- **国際的な協調、長期的観測の必要**

- WIDE**プロジェクトが関係する**DNS**計測活動とツール**
  - skitter, NeTraMet, rootprobe, dnstop, dsc