DNS measurement

Japan Registry Service (JPRS)

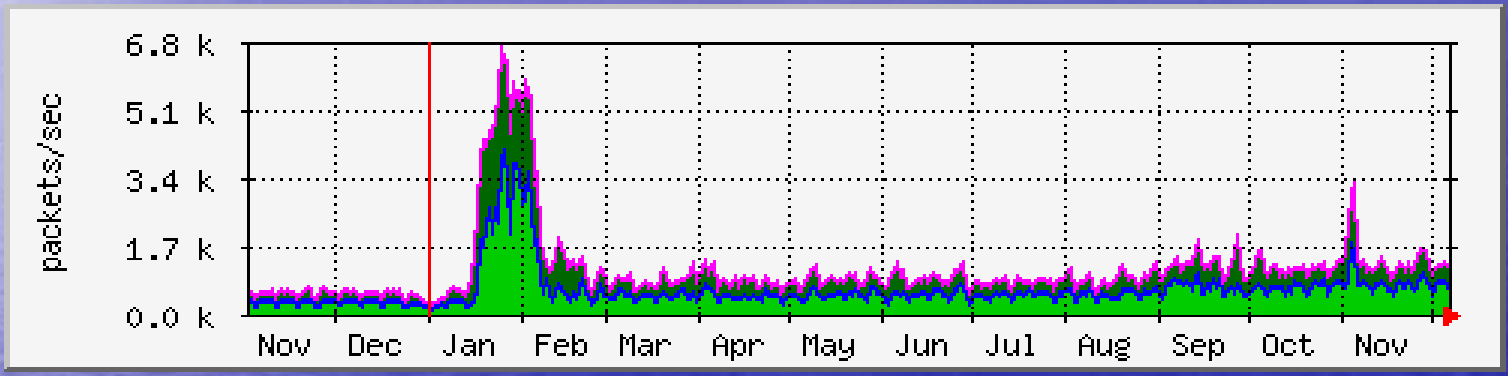
Izuru Shirai <shirai@jprs.co.jp>

DNSの何を計測するのか

- queryの傾向
  - 安定稼動の指標
  - 事件の前兆？を読み取る
  - 特に異常がない限り統計データのみを扱う
- Service Level
  - 耐障害性
  - 品質 (応答時間)

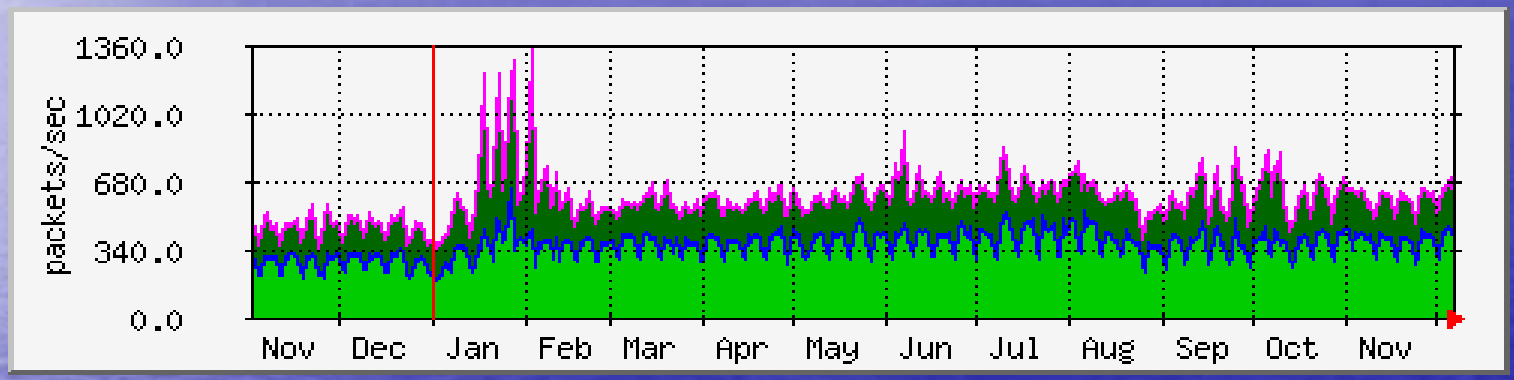
queryの傾向

DNS queryから読み取れるあれこれ



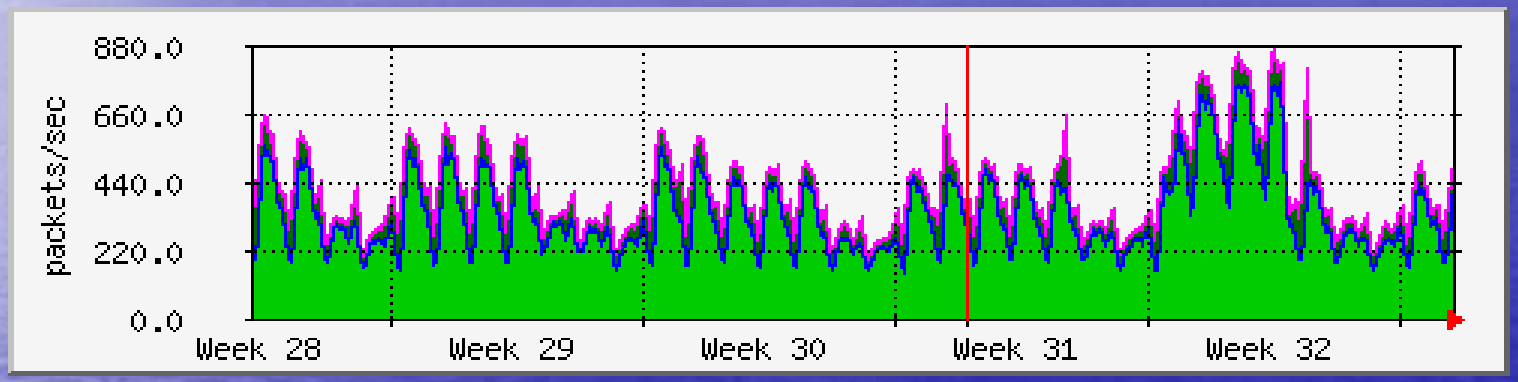
- これは ns0.nic.ad.jp
- bind-8.3.0 の山がはっきりと
- 11月の山も bind-8.3.0

そのころ別の所では…



- これは ns-jp.nic.ad.jp
- だいぶ少ない
- 8月ごろの乱れは…

昨年8月14日のsnapshot



- code red II？
  - 世間で騒ぎ始めた途端こうなった

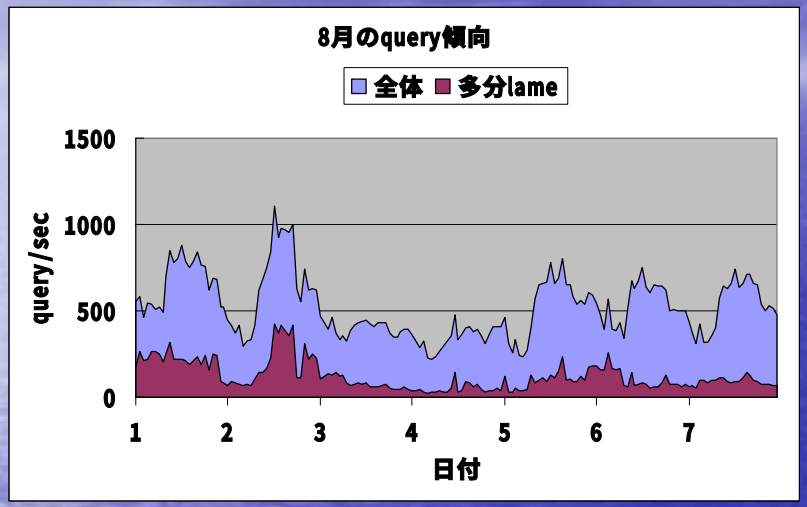
query の傾向を評価する

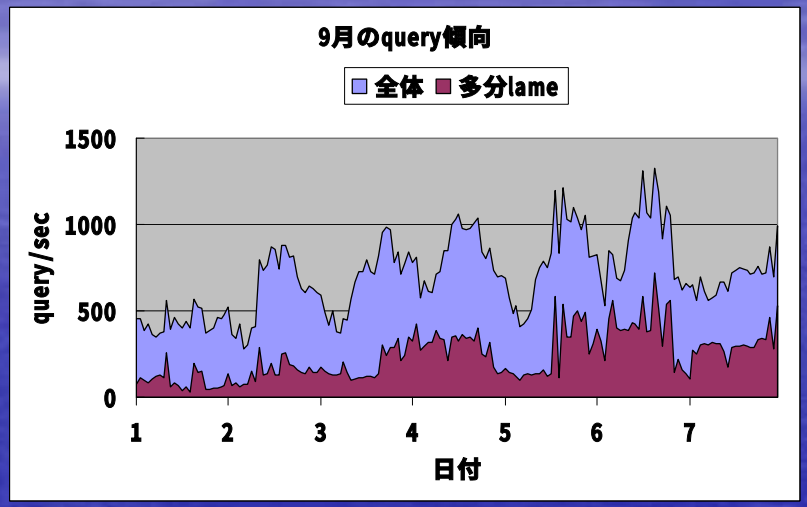
- bind-8.3.0
  - これの影響が邪魔でまともな評価ができない
  - 特徴
    - 同一内容のqueryが一杯
    - lame delegationsが引金
    - 力の限り送出
      - 2000qpsという例も

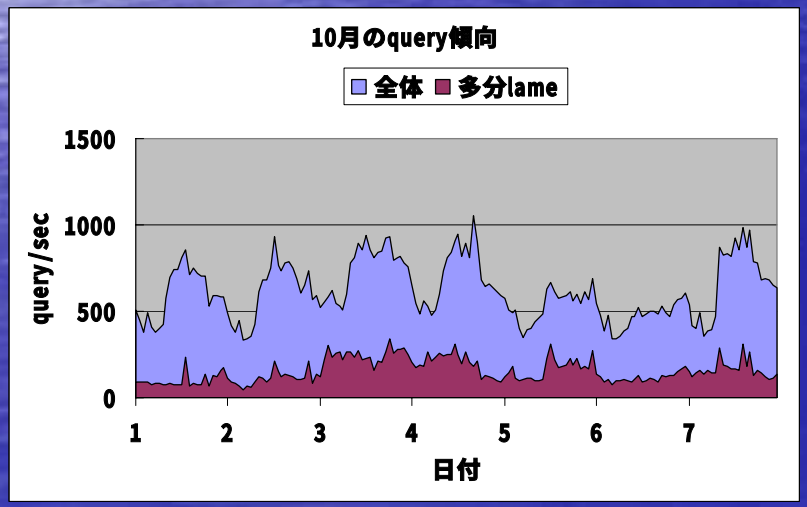
- 影響を取り除く
  - 単位時間当たりのquery
    - サンプリング調査

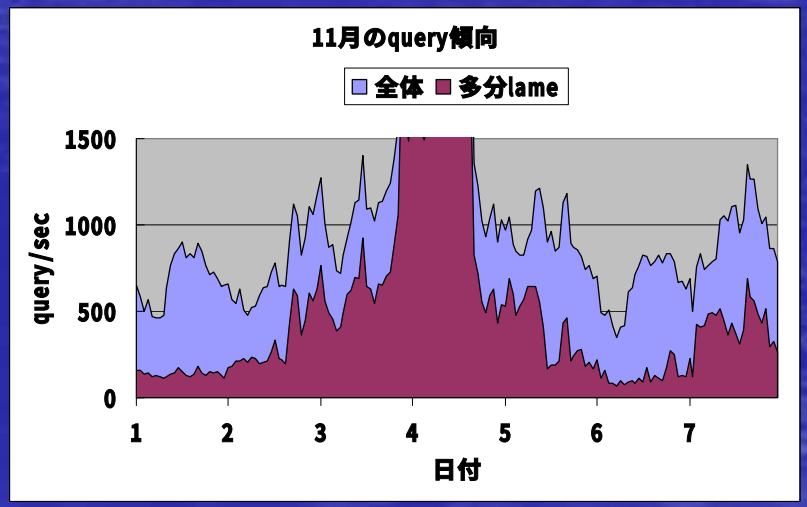
    ⇒確かにlameだ
  - 残ったqueryは？
    - A, SOA, NS, PTR…?
    - 変動 (短期、長期)

ns0.nic.ad.jp

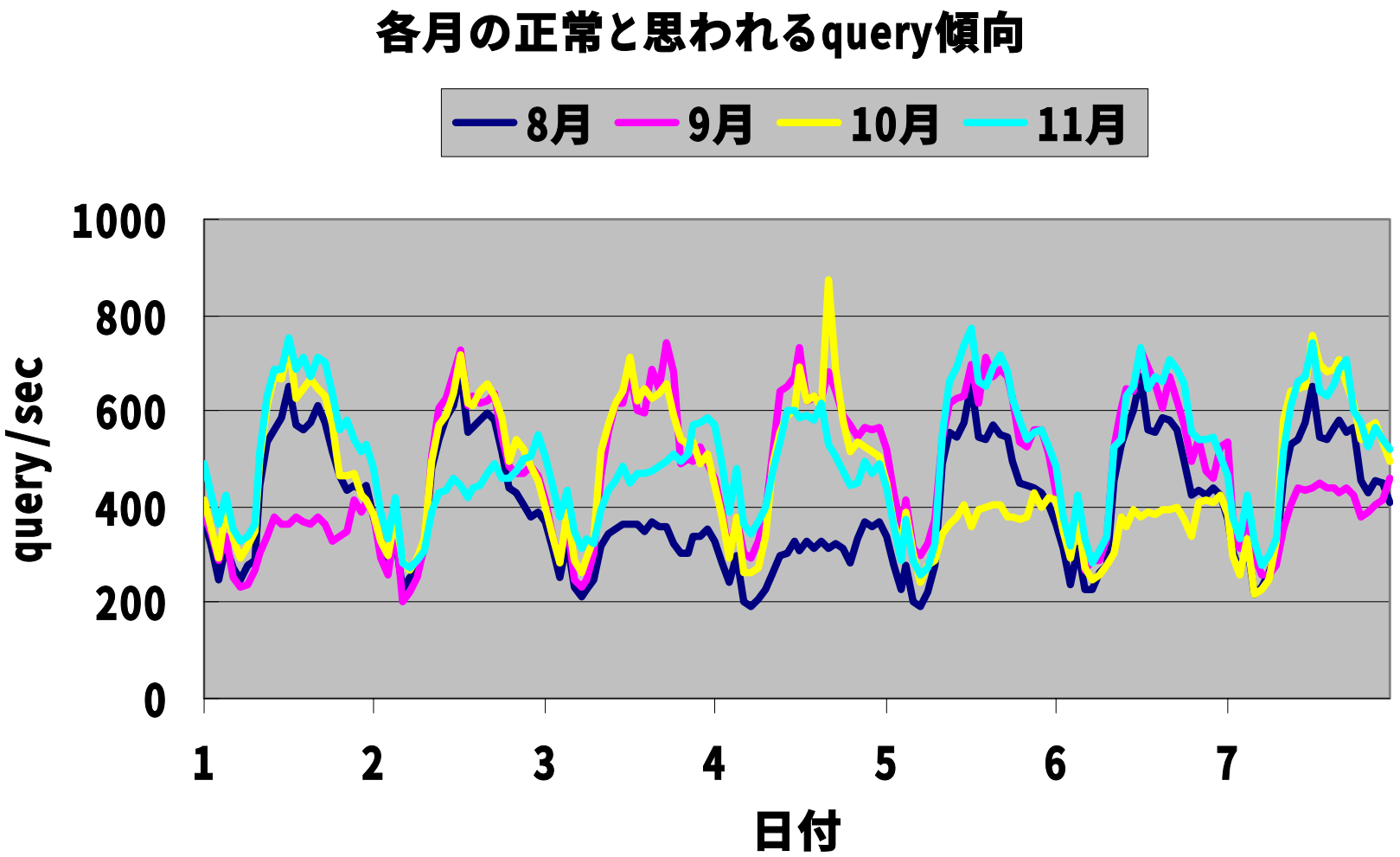

8月のquery傾向
全体
多分lame
1500
1000
500
0
query/sec
1
2
3
4
5
6
7
日付


9月のquery傾向
全体
多分lame
1500
1000
500
0
query/sec
1
2
3
4
5
6
7
日付

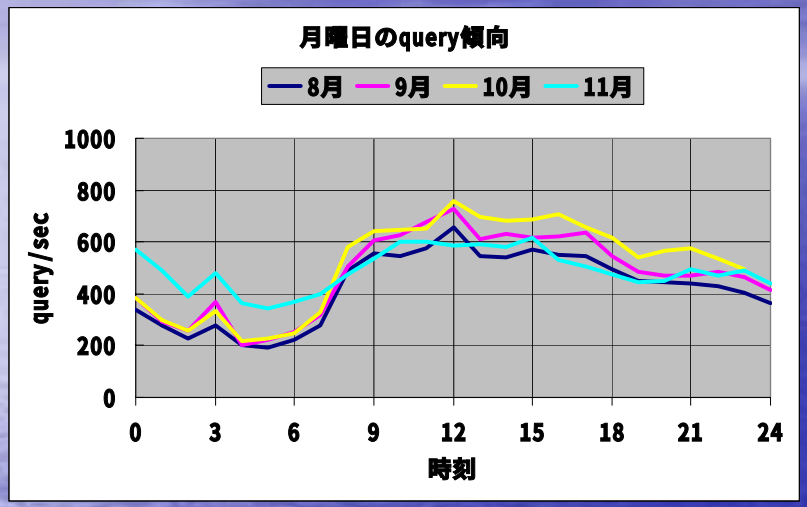

10月のquery傾向
全体
多分lame
1500
1000
500
0
query/sec
1
2
3
4
5
6
7
日付

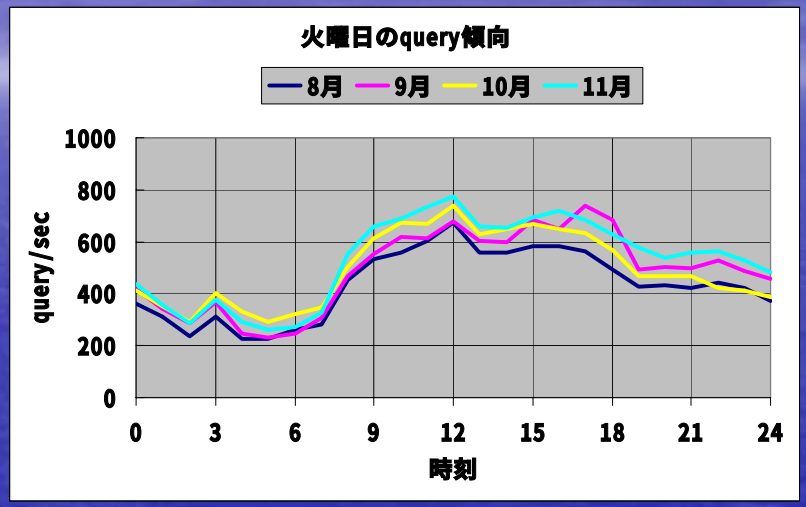

11月のquery傾向
全体
多分lame
1500
1000
500
0
query/sec
1
2
3
4
5
6
7
日付

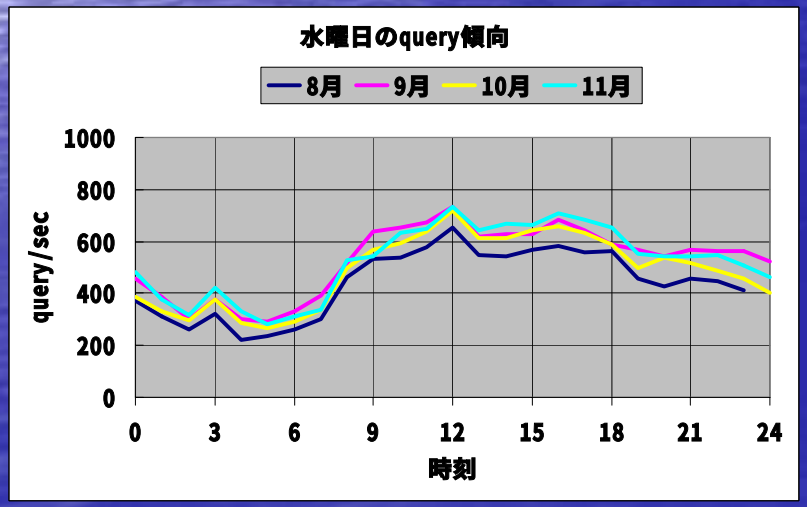
ns0.nic.ad.jp

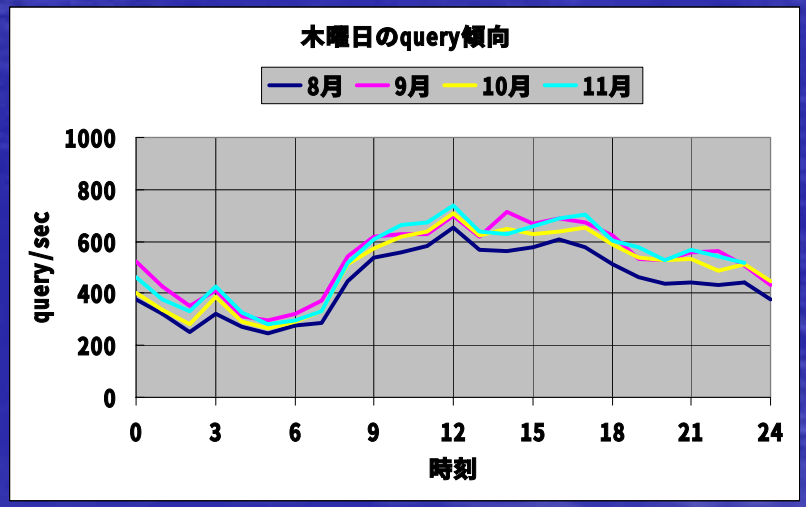

各月の正常と思われるquery傾向
8月
9月
10月
11月
1000
800
600
400
200
0
query/sec
1
2
3
4
5
6
7
日付

ns0.nic.ad.jp

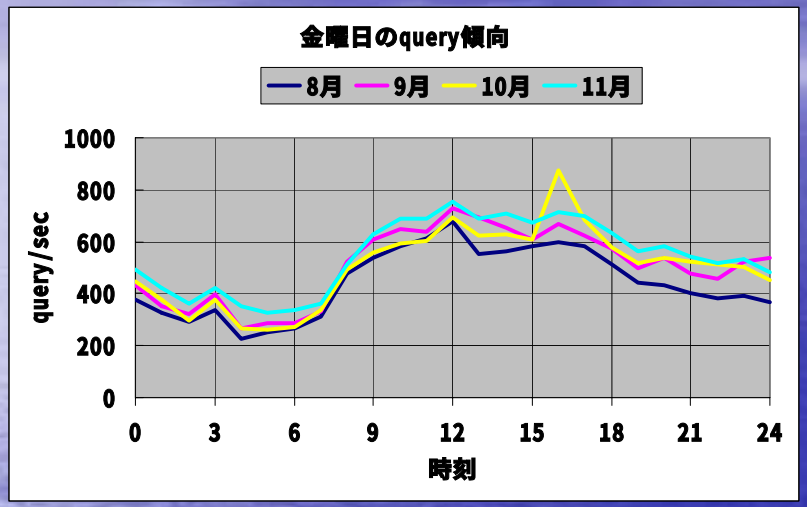

月曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻

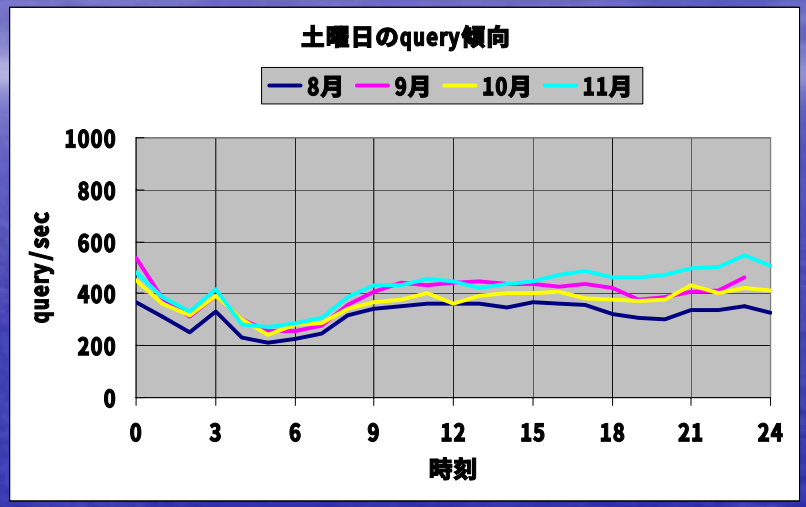

火曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻

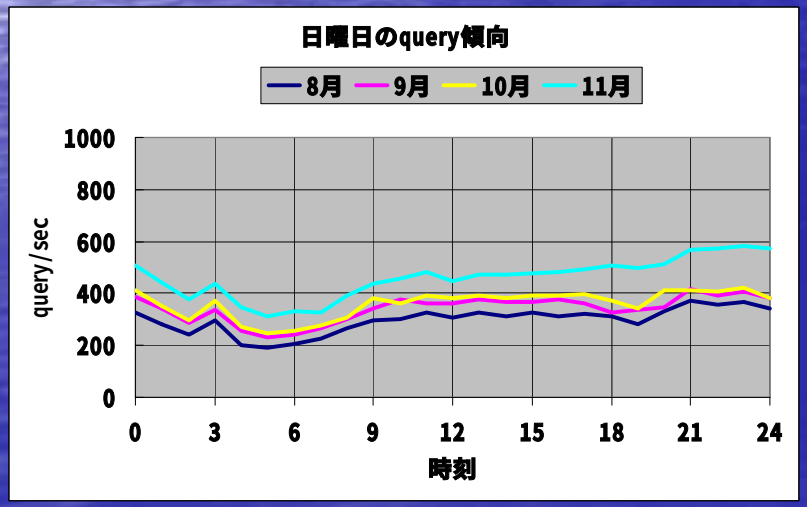

水曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻


木曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻

ns0.nic.ad.jp


金曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻


土曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻


日曜日のquery傾向
8月
9月
10月
11月
query/sec
1000
800
600
400
200
0
0
3
6
9
12
15
18
21
24
時刻

読み取れるもの

- 午前3時のピーク
  - 不明
    - 統計的には局所集中が見られるようだ
    - 逆引きの比率が高い
  - 想像
    - 検索エンジン
    - Log 解析
    - 整合性チェック
    - etc…
- 昼12時のピーク
  - 想像
    - 昔から言われる昼時のサーフタイム
    - 統計データもそれを裏付けている
- 土日は少ない
- 正味では昨年からあまり増えてない

その他

- update が一杯
  - co.jp, ne.jp, jp とか
- recursive queryも
  - 10 qps 程度
  - .com, .net など

ns0.nic.ad.jpに集中

```
; <<>> DiG 9.2.1 <<>> @ns0.nic.ad.jp jp.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17183
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;jp.                            IN      A

;; AUTHORITY SECTION:
jp.                     86400   IN      SOA     ns0.nic.ad.jp. bind-admin.nic.ad.jp. 2002120701 3600
      900 604800 86400

;; Query time: 35 msec
;; SERVER: 202.12.30.131#53(ns0.nic.ad.jp)
;; WHEN: Sat Dec  7 18:06:36 2002
;; MSG SIZE  rcvd: 78
```

やっぱり全体を見たい！

- ということで、2ndary 全体でどかんとquery計測するための計画を算段中です。

Service Level

JPDNSのサービスレベル

- query に確実に答える
  - ping, dig で応答をチェック
    - 対象：全2ndary
- きちんと更新される
  - 更新に応じて dig で SOA のチェック
    - 対象：全2ndary
- 適切な応答時間内に答える
  - 応答時間の計測
    - 対象：.jp, gTLD, その他の全ネームサーバ
    - どこから？：世界各地
    - どうやって：WIDEの手法がとりあえずreasonable

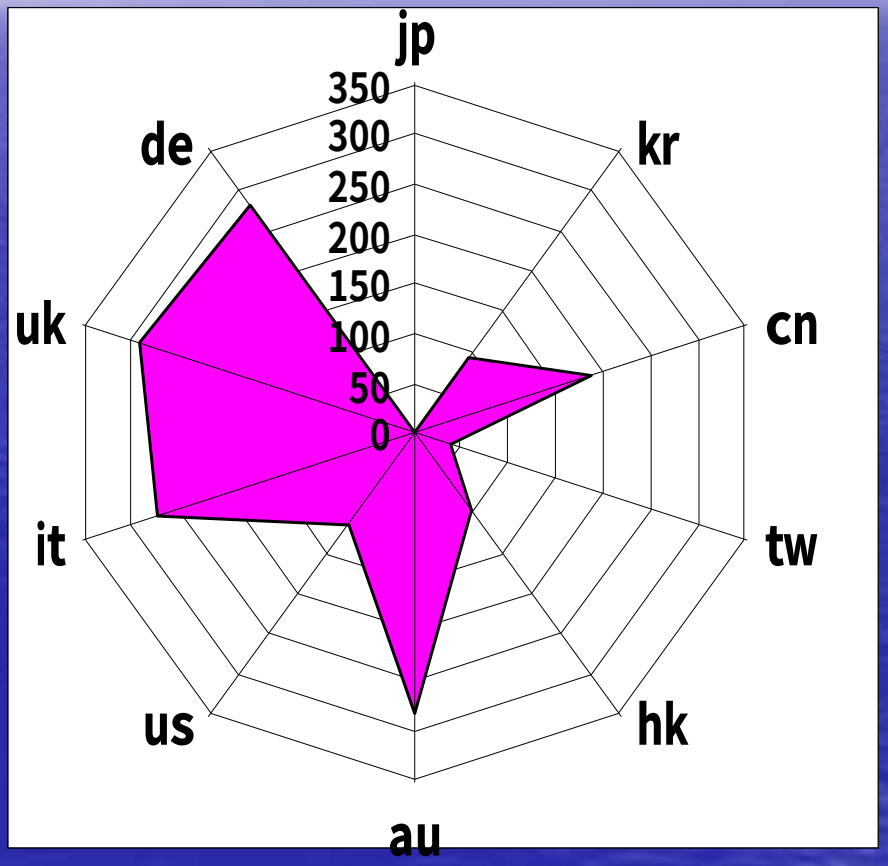
応答時間の計測

- 計測場所
  - 10カ国のアクセスポイントから
    - jp, kr, cn, tw, hk, au, us, it, uk, de
    - GRIC / UUNET / Niftyのローミング
- 手法
  - 各アクセスポイントから全ネームサーバに向けてqueryを投げる
  - 応答時間を適当に補正
    - dial-upによる時間など
  - 最速の応答を採用

JPDNSの応答時間

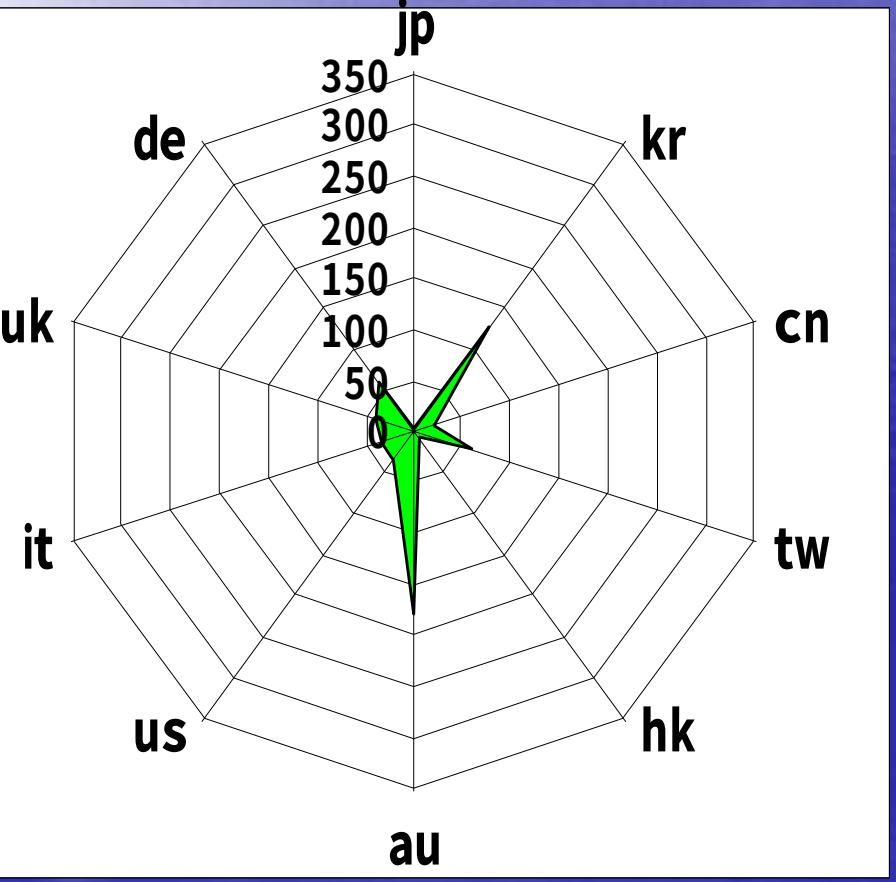
- ヨーロッパが遠い
- オーストラリアも遠い
- APNIC地域は近い

- JPDNSの配置検討
  - 地理的な位置？
  - ネットワーク的な位置？
    - ASとか

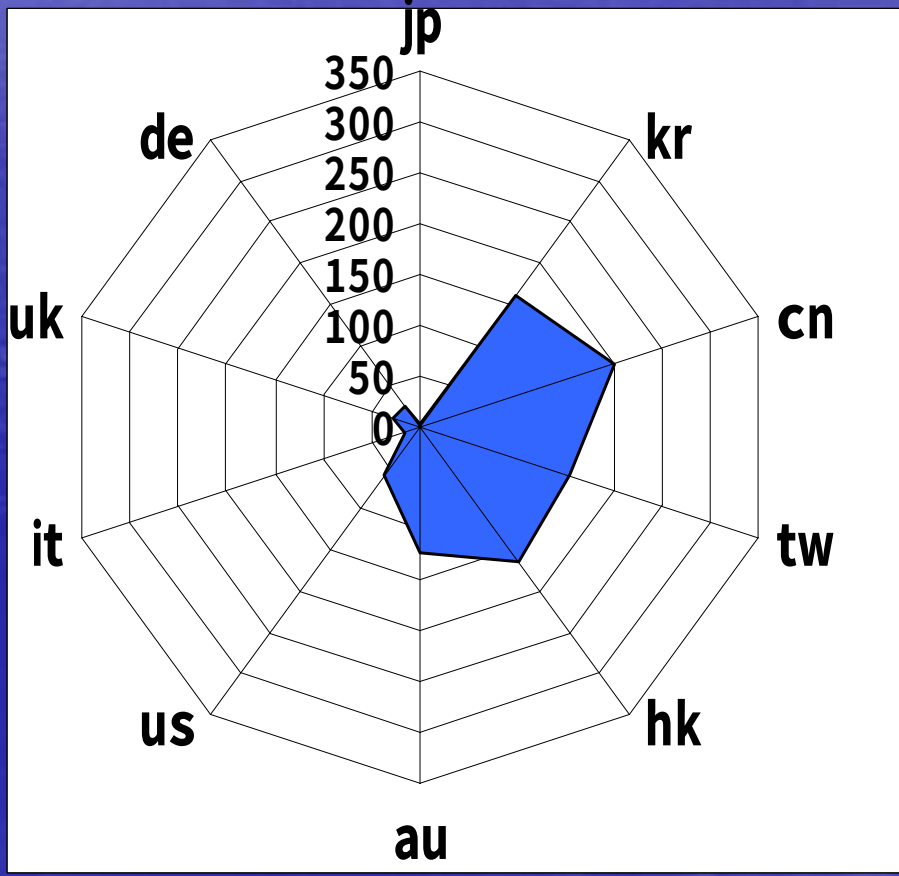


その他のTLD

gTLD(.com, .net, .org)



Euopeのとある国



今後の取り組み

- 計測場所の適正化
  - dial-up をしているので、その地域における標準的な位置かどうかが不明
  - 各国のNICと連携して相互に計測し合う
    - NICやその2ndary組織ならそれなりの場所に？
    - 計測ツールの開発
    - データの収集方法
- 結果を元に配置の最適化
  - ccTLD 間の 2ndary 持ち合い