DNSの可視化と対策

19 Nov 2015

株式会社テリロジー
籠谷和男 (komoriya@terilogy.com)

●サーバ運用の二本柱

可視化
現状を把握

対策
脅威に対応

●可視化から対策へ

可視化

概要把握：長期の傾向把握

↓

特異点特定：局所的な詳細傾向把握

↓

通信特性分析：グラフで兆候を確認

↓

ローデータ確認：packetで裏を取る

↓

対策

対策実施

●既存ツールの様子

DNSサーバの状態を把握したいが、かゆいところに手が届かない

Munin

- サーバ監視ツール
- BIND用プラグインだけでは結構遠い
- rndcと組み合わせればなにかできるかも

Cacti

- ネットワーク可視化ツール
- Muninとある意味同じ感じ
- できなくはない、けど、結構遠い

DSC

- DNS可視化ツール
- 結構見れる
- これでもいいかもしれないけど、詳細情報を調べようとすると掘り下げていけない

●ツールが欲しい

欲しい姿の

既存ツールに出会えない

じゃ、つくろう

欲しいものは

掘り下げられるDNS把握ツール

●欲しいもの

掘り下げられるDNS把握ツール

実現したいこと:

特徴1. 長期傾向から、特異点を特定したい

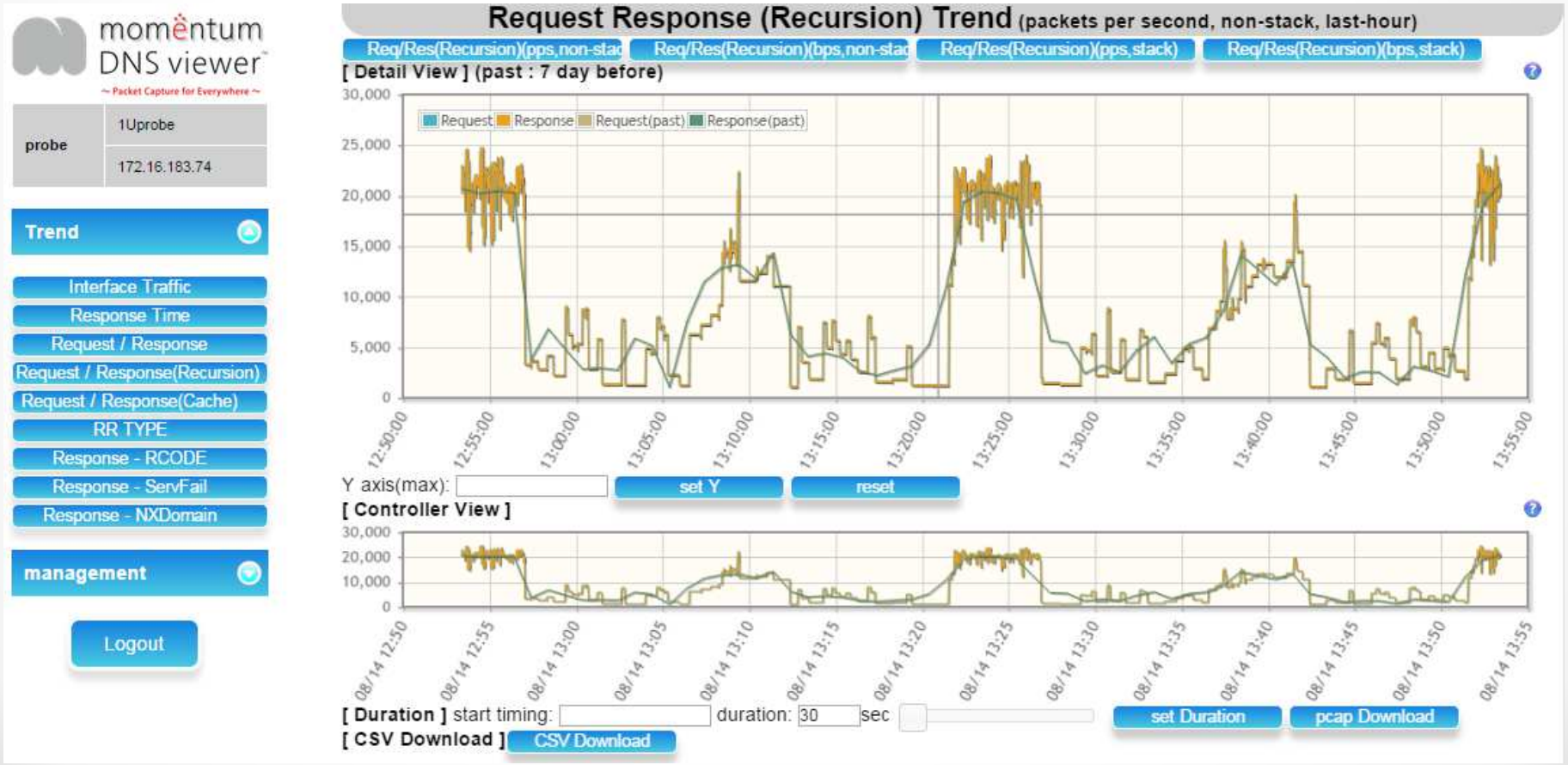
特徴2. 任意の時間帯に対して、状況を把握したい

特徴3. いろいろな切り口で、状況を把握したい

特徴4. 特定の時間帯を、じっくり解析したい

●ツール、つくりました

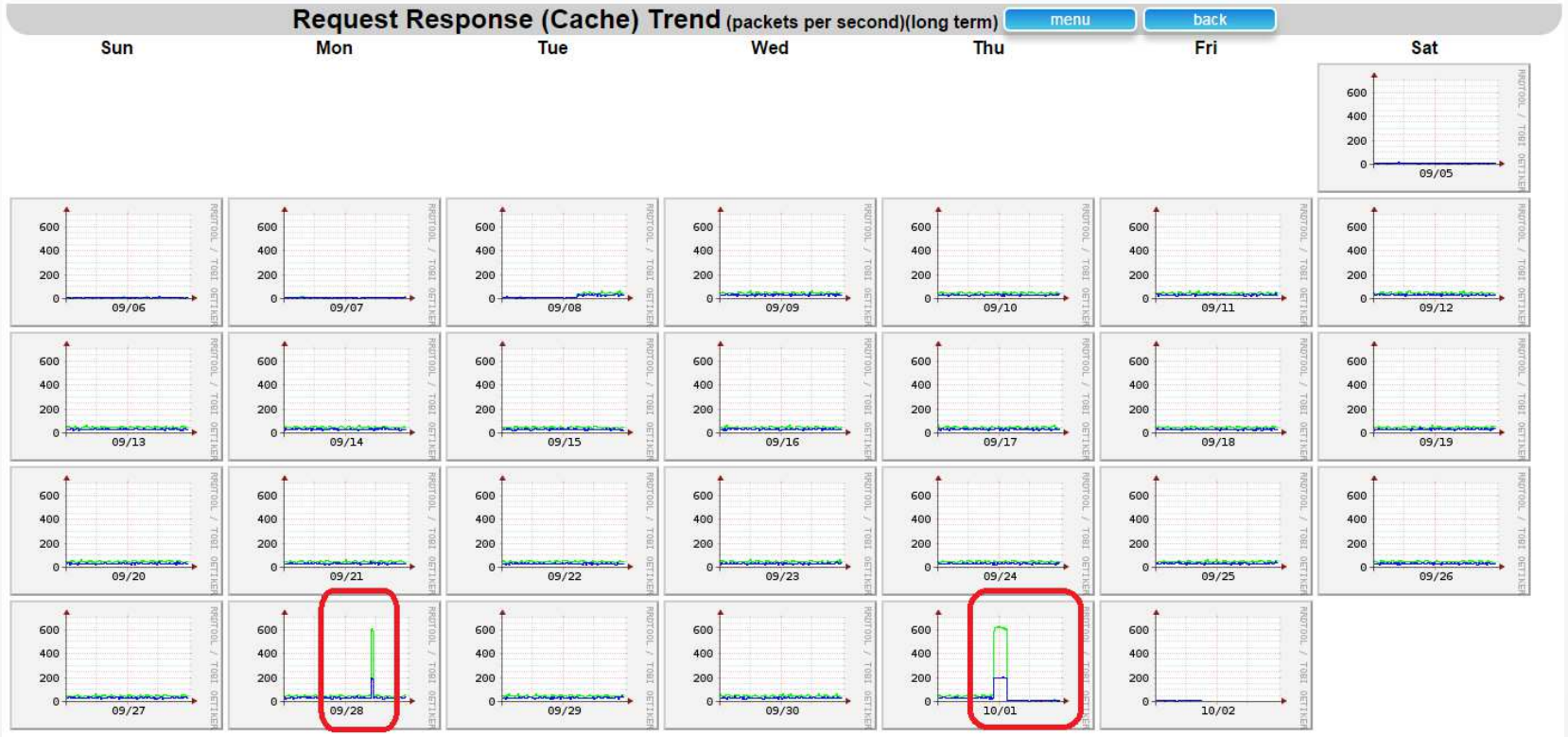
掘り下げられるDNS把握ツール momentum DNS viewer



●特徴1

長期傾向から、特異点を特定したい

4週間の傾向を一望し、特異点を探せる



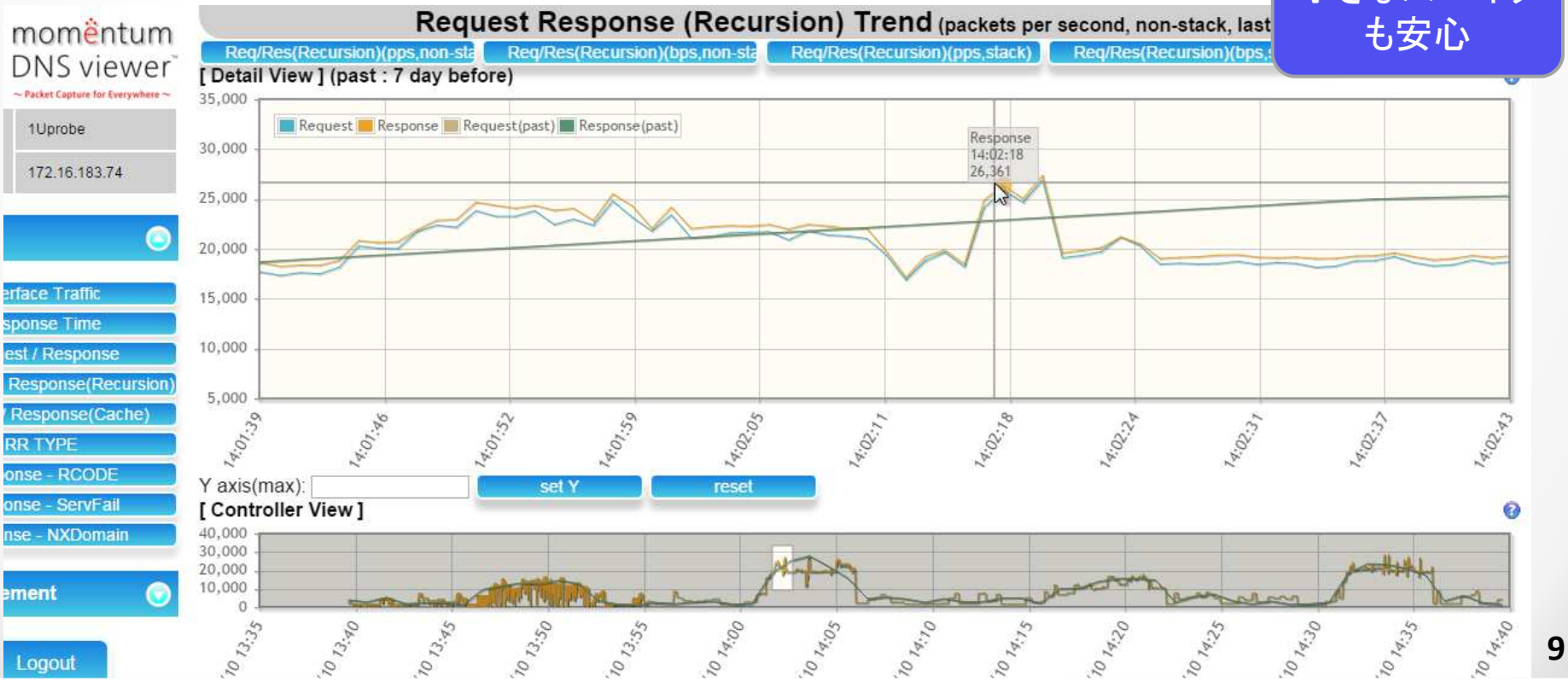
●特徴2

任意の時間帯に関して、状況を把握したい

見たいところに注目できる、ズームインできる

1秒単位で把握できる・bpsもppsもわかる

小さなスパイクも安心



●特徴3

いろいろな切り口で、状況を把握したい

切り口を切り替えながら、傾向把握できる

時系列可視化

- Interface Traffic
- Response Time
- Request / Response
- Request / Response(Recursion)
- Request / Response(Cache)
- RR TYPE
- Response - RCODE
- Response - RCODE Error Rate
- Response - ServFail
- Response - NXDomain

TOP10可視化

- Request TOP Name
- Request TOP Clients
- Response TOP Clients
- TOP DNS Server
- Trend TOP DNS Server
- TOP FQDN NX
- TOP Domain NX

FQDNそのままのNXDomain

FQDNを任意のsub domainで集計したNXDomain

●特徴4

特定の時間帯を、じっくり解析したい

絞り込んでPCAPを取得できる

RCODE TrendからのPCAPダウンロードの例：

[pcap Information]
start time : 2015/11/10 14:44:18
duration : 298 sec

All
pcap size : [46,703,747] packets
: [29,782,315,851] bytes
condition : []

too large pcap(> 1,024,000,000 bytes)

[pcap Download]

too large

DNS Response(All)
pcap size : [1,794,292] packets
: [393,283,132] bytes
condition : [-n 14=1]

Please check pcap file size.

[pcap Download]

Download

DNS Respor
pcap size : [
condition : [

Please check pcap file size.

[pcap Download]

Download

RCODE breakdown list

RCODE	packet count	size(bytes)
1 (FormErr)	7	1,095
2 (ServFail)	420	42,346
3 (NXDomain)	412,421	75,156,796
4 (NotImp)	14	1,072
5 (Refused)	68	5,386
8 (NXRRSet)	4	304
12	2	246

DNS Response(NXDomain)
pcap size : [412,421] packets
: [75,156,820] bytes
condition : [-n '17=3']

Please check pcap file size.

[pcap Download]

Download

DNS Response(Refused)
pcap size : [68] packets
: [5,410] bytes
condition : [-n '17=5']

Please check pcap file size.

[pcap Download]

Download

DNS Response(without NO_ERROR)
pcap size : [412,936] packets
: [75,207,269] bytes
condition : [-n '17!=0']

Please check pcap file size. (breakdown list)

[pcap Download]

Download

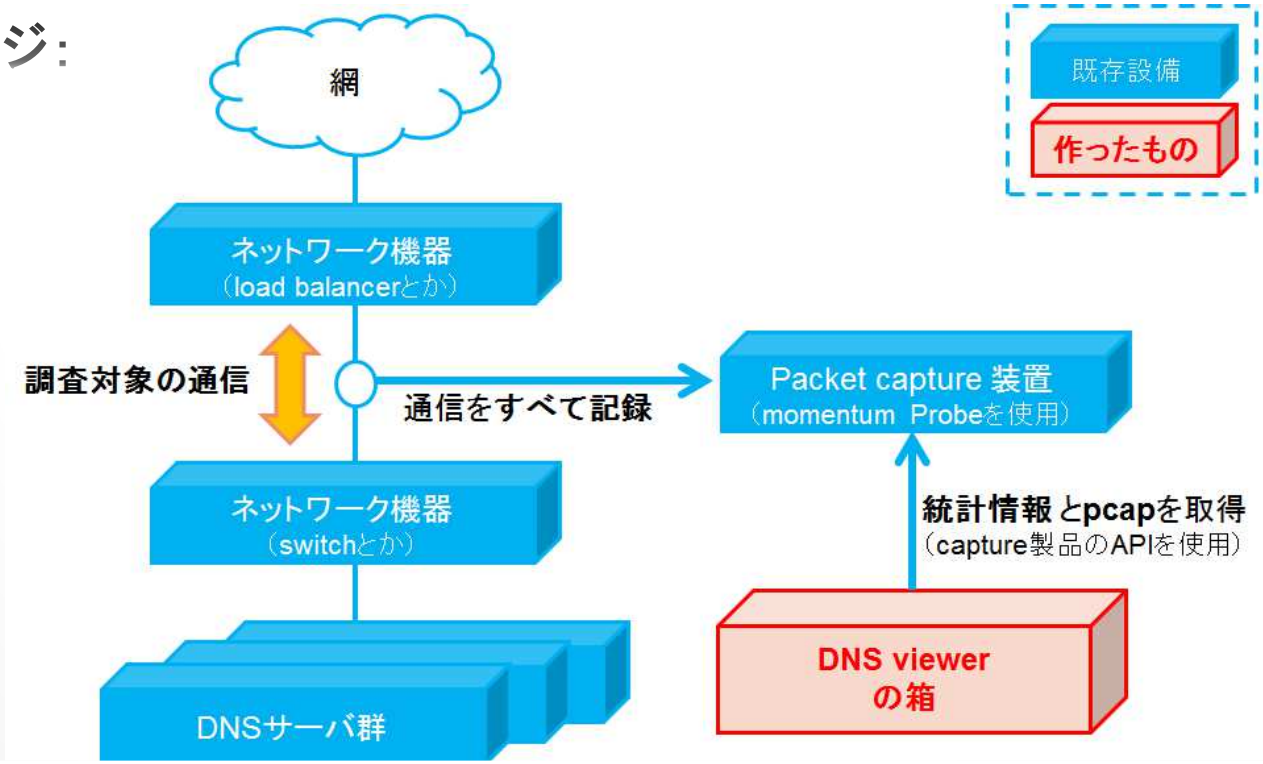
●ツールの利用

http://tapas.terilogy.com/projects/dns_viewer/news

利用前提　　:パケットキャプチャに
momentum Probeを利用する

ユーザ登録　:必要
利用　　:無償でOK

構成イメージ:



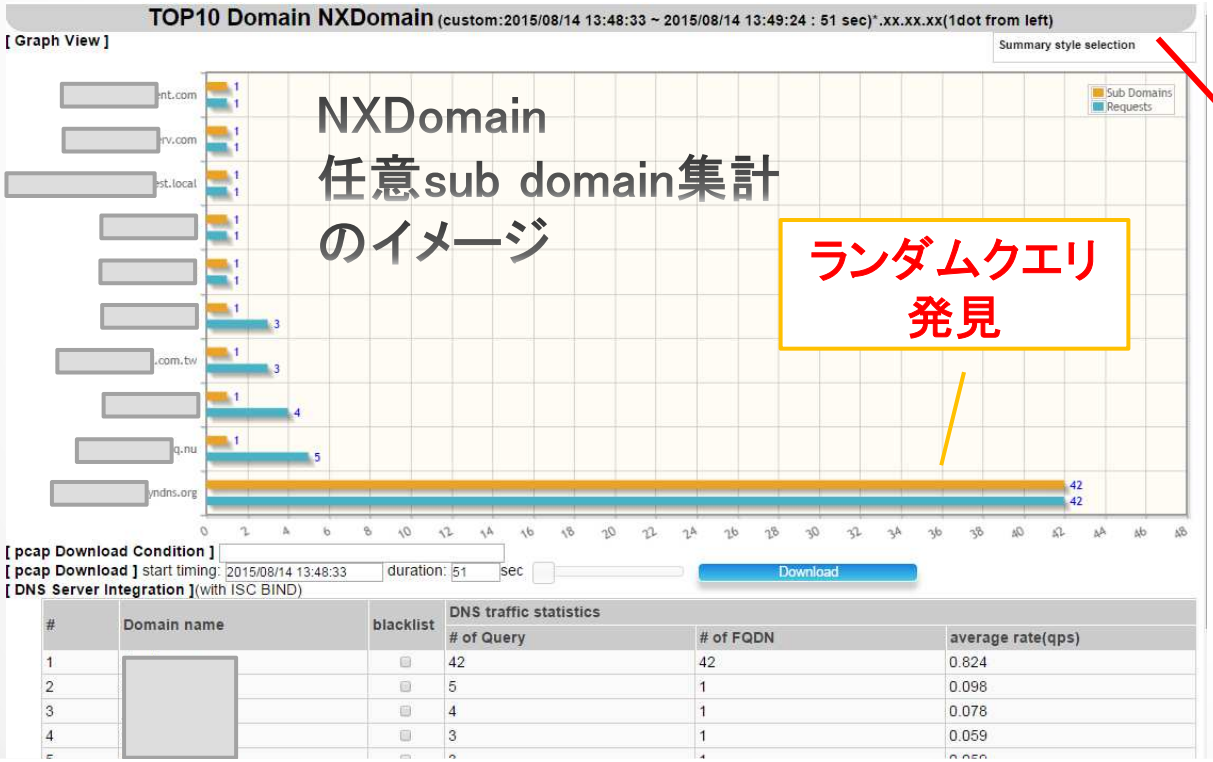
●ツールの利用シーン

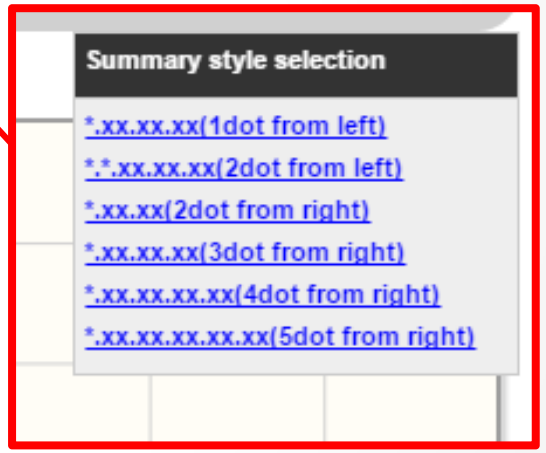
普段使い：

- 日々の業務として、傾向を把握する
  → 早期の兆候把握を実現

個別の利用：

- 障害調査・問い合わせ対応に使う
- Slow Drip（水責め）を簡単に可視化する





画面例において、
一部、伏字

●まとめ

掘り下げられるDNS把握ツール、DNS viewerあります

http://tapas.terilogy.com/projects/dns_viewer/news

特徴1	特徴2	特徴3	特徴4
・長期傾向から特異点を把握できる	・任意の時間帯に関して、状況を把握できる	・いろいろな切り口で、状況を把握できる	・特定の時間帯を、じっくり解析できる

おしまい

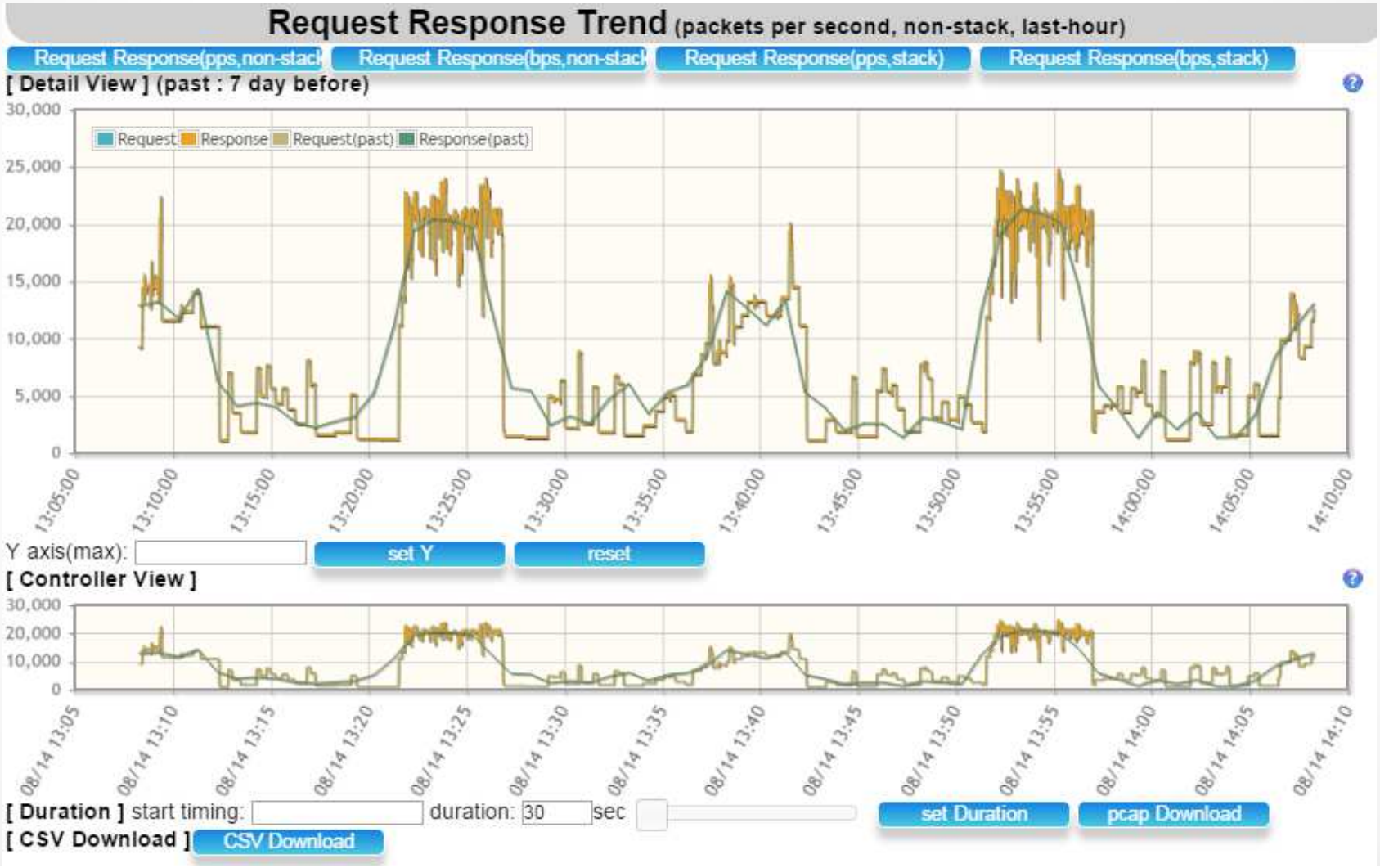
付録

先週より多い、とか確認

DNSの可視化と対策

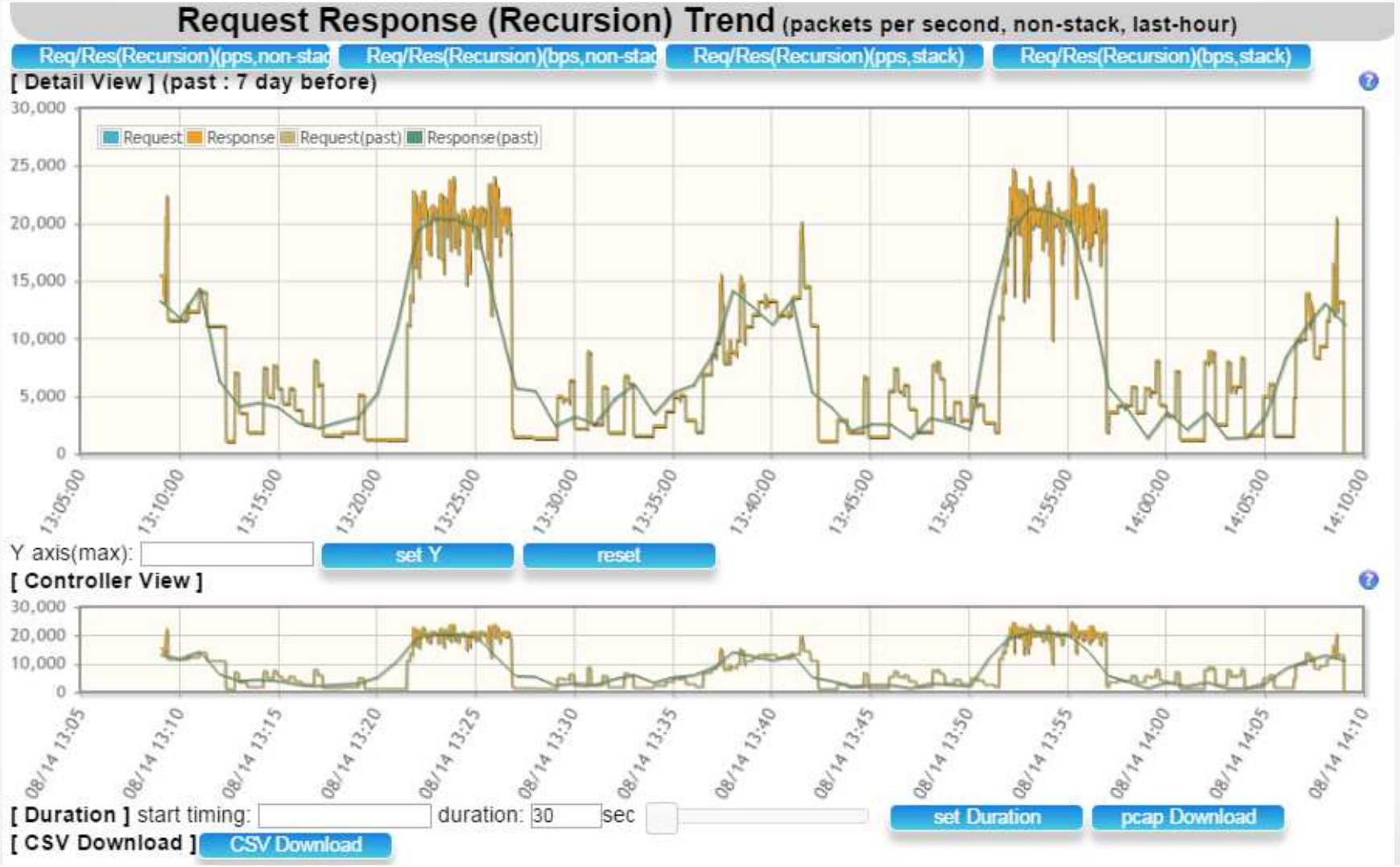
●付録：Trend画面例

DNSのRequestとResponseが見えました（過去情報付）（1秒粒度）



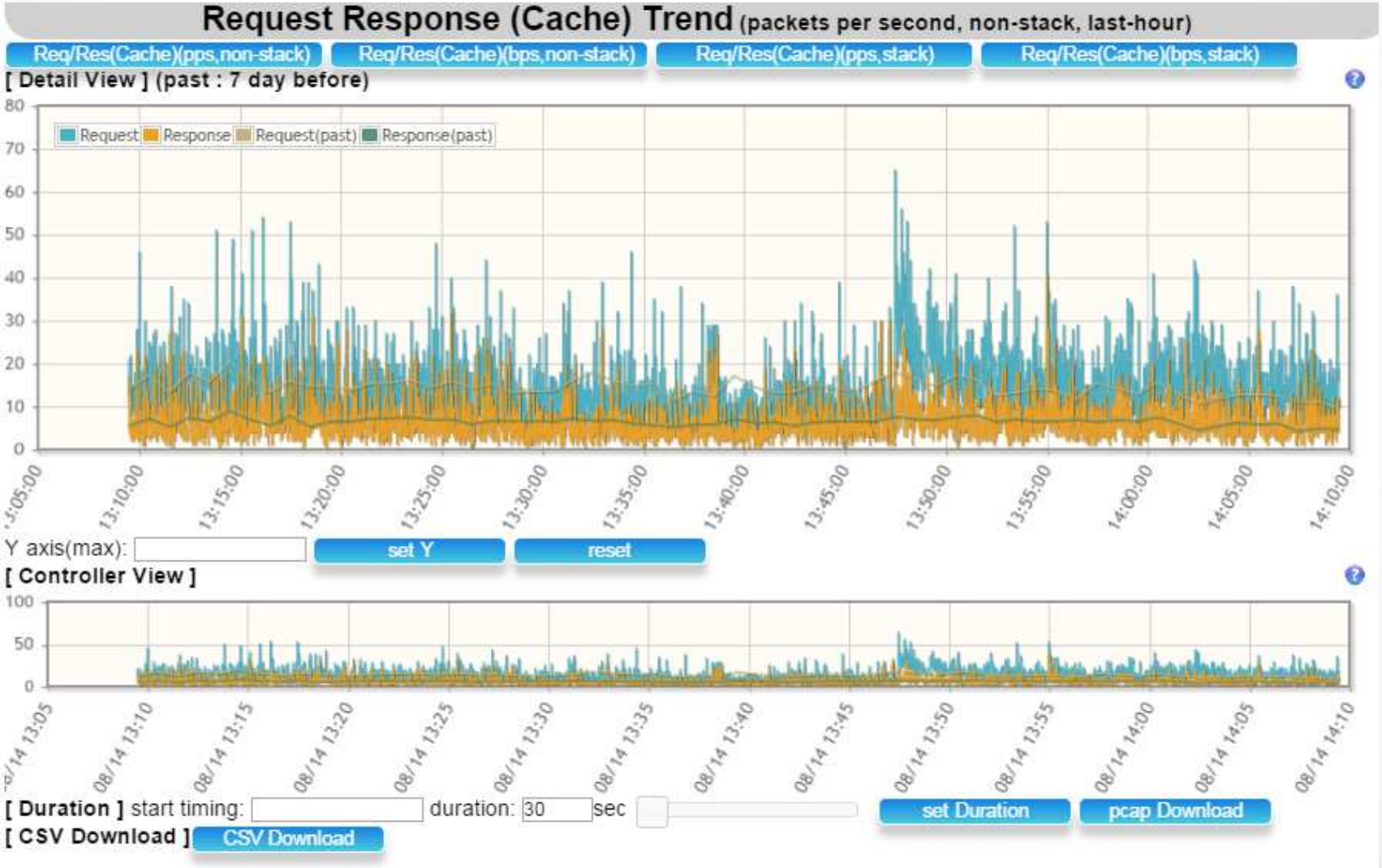
●付録：Trend画面例

DNSのRequestとResponseが見えました（Recursion Desiredのみ）



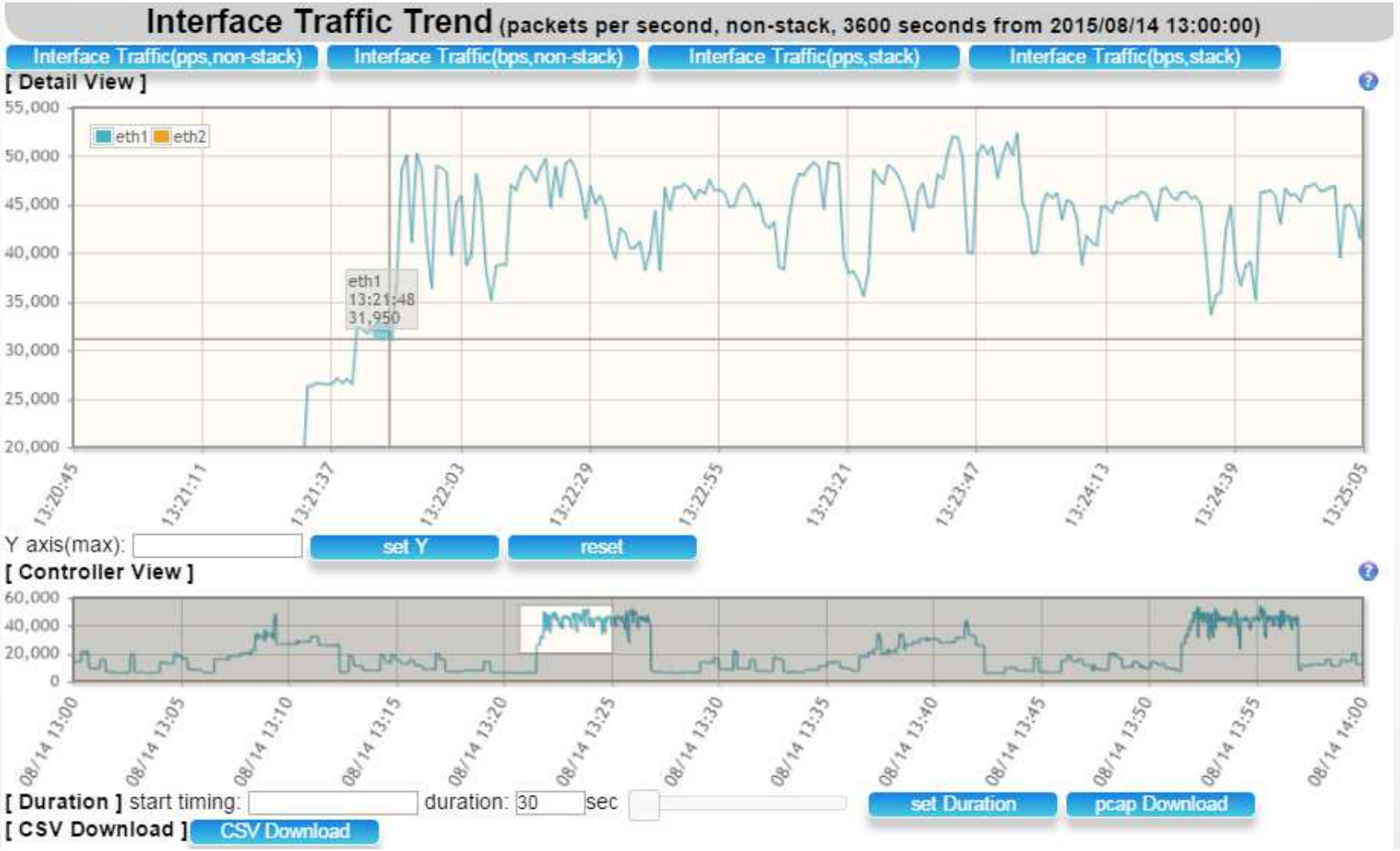
●付録：Trend画面例

DNSのRequestとResponseが見えました（Cache Serverの通信のみ）



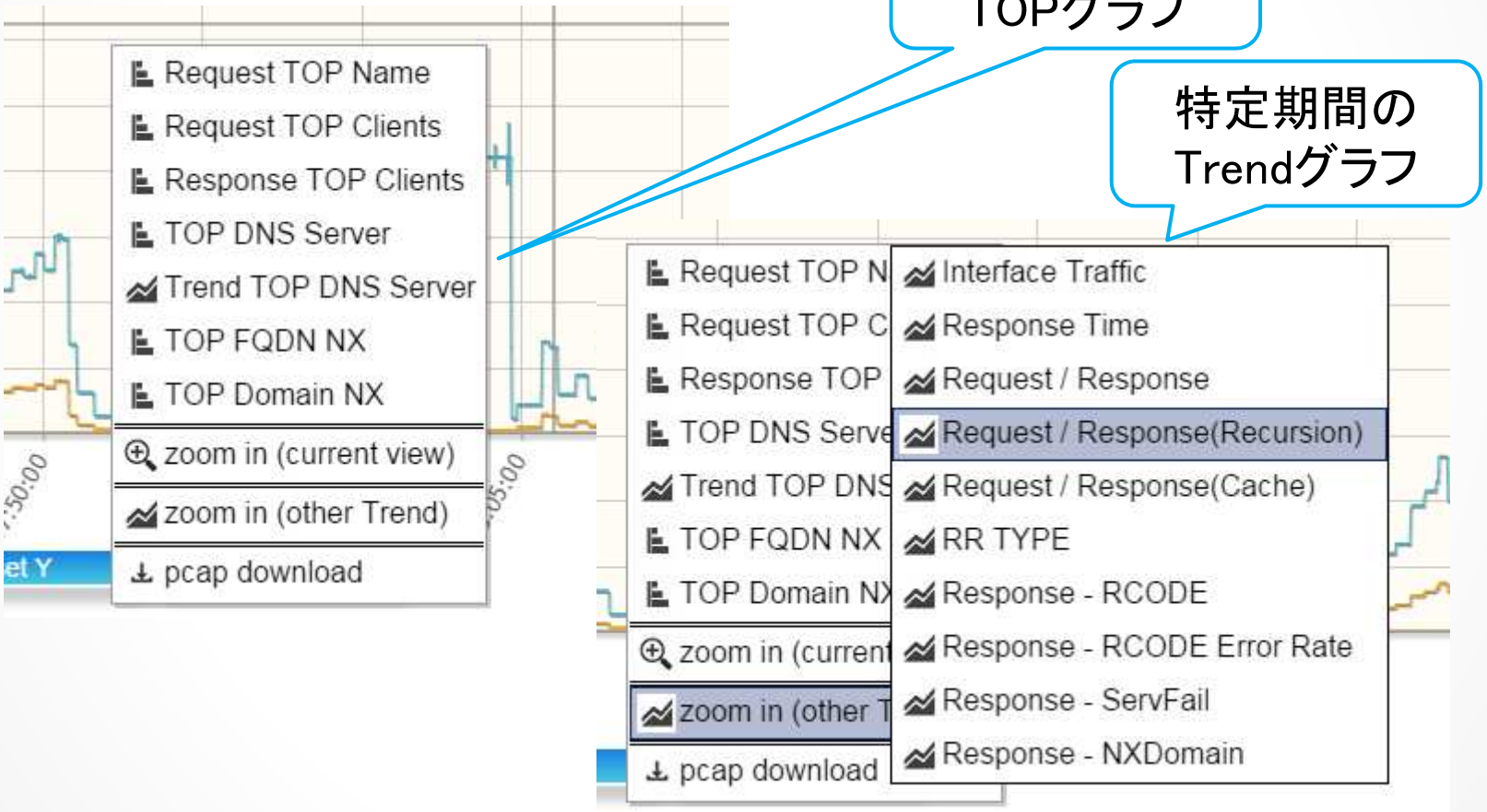
●付録：Trend画面例

拡大できます



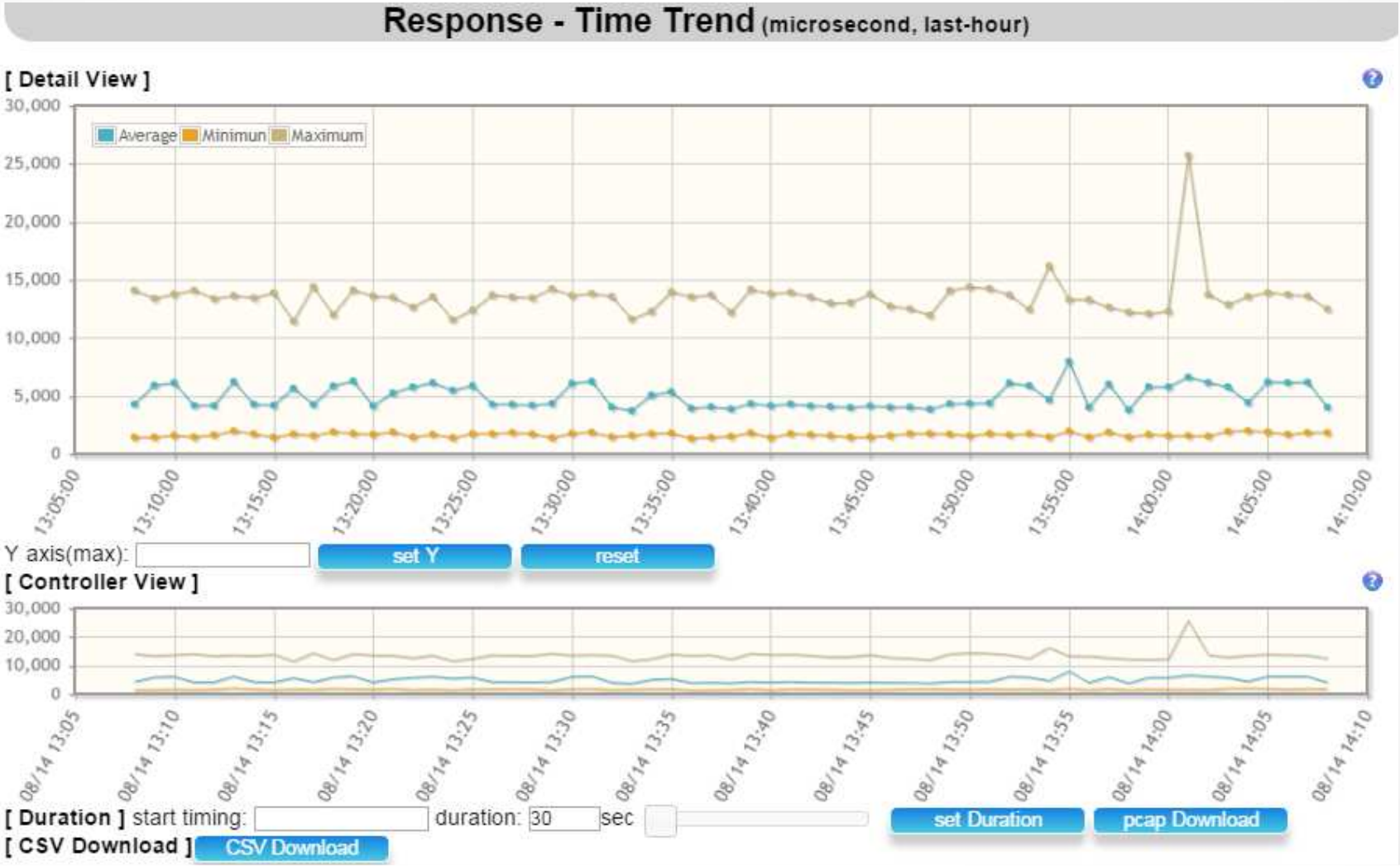
●付録：Trend画面例

各種グラフを確認できます



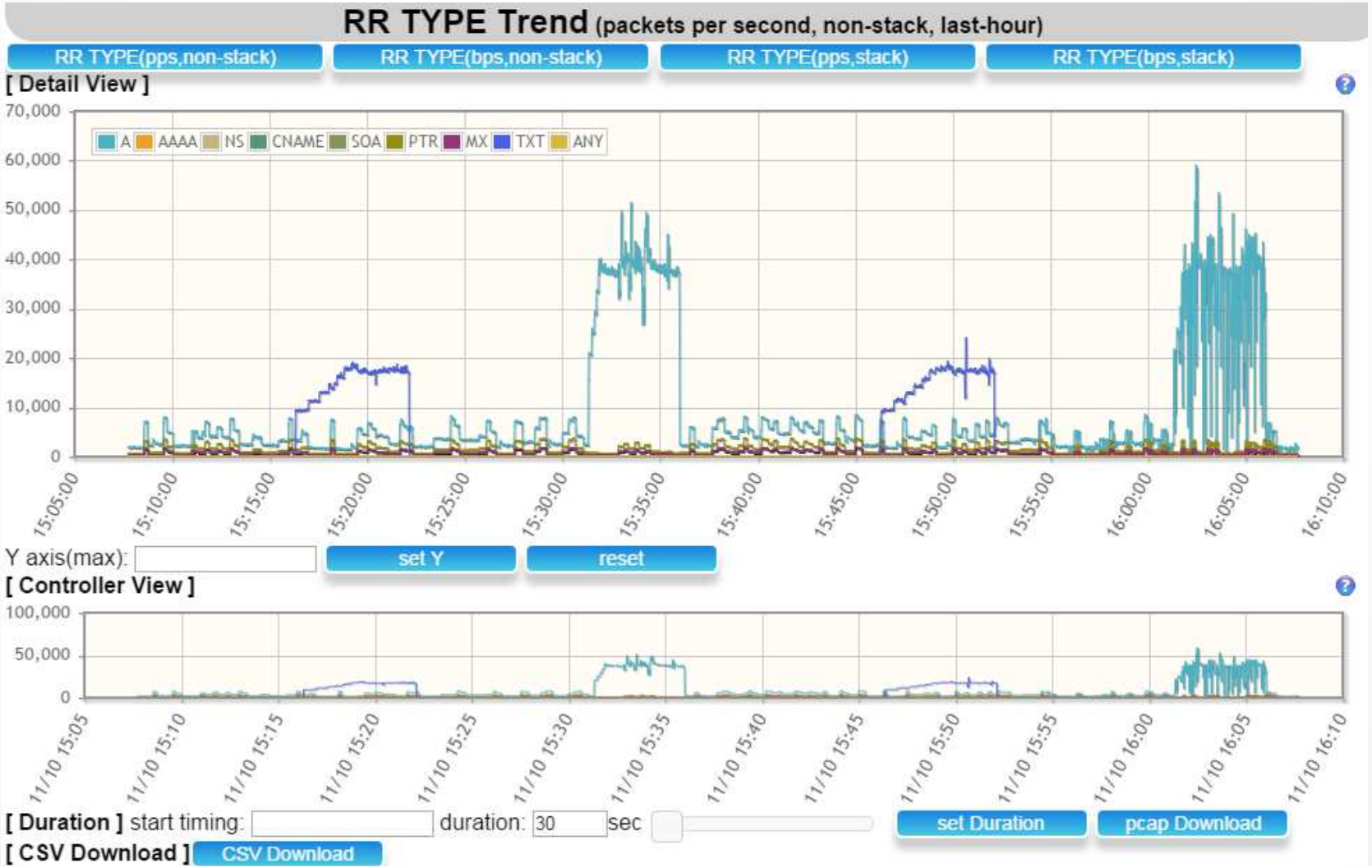
●付録：Trend画面例

DNSサーバ応答時間確認できます（ただしactive検査）



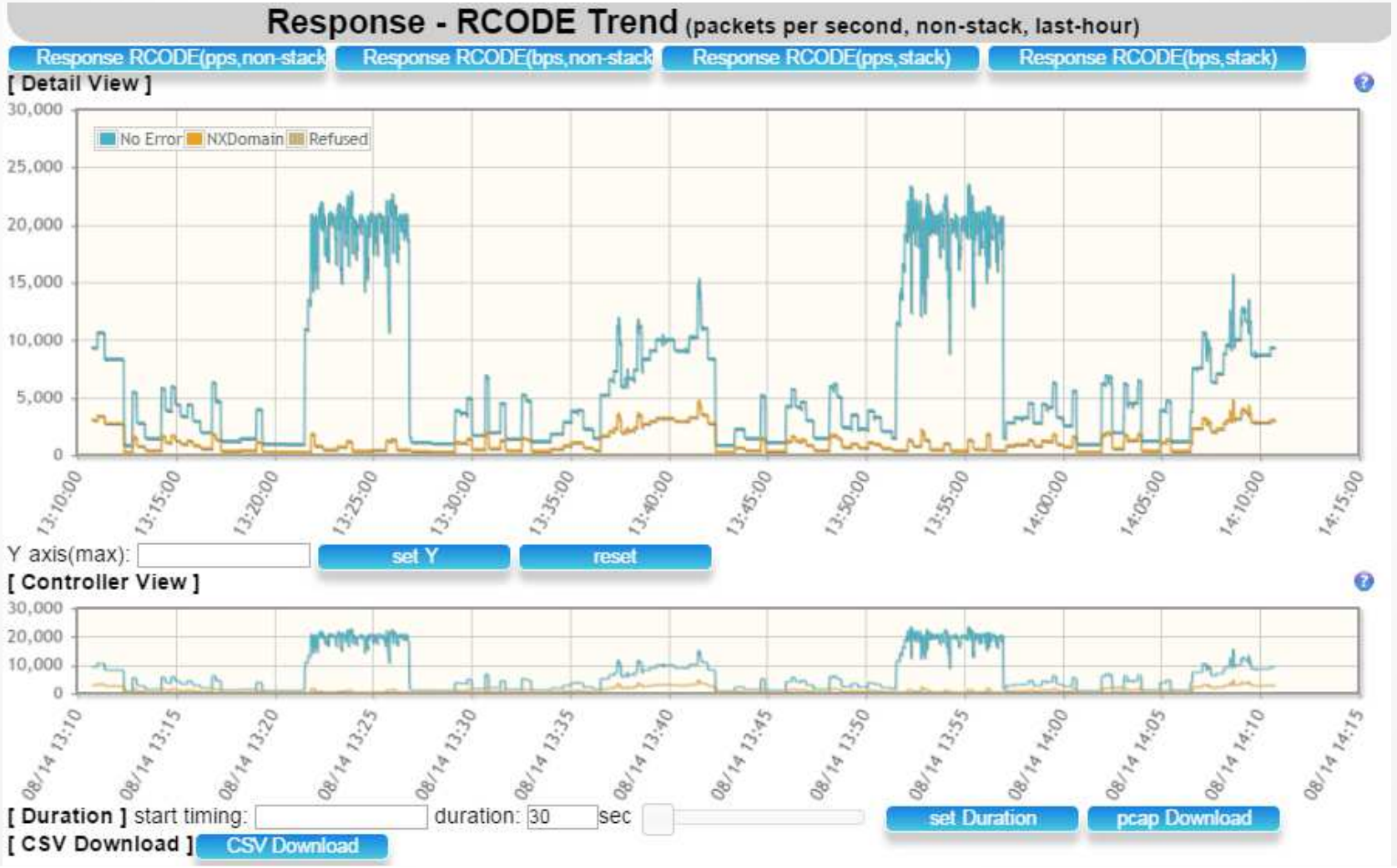
●付録：Trend画面例

DNSのRRの配合見えます



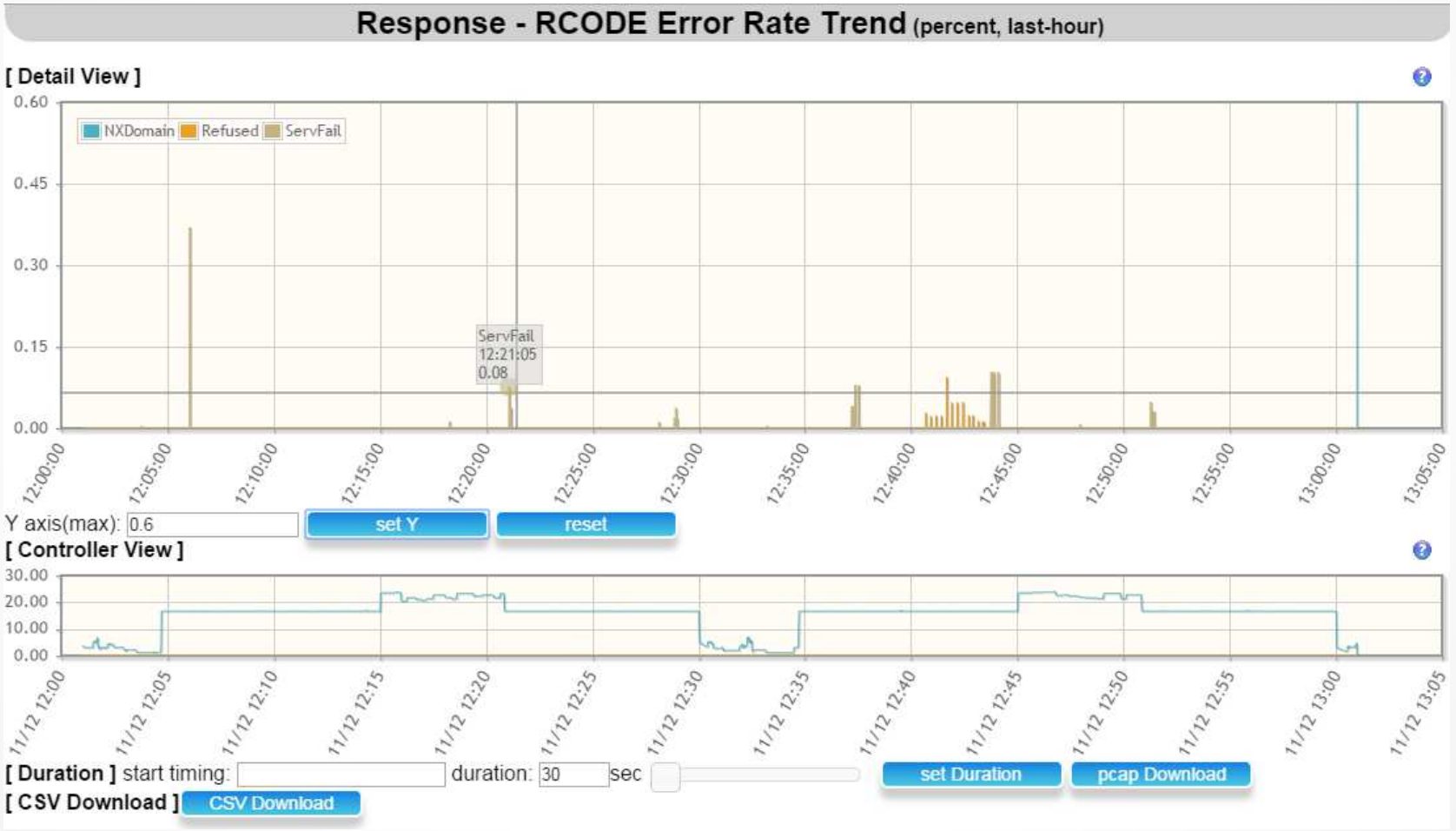
●付録：Trend画面例

DNSのRCODEの配合見えます



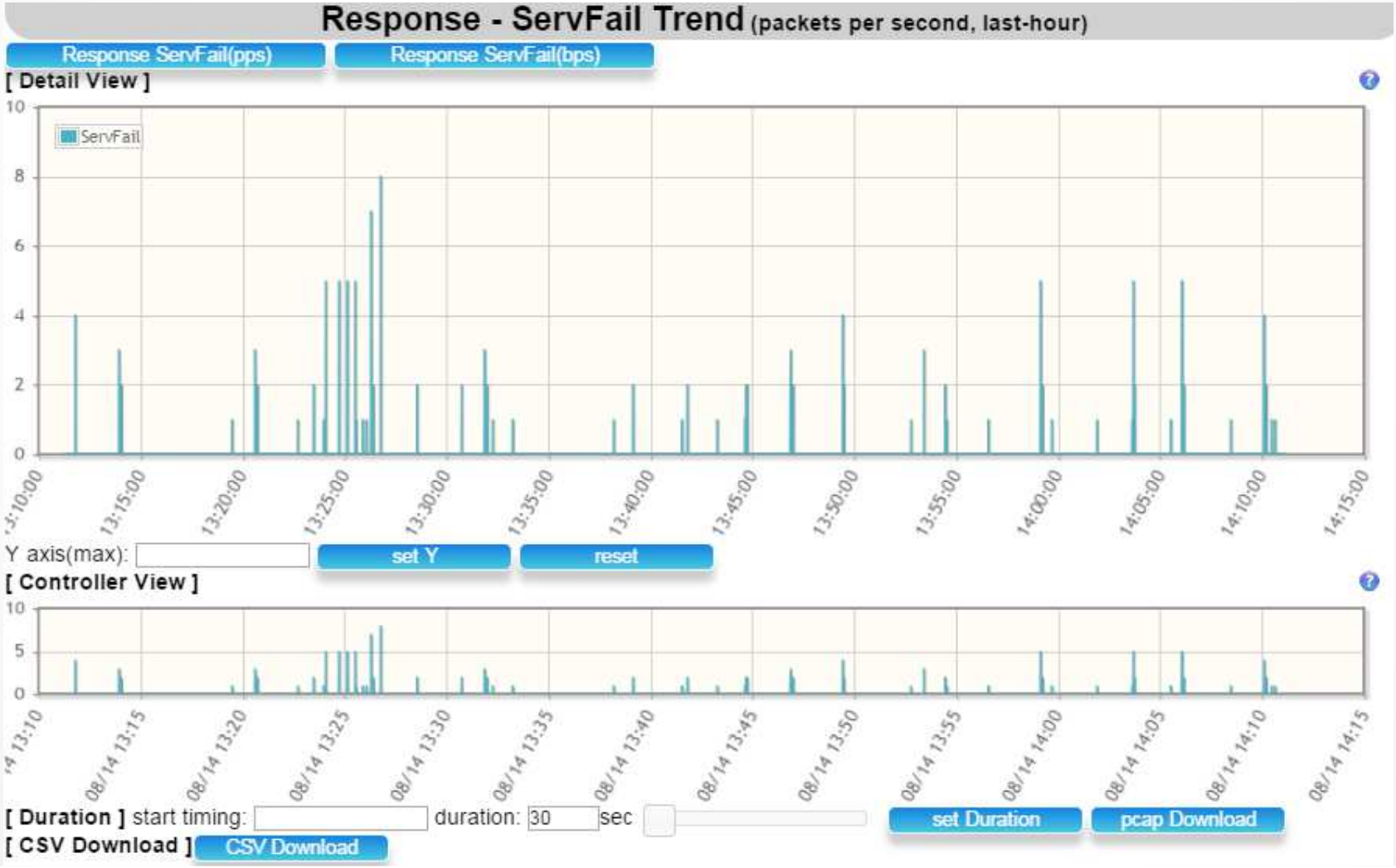
●付録：Trend画面例

DNSのRCODEの比率見えます



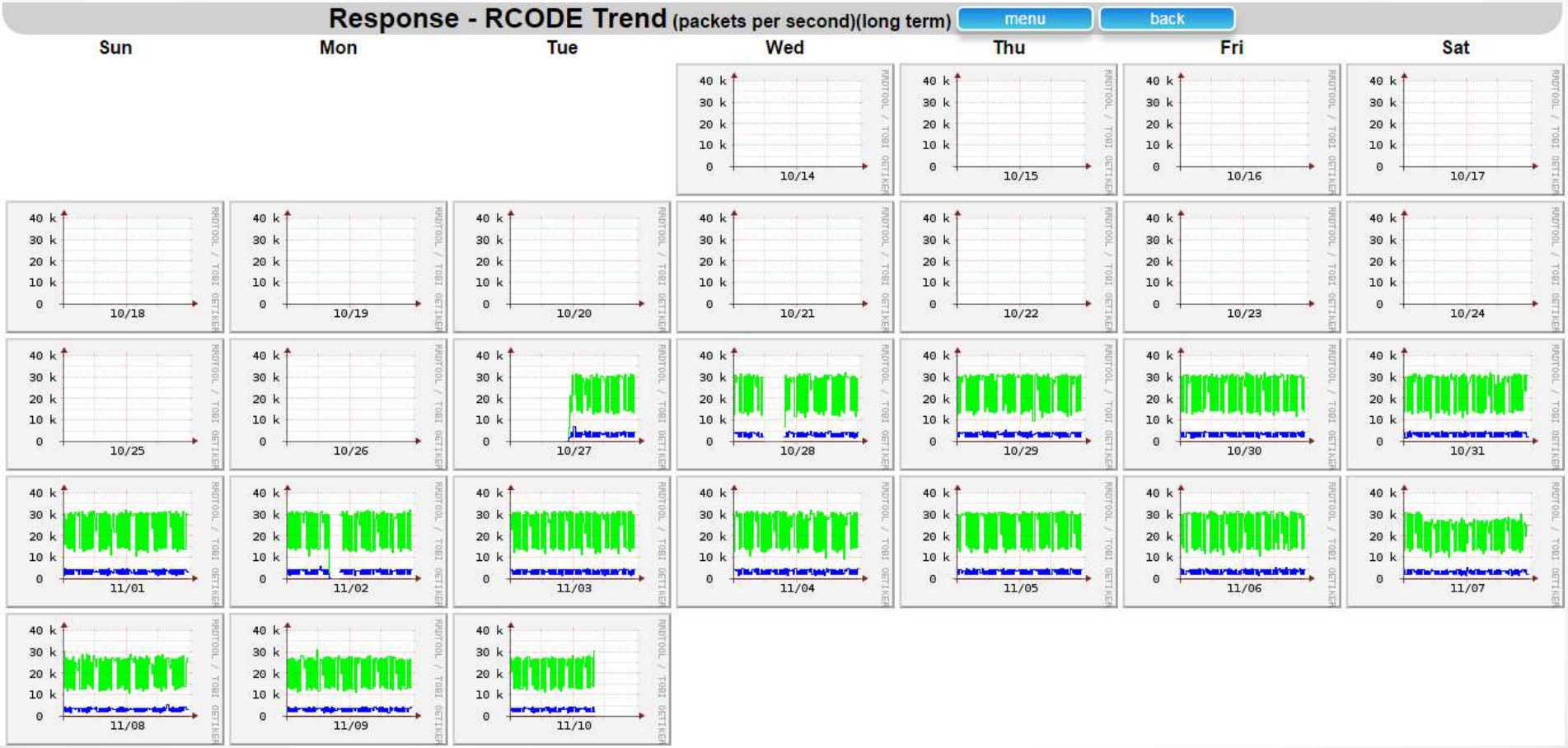
●付録：Trend画面例

ServFail見えます



●付録：Trend画面例

どの種類のTrendも長期傾向が見えます



●付録：キャプチャの統計情報

統計情報が取得できるキャプチャ装置を使っています

momentum Probe ： http://www.terilogy.com/momentum/

統計情報の検索例：