

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

DNSの可視化と対策

可視化
現状を把握

対策
脅威に対応

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

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掘り下げていけない

● ツールが欲しい

DNSの可視化と対策

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

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

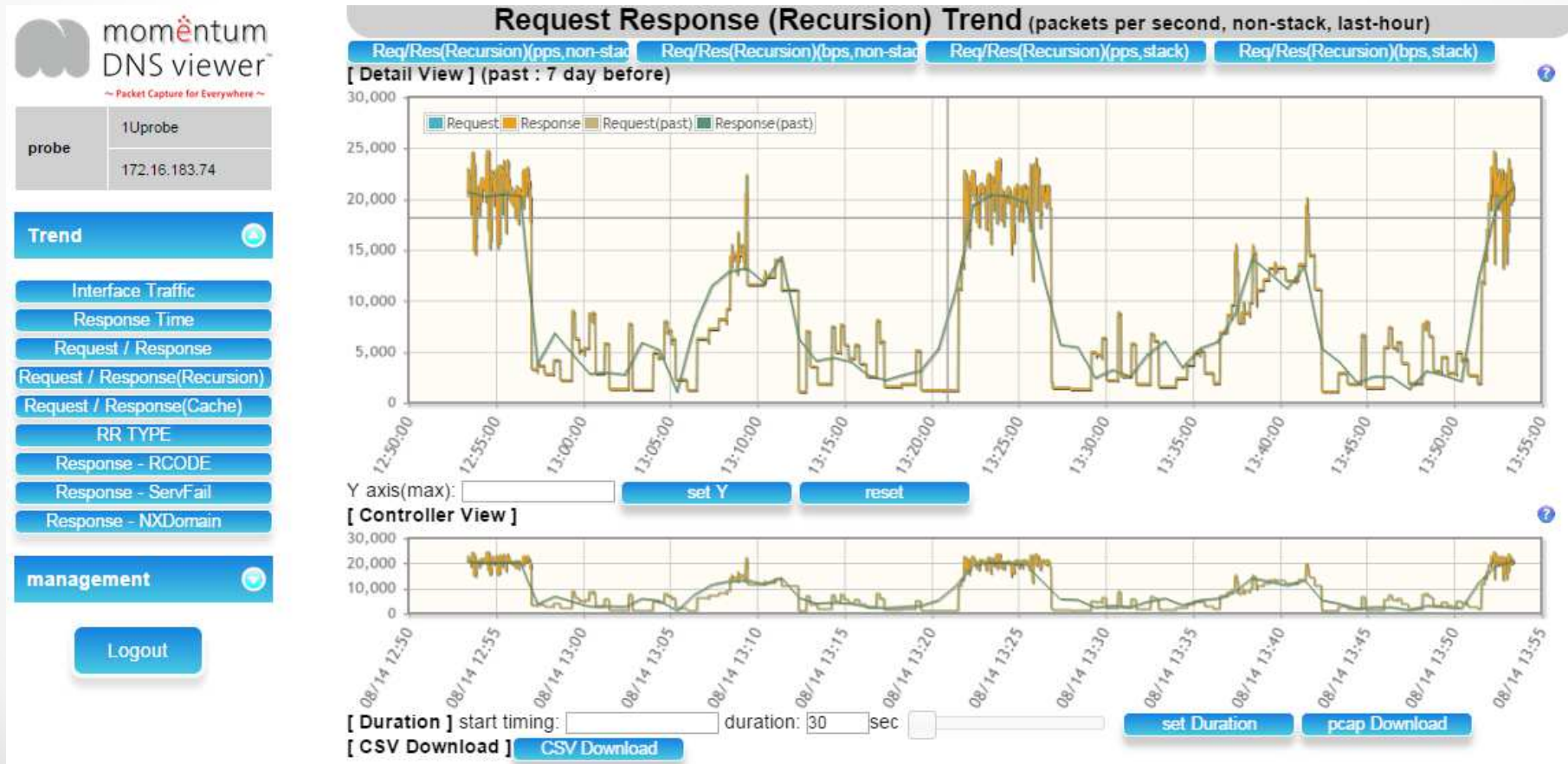
特徴3. いろいろな切り口で、状況を把握したい

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

DNSの可視化と対策

掘り下げられるDNS把握ツール momentum DNS viewer

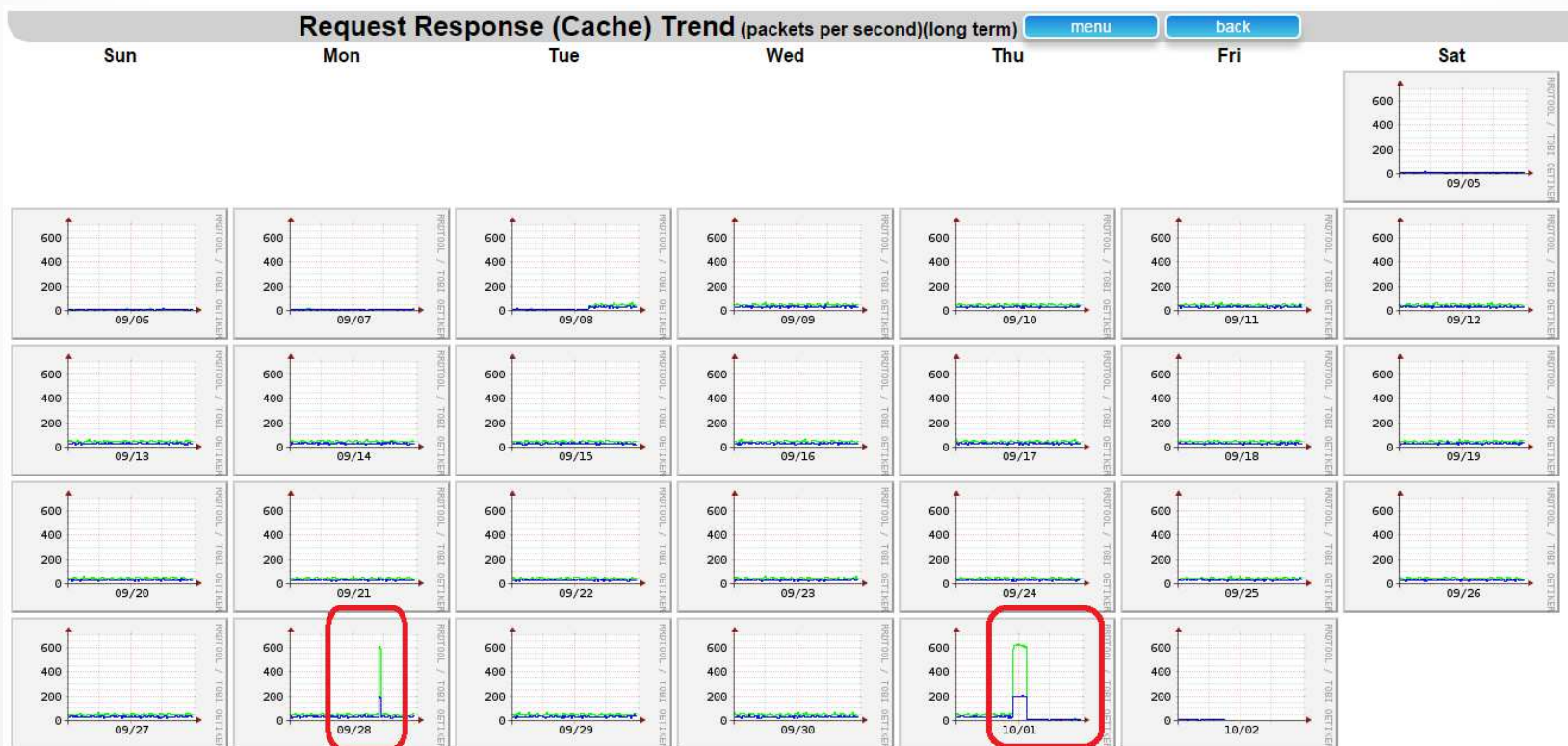


●特徴1

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

DNSの可視化と対策

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

momentum
DNS viewer

1Uprobe

172.16.183.74

Interface Traffic

Response Time

Request / Response

Response(Recursion)

Response(Cache)

RR TYPE

Response - RCODE

Response - ServFail

Response - NXDomain

Element

Logout

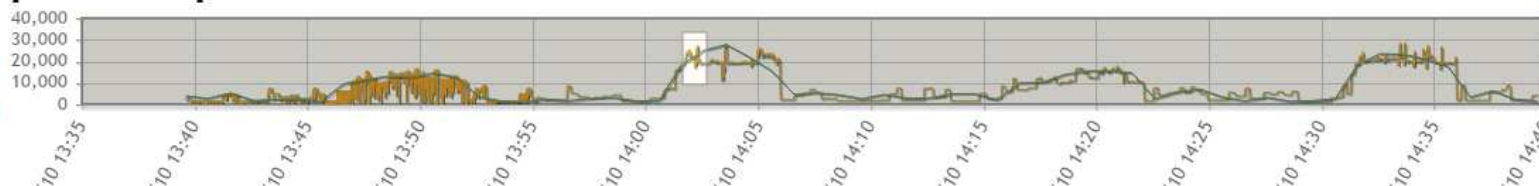
Request Response (Recursion) Trend (packets per second, non-stack, last

Req/Res(Recursion)(pps,non-sta Req/Res(Recursion)(bps,non-sta Req/Res(Recursion)(pps,stack Req/Res(Recursion)(bps,stack
[Detail View] (past : 7 day before)



Y axis(max): set Y reset

[Controller View]



●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

DNSの可視化と対策

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 : [1
 : [8 (NXRRSet)
 : [12

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

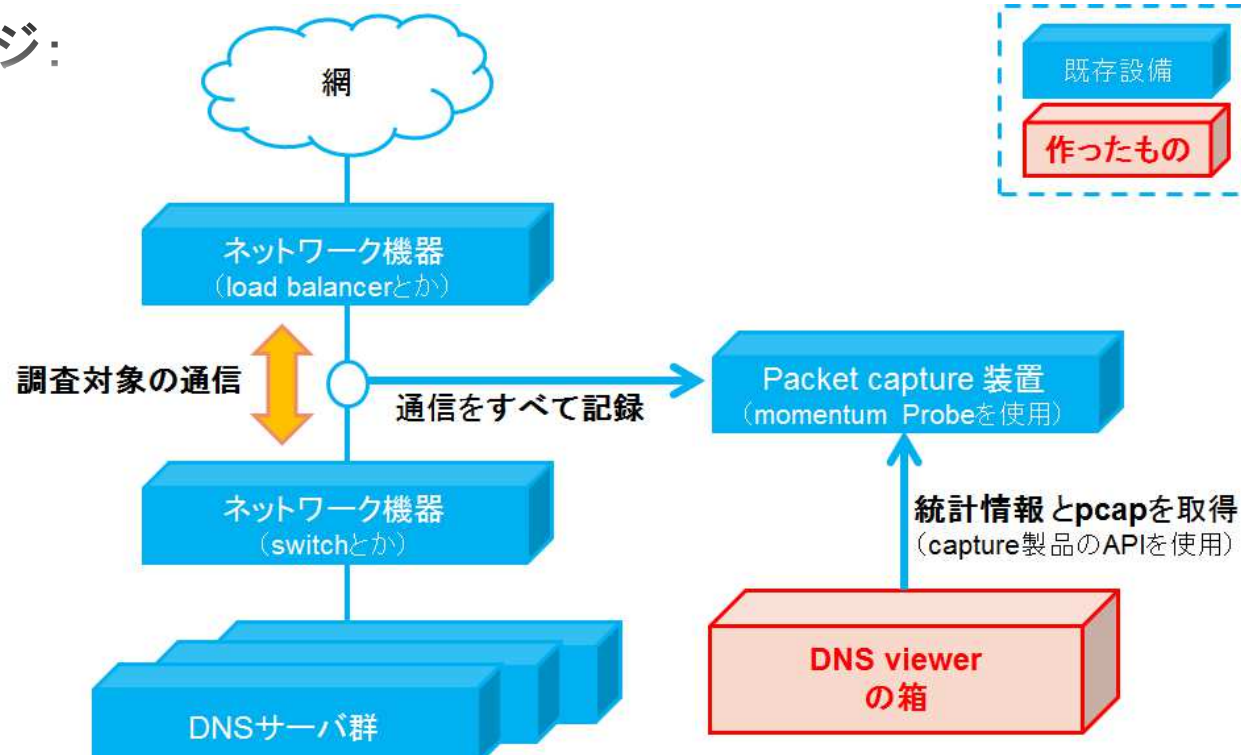
DNSの可視化と対策

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

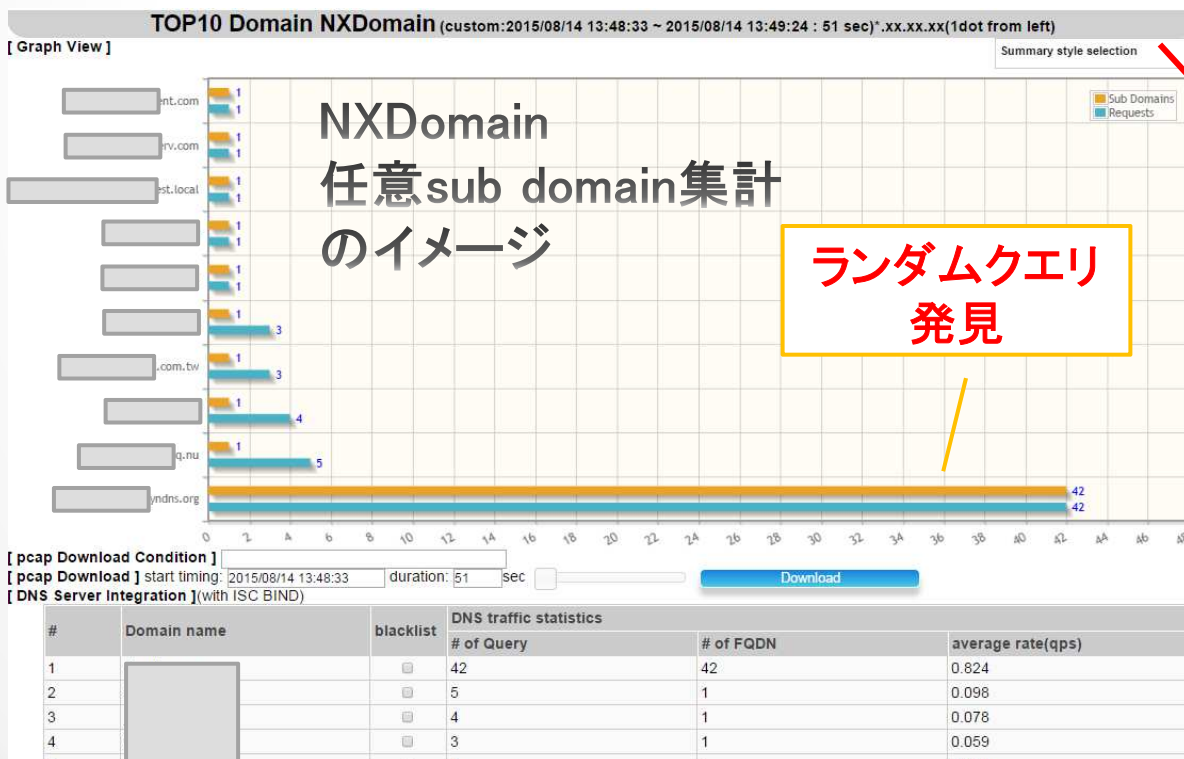
DNSの可視化と対策

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



Summary style selection

- [*.xx.xx.xx\(1dot from left\)](#)
- [*.*.xx.xx.xx\(2dot from left\)](#)
- [*.xx.xx.xx\(2dot from right\)](#)
- [*.xx.xx.xx\(3dot from right\)](#)
- [*.xx.xx.xx.xx\(4dot from right\)](#)
- [*.xx.xx.xx.xx.xx\(5dot from right\)](#)

画面例において、
一部、伏字

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

- ・ 長期傾向から特異点を把握できる

特徴2

- ・ 任意の時間帯に関して、状況を把握できる

特徴3

- ・ いろいろな切り口で、状況を把握できる

特徴4

- ・ 特定の時間帯を、じっくり解析できる

おしまい

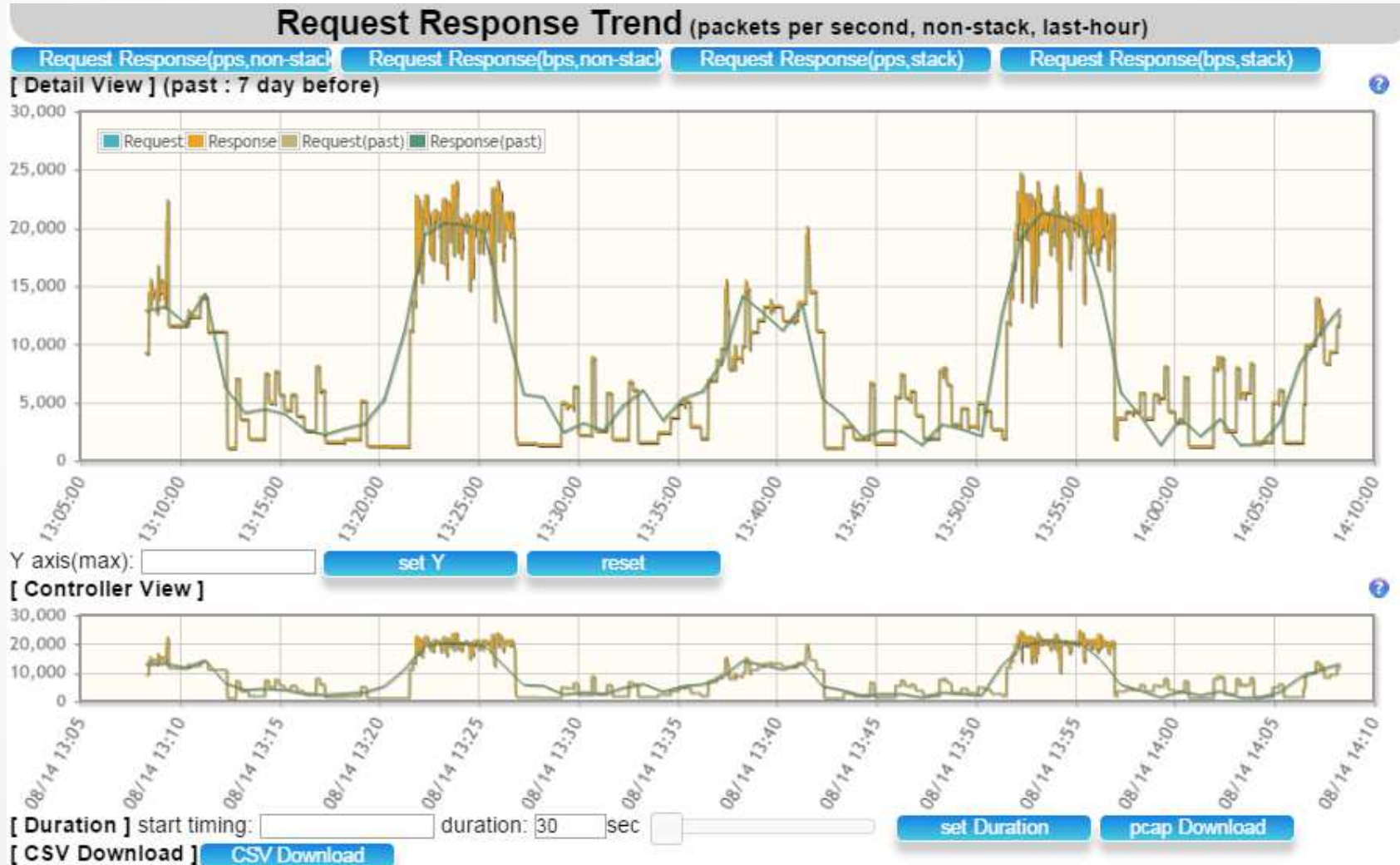
付録

先週より多い、とか確認

●付録：Trend画面例

DNSの可視化と対策

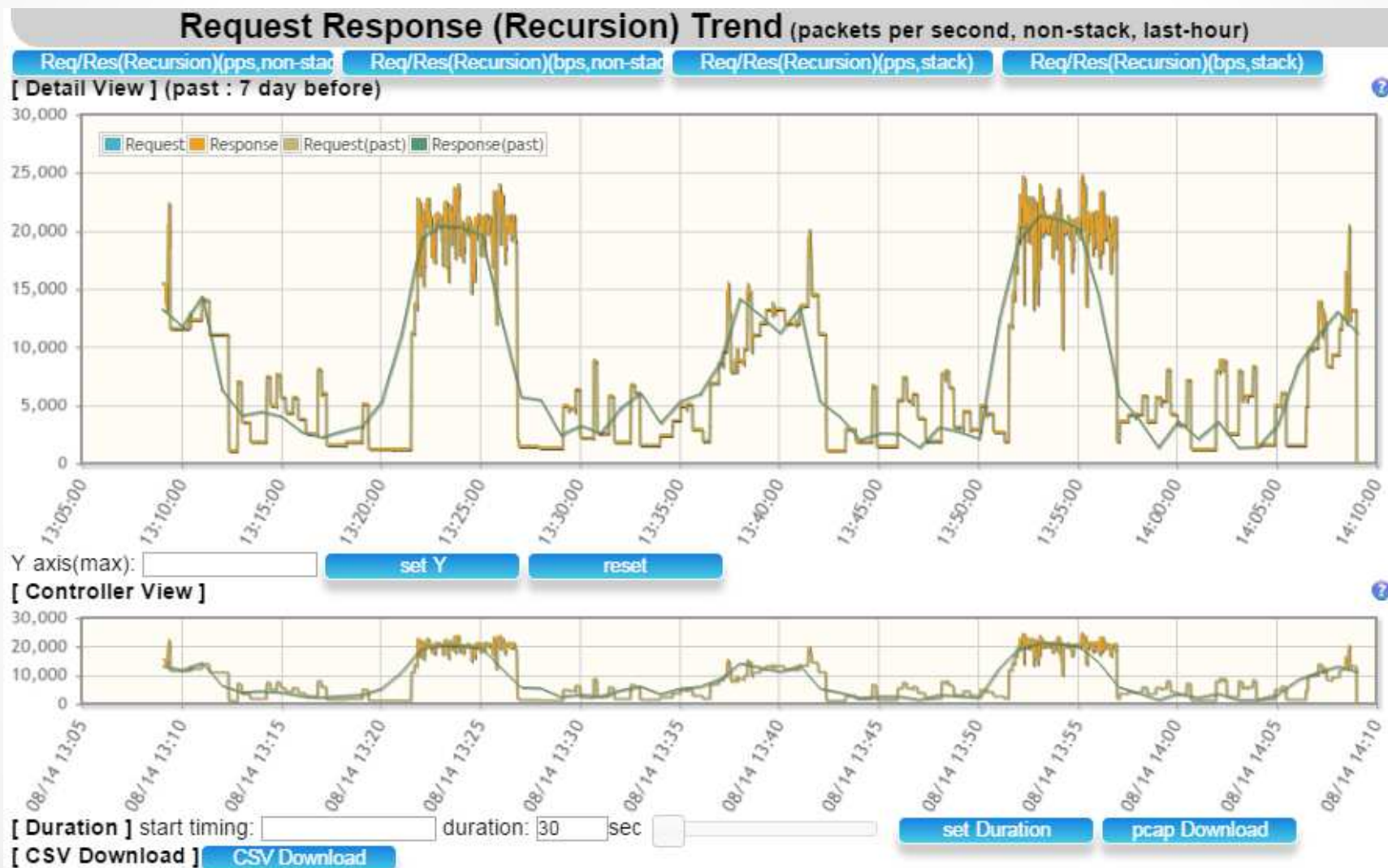
DNSのRequestとResponseが見えました(過去情報付)(1秒粒度)



●付録: Trend画面例

DNSの可視化と対策

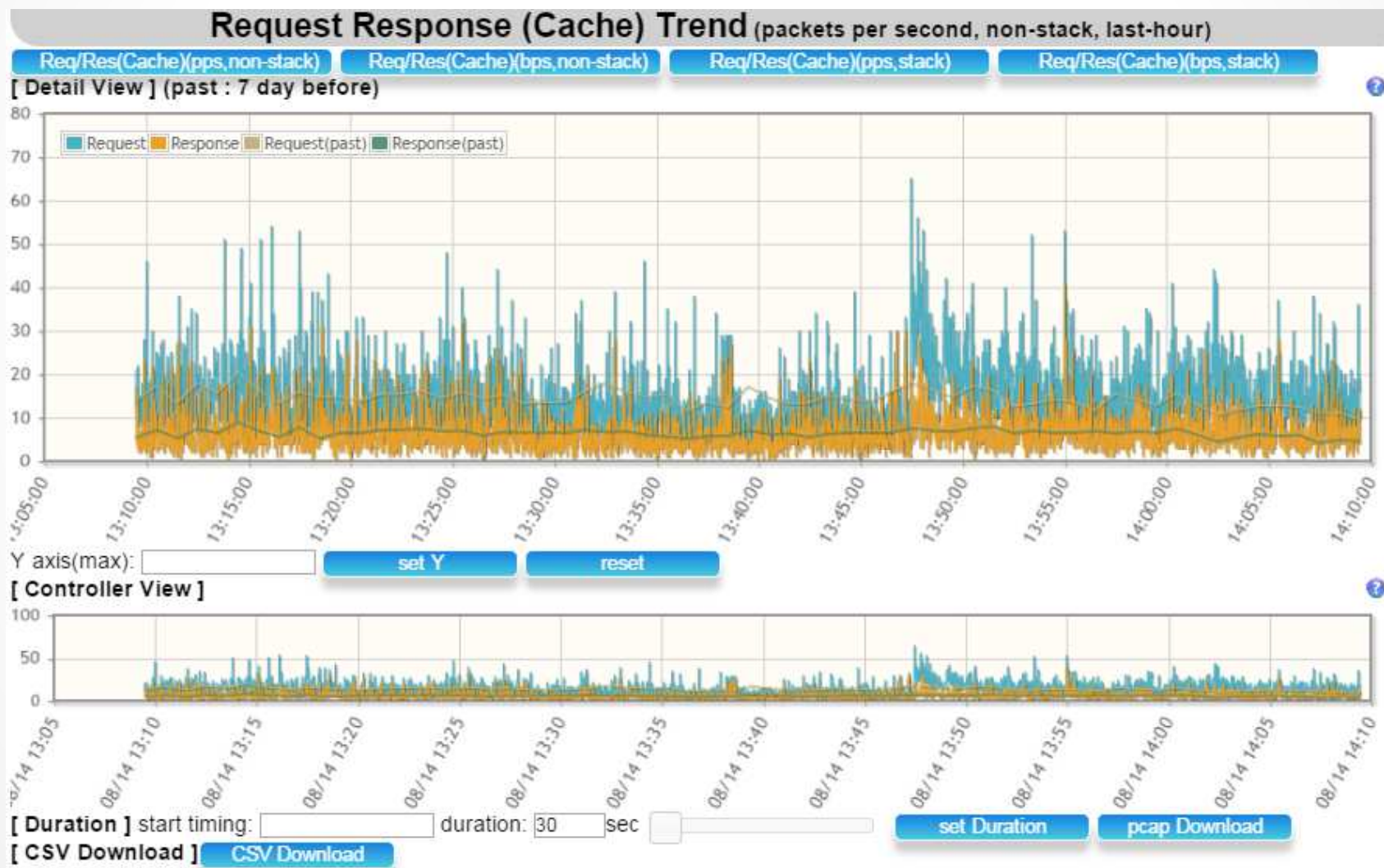
DNSのRequestとResponseが見えました(Recursion Desiredのみ)



●付録: Trend画面例

DNSの可視化と対策

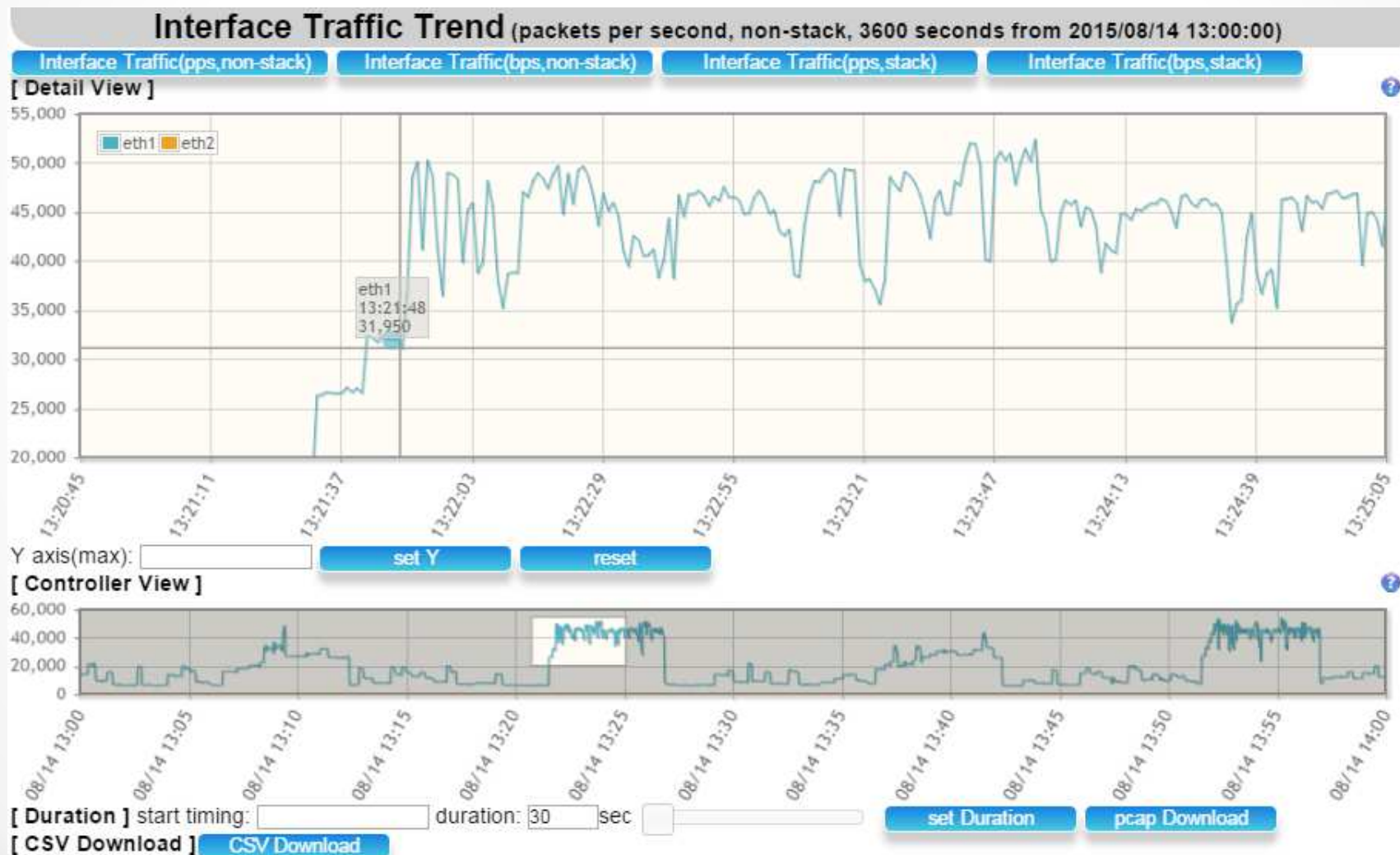
DNSのRequestとResponseが見えました(Cache Serverの通信のみ)



●付録: Trend画面例

DNSの可視化と対策

拡大できます

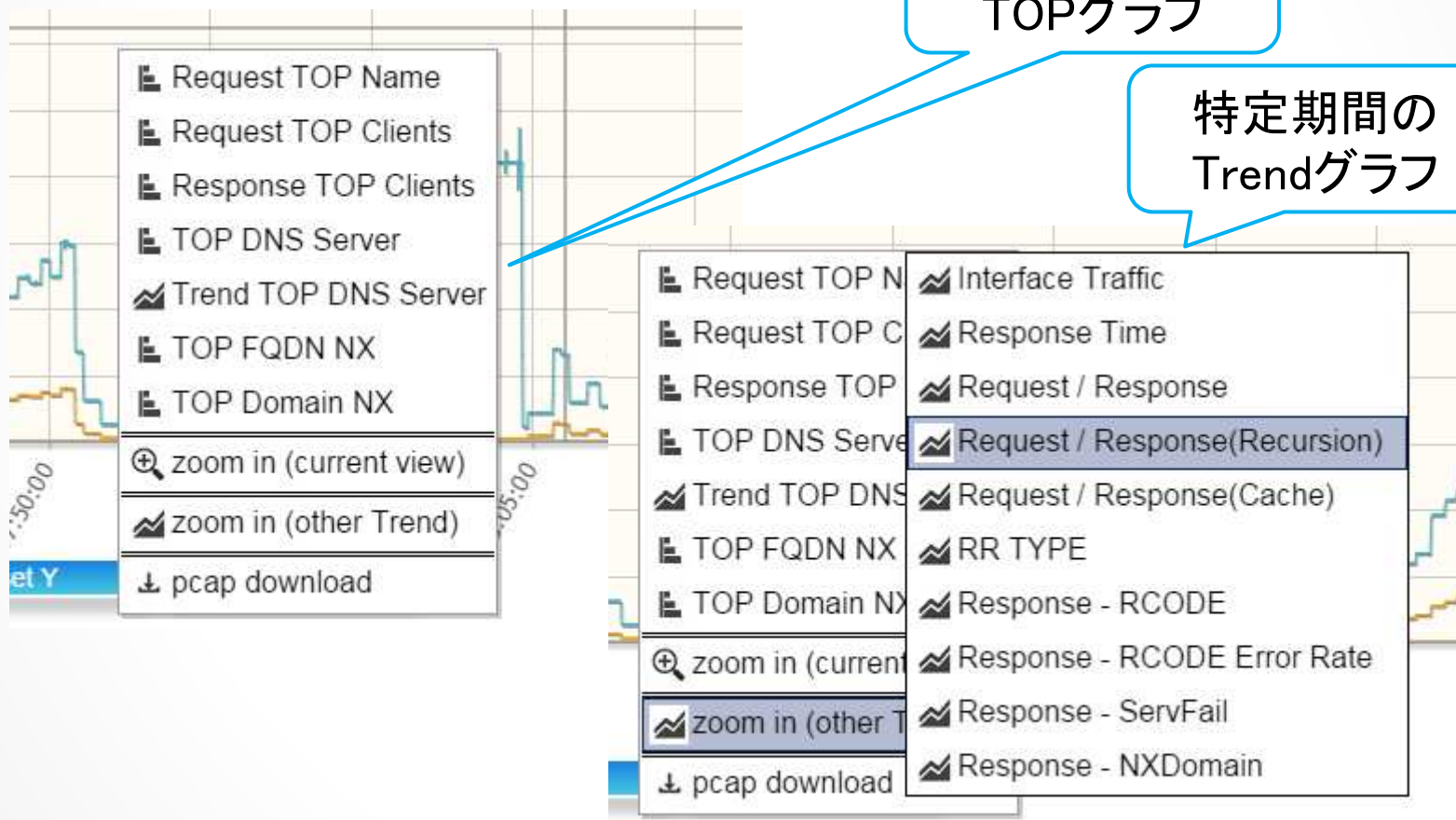


●付録: Trend画面例

各種グラフを確認できます

特定期間のTOPグラフ

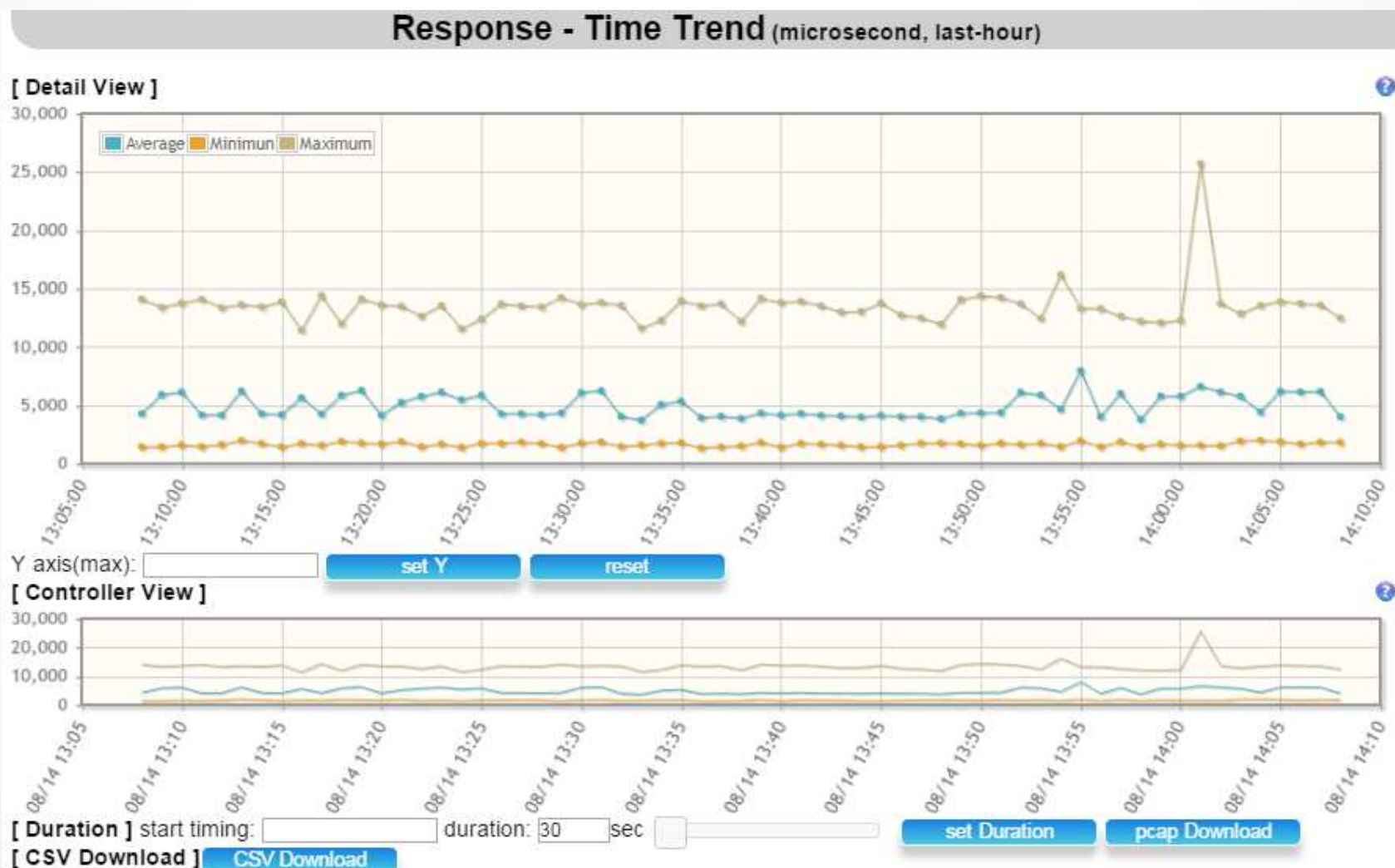
特定期間のTrendグラフ



●付録: Trend画面例

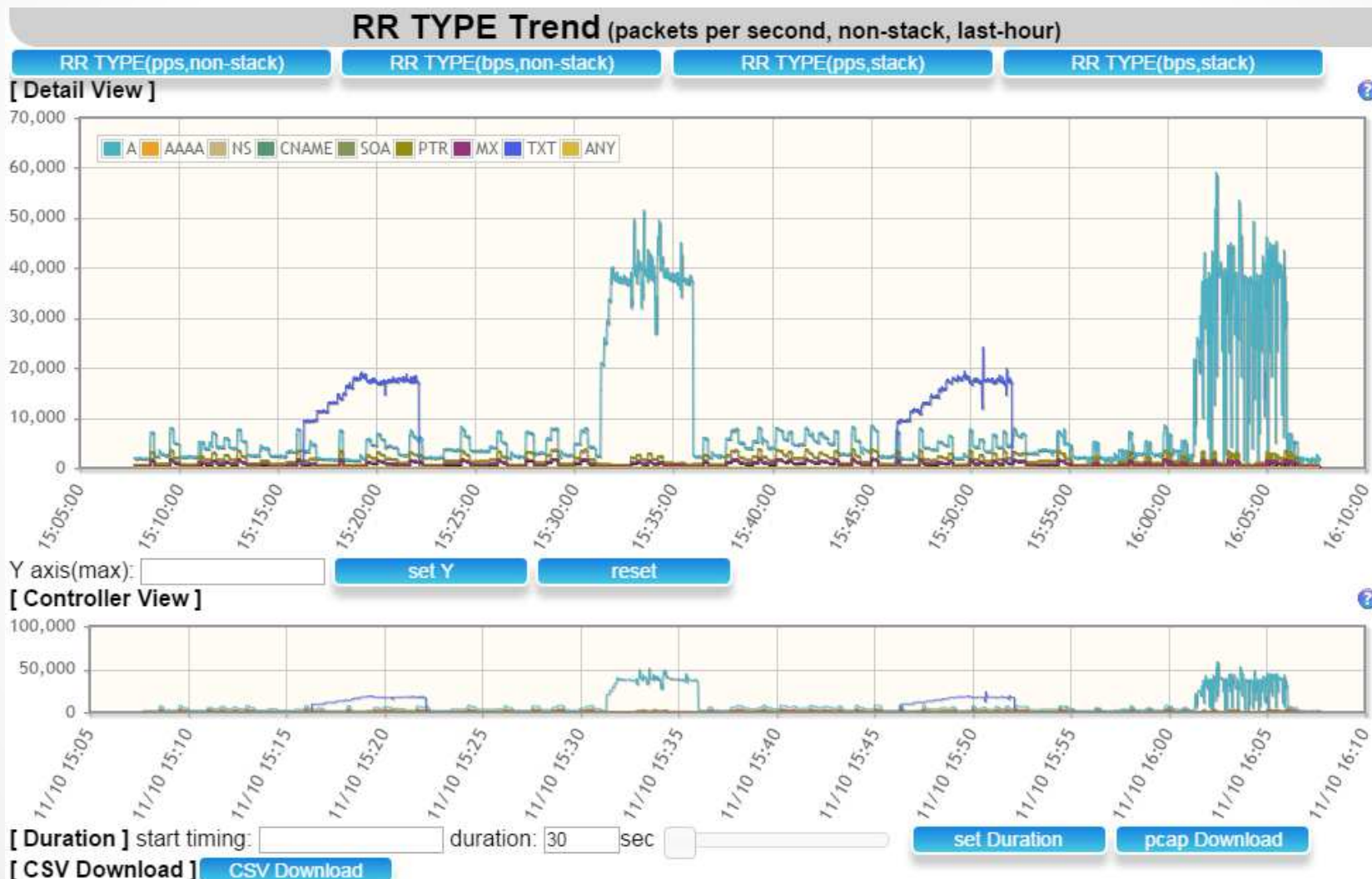
DNSの可視化と対策

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

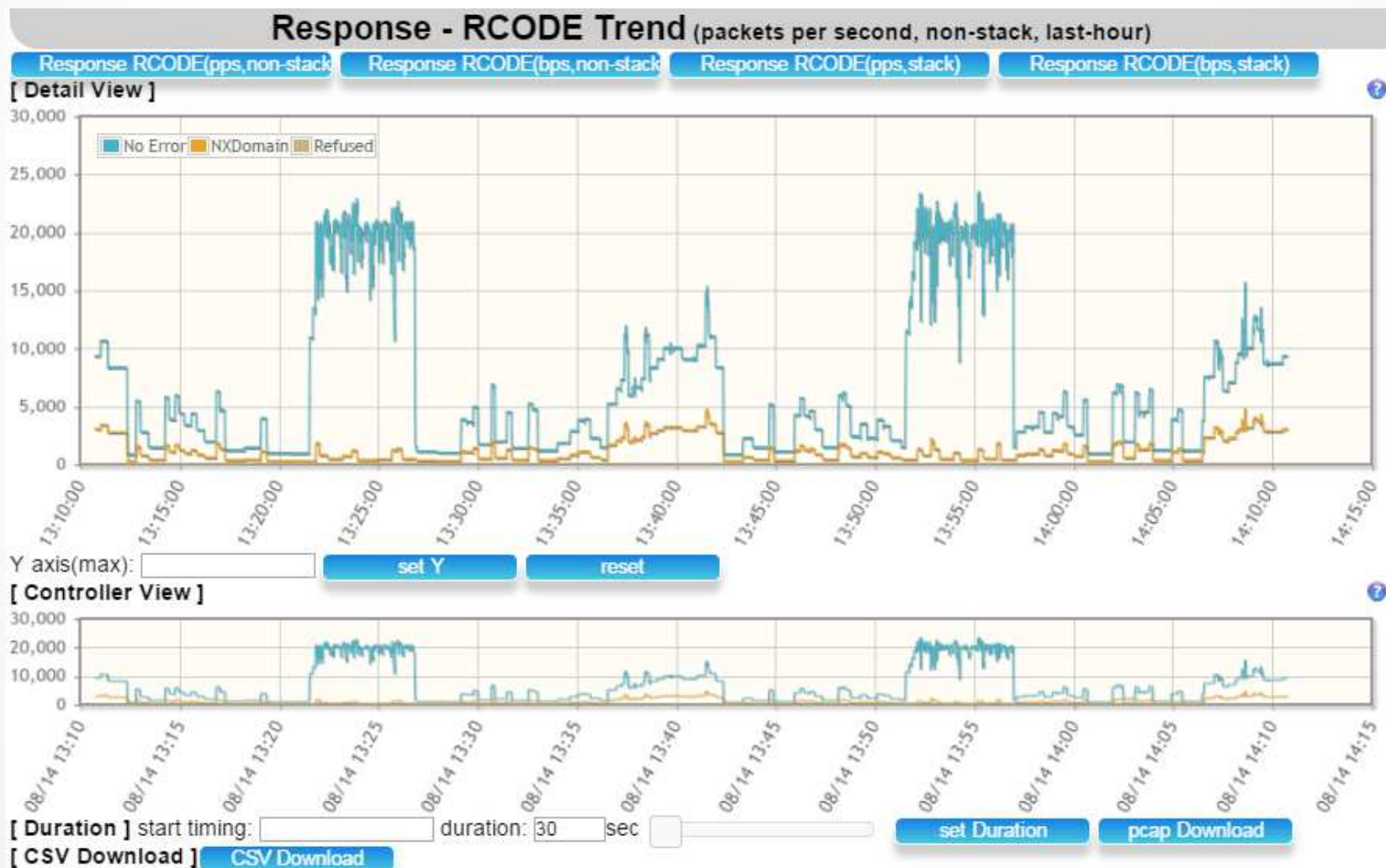
DNSのRRの配合見えます



●付録: Trend画面例

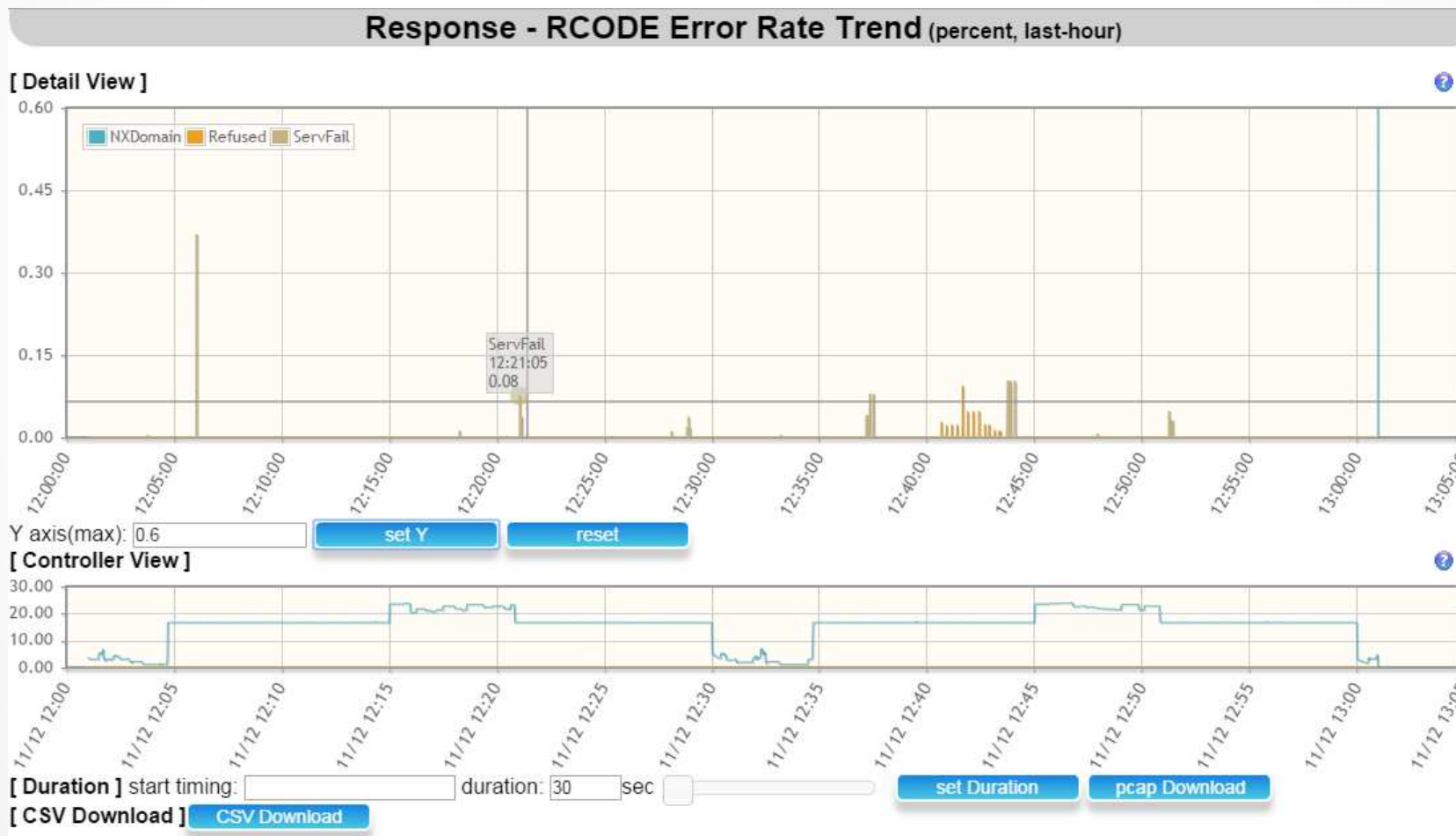
DNSの可視化と対策

DNSのRCODEの配合見えます



●付録: Trend画面例

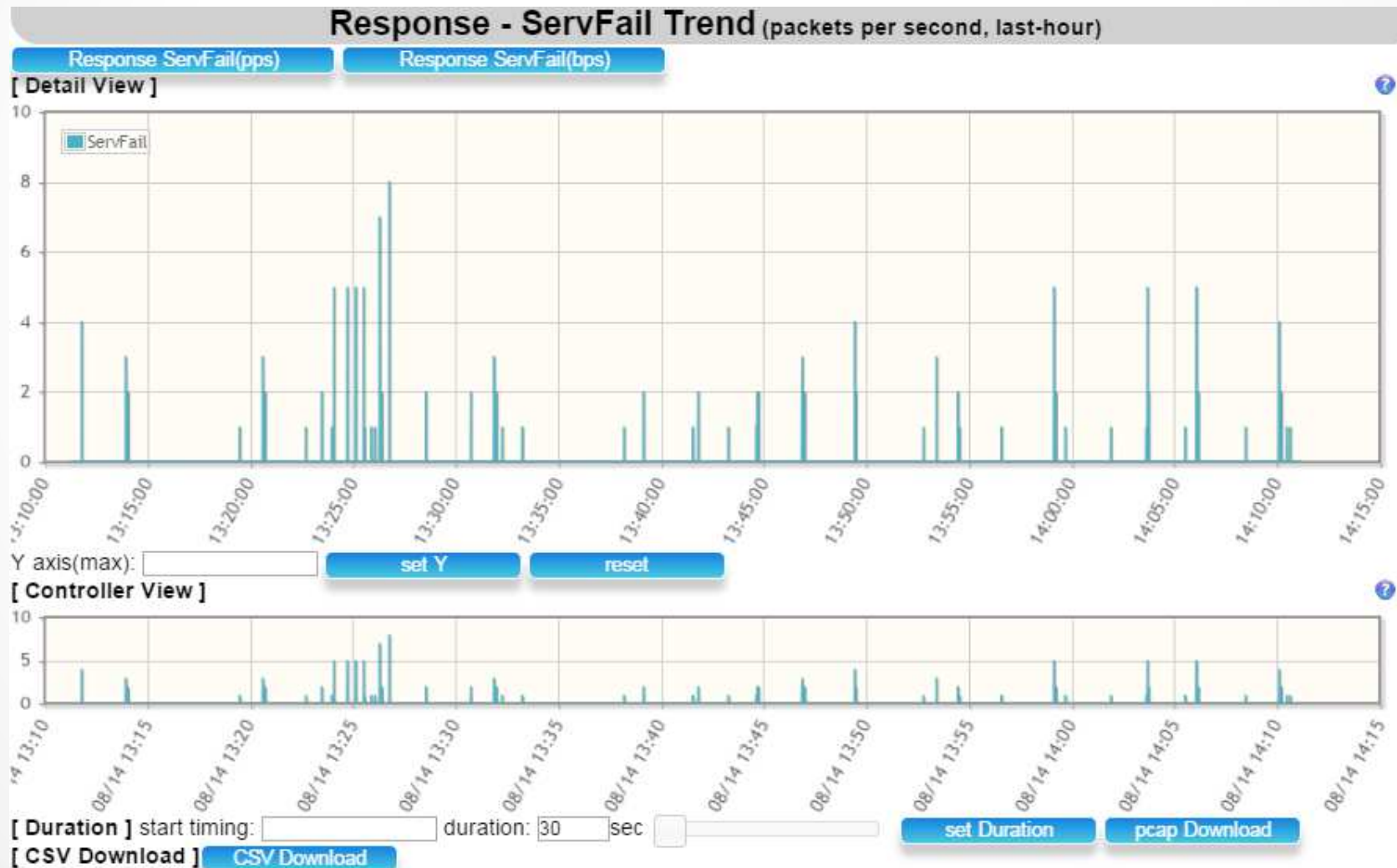
DNSのRCODEの比率見えます



●付録: Trend画面例

DNSの可視化と対策

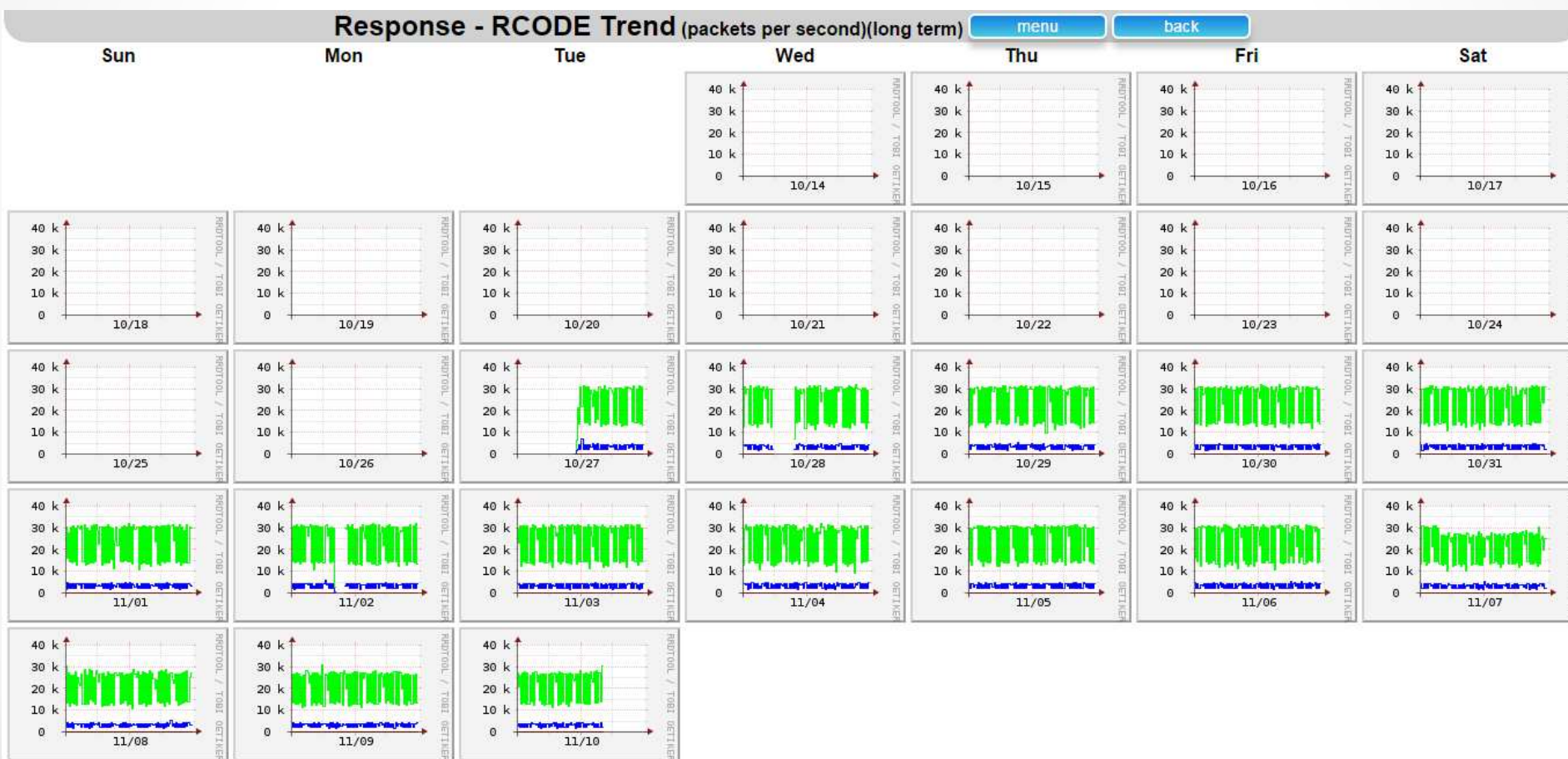
ServFail見えます



●付録: Trend画面例

DNSの可視化と対策

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

DNSの可視化と対策

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:

The image displays two screenshots of the PSGUI-Win application interface. The left screenshot shows the configuration screen with the following fields:

- probe IP: 172.16.183.165
- command: stat
- interface: (eth1_0)
- start time: 20151119075609 (YYYYmddHHMMSS)
- duration: 60 (seconds)
- step: 10 (seconds)
- field id: 27
- narrowing: 7=*terilogy*
- pcap file: C:/Users/komoriya/Desktop/output.pcap

The right screenshot shows the search results for the same configuration, displaying a list of DNS records with IP addresses and domain names like mail.terilogy.com, smtp.terilogy.com, etc.