DNS Summer Day 2017(発表用)

TTLの現状について，分析結果のご紹介

2017年6月28日

NTTコムエンジニアリング株式会社　　佐藤　正春
NTTネットワーク基盤技術研究所　　原田　薫明

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

この発表について

発表者

- 佐藤　正春（NTTコムエンジ）
  - OCN DNS の運用
- 原田　薫明（NTT研究所）
  - 通信トラヒック品質プロジェクトに所属
  - トラヒック測定分析，仮想ネットワーク制御に関わる研究開発に従事

発表の目的

- 下記について情報共有します
  - DNSのTTLの現状について
  - DNSキャッシュサーバの負荷について

資料の構成

- DNSのTTL分析
  - DNSレスポンスから見るTTLの経年変化①：キャッシュサーバ⇒ユーザへのレスポンス分析
  - DNSレスポンスから見るTTLの経年変化②：権威サーバ⇒キャッシュサーバへのレスポンス分析
- DNSキャッシュサーバの負荷
  - CPUを引き上げる要因をグラフから探ってみた

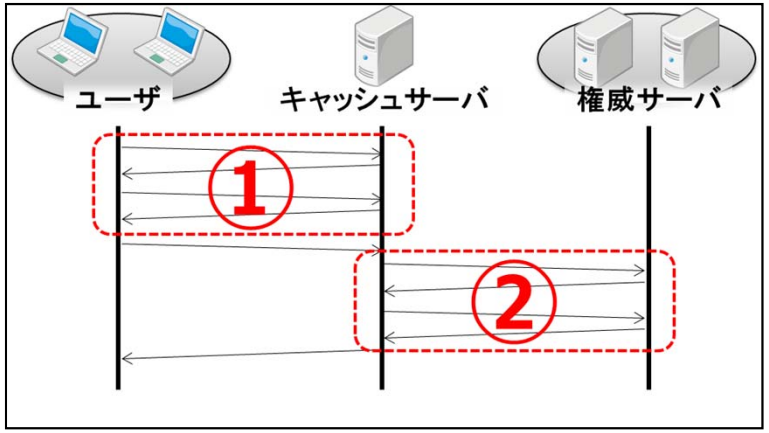
NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

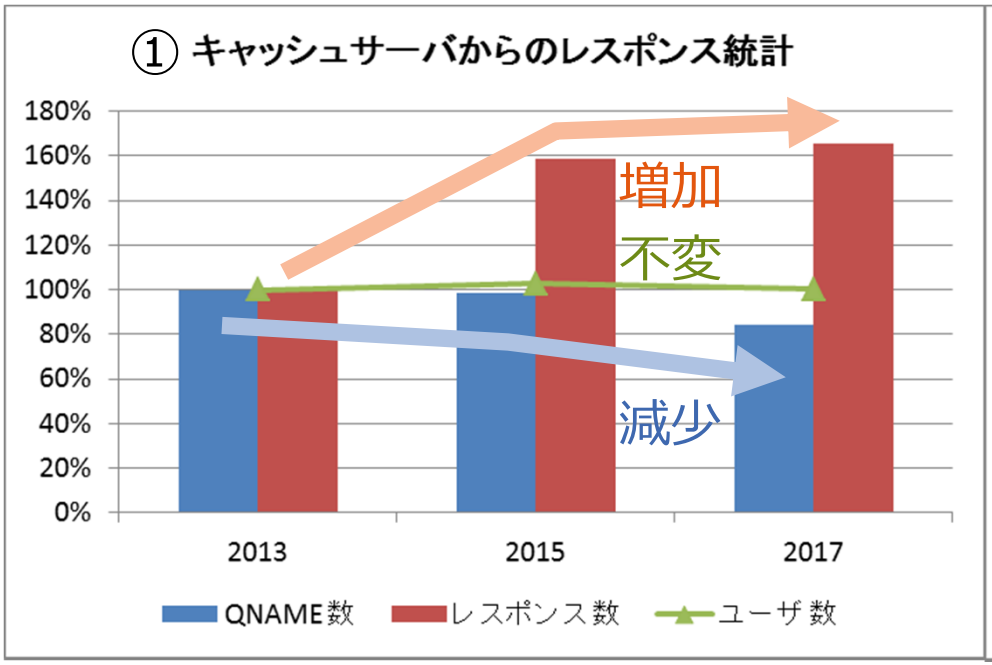
DNSのTTL分析

DNSレスポンスから見るTTLの経年変化

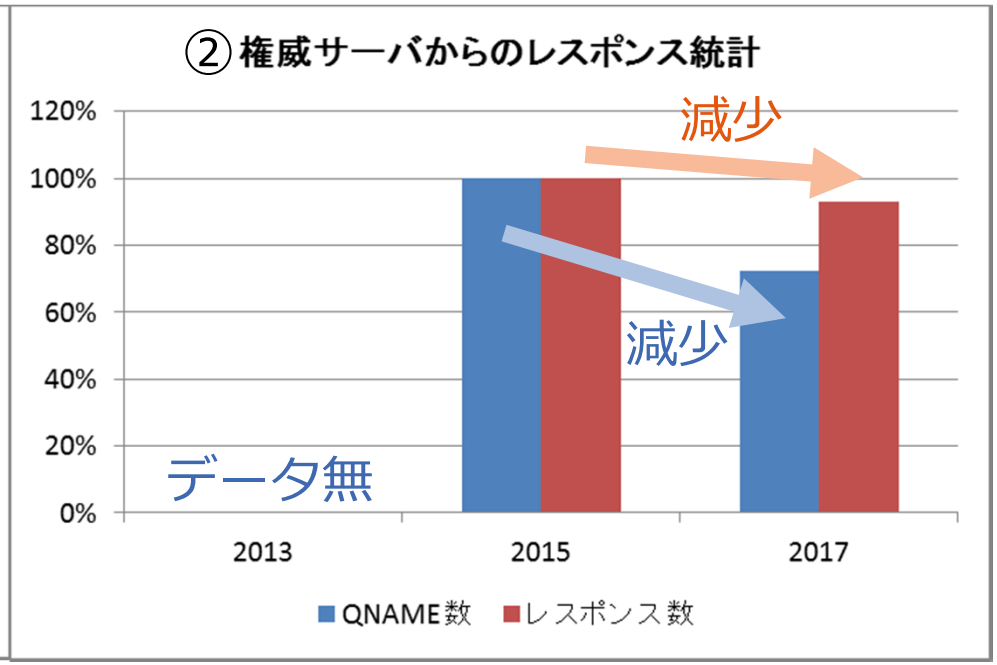
DNS応答の傾向

- 2013年，2015年，2017年のとある日における ピーク時間帯（１時間）のレスポンスを分析.
- ユーザ数（ユーザ側IPアドレス数）はほぼ同一.
  - 2013年から2015年にかけてキャッシュサーバ応答の レスポンス数が増加しているが，スマートフォン等の 普及に伴い宅内端末が増えた影響と推測.
- キャッシュサーバ，権威サーバ共にQNAME数は減少傾向.
- キャッシュサーバのレスポンス数は増加傾向であるのに 対して，権威サーバでは微減.





2013年を100%とした時の相対量

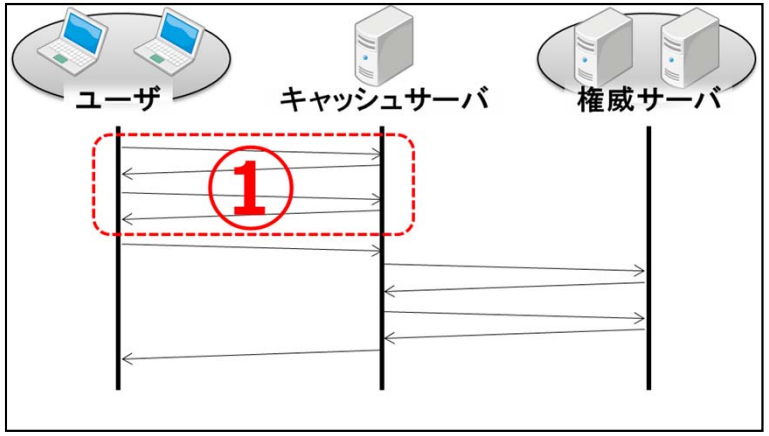


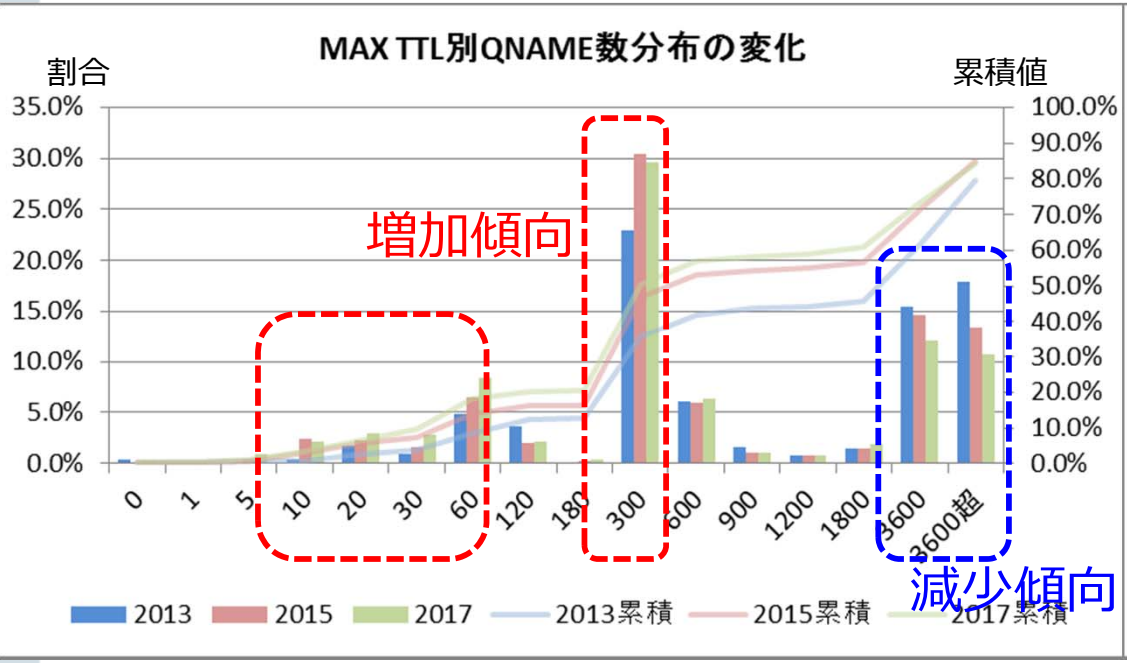
2015年を100%とした時の相対量

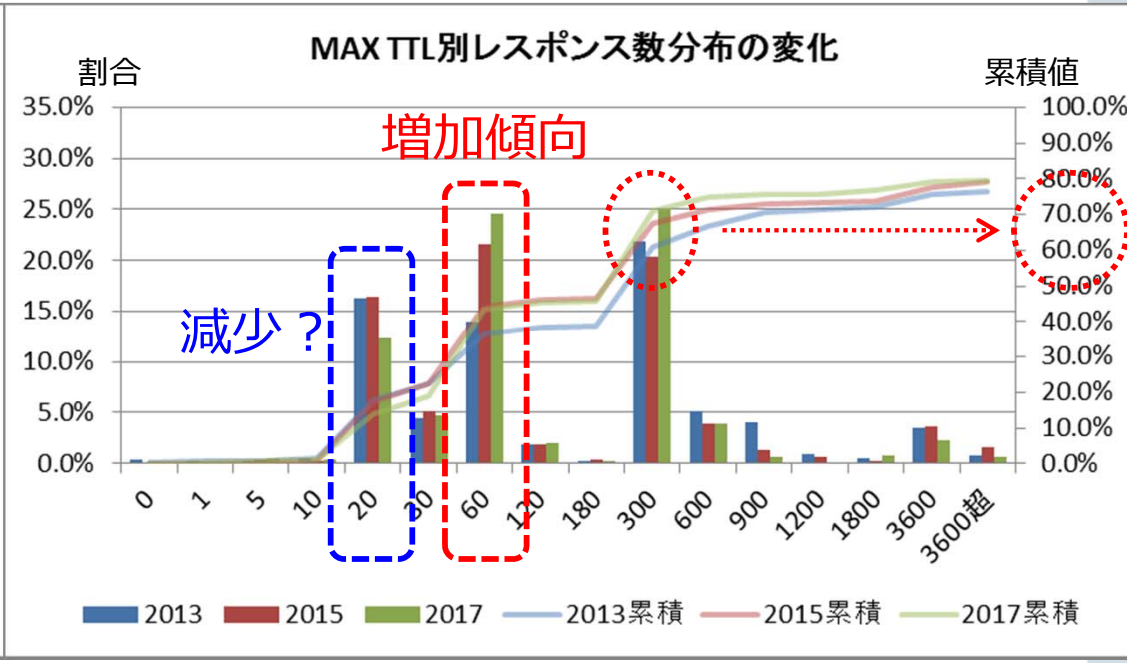
NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

【DNSレスポンスから見るTTLの経年変化①】
キャッシュサーバ⇒ユーザへのレスポンス分析

- MAX TTLが300秒以下のQNAME数，レスポンス数ともに増加傾向.
  - MAX TTL別のQNAME数分布は，300秒よりも短いQNAME数が増加傾向で，3600秒を超えるQNAME数が減少しつつある.
  - MAX TTL=20秒のレスポンス数の割合は減少した一方，MAX TTL=60秒の割合は増加傾向.
  - レスポンスの大部分がMAX TTL=300秒以下であり，その割合も増加傾向にある.



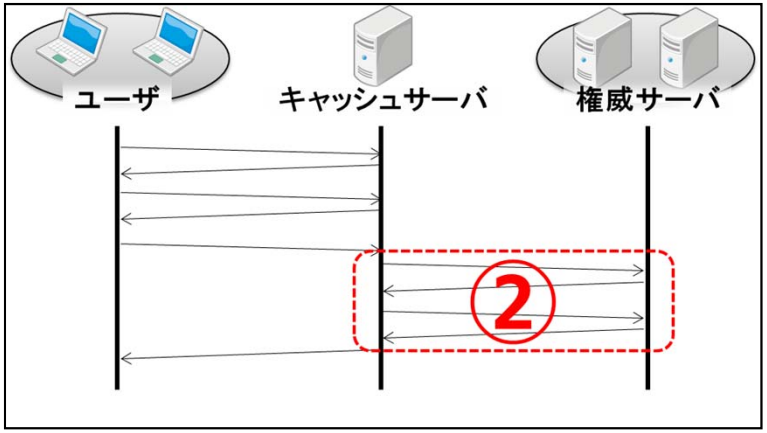


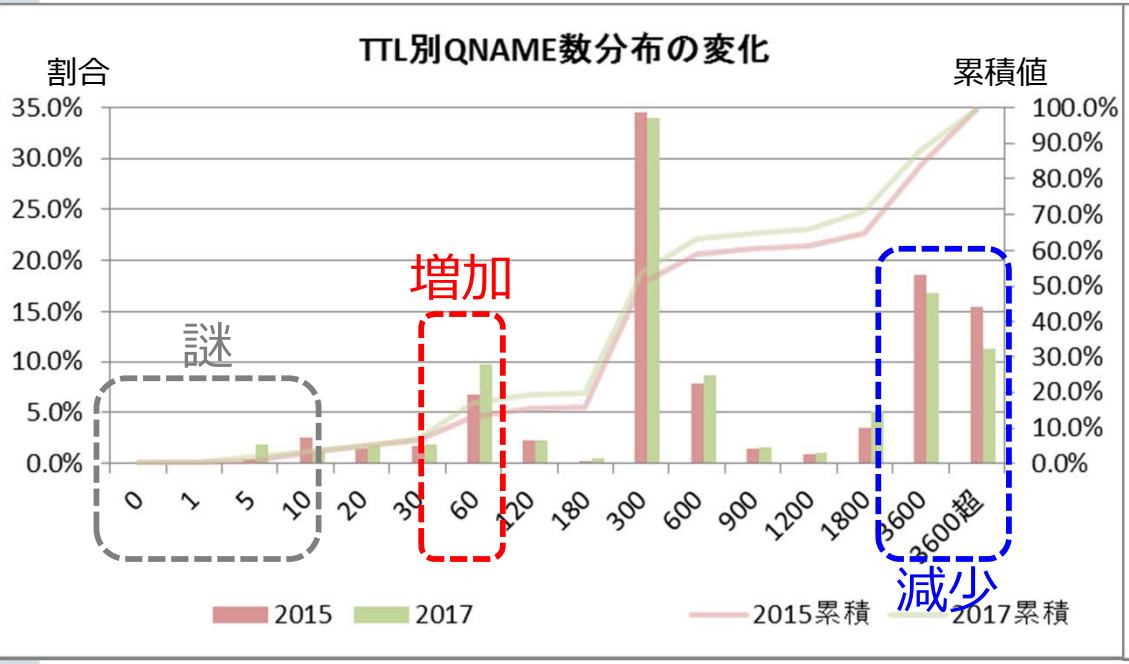


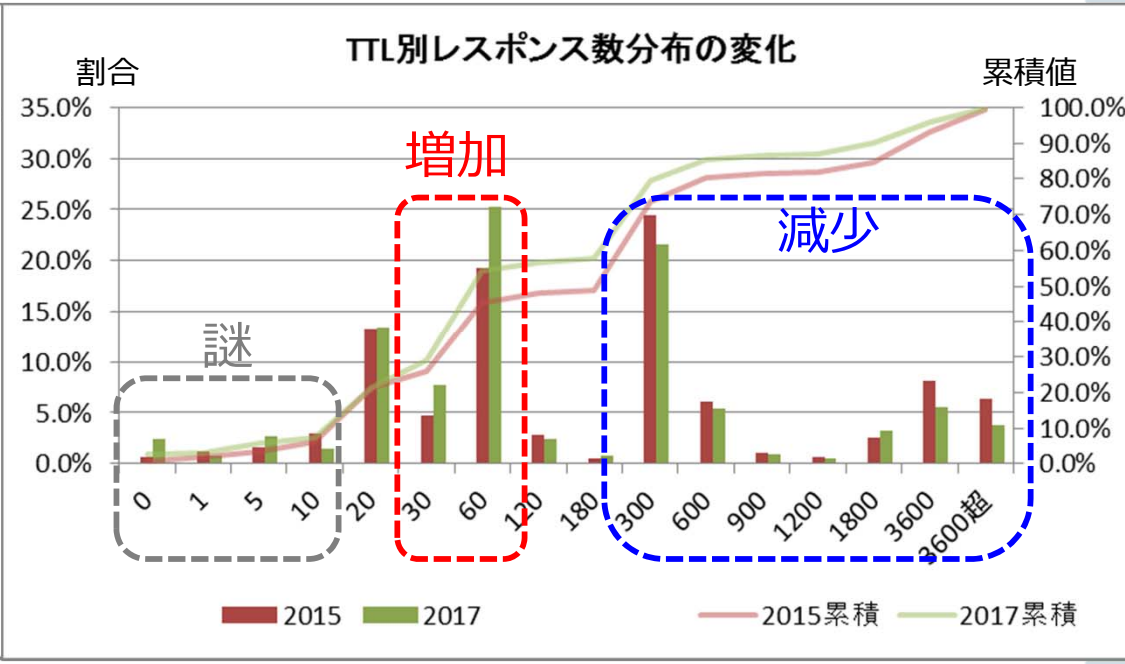
MAX TTLが推定できなかった（半端な数値となった）ものを除外して表示
※全体的な傾向は変わらないことを確認済

【DNSレスポンスから見るTTLの経年変化②】
権威サーバ⇒キャッシュサーバへのレスポンス分析

- キャッシュサーバ⇒ユーザのレスポンスと同様に，TTLが300秒以下のQNAME数，レスポンス数ともに増加傾向.
  - TTL=60秒のQNAME数，レスポンス数の割合が増加.
  - TTL=10秒以下のQNAME，レスポンスも数%存在.







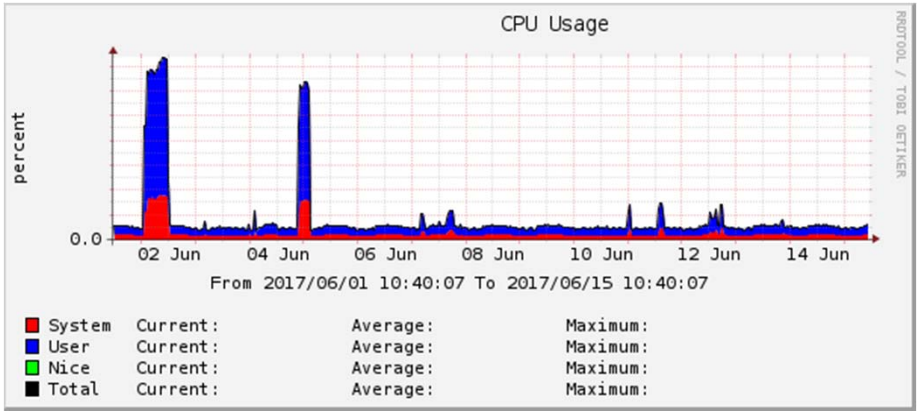
MAX TTLが推定できなかった（半端な数値となった）ものを除外して表示
※全体的な傾向は変わらないことを確認済

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

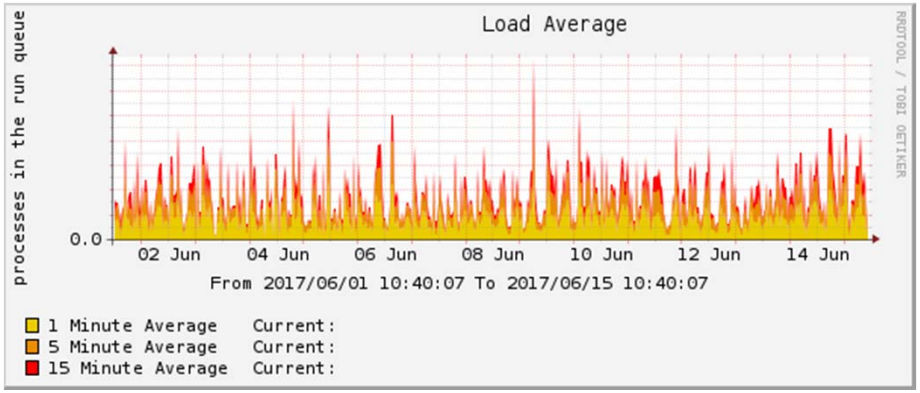
DNSキャッシュサーバの負荷

CPU Usageを引き上げる要因をグラフから探ってみた。

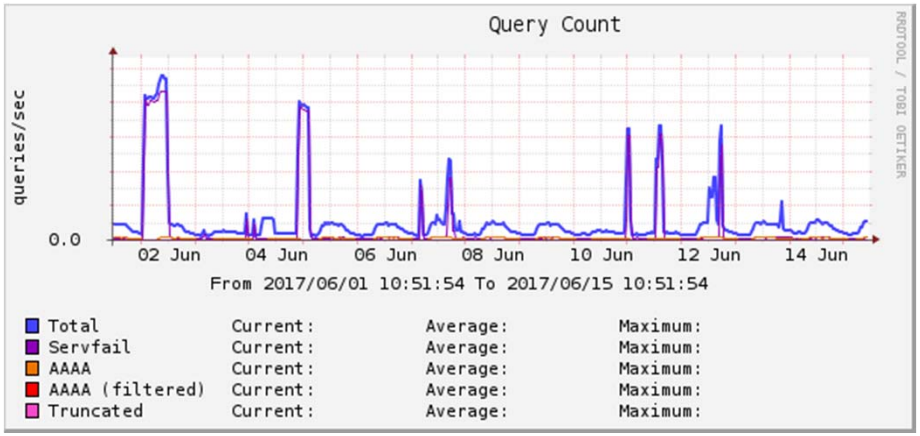
CPUを引き上げる要因をグラフから探ってみた。



6/2,4にCPU Usageがスパイクする状況が発生。
何が原因だったのかな？

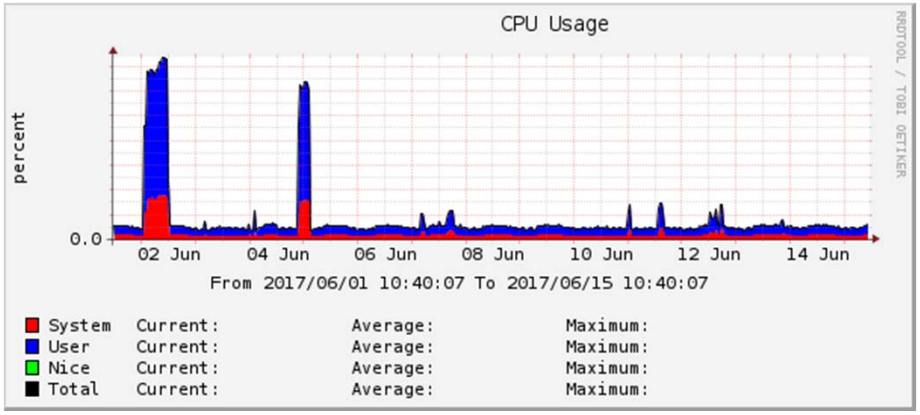


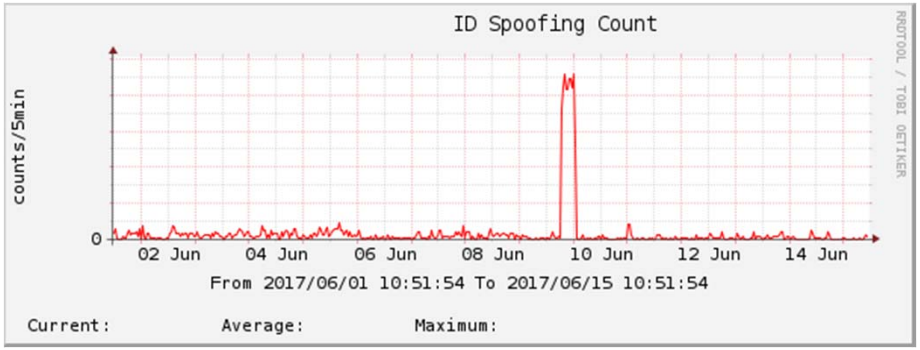
Load Averageは問題なさそう



Query Countが連動しているように見える。
ただ、よく見ると、10-12日にQC的にはスパイクが発生しているが、CU的にはスパイクが発生していない。

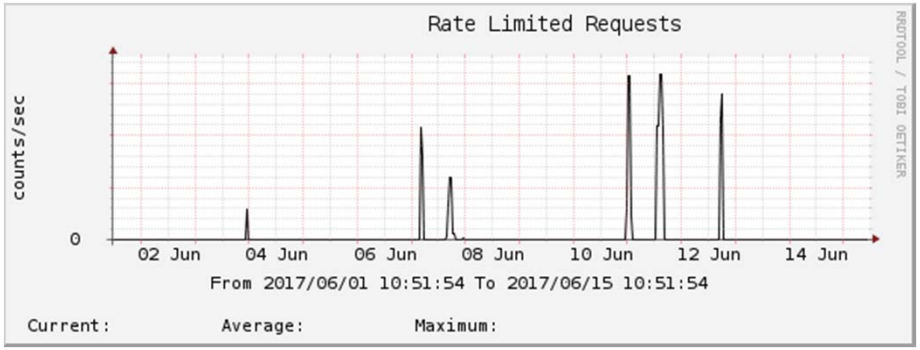
CPUを引き上げる要因をグラフから探ってみた。





ID Spoofing Countも相関はなさそう。

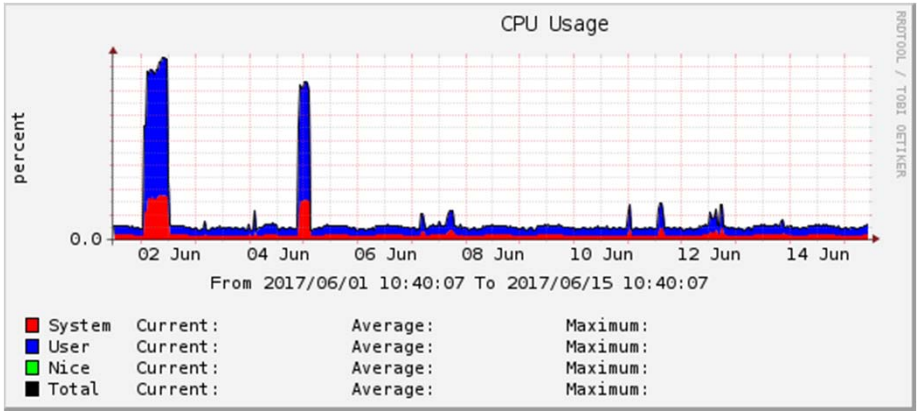
*Defending against ID spoofing attacks
When Server is waiting for a legitimate response from an authoritative server, and
instead gets a response with an incorrect ID value, it takes this as possible evidence that an ID spoofing attack is underway. To protect itself, Server repeats the query using TCP
instead of UDP, because TCP queries aren't vulnerable to the attack.

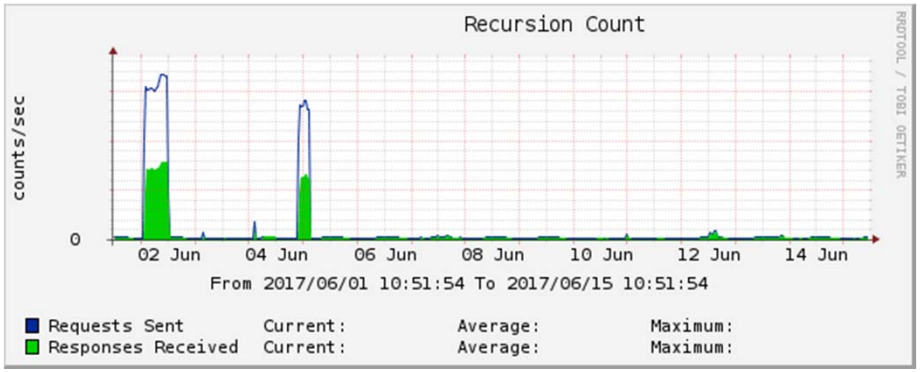


Rate-Limited-Requestsも相関はなさそう。

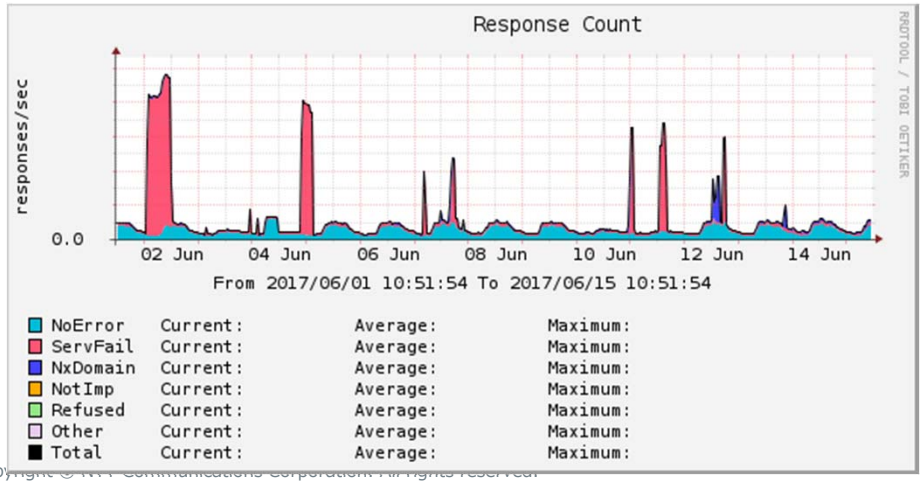
*rate-limited-requests
The number of DNS requests not sent by this resolver to other DNS servers as a result of server-based rate-limiting.

CPUを引き上げる要因をグラフから探ってみた。



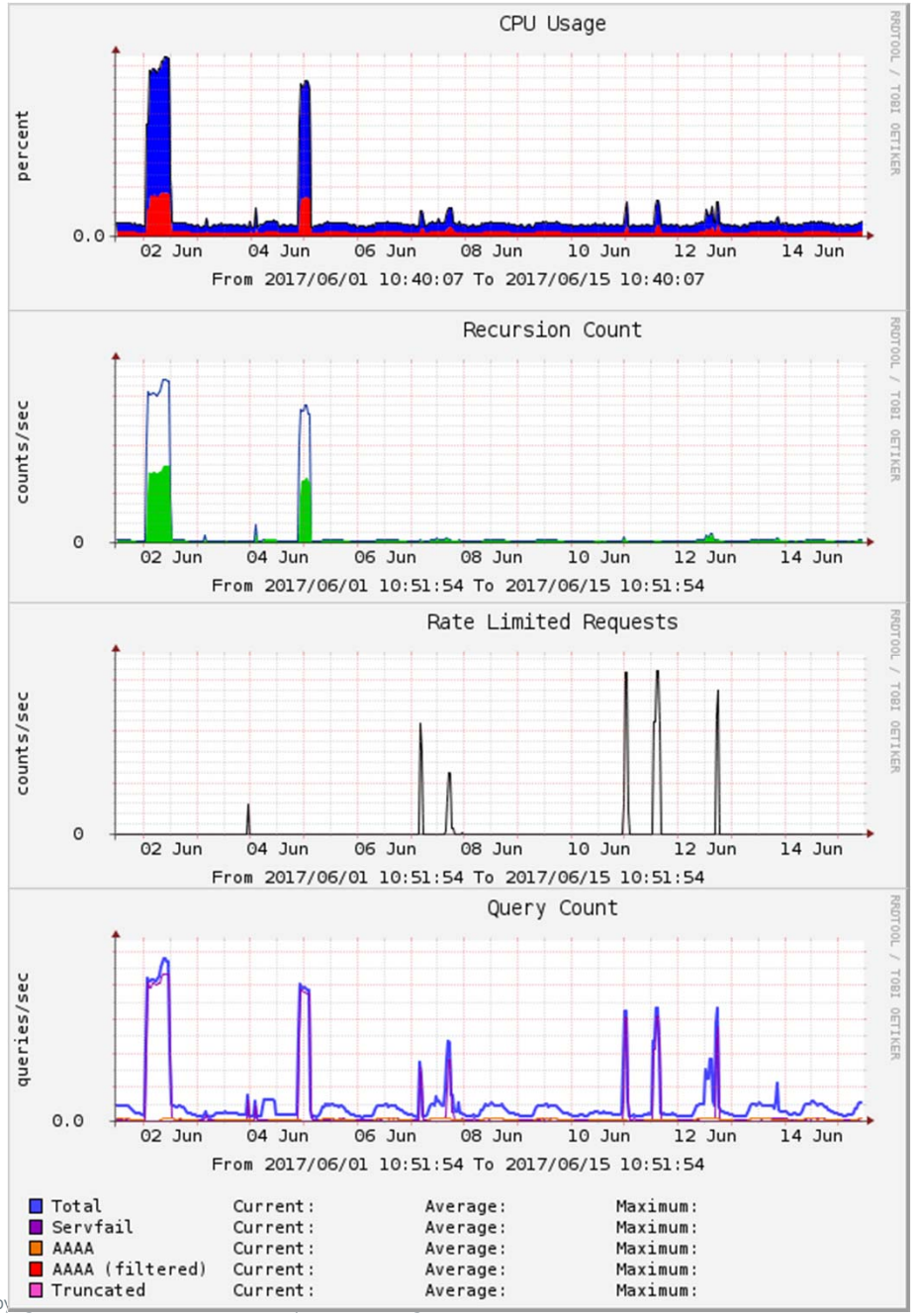


Recursion CountのRequests SentsとResponses Receivedの差分が大きい時により大きくCPU Usageが変化している。



ServFailであっても、権威サーバ側のレスポンスの違いによって、CPU Usageの挙動も異なる模様。

CPUを引き上げる要因をグラフから探ってみた。まとめ



・RRのTTLとサーバの負荷(CPU Usage,Load Average)との関連性については、見出すことは出来なかった。
(TTLを考慮した、運用とか設計も意識したことは……)

・権威サーバの挙動によって、キャッシュサーバでの状態が異なるもよう。
権威サーバが元気に返してくれれば、キャッシュサーバも安泰。

・キャッシュサーバ側でのRate Limitedも有効な感じ。たぶん、権威サーバに対してもやさしい。

・TTLが短いRRを運用している権威サーバのレスポンスが悪くなると、キャッシュサーバの負荷が高くなる可能性がありそうなので、権威サーバ側の運用をしっかりとしてほしい。WTとかの時にも。(キャッシュサーバの運用者側)

ご清聴ありがとうございました！