BIND9の機能によるDNS Water Torture (Slow Drip)攻撃対策について

(機能説明編)

2014年11月20日

DNSOPS.JP

九州通信ネットワーク株式会社 (QTNet)

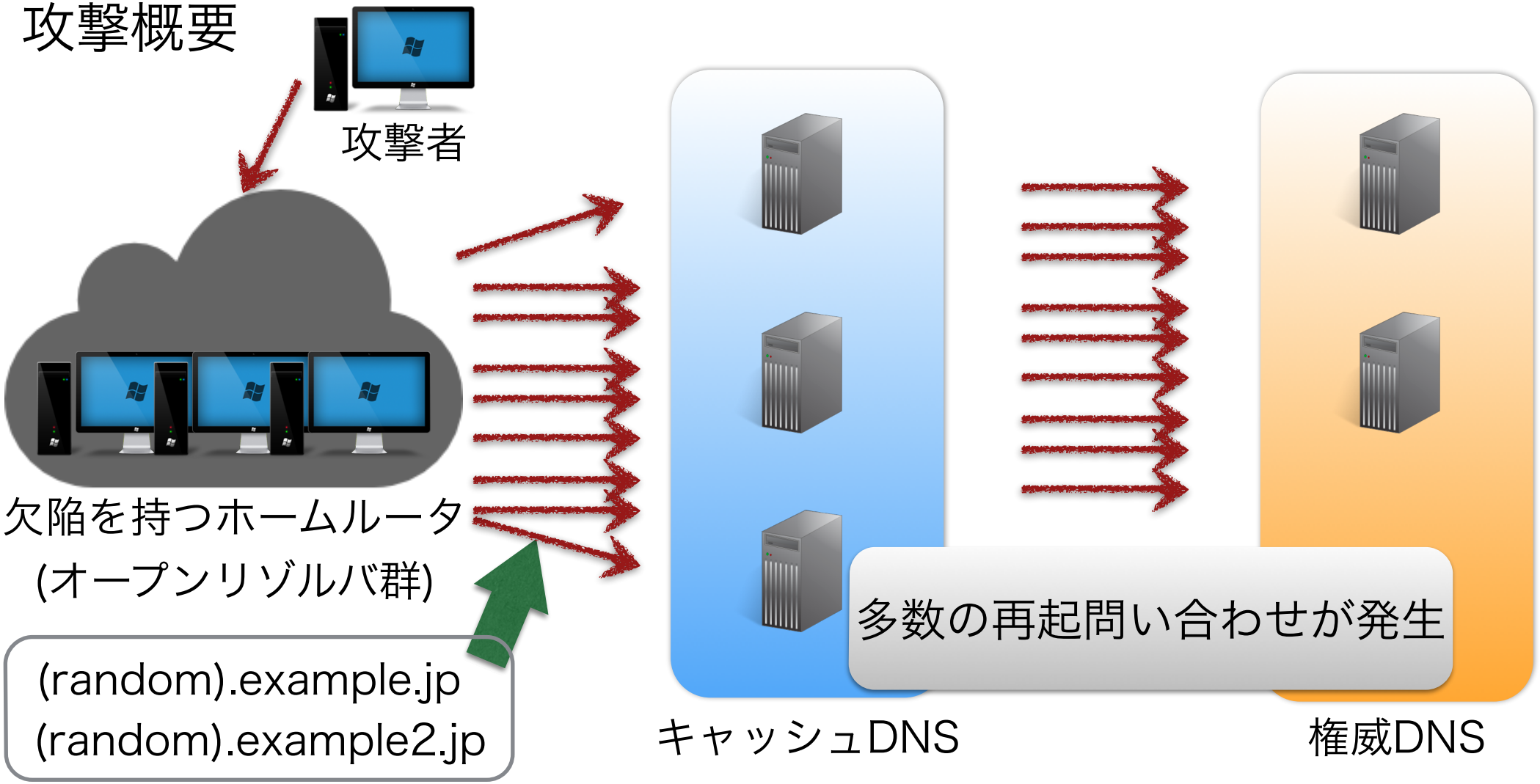
末松慶文 (yo_suematsu at qtnet.co.jp)

本発表の内容

- DNS Water Torture (Slow Drip)攻撃の概要
- BIND9を用いた攻撃対策の紹介

Water Torture (Slow Drip)攻撃とは？

攻撃概要



権威DNSやキャッシュDNSが高負荷に

キャッシュDNS側での攻撃対策例

・攻撃対象のzoneについて偽応答を返す(rpz,その他)
・iptabelsによる、権威DNSへのQuery制御
・IP53B
・エンドユーザのホームルータの改修？（ファームアップ）

対策による影響や通信の秘密に関して十分な考慮が必要

BIND9に対策機能は存在するの？

「BIND9に対策機能はあります。」

※ただし、サブスクリプション版のBIND9限定です..

Subscription branch software features
Subscribers have access to an unpublished branch of the BIND software with added-value features. The limited-access features will change over time, as we will periodically re-integrate with the main open source branch and start a new subscriber-only branch.
http://www.dns-co.com/solutions/bind-subscription/より引用

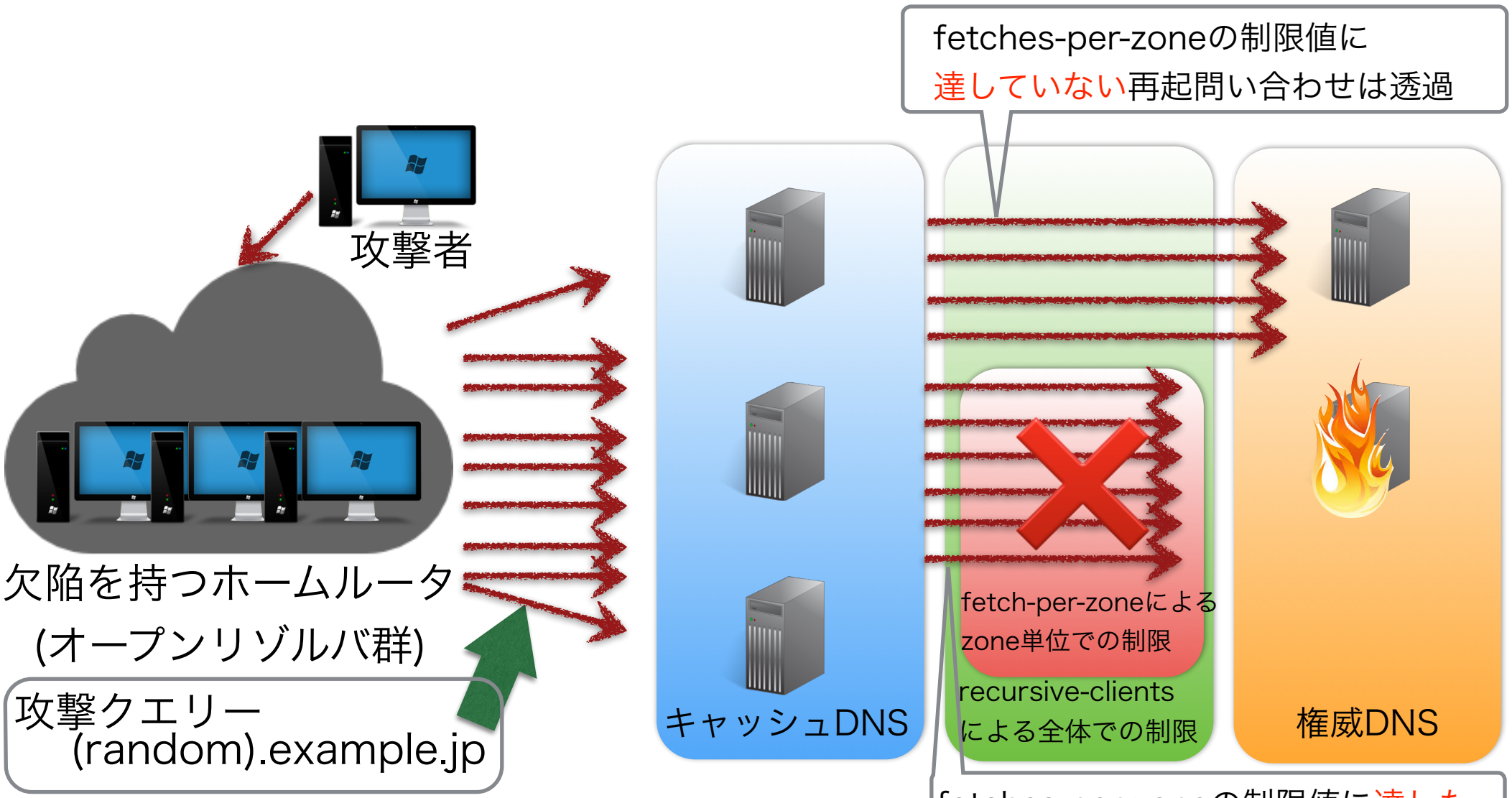
本発表はBIND 9.9.6-EXP-1を基に作成しています。

BIND9を用いた攻撃対策

キャッシュDNSの再起問い合わせを制御する機能

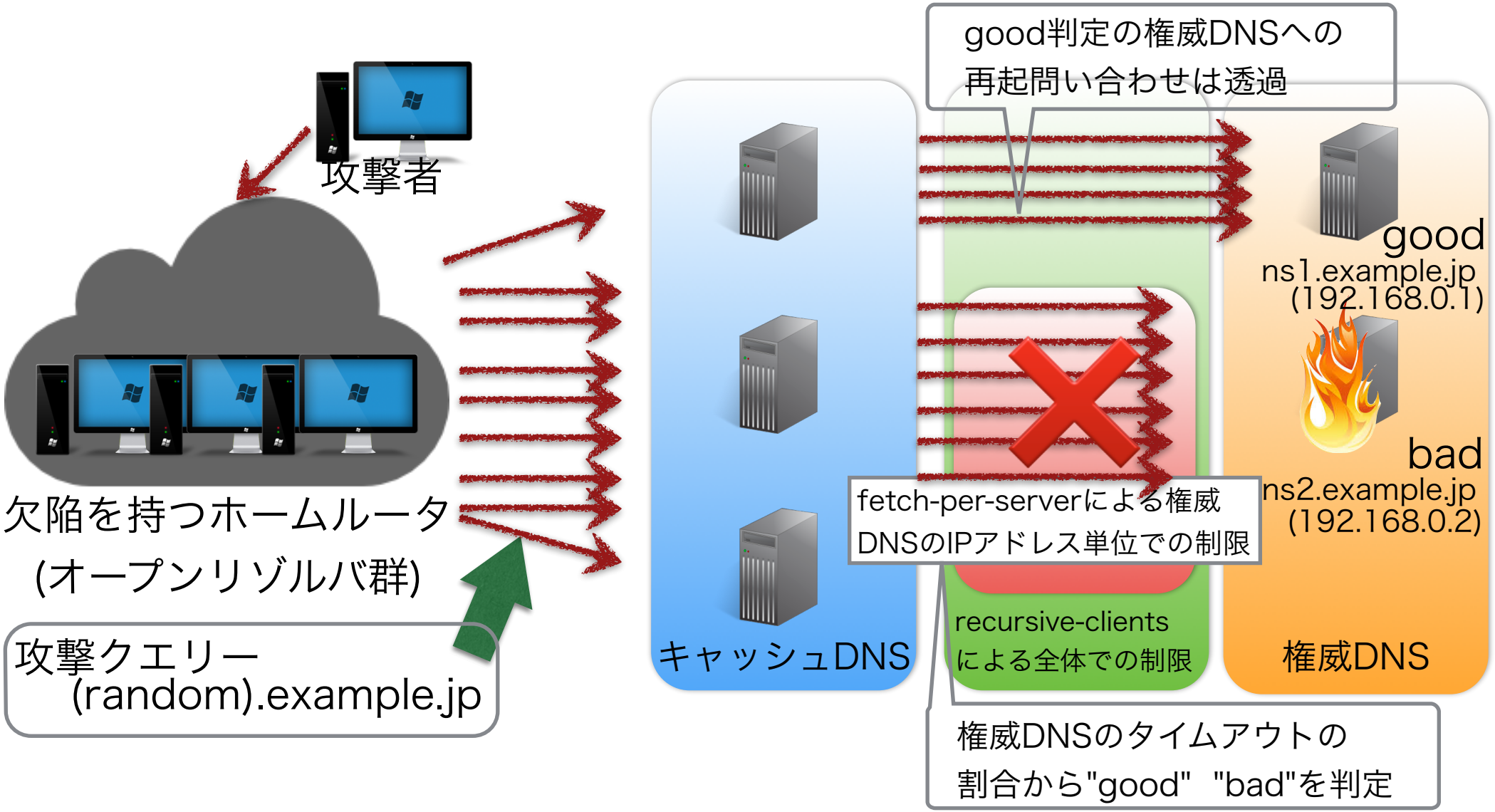
項目	機能
fetches-per-zone number ;	ドメイン単位で再起問い合わせを制限
fetches-per-server number ;	権威DNSのIPアドレス単位で再起問い合わせを制限
fetch-quota-params number fixedpoint fixedpoint fixedpoint ;	fetches-per-serverを制御するパラメータ

fetches-per-zone による再起問い合わせの制限



DNS全体でなく、ドメインに対して再起問い合わせの数を制限

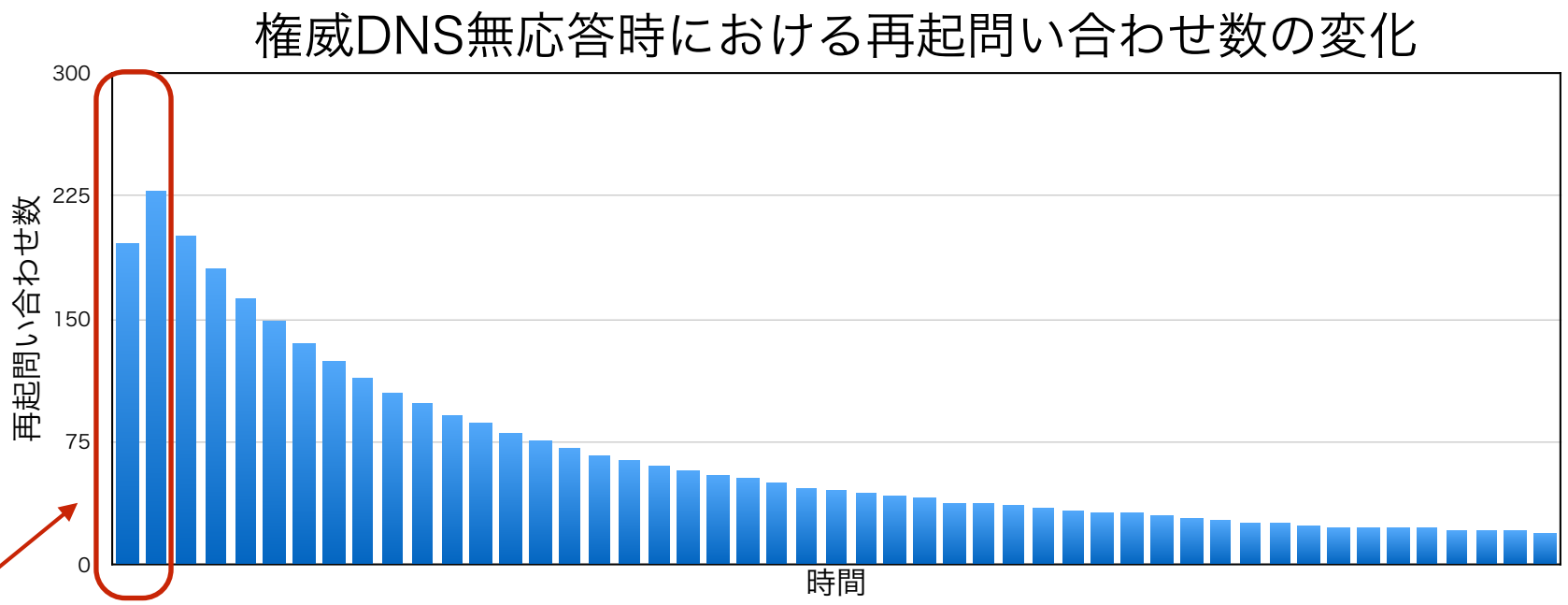
fetches-per-server による再起問い合わせの制限



権威DNSのIPアドレスに対して再起問い合わせを制限

再起問い合わせ数の動的制御について

検証時のパラメータ
fetches-per-server 300;
fetch-quota-params 100 0.1 0.3 0.7;



Q: Are there any edge cases where odd behavior might be observed?
A: When restarting a server, or if the cache has just been cleared via the rndc utility,
then there may be some temporary spikes in traffic that trigger these limits unexpectedly, but the effect should be temporary.
https://kb.isc.org/article/AA-01178/0/Recursive-Client-Rate-limiting-in-BIND-9.9-Subscription-Version.html より引用

グラフに関するコメントを追加する

権威DNSとのタイムアウト率に応じて、再起問い合わせ可能数が動的に変化

まとめ

・機能の詳細について調査や確認が必要
  - オプション導入による影響の検討

・設定パラメータの検討
  - 他のオプションや仕様面の考慮も

・評価(検証)内容の詳細検討
  - 机上での評価
  - フィールドでの評価

正常な通信へ影響をあたえないよう導入にあたっては慎重な評価が必要

参考リンク

- Recursive Client Rate limiting in BIND 9.9 Subscription Version

  <https://kb.isc.org/article/AA-01178/0/Recursive-Client-Rate-limiting-in-BIND-9.9-Subscription-Version.html>

- Tales of the unexpected - handling unusual DNS client behaviour

  <https://indico.uknof.org.uk/getFile.py/access?contribId=7&resId=2&materialId=slides&confId=31>