資料更新:2015/08/18

# DNS水責め(Water Torture)攻撃対策と動向について 2015

2015年07月24日
DNS Summer Days 2015

九州通信ネットワーク株式会社 (QTNet)
技術本部　サービスオペレーションセンター

末松慶文 (yo_suematsu at qtnet.co.jp)

# 自己紹介

- 末松慶文(すえまつ よしぶみ)
  - DNSを含むサーバ関連の構築と保守などを7-8年くらい。
- 九州通信ネットワーク(QTNet)
  - なんでもやってます！
- 児童ポルノブロッキングやってます

  - 実装と運用自動化について(QTNet 久米)

  http://dnsops.jp/event/20130718/20130718-kume-jipo-blocking-kume-1.pdf
- キャッシュDNSのDNSSEC Validateやってます

  - 安定稼働中。
- DNSの耐障害性強化に向けてJPRSと共同研究を開始

  JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始　http://jprs.co.jp/press/2015/150713.html

  QTNet: JPRSとの共同研究について　http://www.qtnet.co.jp/massmedia/2015/20150713_2.html

# 本発表の内容

- 水責め攻撃とは
  - ・DNS水責め(Water Torture)攻撃の概要と動向
- 水責め攻撃の対策
  - ・攻撃対策の紹介

    権威DNSでの対策はここでは扱いません。
- まとめ

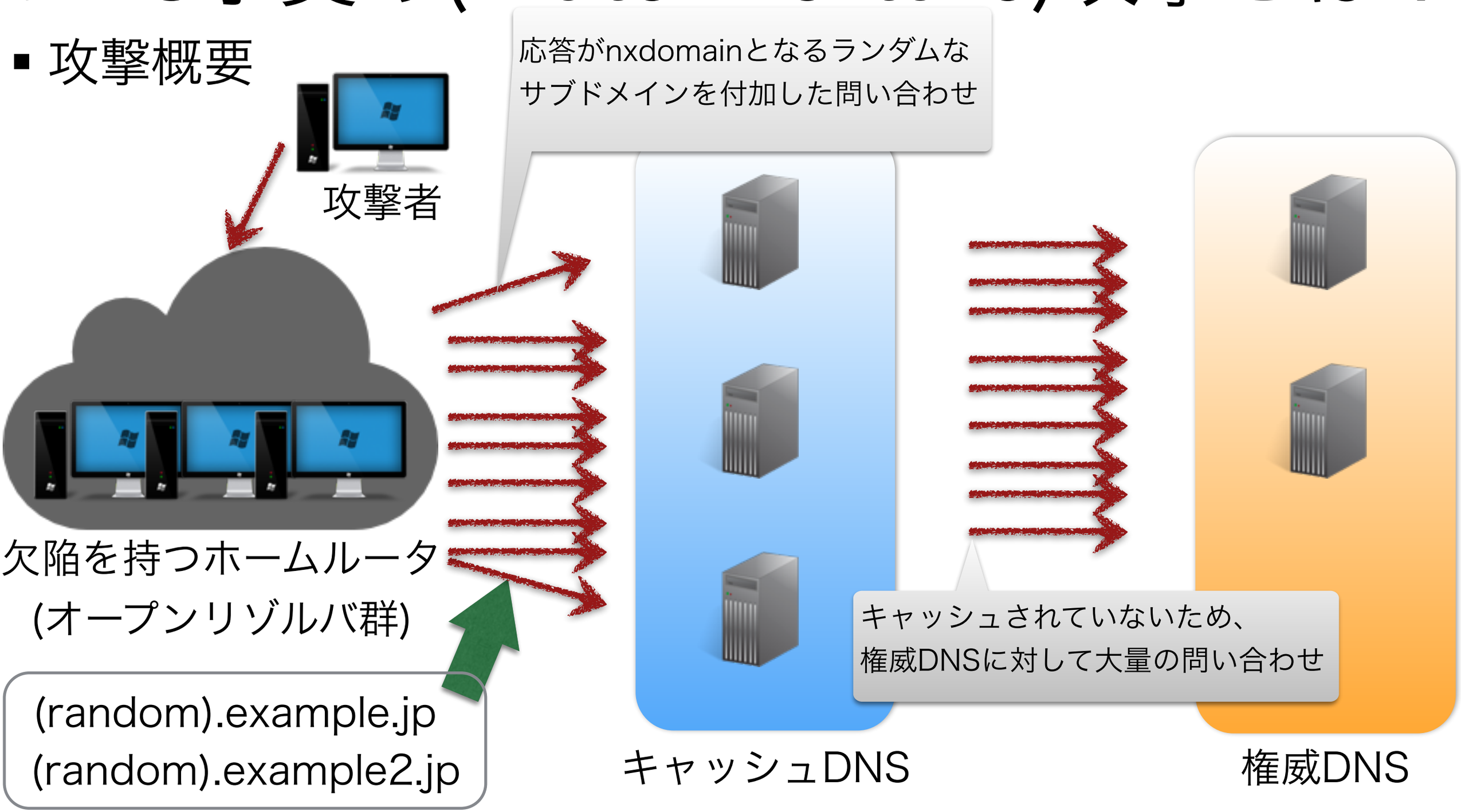
# DNS水責め(Water Torture)攻撃とは？

- 攻撃について
  - ・DNSに対するDDoS攻撃の手法の一つ
  - ・2014年初頭より、世界的に観測され始めた。
  - ・QTNetでは、問題が顕著化する前から、攻撃を検知しオープンリゾルバとなっているユーザに対して問診を開始
  - ・状況から真の攻撃対象は権威DNS
  - ・現在も攻撃は継続中

- 攻撃の特徴
  - ・ランダムなサブドメインを含むクエリで攻撃
  - ・オープンリゾルバを踏み台として攻撃
  - ・1クライアントあたりのクエリ数は低レート

# DNS水責め(Water Torture)攻撃とは？

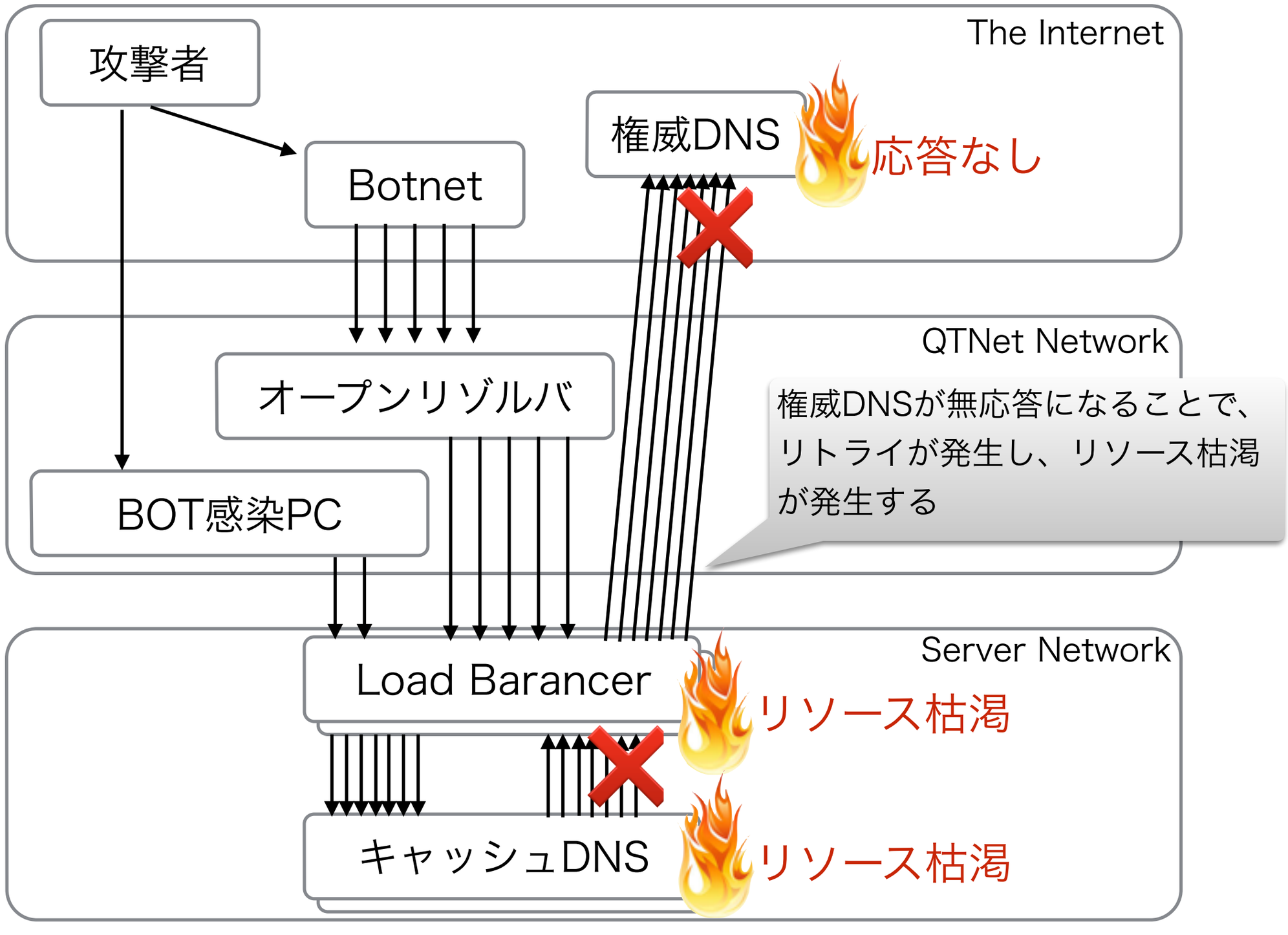
- 攻撃概要




キャッシュDNSや権威DNSが高負荷に

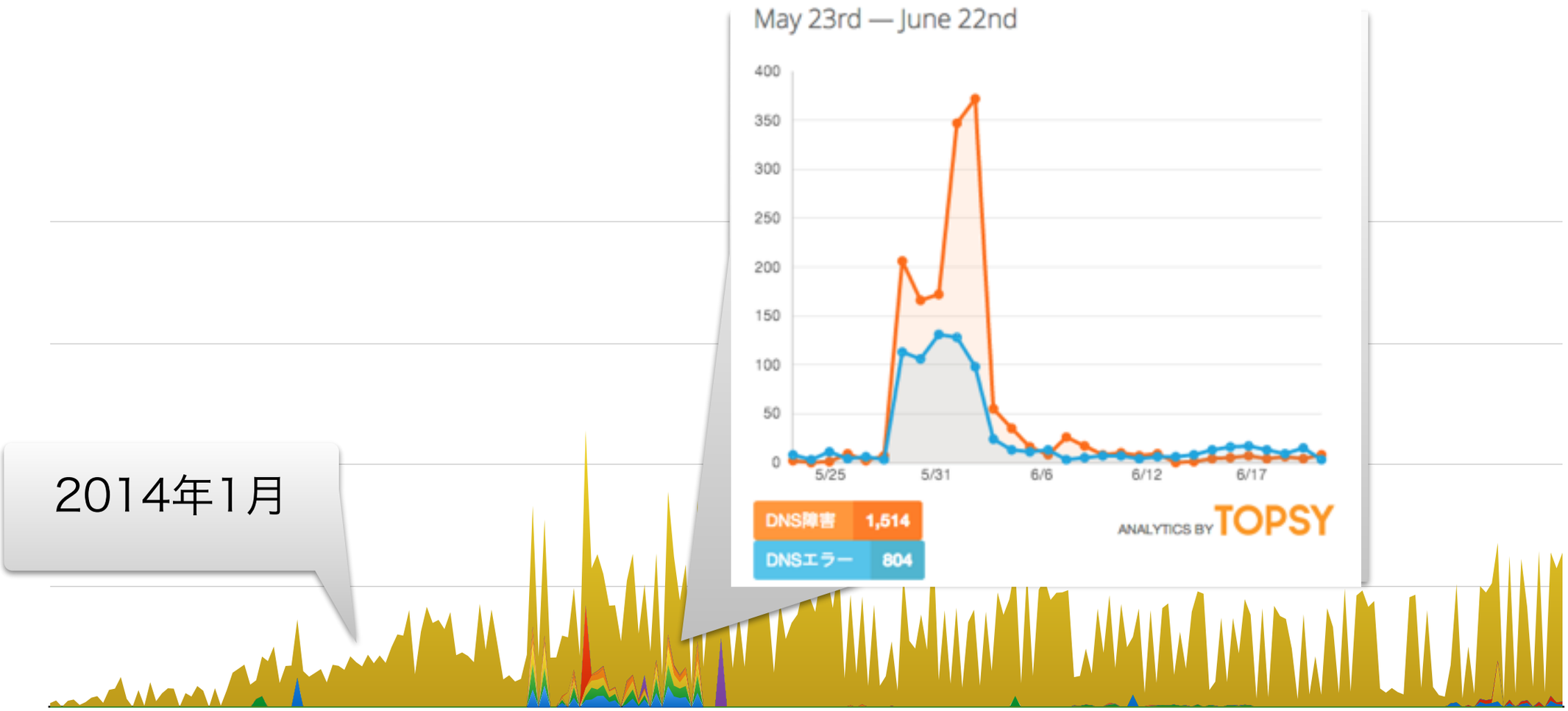
# DNS水責め(Water Torture)攻撃とは？

- 攻撃による影響



# DNS水責め(Water Torture)動向

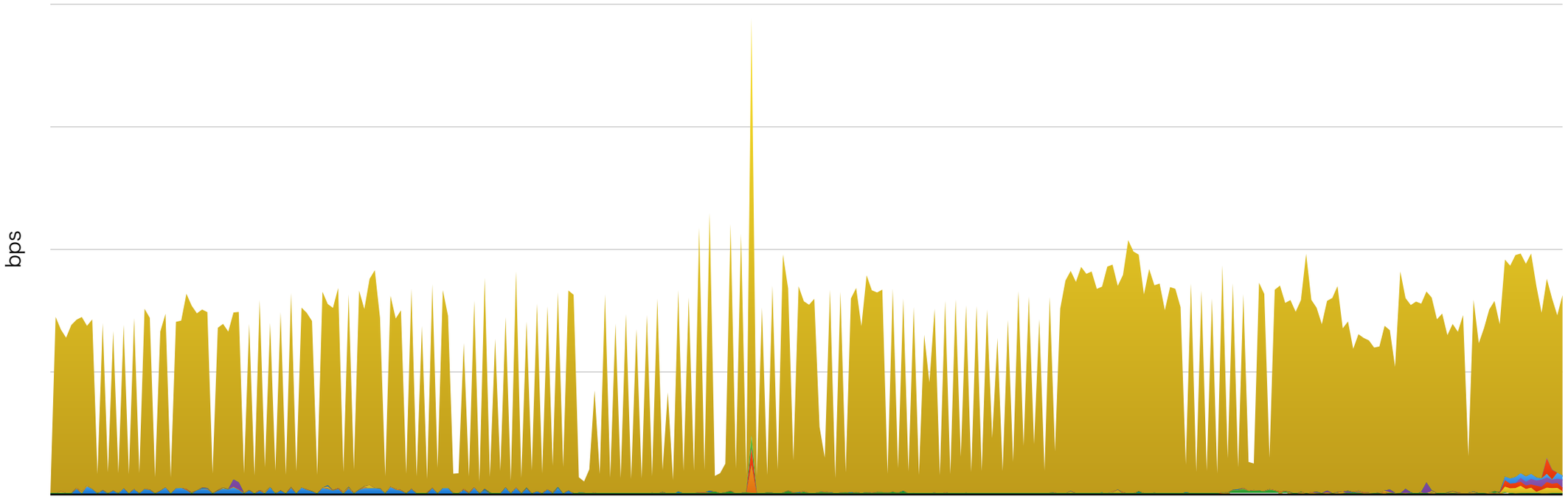
- ISP網内へのdst 53 流入トラフィックの推移 (2013/10/01- 2015/02/25)




Traffic of 53 port destination from Internet to QTNet(2013/10/01- 2015/02/25)

# DNS水責め(Water Torture)動向

- ISP網内へのdst 53 流入トラフィックの推移 (2015/02/26- 2015/07/22)




Traffic of 53 port destination from Internet to QTNet(2015/02/26- 2015/07/22)

現在もISP網内への流入トラフィックは継続中

最近水責めとあわせて、別の攻撃も・・(今回は扱いません)

# DNS水責め(Water Torture)攻撃とは？

ランダムクエリの発生源

・BOT化したPC（ISP網内）

・BOT化したPC（ISP網外）

・WEBカメラ

・オープンリゾルバ ホームルータ

想定もしていなかった機器がクエリ発生源の場合も

# DNS水責め(Water Torture)攻撃とは？

ランダムクエリの対策

・BOT化したPC（ISP網内）

→アンチウイルスソフトによるスキャン？

・BOT化したPC（ISP網外）

→IP53B

・WEBカメラ

→不明

・オープンリゾルバ ホームルータ

→ファームアップ、設定変更

クエリー送出元のほとんどがオープンリゾルバホームルータ

ユーザサイドでの対策には限界も・・・

# DNS水責め(Water Torture)対策

- 対策について

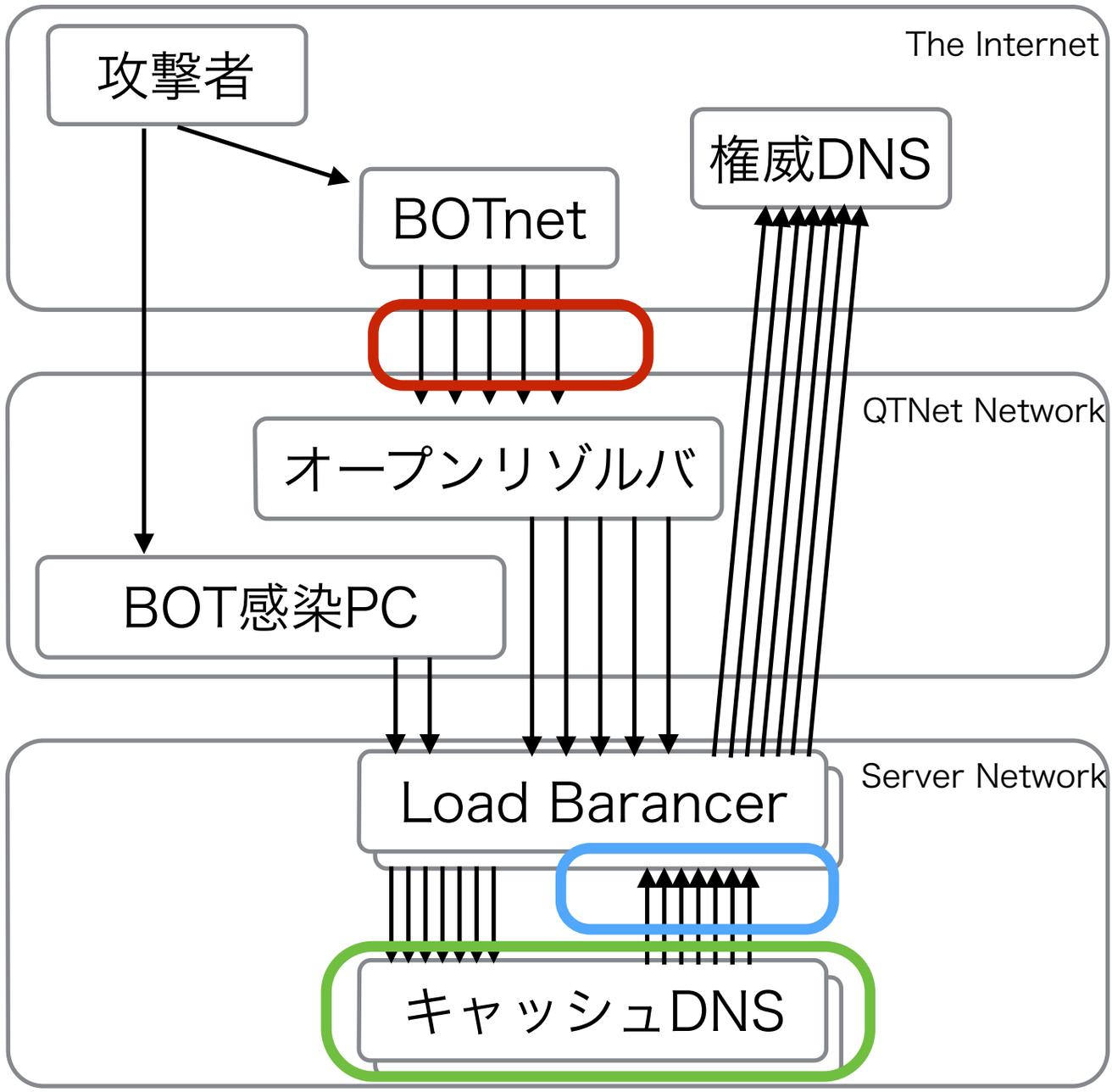
・IP53B

・iptables (hashlimit)

・対象ゾーンをローカルでもたせる

・BIND
(fetches-per-zone,fetches-per-server)

・Unbound




ブルームフィルタを利用したランダムサブドメイン攻撃の対策 (東 大亮さん)
http://www.slideshare.net/hdais/ss-41897131

# DNS水責め(Water Torture)対策

・ISP網内への流入するトラフィックの制御(IP53b)

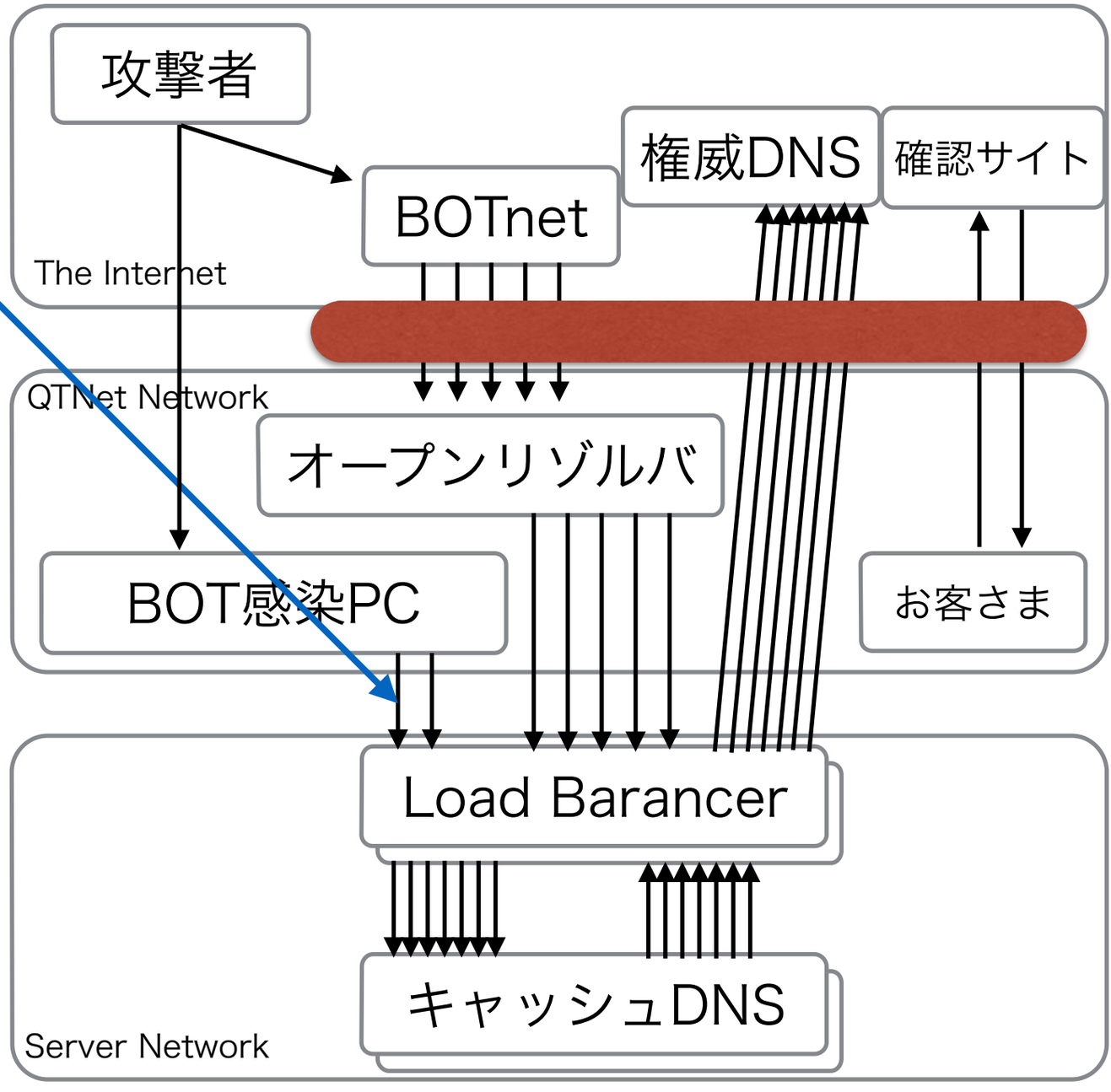
劇的な効果が期待できるが・・課題も

オープンリゾルバ以外から発生するクエリは**数%**

正常な通信を遮断しないよう考慮が必要

DNS以外の通信が存在？

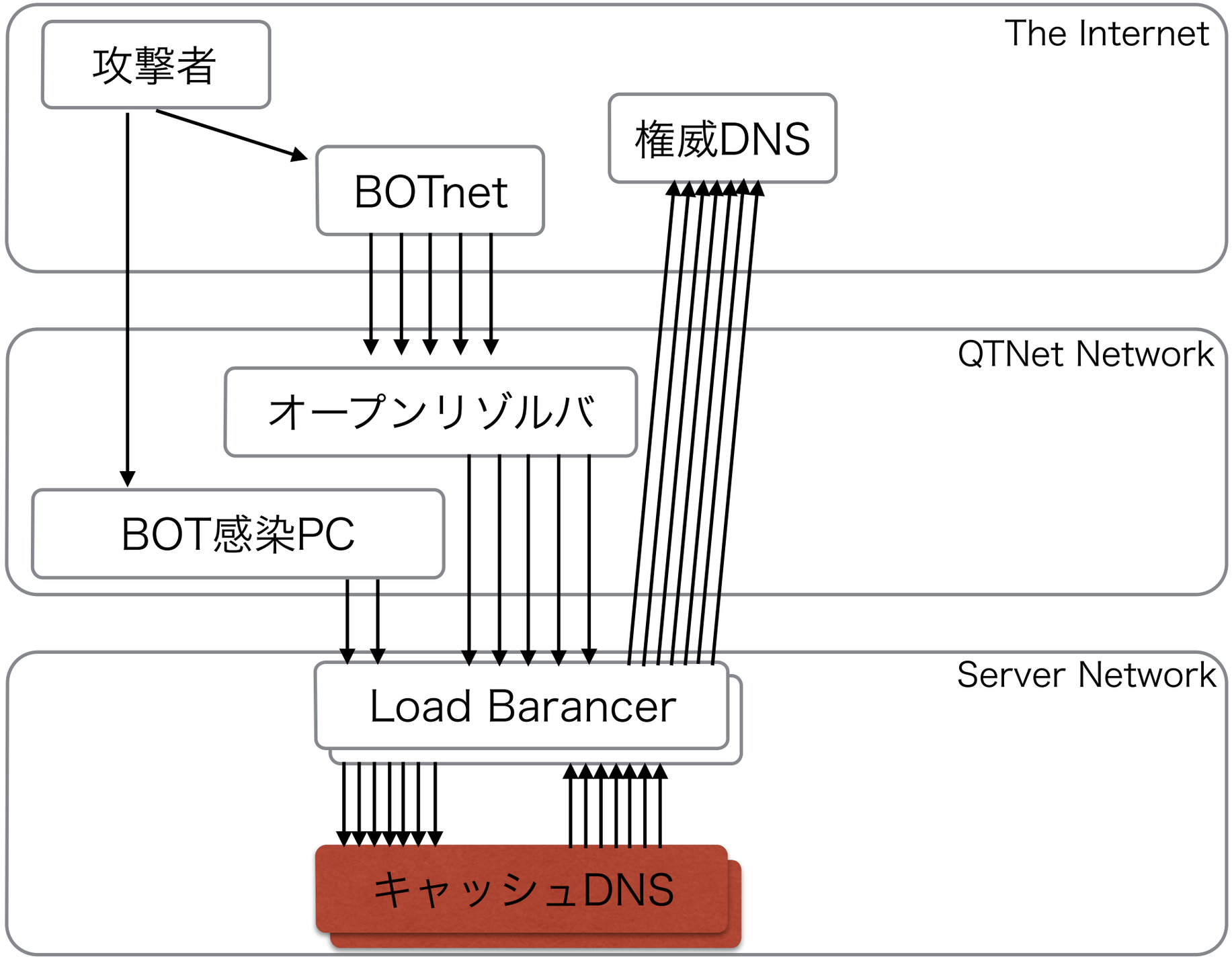
・一部CAT端末 ,XBOXが使用？




オープンリゾルバ確認サイト利用に配慮した手当も必要

# DNS水責め(Water Torture)対策

・対象ゾーンをローカルでもたせる



# DNS水責め(Water Torture)対策

・対象ゾーンをローカルで持たせる

- 特徴(メリットとデメリット)

  ・メリット

  攻撃対象のドメインを持たせればいいだけ
  (ただし、攻撃対象の抽出が課題)

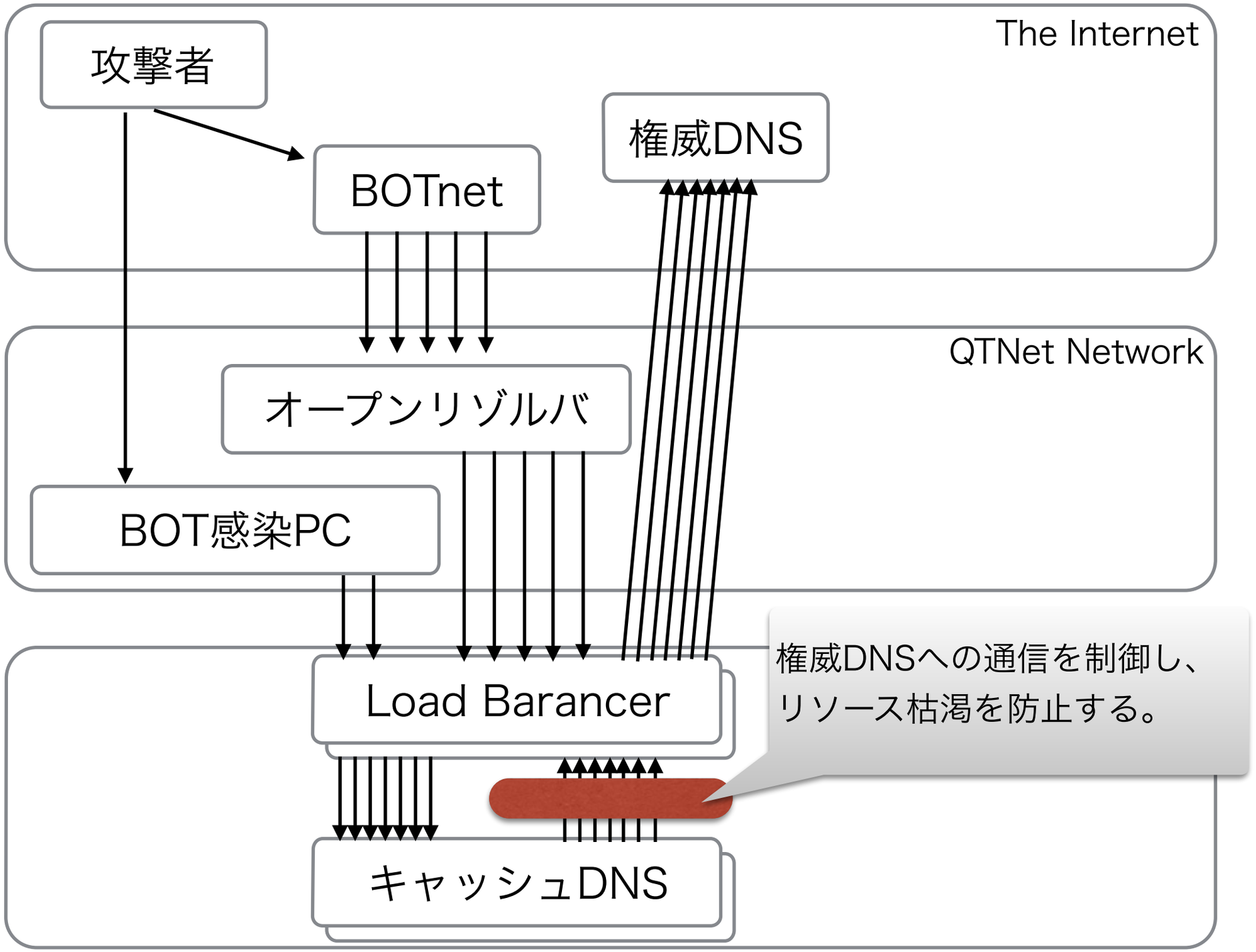
  ・デメリット

  自動化した場合、誤判定による正常な通信への影響が懸念される

権威DNS向けの通信は抑制できるが、DoSとしては成立

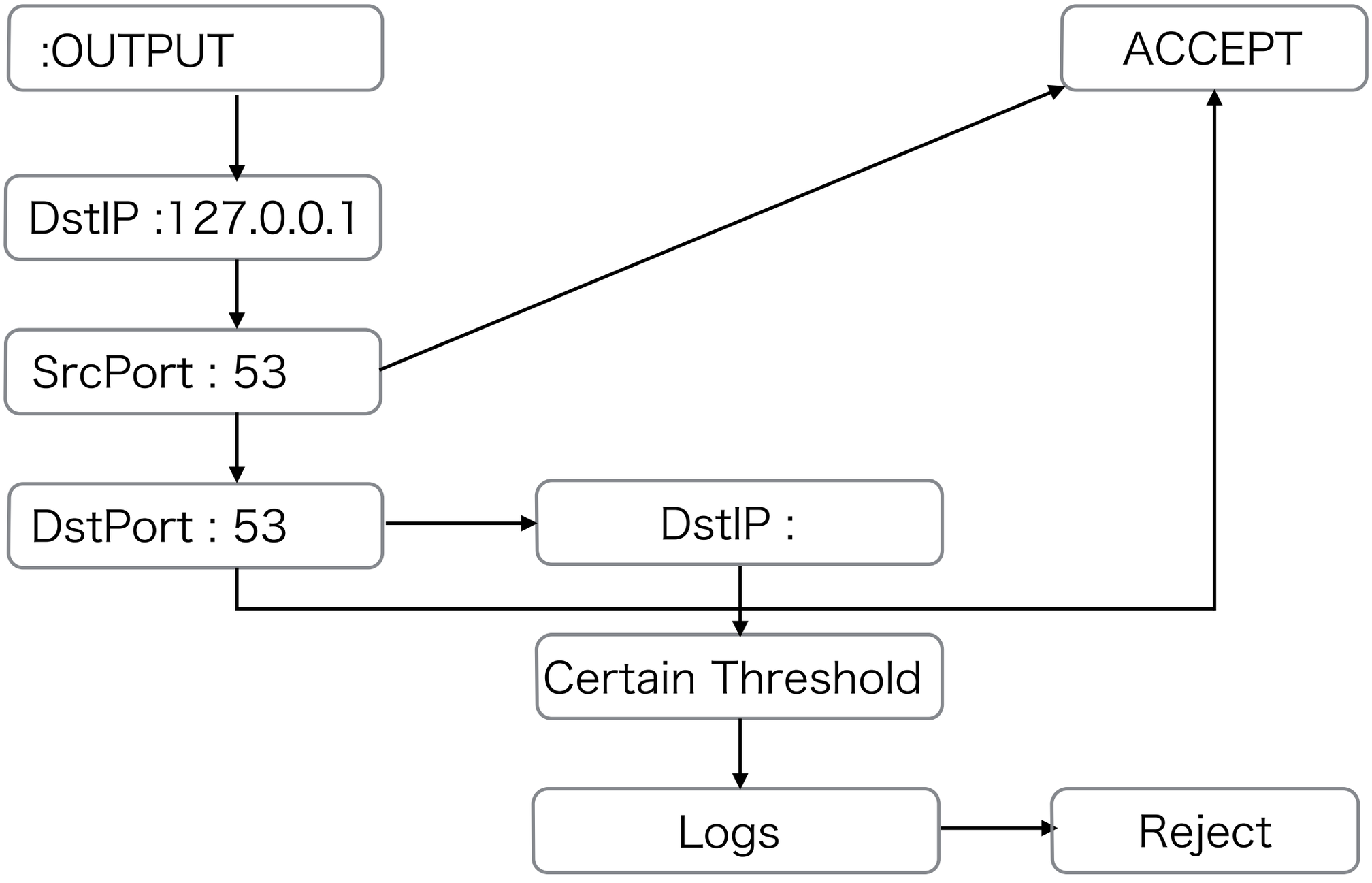
# DNS水責め(Water Torture)対策

## iptables hashlimit



# DNS水責め(Water Torture)対策

iptables hashlimit簡易フロー




OUT方向の通信をIPアドレス毎で判定を行い、権威DNSへの通信を制御

# DNS水責め(Water Torture)対策

- 特徴(メリットとデメリット)

・メリット

・OUT方向のみパケットを監視/制御するため、負荷コスト低
通常、キャッシュヒット率は90%以上

・burstの設定など、細かな制御が行える

・デメリット

・定常的にユニークなクエリを送出するドメイン(サービス)などは考慮が必要

水責め攻撃対策には有効だが、定期的にメンテナンスが必要

# DNS水責め(Water Torture)対策

・BINDによる攻撃影響の軽減

## 「BIND 9に対策機能はあります。」

※今まではSubscription VersionとExperimental Branchのみ

2015/08/07リリース!

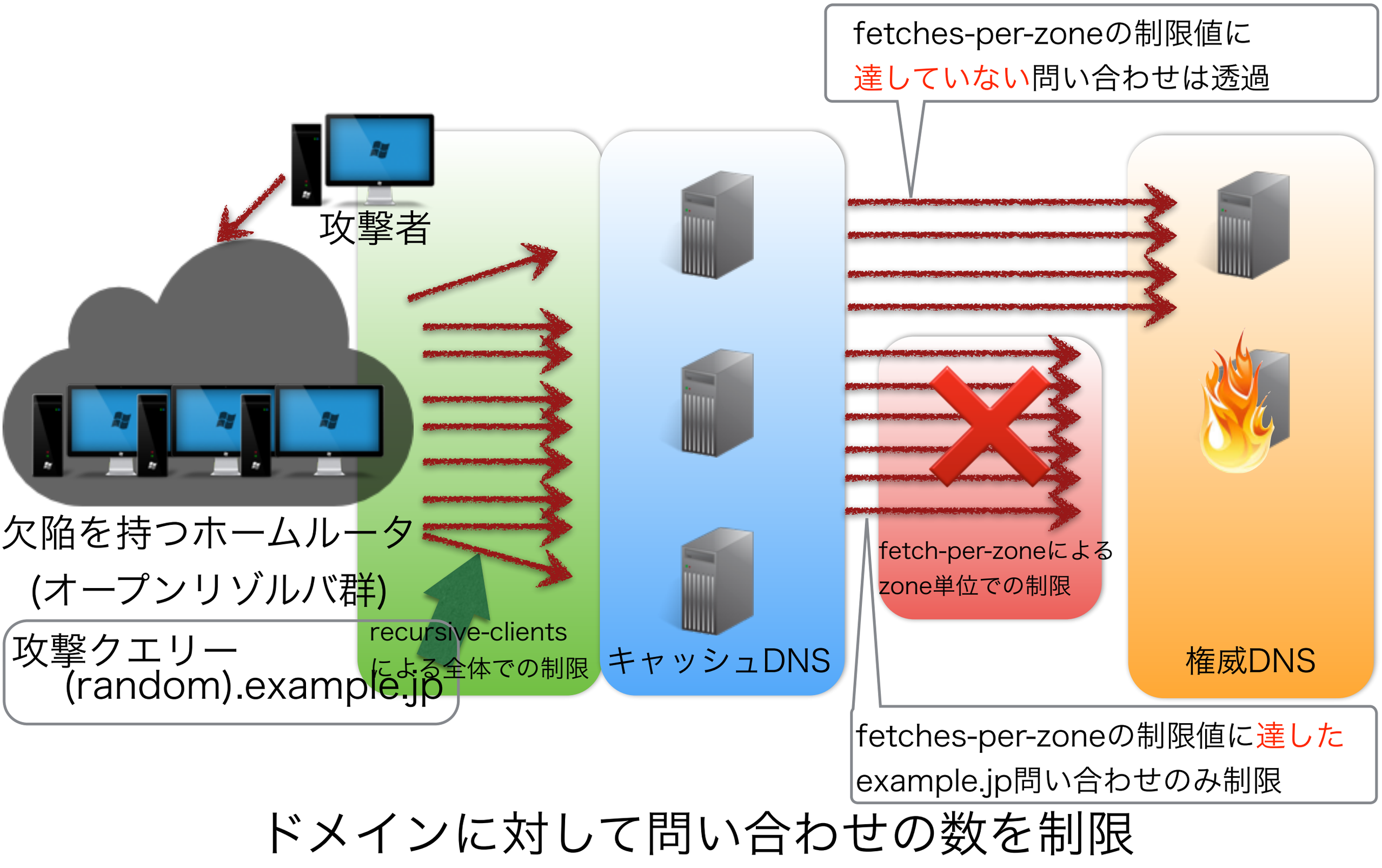
BIND 9.9.8b1 9.10.3b1に機能を搭載！！

https://source.isc.org/betas.shtml

https://lists.isc.org/pipermail/bind-users/2015-August/095428.html

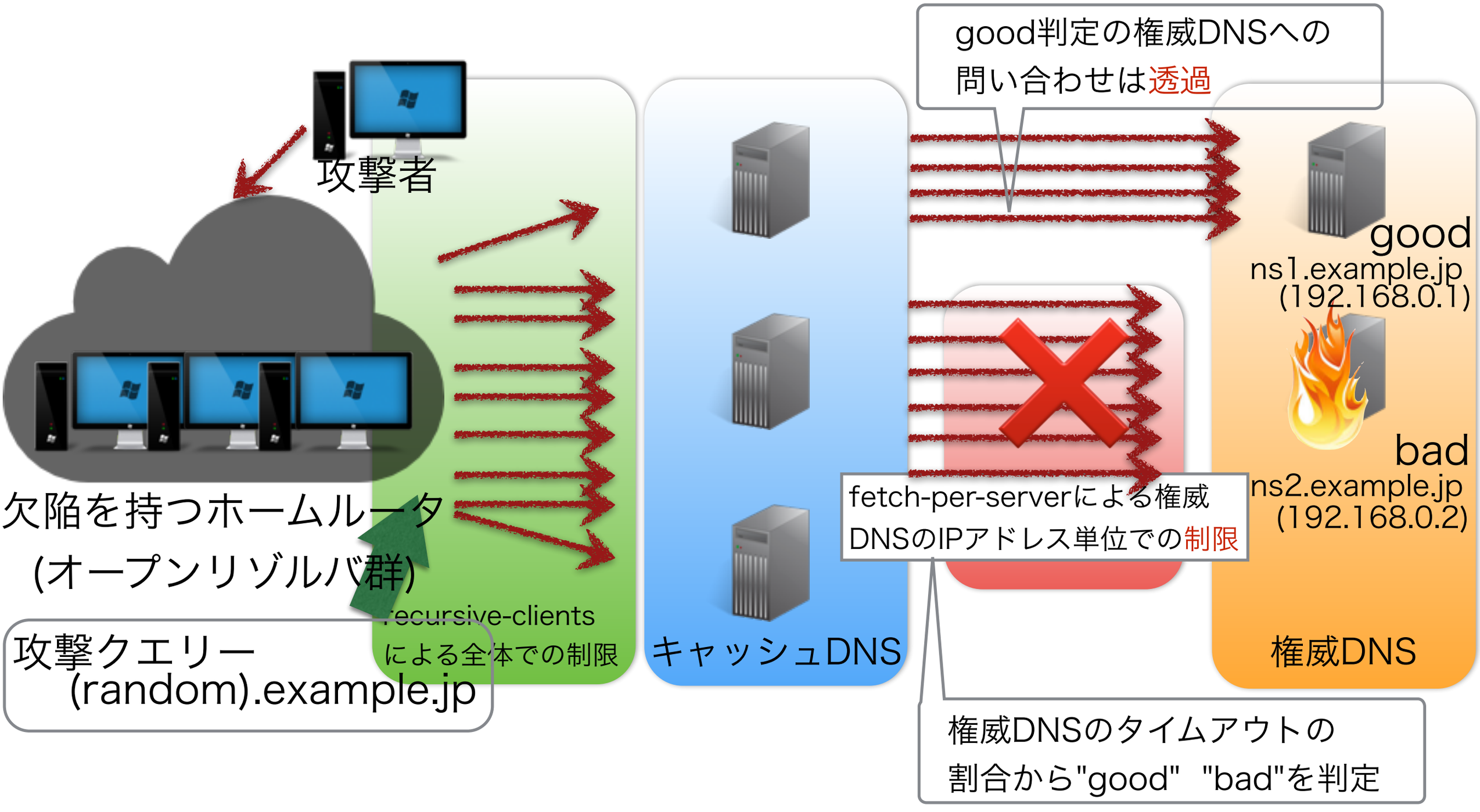
本発表はISCより提供されたBIND 9.9.6-EXP-1を基に作成しています。

# fetches-per-zone による問い合わせの制限




ドメインに対して問い合わせの数を制限

# fetches-per-server による問い合わせの制限




権威DNSのIPアドレスに対して問い合わせを制限

# まとめ

・DNS水責め攻撃の概要を説明
  - 2014年初頭より現在も攻撃は継続
  - ホームルータだけでなく、一部のWEBカメラなどに問題がある場合も

・DNS水責め攻撃の対策を説明
  - iptables hashlimitは低コストで効果的であるが、メンテが必要
  - IP53Bは効果は見込めるが、正常な通信への影響も懸念される
  - 現状、決定打と考えられる対策は存在しない

正常な通信へ影響をあたえないよう各対策実施にあたっては慎重な評価が必要

# 参考リンク


・Water Torture: A Slow Drip DNS DDoS Attack on QTNet by Kei Nishida

http://www.slideshare.net/apnic/dnswatertortureonqtnet-1425130417-1425507043 [APRICOT 2015]

・DNS水責め(Water Torture) 攻撃について

<http://2014.seccon.jp/dns/dns_water_torture.pdf>

・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>