DNS水責め(Water Torture) 攻撃対策と動向について 2016

2016年06月24日

DNS Summer Day 2016

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8年ちょっとくらい。
- 九州通信ネットワーク(QTNet)
  - なんでもやってます！
  - DNSの耐障害性強化に向けてJPRSと共同研究を開始 (2015年7月13日)

    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

NEW！
  - JPRSおよび電力系通信事業者7社による共同研究の実施(2016年1月18日)
    +1社 http://www.qtnet.co.jp/massmedia/2016/20160118.html

NEW！
- [janog38 LT] 大規模災害時のインターネットの継続提供への取り組み

  https://www.janog.gr.jp/meeting/janog38/lt-vt

NEW！
- [janog38] EDNS-client-subnetってどうよ? 改めRFC7871ってどうよ

  http://www.janog.gr.jp/meeting/janog38/program/edns

本発表の内容

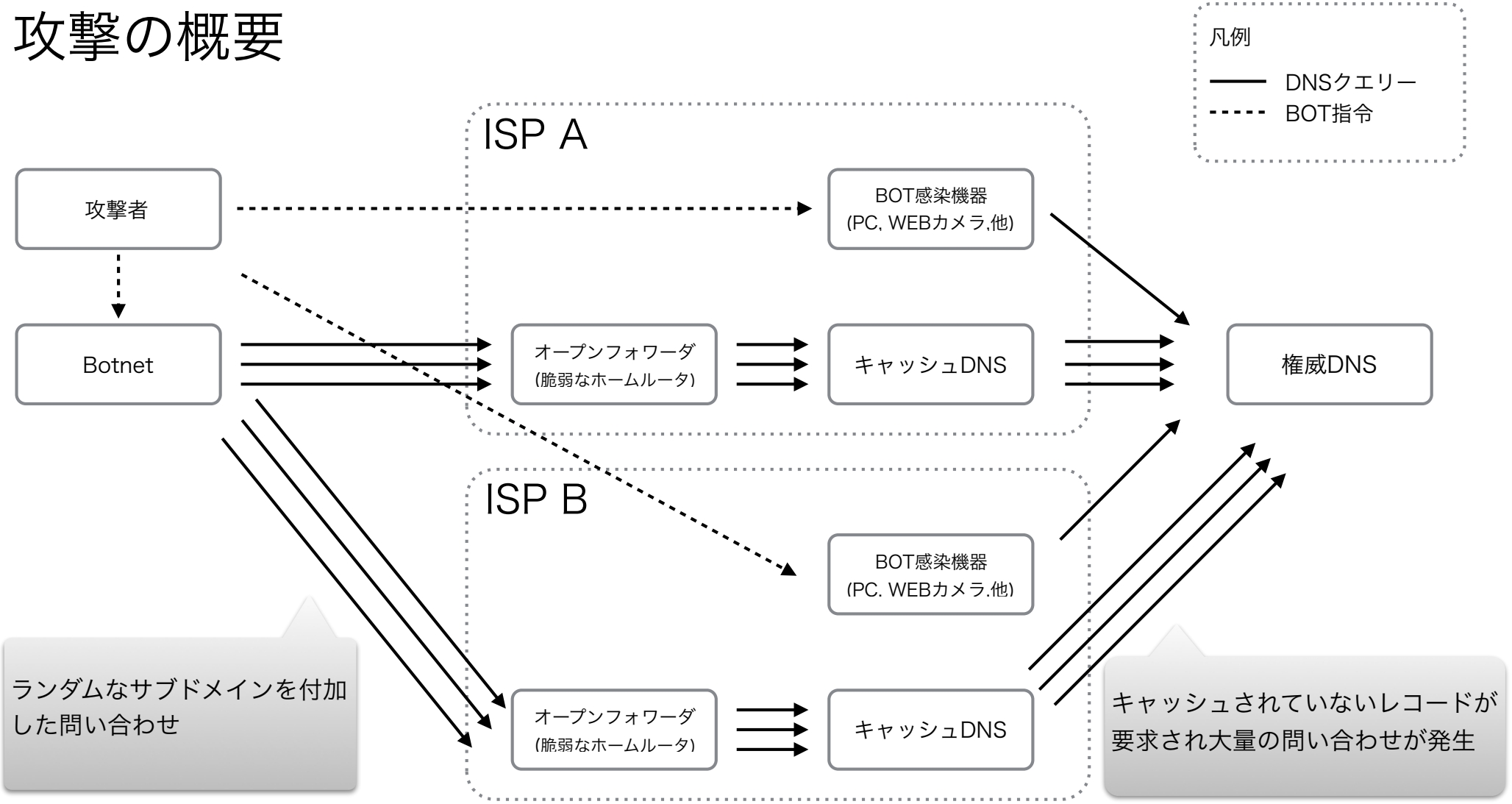
- 水責め攻撃の動向
  - 攻撃の概要
  - 攻撃による影響
  - 流入トラフィックの推移
  - 特徴的な水責め攻撃について
  - **実は・・!!**
- 水責め攻撃の対策
  - 攻撃対策の紹介
- まとめ

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。
  - ・真の攻撃対象は権威DNS
    - キャッシュDNSも間接的に大きな影響を受ける。
  - ・日本でも影響が観測された。
    - [2014] 6月から7月に日本の多くのISPでも水責めが観測された。
    - [2015] JPドメイン名を標的とした“DNS水責め攻撃”を確認
- 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水責め攻撃の動向

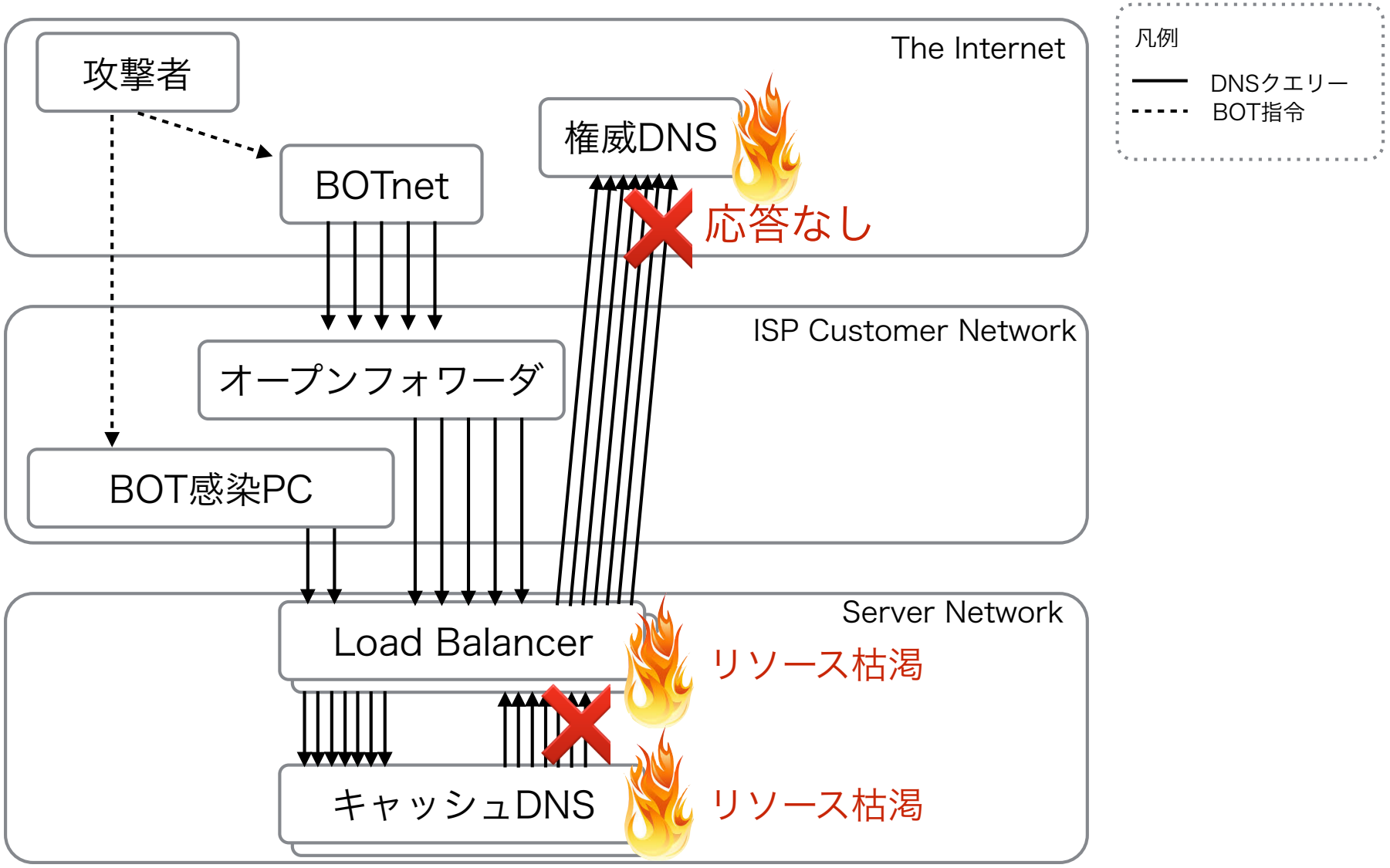
- 攻撃の概要



- 広く浅く、キャッシュDNSに突き刺さる。
- 権威DNSが真のターゲット、キャッシュDNSは巻き添え

DNS水責め攻撃の動向

- 攻撃による影響



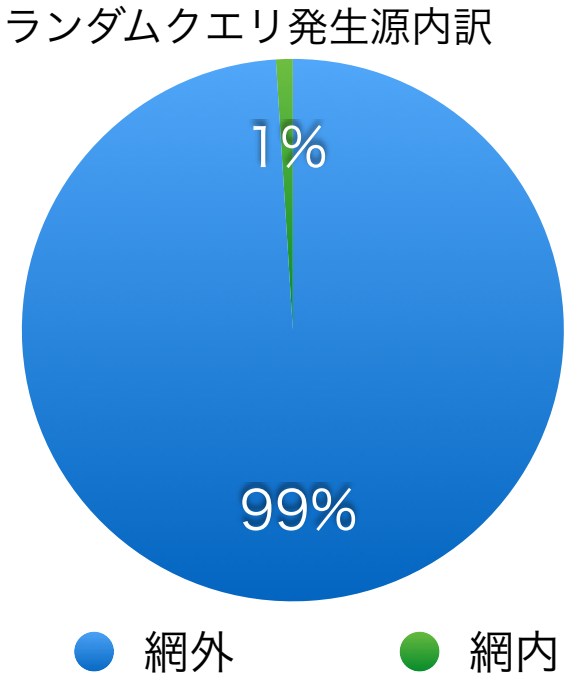
権威DNSが応答を返せないことにより

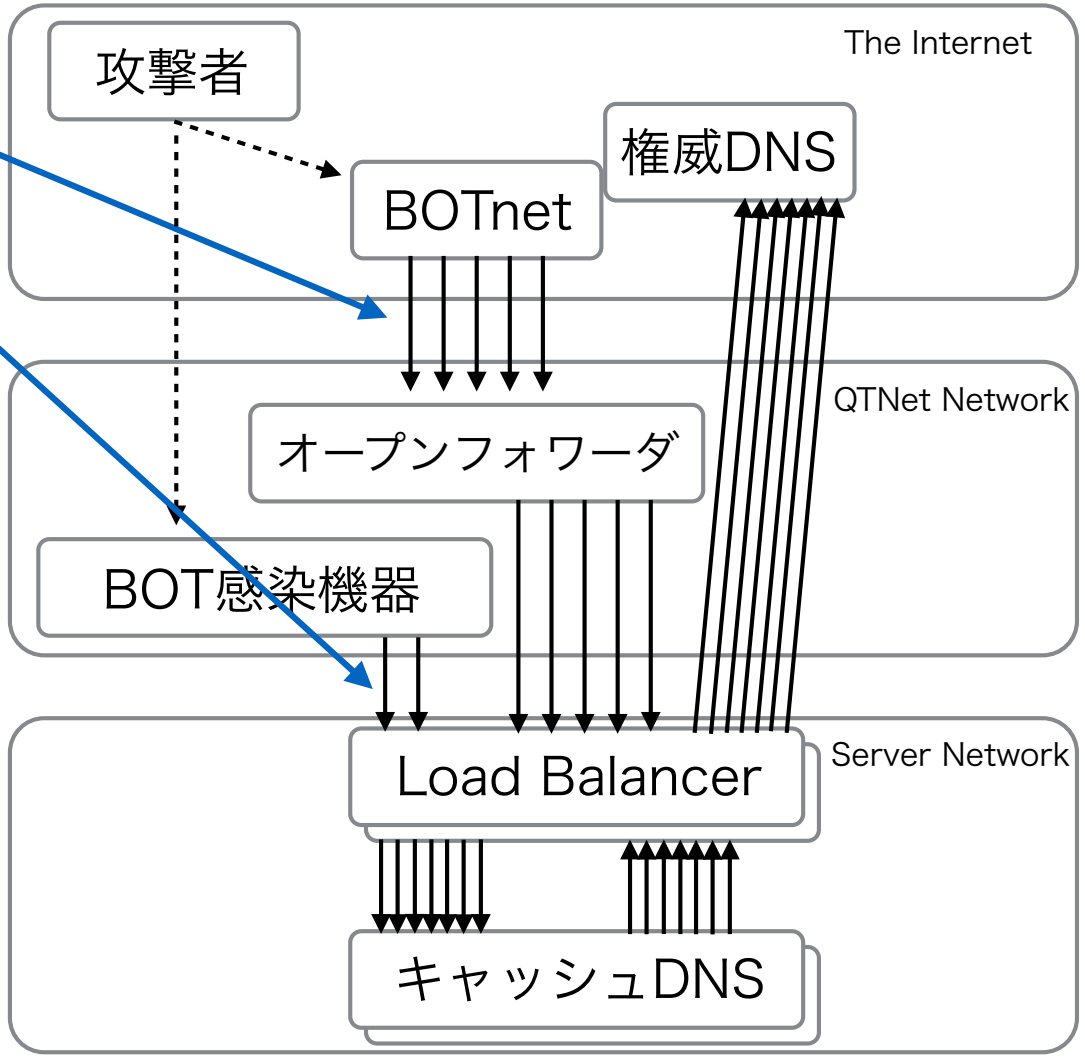
キャッシュDNSやLoad Balancerでリソース枯渇が発生

DNS水責め攻撃の動向

キャッシュDNSに到達する

- ランダムクエリの発生源について
  - ISP**網外**のBOTnetに由来
  - ISP**網内**のBOT感染機器に由来

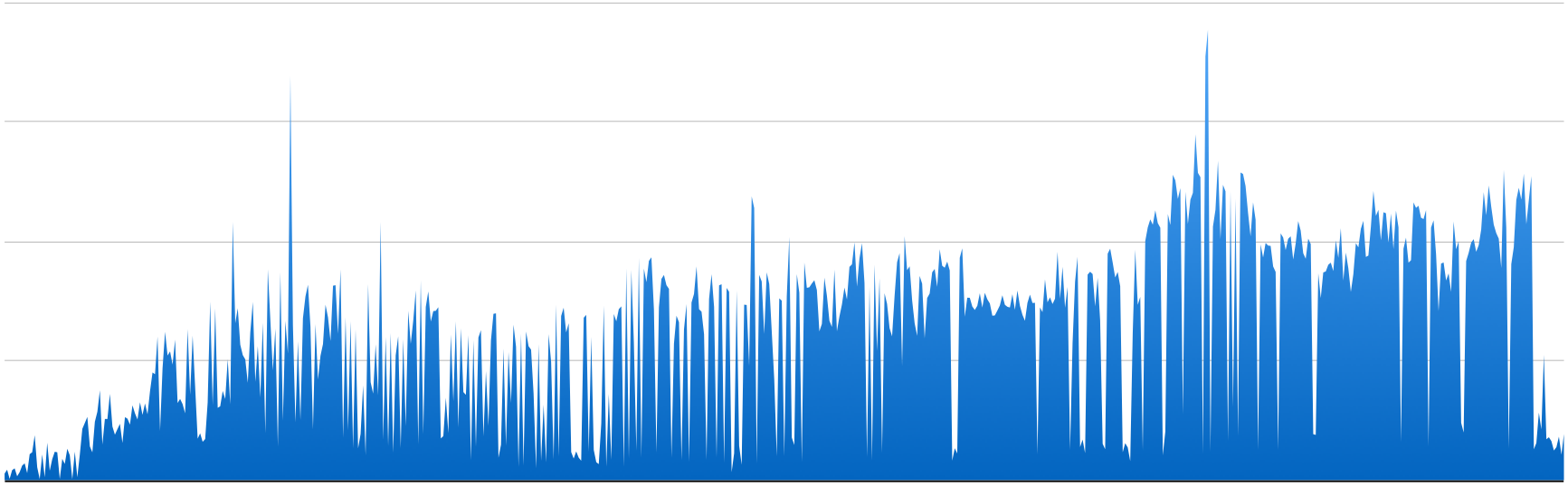




発生源の99%を占めるISP網外からのトラフィック動向についてもう少し詳しく。

DNS水責め攻撃の動向

- ISP網内への流入トラフィックの推移 (2013/12/13- 2016/06/09)



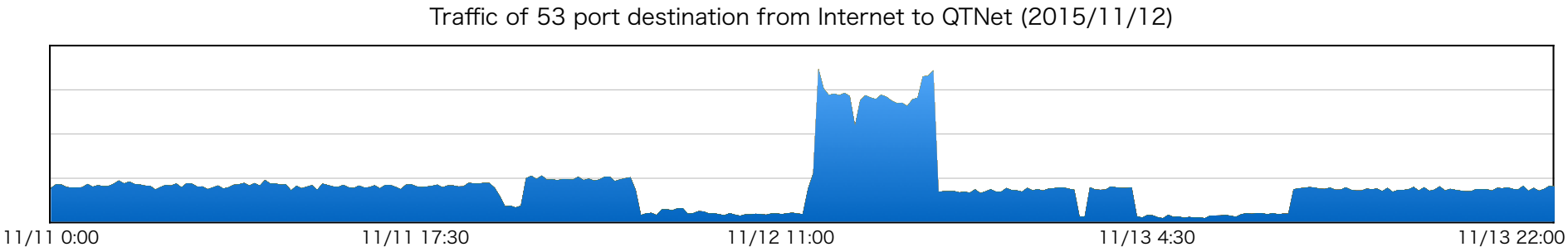
Traffic of 53 port destination from Internet to QTNet (2013/12/13- 2016/06/09)

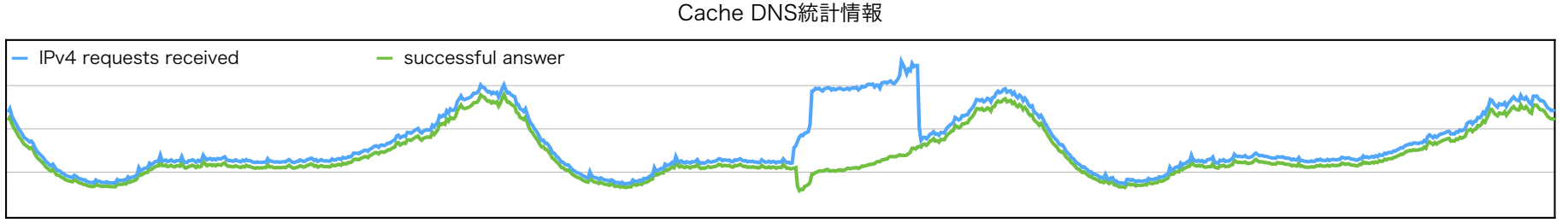
2014年初頭から2016年まで継続してトラフィックが発生

DNS水責め攻撃の動向

- 特徴的な水責め攻撃について(2)

- 高トラフィック流入型　(2015/11/12)



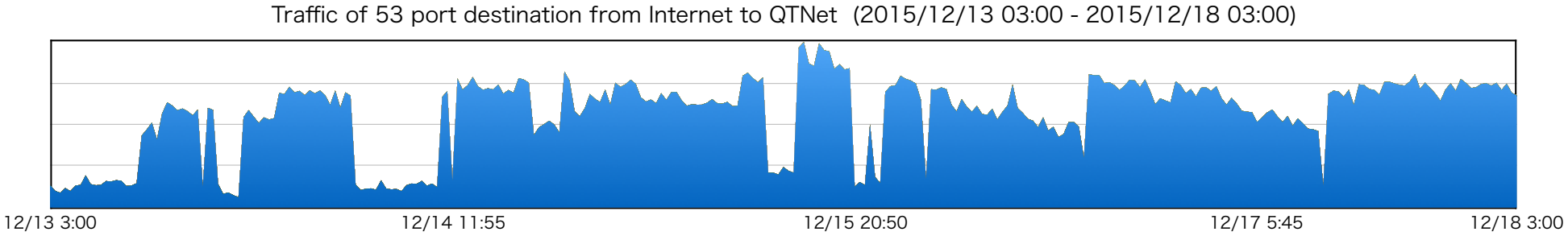


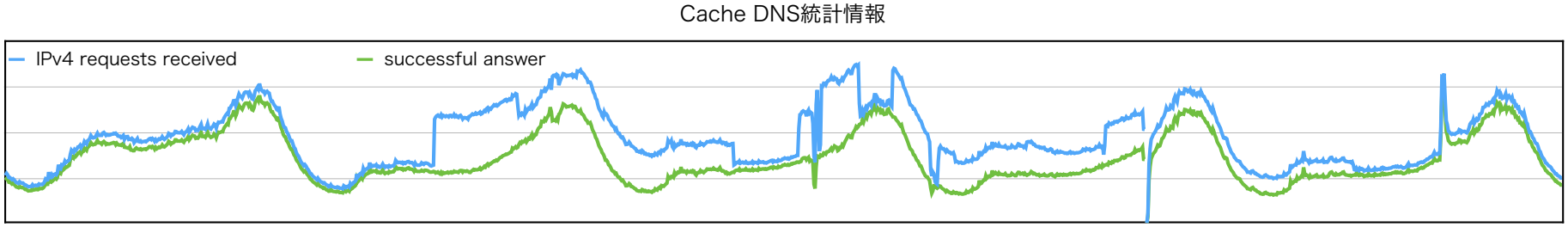
流入トラフィックが通常時の約3倍、キャッシュDNSへの到達クエリーも増加

DNS水責め攻撃の動向

- 特徴的な水責め攻撃について(2)

  更新されたオープンリゾルバのリストを使用し、的確にISP網内のオープンリゾルバを狙う - 高ヒット率型 (2015/12/13 03:00 - 2015/12/18 03:00)

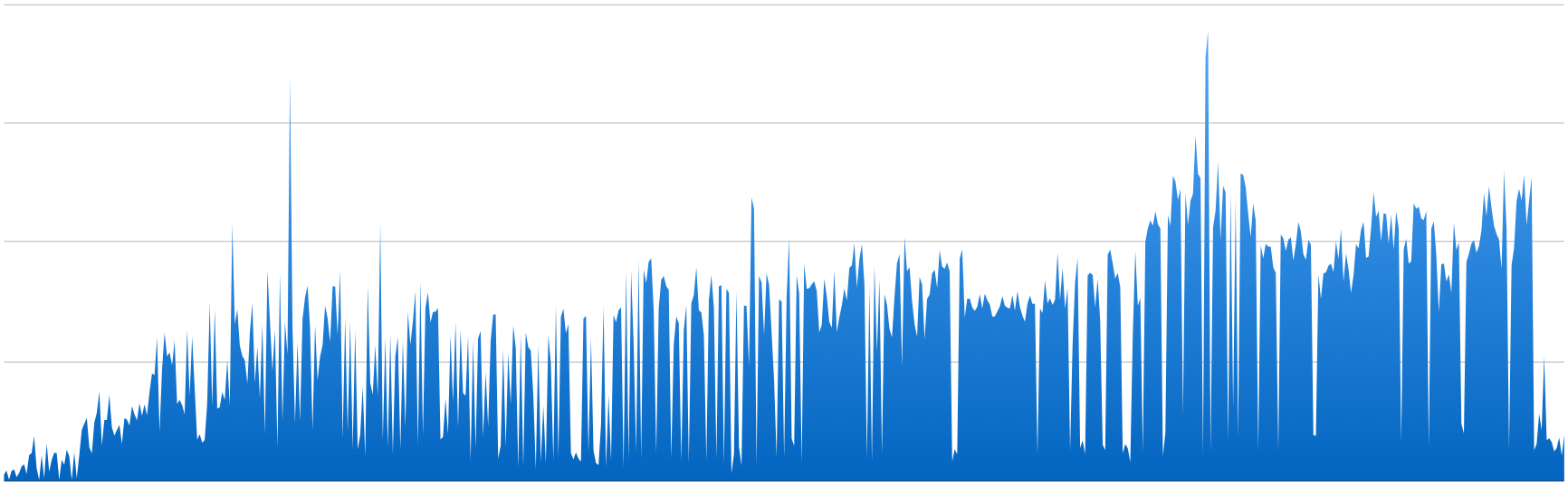




流入トラフィックが通常時と変わらないが、キャッシュDNSへの到達クエリーが増加

DNS水責め攻撃の動向

- ISP網内への流入トラフィックの推移 (2013/12/13- 2016/06/09)



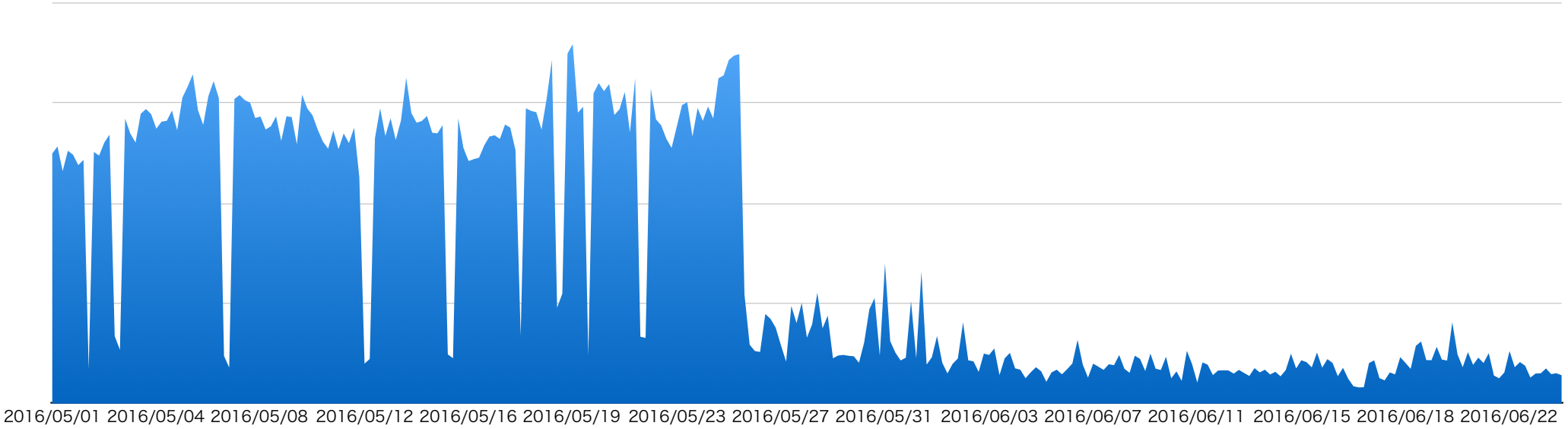
Traffic of 53 port destination from Internet to QTNet (2013/12/13- 2016/06/09)

全体的には右肩上がりにトラフィック増加、でも・・なにか気がつきませんか？

DNS水責め攻撃の動向

- ISP網内への流入トラフィックの推移(2016/05/01- **2016/06/24 12:00**)

5/25より約1ヶ月間、流入トラフィックが**激減**



2014年から今まで流入トラフィックが長期間激減したことは**初めて**

今後も十分な注意と攻撃再開に備えて対策を進めることが重要

DNS水責め攻撃の対策

- 対策について

・IP53B

ISP網内への流入トラフィックの抑止

・対象ゾーンをローカルでもたせる

攻撃対象ドメインのNSへの通信を抑制

※発生後の対策となること、DoS自体は成立

・iptables (hashlimit)

攻撃対象ドメインのNSへの通信を制限

※閾値の調整が難しい、NSが多くなると・・

・BIND

(fetch-per-zone, fetch-per-server)

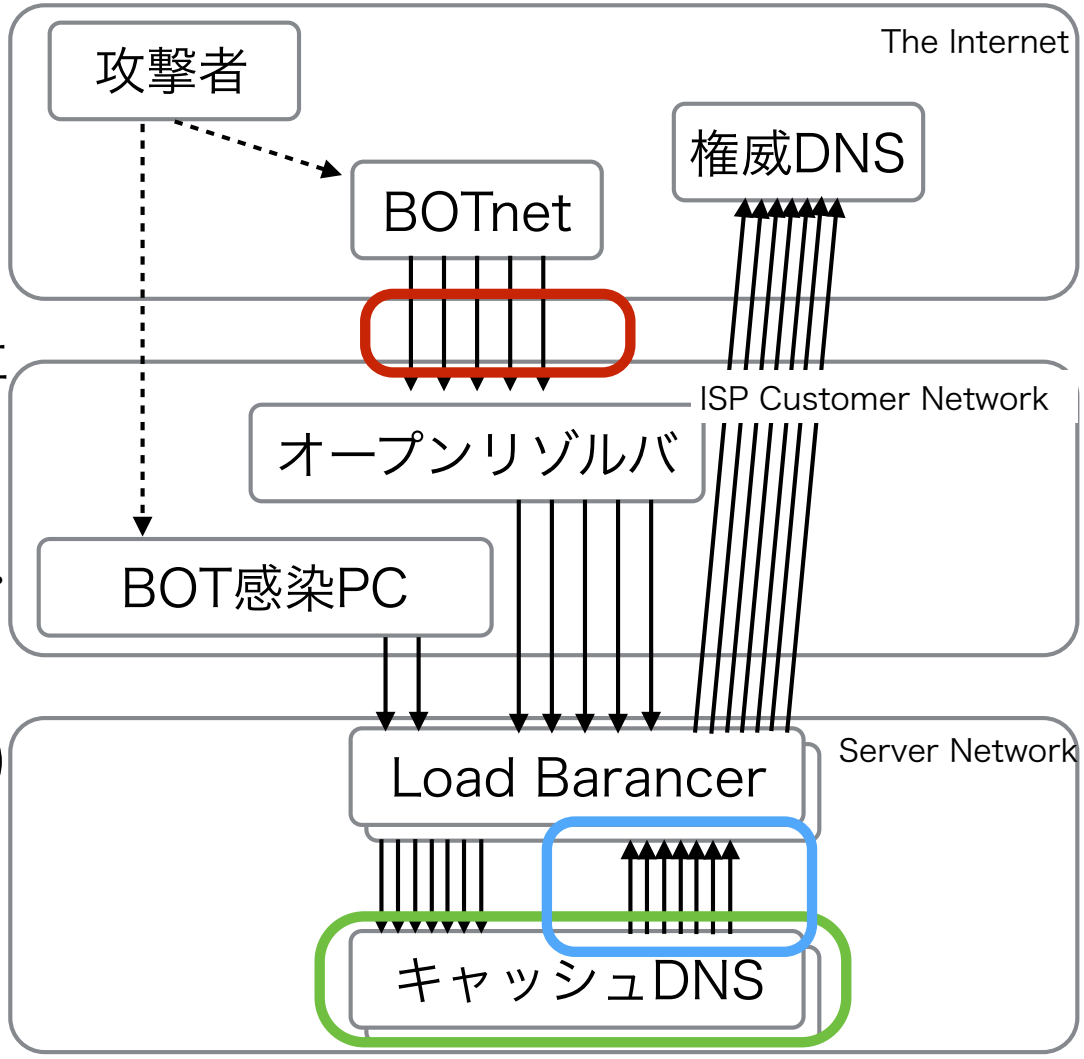
・Unbound

(ratelimit-for-domain, ratelimit)

実験的？

・Nominum Vantio

(応答のないNSへの通信を抑制, ThreatAvert)



DNS水責め攻撃の対策

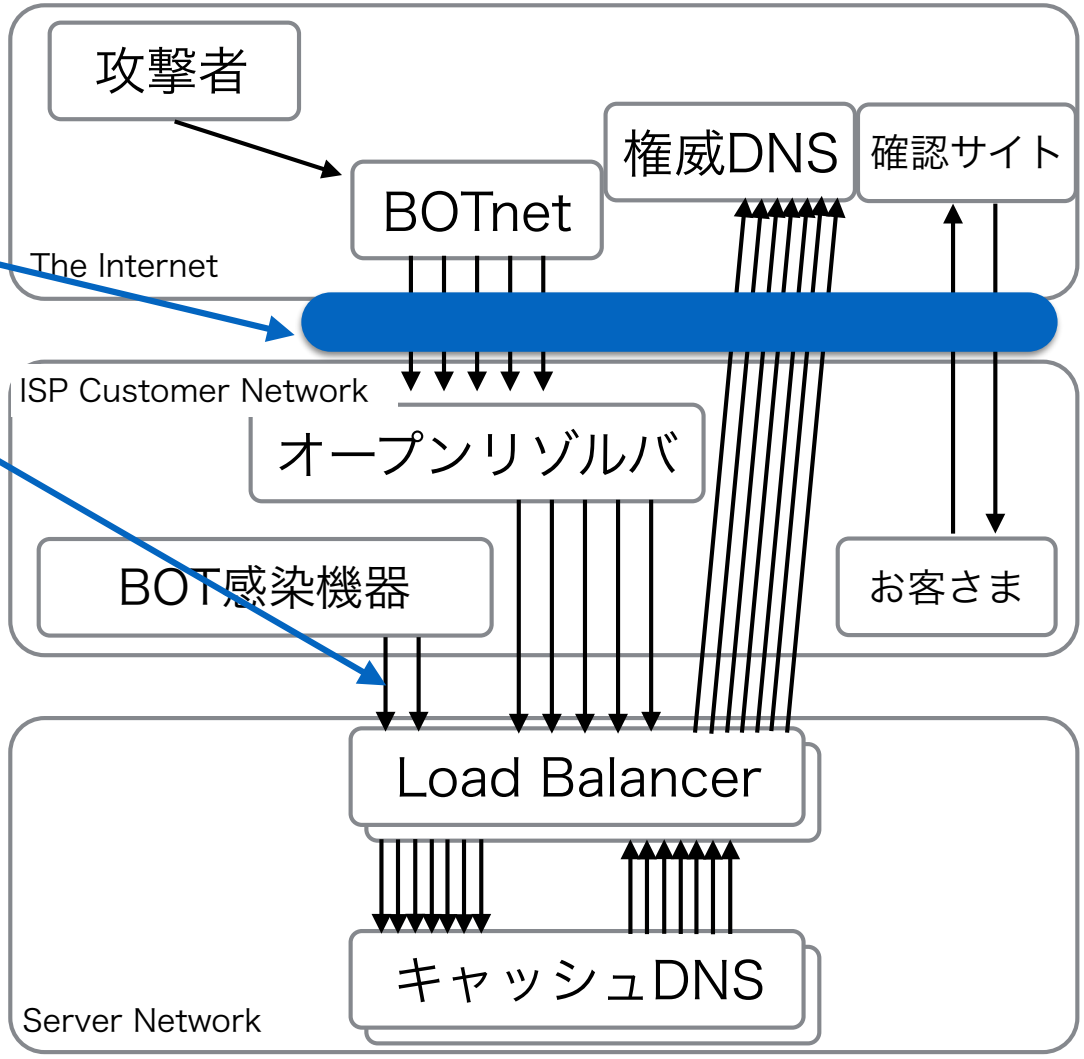
- ISP網内への流入するトラフィックの制御(IP53b)

- 効果と問題点

・キャッシュDNSに到達する水責めトラフィックのほとんどを抑制することが可能。

・ISPによっては網内のBOT感染機器に由来するトラフィックの方が多いケースも。この場合IP53bは効果が薄い。

・DNS以外の通信が存在？
(一部CAT端末？XBOX? 他には？)



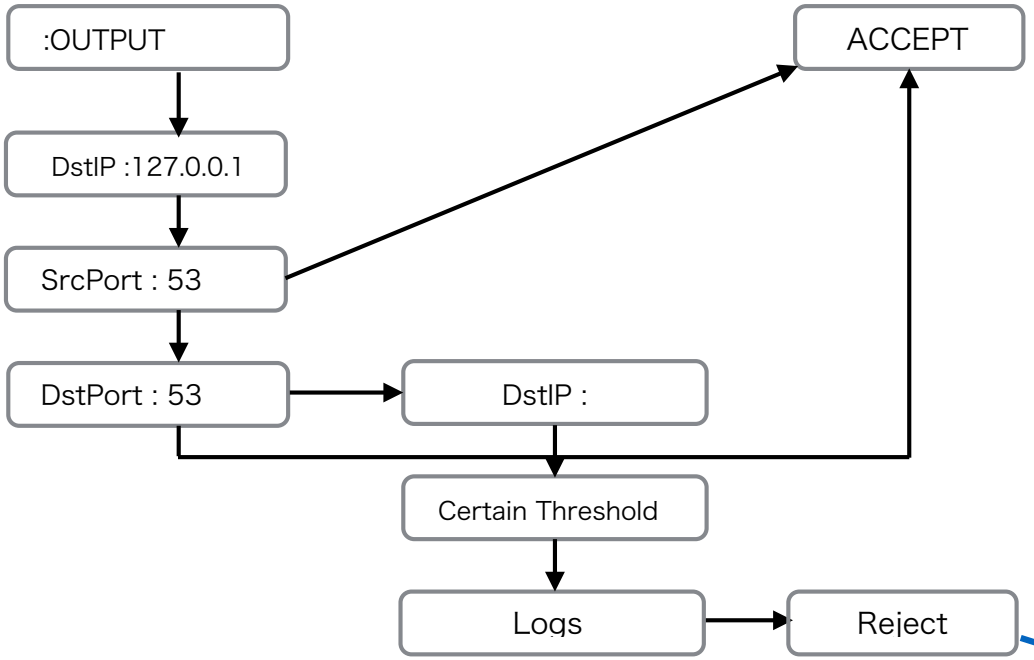
オープンリゾルバ確認サイト利用に配慮した手当も必要

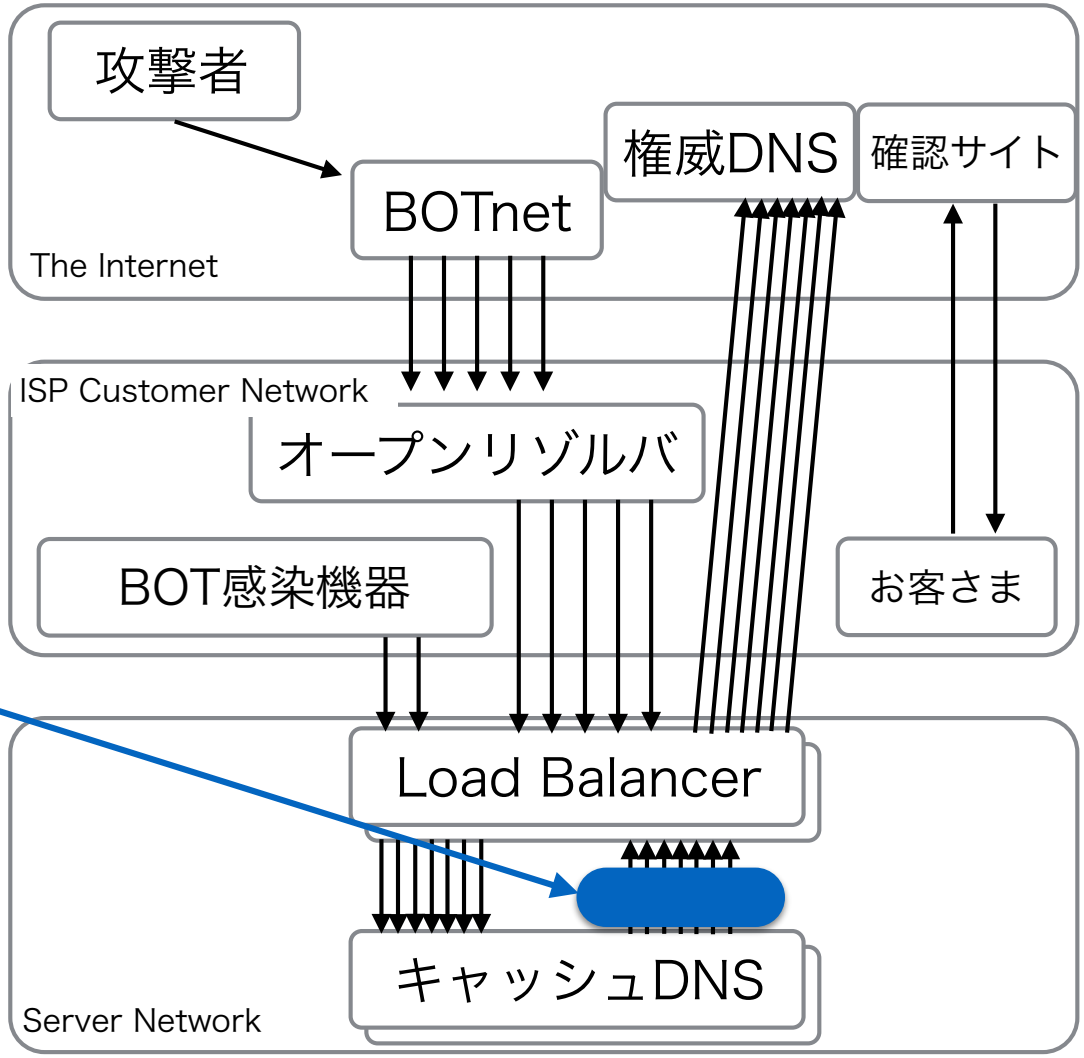
劇的な効果が期待できるが、正常な通信を遮断しないよう考慮が必要

DNS水責め攻撃の対策

- iptables hashlimit

iptables hashlimitフロー





- 特徴(メリットとデメリット)
  - 動作が軽い(外にでるパケットのみ)
  - 自動で制御が可能
  - 完全なDoSとはならない
  - 定常的にユニークなクエリを送出するドメインは考慮が必要
  - 閾値の調整が難しく、NSが多くなるとかなり厳しい

DNS水責め攻撃の対策

・BINDによる攻撃影響の軽減

※ 昨年の話

「BIND 9に対策機能はあります。」

※ただし、サブスクリプション版のBIND 9限定です..

BIND 9.X以降に実装されるらしい
9.9Xへの実装は確認中(一時期公式blogに掲載された)

本発表はBIND 9.9.6-EXP-1を基に作成しています。

DNS水責め攻撃の対策

- BINDによる攻撃影響の軽減
  最新の9.9.9-P1(ESV), 9.10.4-P1は対応済！
  ※つい最近までsubscription版でないと対応していませんでした。

デフォルトではこれらオプションは無効なので注意！
./configure --enable-fetchlimit

- fetches-per-server
  - ・権威DNSのIPアドレス単位で状態を判定
  - ・判定結果を基に正常な権威DNSへ問い合わせる
  - ・定期的に状態を判定する。状態が正常となると問い合わせる。

- fetches-per-zone
  - ・ドメイン毎の問い合わせ数を制限

どちらのオプションも

権威DNSへの通信を制御することで、キャッシュDNSのリソース枯渇を軽減することが可能

まとめ

・DNS水責め攻撃の概要を説明

- 2014年初頭から2016年にかけて攻撃は継続
  ※ただし、2016/5/25より約1ヶ月間攻撃が停止
- タイプの異なる水責め攻撃について説明しました。
  高レート型, 高ヒット率型

・DNS水責め攻撃の対策を説明

- iptables hashlimitは効果的であるが、閾値調整が難しい。
- IP53bは劇的な効果が見込めるが、網内要因のクエリーには効果がない。

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