資料更新：2016/12/1

見抜く力を！データを見て対策を考える(フルリゾルバ)

2016年12月1日
Internet Week 2016 DNS DAY

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
  - SOC移転しました！　福岡空港そば？です。(2015年9月1日)
    http://www.qtnet.co.jp/massmedia/2015/20150901.html
  - 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
  - [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
  - [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

どのような局面においても名前解決を継続的に提供し続けたい！

はじめに

- データを見て対策を考える(フルリゾルバ)
  - 水責め攻撃を例にデータを見てフルリゾルバでの対策を取り上げます。
  - 今回、権威側は対象外としています。

- 目次
  - 水責め攻撃とは
    - 攻撃の概要
  - データを見る
    - データから見る水責め攻撃
  - 対策を考える
  - まとめ

水責め攻撃とは

水責め(Water Torture)攻撃とは？

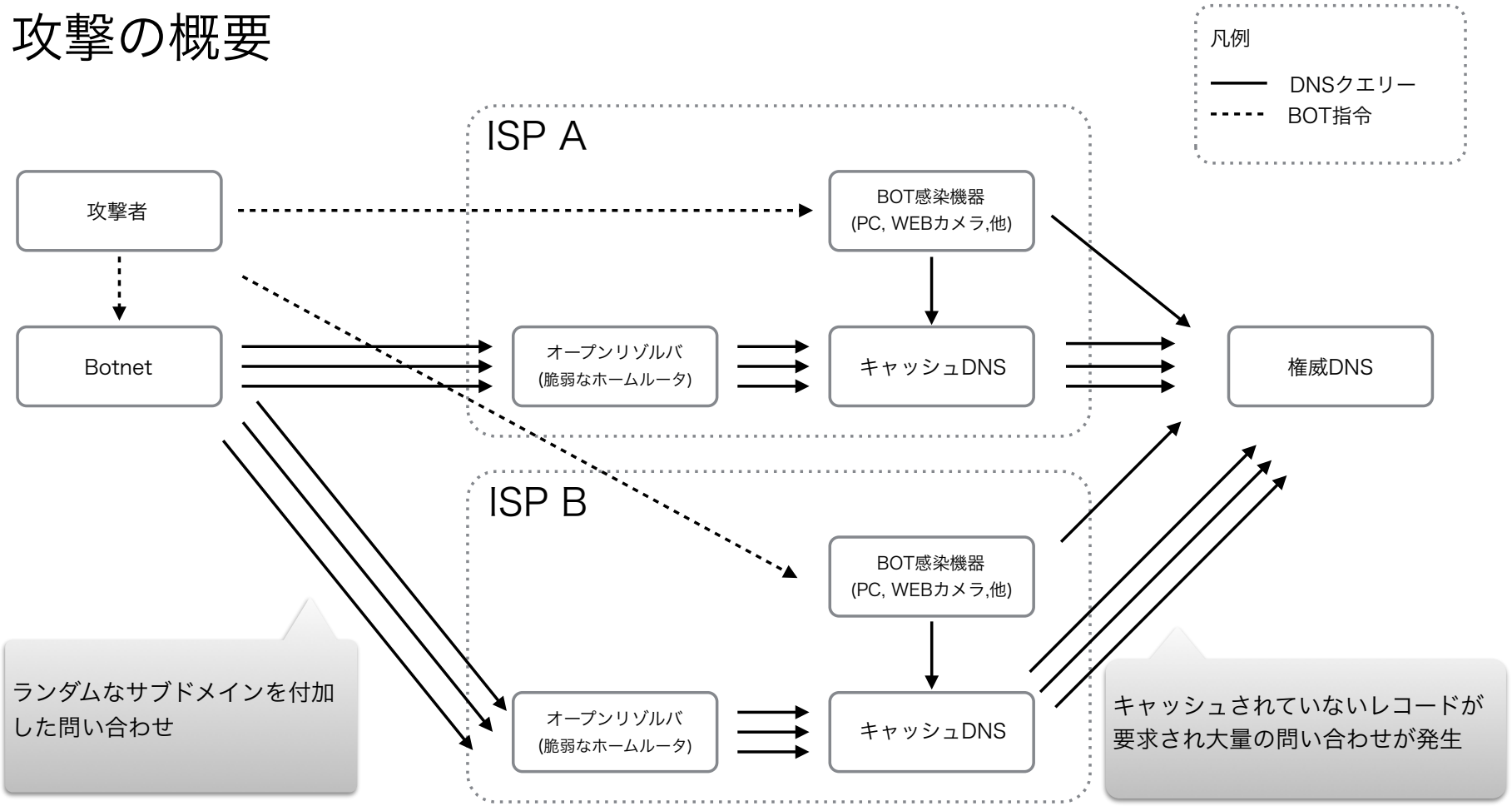
- 攻撃について
  - ・DNSに対するDDoS攻撃の手法の一つ
  - ・2014年初頭より、世界的に観測され始めた。
  - ・真の攻撃対象は権威DNS
    - キャッシュDNSも間接的に大きな影響を受ける。
  - ・日本でも影響が観測された。
    - [2014] 6月から7月に日本の多くのISPでも水責めが観測された。
    - [2015] JPドメイン名を標的とした“DNS水責め攻撃”を確認

インターネット定点観測レポート(2015年 1～3月)
<https://www.jpcert.or.jp/tsubame/report/report201501-03.html>

  - ・2016年5月末より、攻撃停止
  - ・2016年9月末より、攻撃再開

水責め(Water Torture)攻撃とは？

- 攻撃の概要

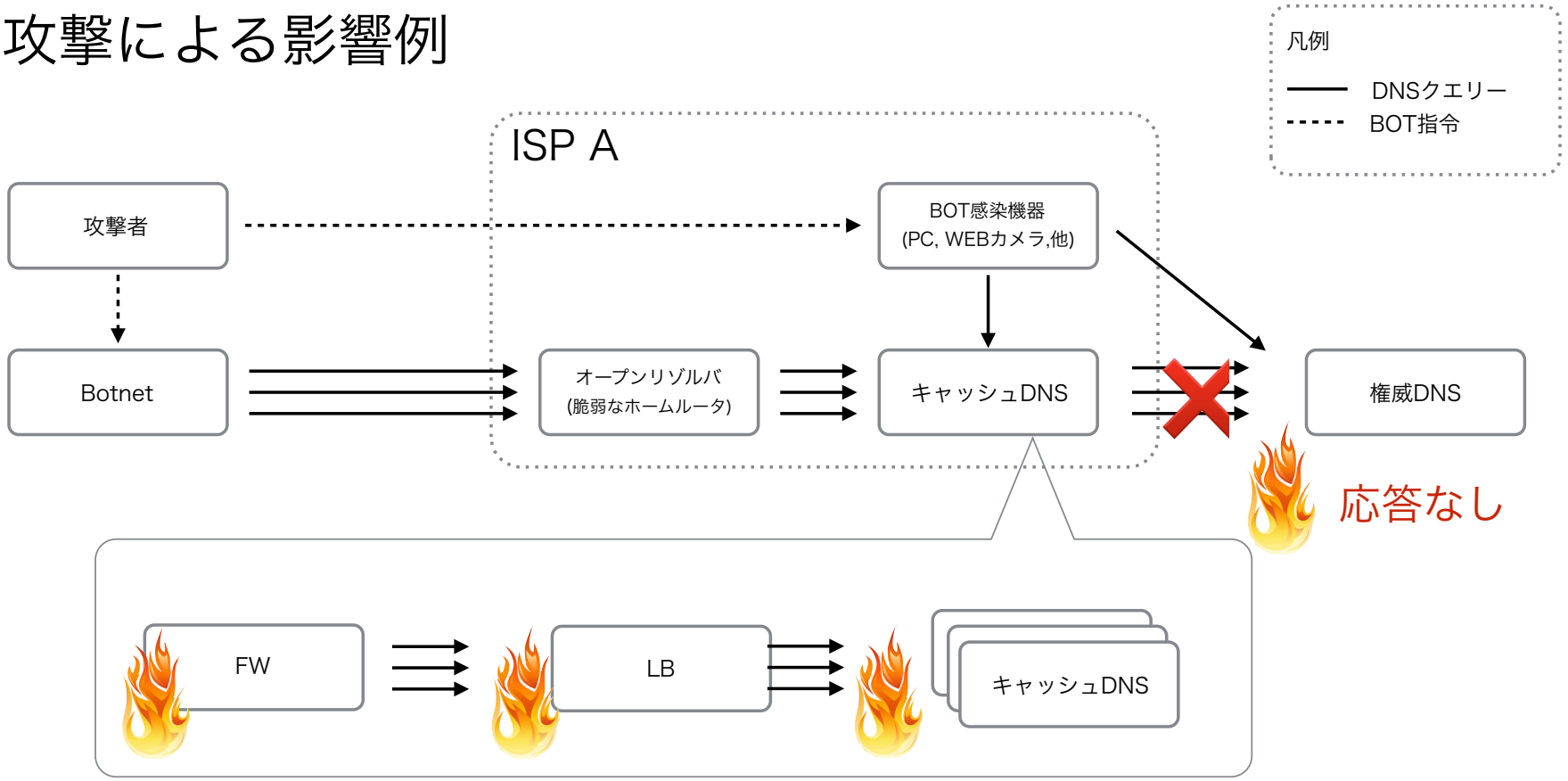


・権威DNSが真の攻撃対象、キャッシュDNSは巻き添え

・広く薄く、キャッシュDNSに突き刺さる。

水責め(Water Torture)攻撃とは？

- 攻撃による影響例

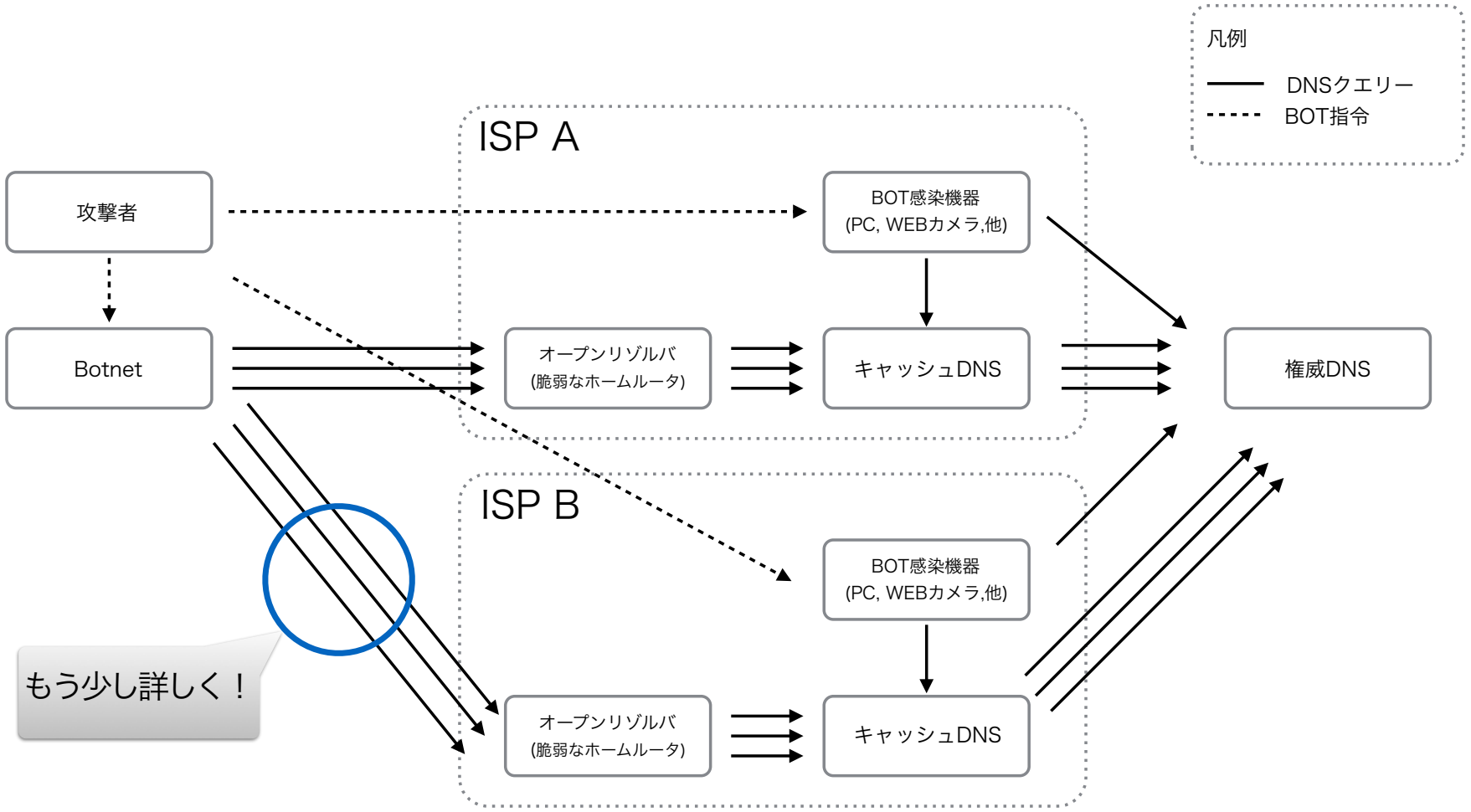


権威DNSが応答を返せないことにより

キャッシュDNSやFW, Load Balancerでリソース枯渇が発生

データを見る

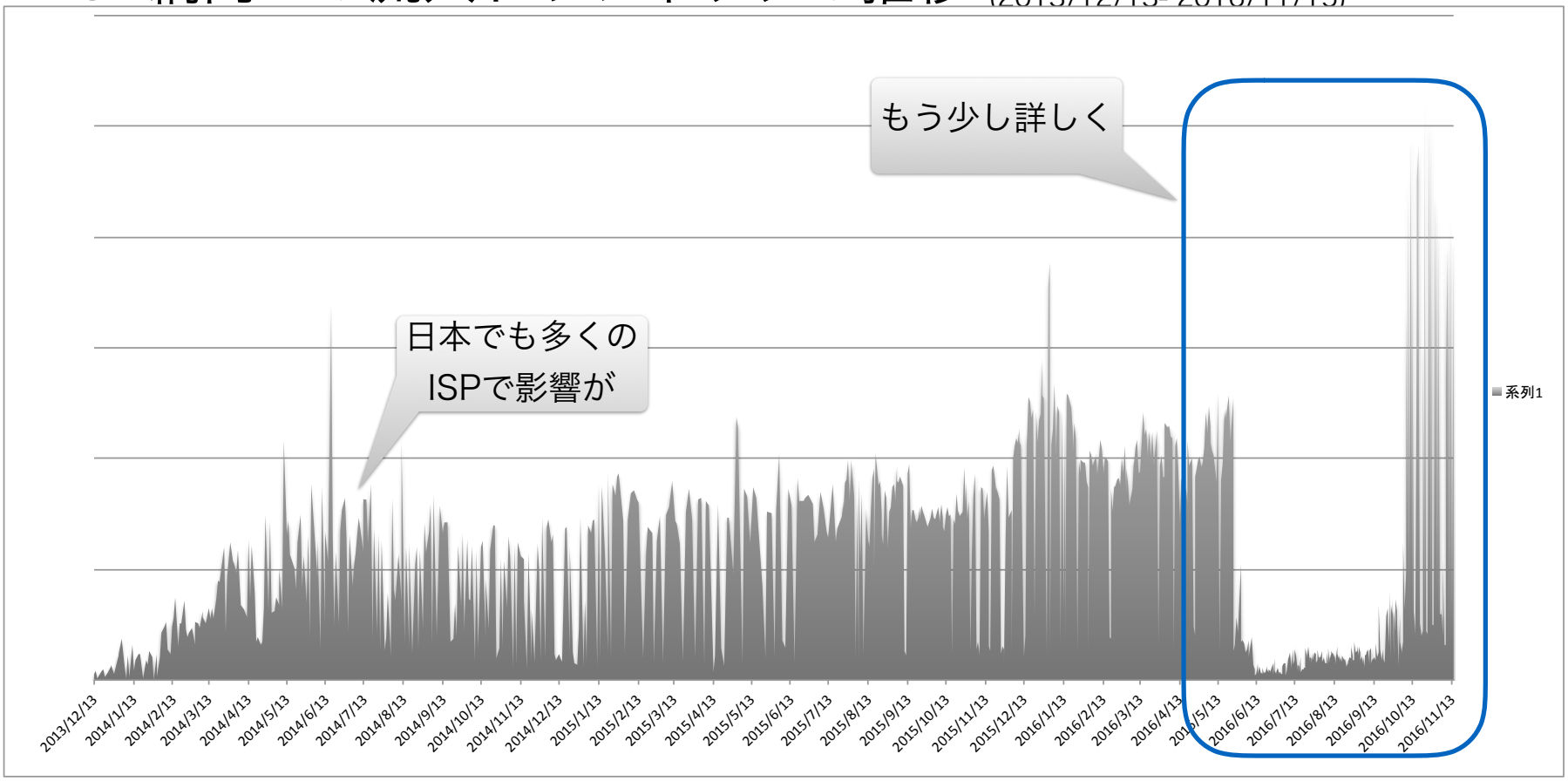
オープンリゾルバを狙うトラフィック



ISP網内のオープンリゾルバを狙うトラフィックについて見ていきます

オープンリゾルバを狙うトラフィック

- ISP網内への流入トラフィックの推移 (2013/12/13- 2016/11/15)



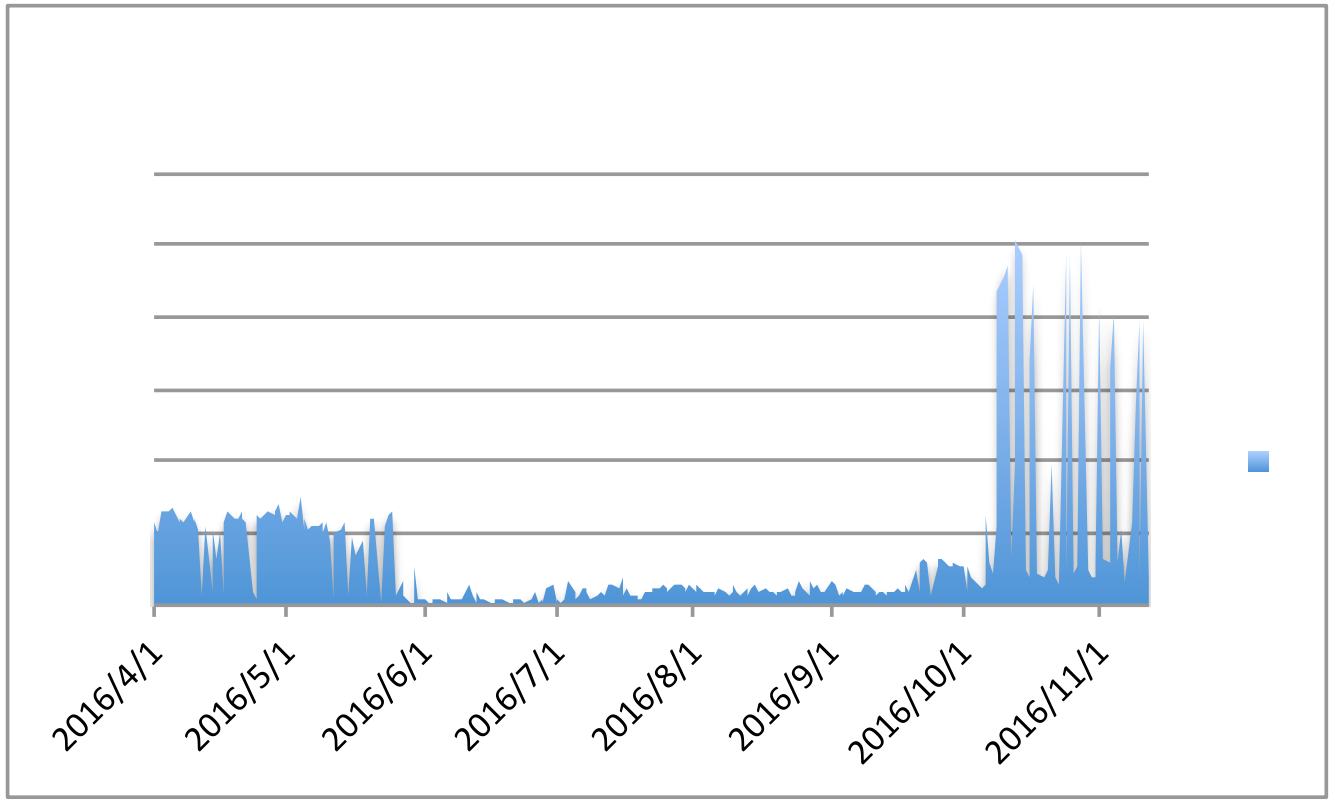
Traffic of 53 port destination from Internet to QTNet (2013/12/13- 2016/11/15)

オープンリゾルバを狙うトラフィックは・・

2014年初頭から顕著化、2016年現在も攻撃が継続している。

オープンリゾルバを狙うトラフィック

- ISP網内への流入トラフィックの推移 (2016/04/01- 2016/11/12)



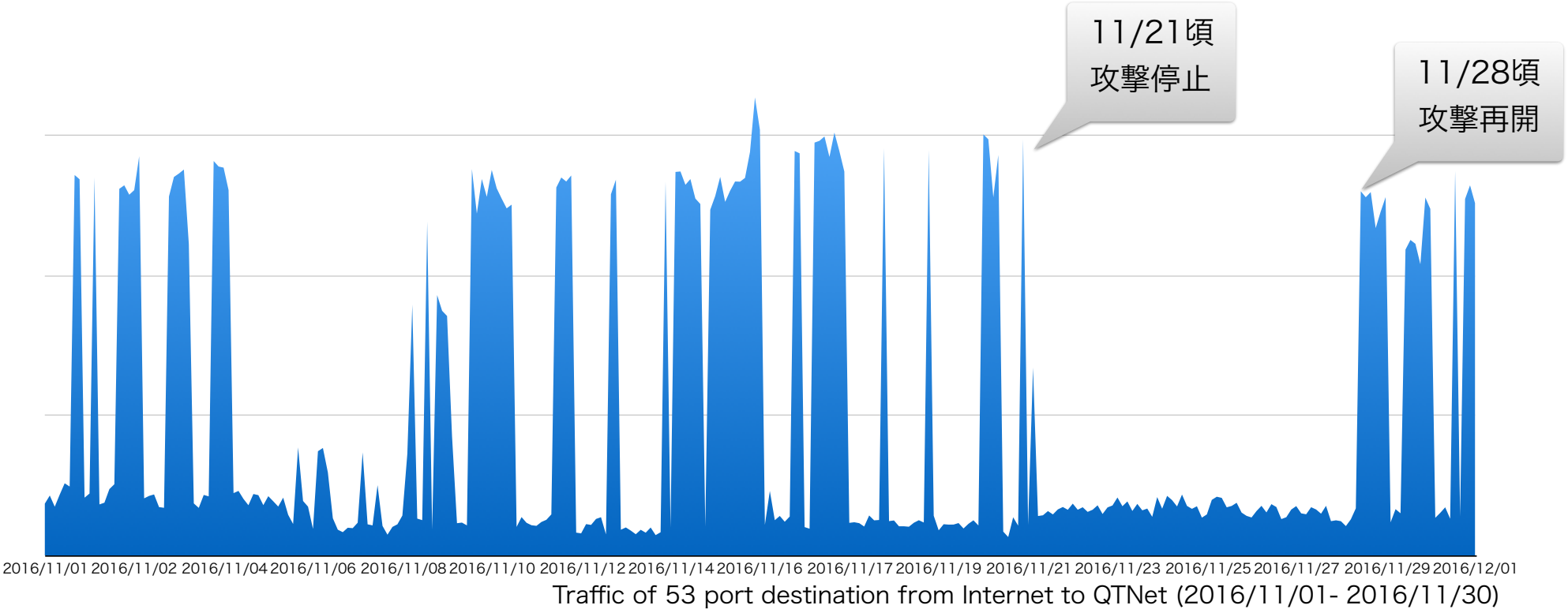
Traffic of 53 port destination from Internet to QTNet (2016/04/01- 2016/11/12)

オープンリゾルバを狙うトラフィックは・・

・2016年5月末より攻撃停止していたが、9月末に攻撃再開
・以前の2倍程度のトラフィックが流入している

オープンリゾルバを狙うトラフィック

- ISP網内への流入トラフィックの推移 (2016/11/01- 2016/11/30)



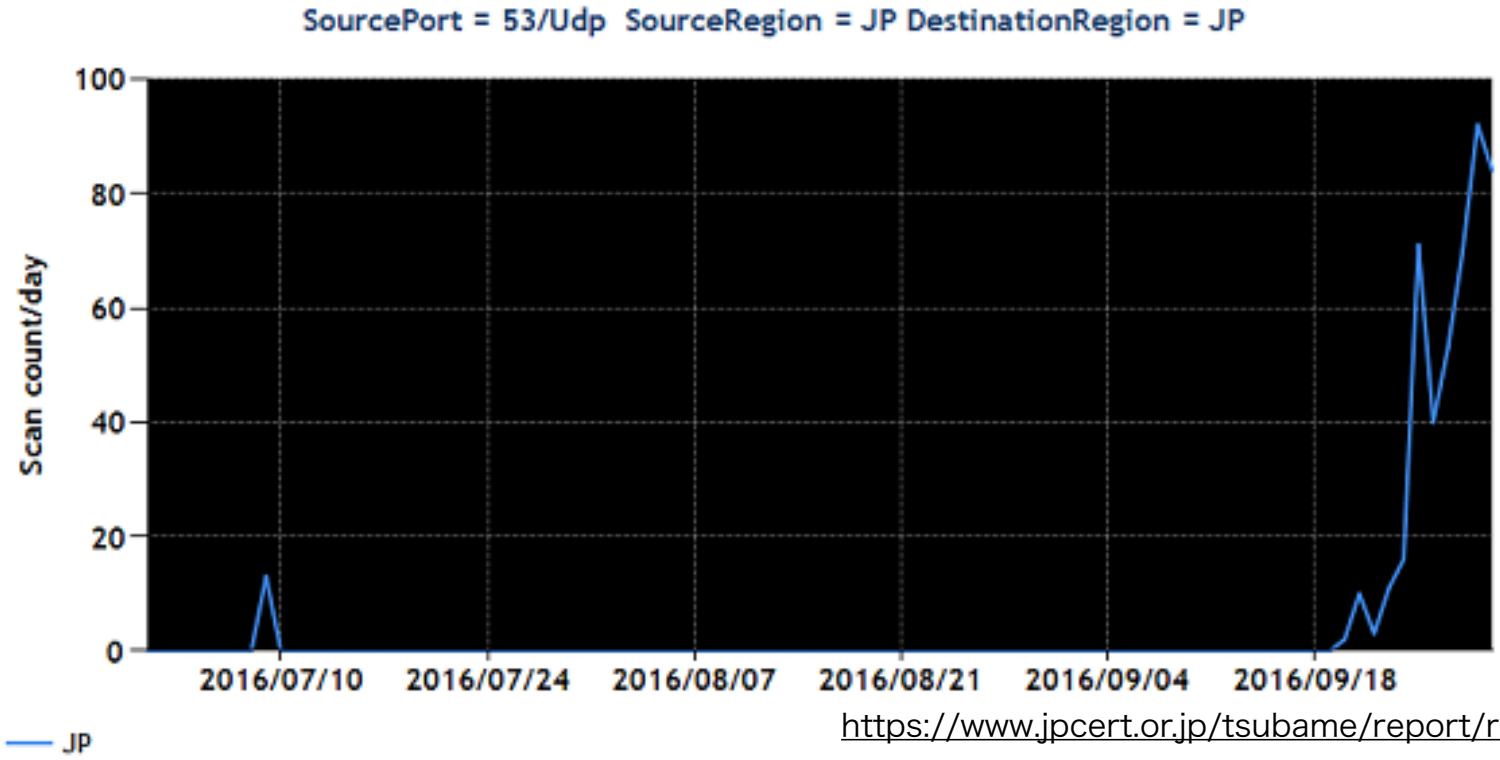
Traffic of 53 port destination from Internet to QTNet (2016/11/01- 2016/11/30)

オープンリゾルバを狙うトラフィックは・・

・2016年11月は一時的に攻撃が停止していた時期があった
・2016年5末と比較流入トラフィックは多く注意が必要

国内のオープンリゾルバ等を使ったDNS水責め攻撃の再開

- JPCERT/CCインターネット定点観測レポート(2016年 7～9月)より引用



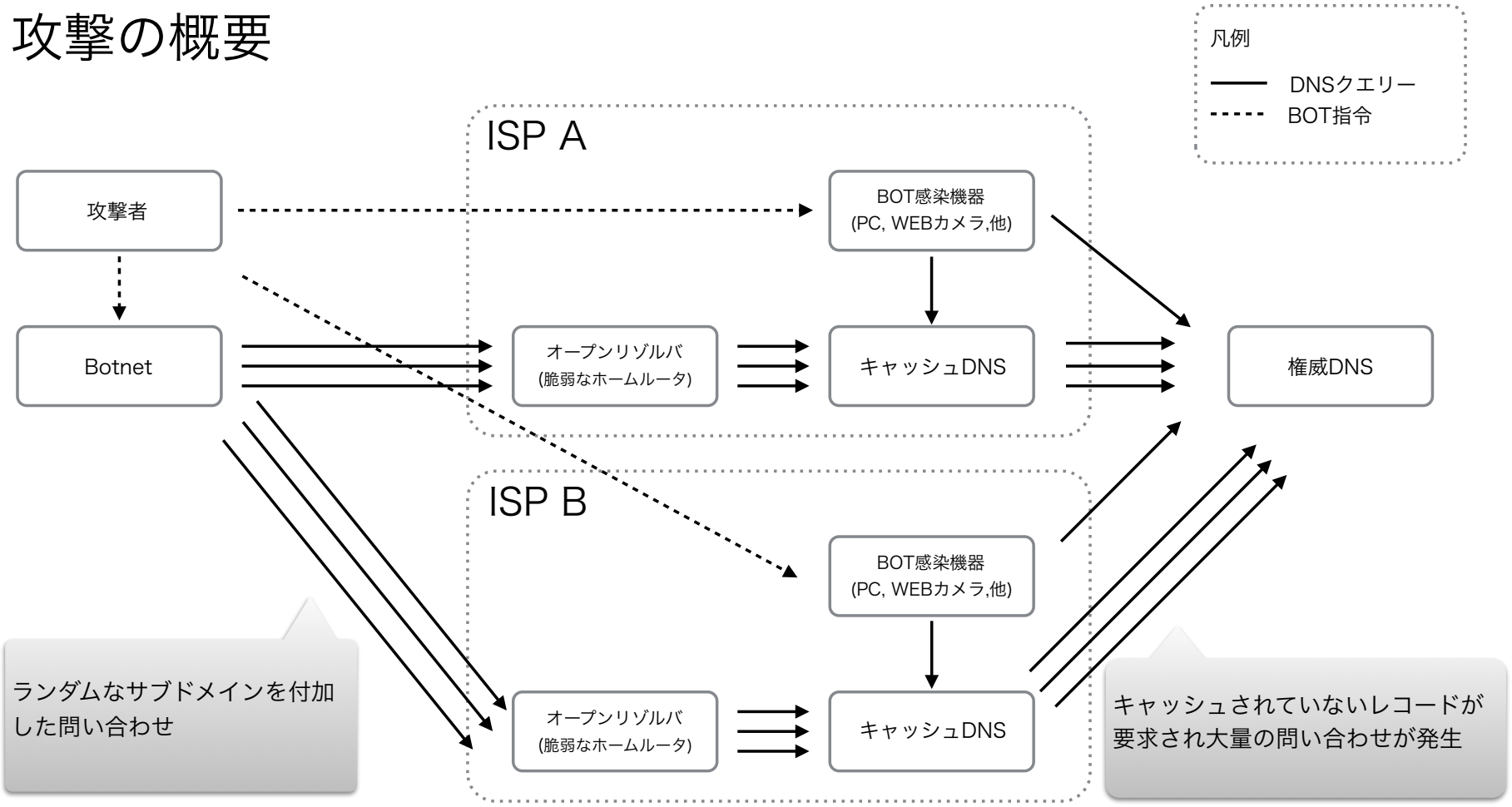
https://www.jpcert.or.jp/tsubame/report/report201607-09.html

弊社だけではなく、

大規模な水責め攻撃が再開されていることを示唆している。

水責め(Water Torture)攻撃とは？

- 攻撃の概要



・権威DNSが真の攻撃対象、キャッシュDNSは巻き添え

・広く薄く、キャッシュDNSに突き刺さる。

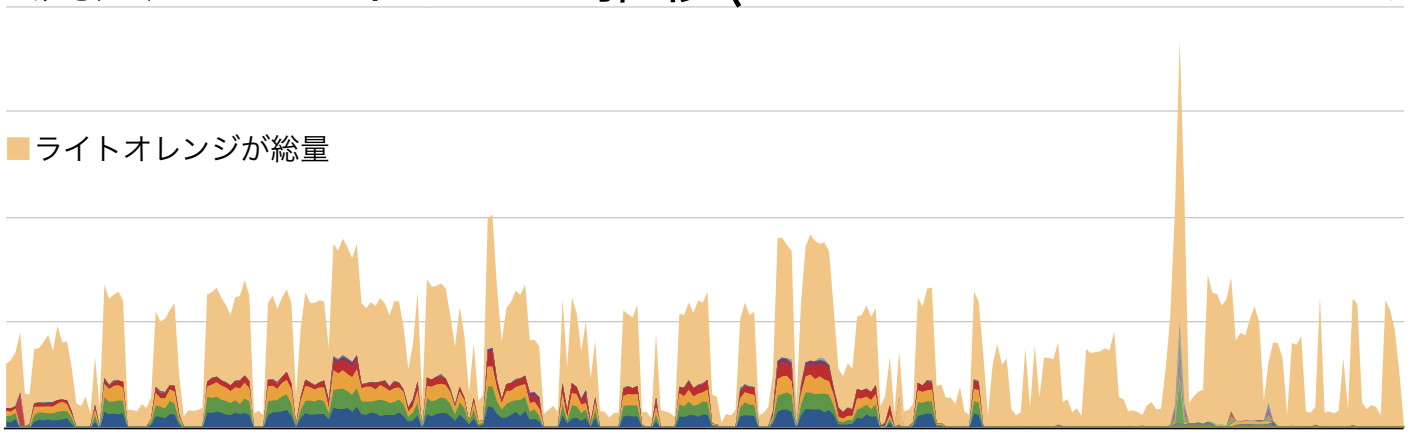
もう少し詳しく

オープンリゾルバを狙うトラフィック

- 「広く薄く、キャッシュDNSに突き刺さる」とは

  ・BotNetから広く薄く

- ISP網内への流入トラフィックの推移(Source IP アドレスでグルーピング)



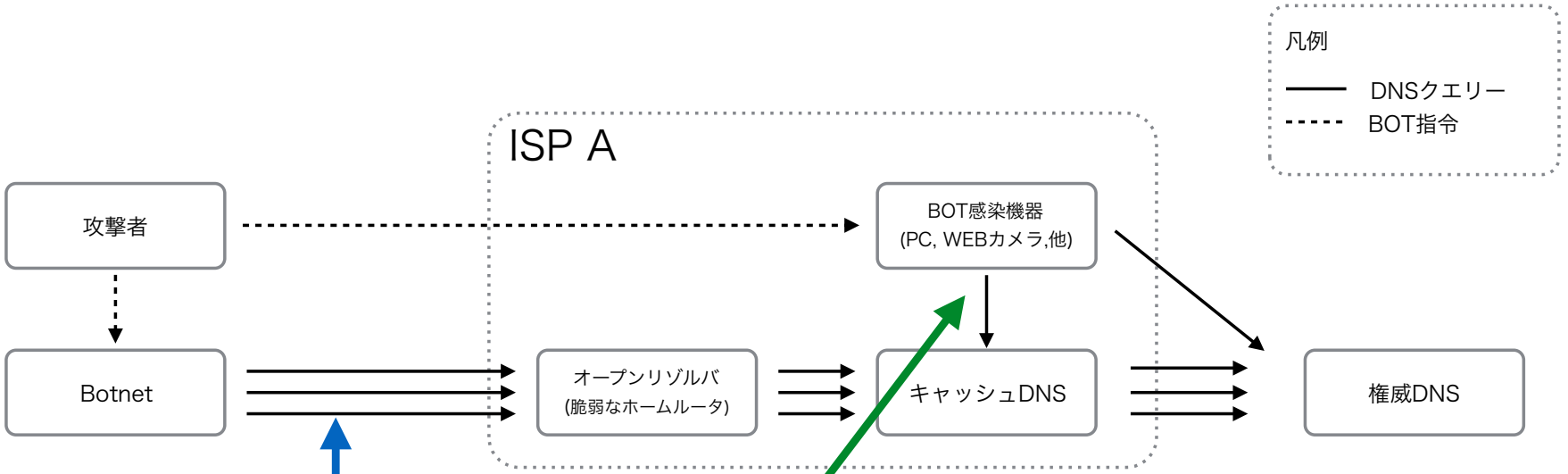
Traffic of 53 port destination from Internet to QTNet

オープンリゾルバを狙うトラフィックは・・

・最初期はSource IPアドレスに偏りがあり、規制が容易であった
・2014年6月～7月には、Source IPアドレスが分散し規制が困難に

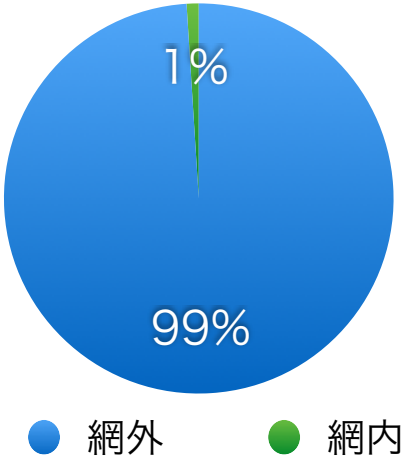
オープンリゾルバを狙うトラフィック

- 「キャッシュDNSに到達するトラフィックの発生源」とは



・ISP**網外**のBOTnetに由来

・ISP**網内**のBOT感染機器に由来



ISP網外からのトラフィックが約99%（ただし、ISPにより異なる）

水責めに関するデータより

- データより見えること
  - ・Source IPアドレスが分散し、規制が困難
  - ・水責めトラフィックの発生源は、網内・網外に存在する
  - ・一時期攻撃は停止していたが、現時点で攻撃は再開

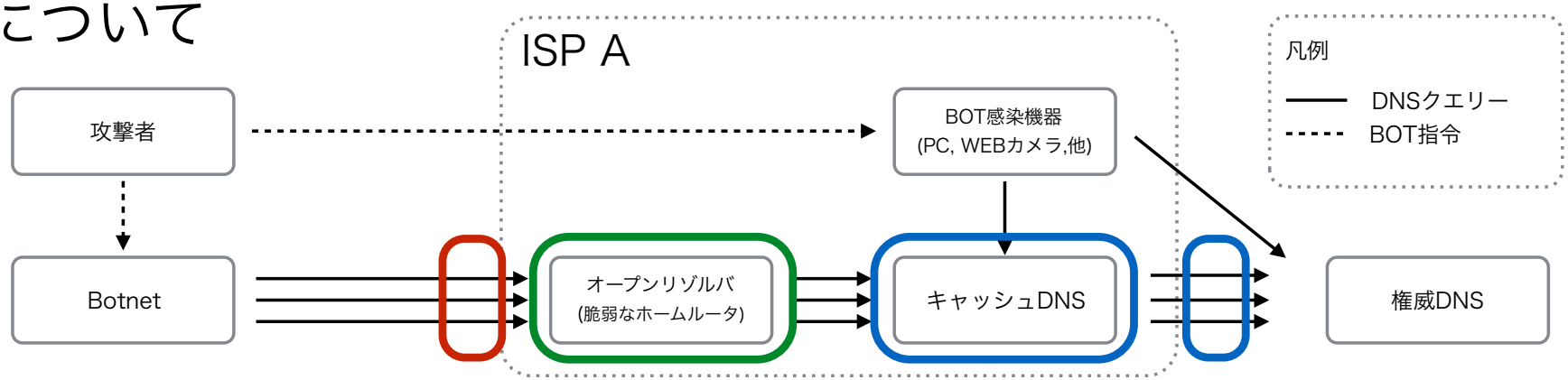
- どのように検知するか
  - ・iptablesなど用いて権威DNSのIPアドレス毎のPacket数を監視
  - ・rndc statusのrecursive clientsを閾値監視
  - ・request receivedとsuccessful answerの差分を閾値監視する
  - ・rndc recursingの出力結果より滞留している問い合わせを確認

キャッシュされていないレコードが要求され特定の権威DNSに大量の通信が発生することに着目

対策を考える

データを見て対策を考える

- 対策について



・IP53B
　網内のBOTに由来するランダムクエリーが多い場合は効果が薄い場合も

・オープンリゾルバの撲滅
　根本的な対策

・攻撃対象ドメインへの通信を**遮断**
　攻撃対象のドメインをキャッシュDNSにもたせる　**(DoSが成立)**

・攻撃対象ドメインへの通信を**制御**
　BIND: fetches-per-zone, fetches-per-server
　Unbound: ratelimit-for-domain, ratelimit
　hashlimit (iptabels)

データを見て対策を考える

- BINDでの対策について

攻撃対象ドメインへの通信を**制御**するオプションが使用可能

- fetches-per-server
- fetches-per-zone

Recursive Client Rate limiting in BIND 9.9.8 and 9.10.3
https://deepthought.isc.org/article/AA-01304/189/Recursive-Client-Rate-limiting-in-BIND-9.9.8-and-9.10.3.html

BIND 9.9 Administrator Reference Manual (ARM)
https://kb.isc.org/article/AA-00845/0/BIND-9.9-Administrator-Reference-Manual-ARM.html

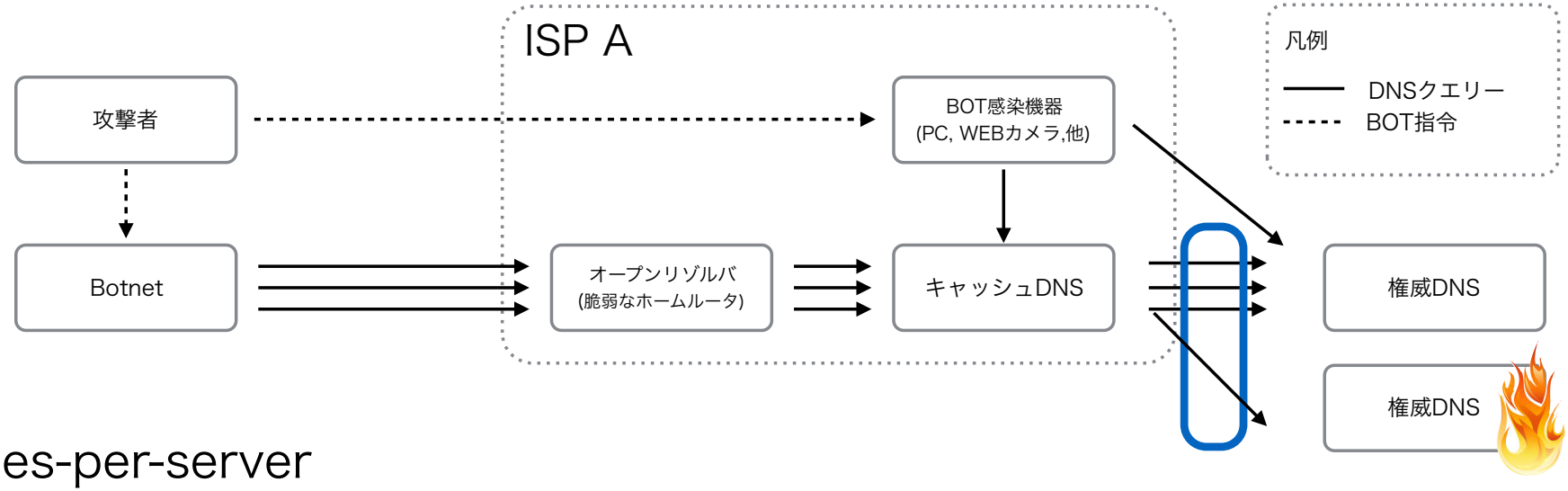
最新の9.9.9-P4, 9.10.4-P4, 9.11.0-P1では使用可能

- 9.9.9-P4, 9.10.4-P4 (デフォルトで無効)
  configure --enable-fetchlimitが**必要**
- 9.11.0-P1 (デフォルトで有効)
  configure --enable-fetchlimitが**不要**

機能の詳細についてはARMやKBを参照ください

データを見て対策を考える

- BINDでの対策について



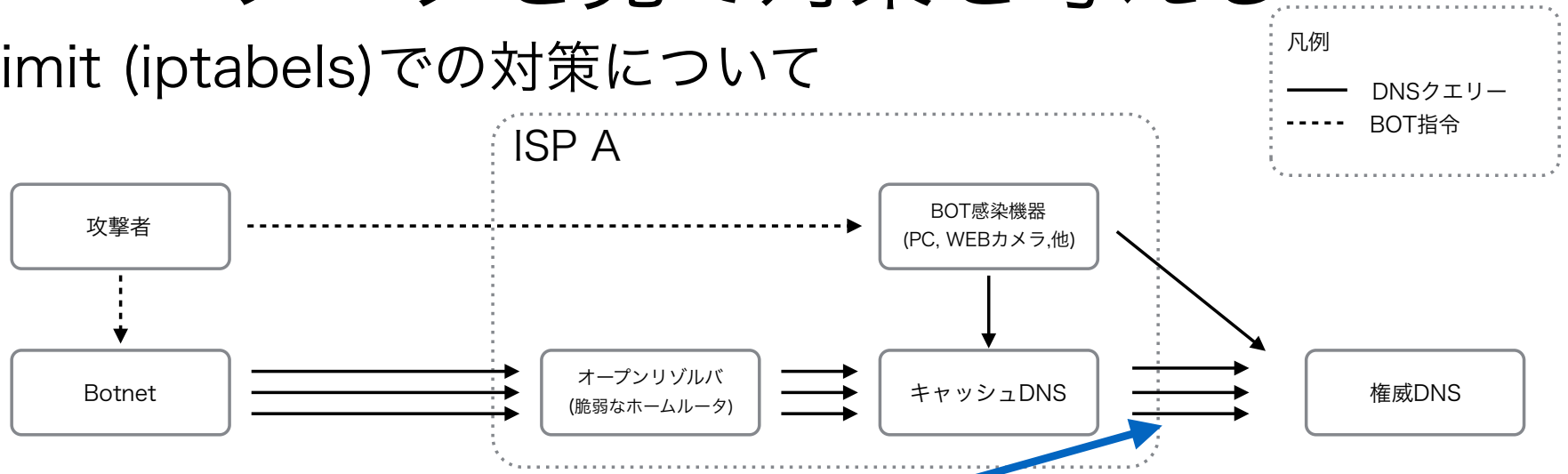
-fetches-per-server

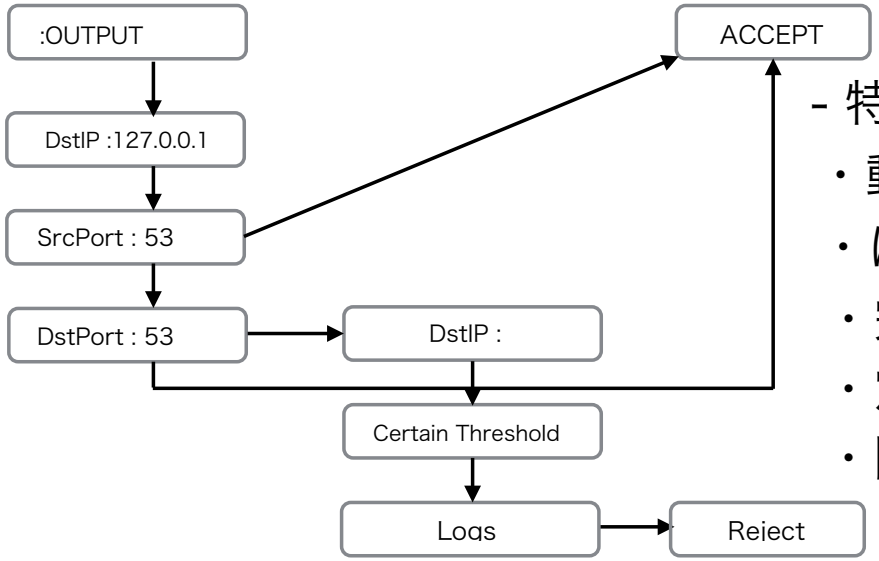
・権威DNSのIPアドレス単位で状態を判定
・判定結果を基に正常な権威DNSへ問い合わせる
・定期的に状態を判定する。状態が正常となると問い合わせる。

権威DNSとのタイムアウト率に応じて、キャッシュDNSから権威DNSへのクエリーを動的に制御
応答のない、権威DNSへのリクエストを抑制

データを見て対策を考える

- hashlimit (iptabels)での対策について





- 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)
  - ・ほぼ自動で制御が可能
  - ・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

まとめ

- 水責め攻撃とは
  - ・攻撃の概要と影響について説明
- データを見る (データから見る水責め攻撃)

  オープンリゾルバを狙うトラフィクの推移と特徴について説明
  - ・2016年5月末より、攻撃停止
  - ・2016年9月末より、攻撃再開　5月の攻撃停止時期よりも攻撃が**激化**

  ISP網外からのトラフィックに起因するものが大半

  通常時からよくデータを観察し、異常に気がつく
- 対策を考える

  「データを見る」で得られた知見を元に様々な対策について説明

全ての攻撃に効果のある万能策は現状なし、複数の対策を検討する必要性がある

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