更新予定あり
資料更新：2017/11/30

フルリゾルバに対する攻撃と対策

2017年11月30日
Internet Week 2017 DNS DAY

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10年くらい。
- 株式会社QTnet （旧 九州通信ネットワーク株式会社）
  - 新社名のお知らせ
    http://www.qtnet.co.jp/massmedia/2017/20170614.html
  - QTmobile (QTモバイル)
    http://www.qtmobile.jp
  - 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
  - APRICOT 2017 TLD Anycast DNS servers to ISPs (JPRS, QTnet)
    https://2017.apricot.net/program/schedule/#/day/9/network-operations-2
  - JPRSおよび電力系通信事業者8社が共同研究の成果を公開
    http://www.qtnet.co.jp/massmedia/2017/20171031_1.html
    https://tldlabs.jprs/acts/s001/

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

- フルリゾルバに対する攻撃と対策
  - フルリゾルバに対する攻撃と対策を取り上げます。
  - パフォーマンスチューニング、権威DNSは対象外としています。
- 目次
  - フルリゾルバに対するDoS,DDoS攻撃について
    - 最近発生した攻撃を題材に
    - 水責め攻撃
  - まとめ

フルリゾルバに対する攻撃について

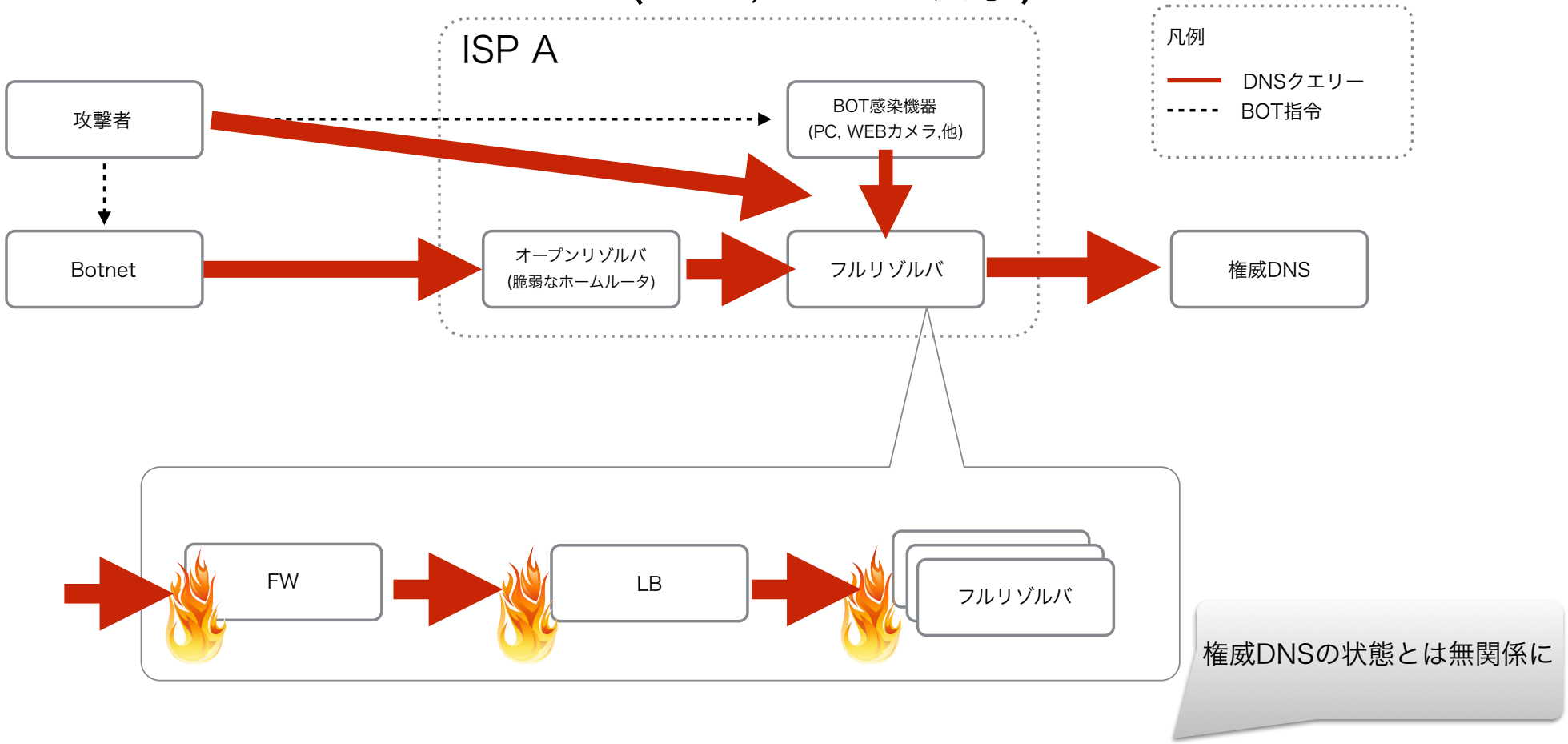
- 量による攻撃
  - ・大量のトラフィックを送りつける(DoS, DDoS攻撃)
    -> 11月に発生した攻撃を例に
  - ・水責め攻撃　(フルリゾルバそのものが攻撃対象ではなく、まきぞえ)
    -> 弊社の対策を例に

今回はこちらを対象にお話しします。

- その他の攻撃
  - ・DNSキャッシュポイズニング攻撃
  - ・DNSアプリケーションの脆弱性に対する攻撃

フルリゾルバに対する攻撃について

- 大量のトラフィックを送りつける(DoS, DDoS攻撃)



散発的に発生することが多く、フルリゾルバが直接影響を受ける

フルリゾルバに対する攻撃について

- どのように検知するか
  - 死活監視、サービスレスポンス監視
    - ping応答、DNS応答 (TTLの短いRRに対して)

      ※キャッシュされている結果からは、フルリゾルバと権威DNSの間の問題に気がつかない場合がある
  - リソース監視
    - OS(CPU使用率、メモリ使用率、NWトラフィック、UDP in/out比率)
  - 統計情報
    - DNSアプリケーション

	増減時に推測される影響
IPv4 request received	増加：大量のトラフィック 減少：上位 NW機器不具合
successful answer	request receivedとsuccessful answerに大きな乖離があれば、権威DNSとの疎通性に問題
NXDOMAIN	増加：キャッシュポイズニング攻撃、DoS攻撃
SERVERFAIL/other query failures	増加：キャッシュDNSから権威DNSへの疎通性に問題、その他攻撃

  - ログ監視
    - OS、DNSアプリケーション

異常な傾向を検知することによって、攻撃検知につながる

DoS, DDoS対策(11/19に発生した攻撃について)

- 攻撃の概要

この場限り

DoS, DDoS対策(11/19に発生した攻撃について)

- 攻撃の対策

この場限り

水責め(Water Torture)攻撃とは？

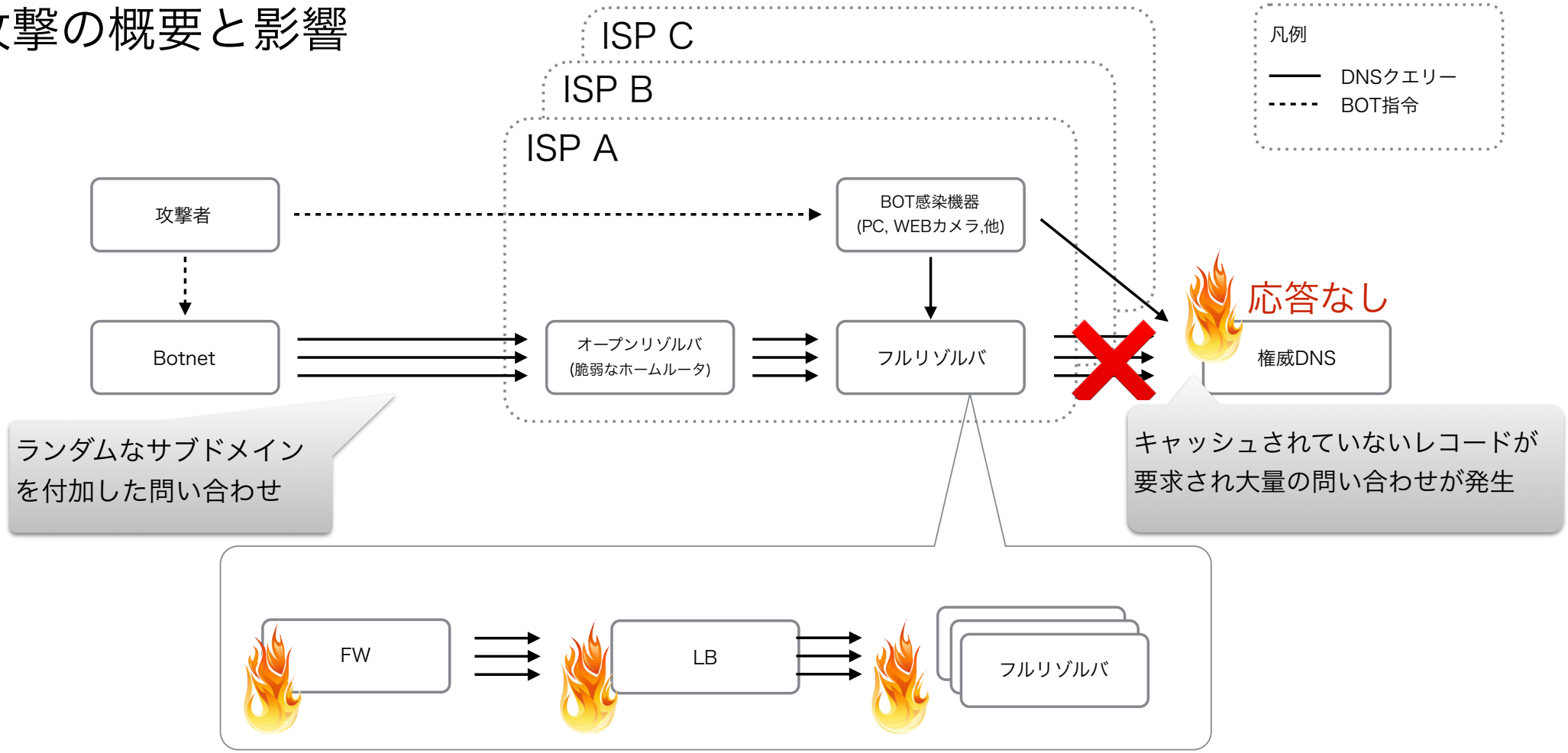
- 攻撃について
  - ・DNSに対するDDoS攻撃の手法の一つ
  - ・2014年初頭より、世界的に観測され始めた。
  - ・真の攻撃対象は権威DNS
    - フルリゾルバも間接的に大きな影響を受ける。
  - ・日本でも影響が観測された。
    - [2014] 6月から7月に日本の多くのISPでも水責めが観測された。
    - [2015] JPドメイン名を標的とした“DNS水責め攻撃”を確認

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] 2016年5月末から9月末まで、攻撃停止
    - [2017] 2017年後半は、水責め攻撃の発生頻度の低下

水責め(Water Torture)攻撃とは？

- 攻撃の概要と影響

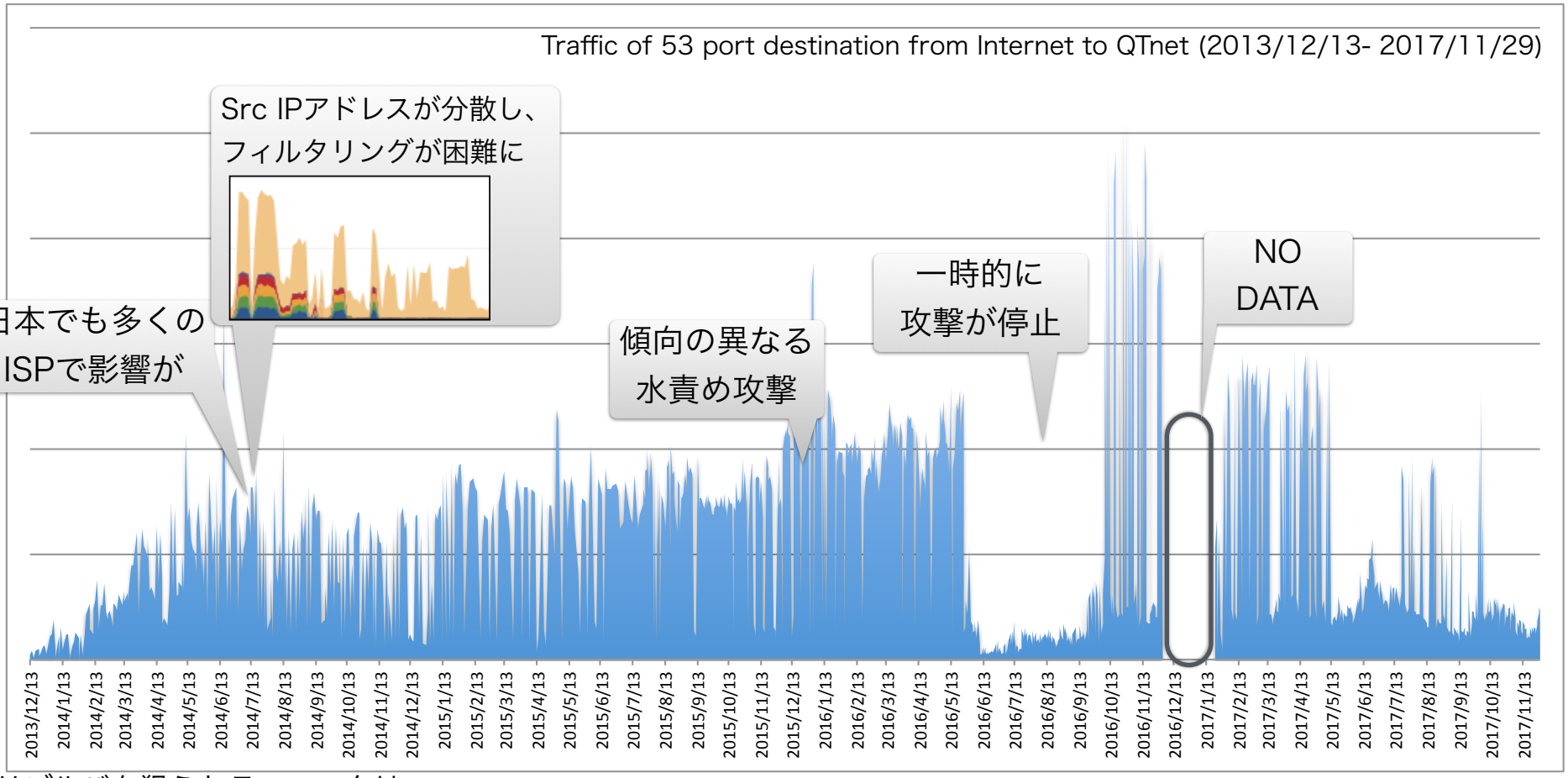


権威DNSが応答を返せないことにより

キャッシュDNSやFW, Load Balancerでリソース枯渇が発生

ISP網内の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



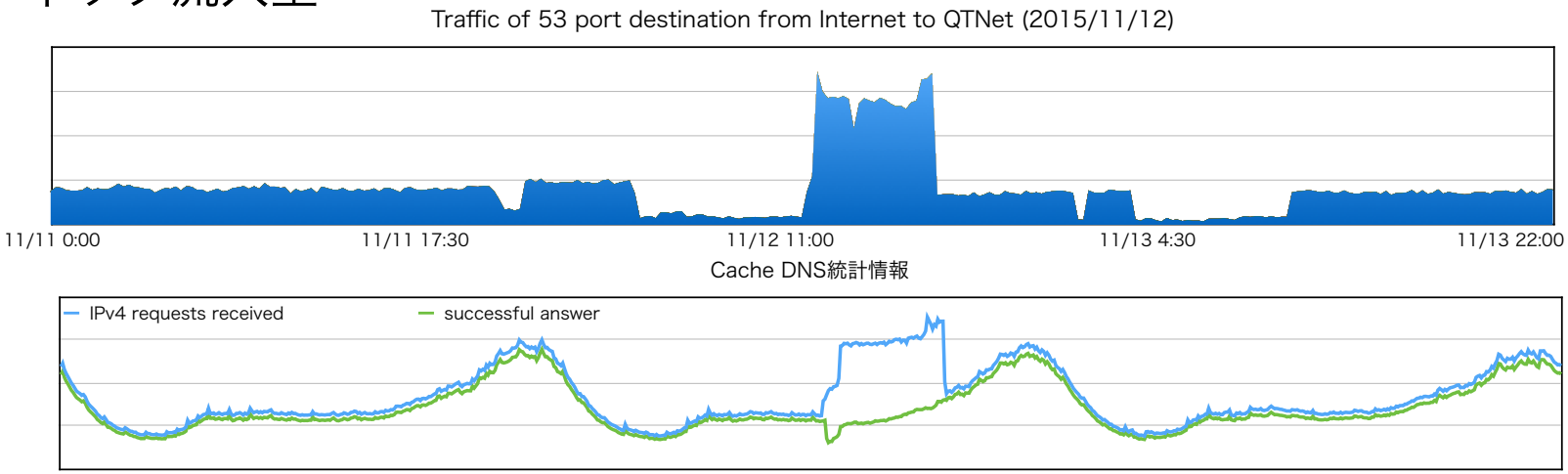
オープンリゾルバを狙うトラフィックは・・

・一時的に攻撃が停止(2016/5末～6末, 11末)

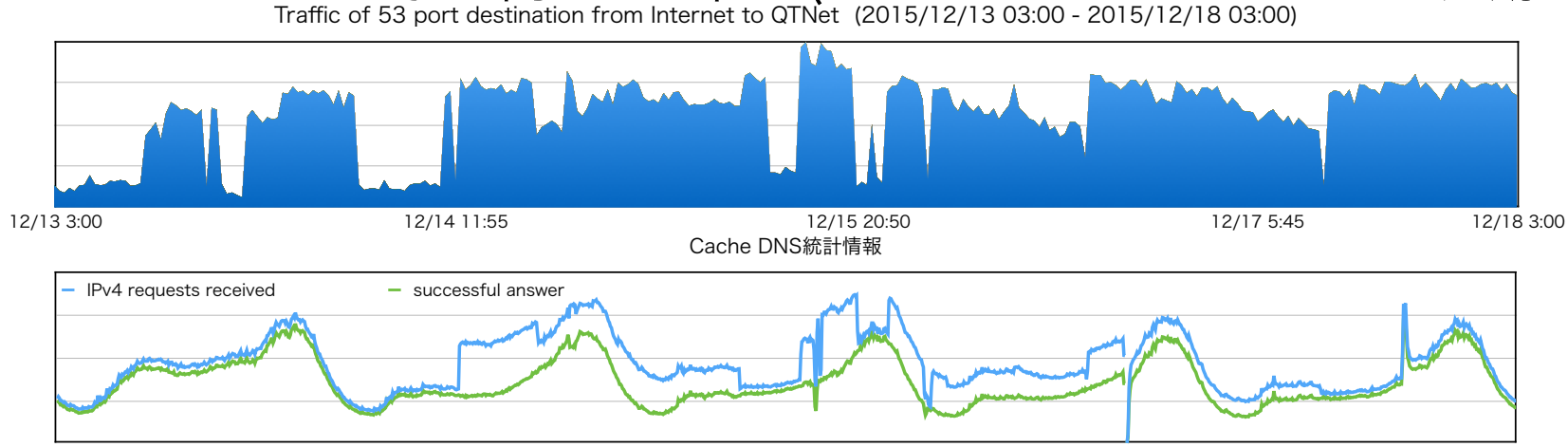
・2014年初頭から顕著化、2017年11月 現在も攻撃が継続している。

特徴的な水責め攻撃について

- 高トラフィック流入型

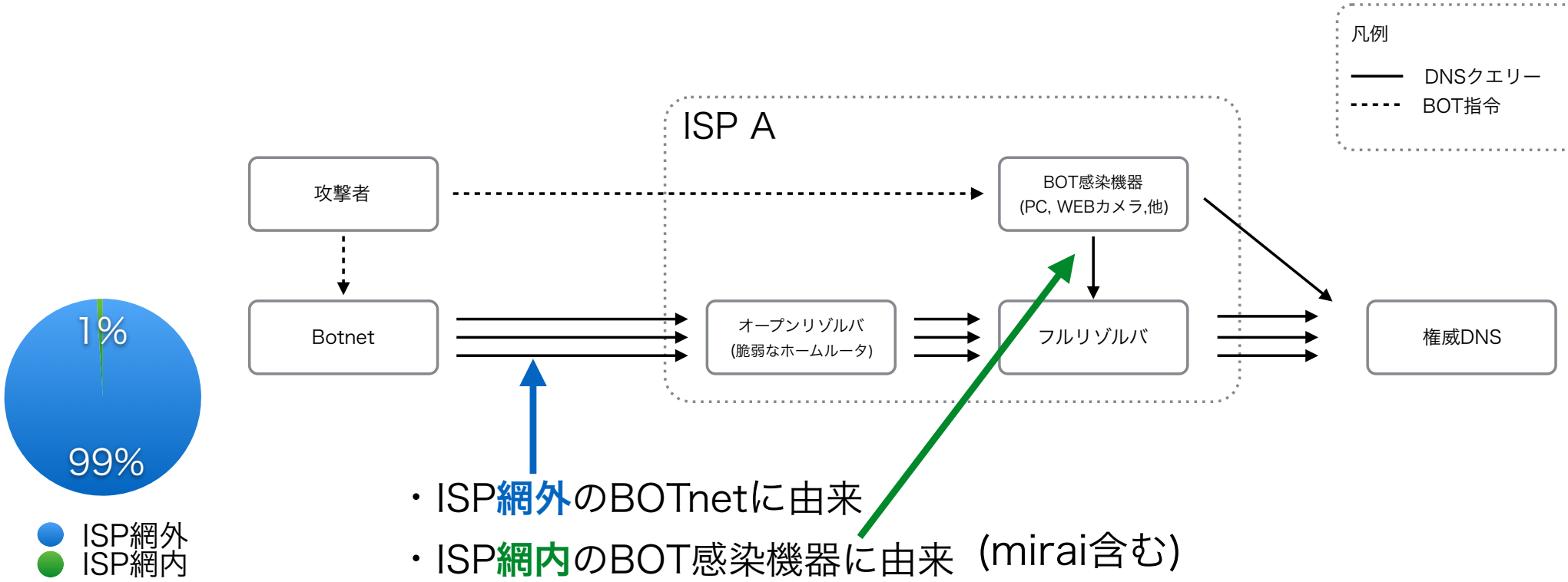


- 的確にオープンリゾルバを狙う高ヒット率型 (オープンリゾルバのリストの定期的な更新を示唆)



水責め攻撃は広く浅くが一般的であるが、傾向が異なる攻撃も観測

水責め攻撃のトラフィック発生源とは



最近わかってきたこと

・ISPによりオープンリゾルバの割合が大きく異なる
・ISPによりBOT感染機器の割合が大きく異なる

水責め攻撃に特化した攻撃の検知について

- どのように検知するか

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

・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

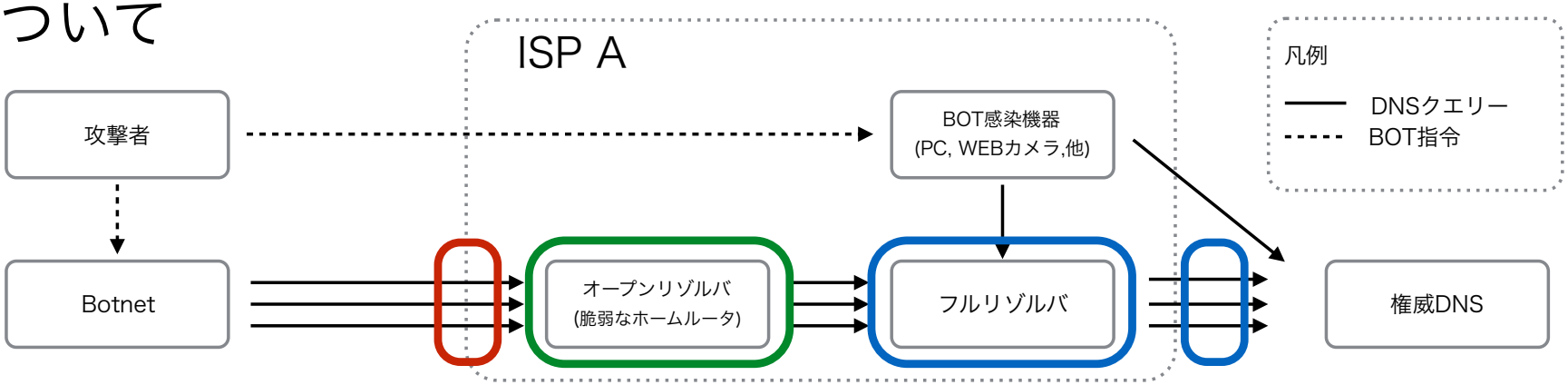
・rndc recursingの出力結果より滞留している問い合わせを確認

Netflowなどから

フルリゾルバだけでなく、ISP網内への流入トラフィックを観測することで異常傾向を把握

水責め攻撃の対策について

- 対策について

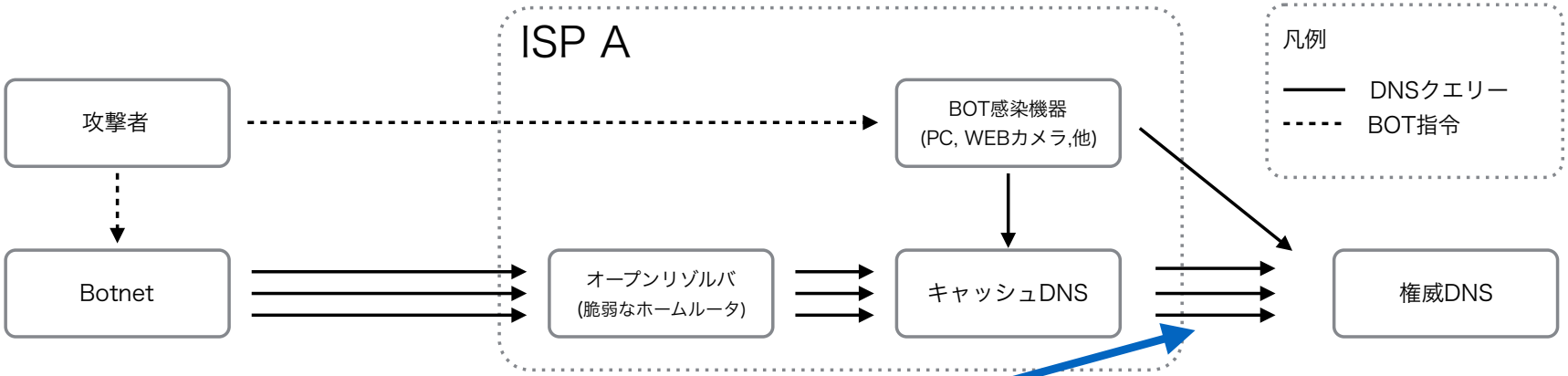


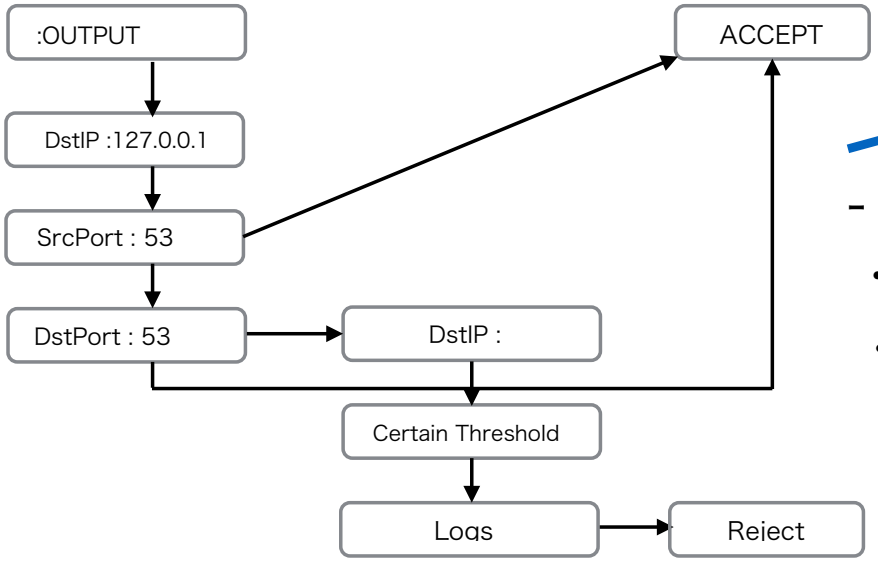
・IP53B (オープンリゾルバを狙うトラフィックをブロック)
　網内のBOTに由来するランダムクエリーが多い場合は**効果が薄い**場合も
・オープンリゾルバの撲滅（フルリゾルバへのトラフィック流入をブロック）
　根本的な対策であるが、非常に困難
・攻撃対象ドメインへの通信を**遮断**
　攻撃対象のドメインをキャッシュDNSにもたせる　**(※DoSが成立)**
・攻撃対象ドメインへの通信を**制御**
　BIND: fetches-per-zone, fetches-per-server
　Unbound: ratelimit-for-domain, ratelimit
　hashlimit (iptabels)
　Nominum Vantio CacheServe: Success-Based Rate-Limiting, Threat Avert
　XACK DNS: 現在スペシャルな機能を開発中！

水責め攻撃の対策について

- hashlimit (iptabels)での対策について

背景: BINDなどで対策機能が実装されておらず(有償版も含め)、自社開発！





- 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
  - ・完全な遮断とはならない
  - ・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

水責め攻撃の対策について

- 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 (最新の9.9系, 9.10系, 9.11系)

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

- 機能を有効にするには

  - 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**

named.conf 記述例 (fetches-per-server)

```
fetches-per-server 200 fail;
fetch-quota-params 100 0.1 0.3 0.7;
```

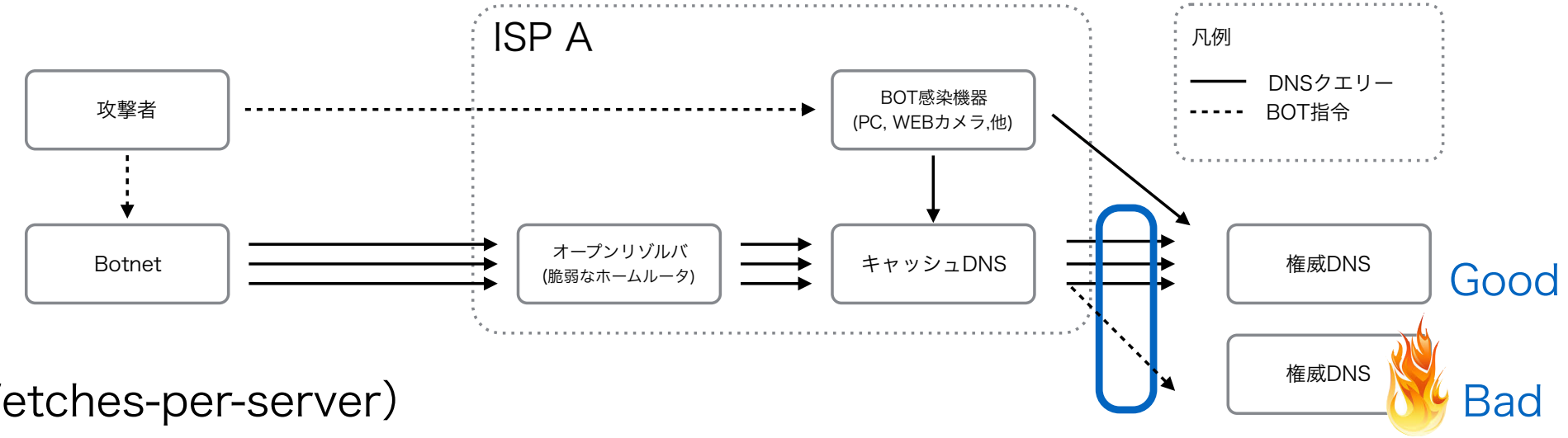
Recursive Client Rate limiting in BIND 9.9.8, 9.10.3 and 9.11.0
https://kb.isc.org/article/AA-01304/0

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

攻撃対象ドメインへの通信を完全に**遮断**せず、**制御**することが可能

水責め攻撃の対策について

- BINDでの対策について



- 特徴 (fetches-per-server)

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

・権威DNSのIPアドレス単位で状態(Good or Bad)を判定
・判定結果を基に状態の良い(Good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。

状態の悪い(Badな)権威DNSへのリクエストを抑制し、権威DNSとフルリゾルバの負荷を軽減

水責め攻撃の対策について

- Unboundでの対策について

- 特徴 (ratelimit ver1.5.4~)

・フルリゾルバから権威側への問い合わせをratelimit
・細かい設定が可能（ratelimitの結果、すべてSERVFAILとするか、確率的に通すかなど・・）
・権威DNSの状態から、ratelimitする機能ではない。

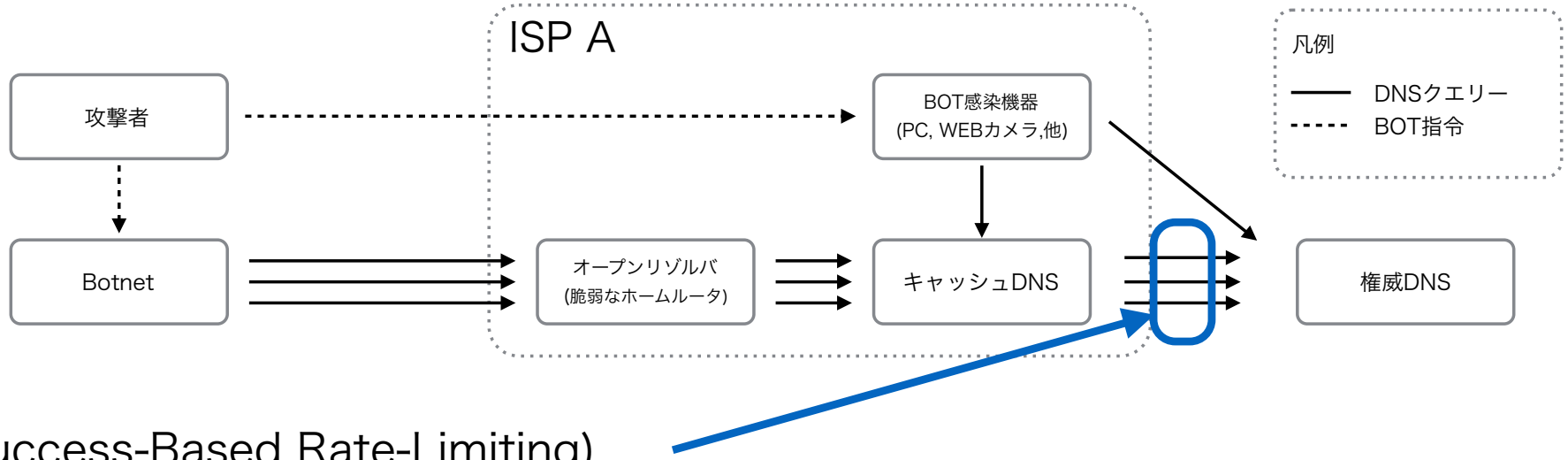
- Unbound+専用モジュール（Ahahi Netさん開発！）

・様々な統計情報(NXDOMAIN数、クエリー頻度、その他・・)から攻撃を検知
・攻撃の対象となっている特定のドメインだけをブロックすることが可能
・攻撃ではない、正常なクエリーは通常通り処理を行う。
・解析はリアルタイム！

- DNS Summer Days 2017
https://dnsops.jp/event/20170628/DNS_Summer_Days_2017_unbound_prsd.pdf

水責め攻撃の対策について

- Nominum Vantio CacheServeでの水責め対策の一つを紹介



- 特徴 (Success-Based Rate-Limiting)

・フルリゾルバから権威DNSへのDNS Queryを自動的rate limit

・権威DNSからの応答の状態をスコアリング
(権威DNSとドメインの組み合わせ毎に)

・スコアリングの結果から、水責めの影響が発生している
権威DNSとドメインの組み合わせに対してrate limit

スコアリングの結果から権威DNSへのリクエストを抑制し、権威DNSとフルリゾルバの負荷を軽減

まとめ

- フルリゾルバに対するDoS,DDoS攻撃について
  - 水責め攻撃の発生状況について
    - ・2017年後半は発生頻度が低下したものの水責め攻撃は継続
  - 攻撃の対策について説明　(11月に発生した事例, 水責め攻撃)
    - ・DoSが成立する遮断ではなく、制御することが重要
    - ・構築時から攻撃を想定し、構成を検討することが重要
    - ・権威DNSの障害時に影響を最小化する技術もでてきた。

通常時からよくデータを観察することで、攻撃の早期発見と攻撃特性から対策を！