資料更新：2017/06/28

BINDから他の実装へ
(フルリゾルバについてISPの視点から)

2017年6月28日
DNS Summer Day 2017

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9年ちょっとくらい。
- 九州通信ネットワーク(QTNet)
  - いわゆる電力系ISP　なんでもやっています！
  - 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
  - [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
  - [APRICOT 2017] TLD Anycast DNS servers to ISPs

    https://www.slideshare.net/apnic/tld-anycast-dns-servers-to-isps

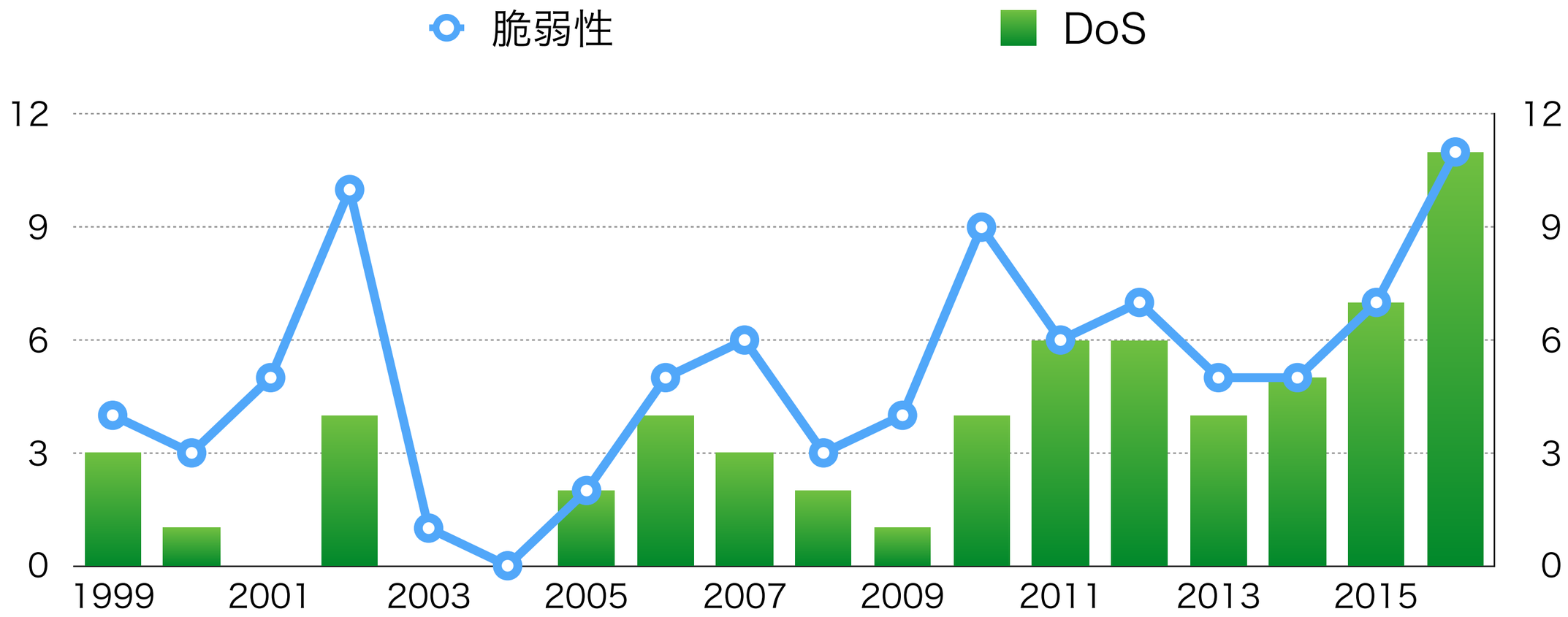
    https://2017.apricot.net/program/schedule/#/day/9/network-operations-2

本発表の内容

- BIND以外の実装を選択したい理由
  - ・BINDの脆弱性の多さ
  - ・BIND修正版パッケージリリースまでの時間
  - ・BINDの脆弱性の特性
- 解決したい課題
- 選択した実装について
  - ・各種攻撃対策について
  - ・パフォーマンスについて
- まとめ

BIND以外の実装を選択したい理由

- BINDの脆弱性の多さ



年々増加傾向の脆弱性、DoSは約7割、2017年もすでに7件

BIND以外の実装を選択したい理由

- BIND修正版パッケージリリースまでの時間

CVE ID	Vulnerability Type(s)	Publish Date	Score	rhel6	rhel7	CentOS7
CVE-2016-8864	DoS	2016-11-01	5	2016-11-02	2016-11-03	2016-11-25
CVE-2016-6170	DoS	2016-07-06	4	Will not fix	Will not fix	
CVE-2016-2848	DoS	2016-10-20	5	2016-10-20	Not affected	
CVE-2016-2776	DoS	2016-09-27	7.8	2016-09-28	2016-09-28	2016-09-28
CVE-2016-2775	DoS	2016-07-18	4.3	Will not fix	Will not fix	
CVE-2016-2088	DoS	2016-03-09	4.3	Not affected	Not affected	
CVE-2016-1286	DoS	2016-03-09	5	2016-03-16	2016-03-16	
CVE-2016-1285	DoS	2016-03-09	4.3	2016-03-16	2016-03-16	2016-03-16
CVE-2016-1284	DoS	2016-02-04	2.6	Not affected	Not affected	
CVE-2015-8705	DoS	2016-01-19	6.6	Not affected	Not affected	
CVE-2015-8704	DoS	2016-01-19	6.8	2016-01-27	2016-01-27	2016-01-27

脆弱性公表から半日程度で攻撃は発生する場合も！

脆弱性アナウンスから、修正パッケージリリースまでの時間差は致命的

BIND以外の実装を選択したい理由

- BINDの脆弱性の特性
  - ・Remode Code Execution(RCE)はない
  - ・新機能には新脆弱性、問題の修正で別の問題
  - ・ACLに関係なくプロセス停止
  - ・外部からPaket一発でプロセス停止
  - ・maliciousなドメインや権威DNSと通信するとプロセス停止
  - ・Workaroundがないものが多い

フルリゾルバの停止 = 参照するサービスの停止

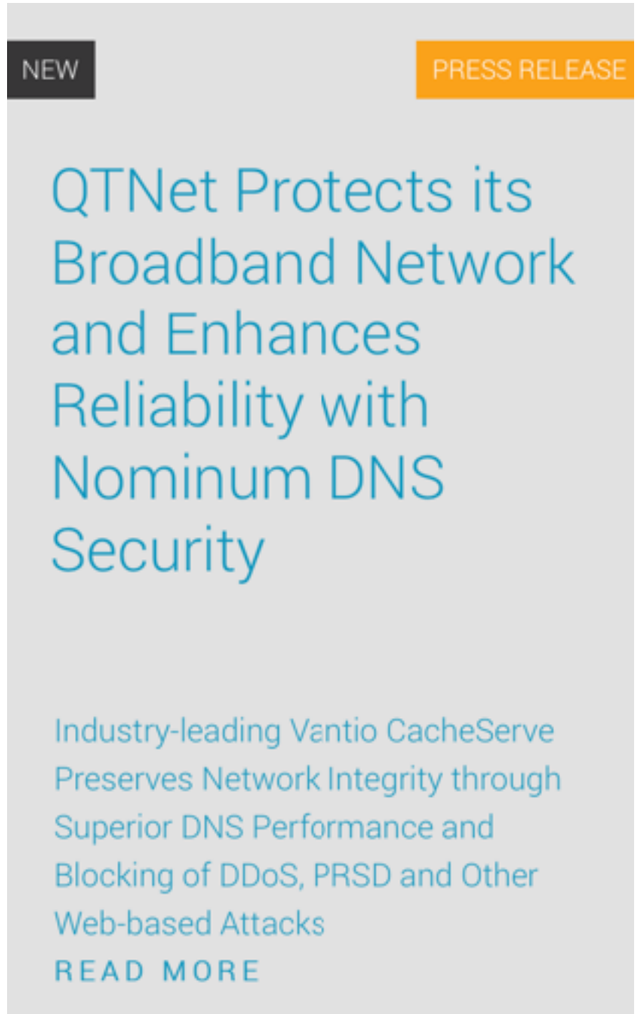
RCEはないが、サービス継続性に影響のある脆弱性が多い

- 実装に多様性を！

無償・有償を含め様々な製品やサービスがでてきた

BINDから他の実装へ

- 解決したい課題や必要な機能
  - フルリゾルバに対する攻撃への対策など
    - ・脆弱性対応
    - ・水責め
    - ・DoS攻撃
  - その他
    - ・DNSSEC
    - ・EDNS Client Subnet
    - ・ログ検索
    - ・パフォーマンス

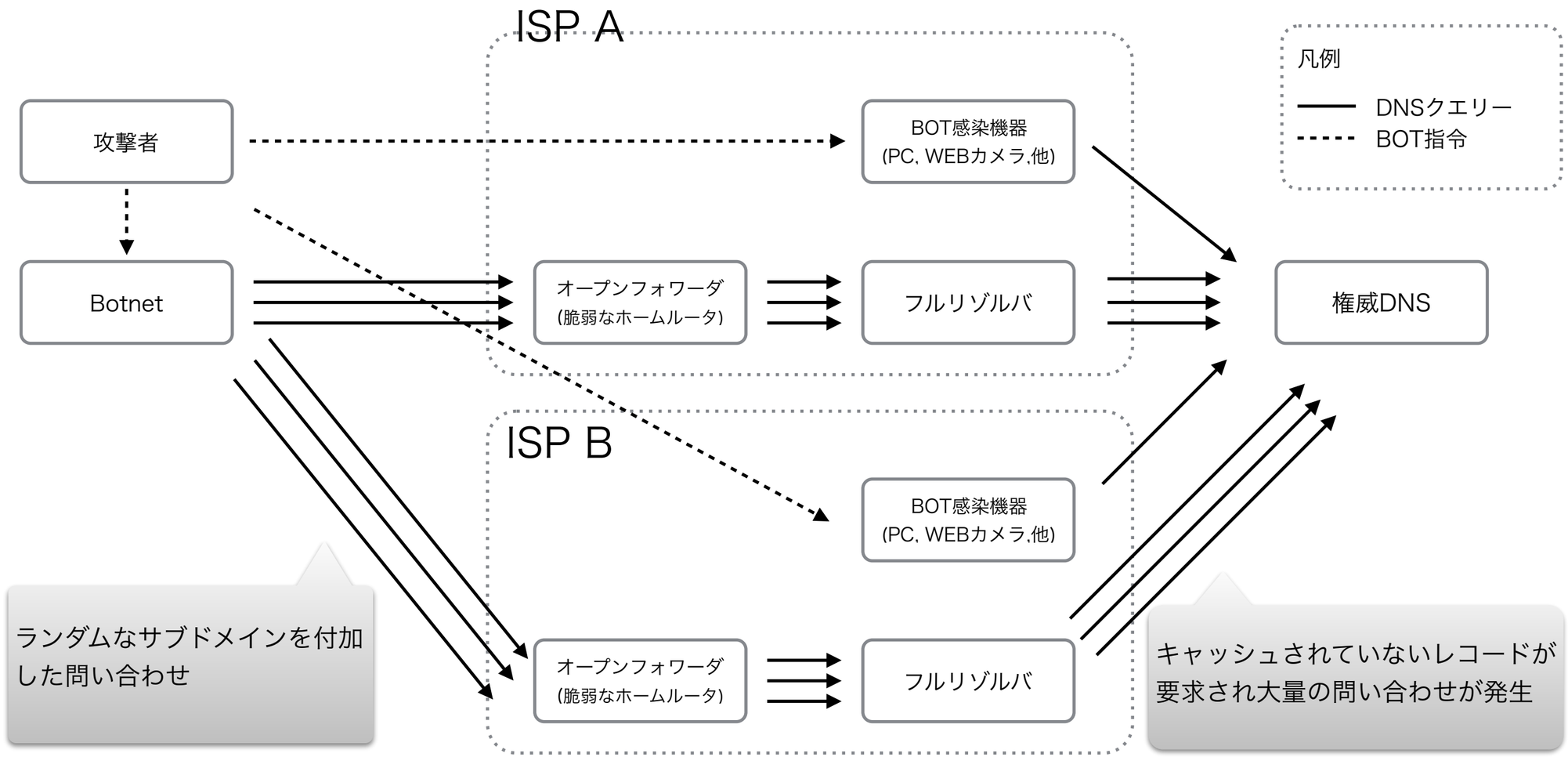


https://www.nominum.com/press_item/qtnet-protects-broadband-network-enhances-reliability-nominum-dns-security/

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！

各種攻撃耐性

(おさらい)
- 水責め攻撃の概要
  - **1クライアントあたりは非常に低いレート**でキャッシュDNSに突き刺さる
  - 正常な通信と判別が難しくIN側のRate Limitでは対策が困難



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

各種攻撃耐性(水責め)

- Nominum Vantio CacheServeでの水責め対策 (Success-Based Rate-Limiting)

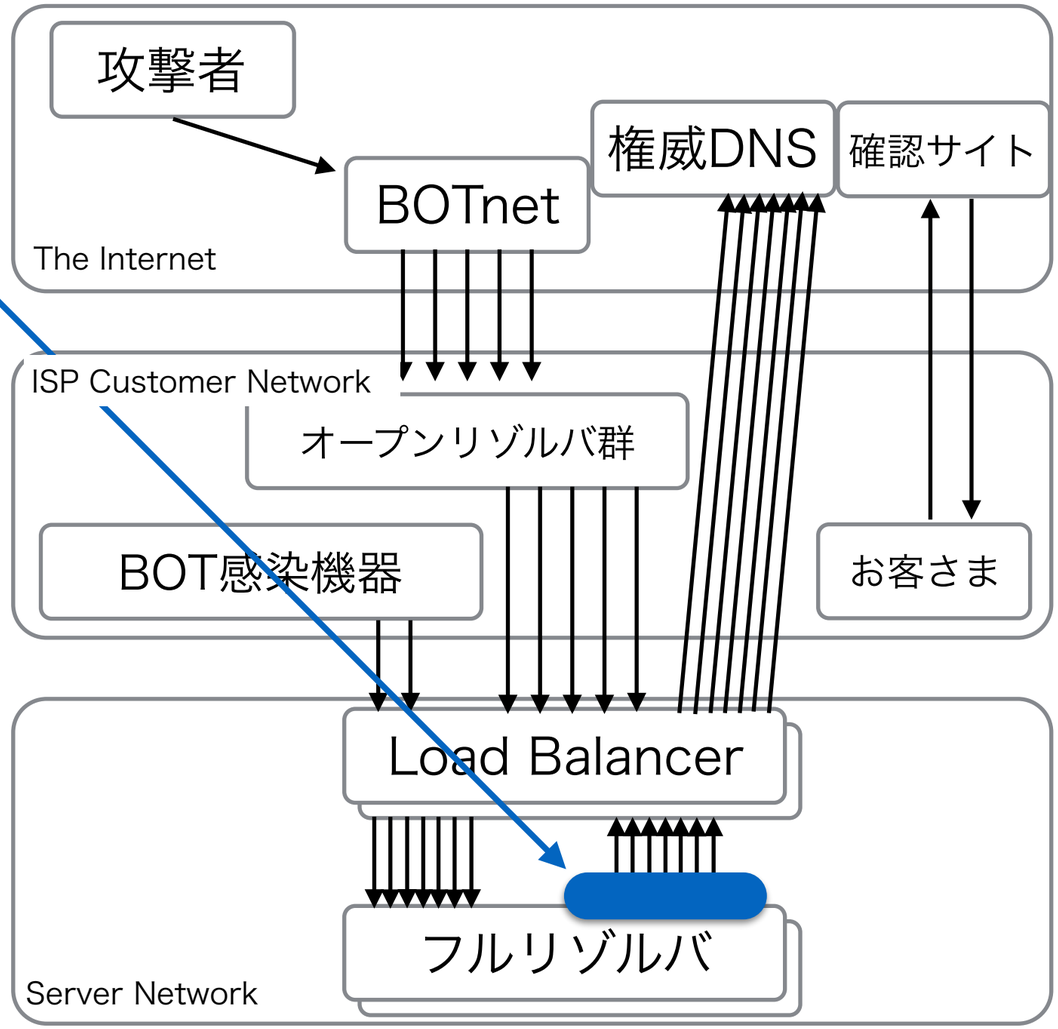
- 特徴

・フルリゾルバから権威DNSへの自動的なrate limit

どのような仕組み？

・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)

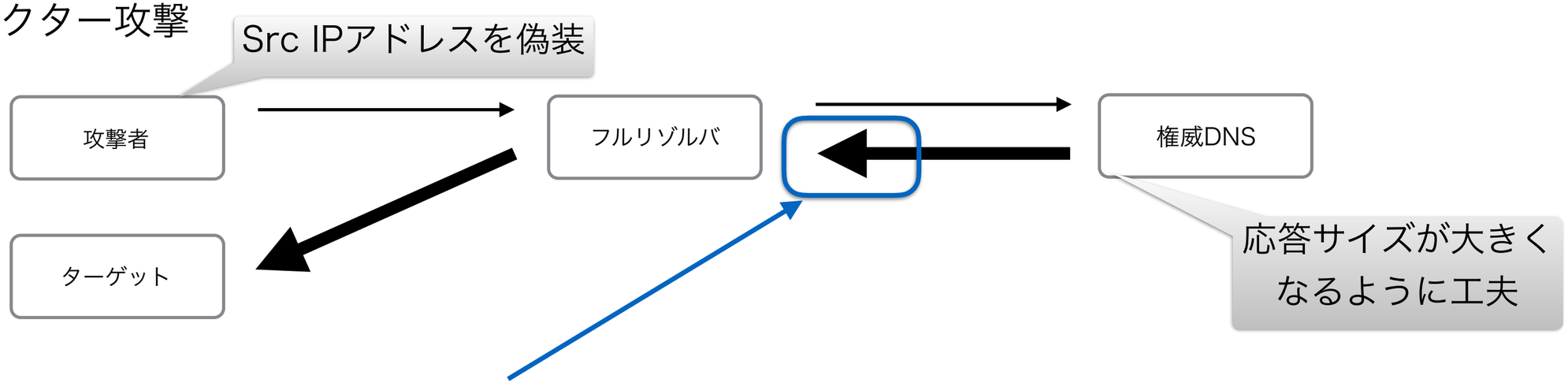
・スコアリングの結果から、水責めの影響が発生している
権威DNSとドメインの組み合わせに対してrate limit



Out側で制御することにより、正常な通信は阻害せず水責め対策が可能

各種攻撃耐性

- Nominum Vantio CacheServeでのレートリミット (Response-Size Rate-Limiting)
  - DNSリフレクター攻撃



- 特徴

・レスポンスサイズによってRate Limit

例えば・・

・レスポンスサイズが2000byte以上は200qpsにRate Limit

..だけではなく、

閾値を超過したものはTrancateを返してTCPで問い合わせなおさせる

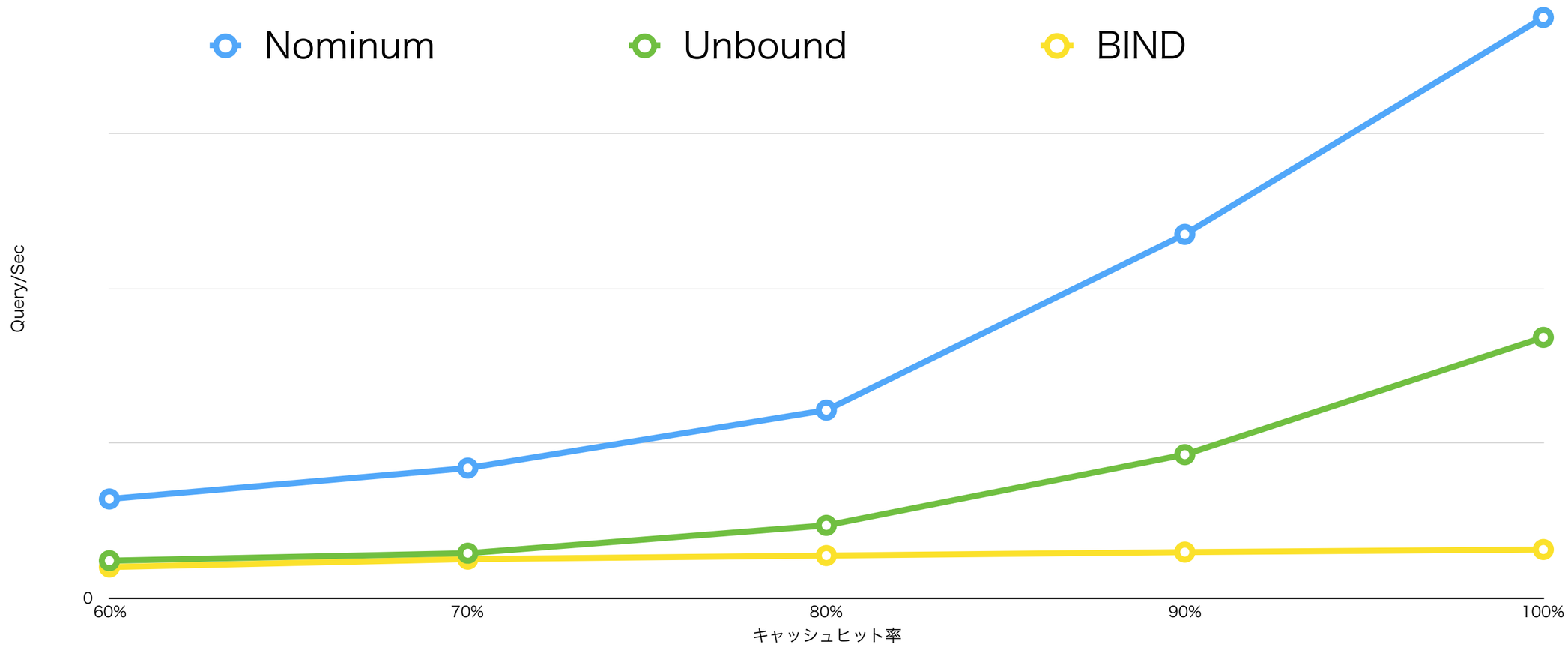
さらに

・qtype = ANYに対してはより厳しく50qpsでRate Limit閾値超過したものは同様にTrancateを返す

様々な条件でRate Limitかけることができ、正常な通信は透過、攻撃からは防御

パフォーマンスの比較

- 実装の違いによるパフォーマンス比較



キャッシュヒット率や遅延など

実環境を想定した環境で正確に測定することが重要

まとめ

- BINDからNominum製品へ

  脆弱性フリー、各種攻撃耐性、高パフォーマンス

- その他、比較検討する中で見落としがちな注意点
  - 導入実績

    権威で？フルリゾルバで？

    エンタープライズ？　ISP?(まさかISPの社内含めてる？)
  - 各種攻撃への対策

    なぜ、対策が有効に機能するのか
  - レスポンス

    QAへの対応、問題があった場合のパッチリリースまでの時間
  - 開発の体制

    開発する人数（層の厚さ）

鵜呑みにせず、裏どりと検証を！！