DNS Open Resolver について考える

JANOG31.5
NTTコミュニケーションズ株式会社
高田 美紀 @mikiT_T

はじめに

- 3月末までは別組織(AS2514)にいました
- 2/26 [janog:11575] オープンリゾルバ
  - CloudFlareの発表@APRICOT2013
    - オープンリゾルバ数、JapanはASIAトップ
    - AS2514はJapan堂々の2位
- Σ(゜◇゜;
- CloudFlareとのやり取りなど開始
  - DDoS元IPアドレスのリスト取得

agenda

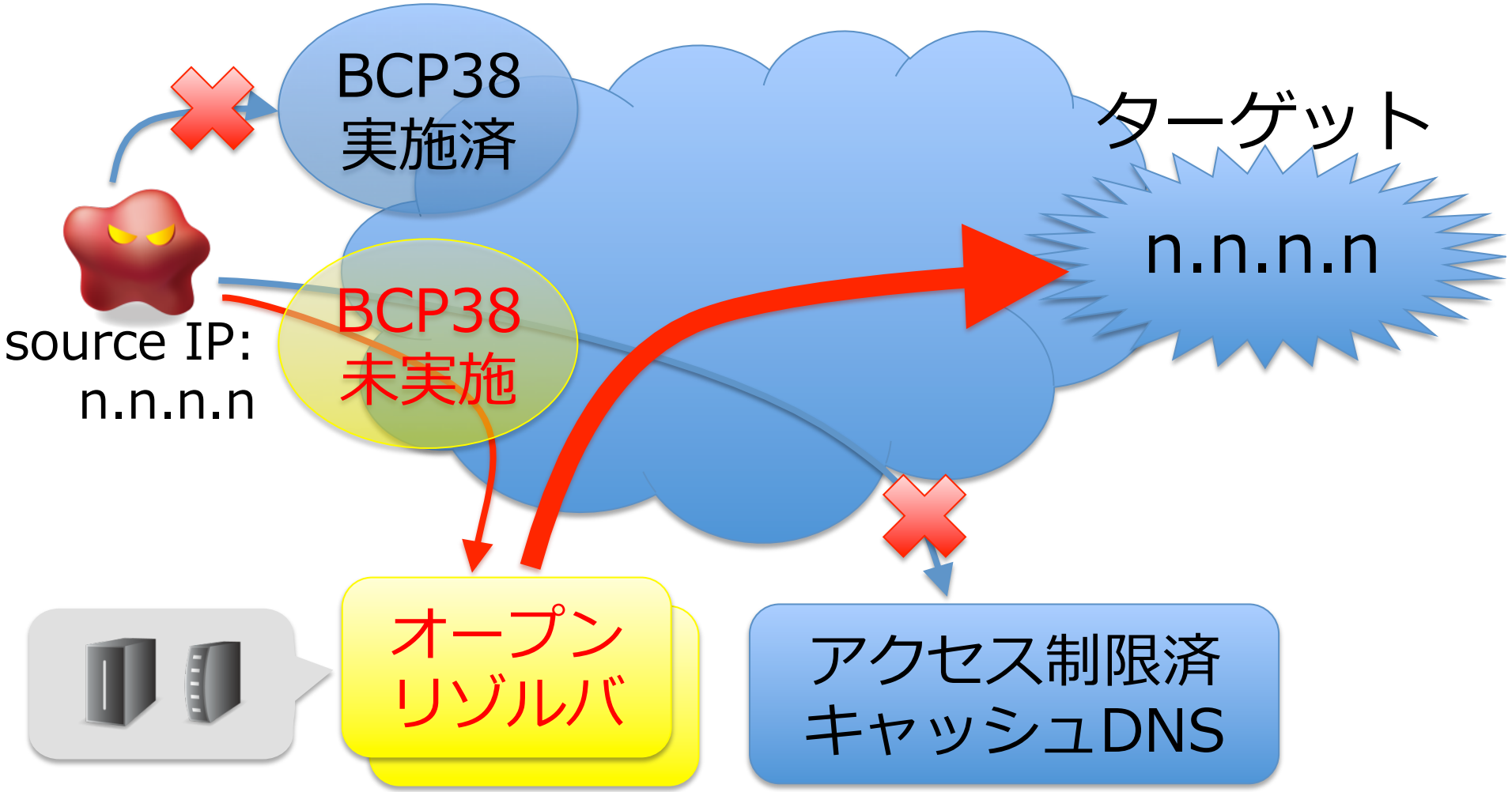
- オープンリゾルバについて
- BCP38について (IIJ 松崎さん)
- 対策モチベーション
- 事業者としてできること
- コミュニティとしてできること
- 現在の状況とお願い (JPCERT/CC 久保さん)
- 議論
- まとめ

オープンリゾルバとは

- サービス利用者の制限をしていない
  キャッシュDNSサーバ
- DNS amplification attacksの踏み台

- よくある構成
  - 権威DNSサーバを上げたらキャッシュも。。
  - 権威DNSとキャッシュDNSを分離してない
  - WAN側からのDNS検索に応えるBBルータ

DNS amplification attacksの構造



何が問題なのか

- そうと知らずに攻撃者となってしまう
- DNS amplification attacksには

オープンリゾルバ対策
と
BCP38

- 両輪の実施が必要

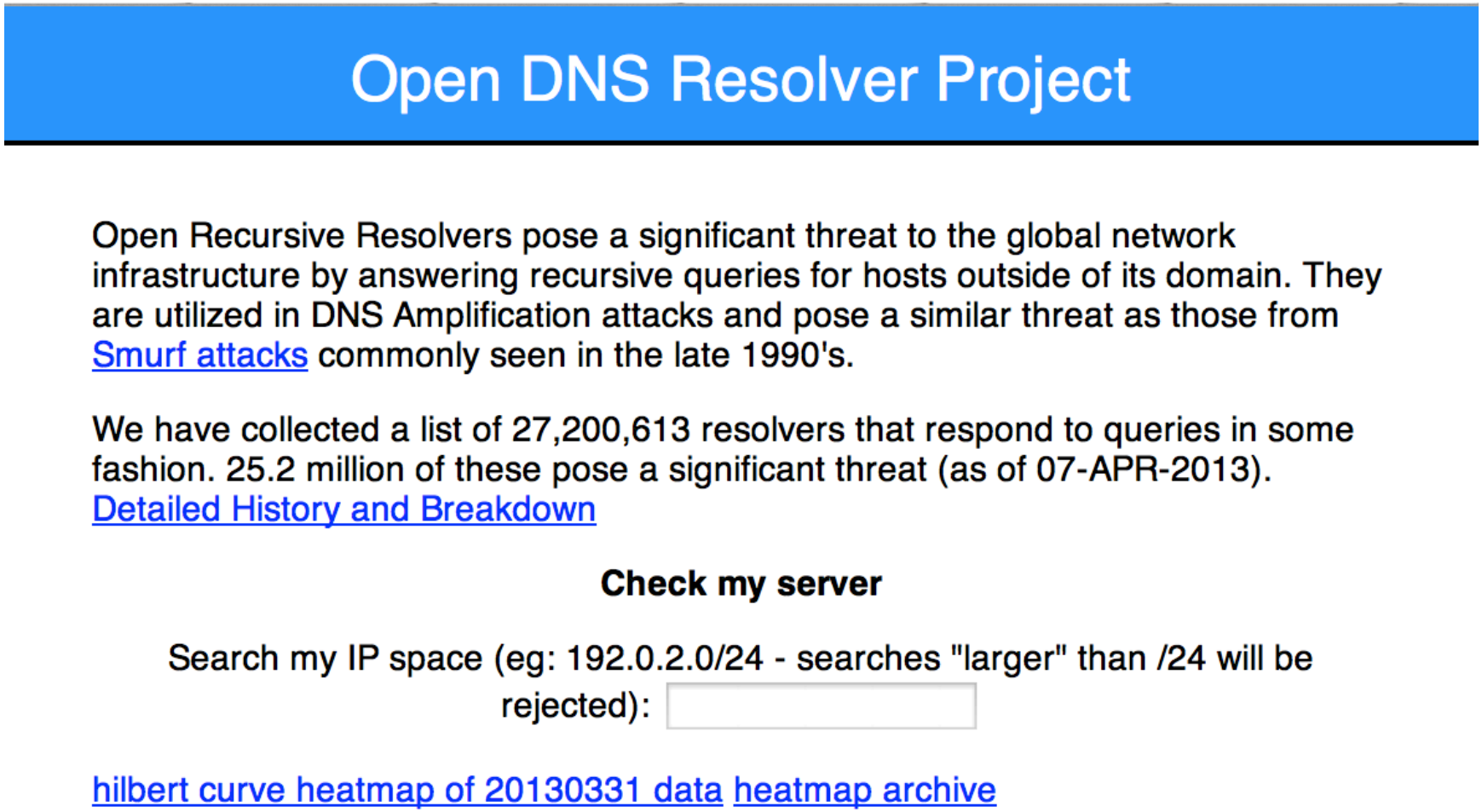
IIJ松崎さん、お願いします。

BCP38について

モチベーション(1)

- 明るいインターネットの未来のために
- 自NW内は?
  - オープンリゾルバの数、種類
    - 把握してますか?
  - http://openresolverproject.org/
- ampに利用されている率(踏み台率)
  - CloudFlareからもらった踏み台IP数/OpenResolverProjectのIP数
  - AS2514では●%程度

OpenResolverProject.org



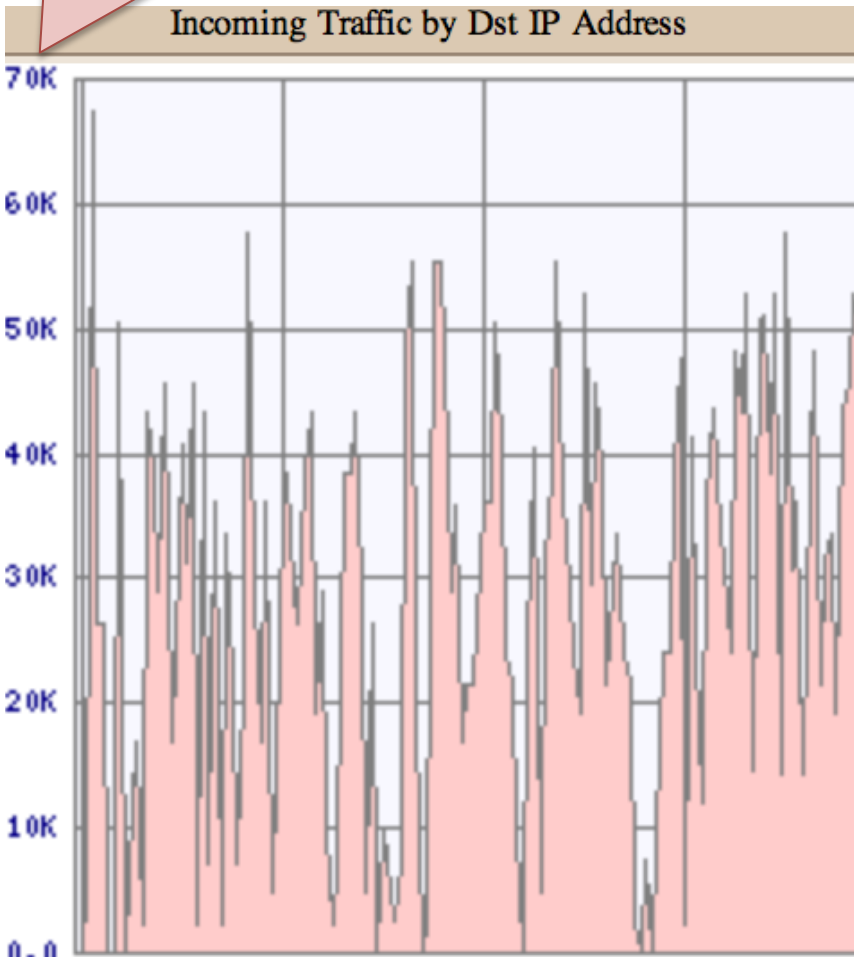
モチベーション(2)

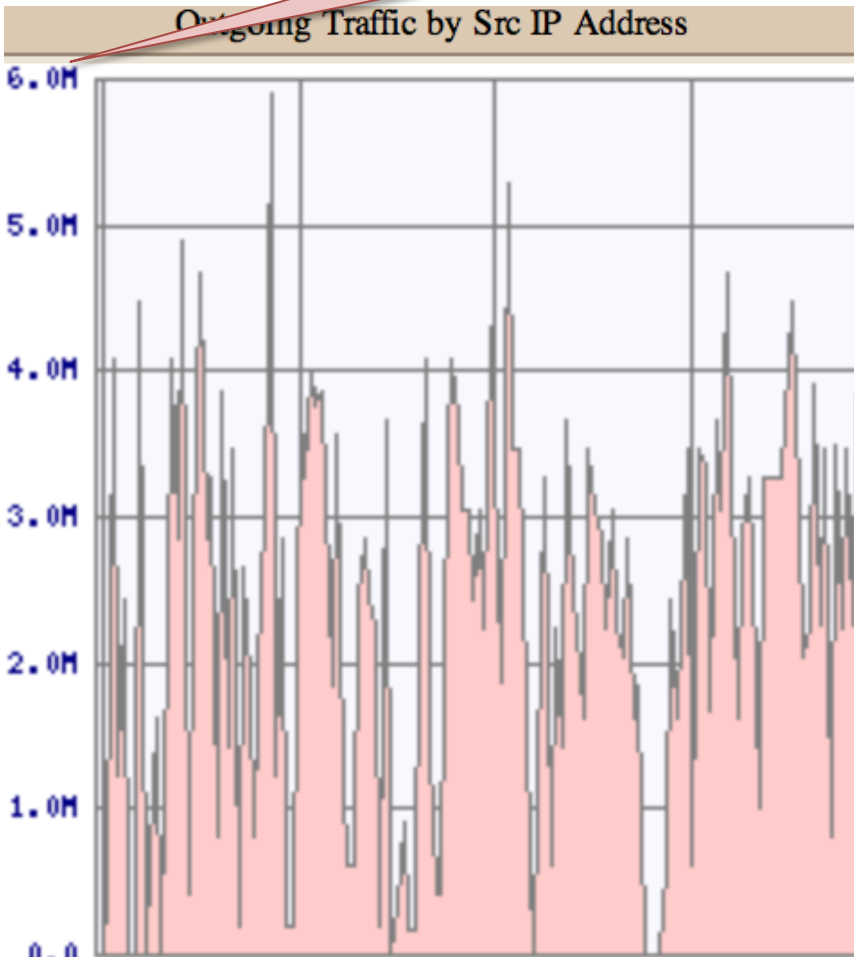
- コスト削減
- DDoSは本来必要のないトラフィック
  - 自NWのオープンリゾルバ数×踏み台率×ひとつの踏み台が叩き出すトラフィック
- 実例
  - とある地方ISP、とあるIP、とある1日のフロー
    - Port 53
  - Outbound:
    - avg: 2.3M, max: 5.9Mbps
  - Inbound:
    - avg: 27.49K, max: 67.28K
  - 増幅率: 90倍

とある様子

Incoming
単位: Kbps

Outgoing
単位: Mbps





デフォルト設定の強さ

- とあるVPSサービス
  - 古いサービスのテンプレ
    - recursion no; なし
  - 新しいサービスのテンプレ
    - recursion no; あり
  - CloudFlareのリストで100:1
- ディストリビューションのデフォルトも同様なのでは

事業者としてできること(1)

- 設備による分類
  - 自設備のDNSサーバ
  - 自設備のルータ
  - お客さまのDNSサーバ
  - お客さまBBルータ
- タイムラインによる分類
  - 既設
  - 新設

事業者としてできること(2)

- 対処方法による分類
  - 不要なキャッシュ機能の停止
  - キャッシュDNSサーバのアクセス制限
  - テンプレの変更
  - BBルータの実装修正
    - ベンダさんと協調
  - IP53B
    - サービスによっては可能なはず
  - その他には?

コミュニティとしてできること

- 周知啓蒙
  - 伝えるべきこと: 必要性、やり方など
  - 誰に?
    - DNSサーバを設定する人たち
    - 著名distributionのbind関連パッケージャ
    - 「bind 設定」とかで上位ランクするページの作者
- BBルータ系
  - 機種特定とか?
- その他には?

JPCERT/CC 久保さん、お願いします。

現在の状況とご協力のお願い

議論

- 事業者として、コミュニティとして
- なにかできそうなことはないですか
  - できそうじゃなくてもいいです☺
  - こういうことをしてほしい、とか
- アイデア募集
- IP53Bの是非についてはスコープ外
  - 方法論は歓迎
- 特定の事業者やベンダへの非難は×

議論まとめ(1)

- 個別にすべての人が対応して行かないと解決しない
  - 啓蒙
    - 加害者であることも含めて
- JANOGに来ない人たちにどうやってリーチするか
  - World IPv6 Launchのようなイベント?
    - 何をするのか、から考えないといけない
  - 日経あたりにどーんと取り上げられると認知が広まるのでは

議論まとめ(2): ルータ

- 機種名等はJPCERT/CCへ
  - 脆弱性ハンドリング対応を開始した
  - 機器やバージョンの特定をしている段階
- 顔の見えてるベンダさんには直接 ☺
- テレコムアイザックでも調査WGが発足
- ファームウェアのアップデート
  - 最近の国内ベンダー製は自動アップデート機能
  - 古いものにはない
- マネージドCPE
  - サービス提供業者がファームアップ
- LAN側にグローバルアドレスがつく場合、そちらからのqueryに答えてしまうものがある

議論まとめ(3): ホスティング

- ホスティング
  - VPS, 専用サーバ等の問題設定ホスト
    - お客さまに確認して変更
  - テンプレートの確認
    - recursion no;
  - Plesk, cPanelの確認
    - OS設定
      - デフォルトでnamedが動いてないか
    - bind設定
      - キャッシュと権威の分離ができているか
      - キャッシュquery元の制限をしているか

議論まとめ(4)

- 既設のDNSサーバの対応
  - 設定変更時、ミスやクレーム等での切り戻し
    - キャッシュ/権威の分離
  - アクセス制限
- アクセスリストのメンテナンス
  - お客さま持ち込みアドレスブロックの更新
  - DNS担当者とバックボーン担当者を仲良しに

議論まとめ(5)

- 用語
  - 「オープン」という言葉は、良い意味で受け取られることが多い
    - オープンソースとか、オープンな企業風土、とか
  - JPRSでは「有害リゾルバ」ということにした
- 8.8.8.8
  - Google Public DNS はレートリミットが入っている
  - 有害なオープンリゾルバではない

なんか思い出した。。

- sendmail→qmail, postfix, exim...
  - 10年～15年くらい前?
  - 3rd party relay
    - POP before SMTP, SMTP AUTH
- bind→unbound, NSD, PowerDNS...
  - 同様の波が来ているのではないか

まとめ

- 2006年とかもっと前から問題に
  - DNS amplification attacks@JANOG18
  - 喉元すぎると「直ちに問題はない」と後回しに
- 「いつやるの? 今でしょ!」
  - すぐにできる人は、今やって
  - そうでない人は、考え始めることを「今から」
- 今後とも活動していきたい
  - 協力者募集中
  - 特に、グラフや数値を出してもいいよ!という方

ここから先は発表しません

APPENDIX

ツール等のポインタ

- テスト＆サーベイ
  - http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl/
  - 10IPv4アドレスをテストできる
- オープンリゾルバのリスト
  - http://openresolverproject.org/
  - 定期的に(?)全IPアドレスにテストを仕掛けている
  - そこから任意の/24でリスト出力
- テスト
  - http://www.thinkbroadband.com/tools/dnscheck.html
  - 今使ってるキャッシュDNSサーバがオープンリゾルバかどうかチェックしてくれる

踏まれてるかチェック

- tcpdump, wireshark
  - isc.org, ripe.net ANYでの問い合わせ、応答
- dig isc.org any +norec @IPアドレス
  - +norec: キャッシュにあれば答える
  - ドメインは ripe.net とかでも
  - DNSKEY, RRSIG RR が返ってきたら踏み台にされている可能性が高い
  - TTL切れでキャッシュから消えてるだけかも

参考資料(1)

- CloudFlare発表@APRICOT2013
  - http://apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf
- DNS amplification attacks@JANOG18
  - http://www.janog.gr.jp/meeting/janog18/program-abstract.html#P8
- DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について@警視庁
  - http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/20060711_DNS-DDoS.pdf

参考資料(2)

- JPCERT/CC, JPNIC, JPRSの3組織で2013/4/18(木)に注意喚起文を発表

- DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起
  - https://www.jpcert.or.jp/at/2013/at130022.html
- オープンリゾルバ(Open Resolver)について
  - https://www.nic.ad.jp/ja/dns/openresolver/
- DNSサーバーの不適切な設定「オープンリゾルバー」について
  - http://jprs.jp/important/2013/130418.html
  - ■技術解説:「DNS Reflector Attacks(DNSリフレクター攻撃)」について
    - http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html
  - ■設定ガイド:オープンリゾルバー機能を停止するには【BIND編】
    - http://jprs.jp/tech/notice/2013-04-18-fixing-bind-openresolver.html