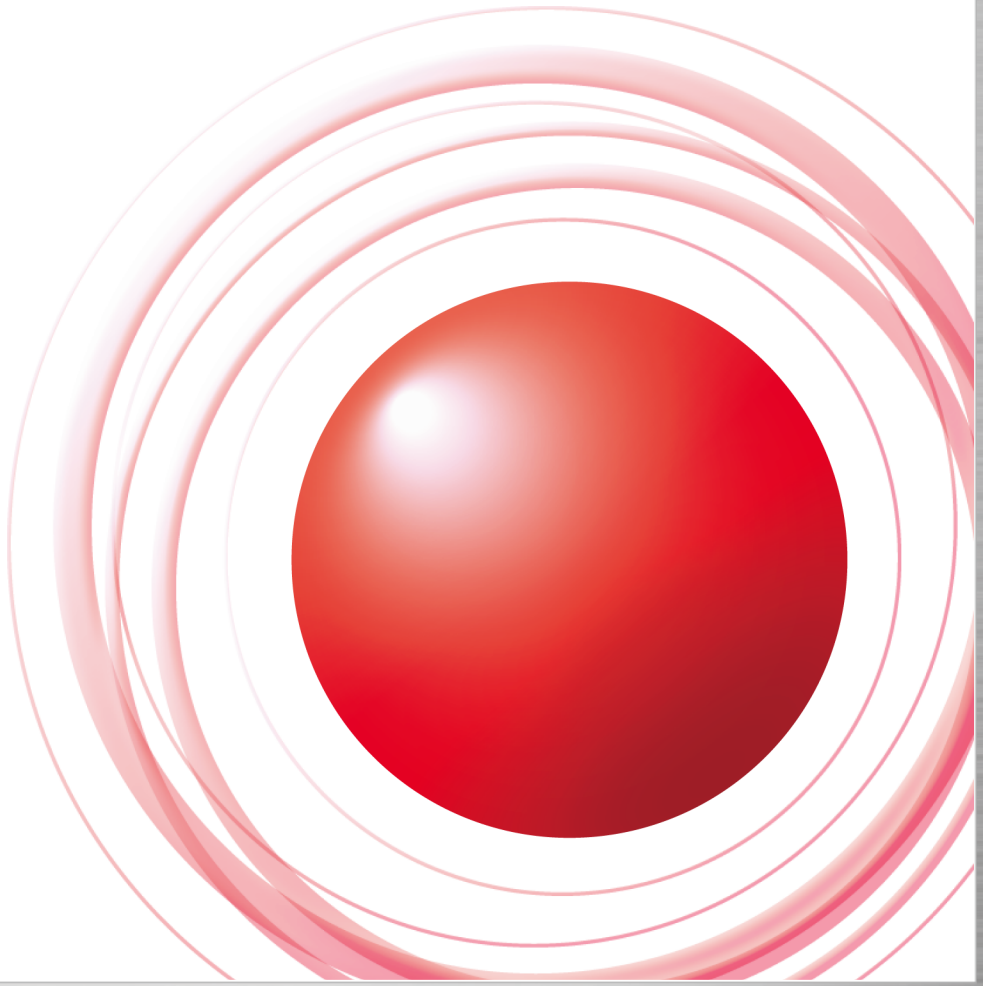
IIJとオープンリゾルバ

IIJ
Internet Initiative Japan



2013/11/28
株式会社インターネットイニシアティブ
山口崇徳

Ongoing Innovation

キャッシュDNSサーバ

IIJって?

- **1992年創業のISP**
  - この業界ではわりと歴史が長い
  - 「歴史的経緯によりうんぬん」がいっぱい
- **iij.ad.jpの権威DNSサーバは、大昔キャッシュ兼用でした**
  - もちろんオープンリゾルバ
  - なんでそんな設定になっていたのかは不明
    - 当時のBINDのデフォルトがそうだったからだと思うけど
- **これダメだよなぁ、と認識したときにはすでにキャッシュサーバとして利用しているユーザ多数**
  - キャッシュサーバとして使えるなんて広報したことは一度もないのに

非公式キャッシュサーバ

- **とりあえず権威とキャッシュを分離**
  - 従来のIPアドレスはキャッシュ専用にして、権威サーバを新設移行
  - 2003年ごろ
- **残った非公式キャッシュサーバをどうしてくれよう…**
  - 実害ないのでとりあえず放置
  - オープンリゾルバの問題があまり認識されていなかった時代
- **ずっと放置していたが、2011年になって閉鎖に乗りだす**
  - DNS ampよりも、ホスト老朽化の方が理由としては大きい

非公式サーバのはずなんだけど…

- **クエリログから利用ユーザを調査していておかしなことに気がつく**
  - 特定ISPのレンジからSRVで_sipな問い合わせが妙に多い
  - そのISPを調べてみるとIP電話サービスをやってる
  - どうやらVoIP端末のキャッシュDNSサーバ設定として、うちの非公式サーバのIPアドレスが埋めこまれてるっぽい…
    - NTPも某大学の非公式サーバを利用していた模様
- **うちが非公式サーバを止めたら、よそのISPのVoIPサービスに障害が起きちゃうってこと?**
  - とりあえず停止予定の1ヶ月前に連絡して対応を依頼
  - 対応が間に合ったのかどうかは不明

停止の影響

- **キャッシュDNSサーバが使えなくなる ≒ インターネットが使えなくなる**
  - 踏み台としての不正目的の利用はごくわずか
  - 悪意を持って使っているわけではない大半の利用者が、突然インターネットを使えなくなる
  - オープンリゾルバを止められない最大の理由
- **停止する前に、「もう使えなくなるから設定変更してくれ」と利用者に案内したい**
  - 接続元からIIJ顧客と判断できるものは個別に連絡
  - が、ほとんどはIIJの顧客ではない → 連絡手段がない

ユーザへの停止告知

- **停止しようとしているキャッシュサーバ自体を告知ツールとして使う**
  - ルートゾーンを書き換えて、どんなURLへのアクセスも停止案内ページに誘導する
  - ふつーにWebブラウザを使っているなら告知が見えるはず
    - ただし、HTTP以外のプロトコルは応答しない
    - メールで問い合わせようとしても届かない
- **この状態で1ヶ月ぐらい運用した後でshutdown**
  - とくに悲鳴などは聞こえてこず

ブラックホール設定

- **DNSサーバ**
  - named.conf: rootゾーンを乗っとる

```
zone "." {
    type master;  // type hintではなく、masterとしてふつうにゾーンを定義
    file "/path/to/fake-root.zone";
};
```

  - fake-root.zone: 何を聞かれても同じアドレスを返す

```
$TTL 60     ; キャッシュされても影響が小さくなるようTTLは短め
@   IN      SOA     ...
    IN      NS      ...
    IN      A       192.0.2.1 ; このIPアドレスでWebサーバを動かす
*   IN      A       192.0.2.1
```

- **Webサーバ**
  - httpd.conf: どんなURLでアクセスされても同じ内容を返す

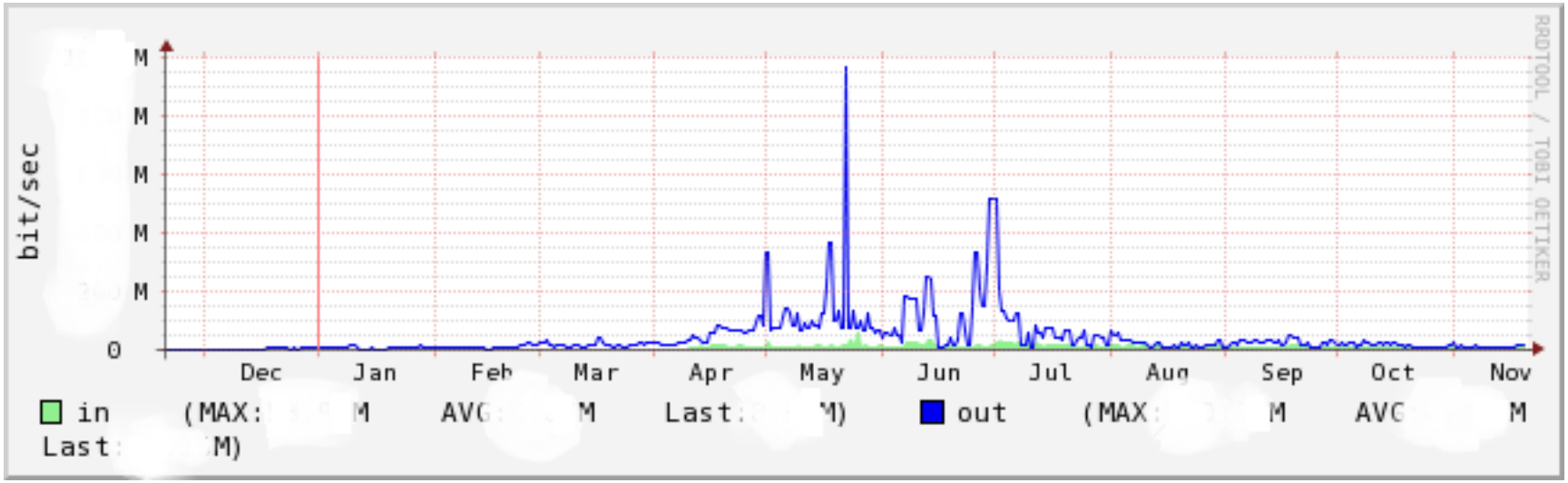
```
AliasMatch . /docroot/index.html
```

公式なキャッシュサーバ

- **公式に提供しているキャッシュサーバもオープンリゾルバ**
  - 20年前からずっと同じIPアドレス
  - お客さんが設備を更新しても、キャッシュサーバの設定も引き継がれてしまって更新されないことが…
  - aclありのサーバももちろん用意しているが、移行が進まない
- **昔はキャッシュサーバは手で設定していた**
  - 自動設定できるようになったのはわりと最近
  - ISPをIIJから他社に変更しても、設定変更漏れでDNSだけはIIJを使い続ける
  - 自宅と外出先で異なるISP回線を利用する場合でも、ノートPCの設定は自動では切り替わらない
  - こういったユーザの名前解決が阻害されるので、制限しづらい
- **とーぜん、踏み台として悪用される**

とあるキャッシュサーバのトラフィック

- 踏み台にされまくっていたサーバ
- あまりに衝撃的すぎるトラフィックのため、縦軸は内緒です
- 夏以降はだいぶ落ち着いてきている
  - いろいろ対策した効果があったのか
  - 単に攻撃が下火になっただけなのか



オープンリゾルバのままamp対策

- **力技のiptablesルール**
  - u32モジュール: パケットのペイロードにマッチさせる
  - hashlimitモジュール: 時間あたりのパケット数を制限する
  - これらを組み合わせて、同一IPアドレスからの大量のANY or RRSIGなクエリを落とすルールを作成
- **DNS ampのためだけに用意されたと思われる名前であればブラックリストへ**

```
zone "domain.invalid" {
    type master;
    file "/path/to/dummy.zone";
    allow-query { none; };      // どこからの問い合わせも受けない
};
```

- **顧客のホームルータが踏み台にされてクエリがforwardされていると思われる場合は、地道に連絡して対応依頼**

閉じる方向でがんばってます

- **遅れぎみですが…**
  - 11月予定だったんですが、12/2に実施することになりました
  - 現在いろいろ準備中
- **影響を受けるユーザにどうやって告知するかが悩み**
  - 2011年に非公式サーバを閉じたときと同じ
  - 利用者の数は比較にならないほど多い

広報活動

- **ということで、不特定多数に向けて告知してみた**
  - IIJ公式サイト
    - http://www.iij.ad.jp/company/development/tech/activities/open_resolver/
    - 「オープンリゾルバ」でぐぐるとかなり上位
  - 技術者ブログ
    - http://techlog.iij.ad.jp/archives/718
    - はてなブックマークで300ブクマ越え
- **こちらの期待以上に広く読まれた**
  - ありがとうございます
  - これでも実際の利用者の大半には届いてないだろう…
  - が、やらないよりはずっとよかったはず
- **閉じた後どうなるかはまだこれから…**
  - 12/2 がんばります

ブロードバンドルータ

IIJはルータも作ってます

- 詳細はSEILでぐぐってください
- こいつがオープンリゾルバに…
- JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題

なぜオープンリゾルバに?

- どちらかというと「わかってる人向け」の製品
  - ネットワーク設計はユーザの裁量に任される部分が大きい
  - どのインターフェイスがWAN用でどれがLAN用なのかといったことはユーザが定義する
  - 用途が広いので、工場出荷状態では必要最低限以外の制限は入れづらい
- 開発当初はDNS ampに関する認識が薄かった
  - DNS forwarderにインターフェイスを指定する機能がなかった
  - 正しくフィルタを書いて適用しないとオープンリゾルバに

踏み台になってたの？

- はい
- 2013年夏ごろがピーク
- SEILを利用している顧客からフォワードされてきたクエリにより、キャッシュサーバが大量トラフィックを吐いた事例が複数
  - 大量に導入していただいた顧客がごっそりまとめて踏み台にされてみたり
- キャッシュサーバの側からは正当なユーザからのクエリに見えるので、アクセス制限では止められない
  - forwarderの側でふさぐ必要がある
  - フィルタの適用をお願いする

IIJの対応

- **ファームウェア修正**
  - DNS forwarderにインターフェイスによりアクセス制限する機能を追加実装
    - デフォルトでLAN側のみ許可
  - ファームウェアを更新することでオープンリゾルバではなくなる
  - 2013年3月から7月にかけて修正ファームウェアをリリース
- **細かく挙動を指定する場合にはフィルタを書いてもらう**
- **ユーザへの案内**

SMF

- **SEIL Management Framework**
  - 個々のサービスアダプタ(SEIL)を遠隔地から集中管理・保守する仕組み
  - 設定変更やファームウェア更新も可能
    - 100台の設定変更でも数分程度
- **多くのSEILはSMFの契約管理下で動作している**
  - 稼動状況や設定内容はIIJが把握できる
- **とはいえ、基本はself managedなサービス**
  - どうするかの最終判断はユーザに委ねられる
  - IIJでできるのは情報提供や対応依頼程度
- **あまり手間がかからないので、方法を案内すれば早々に対応してもらえることが多い**

対応進捗状況

- **修正版ファームウェアをリリースする前から、踏み台になっているらしきユーザにはフィルタ適用を依頼**
- **2013年7月時点でオープンリゾルバだったSEILのうち、10月末までに95%が対応完了**
  - フィルタ設定変更7：ファームウェア更新3ぐらいの割合
- **ファームウェアの一括適用、設定の一括変更が簡単かつ迅速にできる強みを発揮**

- **SMF管理下にないSEILの対応状況は不明**
  - こちらでは把握できない

まとめ

- **オープンリゾルバは、存在しているといつのまにか使われている**
  - DNS ampの踏み台としての悪用だけでなく、悪意のない利用も多数
- **キャッシュサーバが使えない≒インターネットがつながらない**
  - アクセス制限による影響が非常に大きい
  - 影響を受ける利用者への連絡が困難
- **マネージドルータは対応も早い**
  - ユーザへの連絡が可能
  - 設定変更の手間が小さい