キャッシュDNSサーバとフィルタリングの実例

2011/11/30

インターネットイニシアティブ
島村 充
simamura@iij.ad.jp

Ongoing Innovation

アジェンダ

- AAAAフィルタリング
- ブロッキング
  - zone上書き方式
  - RPZ方式

AAAAフィルタリング

AAAAフィルタリング 概要

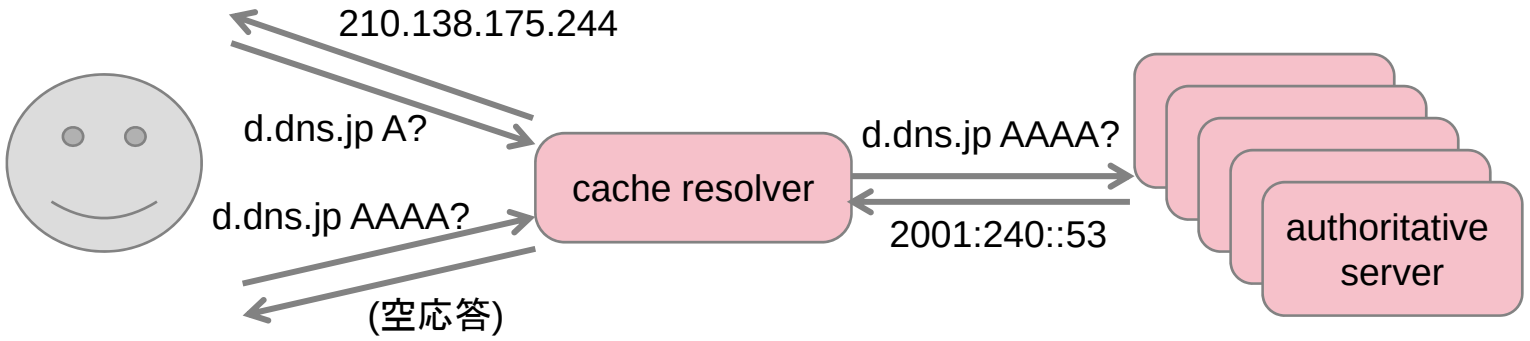
- 2011/06/08 World IPv6 day
  - 世界中の有志が24時間限定でWebサイトにAAAAをつけるイベント
  - Google, Facebook, Yahoo!... 計400
- 何が危惧されたか
  - AAAAが返ってくるとおかしくなる製品
  - IPv4にfallbackできない/時間がかかる
    - 閉域IPv6網に繋がっていて、Internet上のIPv6サーバに疎通がないケース

AAAAフィルタリング 概要

- 本来は個々に対処すべき
  - 古い機器/ソフトの刷新
  - IPv6 reachabilityの提供
  - Policy tableを書いて、閉域IPv6網にパケットを出さないように
- 間に合わないとエンドユーザが混乱する
  - サポートセンターも混乱する
  - ISP側でなんとかしてあげたい

AAAAフィルタリング 概要

- そこでAAAAフィルタリング
  - IPv4で名前解決がリクエストされたとき、AAAAを削って応答をする
  - bind-9.7.2以降の機能



AAAAフィルタリング 設定

- コンパイル時にconfigureで指定が必要

```
./configure --enable-filter-aaaa
make
make install
```

- named.conf

```
options { filter-aaaa-on-v4 yes; };
```

AAAAフィルタリング 応答

```
$ dig -t A d.dns.jp
d.dns.jp. 3600 IN A    210.138.175.244
$ dig -t AAAA d.dns.jp
# AAAAフィルタなし
;; flags: qr rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 7, ADDITIONAL: 1
d.dns.jp. 3600 IN AAAA 2001:240::53
# AAAAフィルタあり
;; flags: qr rd ra; QUERY: 1, ANSWER: 0,
AUTHORITY: 7, ADDITIONAL: 1
(空応答)
```

ブロッキング

ブロッキング 概要

- ある(問題のある)ドメイン・サーバの名前解決をブロック
  - 空応答・別のIP
- 使用目的
  - ISPでは児童ポルノのブロッキング
  - 組織内のブロッキングにも？
- IP直/ISP以外のDNSを使うと閲覧可能
  - ライトユーザ層は見られない

ブロッキング 実施方式

- 2つの実施方式
  - zoneの上書き
    - bind/unboundで利用可能
  - RPZ(Response Policy Zone)
    - bind-9.8.0より利用可能

ブロッキング（zone上書き）設定

- ブロックしたいドメインに対して、応答を上書きするような設定をする
- 安心ネット作り促進協議会様のとても素晴らしいガイドライン

  http://good-net.jp/usr/imgbox/pdf/20110427091336.pdf

  – この通りに設定すればOK

  – 「ブロックしました」ページの構築方法も掲載

ブロッキング（zone上書き）設定

- bindの場合
  - named.conf

```
zone “evil.example.com” {
    type master;
    file “data/block.zone”;
};
```

ブロッキング（zone上書き）設定

– data/block.zone

特定のIPを返す場合

```
$TTL 3600
@ IN SOA localhost. nobody.localhost. (1 60 60 60 60)
  IN NS  localhost.
  IN A   192.0.2.1
* IN A   192.0.2.1 ; サブドメインなどもブロックページに
```

NXDOMAINを返す場合

```
@ IN SOA localhost. nobody.localhost. (1 60 60 60 60)
  IN NS  localhost.
```

ブロッキング（zone上書き）設定

- unboundの場合
  - unbound.conf

特定のIPを返す場合

```
local-zone: “evil.example.com” redirect
local-data: “evil.example.com IN A 192.0.2.1”
```

NXDOMAINを返す場合

```
local-zone: “evil.example.com” static
```

ブロッキング（zone上書き）応答

- bindの場合

```
$ dig –t any evil.example.com
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0,
ADDITIONAL: 0
;; ANSWER SECTION:
evil.example.com. 3600  IN  SOA  localhost.
nobody.localhost. 1 60 60 60 60
evil.example.com. 3600  IN  NS   localhost.
evil.example.com. 3600  IN  A    192.0.2.1
```

```
$ dig –t any www.evil.example.com
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1,
ADDITIONAL: 0
;; ANSWER SECTION:
www.evil.example.com.  3600  IN  A  192.0.2.1
```

ブロッキング（zone上書き）応答

- unboundの場合

```
$ dig –t any evil.example.com
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0
(空応答)
```

```
$ dig –t a evil.example.com
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0
evil.example.com. 3600  IN  A  192.0.2.1
```

ブロッキング（zone上書き）出し分け

- 同じキャッシュDNSサーバを使っている、複数の部署ごとにブロッキングの設定を分けたい場合
  - 例えば…：研究部門はブロッキング無し
- bindなら可能
  - viewを利用

ブロッキング（zone上書き）出し分け

- named.conf

```
acl RESEARCH-UNIT { 192.0.2.128/25; };
view “non-block” {
   match-clients { RESEARCH-UNIT; };
};
view “block” {
   match-clients { any; };
   zone “evil.example.com” {
     type master;
     file “data/block.zone”;
   };
};
```

ブロッキング (zone上書き) 出し分け

- 注意点
  - キャッシュが分離される
    - viewの数だけメモリ消費量が増える
      - * 2個作る：約2倍、3個作る：約3倍
    - キャッシュヒット率が下がる
      - * キャッシュされていない名前のレスポンスタイムが若干悪化
  - unboundでは不可
    - viewが無い

ブロッキング(RPZ) 概要

- “Response Policy Zone(s)”のacronym
- コンセプト
  - キャッシュDNSサーバでブロッキングを簡単に
    - 元々の目的はspamやphishing対策

http://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt

ブロッキング(RPZ) 設定

- bind-9.8.0以降で利用可能
- bind-9.7.3に対するpatchもあった
- named.conf

```
options {
    response-policy { zone “policy.iij.ad.jp” };
};
zone “policy.iij.ad.jp” {
    type master;
    file “data/policy.iij.ad.jp.zone”;
};
```

ブロッキング(RPZ) 設定

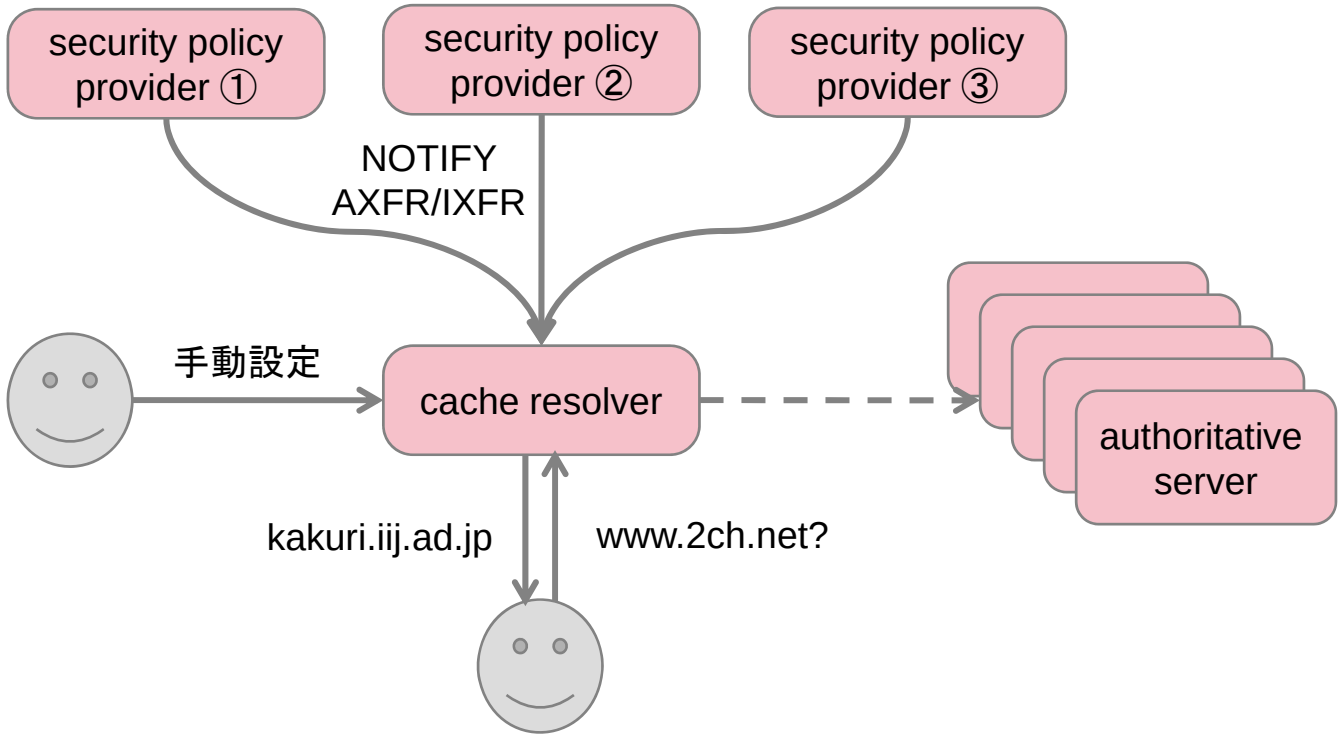
- data/policy.iij.ad.jp.zone

```
$TTL 600
@   IN SOA localhost. nobody.localhost. (1 60 60 60 60)
    IN NS  localhost.
evil.exmaple.jp  IN CNAME *.                  ; NODATA
evil.example.jp  IN CNAME .                   ; NXDOMAIN
www.2ch.net      IN CNAME kakuri.iij.ad.jp.   ; redirect
*.2ch.net        IN CNAME kakuri.iij.ad.jp.   ; redirect
iijad.jp         IN MX 10 blackhole.iij.ad.jp.
;; 左辺は "." で終端しない
```

ブロッキング(RPZ) メリット

- ブロックするドメインの追加削除がrndc reloadで反映
  - zone上書き方式だとrndc reconfig
    - なにかと不安
- AXFRで転送できる
  - (転送元があれば)変更反映が楽
  - 色々なsecurity policy providerを情報提供源に使える

ブロッキング(RPZ) 動作概要



ブロッキング(RPZ) バグ

- zone上書きよりスマートで良い
- 動作検証するとbindが簡単に落ちる
  - digで名前解決すると落ちない
  - FirefoxでWebページを開くと落ちる
    - 原因: FirefoxのDNSSEC検証拡張

https://addons.mozilla.org/firefox/addon/dnssec-validator/

- 根本原因: ブロックしているドメインのRRSIGを引くと落ちる

ブロッキング(RPZ) バグ

- バグレポートしたらすぐ直りました
  - 報告: 4/26夕方,返事(修正): 4/27未明
  - bind-9.8.0-P1リリース: 5/5

http://www.isc.org/CVE-2011-1907

Solution:

Use RPZ only for forcing NXDOMAIN responses and not for RRset replacement.

CVSS Score: Base 6.1, adjusted for lack of targets, score is 1.5 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:P/RL:O/RC:C/TD:L)

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score please visit: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

Thank you to Mitsuru Shimamura at Internet Initiative Japan for finding this defect.

ブロッキング(RPZ) バグ

- 一応バグは修正されたが、採用には不安
- 実績のあるzone上書き方式を採用
- 予感は的中(bind-9.8.0-P4)
  - Using Response Policy Zone (RPZ) with DNAME records and querying the subdomain of that label can cause named to crash. Now logs that DNAME is not supported. [RT #24766]
  - Using Response Policy Zone (RPZ) to query a wildcard CNAME label with QUERY type SIG/RRSIG, it can cause named to crash. Fix is query type independant. [RT #24715] [CVE-2011-1907]

ブロッキング(RPZ) 感想

- コンセプトは良い
  - 安定すれば導入できる
    - そもそも使う人がほとんどいない
    - ブロッキング導入実施済組織が多い
- AXFRで転送できるブロック対象の提供元が出てくると楽
  - zone上書き方式はfileを手書き/script

まとめ

- キャッシュDNSサーバとフィルタリングについて
  - AAAAフィルタリング
  - ブロッキング
    - zone上書きとRPZ
- 名前解決の応答の加工はやりたくない
  - 正しい対応方法は別にある
  - でも必要になる場面もある

IIJ Internet Initiative Japan

Any Questions?

Ongoing Innovation

おまけ：ブロッキングとDNSSEC

- キャッシュDNSでDNSSEC検証ONに。
- DOビットを立てた名前解決はどうなる？
  - AAAAフィルタ
    - `dig +dnssec -t aaaa www.isc.org`
      - * AAAAが返ってくる
    - `filter-aaaa-on-v4: break-dnssec;` なら削る
      - * 当然ADビットは立たない
- ブロッキング
  - 何もしなくてもブロッキングが優先
    - 当然ADビットは立たない