とあるゾーンの親子崩壊

設定ミス

株式会社ブロードバンドタワー

大本　貴

(題字は http://to-a.ru にて作成)

自己紹介

- 職歴
  - 2000年 インターネット総合研究所入社
  - 2001年 プロデュースオンデマンド(PoD)に出向
    - ストリーミング配信技術担当
  - 2007年 インターネット総合研究所に帰任
    - 主に社内システムのサーバ運用、コンサルなど
    - 2010年春からDNSSECジャパンの活動に参加
  - 2010年 ブロードバンドタワーに転籍
    - DNSSECジャパンの活動終了に伴いDNSOPS.jpの活動に合流

twitterでたまにDNSSEC関連のつぶやきをしています。

@taxiJPN

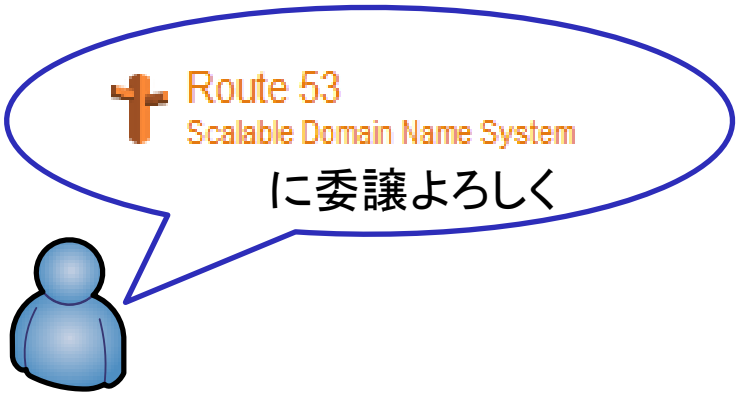
今年もbindの「夏」で
盛り上がった8月

一方、その頃、とある企業の、とあるドメインの、とあるゾーンでは、こんな「夏」が起きていた・・・。

~~人の不幸は蜜の味~~ 他山之石ということで。

amazone.bbtower.netの誕生

- bbtower.netは弊社の社内検証環境用ドメイン。
- ある検証業務のために新しくサブドメインを追加したい。
- 新しいサブドメインはサービス研究の一環でAmazon route53 を利用してみよう。
- route53に新ゾーン(Amazone)を登録。
- 弊社bbtower.net管理担当者にNSレコード登録依頼をした。



amazone.bbtower.net.	86400	IN	NS	ns-854.awsdns-42.net.
amazone.bbtower.net.	86400	IN	NS	ns-1162.awsdns-17.org.
amazone.bbtower.net.	86400	IN	NS	ns-19.awsdns-02.com.
amazone.bbtower.net.	86400	IN	NS	ns-1982.awsdns-55.co.uk.

結果、こんな感じのNS登録が出来ますた。

(注:グルーレコードは外部名なので依頼していない)

- さっそくroute53側のゾーンファイルにAレコードを追加してみる。→設定反映を確認しよう。

が、しかし。

挙動があやしい

- Route53に登録したAレコード(hoge.amazone.bbtower.net)が引けたり引けなかったりする。
  - **何回かに一度NXDOMAINだったりする。**
  - 複数あるroute53のNSでゾーンに差異か?
    - route53のNSへ直接Dig +norecするも、NOERRORで全て意図通りのAレコードを答える。
  - 親ドメインのゾーンでNSレコードに差異がある?
    - bbtower.netのNSに直接dig +norec amazone.bbtower.net NSしても、特に問題なくroute53のNSレコードを答える。

  でも、digするとやはりNXDOMAINが返ってくる。

よろしい、ならばSOAは誰だ

BroadBand Tower, Inc.

```
[root@dti-vps-srv735 entry]# dig amazone.bbtower.net SOA

; <<>> DiG 9.7.0-P2-RedHat-9.7.0-17.P2.el5_9.1 <<>> amazone.bbtower.net SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9185
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;amazone.bbtower.net.            IN      SOA

;; ANSWER SECTION:
amazone.bbtower.net.    900     IN      SOA     ns-1162.awsdns-17.org. awsdns-hostmaster.amazon.com. 1 7200 900
1209600 86400

;; AUTHORITY SECTION:
amazone.bbtower.net.    56067   IN      NS      ns-19.awsdns-02.com.
amazone.bbtower.net.    56067   IN      NS      ns-854.awsdns-42.net.
amazone.bbtower.net.    56067   IN      NS      ns-1162.awsdns-17.org.
amazone.bbtower.net.    56067   IN      NS      ns-1982.awsdns-55.co.uk.

;; ADDITIONAL SECTION:
ns-19.awsdns-02.com.    163231  IN      A       205.251.192.19
ns-854.awsdns-42.net.   163014  IN      A       205.251.195.86
ns-1162.awsdns-17.org.  163019  IN      A       205.251.196.138
ns-1982.awsdns-55.co.uk. 163082 IN      A       205.251.199.190
```

・・・・あれ？

BroadBand Tower, Inc.

```
[root@dti-vps-srv735 entry]# dig amazone.bbtower.net SOA

; <<>> DiG 9.7.0-P2-RedHat-9.7.0-17.P2.el5_9.1 <<>> amazone.bbtower.net SOA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46892
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;amazone.bbtower.net.            IN      SOA

;; ANSWER SECTION:
amazone.bbtower.net.    86400   IN      SOA     ctm01.bbtower.ad.jp. noc.bbtower.ad.jp. 2013072502 3600 1200
3600000 900

;; AUTHORITY SECTION:
amazone.bbtower.net.    86400   IN      NS      ns-19.awsdns-02.com.
amazone.bbtower.net.    86400   IN      NS      ns-854.awsdns-42.net.
amazone.bbtower.net.    86400   IN      NS      ns-1162.awsdns-17.org.
amazone.bbtower.net.    86400   IN      NS      ns-1982.awsdns-55.co.uk.

;; ADDITIONAL SECTION:
ns-19.awsdns-02.com.    159347  IN      A       205.251.192.19
ns-854.awsdns-42.net.   159351  IN      A       205.251.195.86
ns-1162.awsdns-17.org.  159345  IN      A       205.251.196.138
ns-1982.awsdns-55.co.uk. 159358 IN      A       205.251.199.190
```

なんで、SOAがroute53のサーバじゃないときがあるんだ?!

※ctm01はbbtower.netの master

NXDOMAINで間違いない。
と、~~ミサカは~~ctm01は答えます。

```
-bash-3.2$ dig hoge.amazone.bbtower.net

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-20.P1.el5_8.6 <<>> hoge.amazone.bbtower.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31601
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;hoge.amazone.bbtower.net.          IN      A

;; AUTHORITY SECTION:
amazone.bbtower.net.       900     IN      SOA     ctm01.bbtower.ad.jp. noc.bbtower.ad.jp.
2013072502 3600 1200 3600000 900
```

aa。 つまりctm01はこのゾーンの権威をもって正々堂々MXDOMAINだと答えている。と。

実は

- bbtower.netの管理担当者に確認してみたところ、実はamazone.bbtower.netはbbtower.netと別ゾーンとして定義して運用している。(つまりゾーンカットして、named.confには、それぞれ別zoneとして記述している。)
- Route53への委譲を示したNSレコードはamazone.bbtower.netのゾーンファイル内に記載している。
- おまけにbbtower.netのゾーン内にはamazone.bbtower.netのNSレコードは登録していない。

つまり、まぁ、こんなです。

BroadBand Tower, Inc.

named.conf(一部)

```
zone "bbtower.net" {
        type master;
        file "master/entry/bbtower.net";
        allow-transfer {
                172.16.0.1 ;
                172.16.0.3 ;
        };
};


zone "amazone.bbtower.net" {
        type master;
        file "master/entry/amazone.bbtower.net";
        allow-transfer {
                172.16.0.1 ;
                172.16.0.3 ;
        };
};
```

named.confの実装依存で設定していた。

bbtower.netのzone (一部)

```
$TTL 1d

@       IN      SOA     ctm01.bbtower.ad.jp. noc.bbtower.ad.jp (
                2013080101; Serial
                3600    ;       refresh
                900     ;       retry
                104800  ;       expire
                7200    ;       min
)

                IN      NS      ns01.bbtower.ad.jp.
                IN      NS      ns03.bbtower.ad.jp.
```

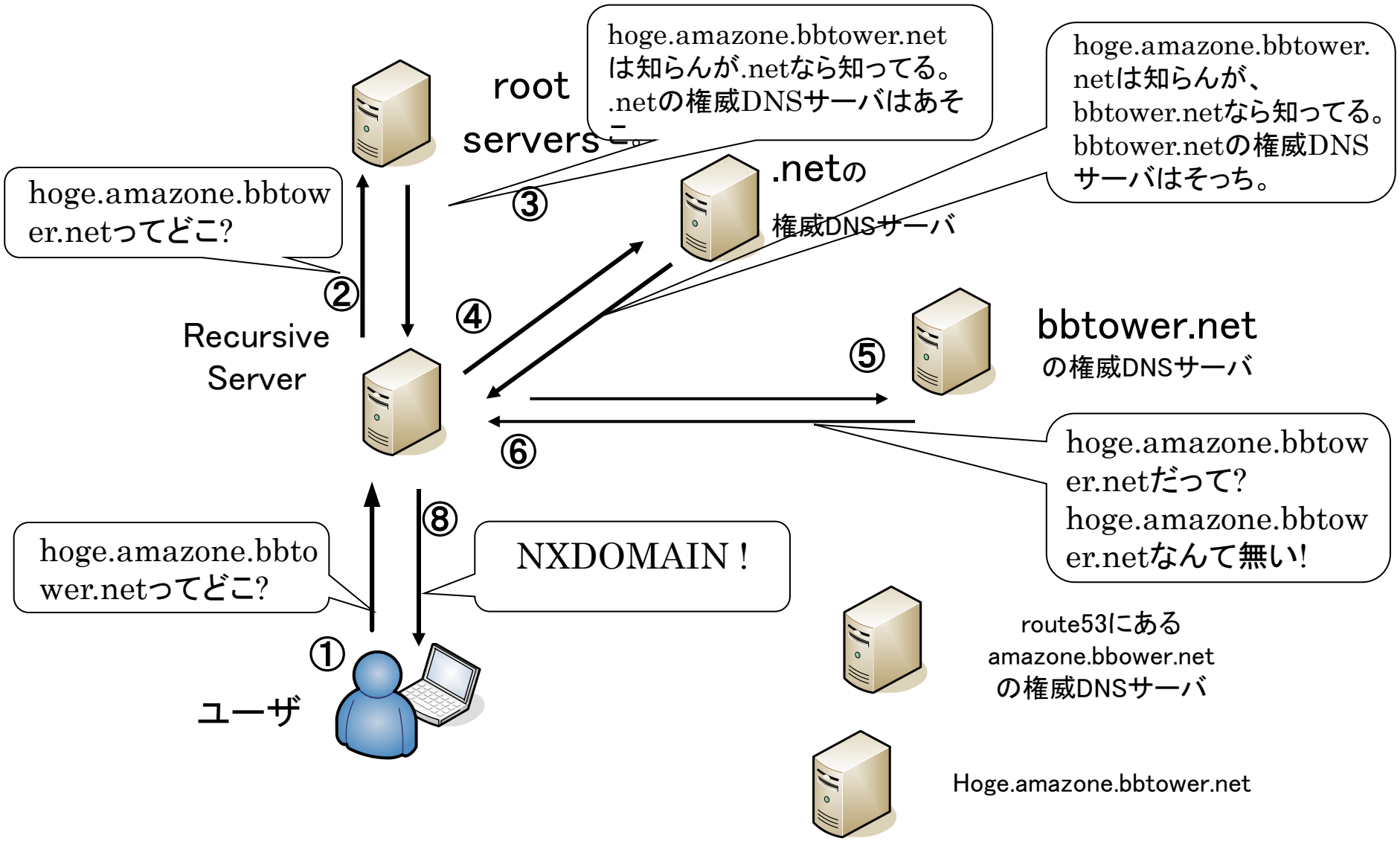
amazone.bbtower.netのzone (一部)

```
$TTL 1d

@       IN      SOA     ctm01.bbtower.ad.jp. noc.bbtower.ad.jp (
                2013080101; Serial
                3600    ;       refresh
                900     ;       retry
                104800  ;       expire
                7200    ;       min
)

amazone   IN      NS      ns-19.awsdns-02.com.
amazone   IN      NS      ns-854.awsdns-42.net.
amazone   IN      NS      ns-1162.awsdns-17.org.
amazone   IN      NS      ns-1982.awsdns-55.co.uk.
```

DNSの名前解決の流れが・・・



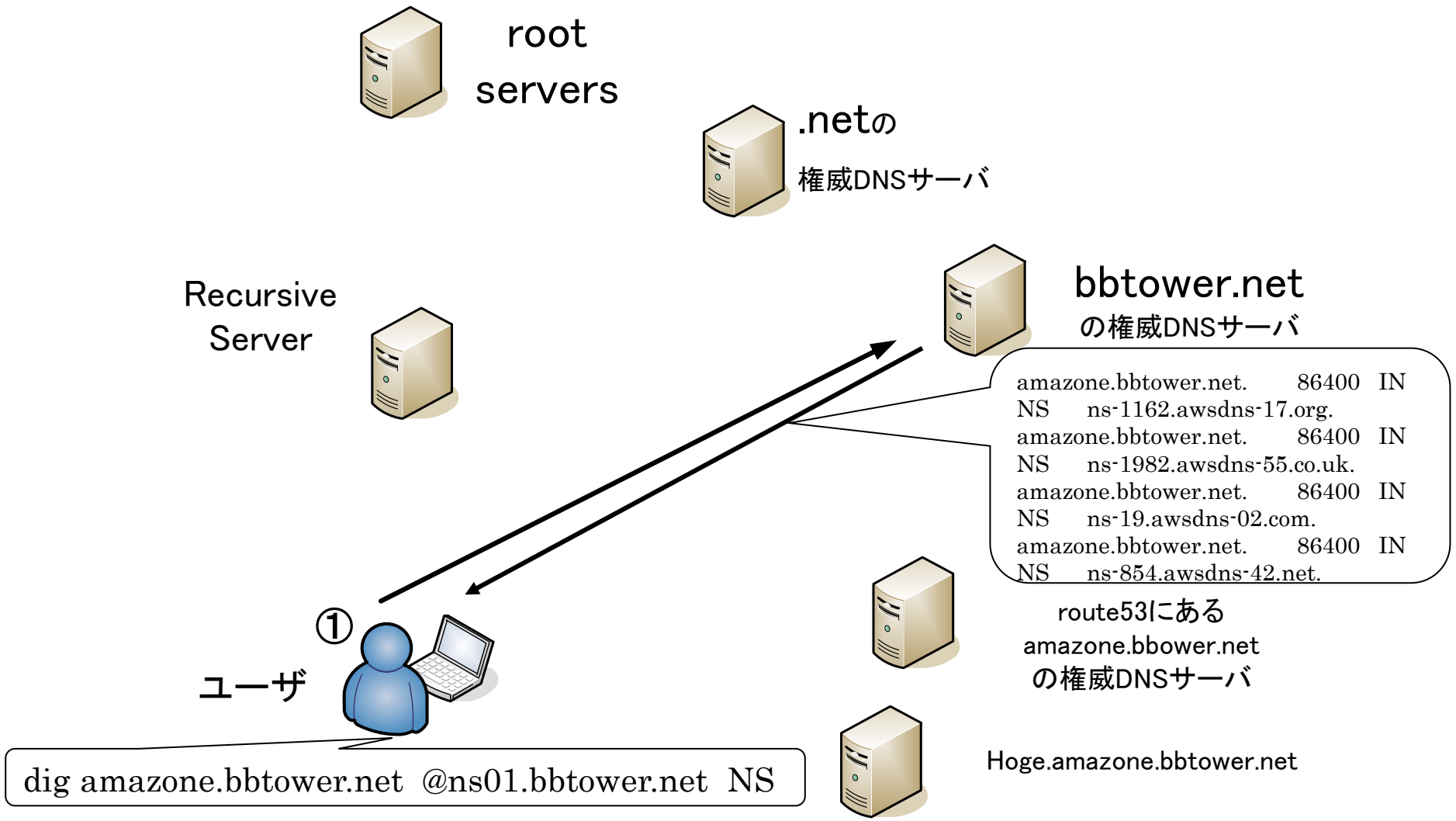
ということで、rootからドメインツリーを順に辿っていくと、bbtower.netを管理しているns0[13].bbtower.ad.jpにクエリが飛んでくるが、bbtower.netゾーンでは”親子の絆”を結んでいない。ので、

「hoge.amazone.bbtower.net?　NXDOMAINじゃ!」

と非再帰問い合わせに答えてしまっていた。

一方でそのamazone.bbtower.netのゾーンを同居して管理していることになっているので、直接ns01.bbtower.netにNSを引くとamazoneのNSを返してくる。

権威DNSサーバにNSを直接問い合わせると・・・



なんでこんなことを・・・?!

BroadBand Tower, Inc.

- 社内検証用ドメインのため、bbtower.netでは各サブドメインに対してwebUIを利用して利用者が任意にRR登録が出来るようになっている。(検証時の頻繁なレコード変更対策)

  このwebUI利用のために指定ドメインを別ゾーンとして切り出して定義することで各サブドメインのゾーンへのアクセス権限をコントロールしていた。

- (ちなみにこのwebUIではNSレコードの登録だけは機能制限しているため、今回は管理者にNSレコード設定をお願いしていた。)

なんで正しい答えが返ってきたり来なかったりしたのか

BroadBand Tower, Inc.

・おそらくリカーシブサーバが route53なNSレコードをキャッシュしていた場合には正しい答えが?
(NSレコードを直接digったりした影響など?)

- 師匠
  「そんなところに隠し子(ゾーン)がおったのか・・・」

- 幽霊ドメイン・親子同居問題・・・・ゾーンにはいろいろありますね☆

- 良い子のみんなも気を付けよう!

おしまい