第５部

特集5 YETI - A Live Root-DNSTestbed

One World, One Internet, One Namespace - Paul Vixie（2014）

加藤 朗

第１章　はじめに

Root DNS Server（以下、Rootサーバと記す）は、木構造の名前空間であるドメイン名の根であるRootに対応したサーバであり、現在インターネットで用いられている名前空間であるドメイン名の解決には必要不可欠なサーバである。実際にはキャッシュを多用して効率を高めているが、基本的な名前解決はRootサーバに問い合わせを送ることからスタートする。そのため、Rootサーバの安定な運用はインターネットの名前解決にとって非常に重要である。殆ど全てのインターネット上のアプリケーションは名前解決に依存しているため、DNSが使えないインターネットは使い物にならないといっても過言ではない。

一方、Rootサーバには、種々の要求があり、それらを実装する場合、既存のDNSを壊さないことを注意深くチェックしていく必要がある。例えば、DNSSECをRoot Zoneに適用する際には、DURZ（deliberately unvalidatable root zone）という手法が使われた[33]。このときは、初期段階では全てのRootサーバがDNSSECに対応していないRoot Zoneを使って運用していたが、徐々にDNSSECで署名済みの、ただし公開鍵を公開しなかったため、署名の検証はできないが、RootZoneを用いるRootサーバを徐々に増やしていった。その際、Rootサーバへの問い合わせデータの計測を実施した。これは、DNSSECで署名したZoneに対応できないfull resolverは、署名されていないRootサーバに再度問い合わせを行うことになるため、それを計測することによって確認する、という手法であった。

一般的には、このような手法を導入するのはコストが大きいが、一方、ラボテストでは、インターネットの一般的な環境ほどの実装のdiversityを得ることは難しい。例えば、DNSのauthoritativeサーバの実証は、主要なもので概ねカバーされるため、その種類はあまり多くないが、Resolver側は、例えば、Home RouterやSecurity Middle Boxなども関係し、それらのversionにも依存するため、ラボテストの結果を以って安全ということはできない。例えば、RootサーバのアドレスにAAAAレコードを追加してIPv6対応にする際、あるベンダのrewall装置が、512byteより大きなUDP応答メッセージを廃棄することが発覚し、問題になったことがある。これは、その装置が比較的ポピュラーだったこと、速やかに修正したsoftwareが配布されたこと、rewall装置のため、このようなupdateを適用することは本質的に重要であるため、短期間で多くの装置が改修されたことから大きな問題にはならなかった。もしこれが、特定の国でしか市販されていないhome routerだったとしたら、その発見は容易ではなかったと想定されるし、対応はさらに困難だったに違いない。

このような状況を考えた場合、ラボテストのみならず、様々な機器ベンターやDNSオペレータが関係するようなテスト環境が必要である。2015年3月に長野市で開催されたWIDE Project合宿で設けられたunconferenceで、Farsight SecurityのPaul Vixie博士、Beijing Internet Instituteの宋林健博士、WIDE Projectからは石原、加藤がこの問題に関して議論を行い、後にYetiと命名されるRootサーバに特化したLive Testbedを運用することで合意した。プロジェクトのWeb Pageとしては、http://www.yeti-dns.org/がある。

> Yeti projectが提供する情報は、基本的にはIANAのRoot ZoneとRoot Apex以外は同一であり、新たなTLDを加えたり、消去したりしていない。つまり、Alternate Rootを目的としたものでは決してない。

第２章　手法

既存のRootサーバに手を入れることはできないため、Rootサーバに代替する環境が必要になる。そのため、既にexpireしているが、"How to scale the DNS root system?" [34]で用いられている方法を応用した。つまり、

1. IANA Root Zoneを入手する
2. Rootサーバのリスト（NSレコード）および全てのRRSIGレコードを削除する[*1]
3. RootのSOAを修正する
4. Yeti ProjectのRootサーバのリストを加える
5. DNSKEYレコードをYeti Projectのものに置き換え、署名する

という方法で変更を加えたものを用いることにした。

Yeti ProjectのResolverは、root.cacheファイルをYeti Projectのものに変更し、また、managed-keysで指定されるRoot Zoneの公開鍵も、IANAのものからYeti Projectのものに変更すればよい。

Yeti Projectでは、Rootノード以外は[*2]IANA Rootのものを使っている。そのため、対応するRRSIGは鍵が異なるため同一ではないが、NSレコードによるdelegationやそのGlueレコードは同じである。従って、上のように設定変更をしたfull resolverは、Yeti Rootサーバが正常に稼働している限り、一般の名前解決を行う上で何の支障もない。そのため、例えば、大学全体や会社全体に対してサービスを提供しているDNS Full ResolverをYeti対応にするのは必ずしも適当ではないが、研究室などの小さな環境のDNS Full ResolverをYeti対応にするのは問題ない。

Operational Live Testbedとしての性格を協調するため、Yeti Projectは、延長する予定までは否定しないが、３年間の、つまり、2018年末までの時限プロジェクトである。

Yeti Projectでは発起人である、BII、TISF[*3]、及びWIDEの３者がプロジェクトのコーディネーションを担っている。概ね２週間に１回程度の電話会議によって運用に関する事項を調整している。

また、Yeti Root Zoneの生成は、この３者が共通のKSKおよびZSKを用いて、IANA Zoneの更新に対応して独立に

```
. 2016010800 1800 900 604800 86400
.                       86400   IN      RRSIG   SOA 8 0 86400 20160207073441 20160108073441 14094 . Rh3HnLw...
.                       518400  IN      NS      bii.dns-lab.net.
.                       518400  IN      NS      yeti.bofh.priv.at.
.                       518400  IN      NS      yeti.ipv6.ernet.in.
.                       518400  IN      NS      yeti.aquaray.com.
.                       518400  IN      NS      dahu1.yeti.eu.org.
.                       518400  IN      NS      dahu2.yeti.eu.org.
.                       518400  IN      NS      ns-yeti.bondis.org.
.                       518400  IN      NS      yeti-ns.ix.ru.
.                       518400  IN      NS      yeti-ns.lab.nic.cl.
.                       518400  IN      NS      yeti-ns.tisf.net.
.                       518400  IN      NS      yeti-ns.wide.ad.jp.
.                       518400  IN      NS      yeti-ns.conit.co.
.                       518400  IN      NS      yeti-ns.switch.ch.
.                       518400  IN      NS      yeti-ns.as59715.net.
.                       518400  IN      NS      yeti-dns01.dnsworkshop.org.
.                       518400  IN      RRSIG   NS 8 0 518400 20160207073441 20160108073441 14094 . DCoRsh7...
.                       86400   IN      NSEC    aaa. NS SOA RRSIG NSEC DNSKEY
.                       86400   IN      RRSIG   NSEC 8 0 86400 20160207073441 20160108073441 14094 . M3zzBG...
.                       86400   IN      DNSKEY  256 3 8 AwEAAde+GDdaG6mBS7KaGWj4rJskKsHOJ7lye5tqBvumVci19Kd...
.                       86400   IN      DNSKEY  256 3 8 AwEAAeMMTHOow6+EE4ZAOnWz3jUx3e76NQDu/5acSTQ2EaMjCWE...
.                       86400   IN      DNSKEY  257 3 8 AwEAAaP3gGQ4db0tAiDEky0dcUNGeI1aTDYP5NFxzhbdpD60ZhK...
.                       86400   IN      RRSIG   DNSKEY 8 0 86400 20160207073441 20160108073441 55954 . DtDS...
```

図2.1　Yeti Root Zone の先頭部分

＊1　IANA Rootサーバのアドレスは.ARPAの委任先に対するglueレコードも兼ねているため、消去しない

＊2　初期の頃は、.ARPAもYeti Projectでホストするような運用をしていたため、NSレコードを書き換えていたが、それはしないことになり、変更は純粋にRootサーバのリストとそのIPアドレスのみとなった。

＊3　Paul Vixieの会社であるFarsight Securityのドメイン名を使うのは適当ではないと判断したため、10年程前に、取得し休眠状態にあったドメイン名をここでは使うことにした。

実施することになった。Yeti ProjectのRootサーバは、表2.1に示すこれらの３つのDistribution Masterからzone dataをAXFRで転送するが、Distribution MasterにおけるIANA Zoneの更新の確認は毎時１回、それぞれ指定された時刻に実施することになっている。なお、Distribution Masterを含め、Yeti RootサーバではIPv6のみサービスをしており、Yeti Rootサーバのアドレスとしては AAAAレコードのみ登録されている。

2015年末時点でのYeti Rootサーバは表2.2に示すように、15台が登録・運用されている。参考のため、ある日のIANA Root Zoneのjp.へのdelegationに関連する部分を図2.2に、同じserialのIANA Root Zoneから生成されたYeti Root Zoneの同じ部分を図2.3に示す。

表2-1　Distribution Master

Operator	IPv6 Address	Offset
BII	240c:f:1:22::7	*hour*+00
WIDE	2001:200:1d9::53	*hour*+20
TISF	2001:559:8000::7	*hour*+40

表2.2 Yeti Rootサーバの一覧

組織	国	サーバ名	IPv6 アドレス
Beijing Internet Institute	CN	bii.dns-lab.net	240c:f:1:22::6
WIDE Project	JP	yeti-ns.wide.ad.jp	2001:200:1d9::35
TISF	US	yeti-ns.tisf.net	2001:559:8000::6
AS59715	IT	yeti-ns.as59715.net	2a02:cdc5:9715:0:185:5:203:53
Dahu Group	FR	dahu1.yeti.eu.org	2001:4b98:dc2:45:216:3eff:fe4b:8c5b
Bond Internet Systems	ES	ns-yeti.bondis.org	2a02:2810:0:405::250
MSK-IX	RU	yeti-ns.ix.ru	2001:6d0:6d06::53
CERT Austria	AT	yeti.bofh.priv.at	2a01:4f8:161:6106:1::10
ERNET India	IN	yeti.ipv6.ernet.in	2001:e30:1c1e:1::333
dnsworkshop/informnis	DE	yeti-dns01.dnsworkshop.org	2001:1608:10:167:32e::53
CONIT S.A.S Colombia	CO	yeti-ns.conit.co	2607:ff28:2:10::47:a010
Dahu Group	FR	dahu2.yeti.eu.org	2001:67c:217c:6::2
Aqua Ray SAS	FR	yeti.aquaray.com	2a02:ec0:200::1
SWITCH	CH	yeti-ns.switch.ch	2001:620:0:ff::29
CHILE NIC	CL	yeti-ns.lab.nic.cl	2001:1398:1:21::8001

```
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
jp.                     172800  IN      NS      c.dns.jp.
jp.                     172800  IN      NS      d.dns.jp.
jp.                     172800  IN      NS      e.dns.jp.
jp.                     172800  IN      NS      f.dns.jp.
jp.                     172800  IN      NS      g.dns.jp.
jp.                     86400   IN      DS      53899 8 1 00DED0BB8203CFB6ABB054318EC95C4F13F4B5B0
jp.                     86400   IN      DS      53899 8 2 C02BA0E5A47E49181EE132BB0612D950766AD9C62FD29BDEE...
jp.                     86400   IN      RRSIG   DS 8 1 86400 20160118170000 20160108160000 54549 . OyTCumjI...
jp.                     86400   IN      NSEC    jprs. NS DS RRSIG NSEC
jp.                     86400   IN      RRSIG   NSEC 8 1 86400 20160118170000 20160108160000 54549 . D2PA4z...
a.dns.jp.               172800  IN      A       203.119.1.1
a.dns.jp.               172800  IN      AAAA    2001:dc4::1
b.dns.jp.               172800  IN      A       202.12.30.131
b.dns.jp.               172800  IN      AAAA    2001:dc2::1
c.dns.jp.               172800  IN      A       156.154.100.5
c.dns.jp.               172800  IN      AAAA    2001:502:ad09::5
d.dns.jp.               172800  IN      A       210.138.175.244
d.dns.jp.               172800  IN      AAAA    2001:240::53
e.dns.jp.               172800  IN      A       192.50.43.53
e.dns.jp.               172800  IN      AAAA    2001:200:c000::35
f.dns.jp.               172800  IN      A       150.100.6.8
f.dns.jp.               172800  IN      AAAA    2001:2f8:0:100::153
g.dns.jp.               172800  IN      A       203.119.40.1
```

図2.2 あるserialのIANA Root Zone（一部）

2015年末の時点で、3つのDistribution Masterが運用され、15台のYeti Rootサーバが稼働している。IPv4アドレスがないため、Yeti Rootサーバ名に関する共通suffixによる圧縮効果があまりないにも関わらず、Yeti Rootサーバに対してpriming queryを送った場合、応答メッセージは881byte（DO bit OFFの場合）および1039byte（DO bit ONの場合）と、あまり大きくない。このlive testbedに関して各種の実験を計画し、実装し、状況を確認するフェーズが2016年の課題である。現在のところ、想定されている実験項目として、以下のようなものが挙げられている：

3.1　Rootサーバの数

Yeti Projectの興味の一つは、Rootサーバの数を、現在のIANA Rootサーバの13より増やした場合に何が起こるか、ということである。IPv4アドレスに関する記述がyeti Rootサーバにはないため、簡単な比較は難しいかも知れないが、一つの基準として、最小の問い合わせ（つまり、priming query: QNAMEが\." でQTYPEがNS）と、最大の問い合わせに関する応答に対して、client環境による問題が発生しないかどうかということである。現在のYeti Rootサーバは15であり、最小の問い合わせに対する応答は881byteあるいは1039byte（DO bitのOFF/ONによる）であるが、サーバ数を更に増やした場合（一台のサーバに複数のアドレスを振り、別名を設けることによって、必ずしもサーバ運用者数を増やす必要はない）、例えば、1232byte（IPv6 default MTUの1280byteからIPv6ヘッダとUDPヘッダを除いたもの）、1432byte（Ethernet MTUの1500byteからIPv6 over IPv4トンネルの分のIPv4ヘッダ、IPv6ヘッダおよびUDPヘッダを除いたもの）、1452byte（Ethernet MTUからIPv6ヘッダおよびUDPヘッダを除いたもの）などの前後での振る舞いを確認する必要がある。

これによって、政治的には必ずしも容易ではないが、IPv6時代になった場合の、Rootサーバの数を増やすことの技術的な裏付けが得られる。

3.2　RootのTrust Anchorの更新

現在のRoot Zoneのtrust anchorは、2010年6月に生成され、同年7月15日から使用が始まったもので、既に５年以上経過している。現在直ちにこれを更新しなければならない事象が発生したわけではないが、長時間同じ鍵を使うことは、実際にその鍵で署名しているのが90日毎に生成されるZSKに対応するDNSKEYレコードの集合（およびKSKに対応するDNSKEYレコード）であるとは言え、

```
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
jp.                     172800  IN      NS      c.dns.jp.
jp.                     172800  IN      NS      d.dns.jp.
jp.                     172800  IN      NS      e.dns.jp.
jp.                     172800  IN      NS      f.dns.jp.
jp.                     172800  IN      NS      g.dns.jp.
jp.                     86400   IN      DS      53899 8 1 00DED0BB8203CFB6ABB054318EC95C4F13F4B5B0
jp.                     86400   IN      DS      53899 8 2 C02BA0E5A47E49181EE132BB0612D950766AD9C62FD29BDEE...
jp.                     86400   IN      RRSIG   DS 8 1 86400 20160207073441 20160108073441 14094 . l/81IcTh...
jp.                     86400   IN      NSEC    jprs. NS DS RRSIG NSEC
jp.                     86400   IN      RRSIG   NSEC 8 1 86400 20160207073441 20160108073441 14094 . BmmHSr...
a.dns.jp.               172800  IN      A       203.119.1.1
a.dns.jp.               172800  IN      AAAA    2001:dc4::1
b.dns.jp.               172800  IN      A       202.12.30.131
b.dns.jp.               172800  IN      AAAA    2001:dc2::1
c.dns.jp.               172800  IN      A       156.154.100.5
c.dns.jp.               172800  IN      AAAA    2001:502:ad09::5
d.dns.jp.               172800  IN      A       210.138.175.244
d.dns.jp.               172800  IN      AAAA    2001:240::53
e.dns.jp.               172800  IN      A       192.50.43.53
e.dns.jp.               172800  IN      AAAA    2001:200:c000::35
f.dns.jp.               172800  IN      A       150.100.6.8
f.dns.jp.               172800  IN      AAAA    2001:2f8:0:100::153
g.dns.jp.               172800  IN      A       203.119.40.1
```

図2.3　図1.2と同じserialのYeti Root Zone（一部）

好ましくはない。Root ZoneのKSKの変更は、RFC5011の "Automated Updates of DNS Security (DNSSEC)Trust Anchors" [35]に規定される方法を用いることにより、自動的にresolver（正確にはvalidator)に反映することができる。しかし、以下のような問題も懸念されている：

・RFC5011をサポートしていない実装を用いている場合
・RFC5011対応の実装だが、マニュアル更新の設定になっている場合
  bind9ではdnssec-enable autoにしないとRFC5011に対応してtrust anchorの自動更新はしない
・新旧２つの鍵が共存している期間（１ヶ月)を超えて落ちているDNS validatorは、鍵の自動更新ができない
・新旧２つの鍵が共存している期間は、パケット長が大きくなる場合があり、rewall等による副作用が発生する

これらを全てYetiで確認することは難しいが、問題が先行して発見できる可能性もある。また、もう一つの課題は、trust anchorの鍵長を現在の2048bitから例えば4096bitに増やすことも検討されており、これらの妥当性をチェックすることも期待されている。

3.3 独立した鍵生成および署名

現在のYeti環境では、３つのDistribution Masterは、共通のKSKおよびZSKを用いて署名している。署名時刻を意図的にずらしているため、それぞれのYeti Root ZoneのRRSIGの値は異なっているが、DNSSECのvalidationは可能である。一つの興味は、仮にKSKは共通だとしても、ZSKをDistribution Master毎に生成し、それぞれのYeti Root Zoneは各々のZSKで署名することである。これは、現在のKSKおよびZSKの生成、それらを用いたRoot Zoneの署名がIANAおよびVeriSignで行われている、いわゆる中央制御方式から、分散化しているという点が特徴であり、大規模災害や戦争などの事象が発生し、鍵の生成や署名が不可能になってしまうことを避けることができる。

第４章　今後の展開

Yeti Projectでは、IANA Root Zoneと同じ情報を、異なったtrust anchorを用いることで、IANA Rootサーバと同じ機能を、IPv6 onlyとは言え、現在15のYeti Rootサーバで提供している。この状態は、実験としてはまだスタート地点に立ったばかりであり、具体的な実験に着手できる準備が整ったに過ぎない。一方、Yeti Projectへの参加は、Yeti Rootサーバという点では一定の広がりを確保することはできたが、実際には、この基盤を利用し、問題を発見する環境が必要である。具体的には、CPEやFirewallなどの装置を開発しているベンダの参加も必要となる。また、このYeti Rootサーバに依存してしまうことは、その信頼性から好ましくない、という感触があるのは自然であるが、例えば、既存のfull resolverと協調し、

1. Full resolverからIANA Rootサーバに関するtrafficをcaptureし、
2. Yeti Rootサーバにも同じ問い合わせを送り、
3. 得られた応答を比較し、差異があった場合には記録・報告する

のような機構を開発することにより、仮にYeti Rootサーバへの到達性が失われたとしても、実際のユーザに影響を及ぼすことはなく、また、実際の問い合わせによってYeti Rootサーバ環境を、場合によってはCPEやFirewall

```
. IN DNSKEY 257 3 8 AwEAAaP3gGQ4db0tAiDEky0dcUNGeI1aTDYP5NFxzhbdpD60ZhKLVV4K
                   yxPmoSNUpq5Fv5M0iBwK1Tyswsyq/9sMSoZ8zx8aT3ho1YnPsSqQeJfj
                   TT1WsX6YZ5Kw6B2QkjRNa60MGZ96Kn8AI/slqsw+z8hY49Sn3baeo9iJ
                   xHPzloNc2dQkW4aLqzNEYxnuoJsthCfGrPSAXlUjY9m3YKIaEWR5WFYQ
                   k770fT+gGWLk/54Vp0sG+Lw75JZnwhDhixPFaToTDNqbHQmkEylq1XJL
                   O15uZ/+RZNRfTXZKO4fVR0tMEbMAITqRmyP8xLXY4RXbS4J32gnenQbz
                   ABX8sQmwO7s=
```

図3.1 Yeti Rootの現在のTrust Anchor

装置を経由して評価することができるのではないかと考えている。

Yeti Projectへの参加は無料である。参加を希望する場合には、coordinators@lists.yeti-dns.orgに電子メールをお送り頂きたい。