

qname色々

Matsuzaki 'maz' Yoshinobu

<maz@ijj.da.jp>

障害切り分けに便利なqname

- ネームサーバの識別
- 問い合わせ元情報
- DNSSECの検証テスト
- これらは概ね各組織の勝手実装であったり、
ネームサーバ設定に依存しているので、挙動や
応答が変わることがあります

ISC BIND由来

- `hostname.bind. CH TXT`
 - ホスト名っぽいものを答える
- `version.bind. CH TXT`
 - 実装のバージョンっぽいものを答える
- 最近は隠すのが流行って来たね
- `hostname`はanycastなノードの判定に便利

例えば噂の9.9.9.9

```
pro2015:~ maz$ dig @9.9.9.9 hostname.bind. txt ch

; <<>> DiG 9.9.7-P3 <<>> @9.9.9.9 hostname.bind. txt ch
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2186
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hostname.bind.                CH      TXT

;; ANSWER SECTION:
hostname.bind.                0      CH      TXT      "res100.qpg.rrdns.pch.net"

;; Query time: 82 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Tue Nov 28 15:13:28 JST 2017
;; MSG SIZE rcvd: 79

pro2015:~ maz$
```

例えば噂の9.9.9.9

```
pro2015:~ maz$ dig @9.9.9.9 version.bind. txt ch

; <<> DiG 9.9.7-P3 <<> @9.9.9.9 version.bind. txt ch
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 6278
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;version.bind.                CH      TXT

;; ANSWER SECTION:
version.bind.                0      CH      TXT      "Q9-U-5.0"

;; Query time: 74 msec
;; SERVER: 9.9.9.9#53(9.9.9.9)
;; WHEN: Tue Nov 28 15:19:05 JST 2017
;; MSG SIZE rcvd: 62

pro2015:~ maz$
```

例えばここの参照用サーバ

```
pro2015:~ maz$ dig hostname.bind. txt ch

; <<> DiG 9.9.7-P3 <<> hostname.bind. txt ch
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 21524
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;hostname.bind.                CH      TXT

;; ANSWER SECTION:
hostname.bind.                0      CH      TXT      "dns"

;; Query time: 42 msec
;; SERVER: 2001:dc2:cafe:1::11#53(2001:dc2:cafe:1::11)
;; WHEN: Tue Nov 28 15:17:38 JST 2017
;; MSG SIZE rcvd: 58

pro2015:~ maz$
```

例えばこここの参照用サーバ

```
pro2015:~ maz$ dig version.bind. txt ch

; <<>> DiG 9.9.7-P3 <<>> version.bind. txt ch
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6364
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;version.bind.                CH      TXT

;; ANSWER SECTION:
version.bind.                0      CH      TXT      "unbound 1.5.8"

;; Query time: 41 msec
;; SERVER: 2001:dc2:cafe:1::11#53(2001:dc2:cafe:1::11)
;; WHEN: Tue Nov 28 15:18:07 JST 2017
;; MSG SIZE rcvd: 67

pro2015:~ maz$
```

RFC4892的qname

- id.server. CH TXT
 - ネームサーバを特定するための文字列を答える

例えば1.2.4.8

10.20.5.0/24だと外側？ 10.20.8.0/24だと内側？

```
pro2015:~ maz$ dig @1.2.4.8 id.server. txt ch

; <<> DiG 9.9.7-P3 <<> @1.2.4.8 id.server. txt ch
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 11094
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;id.server.                CH      TXT

;; ANSWER SECTION:
id.server.                0      CH      TXT      "10.20.5.34"

;; Query time: 60 msec
;; SERVER: 1.2.4.8#53(1.2.4.8)
;; WHEN: Tue Nov 28 15:20:42 JST 2017
;; MSG SIZE rcvd: 61

pro2015:~ maz$
```

l.root-servers.netでの取り組み

- identity.l.root-servers.org. IN txt
- identity.l.root-servers.org. IN A
- おまけ
 - RFC5001的NSID

```
[pro2015:~ maz$ dig +nsid @l.root-servers.net
; <<> DiG 9.9.7-P3 <<> +nsid @l.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 22392
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; NSID: 6c 61 78 35 36 2e 6c 2e 72 6f 6f 74 2d 73 65 72 76 65 72 73 2e 6f 72 67
(1) (a) (x) (5) (6) (.) (1) (.) (r) (o) (o) (t) (-) (s) (e) (r) (v) (e) (r) (s)
(.) (o) (r) (g)
;; QUESTION SECTION:
; .                               IN      NS

;; ANSWER SECTION:
.                               518400 IN     NS     a.root-servers.net.
.                               518400 IN     NS     b.root-servers.net.
.                               518400 IN     NS     c.root-servers.net.
.                               518400 IN     NS     d.root-servers.net.
.                               518400 IN     NS     e.root-servers.net.
```

問い合わせ元情報

- 権威サーバで見えた情報
 - 参照しているフルリゾルバのIPアドレス
 - あればedns0-client-subnetの情報
- whoami.akamai.com. IN A
 - IPv4のみ
- o-o.myaddr.l.google.com. IN TXT
 - IPv4/IPv6, ecs対応
- maxmind.test-ipv6.com. IN TXT
 - さらに追加の情報を表示

例えばこここの参照用サーバ

```
pro2015:~ maz$ dig whoami.akamai.com. a in

; <<> DiG 9.9.7-P3 <<> whoami.akamai.com. a in
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 45616
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;whoami.akamai.com.      IN      A

;; ANSWER SECTION:
whoami.akamai.com.      244     IN      CNAME   whoami.akamai.net.
whoami.akamai.net.     170     IN      A       74.125.41.11

;; Query time: 42 msec
;; SERVER: 2001:dc2:cafe:1::11#53(2001:dc2:cafe:1::11)
;; WHEN: Tue Nov 28 16:48:47 JST 2017
;; MSG SIZE rcvd: 93

pro2015:~ maz$
```

例えばここの参照用サーバ

```
pro2015:~ maz$ dig o-o.myaddr.l.google.com. IN TXT

; <<> DiG 9.9.7-P3 <<> o-o.myaddr.l.google.com. IN TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27778
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;o-o.myaddr.l.google.com.      IN      TXT

;; ANSWER SECTION:
o-o.myaddr.l.google.com. 59      IN      TXT      "173.194.93.12"
o-o.myaddr.l.google.com. 59      IN      TXT      "edns0-client-subnet 118.6.228.109/32"

;; Query time: 45 msec
;; SERVER: 2001:dc2:cafe:1::11#53(2001:dc2:cafe:1::11)
;; WHEN: Tue Nov 28 16:47:40 JST 2017
;; MSG SIZE rcvd: 127

[pro2015:~ maz$
```

例えばこここの参照用サーバ

```
~ — -bash — 80x24
[pro2015:~ maz$ dig maxmind.test-ipv6.com txt in ]
; <<> DiG 9.9.7-P3 <<> maxmind.test-ipv6.com txt in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 23745
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

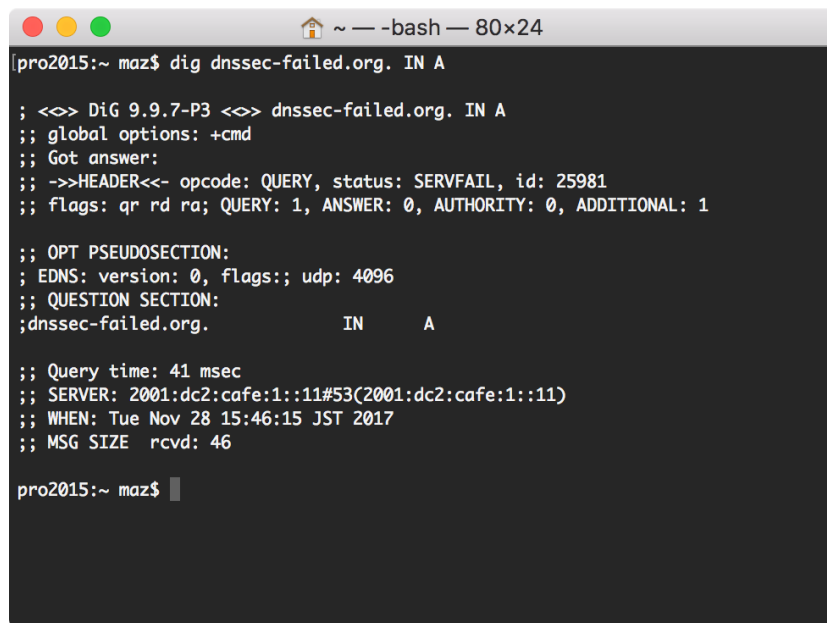
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;maxmind.test-ipv6.com.      IN      TXT

;; ANSWER SECTION:
maxmind.test-ipv6.com.  0      IN      TXT      "ip='172.217.42.11' as='15169' i
sp='Google LLC' country='US'"
maxmind.test-ipv6.com.  0      IN      TXT      "ip='118.6.228.0' as='4713' isp=
'Open Computer Network' country='JP'"

;; Query time: 583 msec
;; SERVER: 2001:dc2:cafe:1::11#53(2001:dc2:cafe:1::11)
;; WHEN: Tue Nov 28 15:42:24 JST 2017
;; MSG SIZE rcvd: 202
```

DNSSEC検証の確認

- dnssec-failed.org. IN A
 - DNSSEC検証が失敗するはず
 - SERVFAILが得られないと、そもそもDNSSEC検証していないか、何か設定間違い



```
pro2015:~ maz$ dig dnssec-failed.org. IN A

;<> DiG 9.9.7-P3 <> dnssec-failed.org. IN A
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: SERVFAIL, id: 25981
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

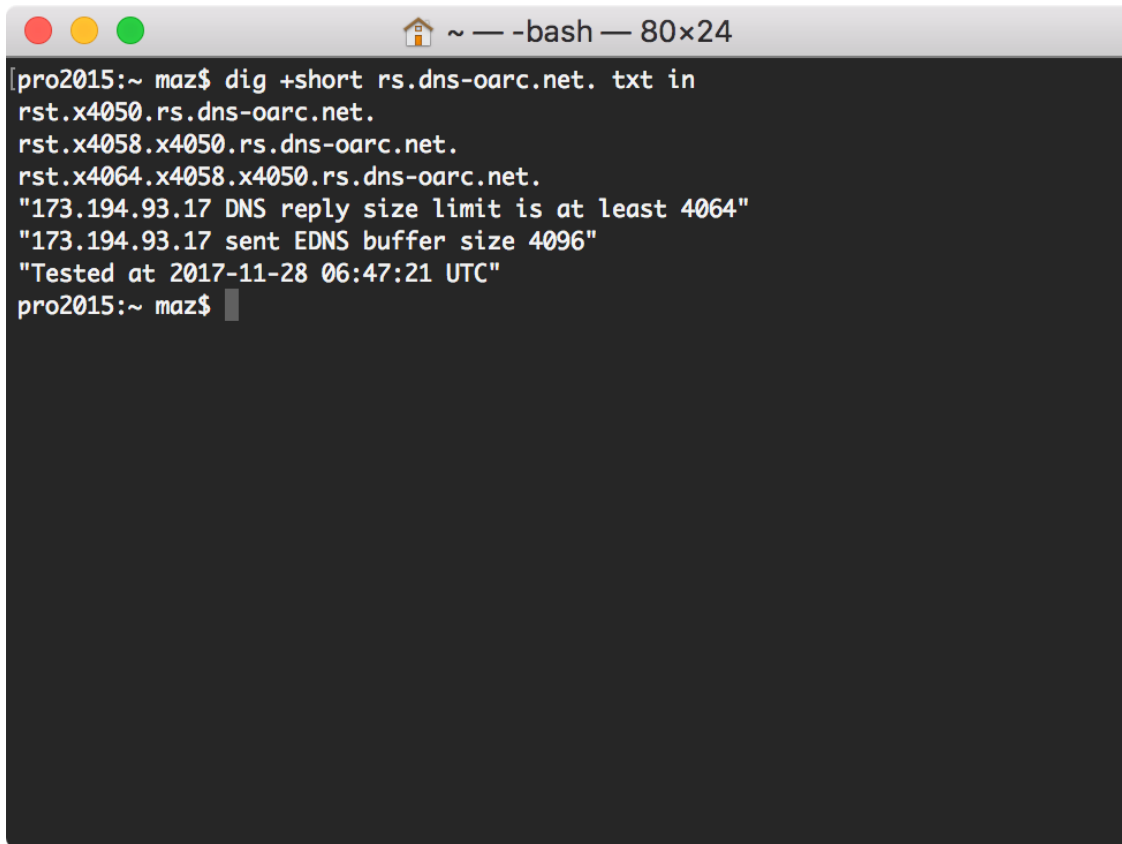
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnssec-failed.org.          IN      A

;; Query time: 41 msec
;; SERVER: 2001:dc2:cafe:1::11#53(2001:dc2:cafe:1::11)
;; WHEN: Tue Nov 28 15:46:15 JST 2017
;; MSG SIZE rcvd: 46

pro2015:~ maz$
```

受け入れ可能な応答サイズ確認

- rs.dns-oarc.net. IN TXT



```
pro2015:~ maz$ dig +short rs.dns-oarc.net. txt in  
rst.x4050.rs.dns-oarc.net.  
rst.x4058.x4050.rs.dns-oarc.net.  
rst.x4064.x4058.x4050.rs.dns-oarc.net.  
"173.194.93.17 DNS reply size limit is at least 4064"  
"173.194.93.17 sent EDNS buffer size 4096"  
"Tested at 2017-11-28 06:47:21 UTC"  
pro2015:~ maz$
```


Google Public DNS用

- `locations.publicdns.goog. IN TXT`
 - Google Public DNSのネームサーバ群で利用しているIPアドレスブロック
- `test.dns.google.com. IN TXT`
 - Google Public DNSのみが応答するレコードで、“Thanks for using Google Public DNS.”が期待される

OpenDNS用

- debug.opendns.com. IN TXT

```
pro2015:~ maz$ dig debug.opendns.com txt @208.67.220.220

; <<>> DiG 9.9.7-P3 <<>> debug.opendns.com txt @208.67.220.220
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7145
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
debug.opendns.com.          IN      TXT

[;; ANSWER SECTION:
[debug.opendns.com.        0      IN      TXT      "server m37.nrt"
[debug.opendns.com.        0      IN      TXT      "flags 20 0 70 79508000000000000000"
[debug.opendns.com.        0      IN      TXT      "originid 0"
debug.opendns.com.        0      IN      TXT      "actype 0"
debug.opendns.com.        0      IN      TXT      "source 118.6.228.109:36899"

;; Query time: 41 msec
;; SERVER: 208.67.220.220#53(208.67.220.220)
;; WHEN: Tue Nov 28 15:54:12 JST 2017
;; MSG SIZE rcvd: 202
```

まとめ

- 便利なqname色々あります
- 障害切り分け時に便利
- これらは概ね各組織の勝手実装であったり、
ネームサーバ設定に依存しているので、挙動や
応答が変わることがあります