夏のDNS祭り 2014　2014-07-05

ハンズオン - dig編

株式会社ハートビーツ 滝澤 隆史

注意事項

- 教材として会場を提供していただいているConoHaさんのドメイン名とその権威ネームサーバを使用しています。
  - www.conoha.jp
  - conoha.jp
  - ns1.gmointernet.jp

権威ネームサーバへの問い合わせ

- 「@権威サーバ」と「+norec」を付ける
- 例) www.conoha.jpのAレコードを調べる。

```
$ dig @ns1.gmointernet.jp. www.conoha.jp. A +norec
```

権威ネームサーバへの問い合わせ

$ dig @ns1.gmointernet.jp. www.conoha.jp. A +norec
中略

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52740
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.conoha.jp.                 IN      A

;; ANSWER SECTION:
www.conoha.jp.          60      IN      A       157.7.143.77
www.conoha.jp.          60      IN      A       157.7.143.78

;; AUTHORITY SECTION:
conoha.jp.              86400   IN      NS      ns1.gmointernet.com.
conoha.jp.              86400   IN      NS      ns1.gmointernet.jp.

;; Query time: 1 msec
;; SERVER: 2400:8500:3fff::254#53(2400:8500:3fff::254)
;; WHEN: Thu Jul  3 21:17:12 2014
;; MSG SIZE  rcvd: 126
```

フルサービスリゾルバへの問い合わせ

- 「@フルサービスリゾルバ」と「+rec」を付ける。
- 「@フルサービスリゾルバ」を省略するとホストのリゾルバ（/etc/resolv.conf）が使用される。
- 「+rec」はデフォルトなので省略可能。
- 例）

```
$ dig @8.8.8.8 www.conoha.jp. A
```

フルサービスリゾルバへの問い合わせ

```
$ dig @8.8.8.8 www.conoha.jp. A
中略
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6342
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.conoha.jp.                 IN      A

;; ANSWER SECTION:
www.conoha.jp.          59      IN      A       157.7.143.77
www.conoha.jp.          59      IN      A       157.7.143.78

;; Query time: 115 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Jul  3 21:32:24 2014
;; MSG SIZE  rcvd: 63
```

+multiline

- RDATAが長いときには複数行の形式にして表示してくれる。
- 「+multiline」なしの場合の例

```
$ dig @ns1.gmointernet.jp. conoha.jp. SOA +norec
;; ANSWER SECTION:
conoha.jp.      86400   IN      SOA     ns1.gmointernet.com.
hostmaster.gmointernet.com. 2014012105 3600 300 3600000 7200
```

- 「+multiline」ありの場合の例

```
$ dig @ns1.gmointernet.jp. conoha.jp. SOA +norec +multiline
;; ANSWER SECTION:
conoha.jp.      86400 IN SOA ns1.gmointernet.com.
hostmaster.gmointernet.com. (
                        2014012105 ; serial
                        3600       ; refresh (1 hour)
                        300        ; retry (5 minutes)
                        3600000    ; expire (5 weeks 6 days 16 hours)
                        7200       ; minimum (2 hours)
                        )
```

-x

- 逆引きを行う。
- 例）www.conoha.jpを正引きすると157.7.143.77なので、その逆引きを行ってみる。

```
$ dig -x 157.7.143.77
中略
;; QUESTION SECTION:
;77.143.7.157.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
77.143.7.157.in-addr.arpa. 300  IN      PTR     v157-7-143-77.myvps.jp.
```

-4, -6

- 「-4」はIPv4のトランスポートを使う。
- 「-6」はIPv6のトランスポートを使う。
- IPv4の例）

```
$ dig @ns1.gmointernet.jp. -4 www.conoha.jp. A +norec
中略
;; Query time: 1 msec
;; SERVER: 157.7.33.254#53(157.7.33.254)
;; WHEN: Thu Jul  3 22:12:33 2014
;; MSG SIZE  rcvd: 126
```

- IPv6の例）

```
$ dig @ns1.gmointernet.jp. -6 www.conoha.jp. A +norec
中略
;; Query time: 2 msec
;; SERVER: 2400:8500:3fff::254#53(2400:8500:3fff::254)
;; WHEN: Thu Jul  3 22:14:32 2014
;; MSG SIZE  rcvd: 214
```

+tcp

- TCPで問い合わせを行う
- TCPでのトランスポートができるか確認する際に使用する。
- 失敗例（IPv6のTCPのポートが開いていない）

```
$ dig @ns1.gmointernet.jp. -6 www.conoha.jp. A +norec +tcp
;; communications error to 2400:8500:3fff::254#53: connection reset
;; communications error to 2400:8500:3fff::254#53: connection reset
;; communications error to 2400:8500:3fff::254#53: connection reset

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.23.rc1.el6_5.1 <<>>
@ns1.gmointernet.jp. www.conoha.jp. A +norec +tcp
; (2 servers found)
;; global options: +cmd
```

セグメンテーション違反です（コアダンプ）

+trace

- rootネームサーバから委任パスを追跡する。
- 委任パスが切れていないかの確認ができる。
- 例）

```
$ dig @m.root-servers.net. www.conoha.jp. A +trace
```

+trace

```
$ dig @m.root-servers.net. www.conoha.jp. A +trace
中略
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
;; Received 492 bytes from 2001:dc3::35#53(2001:dc3::35) in 149 ms
中略
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
;; Received 427 bytes from 192.36.148.17#53(192.36.148.17) in 9 ms

conoha.jp.              86400   IN      NS      ns1.gmointernet.com.
conoha.jp.              86400   IN      NS      ns1.gmointernet.jp.
;; Received 138 bytes from 2001:dc4::1#53(2001:dc4::1) in 3 ms

www.conoha.jp.          60      IN      A       157.7.143.77
www.conoha.jp.          60      IN      A       157.7.143.78
conoha.jp.              86400   IN      NS      ns1.gmointernet.com.
conoha.jp.              86400   IN      NS      ns1.gmointernet.jp.
;; Received 126 bytes from 2400:8500:3fff::254#53(2400:8500:3fff::254) in
1 ms
```

+nssearch

- 指定したゾーンの権威サーバを調べて、それぞれの権威サーバに登録されているSOAレコードを表示する。
  - シリアル値を確認することでゾーン転送の失敗の検出などに利用
- 例）

```
$ dig conoha.jp. +nssearch
SOA ns1.gmointernet.com. hostmaster.gmointernet.com. 2014012105 3600 300
3600000 7200 from server 157.7.33.254 in 14 ms.
SOA ns1.gmointernet.com. hostmaster.gmointernet.com. 2014012105 3600 300
3600000 7200 from server 2400:8500:3fff::254 in 15 ms.
SOA ns1.gmointernet.com. hostmaster.gmointernet.com. 2014012105 3600 300
3600000 7200 from server 157.7.32.254 in 15 ms.
SOA ns1.gmointernet.com. hostmaster.gmointernet.com. 2014012105 3600 300
3600000 7200 from server 2400:8500:3000::254 in 15 ms.
```

+dnssec

- DNSSECの検証の要求を行う。
  - DNSSECの検証に対応したフルサービスリゾルバに対して行う。
- 例)

```
$ dig @8.8.8.8 jp. SOA +dnssec +multiline
```

+dnssec

```
$ dig @8.8.8.8 jp. SOA +dnssec +multiline
中略
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56562
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
中略
;; QUESTION SECTION:
;jp.                    IN SOA

;; ANSWER SECTION:
jp.                    21599 IN SOA z.dns.jp. root.dns.jp. (
                             1404396902 ; serial
                             3600       ; refresh (1 hour)
                             900        ; retry (15 minutes)
                             1814400    ; expire (3 weeks)
                             900        ; minimum (15 minutes)
                             )
jp.                    21599 IN RRSIG SOA 8 1 86400 20140728174502 (
                             20140628174502 62433 jp.
                             S0088kT/On3O/u6J68eLecOYqQSzkbV5Jlv2+buTmx9j
                             /w+jcab7HazhEfCiaphp6UshASRfBnaOFdc7oKF8Q/7Q
                             SZW3cBbg0nqGoX1EtybpvgB58l5+OMl1m8I0R2uTCfNd
                             9Of47MJH1JBI9DJwj558vZx385nYGfejzRKOtPE= )
```

おわり