あたらしい dig

アカマイ・テクノロジーズ合同会社
シニア・ソリューションズエンジニア
松本 陽一

発表 2023 年 6 月 23 日
資料(修正) 2023 年 6 月 26 日

このプレゼンテーションにおいてなされる記述は作成者個人の見解を示すものであり、アカマイ・テクノロジーズの見解を示すものではありません。提供される情報は作成時点において正確なものであると考えておりますが、当該情報についてなんら表明又は保証を行いません。

いきなりですが、ごめんなさい (>_<)

- 「次世代の dig 」とかいう話ではありません
- dig の最新機能の解説でもありません

dig

- DNS のふるまいを表現する事実上の標準語
  - みんなが知っている
  - 多くの環境でデフォルトで用意されている

- 一方で、気になる点も…
  - 自分がどんなクエリを出しているのかがわかりにくい
  - デフォルト動作がわかりにくい

  (デフォルト動作に開発者の思いが反映されている？)

話が通じない例

A:「dig でエラーが返ってくるんですけど。」

B:「ちゃんとアンサー返ってきますが。」

↓

- A と B の使っている dig のバージョンが違った
  (dig は 9.11.0 あたりからデフォルトで DNS cookie をつけるようになった。)
- このネームサーバは未知の EDNS オプションを受け取ると FORMERR を返していた

dig の開発者は DNS cookie を普及させたい？

クエリに cookie がついていたことは コマンド出力からは分からない

```
% dig @XXX.XX.XXX.XX example.com +norecurse

; <<>> DiG 9.18.15 <<>> @XXX.XX.XXX.XX example.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44953
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
example.com.                    86400      IN        A
           XX.XXX.XXX.XX

;; Query time: 121 msec
;; SERVER: XXX.XX.XXX.XX#53(XXX.XX.XXX.XX) (UDP)
;; WHEN: Sun Jun 18 12:00:00 JST 2023
;; MSG SIZE  rcvd: 56

%
```

(サーバが cookie に対応しておらず) レスポンスに cookie がない場合、クエリに cookie があったことに気づけない

```
% dig @XXX.XX.XXX.XX example.com +norecurse +qr

; <<>> DiG 9.18.15 <<>> @XXX.XX.XXX.XX example.com +norecurse +qr
; (1 server found)
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25308
;; flags: ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4010bedff8bdfc31
;; QUESTION SECTION:
;example.com.                                   IN          A

;; QUERY SIZE: 52

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25308
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
example.com.            86400       IN          A           XX.XXX.XXX.XX

(以下略)
```

+qr オプション

クエリも表示するオプション

(QR ビットの指定ではない)

あれ？という例

```
% dig @X.X.X.X XXXX.XXX ANY +noanswer

; <<>> DiG 9.16.41 <<>> @X.X.X.X XXXX.XXX ANY +noanswer
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31887
;; flags: qr rd ra; QUERY: 1, ANSWER: 40, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;XXXX.XXX.                              IN      ANY

;; Query time: 1 msec
;; SERVER: X.X.X.X#53(X.X.X.X)
;; WHEN: Sun Jun 18 12:00:00 JST 2023
;; MSG SIZE  rcvd: 3800

%
```

レスポンス・メッセージ・サイズが大きいと Truncate (TC=1)が返ってくるんじゃなかったっけ？

ANY クエリでは TCP がデフォルト

```
+tcp, +notcp
       This option indicates whether to use TCP when querying name
       servers.  The default behavior is to use UDP unless a type any or
       ixfr=N query is requested, in which case the default is TCP. AXFR
       queries always use TCP. To prevent retry over TCP when TC=1 is
       returned from a UDP query, use +ignore.
```

- クエリタイプ ANY のときは TCP がデフォルト
- +ignore をつけないと TC=1 が返るとTCP で再試行

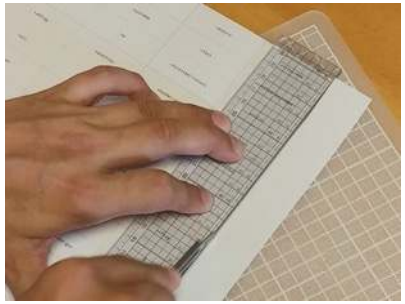
Truncate (TC=1) のレスポンスを確認するには +notcp と +ignore をつける必要があった。

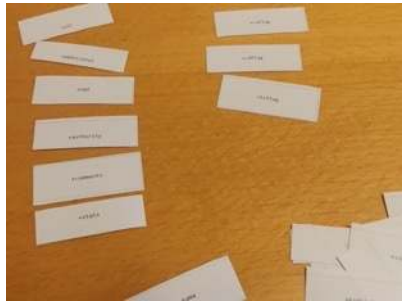
dig のコマンドライン・オプションは全部おさえておきたいなぁ

man ページを見ると…

```
BUGS
       There are probably too many query options.
```

しかもアルファベット順…。わかりやすく整理したい！

dig のコマンドライン・オプションを整理

バージョン 9.18.15

man ページまたは dig -h で列挙されるオプション (-X / +XXX / @)

[no] は省略

- トランスポート (L3 / L4 / DoH / DoT)
- 再送、タイムアウト、フォールバック
- クエリの内容の指定 (一般 / TSIG / EDNS / 特殊な指定の仕方)
- 表示
- その他

トランスポート等

L3 / L4

```
-4
-6
@server
-p port
-b address[#port]
+tcp / +vc
+keepopen
```

DoH / DoT

```
+https[=###] /
+https-post[=###]
+https-get[=###]
+http[=###] /
+http-post[=###]
+http-get[=###]
+tls
+tls-hostname=hostname
+tls-ca[=###]
+tls-certfile=file
+tls-keyfile=file
```

再送 / タイムアウト / フォールバック

```
+tries=###
+retry=###
+timeout=###
+ignore
+fail
```

クエリの内容 (一般 / TSIG)

一般

```
+qid=###
+opcode=###

+aaflag / +aaonly
+tcflag
+rdflag / +recurse
+raflag
+zflag
+adflag
+cdflag
```

```
+header-only

-q name
-t type
-c class
```

TSIG

```
-k keyfile
-y
[hmac:]keyname:secret
+fuzztime[=###]
```

クエリの内容（EDNS / 特殊な指定）

EDNS

```
+bufsize[=###]
+edns[=###]
  +ednsnegotiation
+do / +dnssec
+ednsflags[=#]
```

オプション

```
+nsid (3)
+subnet=addr[/prefix-
length] (8)
+expire (9)
+cookie[=####] (10)
  +badcookie
  +showbadcookie
+keepalive (11)
+padding (12)
+dnsopt[=code[:value]]
```

特殊な指定のしかた

```
-f file
+domain=###
+search / +defname
+ndots=###
-x addr
+dns64prefix
```

表示

部分の選択

```
+all
+cmd
+comments
+question
+answer
+authority
+additional
+stats
```

フォーマットの選択

```
-u
+ttiunits
+expandaaaa
+unknownformat
+multiline
+split=##
+crypto
```

その他

```
+qr
+showsearch
+ttlid
+class
+rrcomments
+onesoa
+besteffort
```

表示全体の形式を変更

```
+short
  +identify
+yaml
```

その他

国際化ドメイン(IDN)

```
+idnin
+idnout
```

その他

```
-v
-h
-r
-m
```

Obsolete (効果なし)

```
+sigchase
+topdown
+trusted-key=###
+dscp[=###]
```

特別な動作(一連の複数種類のクエリ)

```
+trace
+nssearch
```

「あたらしい」こと？

9.18.0 のリリースノートより

「dig output now includes the transport protocol used (UDP, TCP, TLS, HTTPS).」

```
;; Query time: 1 msec
;; SERVER: X.X.X.X#53(X.X.X.X) TCP
;; WHEN: Sun Jun 18 12:00:00 JST 2023
;; MSG SIZE  rcvd: 3800
```

前述の「あれ？」に関しても、9.18.0 以降ならTCP でのレスポンスが表示されていることに気づけたかも

まとめ


Akamai