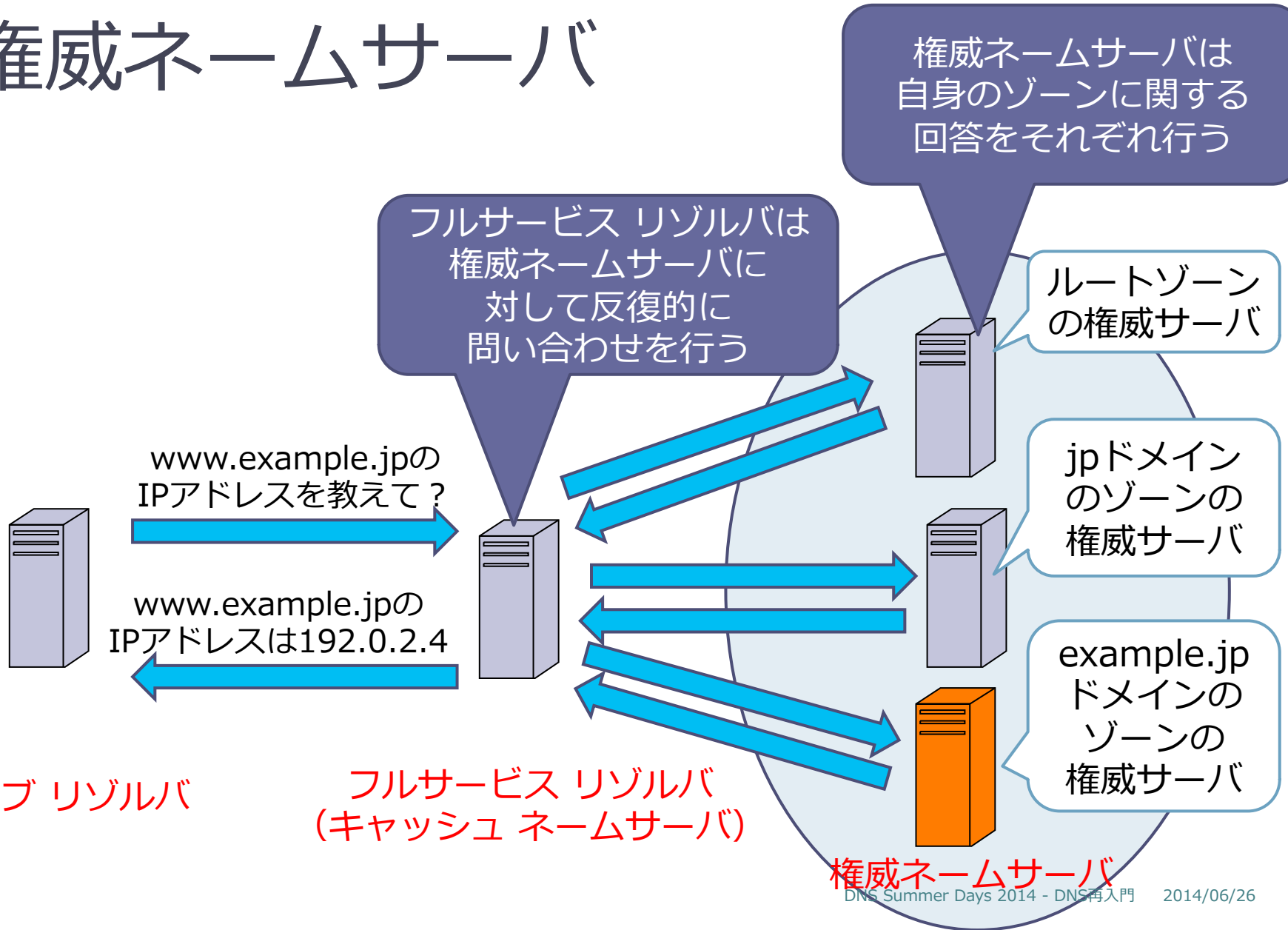
夏のDNS祭り 2014　2014-07-05

ハンズオン – NSD編

株式会社ハートビーツ 滝澤 隆史

権威ネームサーバ


権威ネームサーバは
自身のゾーンに関する
回答をそれぞれ行う
フルサービス リゾルバは
権威ネームサーバに
対して反復的に
問い合わせを行う
ルートゾーン
の権威サーバ
www.example.jpの
IPアドレスを教えて？
jpドメイン
のゾーンの
権威サーバ
www.example.jpの
IPアドレスは192.0.2.4
example.jp
ドメインの
ゾーンの
権威サーバ
スタブ リゾルバ
フルサービス リゾルバ
(キャッシュ ネームサーバ)
権威ネームサーバ

NSD 4のインストール

NSD 4のインストール

- NSD 4のRPMパッケージは提供されていない。
- このハンズオンではスピーカーが作ったRPMパッケージを利用する。

```
$ wget http://www.sub.emaillab.jp/
nsd-4.0.3-1.el6.x86_64.rpm
$ sudo rpm -ivh nsd-4.0.3-1.el6.x86_64.rpm
```

nsd-controlの準備

- nsd-control用の公開鍵証明書とプライベート鍵のペアの作成

```
$ cd /etc/nsd
$ sudo nsd-control-setup
$ sudo chgrp nsd nsd_*.{key,pem}
$ ls -l nsd_*.{key,pem}
-rw-r----- 1 root nsd 1281  7月 4 21:49 2014 nsd_control.key
-rw-r----- 1 root nsd  790  7月 4 21:49 2014 nsd_control.pem
-rw-r----- 1 root nsd 1281  7月 4 21:49 2014 nsd_server.key
-rw-r----- 1 root nsd  782  7月 4 21:49 2014 nsd_server.pem
```

ディレクトリの作成

- ゾーンファイル配置用のディレクトリの作成

```
$ sudo mkdir /etc/nsd/primary
$ sudo mkdir /etc/nsd/secondary
$ sudo chown nsd:nsd /etc/nsd/secondary
```

NSDの設定

- 設定ファイルのディレクトリに移動

```
$ cd /etc/nsd
```

- インストール時の設定をバックアップ

```
$ sudo cp -p nsd.conf{,.orig}
```

- 設定の確認

```
$ sed '/^.*#/ d;/^$/ d' nsd.conf
```

設定ファイルの編集

```
$ sudo vim /etc/nsd/nsd.conf
server:
        ip-address: 192.0.2.1
        ip-address: 2001:db8:dead:beef::53
remote-control:
        control-enable: yes

$ sudo sudo nsd-checkconf /etc/nsd/nsd.conf
```

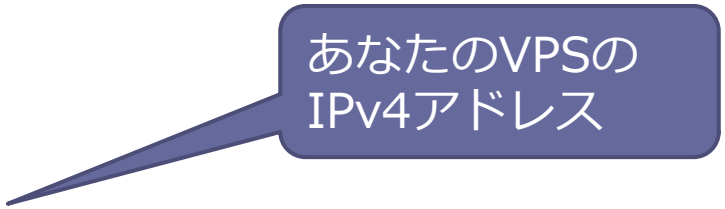
あなたのVPSのIPv4アドレスとIPv6アドレスを記述

nsd-controlによる制御を有効にする。

設定ファイルのチェック

nsdの起動

```
$ sudo nsd-control start
$ ps axf | grep [n]sd
23398 ?    Ss    0:00 nsd -c /etc/nsd/nsd.conf
23399 ?    S     0:00  \_ nsd -c /etc/nsd/nsd.conf
23400 ?    S     0:00      \_ nsd -c /etc/nsd/nsd.conf
$ sudo nsd-control status
version: 4.0.3
verbosity: 0
ratelimit: 200
$ dig @192.0.2.1 version.server. CH TXT +norec
;; ANSWER SECTION:
version.server.   0     CH    TXT   "NSD 4.0.3"
```



ゾーンファイルの作成

- ゾーン名とIPアドレスの確認
  - http://goo.gl/hYHd5U
- 例）
  - あなたのゾーンのラベル: s01
  - 隣の人のゾーンのラベル: s02
  - あなたのIPアドレス: 192.0.2.1
  - 隣の人のIPアドレス: 192.0.2.2
  - マスター:
    - ゾーン名: s01.sub.emaillab.jp
    - ネームサーバ: ns1.s01.sub.emaillab.jp. (192.0.2.1)
  - スレーブ:
    - ゾーン名: s02.sub.emaillab.jp
    - ネームサーバ: ns2.s02.sub.emaillab.jp. (192.0.2.2)

ゾーンファイルの例

```
$TTL    300
@       IN   SOA ns1.s01.sub.emaillab.jp. root.emaillab.jp.  (
                    2014070501      ; Serial
                    3600    ; Refresh
                    900     ; Retry
                    604800  ; Expire
                    300 )   ; Minimum
@       IN   NS   ns1.s01.sub.emaillab.jp.
@       IN   NS   ns2.s01.sub.emaillab.jp.
ns1     IN   A    192.0.2.1
ns2     IN   A    192.0.2.2

www     IN   A    157.7.234.43
```

動作確認が取れるまでは
TTLは小さい値にしておく。

マスターの
権威ネームサーバ

マスターの
権威ネームサーバ

スレーブの
権威ネームサーバ

マスターの
IPv4アドレス

スレーブの
IPv4アドレス

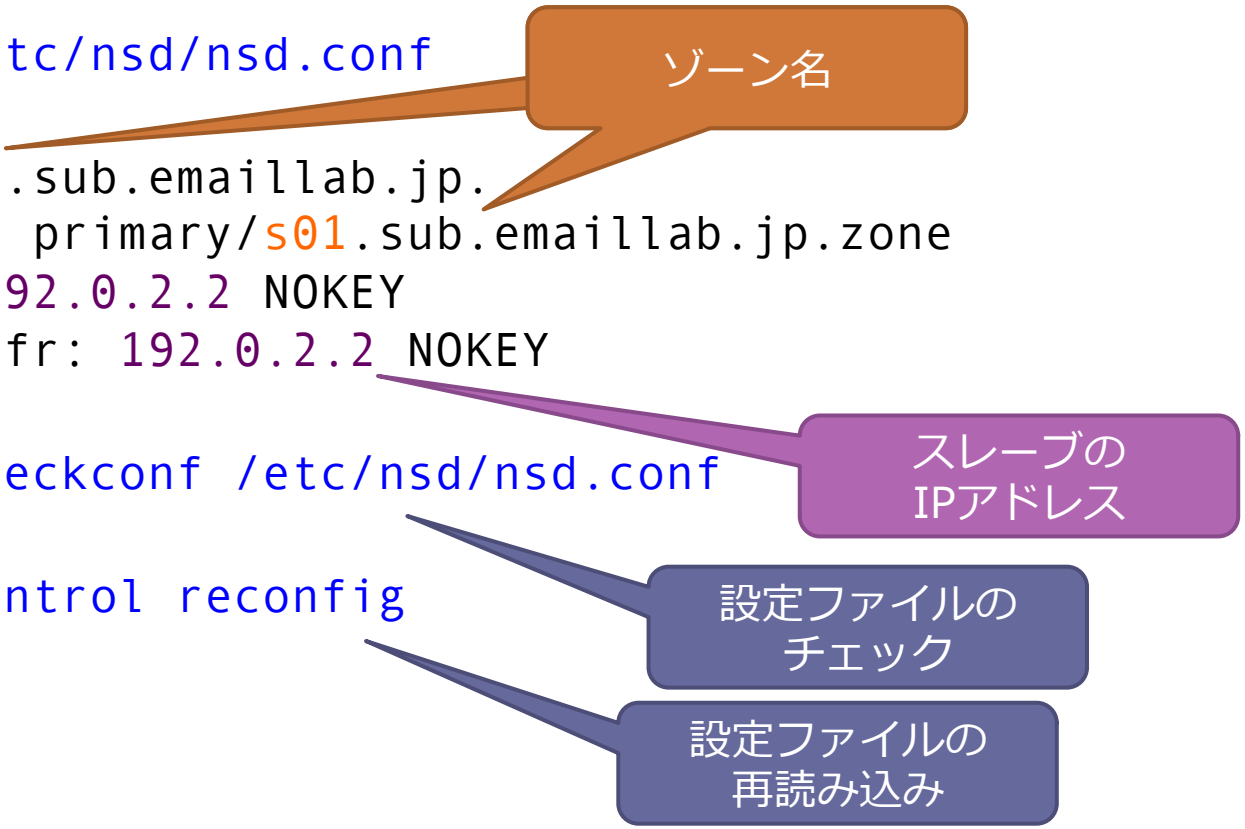
ウェブサーバの
IPv4アドレス

ゾーンファイルの配置とロード（マスター側）（あなたのゾーン）

```
$ sudo vim /etc/nsd/nsd.conf
zone:
        name: s01.sub.emaillab.jp.
        zonefile: primary/s01.sub.emaillab.jp.zone
        notify: 192.0.2.2 NOKEY
        provide-xfr: 192.0.2.2 NOKEY

$ sudo nsd-checkconf /etc/nsd/nsd.conf

$ sudo nsd-control reconfig
```

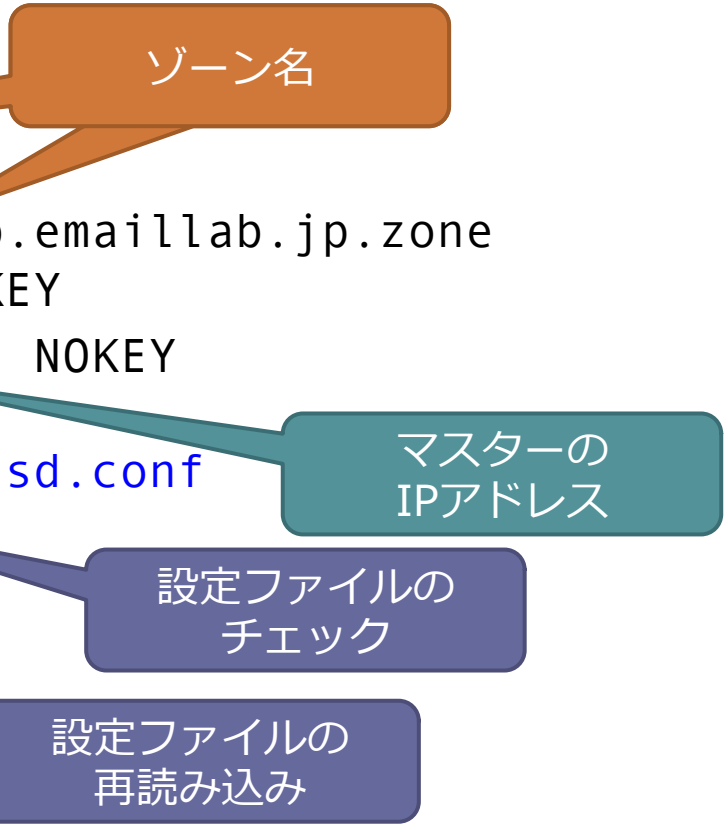


ゾーンファイルの配置とロード（スレーブ側）（隣の人のゾーン）

```
$ sudo vim /etc/nsd/nsd.conf
zone:
        name: s02.sub.emaillab.jp.
        zonefile: secondary/s02.sub.emaillab.jp.zone
        allow-notify: 192.0.2.2 NOKEY
        request-xfr: AXFR 192.0.2.2 NOKEY

$ sudo nsd-checkconf /etc/nsd/nsd.conf

$ sudo nsd-control reconfig
```



（あなたのゾーンの）マスターの確認

- あなたのゾーンのマスターのSOAレコード、NSレコードが意図した通りに設定されていることを確認する。

```
$ dig @192.0.2.1 s01.sub.emaillab.jp. SOA +norec +multi
$ dig @192.0.2.1 s01.sub.emaillab.jp. NS +norec
```

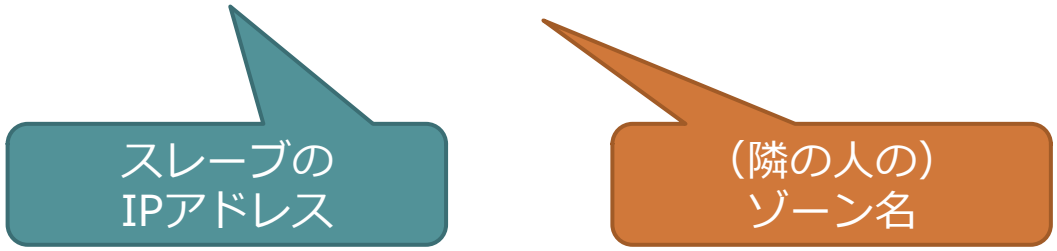
- www.～が引けることを確認。

```
$ dig @192.0.2.1 www.s01.sub.emaillab.jp. A +norec
中略
;; ANSWER SECTION:
www.s01.sub.emaillab.jp. 120  IN  A  157.7.234.43
```

（隣の人のゾーンの）スレーブの確認

- 隣の人のゾーンのスレーブのSOAレコード、NSレコードが引けることを確認する。

```
$ dig @192.0.2.1 s02.sub.emaillab.jp. SOA +norec +multi
$ dig @192.0.2.1 s02.sub.emaillab.jp. NS +norec
```



- 引けない場合はnsd-controlでゾーン転送を試みる。

```
$ sudo nsd-control transfer s02.sub.emaillab.jp.
```

ゾーンファイルの出力（スレーブ側）

ゾーンデータはデータベースとして保持しているため、ゾーンファイルとして出力する必要はない点に注意。

```
$ sudo nsd-control zonestatus
zone: s02.sub.emaillab.jp.
    state: ok
    served-serial: "2014070501 since 2014-07-05T12:00:00"
    commit-serial: "2014070501 since 2014-07-05T12:00:00"
$ ls -l /etc/nsd/secondary/
total 0
$ sudo nsd-control write
ok
$ ls -l /etc/nsd/secondary/
total 4
-rw-r--r-- 1 nsd nsd 366 Feb 11 14:36 s02.sub.emaillab.jp.zone
$ cat /etc/nsd/secondary/s02.sub.emaillab.jp.zone
```

ゾーンの状態の出力

ゾーンファイルの出力

みんな、ここまでできたかな？

- この時点ではまだ権威の委任は行っていないのです。

権威の委任前なので

- www.～を再帰検索要求で引いてみると

```
$ dig www.s01.sub.emaillab.jp. A +multi
中略
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 46300
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.s01.sub.emaillab.jp. IN A

;; AUTHORITY SECTION:
sub.emaillab.jp.    300 IN SOA ns1.sub.emaillab.jp. root.emaillab.jp. (
                            2014070406 ; serial
                            3600       ; refresh (1 hour)
                            900        ; retry (15 minutes)
                            604800     ; expire (1 week)
                            300        ; minimum (5 minutes)
                            )
```

- 引けないですね。

委任してみたので、

- www.～を引いたら引けるはず。

```
$ dig www.s01.sub.emaillab.jp. A +multi
中略
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 46300
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.s01.sub.emaillab.jp. IN A

;; AUTHORITY SECTION:
sub.emaillab.jp.     62 IN SOA ns1.sub.emaillab.jp. root.emaillab.jp. (
                           2014070406 ; serial
                           3600       ; refresh (1 hour)
                           900        ; retry (15 minutes)
                           604800     ; expire (1 week)
                           300        ; minimum (5 minutes)
                           )
```

- あれ、引けない……

委任してみたので、

- www.～を引いたら引けるはず。

```
$ dig www.s01.sub.emaillab.jp. A +multi
中略
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 46300
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.s01.sub.emaillab.jp. IN A

;; AUTHORITY SECTION:
sub.emaillab.jp.      62 IN SOA ns1.sub.emaillab.jp. root.emaillab.jp. (
                            2014070406 ; serial
                            3600       ; refresh (1 hour)
                            900        ; retry (15 minutes)
                            604800     ; expire (1 week)
                            300        ; minimum (5 minutes)
                            )
.....
```

ゾーンの委任前にクエリーを行うと、委任元ゾーンのSOA MINIMUMの値の秒数だけネガティブキャッシュされてしまう。

ネガティブキャッシュの期間が過ぎたので

- www.～を引いたら引けるはず。

```
$ dig www.s01.sub.emaillab.jp. A +multi
中略
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44506
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.s01.sub.emaillab.jp. IN A

;; ANSWER SECTION:
www.s01.sub.emaillab.jp. 120 IN A 157.7.234.43

;; AUTHORITY SECTION:
s01.sub.emaillab.jp.    120 IN NS ns1.s01.sub.emaillab.jp.

;; ADDITIONAL SECTION:
ns1.s01.sub.emaillab.jp. 120 IN A 192.0.2.1
```

- 引けた！

教訓

- 委任前に再帰検索要求のクエリーを行ってはいけない。絶対だ

委任されたらまず行うことは

- SOAレコードとNSレコードを再帰検索要求してみる。

```
$ dig s01.sub.emaillab.jp. SOA +multi
$ dig s01.sub.emaillab.jp. NS
```

- +trace付きで調べてみるのもよい。委任元と委任先のNSレコードが異なっていないことを確認する。

```
$ dig @m.root-servers.net. s01.sub.emaillab.jp. NS
+trace
```

ゾーンファイルの更新

```
$TTL    3600
@       IN  SOA ns1.s01.sub.emaillab.jp. root.emaillab.jp.  (
                    2014070502      ; Serial
                    3600    ; Refresh
                    900     ; Retry
                    604800  ; Expire
                    300 )   ; Minimum
@       IN  NS  ns1.s01.sub.emaillab.jp.
@       IN  NS  ns2.s01.sub.emaillab.jp.
ns1     IN  A   192.0.2.1
ns2     IN  A   192.0.2.2

$TTL    600
www2    IN  A   157.7.235.30
www     IN  A   157.7.234.43
```

ゾーンの動作確認が取れたら、TTLを大きくする。

シリアル値を増加させる。

新ウェブサイト

ゾーンの更新の反映

- 更新方法

```
$ sudo nsd-control reload
```

- 先ほど登録したレコードを引いてみる。

```
$ dig @192.0.2.1 www.s01.sub.emaillab.jp. A +norec
```

おわり