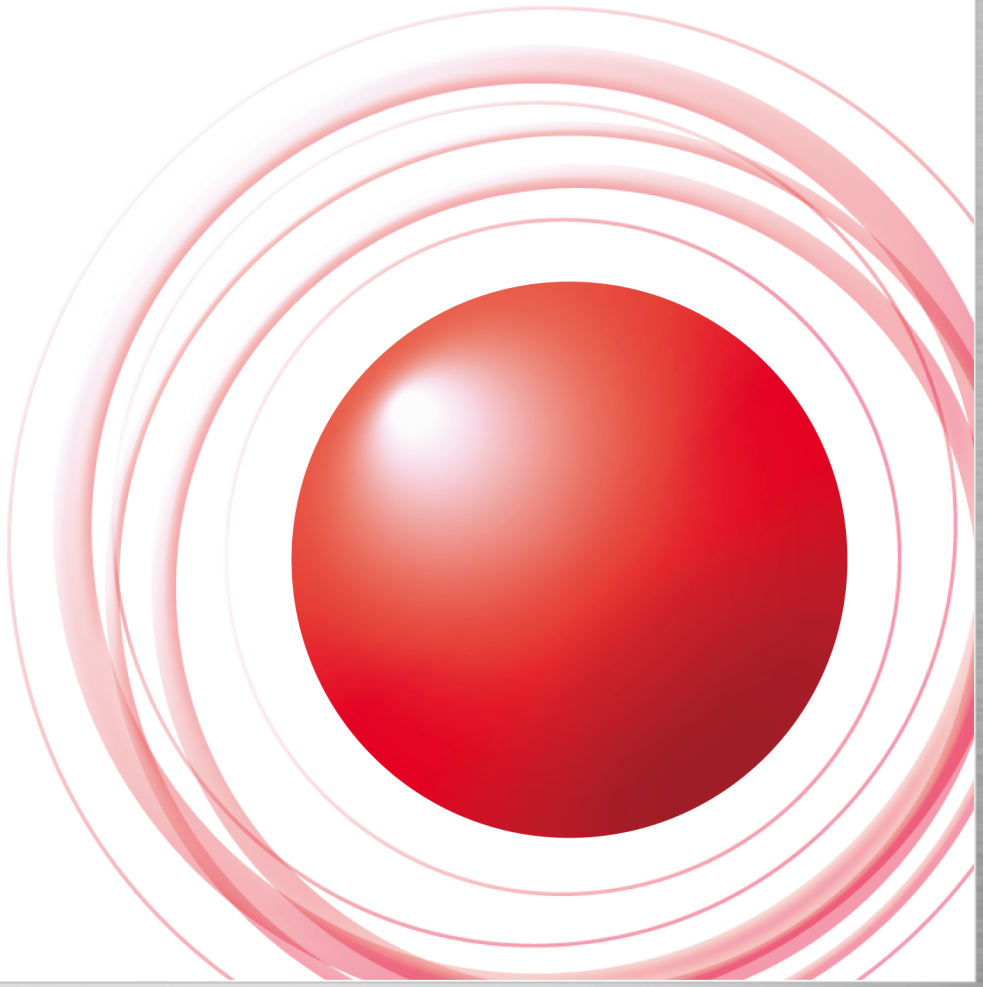
DNSハンズオン DNS運用のいろは
DNSSEC トラブルシュート編

IIJ
Internet Initiative Japan



株式会社インターネットイニシアティブ
其田　学

Ongoing Innovation

はじめに

このセッションでは、DNSSECのトラブルシュートを行います。
おもな登場人物は３人です。

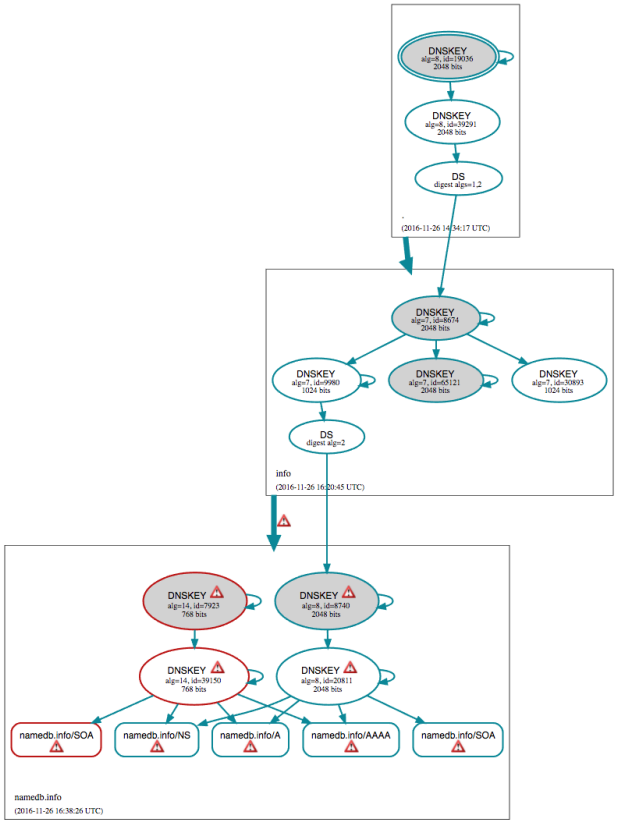
1.権威DNSサーバ（さっきたてた権威DNSサーバ）
2.自組織のキャッシュDNSサーバ　（さっき立てたキャッシュDNSサーバ）
3.他組織のキャッシュDNSサーバ （共用のキャッシュDNSサーバ）

事故は大抵権威DNSサーバが原因で発生します。
このセッションでは、１と２をみなさんに担当してもらい、それぞれ復旧や軽減策を実施してもらいます。

はじめに

なおスライドに書いてなくても随時、２、３の状態を確認して、
状態の比較を見るのも面白いかと思います。

また、dnsvizで状態を確認するのは、実際に障害が起こった時
にも手っ取り早く解析でき、情報共有ができるので便利です。



トラブル例

1.キャッシュDNSサーバの時刻ずれ
2.署名期間からの逸脱
3.移譲されなかった子ゾーン
4.違うDSを登録してしまった

1.キャッシュDNSサーバの時刻ずれ

署名レコードRRSIGには有効**期間**が設定されています。
数分のずれだと問題ない場合が多いですが、
1時間以上のズレの場合は検証エラーになる場合があります。

例：

```
iw2016-0036.jp. RRSIG SOA 8 23600 20161206092332 20161108092332
23418 iw2016-0036.jp. HkUNaozb(以下署名データなので略
```

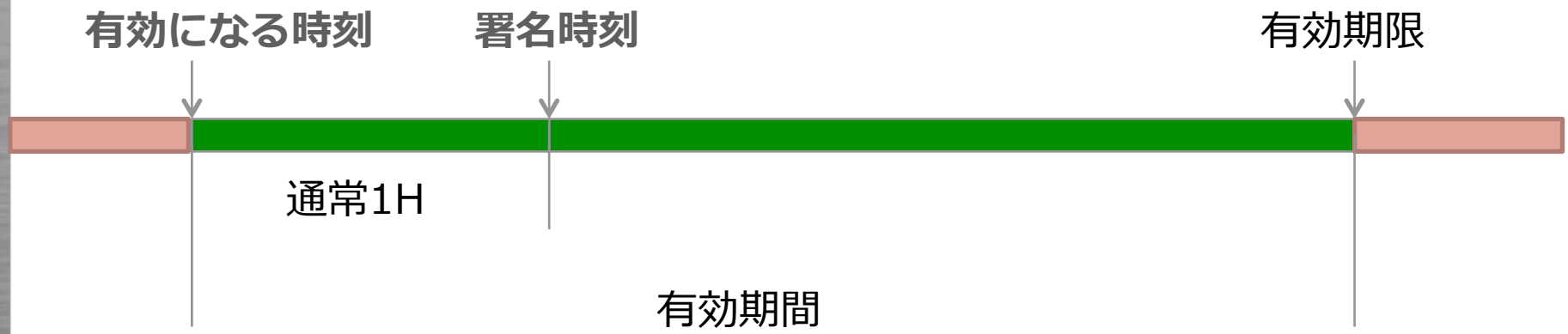
署名が有効になる時刻：２０１６年１１月８日９時２３分３２秒(UTC)
署名が無効になる時刻：２０１６年１２月６日９時２３分３２秒(UTC)

キャッシュDNSサーバの時刻がこの間であれば署名は検証に使える

1.キャッシュDNSサーバの時刻ずれ

１時間の根拠

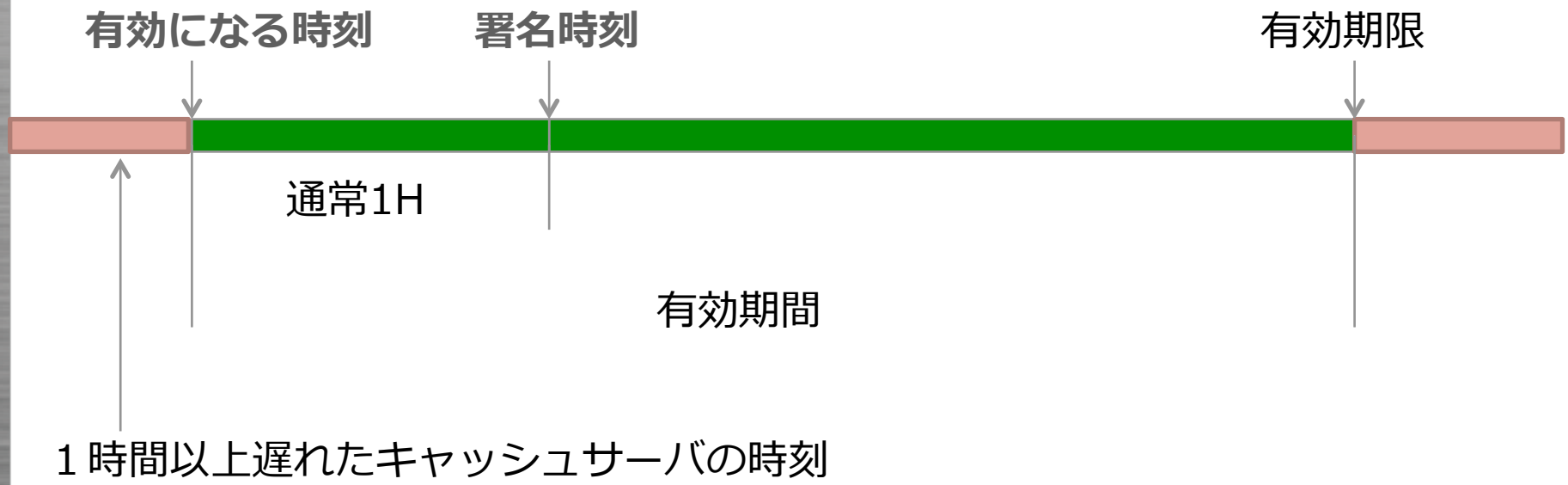
- **署名ソフトのデフォルトの多くが署名が有効になる時刻を署名した時刻の１時間前にするため。**



1.キャッシュDNSサーバの時刻ずれ

１時間以上時間が遅れていると署名検証に失敗する可能性が増えます。
この時間は変更することもできます。

- タイムゾーンをまちがちゃったうっかりさんをケアするために、24h前を設定など。



1.キャッシュDNSサーバの時刻ずれ

時間が進んでいる場合

- 署名は再署名する必要がある。
- 再署名を行う間隔はTTLの関係で、有効期限ギリギリではなく数日前に行うことがほとんど
- そのため、極端にずれていない限り、あまり問題にはならない

例： 署名して１０日有効で、７日目に再署名など

1.キャッシュDNSサーバの時刻ずれ

障害トリガー例:
まちがって date -s で間違った時刻を設定してしまった。

```
# date -s 20171130
```

キャッシュDNSサーバの挙動：

```
# @localhost iw2016-0036.jp
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 27738
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
```

SERVFAILが返ったので、CD bit付きで問い合わせます

```
# @localhost iw2016-0036.jp +cd
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24133
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; ANSWER SECTION:
iw2016-0036.jp.    3594       IN          A          202.221.128.104
```

CD bit付きで問い合わせると応答が返る＝検証エラー

1.キャッシュDNSサーバの時刻ずれ

復旧例：

```
# ntpdate –b ntp.nict.jp
# unbound-control flush_zone .
```

キャッシュサーバをrestart or cache clearしないと
検証失敗したキャッシュが残ります。
運悪くTLDのBADCACHEがあると影響が長期化します

対策：

NTP等で時刻を同期
時刻がずれていないか監視
- BIOSの時刻狂っていてrebootなどで、時刻がずれる可能性も。。

署名の有効期間からの逸脱はトラブルの中で一番多い事象です

- 再署名されておらず、有効期限を過ぎた
  - 再署名処理自体を忘れている場合。。。
  - なんらかの原因で再署名が動かなかった場合
    - プログラムのエラー
    - 停電等で再署名処理が行われず、復帰後も再実行しなかった。
- 署名サーバの時刻がずれていて、署名した時に有効期限を外れた。
  - キャッシュと同じ理由

2.署名の有効期間からの逸脱

トリガー例：
昔の日付で署名してしまった。

```
# vi /etc/nsd/dnsseczonetool.conf

SIGN_PARAM="-i 20161101 -e 20161107”

# /etc/nsd/dnsseczonetool sign iw2016-0036.jp
```

2.署名の有効期間からの逸脱

キャッシュDNSサーバの挙動：

1.と同じようにSERVFAILが返るはず

キャッシュDNS側でできる対応：

一時的に検証を無効にする方法（Negative Trust Anchor）

```
# unbound-control insecure_add iw2016-0036.jp
Ok
# unbound-control list_insecure
iw2016-0036.jp.
```

NTAはcacheに入ったものには適用されないので、flushする

```
# unbound-control flush_bogus
```

digすると検証しないようになっている。

```
# dig @localhost iw2016-0036.jp
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32463
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
ADDITIONAL: 1

;; ANSWER SECTION:
iw2016-0036.jp. 29      IN      A       202.221.128.104
```

2.署名の有効期間からの逸脱

復旧例：

権威DNS側

パラメータを元に戻して再署名＆reload

```
# vi /etc/nsd/dnsseczonetool.conf

SIGN_PARAM=“”

# /etc/nsd/dnsseczonetool sign iw2016-0036.jp
```

キャッシュDNS側

NTAを無効にする

```
# unbound-control insecure_remove iw2016-0036.jp
# unbound-control list_insecure
# <- 何も表示されないこと
```

キャッシュ側でキャッシュクリア

```
# unbound-control flush_zone iw2016-0036.jp
```

2.署名の有効期間からの逸脱

対策例：

時刻のズレに対してはntpクライアントを動かしておくこと。
また、**再署名ができなかった時検知**できる仕組みが必要です。

例：有効期限１０日間で、再署名７日間隔の場合
有効期限まで３日未満になったら検知するのscript

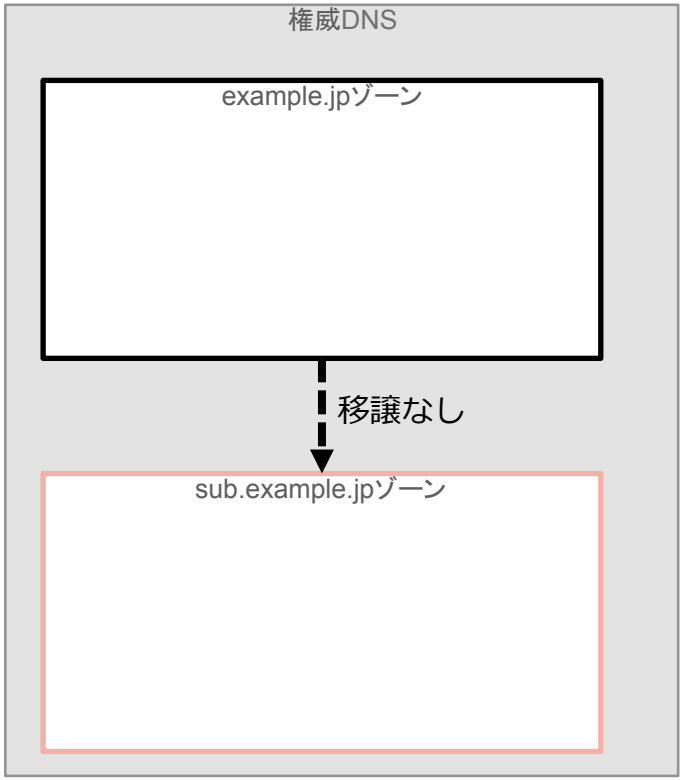
```
$ cat ~/src/watch.sh
#/bin/bash
THRESHOLD=3
DOMAIN=iw2016-0035.jp
IP=$(ip -4 a show dev eth0 | grep inet | awk '{print $2 }' | awk -F '/' '{ print $1 }' )
ET=$(dig @$IP $DOMAIN +dnssec +noall +ans +norec| grep RRSIG | awk '{print $9 }' | cut -c 1-8)

if [ "x$ET" == "x" ] ; then
  echo "zone not signed"
  exit 1
fi
ES=$(expr `date -d $ET +%s` - `date +%s` )
ED=$(expr $ES / 86400)
if [ $ED -lt $THRESHOLD ] ; then
  echo "check faild, $ED days"
  exit 2
fi
echo "check success, $ED days"
exit 0
```

3.移譲されなかった子ゾーン

同じ権威DNSサーバ上で、親ゾーンと子ゾーンが同居する状態は
好ましくないですが、
ファイルの管理とか諸々の理由で分割することがあります。

その際に、適切に移譲しない場合、子ゾーンの検証に失敗します。



3.移譲されなかった子ゾーン

例：
iw2016-0036.jp ゾーン（変更なし）

```
$TTL 60
$ORIGIN iw2016-0036.jp.
@       IN      SOA     ns1     root    _SERIAL_ 3600 900 120960
900
        IN      NS      ns1
        IN      A       202.221.128.104
ns1     IN      A       <指定されたIP>
www     IN      A       202.221.128.104
```

sub.iw2016-0036.jp ゾーン

```
$TTL 60
$ORIGIN sub.iw2016-0036.jp.
@       IN      SOA     ns1     root    1 3600 900 120960 900
        IN      NS      ns1.iw2016-0036.jp.
        IN      A       202.221.128.104
```

3.移譲されなかった子ゾーン

nsd.conf

```
（省略）
zone:
        name: "iw2016-0036.jp."
        zonefile: "iw2016-0036.jp.signed"
zone:
        name: "sub.iw2016-0036.jp."
        zonefile: "sub.iw2016-0036.jp"
```

反映

```
# nsd-checkzone sub.iw2016-0036.jp sub.iw2016-0036.jp
zone sub.iw2016-0036.jp is ok
# nsd-checkconf nsd.conf ; echo $?
0
# nsd-control reconfig
reconfig start, read /etc/nsd/nsd.conf
ok
```

3.移譲されなかった子ゾーン

移譲されなかった子ゾーンの検証結果

```
dig @127.0.0.1 sub.iw2016-0036.jp A +dnssec +norec
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 29633
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

親ゾーンからの移譲がない場合、子ゾーンのDSに対するレスポンスに不在証明レコードが入ります。

```
dig @指定されたIP sub.iw2016-0036.jp ds +dnssec +norec
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6653
ns1.iw2016-0036.jp. 900 IN NSEC www.iw2016-0036.jp. A RRSIG NSEC

(SOA,RRSIGは省略してます。)
```

この応答からns1からwwwの間のlabelは無いことがわかます。
つまり、この間に子ゾーンはいないと親ゾーンが答えたことになります。

sub.iw2016-0036.jpはこの間なので（アルファベット順）
親から子への移譲が無いことになり、子ゾーンの応答は検証に失敗します。

3.移譲されなかった子ゾーン

対応例：
iw2016-0036.jp ゾーン

```
（略）
sub IN    NS    ns1.iw2016-0036.jp.
```

移譲を書きます

再署名&reload

```
# /etc/nsd/dnsseczonetool sign iw2016-0036.jp
```

確認

```
# unbound-control flush_bogus
# dig @127.0.0.1 sub.iw2016-0035.jp +dnssec +short
202.221.128.104
```

4.違うDSを登録してしまった

間違って違うKSKのDSを登録してしまって、
信頼の連鎖が断ち切られるパターンです。

ときどき大きいところがやらかします。。。。（最近だとAPNICとか。。）

また、DSレコードはTLDのゾーンにあるため、TTLが比較的長く
設定されている場合が多く、影響が長引く傾向にあります。

4.違うDSを登録してしまった

トリガー例：
違うDSを登録してしまった。

```
iw2016-0036.jp.        DS       26002 8 2
1234567890123456789012345678901234567890123456789012345678901234
```

JPDirectから違うDSを登録してみましょう

4.違うDSを登録してしまった

対応例１：検証できないようにする

DSを消して検証できないようにします。
これは、あらゆるDNSSECの検証エラーで使える手ですが、
DSのTTLは長めです。

zoneのTTLを短めに設定していても、検証エラーはDSのTTLに
引きづられます。
DSは親ゾーンなので、TLDによってTTLは異なります。

DSのTTLの例

```
iw2016-0036.jp.        7200    IN      DS      26002 8 2
1234567890123456789012345678901234567890123456789012345
890123456 78901234
paypal.com.     86400   IN      DS      21037 5 2
0DF17B28554954D819E0CEEAB98FCFCD56572A4CF4F551F
0A9BE6D04 DB2F65C3
isc.org.86400   IN      DS      12892 5 1
982113D08B4C6A1D9F6AEE1E2237AEF69F3F9759
```

対応例２：検証できるようにする

- DSを正しいものに変更します。
  - ただし、DSのTTLが切れるまでは影響がある可能性があります。
- 署名するKSKを正しいものにして、署名します。
  - 署名前のRRSIGのTTLが切れるまで影響がある可能性があります。

今回は間違ったDSを登録してしまったので正しいDSを登録し直します。

DSレコードの確認

```
# /etc/nsd/dnsseczonetool status iw2016-0036.jp
iw2016-0036.jp's KSK = Kiw2016-0036.jp.+008+13864
iw2016-0036.jp.   3600      IN          DS          13864 8 2
7bfdf25d83c27dfe44e64253c412fbc66e25992d0b2a0774d5307f719d8637c5
iw2016-0036.jp's ZSK = Kiw2016-0036.jp.+008+43443
```

対策例：

- 事前に正しいDSか確認する。http://dnscheck.jp/ など
- 手動でDS登録するのをやめる。
  - （APIなどを利用して、チェックも含めて完全自動化する）

まとめ

権威DNS側：

- DSが信頼の連鎖の肝、DSの変更には神経を使え！
- 時刻同期,監視は忘れずに
- 署名期限の監視
- トラブったらとりあえずdnsviz

キャッシュDNS側：

- 困ったときのNTA
- 何か対応をしたらキャッシュクリア、実際引いての確認を忘れずに

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ——IIJはいつもはじまりであり、未来です。

Ongoing Innovation

お問い合わせ先　IIJインフォメーションセンター
TEL：03-5205-4466 （9：30～17：30 土/日/祝日除く）
info@iij.ad.jp
http://www.iij.ad.jp/