http://test.dnssec-or-not.org/ のヒ･ミ･ツ

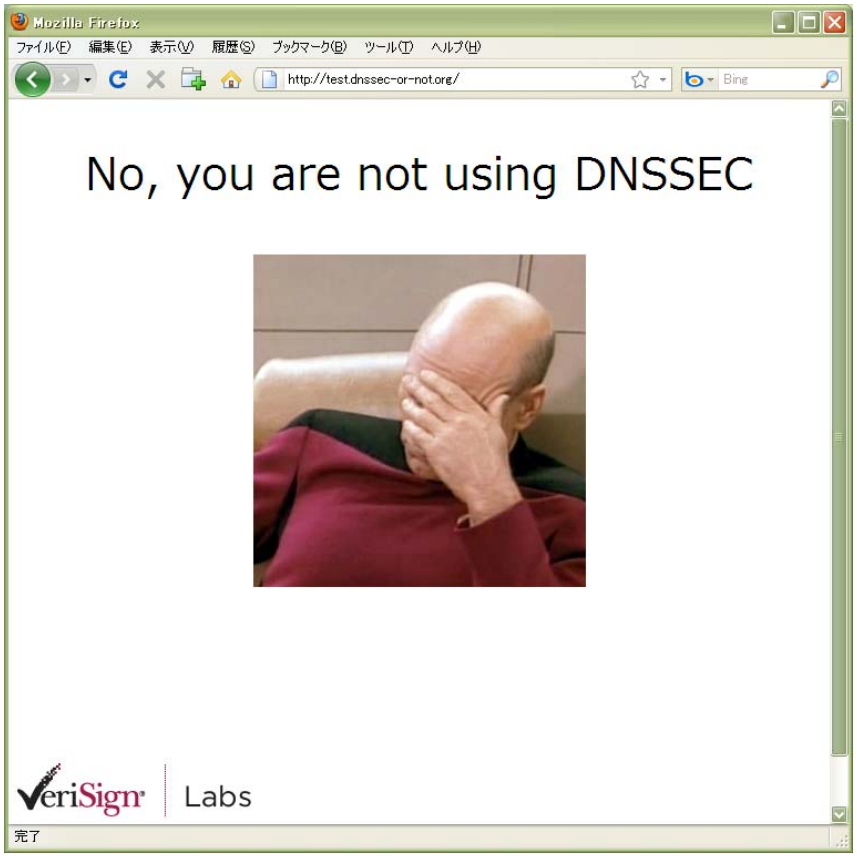
民田雅人
株式会社日本レジストリサービス
2010-11-25 dnsops.jp BoF@IW2010

http://test.dnssec-or-not.org/

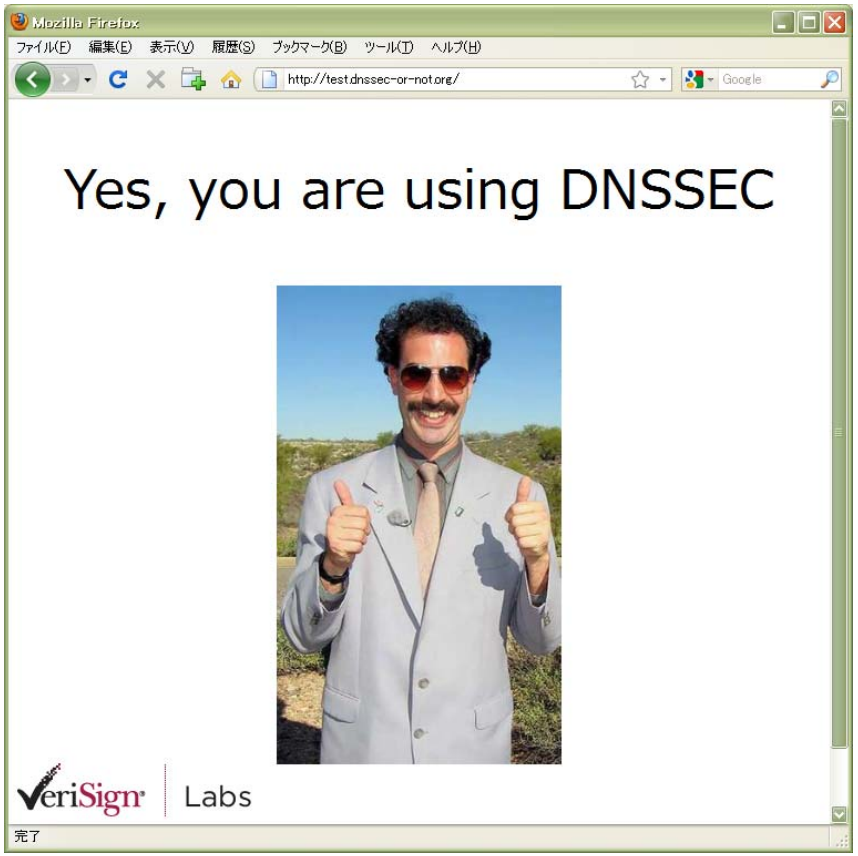
- WEBサイトへアクセスすると、
  利用しているキャッシュDNSサーバが
  DNSSEC署名検証している
  又は
  DNSSEC署名検証していない
  を判定可能
- VeriSign Labsが実験的に始めたサービス
  - DNSSEC署名検証対応状況により、異なったコンテンツが表示される

何が見えるの?

DNSSEC署名検証無し



DNSSEC署名検証有り



digで「署名検証無し」を見てみる

```
; <<>> DiG 9.7.2-P2 <<>> test.dnssec-or-not.org a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44246
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;test.dnssec-or-not.org.                IN      A

;; ANSWER SECTION:
test.dnssec-or-not.org. 60      IN      CNAME   12fc0e22a8002d27.dnssec-or-not.org.
12fc0e22a8002d27.dnssec-or-not.org. 60 IN A     72.13.58.76

;; AUTHORITY SECTION:
dnssec-or-not.org.      60      IN      NS      ns2.dnssec-or-not.org.
dnssec-or-not.org.      60      IN      NS      ns1.dnssec-or-not.org.
dnssec-or-not.org.      60      IN      NS      ns5.dnssec-or-not.org.
dnssec-or-not.org.      60      IN      NS      ns3.dnssec-or-not.org.
dnssec-or-not.org.      60      IN      NS      ns4.dnssec-or-not.org.

;; Query time: 591 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Nov 18 16:37:48 2010
;; MSG SIZE  rcvd: 177
```

digで「署名検証有り」を見てみる

```
; <<>> DiG 9.7.2-P2 <<>> test.dnssec-or-not.org a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33008
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;test.dnssec-or-not.org.                IN      A

;; ANSWER SECTION:
test.dnssec-or-not.org. 60      IN      CNAME   cd56439818abb4fa.dnssec-or-not.org.
cd56439818abb4fa.dnssec-or-not.org. 60 IN A     72.13.58.77

;; Query time: 1930 msec
;; SERVER: 203.178.129.44#53(203.178.129.44)
;; WHEN: Thu Nov 18 16:40:02 2010
;; MSG SIZE  rcvd: 87
```

署名検証の有無でどこが違う? (1)

- TTLは60秒で同じ
- なんとIPアドレスが違う
  - 署名検証無しの場合　　72.13.58.76
  - 署名検証有りの場合　　72.13.58.77
  - だからと言って、直接IPアドレスで、
    http://72.13.58.77/
    とかをアクセスすると、リダイレクトされ
    http://test.dnssec-or-not.org/
    となるため表示結果は変わらない

署名検証の有無でどこが違う? (2)

- test.dnssec-or-not.orgはCNAME
  しかもCNAMEで指すドメイン名が違う
  - 検証有無とは関係なく、ドメイン名は毎回変わる
- 署名検証有りでは、権威セクションが無い
- Query timeが違う
  - 署名検証無し　　591 msec
  - 署名検証有り　　1930 msec

    ⇒ 検証有無の差が大きすぎでは…

    ⇒ そもそも時間かかりすぎなのでは…

仮定

- キャッシュDNSサーバがDNSSECで署名検証する場合、DNSKEY RRを問い合わせる
- この挙動の違いを判断し、応答を変えているのではないか?
  - DNSKEY RRを問い合わせない
    ⇒ DNSSEC署名検証を行っていない
    ⇒ 72.13.58.76 を単純に返す
  - DNSKEY RRを問い合わせてきた
    ⇒ DNSSEC署名検証を行っている
    ⇒ 72.13.58.77 を署名して返す

DNSパケットを見てみよう

- キャッシュDNSサーバと外部の権威サーバのDNSパケットを覗いてみる ⇒ 結果は次スライド
- tcpdumpの結果そのままでは見づらいので部分的に省略し以下のように表記
  - Q.数字、A.数字　　問合せとその応答
  - D　　DNSSEC関連の問合せと応答
  - CACHE　　手元のキャッシュDNSサーバ
  - X.root　　X.root-servers.net
  - XX.ORG　　.orgの権威DNSサーバ
  - nsX　　nsX.dnssec-or-not.org

署名検証有りをtcpdump (1/2)

```
Q.01   CACHE  > h.root: [1au] A? test.dnssec-or-not.org. (51)
Q.02   CACHE  > h.root: [1au] NS? . (28)
A.02   h.root > CACHE : 14/0/22 <rootのNSがずらずら> (829)
Q.03 D CACHE  > b.root: [1au] DNSKEY? . (28)
A.01   h.root > CACHE : 0/9/13 (699) <.orgへのReferral>
Q.04   CACHE  > b0.ORG: A? test.dnssec-or-not.org. (51)
A.03 D b.root > CACHE : 3/0/1 DNSKEY, DNSKEY, RRSIG (736)
A.04   b0.ORG > CACHE : 0/7/6 (432) <dnssec-or-not.orgへのReferral>
Q.05   CACHE  > ns1: A? test.dnssec-or-not.org. (51)
A.05   ns1 > CACHE : 2/6/0 CNAME 3c8548f28766e247.dnssec-or-not.org., RRSIG (515)
Q.06 D CACHE  > ns5: [1au] DNSKEY? dnssec-or-not.org. (46)
A.06 D ns5 > CACHE : 3/6/0 DNSKEY, DNSKEY, RRSIG (775)
Q.07 D CACHE  > c0.ORG: [1au] DS? dnssec-or-not.org. (46)
A.07 D c0.ORG > CACHE : 2/7/5 DS, RRSIG (646)
Q.08 D CACHE  > c0.ORG: [1au] DNSKEY? org. (32)
A.08 D c0.ORG > CACHE : 6/0/1 DNSKEY, DNSKEY, DNSKEY, DNSKEY, RRSIG, RRSIG (1334)
Q.09 D CACHE  > a.root: [1au] DS? org. (32)
A.09 D a.root > CACHE : 3/14/22 DS, DS, RRSIG (1076)
```

署名検証有りをtcpdump (2/2)

```
Q.10   CACHE  > ns4: [1au] A? 3c8548f28766e247.dnssec-or-not.org. (63)
A.10   ns4 > CACHE : 1/6/0 A 72.13.58.76 (352)
Q.11 D CACHE  > ns2: [1au] DS? 3c8548f28766e247.dnssec-or-not.org. (63)
A.11 D ns2 > CACHE : 2/0/0 DS, RRSIG (277)
Q.12   CACHE  > ns3: [1au] A? 3c8548f28766e247.dnssec-or-not.org. (63)
A.12   ns3 > CACHE : 1/6/0 A 72.13.58.76 (352)
Q.13   CACHE  > ns2: [1au] A? 3c8548f28766e247.dnssec-or-not.org. (63)
A.13   ns2 > CACHE : 1/6/0 A 72.13.58.76 (352)
Q.14   CACHE  > ns1: [1au] A? 3c8548f28766e247.dnssec-or-not.org. (63)
A.14   ns1 > CACHE : 2/6/0 A 72.13.58.77, RRSIG (546)
Q.15 D CACHE  > ns2: [1au] DNSKEY? 3c8548f28766e247.dnssec-or-not.org. (63)
A.15 D ns2 > CACHE : 3/0/0 DNSKEY, DNSKEY, RRSIG (542)
```

BIND 9のキャッシュDNSサーバでの例

- キャッシュは空の状態から計測
- unboundもテストしたが、例にするには行数多過ぎ (^^;

tcpdumpの結果説明 (1/2)

- Q.01～A.04
  - dnsec-or-not.orgの権威DNSサーバである ns[1-5].dnssec-or-not.orgのグルーを得る
- Q.05, A.05
  - ns1にtest.dnssec-or-not.orgのAを問合せ、**CNAME**と **RRSIG**を得る
- Q.06～A.09
  - A.05で得たRRSIGの検証に必要な情報の検索
- Q.10, A.10
  - ns4に“3c8548f28766e247.dnssec-or-not.org”のAを問合せると、**署名検証無しの結果**である“72.13.58.76”を **RRSIG無し**で得る

tcpdumpの結果説明 (2/2)

- Q.11, A.11
  - ここでDSを問合せる必要は無いと思われるが念の為か? (しかもRRSIG付きでDSを答えている)
- Q.12～A.13
  - Q.10,A.11と同じ問合せをns3、ns2に実行。やはり...76でRRSIGが無い
- Q.14, A.14
  - さらに同じ問合せをns1に実行。ここで**署名検証有りの結果**である“72.13.58.77”を**RRSIG有り**で答える
- Q.15, A.15
  - Q.11, A.11同様にDNSKEYを問合せる

nsX.dnssec-or-not.orgの挙動 (tcpdump結果のまとめ)

- test.dnssec-or-not.org のAを問合せる
  - ns1 ⇒ CNAMEが**RRSIG有り**
- そのCNAMEの値のAを問合せる
  1. ns4 ⇒ 72.13.58.76がRRSIG無し
  2. ns3 ⇒ 72.13.58.76がRRSIG無し
  3. ns2 ⇒ 72.13.58.76がRRSIG無し
  4. ns1 ⇒ 72.13.58.77が**RRSIG有り**
- キャッシュDNSサーバが
  - DNSSEC**署名検証する**場合、上記1～3は署名検証に失敗して捨てられ、4の結果を信用する
  - DNSSEC**署名検証しない**場合、上記1の結果を信用して終了

あらたな仮定

- 通常のDNSにおいて、ゾーンデータ提供側でキャッシュDNSサーバがどのNSに対して問合せるかを指定することは出来ない
  - この例の場合、ns1に当たったとか、CNAMEを答えたサーバと同じになったからRRSIG付きになったわけじゃなさそう

ひょっとして何回問合せたかで決まる?

ns5.dnssec-or-not.orgで実験

```
$ dig +short +dnssec @ns5.dnssec-or-not.org test.dnssec-or-not.org a
8179b5c5dad1b9e1.dnssec-or-not.org.
CNAME 5 3 60 20101219082953 20101119082953 12360 dnssec-or-not.org.
   w7a/rXQhzkhwYJskpOmuF1n0y+ZlK83bC87LqdhJk4+W1lV2cpOyojBR
   o0K3K5/o/OOCqVYGww7r6Hqwizl4XKvPocS/whVwzUd+rh1Og7LPkmbQ
   ia/vHvmzXOGvZigvSOW//FvDniiQkOdivmtiQUtyvwUKbC7XS3ZKxRFA zrw=
$ dig +short +dnssec @ns5.dnssec-or-not.org 8179b5c5dad1b9e1.dnssec-or-not.org. a
72.13.58.76
$ dig +short +dnssec @ns5.dnssec-or-not.org 8179b5c5dad1b9e1.dnssec-or-not.org. a
72.13.58.76
$ dig +short +dnssec @ns5.dnssec-or-not.org 8179b5c5dad1b9e1.dnssec-or-not.org. a
72.13.58.76
$ dig +short +dnssec @ns5.dnssec-or-not.org 8179b5c5dad1b9e1.dnssec-or-not.org. a
72.13.58.77
A 5 3 60 20101219083010 20101119083010 36051 8179b5c5dad1b9e1.dnssec-or-not.org.
   qDjUvyjjNZ8XsK90C2mrHrwFSFbKeVY5EYZqi1JUbizjjHeET4zCXZgi
   ehT5+wENA5/RC2KeV8IIWSREhB1aPF3Ulz2vPrbwwSPdeqAY2SSe/Vxo
   Q9o8Od06WleBKzVnpJk/P3D0xmhzjIJHBqBuXypX7OoOESK9NubS8WFR hoQ=
```

dnssec-or-not.orgのNSの挙動

- test.dnssec-or-not.orgのA RRの問いには、ダイナミックに生成したCNAMEを返す
  - このとき署名も作っていると思われる
- CNAMEで得られた値のA RRの問いには、3回目までは署名無しで返す
  - ある程度のリトライを想定しているのか?
- 4回目のAの問いに対して、署名付きで返す
- しばらくすると、生成された名前は削除される
  - Name Errorとなる

得られた知見

- キャッシュDNSサーバが署名検証を行う際、万が一署名検証に失敗すると、NS RRにある別の権威DNSサーバで再度確認を行う
  ⇒NSが複数あれば、1回署名検証に失敗しただけで直ちにSERVFAILとはならない
- この挙動は、非DNSSEC環境で、キャッシュDNSサーバが権威DNSサーバからSERVFAILを得たときと変わらない

Q and A

JAPAN REGISTRY SERVICES