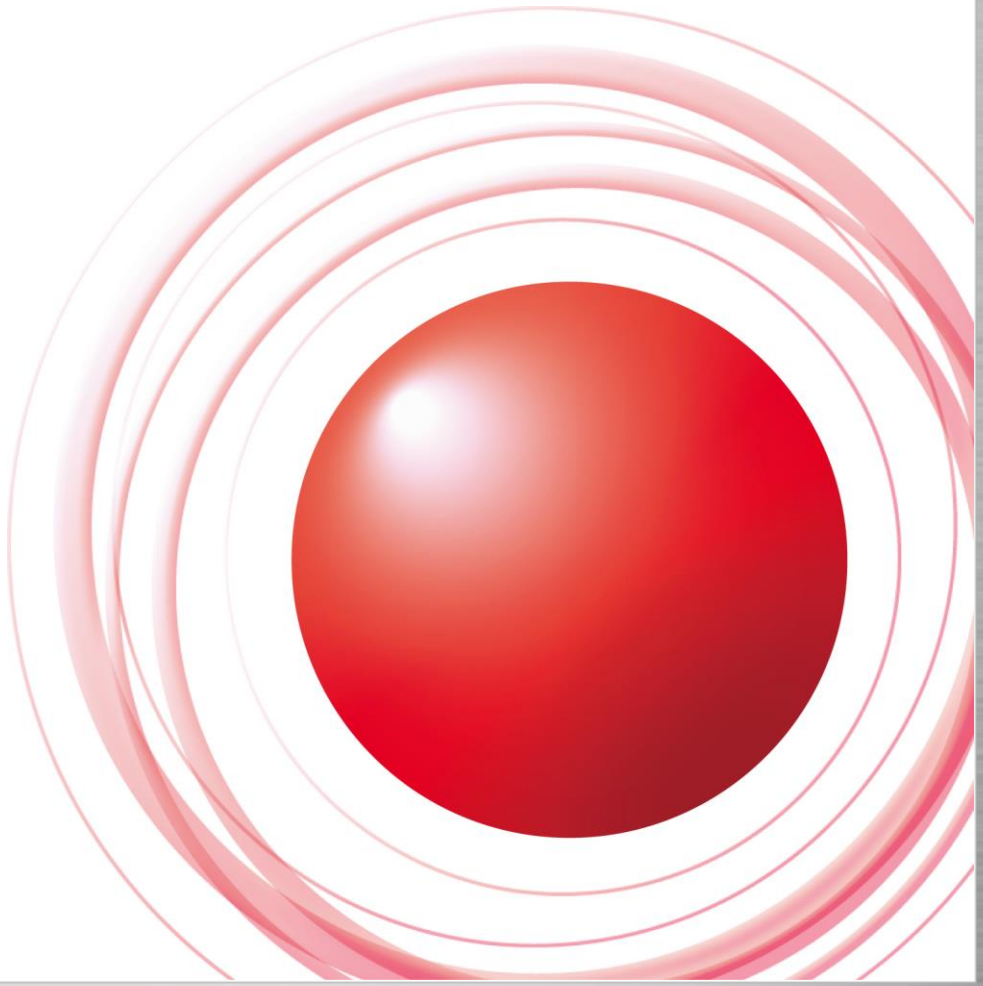
キャッシュDNSサーバー DNSSECトラブルシューティング

IIJ
Internet Initiative Japan



株式会社インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

はじめに おことわり

- 私、島村は参照用DNSサーバーの運用をしていますが、IIJの参照用DNSサーバーでは DNSSEC Validationを有効にしていません。

  本発表は、個人的な趣味・検証を基に行われていることをご留意ください。

- 本発表資料は、IW 2012の「T9 DNSSEC チュートリアル」の其田 学さん(三洋ITソリューションズ(当時))の資料を多大に参考させていただいています。ありがとうございます。

DNSSEC validation失敗。そのとき

- client(エンドユーザー)にどう見えるか？
  - SERVFAIL応答
- ブラウザでは…？

DNSSEC validation失敗。そのとき

- client(エンドユーザー)にどう見えるか？
  - SERVFAIL応答
- ブラウザでは…？

エンドユーザー側では何もわからない

「インターネットがつかえません！！」

監視 ログ編 設定

- DNSSEC Validation失敗のログを出力する
  - BIND: named.confに以下を追加

```
logging {
   category dnssec { dnssec_log; };
   category lame-servers { dnssec_log; };
   channel dnssec_log {syslog local2;
                       severity info; }; };
```

  - Unbound: unbound.confに以下を追加

```
server:
   val-log-level: 1
```

or

```
server:
   val-log-level: 2
```

（より詳細に出る）

監視 ログ編 bind

- bind

```
dnssec channel:
 初回: validating dnssec-failed.org/DNSKEY: no valid signature found (DS)
 cachehit: validating dnssec-failed.org/A: bad cache hit
              (dnssec-failed.org/DNSKEY)          ← 名前解決するたびに出る
```

```
lame-server channel:
 no valid RRSIG resolving 'dnssec-failed.org/DNSKEY/IN':
   2001:558:1004:7:68:87:85:132#53          ← 初回だけ出る

 broken trust chain resolving 'dnssec-failed.org/A/IN':
   2001:558:fe23:8:69:252:250:103#53        ← 名前解決するたびに出る
```

監視 ログ編 unbound

- unbound
  - val-log-level: 1

```
info: validation failure dnssec-failed.org. AAAA IN
info: validation failure dnssec-failed.org. A IN
```

  - val-log-level: 2

```
info: validation failure <dnssec-failed.org. AAAA IN> no keys have a DS with algorithm RSASHA1 from 68.87.72.244 for key dnssec-failed.org. while building chain of trust

info: validation failure <dnssec-failed.org. A IN> key for validation dnssec-failed.org. is marked as invalid because of a previous validation failure <dnssec-failed.org. AAAA IN>: no keys have a DS with algorithm RSASHA1 from 68.87.72.244 for key dnssec-failed.org. while building chain of trust
```

監視 統計編

- 統計情報を出力する

	bind (rndc stats)	unbound (unbound-control stats)
SERVFAIL応答数	queries resulted in SERVFAIL	num.answer.rcode.SERVFAIL
検証失敗数	DNSSEC validation failed	num.answer.bogus

- queries resulted in SERVFAIL
  - bogusになるRRを引かれた回数
- DNSSEC validation failed
  - bogusなRRを1回引くとかなり増える
- num.answer.rcode.SERVFAIL/num.answer.bogus
  - どちらも、bogusなRRを1回引くと概ね1増える
  - num.answer.bogusが増えない時もある(謎)

    e.g. fail.dnssec.jp

Validationが失敗する場合とは

1. 本当に毒入れされた
2. 参照用DNSサーバーの時刻がずれている
3. 途中のNWの問題
4. root KSK rollover時の問題
5. 権威DNS側の問題

キャッシュポイゾニングにかかる時間

$$H = \frac{\log(1-Q)}{\log\left(1-\frac{F}{D \times U \times S}\right)} \Big/ 1000/W$$

H：攻略所要時間 (sec)

W: 攻撃可能時間 (ms) (Attacker⇔cacheのRTT)

Q：攻撃成功確率

F：攻撃可能回数 (攻撃パケット数 (pps) × 攻略可能時間 (sec))

D：transaction ID数 (0-65535)

U：source Port数 (1024-65535)

S：攻撃対象のRRの権威サーバーの数

応答サイズ: 125byte,帯域: 50Mbps,
Attacker⇔cacheのRTT: 0.5ms,
cache⇔権威のRTT: 170ms, 権威サーバー:2IPの条件下で
Q=0.90→106hr, Q=0.95→138hr, Q=0.99→211hr
で攻略可能

Emanuel Petr. An analysis of the DNS cache poisoning attack

本当に毒入れされた場合

- とりあえず再起動すれば(もちろんcacheの破棄でも良い)、その場は回復する
- 攻撃が続いていれば、当然再度毒入れされる
- 攻撃を取り除く必要がある
  - オープンリゾルバ → 論外なので閉じる
  - 正当なユーザ・踏み台にされているユーザ
    - 原因の特定と遮断、及びabuse対応
      - ランダム文字列なサブドメインを付けたクエリを送っている
      - 偽の応答をひたすら送ってきている
      - そのユーザーからやけにpps(bps)が多い

サーバーの時刻がずれている場合

- DNSSEC署名には有効期限がある
- 検証側の時刻がずれていると…
  - 早い場合: 実際は署名の終了期限に達していないのにexpireしていると判断してbogusに
  - 遅い場合: 実際は署名の開始時刻に達しているのに、まだ開始前だと判断してbogusに
- ちゃんとNTP(など)で時刻を合わせましょう…
- 時刻があっているか監視しましょう
- タイムゾーンも気にしましょう

※基本的には余裕をもって再署名されるはずなので、余程派手にずれなければ大丈夫…か？

途中のNWの問題の場合

- 途中のFirewall(権威側 or 参照用側どちらでも)で大きなUDPパケットを遮断
  - 512byteは超えられたとして、もっと大きいものは…？
- 途中の通信路のpMTUディスカバリ―が正常に動作していない
  - キャッシュ側は事前に確認する**はず**なので、まぁ平気でしょう
  - 権威側がpMTUディスカバリー問題を抱えたまま、ドメインのDSを登録したら… bogus
- ZSK/KSKロールオーバーの時だけbogus

途中のNWの問題の場合

- 参照用(自組織)側の問題の場合は直しましょう
- 権威側や、通過する他組織の問題の場合はどうにもならないので、「権威側の問題の場合」と同じ対処

Root KSK rollover

- 詳しくはこの後の石原先生のセッションで！！
- RFC5011に対応していて、自動更新の設定になっていれば、(現状、たぶん)何もしなくて平気だけど、こけたら全bogus！
- 不安だったらvalidation OFFしておく…？

権威側の問題の場合

- 基本的にValidationを行う側でできることはない
  - bogusな状態が継続していない場合はキャッシュの削除をしてあげると回復する
- 唯一の例外: Validation OFF
  - bogusになっているドメインの重要度・影響範囲を考慮して、必要に応じてValidationをOFF

キャッシュの削除(flush)

- 権威側の問題でbogusになっていたが、すでにbogusでなくなっている場合は手動でキャッシュを削除してあげることでsecureになる
- bind

```
$ rndc flush (抱えてるすべてのキャッシュ)
$ rndc flushname $NAME
$ rndc flushtree $NAME
```

- unbound

```
$ unbound-control flush_zone $NAME
$ unbound-control flush_bogus
```

Validation OFF (全体)の方法 (bind)

- bind:
  1. named.confで

     ```
     dnssec-validation: no;
     ```

     にしてrndc reconfig (or 再起動)

  2. ```
     $ rndc validation disable
     ```

     enableで有効に
     ```

Validation OFF (全体)の方法 (unbound)

- unbound:
  1. unbound.confから `auto-trust-anchor-file` の記述を削除してunbound-control realod (or 再起動)
  2. unbound.confで以下に変更して再起動

```
server:
    module-config: “iterator”
```

  3. unbound.confに以下を追加してreload (or 再起動)

```
server:
    val-permissive-mode: yes
```

bogusになるRRだけCD bitを立てた様な振る舞い

Validation OFF (個別)の方法

- Negative Trust Anchors (NTA)
  - RFC7646
  - unbound, bind(9.11以降), Nominum Vantioなどで使える
    - unboundとVantioはずっと前から使える

Validation OFF (個別)の方法 (bind)

- BIND
  - 9.10まで: 丸ごとOFFにするしかない
  - 9.11から(&サブスクリプション版):
    - dnssec.failのvalidationを1日無効化

```
$ rndc nta –lifetime 86400 dnssec.fail
Negative trust anchor added: dnssec.fail/_default,
  expires 11-Nov-2015 10:38:46.000
```

      - lifetimeはデフォルト1時間で短い
      - 最長1週間まで

Validation OFF (個別)の方法 (bind)

- 無効化されている名前と有効期限の一覧

```
$ rndc nta –dump
dnssec.fail: expiry 11-Nov-2015 23:15:18.000
fail.dnssec.jp: expiry 18-Nov-2015 20:56:01.000
```

- 再有効化

```
$ rndc nta -remove dnssec.fail
Negative trust anchor removed: dnssec.fail/_default
```

Validation OFF (個別)の方法 (unbound)

- unbound
  - 1.4.20まで:
    unbound.confに以下を追加してreload or 再起動

```
domain-insecure: “dnssec.fail”
```

  - 1.4.21から: 上記の他に
    - 追加

```
$ unbound-control insecure_add
    dnssec.fail
```

Validation OFF (個別)の方法 (unbound)

- 一覧

```
$ unbound-control list_insecure
fail.dnssec.jp.
dnssec.fail.
```

- 削除

```
$ unbound-control insecure_remove
    dnssec.fail
```

解析

- dig +cd
  - CD(Checking Disabled) bitを立てる
  - CD bitがたっていると(BADな)cacheをそのまま返す(SHOULD)
    - 普通のSERVFAILと区別ができ、DNSSEC起因と判断することができる

解析

- delv (DNS lookup and validation utility)
  - bind 9.10以降に付属のツール
  - “Eleven, twelve, dig and delve”
  - https://kb.isc.org/article/AA-01152/0/Eleven-twelve-dig-and-delv%3A-BIND-9.10.html
  - 注) DNSSEC対応キャッシュDNSサーバーに対して、bogusな名前を検査するときは+cdをつけないとこける

```
$ ./bind/bin/delv +cd +multi dnssec-failed.org
;; validating dnssec-failed.org/DNSKEY: no valid signature found (DS)
;; no valid RRSIG resolving 'dnssec-failed.org/DNSKEY/IN': 127.0.0.1#53
;; broken trust chain resolving 'dnssec-failed.org/A/IN': 127.0.0.1#53
;; resolution failed: broken trust chain
```

解析

- +rtrace
  toggle resolver fetch logging

```
$ ./bind/bin/delv +cd +multi +rtrace dnssec-failed.org
;; fetch: dnssec-failed.org/A
;; fetch: dnssec-failed.org/DNSKEY
;; fetch: dnssec-failed.org/DS
;; fetch: org/DNSKEY
;; fetch: org/DS
;; fetch: ./DNSKEY
;; validating dnssec-failed.org/DNSKEY: no valid signature found (DS)
;; no valid RRSIG resolving 'dnssec-failed.org/DNSKEY/IN': 127.0.0.1#53
;; broken trust chain resolving 'dnssec-failed.org/A/IN': 127.0.0.1#53
;; resolution failed: broken trust chain
```

- +vtrace
  toggle validation logging

解析

- +vtrace

  toggle validation logging

```
$ ./bind/bin/delv +cd +multi +vtrace dnssec-failed.org
;; fetch: dnssec-failed.org/A
;; validating dnssec-failed.org/A: starting
;; validating dnssec-failed.org/A: attempting positive response validation
;; fetch: dnssec-failed.org/DNSKEY
;; validating dnssec-failed.org/DNSKEY: starting
;; validating dnssec-failed.org/DNSKEY: attempting positive response validation
;; fetch: dnssec-failed.org/DS
;; validating dnssec-failed.org/DS: starting
;; validating dnssec-failed.org/DS: attempting positive response validation
;; fetch: org/DNSKEY
;; validating org/DNSKEY: starting
;; validating org/DNSKEY: attempting positive response validation
;; fetch: org/DS
;; validating org/DS: starting
;; validating org/DS: attempting positive response validation
;; fetch: ./DNSKEY
;; validating ./DNSKEY: starting
;; validating ./DNSKEY: attempting positive response validation
;; validating ./DNSKEY: verify rdataset (keyid=19036): success
;; validating ./DNSKEY: signed by trusted key; marking as secure
;; validating org/DS: in fetch_callback_validator
;; validating org/DS: keyset with trust secure
;; validating org/DS: resuming validate
;; validating org/DS: verify rdataset (keyid=62530): success
;; validating org/DS: marking as secure, noqname proof not needed
;; validating org/DNSKEY: in dsfetched
;; validating org/DNSKEY: dsset with trust secure
;; validating org/DNSKEY: verify rdataset (keyid=9795): success
;; validating org/DNSKEY: marking as secure (DS)
;; validating dnssec-failed.org/DS: in fetch_callback_validator
;; validating dnssec-failed.org/DS: keyset with trust secure
;; validating dnssec-failed.org/DS: resuming validate
;; validating dnssec-failed.org/DS: verify rdataset (keyid=1445): success
;; validating dnssec-failed.org/DS: marking as secure, noqname proof not needed
;; validating dnssec-failed.org/DNSKEY: in dsfetched
;; validating dnssec-failed.org/DNSKEY: dsset with trust secure
;; validating dnssec-failed.org/DNSKEY: no DNSKEY matching DS
;; validating dnssec-failed.org/DNSKEY: no valid signature found (DS)
;; no valid RRSIG resolving 'dnssec-failed.org/DNSKEY/IN': 127.0.0.1#53
;; validating dnssec-failed.org/A: in fetch_callback_validator
;; validating dnssec-failed.org/A: fetch_callback_validator: got SERVFAIL
;; broken trust chain resolving 'dnssec-failed.org/A/IN': 127.0.0.1#53
;; resolution failed: broken trust chain
```

解析

- drill –S
  - ldns付属ツール
  - -kでtrust anchorを指定する必要あり
  - validationの途中経過をツリー表示する (ただし、根元が逆)

```
$ drill -k root.auto.anchor -S dnssec-failed.org
;; Number of trusted keys: 1
;; Chasing: dnssec-failed.org. A


DNSSEC Trust tree:
dnssec-failed.org. (A)
|---dnssec-failed.org. (DNSKEY keytag: 10032 alg: 5 flags: 256)
    |---dnssec-failed.org. (DNSKEY keytag: 29521 alg: 5 flags: 257)
No trusted keys found in tree: first error was: No DNSSEC public key(s)
;; Chase failed.
```

解析

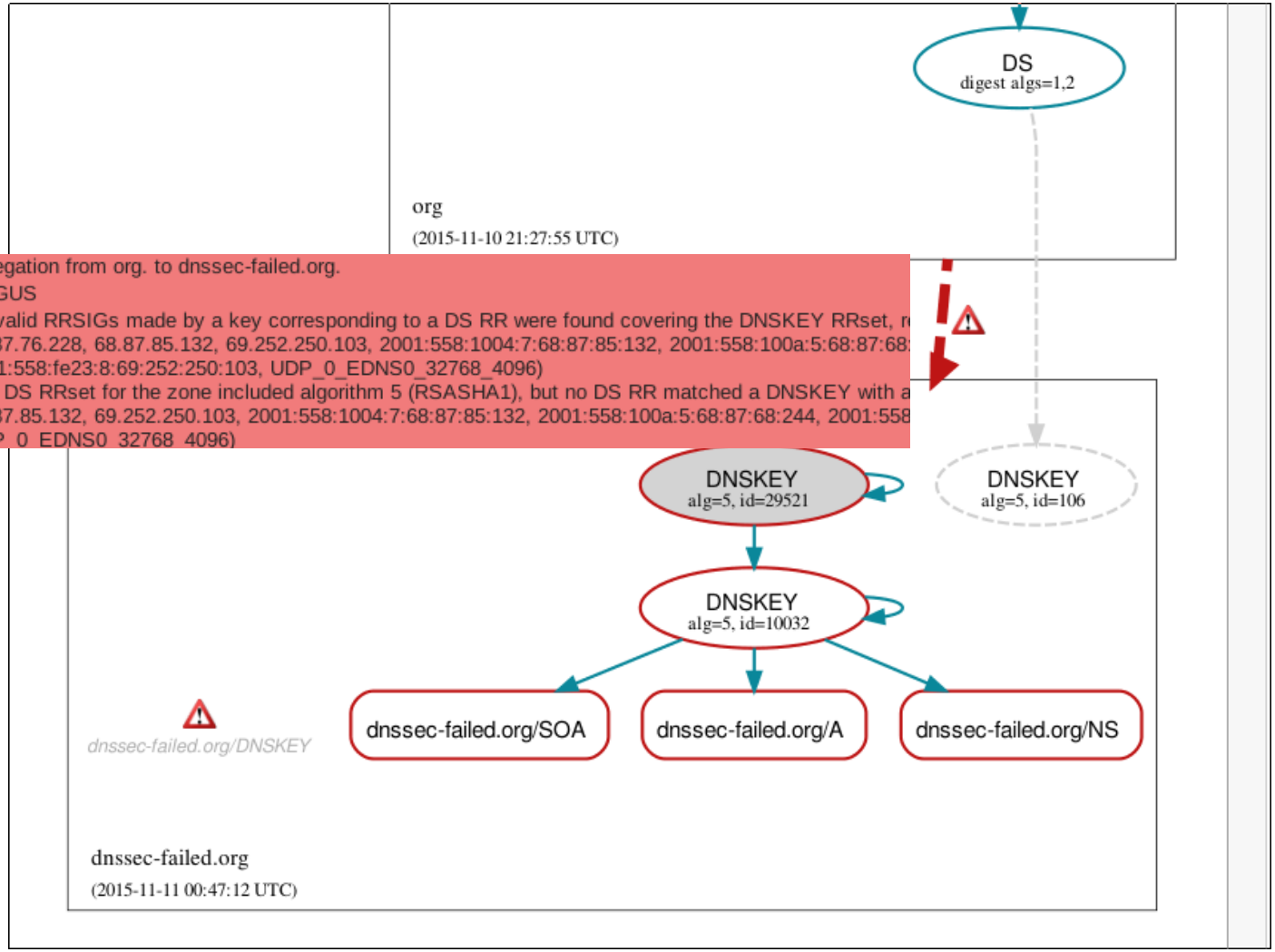
- drill –S

```
$ drill -k root.auto.anchor -S www.iij.ad.jp
;; Number of trusted keys: 1
;; Chasing: www.iij.ad.jp. A


DNSSEC Trust tree:
www.iij.ad.jp. (A)
|---iij.ad.jp. (DNSKEY keytag: 50334 alg: 8 flags: 256)
    |---iij.ad.jp. (DNSKEY keytag: 10876 alg: 8 flags: 257)
    |---iij.ad.jp. (DS keytag: 10876 digest type: 2)
    |   |---jp. (DNSKEY keytag: 46491 alg: 8 flags: 256)
    |       |---jp. (DNSKEY keytag: 53899 alg: 8 flags: 257)
    |       |---jp. (DS keytag: 53899 digest type: 2)
    |       |   |---. (DNSKEY keytag: 62530 alg: 8 flags: 256)
    |       |       |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
    |       |---jp. (DS keytag: 53899 digest type: 1)
    |           |---. (DNSKEY keytag: 62530 alg: 8 flags: 256)
    |               |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
    |---iij.ad.jp. (DS keytag: 10876 digest type: 1)
        |---jp. (DNSKEY keytag: 46491 alg: 8 flags: 256)
            |---jp. (DNSKEY keytag: 53899 alg: 8 flags: 257)
            |---jp. (DS keytag: 53899 digest type: 2)
            |   |---. (DNSKEY keytag: 62530 alg: 8 flags: 256)
            |       |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
            |---jp. (DS keytag: 53899 digest type: 1)
                |---. (DNSKEY keytag: 62530 alg: 8 flags: 256)
                    |---. (DNSKEY keytag: 19036 alg: 8 flags: 257)
;; Chase successful
```

解析

- dnsviz.net



解析

- DNSSEC Analyzer

Analyzing DNSSEC problems for dnssec-failed.org

.	✓ Found 2 DNSKEY records for . ✓ DS=19036/SHA-1 verifies DNSKEY=19036/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
org	✓ Found 2 DS records for org in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=62530 and DNSKEY=62530 verifies the DS RRset ✓ Found 4 DNSKEY records for org ✓ DS=9795/SHA-1 verifies DNSKEY=9795/SEP ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG=1445 and DNSKEY=1445 verifies the DNSKEY RRset
dnssec-failed.org	✓ Found 2 DS records for dnssec-failed.org in the org zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=1445 and DNSKEY=1445 verifies the DS RRset ✓ Found 2 DNSKEY records for dnssec-failed.org ✗ None of the 2 DNSKEY records could be validated by any of the 2 DS records ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG=29521 and DNSKEY=29521/SEP verifies the DNSKEY RRset ✗ The DNSKEY RRset was not signed by any keys in the chain-of-trust ✓ dnssec-failed.org A RR has value 69.252.80.75 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=10032 and DNSKEY=10032 verifies the A RRset

Move your mouse over any ✗ or ⚠ symbols for remediation hints.

おまけ: DNSSEC failureのバリエーション

- Comcast DNS (blog)
- 2012/01/10~ DNSSEC validation
- 2012/01/24~ failure report (nasa.gov)
- 74件のDNSSEC failure

おまけ: DNSSEC failureのバリエーション

- 署名有効期限切れ 23件
- DSと署名の非対応 15件
  - 概ねKSKロールオーバー失敗かと
    - 新鍵をpublishしていない
    - TTL考慮不足
    - DS更新忘れ
  - 署名してないのにDSを登録(!?)
- pMTU discovery問題 6件

IIJ Internet Initiative Japan

Any Questions ?

Ongoing Innovation