いますぐDNSSECで遊ぶには

--- 世の中が対応するまで待ってられない ---

JPRS / 株式会社日本レジストリサービス

藤原和典 <fujiwara@jprs.co.jp>

2009/9/4 dnsops.jp BoF

いますぐDNSSECで遊びたい

- 使ってるTLDや、使いやすいTLDはまだ対応してません
  - .SEなら登録できるけど、、、高い？
  - .ORGはまだDS受け付けてくれません
- DLVなら既存ドメイン名でDNSSEC可能
  - TLDが対応したら、移行すればよい

DLV

- RFC 4431: The DNSSEC Lookaside Validation (DLV) DNS Resource Record
- RFC 5074: DNSSEC Lookaside Validation (DLV)
- DNSSECは、ルートからの権限委任と同じ形で信頼の連鎖を構築します
- DLVではDLVを提供する事業者により各組織の鍵情報(DS)が署名されます
  - 既存ドメイン名の鍵情報をDLVに登録できます
  - DLVリソースレコードはDSと同じ内容
  - TLDが対応してなくても大丈夫です
- DLVは、TLDの対応が完了するまでの時間稼ぎだと考えられているようです

ISC DLV

- ISCはBIND 9の開発元
- ISCがDLV登録サービスを現在は無償で提供中
  - https: //dlv.isc.org/
  - BIND 9.7では一行でDLV設定可能
    - dnssec-lookaside auto;
- しばらくISC DLV生活をしてみるのはいかがでしょうか

DLVでの登録

- たとえば、ISC DLVに登録すると、以下の情報が登録されます
  - dig fujiwara.asia.dlv.isc.org dlv
  - ;; ANSWER SECTION:
  - fujiwara.asia.dlv.isc.org. 544 IN DLV 24643 5 1 AB8BDA49046FA5C2F244851CB023D45FF7AAEDFF
  - fujiwara.asia.dlv.isc.org. 544 IN DLV 24643 5 2 056B40CADE140C943C4CD785AEC1EB3CD76FE0E2E2DB429CCA16593B 01473EB8
- dlv.isc.org以下に fujiwara.asia というエントリが登録され、DS情報がDLVとして登録されています。

DLVでの検索

- すべてのDNS検索時に、DLVに情報が登録されているか確認します
  - 例: dlvがない場合 (www.example.com)
    1. www.example.com.dlv.isc.org DLV 検索
    2. example.com.dlv.isc.org DLV 検索
    3. com.dlv.isc.org DLV 検索
    4. DLVがないことを検知
  - 例: dlvがある場合 (www.fujiwara.asia)
    1. www.fujiwara.asia.dlv.isc.org検索
    2. fujiwara.asia.dlv.isc.org検索 → 存在応答
- すべてのクエリでDLVが存在するか調べるため、無駄なクエリが発生する問題点があります

DLVでの検証の設定

1. BIND 9.7の導入
2. named.conf の修正
3. named再起動

1: BIND 9.7の導入

- ISCからBIND 9.7の最新をとってきてinstallしました
- 現在はBIND 9.7.0a2です
- アルファ版だからといって動かないわけではありません
- ./configure –with-openssl=yes; make; make install ぐらい？

- 9.6だとDLVの設定が一行ですまないので https://dlv.isc.org/ よんでください

2: named.confの微修正

- Options中に以下の三行を追加しました
  - dnssec-enable yes;
  - dnssec-validation yes;
  - dnssec-lookaside auto;

- 9.3、9.4あたりでPid-fileの場所が変わっているので注意しましょう

3: named再起動

- これでDLVでの検証が有効になります

DLVでの検証例

```
% dig +dnssec isc.org mx
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3,
    AUTHORITY: 5, ADDITIONAL: 9
;; ANSWER SECTION:
isc.org.  2143  IN   MX      10 mx.isc.org.
isc.org.  2143  IN   MX      13 mx.ams1.isc.org.
isc.org.  2143  IN   RRSIG   MX 5 2 43200
    20090928233314 20090829233314 48684 isc.org.
      SIGNATURE
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
```

自ドメイン名のDNSSEC対応

1. BIND 9.7の導入
2. named再起動
3. 補助ツール作成 dnssec.sh
4. ゾーンファイルの微修正
5. named.confの修正
6. 鍵生成 dnssec.sh keygen ゾーン名
7. 署名　dnssec.sh sign ゾーン名
8. 定期的な再署名の設定
9. ISC DLVへの登録

3: dnssec.sh

- dnssec-keygen, dnssec-signzone, rndcをそのままつかうのは不便なのでshell scriptを書きました
- http://member.wide.ad.jp/~fujiwara/dnssec/ に置いています
- Usage:
  - dnssec.sh keygen ゾーン名　で鍵生成
  - dnssec.sh sign ゾーン名　　で署名
- Shell scriptなんで適度に直せます

4: ゾーンファイルの微修正

- ゾーンファイルのファイル名を変更
  - /etc/namedb/master/ゾーン名
  - 例: /etc/namedb/master/fujiwara.asia
- ゾーンファイルに以下を追加
  - $INCLUDE “ゾーン名.keys”
  - 例: $INCLUDE “fujiwara.asia.keys”

- パスなどはdnssec.shやnamed.confとあわせて変更してください

5: named.confの微修正

- DNSSEC対応するゾーンのゾーンファイル名を ゾーン名.signed に変更

```
zone “example.com” in {
    type master;
    file “/etc/namedb/master/fujiwara.asia.signed”;
};
```

6: 鍵生成

- dnssec.sh keygen ゾーン名
  - 例: dnssec.sh keygen fujiwara.asia
  - 鍵のパラメータは標準では
    - ZSK 1024bit RSASHA1
    - KSK 2048bit RSASHA1
    - /etc/namedb/masterに鍵ファイルが生成される
  - 同時にdnssec.sh signで使うファイルを生成
    - /etc/namedb/master/config/ に生成

7: 署名

- dnssec.sh sign ゾーン名
  - 例: dnssec.sh sign fujiwara.asia

  - 標準ではNSEC方式
  - SERIALは署名時のunixtime
  - 勝手にrndc reload するので注意

8: 定期再署名

- crontabに以下を毎週実行するように登録
  - dnssec.sh sign ゾーン名
  - 8 8 * * * root /etc/namedb/master/dnssec.sh sign fujiwara.asia

9: ISC DLVへの登録 (1)

- https://dlv.isc.org/ にアクセス
- Registerでアカウント生成
- Manage Zones でゾーン設定

9: ISC DLVへの登録 (2)

- Manage Zones でゾーン設定
  - Add Zoneで、ゾーン追加
  - Add DNSKEY Recordで公開鍵登録
    - コピーペーストか、ファイルのアップロード
    - /etc/namedb/master/ゾーン名.keys ファイルのなかの、”DNSKEY 257”を含む行をいれる
  - dlv.ドメイン名に指定されたTXT RRを追加すると認証するといわれるのでゾーンファイルにコピーして署名、reloadする（dnssec.sh sign ゾーン名）
- しばらく待つとドメイン名.dlv.isc.org に DLV RR が追加されます

*:鍵更新

- そのうち dnssec.sh に機能追加します。
  - KSKとZSKの更新が必要
  - KSKを変更するとISC DLVの設定も変更しないといけません
    - Add key したあと認証コードを追加

署名検証

- dig ドメイン名 soa などしてAD=1であることを確認します

```
% dig fujiwara.asia soa
;; flags: qr rd ra ad; QUERY: 1, ANSWER:
AUTHORITY: 3, ADDITIONAL: 5
;; ANSWER SECTION:
fujiwara.asia.          3600    IN      SOA     f.fujiwara.asia.
    postmaster.fujiwara.asia. 1251786921 3600 900 1209600
    900
fujiwara.asia.          3600    IN      RRSIG   SOA 5 2 3600
    20091001053521 20090901053521 23397 fujiwara.asia.
    SIGNATURE
```

まとめ

- 個人でもDNSSECで遊べます
  - http://member.wide.ad.jp/~fujiwara/dnssec/ にメモを書いています
- TLDが対応したら、DSをTLD Registryに登録すればよいだけです
- TLDが対応するまでのつなぎとしてISC DLVで遊ぶのはいかがでしょうか？