DNSSECの拡張と BIND 9.7の新機能、 小規模なDNSSEC遊びその後

藤原和典
<fujiwara@jprs.co.jp>
<fujiwara@wide.ad.jp>

2009/11/24 dnsops.jp BoF

DNSSECを拡張するRFC

- RFC 5011: トラストアンカーの自動更新
- RFC 5155: NSEC3 (略)
- RFC 5625: DNS Proxy Implementation Guideline
- RFC 5702: RSASHA256, RSASHA512の追加

RFC 5011

- DNSKEYのFlagにRevoke bitを追加
  - Bit 8 ... MSBから0開始で数えるので128
  - 従来は 256(ZSK), 257(KSK)
  - RevokeされたKSKだと 385 となる
  - Revoke bitが1のDNSKEY(自己署名あり)は、
    永久的に無効として扱うこと (MUST)
    トラストアンカーのリストからは永久的に消すこと
  - 通常のDSを使うDelegationでの鍵更新では不要
    - DNSKEYがキャッシュされていれば、緊急でRevokeしても対応できない
    - DNSKEYがキャッシュされていなければ、緊急にDNSKEYをいれかえるだけで、古い鍵はされない

RFC 5011 (2)

- トラストアンカーを初期設定しておく
- 現在有効なトラストアンカーで署名されている新しいトラストアンカーを信用
  - 有効なトラストアンカーとして追加
  - 信用する条件: Add Hold-Down時間 (30日) 連続して有効にゾーンに存在すること
- RevokeやRoll over手順も規定

RFC 5625

- DNS Proxy Implementation Guidelines
- DNS Proxyを実装するガイドでBest Current Practiceなので実装しなければならないもの

- EDNS0対応、TCP対応
- DO bit, AD bit, CD bitを通過させること
- Proxyが知らないRRなどを通過させること
- DNSレスポンスサイズの要件
- など

RFC 5702

- Use of SHA-2 algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
- 従来は、RRSIGの作成にはSHA1の結果を暗号化していた
- SHA1のかわりにSHA256, SHA512を使う
- 暗号自体はRSAで同じ

- BINDでは9.7に実装された
- RootのDNSSEC対応ではRSASHA256を使用することとなっている

BIND 9.7での変更点

- DNSSEC for Humans
- RSASHA256, RSASHA512対応
  - 9.6系に入るかは不明
- DNAME
  - DNAMEが生成するCNAMEのTTLが0から DNAME TTLに変更 → キャッシュ可能

DNSSEC for Humans

- Smart Signing
  - 鍵ファイルに日付情報を追加
  - dnssec-signzoneコマンドが署名時に自動的にDNSKEYをゾーンにマージ
  - dnssec-signzoneコマンドが署名時に鍵の日付情報と属性を見て鍵を選定
  - namedによる自動署名も拡張
- RFC 5011対応

鍵ファイルの拡張

- Version 1.2から1.3へ
- 日付情報が追加
  - -P:Publication date → ゾーンに出す時刻
  - -A:Activation date → 署名鍵として使用開始する時刻
  - -R:Revocation date → 破棄時刻
  - -I:Inactivation date → 署名鍵としての使用をやめる時刻
  - -D:Deletion date → ゾーンから消す時刻
- dnssec-keygen, dnssec-settimeにて指定可能
- dnssec-signzone, namedが鍵の時刻情報を参照

Smart Signingの例 (1)

```
% cat > tld                                    ゾーンファイル
tld. 3600 IN SOA a.tld. postmaster.tld. 1 3600 300 86400 600
tld. 3600 IN NS ns.tld.
ns.tld. 3600 IN A 192.168.0.1
% dnssec-keygen -q -f ksk tld        KSK生成
Ktld.+005+20353
% dnssec-keygen -q -I +604800 -D +1209600 tld
     今すぐ有効になり、一週間後(7*86400)に署名に使用しなくなり、
     二週間後(14*86400)にゾーンから消えるtldのZSK生成
Ktld.+005+22332
% dnssec-keygen -q -A +604800 -I +1209600 -D +181440 tld
    一週間後(7*86400)に有効になり、二週間後(14*86400)に署名に使用しなくなり、
    三週間後(21*86400)にゾーンから消えるtldのZSK生成
Ktld.+005+22512
```

Smart Signingの例 (2)

% dnssec-signzone –S tld
Fetching KSK 20353/RSASHA1 from key repository
Fetching ZSK 22332/RSASHA1 from key repository
Fetching ZSK 22512/RSASHA1 from key repository
Verifying the zone using the following algorithms: RSASHA1.
Zone signing complete:
Algorithm: RSASHA1: KSKs: 1 active, 0 stand-by, 0 revoked
ZSKs: 1 active, 1 stand-by, 0 revoked
tld.signed

現在有効なKSKは1つ、現在有効なZSKは1つ
ゾーンには来週から署名に使用されるZSKをstand-byで1つ

一週間後にdnssec-signzone –S tldすると、stand-byキーで署名するはず

Dynamic Update + DNSSEC

- Dynamic UpdateによるDNSSEC署名の強化
  - 9.6では#ifdefで抑制されていた機能のサポート
  - NSECゾーンからNSEC3ゾーンへの変更
  - NSEC3PARAMの変更
  - 未署名ゾーンにDNSKEY RRを追加することでnamedによる署名開始
  - 署名済ゾーンからDNSKEY RRを削除することでDNSSEC対応をOFFに
- ゾーンにauto-dnssecオプションの追加
  - KEYの自動生成・更新などの制御
  - rndc sign

RFC 5011 トラストアンカー自動更新

- named.confに以下を記述

managed-keys {
    “domain” initial-key Flag Protocol Algorithm “public-key-data”;
};

- Trusted-keysと似た記述 (initial-keyが追加)
- 更新された鍵情報は、managed-keys.bindというゾーンに保存される (どこに保存されるのか？)

- ルートやTLDがRFC 5011に対応すれば使える
- dlv.isc.orgのトラストアンカーはすでに対応済?
  - dns-lookaside auto;

BIND 9.7.0の新コマンド

- dnssec-revoke [options] keyfile
  - 鍵を書き換えてrevoke bitを1にする
- dnssec-settime [options] keyfile
  - 鍵の時刻情報を変更する
- dnssec-keyfromlabel -l label [options] name
  - Pkcs11ハードウェア(HSM)からDNSKEYを取り出す
- dnssec-dsfromkey (9.6から)
  - DNSKEYからDSを作成する

BIND 9.7の新コマンド (2)

- arpaname　IPアドレス
  - IPアドレスから逆引きドメイン名生成
- genrandom
  - generate a file containing random data
- journalprint　ファイル名
  - journalファイルを見やすく表示
- nsec3hash　salt hash iteration domain
  - nsec3のドメイン名生成

9.7.0 betaで直面した問題

- Ixfr-from-differencesがNSEC3 ownernameに対して最小の差分を出さない → レポート後対応済み
  - 9.6~9.7.0b2: 差分生成時にすべてのNSEC3 ownernameのRRの削除・追加という差分を生成
- dnssec-signzoneでSmart Signを使用せず、署名鍵を明に指定しても、指定しない鍵も含めて署名に使用する
  - 使用しない鍵はdnssec-signzoneから見えないところに置かないといけない → dnssec.shのアップデートへ
  - 9.7.0alphaからbetaになったところで変わった、おそらくバグ

DNSSEC遊びその後

- 現在の家の設定
  - 家ではすべてのアクセスをDLV
  - named 9.7 alpha → beta
  - NAT箱はぼろくてFragment通しません
    - ほとんどのDNSSEC queryはTCPで
- 結果
  - 特に困ることなし
  - 遅いときもあるけど、ブラウザの最初のアクセスが遅いのは許容範囲
    - そのあとはキャッシュされる
  - sshdの逆引きはとめてあるのでremote login時は問題なし
  - ssh loginは、一度つないだらつなぎっぱなしなので問題なし
- dnssec.sh
  - 複数個所メインテナンスするのをやめるために機能追加

dnssec.sh

- http://member.wide.ad.jp/~fujiwara/dnssec/dnssec.sh

1. CentOSでも動くように修正 (以前はFreeBSDでのみ確認)
2. BIND 9.7.0beta に対応 (9.7.0のバグっぽい挙動に対応)
   - BIND 9.6, 9.7の双方で動くが、9.7のdnssec-keygenで生成した新しいフォーマットの鍵は9.6では使用できないことに注意
3. ZSK Rolloverに対応
4. KSKのDS表示機能追加 dnssec.sh status zone(s)
5. dnssec.shと同一ディレクトリのdnssec.confを読むように改良
   - dnssec.sh自体の変更をする必要は減った
   - 同じdnssec.shを自宅と会社の両方で使用

- 9月のバージョンからは、鍵を置くディレクトリを変更したので互換性ありません。