権威サーバでの DNSSEC

2015/1/15

JANOG35@静岡

IIJ 山口崇徳

DNSSEC って?

- DNS + 電子署名
- DNS にはキャッシュがある
  - もちろん DNSSEC でも
- 権威 DNS サーバからすでに消えた情報でも、キャッシュがまだ生きている可能性がある
  - キャッシュまで含めて完全性を担保しなければならない

キャッシュを考慮した運用

- 署名や鍵の公開について、手順を厳密に守る必要がある
  - 鍵を切り替えるときに、古い鍵による署名も検証できるように、一定期間は新旧の署名鍵を同時に見えるようにしておく、など
  - DNSSEC のプロトコルそのものとは別
- 手順を守らないと検証に失敗する(こともある)
  - キャッシュの状態によって、あちらでは検証できるけどこちらではダメということが起きうる

めんどくさい

dnssec-signzone

- BIND のおまけの署名コマンド

NAME

dnssec-signzone - DNSSEC zone signing tool

SYNOPSIS

dnssec-signzone [-a] [-c class] [-d directory] [-e end-time] [-f out-put-file] [-g] [-h] [-k key] [-l domain] [-i interval] [-I input-format] [-j jitter] [-N soa-serial-format] [-o origin] [-O output-format] [-p] [-r randomdev] [-s start-time] [-t] [-v level] [-z] [-3 salt] [-H iterations] [-A] {zonefile} [key...]

- 引数をたくさん指定する必要がある
- 鍵の名前などパラメータがしょっちゅう変わる

めんどくさい

DNSSECの運用

- めんどくさい作業手順
- めんどくさいコマンド

- 手作業でトラブルなしで運用するのは極めて困難

だから DNSSEC やらないの?

正しい運用

× 煩雑で間違いやすいけど手でがんばる

× 煩雑で間違いやすいからやらない

○ 煩雑で間違いやすいから自動化する

IIJ の DNSSEC

- Web UI でチェックボックスを on にするだけ
- 完全自動化
- 煩雑な作業なし
  - ユーザも、IIJ の中の人も

俺流 DNSSEC

- 個人所有のドメインを自家製スクリプトで DNSSEC 運用中
- ほぼ完全に自動化
  - DS 更新のみ手作業(年1回だけ)
- 煩雑な作業なし

- 自分の近辺では、DNSSEC 運用に手間も時間もほとんどかかってない
  - DNSSEC は煩雑でめんどくさい、という風評とは無縁
  - スクリプトはどちらも自作したので、その開発・保守コスト、学習コスト、ユーザサポート程度
    - 既存のものを使うならだいぶ削れるはず

DNSSEC は可用性が落ちる?

- 人間は間違える生き物である
  - 作業手順をきちんとマニュアル化しても、失敗がゼロになるわけではない
  - 精神論(正しい手順を心がける)は愚策
- 運用支援ツールで作業手順をシステム化して、人間の介入するポイントを極力減らす
  - OpenDNSSEC、DNSSEC-Tools、自作など
  - 可用性にそれほど大きな影響なく運用できる

自動化システムの障害

- もちろん、自動化した部分が原因で障害になることもありうる
  - IIJ では導入当初、DNSSEC を off にしたドメインの DS レコードが消されない(場合がある)というバグがあった
- システムが増える以上、署名なし DNS より可用性が上がることはありえない
  - とはいえ、完全手作業よりはミスも手間も確実に減る

DNSSEC 運用失敗事例

- dnssec.jp に事例集あり
  - http://dnssec.jp/?page_id=979
  - http://dnssec.jp/?page_id=890
- 「多くの失敗は署名の有効期間からの逸脱や鍵管理に関するものであるが、それぞれの根本原因に共通点は多くは見つからなかった」
- …とあるんだけど、改めて見直してみると、このうちのいくつかは自動化システムをしっかり作りこめば防げたのではないか?

まとめ

- 権威サーバでの DNSSEC は自動化すべし
  - 手作業でトラブルを起こしてない例があったとしても、それは単なる偶然であって褒めてはいけない
- ちゃんとシステム化すれば、世間で喧伝されるほどキケンなシロモノではない
  - そのためのツールに関する情報が不足してるのは否めない
- 運用が不安ならアウトソースするのも一案

ところで...

DNSSEC 対応の流れ

1. example.jp ゾーンに署名する
2. 署名に使った KSK 鍵に対応する DS レコードを親ゾーン(jp)に登録してもらう

DS 登録

- DS はドメイン所有者からレジストリに直接登録するのではなく、レジストラ経由で登録する
  - レジストリ: ドメイン管理組織(.jp なら JPRS)
  - レジストラ: ドメイン登録事業者(お名前.com など)
- レジストラが DS を取り次いでくれないと、DNSSEC に対応したくてもできない
- 現状、大半のレジストラが DS 取次に未対応
  - DNSSEC 対応するにはレジストラを移管するか、そうでなければあきらめるしかない

レジストラへのお願い

- あるドメインを DNSSEC に対応させるか否かを決めるのは、ドメイン所有者であるべき
  - レジストラがその判断を妨げるべきではない
- DNS ホスティングで DNSSEC 署名をやってくれとまでは言わない
- せめて DS の取次には標準で対応してほしい