失敗事例研究まとめ

平成 24 年 4 月

DNSSEC ジャパン 運用技術 WG

目次

1. はじめに

1.1. 背景

2010 年 7 月にルートゾーンでの DNSSEC の運用が開始されて以来、各 TLD 運用組織でも本格的に DNSSEC 導入が進んできている。一方で、先行して導入した組織においては、様々な DNSSEC に関連する運用トラブルが発生している。DNSSEC ジャパン運用技術 WG では、先行導入組織における失敗事例を調査および考察することで、将来 DNSSEC を導入する組織に対しての知見とすべく、失敗事例情報をまとめた。なお、調査した失敗事例全体から総括した考察については、別資料にまとめているので参照されたい。

- DNSSEC 運用失敗事例の研究 総括

  http://dnssec.jp/?page_id=979

1.2. 注意事項

- 免責事項

本ドキュメントは保証されたものではない。下記 Web サイトの免責事項を確認のうえ、本ドキュメントを使用して頂きたい。

http://dnssec.jp/?page_id=16

- 問合せ先

本ドキュメントに関する改善点などのコメントは下記事務局まで連絡いただきたい。

DNSSEC ジャパン事務局 <sec@dnssec.jp>

2. 失敗事例の紹介

以下の情報は 2012 年 6 月～2012 年 8 月までに開催した WG 会合において調査・考察した内容のサマリーである。失敗事例として調査した内容はこの会合日時以前に発生し、かつ公表されていた失敗事例を対象としている。このため、2012 年 8 月以降に発生した事例については、ここでは対象としていない。

2.1. Jun/5/2010 arpa

- http://dnssec-deployment.org/pipermail/dnssec-deployment/2010-June/003872.html
- 署名有効期限切れ。

- 原因
- ISC DLV は署名の有効期限が切れると自動で DS を抜く。そして再度署名が有効になると DS が復活する。

- 教訓
- 署名の有効期限はきっちり管理・把握してなくてはならない。

2.2. Oct/7/2010 be

- https://lists.dns-oarc.net/pipermail/dns-operations/2010-October/006166.html
- 署名有効期限切れ。

- 原因
- KSK は 2 つあったが片方だけしか DS 登録してなかった。

- 教訓
- どの KSK から生成した DS を上位ゾーンに登録しているか把握しておく必要がある。

2.3. Sep/11/2011 uk

- http://blog.nominet.org.uk/tech/wp-content/uploads/2010/09/dnssec-incident-report.pdf
- 署名検証不能。HSM 不具合。

- 原因
- 予備系との鍵同期に難があった中でハードウェア故障。

- 教訓
- TTL は長すぎると不幸。不幸があったときの連絡体制の確立。(DNS 障害のため障害該当ドメインでのメールは機能しなくなる。)

2.4. Sep/16/2011 mozilla.org

- http://blog.mozilla.com/it/2010/09/16/mozilla-outage-report-mozilla-org-dnssec-09162010/
- 署名検証不能。

- 原因
- 手順ミス。DNSSEC 対応まだ開始してないのに、先に DS 登録してしまった。

- 教訓
- 手順書が必要。

2.5. Feb/12/2011 fr

- http://www.afnic.fr/en/about-afnic/news/operations-news/4237/showOperational/study-and-action-plan-following-the-incident-with-validating-resolvers-on-12-february-2011.html
- 検証不能。

- 原因
- HSM 不具合と bind のバグ。

- 教訓
- 監視対象が適切ではなかったため検知できず。ゾーンの整合性確認もできるようにする必要がある。
- 障害時の連絡体制の確立が必要。

2.6. Feb/22/2011 kg

- http://dnssec-deployment.org/pipermail/dnssec-deployment/2011-February/004816.html
- 署名が未来の時間(+6 時間)なので検証不能。

- 原因
- サーバの内部時計がローカルタイムに設定されていた。

- 教訓
- サーバのクロック設定は hwclock、date のずれなど、セットアップ時に充分気をつけること。

2.7. e164.arpa, ripe.net, 0.a.2.ip6.arpa

- Mar/4/2011 e164.arpa
- https://lists.dns-oarc.net/pipermail/dns-operations/2011-March/006945.html
- Apr/14/2011 ripe.net & Apr/15/2011 0.a.2.ip6.arpa
- https://lists.dns-oarc.net/pipermail/dns-operations/2011-April/007206.html
- KSK キーロールオーバーで不具合発生。

- 原因
- サードパーティ製 Proxy ツールの bug が直接的な要因だが・・・。

- 教訓
- 外的な公開前に、内側で One Step 検証を踏む必要がある。
- システムの更正と DS のロールオーバーとを一緒にやった。一つずつ適時行うべきだった。
- ロールバックの手順がない。
  - Point of no return の意識がない。
  - アトミックにするべき処理を重ねて行った結果、システムの整合性が取れなくなった。

以上