2012 年 5 月 10 日
DNSSEC ジャパン
運用技術 WG

DNSSEC 運用失敗事例の研究　総括

1. はじめに

1.1. 本文書について

DNSSEC の運用では、特に権威 DNS サーバにおいては通常の運用よりはるかに複雑なシステムや運用手順が必要とされる。鍵の更新ミスやゾーン署名有効期限切れなどで、ゾーンデータの整合性が失われると署名の検証に失敗することになる。ルートや TLD レベルでの DNSSEC 運用が始まってから 1 年以上が経過するが、複数の TLD 等で署名検証が失敗するような事例が報告されている。

DNSSEC ジャパン 運用技術 WG では、主に TLD 等の権威 DNS サーバでの DNSSEC 運

用の失敗事例を研究した。失敗事例の研究は、以下から入手可能である。
http://dnssec.jp/?page_id=890
この文書では、それらの事例から得られた知見を以下に総括する。

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. 失敗事例の分析

権威 DNS サーバでの DNSSEC 運用の失敗は、ほとんどが署名されたゾーン検証に失敗する、というものである。それぞれの事例について、公開されているレポートから原因を読み取り、反省点とその対策を議論、検討した。

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。まったく同じ失敗をしないようにという意味では参考になるが、そこから一般的な要因を見いだすことはできなかった。署名システムはレジストリシステムや業務システムと連携していることが多く、システムが複雑化しているため、不具合の発生を未然に防止することには限界がある。

また、事例では DNS ソフトウェアそのものや HSM のバグに由来する不具合もあり、これらのソフトウェアや製品の導入前の事前検証をいくら綿密に行なったとしても、すべてを事前に洗いだすことは困難である。DNSSEC は実際のインターネット環境での運用が開始されてからまだ日が浅く、まだまだ未知の不具合に遭遇する可能性は無視できないレベルであると考えられる。

3. 失敗への対応

そのため、WG での議論では、署名や鍵更新の失敗は起こりえるものであり、そのことを想定してシステムや運用手順を組み立てるべきである、という結論になった。以下に、WG での議論から一般的に役に立つと思われるプラクティスとしてまとめたものを紹介する。

(1) ゾーンデータの公開前の検証

DNS では、検索されたレコードは TTL で定めた時間キャッシュ DNS サーバにキャッシュされるため、一般的な死活監視のようにシステムの外からの監視では障害復旧までの時間が長引いてしまう。DNS の障害が長時間継続することは許容されないため、署名や鍵更新の失敗は、署名したゾーンを権威 DNS サーバで公開する前に検知することが必須となる。

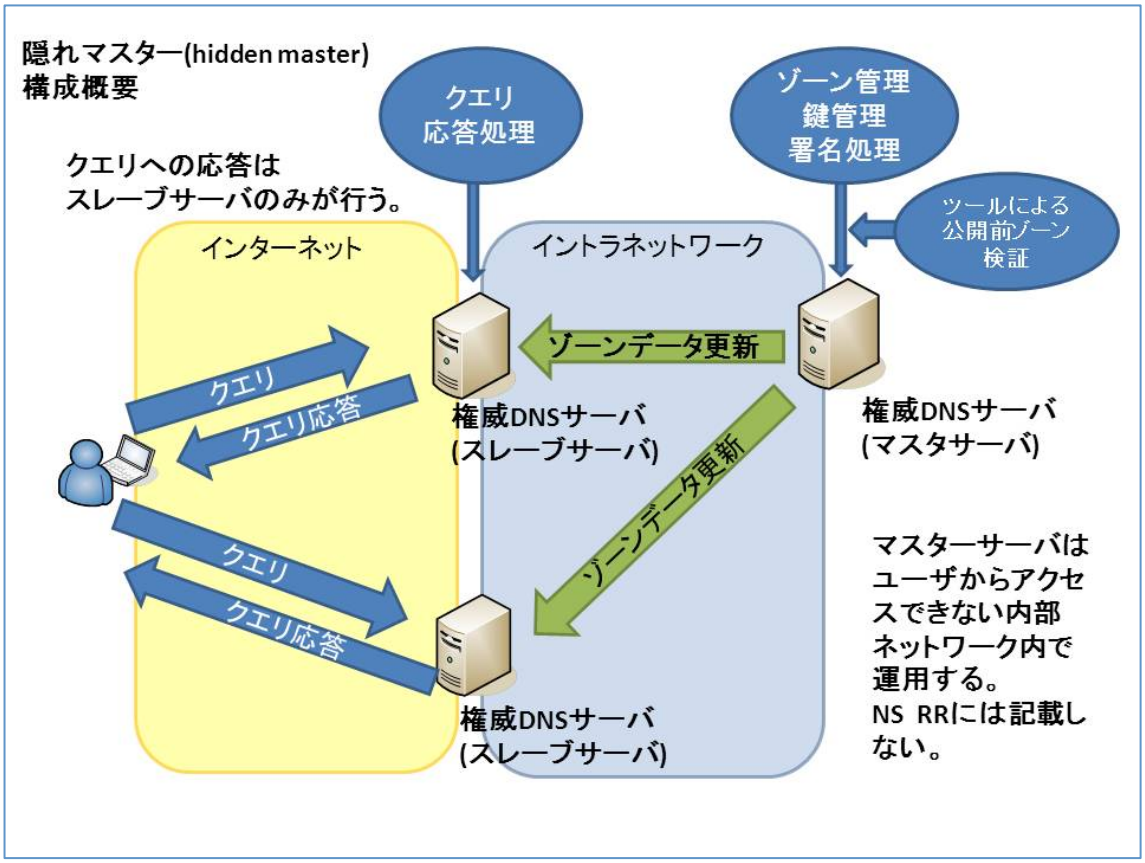
運用技術 WG で作成した別資料「DNSSEC ゾーン検証ツール調査報告」で紹介するツールでは、生成したゾーンの DNSSEC 的な整合性を含めたチェックができる。これらのツールを用いて、ゾーンの公開前にチェックすることが推奨される。

- DNSSEC ゾーン検証ツール調査報告
  http://dnssec.jp/?page_id=771

(2) 署名／鍵管理システムと対外公開権威 DNS サーバ(NS レコードとして指定するサーバ)の分離

DNS の権威 DNS サーバでは、ゾーンの NS レコードとして指定する権威 DNS サーバ群のうち、1 台をマスターサーバ、残りをマスターサーバからゾーン転送などの手段でゾーンを同期するスレーブサーバとして構成する方法がよく行なわれている。一部では、このマスターサーバを NS レコードで指定されないサーバ（隠れマスター:hidden master)とする構成が有用であることが知られている。

これと同様の考え方で、署名／鍵管理システムを隠れマスターとして論理的に分離することができる。隠れマスターである署名／鍵管理システムにおいて、署名済みのゾーンデータの整合性をチェックし、チェックを通過したゾーンデータのみを対外公開権威 DNS サーバに転送することにより、署名の結果や DNS サーバソフトウェアの不具合があったとしても、対外的に公開されている権威 DNS サーバでの障害を防止することができる。この構成では(1)でのゾーンの静的なチェックに加えて、実際に DNS サーバにゾーンを読み込ませないと発覚しないケースの障害も検出することができると考えられる。



また、hidden master については下記の資料にも言及されているので参考にされたい。

●ISC BIND9 Administrator Reference Manual

http://www.isc.org/files/arm97.pdf

1.4.4.3 項 Stealth Servers

●NIST (SP 800-81r1) Secure Domain Name System Deployment Guide

http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf

7-2-7 項 Network and Geographic Dispersion of Authoritative Name Servers

(3) 失敗時の対応の明文化

署名／鍵管理の失敗は起こりえることとして想定し、事前に検知することを前に述べた。実際に、事前に検知された時にどのような対応をとるかを検討して明文化しておくことは重要である。失敗を検知したら、定期的に行なわれている鍵の更新や再署名などのタスクを停止すること、対外公開サーバへのゾーンの同期を停止すること、また障害復旧時の再開手順などが含まれるだろう。

また、レコードの TTL や署名の有効期間などのパラメータから、失敗時にどの程度の期間権威 DNS サーバのレコード更新を停止していられるのかを把握しておくと、障害対応のフローが作りやすい。

項目(1)では、ゾーンの公開前に検証することを推奨したが、それでも公開したゾーンで失敗が発生することはありうる。その際、障害が発生しているドメイン名に依存したメール等の通信手段は機能しない可能性がある。失敗時の対応を検討する際には、DNS に依存しない電話等の連絡手段や、自ドメイン外での web やメール、SNS 等の連絡、広報手段を考慮に入れておくことが望まれる。

4. まとめ

DNSSEC の権威 DNS サーバでは、署名や鍵更新の失敗は様々の要因から完全に防止することは困難であるにもかかわらず、発生すると致命的な結果となりうる。署名／鍵管理のシステムと公開権威 DNS サーバは論理的に分離することが可能であり、権威 DNS サーバでゾーンを公開する前に失敗を検知することが重要となる。

また、失敗が発生することを想定した上で、発生時の対応を事前に検討、明文化しておくことが望まれる。

以上