DNS サーバ DNSSEC 導入
Load Balancer 機能チェックリスト

平成 23 年 1 月
DNSSEC ジャパン

DNSSEC サーバ DNSSEC 導入
Load Balancer 機能チェックリスト

（目次）

DNS サーバ DNSSEC 導入
Load Balancer 機能チェックリスト

1. はじめに

近年、インターネットの根幹を支える重要な仕組みである DNS に対して、DNS 応答を偽造することで引き起こされるセキュリティ上の脅威(キャッシュポイズニング)が顕在化している。

その対策として、DNS のセキュリティ拡張機能である DNSSEC の導入が急がれ、2010 年 7 月、ルートサーバに導入されたのをきっかけに、各 gTLD,ccTLD も続々と導入に向けての施策を進めている。

1.1. 目的

「DNS サーバ DNSSEC 導入 Load Balancer 機能チェックリスト」（以下、「本ドキュメント」という。）は、DNS サーバの DNSSEC 導入に伴い、DNS サーバ上位の NW 機器においても考慮しなければならない確認事項を取りまとめ、チェックリストとして提示することで、スムーズに DNSSEC 導入ができることを目的としている。
本ドキュメントが、健全な DNSSEC 運用を確保することの一助になれば、幸いである。

1.2. 注意事項

・免責事項

本ドキュメントの内容は保証されたものではない。下記 Web サイトの免責事項をご確認頂き、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等のコメントは下記事務局までご連絡頂けると幸いである。

DNSSEC ジャパン事務局　＜sec@dnssec.jp＞

1.3. 想定する読者

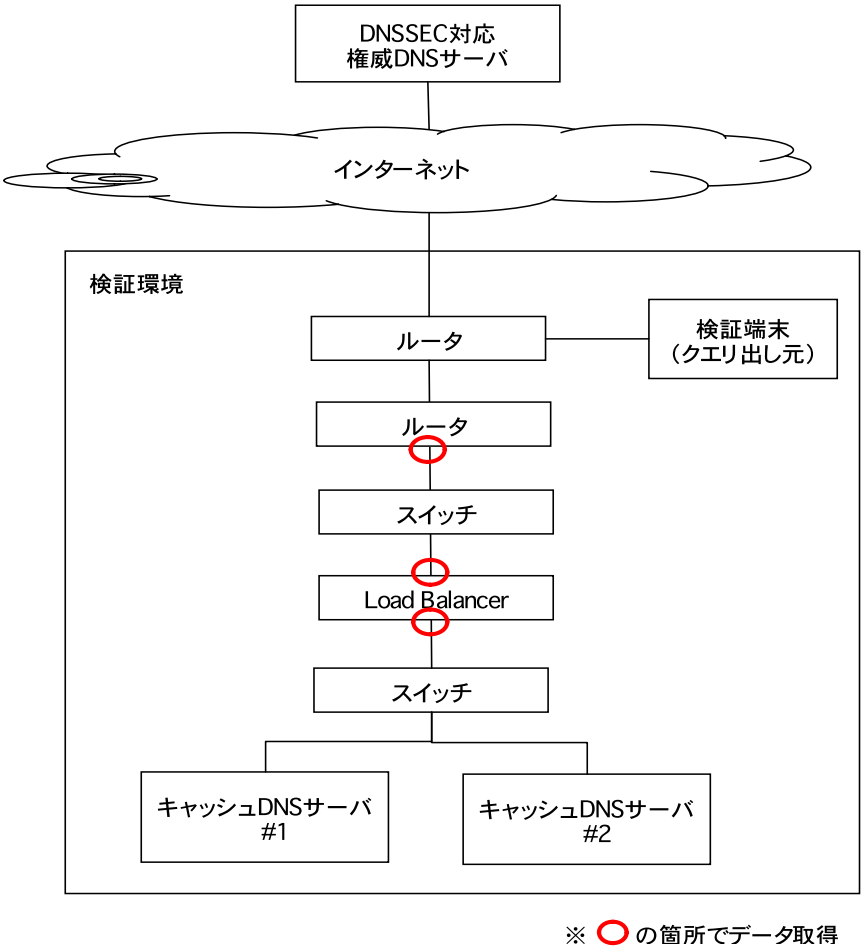
本ドキュメントは、ドメイン名を DNSSEC 対応する必要のあるドメイン名登録者、ドメインレジストラ(JP ドメイン名の場合は指定事業者)、DNS サーバ運用者を読者として想定している。本ドキュメントの完全な理解のためには、DNSSEC を含む DNS の概念について基本的な理解があることが望ましい。

・DNSSEC の仕組みと現状
http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-DNSSEC-mechanisms-and-status.pdf
・DNSSEC 導入に当たって
http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-DNSSEC-deployment.pdf
・DNSSEC 関連 RFC
http://dnssec.jp/?page_id=124
RFC 4033 DNS Security Introduction and Requirements.
RFC 4034 Resource Records for the DNS Security Extensions.
RFC 4035 Protocol Modifications for the DNS Security Extensions.

1.4. 本ガイドラインにおける前提条件

本ドキュメントは、以下の前提に基づいて作成している。

1. 以下に示すテスト環境を基に Load Balancer 機能チェックリストを作成している。



2. 構成上、DNS サーバも記載しているが、NW 機器にフォーカスをあてている。

2. チェックリスト

Load Balancer 機能における最低限確認すべき項目を以下に提示する。

#	確認項目	結果 OK / NG
1	署名検証を有効にして名前解決できること　※1	
2	署名検証を無効にして名前解決できること　※2	
3	IP フラグメントした場合も正常に名前解決できること	
4	TCP クエリでも名前解決できること	
5	大量のクエリを投げた場合も正常に名前解決できること	
6	DNS 負荷ツールで投げた場合、各組織で必要不可欠な性能がでること	
7	IP フラグメント化した上で大量のクエリを投げた場合、クエリが振り分けられていること	
8	UDP フラグメント化した上で大量のクエリを投げた場合、クエリが振り分けられていること	
9	IP フラグメントされ、再構築されたパケットの送信元が、キャッシュ DNS サーバであること	
10	UDP フラグメントされ、再構築されたパケットの送信元が、キャッシュ DNS サーバであること	
11	Load Balancer でフラグメントさせた場合も正常に問合せ結果を得ることができること	

＜補足説明＞

※ 1. 署名検証を有効にして名前解決できる場合とは、DO,CD,AD ビットが通る、EDNS0 に対応していること。

※ 2. 署名検証を無効にして名前解決できる場合とは、CD ビットが通ること。

3. 総括

DNSSEC ジャパンのメンバーが上記チェックリストを用いて使用している NW 機器を検証し、以下の知見が得られた。

- NW 機器(Load Balancer)側でも DNSSEC クエリを正常に処理できること。
- DNSSEC 導入前と比較し、DNSSEC 導入後はネットワークのトラフィックの増加、DNS サーバ側のリソース(CPU / Memory)、及び Load Balancer 側の負荷も増加すること。

そのため、NW 設計、各機器の収容設計の見直し等について検討することを推奨する。
また、各 NW 機器の設定に関しては、各組織のポリシーに則っとり適宜設定すること。

4. 参考情報

DNSSEC ジャパン(DNSSEC.jp)
http://dnssec.jp/

JPRS(DNSSEC 関連情報)
http://jprs.jp/dnssec/

JPNIC（DNSSEC)
http://www.nic.ad.jp/ja/newsletter/No43/0800.html

以上