キャッシュ DNS サーバ
DNSSEC 導入ガイドライン

平成 23 年 1 月
DNSSEC ジャパン

キャッシュ DNS サーバ
DNSSEC 導入ガイドライン

（目次）

1　はじめに
1.1 注意事項
1.2 目的
1.3 想定する読者
1.4 本ガイドラインにおける前提条件

2　シナリオシミュレーション
2.1 STEP 1【検討段階】
2.2 STEP 2【導入前段階】
2.3 STEP 3【パイロット拠点展開段階】
2.4 STEP 4【全台展開段階】
2.5 STEP 5【導入済段階】

3　参考情報

キャッシュ DNS サーバ
DNSSEC 導入ガイドライン

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が顕在化し、特にキャッシュ DNS サーバへのリスク(キャッシュポイズニング)が急激に増大している。

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 月のルートサーバ導入を契機に、各 gTLD,ccTLD も続々と導入に向けての施策を進めている。
DNSSEC の普及を進める為には、ルートゾーンや各 TLD の対応だけでなく、キャッシュ DNS サーバの対応が必要不可欠だが、現状では DNSSEC 対応に向け導入を含めたノウハウが蓄積されていない。

そこで、我々DNSSEC ジャパンでは、一般的なキャッシュ DNS サーバの構成を基に、キャッシュ DNS サーバへの設定方法だけではなく、DNSSEC の導入方法を検討した。
「キャッシュ DNS サーバ DNSSEC 導入ガイドライン」(以下、「本ガイドライン」という。)はその検討を取り纏めたもので、現在のキャッシュ DNS サーバを DNSSEC 導入する際における確認事項を取りまとめ、スムーズに導入が行えることを目的にしている。

DNSSEC ジャパンでは、本ガイドラインによって健全な DNSSEC 対応のキャッシュ DNS サーバを構築する一助になれば幸いである。

1.1　注意事項

・免責事項

本ガイドライン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、本ガイドラインを使用して頂きたい。

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

・問合せ先

本ガイドライン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＞

1.2　目的

本ガイドラインは、キャッシュ DNS サーバの DNSSEC への導入において、何を以て DNSSEC への導入ができたかの指標として、一般的なキャッシュ NW 構成を基にチェックリストを提示し、健全な DNSSEC 運用を確保することを目的とする。

1.3　想定する読者

本ガイドラインは、既にキャッシュ DNS サーバを運用しており、且つ、キャッシュ DNS サーバの DNSSEC への導入を考えている、ISP、DNS サーバ運用者を読者として想定している。本ガイドライン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 ジャパンが公開している下記の文書を参考にするとよい。

・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.

1.3　本ガイドラインにおける前提条件

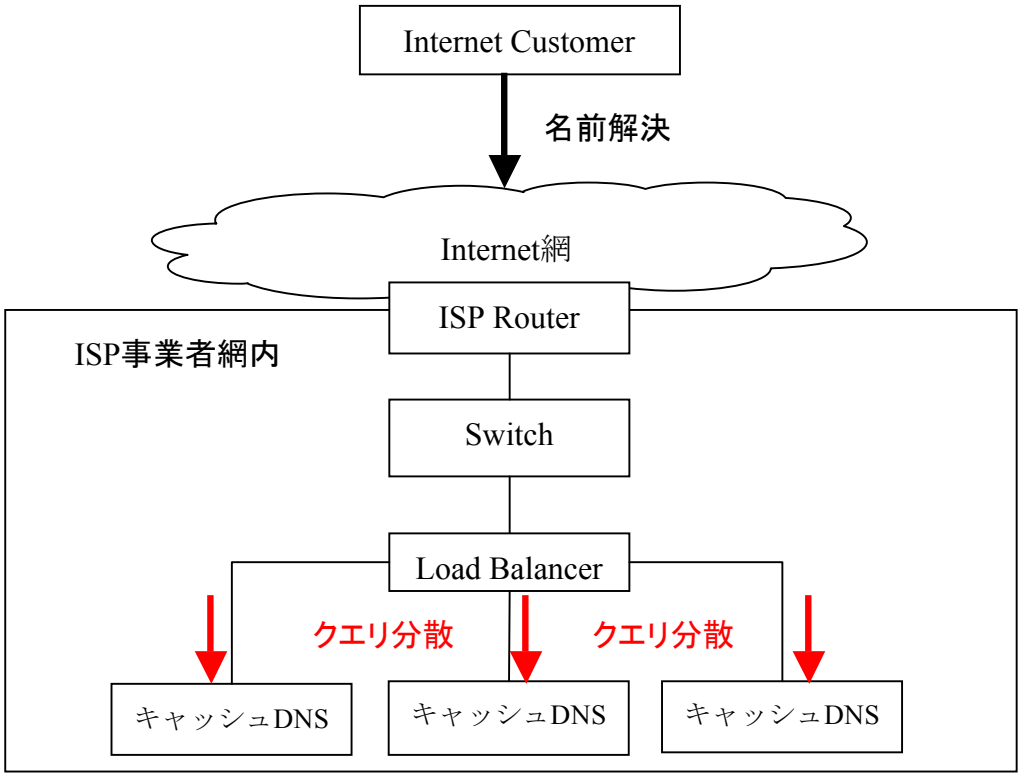
本ガイドラインは、以下の条件を踏まえ、安全な導入フローを作成している。

1. DNSSEC 対応するキャッシュ DNS サーバは、既に運用しているサーバの導入方法を想定している。

2. Load Balancer を経由した負荷分散構成下におけるキャッシュ DNS サーバを対象に、DNSSEC への導入シナリオ及びチェックリストを作成している。

3. キャッシュ DNS サーバのアプリケーションは広く使用されている BIND とする。

● 前提条件 2.の図



2.シナリオシミュレーション

現在キャッシュ DNS サーバを運用している ISP、DNS 運用者が、DNSSEC へ導入するにあたり【準備段階】【導入前段階】【パイロット拠点展開段階】【全台展開段階】【導入済段階】の 5 ステップに分けて DNSSEC への導入を行うと想定し、各ステップで必要な検討項目を提示する。

また、導入に関して、STEP1 から順番に進めることを推奨する。

2.1 STEP 1【準備段階】

・DNSSEC 導入を検討する前に、まず自ネットワークにおいて下記事項を把握することを勧める。

1. 運用中（DNSSEC 導入前）のキャッシュ DNS サーバの統計情報。
   例：サーバリソース（CPU、MEM 使用率)、クエリ数、TCP/UDP パケット数など
2. DNSSEC 導入における概算費用(設備投資費、稼動費など)の試算。
3. DNSSEC 導入に伴う工数試算（導入計画)。
4. DNSSEC 対応するアプリケーションのバージョン確認。
   最新のバージョンを適用することを推奨する。

2.2 STEP 2【導入前段階】

・DNSSEC 導入前にキャッシュ DNS サーバに対し検証環境下で負荷試験を実施し、導入後の影響を調査することを勧める。特に注意すべき点は以下の通り。

1. DNS 負荷試験ツール(resperf,queryperf 等)で大量のクエリを投げた場合も正常に名前解決出来ること。
2. DNS 負荷試験ツールで大量のクエリを投げた場合、各組織のポリシーで定めたクエリを処理できていること。
3. 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ること。
4. キャッシュ DNS サーバに対し以下の 4 パターンの性能試験を実施し、クエリ処理能力、NW 帯域の変化、リソースの変化等を確認し、キャッシュ DNS サーバのスペック、収容設計の見直し、増設等の検討を推奨する。

（DNSSEC 対応パターン）

キャッシュ DNS サーバ DNSSEC の設定有り × Cache 情報有り
キャッシュ DNS サーバ DNSSEC の設定有り × Cache 情報無し
キャッシュ DNS サーバ DNSSEC の設定無し × Cache 情報有り
キャッシュ DNS サーバ DNSSEC の設定無し × Cache 情報無し

※上記の『DNSSEC の設定有り』とは、署名検証を有効にしていることを指す。
※上記の『DNSSEC の設定無し』とは、署名検証を無効にしていることを指す。

2.3 STEP 3 【パイロット拠点展開段階】

・パイロット拠点に対して、以下のチェック項目を基に、DNSSEC への導入が問題ないと判断できた場合、全台展開のステップへと進む。

1. キャッシュ DNS サーバで DNSSEC の設定が出来ること。

●BIND における DNSSEC の設定

- named.conf の options の中で dnssec-enable と dnssec-validation が明示的に no と設定されていないこと。
- named.conf に下記のように trusted-keys を追記し公開鍵を登録すること。

```
trusted-keys {
        ※公開鍵情報※
};
```

- 必要に応じて、忘れずに新しい公開鍵を追加しておくこと。
- トラストアンカーの設定方法、及び、ルートゾーンの公開鍵の更新確認については、DNSSEC ジャパンが公開している下記文書を参考にすること。

DNSSEC を利用するリゾルバーのためのトラストアンカーの設定方法について
http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-dnssec-trustanchor-install-howto.pdf

- 署名検証を無効にして名前解決出来ること。
- 名前解決時に時間がかかりすぎたり、タイムアウトが発生したりしないこと。
- 署名検証を有効にして名前解決出来ること。
- 名前解決時に時間がかかりすぎたり、タイムアウトが発生したりしないこと。
- 署名検証が成功している(ad ビットがたっている)こと。
- 署名検証が失敗した場合には、再度 cd ビットをたてレスポンスがあること。
- クライアントから UDP クエリで名前解決出来ること。
- 権威 DNS サーバから UDP クエリで名前解決出来ること。
- クライアントから TCP クエリで名前解決出来ること。
- 権威 DNS サーバから TCP クエリで名前解決できること。
- IP フラグメントした場合も正常に名前解決出来ること。
- UDP フラグメントした場合も正常に名前解決できること。
- Load Balancer でフラグメントさせた場合も正常に問い合わせ結果を得ることが出来ること。
- DNSSEC の機能面だけでなく、NW 帯域にも注意すること。

（特に権威 DNS サーバ→キャッシュ DNS サーバの NW 帯域）

2.4 STEP 4【全台展開段階】

・チェック項目は【パイロット拠点展開段階】時と同様。

2.5 STEP 5【導入済段階】

・定期的にデータ（各ステップで提示した検討項目等）を把握して傾向監視を継続すること。

・業界の DNSSEC 対応状況やアプリケーションのバージョン情報も把握することを推奨する。

3.参考情報

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