DNS設定におけるよくある間違い
&
DNS設定チェックリスト

インターネット総合研究所

伊藤 高一

kohi@iri.co.jp

Q.1

PC UNIXより遅いので始末に困っていた3年前のワークステーションをネームサーバにした。

保守契約には入っていないのでOSは3年前のままだが、運よくnamedがOSについてきていたので、それを使っている。

3年前のnamedにはセキュリティホールが存在します。

BINDでセキュリティホールが見つかっていないのは以下のバージョンだけです。

- 4.9.11
- 8.2.7
- 8.3.4
- 9.2.1
  - 資料作成時点、TxB、rcなどは除く。

BIND 9.2.1をインストールしているが、レゾルバライブラリのセキュリティ対策のためにOSのパッチを当てた。

○

BIND 9では、意識的にインストールしないとレゾルバライブラリはコンパイルすらされません。

後からレゾルバライブラリをインストールしても、バイナリを再リンクしたり動的ライブラリのモジュールを差し替えるなどしないと、元々のルーチンが使われています。

Q.3

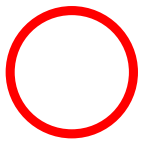
11月の頭にメーリングリストでnamed.rootがどーのこーのと書いてあるメールが流れてきたが、英語だったので読み飛ばした。

×

11月5日にJ.ROOT-SERVERS.NET.のアドレスが変更されたnamed.rootが配布されました。

Q.4

メールサーバはyamada.nishiki.gr.jp.というホストがやっているが、MXレコードにはmail.nishiki.gr.jp.と書きたかったので、yamadaとは別にmailというAレコードを作ってyamadaと同じIPアドレスを書いた。



mailのAレコードを作らずにyamadaを指すCNAMEレコードを作ってはいけません。同様にNSのRDATAもaliasではいけません。

– (RFC2181)

送信元のMTAによってはMXを要求してCNAMEが返ってくると無視する実装もあるそうです。

ちなみに次ホップでのReceived:ヘッダにはmailではなく逆索きして得られたyamadaが表示される可能性があります。

Q.5

ルータのSerial4/0:17に振ったアドレスを DNSに登録するのに

Serial4/0:17.ko.nishiki.gr.jp.

という名前でAレコードとPTRレコードを設定した。

×

ホスト名は

- **数字またはアルファベットで始まり**
- **数字、アルファベット、ハイフンを繰り返し**
- **数字またはアルファベットで終わること**

になっています。

- (RFC1035,RFC1123)

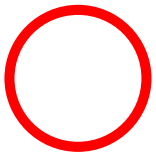
メールサーバは

- yamada.nishiki.gr.jp.
- sasa.nishiki.gr.jp.

の2台なのでnishiki.gr.jp.ゾーンに

```
@   IN   MX 10 yamada.nishiki.gr.jp.
    IN   MX 20 sasa.nishiki.gr.jp.
```

と設定した。



末尾の‘.’を忘れると相対表記と解釈され

```
yamada.nishiki.gr.jp.nishiki.gr.jp.
sasa.nishiki.gr.jp.nishiki.gr.jp.
```

に展開されてしまいますので注意しましょう。

ISPから来たセカンダリネームサービスの案内という紙に書いてあったセカンダリのホスト名を自分のところのNSレコードに書いた。

プライマリの設定さえしておけば、商売なんだから後はISPが勝手に設定して当然だ。

×

参照すべきマスタのIPアドレスがわからなければISP側も設定のしようがありません。

ましてやセカンダリの希望の有無は、言われなければもっとわかりません。

Q.8

ISPからの案内にしたがって

32/27.0.168.192.in-addr.arpa.

というゾーンを設定したが、逆索きできないのでメーカーのサポートを呼んだところ、「ゾーン名が間違ってますね」と言って

0.168.192.in-addr.arpa.

に直してくれたら索けるようになった。

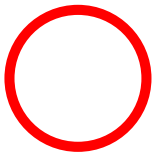
やはりISPのサポートよりメーカーのサポートの方が腰も低いしソフトのことをよく知っているので頼りになる。

×

RFC2317を使う場合はISP側の設定が済まないと逆索きできません。

ユーザ側が/24に対応するゾーン名で設定してしまうとISP側からauthorityが委任できないばかりでなく、ユーザ側でも同じ/24に同居するサイトの逆索きができなくなります。

古い本に載っていた例ではSOAレコードの最後の数字が86400になっていたが、$TTL 86400と書いたので、SOAレコードの最後の数字は7200に設定した。



SOAレコードの最後の数字は、以前はTTLのデフォルト値でしたが、BIND 8以降ではnegative cacheのTTLに意味が変更されています。

Q.10

マスタサーバのホスト名は
miyama.nishiki.gr.jpで

```
@ IN NS miyama.nishiki.gr.jp.
```

と設定しているが、ns.nishiki.gr.jpの方が体裁がいいので、JPRSにはns.nishiki.gr.jpというホスト名で登録した。

×

例えばクライアント側のサーバで

```
nishiki.gr.jp. IN NS ns.nishiki.gr.jp.
```

はキャッシュ上にあり、ns.nishiki.gr.jp.**のA**レコードのTTL**が切れると**authority**にたどり着けなくなります。**

また実装によってはmiyama**が返した**NS**レコードを無視する物もあるようです。**

Q.11

www.nishiki.gr.jp.とimap.nishiki.gr.jp.は
tochi.nishiki.gr.jp.を指すCNAMEレコード
として定義していたが、tochi.nishiki.gr.jp.
のリースが切れたので、tochi.nishiki.gr.jp.
のAレコードもkoto.nishiki.gr.jp.を指す
CNAMEレコードに書き換えた。

これでwwwとimapもkoto.nishiki.gr.jp.を指
すようになった。

△

循環参照を避けるために、多段CNAME**の段数が制限されている実装もあります。**

- BIND 4.x/8.x: 8**段**
- BIND 9.x: 16**段**
- djbdns: 4**段**

Authority**側のサーバではなくクライアント側のサーバに依存するので、使わないのが無難です。**

Q.12

NOTIFYが導入されたので、ゾーンデータを変更した後、serialを増やす必要はなくなった。

×

NOTIFYが届かないこともありますし、解釈しない実装もあります。

それ以前にNOTIFYはSOAが変更されたことの通知なので、NOTIFYが飛んできたのに実際にはserialが変化していなければ、slaveはゾーン転送しないかもしれません。

- 最後までお付き合いありがとうございました。
- あなたのサーバ、大丈夫でしたか?

Errata

×

例えばクライアント側のサーバで

```
nishiki.gr.jp. IN NS miyama.nishiki.gr.jp.
```

はキャッシュ上にあり、miyama.nishiki.gr.jp.**のA**レコードのTTL**が切れると**glue**がないので**authority**にたどり着けなくなります。**

このような状況が発生するシナリオについては森下さんのスライド#33,#34(NS**レコードの取り扱い)を参照して下さい。**