DNS Summer Day 2019

XACK DNS開発とRFC

株式会社XACK

技術部　松原 豊和

会社概要

XACK とは

- ネットワークアプリケーションシステムのソフトウェア開発

こんな製品を作っています。

- XACK RADIUS：大規模システム向け高性能RADIUSサーバ
- XACK DHCP：DHCPサーバ（IPv4/v6-PD対応）
- XACK DNS：通信事業者向けセキュアDNSサーバ (GUI対応)
- XACK DNS Zone Editor：XACK DNS マルチテナント編集システム

XACK DNS Zone Editor 編集可能ゾーン一覧画面

登録ユーザごとに編集・参照可能なゾーン一覧を表示

XACK DNS Zone Editor ゾーン編集画面

GUIによる直感的な操作でのゾーン編集

リアルタイムにエラーを検知

XACK DNSとは

XACK DNSの特徴

- フルスクラッチ開発のDNSサーバ
- 権威サーバ、フルリゾルバ、フォワーダー、etc…
- モジュール化による機能の足し引きが可能
- 仮想サーバ機能(BINDのView機能相当)
- XACK DNS Manager(GUI)を無償バンドル
- 通信事業者様や企業・大学様での採用実績あり

RFC (Request for Comments)とは

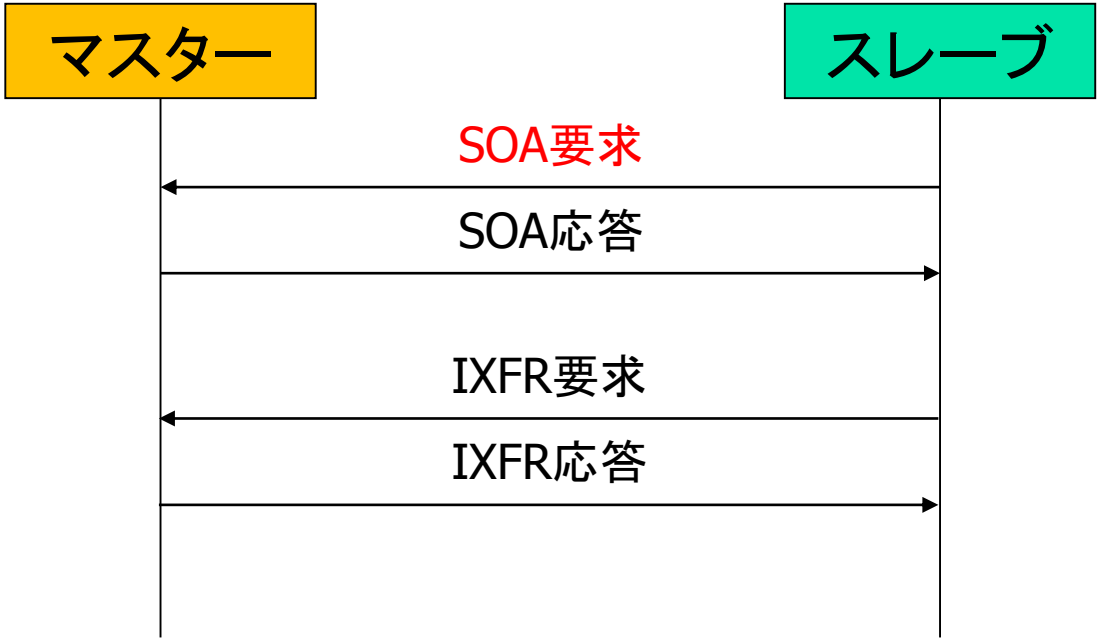
- IETFによる技術仕様の保存や公開を示します。主にプロトコルやデータフォーマットが取り扱われます。標準仕様。

- XACK DNSもRFCに準拠するように開発しています。
- ですが、一部の記述で曖昧な点などがあります。

- 開発中にどう扱うべきか、どのように解釈すべきかなど困った事例や悩んだ事例をご紹介します。

1. 差分ゾーン転送

- 最初にスレーブからSOA要求を行う目的は？
- スレーブ側でマスターに更新があったかを確認するため。



1. 差分ゾーン転送

- 差分ゾーン転送のRFCはRFC 1995（最新）。

> 2. Brief Description of the Protocol
>
> If an IXFR client, which likely has an older version of a zone, thinks it needs new information about the zone (typically through SOA refresh timeout or the NOTIFY mechanism), it sends an IXFR message containing the SOA serial number of its, presumably outdated, copy of the zone.

- スレーブからのSOA要求は直接的に書かれていないような、、

1. 差分ゾーン転送

- RFC 1034に記述があります。

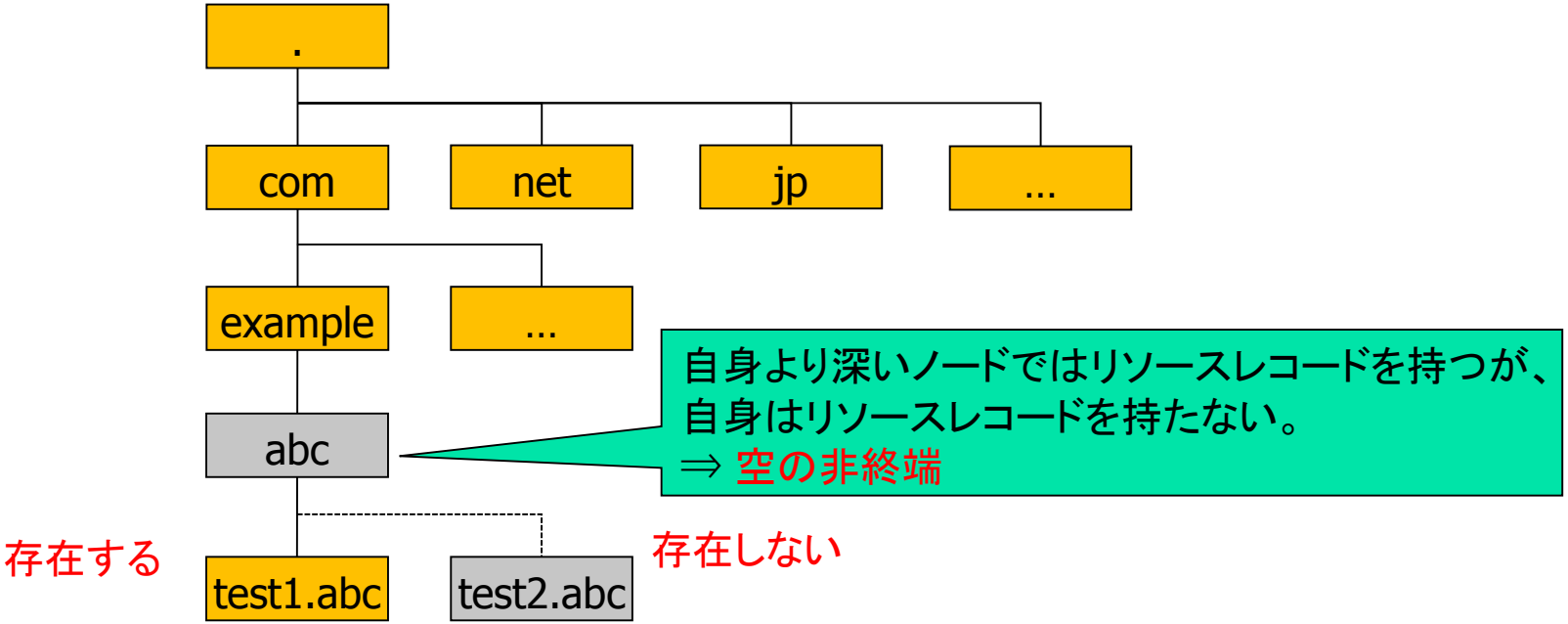
> 4.3.5. Zone maintenance and transfers
> ～（中略）～
> Whenever a new zone is loaded in a secondary, the secondary waits REFRESH seconds before checking with the primary for a new serial. If this check cannot be completed, new checks are started every RETRY seconds. The check is a simple query to the primary for the SOA RR of the zone.

ポイント1:

- ある1つの機能を実現すべき内容が複数のRFCに点在する。

2. 空の非終端(Empty Non-Terminal)

- 空の非終端とは



2. 空の非終端(Empty Non-Terminal)

QNAME	レコード	RCODE
example.com	ある（頂点）	NoError
test1.abc.example.com	ある	NoError
test2.abc.example.com	ない	NXDomain
abc.example.com	ない	NoError(NoData)

- 空の非終端の問い合わせにはNoError(NoData)を応答する。
- RFC 1034,1035では一部触れられているものの、明示的に「Empty Non-Terminal」という記述はない。

2. 空の非終端(Empty Non-Terminal)

- どこに書いてある？RFC 5155に記述されています。

> B.2.1. No Data Error, Empty Non-Terminal
>
> A "no data" response because of an empty non-terminal. The NSEC3 RR proves that the name exists and that the requested RR type does not.

- RFC 8020で明記されています。

> 3.1. Updates to RFC 1034
> ～（中略）～ *ENTはEmpty Non-Terminalの略
> The correct response to ENTs is NODATA (i.e., a response code of NOERROR and an empty answer section).

2. 空の非終端(Empty Non-Terminal)

ポイント2:

- 後々のRFCで明記されるまでは動作仕様が曖昧なものがある。

3. TTL関連 ～ ゾーンファイル ～

- RFC 2181にTTLの最小値と最大値が記述されています。

> 8. Time to Live (TTL)
> ～（中略）～
> with a minimum value of 0, and a maximum value of 2147483647.
> That is, a maximum of 2^31 - 1.

- XACK DNSではこの記述を根拠にゾーンファイルに最大値を超過するTTLを設定するとエラーとしていました。

3. TTL関連 ～ ゾーンファイル ～

- RFC 2181にはこのような記述もあります。

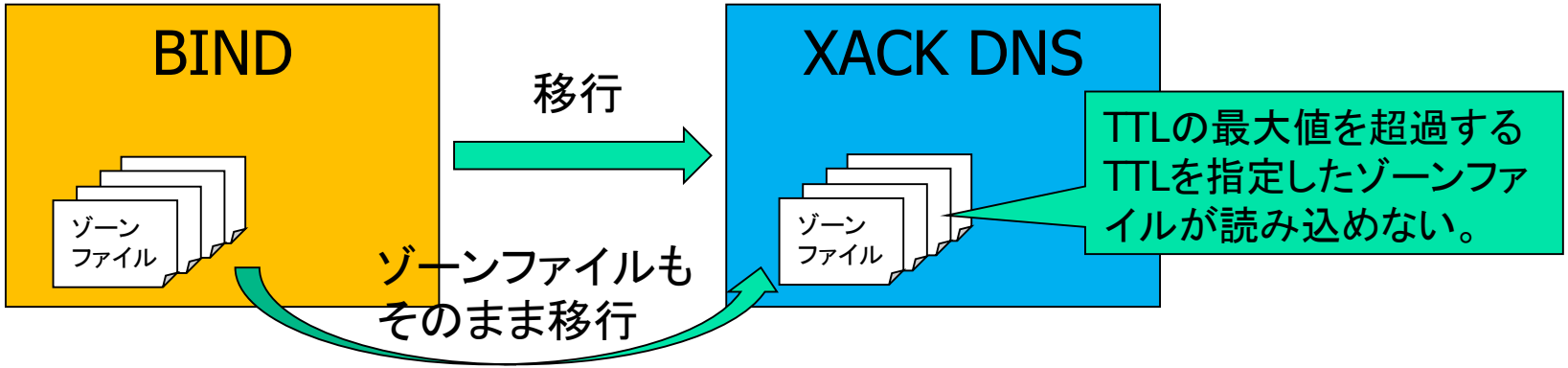
> Implementations should treat TTL values received with the most significant bit set as if the entire value received was zero.

- BINDではこの記述を根拠にゾーンファイルに最大値を超過するTTLの設定を許容する模様。（応答のTTLは0）

- XACK DNSはRFCに準拠している動作ですが、BINDは若干拡大解釈しているような、、

3. TTL関連 ～ ゾーンファイル ～

- BINDからの移行でこのようなTTLが指定されているゾーンファイルがあってもXACK DNSで受け入れたい。



- XACK DNS側も追従して、設定で許容可能としました。

3. TTL関連 ～ SOAのMINIMUM ～

- RFC 2308でSOAレコードのMINIMUMフィールドが再定義されています。

> 4 - SOA Minimum Field
> ～（中略）～
> The remaining of the current meanings, of being the TTL to be used for negative responses, is the new defined meaning of the SOA minimum field.

- ネガティブキャッシュのTTLはSOAレコードのMINIMUMフィールドとSOAレコードの小さい方を採用します。

> 5 - Caching Negative Answers
> ～（中略）～
> When the authoritative server creates this record its TTL is taken from the minimum of the SOA.MINIMUM field and SOA's TTL.

3. TTL関連 ～ SOAのMINIMUM ～

- SOAレコードのMINIMUMフィールドはTTLのように扱われますが、BINDでは最大値をTTLの最大値としていないようです。

```
$ORIGIN example.jp.
$TTL 3600
@           IN          SOA         ns1.test.jp. a.test.jp. (
                        2019062801 ; serial
                        3000 ; refresh
                        3000 ; retry
                        100 ; expire
                        2147483648 ; minimum ← TTLの最大値+1の値
                        )
```

- XACK DNS側も追従して、設定で許容可能としました。

3. TTL関連 ～ SOAのMINIMUM ～

ポイント3:

- 実装によってRFCの解釈が異なる場合がある。

3. TTL関連 ～ RRSIGレコード ～

- RFC 4034にはRRSIG RRのTTL値は、署名対象のRRsetのTTL値と一致しなければならないと記述されています。

> 3. The RRSIG Resource Record
> ～（中略）～
> The TTL value of an RRSIG RR MUST match the TTL value of the RRset it covers.

3. TTL関連 ～ RRSIGレコード ～

- RFC 4035には複数のRRSIG RRがある場合、どれか1つでもRRsetのTTLと同じであればよいようにとれる記述があります。

> 2.2. Including RRSIG RRs in a Zone
> ～（中略）～
> For each authoritative RRset in a signed zone, there MUST be at least one RRSIG record that meets the following requirements:
> ～（中略）～
> o The RRSIG RR's TTL is equal to the TTL of the RRset.

3. TTL関連 ～ RRSIGレコード ～

- RFC 4035にはこのような記述もあり、1つのRRsetで複数のRRSIG RRを持つ可能性があると示されています。

> The process for constructing the RRSIG RR for a given RRset is described in [RFC4034]. An RRset MAY have multiple RRSIG RRs associated with it.
> ～（中略）～
> In particular, the TTL values among RRSIG RRs with a common owner name do not follow the RRset rules described in [RFC2181].

- 異なるTTLを持つRRSIG RRが存在しても良いような、、

3. TTL関連 ～ RRSIGレコード ～

- 同じ所有者名で異なるTTLを持つRRSIG RRが複数ある場合、時間経過で一部のRRSIG RRが消えた時に署名検証ができなくなるのでは。
- XACK DNSでは同一署名対象のRRsetごとに、最小のTTLの値に合わせています。

ポイント4:

- エラーケースなどの記述が網羅されていない。

4. NSECからNSEC3への移行・戻し

- RFC 5155の10.4.と10.5.には署名ゾーンにおけるNSECからNSEC3への移行・戻しの手順が記述されています。

> 10.4. Transitioning a Signed Zone from NSEC to NSEC3
>
> When transitioning an already signed and trusted zone to this specification, care must be taken to prevent client validation failures during the process.
>
> The basic procedure is as follows:
> ～（中略）～
> 10.5. Transitioning a Signed Zone from NSEC3 to NSEC
>
> To safely transition back to a DNSSEC [RFC4035] signed zone, simply reverse the procedure above:

4. NSECからNSEC3への移行・戻し

- 署名ツールでできることは、以下の通り。
  1. NSEC署名を行う
  2. NSEC3署名を1つだけ行う

- したがって、署名ツールを使っての2.と3.の実施ができない。

> 2. Add signed NSEC3 RRs to the zone, either incrementally or all at once. If adding incrementally, then the last RRSet added MUST be the NSEC3PARAM RRSet.
>
> 3. Upon the addition of the NSEC3PARAM RRSet, the server switches to serving negative and wildcard responses with NSEC3 RRs according to this specification.

4. NSECからNSEC3への移行・戻し

ポイント5:

- RFCに手順が記述されているものの具体的な実行手順が示されていないものがある。

おわりに

- 標準仕様であるRFCに準拠することは製品の品質を担保する上では必要不可欠。
- 文章の解釈の違いにより、他の実装と動作が異なる場合には調整が必要。
- RFCに準拠しない対向先への考慮も必要。

- XACKではよりよい製品開発を目指して参ります。

https://www.xack.co.jp