IIJ Internet Initiative Japan

DNSの怪しい伝説を紐解く
~~怪しげな~~RR Typeたち
増え続けるRR Typeとどう付き合う？

InternetWeek 2016プログラム委員
株式会社インターネットイニシアティブ
其田　学

Ongoing Innovation

最近 RR Typeが
増えてる気がしませんか？

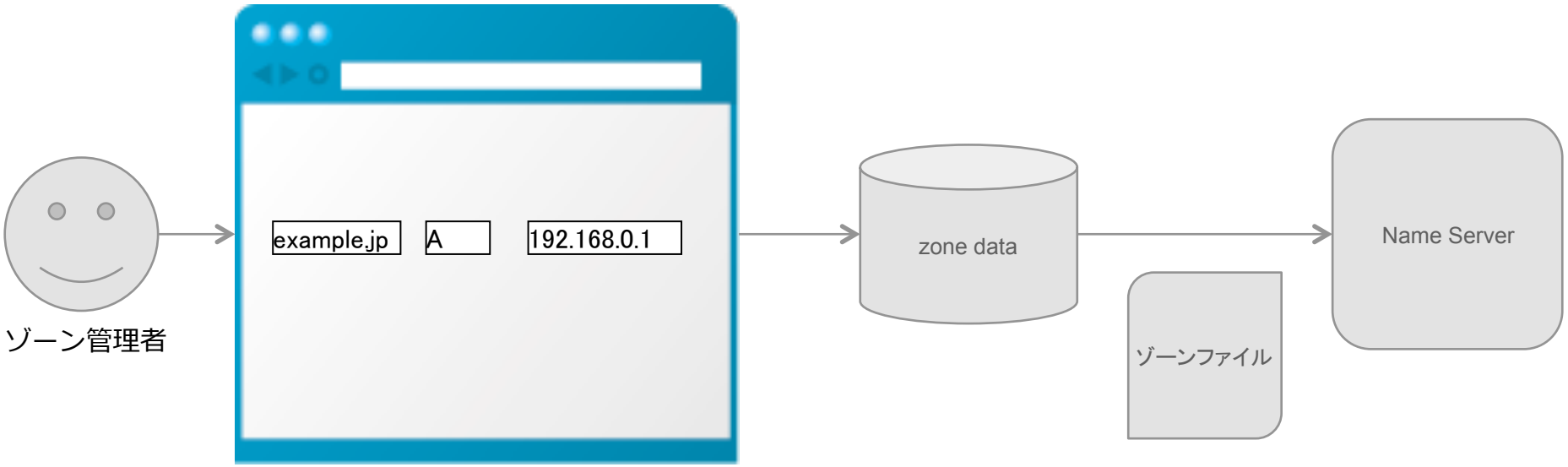
2010年から追加されたRR TYPE

HIP	LP	CSYNC
TALINK	EUI48	URI
TLSA	EUI64	OPENPGPKEY
NID	CAA	AVC
L32	CDS	SMIMEA
L64	CDNSKEY	

DNSプロバイダからすると、どれを対応すればいいのか、よく分からない。

DNSサービス提供者の視点からのRR追加

DNSサービスの概要



1. WEB画面で、RRTYPEを選んで編集

2.RRTYPE毎のRDATAのバリーデーション

3.ゾーンファイル作成＆反映

- 対応するRRを追加するのはバックエンドの処理を追加するため、結構大変
- 需要？がないRRTYPEを追加しても顧客満足度上がらない

今後需要がありそうなRRはどれか？

DNSプロバイダとして対応が求められるRRType（2017年版 ）

2017年版 DNSプロバイダーに求められるRR対応

- **選定方法**
  - 国内、国外の大手DNSプロバイダの対応状況
    - Route53
    - Google Cloud DNS
    - Azure DNS
    - Akamai
    - CloudFlare
    - Dyn Managed DNS
    - DNSimple
    - お名前.com
    - さくらインターネット
    - NTT-COM
    - NTT-PC
    - KDDI
    - IIJ
  - 最近のRRTYPEについては流行りそうなものを主観に基づいてあげます。

2017年版 DNSプロバイダーに求められるRR対応

- **カテゴリー１ 対応が必須なRR**

RRTYPE	対応数	コメント
A	13	IPv4 Address
AAAA	12	IPv6 Address
CNAME	13	Canonical Name
NS	13	Name Server
MX	13	Mail Exchange
SRV	13	Service
TXT	13	Text

- **カテゴリー１.1 DNSSECに対応している場合は、対応が必須なRR**

RRTYPE	対応数	コメント
DS	4	Delegation Signer

2017年版 DNSプロバイダーに求められるRR対応

カテゴリー２ 対応を強く推奨するRR

RRTYPE	対応数	コメント
NAPTR	5	sipで使われてるらしい
CAA	2	証明書を発行しても良いCAの情報 2017年９月から証明書発行時に確認されるようになる

カテゴリー３ 対応を推奨するRR

RRTYPE	対応数	コメント
TLSA	1	TLS証明書の検証に使える
LOC	3	緯度、経度
SSHFP	3	sshのホストのフィンガープリント

CAA

- **証明書を発行できる証明局を認可するレコード**
  - フォーマット

    CAA フラグ タグ 値

  - フラグ 0 or 1
    - 1の場合は、証明局はCAAレコードを正しく解釈する必要がある。解釈できない場合は証明書を発行してはならない。
  - タグ
    - issue
      - そのリソースレコード名の証明書を発行できる証明局を値に書く。
    - issuewild
      - そのリソースレコード名に*をつけたワイルドカード証明書を発行できる証明局を値に書く
    - iodef
      - 証明書を発行できかった場合に連絡する通知先（email, http, https)

例

```
dnsops.jp.  300  IN  CAA  0 issue "letsencrypt.org”
dnsops.jp.  300  IN  CAA  0 issuewild “;”
dnsops.jp.  300  IN  CAA  0 iodef "mailto:hoge@example.jp"
```

CAA

- **2017年９月8日から大手証明局は証明書発行時にCAAレコードを確認するようになります**
  - https://cabforum.org/pipermail/public/2017-March/009988.html
  - https://cabforum.org/pipermail/public/2017-March/009979.html

- **証明書発行にCAAレコードは必須か？**
  - 必須ではありません

- **DNSSECへの対応**
  - そもそも、CAAレコードが信用できるかという問題があります。
  - 現時点では、DNSSECの対応は必須ではありませんが！
  - 証明局のポリシーでIANA ROOTサーバからの信頼の連鎖がつながっていないCAAレコードは検索失敗として扱うことができます。
    - 対応した方が無難

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――――――――――――IIJはいつもはじまりであり、未来です。

Ongoing Innovation