ドメイン名のつかいかた

2022年06月24日 DNS Summer Day 2022

株式会社インターネットイニシアティブ
其田 学

色々なオンラインサービスを構築する上で欠かせないドメイン名

ドメイン名を利用開始するにあたって、確認、実施しておいた方が良い事を、DNS技術者目線で紹介します。

なお、本発表は個人の見解です。
私が所属している組織、団体の見解と相違があるかもしれません。

- **ドメイン名の選び方**
- **サービスの選び方**
  - レジストラサービス
  - 権威DNSサービス
- **登録すべきレコード**

ドメイン名の選び方

1. 自組織のドメイン名ポリシーを確認

- 組織によってはドメイン名登録に規則がある場合があり、
  それに従う必要があります。

- 新規の組織ドメイン名の登録が制限されている場合もあります

2. 既存のドメイン名を使うか、新規登録するか

基本的には、既存組織ドメイン名のサブドメインを利用

- 特にこだわりがない場合は、こちらが無難

要件上、新規登録する場合も

- 文字列数を短くしたい
- 既存のゾーンに影響されたくない・したくない

新規登録する場合に気をつける事

- 利用停止後も、相当な期間、登録を維持することが必要
  - Expireすると、第三者に取得されます(ドロップキャッチと言う)
    - 「ドメイン名のライフサイクルマネージメント」で検索
    - 大抵の場合は怪しいサイトに変わります。
  - 維持するのは、支払い処理を継続できるかが課題（組織面で）
  - 既に常識とは思いますが、一時的なキャンペーンサイトは絶対に新規登録してはいけない

(例)IIJの場合

- 外部公開するドメイン名に関しては、使用許可が必要
- 原則として、既存組織ドメイン名のサブドメイン名を利用する
- 例) manual.iij.jp, public.dns.iij.jp,など

- 正当な理由があれば、新規の組織ドメイン名登録も認められるが、利用終了後も10年間登録維持することが前提
  - 利用終了時はドメイン管理部署が最後まで面倒見る仕組みになっている。
- 例) dns-platform.jpなど

3. 組織ドメイン名のTLDの選び方

- **TLDの継続性**
  - レジストリの継続性
- **ネームサーバを含む、インフラの可用性**
  - Anycast DNS
  - DR対応

例) IIJ DNSプラットフォームサービスの場合

サービスサイト用ドメイン名
- **dns-platform.jp**

ネームサーバ用ドメイン名
- **d-53.jp, d-53.net, d-53.info**

選定優先度

1. JP
- ccTLDは国が無くならない限りは存続する（はず
- DNSも複数サービスを利用したAnycast DNSになっている

2. COM / NET
- gTLDが無くなることはない（新gTLDは除く）
- ベリサインが運用

3. INFO / ORG
- Afiliasが運用

サービスの選び方

DNSレコードを書き換えられたり、勝手に移管されると、
莫大な損害を被るので、セキュリティが最重要

最低でも認証、認可機能、ロギングは必須

認証、認可

- ユーザを複数作ることができ、共有アカウント状態にならないこと
  - ロギングも合わせて、誰が処理を行ったかの追跡ができること
- 多要素認証ができること
  - OTP系、FIDO系の認証ができると良い
- 認可
  - ログイン時、API実行時のACLがかけられること

ロギング

- ゾーン編集や、ネームサーバの変更などの、リソースを変更した処理を実行した時刻、ユーザを追跡可能なこと
- ログが改竄されないこと

ISMSクラウドセキュリティ認証(ISO/IEC 27017)などを利用するのも手

- **メガクラウド系とか、大手のサービスは大抵、認証取得済み**
- **自社サービスで認証取得する際も、利用するサービスが認証取得していると、対応が楽**
- **サービス側はユーザを保護する手段は提供するが、実施するのはユーザ側**
  - 責任分界点は理解しておくこと

1. 意図しないドメイン名移管を防ぐ仕組みがあること

- 移管承認時に契約者に移管の確認を実施していること
- レジストラロック

2. DNSSECに対応していること

- DSレコードの登録が可能なこと

権威DNSサービスは様々な観点が存在するが、以下は特に重要だと思うこと

1. **新しいリソースレコードタイプにも対応していること**
   - (MUST) A,AAAA,CNAME,NS,MX,TXT,CAA,SVC
   - (MAY) TLSA,SVCB,HTTPS

2. **ドメイン名の形式として、ホスト名形式が指定されていないリソースレコードタイプは、アンダースコア付きの名前が書けること**
   - 要は _dmarc.example.jp とかが書けること
   - DKIMは、NSやCNAMEで指定することが多いので、これらが書けること

3. **IPv6に対応していること**
   - AAAAは書けるのは当然として、IPv6の権威DNSサーバがあること

4. **サブドメインハイジャック対策がされていること**
   - 同一の権威DNSサーバ内に、別契約で子ゾーンを作ることができないこと
   - 権威DNSサーバが分かれている場合は問題ない

5. **DNSSECに対応していること**
   - DNSSEC運用が自動化されていること

全部個別で調べるのも大変なので、
権威DNSサービスの調査報告書も参考にしてください

登録すべきレコード

新規でドメイン名を登録し、ゾーンを作成したときに、登録を推奨するレコード

メール系レコード

- メールを使い始めるまでは、明示的にメールを送受信しないことを宣言する

1. **SPF**
   メールは送信しないという意思表示

```
@       TXT    “v=spf1 -all”
```

2. **DMARC**
   SPFと合わせて、このドメインからのメールを受信したらdropするという意思表示

```
_dmarc        TXT    “v=DMARC1; p=reject; aspf=s"
```

3. **NULL MX**
   このドメイン宛のメールは受信しないという意思表示

```
@       MX     0 .
```

新規でドメイン名を登録し、ゾーンを作成したときに、登録を推奨するレコード

証明書系

1. **CAA**
   証明書を発行できるCAを設定しておく

```
@       CAA    0 issuewild ”CA名”
@       CAA    0 issue " CA名”
```

登録しない方が良いレコード

組織ドメイン名のA,AAAAレコード

```
@       IN A 192.168.0.1
www  IN A 192.168.0.1
```

wwwと同じコンテンツを表示させたいので、組織ドメイン名にA,AAAAを書くケースが多い。
組織ドメイン名は、ゾーン名と等しいので、SOAとNSレコードが必ず存在する。
CNAMEは同名のレコードと共存できない。
つまり、ゾーンAPEXにはCNAMEレコードが書けません。

- **CNAME Flatteningは万能ではありません。サービス毎に色々な制約があります。**
- **将来的にWAFやCDNを入れたくなったときにCNAMEが書けないことにより、選択肢が狭まります。**

ドメイン名の利用は計画的に

- 新規の組織ドメイン名の登録は慎重に
  - 長期間の維持が前提
  - 登録する必要をよく考えて

- レジストラサービス、権威DNSサービス共にセキュリティが最重要
  - 共に一番クリティカルな部分

  - 今から登録するドメイン名なら、DNSSECへの対応は必須

- 登録するレコード、しないレコード
  - 迷惑メール対策で、最初にDENY ALLしましょう
  - 組織ドメイン名のA,AAAAレコードは、後々の負債になるのでやめましょう

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。