グルーレコードについて改めて考える
～ランチのおともにDNS～

2023年11月21日

Internet Week 2023 ランチタイムセミナー

株式会社日本レジストリサービス（JPRS）

森下 泰宏・礒浪 直生

今年も現地で、ランチのおともにDNS！

- 今年のInternet Weekは、**オンラインWeekとカンファレンスWeekの2本立て**で開催されています
- 今年のランチタイムセミナーはカンファレンスWeekのプログラムの一つとして、**現地開催**となりました！
- ご参加のみなさまに、**ランチ**をご提供しております！

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 所属：JPRS 技術広報担当・技術研修センター
  - 主な業務内容：技術広報活動全般・社内外の人材育成
  - 一言：**本日は満席のご予約をいただいております！**

- 礒浪 直生（いそなみ なおき）
  - 所属：JPRS システム部
  - 主な業務内容：データセンターネットワークの構築・運用、JP DNSサーバーの構築・運用
  - 一言：**Internet Week初参加です！がんばります！**

今回のテーマは「**グルーレコード**」

- **DNSができた当初から存在**
  - しかし、**仕様のあいまいさ**や**実装・運用における取り扱いの不備**により、**トラブルやセキュリティインシデントの原因**となっている
- かつ、**登録者・DNS運用者が直接取り扱う**、**基本情報**の一つ
  - レジストリに登録する「**ネームサーバーホスト情報**」
  - しかし、現在のドメイン名の登録・運用では**グルーレコードが必要な条件とネームサーバーホスト情報の登録が必要な条件が一致しておらず**、**混乱の原因**となっている

DNSの仕組みの中でも**特に面倒くさく、説明が省略されがち**な情報の一つ

本日の内容

1. グルーレコードの概要と役割　（話者：礒浪）
2. グルーレコードに関する最近の動きと現状（話者：森下）
3. DNS運用におけるあるべき姿　（話者：森下）

1. グルーレコードの概要と役割

グルー（glue）とは？

① 接着剤；のり

– quick-drying *glue*：瞬間接着剤

② にかわ（質）

出典：プログレッシブ英和中辞典 第5版

グルー ＝ 何かと何かを接着する**接着剤**

※にかわ（膠）：動物の皮膚や骨、腱などの組織に熱を加えて抽出したもので
主成分はゼラチン。古来より接着剤として使われた。

日常生活におけるグルーの例

- グルーガン
  - 特殊な樹脂を**接着剤**として塗り、さまざまなものを接着する道具

- マツエクグルー
  - まつ毛と人工まつ毛を接着する**接着剤**

- 今回のテーマは「**グルーレコード**」
  - グルーレコードは、何と何を接着しているのか？

※まつ毛エクステ（マツエク）：まつ毛に人工まつ毛を1本ずつ接着する技術。付けまつ毛より長持ちする。

グルーレコードの例

- JP DNSサーバーにjprs.jpのAレコードを問い合わせた時の応答（**委任応答**）

```
% dig +norec jprs.jp a @a.dns.jp
…
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9174
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
…
;; AUTHORITY SECTION:
jprs.jp.                86400 IN NS ns1.jprs.jp.
jprs.jp.                86400 IN NS ns2.jprs.jp.
jprs.jp.                86400 IN NS ns3.jprs.jp.
jprs.jp.                86400 IN NS ns4.jprs.jp.

;; ADDITIONAL SECTION:
ns1.jprs.jp.            86400 IN A 202.11.16.49
ns2.jprs.jp.            86400 IN A 202.11.16.59
ns3.jprs.jp.            86400 IN A 203.105.65.178
ns4.jprs.jp.            86400 IN A 203.105.65.181
ns1.jprs.jp.            86400 IN AAAA 2001:df0:8::a153
ns2.jprs.jp.            86400 IN AAAA 2001:df0:8::a253
ns3.jprs.jp.            86400 IN AAAA 2001:218:3001::a153
ns4.jprs.jp.            86400 IN AAAA 2001:218:3001::a253
```

ネームサーバーの名前に対応するIPアドレス（**グルーレコード**）

注：本資料では「ネームサーバー」を「権威DNSサーバー」の意味で使用します。

グルーレコードが接着するもの

- 委任応答のネームサーバーの**名前に対応するIPアドレス**を、**接着剤**として追加している
- つまり、**NSレコードにA/AAAAレコードを接着剤として追加する**ことで、**親ゾーンと子ゾーンを接着している**

グルーレコード = 親ゾーンと子ゾーンを接着する**接着剤**

なぜ、接着剤による IPアドレスの追加が必要なのか？

- DNSが開発された当時の**時代背景**による
  - DNSは委任先のネームサーバーを、**名前**で指定する形で設計された
    - 当時は、IPがデファクトスタンダードになるとは限らなかった

このことが、これから話す諸問題の原因になった

- ネームサーバーを名前で指定するため、名前解決の際に**何らかの方法で、名前に対応するIPアドレスを知る必要がある**
  - そのための方法の一つが、**接着剤による<u>A/AAAAレコードの追加</u>**
    ⇒ これが**グルーレコード**

ネームサーバーのIPアドレスを知る方法

- いくつかの方法が使われている
  - **情報を事前に設定しておく**
    - ルートヒント、Split DNS、Root Server Local（RFC 8806）など
  - **得られた情報を使い回す**
    - それまでに得られた情報をキャッシュし、有効活用する
  - **接着剤として情報を追加する**
    - **グルーレコード**
- これらが使えない場合、**別途名前解決**する必要がある
  - 現在の名前解決を**いったん保留**して、**ネームサーバーの名前を名前解決**する

1回目の
名前解決の
効率が下がる

パート2の内容

- DNSの実装・運用におけるグルーレコードの取り扱いについて考える場合、**委任先ゾーンとネームサーバーホスト名の関係を定義し、場合分けする**必要がある
- パート2では**グルーレコードに関する最近のIETFの活動**と、**ドメイン名登録における取り扱いの現状**について解説する

2. グルーレコードに関する最近の動きと現状

このパートで解説する内容

- グルーレコードにまつわる、以下の二つの話題を解説
  - **目的の異なる2種類のグルーレコード**
  - **.jpと.com/.netにおける**
    ネームサーバーホスト情報の取り扱いの違い

目的の異なる2種類のグルーレコード

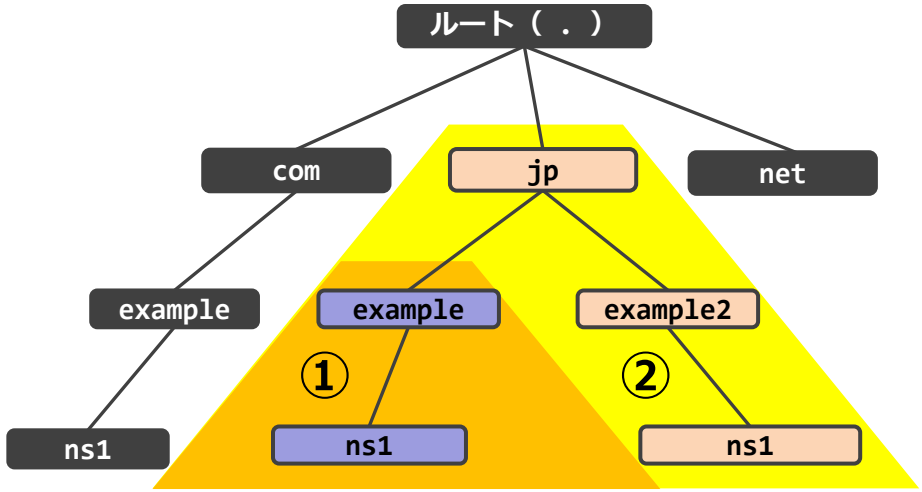
委任先ゾーンとネームサーバーホスト名の関係

- DNSの用語を定義するRFC 8499で、**4種類に整理**されている
  - In-domain/Sibling domain/In-bailiwick/Out-of-bailiwick
- In-で始まる用語が**2種類存在**する

番号	用語（RFC 8499の定義）	委任元がjpで委任先がexample.jpの場合のネームサーバーホスト名の例
①	**In-domain**	ns1.**example.jp**
②	**Sibling domain**	ns1.**example2.jp**
③	**In-bailiwick**	この表の①と②
④	**Out-of-bailiwick**	ns1.**example.com**

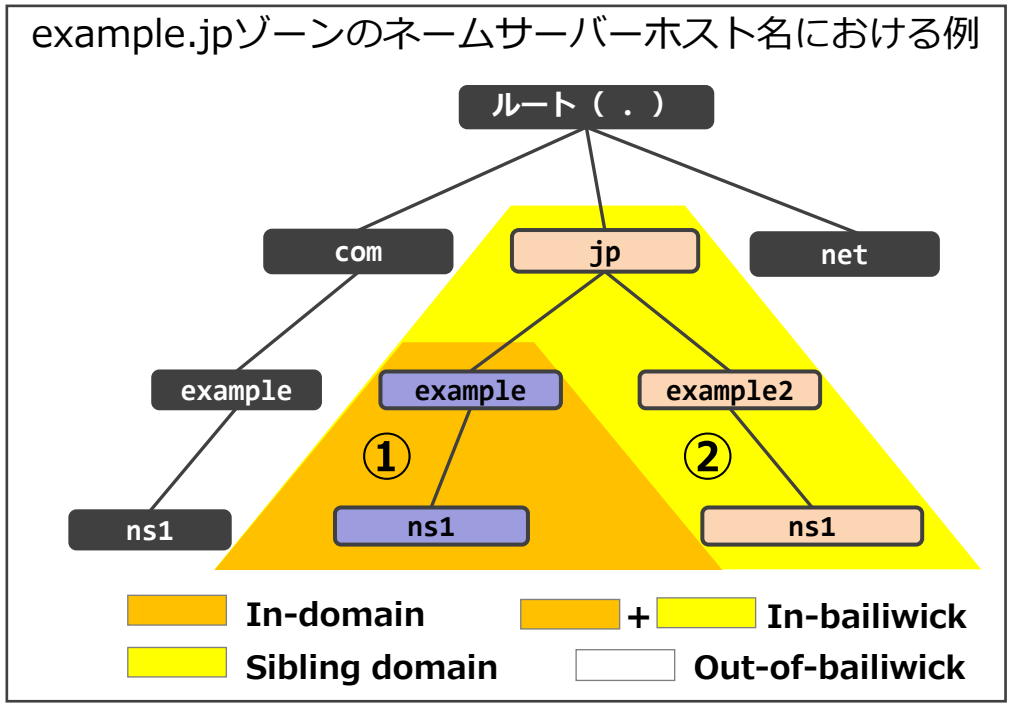
※sibling：兄弟・姉妹

example.jpゾーンのネームサーバーホスト名における例



内部名/In-bailiwickの意味の揺れ

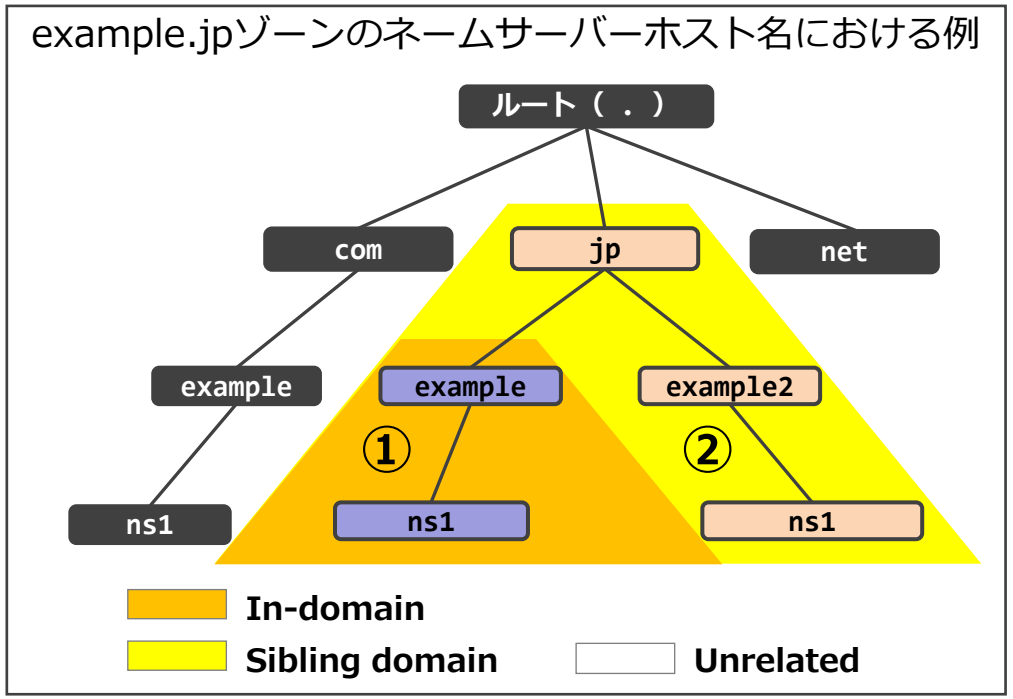
- **内部名/In-bailiwick**の意味に**揺れ**が見られる
  - **内部名がIn-domainの意味で使われる例**と、**In-bailiwickの意味で使われる例**の双方が存在する
  - 加えて、**In-bailiwickがIn-domainの意味で使われている英語の文書**も存在する
    - In-domainという用語が、技術者の間に十分に浸透していないことも原因の一つとして挙げられる



委任先ゾーンとネームサーバーホスト名の関係を示す用語の再整理

- RFC 8499を置き換え予定の**新しいI-D（draft-ietf-dnsop-rfc8499bis）**では、用語が**3種類に再整理**されている
  - IETF dnsop WGでの標準化作業は終了しており、RFC発行待ちの状態

番号	用語（rfc8499bisの定義）	委任元がjpで委任先がexample.jpの場合のネームサーバーホスト名の例
①	**In-domain**	ns1.**example.jp**
②	**Sibling domain**	ns1.**example2.jp**
③	**In-bailiwick**	**（定義が混乱を引き起こしており、historicと見なされるべき）**
④	**Unrelated**	ns1.**example.com**



In-domain/Sibling domain/Unrelated

- **In-domain/Sibling domain/Unrelated**の3種類に分類
  - In-bailiwickとOut-of-bailiwickは**historic（歴史的）**として**非推奨**に
- これを踏まえ、本セミナーでは委任先ゾーンとネームサーバーホスト名の関係について、以下の用語を使用する
  - **In-domain**（例：**example.jp**と**ns1.example.jp**）
  - **Sibling domain**（例：**example.jp**と**ns1.example2.jp**）
  - **Unrelated**（例：**example.jp**と**ns1.example.com**）

「内部名」「外部名」は混乱を避けるため、
本セミナーでは使用しない

それぞれの関係における グルーレコードの取り扱い

- 委任先ゾーンとネームサーバーホスト名の関係により、権威DNSサーバーとフルリゾルバーにおける、**グルーレコードの取り扱いが変化する**

委任先ゾーンとネームサーバーホスト名の関係	名前解決におけるグルーレコードの必要性	権威DNSサーバーにおけるグルーレコードの取り扱い	フルリゾルバーにおけるグルーレコードの取り扱い（当該A/AAAAがキャッシュされていなかった場合）
In-domain	必要	追加する	受け入れる
Sibling domain	必ずしも必要ではない	多くの実装が追加する	多くの実装が受け入れる
Unrelated	有害（後述）	追加しない	破棄する

委任先ゾーンとネームサーバーホスト名の関係とグルーレコードの取り扱いの現状

In-domainの場合の取り扱い

- 名前解決において、グルーレコードが**必要**
- 2023年9月に発行されたRFC 9471で、**応答にグルーレコードをすべて含めるか、応答サイズに制約がある場合は再問い合わせを促さなければならないことが明確化**された

> 3.1. In-domainのネームサーバーのためのグルー
>
> この文書は、ネームサーバーが参照応答を生成する時、**additional sectionにIn-domainのネームサーバーの利用可能なすべてのグルーレコードを含めるか、 メッセージサイズに制約がある場合にはTC=1を設定しなければならないことを明確にする。**

出典：RFC 9471: DNS Glue Requirements in Referral Responses（参考訳）

In-domainのグルーレコードは、**名前解決できるようにするために追加**される

Sibling domainの場合の取り扱い

- 名前解決において、グルーレコードは**必ずしも必要ではない**
- 2023年9月に発行されたRFC 9471で、**Sibling domainのグルーレコードにおける実装の取り扱いと目的が記述**された

> 2.2. Sibling domainのネームサーバーのためのグルー
>
> …
> 多くの場合、Sibling domainのネームサーバーのグルーは**名前解決にとって厳密には必要ではない。**（中略）しかし、**ほとんどのネームサーバー実装は今日、反復リゾルバーからの追加のトラフィックの必要性を回避するための最適化として、グルーレコードを提供する。**

出典：RFC 9471: DNS Glue Requirements in Referral Responses（参考訳）

Sibling domainのグルーレコードは、**名前解決の効率を上げるために追加**される

Unrelatedの場合の取り扱い

- 名前解決において、グルーレコードは**有害**
- グルーレコードは応答に**追加されず**、追加されていても受け取り側で**破棄される**
  - この動作は1997年に実行された、**Kashpureff型攻撃手法**への対策として導入された

＜参考：Kashpureff型攻撃手法＞
- 応答のadditional sectionに**管理外のA/AAAAレコードを設定**した応答を返し、キャッシュポイズニングを図る手法
- 1997年にEugene Kashpureff氏がこの方法を用いて、InterNICへのアクセスを自身が運営するAlterNICに誘導する攻撃を実行した
- 応答の**管理外のレコードを、受け取り側で破棄する**ことで対策された

まとめ：目的の異なる2種類のグルーレコード

- このように、In-domainの場合とSibling domainの場合では、**グルーレコードの目的が異なっている**ことに注意が必要
  - In-domain：**名前解決できるようにする**
    - グルーレコードは**必要**
  - Sibling domain：**名前解決の効率を上げる**
    - グルーレコードは**必ずしも必要ではない**

目的の異なる2種類のグルーレコードの存在が、
グルーレコードに関する理解の妨げになっている

.jpと.com/.netにおけるネームサーバー ホスト情報の取り扱いの違い

グルーレコードはレジストリにどう登録されるか

- グルーレコードに使われる情報は**ネームサーバーホスト情報（以下、ホスト情報）**として、レジストリに登録される


検索タイプ　検索キーワード

ネームサーバホスト情報　ns1.jprs.jp　検索　検索方法

Host Information: [ホスト情報]
[Host Name]　ns1.jprs.jp

[IPv4アドレス]　202.11.16.49
[IPv6アドレス]　2001:0df0:0008:0000:0000:0000:0000:a153

[登録年月日]　2012/01/06
[有効期限]　2024/02/29
[最終更新]　2023/11/12 08:06:07 (JST)

株式会社日本レジストリサービス Copyright© Japan Registry Services Co., Ltd.

プライバシーポリシー | 著作権 | お問い合わせ：info@jprs.jp

JPRS Whoisでns1.jprs.jpのネームサーバーホスト情報を検索した結果

.jpと.com/.netにおける取り扱いの違い

- .jpと.com/.netでは、**ドメイン名の登録における**
  ホスト情報の取り扱いに関する仕様が一部異なっている
- 異なっている仕様の例
  - ホスト情報の登録の要・不要の条件
  - ホスト情報の登録者
  - グルーレコードとして設定される条件

注：本セミナーで紹介する.com/.netの仕様は、発表者自身の調査結果に基づいています。

.jpにおける取り扱い

登録ドメイン名	ネームサーバー ホスト名	関係	ホスト情報の登録	ホスト情報の登録者
example.jp	ns1.**example.jp**	In-domain	**必要**	**example.jpの登録者**
example.jp	ns1.**example2.jp**	Sibling domain	不要	—
example.jp	ns1.**example.ne.jp**	Sibling domain	不要	—
example.jp	ns1.**example.com**	Unrelated	不要	—

- 登録ドメイン名とネームサーバーホスト名の関係が**In-domainである場合のみ、ホスト情報の登録が必要**
  - 名前解決において、グルーレコードが必要な場合のみ
- ホスト情報の登録者は、**登録ドメイン名の登録者**

.com/.netにおける取り扱い

登録ドメイン名	ネームサーバー ホスト名	関係	ホスト情報の登録	ホスト情報の登録者
example.com	ns1.**example.com**	In-domain	**必要**	**example.comの登録者**
example.com	ns1.**{任意}.com**	Sibling domain	**必要**	**{任意}.comの登録者**
example.com	ns1.**{任意}.net**	Unrelated	**必要**	**{任意}.netの登録者**
example.com	ns1.**example.jp**	Unrelated	不要	—
example.com	ns1.**example.info**	Unrelated	不要	—

- 登録ドメイン名とネームサーバーホスト名のTLDを**同じレジストリが管理している場合、ホスト情報の登録が必要**
  - 関係がUnrelatedである場合、登録されたホスト情報は**グルーレコードとして追加されない**
- ホスト情報の登録者は、**ネームサーバーホスト名が属するドメイン名の登録者**

まとめ： .jpと.com/.netにおける ネームサーバーホスト情報の取り扱いの違い

- .jpと.com/.netでは、**ホスト情報とグルーレコードの取り扱いに関する仕様**が一部異なっており、**運用に影響を及ぼしている**
  - ホスト情報の登録の要・不要の条件
  - ホスト情報の登録者
  - グルーレコードとして設定される条件
- 特に、.com/.netでは**グルーレコードとして追加されないにも関わらず、ホスト情報の登録が必要になる**場合がある
  - 調査した範囲では、他の複数のgTLDも.com/.netと同様の仕様になっている

ホスト情報の取り扱いとその仕様の違いが、
グルーレコードに関する理解の妨げになっている

3. DNS運用におけるあるべき姿

ドメイン名とDNSの運用における、
グルーレコードとわれわれのあるべき姿は？

再掲：グルーレコードの現状

- **DNSができた当初から存在**
  - しかし、**仕様のあいまいさ**や**実装・運用における取り扱いの不備**により、**トラブルやセキュリティインシデントの原因**となっている
- かつ、**登録者・DNS運用者が直接取り扱う**、**基本情報**の一つ
  - レジストリに登録する「**ネームサーバーホスト情報**」
  - しかし、現在のドメイン名の登録・運用では**グルーレコードが必要な条件とネームサーバーホスト情報の登録が必要な条件が一致しておらず**、**混乱の原因**となっている

パート2で、こうした状況の具体例について解説

こうなってしまった原因は…

- 過去のランチセミナーで、その手掛かりを解説している
  - 2021年のランチセミナー資料から引用

    - **設計思想**
      - 動かすことが優先、悪意の存在を想定せず

    設計時に悪意の存在を
    想定していなかったことが
    Kashpureff型攻撃の原因に

  - 2022年のランチセミナー資料から引用

    - **委任情報の取り扱い**と**メッセージ圧縮機能**はいずれも、**DNSの仕様（設計）における代表的な弱点**の一つ
      - **実装の不備・不具合、運用ミス**などが発生しやすく、さまざまな**トラブル・脆弱性の原因**になっている

    グルーレコードは
    委任情報の一部で
    あり、DNSの弱点
    の一つ

こう設計しておけば良かったのかも…

- **接着剤で接着する（グルーレコードを追加する）という設計**が、そもそも良くなかったのでは？
  - 2012年のランチセミナー資料から引用

> • こんな感じにすればよかったのかもしれない
> – 名前ではなくIPアドレスで指定
>
> ```
> sub.example.jp.  IN NSIP     192.0.2.1
> sub.example.jp.  IN NSIP6    2001:db8::1
> ```

- **接着剤を常に使う（In-domainしか許さない）ように設計**しておけば、ここまでの混乱はなかったのでは？
  - パート2で解説した、複雑な場合分けは必要なかったはず

でも、今の設計だから良かったこともある

- **DNS運用者をネームサーバーホスト名で示せる（見てわかる）**
  - トラブルシューティングの点でも有用（設定内容を判別しやすい）
- **外部DNSサービスを運用しやすくなる**
  - 運用上の理由でネームサーバーのIPアドレスを変更する際に、顧客側の作業（ネームサーバーホスト情報の変更申請）が不要になる
- **IPv6が追加された時、柔軟に対応できた**
  - 権威DNSサーバーとフルリゾルバーがIPv6トランスポートをサポートし、グルーレコードにAAAAを追加することでIPv6対応できた
    - DNSそのものの設計を変更したり、機能拡張したりしなくても対応できた

グルーレコードのあるべき姿は？

- **名前解決の安定性を高める観点**から、ネームサーバー設定のあるべき姿は「~~内部名~~**In-domain**」であるとされてきた
  - グルーレコードで親子間を接着する形
- JPRSもかつて、そのように発表していた

> ネームサーバは内部名で – Internet Week 2004 DNS DAY
> <https://jprs.jp/tech/material/IW2004-DNS-DAY-internal-hostname-in-nameserver-minda.pdf>

- 自前のDNS運用が主流だった時代は、あるべき姿であった

あるべき姿は時代と共に変わる

- 名前解決において、**グルーレコードでIPアドレスを入手する方法が必須である**ことは、以前から変わっていない
  - ネームサーバーを**In-domainに設定し、ホスト情報を登録**
- しかし、適切に設定・運用されない場合、グルーレコードは運用上のトラブルやセキュリティインシデントにつながり得る
  - **適切に運用できない場合、設定しなくて済む方が安定運用につながる**
  - JANOG40のJPRS藤原の発表資料から引用

- 外部名のほうが、エラー率が少ない
  - おそらく運用サービスなので正しく運用されている
  - 一般の登録者はDNSプロバイダに任せると間違いが少ない

出典：DNSに関する常識の変化
<https://www.janog.gr.jp/meeting/janog40/application/files/3415/0146/9364/janog40-dns-fujiwara-1.pdf>

グルーレコードについて DNS運用者がすべきこと（1/2）

- グルーレコードに使われる**ネームサーバーホスト情報**を
  ドメイン名の登録情報と同様、**適切に管理する必要がある**
- 委任元のネームサーバーから**どのようなグルーレコードが応答されているか/いないかを、正確に把握する必要がある**
  - **In-domain**の場合に加え、**Sibling domain**の場合も必要

親ゾーンと子ゾーンの間が、**適切な接着剤で適切に接着される**ようにする

グルーレコードについて DNS運用者がすべきこと（2/2）

- 外部DNSサービスを提供するためのゾーンをIn-domainで名前解決できるように設定・運用すると、**参照の回数が減って名前解決の効率が上がり、安定運用が可能になる**
  - 外部サービス用のネームサーバーホスト名が属するドメイン名
- 外部DNSサービスの利用を踏まえた運用上の推奨事項については、**2017年にJPRSが公開した技術解説も参照**

技術解説：内部名の概要と設定・利用における推奨事項について
<https://jprs.jp/tech/notice/2017-07-27-nameserver-in-bailiwick.html>

DNSホスティングサービスの利用におけるネームサーバーホスト名の設定について
<https://jprs.jp/tech/notice/2017-07-27-nameserver-ipaddress.html>

おわりに

- 今回のランチセミナーでは**DNSができた当初から存在**する、**グルーレコード**について取り上げました
- 今日取り上げた項目以外にも、グルーレコードを含むDNSの委任の取り扱いの仕組みには、**さまざまな[redacted]があります**
  - [redacted]には、みなさんが適切と思う言葉を入れてください
- グルーレコードとそれに関連する状況を理解することは、**ドメイン名とDNSに関するより深い理解**につながります

このセミナーがグルーレコードの、そしてドメイン名とDNSのよりよい理解と運用に、少しでも役立てば幸いです

余談

グルーレコードと虫垂の共通点？

- Wikipediaの「盲腸」に、**こんな記述**を見つけました

  「腸内フローラを管理する免疫細胞が多数存在していることが判明」

出典：盲腸 - Wikipedia <https://ja.wikipedia.org/wiki/%E7%9B%B2%E8%85%B8>

- 調べてみたら**本当でした**

無用の長物と考えられていた虫垂の免疫学的意義を解明（大阪大学・科学技術振興機構）
<https://www.jst.go.jp/pr/announce/20140410/index.html>

- 上記のリリース文には、**こんな記述**が書かれていました

  「**虫垂がなくなると、大腸の腸内細菌叢のバランスが崩れる**ことも明らかにしました」

※細菌叢 = 腸内フローラ

もしかするとグルーレコードと虫垂には、一脈通じるものがあるのかもしれません

最後までご清聴いただき
ありがとうございました！

<https://jprs.jp/tech/>

@JPRS_official　JPRSofficial　JPRSpress