グルーレコードについて改めて考える
～ランチタイムにDNS～

2024年7月26日

Internet Week ショーケース in 福岡

株式会社日本レジストリサービス（JPRS）

森下 泰宏

本セミナーはInternet Week 2023 ランチタイムセミナーのUpdate版です

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・社内外の教育啓発

＜略歴＞

1988年	東京理科大学を卒業後、ディジタルコンピュータ株式会社（DCL、独立系SIer）に入社 1990年よりWIDE Projectメンバーとして、 日本のインターネット構築に創始期より参加。
1993年	学校法人東京理科大学情報処理センター着任 キャンパスネットワーク及び教育用システムの設計・ 構築・運用に従事。
1998年	社団法人日本ネットワークインフォメーションセンター（JPNIC）着任 JPドメイン名登録システム及びJP DNSの管理運用に従事。
2001年	株式会社日本レジストリサービス（JPRS）に転籍 DNSに関する技術研究を中心に活動。
2007年	同社技術広報担当として、 DNSおよびドメイン名関連技術に関する情報提供・教育啓発を中心に活動中（現職）。
2021年	同社技術研修センター主任講師として、教育・研修を通じた社内外の人材育成を担当（兼務・現職）。

グルーレコード（glue records）

- **DNSができた当初から存在する、委任の仕組みの一部**
  - 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
2. グルーレコードに関する最近の動きと現状
3. **委任情報の取り扱いに関する最近の動き**
   - **DELEGレコード**に関する検討状況

以降では、Internet Week 2023発表資料からの更新内容を**青字**で示します
（スライド全体を追加・更新したページは、**タイトルを青字**にしています）

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**

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
  - 例：**jp**から見た場合の、**example.jp**と**ns1.example.jp**
- 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

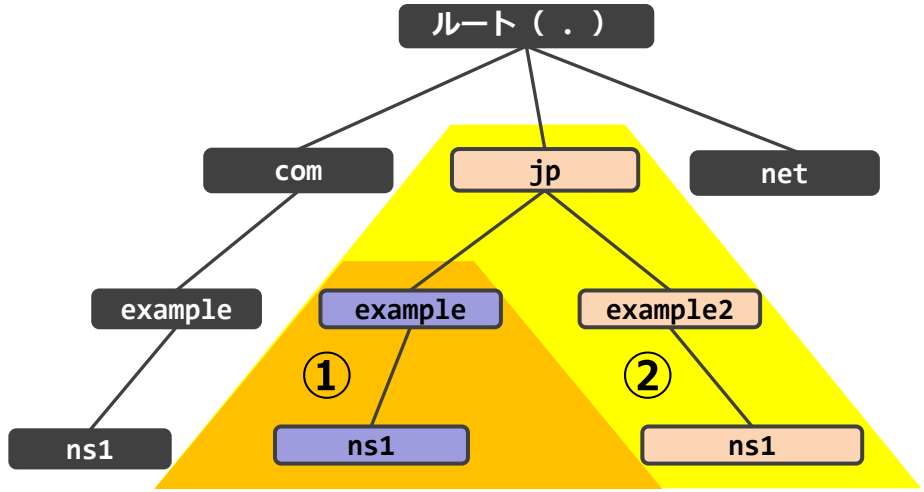
委任先ゾーンとネームサーバーホスト名の関係

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

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**

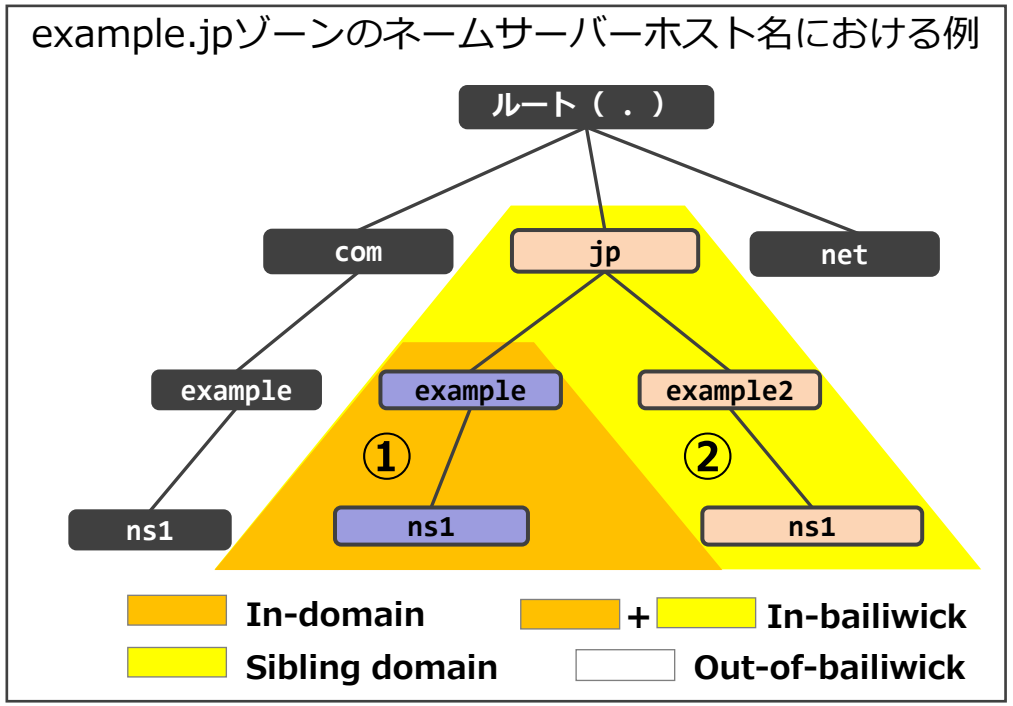
※sibling：兄弟・姉妹

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

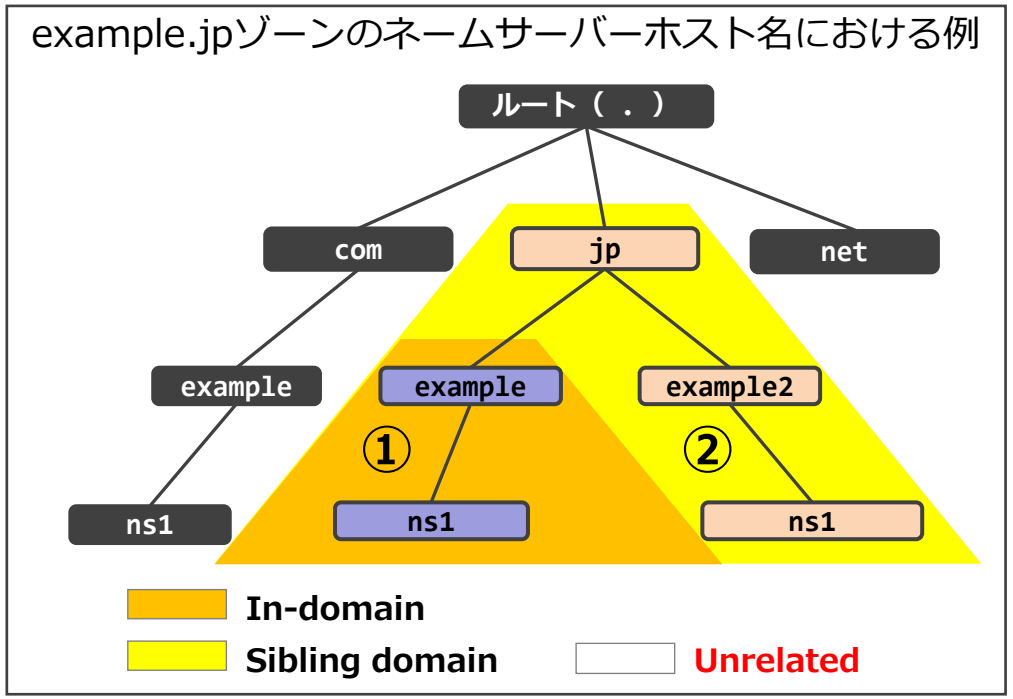
- **内部名/In-bailiwick**の意味に**揺れ**が見られる
  - **内部名がIn-domainの意味で使われる例**と、**In-bailiwickの意味で使われる例**の双方が存在する
  - 加えて、**In-bailiwickがIn-domainの意味で使われている既存の英語の文書**も存在する
    - In-domainという用語が、技術者の間に十分に浸透していないことも原因の一つとして挙げられる



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は**2024年3月にRFC 9499に置き換えられ**、委任先ゾーンとネームサーバーホストの関係を示す用語が従来の4種類から**3種類に再整理された**

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**
  - 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**
  - 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

ドメイン名登録におけるネームサーバーホスト情報の取り扱いの現状

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の場合、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. 委任情報の取り扱いに関する最近の動き

DELEGレコードに関する検討状況

再掲：グルーレコードの現状

- **DNSができた当初から存在する、委任の仕組みの一部**
  - 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**を解説

グルーレコードを含む**委任情報の取り扱い**は DNSの設計における**代表的な弱点の一つ**

- Internet Week 2022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**
  - **委任情報の取り扱い**は、**DNSの仕様（設計）における代表的な弱点の一つ**として認識されている

DNSの識者は以前から、**この状況を何とかできないか**と考えていた

DELEGレコードの誕生

- 2023年11月のIETF 118ハッカソン[*1]で、DNSの委任情報を記述するための**新しいリソースレコード「DELEG」**のアイディアが提案された
  - 「デレグ」のように読まれている
    - DNS **DELEG**ation（DNSの委任）に由来
- 委任に関する**さまざまな問題を解決できる可能性がある**と認識され、**本格的な検討に向けた動き**が始まった

[*1] ハッカソン（Hackathon）：エンジニアが集中的に共同作業をする場を意味している。IETFではIETF 92からハッカソンが実施されており、新しく標準化された、あるいは標準化作業中のプロトコルの実験実装の試作が集中的に行われている。

DELEGレコードの**アイディア**

- **SVCB/HTTPSレコードのフォーマット**を使って**委任に関する情報を親ゾーンにまとめて記述**し、従来のNSレコードとグルーレコードは**互換性のために残す**、というアイディアに基づいている

（jp⇒example.jp：**NSとグルー**による委任）

```
$ORIGIN jp.
example.jp.      IN NS ns1.example.jp.
ns1.example.jp.  IN A 192.0.2.1
                 IN AAAA 2001:db8::1
```

（jp⇒example.jp：**DELEG**による委任）

```
$ORIGIN jp.
example.jp.      IN DELEG 1 ns1.example.jp. (
                            ipv4hint=192.0.2.1
                            ipv6hint=2001:db8::1
                            transport=dot
                            otherinfo=... )
```

委任に関する**さまざまな追加情報をまとめて記述できる**

検討が始まった段階であり、DELEGレコードを**委任ポイント（ゾーンカットの親側）に書くかも含め、決定・合意事項ではない**ことに注意

DELEGレコードで**解決できるかもしれないと考えられていること**

- これまでの提案・発表で、以下の項目に言及されている
  - DNSSECによる**委任情報の保護**
  - NS/DS/グルーレコードの**統合**
  - フルリゾルバーと権威DNSサーバーの間の**通信の暗号化**
  - 外部のDNSプロバイダーへの**より効率的なアウトソーシング**
  - 新しいプロトコルの**段階的な導入**
  - ドメイン名の**管理境界の識別・判定**

DELEGレコードの**潜在能力**に対する、**高い期待**が伺える

IETFにおける**検討状況**

- IETF 118（2023年11月）
  - IETFハッカソンでDELEGレコードの**アイディア誕生**、dnsop WGで報告
- 2024年1月23日
  - **最初のインターネットドラフト**が公開
- 2024年2月6日
  - DELEGレコードについて議論する**メーリングリスト「dd」**が発足
- IETF 119（2024年3月）
  - **deleg BoF**開催、**WGの創設に向けた議論・プロセス**が進行
- 2024年6月26日
  - **deleg WG**が正式発足
- IETF 120（2024年7月）
  - deleg WGが**初開催**

DELEGレコードに関する**今後の展望**

- IETFにおける標準化作業は**まだ始まったばかり**であり、今後、**多大な作業と時間を要する**ことが予想される
  - WGのチャーターには、2025年12月までのマイルストーンが記述されている
- 委任は**DNSの根本に関わる仕組み**であり、仕様の追加・変更の際には**既存のプロトコル・実装・運用への影響を最小限に留める**必要がある
  - 技術だけではなく、**レジストリ・レジストラのサービス**や**ICANNとの契約内容**などにも影響を及ぼす
- それでも、**DELEGレコードの標準化には多くの関係者が期待している**

おわりに

- 今回のセミナーでは**グルーレコード**に注目し、**ドメイン名とDNSの運用における取り扱いの現状**について解説しました。
  - パート1では**グルーレコードの概要と役割**、パート2では**グルーレコードに関する最近の動きと、ドメイン名登録における取り扱いの現状**について解説しました。
  - パート3では**Internet Week 2023以降のアップデート**として、IETFで検討が始まっている、**委任に関する新しいリソースレコード「DELEG」の状況と今後の展望**について解説しました。

このセミナーが**グルーレコードの、そしてDNSの委任の取り扱いに関する現状と今後のより深い理解**に、少しでも役立てば幸いです。

最後までご清聴・ご視聴いただき ありがとうございました！

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

@JPRS_official　JPRSofficial　JPRSpress