DNSにおける最近の変化
『DNSがよくわかる教科書 第2版』の改訂内容から
～午後のひとときにDNS～

2026年6月30日

Internet Week Showcase in 静岡

株式会社日本レジストリサービス（JPRS）

森下 泰宏・熊谷 維魅

本セミナーはInternet Week 2025 ランチタイムセミナーのアップデート版です

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・社内外の人材育成
  - 一言：**JANOG35以来、11年ぶりに静岡に来ました！**

- 熊谷 維魅（くまがい いみ）
  - 所属：JPRS システム部・技術研修センター
  - 主な業務内容：ネットワークの構築運用・DNS関連イベントの講師など
  - 一言：**バージョンアップした説明で、今年もわかりやすさにこだわります！**

本日の内容

- 『**DNSがよくわかる教科書**』が発売された2018年から、『**DNSがよくわかる教科書 第2版**』が発売された2026年までに起こった**ドメイン名とDNSにおける変化**を、**第2版への反映内容**と共にご紹介します。
- 加えて、**Internet Week 2025 ランチタイムセミナー**で予告した改訂項目が**第2版で実現できたか**を改めて確認し、最後に『**DNSがよくわかる教科書**』**の今後**についてお話しします。

ドメイン名とDNSにおける最近の変化と第2版への反映内容

このパートの内容

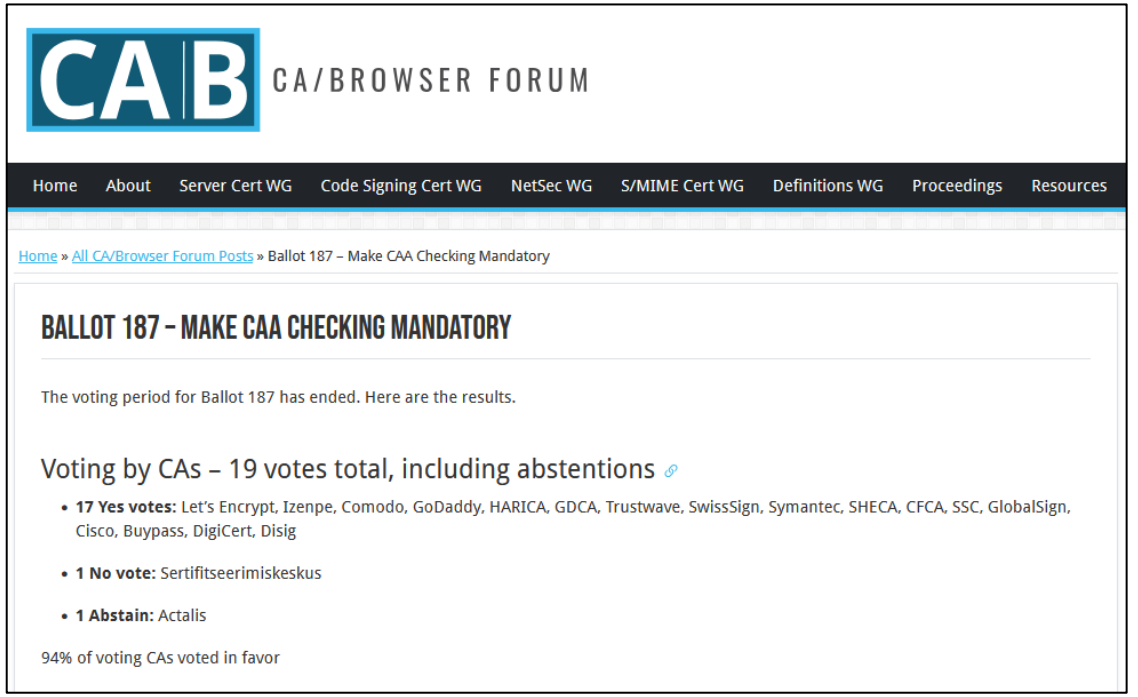
- 2018年から2026年までに起こった**ドメイン名とDNSにおける変化と、『DNSがよくわかる教科書 第2版』への反映内容**をご紹介します

＜紹介する項目＞

- **CAAレコードの義務化と対応**
- **HTTPSレコードの先行対応と標準化**
- **QNAME minimisationの普及**
- **サブドメインテイクオーバーの流行**
- **レジストリサービスプロバイダーの成長**
- **gTLDにおけるWHOISの非義務化**
- **委任の再設計**

CAAレコードの義務化と対応

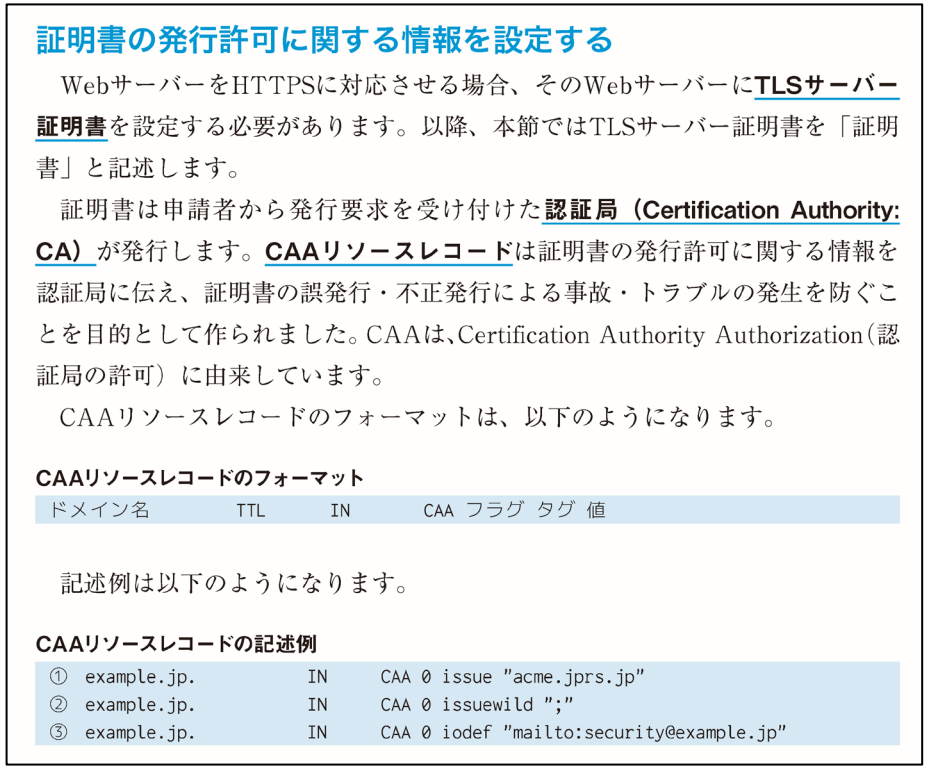
- 2013年に**RFC 6844**として標準化され、2019年に**RFC 8659**に置き換えられました
- 2017年に証明書の業界団体**CA/Browser Forum**が、認証局における**CAAレコードのチェックを義務化**し、実装・サービスにおける対応が広まりました



引用元：Ballot 187 – Make CAA Checking Mandatory | CA/Browser Forum <https://cabforum.org/2017/03/08/ballot-187-make-caa-checking-mandatory/>

第2版への反映内容

- 6章に「**証明書の発行許可に関する情報を設定する**」を追加しました
  - **CA/Browser Forumの意思決定の仕組み**も紹介しました



証明書の発行許可に関する情報を設定する

WebサーバーをHTTPSに対応させる場合、そのWebサーバーに**TLSサーバー証明書**を設定する必要があります。以降、本節ではTLSサーバー証明書を「証明書」と記述します。

証明書は申請者から発行要求を受け付けた**認証局（Certification Authority: CA）**が発行します。**CAAリソースレコード**は証明書の発行許可に関する情報を認証局に伝え、証明書の誤発行・不正発行による事故・トラブルの発生を防ぐことを目的として作られました。CAAは、Certification Authority Authorization（認証局の許可）に由来しています。

CAAリソースレコードのフォーマットは、以下のようになります。

CAAリソースレコードのフォーマット

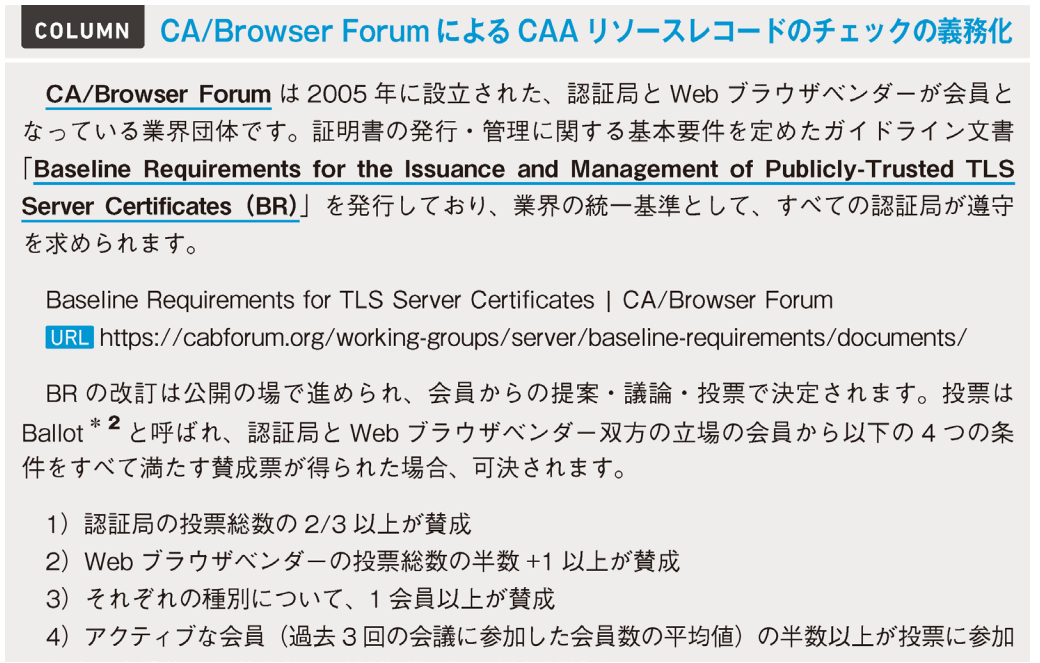
```
ドメイン名        TTL      IN       CAA フラグ タグ 値
```

記述例は以下のようになります。

CAAリソースレコードの記述例

```
① example.jp.          IN     CAA 0 issue "acme.jprs.jp"
② example.jp.          IN     CAA 0 issuewild ";"
③ example.jp.          IN     CAA 0 iodef "mailto:security@example.jp"
```

p.143「証明書の発行許可に関する情報を設定する」



COLUMN CA/Browser Forum による CAA リソースレコードのチェックの義務化

CA/Browser Forum は 2005 年に設立された、認証局と Web ブラウザベンダーが会員となっている業界団体です。証明書の発行・管理に関する基本要件を定めたガイドライン文書「**Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates（BR）**」を発行しており、業界の統一基準として、すべての認証局が遵守を求められます。

Baseline Requirements for TLS Server Certificates | CA/Browser Forum
URL https://cabforum.org/working-groups/server/baseline-requirements/documents/

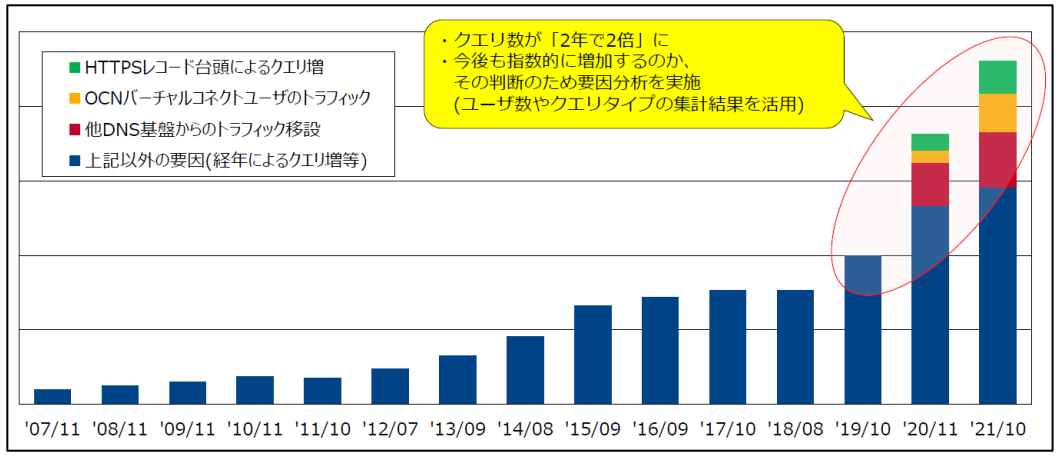
BR の改訂は公開の場で進められ、会員からの提案・議論・投票で決定されます。投票は Ballot *2 と呼ばれ、認証局と Web ブラウザベンダー双方の立場の会員から以下の 4 つの条件をすべて満たす賛成票が得られた場合、可決されます。

1）認証局の投票総数の 2/3 以上が賛成
2）Web ブラウザベンダーの投票総数の半数 +1 以上が賛成
3）それぞれの種別について、1 会員以上が賛成
4）アクティブな会員（過去 3 回の会議に参加した会員数の平均値）の半数以上が投票に参加

p.145「CAAリソースレコードのチェックの義務化」

HTTPSレコードの先行対応と標準化

- Webブラウザーやサービスプロバイダーが**RFCの発行を待たずに、HTTPSレコードに先行対応**しました
- その結果、2019年から2021年にかけて、**フルリゾルバーに到達するDNSトラフィックが急増**しました
- HTTPSレコードは2023年に、**RFC 9460**として標準化されました

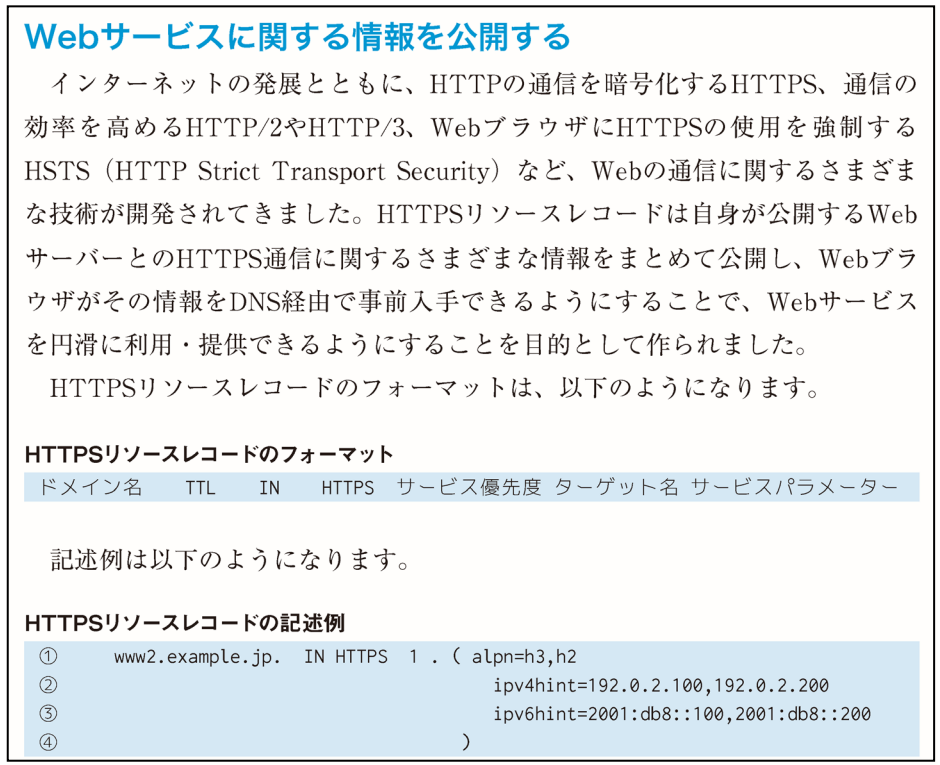


- HTTPSレコード(Type65)の増加によりPrimaryのサーバが性能不足が顕著化。
  - P/S片方が落ちるとトラヒックが溢れる。
  - なぜ予想できなかったのか？と詰められる。

引用元：DNSの可視化検討 JANOG49 Meeting
<https://www.janog.gr.jp/meeting/janog49/dns/>

第2版への反映内容

- 6章に「**Webサービスに関する情報を公開する**」を追加しました
  - DNSトラフィックの急増に伴う、**ISPにおける緊急対応**も紹介しました



Webサービスに関する情報を公開する

インターネットの発展とともに、HTTPの通信を暗号化するHTTPS、通信の効率を高めるHTTP/2やHTTP/3、WebブラウザにHTTPSの使用を強制するHSTS（HTTP Strict Transport Security）など、Webの通信に関するさまざまな技術が開発されてきました。HTTPSリソースレコードは自身が公開するWebサーバーとのHTTPS通信に関するさまざまな情報をまとめて公開し、Webブラウザがその情報をDNS経由で事前入手できるようにすることで、Webサービスを円滑に利用・提供できるようにすることを目的として作られました。

HTTPSリソースレコードのフォーマットは、以下のようになります。

HTTPSリソースレコードのフォーマット

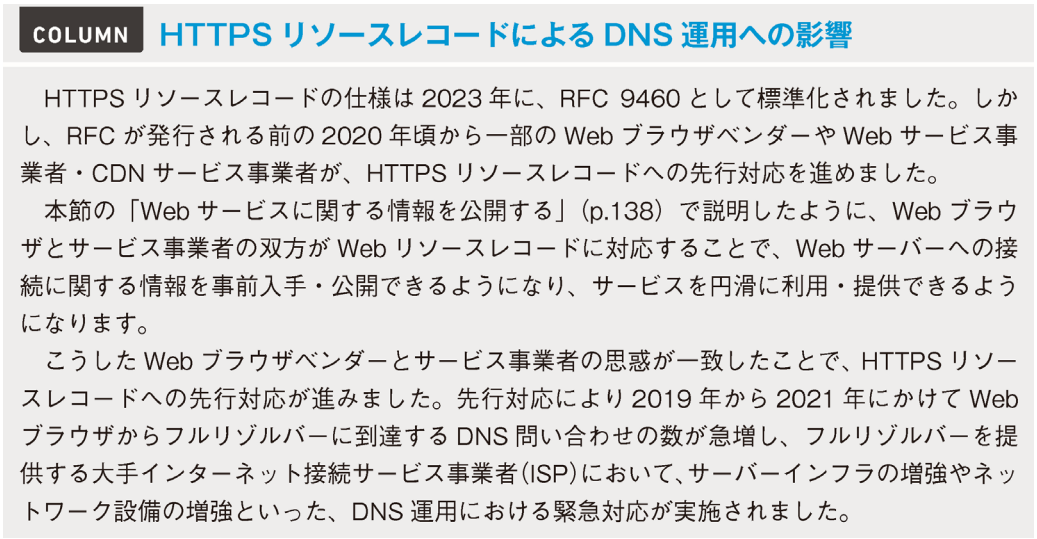
```
ドメイン名    TTL    IN    HTTPS  サービス優先度 ターゲット名 サービスパラメーター
```

記述例は以下のようになります。

HTTPSリソースレコードの記述例

```
①    www2.example.jp.  IN HTTPS  1 . ( alpn=h3,h2
②                                      ipv4hint=192.0.2.100,192.0.2.200
③                                      ipv6hint=2001:db8::100,2001:db8::200
④                                   )
```

p.138「Webサービスに関する情報を公開する」



COLUMN **HTTPS リソースレコードによる DNS 運用への影響**

HTTPS リソースレコードの仕様は 2023 年に、RFC 9460 として標準化されました。しかし、RFC が発行される前の 2020 年頃から一部の Web ブラウザベンダーや Web サービス事業者・CDN サービス事業者が、HTTPS リソースレコードへの先行対応を進めました。

本節の「Web サービスに関する情報を公開する」（p.138）で説明したように、Web ブラウザとサービス事業者の双方が Web リソースレコードに対応することで、Web サーバーへの接続に関する情報を事前入手・公開できるようになり、サービスを円滑に利用・提供できるようになります。

こうした Web ブラウザベンダーとサービス事業者の思惑が一致したことで、HTTPS リソースレコードへの先行対応が進みました。先行対応により 2019 年から 2021 年にかけて Web ブラウザからフルリゾルバーに到達する DNS 問い合わせの数が急増し、フルリゾルバーを提供する大手インターネット接続サービス事業者（ISP）において、サーバーインフラの増強やネットワーク設備の増強といった、DNS 運用における緊急対応が実施されました。

p.141「HTTPSリソースレコードによるDNS運用への影響」

QNAME minimisationの普及

- 2016年に**RFC 7816**として実験仕様が作られ、2021年に**RFC 9156**として標準化されました
- 仕様の作成を受け、**主なフルリゾルバーやパブリックDNSサービスのデフォルトの動作**が、**QNAME minimisationに変更**されました
- その結果、**.com/.netの権威サーバーに到達する問い合わせの65%以上**が、QNAME minimisationによるものになりました

参考：Minimized DNS Resolution: Into the Penumbra - Verisign Blog
<https://blog.verisign.com/security/minimized-dns-resolution/>

JPRS

第2版への反映内容

- 14章に「**QNAME minimisationによる名前解決**」を追加し、8章で紹介している従来の名前解決との違いを確認できるようにしました

CHAPTER 14
Advanced Guide to DNS

03 QNAME minimisationによる名前解決

8章04「digコマンドの応用～フルリゾルバーになって名前解決」(p.184) で、フルリゾルバーの名前解決の動作をコマンドラインツールで模倣しました。ここでは、QNAME minimisationで同じ名前解決を実行し、従来の名前解決との違いを確認します。

例1）www.jprs.co.jpのAリソースレコードを問い合わせる

❶ルートサーバーに jp の A リソースレコードを問い合わせ

まず、名前解決の起点であるルートサーバーに**jpのAリソースレコード**を問い合わせます。ルートサーバーのIPアドレスは、7章のコラム「ヒントファイルとプライミング」(p.153) で説明したプライミングで得たものを使います。次の例では、a.root-servers.netのIPv4アドレスに問い合わせています。

- statusがNOERROR
- Answerセクションに応答が2つある（ANSWERが2）
- 権威を持つ応答である（flagsにaaがある）

そして、以下のことが示されています。

- Answerセクションにwww.ietf.orgのAAAAリソースレコードセットがある

したがって、これが求める情報となります。www.ietf.orgのIPv6アドレスは、2606:4700::6810:2c63と2606:4700::6810:2d63でした。

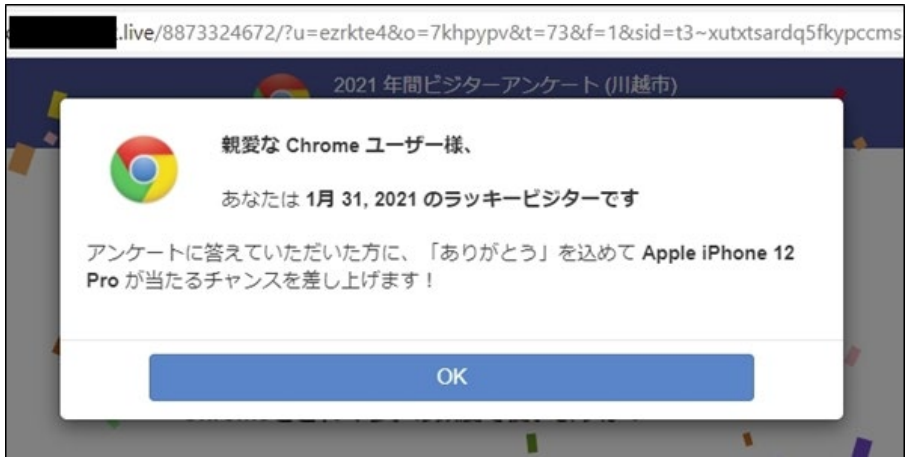
従来の名前解決とQNAME minimisationによる名前解決の比較

8章で説明した従来の名前解決と比べ、QNAME minimisationによる名前解決ではwww.jprs.co.jpのAリソースレコードを問い合わせる場合、www.ietf.orgのAAAAリソースレコードを問い合わせる場合のいずれについても、名前解決に必要なステップが増えています。しかし、QNAME minimisationによってルートサーバーやTLDの権威サーバーにクライアント（スタブリゾルバー）から受け取った問い合わせ内容（ドメイン名・タイプ）をそのまま送信しなくなったため、ルートサーバーやTLDの権威サーバーの運用者は、利用者が問い合わせたドメイン名・タイプを知ることができなくなっています。

pp.346-361「QNAME minimisationによる名前解決」

サブドメインテイクオーバーの流行

- 2020～2022年に流行した**iPhone当選詐欺**に利用されました
- 2025年1月に**複数のgo.jpドメイン名の被害事例**が報告され、**デジタル庁と国家サイバー統括室（NCO、旧NISC）のガイドライン**が**改訂**されるに至りました



なお、電子メールにおけるなりすまし防止の観点からも、管理するドメイン名の SPF レコード等を記述する TXT レコードの内容が正確であるか否かを確認する必要がある。また、ホスティングサービス等の利用終了後に残ったままになっている設定情報を利用して意図しないウェブサイト等を公開されてしまうサブドメインテイクオーバー・NS テイクオーバーと呼ばれる攻撃を避けるため、当該ウェブサイト等の利用を終了する場合には、当該ホスティングサービス等の利用開始時に設定した CNAME や NS レコードを全て削除・修正することが重要である。

加えて、クラウドサービスによっては、使用中のサービスにテイクオーバー可能な DNS 設定がないかを利用者において確認できるツールを公開している場合もあるので、そのようなツールを活用することも有用である。

引用元：政府機関等の対策基準策定のためのガイドライン（令和7年度版）令和7年9月5日 一部改定 341ページ
<https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf>

第2版への反映内容

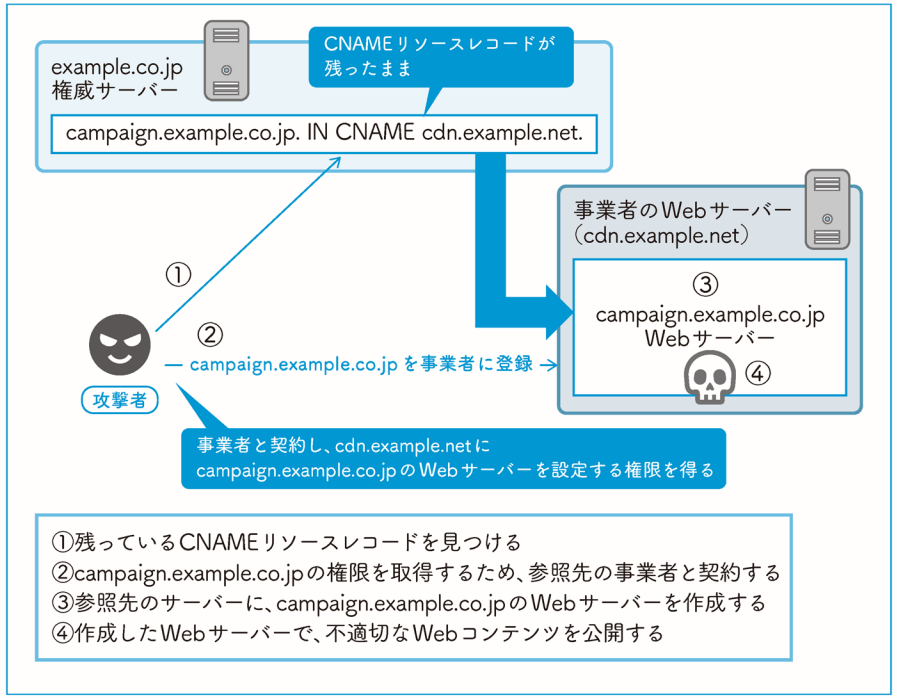
- 9章に「**サブドメインテイクオーバー、NSテイクオーバー**」と「**サブドメインテイクオーバー、NSテイクオーバーへの対策**」を追加しました

サブドメインテイクオーバー、NSテイクオーバー

サブドメインテイクオーバー、**NSテイクオーバー**はともに、リソースレコードで指定した指定先の実体が無効になっていることを利用して、ドメイン名の乗っ取り（テイクオーバー）を図る攻撃手法です。

サブドメインテイクオーバーでは、外部のCDN（Content Delivery Network）サービスやWebサービスを利用するための**CNAMEリソースレコード**（6章05「サービスを提供するために設定する情報」（p.135）を参照）が悪用されます。サービスの利用開始時に設定したCNAMEリソースレコードがサービスの解約後も残ったままになっており、かつ、事業者側で、解約されたサーバーのドメイン名と同じドメイン名のサーバーを第三者が再設定できるようになっている場合、サブドメインテイクオーバーによりドメイン名が乗っ取られる危険性があります（**図9-9**）。

図9-9　サブドメインテイクオーバー



p.235「サブドメインテイクオーバー、NSテイクオーバー」

レジストリサービスプロバイダーの成長

- 2012年のgTLD追加募集で**多数のgTLDが創設**され、ドメイン名レジストリの技術や運用に関する需要が高まりました
  - レジストリから委託を受けてそれらのサービスを提供する、**レジストリサービスプロバイダー（RSP）**が出現・成長しました
- 現在進行中の**gTLD追加募集（2026 Round）**において、RSPの技術をICANNが評価する、**レジストリサービスプロバイダー評価プログラム**が実施されています

参考：Registry Service Provider Evaluation Program | New gTLD Program
<https://newgtldprogram.icann.org/en/application-rounds/round2/rsp>

第2版への反映内容

- 2章にコラム「**レジストリサービスプロバイダー**」を追加しました
  - **レジストリサービスプロバイダー評価プログラム**と、2026年1月31日に最初のリストが公開された、**評価済みレジストリサービスプロバイダー**も紹介しました

COLUMN　レジストリサービスプロバイダー

レジストリと契約し、その運用実務を担う組織を**レジストリサービスプロバイダー（RSP）**といいます。

本章のコラム「gTLD の変遷」（p.34）で解説したように、2012 年の gTLD の追加募集では要件を満たした申請については基本的に、gTLD の創設が認められました。その結果 1,200 件を超える gTLD が創設され、現在も約 1,000 件の gTLD が運用されていますが、いくつかの gTLD は運用を終了しています。

gTLD の運用状況
URL https://www.icann.org/en/registry-agreements

レジストリの運用には、レジストリデータベースの管理、DNS の運用、RDDS（Registration Data Directory Services）の運用など、高い専門性を必要とします。そのため、多数の gTLD が創設されたことでこれらの技術や運用に関する需要が高まり、それらを専門サービスとしてレジストリに提供する RSP が出現、増加しました。

多数の gTLD を運用する主な RSP を、**表 2-3** に示します。

表2-3　gTLDを運用する主なRSP

レジストリサービスプロバイダー（RSP）	運用する新gTLDの数
Identity Digital Inc.	461
Registry Services, LLC（GoDaddy Registry）	196
Centralnic Registry	100

＊new gTLD Statistics by Backends https://ntldstats.com/backendの2026年2月時点のデータをもとに作成しています。

2026 年に予定されている gTLD の追加募集では RSP の技術を ICANN が評価し、その結果を公開する、**レジストリサービスプロバイダー評価プログラム（Registry Service Provider Evaluation Program）**が実施されています。

このプログラムでは、RSP が提供するドメイン名サービス・DNS・DNSSEC・RDAP などの技術を ICANN が総合的に評価し、結果が公開されます。gTLD の申請者がプログラムに合格した RSP に管理を委託することで、技術評価プロセスが免除されます。

JPRS は ICANN のすべての評価項目に合格し、メイン・DNS・DNSSEC の**評価済みレジストリサービスプロバイダー（Evaluated RSPs）**として公開されました。

p.36「レジストリサービスプロバイダー」

gTLDにおけるWHOISの非議務化

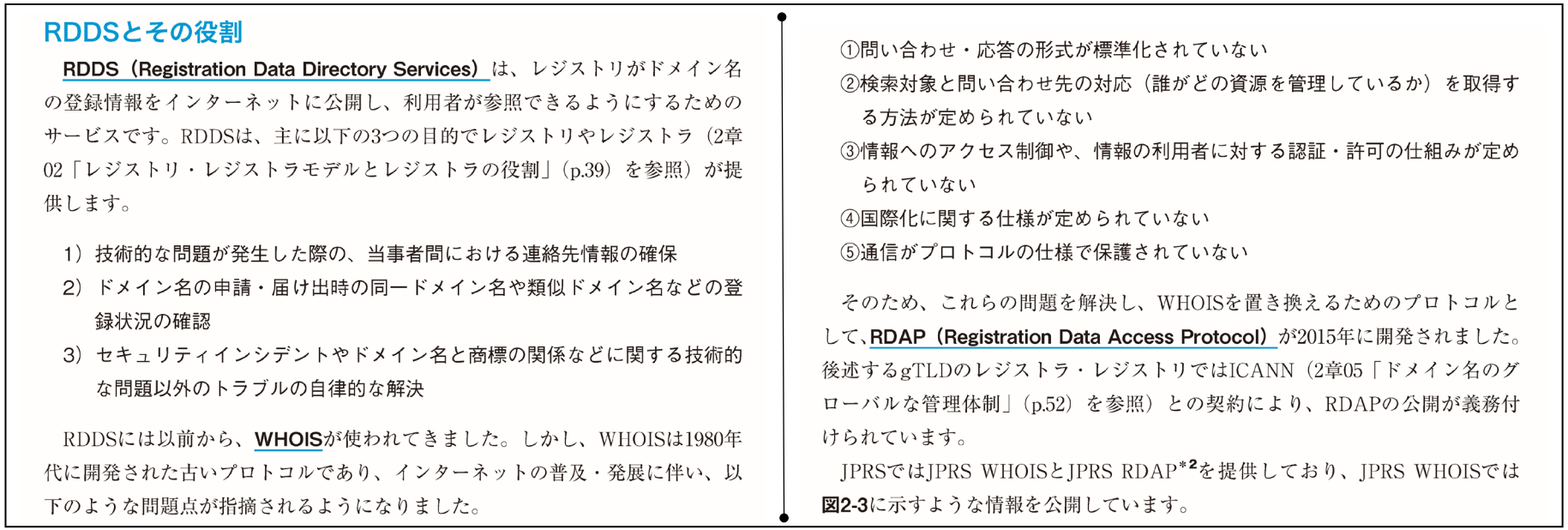
- 2025年にgTLDレジストラ・レジストリにおいて**WHOISの提供が非議務化**され、**RDAPへの移行**が図られています
  - 一部のgTLDレジストラ・レジストリは、**WHOISの提供を終了**しています

（参考訳）
Identity DigitalのWhoisサービスは、Identity Digitalが運用するすべてのTLDをサポートしていない可能性があります。お探しのTLDがサポートされていない場合は、ICANNが提供するこちらのツールなど、公開されている別のRDAPツールをご利用ください：https://lookup.icann.org/

引用元：<https://whois.nic.mobi/>

第2版への反映内容

- 第1版の「Whoisとその役割」を加筆・拡充する形で、2章に「**RDDSとその役割**」を追加しました
  - RDDSは「登録データディレクトリサービス」に由来する、**WHOIS・RDAPを含む登録情報を公開・参照するためのサービス全般を示す用語**です



RDDSとその役割

RDDS（Registration Data Directory Services）は、レジストリがドメイン名の登録情報をインターネットに公開し、利用者が参照できるようにするためのサービスです。RDDSは、主に以下の3つの目的でレジストリやレジストラ（2章02「レジストリ・レジストラモデルとレジストラの役割」（p.39）を参照）が提供します。

1）技術的な問題が発生した際の、当事者間における連絡先情報の確保
2）ドメイン名の申請・届け出時の同一ドメイン名や類似ドメイン名などの登録状況の確認
3）セキュリティインシデントやドメイン名と商標の関係などに関する技術的な問題以外のトラブルの自律的な解決

RDDSには以前から、WHOISが使われてきました。しかし、WHOISは1980年代に開発された古いプロトコルであり、インターネットの普及・発展に伴い、以下のような問題点が指摘されるようになりました。

①問い合わせ・応答の形式が標準化されていない
②検索対象と問い合わせ先の対応（誰がどの資源を管理しているか）を取得する方法が定められていない
③情報へのアクセス制御や、情報の利用者に対する認証・許可の仕組みが定められていない
④国際化に関する仕様が定められていない
⑤通信がプロトコルの仕様で保護されていない

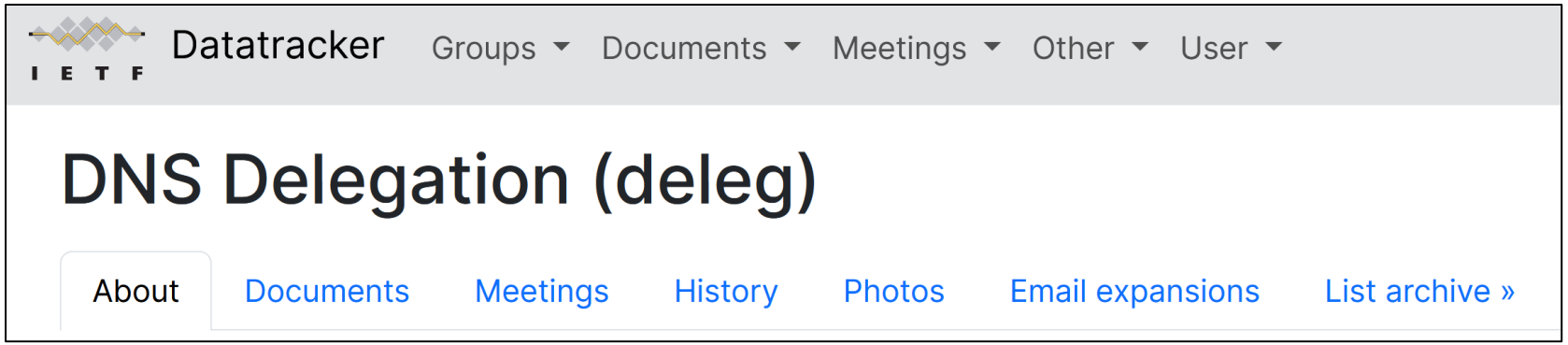
そのため、これらの問題を解決し、WHOISを置き換えるためのプロトコルとして、RDAP（Registration Data Access Protocol）が2015年に開発されました。後述するgTLDのレジストラ・レジストリではICANN（2章05「ドメイン名のグローバルな管理体制」（p.52）を参照）との契約により、RDAPの公開が義務付けられています。

JPRSではJPRS WHOISとJPRS RDAP[*2]を提供しており、JPRS WHOISでは図2-3に示すような情報を公開しています。

p.32「RDDSとその役割」

委任の再設計（1/3）

- 2023年11月のIETF 118ハッカソンで**DNSの委任を再設計**する**DELEG（デレグ）のアイディアが提案**され、注目を集めました
- 議論の結果、DELEGの標準化作業にIETFとして**集中的に取り組む**こととなり、2024年6月に**deleg WG**が発足しました



引用元：<https://datatracker.ietf.org/group/deleg/about/>

委任の再設計（2/3）

- DELEGの導入により、**さまざまな課題を解決**しようとしています
  - 親の委任情報を**DNSSECで保護する**
  - 外部/複数のDNSプロバイダーに**委任する方式を簡略化・改良する**
  - フルリゾルバーと権威サーバーの間の**安全な暗号通信を実現する**
- 導入を円滑に進めるため、WGで以下の**要求仕様が定義**されました
  - 現在の**ドメイン名登録管理モデル**を壊さない
  - 従来のプロトコル/実装との**後方互換性**を保つ
  - **段階的な導入**を実現する

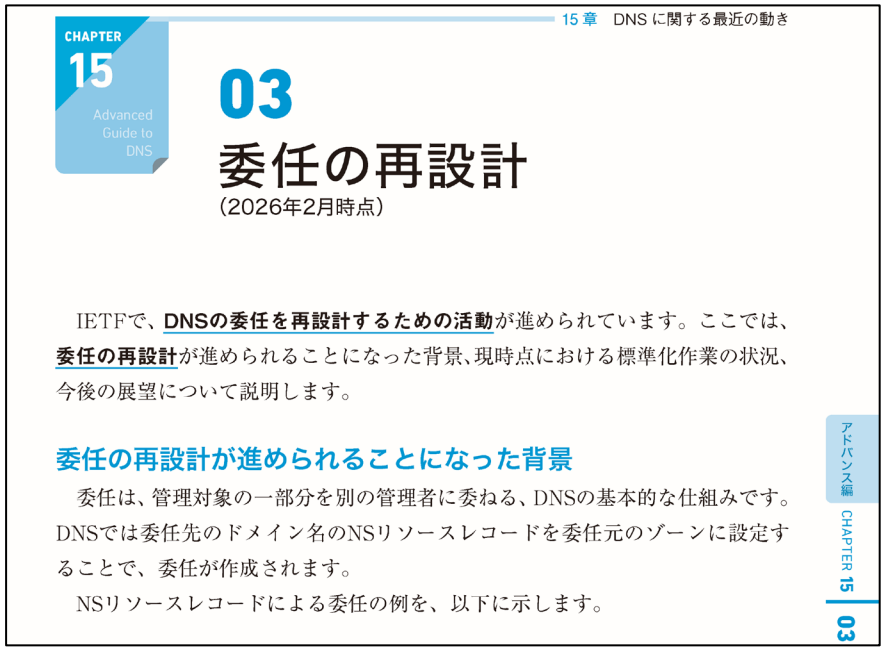
委任の再設計（3/3）

- 要求仕様に基づき、以下の手順で作業を進めることになりました
  ① まず、現在の**NSとグルーの委任とDELEGの委任を置き換える/併存させる部分のみを標準化**する
  ② その後、安全な暗号通信などの**より高度な機能を追加で標準化**する
- 現在、WGで**①の作業**が進められています
  – 2026年6月22日から**WG Last Callが開始**されました（7月6日まで）

第2版への反映内容

- 新設した15章に「**委任の再設計**（2026年2月時点）」を追加しました
  - 発売後に**基本仕様の一部が変更**されたため、**増刷時に更新する予定**です
    - 更新内容は公式サポートページに掲載されます

DNSがよくわかる教科書 第2版 | SBクリエイティブ
<https://www.sbcr.jp/support/4815637491/>


15章　DNSに関する最近の動き

CHAPTER 15 Advanced Guide to DNS

03
委任の再設計
（2026年2月時点）

IETFで、**DNSの委任を再設計するための活動**が進められています。ここでは、**委任の再設計**が進められることになった背景、現時点における標準化作業の状況、今後の展望について説明します。

委任の再設計が進められることになった背景

委任は、管理対象の一部分を別の管理者に委ねる、DNSの基本的な仕組みです。DNSでは委任先のドメイン名のNSリソースレコードを委任元のゾーンに設定することで、委任が作成されます。

NSリソースレコードによる委任の例を、以下に示します。

アドバンス編 CHAPTER 15 03

p.381「委任の再設計」

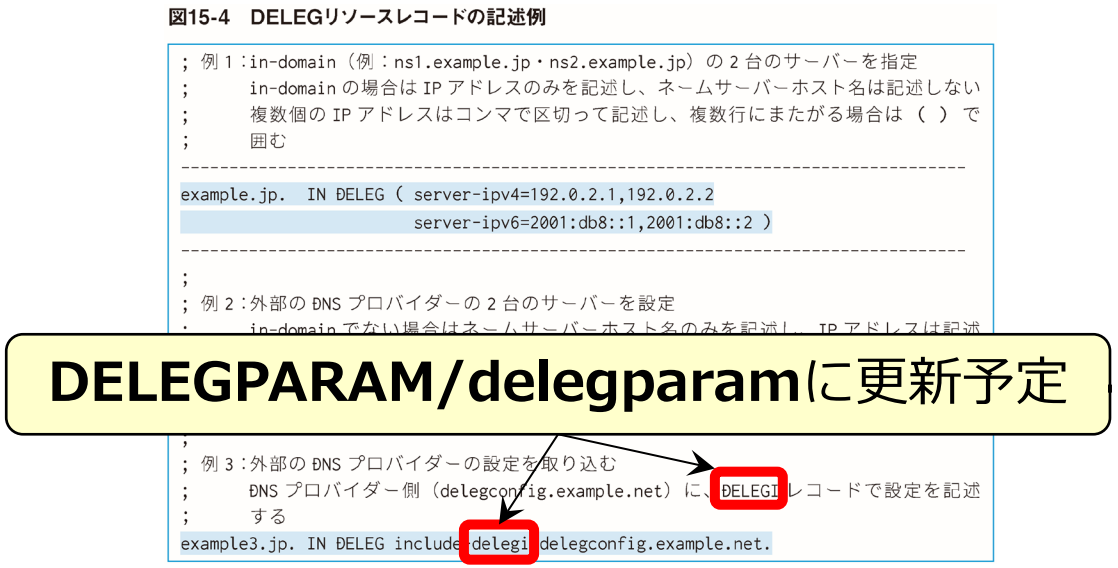


図15-4　DELEGリソースレコードの記述例

```
; 例1：in-domain（例：ns1.example.jp・ns2.example.jp）の2台のサーバーを指定
;       in-domainの場合はIPアドレスのみを記述し、ネームサーバーホスト名は記述しない
;       複数個のIPアドレスはコンマで区切って記述し、複数行にまたがる場合は（ ）で
;       囲む
------------------------------------------------------------------------
example.jp.   IN DELEG ( server-ipv4=192.0.2.1,192.0.2.2
                         server-ipv6=2001:db8::1,2001:db8::2 )
------------------------------------------------------------------------
;
; 例2：外部のDNSプロバイダーの2台のサーバーを設定
;       in-domainでない場合はネームサーバーホスト名のみを記述し、IPアドレスは記述
;
; 例3：外部のDNSプロバイダーの設定を取り込む
;       DNSプロバイダー側（delegconfig.example.net）に、DELEGIレコードで設定を記述
;       する
example3.jp. IN DELEG include-delegi delegconfig.example.net.
```

DELEGPARAM/delegparamに更新予定

p.384「DELEGリソースレコードの記述例」

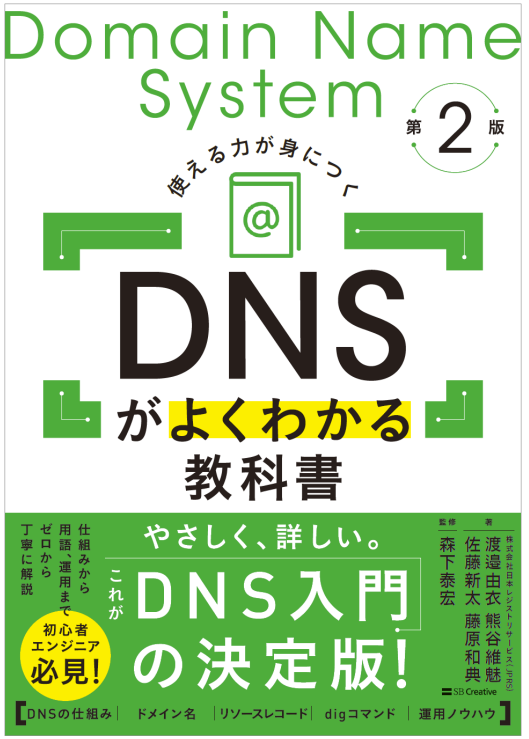
このパートのまとめ

- このパートでは『DNSがよくわかる教科書』が出版された2018年から現在までの**ドメイン名とDNSにおける最近の変化**の一部と、それらの項目が『**DNSがよくわかる教科書 第2版』にどう反映されたか**をご紹介しました。
- 次のパートでは、 Internet Week 2025 ランチタイムセミナーで予告した改訂項目が、**第2版で実現できたか**を確認していきます。

『DNSがよくわかる教科書 第2版』の概要
～予告した項目は実現できたのか～

予告した内容

- 著者：株式会社日本レジストリサービス（JPRS）
  渡邉結衣、**熊谷維魅**、佐藤新太、藤原和典
- 監修者：森下泰宏
- 出版社：SBクリエイティブ
- 発売日：**2026年3月11日**
- ページ数：400（予定）
- 定価：2,970円（予価・税込）

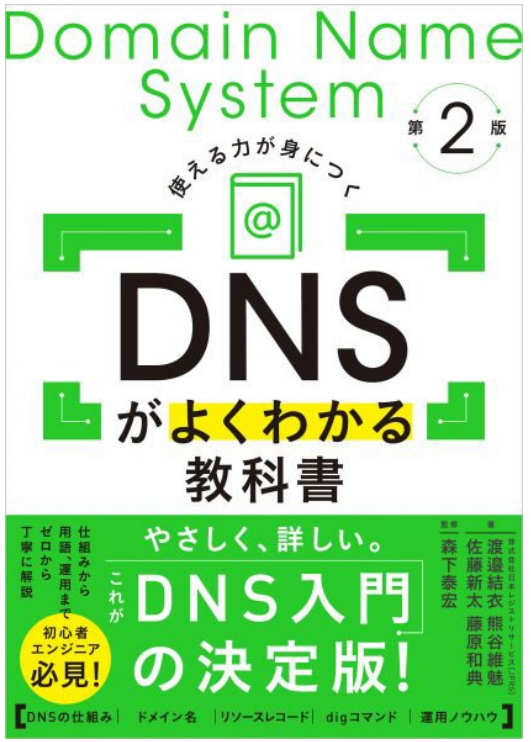


DNSがよくわかる教科書 第2版 | SBクリエイティブ
<https://www.sbcr.jp/product/4815622657/>

※カバーデザインは制作中のもので、変更される場合があります。

実際の内容

- 著者：株式会社日本レジストリサービス（JPRS）
  渡邉結衣、**熊谷維魅**、佐藤新太、藤原和典
- 監修者：森下泰宏
- 出版社：SBクリエイティブ
- 発売日：**2026年3月11日**
- ページ数：**424**（約25%増）
- 定価：**2,860円**（税込）



予定通り！

予定より増えた！

予価より安くしていただいた！

DNSがよくわかる教科書 第2版 | SBクリエイティブ
<https://www.sbcr.jp/product/4815622657/>

予告した内容

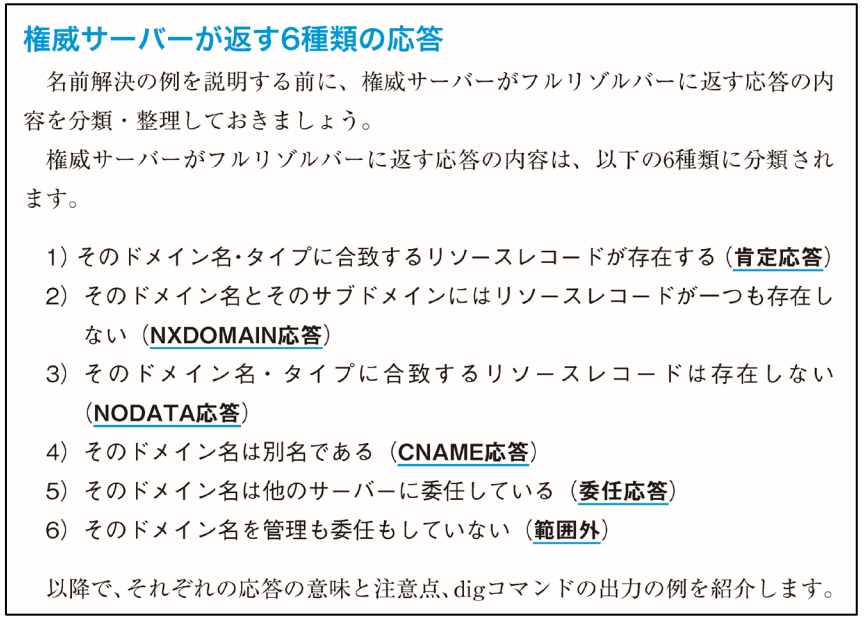
- **教科書**として**最新情報に対応**し、**完成度を高める**予定です
  - パート1で説明した、**第1版発行以降の変化**に対応
  - **第1版に記述しなかった項目**を追加
    - 権威サーバーが返す6種類の応答
    - 応答の圧縮
    - EDNS Client Subnet
  - **今後のDNSに影響を及ぼす項目**を追加
  - その他、**全般的な更新・修正**
    - digの出力・画面イメージの更新、古くなった記述・コラムの削除・修正など

説明済み

以降で説明

第1版に記述しなかった項目を追加

- 前述した3項目を**すべて追加**しました
  - **権威サーバーが返す6種類の応答**（8章）
  - **応答の圧縮**（8章）
  - **EDNS Client Subnet**（11章）
- それらに加え、第1版で漏れていた**いくつかの項目を追加**しました
  - **例示用のドメイン名**（1章）
  - **Public Suffix List**（3章）
  - **先頭が”_”で始まるラベル**（11章）、など



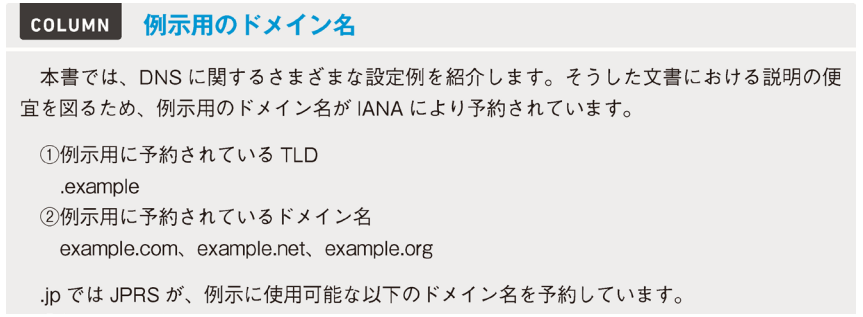
権威サーバーが返す6種類の応答

名前解決の例を説明する前に、権威サーバーがフルリゾルバーに返す応答の内容を分類・整理しておきましょう。

権威サーバーがフルリゾルバーに返す応答の内容は、以下の6種類に分類されます。

1）そのドメイン名・タイプに合致するリソースレコードが存在する（**肯定応答**）
2）そのドメイン名とそのサブドメインにはリソースレコードが一つも存在しない（**NXDOMAIN応答**）
3）そのドメイン名・タイプに合致するリソースレコードは存在しない（**NODATA応答**）
4）そのドメイン名は別名である（**CNAME応答**）
5）そのドメイン名は他のサーバーに委任している（**委任応答**）
6）そのドメイン名を管理も委任もしていない（**範囲外**）

以降で、それぞれの応答の意味と注意点、digコマンドの出力の例を紹介します。



COLUMN **例示用のドメイン名**

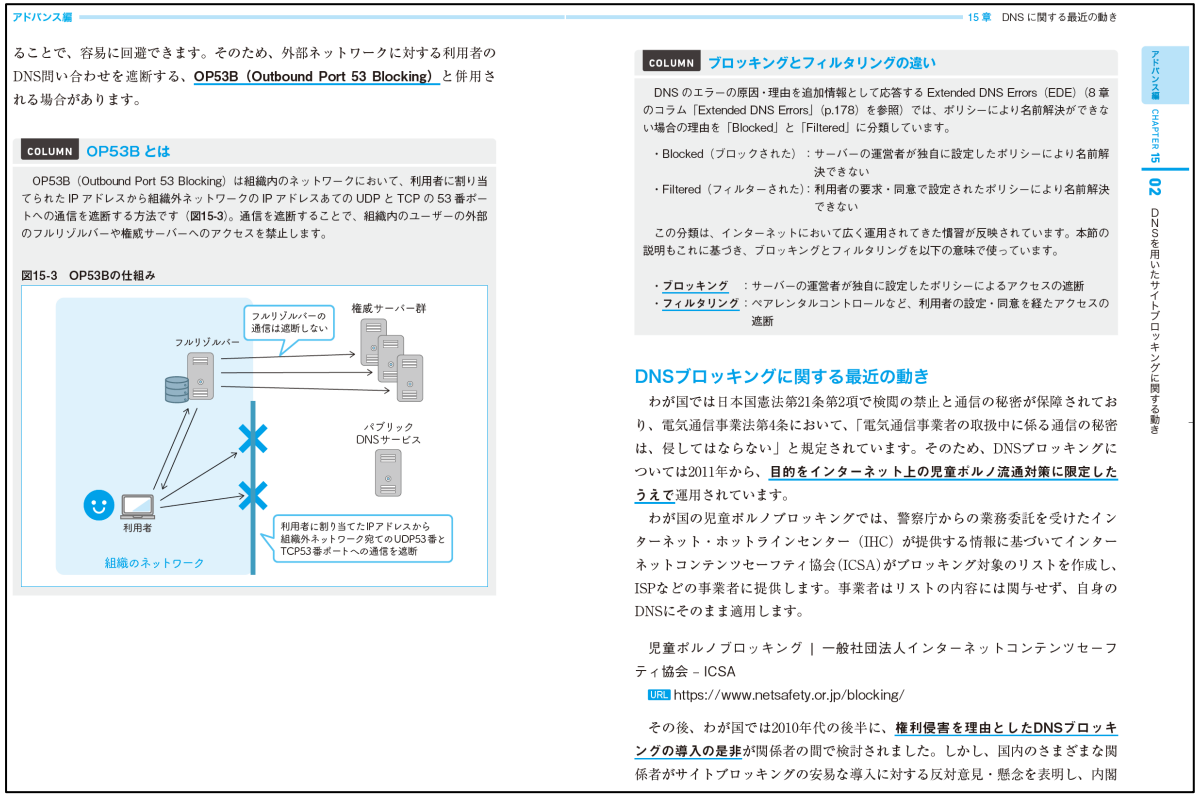
本書では、DNS に関するさまざまな設定例を紹介します。そうした文書における説明の便宜を図るため、例示用のドメイン名が IANA により予約されています。

①例示用に予約されている TLD
.example
②例示用に予約されているドメイン名
example.com、example.net、example.org

.jp では JPRS が、例示に使用可能な以下のドメイン名を予約しています。

今後のDNSに影響を及ぼす項目を追加

- 15章「**DNSに関する最新の動き**」を追加し、以下を記述しました
  - **新しいリソースレコードタイプの追加**
  - **DNSを用いたサイトブロッキングに関する動き**
  - **委任の再設計**（2026年2月時点）
  - **ルートゾーンのアルゴリズムロールオーバーに向けた検討**（2026年2月時点）



アドバンス編　15章　DNSに関する最近の動き

ることで、容易に回避できます。そのため、外部ネットワークに対する利用者のDNS問い合わせを遮断する、OP53B（Outbound Port 53 Blocking）と併用される場合があります。

COLUMN　OP53Bとは

OP53B（Outbound Port 53 Blocking）は組織内のネットワークにおいて、利用者に割り当てられたIPアドレスから組織外ネットワークのIPアドレスあてのUDPとTCPの53番ポートへの通信を遮断する方法です（図15-3）。通信を遮断することで、組織内のユーザーの外部のフルリゾルバーや権威サーバーへのアクセスを禁止します。

図15-3　OP53Bの仕組み

COLUMN　ブロッキングとフィルタリングの違い

DNSのエラーの原因・理由を追加情報として応答するExtended DNS Errors（EDE）（8章のコラム「Extended DNS Errors」（p.178）を参照）では、ポリシーにより名前解決ができない場合の理由を「Blocked」と「Filtered」に分類しています。

- Blocked（ブロックされた）：サーバーの運営者が独自に設定したポリシーにより名前解決できない
- Filtered（フィルターされた）：利用者の要求・同意で設定されたポリシーにより名前解決できない

この分類は、インターネットにおいて広く運用されてきた慣習が反映されています。本節の説明もこれに基づき、ブロッキングとフィルタリングを以下の意味で使っています。

- ブロッキング：サーバーの運営者が独自に設定したポリシーによるアクセスの遮断
- フィルタリング：ペアレンタルコントロールなど、利用者の設定・同意を経たアクセスの遮断

DNSブロッキングに関する最近の動き

わが国では日本国憲法第21条第2項で検閲の禁止と通信の秘密が保障されており、電気通信事業法第4条において、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」と規定されています。そのため、DNSブロッキングについては2011年から、**目的をインターネット上の児童ポルノ流通対策に限定したうえで**運用されています。

わが国の児童ポルノブロッキングでは、警察庁からの業務委託を受けたインターネット・ホットラインセンター（IHC）が提供する情報に基づいてインターネットコンテンツセーフティ協会（ICSA）がブロッキング対象のリストを作成し、ISPなどの事業者に提供します。事業者はリストの内容には関与せず、自身のDNSにそのまま適用します。

児童ポルノブロッキング | 一般社団法人インターネットコンテンツセーフティ協会 - ICSA
URL https://www.netsafety.or.jp/blocking/

その後、わが国では2010年代の後半に、**権利侵害を理由としたDNSブロッキングの導入の是非**が関係者の間で検討されました。しかし、国内のさまざまな関係者がサイトブロッキングの安易な導入に対する反対意見・懸念を表明し、内閣

「DNSを用いたサイトブロッキングに関する動き」より（pp.378-379）

既存の例示・図版・説明を更新・修正

- digの出力結果に、**どこをどう読めばよいかを示す注釈を追記**しました
  - 併せて「**この部分がこうなっているため、こう判断できる**」という説明を追加しました

画面8-1　ルートサーバーへ"www.jprs.co.jp A"を問い合わせ

```
% dig +norec @198.41.0.4 www.jprs.co.jp A↵

; <<>> DiG 9.12.1 <<>> +norec @198.41.0.4 www.jprs.co.jp A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 271
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 16

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.jprs.co.jp.                        IN      A

;; AUTHORITY SECTION:
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
jp.                     172800  IN      NS      c.dns.jp.
jp.                     172800  IN      NS      d.dns.jp.
jp.                     172800  IN      NS      e.dns.jp.
jp.                     172800  IN      NS      f.dns.jp.
jp.                     172800  IN      NS      g.dns.jp.
jp.                     172800  IN      NS      h.dns.jp.
```

画面8-1　ルートサーバーにwww.jprs.co.jpのAリソースレコードを問い合わせ

```
% dig +norec @198.41.0.4 www.jprs.co.jp A↵

; <<>> DiG 9.20.15 <<>> +norec @198.41.0.4 www.jprs.co.jp A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44357
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 16

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.jprs.co.jp.          IN A

;; AUTHORITY SECTION:
jp.                 172800 IN NS e.dns.jp.
jp.                 172800 IN NS g.dns.jp.
jp.                 172800 IN NS c.dns.jp.
jp.                 172800 IN NS a.dns.jp.
jp.                 172800 IN NS h.dns.jp.
jp.                 172800 IN NS d.dns.jp.
jp.                 172800 IN NS f.dns.jp.
jp.                 172800 IN NS b.dns.jp.
```

statusがNOERROR

ANSWERが0

flagsにaaがない

Authorityセクションに
jpへの委任が応答されている

委任先はa.dns.jp ～ h.dns.jpである

ということで…

- ランチタイムセミナーで予告した項目は、**ほぼすべて実現できました！**
- 教科書として最新情報に対応し、完成度が高まりました！

第1版をお持ちの皆さまにも
自信を持っておすすめ出来る内容に
仕上がったと思います！

おわりに～『DNSがよくわかる教科書』の今後

- DNSは枯れたプロトコルではなく、**現在も変化・進化を続けています。**
- そのため、**『DNSがよくわかる教科書』が教科書として十分ではなくなった時**には、**第3版**について検討する必要があると考えています。
- 例えば、委任を再設計する**DELEGレコードが標準化され、本格的に使われ始める時**は、その有力候補の一つだと思います。
  - Internet Week 2025会場のアンケートでは「**2035年～**」が多数でした。

『DNSがよくわかる教科書 第2版』を今後ともよろしくお願いします！

最後までお聞きいただき
ありがとうございました！

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

@JPRS_official　JPRSofficial　JPRSpress