

JPRSの技術情報発信 (2021年7月～2022年6月)

2022年6月24日

DNS Summer Day 2022

株式会社日本レジストリサービス (JPRS)

森下 泰宏

「DNSがよくわかる教科書」増刷！

- **6刷**になりました！
 - 2018年11月22日 発売（1刷）
 - 2018年12月（2刷）
 - 2019年7月（3刷）
 - 2020年6月（4刷）
 - 2021年2月（5刷）
 - **2021年12月（6刷）**
- 出版社サポートページに更新情報を随時掲載
 - 増刷時に書籍（紙・電子版）に反映



DNSがよくわかる教科書 | SBクリエイティブ
<<https://www.sbcr.jp/product/4797394481/>>

6刷での変更点

1. HTTPSリソースレコードに関する記述を追加

- コラム「HTTPS/SVCBリソースレコードの概要」追加（p.126）

2. Zonemasterの仕様変更への対応

3. QNAME minimisationのRFCが置き換わったことへの対応

4. DNS over HTTPSのOSでのサポートが進んだことへの対応

『DNSがよくわかる教科書』第6刷での変更点について
<<https://www.sbcr.jp/support/4815610010/>>

JPRSの技術情報発信

JPRSではインターネットの安定運用を目的として、さまざまな形でドメイン名・DNS・サーバー証明書に関する技術情報を発信しています。

- Web
 - JPRS DNS関連技術情報 <<https://jprs.jp/tech/>>
 - サーバー証明書発行サービス <<https://jprs.jp/pubcert/>>
 - 技術解説「JPRS トピックス & コラム」 <<https://jprs.jp/related-info/guide/>>
 - メディアへの寄稿
- 電子メール
 - メールマガジン「FROM JPRS」（登録は <<https://jprs.jp/mail/>> から）
 - 技術コミュニティのメーリングリストにおける情報提供
- SNS公式アカウント（[Twitter](#)、[Facebook](#)、[YouTube](#)）
- カンファレンス・イベントなどにおける発表・ブース出展

本日より紹介する技術情報発信

1. 脆弱性情報

- BIND（7件）
- BIND以外のDNS実装（8件）

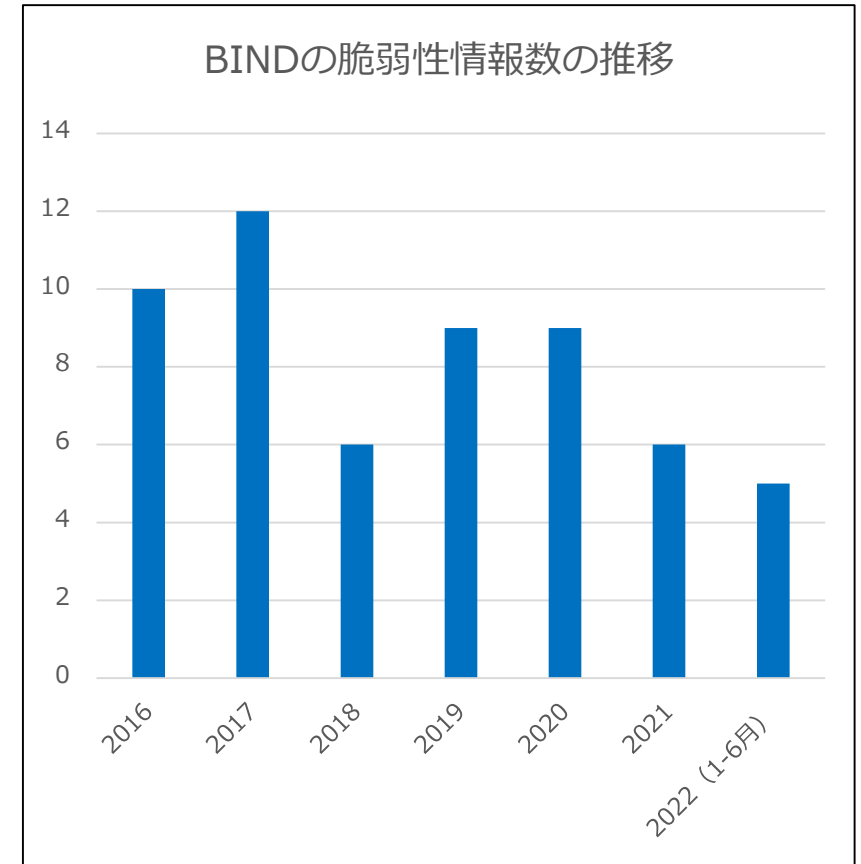
2. 技術解説

- トピックス&コラム公開（1件）

3. 新サイト「ポン太のインターネット教室」開設

脆弱性情報

- BIND（7件（緊急4件））
 - 2021年7月～12月：2件（前年同期：5件）
 - 2022年1月～6月：5件（前年同期：4件）
- BIND以外のDNS実装（8件）
 - PowerDNS Authoritative Server（2件）
 - PowerDNS Recursor（1件）
 - Windows DNS（5件）



（カッコ内は、JPRSが発信した脆弱性情報の件数）

脆弱性情報 (BIND) [1/2]

公開日	タイトル・URL	対象
2021/8/19	■ (緊急) BIND 9.16.19の脆弱性 (DNSサービスの停止) について (CVE-2021-25218) < https://jprs.jp/tech/security/2021-08-19-bind9-vuln-rrl.html >	9.16.19のみ
2021/10/28	■ BIND 9.xの脆弱性 (パフォーマンスの低下) について (CVE-2021-25219) < https://jprs.jp/tech/security/2021-10-28-bind9-vuln-lamecache.html >	9.3.0以降
2022/3/17	■ (緊急) BIND 9.18.0の脆弱性 (DNSサービスの停止) について (CVE-2022-0667) < https://jprs.jp/tech/security/2022-03-17-bind9-vuln-dslookup.html >	9.18.0のみ
2022/3/17	■ (緊急) BIND 9.18.0の脆弱性 (DNSサービスの停止) について (CVE-2022-0635) < https://jprs.jp/tech/security/2022-03-17-bind9-vuln-aggressiveuse.html >	9.18.0のみ
2022/3/17	■ BIND 9.xの脆弱性 (システムリソースの過度な消費) について (CVE-2022-0396) < https://jprs.jp/tech/security/2022-03-17-bind9-vuln-keep-response-order.html >	9.16.11以降
2022/3/17	■ BIND 9.xの脆弱性 (キャッシュポイズニングの危険性) について (CVE-2021-25220) < https://jprs.jp/tech/security/2022-03-17-bind9-vuln-forwarder.html >	9.1.0以降
2022/5/19	■ (緊急) BIND 9.18.xの脆弱性 (DNSサービスの停止) について (CVE-2022-1183) < https://jprs.jp/tech/security/2022-05-19-bind9-vuln-dns-over-https.html >	9.18.0以降

「9.18.0のみ」 「9.18.0以降」

脆弱性情報（BIND） [2/2]

- CVE-2022-0667 ・ CVE-2022-0635 （2022年3月）
 - DSレコードを要求する部分の処理において、namedが異常終了
 - 特定のクエリパターンを繰り返し受け取った際に、namedが異常終了

原因：コードのリファクタリングにおける不具合

- CVE-2022-1183 （2022年5月）
 - DNS over HTTPSの接続が早期に破棄されると、namedが異常終了

原因：新機能の実装における不具合

メジャーバージョンアップ（9.xx.yyのxxが上がる）の後や
新機能が追加された後は要注意

脆弱性情報（BIND以外） [1/2]

公開日	タイトル・URL
2021/7/16	■ Windows DNSの脆弱性情報が公開されました（CVE-2021-33745、他12件） < https://jprs.jp/tech/security/2021-07-16-windowsdns.html >
2021/7/29	■ PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2021-36754） < https://jprs.jp/tech/security/2021-07-29-powerdns-auth.html >
2021/9/17	■ Windows DNSの脆弱性情報が公開されました（CVE-2021-36968） < https://jprs.jp/tech/security/2021-09-17-windowsdns.html >
2021/10/15	■ Windows DNSサーバーの脆弱性情報が公開されました（CVE-2021-40469） < https://jprs.jp/tech/security/2021-10-15-windowsdns.html >
2022/2/10	■ Windows DNSサーバーの脆弱性情報が公開されました（CVE-2022-21984） < https://jprs.jp/tech/security/2022-02-10-windowsdns.html >
2022/3/30	■ PowerDNS Recursorの脆弱性情報が公開されました（CVE-2022-27227） < https://jprs.jp/tech/security/2022-03-30-powerdns-recursor.html >
2022/3/30	■ PowerDNS Authoritative Serverの脆弱性情報が公開されました（CVE-2022-27227） < https://jprs.jp/tech/security/2022-03-30-powerdns-auth.html >
2022/4/15	■ Windows DNSサーバーの脆弱性情報が公開されました（CVE-2022-24536、他17件） < https://jprs.jp/tech/security/2022-04-15-windowsdns.html >

「他12件」 「他17件」

脆弱性情報（BIND以外）[2/2]

- マイクロソフトのセキュリティ更新プログラム（月例）における大量報告
 - 2021年7月（13件）（**RCE10件**、DoS3件）
 - 13件中12件の謝辞に、Yuki Chen氏のクレジットあり
 - 2022年4月（18件）（**RCE17件**、情報漏えい1件）
 - 18件中15件の謝辞に、Yuki Chen氏のクレジットあり
- Yuki Chen（陳雪斌）氏とは？
 - 中国のセキュリティ企業に勤務する研究者
 - 著名なバグバウンティハンターとして、他にも多数の脆弱性を報告

技術解説

• トピックス&コラムNo.25 「トップレベルドメインのラベル生成ルール『ルートゾーンLGR』の概要」公開（2022年6月9日）

PDF版

<<https://jprs.jp/related-info/guide/025.pdf>>

HTML版

<<https://jprs.jp/related-info/guide/topics-column/no25.html>>

- ルートゾーンLGR（**Label Generation Rules**）とは？
 - ルートゾーンに登録可能なラベルの文字に関するルール
 - JPRSは日本語ラベルのルール検討に主体的に関与
 - 今後のgTLD募集では、ルールに従ったラベルのみ登録可能に
- コラムでは、作成の背景・作成のプロセス・全体ルール・日本語ラベルのルールについて解説


JAPAN REGISTRY SERVICES

JPRS トピックス & コラム
No.025


トップレベルドメインのラベル生成ルール「ルートゾーンLGR」の概要

トップレベルドメイン（TLD）に登録できるラベルの文字に関するルールである、「ルートゾーンLGR」の作成背景や作成プロセス、ルール概要、日本語ラベルのルールについて解説します。

日本語ラベルのルールを含む「ルートゾーンLGR（Root Zone Label Generation Rules）」の第3版が、ICANN*から2022年5月26日に公開されました。

ルートゾーンLGRは、トップレベルドメインのラベルの文字（英字や英字以外も含む）に関するルールを定めたものです。このルールに従ったトップレベルドメインだけが、ルートゾーン**に登録可能になります。

■ルートゾーンLGR作成の背景

ドメイン名のTLD部分（ラベル）には、英字（a～z）以外にも、漢字や平仮名、片仮名、ギリシャ文字といったさまざまな言語の文字（スクリプト）の利用が認められています。ただし、文字は言語を混ぜるものでなければなりません（記号や、改行などの制御文字は禁止されています）。

https://example.テスト → https://example.ドットイム

例1 ドメイン名のTLD部分（ラベル）

TLD部分は世界中のインターネット利用者がアクセスするため、インターネット利用者が「ラベルの認識」を混乱しないよう、言語・文字種で整合の取れたルールが必要です。特に、同時に使用できる文字の範囲や、同一とみなす文字の組の定義が重要です。

言語によっては、例えば漢字であれば「国」と「國」のように、異体字が存在します。通常、異体字は意味や発音が同じものを指しますが、ルートゾーンLGRでは、「カ（カタカナ）」と「カ（漢字）」のように発音が同じでも異なります。

また、先述や本文に用いることができない文字、特定の文字にのみ続く文字、文字の位置のルールも含まれます。

ルートゾーンの安定運用に支障を及ぼさないようにするためには、言語ごとにルールを適用し、それらが互いに整合していることが必要です。そこでICANNは、各言語コミュニティにおいて、それぞれの言語ルール案を作成し、それら各言語ルール案を統合して、TLDで利用可能な文字とその異体字を統合的に取り扱うためのルール「ルートゾーンLGR」を作成することにしました。

■ルール作成のプロセス（2種のパネル）

ルートゾーンLGRの作成は、以下の2種のパネルが行われます。

1. 生成パネル（GP: Generation Panel）

各言語のコミュニティを代表する有識者・言語やドメイン名の専門家により構成される。その言語に関するラベル生成ルールを作成するためのパネルです。生成パネルはルートゾーンに追加する言語ごとに組織されます。

2. 統合パネル（IP: Integration Panel）

文字コードや国際化ドメイン名の専門家により構成される。各言語の生成パネルが作成したルールの整合をとる、一つに統合するためのパネルです。ルールを一つに統合するため、統合パネルは一つしか存在しません。



図2 作成プロセスの概要

各言語の生成パネルは、言語コミュニティと連携し、言語ルール案の提案を作成します。統合パネルが提案書に技術的問題がないことを確認すれば、ICANNによる「パブリックコメント（意見募集）」の手続きが行われ、統合パネルによる最終評価の後、ルートゾーンLGRに統合されます。

2022年5月26日に公開されたルートゾーンLGRでは、25の言語ルールが統合されています。

* ICANN: Internet Corporation for Assigned Names and Numbers
 * Root Zone Label Generation Rules
 https://www.icann.org/news/2022/05/26/rz-lgr-22-05-26-en
 * トップレベルドメインを登録に必要となるICANNの報告書またはファイル
 * Minimal Starting Repertoire
 https://www.icann.org/news/2022/05/26/rz-lgr-22-05-26-en
 * ロンジン文字で「テスト」の意味

新サイト「ポン太のインターネット教室」開設！

- ドメイン名・DNSをはじめとする、インターネットの基盤技術について学べるサイト
- マンガ小冊子「ポン太のネットの大冒険」と連動
 - 過去12年間で約1,800の教育機関に、33万冊以上を無償配布



ポン太のインターネット教室
<<https://withponta.jp/>>

コンテンツのご紹介

- **公開済み**（2022年5月16日）

01 インターネットの世界ってどうなっているの？

02 URLとドメイン名って同じじゃないの？

03 DNS（ドメインネームシステム）を学ぼう！

- **公開予定**（2022年6月30日）

04 日本のドメイン名「.jp」のヒミツ

05 みんなで動かすインターネット



各章の構成 [1/2]

- 技術解説（メインページ）

DNSに欠かせない存在「ルートサーバー」

DNSの「分散管理」下で、「情報を探す人」は「情報を持っている人たち」から目的の情報をどうやって探し出すのでしょうか？

分散管理では、ドメイン名の階層構造に合わせる形で情報を持ちます。つまり、「情報を持っている人たち」は「自分が管理する階層の情報」と「その下の階層の管理を誰に任せたのか」という情報だけを持つことになります。



さらに、ドメイン名の一番上の階層は「ルート」と言います。図の赤い点がルートです。ルートはIPアドレスを探す旅の起点となります。ルートはDNSにとってとても大切なものですが、ドメイン名を書く時、通常は省略されています。

そして、ルートは「ルートサーバー」と呼ばれるサーバーで管理されています。

TIPS

ルートサーバーはどこにあるの？

- 解説動画

「教えて、ドメイン名先生！」

DNSの名前解決

情報を探す人
フルリゾルバー

情報を持っている人たち
権威DNSサーバー

どっちも「DNSサーバー」と呼ばれているけど
全然別のサーバーで、役割も違う！

各章の構成 [2/2]

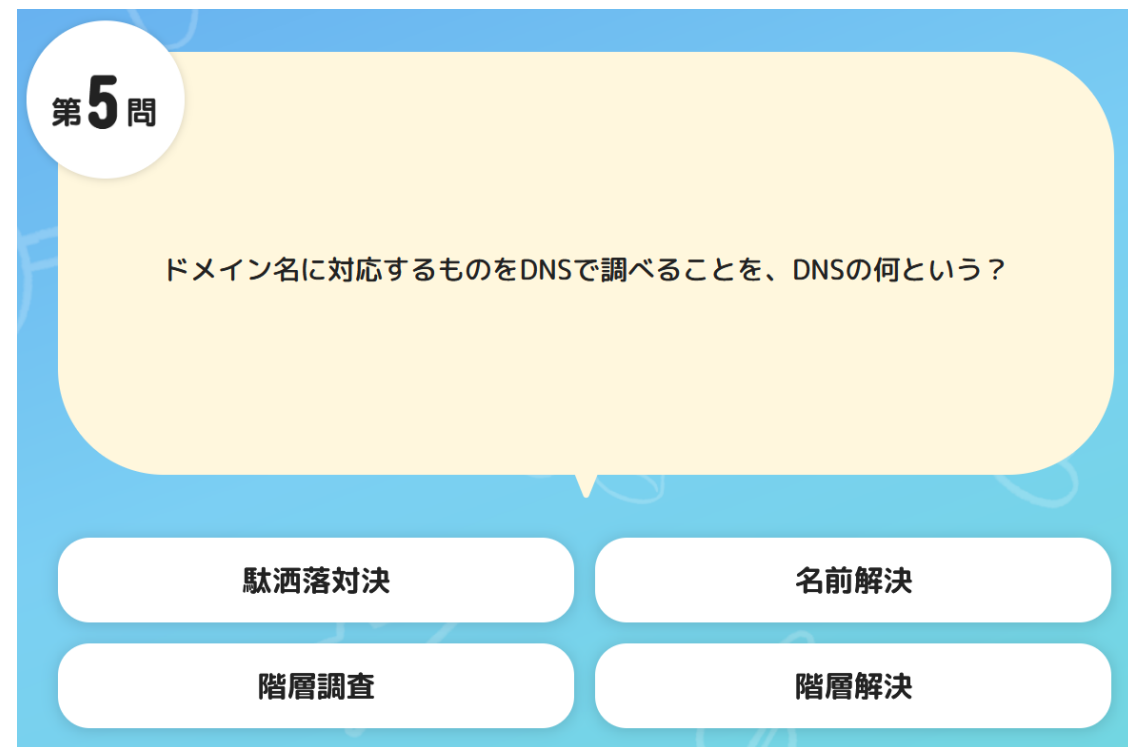
- 体験コーナー

- 「情報を探す人」を体験



- チェックテスト

- 章ごとに10問の問題を準備



テクニカルレビュー担当者としての所感

- **嘘をつかずに、わかりやすく省略する難しさ**を痛感しました
 - NHK「ブラタモリ」のアウトリーチ手法だそうです

参考：地球科学者・尾方隆幸氏のツイート

<<https://twitter.com/s15taka/status/1132667988539203584>>

“ブラタモリから地球科学研究者が学べることはたくさんあるが、私としては特に「**科学性とわかりやすさを両立する手法**」「**省略する勇気**」「お隣さんが何をやっているかを知るきっかけ」を得たことが大きかった。**妥協できない部分**を知ることができた点も、ブラタモリから学んだことといえるかもしれない。”

- さまざまな場面で、ご活用いただければ幸いです
 - **当社の新入社員の教育にも活用しています**

JPRSでは今後もさまざまな形で
技術情報発信を続けていきます



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



[@JPRS_official](#)



[JPRSofficial](#)



[JPRSpress](#)