Engineer

DNS

名前をアドレスへ変換するディレクトリー

どのようなものか

DNS、Domain Name Systemは、インターネットが、ほかのほとんどの処理の前に参照する、分散したディレクトリーです。`example.com`のような名前について、プログラムが接続先のアドレスを問い合わせます。同じ仕組みが、ほかの問いにも答えます。その名前のメールを受け取るサーバー、所有者が公開したテキスト、その名前を管理するサーバーなどです。

ディレクトリーは、右から左へ読む木です。最上位にルートがあり、その下に`.com`や`.dk`のようなトップレベルドメイン、さらにその下に登録するドメイン、その下に所有者が作るサブドメインがあります。一台のサーバーが、木全体を持つわけではありません。各段階が、次の段階の責任を、名前で指定したサーバーへ委譲します。一組のサーバーが回答に責任を持つ木の範囲を、ゾーンと呼びます。ゾーンを管理する人が、名前の解決先を決めます。

二種類のサーバーが働きます。権威サーバーは、ゾーンを保持し、確定的な答えを返します。インターネットプロバイダー、企業、公開サービスが運用する再帰リゾルバーは、クライアントの代わりに木をたどります。ルートサーバーに`.com`の場所を聞き、`.com`に`example.com`の場所を聞き、そのドメインのサーバーにレコードを問い合わせ、答えを返します。OS側で動くのは、小さなスタブリゾルバーだけです。再帰リゾルバーへ問いを渡し、待ちます。

答えは、型を持つレコードです。ゾーンファイルは、それらを記述する従来からの方法です。

```
$ORIGIN example.com.
$TTL 3600
@     IN  SOA    ns1.example.net. hostmaster.example.com. (
                 2026101701 7200 900 1209600 300 )
@     IN  NS     ns1.example.net.
@     IN  A      192.0.2.10
```

```
@     IN  AAAA   2001:db8::10
www   IN  CNAME  example.com.
@     IN  MX     10 mail.example.net.
@     IN  TXT    "v=spf1 include:_spf.example.net -all"
```

`A` と `AAAA` は、IPv4とIPv6のアドレスを示します。 `CNAME` は、ある名前を別の名前の別名にします。 `MX` は、メールを受け取るサーバーを示し、 `TXT` は自由なテキストを運びます。実務では、メール認証の方針や、ドメインを管理している証明です。 `NS` と `SOA` は、ゾーン自体を説明します。

すべてのレコードには有効期間があり、この例では3,600秒です。この数字が、DNSの動作を決めます。答えを取得したリゾルバーは、TTLが切れるまで、再度問い合わせずに使い続けられます。そのため、ほとんどの問い合わせに、クライアントに近いキャッシュから答え、権威サーバーへ一時的に届かなくても、応答し続けられます。その代わり、世界中にある古い答えを、期限前に強制的に忘れさせることはできません。

概念を判断に生かす

「DNSとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 Wi-Fi、ファイアウォール、リモートアクセスを整え、どこからでも働け、権限のある人だけが接続できるようにします。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Ubuntu Linux VPSインスタンス30台を管理 — 30 復旧計画とともに管理したLinuxサーバー

Ubuntu Linux VPSインスタンス30台を管理 お問い合わせ →

なぜ重要なのか

名前付きのサービスへ接続するときは、まず名前を調べます。DNSが間違っていれば、サーバー自体は完全に正常でも、サイト、API、メールは止まって見えます。何も届かないためです。正しければ誰も気にしないので、システムの中で、最も文書化が手薄になりがちです。

DNSは、ドメインの管理権を行使し、証明する場所でもあります。メールのプロバイダーは、 `TXT` レコードからSPF、DKIM、DMARCの方針を読み、そのドメインから来たというメッセージが本物かを判断します。そのため、レコードが間違っていたり、なかったりすると、正当なメールが迷惑メールになります。認証局やホスティングサービスは、名前を所有している証明として、特定の値のレコー

ドを求めます。ゾーンを編集できれば、サイトを転送し、メールを横取りし、ドメインの証明書を取得できます。DNSアカウントへのアクセスは、サーバーへのアクセスと同じほど、慎重に扱う必要があります。

キャッシュが、すべての変更を左右します。伝播と呼ばれるものは、実際には、何千ものリゾルバーが、自分のコピーの期限切れを待っている状態です。影響を抑えてサイトを移すには、一日ほど前にTTLを下げ、古いTTLの時間が過ぎるのを待ち、変更し、落ち着いてからTTLを上げ直します。

従来のDNSは平文で流れ、問いも答えも、秘密にはなりません。DNSSECを使うと、答えが本当にゾーンの所有者から来て、改変されていないことを確かめられます。その仕様自体が、機密性は加えないとしています。DNS over HTTPSのような暗号化した通信は、経路上のネットワークから問いを隠しますが、相手側のリゾルバーは、調べた名前をすべて見ます。リゾルバーを選ぶことは、その一覧を渡す相手を選ぶことです。

実際の活用例

自社のゾーンは、よくある出発点と、抜け出す方法を示します。プロバイダーの管理画面に、約二十のレコードを保持していました。ウェブ、gitサブドメイン、個人用の二つの転送、外部のメールボックスプロバイダーを経由するメール、トランザクションメールの送信ドメイン、両方の認証レコードです。管理画面では、現在の状態は、最後にクリックした人が残したものです。今は、ゾーンをリポジトリのデータとして保持します。稼働中のレコード、アプリ用のレコード、トランスポートポリシーのレコード、削除予定のレコードの別一覧です。一つのプレイが、宣言した内容をプロバイダーのAPIと突き合わせ、反映します。さらに二つの実行経路は、明示的にタグを指定した場合にだけ有効になります。何も変更せず差分を報告する監査と、標準のゾーンファイル形式に書き出すエクスポートです。リポジトリ以外でも読めるようにします。最もよく使うのは監査です。差分をなくすよりも、知りたい場合の方が多いためです。

同じプロバイダーの仕事は、意図的に狭くしています。クレジットのページは、CloudflareがサイトのDNSだけに応答すると説明します。前段のプロキシは使いません。また、サーバーのアドレスをそのまま載せています。DNSが、尋ねる人すべてへ、すでに渡しているためです。

DNSを読むことも、管理するシステム群の通常の状況報告に含まれます。稼働中のホストをMarkdownへ書き出す、七つの読み取り専用レポートロールの一つに、プロバイダーのインベントリーがあります。二つのクラウドAPIと、一つの

専用サーバーAPIに加え、DNSを読みます。その実行で測っていない数字は、どのレポートも出力しない規則に従います。

問題が起きるところ

DNSの障害は、遅れて現れ、キャッシュに残り、人によって結果が分かれることが多くあります。そのため、同じ名前が、ある人には使えても、別の人には使えません。繰り返す例は、次のとおりです。

変更が届きません。有効期間が一日のレコードを変え、すぐ新しいアドレスになると期待しても、古い答えをキャッシュしたリゾルバーは、そのコピーの期限が切れるまで使います。新しい名前にも、目立ちにくい別の問題があります。レコードができる前に問い合わせると、存在しないという答えも、ゾーンの `SOA` が許す期間、キャッシュされます。RFC 2308が定める動作です。予定した変更の前にTTLを下げ、何かが尋ねる前にレコードを作ります。

別名を、置けない場所へ置きます。RFC 1034では、 `CNAME` のある名前には、ほかのデータを置けません。ドメインの頂点である `example.com` 自体には、必ず `SOA` と `NS` があります。そのため、標準に従うゾーンは、頂点を別名にできません。 `MX` や `TXT` も必要なサブドメインへ `CNAME` を置くと、同じ規則に反します。プロバイダーは、独自の回避策として、フラット化したレコードや `ALIAS` を提供します。動作はそれぞれ少し異なるので、使うプロバイダーが実際に何を返すか、その説明を読みます。

メール認証が、限界を超えます。SPFの `include` は、それぞれDNSの問い合わせを起こし、RFC 7208は合計を十回に制限します。ニュースレターやチケット管理のサービスを一つ増やすだけで、超える場合があります。受信側は、方針を恒久的なエラーと扱い、認証するはずのメールを、その方針なしで判断します。送信者を加えるたびに、問い合わせ数を数えます。

レコードだけが、宛先より長く残ります。サブドメインの `CNAME` が、削除済みのクラウドストレージのバケットやホスティングアプリを指します。プロバイダーが、そのリソース名を誰にでも取得させるなら、第三者が取得し、ドメインの評判を伴って、自分のコンテンツをそのサブドメインで提供できます。宛先を削除する変更と一緒に、レコードも消します。

ゾーンが、管理画面にしかありません。履歴、レビュー、差分がないので、 `MX` を誤って消しても、メールが届かなくなって初めて気付きます。前の値は、記憶から再現しなければなりません。定期的なエクスポート、さらによい方法として

コードによる宣言を行うと、どの変更にも、記録と戻る道ができます。

参考資料

- RFC 1035：ドメイン名、実装と仕様 — レコード形式、ゾーンファイルの構文、通信時のプロトコルです。
- RFC 1034：ドメイン名、概念と機能 — 木、ゾーン、委譲、リゾルバーによる探索です。
- RFC 9499：DNSの用語 — このページで使う言葉の、厳密な定義です。
- RFC 2308：DNS問い合わせの否定的応答のキャッシュ — 名前が存在しないことを、リゾルバーが覚えていてよい期間です。
- RFC 4033：DNSセキュリティーの概要と要件 — DNSSECが守るものと、守らないものです。
- RFC 8484：HTTPS経由のDNS問い合わせ — 通常の暗号化したウェブ通信の中で、問い合わせを運ぶ方法です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「DNSとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/dns/