JPRS トピックス＆コラム

■DNSのしくみと動作原理 ～インターネットを支え続けるDNS～

DNSはインターネットにとって不可欠な存在です。しかし、その動作原理について正しく理解している人は意外に多くないようです。今回はDNSのしくみと動作について解説します。

■インターネットにおける通信のしくみ

DNS について解説する前に、インターネットにおける通信のしくみについて簡単におさらいしておきましょう。

インターネットでは通信相手を「IP アドレス」という番号で指定・識別しています。IP アドレスはインターネットに接続しているすべての機器に割り当てられ、各機器は割り当てられた IP アドレスによって識別されます。

IP アドレスはインターネットに接続しているすべての機器で異なっており、同じ IP アドレスが異なった機器に重複して割り当てられることは原則としてありません。

そして、インターネットで機器同士が通信を行う場合、送信側で受信側の IP アドレスを指定してデータを送信します。そして、受信側で送信されてきたデータの IP アドレスを調べることにより、どの相手からデータが送られてきたのかを調べることができます（図1）。

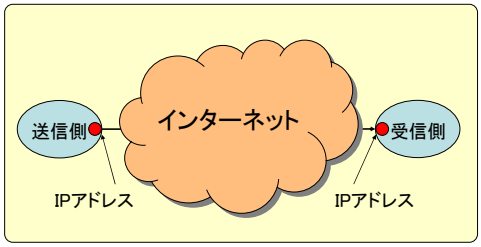

図1: インターネットにおける通信のしくみ

■DNS の役割

このようにインターネットでは、IP アドレスが送信先の指定や送信元の特定に使われています。実際に、ユーザーが接続先を、例えば http://192.0.2.1/ （IPv4 の場合）や http://[2001:db8::1]/[1] （IPv6 の場合）のように IP アドレスで直接指定しても、Web サイトを見ることができます[2]。

しかし、我々がインターネットを使う場合、このような形で IP アドレスを直接指定する必要はほとんどありません。通常は http://jprs.jp/ のような覚えやすい名前（**ドメイン名**）を使って接続先を指定できるからです。

DNS（Domain Name System）はこのように、人間が記憶しにくい IP アドレスに替え、より記憶しやすく使いやすい「名前」をインターネット上で使えるようにするために開発されたシステムです（図 2）。

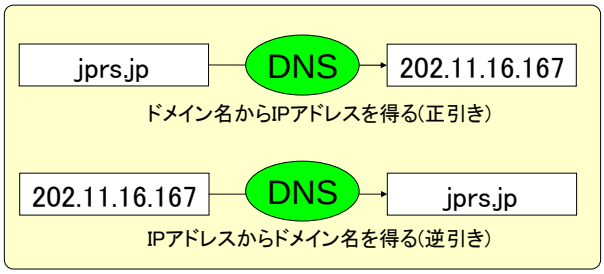

図2: DNS の役割（名前と IP アドレスの関連付け）

■DNS 開発物語—HOSTS.TXT から DNS へ

ここでは DNS が開発され、実際に使われるようになるまでの歴史を振り返りながら、DNS の成り立ちについて解説します。

インターネットの前身であった ARPANET[3]では、ホスト名と IP アドレスの対応表として、HOSTS.TXT というテキストファイルを使っていました。

ARPANET が運用されていた 1970 年代から 80 年代にかけ、HOSTS.TXT のマスターファイルは IP アドレスの国際割り当て機関であった米国の SRI-NIC[4]で管理され、FTP により公開されていました。新しく ARPANET に接続した組織は最新の HOSTS.TXT を SRI-NIC から入手し、自分のコンピューターに導入していました。

---

[1] IPv6 接続環境が必要になります。
[2] Web サーバー側でバーチャルホスト機能を使用している場合など、IP アドレスを直接指定して見ることができない場合もあります。
[3] 1969 年に米国国防総省高等研究計画局（ARPA）により構築されたコンピューターネットワーク。
[4] Stanford Research Institute – Network Information Center

※掲載内容は2014年12月現在のものです。

HOSTS.TXTを入手し、自分のコンピューターに導入することにより、相手先のコンピューターを名前で指定することができるようになります(図3)。

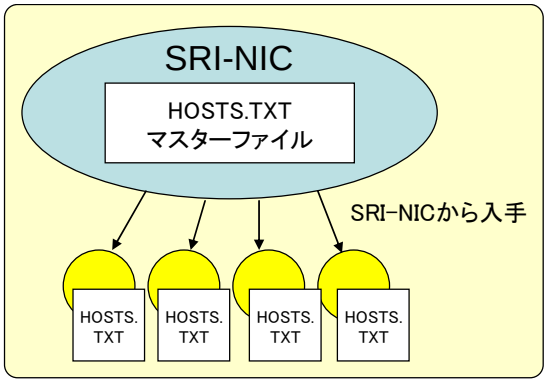

図3: HOSTS.TXTによる名前管理

名前とIPアドレスの対応に追加や変更などがあった場合、ユーザーはその変更内容をSRI-NICに電子メールで通知します。SRI-NICではその都度HOSTS.TXTの更新作業を行い、更新したファイルを公開します。各組織では定期的にSRI-NICからHOSTS.TXTを入手、更新することにより、常に最新の情報に保つことができることになります。

しかしこの方法は、

① 接続ホスト数の増加による、HOSTS.TXTファイル自身の肥大化
② HOSTS.TXTファイルの更新頻度の増大による、SRI-NICの作業量の増加
③ マスターファイルを集中管理する、SRI-NICのサーバーの負荷の増大

などの理由により、1980年代の初頭には既に限界に達していました。そのため当時、問題を解決するための新たな仕組みの開発が急務となっていました。

そして、問題解決の手段として**DNS**が開発され、最初のバージョンが1983年にRFC 882およびRFC 883として公開されました。その後、RFC 882とRFC 883は1987年に**RFC 1034**と**RFC 1035**に改版され、現在のDNSになりました。DNSはその後も多くの機能付加や改良が施され、開発から30年以上が経過した現在も、インターネット上で広く使われています。

■DNSの基本—階層構造と委任の原理

DNSのしくみのうち最も重要な、「**階層構造による分散管理**」と「**委任の原理**」について解説しましょう。

従来からのHOSTS.TXTによる集中管理方式では、インターネット(ARPANET)におけるすべての名前とIPアドレスの対応表を、SRI-NICやDDN NICにおいて集中管理していました。そのため、インターネット自身の成長により名前の管理が限界に達してしまいました。

そこでDNSでは、この対応表を各組織において**分散管理**することにより全体の負荷を軽減し、かつネットワーク全体で**一つの大きな対応表のように連携して動作する**ようにするための仕組みの開発が、重要なテーマとなりました。

▼ドメイン名の導入と対応表の分散

そこでDNSでは、「**ドメイン名**」と呼ばれる新しい概念が導入されました。従来のHOSTS.TXTによる名前管理方式ではすべての名前を一カ所で集中管理していたのに対し、DNSではドメイン名を用いた**階層構造**の導入を行い、階層的な名前(**名前空間**)による分散管理を実現したわけです。

DNSによる管理では、まず名前空間の起点となる「**ルートサーバー**」と呼ばれるDNSサーバーを配置します。ルートサーバーは「jp」や「com」など、各ドメイン名の一番右側[5]のドメイン名(**TLD**)のDNSサーバーが、インターネット上のどこにあるのか(どのIPアドレスにあるのか)を管理します。

そしてルートサーバーでは通常、各組織内の実際のドメイン名とIPアドレスの対応表は管理しません(図4)。

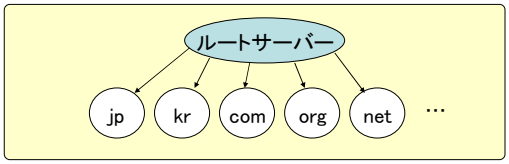

図4: ルートサーバー

[5] ドメイン名による管理方法では左から右に行くに従い、より広い名前空間を表します。

次に「jp」や「com」などといったTLDを管理するDNSサーバー（**TLDサーバー**）では、自分が管理しているTLD内の情報のみを管理します。例えばjpのDNSサーバーではjpの下の階層、つまり「example.jp」や「日本語.jp」などのDNSサーバーがどこにあるか（どのIPアドレスにあるか）という情報のみを管理します。

TLD サーバーにおいても通常、各組織内の実際のドメイン名とIP アドレス対応表は管理しません（図5）。

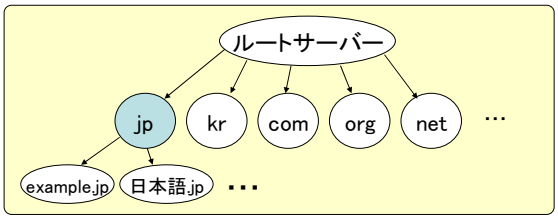

図5: TLD サーバー

その下の階層に準備される DNS サーバーでは、例えば「example.jp」というドメイン名内の名前のみを管理することになります。例えば「www.example.jp」のような名前とIP アドレスの実際の対応表を持たせることもできますし、「subdomain.example.jp」といった、更に深い階層のドメイン名を設定することも可能です（図6）。

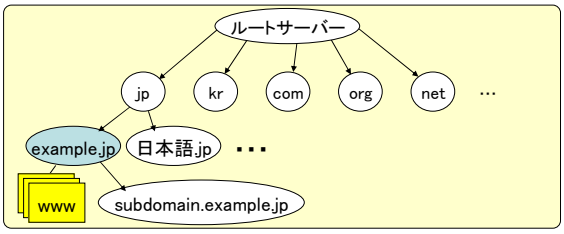

図6: 各組織の DNS サーバー（対応表を管理）

DNS では、このようなドメイン名の**委任**（delegation）により、それぞれの名前の管理権限を明確にすることができます。そして、ドメイン名と IP アドレスの対応表は、各組織の DNS サーバーにおいて分散管理されるため、データの一極集中を回避することができます。

■DNS における実際の問合せの流れ

では、このようにデータが分散管理された DNS における**名前解決**（ある名前に対応する IP アドレスを得ること）は、どのように行われるのでしょうか。

www.example.jp のIP アドレス情報をDNS で入手する場合を例に、順を追って解説しましょう（図7）。

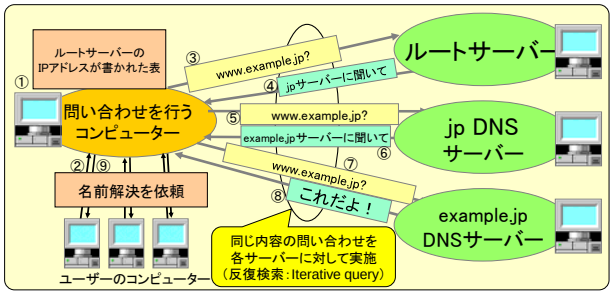

図7: 実際の問い合わせの流れ

① まず「**それぞれの DNS サーバーに対し、問い合わせを行うコンピューター**」を用意します。そのコンピューターには**ルートサーバーの IP アドレスが書かれた表を、あらかじめ準備**しておきます。

② www.example.jp に対する IP アドレスの情報が必要になった場合、ユーザーは問い合わせを行うコンピューターに**名前解決を依頼**します。

③ 依頼を受けたコンピューターは、ルートサーバーに www.example.jp の IP アドレスを問い合わせます。

④ ルートサーバーはこの名前に対する IP アドレスの情報を管理していません。しかし、**jp を管理している DNS サーバーの情報は知っている**ので、問い合わせ元に jp の DNS サーバーの情報を返します。

⑤ 応答を受け取ったコンピューターはその情報を元に jp の DNS サーバーに対し、**③と同様の形で** www.example.jp の IP アドレスを問い合わせます。

⑥ jpの DNS サーバーもルートサーバーと同様、自分が知っている example.jp の DNS サーバーの情報を、問い合わせ元に返します。

⑦ 応答を受け取ったコンピューターはその情報を元に example.jp の DNS サーバーに対し、③と同様の形で www.example.jp の IP アドレスを問い合わせます。

⑧ example.jp の DNS サーバーは、自分が管理している対応表から www.example.jp の IP アドレス情報を、問い合わせ元に返します。

⑨ 応答を受け取ったコンピューターは、入手した IP アドレスの情報をユーザーに返します。

以上の①から⑨までの手順によりユーザーは、www.example.jp の IP アドレス情報を入手できます。

このように DNS では、問い合わせを行うコンピューターが、情報を管理しているそれぞれの DNS サーバーに対し、ルートサーバーから順に**反復検索**（Iterative query）を行うことにより、名前解決が行われます。

■異なった機能を持つ 2 種類の DNS サーバー

前述した「問合せを行うコンピューター」は、ユーザーのコンピューターに対し名前解決のサービスを提供する役割を備えていることから、**階層構造を構成する DNS サーバーと同様、DNS サーバーと呼ばれています。**

しかし、この DNS サーバーはこれまでに説明した DNS サーバーとは異なり、下の階層の DNS サーバーの情報やホスト名と IP アドレスの対応表など、名前情報の**実体は管理していない**ことに注意する必要があります。

すなわち DNS では、

①**階層構造をたどり、名前解決を行う**サーバー

②**階層構造を構成し、情報を管理する**サーバー

の、**異なった機能を持つ 2 種類の「DNS サーバー」**が存在することになります（図8）。

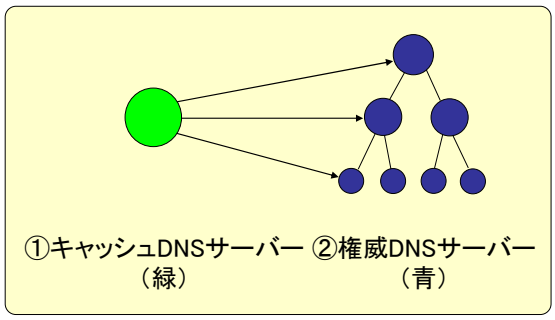

図8: 2 種類の DNS サーバー

DNS では①のサーバーを「フルリゾルバー（full resolver）」と呼びます。フルリゾルバーは名前解決の際に得られた名前情報をキャッシュする機能[6]を備えていることから、**キャッシュ DNS サーバー**（caching DNS server）と呼ぶことが一般的です。

また、②のサーバーを、それぞれのドメイン名に対する管理権限（オーソリティ）を持つことから、**「権威 DNS サーバー**（authoritative DNS server）」と呼びます。

DNS を理解する場合、この 2 種類のサーバーの動作と役割を**きちんと区別して把握する**ことが重要です。

[6] 得た情報を一時的に記憶し、非効率な再検索を防ぐための機能。

■サーバーの機能の違いに注意―機能分割を

DNS リフレクター攻撃[7]やカミンスキー型攻撃手法[8]に対する防御のため、権威 DNS サーバーとキャッシュ DNS サーバーを別のサーバー、あるいは別の IP アドレスに**機能分割**し、そのうえでキャッシュ DNS サーバーに適切な**アクセスコントロールを実施**し、オープンリゾルバー[9]として利用されないように対策することが強く推奨されています。

また、権威 DNS サーバーでは名前解決を行う必要がないため、階層構造をたどる反復検索機能は必要ありません。そのため権威 DNS サーバーではオープンリゾルバーとして利用されないように、**再帰検索要求の受け付けを無効に設定**することが強く推奨されています。

■重要な DNS サーバーの多重化と信頼性の向上

DNS では階層構造によって名前が管理されているため、階層構造を構成している権威 DNS サーバーに障害が発生した場合、その影響はインターネット全体に及ぶことになります。

そのため、特に重要な役割を負っているルートサーバーや TLD の DNS サーバーなどでは、権威 DNS サーバー自身の冗長化に加え、IP Anycast[10]などの技術を導入することにより、DNS サービスが停止することがないよう、細心の注意を払った運用が行われています。

■インターネットを支え続ける DNS

インターネットで DNS が運用され始めてから、既に 30 年以上が経過しています。しかし DNS は現在も運用開始当初と基本的に同じ仕組みで運用されており、最近では電子メールの送信元認証（SPF や DKIM）に使われるなど、その重要度がさらに高まっています。

DNS は今後も、成長し続けるインターネットを支える、重要な基本機能の一つであり続けることでしょう。

[7] DNS リフレクター攻撃については JPRS トピックス&コラム No.003「DDoS にあなたの DNS が使われる」をご参照ください。

[8] カミンスキー型攻撃手法については JPRS トピックス&コラム No.009「新たなる DNS キャッシュポイズニングの脅威」をご参照ください。

[9] 必要なアクセスコントロールや機能制限が実施されておらず、インターネット上のどこからの名前解決要求であっても実行してしまう状態の DNS サーバー。

[10] IP Anycast の詳細については JPRS トピックス&コラム No.005「DNS のさらなる信頼性向上のために」をご参照ください。

