DNS(ネーム)サーバ

(1)DNS サーバとは・・・

DNS(Domain Name Server)はインターネットに接続するときに IP アドレス(xxx.xxx.xxx.xxx)を、hal.com の様に人間に分かりやすくアドレスを変換してくれるサーバです。

(2)ドメイン名のしくみ

郵便で手紙を送る時に住所が必要であるのと同様に、インターネットでは、電子メールを送ったりウェブサイトを見たりするために、相手がインターネット上のどこにいるのかを特定する必要があります。ドメイン名は、言ってみれば「インターネット上の住所」にあたるものです。

●ドメイン名の構成・・・ドメイン名は、以下のように表示されます。(赤字の部分がドメイン名)

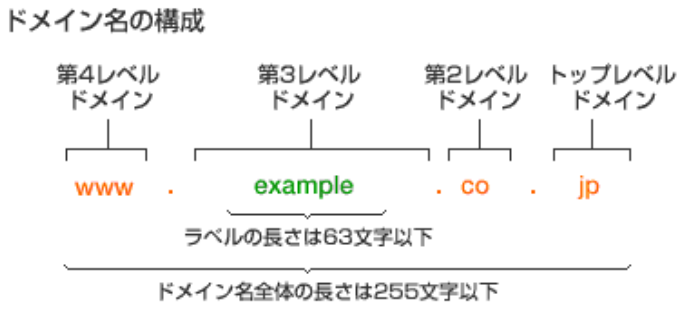
電子メールアドレスの場合　　taro@**example.co.jp**

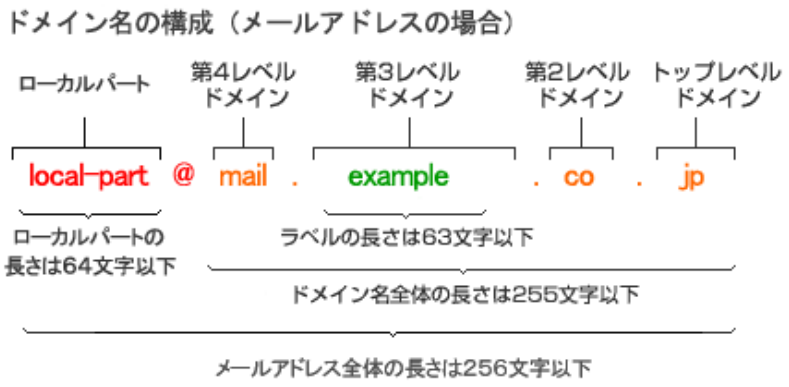
ウェブアドレスの場合　　**www.example.co.jp**

ピリオド(.)で区切られた部分は「ラベル」と呼ばれます。1 つのラベルの長さは 63 文字以下、ドメイン名全体の長さは、ピリオドを含めて 255 文字以下でなければなりません。ラベルには、英字(A～Z)、数字(0～9)、ハイフン(-)が使用できます(ラベルの先頭と末尾の文字をハイフンとするのは不可)。ラベル中では大文字・小文字の区別はなく、同じ文字とみなされます。

ただし、「ジェーピーニック.jp」などの日本語ドメイン名の場合は、上記に加えて全角ひらがな、カタカナ、漢字なども使用できます。また、1 つのラベルの長さは 15 文字以下となります。

ドメイン名を構成する最も右側のラベルを「トップレベルドメイン」と呼び、以下左へ順に「第 2 レベルドメイン」、「第 3 レベルドメイン」、……と呼びます。





(3)DNS とは

実は、インターネット上のコンピュータ同士が通信する際には、「123.45.67.89」といった数字をピリオドでつないだ**「IP アドレス」と呼ばれる番号によって通信相手を特定している**のですが、このような数字の羅列を人間が識別するのは非常に困難です。そこで、人間が覚えやすいように「hal.ac.jp」といった文字列からなるドメイン名が利用されているわけです。

ドメイン名を使ってインターネット上でやりとりを行うためには、これをコンピュータ同士が通信するために必要な IP アドレスに変換させなければなりません。この**ドメイン名と IP アドレスを対応づけるしくみがドメインネームシステム(DNS)**であり、「インターネットの住所録」にあたります。

(4)DNS の構造

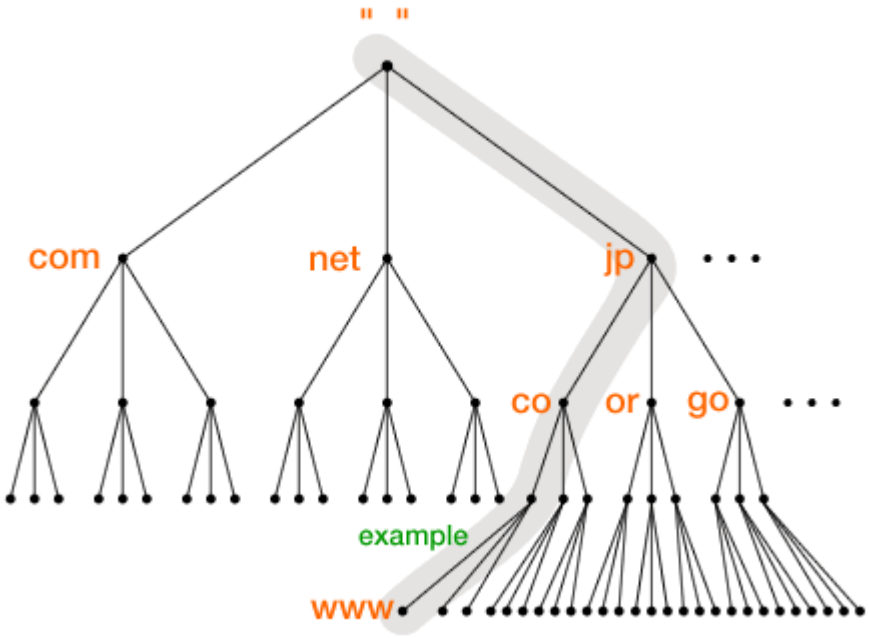
下の図は DNS の構造を表したもので、**ドメイン名空間**と呼ばれます。これは、木をさかさまにした形となっており、一番上の「ルート(root)」と呼ばれる部分(「　」で表現される)を頂点にして、下の階層へと空間が広がっていきます。ルートの下には「com」「net」「jp」などのトップレベルドメインが配置され、そのさらに下に第 2 レベルドメイン、第 3 レベルドメイン……と続きます。

あるドメインの下の階層に複数のドメインを新設する場合は、必ず異なるラベルをつけるようにしなければなりません。これによって、ドメイン名空間を構成するすべてのドメイン名は必ず一意性が保証されるようになっています。

それぞれの階層の各ドメインには**「ネームサーバー」と呼ばれるデータベース機能が配置**され、その空間にある名前の管理を行っています。ネームサーバーは、基本的にはその配下にあるドメイン名と IP アドレスの対応関係を管理するものですが、そのさらに下の階層のドメイン(サブドメイン)を管理しているネームサーバーの位置を示す役割も担っています。

ドメイン名空間の最上位にあるネームサーバーは**「ルートサーバー」**と呼ばれます。このルートサーバーが管理している「ルートゾーン」には、「jp」や「com」といったトップレベルドメインのネームサーバー(のホスト名と IP アドレス)が記述されており、ルートサーバーはそれらのネームサーバーがどこに位置しているのかを把握しているというわけです。

ドメイン名空間



(5)DNS が誕生した理由

現在のインターネットの前身である ARPANET では、**「HOSTS.TXT」というテキストファイル**を使用して名前の管理を一元的に行っていました。しかし、ARPANET の規模拡大とともに、HOSTS.TXT による集中管理は破綻をきたすことになります。HOSTS.TXT の更新が週 1、2 回であったということもあり、ローカルサイトのホスト情報が変わっても、それが HOSTS.TXT に反映されるまでに時間がかかるという問題がありました。また、ネットワークに接続するホスト数の増加に伴い、HOSTS.TXT が巨大なファイルとなり、これをダウンロードするトラフィックがネットワークの大きな負荷となってしまうという問題も発生しました。

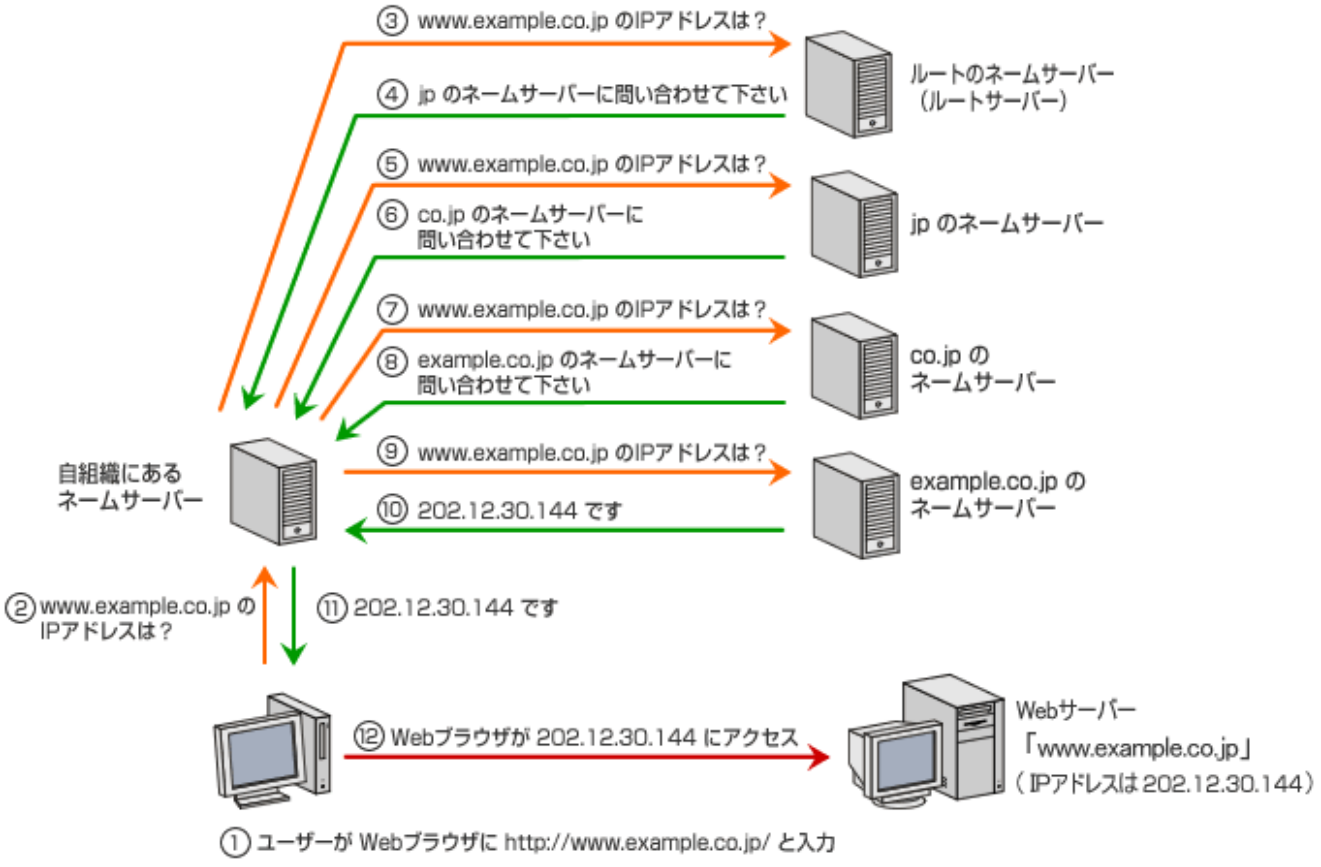
そこで、こうした問題を解決するための新たな仕組みとして DNS が考案されました。DNS は、上の図に示したような階層構造を持つことによって、**データを分散管理することが可能**になっています。これにより、DNS ではローカルに管理されているネームサーバーでホスト情報を更新することができるようになり、その更新結果がネットワーク全体に反映される仕組みとなっています。

Windows10 では　C:¥Windows¥System32¥drivers¥etc
MAC では　/private/etc/hosts　にあります

(6)DNS における名前解決の方法

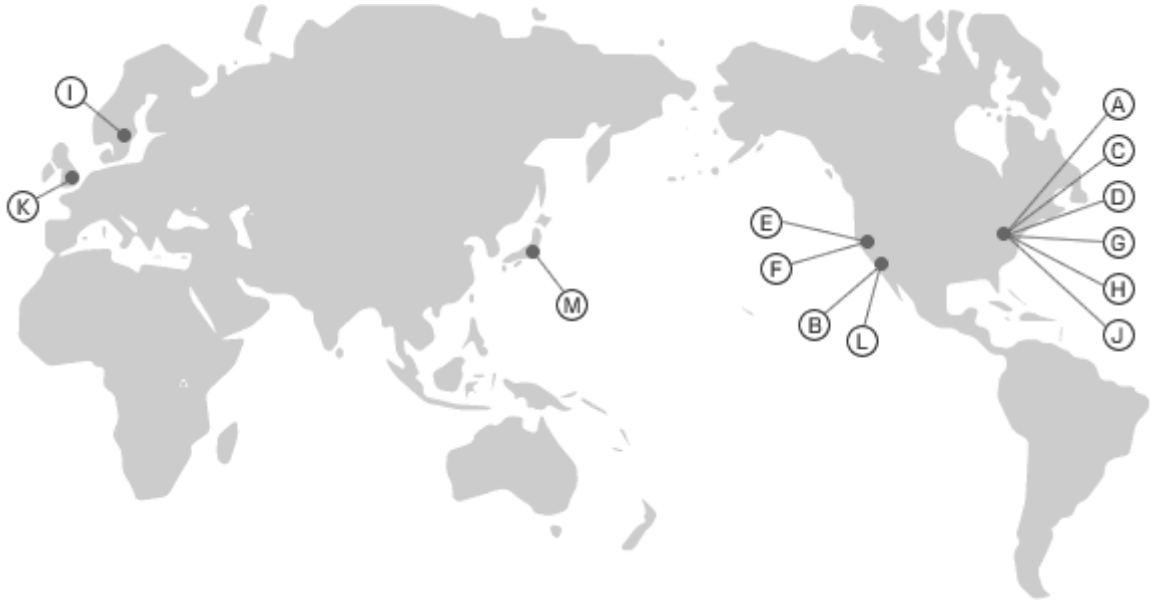
DNS を使って、あるドメイン名からそれに対応する IP アドレスを引き出すことを「名前解決」と呼びます。以下の図は、ユーザーが「www.example.co.jp」のウェブサイトにアクセスしようとした場合に、実際にどのようにして名前解決が行われるかを示しています。

名前解決の流れ



ネームサーバーはユーザーの目に触れることはありませんが、それが止まってしまうとドメイン名を利用しているインターネットのあらゆる機能が使えなくなってしまいます。このため、各ドメイン毎に配置されるネームサーバーは最低 2 台運用するという慣行になっていて、1 台が止まってももう 1 台がバックアップするという形になっています。上位の階層のドメインのネームサーバーほど止まった時の影響が大きく、**最上位のルートサーバーは全世界に 13 組配置**されています。

ルートサーバーの配置図

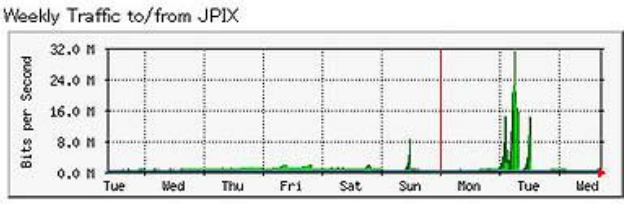


ルートサーバー一覧		
ルートサーバー	運用組織	所在地
A	VeriSign, Inc.	米国バージニア州
B	南カリフォルニア大学情報科学研究所(ISI)	米国カリフォルニア州
C	Cogent Communications	米国バージニア州
D	メリーランド大学	米国メリーランド州
E	米航空宇宙局(NASA)エイムズ研究所	米国カリフォルニア州
F	Internet Systems Consortium, Inc.(ISC)	米国カリフォルニア州
G	米国防総省ネットワークインフォメーションセンター	米国バージニア州
H	米陸軍研究所	米国メリーランド州
I	Autonomica	ストックホルム
J	VeriSign, Inc.	米国バージニア州
K	Reseaux IP Europeens -Network Coordination Centre(RIPE NCC)	ロンドン
L	Internet Corporation for Assigned Names and Numbers(ICANN)	米国カリフォルニア州
M	WIDE プロジェクト	東京

●DNS ルートサーバーへの攻撃

(1) 2002 年 10 月 21 日午後 5 時ごろ（米国東部時間)、世界 13 のルートサーバに一斉に DDoS（Distributed Denial of Service attack／分散型サービス拒否攻撃）攻撃が仕掛けられた

米国メディアの報道によると、10 月 21 日午後 5 時ごろ（米国東部時間)、世界 13 のルートサーバに一斉に DDoS 攻撃が仕掛けられた。
攻撃は米国当局が防御策を講じるまで約 1 時間にわたって続けられたという。急激なトラフィック増加を受け、米国内と東京、ストックホルムなどの 7 台に大きな影響が出たが、一般ユーザーのネット利用に問題は生じなかったという。13 台のルートサーバすべてに一斉攻撃が仕掛けられたまれなケースだと報じられている。攻撃者は分かっておらず、米国連邦捜査局(FBI）が捜査に乗り出した。



※東京に置かれたルートサーバ「M」のトラフィック。日本時間の 22 日早朝に増大している

(2) Anonymous が予告、3 月 31 日に DNS ルートサーバーへ DDoS 攻撃

ハッカー集団の「Anonymous」を名乗り、DNS ルートサーバーに対して 2012 年 3 月 31 日に DDoS 攻撃を行うとする声明が、インターネット上に公開された。

インターネットのドメイン名は、世界に 13 ある DNS ルートサーバーを基点としたツリー構造となっており、もしすべての DNS ルートサーバーがアクセス不能になれば、ドメイン名によるアクセスが利用できない状態となってしまう。
声明では、「Operation Global Blackout」と称し、米国議会に提出された著作権保護法案「SOPA」やウォール街への抗議などを理由として、3 月 31 日に DNS ルートサーバーに対して DDoS 攻撃を行うことを予告。DNS を利用不能な状態とし、インターネット全体をダウンさせるとしている。攻撃には、送信元 IP アドレスを偽装した DNS クエリを使ってターゲットを攻撃する「DNS Amplification」と呼ばれる手法を用いるツールを用意したという。

WWW へのアクセス権を持つ 7 人

MSN トピックスより引用

上の画にあるこのカード。**世界で 7 人だけが保持している、大災害時に World Wide Web を再起動(！)させる力を持つカード**なのです！

もしインターネットで大変動・大惨事が生じたら。例えば DNSSEC（Domain Name System Security）がダメージを受け、URL から目的のウェブサイトに誘導できなくなった時等。そういった緊急事態にこのカードを保持している人が出動するそうです。

7 人は、**イギリス、アメリカ、ブルキナファソ、トリニダード・トバゴ共和国、カナダ、中国、チェコ共和国の 7 カ国**から選出されており、再起動する際はアメリカにあるベースにこのカードを持って集合しなければなりません。

7 ってところがまたいいですね。

再起動のためには 7 人中 5 人が必要です。それぞれのカードには断片的な情報しかはいっておらず、5 人集まると起動が可能に！

マンガみたいだ。かっこいい！！

※存在は知っていましたが、私も見るのは初めてです！(゜∀゜)