

インターネットのしくみ

～インターネットを支える基本技術～

森下 泰宏 ((社)日本ネットワークインフォメーションセンター)

1998年12月16日

Internet Week 98 国立京都国際会館

(社)日本ネットワークインフォメーションセンター編

この著作物は、Internet Week98における森下泰宏氏の講演をもとに当センターが編集を行った文書です。この文書の著作権は、森下泰宏氏および当センターに帰属しており、当センターの書面による同意なく、この著作物を私的利用の範囲を超えて複製・使用することを禁止します。

©1998 Yasuhiro Morishita, Japan Network Information Center

目次

1	概要	1
2	目的	1
3	3つのキーワード	2
4	ドメイン名	3
5	IP アドレス	8
6	DNS	21

1 概要

この講義では、ドメイン名、IP アドレス、DNS に関する基礎技術について説明します。

これらは、インターネットの基本部分を支えている技術です。インターネットを動かすためのさまざまな「しくみ」のうち、最も基本的なものであるとも言えます。

2 目的

この講義では、次の方に対して説明を行います。

- 普段使っているインターネットのしくみを知りたい人、しくみについて興味がある人
- ネットワーク管理担当者
 - 新米の管理担当者（もしくは、管理担当者に「させられた」人）
 - なんとなくマニュアル通りに管理しているが、訳がわかっているわけではない人
- マウスでクリックしたときに何が行われているか、つまり、「マウスでクリック」の向こう側にあるものを知りたい人

この講義では、次の事柄については説明しません。

- どのプロバイダにつないだらよいか
- どのホスティングサービスを使えばよいか
- 「自分の会社 .co.jp」を使いたいが、どうすればよいか

「自分の会社 .co.jp」の登録のしかたなどについては、JPNIC の Web ページ (<http://www.nic.ad.jp/index-j.html>) などを参考にしてください。

3 3つのキーワード

ここで、「インターネットのしくみ」というこの講義における、3つのキーワードを挙げます。

- 「ドメイン名 (Domain Name)」
 - インターネット上における「住所」の管理方法
- 「IP アドレス (IP Address)」
 - インターネット上における意思の疎通 (データのやりとり) を行う際に必要な識別番号
- 「DNS (Domain Name System)」
 - 「ドメイン名」を管理するための手段
 - 「ドメイン名」と「IP アドレス」を結びつけるための手段

DNS は、ドメイン名と IP アドレスに比べると、あまり一般的ではないかもしれませんが。

ドメイン名、IP アドレス、DNS という、この3つはインターネットを支える大きなしくみです。これらが使えて当たり前であり、いずれが欠けてもインターネットが満足に使いえなくなってしまうほどに重要です。

また、注目したいのは、この3つのいずれもが、日本でのユーザが何千万人というように、インターネットが爆発的に普及する以前に、つまり、日本でのユーザが何百人程度だった頃に開発された技術だという点です。インターネットの規模が数万倍以上に拡張した現在も、これら3つの基本的なしくみは、設計を変えずに使われています。元の設計が良かった、実に良くできたしくみだったとすることができます。

インターネット全体で共通に利用される、ドメイン名、IP アドレス、プロトコル番号 (講義では触れません) などは、インターネットの「共通資源 (common resources)」と呼ばれています。日本で、これら共通資源の効率的な割り当て業務、円滑な管理運用という重要な業務を担っているのが、JPNIC です。

4 ドメイン名

4.1 ドメイン名の概要

4.1.1 ドメイン名とは

まず、一番馴染みがあると思われる「ドメイン名」から説明を始めましょう。

ドメイン名とは、ある組織やホストなどが属する「ドメイン(領域)」を表す文字列のことです。ドメイン名は、URL や電子メールアドレスとして利用されます。ドメイン名を一般社会における「住所」「屋号」であると考えると、わかりやすいかもしれません。

ドメイン名の例を挙げましょう。

- URL における使用例
 - `http://www.nic.ad.jp/index-j.html`
- 電子メールアドレスにおける使用例
 - `yasuhiro@nic.ad.jp`
 - `query@domain.nic.ad.jp` (サブドメインを伴った例)

4.1.2 ドメイン名の構成要素

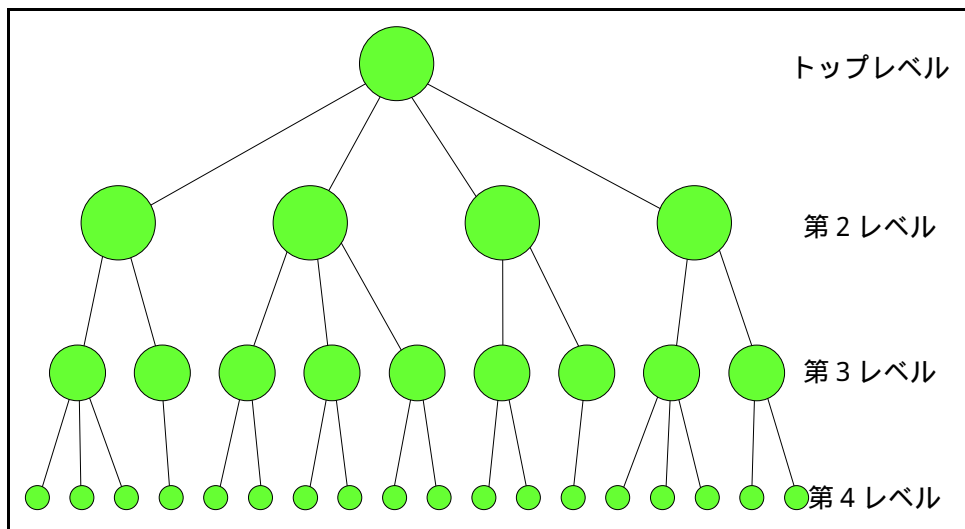
ドメイン名の構成要素は次のとおりです。

- ドメイン名は、アルファベット、数字、一部の記号(- など)、ピリオド(.)で構成される
- ピリオドは、各要素の区切り文字として用いられる
- 大文字と小文字は区別されない
- 今のところ、漢字などは使えない(漢字のような多バイト文字、ウムラウトやアクセント付きの文字が使えるようになる可能性はある)

4.1.3 ドメイン名における階層構造

ドメイン名は、階層構造を持っています。ドメイン名表記においては、より右に来る要素が「より広い」領域を表すことになります。たとえば、「NIC.AD.JP」では、NIC よりも AD が、AD よりも JP が広い領域を表しています。

階層構造を図に表すと、次のようになります。これを、「逆向き木構造(Inverse Tree Structure)」と呼びます。



図中では一番上、ドメイン名では一番右側の要素であるドメインを、「トップレベルドメイン (Top Level Domain: TLD)」と呼びます。以下、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。

4.1.4 TLD

ドメイン名に関して、最近ホットな話題となっているトップレベルドメイン (TLD) ですが、TLD には、次の 2 種類があります。

- 2 文字の TLD (ccTLD)
 - 国別コード (ISO3166 country code) に基づく 2 文字ドメイン
 - 基本的には国単位で利用される
 - 日本には「JP」が割り当てられている
 - JP 以外には、KR (韓国)、DE (ドイツ)、CA (カナダ) など
 - 管理ポリシーは、各国に委ねられている
- 3 文字の TLD
 - ドメイン名が利用されるようになった当初から使われていたもの
 - 主に米国を中心に使われてきた
 - 国に関係なくグローバルに使用されている gTLD (現在は COM、ORG、NET の 3 つ) と、米国で使われる TLD (EDU、GOV、MIL など) に分類される

特に 3 文字の TLD については、今後どのように管理されるかが流動的な状況です。

4.2 JP ドメイン

4.2.1 JP ドメインの現状

先に説明したように、日本を表す TLD は「JP」です。この JP は、ISO3166 により定義されたものです。

TLD が JP であるドメイン名については、基本的には、JPNIC が第 2 レベルまでを管理しています。

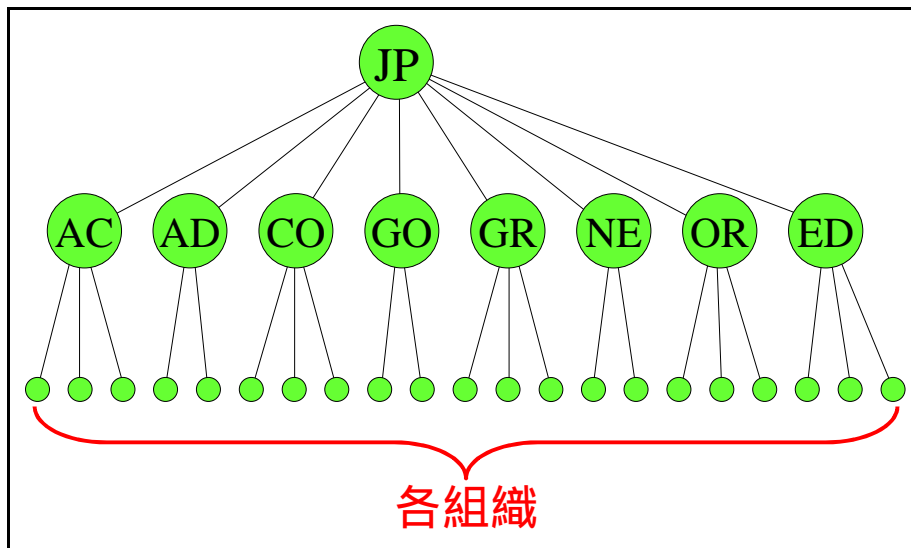
JP ドメインには、次の2種類の第2レベルドメインがあり、構造が異なります。

- 属性型ドメイン
会社法人が使える CO、ネットワークサービスが使える NE など、組織の属性によって第 2 レベルドメインが決まるドメインです。
- 地域型ドメイン
都道府県名、政令指定都市名を利用した、地域に根ざしたドメインです。

この 2 種類のドメインについて、引き続き説明します。

4.2.2 属性型ドメイン

属性型ドメインは、組織の属性により第 2 レベルドメインが決定されるドメインです。



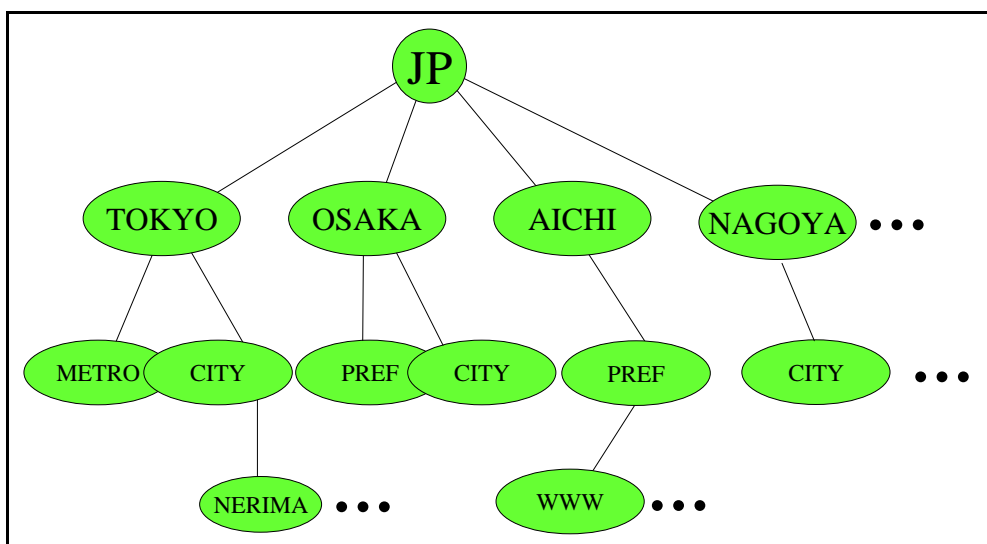
図に示すように、属性はアルファベット2文字で表され、次の8つがあります。

- AC
- AD
- CO
- GO
- GR

- NE
- OR
- ED (1999年より、追加予定)

4.2.3 地域型ドメイン

地域型ドメインは、第2レベルに都道府県名 (tokyo、osaka、aichi など) または政令指定都市名 (sapporo、yokohama など) を利用したドメインで、地域に根ざしたドメインと言えます。



たとえば、東京都であれば「METRO.TOKYO.JP」、大阪府であれば「PREF.OSAKA.JP」、大阪市であれば「CITY.OSAKA.JP」となります。

地域型ドメイン名は、都道府県庁、地方公共団体、個人などが利用することを念頭において設定されましたが、属性型ドメイン名を登録できる組織が地域型ドメイン名を登録してもかまいません。

4.3 サブドメイン

4.3.1 サブドメインとは

「サブドメイン」とは、あるドメイン階層から見た、すぐ下のドメイン階層のことです。

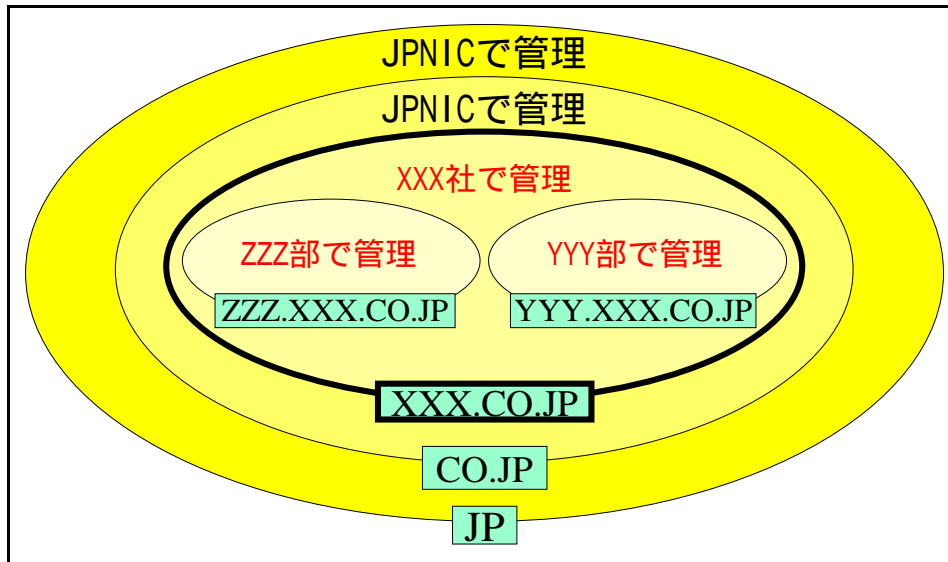
たとえば、「NIC.AD.JP」は「AD.JP」のサブドメインになります。属性型ドメインや地域型ドメインは、JP ドメインのサブドメインに相当します。

4.3.2 サブドメインと管理の委譲

自組織のドメインの下流 (1つ下、または1つ以上下) に、「任意に」サブドメインを設定することが可能です。サブドメインを設けると、1つの組織

の中で、ドメイン名をより細かく分割できることになり、分散管理が可能になります。

たとえば、次のように、管理部署ごとに分割管理する手法がとれるようになります。



ここで、「XXX.CO.JP」はXXX社が登録したドメイン名です。そして、ZZZという部が管理する「ZZZ.XXX.CO.JP」とYYY部が管理する「YYY.XXX.CO.JP」というサブドメインを設定したとします。たとえば、ZZZ部で管理する「ZZZ.XXX.CO.JP」は、上流には影響を与えません。この場合、XXX社では「ZZZ.XXX.CO.JP」についてはZZZ部に管理を委譲していることになります。

このように、サブドメインを設定すると、部署などの内部の都合に合わせて（悪くいえば勝手に）管理を行えます。

4.4 ドメイン名に関する FAQ

ドメイン名に関して、よく聞かれる質問（FAQ）に「ドメイン名について実体（実際のマシン）は必要か？」というものがあります。結論から言うと、ドメイン名に「実体」は必ずしも必要ではありません。たとえば、次のことが可能です。

- 1台のマシンに、仮想的に複数のドメイン名を割り当てることできる（マシンとドメイン名の対応は1対1でなくてもかまわない）
- 依頼を受けた場合に、自組織のマシンに、別組織のドメイン名を付与できる

この2番目の特徴を活かしたのが、インターネットにおける最近の流行語にもなっている「ホスティングサービス」や「バーチャルドメインサービス」です。

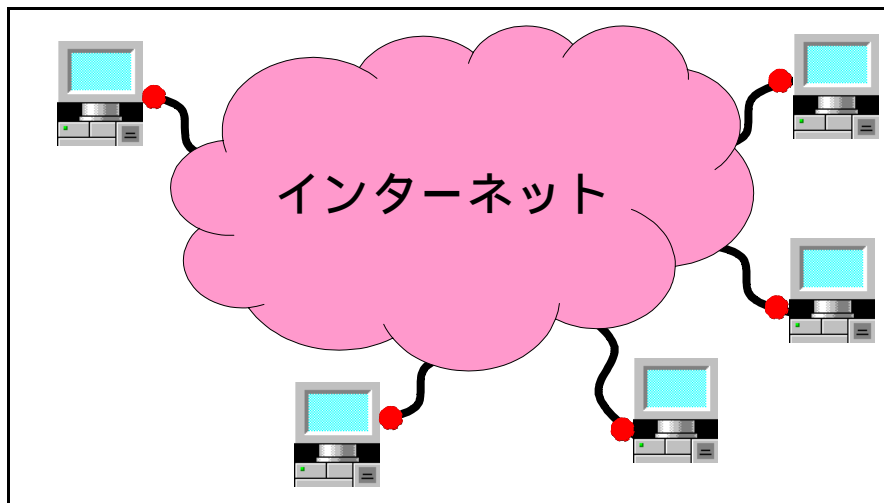
5 IP アドレス

5.1 IP アドレスの概要

5.1.1 IP アドレスとは

「IP アドレス」とは、インターネット上の機器を識別するための番号です。

インターネットに接続中のすべての機器には、IP アドレスが割り当てられています（次の図の の部分に IP アドレスが付けられています）。



IP アドレスは、電話における「電話番号」に相当します。電話をかけるとき、必ず電話番号をダイヤルするのと同様、インターネットを利用するには IP アドレスが必要不可欠です。逆に言えば、IP アドレスがあれば、Web アクセスなどが可能になります。

5.1.2 用語の説明

ここで、IP アドレスの説明に出てくる用語を紹介しておきましょう。

- プロトコル (Protocol)
プロトコルの英語本来の意味は、「条約案」、「議定書」などです。コンピュータ的に言えば、「コンピュータ同士を接続して、データやメッセージをやりとりする（通信する）ために必要な手順や約束事、決まり」が「プロトコル」になります。

プロトコルにより、物理的な接続方法、ネットワーク接続方法データの転送方法などが定められます。これらの決まりがなければ、通信は行えないのです。

- RFC (Request For Comments)
RFC とは、インターネットで利用されている各種プロトコルを記述した文書です。1998 年 12 月現在、2500 近くの文書があります。

RFC を策定しているのは、IETF (The Internet Engineering Task Force) という組織です (<http://www.ietf.org/>)。

インターネット接続して通信を行う場合は、RFC に準拠する必要がありますが、RFC は「絶対的なもの」ではありません。もし、RFC に不備があれば、IETF に対してコメントを送ることができます。皆でどんどん良いものにしていくというのが、RFC の方針です。

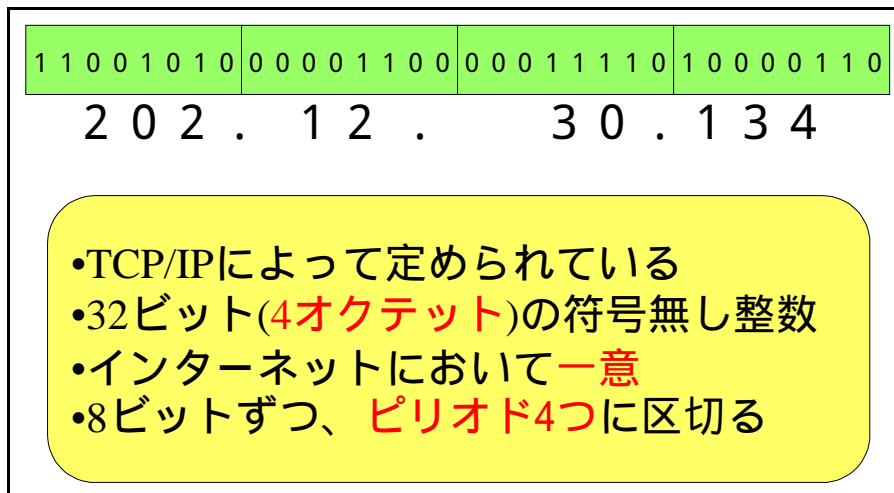
- TCP/IP (Transmission Control Protocol / Internet Protocol)
「インターネット上でデータをどのように送受信するか」を定めたプロトコルが TCP/IP です。TCP/IP の特徴は次のとおりです。
 - IP アドレスを使う
通信元、通信先を判断するのに「IP アドレス」を用います。
通信元、通信先双方の機器に IP アドレスが割り当てられている必要があります。
 - 常時接続が必要でない
使いたいときだけ IP アドレスが割り当てられれば十分です。このため、ダイヤルアップ IP、DHCP などの手法による効率的な利用が可能です。
 - 媒体に依存しない
データの到達性さえあれば、接続するためのメディアを選びません。
このため、電話線、無線、UTP ケーブル、光ファイバなど、さまざまな媒体を利用することができます。

TCP/IP は、故 Jon Postel 編の RFC791 により、1980 年代の初めに定められたものです。「どの機器が繋がってもよい、必要なときだけ繋がればよい、どのように繋いでもよい」という、良い意味でのいい加減さによって、TCP/IP は現在まで生き残ったと言えるかもしれません。

5.2 IP アドレスのより詳しい説明

5.2.1 IP アドレスの仕様

IP アドレスの仕様を次に示します。



図に示したように、IP アドレスは「1」、「0」が 32 個並んだものです。コンピュータ内部では、データが 2 進数で表されるので、「1」、「0」の並びになりますが、人間には分かりづらいので、8 ビットずつ区切って、10 進数で表記するのが一般的です。

5.2.2 IP アドレスの体系

IP アドレスには、次の 2 つの体系があります。

- 従来からの体系
 - クラスによる体系
 - クラス A、クラス B、クラス C
- クラスレス (classless) な IP アドレス体系
 - CIDR (サイダー) による体系

従来からのクラスによる IP アドレス体系で、数年前まで IP アドレスの割り当てが行われていました (今でも使われています)。ここ数年は、クラスレスな IP アドレス体系での割り当てが行われており、CIDR が一般的になっています。

5.2.3 IP アドレスにおけるクラス

クラスレスな CIDR が一般的になったとは言え、クラスによる体系からクラスレスな体系へと変化した理由を理解するためにも、IP アドレスにおける「クラス」について、ここで説明しておきましょう。

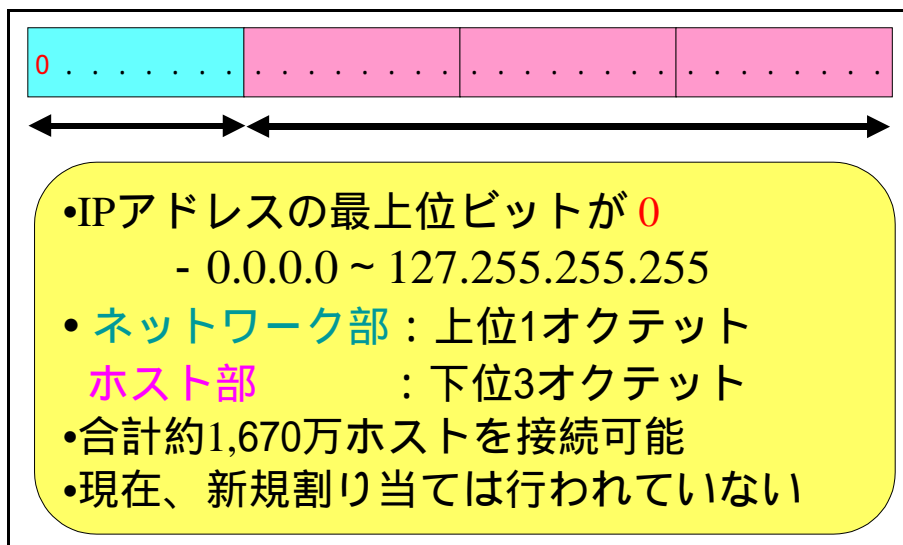
クラスによるアドレス体系では、IP アドレスを上の方の「ネットワーク部」と下のほうの「ホスト部」に分割します。そして、ネットワーク部が同じアドレスを、一つのネットワーク単位として取り扱います。電話番号で言えば、市外（市内）局番がネットワーク部であり、個々の番号（電話番号の最後の 4 桁）がホスト部に相当します。

クラスによるアドレス体系では、利用する組織のネットワークの規模に応じて、IP アドレスを次の 3 つに分類していました。

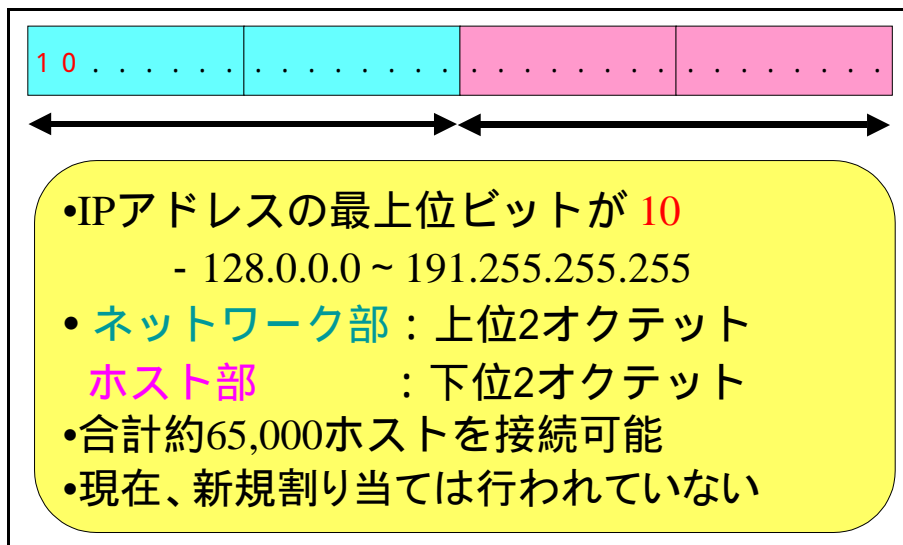
- 大規模（クラス A）
- 中規模（クラス B）
- 小規模（クラス C）

クラス A ~ C の、ネットワーク部とホスト部の分割の様子を次に示します。

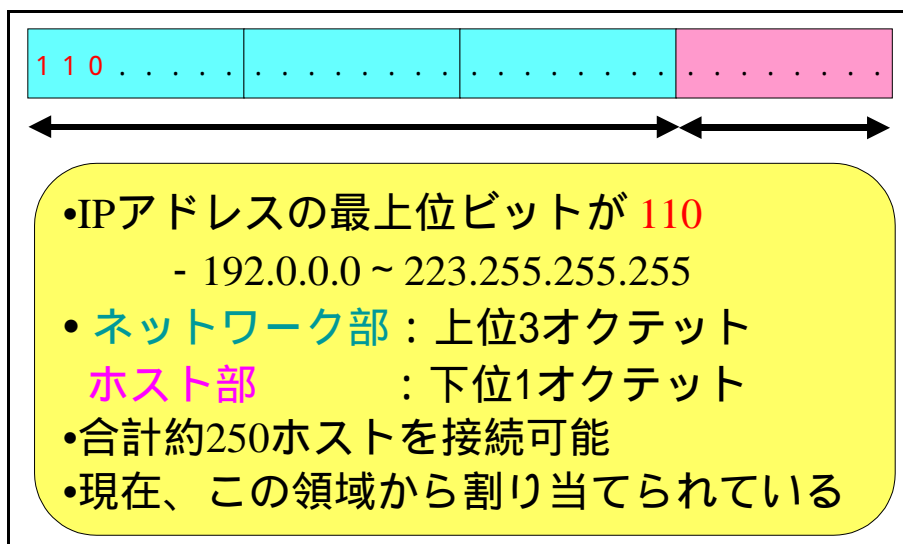
クラス A



クラスB



クラスC



ネットワークの規模に応じて、ネットワーク部の長さが変わるというのは、東京や大阪の電話番号では局番が短く、地方にいくと局番が長くなるということに相当しているとも言えるでしょう。

なお、図にも示しましたが、インターネットの黎明期にはIPアドレスの割り当てに、クラスA、Bを使いましたが、それ以降、数年前まではクラスCからの割り当てが行われてきました。

また、特殊な用途のためのクラスとして、クラス D、クラス E があります。これらのアドレスは、組織には割り当てられません。

- クラス D
 - IP アドレスの上位 4 ビットが “ 1110 ”
 - IP マルチキャスト（映像の送信など）で利用
- クラス E
 - ICANN（IANA）により予約（現在利用されていない）

5.2.4 CIDR への移行

クラス A ~ C による IP アドレス割り当てには、問題がありました。それぞれのクラスにおける最大接続可能ホスト数にあまりにも差があるという点です。

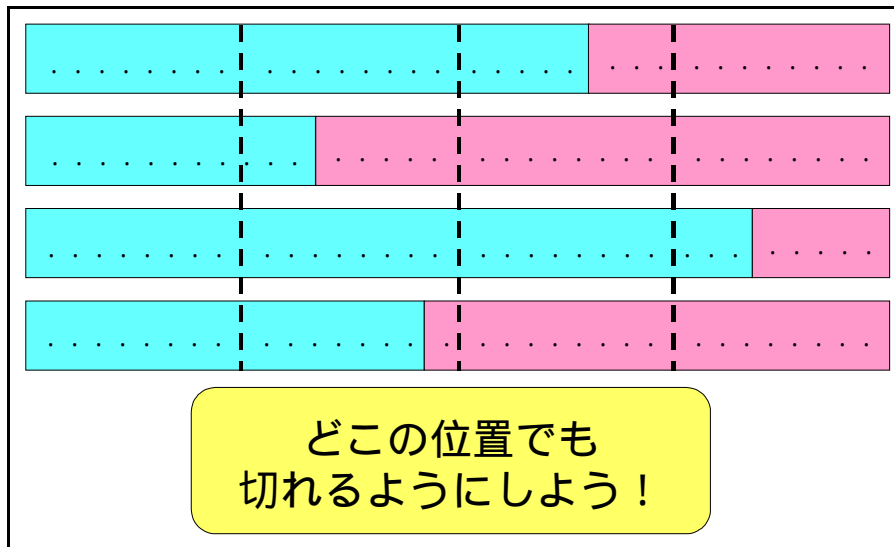
- クラス A : 16,777,216 (2^{24})
- クラス B : 65,536 (2^{16})
- クラス C : 256 (2^8)

ホスト数に差があるのも問題ですが、なにより、クラスによるアドレス体系はアドレスの効率が良くありません。クラス A を十分に使い切れるような組織は世界にほとんどありません。にもかかわらず、IP アドレスの半分はクラス A なのです。また、最低単位がクラス C になりますが、これでも 256 の IP アドレスが割り当てられることになります。1 台 ~ 数台しか接続しない小さな組織でも、1 つのクラス C を割り当てるしかないというのは、やはり効率が良くないのです。

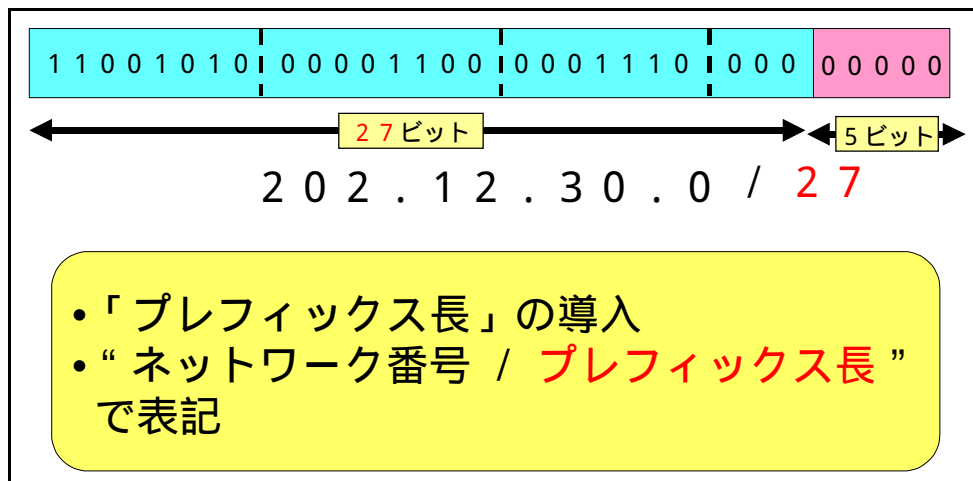
このように、クラスによる IP アドレス体系には問題があったので、数年前からは、クラスレスな IP アドレス体系の使用が一般的になっています。クラス単位での IP アドレス割り当てをやめ、任意のブロック単位で IP アドレスを割り当てるようになったのです。

クラスレスな IP アドレス体系では、「CIDR（Classless Inter-Domain Routing）」に基づいて IP アドレス割り当てを行います。ここで、Routing というのは「経路制御」の意味であり、データをどのルートで通せばよいかということに CIDR が係わっていることを示します。

CIDR の思想を表すと、次の図のようになります。



CIDR では、「プレフィックス長」が導入されています。「ネットワーク番号 / プレフィックス長」でアドレスを表すのが、CIDR の大きな特徴です。



CIDR の導入により、次の事柄が可能になりました。

連続したクラスCを1つのCIDRブロックとして取り扱うことが可能

11001010	00001100	000111	0100000000
----------	----------	--------	------------

CIDR表記：202.12.30.0 / 23
→ 202.12.30.0 - 202.12.31.255

クラスCよりも小さなアドレスブロックも、他のブロックと同様に扱うことが可能

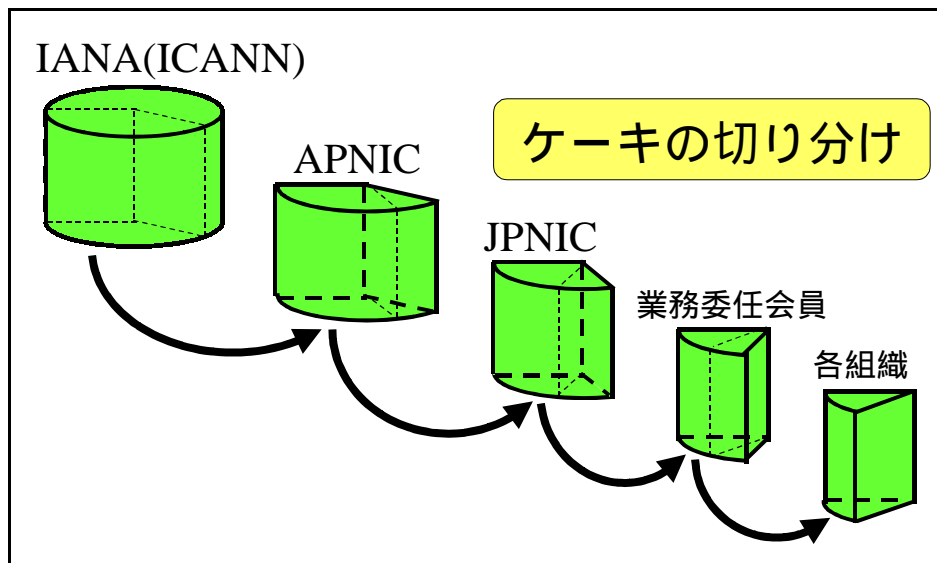
11001010	00001100	0001110	000	00000
----------	----------	---------	-----	-------

CIDR表記：202.12.30.0 / 27
→ 202.12.30.0 - 202.12.30.31

CIDR の別の利点としては、次のことが挙げられます。

- IP アドレスの割り当て効率の向上
限りある IP アドレスの有効活用が可能となります。
 - IP アドレスの管理体系の構造化が可能
階層的にアドレスブロックを管理できるようになります。この構造化された管理体系は、現在の IP アドレスの管理体系に合致しています。
- 2 番目に挙げた、構造化された管理体系について、さらに説明しましょう。

5.2.5 CIDR による構造化された管理体系



現在、IP アドレスは、次のような管理構造で割り当てを行っています。このことから、アドレスをブロック (CIDR ブロック) 毎にまとめて管理できる、CIDR が適していると言えます。

1. ICANN が APNIC にアドレスブロックを割り当て、
2. APNIC が JPNIC にアドレスブロックを割り当て、
3. JPNIC はそのブロックから業務委任会員のプロバイダ (ISP) にアドレスブロックを割り当て、
4. 業務委任会員のプロバイダが各ユーザの規模に応じてアドレスブロックを割り当てる

また、CIDR を使用することによって、経路制御も楽になります。管理されているブロックごとに経路を制御すればよくなるからです。

これを、交通標識で考えてみましょう。たとえば、東京から大阪のある場所へ向かうとします。経路がブロックで管理されていれば、まず、最初は「大阪方面」の交通標識に沿って進む、大阪に入れば、大阪の「何区」という交通標識に沿って進む...というように、徐々に小さなブロックの経路情報を参照するようになれるのです。もし、ブロックごとに管理されていなければ、東京から「大阪市何区どこ」という交通標識が必要になってしまいます。

CIDR を使えば、経路表を 2 のべき乗単位でまとめることができるので、経路情報テーブルが小さくなります。

5.3 IP アドレスの有効活用

ここで、有限の資源である IP アドレスを、いかに有効活用するかについて考えてみましょう。

IP アドレスで表せる大きさは、 2^{32} (4,294,967,296) つまり 43 億弱です。これは、世界人口(約 60 億)や、携帯電話の桁数で表せる電話番号(10^{10} =100 億)よりも少ない数なのです。このため、「IP アドレスが 21 世紀前半には枯渇する」と言われています。

そこで、新しい IP プロトコルである「IPv6」が現在開発されています(現在の IP プロトコルはバージョン 4 です)。

5.3.1 新しい IP プロトコル (IPv6)

IPv6 は、RFC2460 (1998 年 12 月発行) で定義され、Standards Track (標準化の草稿) の段階にあります。まだ、コメントを受けつけている状態です。

IPv6 では、アドレス空間が 128 ビットに拡張されます。

大変期待されている IPv6 ですが、IP アドレスの場合、電話のように「端末の仕様変更をせずに桁を増やす」ことが非常に難しく、どうしても、端末の仕様変更が必要になります。つまり、IPv6 をすぐに使えるようになるわけではありません

IPv6 が完成し普及するまで、現在の IP (IPv4) を「もたせる(アドレスの枯渇を防止する)」必要があると言えます。そのための手法として、次の技術が現在使われています。

- プライベートアドレス
- アドレス変換 (NAT、IP マスカレード)

これらについて、引き続き説明します。

5.3.2 プライベートアドレス

「プライベートアドレス」とは、組織内で自由に使ってよい IP アドレスです。いろいろな用途がありますが、アドレスの枯渇を防止するために有効な手段となっています。

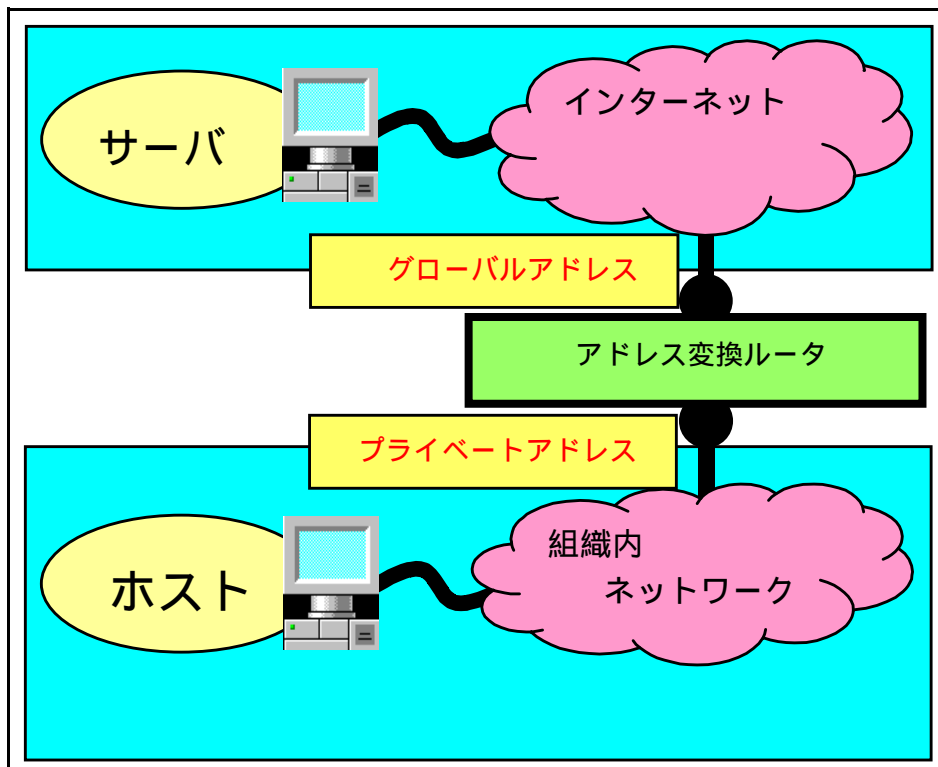
プライベートアドレスについては、RFC1918 の定義により、「インターネット上で使われていない（インターネットには直接繋がっていない）」ことが保証されています。

プライベートアドレスには、次のものがあります。

- 10.0.0.0 ~ 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 ~ 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 ~ 192.168.255.255 (192.168.0.0/16)

5.3.3 アドレス変換

アドレス変換では、プライベートアドレスとグローバルアドレス（広く使われているアドレス）間の相互変換が行われます。このアドレス変換機能は、アドレスの枯渇防止に役立っています。



アドレス変換によって、プライベートアドレスが付けられた組織内のマシンからも、インターネットを利用できるようになります。最近のルータには、標準でアドレス変換機能が装備されています。

アドレス変換には、次の2種類があります。

- NAT (Network Address Translation)
IP アドレスだけを変換します。
- IP マスカレード
IP アドレスだけではなく、ポート番号も変換します。複数のプライベートアドレスを持つマシンが、1つのグローバルアドレスで同時にインターネットを利用できるようになるので、IP アドレスを節約できます。

なお、アドレス変換の考え方は、IPv4 と IPv6 との変換にも応用できます。たとえば、組織内のネットワークを先に IPv6 にしても、アドレス変換によって、インターネット上を IPv4 で通信することができます。また、将来、インターネット上で IPv6 が普及した後、組織内のネットワークが IPv4 のままであっても、アドレス変換によって、やはり通信が可能となります。

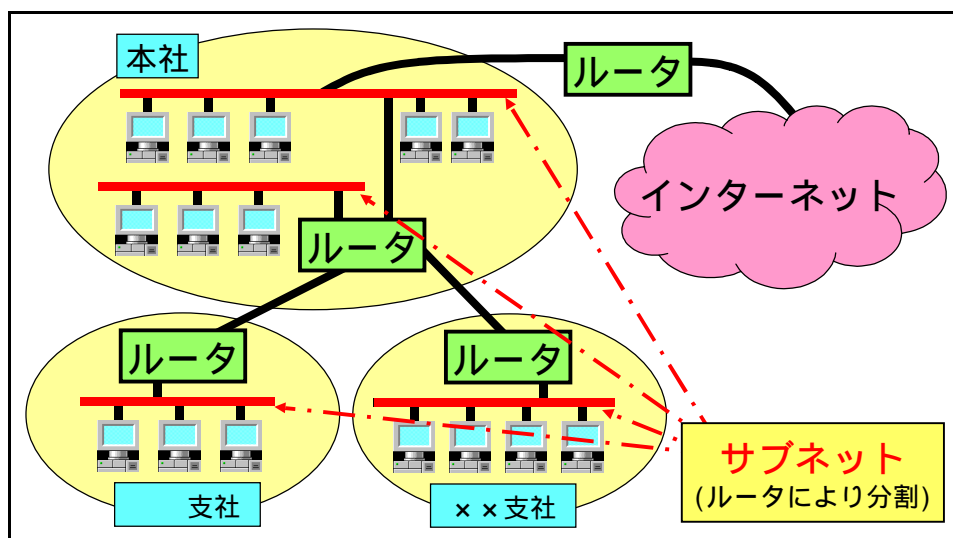
5.4 IP アドレスに関するその他の技術

5.4.1 サブネット

「サブネット」とは、1つのネットワークを、複数のネットワークに再分割して使用する技術です。サブドメインの考え方に似ています。

サブネットの技術によって、1つの組織内においてネットワークをより細かく分割できるようになります。つまり、管理部署毎に、ネットワークを分割したりできるようになるのです。言い換えれば「組織内においても、CIDR による効率のよい管理を行おう」ということになります。

サブネットの例を示します。



5.4.2 特別な IP アドレス

特別な機能を持つ IP アドレスについて、ここでまとめておきます。

- 自分自身を表すアドレス
 - 127.0.0.1 (127.0.0.1/32)
 - ループバックアドレス
 - ソフトウェアのテスト等の際に有効
- ネットワークを表すアドレス
 - IP アドレスのホスト部のビットがすべて 0
 - マシンには割り当てない
 - ネットワークそのものを表し、経路制御の際などに利用される
 - ネットワークを複数のサブネットに分割した場合には、それぞれのサブネットについてそれぞれ 1 つずつ割り当てられる
- ブロードキャストアドレス
 - IP アドレスのホスト部のビットがすべて 1
 - その (サブ) ネットワークに接続されているすべてのマシンを表す
 - ネットワークを表すアドレスと同様、それぞれのサブネットについてそれぞれ 1 つずつ割り当てられる
 - 同報通信 (ブロードキャスト) に使用される

5.4.3 アドレス割り当ての実際

ここで、インターネット接続を行う際に、実際に行われているアドレス割り当ての様子を簡単に説明しておきます。

- 動的な割り当て (自動)
 - ダイアルアップ接続した際にプロバイダから割り当て (PPP プロトコルを使用)
 - LAN に接続した際にサーバから割り当て (DHCP プロトコルを使用)
- 静的な割り当て (手動)
 - 常時接続する際にプロバイダから割り当て
 - LAN にサーバを接続する際に割り当て
(たとえば、DHCP サーバを接続する場合は、手動での割り当てが必要)

6 DNS

6.1 DNS とは

DNS とは、「Domain Name System」の略称であり、ドメイン名と IP アドレスを結びつけるためのしくみです。

インターネットでは、通信は IP アドレスでしか行えませんので、ドメイン名を使うためには、ドメイン名と IP アドレスを結びつける必要があります。このための 1 つの手法が DNS です。また、DNS を利用すると、ドメイン名を階層的に管理することもできます。

DNS が使われるようになった背景を説明しましょう。1980 年代までは、「HOSTS.TXT」というファイルに、インターネットに接続されるホストの名前と IP アドレスを記述するという形で、その対応を管理していました。インターネットに接続した組織は、HOSTS.TXT を定期的に FTP 等で入手していたのです。

しかし、インターネットの普及に応じて、接続ホストが増加しました。HOSTS.TXT という一種のデータベースが巨大化して、変更履歴の即時反映が困難になってしまったのです。そこで、自動更新が可能な、分散型データベースへの移行の必要性が高まりました。そして、DNS (RFC882, RFC883) が誕生したのです。なお、現在では RFC1034 と RFC1035 に更新されています。

DNS には、次のような特徴があります。

- 複数のホストにより管理
- 自動的に更新される分散型データベース
- 階層構造（木構造）を持つ
- 立体的な広がりを持つという意味で「名前空間」と呼ばれる

分散型データベースで、自動更新が可能という使いやすさが、インターネット普及の一因ともなりました。

6.2 DNS のしくみ

6.2.1 ネームサーバとリゾルバ

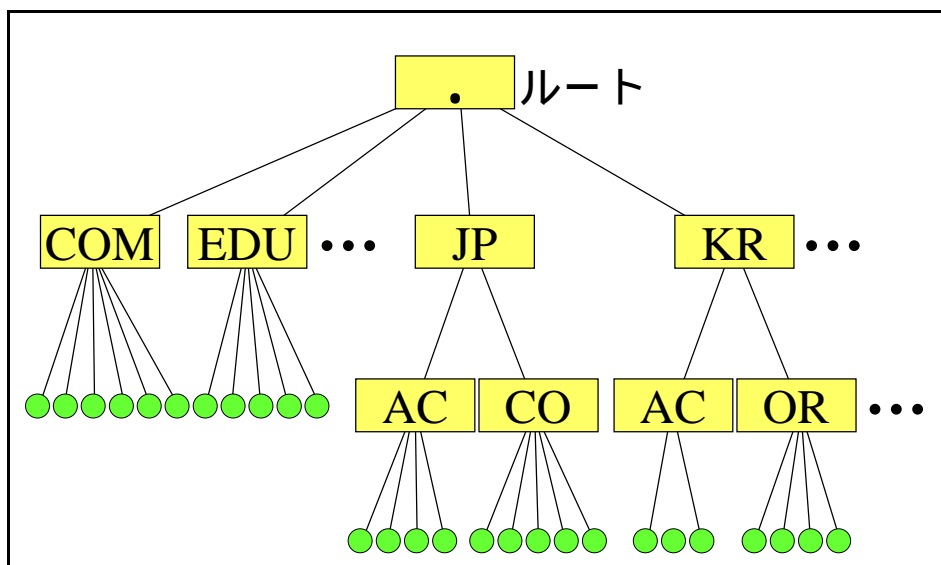
DNS は、「ネームサーバ」と「リゾルバ」の組み合わせで機能します。

- ネームサーバ : DNS のサーバ機能
リゾルバからの要求により名前空間の検索を行い、結果をリゾルバに渡します。
- リゾルバ : DNS のクライアント機能
WWW ブラウザ等のアプリケーションから呼び出され、ネームサーバに名前解決を要求するためのプログラムです。

アプリケーションが直接ネームサーバに問い合わせるのではなく、リゾルバというワンクッションを置いていることが DNS のメリットの 1 つです。たとえば、IPv4 から IPv6 への移行の際に、各アプリケーションを修正する必要はありません。間に入っているリゾルバだけを IPv6 対応に修正すれば済むのです。

6.2.2 DNS の木構造

DNS は、次のような木構造を持っています。



DNS の最上位に存在するのが、ルート (.) ゾーンです。このルートゾーンの存在が、ドメイン名とは異なる点です。

ルートゾーンはルートサーバによって管理されます。そして、各ゾーンのネームサーバは、一つ上位のサーバから指し示されます。この管理体系は、ドメイン名の木構造にうまく適合しています。

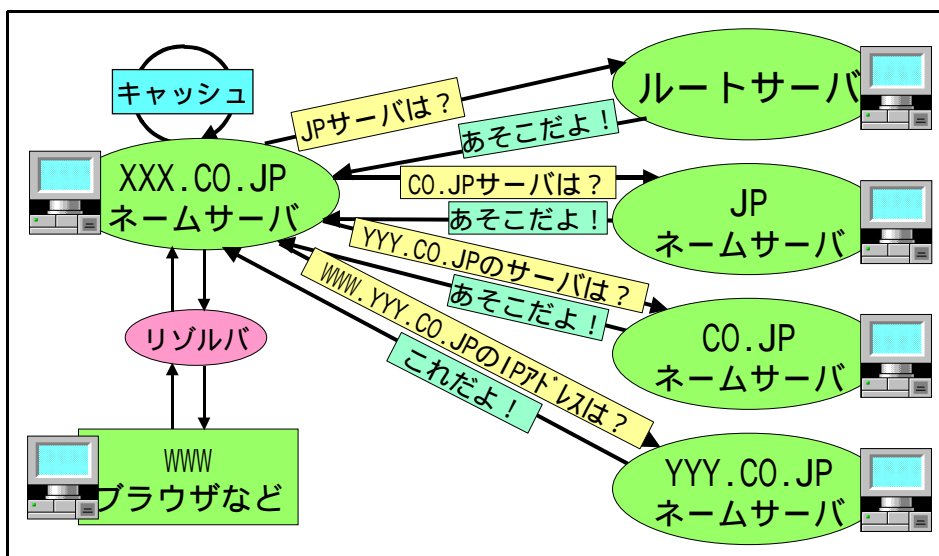
6.2.3 ルートサーバ

ルートゾーンを管理しているネームサーバが「ルートサーバ」です。

ルートサーバは、世界に13個あります(a.root-servers.net ~ m.root-servers.net)。日本にも、ルートサーバ m.root-servers.net があり、東京大手町の KDD にある NSPIX2 に接続されています。日本のルートサーバは WIDE Project で管理・運用されています。

6.2.4 名前解決

DNS の木構造とルートサーバについて理解したところで、次に、ドメイン名から IP アドレスを得る「名前解決」の流れについて説明しましょう。



「XXX.CO.JP」の組織のマシンから、「WWW.YYY.CO.JP」の IP アドレスを調べるとします。

1. 自組織のネームサーバが「知っている」名前かどうかを確認します。前に調べたことのあるドメイン名なら、キャッシュされていることがあるからです。
2. 知らない名前であることが判明したら、ネームサーバはルートサーバに対して、1 つ下位の、「JP」を管理しているネームサーバの場所 (IP アドレス) を問い合わせます。
3. 返された IP アドレスを使って、JP ネームサーバに対して、「CO.JP」を管理しているネームサーバの IP アドレスを問い合わせます。
4. 返された IP アドレスを使って、CO.JP ネームサーバに対して、「YYY.CO.JP」を管理しているネームサーバの IP アドレスを問い合わせます。
5. 返された IP アドレスを使って YYY.CO.JP ネームサーバに対して、「WWW.YYY.CO.JP」の IP アドレスを問い合わせます。

DNS では、自分が解決できない名前の場合、必ずルートサーバに問い合わせを行います（ネームサーバに、ルートサーバの IP アドレスが仕込まれているので、これが可能なのです）。

このため、DNS が機能するためには、最低 1 台のルートサーバへの到達性が保証されていなければなりません。m.root-servers.net が日本にない頃は、海外リンクがダウンするとルートサーバへの到達性が失われてしまいましたが、前述の m.root-servers.net の運用開始により、この問題は解決されました。

6.3 ドメイン名 / IP アドレスと DNS

6.3.1 ゾーンとドメイン名

それぞれのドメインの階層毎に、ゾーン（名前空間）を設定します。これにより、ドメイン名との対応付けを行うことができます。

たとえば、「NIC.AD.JP」ゾーンの管理は、NIC.AD.JP ドメインのネームサーバにより行われます。逆に、「NIC.AD.JP ドメインのネームサーバで管理される領域を、NIC.AD.JP ゾーンと呼ぶ」という定義も可能です。

つまり、DNS によって、ドメインとゾーンが 1 対 1 に対応することになるのです。

6.3.2 ネームサーバの重要性

以上の説明からも分かるように、「ドメイン名 / IP アドレスと DNS」のしくみにおいては、ネームサーバが重要な役割を担っています。

もし、該当する組織（ゾーン）のネームサーバにアクセスできなかつたら、たとえその組織の WWW サーバなどが動作していても、WWW ブラウザからアクセスできないことになってしまいます。このような状況を防ぐため、通常、1 つのゾーンについて複数のネームサーバを設定します。

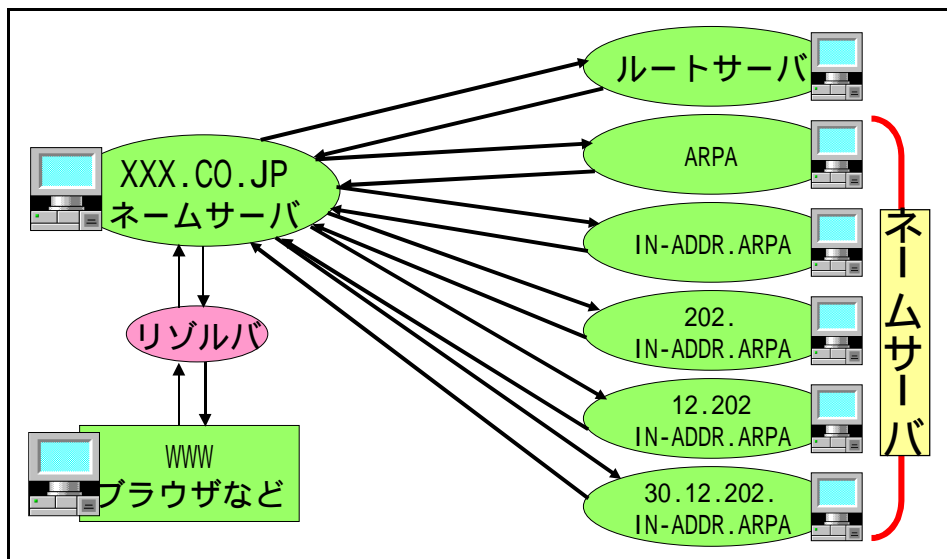
複数のネームサーバを設定し、稼動する場合は、データの一意性を保つ必要があります。このため、次の 2 種類のネームサーバを設定することが推奨されています。

- プライマリサーバ
 - 元データを管理するサーバ
 - プライマリサーバは、1 つのゾーンに対して 1 台
- セカンダリサーバ
 - プライマリサーバのデータを定期的に複製する
 - セカンダリサーバは、1 つのゾーンに対して複数設定可能

6.3.3 正引きと逆引き

今まで説明した、ドメイン名から IP アドレスを得ることを「正引き」と言います。たとえば、「WWW.NIC.AD.JP 202.12.30.134」を得るのは正引きです。正引きは、主にサービスを利用する場合に使用されます。

一方、「逆引き (Inverse Query)」もあります。IP アドレスからドメイン名を得るのが、逆引きです。「202.12.30.33 NS1.NIC.AD.JP」を得るのが逆引きです。逆引きは、主にサービスを提供する側で、統計情報などを作成する際に使用されます。



逆引きには、「in-addr.arpa」特殊なドメイン名を使用します。たとえば、「202.12.30.134」という IP アドレスを逆引きするには、「134.30.12.202.in-addr.arpa」というドメイン名に対して問い合わせを行います。逆引きの場合は、必ずルートサーバが参照される点に注意してください。

6.4 より効果的な DNS の利用

6.4.1 別名 (CNAME) の指定

DNS では、特定のホスト名に対して「別名 (CNAME : Canonical Name)」を指定することも可能です。別名を適切に利用することにより、ユーザにとって分かりやすいだけでなく、サーバホストの切り替えや更新の際の移行がスムーズに行えます。

別名は「CNAME」レコードにより指定されます。変換は、「名前 正式名 そのホストの IP アドレス」の順に行われます。たとえば、「ftp.nic.ad.jp mw134.nic.ad.jp 202.12.30.134」というような変換が行われます。

6.4.2 メールホスト (MX) の指定

特定のドメイン名のメールを取り扱うためのホスト(メールホスト)を指定することができます。これにより、あるドメインのメールを特定のホストに集めることが可能になります。

メールホストは「MX (Mail Exchanger)」レコードにより指定します。

メールホストを複数指定することにより、より安定したサービスを実現することが可能になります。

6.4.3 BIND

DNS はあくまでも「しくみ」なので、RFC に基づいたものでさえあれば、何を使ってもかまいません。

BIND (Berkeley Internet Name Domain) は、最も広く利用されている DNS の実装の 1 つです。BIND は、各種 UNIX、および Windows NT で動作します。BIND は無償で利用可能であり、ソースコードも公開されています。

現在の最新版は 8.1.2 です。古いバージョンのものはセキュリティ上問題があるので、使用しないでください。BIND の最新情報については、URL: [ftp://ftp.isc.org/isc/bind/](http://ftp.isc.org/isc/bind/) を確認してください。ただし、入手する場合は、ミラーサイトを利用するようにしてください。