ソフトウェアアーキテクチャ
第9回　名前解決

環境情報学部
萩野　達也

lecture URL

https://vu5.sfc.keio.ac.jp/slide/

OSI参照モデル

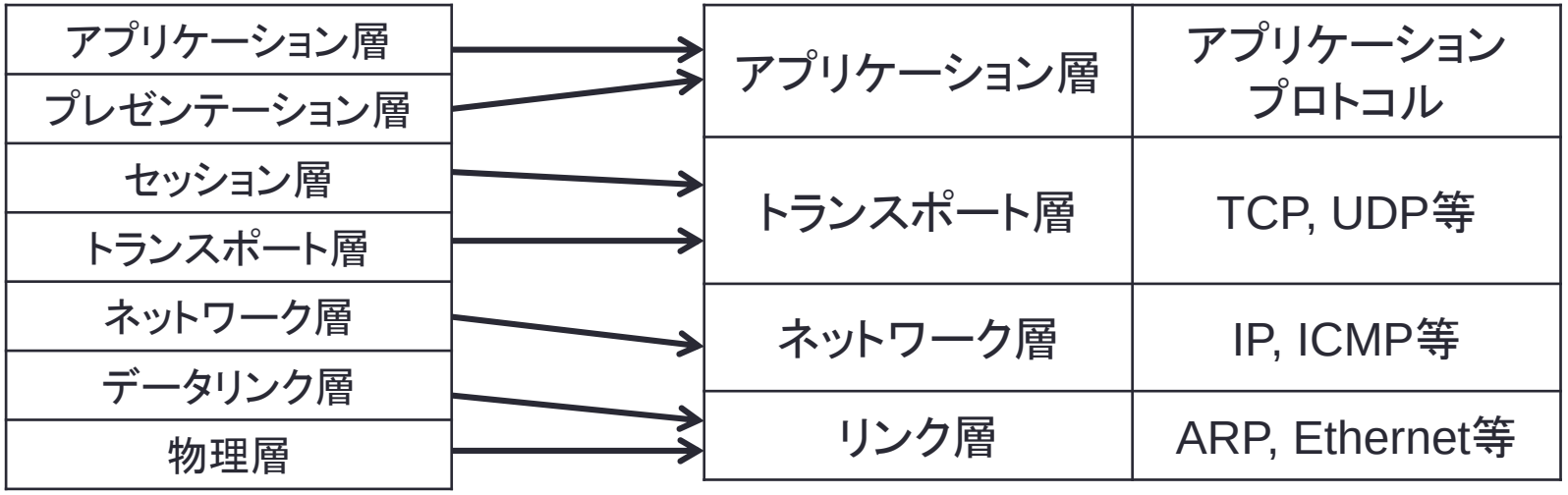
- Open Systems Interconnect
  - ISOが1984年ごろに作成

アプリケーション層	ユーザが操作するインターフェイス
プレゼンテーション層	データの表現形式
セッション層	通信プログラム間の通信の開始から終了までの手順
トランスポート層	ネットワークにおける通信監理
ネットワーク層	ネットワークにおける通信経路の選択
データリンク層	通信機器間の直接的な信号の受け渡し
物理層	電気・光信号への変換

TCP/IPプロトコル

- TCP/IPプロトコル
  - TCP = Transmission Control Protocol
  - IP = Internet Protocol
  - OSIのように専門家の委員会で作られたものではない
  - 実験目的で出てきた
  - 1982年ごろには確定

- 7層ではなく4層



TCP/IPの下位レイヤーが提供するもの

- 通信路の確保
  - IPによるEnd-to-endでデータ通信
  - ARP (Address Resolution Protocol)
  - 経路制御プロトコル
- 多重化
  - ひとつの通信路を複数の目的に多重化して使う
  - ソケット：IPアドレス＋ポート番号（16ビット）
- 信頼性のある通信
  - TCPの場合
    - データを確実に届ける
    - 重複させない
    - データの順番を守る

TCP Transmission Control Protocol	UDP User Datagram Protocol
• データを確実に届ける • セッションを作る • ストリームとしてデータを送信する	• データが確実に届くとは限らない • セッションを作らない • 軽いプロトコルで利用 • RPC at-least-once

アプリケーションプロトコルの例

- 名前解決
  - DNS
- 遠隔利用
  - telnet
  - rlogin
  - ssh
- ファイル共有
  - NFS
  - AFS
- 電子メール
  - SMTP
  - POP
  - IMAP
- ファイル転送
  - ftp
  - rcp
  - scp
- Web
  - HTTP
  - WebDAV
- ウインドウシステム
  - Xプロトコル
- IP電話
  - SIP

ネットワーク上の名前解決

ホスト名

- ホスト(コンピュータ)には名前とアドレスが付けられている.
  - 複数の名前やアドレスを持つものもある.

- ホスト名
  - ホストの名前
  - 組織内で自由につけることができる

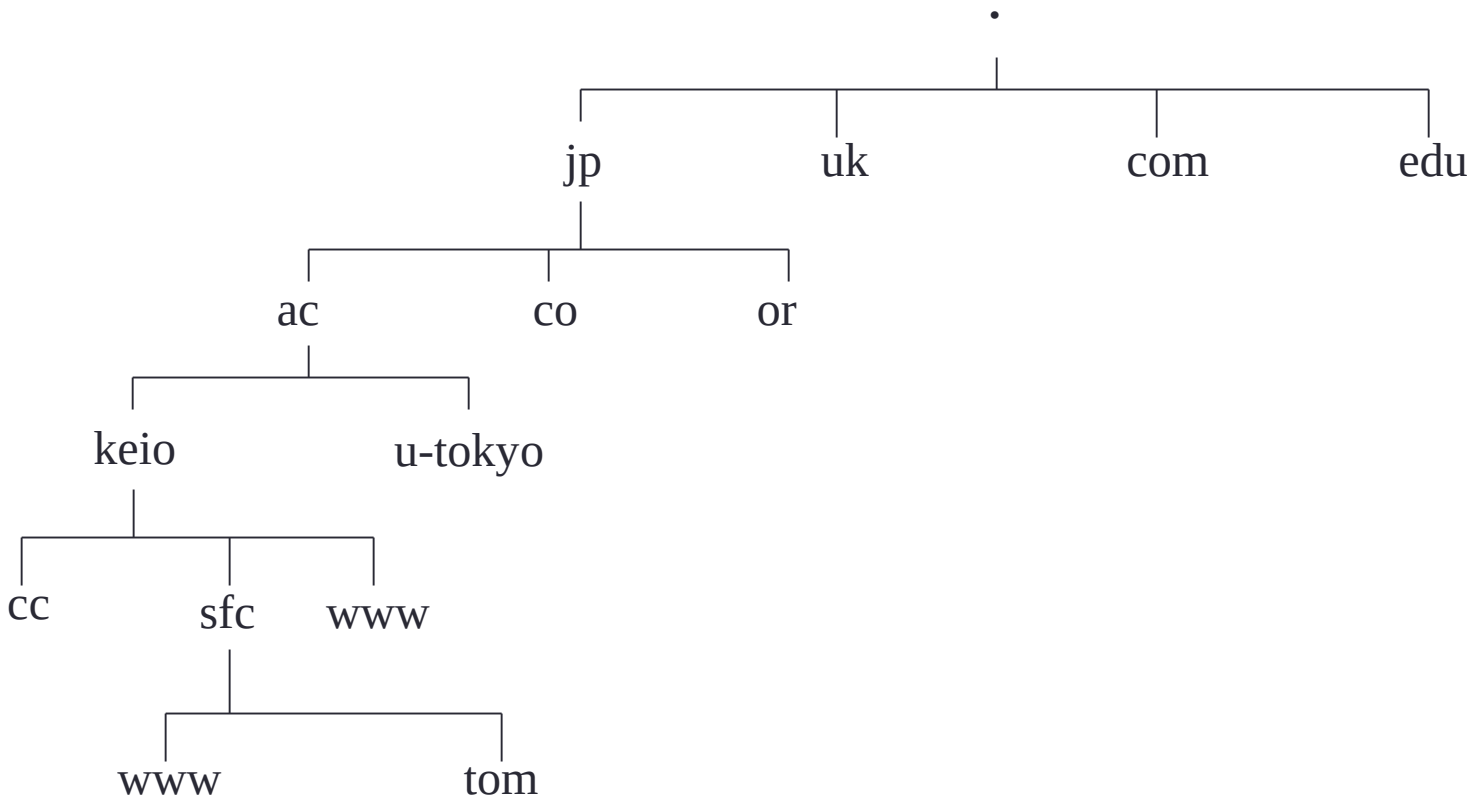
- IPアドレス
  - ネットワークでの番地
  - 組織に割り当てられた番号から選ぶ
  - 全世界的に一意的でなければならない
    - ローカルな部分で利用するローカルアドレスもある
    - IPv4: 192.168.xxx.xxx, 172.16-31.xxx.xxx, 10.xxx,xxx,xxx

ホスト名とIPアドレスとの対応

- ホスト名とIPアドレスの対応表をそれぞれのホストが持っている
  - /etc/hosts
  - LMHOSTS
- 対応表を組織内で共有化して使う
  - NIS（またはYP）
- インターネット全体で階層的に管理する
  - DNS（Domain Name System）

名前の構成

- www.sfc.keio.ac.jp



ドメイン名空間（Domain Name Space）

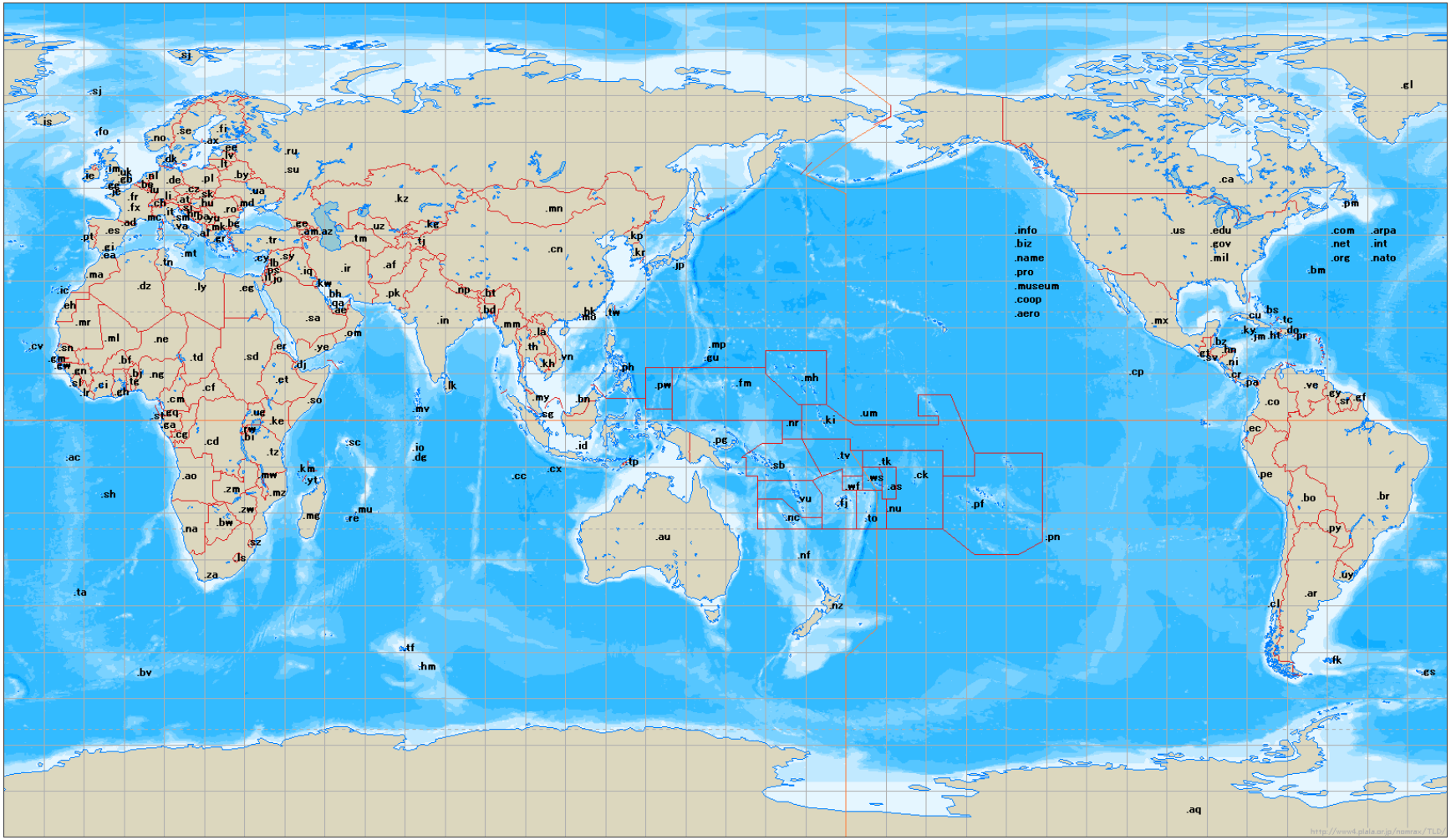
- ドメイン空間
  - 木構造の名前空間
- ルートドメイン
  - 木構造のルート
  - 通常「 . 」であらわす
- ラベル
  - 木構造のノードには最長63文字のラベルが付けられる
- ドメイン名
  - あるノードからルートドメインにたどり着くまでのラベルを列挙したもの
- ドメイン
  - ドメイン名前空間での部分木

トップレベルドメイン（TLD）

ルート直下のドメイン

- gTLD: ジェネリック
  - com: 商用
  - net: ネットワーク団体
  - org: 組織・団体
  - info: 特に制限なし
  - biz: 商用
  - name: 個人
  - pro: 弁護士・医師・会計士
- sTLD: スポンサー付
  - aero: 航空会社・空港
  - coop: 共同組合
  - museum: 博物館・美術館
  - jobs: 人事管理
  - travel: 旅行業
  - mail: eメール
  - cat: カタルーニャ語
  - post: 郵便事業
  - asia: APEC地域企業
  - mobi: モバイル向け
  - tel: IP電話
  - xxx: アダルトサイト用
- ccTLD: 国別コード
  - jp, kr, cn, ukなど
- iTLD: 国際
  - int: 国連・EU・NATO
- 特殊用途
  - gov: 政府関連の組織
  - mil: 軍関連の組織
  - edu: 教育を目的とした組織
  - arpa: 逆引き用
  - example: 例示
  - invalid: 誤り
  - localhost
  - test

Country Code



JPドメインの分類

- 属性型
  - ac.jp: ed以外の学校（大学など）
  - co.jp：株式会社，有限会社などの会社
  - go.jp: 政府機関，独立行政法人など
  - or.jp: 財団法人など，国連などの公的な国際機関など
  - ad.jp: JPNICの正会員が運用するネットワークなど
  - ne.jp: ネットワークサービス提供者が提供するネットワーク
  - gr.jp: 任意団体など
  - ed.jp: 保育所，幼稚園，小中高など18歳未満を対象とする各種学校
  - lg.jp: 地方公共団体など
- 地域型
  - 一般地域型ドメイン名：example.shinjuku.tokyo.jpなど
  - 地方公共団体ドメイン名: pref.hokkaido.jp, city.yokohama.jpなど
- 汎用JPドメイン名
  - 日本に住む個人，法人，組織など

ドメイン名の登録

- ICANN (The Internet Cooperation for Assigned Names and Numbers)
  - gTLD (global Top Level Domain)
    - com, net, org, info, biz, name, pro, museum, coop, aero, edu, gov, mil, arpa, int, nato
  - ccTLD (country code Top Level Domain)
    - jp
    - JPRSが管理
    - 3種類
      - 汎用JPドメイン名
      - 属性型JPドメイン名
        - co, or, ne, ac, ad, ed, go, gr, lg
      - 地域型JPドメイン名

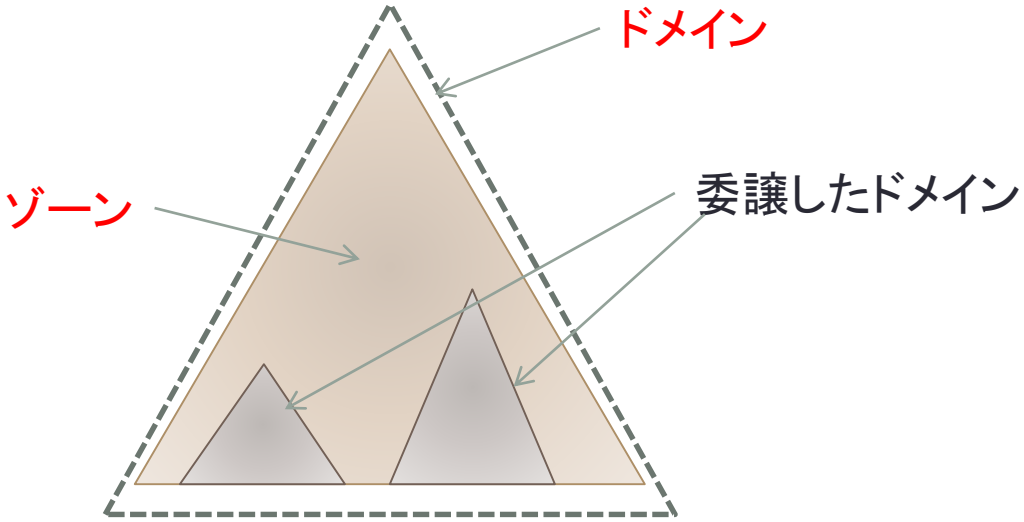
日本語ドメイン名

- ドメイン名として日本語(Unicode文字)を利用可
  - 慶應義塾大学.jp

- DNSのユニコードへの拡張
  - 文字コードとしてUTF-8を直接許すようにしたわけではない
  - Punycodeによるエンコーディング
    - 7bit表現，ASCII 37文字で表現
    - http://www-serv.jprs.jp/ace_chk/index_mini.html
    - 「慶應義塾大学.jp」⇒「xn--vns4ou9ck7j4lai49l.jp 」
    - 「慶應.jp」⇒「xn--hju2g.jp」
    - 「慶應SFC.jp」⇒「xn--sfc-2b5fjo.jp」

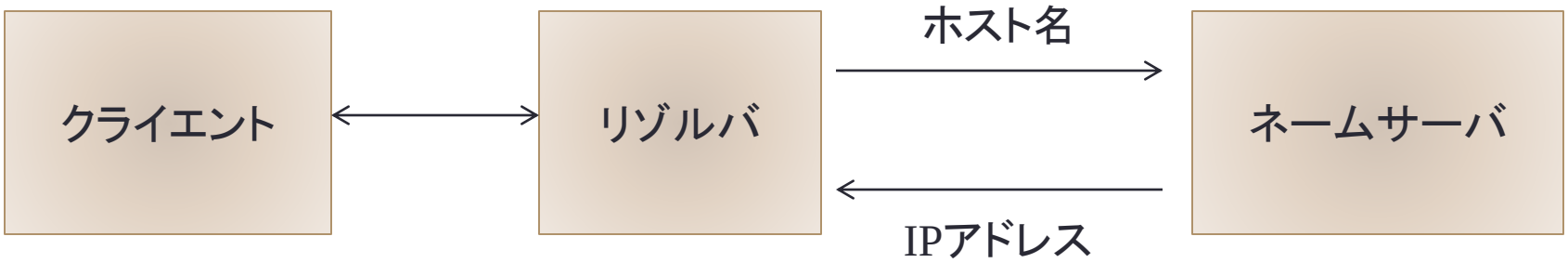
ネームサーバ(Name Server)

- ドメイン名空間に関する情報をあつかうプログラム
  - ゾーン(zone)に関する完全な情報を管理
  - ゾーンはドメインと同じだが，権威を委任した部分を除く
  - ネームサーバの種類
    - プライマリマスタ(primary master)
    - セカンダリマスタ(secondary master)



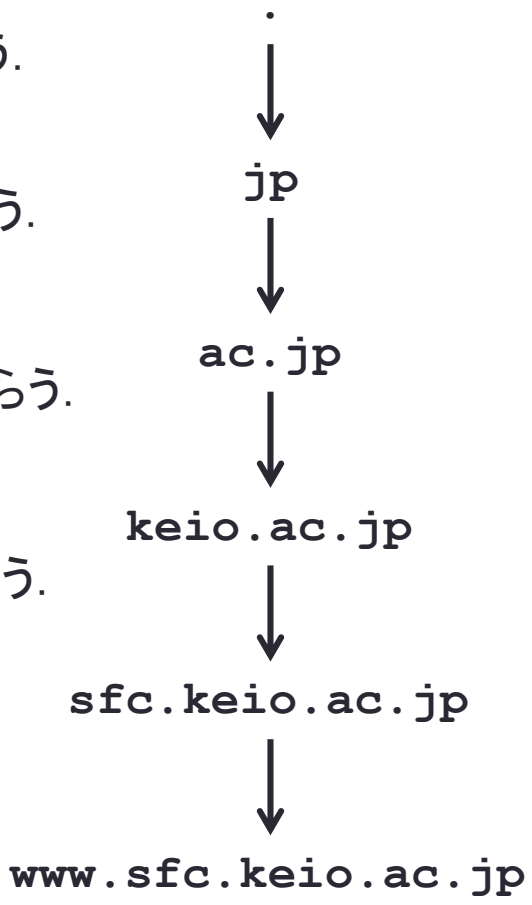
リゾルバ(Resolver)

- ネームサーバをアクセスするクライアント
  - ネームサーバへ問い合わせる
  - 応答の解釈を行う
  - 要求側のプログラムへ情報を返送する
- telnet, ftpなどで用いられるBIND
  - ライブラリルーチン
  - スタブリゾルバ(stub resolver)と呼ばれる



名前の解決

- **www.sfc.keio.ac.jp**のアドレスを問い合わせる
  1. ルートネームサーバに問い合わせる.
     - jpネームサーバに問い合わせるように返事をもらう.
  2. jpネームサーバに問い合わせる.
     - acネームサーバに問い合わせるように返事をもらう.
  3. acネームサーバに問い合わせる.
     - keioネームサーバに問い合わせるように返事をもらう.
  4. keioネームサーバ問い合わせる.
     - sfcネームサーバに問い合わせるように返事をもらう.
  5. sfcネームサーバに問い合わせる,
     - wwwのアドレスを教えてもらう.



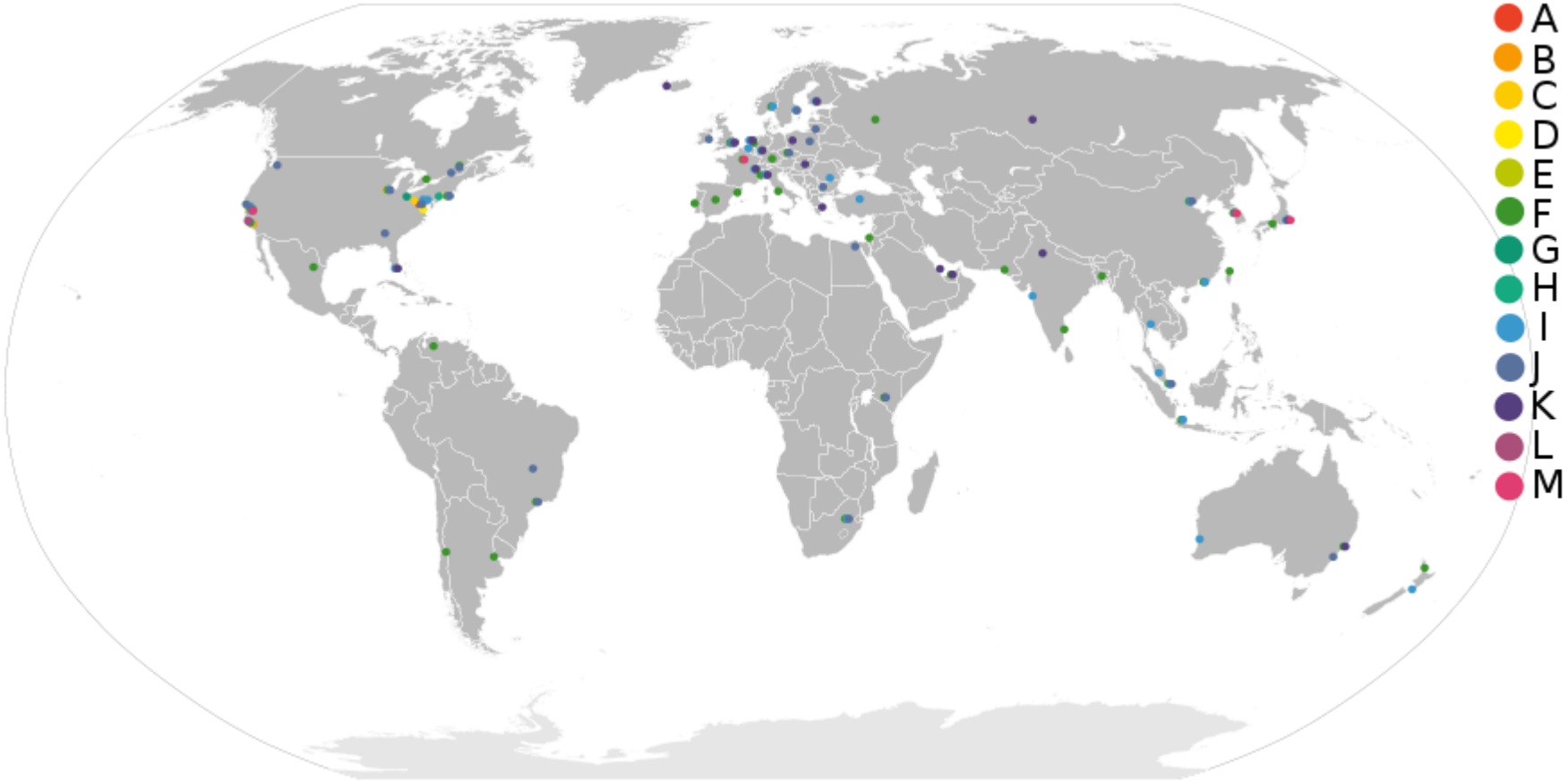
キャッシュ

- ネームサーバに対する負荷を軽減させなくてはいけない.
  - 問い合わせた結果はキャッシュしておく
  - キャッシュされたデータにはTTL（Time To Live）が設定されていて，その時間が過ぎると無効になる.
  - 存在しない名前に対する返答（存在しないこと）もキャッシュしておかないと，DOSの標的となる.
- TTLは通常1日程度に設定されている.
  - IPアドレスの変更は頻繁に行うものではない.
  - 長く設定しすぎると，IPアドレスの変更が反映に時間がかかる.

13個のルートネームサーバ

頭文字	IPv4アドレス	IPv6アドレス	管理者	サーバ所在地
A	198.41.0.4	2001:503:ba3e::2:30	Verisign (US)	anycast
B	199.9.14.201	2001:500:84::b	UCS-ISI (US)	Marina Del Rey, California, USA
C	192.33.4.12	2001:500:2::c	Cognet Communications (US)	anycast
D	128.8.10.90	2001:500:2d:d	University of Maryland (US)	College Park, Maryland, USA
E	192.203.230.10	2001:500:a8::e	NASA (US)	Mountain View, California, USA
F	192.5.5.241	2001:500:2f::f	ISC (US)	anycast
G	192.112.36.4	2001:500:12::d0d	U.S. DoD NIC	anycast
H	198.97.190.53	2001:500:1::53	U.S. Army Research Lab	Aberdeen, Proving Ground, Maryland, USA
I	192.36.148.17	2001:7fe::53	Netnod (Sweden)	anycast
J	192.58.128.30	2001:503:c27::2:30	Verisign (US)	anycast
K	193.0.14.129	2001:7fd::1	RIPE NCC (Holand)	anycast
L	199.7.83.42	2001:500:3::42	ICANN (US)	anycast
M	202.12.27.33	2001:dc3::35	WIDE Project (Japan)	anycast

ルートネームサーバの位置



http://en.wikipedia.org/wiki/Root_name_server

アドレスから名前へのマッピング

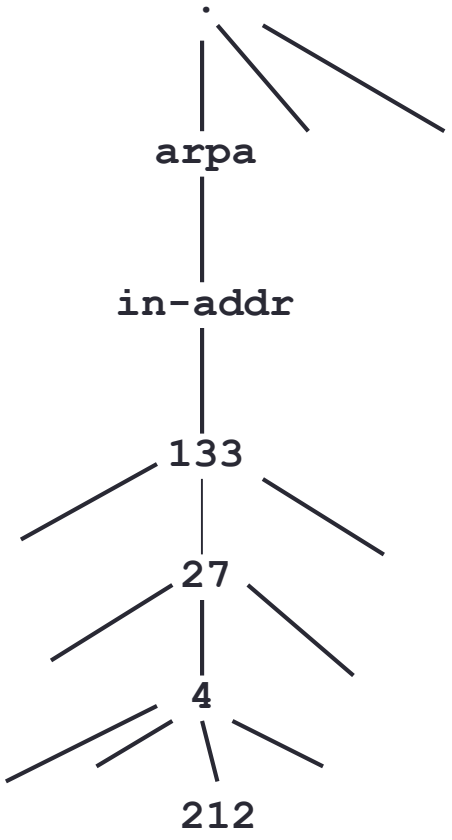
- IPアドレスからホスト名を知りたい
  - 逆引き
  - 信用してよいアドレスかどうか調べたい

- **in-addr.arpa**ドメインを用いる.
  - 133.27.4.212のホスト名を聞くには,

    212.4.27.133.in-addr.arpa

    と問い合わせる

- 問題点
  - 管理単位が8ビット毎であり，サブネットの単位と異なることがある



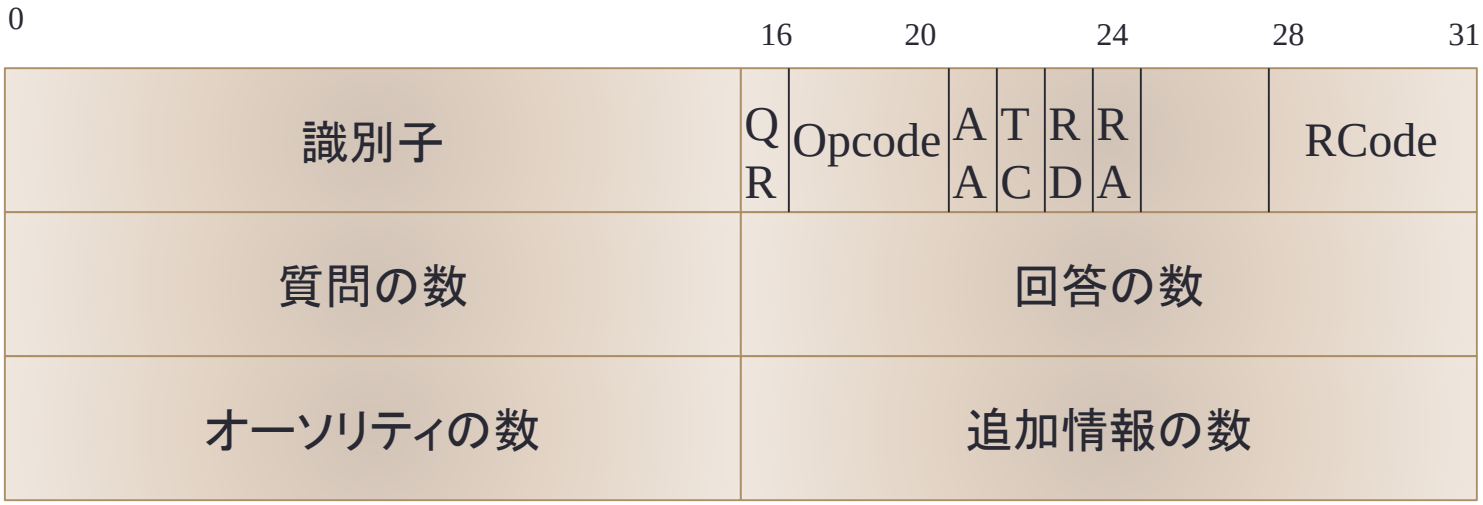
ネームサーバの管理している情報

- RFC1035
  - A: IPアドレス
  - CNAME: 正規名
  - HINFO: ホスト情報(cpu, os)
  - MB: メールボックスドメイン名(実験的)
  - MD: メールデスティネーション(MXに置き換え)
  - MF: メールフォワード(MXに置き換え)
  - MG: メールグループメンバー(実験的)
  - MINFO: メールボックスまたはメールリスト情報(実験的)
  - MR: メールリネーム(実験的)
  - MX: メールエクスチェンジャ
  - NS: ネームサーバ
  - NULL: バイナリデータ(実験的)
  - PTR: ポインタ(IPアドレス逆引用)
  - SOA: 権限開始
  - TXT: テキスト
  - WKS: 良く知られたサービス(TCP telnet smtp ftp)
- RFC1183
  - AFSDB: AFSデータベース(実験的)
  - ISDN: ISDNアドレス(電話番号，実験的)
  - RP: 担当者(実験的)
  - RT: 経路(実験的)
  - X25: X.25アドレス(実験的)
- RFC1664
  - PX: X.400/RFC822マッピング情報へのポインタ

DNSプロトコルのフォーマット

- UDPのポート53
- DNSメッセージフォーマット

DNSメッセージヘッダ



- 識別子:　自由に利用可能
- Opcode:問い合わせ
- QR:0は問い合わせ，1は応答
- AA:応答が正式なもの，TC:メッセージが短縮されている
- RD:再帰呼び出し希望，RA:再帰呼び出し可能
- RCode:回答

DNS Query and Reply

まとめ

- インターネットプロトコル
  - TCP/IP
  - IPv4とIPv6
- アプリケーションプロトコル
- 階層的な名前管理
  - DNS
  - ルートサーバ
    - 13個
    - anycastの利用
  - キャッシュの活用
  - メールアドレスの解決