ITPASS
Information Training Program
with a Spirit of Self-help

DNS

地球及び惑星大気科学研究室
M1 市田春菜

0. Index

1. DNS とは

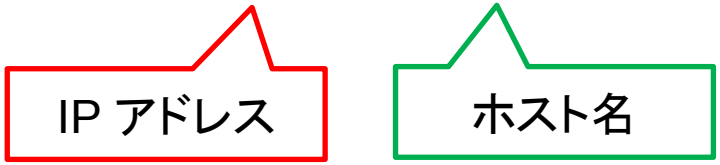
- Domain Name System
- ドメイン名と IP アドレスを対応づける (名前解決する) ためのしくみ
  - ドメイン名：人間用のインターネット上の住所
    - ex. itpass.scitec.kobe-u.ac.jp
  - IP アドレス：機械用のインターネット上の住所
    - ex. 133.30.109.22

2. DNS の役割

- ARPANETの時代
  - 初期のネットワーク
    - ネットワークの規模が小さかった
    - Internet のように不特定多数が参加することを考慮する必要がなかった
    - 各ユーザ毎に hosts ファイル (単純な対照表)で情報を管理

ex.

```
127.0.0.1       localhost
192.168.1.10    host1
192.168.1.1     gw
10.1.210.10     www
```

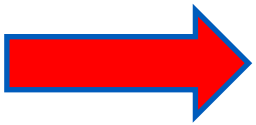


2. DNS の役割

- Internet 登場後
  - 不特定多数のホストが参加
    - 接続する機器が増える度に hosts ファイルを書き直す必要性
    - 各ホストに名前解決の情報を持たせることは非現実的

→ユーザの負担が増大する

→一元的な名前解決法の必要性



DNS の導入

2. DNS の役割

- DNS による一元的な名前解決
  - hosts ファイルのような対照表を管理する, 専用のサーバ(DNS サーバ)に情報を集約
  - 各ホストがサーバに問い合わせる
  - メリット

① ユーザに通知しなくてもホストのIPアドレスを変更できる

② ユーザが hosts ファイルを定義する必要がない

2. DNS の役割

- 課題
  - ドメイン名が重複しないようにして誰もが理解しやすいようにしなければならない

    →ドメイン名空間の導入

  - 1カ所のサーバが世界中のホスト情報を管理，運営するのは負担が大きい
  - 複数のサーバを稼働させるとしても，各々が全てのホスト情報を持っているのは非効率

    →管理の分散化

3. DNS の仕組み

- 3. DNS の仕組み
  - 3-1. ドメイン名の構成
  - 3-2. ドメイン名空間
  - 3-3. 委任
  - 3-4. ゾーン
  - 3-5. リソースレコード
  - 3-6. ゾーン転送, SOA レコード

3-1. ドメイン名の構成

- 各ホストの“住所“の構成

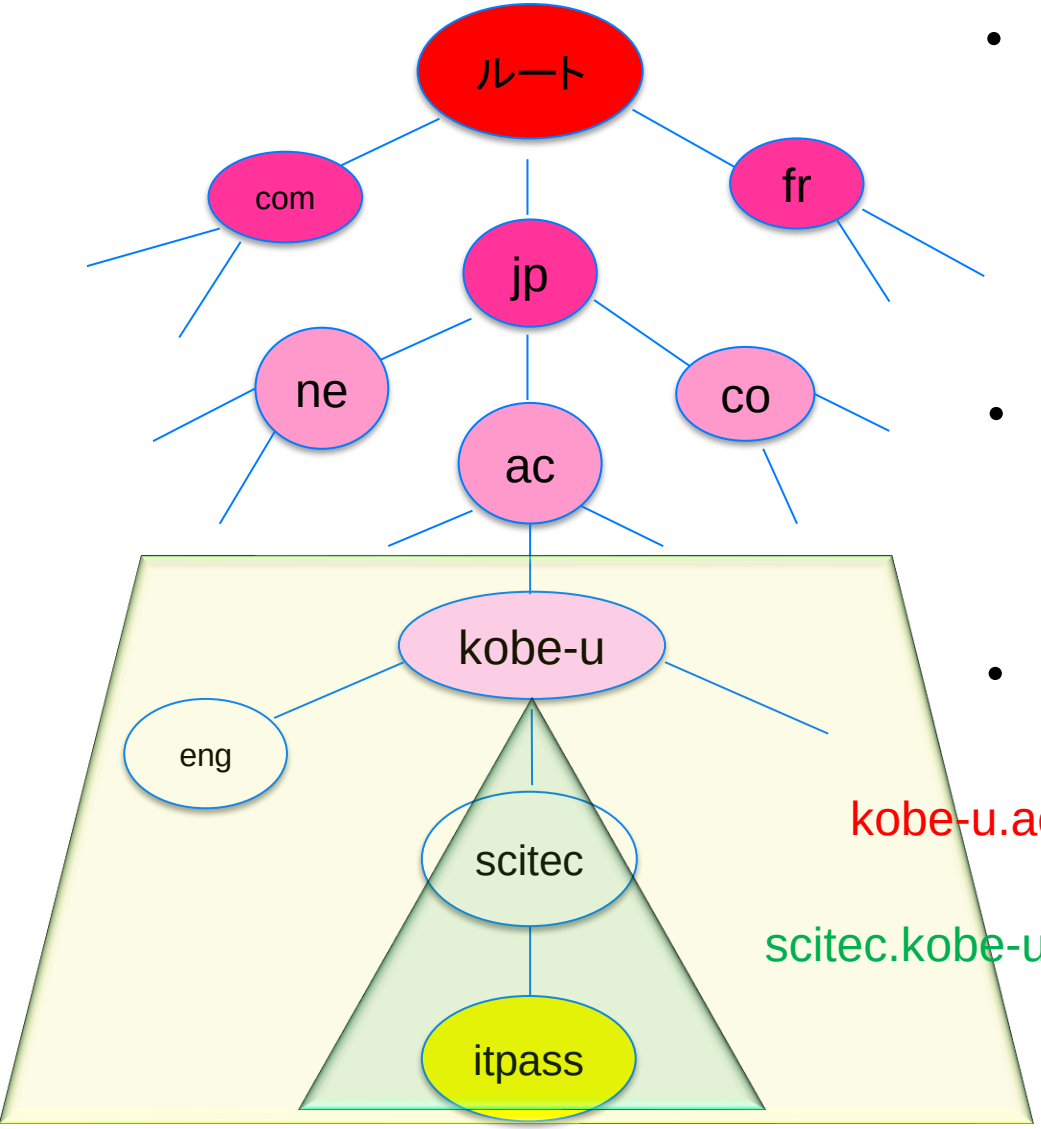
ー “ . “で区切る
ー 区切られた部分を“ラベル“という(1つのラベルの長さは63文字以下)
ー 全体をドメイン名と呼ぶ
ー 全体は最大 253 文字(ピリオドを含む)

3-2. ドメイン名空間

- ドメイン名空間(DNS ツリー構造)
  - ルートを頂点とした階層構造 (c.f. UNIX ファイルシステム)
    - UNIX : ファイルの指定
      - /usr/local/…/…. (絶対パス)
    - DNS : ホスト名 (ドメイン名) の指定(後→前)
      - www.example.co.jp.
  - 各階層にグループとしての意味を持たせる
    - 下位のドメイン (サブドメイン) やホスト名を管理する分散型の構造

※サブドメイン : あるドメインの一つ下にあるドメインのこと

3-2. ドメイン名空間（ドメイン名ツリー）



- ノード
  - ツリーの構成要素
  - それぞれに DNS サーバを設置
  - 各ノードで自分が管理するドメイン内の情報とサブドメインの情報をもっている
- ドメイン
  - ドメイン名空間の部分木
  - あるノード及びそれ以下の構成要素
- サブドメイン
  - ドメインより下位の部分木

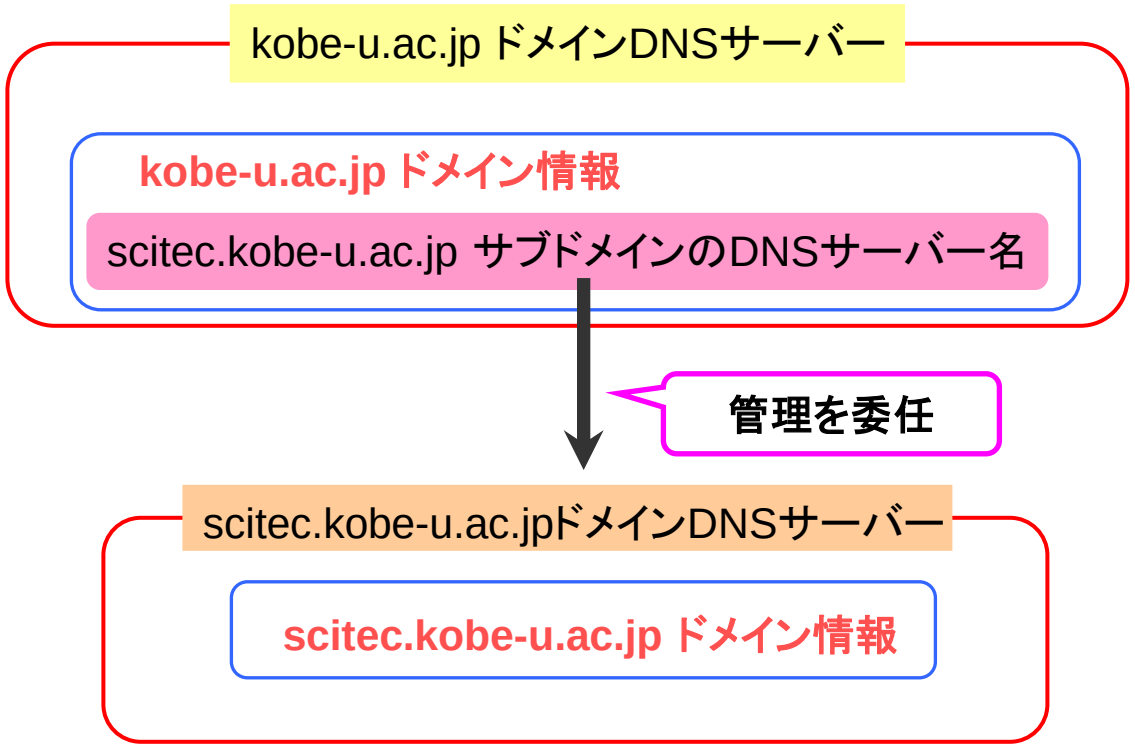
kobe-u.ac.jp ドメイン

scitec.kobe-u.ac.jp サブドメイン

：ノード

3-3. 委任

- 委任
  - ドメインを複数のサブドメインに分割し，それぞれのサブドメインに関する管理を他の組織に委任する



・各 DNS サーバは自分が管理する範囲(ゾーン)というものを持っている

・各 DNS サーバは基本的に上位の DNS サーバから権限委任された範囲を管理する

→ 名前解決は1つずつ下へ情報を聞いていく

3-4. ゾーン

- ゾーン
  - DNS サーバが管理する範囲
  - リソースレコードを含んでいる

3-5. リソースレコード

- リソースレコード
  - ドメインやホストの設定を示したひとまとまりのデータ
  - 代表的なものは以下の 6 種類

A	ホスト名から IP アドレスへの対応
PTR	IP アドレスからホスト名への対応
NS	ドメインの DNS サーバ名を指定する
SOA	ゾーン(ドメイン)情報を記載する
CNAME	ホスト名の別名(エイリアス)を正規名へ変換する
MX	ドメインとメールアドレスを対応付ける

3-5. リソースレコード

- A レコード
  - ドメイン名とそれに対応する IP アドレスを記述

- CNAME レコード
  - 1つの IP アドレスに複数のドメイン名を持たせる際に使用
  - A レコード以外の名前をつけるときに使用

- PTR レコード
  - IPアドレスからドメイン名を調べる際に使用

3-5.リソースレコード

- NSレコード

ドメインとそのドメインを管理する DNS サーバ名を定義する

– ドメインと DNS サーバの対応を記述

– ex.

ドメイン名	TTL	ネットワーククラス	レコード名	DNS サーバ名
example.jp.	3600	IN	NS	ns1.example.jp.

– example.jp. のIP アドレスは ns1.example.jp. の DNS サーバが知っていることを示している

※TTL：キャッシュされたデータの有効期間を表すもの

3-5. リソースレコード

- MX レコード

  メールサーバー, メールを配送するホストを指定するリソースコード

  ー メールアドレスにはドメイン名とメールサーバのホスト名を結びつけるものが必要

  → MX レコード

  ー メールを送信するメールサーバは宛先のメールアドレスの MX レコードを調べ，実際にメールを送るメールアドレスを入手する

3-5. リソースコード

- SOA レコード

  DNSで定義されるドメインの情報の種類の一つ

  ゾーンの管理のための情報や設定などを記述

ゾーンの起点			プライマリマスタ	ドメイン管理者のメールアドレス
@	IN	SOA	dns.kobe-u.ac.jp.	root.kobe-u.ac.jp. (
			2009101601	; Serial
			3600	; Refresh
			900	; Retry
			604800	; Expire
			3600)	; Minimum

serial: シリアル番号,更新する度に数字を大きくする(日付などにすると便利)
Refresh: プライマリマスタの最新性を確認する間隔 (1時間に一回更新)
Retry: プライマリマスタへの再試行間隔 (15分後に再試行)
Expire: アクセスを諦めるまでの時間 (1週間後に期限切れ)
Minimum: ネガティブキャッシュの最小TTL (1時間を指定)

3-6. ゾーン転送

- ゾーン転送
  - DNS サーバは通常 2 系統以上用意される
    - プライマリ DNS
      - ゾーン情報を有する
        - » 管理しているドメインの情報を有する
    - セカンダリ DNS
      - プライマリ DNS のゾーン情報のコピーを有する
  - セカンダリ DNS の情報を最新に保つためにプライマリ DNS の情報をコピーすることをゾーン転送という

4. 名前解決の流れ

- 4-1. 検索方法
- 4-2. リゾルバ
- 4-3. 正引き･逆引き

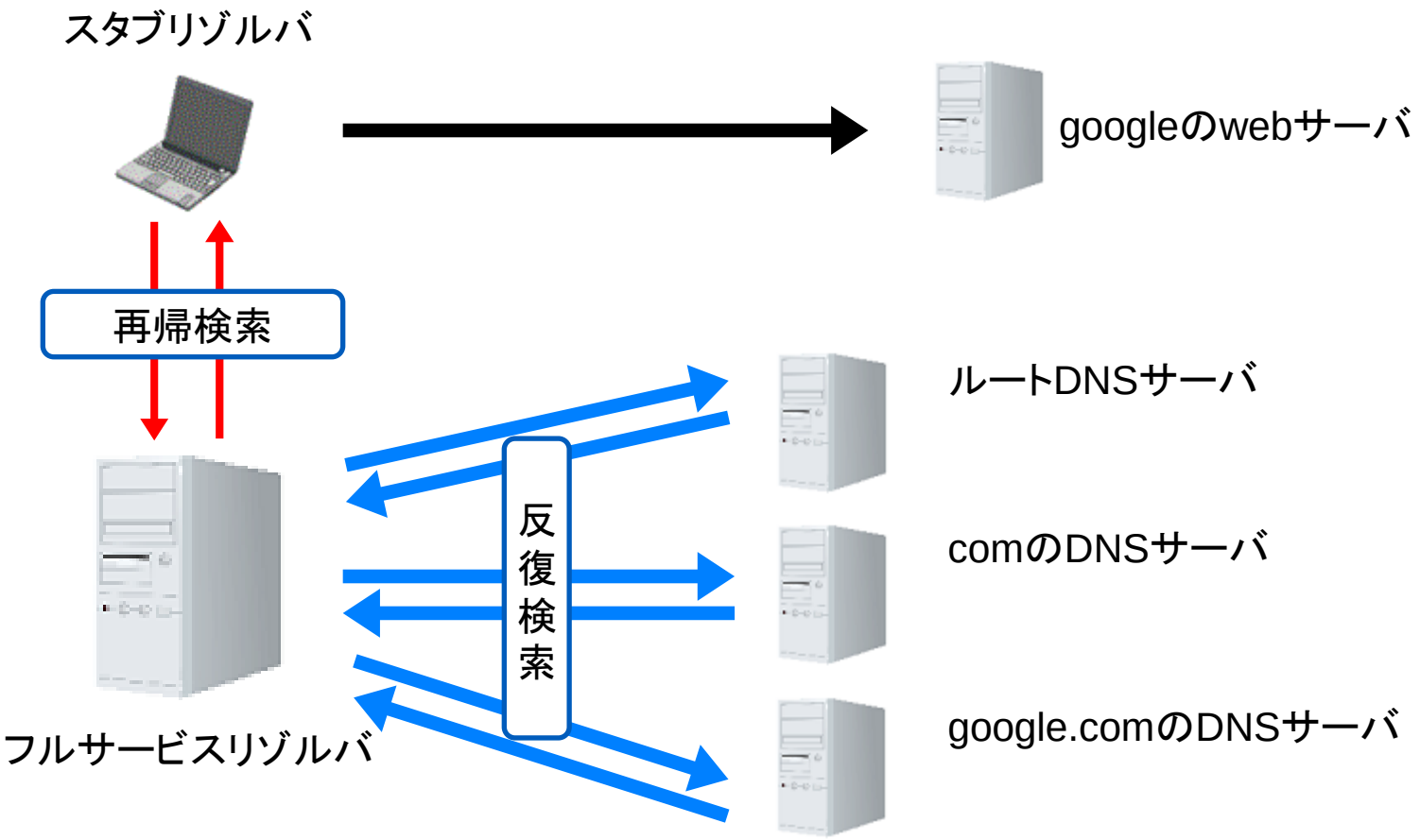
4-1. 検索方法

- 再帰検索
  - 名前が解決するまで他のサーバに対して検索を行い, 最終結果を返させる
- 反復検索
  - 他のサーバに問い合わせをせず, 自分のゾーンの情報のみに返答させる.

4-2. リゾルバ

- リゾルバ
  - 名前解決を行うソフトウェア
    - フルサービスリゾルバ
      - 反復検索によって完全に名前解決ができる
    - スタブリゾルバ
      - フルサービスリゾルバに検索要求だけ行う

4-2. リゾルバ


スタブリゾルバ
googleのwebサーバ
再帰検索
ルートDNSサーバ
comのDNSサーバ
反復検索
google.comのDNSサーバ
フルサービスリゾルバ

4-3. 正引き, 逆引き

- 正引き
  - ホスト名から IP アドレスを求めること
    - ex. ltpass.scitec.kobe-u.ac.jp というホストの IP アドレスを知りたいとき
      - 最初はルートに訊きに行く
        - » ドメイン名空間の最上位からツリーに従って検索していく
      - 用いるリソースレコード
        - » SOA レコード
        - » A レコード
        - » MX レコード　etc.

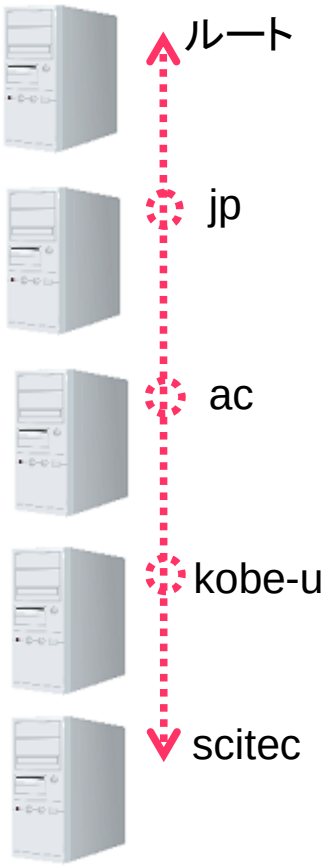
4-3. 正引き, 逆引き

- 逆引き
  - IP アドレスからホスト名を求めること
    - ex. 133.30.109.22 というホストのドメイン名を知りたいとき
      - 22.109.30.133.in-addr.arpa. とする
        - » in-addr.arpa は逆引き専用のドメイン名
      - 用いるリソースレコード
        - » PTR レコード

5. ITPASS サーバの DNS に関する仕事

- フルサービスリゾルバ
  - スタブリリゾルバからの問い合わせに対し, 応答するサーバのこと
  - かつてはキャッシュ専用サーバで, スタブリゾルバだったが, 2011 年からフルサービスリゾルバになった

- キャッシュに以前の問い合わせが残っているならば, 直接答えを返す.
- DNS 情報がない場合には, 他の DNS サーバに訊きに行く



6. DNS まとめ

- DNS とは
  - ドメイン名と IP アドレスを対応づける仕組み
- ドメイン名空間
  - ルート (根) とドメイン (枝) からなるツリー構造
    - DNS サーバの負担軽減やホスト名の一意性の担保
- リソースレコード
  - ドメインやホストの設定を示したひとまとまりのデータ
- 名前解決
  - ツリー構造をたどり, 各 DNS サーバに問い合わせる
- ITPASS サーバは
  - DNS に関してはフルサービスリゾルバ

参考文献

- 2011 ITPASS セミナー「DNS」のおはなし
  https://itpass.scitec.kobe-u.ac.jp/seminar/lecture/fy2011/111028/pub/
- 2012 ITPASS セミナー「DNS」
- https://itpass.scitec.kobe-u.ac.jp/hiki/hiki.cgi?cmd=view&p=%5BSemi2012%5D%E5%8B%89%E5%BC%B7%E4%BC%9A%E8%B3%87%E6%96%99&key=DNS
- 2014 ITPASS セミナー「DNS」
  https://itpass.scitec.kobe-u.ac.jp/seminar/lecture/fy2014/141016/pub/
- 2015 ITPASS セミナー「DNS」
  https://itpass.scitec.kobe-u.ac.jp/~itpass/seminar/lecture/fy2015/150928/pub/
- 2016 ITPASS セミナー「DNS」
  https://itpass.scitec.kobe-u.ac.jp/~itpass/seminar/lecture/fy2016/161011/pub/
- 2021ITPASSセミナー「DNS」
  https://itpass.scitec.kobe-u.ac.jp/~itpass/seminar/lecture/fy2021/211008/pub/
- IT 用語事典
  http://e-words.jp/
- Wikipedia DNS
  http://win.kororo.jp/archi/tcp_ip/dns.php

参考文献

- @IT : DNS Tips
  http://www.atmarkit.co.jp/flinux/index/indexfiles/bind9index.html
  http://www.atmarkit.co.jp/ait/articles/0112/18/news001.html
- 3分間 Net Working
  http://www5e.biglobe.ne.jp/%257eaji/3min/index.html
- http://ascii.jp/elem/000/000/458/458858/index-2.html
- 小悪魔女子大生のサーバエンジニア日記
  https://coakuma.directorz.jp/blog/category/dns%E3%81%A3%E3%81%A6%E4%BD%95%EF%BC%9F/
- JPNIC
  https://www.nic.ad.jp/ja/dom/system.html
- Network Study TCP/IPをはじめから
  https://www.infraexpert.com/study/study15.html

参考文献

- 絵で見てわかるDNS用語(絵で見てわかるDNS用語 - Qiita)
- JPRS用語辞典

https://jprs.jp/glossary/index.php?

参考

- 世界のルートサーバ運用機関

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

http://www.nic.ad.jp/ja/dom/system.html

参考

- ルートサーバの位置

JPNIC ニュースレター No.45 /2010 年 7 月発行 図 3 <https://www.nic.ad.jp/ja/newsletter/No45/0800.html>

名前解決とは

- 名前解決
  - ソフトウェアなどが扱う対象の識別名と、その名前が指し示す実体を対応付ける処理や操作
  - ドメイン名やホスト名と対応する IP アドレスを対応付ける

BIND

- **B**erkeley **I**nternet **N**ame **D**omain
  - 最も広く普及している DNS　サーバソフトウェアの一つ
    - DNS サーバ, リゾルバライブラリ, 各種ツールの集合体
    - 13 台あるルートサーバのうち 10 台は BIND を使用
  - オープンソースソフトウェア
  - 歴史も長く, 機能がとても豊富である
    - その反面, 複雑で導入が難しいとされることも
  - 広く普及しているので, 攻撃対象になりやすく, 頻繁にセキュリティ脆弱性が発見される

適切にバージョンアップする必要がある