

UNIXサーバー構築Ⅱ

第4章 DNSサーバー

DNSの概要①

■DNS (Domain Name System)

IPアドレスとホスト名の名前解決を行う。

インターネットの初期ではhostsファイルを使用して名前解決を行っていました。ただ、多くのユーザーが利用するようになり、大量のコンピュータをIPアドレスやホスト名を識別できなくなりました。そこでDNSが採用されました。

ドメイン名は、組織を表し、ホスト名は組織が管理するコンピュータを表します。

(例) **click.ecc.ac.jp** **click(ホスト名).ecc.ac.jp(ドメイン名)**

FQDN・・・完全修飾ドメイン、ホスト名 + 省略のないドメイン名

DNSの概要②

■ドメイン名

ドットで区切られた文字列で構成されます。1つ1つの文字列を**ラベル**とよびます。

ラベルは右側から、**トップ**(第1レベル)ドメイン、サブ(第2レベル、第3レベル、...)ドメイン、左端が**ホスト名**

(例) **click**.ecc.ac.**jp**の場合



DNSサーバーの種類

■DNSサーバーの種類

DNSサーバーは、キャッシュサーバーとコンテンツサーバー（権威サーバーとも呼ばれる）に大別されます。

①キャッシュサーバー

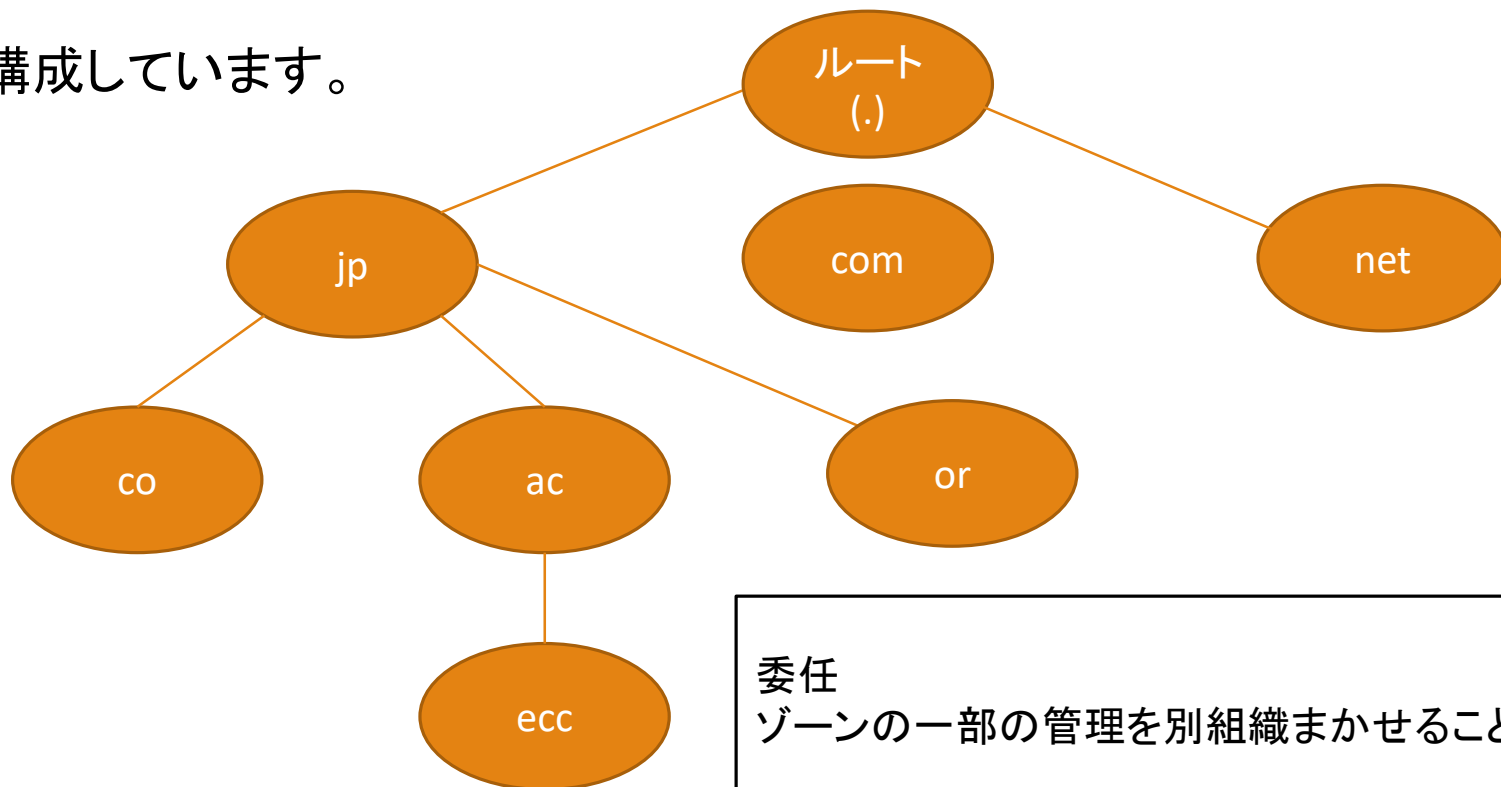
クライアントから問い合わせ（クエリー）を受け、代わりにインターネットに問い合わせを行うDNSサーバー。一度名前解決した情報を一定期間保存するためキャッシュサーバーと呼ばれます。

②コンテンツサーバー（権威サーバー）

自分が管理するドメインに関する問い合わせを受けるDNSサーバー。

DNSの名前空間

DNSの情報は分散管理されています。ルートを中心としたツリー構造を構成しています。



名前解決

クライアントから問い合わせ(クエリー)を受けた**キャッシュ**サーバーは、受け取ったドメイン名を右から順に検索し、そのドメイン名を管理する**コンテンツ**サーバーを**ルートサーバー**からたどっていきます。

*** 名前空間の図の上から下へたどります。**

たどり着いた**コンテンツ**サーバーは、**ホスト名+ドメイン名**に対するIPアドレスを返します。この仕組みを**名前解決**といいます。

コンテンツサーバー

■コンテンツサーバー（権威サーバー）

コンテンツサーバーは、自ドメイン内のホスト名を**ゾーンファイル**というデータベースで管理します。ゾーンファイルを検索することで、該当するIPアドレスなどを返します。

コンテンツサーバーは**プライマリサーバー**と**セカンダリサーバー**と役割を持っています。

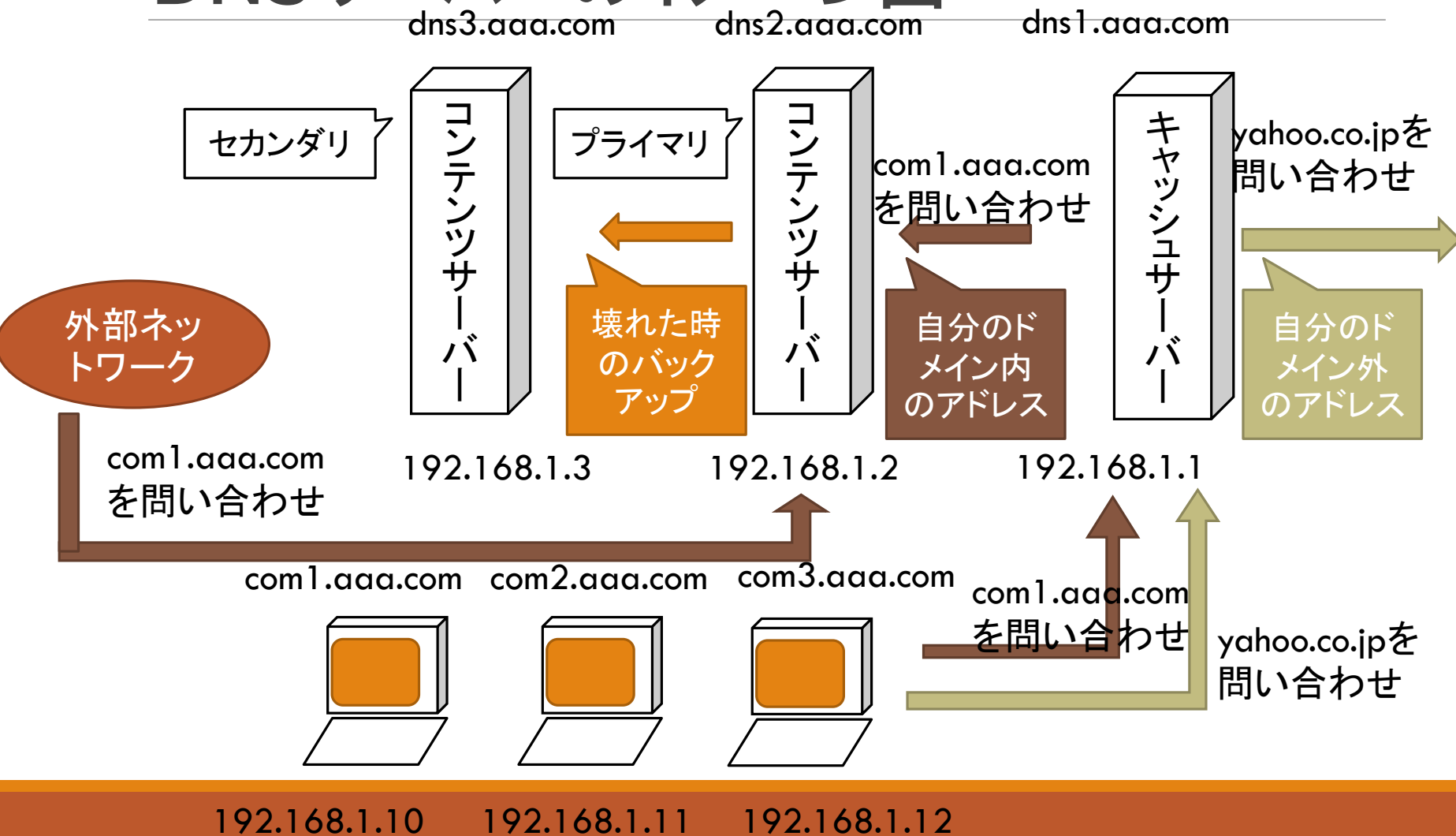
- ・**プライマリサーバー（マスターサーバー）**

ドメインの情報を管理するDNSサーバーのこと。

- ・**セカンダリサーバー**

プライマリサーバーのバックアップとして動作します。

DNSサーバーのイメージ図



名前解決

①正引き

ホスト名からIPアドレスを解決します。

②逆引き

- IPアドレスからホスト名を解決します。

正引き用のゾーンファイルと逆引き用のゾーンファイルを別で用意する必要があります。

DNSクライアント環境の確認

- ・DNSサーバーのIPアドレスを登録しているファイル
[/etc/resolv.conf](#)
- ・DNSサーバーに問い合わせるコマンド(ネットワークツール)
 - ① **nslookup ホスト名** 正引きの場合
 nslookup IPアドレス 逆引きの場合
 - ② **host ホスト名** 正引きの場合
 host IPアドレス 逆引きの場合
 - ③ **dig ホスト名** 正引きの場合
 dig -x IPアドレス 逆引きの場合

DNSサーバーの構築

①BINDのインストール

sudo apt install -y bind9 dnsutils

BINDとnslookupなどのツールをインストールします。

②BIND設定ファイルの修正・作成

named.conf、named.conf.optionsなどのファイル

③ゾーンファイルの作成

正引き用、逆引き用のゾーンファイルを作成します。

④bind(named)サービスを起動する

sudo systemctl start bind9 または

sudo systemctl start named

BIND設定ファイル

① **named.conf**ファイル

設定を記述します。今回は、別の設定ファイルをこのファイルに読み込み実行します。

② **named.conf.options**ファイル

フォワーダーやクエリーの許可など、DNSに必要な設定を記載します。

③ **named.conf.local**(ファイル名は任意)ファイル

該当するドメイン名やIPアドレスの解決する時に使用されます。どのドメインの時にどのゾーンファイルを使用するのかなど記載します。

④ ゾーンファイル(ファイル名は任意)

名前解決に使用するファイル。

設定ファイル(例 named.conf.local)

```
zone "ecccomp.ac.jp" IN {    ... ドメイン名
    type master;            ... マスター(プライマリ)
    file "/etc/bind/db.local";
    ...ドメインの検索に使用するゾーンファイル
};

zone "2.200.10.in-addr.arpa" IN {    ... 逆引き(ネットワークアドレス)
    type master;
    file "/etc/bind/db.local.rev";    ... ゾーンファイル
};
```

ゾーンファイル

ファイルの保存場所(任意): **/etc/bnid/**

ファイル名: 任意。db.localをコピーして使用してもOKです。

構文チェックコマンド

named-checkconf ... 設定ファイルの構文チェック

named-checkzone **ORIGIN名** **ゾーンファイル名**

例) `named-checkzone 0.200.10.in-addr.arpa kad06.rev`

ゾーンファイル(正引き)

\$TTL 604800

@ IN SOA sv.ecccomp.ac.jp. root.ecccomp.ac.jp. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

;

* sv.ecccomp.jp.(DNSサーバー)、 root.ecccomp.jp.(管理者)

ゾーンファイル(正引き)続き

	IN	NS	sv.ecccomp.ac.jp.	... DNSサーバー
	IN	A	10.200.2.158	... IPアドレス(DNS)
sv	IN	A	10.200.2.158	... Aレコード
web	IN	CNAME	sv.ecccomp.ac.jp.	... CNAMEの指定

* **AAAA**の場合は、Ipv6アドレス

@...ドメイン名を表す(@は.で表す)

;...コメント

nslookupの実行結果

ecc@ecc:~\$ **nslookup web.ecccomp.ac.jp**

Server: 10.200.2.158 ... DNSサーバーの情報

Address: 10.200.2.158 #53

web.ecccomp.ac.jp canonical name = sv.ecccomp.ac.jp.

... web.ecccomp.ac.jpはCNAMEが設定されていることがわかる

Name: sv.ecccomp.ac.jp

Address: 10.200.2.158 ... 回答のIPアドレス

逆引きゾーンファイル

\$TTL 604800

@ IN SOA sv.ecccomp.ac.jp. root.ecccomp.ac.jp. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800) ; Negative Cache TTL

;

逆引きゾーンファイル

	IN	NS	sv.ecccomp.ac.jp.	...	DNSサーバー
	IN	PTR	10.200.2.158	...	IPアドレス
	IN	A	10.200.2.158		
	IN	A	255.255.255.0	...	サブネットマスク
158	IN	PTR	sv.ecccomp.ac.jp.		
100	IN	PTR	web.ecccomp.ac.jp.		

ゾーンファイルのアドレスについて

ゾーンファイルのアドレスは最後に.が付いている

例) ie2a99.ecccompac.jp.

最後に.が付いているとFQDN(完全修飾ドメイン名)とみなされます。

.を付け忘れるとドメイン名が自動的に付加されてしまいます。

例) ie2a99.ecccomp.ac.jp

→ ie2a99.ecccomp.ac.jp.**ecccomp.ac.jp(追加されてしまう)**