DNS

/etc/named.conf　とは？
⇨DNSサーバーであるBIND（Berkeley Internet Name Domain）の設定ファイル

どんな内容が書かれているのか？
⇨

①ゾーン設定: ドメイン名とそのゾーンファイルの関連付けを行います。

単語の意味⇨ゾーンとは：

ゾーンとは、DNS（Domain Name System）における特定のドメイン名やサブドメインに関連する情報を管理するための単位です。具体的には、ゾーンは以下のような特徴を持っています。

1. **管理単位**: ゾーンは、特定のドメイン名やそのサブドメインに関連するDNSレコード（Aレコード、MXレコード、CNAMEレコードなど）を含むファイルやデータベースのことを指します。
2. **権威サーバー**: ゾーンに関連するDNSサーバーは、そのゾーンに対する権威を持つサーバーです。このサーバーは、該当するドメイン名に対して正確なDNS情報を提供します。
3. **階層構造**: DNSは階層的な構造を持っており、ゾーンはその階層の一部を形成します。例えば、`example.com` というドメインのゾーンには、その下のサブドメイン（`www.example.com` や `mail.example.com` など）に関する情報が含まれることがあります。
4. **ゾーンファイル**: ゾーンの情報は通常、ゾーンファイルというテキストファイルに保存されており、各レコードが特定の形式で記述されています。

ゾーンの設定をすると何が出来るのか？

ゾーンの設定を行うことで、以下のようなことが可能になります：

1. **DNSレコードの管理**:
   - ゾーンには、Aレコード（IPアドレスのマッピング）、MXレコード（メールサーバーの指定）、CNAMEレコード（別名の指定）など、さまざまなDNSレコードを設定できます。これにより、ドメイン名に関連する情報を適切に管理できます。
2. **ドメイン名の解決**:
   - ゾーン設定により、特定のドメイン名やサブドメイン名を、対応するIPアドレスに解決することができます。これにより、ユーザーはドメイン名を使ってウェブサイトやサービスにアクセスできます。
3. **メールのルーティング**:
   - MXレコードを設定することで、ドメインに送信されるメールが正しいメールサーバーにルーティングされるようにできます。

4. **サブドメインの管理**:
    - ゾーン設定を使って、サブドメインを作成し、それぞれに異なるDNSレコードを設定することができます。これにより、複数のサービスを同一ドメイン内で運用できます。
5. **DNSの冗長性と負荷分散**:
    - 複数のDNSサーバーにゾーン情報を設定することで、冗長性を確保し、負荷分散を行うことができます。これにより、システムの可用性が向上します。
6. **セキュリティの強化**:
    - DNSSEC（DNS Security Extensions）を使用して、ゾーンに対するセキュリティを強化することができます。これにより、DNS情報の改ざんを防ぐことができます。
7. **動的更新**:
    - ゾーン設定を通じて、DNSレコードを動的に更新することができます。これにより、頻繁に変わるIPアドレスに対応しやすくなります。

これらの機能により、ゾーン設定はドメイン名の管理や運用において非常に重要な役割を果たします。

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

- この部分がゾーン設定に該当します。ルートゾーン（"."）を指定し、そのゾーンファイルとして `named.ca` を使用しています。
- auto-dnssecやinline-signingも記述する事が出来る。

- auto-dnssec … 鍵の管理およびゾーン署名を自動化する（BIND 9.7〜）
- inline-signing … BIND（named）が自動的にゾーンへの署名を行う（BIND 9.9〜）

```
zone "example.com" {
        file    "example.com";
        : (省略)
        auto-dnssec maintain;
        inline-signing yes;
};
```

auto-dnssecを有効化した場合はinline-signingも有効化する必要がある。

従来は、ゾーンへの署名が必要になる際には、コマンド「dnssec-signzone」を用いる必要があったが、BIND9.9以降はauto-dnssecおよびinline-signingを有効化することにより、これらの更新作業はBINDが行うようになる。

BINDのバージョンの調べ方：

```
[root@localhost ~]# named -v
BIND 9.16.23-RH (Extended Support Version)
```

設定を有効化すると、ゾーンファイルへ署名したファイルがBINDによって自動的に作成される。

② **オプション**: DNSサーバーの動作に関する一般的な設定（例：ポート番号やリスニングアドレスなど）。

```
options {
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    allow-query { localhost; };
    recursion yes;
    dnssec-validation yes;
    managed-keys-directory "/var/named/dynamic";
    geoip-directory "/usr/share/GeoIP";
    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
    include "/etc/crypto-policies/back-ends/bind.config";
};
```

- この部分がオプションに該当する。サーバーの動作や設定（ポート番号、リスニングアドレス、ディレクトリパス、クエリの許可など）が含まれている。

③**アクセス制御**: どのIPアドレスからのクエリを受け付けるかを指定する設定。

```
allow-query { localhost; };
```

- この設定がアクセス制御に該当する。ここでは、ローカルホストからのクエリのみを受け付けるように設定されている。

④**転送設定**: 他のDNSサーバーへのクエリ転送の設定。

転送が必要な場合は `forward` オプションを追加することができる。転送設定が必要な場合、別途設定を行うことになる。