### (5) bind9 におけるキャッシュサーバの設定

DNS キャッシュサーバはクライアントの名前解決に利用されるが，不正に利用されると DDoS 攻撃につながる恐れがある．そのため，セキュリティを考慮して自分の管理するネットワーク以外の問い合わせは受け付けないようにする必要がある．この対策の一つにとして DNS コンテンツサーバと DNS キャッシュサーバの問い合わせを明示的に分けることにより，セキュリティを高めることができる．本実習では ns1 の IP アドレス 172.22.199.1 に対して 172.22.199.2 を新たに追加することでコンテンツサーバとキャッシュサーバの役割を分ける．この時の具体的な設定例として，ネットワークアドレス 172.22.199.0/24 による DNS キャッシュサーバの設定例をリスト 8-6～8-9 に示す（コメント行を除く）．ここで，リスト 8-6 は二つ目の IP アドレス 192.168.199.2 を追加したネットワークインタフェースの設定例を表しており，リスト 8-7～8-9 は bind9 における DNS キャッシュサーバの設定例を表している．

リスト8-6. IPを追加したインタフェースの設定例「/etc/netplan/99-myconfig.yaml」

```
network:
  ethernets:
    enp0s3:
      addresses: [172.22.199.1/24, 172.22.199.2/24]  #カンマ区切りで IP アドレスを追加
      routes:                                        #static ルートの設定
        - to: default                                #デフォルトゲートウェイの指定
          via: 172.22.199.254                        #上記ルートのネクストホップ IP アドレス
          metric: 100                                #上記 IP アドレスに対する重みづけ
      nameservers:                                   #DNS キャッシュサーバ設定
        addresses: [172.22.199.2]                    #DNS キャッシュサーバの IP アドレス
        search: [s2232199.labo.cit]                  #ホスト名による問い合わせ時のサーチドメイン
      dhcp4: false                                   #DHCP 設定
  version: 2
```

リスト8-7. bind9のDNSキャッシュサーバ設定例「/etc/bind/named.conf」

```
include “/etc/bind/named.conf.options”;          #オプション設定の読み込み
include “/etc/bind/named.conf.local”;            #ローカル設定の読み込み（このファイルに設定を書く）
#include “/etc/bind/named.conf.default-zones”; #デフォルトゾーン設定のコメントアウト（リスト 8-9 で読み込み）
```

リスト8-8. bind9のDNSキャッシュサーバ設定例「/etc/bind/named.conf.options」

```
options {
    directory “/var/cache/bind”;
    //dnssec-validation no;        # forward 有効化の設定，「//」を削除して「auto」を「no」へ変更
    listen-on-v6 { any; };
};
```

リスト8-9. bind9のDNSキャッシュサーバ設定例「/etc/bind/named.conf.local」

```
acl “localnet” {                                    #アクセスリストの作成
    172.22.199.0/24;
};

view “localnet_resolver” {                          #DNS キャッシュサーバ用の設定
    match-clients { localhost; localnet; };         #アクセス元のチェック（アクセス対象）
    match-destinations { localhost; 172.22.199.2; }; #アクセス先のチェック（DNS キャッシュサーバ）

    recursion yes;                                  #再帰問い合わせの許可（DNS キャッシュサーバの設定）
    allow-query { localhost; localnet; };           #問い合わせの許可対象（保険）
    allow-recursion { localhost; localnet; };       #再帰問い合わせの許可対象（保険）

    forward first;                                  #再帰問い合わせの動作を指定（最初にフォワードする）
    forwarders { 172.31.255.1; };                   #再帰問い合わせ先ホストの指定（上流の DNS サーバ）

    include “/etc/bind/named.conf.default-zones”;   #インターネットへ問い合わせを流さない名前解決設定
};
```