

新規にゾーンを作成

Webminで[サーバ]-[BIND DNSサーバ]を開きます．まず，このDNSサーバが管理するゾーンを新規に作成します．5.1の操作の後，図8の[BIND DNSサーバ]画面が表示されるので，その中の[新規のマスターゾーンを作成]をクリックします．



図8 「BIND DNSサーバ」画面で，[新規のマスターゾーンを作成]をクリックする

すると，図9の「マスターゾーンの作成」画面が開きます．ここでは，学生ごとに異なる設定をしますので，画面通りの設定ではなく別途各学生に送られている「構築するサーバの仕様」の通りに設定を行ってください．ここでは，次のようなゾーンを作成することとして説明します．

新規に作成するゾーン

- ドメイン名：nss00t000.teikyo. （※00t000は学籍番号に置き換える）
- マスタサーバ：svr01.nss00t000.teikyo. （このサーバのFQDN）
- Eメールアドレス：00t000xx@stu.teikyo-u.ac.jp

まず，[ゾーンの種類]は，[順引き]を選択します．

次に，[ドメイン名/ネットワーク]に，ドメイン名で指定されている "nss00t000"(自分の学籍番号) を入力します．

ここで作成するゾーンのマスターサーバはこのマシンなので，[マスターサーバ]にはこのサーバのFQDNである "svr01.nss00t000.teikyo"(自分の学籍番号を用いる) を入力します．

[ネームサーバレコードをマスタサーバに追加しますか?]はチェックしておきます．

[Eメールアドレス]には，仮に大学のメールアドレス "00t000xx@stu.teikyo-u.ac.jp" を入力しておきます．インターネットに公開するDNSサーバの場合は，そのドメインのメールアドレスを載せておくといいでしょう．

その他の設定は図9にあるデフォルトのままでいいでしょう．

設定が終わったら，[作成]ボタンを押します．

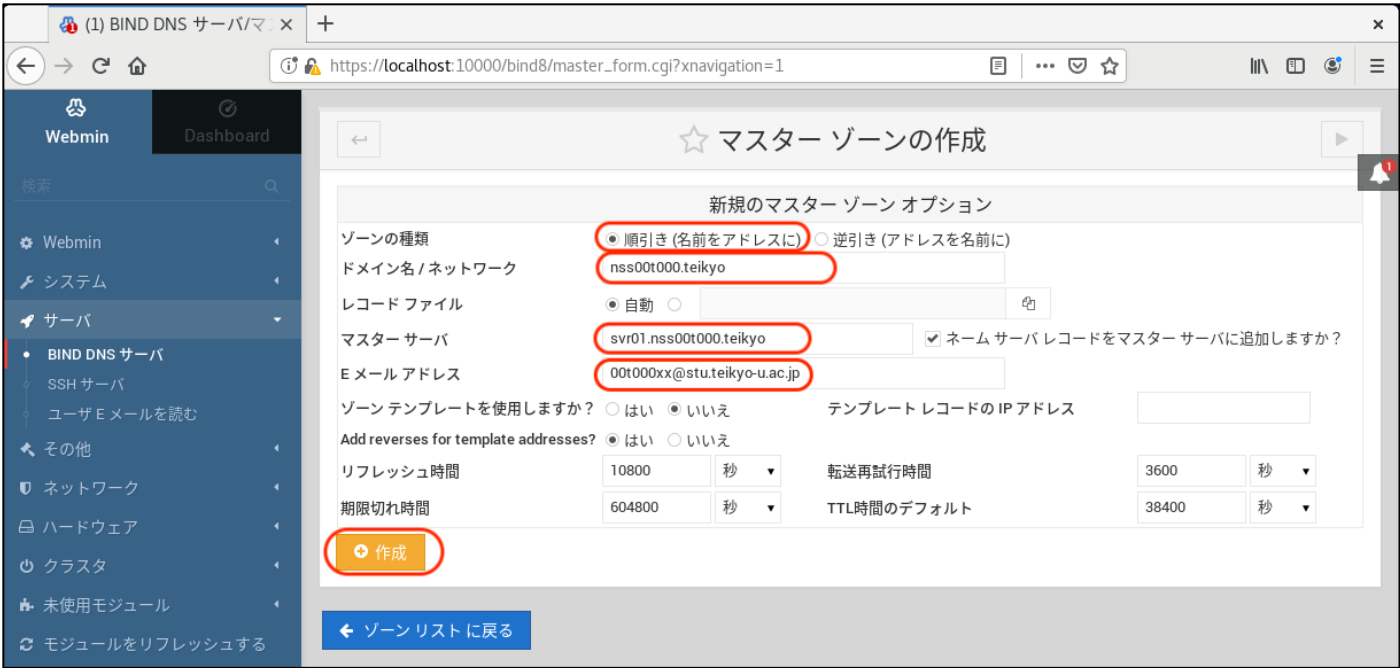


図9 「マスターゾーンの作成」画面

新規にゾーンを作成

続いて図10の「マスターゾーンの編集」画面が開きます。この画面では、このDNSサーバが管理する、このゾーン(nss00t000.teikyo)のホストマシン(図5のpc01, pc02)およびサーバ自身であるsvr01を登録します。

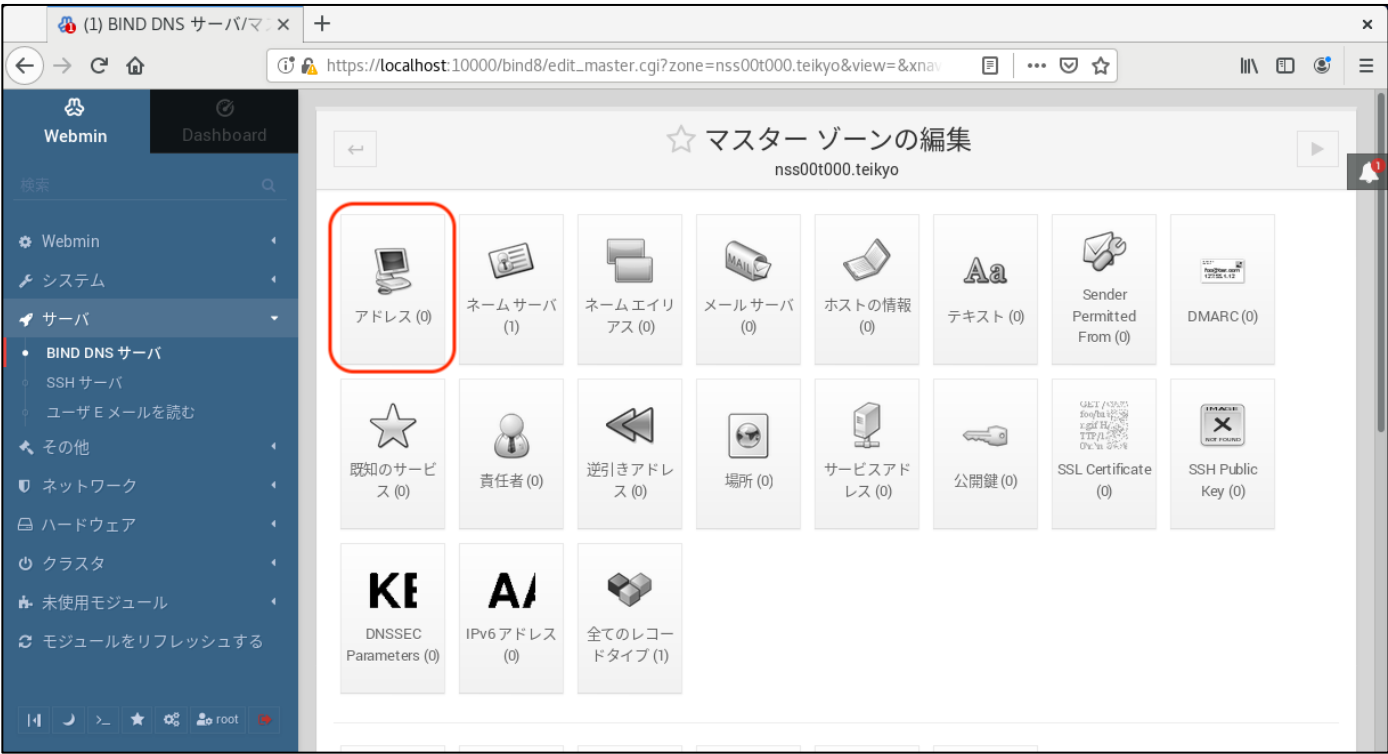


図10 「マスターゾーンの編集」画面。管理するホストを[アドレス]から登録する

※図9の手順で新規にマスターゾーンを作成すると、図8の[BIND DNSサーバ]画面に、[既存のDNSゾーン]というカテゴリが追加され、作成したゾーンのアイコンが表示されます。作成されたゾーンのアイコン(ここではnss00t000.teikyo)をクリックすると、図10の「マスターゾーンの編集」画面が開きます。



図11の「アドレス レコード」画面が開きますので、「レコード名」に登録するホストのFQDN(図11ではsvr01.nss00t000.teikyo.)を入力し、「アドレス」にこのホストのIPアドレス(図11では10.0.2.100)を入力します。その他の項目はデフォルトのままで構いません。入力が終わったら、[作成]ボタンを押します。

図11 「アドレス レコード」画面。ゾーンに登録するホストの**FQDN**と**IP**アドレスを設定する

作成ボタンを押すと、登録したアドレスのレコードが追加されます(図12)。ゾーン内のホストとして、サー/自身も忘れずに登録しておきましょう。そうしないと、DNSサーバ自身のドメイン名(ここではsvr01.nss00t000.teikyo)のIPアドレスの名前解決ができません。

レコード名	TTL	アドレス
svr01.nss00t000.teikyo.	デフォルト	10.0.2.100
pc01.nss00t000.teikyo.	デフォルト	10.0.2.121

図12 登録されたアドレスのレコードが一覧に追加される
(svr01, pc01, pc02の3つのレコードを登録する)

5.1 と , 5.2のここまでの設定が終わったら , 図13の「BIND DNSサーバ」画面で , [サービスを開始]ボタンを押します . (すでにBINDを起動している場合は , [変更を適用する]ボタンを押します .) これで設定した内容で BINDが動作します .

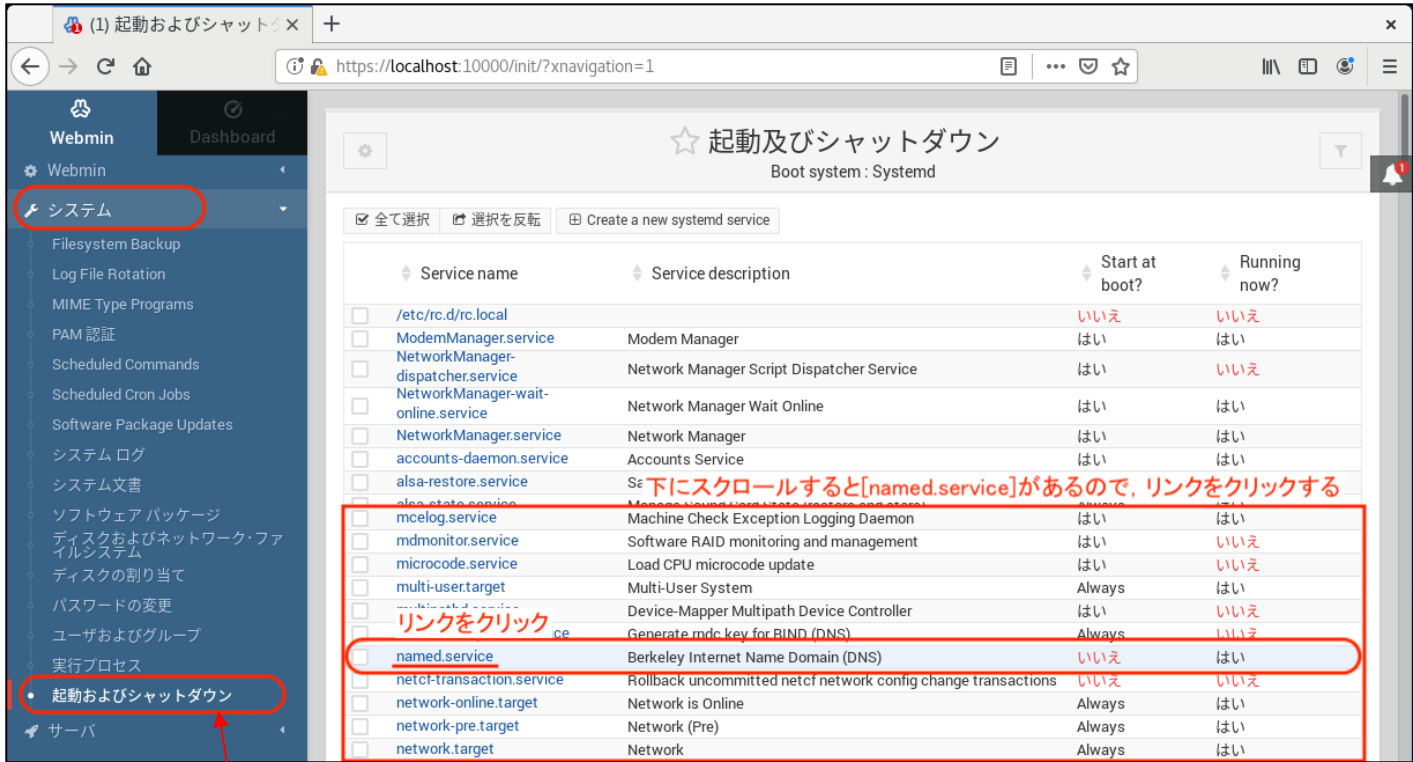


図13 設定が終わったら , 「**BIND DNSサーバ**」画面の[Start bind]ボタンを押す

起動時にDNSサーバが開始する設定

これまで設定したDNSサーバがOS起動時に自動的に開始する設定をしておきます。こうすることで、OSを再起動した場合など、手動でサーバ機能を開始する必要がなくなります。

Webminのインデックスページの「システム」タブを開き、その中にある「起動およびシャットダウン」の設定画面を開きます(図a01)。

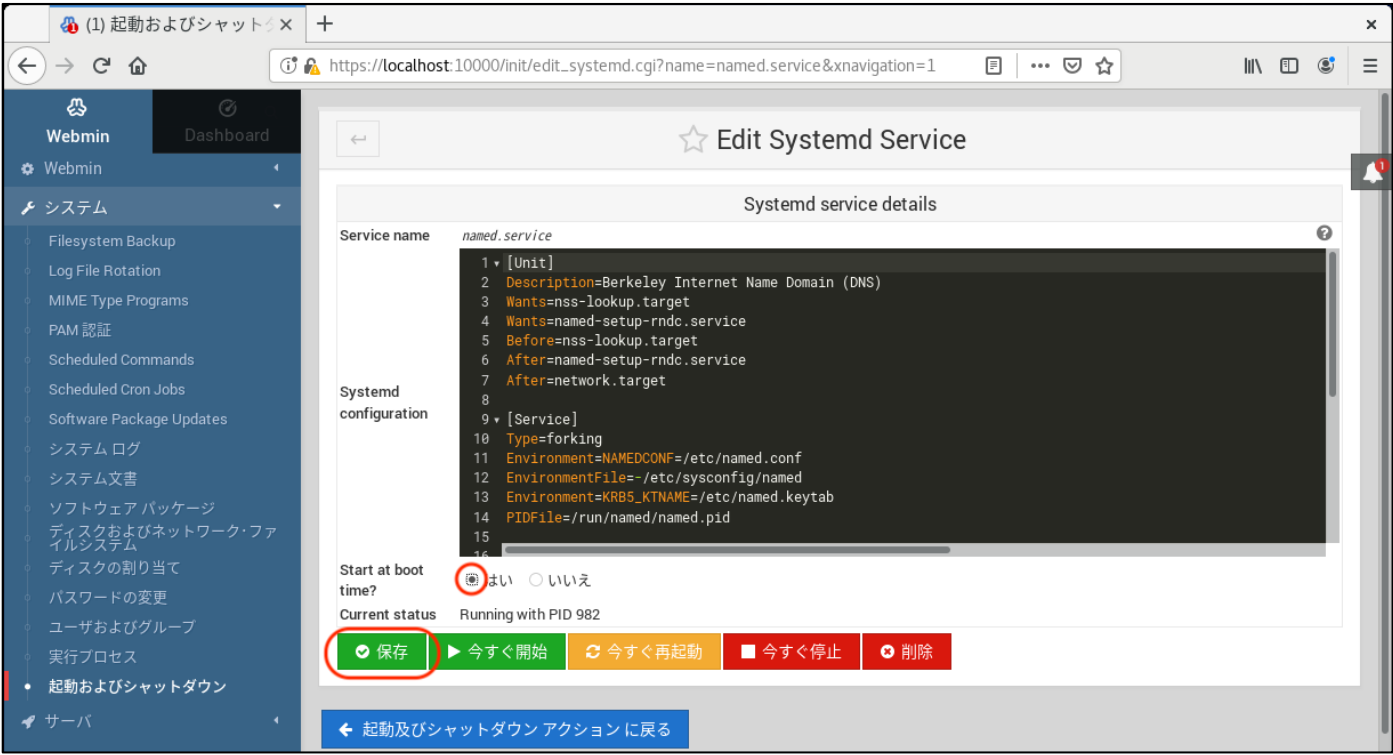


「Bootup and Shutdown」と表示される場合もあります

図a01 「起動およびシャットダウン」の設定画面を開く

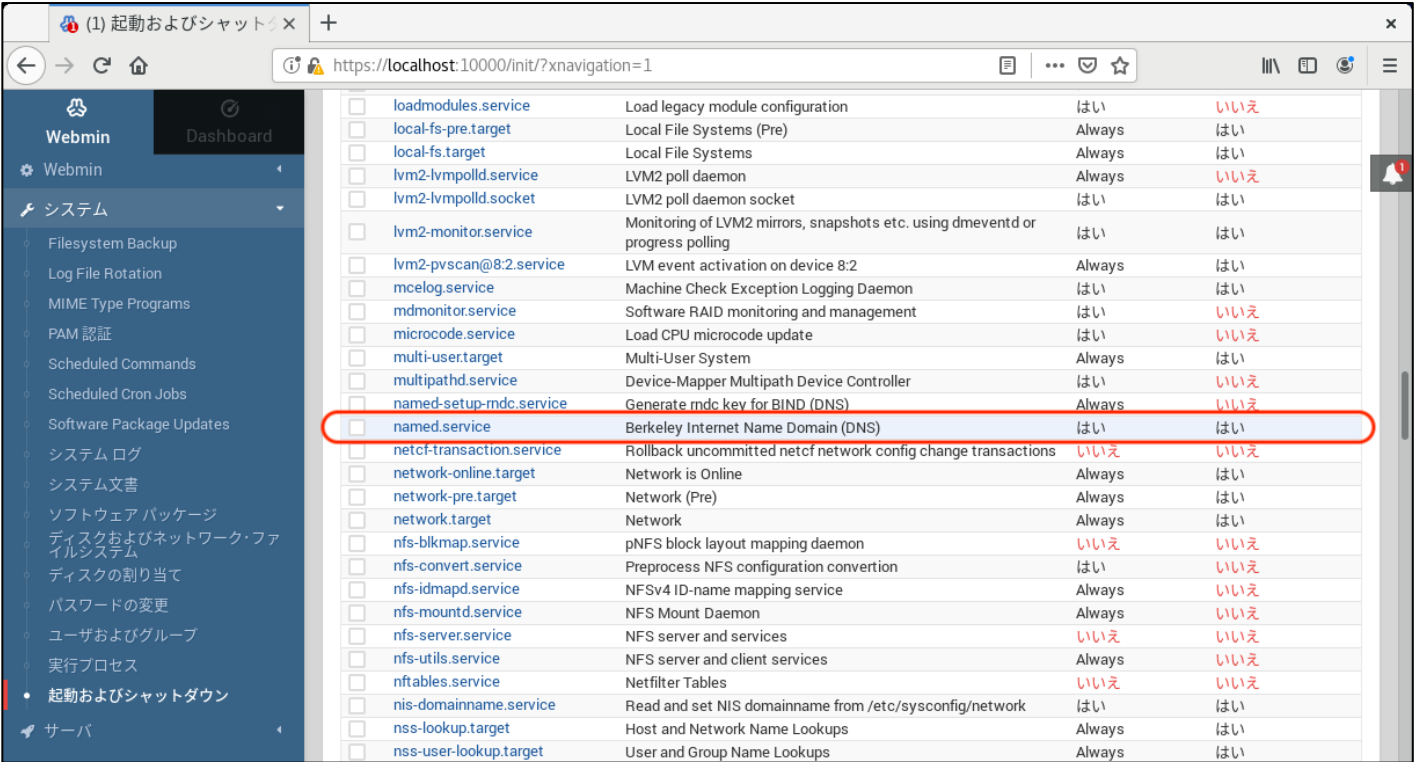
「Service name」が「named.service」となっている項目の「Start at boot?」が「いいえ」になっています。この設定を変更するため、「named.service」のリンクをクリックします。

すると、図a02の「アクションの編集」画面が表示されますので、「起動時に開始しますか？」で「はい」を選択して、「保存」ボタンを押します。



図a02 「起動時に開始しますか？」で「はい」を選択する

「起動およびシャットダウン」の設定画面で、named.serviceの「Start at boot?」が「はい」に変わりました。



図a04 named.serviceの「Start at boot?」が「はい」になった

外部からのアクセスを許可する

インストールしたままのCentOSでは，デフォルトでDNSの問い合わせを受け付けない設定になっているため，外部からのアクセスを許可しておく必要があります．[サーバ]-[BIND DNSサーバ]の[アドレスとトポロジ]および[ゾーン デフォルト]の設定画面から設定します．

※2つの設定が終了したら，画面右上の[変更を適用]ボタンを押します．



図15 ファイアウォール設定ツールの起動

[アドレスとトポロジ]画面(図16)では，[リッスン対象のポートとアドレス]の[アドレス]に，サーバのIPアドレスとして設定した「10.0.2.100」を追加します．(IPアドレスは空白で区切って入力します.) 入力したら[保存]ボタンを押します．



図16 アドレスとトポロジの設定画面

[ゾーン デフォルト]画面(図17)では，[ゾーンデフォルトの設定][次からのクエリーを許可]を，localhostから any に変更します．変更したら[保存]ボタンを押します．

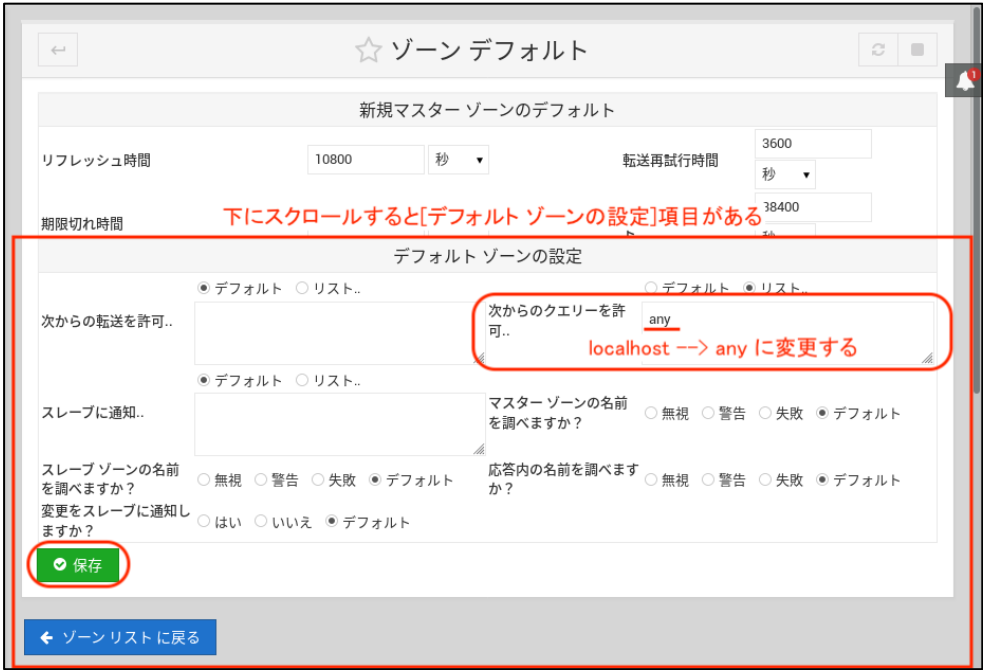


図17 ゾーンデフォルトの設定画面

2つの項目の設定が終わったら，図15の画面で[変更を適用]ボタンを押して，これらの変更を適用させるためサービスを再起動します．

※ファイアウォールの設定

CentOS自体が外部からのアクセスを受け付ける設定も変更しておきます．[端末]を開き，suコマンドで管理者に変更してから，下図のコマンドを実行します．

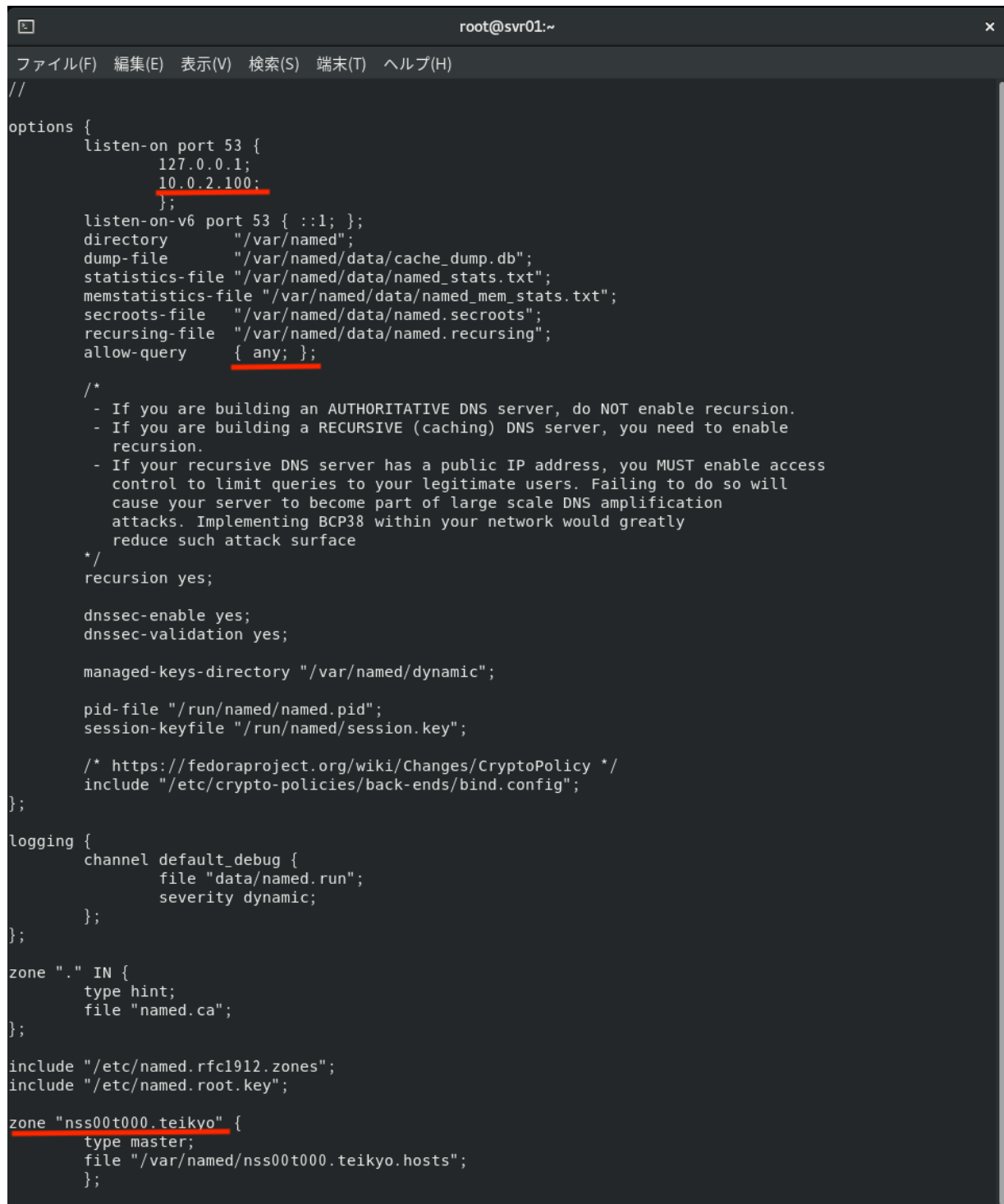
```
root@svr01:~
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)
[admin@svr01 ~]$ su -
パスワード:
[root@svr01 ~]# firewall-cmd --add-service=dns --zone=public --permanent
success
[root@svr01 ~]# firewall-cmd --reload
success
[root@svr01 ~]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client dns ssh
ports:
protocols:
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[root@svr01 ~]#
```

設定内容の確認

Webminで行ったDNSサーバの設定内容は、設定ファイルに保存されています。ここでは設定ファイルの内容を確認しておきます。今回設定した内容が保存されているのは、named.confファイルとnss00t000.teikyoゾーンのゾーンファイルです。ゾーンファイルはnss00t000.teikyo.hosts という名前で保存されます。

named.confファイル

Webmin上で「新規のマスタゾーンを作成」において設定した内容は、`/etc/named.conf` に保存されています。`named.conf` をviエディタで開いたものを図18に示します。(端末を開き、`su`コマンドで管理者に変更して、`vi /etc/named.conf` で開くことができます。)



```
root@svr01:~
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)
//
options {
    listen-on port 53 {
        127.0.0.1;
        10.0.2.100;
    };
    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 { any; };

    /*
     - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
     - If you are building a RECURSIVE (caching) DNS server, you need to enable
       recursion.
     - If your recursive DNS server has a public IP address, you MUST enable access
       control to limit queries to your legitimate users. Failing to do so will
       cause your server to become part of large scale DNS amplification
       attacks. Implementing BCP38 within your network would greatly
       reduce such attack surface
    */
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;

    managed-keys-directory "/var/named/dynamic";

    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";

    /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
    include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

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

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

zone "nss00t000.teikyo" {
    type master;
    file "/var/named/nss00t000.teikyo.hosts";
};
```

図18 named.confファイルの内容

この演習で作成したnamed.conf ファイルは、複数の項目からなります。named.confファイルでは、これらの項目を「ステートメント」と呼びます。1つめのステートメントは、optionsステートメントです。optionsステートメントでは、DNSサーバ全体の設定を行います。

また、optionsステートメントに続いて、zoneステートメントがあります。Zoneステートメントはゾーンごとに用意しますので、このnamed.confファイルには、先ほど作成したゾーン "nss00t000.teikyo" に関する設定が書かれています。zoneステートメントには次の2つのオプションが書かれています。

○ **zone**ステートメントのオプション

type :

DNSサーバのタイプを指定します。タイプには、master、slave、hintなどがあります。masterは、このゾーンを管理するマスタサーバ(プライマリサーバ)であることを示します。masterを指定した場合は、必ずzoneファイルの場所を指定し、ゾーンの情報を保持するゾーンファイルを作成しておく必要があります。slaveを指定した場合は、このゾーンのマスタサーバからゾーンの情報を受け取りゾーンの情報を保持するスレーブサーバとして動作します。hintを指定すると、このゾーンへの問い合わせについてはキャッシュだけを行います。

file :

ゾーンの情報を保持する、ゾーンファイル名を指定します。

[illegible]

図19のゾーンファイルには、4つの項目が記述されています。ゾーンファイルの項目のことを「レコード」といいます。図19にはSOAレコード、Aレコード、NSレコードとデフォルトのTTLがあります。

1行目の \$ttl 38400 はレコードではなく、デフォルトのTTL(Time To Live, 生存時間)を設定しています。TTLとは、キャッシュされたデータの有効期限です。この例では、TTLを38400秒(=10時間半くらい)に設定しています。この値は、各レコードのTTLのデフォルト値としてつかわれます。

図19の2行目～7行目まではSOA(Start Of Authority)レコードです。SOAレコードには管理するゾーンの情報記述されています。ドメイン名から、そのドメインを管理するホスト、管理者、シリアル番号などを保持しています。

図20にSOAレコードの各項目の意味を示します。

```
$ttl 3840 (1)ゾーン名 (2)マスタサーバ (3)管理者のメールアドレス
nss00t000.teikyo. IN SOA svr01.nss00t000.teikyo. 00t000xx.stu.teikyo-u.ac.jp. (
1594199234 ←(4)シリアル
10800 ←リフレッシュ
3600 ←リトライ
604800 ←破棄
38400 ) ←ネガティブTTL
```

図20 SOAレコードの各項目の意味

- (1)は「ゾーン名」です。ゾーン名の最後に"."(ドット)が付いていることに注意してください。ここでは、LANの中でだけ使うドメイン名としてnss00t000.teikyo.を指定しています。インターネットに公開する場合には、正式に取得したドメイン名を書きます。(たとえば帝京大学の場合は、teikyo-u.ac.jp.となります。)
- 次の「IN SOA」は、これがSOAレコードであることを表しています。INはInter Netの略で、インターネットで使うレコードであることを表しています。
- (2)は、マスタサーバのドメイン名です。ここではsvr01.nss00t000.teikyo.としています。これも最後に"."が付いていることに注意してください。
- (3)は、管理者のメールアドレスです。"(アットマーク)はゾーンファイルではゾーンの機転を表す記号としてつかわれますので、メールアドレスの"@"は"."(ドット)に置き換えて記述します。
- (4)以降の数値は、スレーブサーバを構築する際の設定です。この演習ではスレーブサーバを用意しないため関係ありません。
- 「シリアル番号」は、ゾーンデータのバージョンを表します。ゾーンの情報を更新したら、この番号を増やしておきます。「リフレッシュ」はスレーブサーバがデータを更新する間隔、「リトライ」は更新に失敗したときに、再度試すまでの間隔、「破棄」はゾーンデータを破棄するまでの間隔、「ネガティブTTL」は、ドメイン名が存在しなかったという情報を保持(ネガティブキャッシュ)する期間を表しています。

Aレコード

図19の9-11行目はA(Address)レコードです。このゾーンのホストのFQDNを定義して、ホストのFQDNとIPアドレスを関連付けます。図21にAレコードの各項目の意味を示します。

```
(1)FQDN (2)IPアドレス
svr01.nss00t000.teikyo. IN A 10.0.2.100
pc01.nss00t000.teikyo. IN A 10.0.2.121
pc02.nss00t000.teikyo. IN A 10.0.2.122
```

図21 Aレコードの各項目の意味

- 最初に(1)のFQDNを記述します。FQDNの最後が"."で終わっていることに注意してください。図21の例では、登録したホストのFQDNであるsvr01.nss00t000.teikyo.等が記述してあります。次の「IN A」はこれがAレコードであることを表しています。
- (2)に、FQDNに対応するIPアドレスを記述します。図21では、登録したIPアドレス10.0.2.100等が記述してあります。

NSレコード

図19の8行目はNS(Name Server)レコードです。このゾーンを管理するDNSサーバをしていします。NSレコードは、下位のゾーンを管理するDNSサーバを定義するために用いられます。インターネット上で再帰問い合わせをする場合は、NSレコードの情報から下位のドメインの情報を持つDNSサーバの情報を得ることになります。この演習では、下位のゾーンを作っていないので、このゾーンを管理するDNSサーバのレコードが1つだけ記述してあります。下位のゾーンがある場合などは、DNSサーバの数だけNSレコードを作成します。図22にNSレコードの各項目の意味を示します。

(1)ゾーン名			(2)ゾーンを管理するDNSサーバ
nss00t000.teikyo.	IN	NS	svr01.nss00t000.teikyo.

図22 NSレコードの各項目の意味

最初に(1)ゾーン名を記述します。ゾーン名の最後に"."が付いていることに注意してください。ここでは、作成したゾーン nss00t000.teikyo. が記述してあります。

次の「IN NS」はこれがNSレコードであることを表しています。

(2) に、(1)のゾーンを管理するDNSサーバのFQDNを記述します。ここでは、このサーバのFQDNである svr01.nss00t000.teikyo.が記述してあります。

DNSサーバの検証の概要

構築したDNSサーバが正しく利用できるか検証してみましょう。まず、構築したDNSサーバを利用するため環境のを整えます。DNSサーバは、LAN内の中の別のホストからこのサーバの管理するゾーンの名前解決を依頼されたら、名前解決をして結果を返す必要があります。また、サーバマシン自体から、自分の管理するゾーンの名前解決を行うために利用することもあります。したがって、DNSサーバ上からと、LAN内の別のホストから(※これは行いません)、DNSサーバが正しく動作しているかの検証を行います。

○DNSサーバ上からの検証

DNSサーバ上からの検証は、次の手順で行います。

1. まず、構築したDNSサーバを、登録したローカルのゾーンの名前解決に利用するように設定します。
2. 次に、BINDが起動しているかを検証します。
3. さらに、DNSサーバとして正しく動作しているかを検証します。

○[発展的な学習]LAN内の別のホストからの検証

LAN内の別のホストからの検証は、次の手順で行います。

1. まず、構築したDNSサーバを、登録したローカルのゾーンの名前解決に利用するように設定します。
2. 次に、DNSサーバとして正しく動作しているかを検証します。

DNSサーバを、登録したローカルのゾーンの名前解決に利用するように設定するには、NSS2の「5.2 Webminによるネットワークの設定」の「DNSクライアントの設定」で行います。

BINDが起動しているかどうかは、rndcコマンドで確認します。BINDの設定が正しく行われていない場合、BINDが起動しません

DNSサーバとして正しく動作しているかは、digコマンドを使って検証します。(nslookupコマンドでも検証できます。)

検証1：DNSサーバ上からの検証

次の手順でDNSサーバ上からの検証を行います。

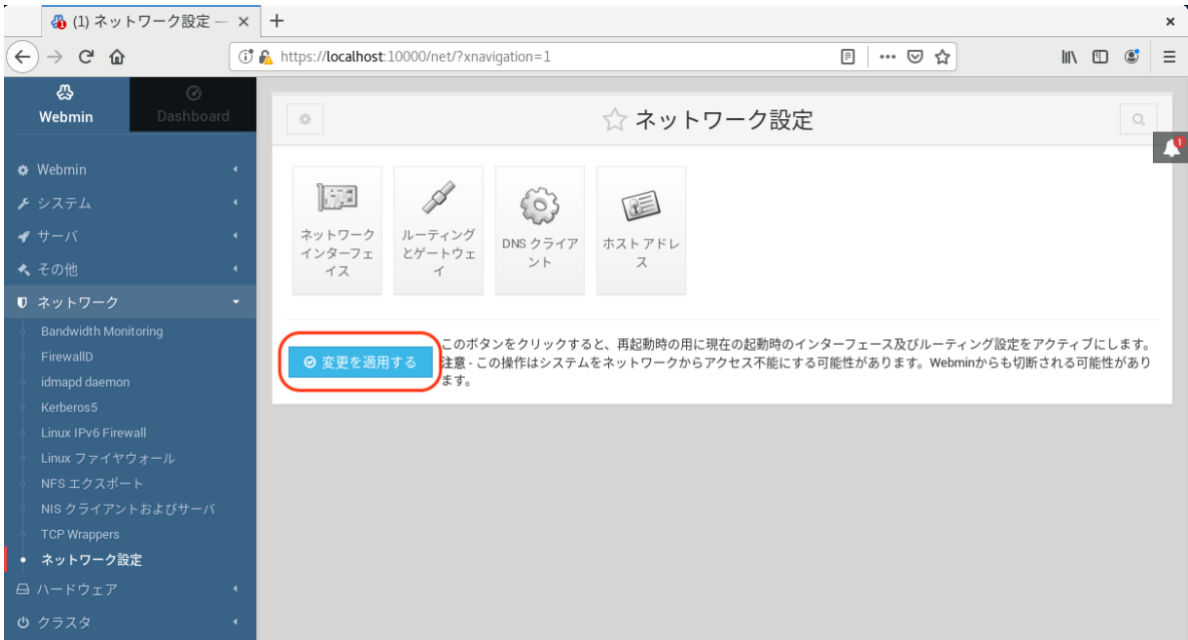
1. DNSクライアントの設定
2. BINDが起動しているかの検証
3. ローカルのゾーンの名前解決ができるかの検証

DNSクライアントの設定

DNSクライアントとしての設定は，NSS2の演習の「5.2 Webminによるネットワークの設定」において行いました．ここでも同じ手順で設定を行います．Webminのメイン画面の[ネットワーク]タブから，[ネットワーク設定]を開き，その中の[DNSクライアント]を開きます(図23)．ここでは，LANの中のゾーンに関しては構築したDNSサーバへ問い合わせを行い，インターネット上のホストに関しては，別のDNSサーバへ問い合わせを行うように設定します．図23のように，1つめのDNSサーバとしてこのサーバのIPアドレス(図22では10.0.2.100)を，2つめ以降のDNSサーバとして前に入れておいたDNSサーバのIPアドレス(図では8.8.8.8と157.102.5.2)を入力します．入力が終わったら[保存]ボタンを押して設定を保存します．そのあと，「ネットワークの設定」画面で[変更を適用する]ボタンを押すのを忘れないでください．



図23 このサーバのDNSクライアントの設定



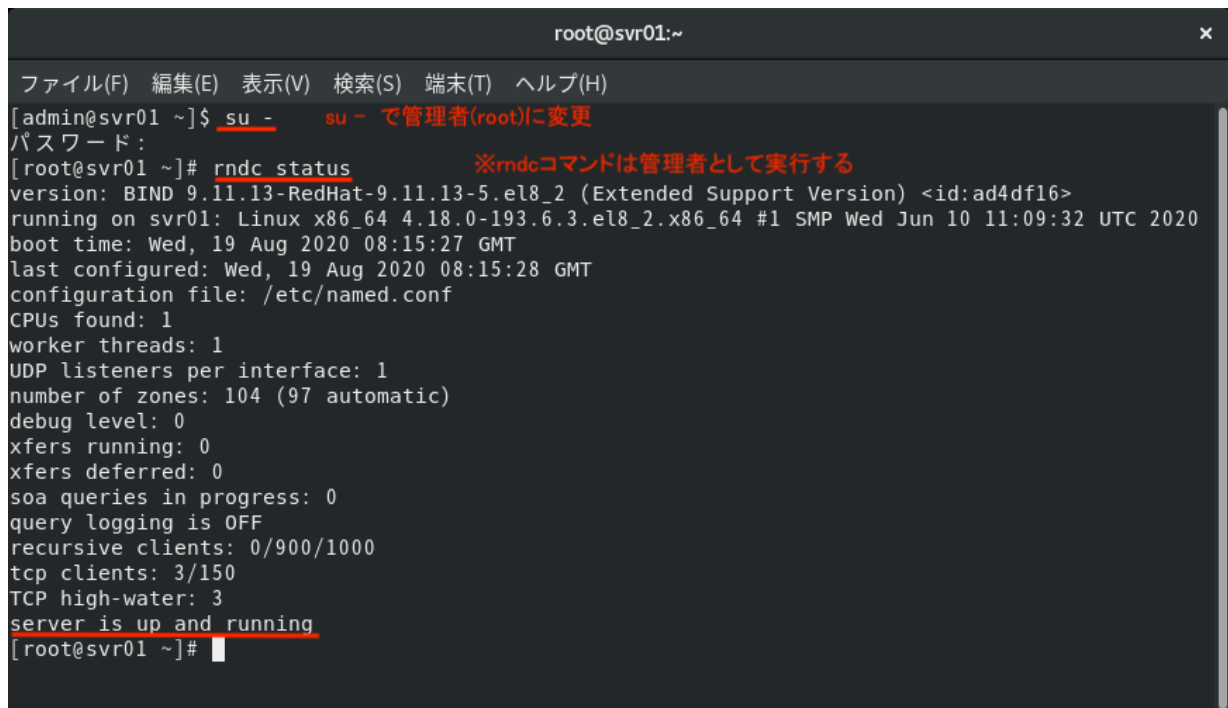
BINDが起動しているかの検証

BINDは設定が間違っていると起動しません。rndcコマンドでBINDが起動しているかどうか検証します。GNOME端末などのプロンプトから次のように入力してEnterキーを押します。

※rndcコマンドは管理者として実行する必要があります。

```
rndc status
```

rndcコマンドの実行例を図24に示します。



```
root@svr01:~
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)
[admin@svr01 ~]$ su -      su - で管理者(root)に変更
パスワード:
[root@svr01 ~]# rndc status      ※rndcコマンドは管理者として実行する
version: BIND 9.11.13-RedHat-9.11.13-5.el8_2 (Extended Support Version) <id:ad4df16>
running on svr01: Linux x86_64 4.18.0-193.6.3.el8_2.x86_64 #1 SMP Wed Jun 10 11:09:32 UTC 2020
boot time: Wed, 19 Aug 2020 08:15:27 GMT
last configured: Wed, 19 Aug 2020 08:15:28 GMT
configuration file: /etc/named.conf
CPUs found: 1
worker threads: 1
UDP listeners per interface: 1
number of zones: 104 (97 automatic)
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/900/1000
tcp clients: 3/150
TCP high-water: 3
server is up and running
[root@svr01 ~]#
```

図24 rndcコマンドの実行結果

最後に“server is up and running”と表示されていれば、BINDは起動しています。

(※BINDが起動していなければ、“connection failed”、“connection refused”などのメッセージが表示されます。)

ローカルのゾーンの名前解決ができるかの検証

BINDが起動していることが確認出来たら，次はDNSとして正しく動作しているかを調べます．ここでは，DNSにローカルのゾーンに登録したホストの名前解決を依頼して，正しい結果が返ってくるかなどを調べます．DNSサーバへの問い合わせには，「dig」を用います．dig (domain information groper，groperは手探りで探すという意味)の使い方は次のとおりです．

```
dig [@問い合わせ先サーバ] ドメイン名 [レコードタイプ] [+クエリオプション]
```

※digコマンドにはこのほかにもオプションがありますが，この演習では扱いません．)

たとえば，digコマンドで wsa.nss-01 というホストのIPアドレスを問い合わせるには次のように書きます．

```
dig @10.0.2.100 pc01.nss00t000.teikyo +nored
```

オプションの詳細は次のとおりです．

○@問い合わせ先サーバ

問い合わせ先のサーバのドメイン名あるいはIPアドレスを，@(アットマーク)を頭につけて指定します．ここで構築したサーバをDNSサーバとして指定しますので，構築したサーバのIPアドレスかドメイン名を指定します．(上の例では，IPアドレスを"@10.0.2.100"と指定しています．) この記述を省略すると，resolv.conf で設定されているDNSサーバに問い合わせを行います．

○ドメイン名

問い合わせるドメイン名を指定します．上の例では，登録した"pc01.nss00t000.teikyo"を指定しています．(※IPアドレスからドメイン名を問い合わせる逆引きをする場合は，ドメイン名の代わりに -x IPアドレス とします．)

○レコードタイプ

ゾーンファイルに記録されているどのレコードを問い合わせるかを指定します．上の例では省略していますが，省略した場合はAレコードあるいはCNAMEレコードを問い合わせます．

(※CNAMEレコードは，既存のドメイン名に対して別名を定義するためのレコードですが，ここでは説明は省略します．)

○+クエリオプション

問い合わせの際のオプションを指定します．上の例では，問い合わせたサーバで解決できなくても再

LAN内のホストからローカルのゾーンの名前解決ができるかの検証

帰問い合わせは行わないように “+norec” というオプションを設定しています。

上の例のように dig コマンドを実行した結果を図25に示します。(Aレコードの問い合わせであることを明示して “dig @10.0.2.100 pc01.nss00t000.teikyo A +norec” としても同じ結果が得られます。

```
admin@svr01:~
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)

[admin@svr01 ~]$ dig @10.0.2.100 pc01.nss00t000.teikyo +norec

; <<>> DiG 9.11.13-RedHat-9.11.13-5.el8_2 <<>> @10.0.2.100 pc01.nss00t000.teikyo +norec
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45317
; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 04862ceabd943778f0d5c3935f068748e1d41c8f448e12d4 (good)
;; QUESTION SECTION:
pc01.nss00t000.teikyo.      IN      A

;; ANSWER SECTION:
pc01.nss00t000.teikyo. 38400 IN      A      10.0.2.121
;; AUTHORITY SECTION:
nss00t000.teikyo.      38400 IN      NS      svr01.nss00t000.teikyo.
;; ADDITIONAL SECTION:
svr01.nss00t000.teikyo. 38400 IN      A      10.0.2.100

;; Query time: 0 msec
;; SERVER: 10.0.2.100#53(10.0.2.100)
;; WHEN: 木 7月 09 11:56:08 JST 2020
;; MSG SIZE rcvd: 130

[admin@svr01 ~]$
```

図25 digコマンドでDNSサーバにpc01.nss00t000.teikyoの名前解決を
問い合わせた結果

digコマンドの実行結果を、注目すべきところだけ抜き出してみています。

- 1. まず，“status”が“NOERROR”の場合は，正常に応答しています。ここが“NODOMAIN”の場合は，問い合わせたドメインが見つからなかったということになります。
- 2. “ANSWER SECTION”は問い合わせの結果です。pc01.nss00t000.teikyoのIPアドレス10.0.2.121 を得ることができていますので，正しく動作しています。
- 3. “AUTHORITY” は問い合わせたゾーンを管理しているDNSサーバ(ゾーンファイルのNSレコード)を返します。ゾーンファイルのNSレコードと同じ内容が得られていますので，正しく動作しています。

次に，NSレコードを問い合わせます。NSレコードの問い合わせでは，nss00t000.teikyoドメインを管理しているDNSサーバを問い合わせるので，ドメイン名としてnss00t000.teikyoを指定します。また，NSレコードの問い合わせなのでレコードタイプに“NS”を指定します。プロンプトから次のように入力してEnterキーを押します。

```
dig @10.0.2.100 nss00t000.teikyo NS +norec
```

LAN内のホストからローカルのゾーンの名前解決ができるかの検証

NSレコードを問い合わせた結果を図26に示します。

```
admin@svr01:~  
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)  
[admin@svr01 ~]$ dig @10.0.2.100 nss00t000.teikyo NS +norec  
;<<> DiG 9.11.13-RedHat-9.11.13-5.el8_2 <<> @10.0.2.100 nss00t000.teikyo NS +norec  
; (1 server found)  
; global options: +cmd  
; Got answer:  
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57271  
; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2  
;<<> OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 4096  
; COOKIE: 971a43ealb72c4aa5ba65205f0687730907eaa04d4885bd (good)  
; QUESTION SECTION:  
; nss00t000.teikyo. IN NS  
;<<> ANSWER SECTION:  
; nss00t000.teikyo. 38400 IN NS svr01.nss00t000.teikyo.  
;<<> ADDITIONAL SECTION:  
; svr01.nss00t000.teikyo. 38400 IN A 10.0.2.100  
;<<> Query time: 3 msec  
;<<> SERVER: 10.0.2.100#53(10.0.2.100)  
;<<> WHEN: 木 7月 09 11:56:51 JST 2020  
;<<> MSG SIZE rcvd: 109  
[admin@svr01 ~]$
```

図26 digコマンドでNSレコードを問い合わせた結果

ANSWER SECTIONにNSレコードが得られていますので，正しく動作しています。

※これらの検証は，digコマンドの代わりにnslookupコマンドを使っても行うことができます。Windowsのコマンドプロンプトから検証する場合は，nslookupコマンドを使います。nslookupコマンドの使い方は，次のとおりです。

```
nslookup [-type=レコードタイプ] ドメイン名 [DNSサーバ]
```

DNSサーバ(10.0.2.100)にpc01.nss00t000.teikyo の名前解決を問い合わせるには次のように書きます。Aレコードの問い合わせの場合はレコードタイプを省略できます。

```
nslookup pc01.nss00t000.teikyo 10.0.2.100
```

また，NSレコードの問い合わせは次のように書きます。

```
nslookup -type=NS nss00t000.teikyo 10.0.2.100
```

nslookupコマンドの実行結果を図27に示します。pc01.nss00t000.teikyoのIPアドレスと，nss00t000.teikyoドメインのネームサーバのドメイン名が取得できています。


```
admin@svr01:~
ファイル(F) 編集(E) 表示(V) 検索(S) 端末(T) ヘルプ(H)
[admin@svr01 ~]$ nslookup pc01.nss00t000.teikyo 10.0.2.100
Server:      10.0.2.100
Address:     10.0.2.100#53

Name:   pc01.nss00t000.teikyo
Address: 10.0.2.121

[admin@svr01 ~]$ nslookup -type=NS nss00t000.teikyo 10.0.2.100
Server:      10.0.2.100
Address:     10.0.2.100#53

nss00t000.teikyo      nameserver = svr01.nss00t000.teikyo.

[admin@svr01 ~]$
```

図27 nslookupコマンドの実行結果