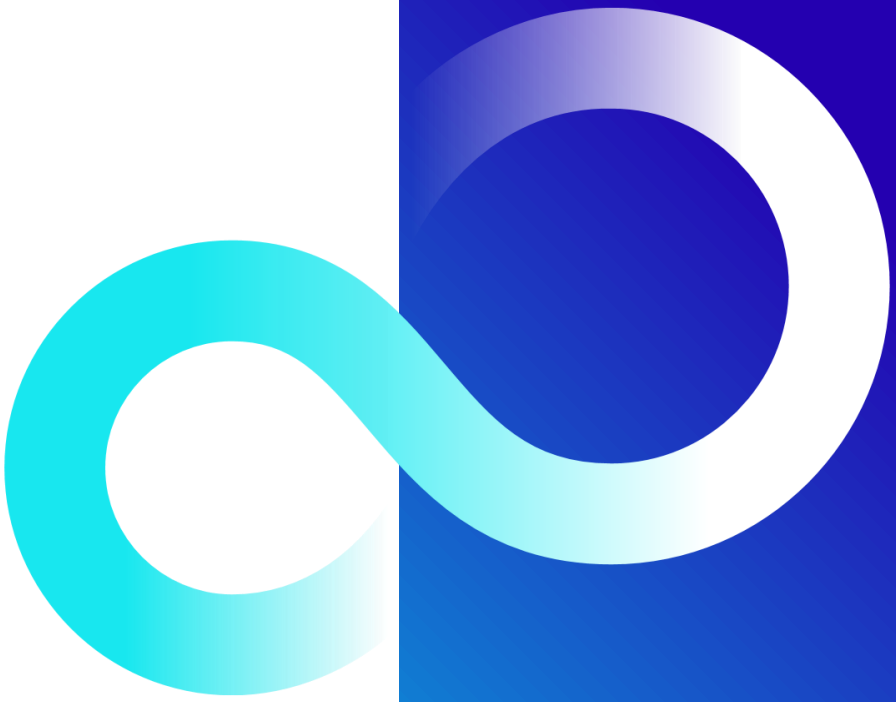
FUJITSU

Oracle Solaris DNS サーバ構築手順書 -BIND の利用-



2018 年 4 月

第 2.0 版

富士通株式会社

■使用条件

- 著作権・商標権・その他の知的財産権について

  コンテンツ（文書・画像・音声等）は、著作権・商標権・その他の知的財産権で保護されています。

  本コンテンツは、個人的に使用する範囲でプリントアウトまたはダウンロードできます。ただし、これ以外の利用（ご自分のページへの再利用や他のサーバへのアップロード等）については、当社または権利者の許諾が必要となります。
- 保証の制限

  本コンテンツについて、当社は、その正確性、商品性、ご利用目的への適合性等に関して保証するものではなく、そのご利用により生じた損害について、当社は法律上のいかなる責任も負いかねます。本コンテンツは、予告なく変更・廃止されることがあります。
- 輸出または提供

  本製品を輸出又は提供する場合は、外国為替及び外国貿易法及び米国輸出管理関連法規等の規制をご確認の上、必要な手続きをおとりください。

■商標について

- UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。
- SPARC Enterprise、SPARC64 およびすべての SPARC 商標は、米国 SPARC International, Inc.のライセンスを受けて使用している、同社の米国およびその他の国における商標または登録商標です。
- Oracle と Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- その他各種製品名は、各社の製品名称、商標または登録商標です。

はじめに

本書の内容

- 本書は、Oracle Solaris 11 に標準でインストールされている、BIND を使用した DNS サーバの構築手順を記載しています。
- Oracle Solaris 11 の詳細については、以下の URL をご参照ください。
  - Oracle Solaris 11.3 Information Library
    https://docs.oracle.com/cd/E62101_01/
  - Oracle Solaris 11 を使ってみよう
    http://www.fujitsu.com/jp/sparc-technical/document/solaris/#os

留意事項

- 本書は、Oracle Solaris 11.3 の機能を基に作成しています。
- 本書に記載の設定値（ホスト名、IP アドレスなど）は参考例です。実際のシステム環境に応じて読み替えてください。

本書での表記

- 本書では、以下の用語は略称を用いて表記する場合があります。

略称	正式名称
Solaris	Oracle Solaris

- 本書では、コマンドの実行環境によって以下のプロンプト表記を使用しています。

実行環境	プロンプト
DNS サーバ（マスタ）	Master#
DNS サーバ（スレーブ）	Slave#
クライアント	Client#

検証環境

- 本書は以下の環境を使用した手順を記載しています。記載の手順やコマンドの実行結果については環境によって異なる場合があります。

DNS サーバ	
サーバ	SPARC M10-1
OS	Oracle Solaris 11.3
SRU	SRU17101（SRU11.3.25.3.0）
BIND	BIND 9.6-ESV-R11-S10
クライアント	
サーバ	SPARC Enterprise T5120
OS	Oracle Solaris 11.3

目次

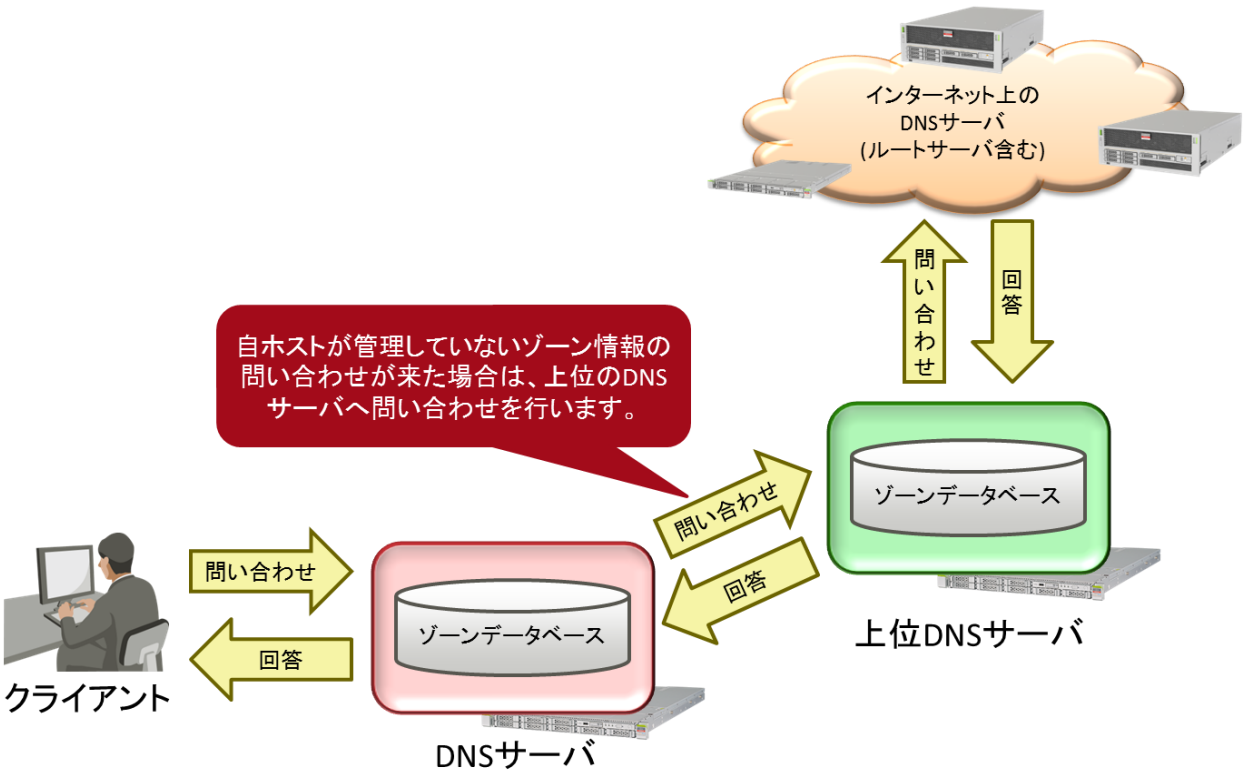
1. DNS サーバの概要

1.1. DNS（Domain Name System）とは

自ホストが管理するネットワークに接続されたコンピュータのホスト（ドメイン）名と IP アドレスの対応表を持ち、外部からの名前解決の問い合わせに応答するシステムです。

1.1.1. DNS サーバの名前解決

DNS サーバは、自ホストが管理する範囲（ゾーン）の情報をゾーンデータベースで管理します。ゾーンデータベースには、IP アドレスとホスト名のマッピング情報が記載されており、クライアントからの要求に対して、自ホストが管理しているゾーンの情報であれば名前解決を行いその回答を返します。自ホストが管理していないゾーン情報が要求された場合は、上位 DNS サーバへ問い合わせを行い、その結果をクライアントへ返します。



☛ ルートサーバとは、DNS においてドメイン名の最上位（com や jp など）の情報を保持するサーバです。自分自身で解決できないインターネット上のドメイン名などの名前解決時に最初に問い合わせます。

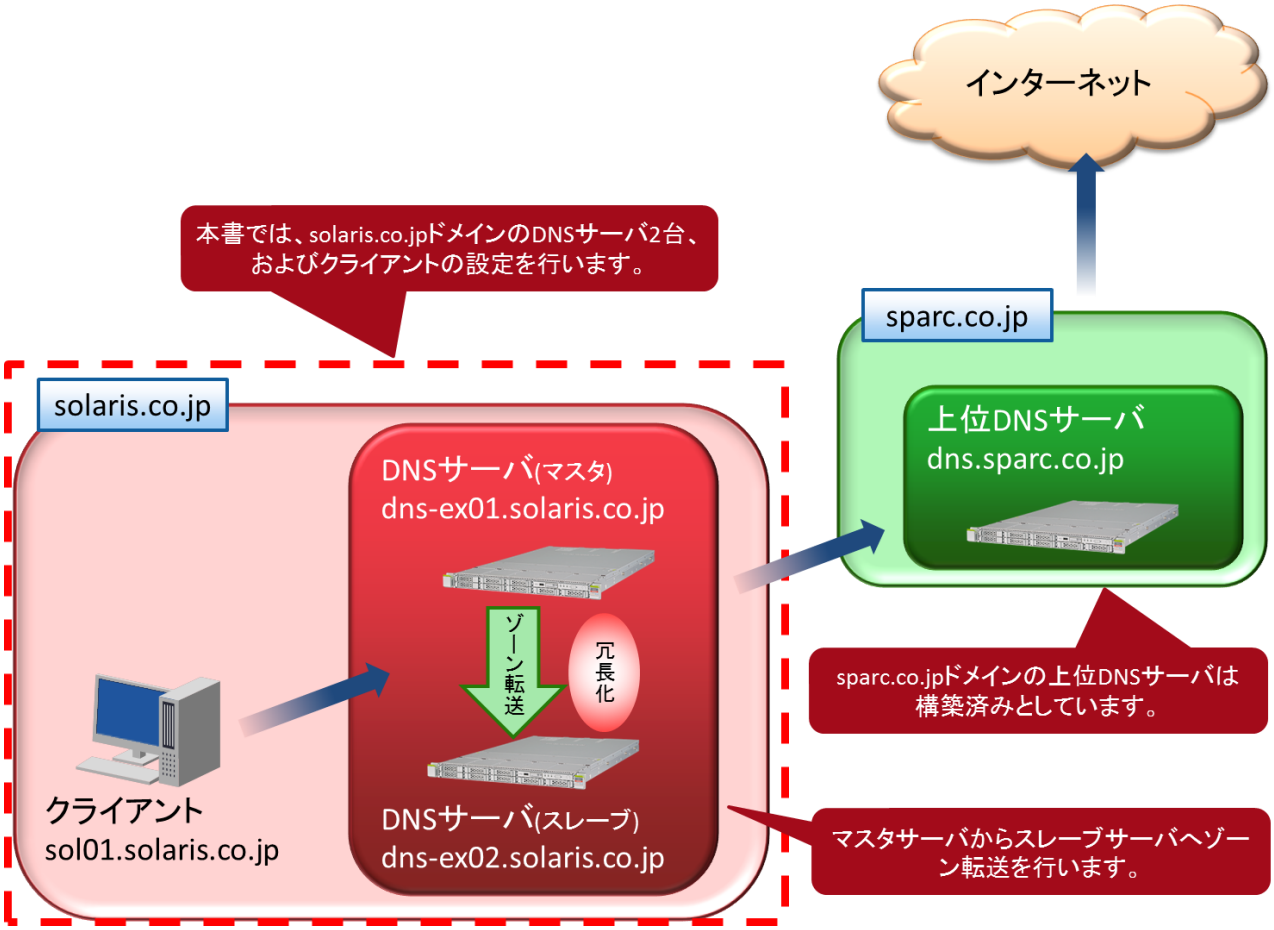
2. 本書での環境

2.1. 本書で構築する DNS サーバの構成

本書で構築する DNS サーバの構成を説明します。

- 上位 DNS サーバは構築済みとします。
- 構築するのは、DNS サーバ 2 台（マスタ／スレーブ）とクライアント 1 台の計 3 台です。
  マスタサーバと同じゾーン情報を持つサーバをもう 1 台作成し、DNS サーバの冗長化を行います。
- キャッシュサーバは使用しません。

☞ キャッシュサーバとは、自らにゾーンデータベースを持たず、クライアントからの問い合わせに対してはほかの DNS サーバへ問い合わせて、結果を返すサーバです。また、その結果はキャッシュとしてサーバ内部に蓄積し、同じ問い合わせが来た場合には、キャッシュから結果を返します。



オリジナルのゾーン情報を持っているサーバを「マスタサーバ」、ゾーン情報をマスタサーバから複製して使用するサーバを「スレーブサーバ」と呼びます。
なお、クライアント側から見た場合は、どちらのサーバも DNS としての動作に違いはありません。

役割	ホスト名	IP アドレス	ドメイン名	備考
上位 DNS サーバ	dns	192.168.100.10/24	sparc.co.jp	本書では構築済みとします。
DNS サーバ(マスタ)	dns-ex01	192.168.200.10/24	solaris.co.jp	3 章参照
DNS サーバ(スレーブ)	dns-ex02	192.168.200.11/24		5 章参照
クライアント	sol01	192.168.200.12/24		4 章参照

2.2. 構築前の環境確認

環境の構築前に本書で使用する DNS サーバ(マスタおよびスレーブ)環境の確認を行います。

1) ログイン

マスタとスレーブ、それぞれのサーバにログインします。

```
login:
```

☛ 本章では、すべて両方のサーバで操作します。

2) root 権限の切替

```
$ su -
```

☛ 本章では、すべて root 権限で操作します。

☛ 以降では、マスタサーバにログインした例で説明します。

3) Solaris 11 の OS バージョンを確認する

```
Master# cat /etc/release
                            Oracle Solaris 11.3 SPARC
     Copyright (c) 1983, 2016, Oracle and/or its affiliates.  All rights reserved.
                            Assembled 03 August 2016
```

4) BIND のパッケージのインストール状態を確認する

```
Master# pkg info pkg:/service/network/dns/bind
                名前: service/network/dns/bind
            サマリー: BIND DNS name server and configuration tools.
                説明: BIND is open source software that implements the Domain
                      Name System (DNS) protocols for the Internet.  This
                      package contains the DNS server 'named' and tools used
                      to setup and validate configuration.
            カテゴリ: System/Services
                状態: インストール済み
      パブリッシャー: solaris
          バージョン: 9.6.3.11.10 (9.6-ESV-R11-S10)
      ビルドリリース: 5.11
                分岐: 0.175.3.17.0.3.0
  パッケージ化の日付: 2017 年 01 月 31 日  23 時 42 分 40 秒
            サイズ: 2.78 MB
```



```
                  FMRI: pkg://solaris/service/network/dns/bind@9.6.3.11.10,5.11-0.17
5.3.17.0.3.0:20170131T234240Z
```

☛ BIND のパッケージがインストールされていない場合は、pkg install コマンドで適用してください。

5) BIND のバージョンを確認する

```
Master# /usr/sbin/named -v
BIND 9.6-ESV-R11-S10
```

☛ Solaris 11.3 SRU17101(SRU11.3.25.3.0)では、上記のバージョンのパッケージがインストールされています。

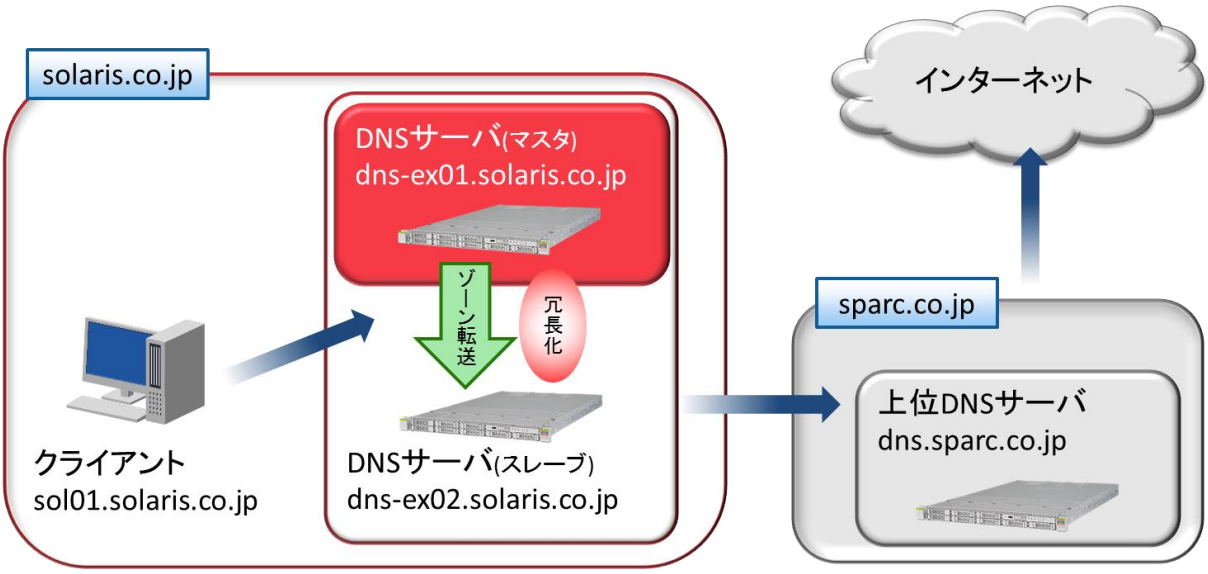
6) named サービスの状態を確認する

```
Master# svcs svc:/network/dns/server:default
STATE          STIME    FMRI
disabled       11:13:11 svc:/network/dns/server:default
```

☛ サービスの初期状態は disabled です。

☛ named サービスが enable の場合は、disabled に変更してください。

3. DNS サーバ(マスタ)の構築



DNS のサービスである named は、起動時に構成ファイル(/etc/named.conf)を読み込み、記載された情報に従って動作します。

DNS サービスを利用するには、構成ファイルに加えてゾーンファイル、ルートキャッシュファイルが必要になります。

各ファイルはデフォルトでは存在しないため、手動で作成する必要があります。

本書で作成するファイルは全部で以下の 6 ファイルです。

項番	ファイル	役割	配置先
1	構成ファイル	DNS の構成情報を記載	/etc/named.conf
2	ゾーンファイル	正引き用ファイル	任意
3		逆引き用ファイル	
4		ループバック正引き用ファイル	
5		ループバック逆引き用ファイル	
6	ルートキャッシュファイル	ルートサーバの情報を記載	

- **構成ファイル** (/etc/named.conf)

  DNS の構成情報を記載しており、ゾーンファイルやルートキャッシュファイルの配置先ディレクトリの情報などを記載しています。

- **ゾーンファイル**
  名前解決を行うために必要なゾーンに関する情報が記載されたファイルです。ゾーンファイルは複数あり、環境にあわせて、必要なゾーンファイルを用意します。なお、構成ファイル内に配置するゾーンファイルの任意のディレクトリとファイル名を記載する必要があります。
- **ルートキャッシュファイル**
  クライアントの問い合わせに対して自分自身で解決できなかった場合に、最初に問い合わせを行うサーバ（ルートサーバ）の情報を定義するファイルです。構成ファイル内に配置する任意のディレクトリとファイル名を記載する必要があります。
  ルートキャッシュファイルは、手動で作成するか、以下のいずれかの URL から入手可能です。
  - ftp://rs.internic.net/domain/named.root
  - ftp://ftp.nic.ad.jp/internet/rs.internic.net/domain/named.root

3.1. DNS の構成情報の設定

3.1.1. 構成ファイルのオプション／ステートメント

構成ファイル内では、様々なオプションやステートメントが使用可能です。
以下に代表的なものを記載します。

オプション	意味
directory	ネームサーバのワーキングディレクトリ（ゾーンファイルなどの格納先）の絶対パスを指定します。
forwarders	指定した DNS サーバへ問い合わせを回送します（上位サーバの指定）。
forward only | first ※設定を省略した場合は、first の動作になります。	forwarders 設定時の転送方法を指定します。 「only」を指定すると、フォワーダーから有効な回答が得られない場合は、問い合わせそのものが失敗します。 「first」を指定すると、フォワーダーから有効な回答が得られない場合は、フォワーダー以外の DNS サーバへ問い合わせを繰り返します。

☞ 自分自身で解決できない名前解決を受け付けた場合には、通常はルートサーバから名前解決を図りますが、forwarders で上位サーバを指定していれば、上位サーバへ問い合わせを回送する動作になります。

ステートメント		意味
type		ゾーンファイルのタイプを指定します。
	master	マスタサーバであることを表します。
	slave	スレーブサーバであることを表します。
	hint	ルートサーバであることを表します。
file		ゾーンファイルのファイル名を指定します。

3.1.2. 構成ファイルの作成

1) 構成ファイルを新規作成する

```
Master# vi /etc/named.conf
```

（記載例）

```
options{
        directory       "/var/named";           //ゾーンファイルの配置先
        forwarders      { 192.168.100.10;       //上位 DNS サーバの IP アドレス指定
        };
};

zone "solaris.co.jp"{                           //正引きファイルの指定
        type    master;
        file    "named.zone";
};

zone "200.168.192.in-addr.arpa"{                //逆引きファイルの指定
        type    master;
        file    "named.rev";
};

zone "localhost"{                               //ループバック正引きファイルの指定
        type    master;
        file    "localhost.zone";
};

zone "0.0.127.in-addr.arpa"{                    //ループバック逆引きファイルの指定
        type    master;
        file    "localhost.rev";
};

zone "."{                                       //ルートキャッシュファイルの指定
        type    hint;
        file    "named.root";
};
```

- ☛ それぞれのファイル名に規則はありませんので、任意に指定が可能です。本書では上記のとおりとしています。
- ☛ /var/named フォルダ配下に各ファイルを格納する設定としています。
- ☛ 正引きとは、ドメイン名から IP アドレスを解決することをいいます。正引きゾーンを宣言するには、「zone "ドメイン名"」で行います。
- ☛ 逆引きとは、IP アドレスからドメイン名を解決することをいいます。逆引きゾーンを宣言するには、IP アドレスを逆に並べて、逆引きゾーンを表すサブドメイン名「in-addr.arpa」をつけます。上記例では、「zone"200.168.192.in-addr.arpa"」としていますが、これは、192.168.200.0/24 の逆引きゾーンであることを示しています（/24 は省略されている）。
- ☛ ループバックとは、自分自身が動作させている DNS へ接続し、正しく動作するか確認することをいいます。宣言方法は、正引きゾーンおよび逆引きゾーンと同様です。自分自身を設定するため、宣言はドメイン名「localhost」、IP アドレス「127.0.0.1/24」で行います（指定は.1/24 を省略します）。

（参考）IPv6 を定義する場合

```
options{
        directory       "/var/named";
};

zone "solaris.co.jp"{                                           //正引き
        type    master;
        file    "named.zone";
};

zone "2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa"{          //逆引き
        type    master;
        file    "named.rev";
};

zone "localhost"{                                               //ループバック正引き
        type    master;
        file    "localhost.zone";
};

zone " 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa"{
                                                                //ループバック逆引き
        type    master;
        file    "localhost.rev";
};

--<省略>--
```

- ☛ 正引きの指定は、ループバック含めて IPv4 と同じです。
- ☛ 逆引きの場合は、IP アドレスを省略しない形で逆に並べて、1 文字ごとにドットで区切ります。そして、逆引きゾーンを示す.ip6.arpa をつけます。
  逆引きについては、/64 のプレフィックスで記載しています。ループバック逆引きはすべて記載しています。

3.2. ゾーンファイル（ゾーンデータベース）の作成

3.2.1. ゾーンファイルの各レコード

- ゾーンファイル内に記載可能な主なレコード

リソースレコード	定義する情報
SOA	ゾーンの管理情報
A	ホスト名に対する IPv4 アドレス
PTR	IP アドレスに対するホスト名
NS	ドメインのネームサーバ名
CNAME	ホストの別名
MX	ドメインのメールサーバ名
AAAA	ホスト名に対する IPv6 アドレス

- SOA レコードに記載する設定

  ゾーンの管理情報であるSOAレコードには以下の設定を行います。主に、スレーブサーバを構築した際に、スレーブサーバ側から参照する設定です。

SOA レコード	定義する情報
Serial	ゾーン情報のバージョンを確認するための値（10 桁）を表します。 値が大きくなることで、スレーブサーバはマスタサーバのゾーン情報に変更があったことを認識します。 本書では、「西暦+月+日+2 桁の数字」を組み合わせた値を使用します。
Refresh	スレーブサーバがマスタサーバのデータ更新を確認する間隔を表します。
Retry	スレーブサーバがマスタサーバのデータ更新に失敗した場合の再試行する間隔を表します。
Expire	スレーブサーバがマスタサーバと一定期間データ更新が行えなかった場合、保持しているデータを無効化する期限を表します。
Minimum	ネガティブキャッシュの最小生存時間を表します。

☛ ゾーンファイルを変更した場合は、Serial の値を大きくする必要があります。それによりスレーブサーバがマスタサーバのゾーン情報に変更があったことを認識します。

☛ ネガティブキャッシュとは、問い合わせ対象が存在しなかった場合に保持したキャッシュのことです。

その他のゾーンファイル内に表記する内容です。

	意味
$TTL	デフォルトのキャッシュ有効時間を指定します。
;	セミコロンから行末まではコメントになります。
IN	IN の後ろに記載したレコードが、インターネットで使用するレコードであることを定義します。
@	そのファイルが設定するドメイン名を表します。

3.2.2. 正引き用ゾーンファイルの作成

1) 各ゾーンファイルを配置するディレクトリを作成する

```
Master# mkdir -p /var/named
```

☛ 配置先は、構成ファイル内の directory に記載した場所を指定します。

2) 正引き用ゾーンファイルを作成する

```
Master# vi /var/named/named.zone
```

☛ ファイル名は、構成ファイルに記載した名称（本書では named.zone）にします。

（記載例）

```
$TTL 3600
@       IN      SOA     dns-ex01.solaris.co.jp.  root.mail.solaris.co.jp.(
                2017011501              ;Serial
                10800                   ;Refresh
                3600                    ;Retry
                604800                  ;Expire
                86400 )                  ;Minimum
;
;-------------------------------------------------------
                IN      NS      dns-ex01.solaris.co.jp.         ;マスタサーバ
                IN      NS      dns-ex02.solaris.co.jp.         ;スレーブサーバ
dns-ex01        IN      A       192.168.200.10
dns-ex02        IN      A       192.168.200.11
sol01           IN      A       192.168.200.12
```

☛ SOA レコードの Refresh、Retry、Expire、Minimum 値の単位は秒です。

☛ IPv6 の場合は、AAAA レコードで以下のように記載します。

```
sol01       IN      AAAA      fec0:0000:0001:0002:0003:0004:e731:3c50
```


3.2.3. 逆引き用ゾーンファイルの作成

1) 逆引き用ゾーンファイルを新規作成する

```
Master# vi /var/named/named.rev
```

☞ ファイル名は、構成ファイルに記載した名称（本書では named.rev）にします。

（記載例）

```
$TTL 3600
@       IN      SOA     dns-ex01.solaris.co.jp.  root.mail.solaris.co.jp.(
                2017011501                ;Serial
                10800                     ;Refresh
                3600                      ;Retry
                604800                    ;Expire
                86400 )                    ;Minimum
;
;-------------------------------------------------------
                IN      NS      dns-ex01.solaris.co.jp.          ;マスタサーバ
                IN      NS      dns-ex02.solaris.co.jp.          ;スレーブサーバ
10              IN      PTR     dns-ex01.solaris.co.jp.
11              IN      PTR     dns-ex02.solaris.co.jp.
12              IN      PTR     sol01.solaris.co.jp.
```

☞ IPv6 の場合でも、PTR レコードを使用し、以下のように記載します。

0.5.c.3.1.3.7.e.4.0.0.0.3.0.0.0 IN PTR sol01.solaris.co.jp.

3.2.4. ループバック正引き用ゾーンファイルの作成

1) ループバック正引き用ゾーンファイルを新規作成する

```
Master# vi /var/named/localhost.zone
```

☛ ファイル名は、構成ファイルに記載した名称（本書では localhost.zone）にします。

（記載例）

```
$TTL 3600
@       IN      SOA     dns-ex01.solaris.co.jp.  root.mail.solaris.co.jp.(
                2017011501              ;Serial
                10800                   ;Refresh
                3600                    ;Retry
                604800                  ;Expire
                86400 )                  ;Minimum
;
;-------------------------------------------------------
              IN      NS      dns-ex01.solaris.co.jp.
              IN      A       127.0.0.1
```

☛ IPv6 の場合は、AAAA レコードで以下のように記載します。

```
IN      AAAA      ::1
```

3.2.5. ループバック逆引き用ゾーンファイルの作成

1) ループバック逆引き用ゾーンファイルを新規作成する

```
Master# vi /var/named/localhost.rev
```

☛ ファイル名は、構成ファイルに記載した名称（本書では localhost.rev）にします。

（記載例）

```
$TTL 3600
@       IN      SOA     dns-ex01.solaris.co.jp.  root.mail.solaris.co.jp.(
                2017011501              ;Serial
                10800                   ;Refresh
                3600                    ;Retry
                604800                  ;Expire
                86400 )                  ;Minimum
;
;-------------------------------------------------------
                IN      NS      dns-ex01.solaris.co.jp.
1               IN      PTR     localhost.
```

☛ IPv6 の場合でも、上記記述と同じ内容になります。

3.3. ルートキャッシュファイルの作成

1) ルートキャッシュファイルを新規作成する

```
Master# vi /var/named/named.root
```

ルートキャッシュファイルは、手動で作成が可能ですが、以下いずれかの URL から入手することもできます。

- ftp://rs.internic.net/domain/named.root
- ftp://ftp.nic.ad.jp/internet/rs.internic.net/domain/named.root

本書では URL から入手した記載内容を使用します。

（記載例）

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     November 16, 2017
;       related version of root zone:     2017111601
;
; FORMERLY NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     199.9.14.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
```



```
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     199.7.91.13
D.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
E.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:a8::e
;
; FORMERLY NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
F.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
G.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:12::d0d
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     198.97.190.53
H.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:1::53
;
; FORMERLY NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
I.ROOT-SERVERS.NET.     3600000      AAAA  2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
J.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
K.ROOT-SERVERS.NET.     3600000      AAAA  2001:7fd::1
;
; OPERATED BY ICANN
;
```



```
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     199.7.83.42
L.ROOT-SERVERS.NET.     3600000      AAAA  2001:500:9f::42
;
; OPERATED BY WIDE
;
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
M.ROOT-SERVERS.NET.     3600000      AAAA  2001:dc3::35
; End of file
```


3.4. 構成ファイルとゾーンファイルのチェック

作成した各種ファイル（構成ファイル、ゾーンファイル）の書式について、チェックツールを実行して正しいことを確認します。

- 構成ファイルのチェック
  named-checkconf [構成ファイル名]
- ゾーンファイルのチェック
  named-checkzone [ゾーン名] [ゾーンファイル名]

3.4.1. 構成ファイルのチェック

1) 構成ファイルをチェックする

```
Master# named-checkconf /etc/named.conf
```

☛ エラーがない場合は何も返しません。

☛ 戻り値を出力させて確認することもできます。その場合は以下を実行してください。「0」が出力されればエラーなしと判断できます。
echo $?

3.4.2. ゾーンファイルのチェック

1) 正引き用ゾーンファイルの文法をチェックする

```
Master# named-checkzone sparc.co.jp /var/named/named.zone
zone solaris.co.jp/IN: loaded serial 2017011501
OK
```

☛ 問題ない場合は「OK」と出力されます。

2) 逆引き用ゾーンファイルの文法をチェックする

```
Master# named-checkzone 200.168.192.in-addr.arpa /var/named/named.rev
zone 200.168.192.in-addr.arpa/IN: loaded serial 2017011501
OK
```

☛ 問題ない場合は「OK」と出力されます。

3) ループバック正引き用ゾーンファイルの文法をチェックする

```
Master# named-checkzone localhost /var/named/localhost.zone
zone localhost/IN: loaded serial 2017011501
OK
```

☛ 問題ない場合は「OK」と出力されます。

4) ループバック逆引き用ゾーンファイルの文法をチェックする

```
Master# named-checkzone 0.0.127.in-addr.arpa /var/named/localhost.rev
zone 0.0.127.in-addr.arpa/IN: loaded serial 2017011501
OK
```

☛ 問題ない場合は「OK」と出力されます。

3.5. DNS サービスの起動

3.5.1. サービスの起動テスト

サービス起動前に構成ファイルとゾーンファイルを使用して起動テストを行い、エラーが表示されないことを確認します。

1) named の起動テストを実施する

```
Master# named -g
30-Nov-2017 16:45:15.333 starting BIND 9.6-ESV-R11-S10 -g
30-Nov-2017 16:45:15.333 built with
'CXX=/ws/on11update-tools/SUNWspro/sunstudio12.1/bin/CC' '--prefix=/usr'
'--mandir=/usr/share/man' '--bindir=/usr/sbin' '--libdir=/usr/lib/dns' '--with-libtool'
'--sbindir=/usr/sbin' '--sysconfdir=/etc' '--localstatedir=/var' '--with-openssl'
'--enable-threads=yes' '--enable-devpoll=yes' '--disable-openssl-version-check'
'--enable-fixed-rrset' '--with-pkcs11' '--with-libxml2=/usr' 'CFLAGS=-m32 -xO4
-xtarget=ultra2 -xarch=sparcvis -xchip=ultra2 -Qoption cg -xregs=no%appl -W2,-xwrap_int
-xmemalign=8s -mt' 'CC=/ws/on11update-tools/SUNWspro/sunstudio12.1/bin/cc'
30-Nov-2017 16:45:15.333 ------------------------------------------------------
30-Nov-2017 16:45:15.333 BIND 9 is maintained by Internet Systems Consortium,
30-Nov-2017 16:45:15.333 Inc. (ISC), a non-profit 501(c)(3) public-benefit
30-Nov-2017 16:45:15.333 corporation.  Support and training for BIND 9 are
30-Nov-2017 16:45:15.333 available at https://www.isc.org/support
30-Nov-2017 16:45:15.333 ------------------------------------------------------
30-Nov-2017 16:45:15.333 found 4 CPUs, using 4 worker threads
30-Nov-2017 16:45:15.334 using up to 4096 sockets
30-Nov-2017 16:45:15.345 loading configuration from '/etc/named.conf'
30-Nov-2017 16:45:15.346 using default UDP/IPv4 port range: [1024, 65535]
30-Nov-2017 16:45:15.346 using default UDP/IPv6 port range: [1024, 65535]
30-Nov-2017 16:45:15.347 listening on IPv4 interface lo0, 127.0.0.1#53
30-Nov-2017 16:45:15.349 listening on IPv4 interface net0, 192.168.200.10#53
30-Nov-2017 16:45:15.350 sizing zone task pool based on 5 zones
30-Nov-2017 16:45:15.350 ignoring non-root hint zone '“.”'
30-Nov-2017 16:45:15.356 open: /etc/rndc.key: file not found
30-Nov-2017 16:45:15.356 couldn't add command channel 127.0.0.1#953: file not found
30-Nov-2017 16:45:15.356 open: /etc/rndc.key: file not found
30-Nov-2017 16:45:15.356 couldn't add command channel ::1#953: file not found
30-Nov-2017 16:45:15.356 not using config file logging statement for logging due to -g
option
30-Nov-2017 16:45:15.357 zone 200.168.192.in-addr.arpa/IN: loaded serial 2017011501
30-Nov-2017 16:45:15.357 zone 0.0.127.in-addr.arpa/IN: loaded serial 2017011501
30-Nov-2017 16:45:15.357 zone sparc.co.jp/IN: loaded serial 2017011501
30-Nov-2017 16:45:15.357 zone localhost/IN: loaded serial 2017011501
30-Nov-2017 16:45:15.358 running
```

☛ [Ctrl] + [C] キーを押して終了させてください。

☛ 上記例では rndc.key が file not found になっていますが、rndc ユーティリティは本書では使用しませんので無視してください。

☛ 「Warning: 'empty-zones-enable/disable-empty-zone' not set」のメッセージが出力される場合がありますが、これは、BIND の

Built-in Empty Zones 機能によるもので、名前解決の動作に影響はありません。
デフォルトで本機能は有効化されていますが、構成ファイル（/etc/named.conf）のオプションに以下のとおり明示的に設定することで Warning メッセージを抑止することも可能です。

```
options{
  empty-zones-enable yes;
};
```

3.5.2. サービスの起動

1) サービスを起動する

```
Master# svcadm enable svc:/network/dns/server:default
```

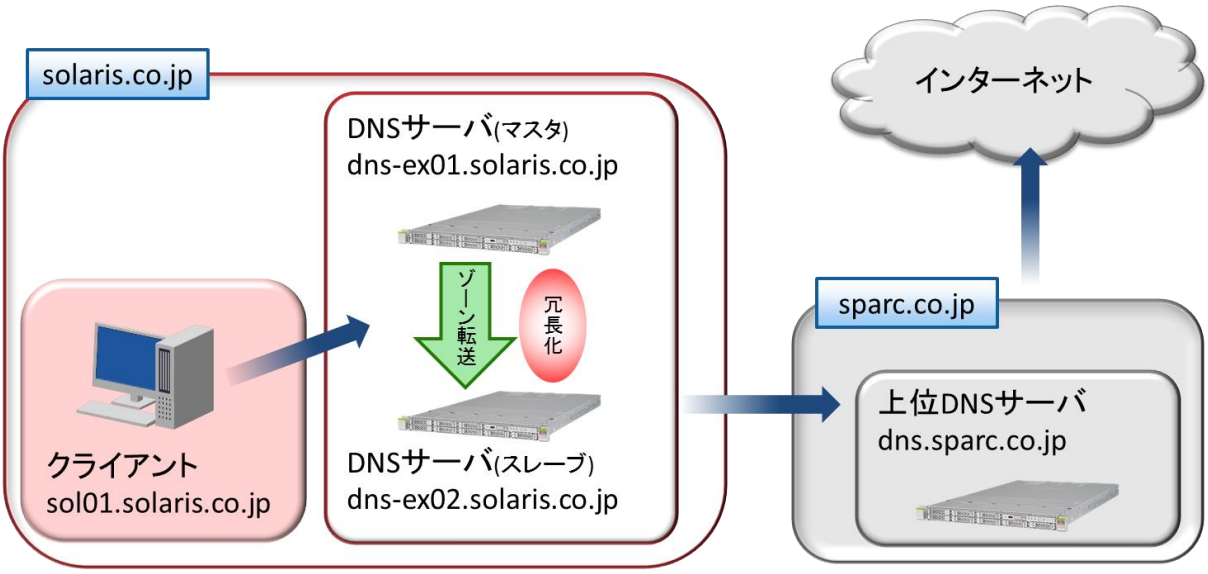
☛ named のログは随時/var/adm/messages に出力されます。エラー情報などを適時確認することができます。

2) サービスの状態を確認する

```
Master# svcs svc:/network/dns/server:default
STATE          STIME    FMRI
online         17:10:37 svc:/network/dns/server:default
```

☛ STATE の値が「online」であることを確認します。

4. クライアントの設定



DNS サーバによる名前解決を行うには、クライアント側での設定が必要になります。

本書では、クライアントサーバの OS が Solaris 11 の場合の設定を記載します。

4.1. 名前解決を行う順番の指定

/etc/nsswitch.conf を編集して名前解決を行う順番を指定します。

1) nsswitch.conf ファイルを編集する

```
Client# vi /etc/nsswitch.conf
```

（記載例）

hosts 行に「dns」を追加します。

```
hosts:  files dns
```

☛ files はデフォルトで記載してあり、ローカルデータベース（/etc/hosts）で名前解決することを示しています。

☛ 上記の設定の場合、名前解決の順番は、はじめにローカルデータベース（/etc/hosts）を参照して名前解決を行い、名前解決ができない場合は DNS サーバへ問い合わせを行う、という動作になります。

4.2. 名前解決を依頼する DNS サーバの指定

名前解決にDNSサーバを使用する場合、DNSサーバの情報を/etc/resolv.confファイルに記載します。

1) resolv.conf ファイルを編集する

```
Client# vi /etc/resolv.conf
```

☛ ファイルがない場合は、新規に作成されます。

（記載例）

問い合わせ先 DNS サーバの IP アドレスとドメイン名を指定します。

```
nameserver 192.168.200.10
nameserver 192.168.200.11
domain solaris.co.jp
```

☛ 上記のとおり、複数の nameserver を記載した場合は上から順番に問い合わせます。

4.3. 名前解決の確認

DNS サーバが管理しているゾーンの名前解決ができることを確認します。
確認は以下のコマンドで実施できます。

- nslookup
- dig

Point

どちらのコマンドも名前解決の確認を行うために使用できますが、通常は nslookup コマンドで十分な情報を得ることができます。ただし、エラー発生時などに DNS サーバの挙動を調べるには dig コマンドを使用します。

4.3.1. nslookup コマンドを使用した名前解決の確認

1) クライアントから自ドメインに対して正引きができることを確認する

```
Client# nslookup sol01.solaris.co.jp
Server:         192.168.200.10
Address:        192.168.200.10#53

Name:   sol01.solaris.co.jp
Address: 192.168.200.12
```

☛ sol01.solaris.co.jp の IP アドレスが「192.168.200.12」と回答が返ってきています。

2) クライアントから自ドメインに対して逆引きができることを確認する

```
Client# nslookup 192.168.200.12
Server:         192.168.200.10
Address:        192.168.200.10#53

12.200.168.192.in-addr.arpa     name = sol01.solaris.co.jp.
```

☛ 192.168.200.12 のドメインが「sol01.solaris.co.jp」と回答が返ってきています。

4.3.2. dig コマンドを使用した名前解決の確認

1) クライアントから自ドメインに対して正引きができることを確認する

```
Client# dig sol01.solaris.co.jp

; <<>> DiG 9.6-ESV-R11-S10 <<>> sol01.solaris.co.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18066
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;sol01.solaris.co.jp.                IN      A

;; ANSWER SECTION:
sol01.solaris.co.jp.     3600    IN      A       192.168.200.12

;; AUTHORITY SECTION:
solaris.co.jp.          3600    IN      NS      dns-ex01.solaris.co.jp.
solaris.co.jp.          3600    IN      NS      dns-ex02.solaris.co.jp.

;; ADDITIONAL SECTION:
dns-ex01.solaris.co.jp. 3600    IN      A       192.168.200.10
dns-ex02.solaris.co.jp. 3600    IN      A       192.168.200.11

;; Query time: 2 msec
;; SERVER: 192.168.200.10#53(192.168.200.10)
;; WHEN: Mon Dec 04 14:43:21 JST 2017
;; MSG SIZE  rcvd: 98
```

☛ 「ANSWER SECTION」に問い合わせ結果が記載されます。

2) クライアントから自ドメインに対して逆引きができることを確認する

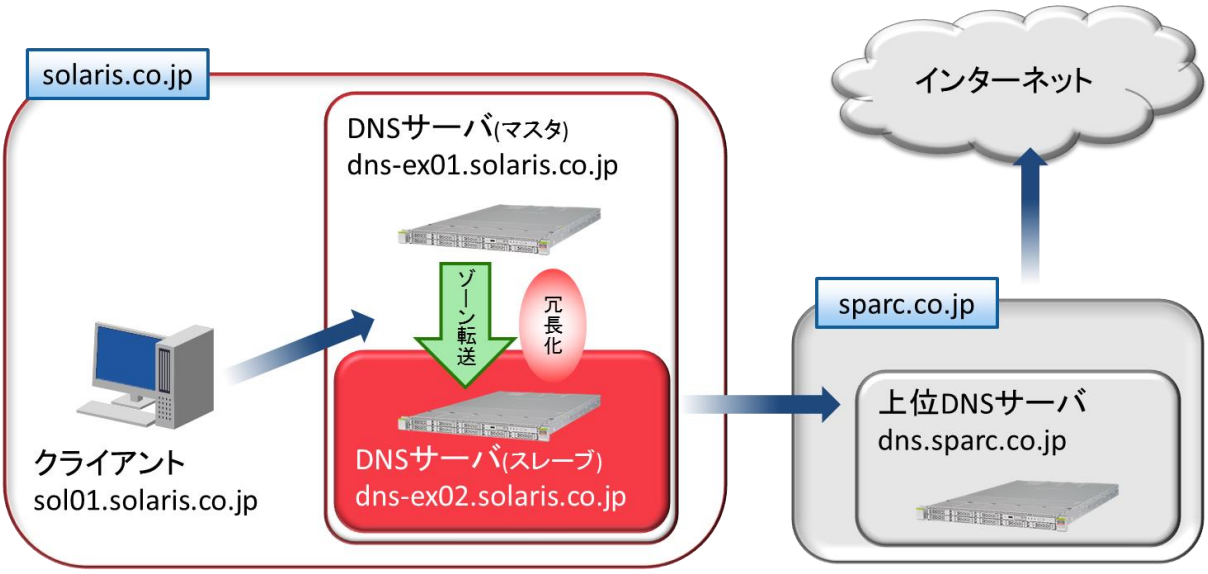
```
Client# dig -x 192.168.200.12

; <<>> DiG 9.6-ESV-R11-S10 <<>> -x 192.168.200.12
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11101
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;12.200.168.192.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
12.200.168.192.in-addr.arpa. 3600 IN      PTR     sol01.solaris.co.jp.

;; AUTHORITY SECTION:
200.168.192.in-addr.arpa.   3600    IN      NS      dns-ex01.solaris.co.jp.
200.168.192.in-addr.arpa.   3600    IN      NS      dns-ex02.solaris.co.jp.

;; ADDITIONAL SECTION:
dns-ex01.solaris.co.jp.     3600    IN      A       192.168.200.10
dns-ex02.solaris.co.jp.     3600    IN      A       192.168.200.11

;; Query time: 2 msec
;; SERVER: 192.168.200.10#53(192.168.200.10)
;; WHEN: Mon Dec 04 15:19:03 JST 2017
;; MSG SIZE  rcvd: 121
```

☞ 「ANSWER SECTION」に問い合わせ結果が記載されます。

本章までで、DNS サーバおよびクライアントが動作する設定は完了です。

これ以降の章では DNS サーバの冗長化とセキュリティ設定を説明します。

5. DNS サーバ(スレーブ)の構築



スレーブサーバを構築する際も、マスタサーバと同様のファイルが必要となります。ただし、構成ファイル内にゾーン転送の設定を行う点がマスタサーバと異なります。正引き用ファイルと逆引き用ファイルをマスタサーバからコピーするため、スレーブサーバ側での設定は不要です。

☞ マスタサーバとスレーブサーバのゾーン情報の一貫性を維持するために、ゾーン転送の機能を使用して定期的にマスタサーバからゾーン情報を転送します。転送設定はスレーブサーバ側で行います。

項番	ファイル	役割	マスタサーバと異なる点	配置先
1	構成ファイル	DNS の構成情報を記載	マスタサーバからのゾーン転送設定を行う	/etc/named.conf
2	ゾーンファイル	正引き用ファイル	マスタサーバから転送するため設定不要	任意
3		逆引き用ファイル		
4		ループバック正引き用ファイル	マスタサーバと同様に設定する	
5		ループバック逆引き用ファイル		
6	ルートキャッシュファイル	ルートサーバの情報を記載		

5.1. DNS 構成情報とゾーン転送の設定

1) 構成ファイルを新規作成する

```
Slave# vi /etc/named.conf
```

（記載例）

ゾーン転送設定のため正引きと逆引きの type に slave を指定し、マスタサーバの IP アドレスを記載します。

```
options{
        directory       "/var/named";
};

zone"solaris.co.jp"{
        type    slave;                          //slave を指定
        masters{
                192.168.200.10;                 //マスタサーバの IP アドレス
        };
        file    "named.zone.bak";
};

zone"200.168.192.in-addr.arpa"{
        type    slave;                          //slave を指定
        masters{
                192.168.200.10;                 //マスタサーバの IP アドレス
        };
        file    "named.rev.bak";
};

zone"localhost"{
        type    master;
        file    "localhost.zone";
};

zone"0.0.127.in-addr.arpa"{
        type    master;
        file    "localhost.rev";
};

zone"."{
        type    hint;
        file    "named.root";
};
```

- ☛ それぞれのファイル名に規則はありません。任意に指定が可能です。
- ☛ /var/named フォルダ配下に各ファイルを格納する設定としています。
- ☛ スレーブサーバの場合でも、ループバックの正引きと逆引き、それからルートキャッシュファイルは設定が必要です。マスタサーバ構築時の手順と同様に作成してください。
- ☛ 正引き、逆引きファイルは作成不要です。ゾーン転送が行われると自動的に作成されます。

5.2. ループバック正引き用ゾーンファイルの作成

1) ゾーンファイルを配置するディレクトリを作成する

```
Slave# mkdir -p /var/named
```

2) ループバック正引き用ゾーンファイルを新規作成する

```
Slave# vi /var/named/localhost.zone
```

（記載例）

```
$TTL 3600
@       IN      SOA     dns-ex02.solaris.co.jp.  root.mail.solaris.co.jp.(
                2017011501
                10800
                3600
                604800
                86400 )
;
;-------------------------------------------------------
                IN      NS      dns-ex02.solaris.co.jp.
                IN      A       127.0.0.1
```


5.3. ループバック逆引き用ゾーンファイルの作成

1) ループバック逆引き用ゾーンファイルを新規作成する

```
Slave# vi /var/named/localhost.rev
```

（記載例）

```
$TTL 3600
@       IN      SOA     dns-ex02.solaris.co.jp.  root.mail.solaris.co.jp.(
                2017011501
                10800
                3600
                604800
                86400 )
;
;-------------------------------------------------------
                IN      NS      dns-ex02.solaris.co.jp.
1               IN      PTR     localhost.
```

5.4. ルートキャッシュファイルの作成

1) ルートキャッシュファイルを新規作成する

```
Slave# vi /var/named/named.root
```

（記載例）

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     November 16, 2017
;       related version of root zone:     2017111601
;
; FORMERLY NS.INTERNIC.NET
;
.                       3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
```



```
B.ROOT-SERVERS.NET.        3600000      A      199.9.14.201
B.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:200::b
;
; FORMERLY C.PSI.NET
;
.                          3600000      NS     C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.        3600000      A      192.33.4.12
C.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                          3600000      NS     D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.        3600000      A      199.7.91.13
D.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                          3600000      NS     E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.        3600000      A      192.203.230.10
E.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:a8::e
;
; FORMERLY NS.ISC.ORG
;
.                          3600000      NS     F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.        3600000      A      192.5.5.241
F.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.                          3600000      NS     G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.        3600000      A      192.112.36.4
G.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:12::d0d
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                          3600000      NS     H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.        3600000      A      198.97.190.53
H.ROOT-SERVERS.NET.        3600000      AAAA   2001:500:1::53
;
; FORMERLY NIC.NORDU.NET
;
.                          3600000      NS     I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.        3600000      A      192.36.148.17
I.ROOT-SERVERS.NET.        3600000      AAAA   2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
.                          3600000      NS     J.ROOT-SERVERS.NET.
```



```
J.ROOT-SERVERS.NET.       3600000      A      192.58.128.30
J.ROOT-SERVERS.NET.       3600000      AAAA   2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
.                         3600000      NS     K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.       3600000      A      193.0.14.129
K.ROOT-SERVERS.NET.       3600000      AAAA   2001:7fd::1
;
; OPERATED BY ICANN
;
.                         3600000      NS     L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.       3600000      A      199.7.83.42
L.ROOT-SERVERS.NET.       3600000      AAAA   2001:500:9f::42
;
; OPERATED BY WIDE
;
.                         3600000      NS     M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.       3600000      A      202.12.27.33
M.ROOT-SERVERS.NET.       3600000      AAAA   2001:dc3::35
; End of file
```

☛ ルートキャッシュファイルは、以下いずれかの URL から入手可能です。最新のルートキャッシュファイルをご使用ください。
ftp://rs.internic.net/domain/named.root
ftp://ftp.nic.ad.jp/internet/rs.internic.net/domain/named.root

5.5. 構成ファイルとゾーンファイルのチェック

作成した各種ファイル（構成ファイル、ゾーンファイル）の書式について、チェックツールを実行して正しいことを確認します。

- 構成ファイルのチェック
  named-checkconf [構成ファイル名]
- ゾーンファイルのチェック
  named-checkzone [ゾーン名] [ゾーンファイル名]

5.5.1. 構成ファイルのチェック

1) 構成ファイルをチェックする

```
Slave# named-checkconf /etc/named.conf
```

☛ エラーがない場合は何も返しません。

☛ 戻り値を出力させて確認することもできます。その場合は以下を実行してください。「0」が出力されればエラーなしと判断できます。
echo $?

5.5.2. ゾーンファイルのチェック

スレーブサーバでは、正引き用および逆引き用のゾーンファイルは作成しないため、ここでは、ループバックの正引き用と逆引き用のゾーンファイルをチェックします。

1) ループバック正引き用ゾーンファイルの文法をチェックする

```
Slave# named-checkzone localhost /var/named/localhost.zone
zone localhost/IN: loaded serial 2017011501
OK
```

☛ 問題ない場合は「OK」と出力されます。

2) ループバック逆引き用ゾーンファイルの文法をチェックする

```
Slave# named-checkzone 0.0.127.in-addr.arpa /var/named/localhost.rev
zone 0.0.127.in-addr.arpa/IN: loaded serial 2017011501
OK
```

☛ 問題ない場合は「OK」と出力されます。

5.6. DNS サーバ(スレーブ)での DNS サービスの起動

5.6.1. サービスの起動テスト

サービス起動前に構成ファイルとゾーンファイルを使用して起動テストを行い、エラーが表示されないことを確認します。

1) named の起動テストを実施する

```
Slave# named -g
18-Jan-2018 18:52:31.614 starting BIND 9.6-ESV-R11-S10 -g
18-Jan-2018 18:52:31.614 built with
'CXX=/ws/on11update-tools/SUNWspro/sunstudio12.1/bin/CC' '--prefix=/usr'
'--mandir=/usr/share/man' '--bindir=/usr/sbin' '--libdir=/usr/lib/dns' '--with-libtool'
'--sbindir=/usr/sbin' '--sysconfdir=/etc' '--localstatedir=/var' '--with-openssl'
'--enable-threads=yes' '--enable-devpoll=yes' '--disable-openssl-version-check'
'--enable-fixed-rrset' '--with-pkcs11' '--with-libxml2=/usr' 'CFLAGS=-m32 -xO4
-xtarget=ultra2 -xarch=sparcvis -xchip=ultra2 -Qoption cg -xregs=no%appl -W2,-xwrap_int
-xmemalign=8s -mt' 'CC=/ws/on11update-tools/SUNWspro/sunstudio12.1/bin/cc'
18-Jan-2018 18:52:31.615 ------------------------------------------------------
18-Jan-2018 18:52:31.615 BIND 9 is maintained by Internet Systems Consortium,
18-Jan-2018 18:52:31.615 Inc. (ISC), a non-profit 501(c)(3) public-benefit
18-Jan-2018 18:52:31.615 corporation.  Support and training for BIND 9 are
18-Jan-2018 18:52:31.615 available at https://www.isc.org/support
18-Jan-2018 18:52:31.615 ------------------------------------------------------

--<省略>--

18-Jan-2018 18:52:31.736 zone 0.0.127.in-addr.arpa/IN: loaded serial 2017011501
18-Jan-2018 18:52:31.737 zone solaris.co.jp/IN: loaded serial 2017011505
18-Jan-2018 18:52:31.738 zone localhost/IN: loaded serial 2017011501
18-Jan-2018 18:52:31.739 running
```

☛ [Ctrl] + [C] キーを押して終了させてください。

5.6.2. サービスの起動

1) サービスを起動する

```
Slave# svcadm enable svc:/network/dns/server:default
```

☛ named のログは随時/var/adm/messages に出力されます。エラー情報などを適時確認することができます。

2) サービスの状態を確認する

```
Slave# svcs svc:/network/dns/server:default
STATE          STIME    FMRI
online         19:01:59 svc:/network/dns/server:default
```

☛ STATE の値が「online」であることを確認します。

5.6.3. ゾーン転送の確認

DNS サーバ(スレーブ)のサービスを起動すると、ゾーン転送が行われます。
正常にゾーン情報が転送されていることを確認します。

1) ゾーンファイルを格納しているディレクトリを確認する

```
Slave# ls -l /var/named
total 16
-rw-r--r--   1 root     root         343 11 月 16 日  18:38 localhost.rev
-rw-r--r--   1 root     root         325 11 月 16 日  18:38 localhost.zone
-rw-r--r--   1 root     root         410 12 月  5 日  20:41 named.rev.bak
-rw-r--r--   1 root     root        3.2K 11 月 29 日  18:23 named.root
-rw-r--r--   1 root     root         378 12 月  5 日  20:41 named.zone.bak
```

☛ スレーブサーバの構成ファイルに指定したファイル名でコピーされていることを確認します。

☛ ゾーン転送されない場合は、以下の問題がある可能性があります。
・TCP の 53 番ポートがマスタサーバとスレーブサーバ間の経路の途中でフィルタリングされている。
※ゾーン転送は TCP プロトコルを使用しているため、ファイアウォールなどで遮断している場合があります。
・マスタサーバ側でゾーン転送の制限をしている。
※ゾーン転送の制限については、次章で説明します。

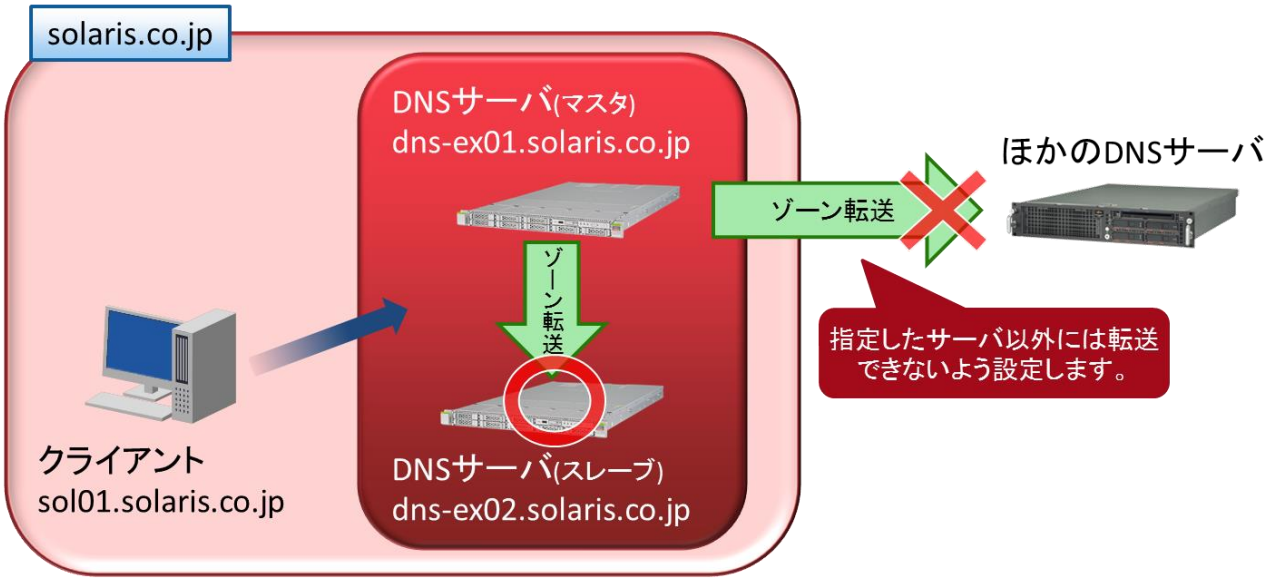
6. セキュリティ設定

DNS サーバは、外部から悪用されたり、不正な情報を送り付けられたりなど、攻撃の対象になりやすい側面があるため、セキュリティの設定は DNS サーバを構築する上で重要な設定の 1 つです。
本章では、BIND のセキュリティの設定として、以下 2 つのセキュリティ機能について紹介します。必要に応じて実施ください。

セキュリティ設定	概要	設定するファイル
ゾーン転送制限	マスタサーバからのゾーン転送をすべて制限、もしくは、特定のサーバのみ許可する。	構成ファイル（/etc/named.conf）
問い合わせ制限	問い合わせに対して、回答するクライアントを制限する。	

6.1. ゾーン転送制限

マスタサーバからのゾーン転送は、デフォルトでは制限なく転送可能な状態になっています。このため、指定したサーバ以外にはゾーン転送できないように設定が必要です。
DNS サーバの場合、予期せぬサーバへゾーン転送が行われると外部にゾーン情報が漏れることになるため、転送制限の設定が必要となります。



1) 特定の IP アドレスに対してのみゾーン転送を許可(全体に設定)する

```
Master# vi /etc/named.conf
```

構成ファイル(/etc/named.conf)に以下を記載します。

```
options{
        directory       "/var/named";
        allow-transfer{ 192.168.200.11; };
};
```

☛ 上記例では、192.168.200.11 のサーバにのみゾーン転送を許可しています。
なお、許可する IP アドレスを複数設定することも可能です。その場合、以下のように記載します。
allow-transfer{ 192.168.200.11; 192.168.200.12; };

☛ すべてのゾーン転送を制限する場合は、以下のとおり「none」を設定します。
allow-transfer{ none; };

2) 特定の IP アドレスのみゾーン転送を許可(ゾーンごとに設定)する

```
Master# vi /etc/named.conf
```

構成ファイル(/etc/named.conf)に以下を記載します。

正引きのゾーンや逆引きのゾーンで個別に転送を制限することもできます。

```
zone"solaris.co.jp"{
        type    master;
        file    "named.zone";
        allow-transfer{ 192.168.200.11; };
};
```

☛ 上記例では、正引きのゾーンを 192.168.200.11 のサーバに対してのみ転送を許可しています。

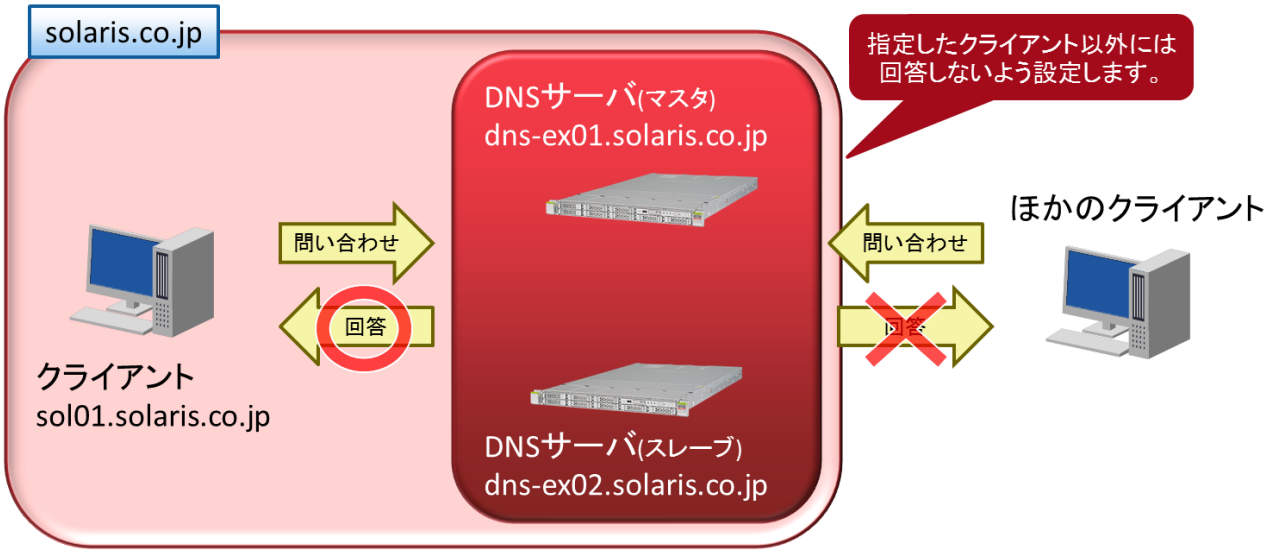
3) サービスを再起動する

構成ファイルの変更を反映するため、サービスを再起動します。

```
Master# svcadm refresh svc:/network/dns/server:default
Master# svcadm restart svc:/network/dns/server:default
```


6.2. 問い合わせ制限

DNS サーバへの問い合わせに対する回答については、デフォルトでは制限なく回答する設定になっています。このため、指定したクライアント以外の問い合わせには回答しないように設定が必要です。
DNS サーバの場合、Dos 攻撃や踏み台にされる恐れがあるため、設定が必要になります。



- DNS サーバを冗長化している場合は、マスタサーバ、スレーブサーバそれぞれで設定が必要です。
- 本書では内部 DNS サーバ向けの設定を記載しています。
- 外部 DNS サーバの場合は、問い合わせ制限を行うと外部からの問い合わせに回答できなくなります。外部からの問い合わせに対しては、問い合わせ制限ではなく、再帰問い合わせ（allow-recursion）とキャッシュ問い合わせ（allow-query-cache）を拒否するように設定してください。

1) ログイン

マスタとスレーブ、それぞれのサーバにログインします。

```
login:
```

☛ 本章では、すべて両方のサーバで操作します。

2) root 権限の切替

```
$ su -
```

☛ 本章では、すべて root 権限で操作します。

☛ 以降では、マスタサーバにログインした例で説明します。

3) 特定の IP アドレスに対してのみ問い合わせを許可(全体に設定)する

```
Master# vi /etc/named.conf
```

構成ファイル(/etc/named.conf)に以下を記載します。

```
options{
        directory       "/var/named";
        allow-query{ 192.168.200.0/24; 127.0.0.1; };
};
```

☛ 上記例では、192.168.200 のネットワークとループバックにのみ問い合わせを許可しています。

4) 特定の IP アドレスに対してのみ問い合わせを許可(ゾーンごとに設定)する

```
Master# vi /etc/named.conf
```

構成ファイル(/etc/named.conf)に以下を記載します。

正引きのゾーンや逆引きのゾーンで個別に問い合わせを制限することもできます。

```
zone"solaris.co.jp"{
        type    master;
        file    "named.zone";
        allow-query{ 192.168.200.0/24; };
};
```

☛ 上記例では、正引きのゾーンを 192.168.200 のネットワークのみ問い合わせを許可しています。

5) 特定の IP アドレスに対してのみ問い合わせを制限する

```
Master# vi /etc/named.conf
```

構成ファイル(/etc/named.conf)に以下を記載します。

```
options{
        directory       "/var/named";
        blackhole{ 192.168.200.12; };
};
```

☛ 上記例では、192.168.200.12 のクライアントのみ問い合わせを制限しています。

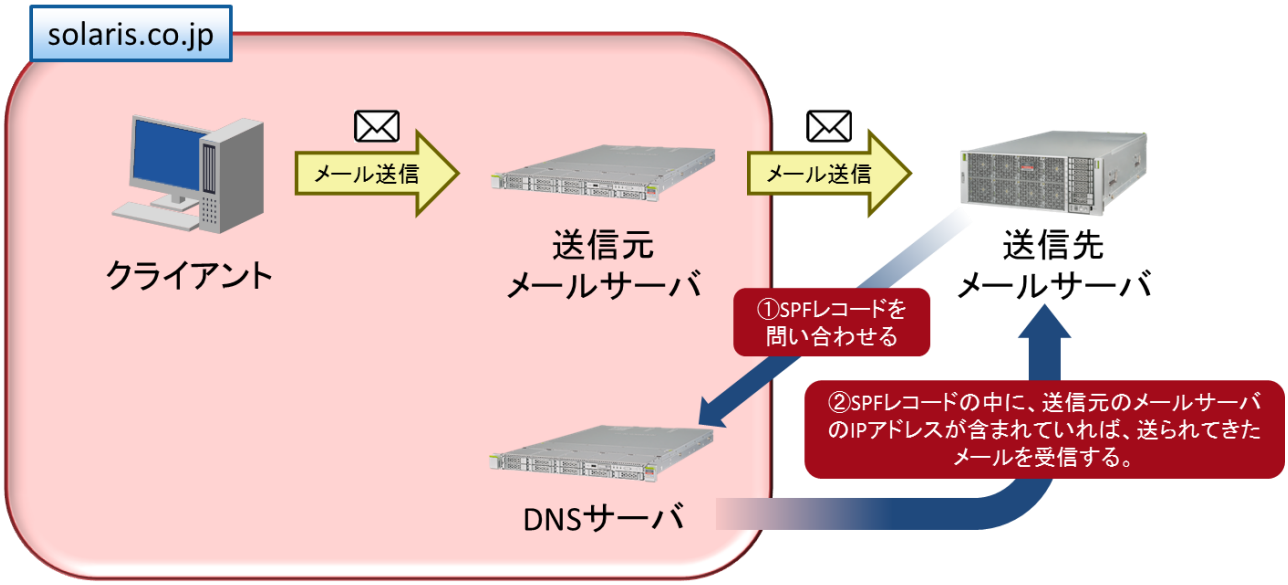
6) サービスを再起動する

構成ファイルの変更を反映するため、サービスを再起動します。

```
Master# svcadm refresh svc:/network/dns/server:default
Master# svcadm restart svc:/network/dns/server:default
```


《参考》SPF レコードの設定

SPF（Sender Policy Framework）は、SMTP を利用した電子メールの送受信において、送信者のドメインの正当性を検証する仕組みです。
メール送信元の DNS サーバに SPF レコードの設定をしておくことで、送信されたメールが偽装されていないかを送信先のメールサーバ側で確認することができます。
なりすましメール防止のため、外部 DNS サーバでは SPF などの送信ドメイン認証設定を行うことを推奨します。



■ SPF レコードの書式

SPF レコードは、qualifier と mechanism から構成されており、mechanism にマッチする条件を記載し、マッチした際の動作を qualifier で指定します。

正引きのゾーンファイル内(/var/named/named.zone)に以下の書式で記載します。

```
“v=spf1 【qualifier】【mechanism】:【値】”
```

BIND では SPF を TXT レコードで設定します。

設定は、「【qualifier】【mechanism】:【値】」で 1 セットとなり、複数記述することができます。複数記述した場合は、左から順に判定されます。

それぞれの要素の意味は以下となります。

- v=spf1

  SPF のバージョンを示し、先頭に記載します。

- qualifier **（省略時は+が設定）**

  mechanism にマッチした際にどのような判定とするかを記述します。

  代表的な qualifier は以下です。

qualifiler	判定結果	意味
+	Pass	メールを許可
-	Fail	メールを拒否
~	SoftFail	メールを拒否するが Fail よりは弱い拒否
?	Neutral	どれにもマッチしなかった場合など

  qualifier は省略することが可能です。省略した場合は、「+」が設定されます。

  なお、判定結果を受けて、送信されたメールをどう処理するかは送信先のメールサーバの設定次第となります。SoftFail で受信するメールサーバもあれば、セキュリティの厳しいメールサーバでは SoftFail でも拒否することがありえます。

- mechanism

  マッチする条件を記載します。

  代表的な mechanism は以下です。

mechanism	意味
ip4	送信元メールサーバの IP アドレスが、指定したネットワークアドレスの範囲内にあればマッチします。 192.168.0.0/16 などの指定も可能です。
a	ドメインの A レコードに送信元メールサーバの IP アドレスがあればマッチします。 何も指定されていない場合は、その SPF レコードが登録されているドメインを示します。
mx	ドメインの MX レコードに送信元メールサーバの IP アドレスがあればマッチします。 何も指定されていない場合は、その SPF レコードが登録されているドメインを示します。
include	引数のドメインの SPF レコードを参照し、参照先でマッチすればマッチします。 参照先のドメインでもさらに include が指定されていて、入れ子構造になっている場合もあります。
all	すべての場合にマッチする。SPF レコードの最後に記載することで、どの条件にもマッチしなかった場合にどうするかを記述できます。

■ SPF レコードの設定方法

1) SPF レコードを設定する

```
Master# vi /var/named/named.zone
```

SPF レコードは、正引きのゾーンファイル内(/var/named/named.zone)に記載します。

```
$TTL 3600
@       IN      SOA     dns-ex01.solaris.co.jp.  root.mail.solaris.co.jp.(
                        2017011502
                        10800
                        3600
                        604800
                        86400 )
;
;-------------------------------------------------------
                IN      NS      dns-ex01.solaris.co.jp.
dns-ex01        IN      A       192.168.200.10

sol01            IN      A       192.168.200.12
solaris.co.jp.      IN      TXT     "v=spf1 +ip4:192.168.200.0/24 -all"
```

- ☛ 上記の例では、solaris.co.jp ドメインからのメールは、192.168.200 のネットワーク内の IP アドレスを持つサーバからのみ送信されるという意味になります。
- ☛ 設定によっては、1 行が長い設定になる場合もありますが、1 行につき 255 文字までしか記入できません。
- ☛ スレーブサーバにマスタサーバのゾーン情報変更を認識させるため、Serialの値を"2017011502"に変更します。

《参考》SMF サービスの管理方法

ここではサービス管理の方法を記載しています。必要に応じて参照してください。

1) サービスの状態を確認する方法

```
Master# svcs svc:/network/dns/server:default
STATE          STIME    FMRI
online         17:10:37 svc:/network/dns/server:default
```

☛ STATE の主な表示は「online」(起動)、「disable」(停止)となります。

☛ サービス名は省略形[dns/server]で指定することも可能です。

2) サービスの停止方法

```
Master# svcadm disable svc:/network/dns/server:default
```

3) サービスの再起動方法

```
Master# svcadm restart svc:/network/dns/server:default
```

4) サービスの起動方法

```
Master# svcadm enable svc:/network/dns/server:default
```


改版履歴

改版日時	版数	改版内容
2010 年 3 月	1.0	新規作成
2018 年 4 月	2.0	・Solaris 11.3 対応 ・「5 章　DNS サーバ（スレーブ）の構築」および「6 章　セキュリティ設定」を追加 ・≪参考≫SPF レコードの設定を追加 ・SMF サービスの管理方法を≪参考≫へ移動 ・レイアウトの変更

