学習目標

この授業を受講すると，DNSサーバの基本的役割と仕組みを理解し， BINDを用いてDNSサーバの基本的な設定が出来るようになります．具体的には次のようなことが出来るように学習しましょう．

- DNSとは何かを説明できるようになる
- DNSがドメイン名からIPアドレスを取得するしくみを説明できる
- BINDによりDNSを構築できるようになる
- DNSサーバの動作確認を行うことができる

DNSとは

DNSとは，Domain Name Systemのことです．DNSとは，ドメイン名とIPアドレスを対応付けるための仕組みです．

WebブラウザでURLを入力してWebページを表示したり，メーラで指定したメールアドレスにメールを送ったりするとき，インターネットでは 相手のWebサーバやメールサーバとのやり取りは，相手サーバのIPアドレスを使って行われます．インターネットでは，IPアドレスを，URLやメールアドレスから取得できる仕組みが用意されています．インターネットでは，IPアドレスを使って通信が行われていますが，数字の列であるIPアドレスではなく，人間が憶えやすい名前を付けて，その名前でアクセスできるようにしているのです．

たとえば，ブラウザに http://www.ics.teikyo-u.ac.jp/ と入力すると，帝京大学理工学部情報科学科のWebページが表示されます．ここでURLのwww.ics.teikyo-u.ac.jp はWebサーバの名前を表しています． このような，インターネット上で用いられるコンピュータなどの名前を「ドメイン名(Domain Name)」といいます．ドメイン名からIPアドレスを取得したりするのがDNSの役割です．

また，00t000xx@str.teikyo-u.ac.jp 宛てにメールを送信すると，学籍番号00t000の学生のメールアドレス宛にメールが送信されます．このとき，メールアドレスの”@”以降の「stu.teikyo-u.ac.jp」もドメイン名です．上のメールアドレスにメールを送信すると，メールサーバ(この場合はGmail)宛てにメールが送信されます．メールサーバのIPアドレスを取得するのもDNSの役割の一つです．

ドメイン名とは

ドメイン(Domain)という言葉には，「領土，領域，範囲」などの意味があります．インターネットで使われる「ドメイン」という言葉は，インターネット上のある領域をさす言葉と考えるといいでしょう．たとえば，www.ics.teikyo-u.ac.jp　というドメイン名は"jp"(日本)という領域の中の，"ac"(アカデミック，学術関連機関)という領域の中にある，"teikyo-u"(帝京大学)という領域の中の，"ics"(情報科学科)という領域にある，"www"というサーバマシン，と解釈することができます．これは住所などと対応させるとわかりやすいでしょう．たとえば，帝京大学宇都宮キャンパスの住所は，「栃木県宇都宮市豊郷台」ですが，これは「栃木県」という領域の中の，「宇都宮市」という領域の中の，「豊郷台」という領域にある，という意味に取れます．大きな領域の中にある，小さな領域，さらにその中の小さな領域，という具合に表しているわけです(図1)．

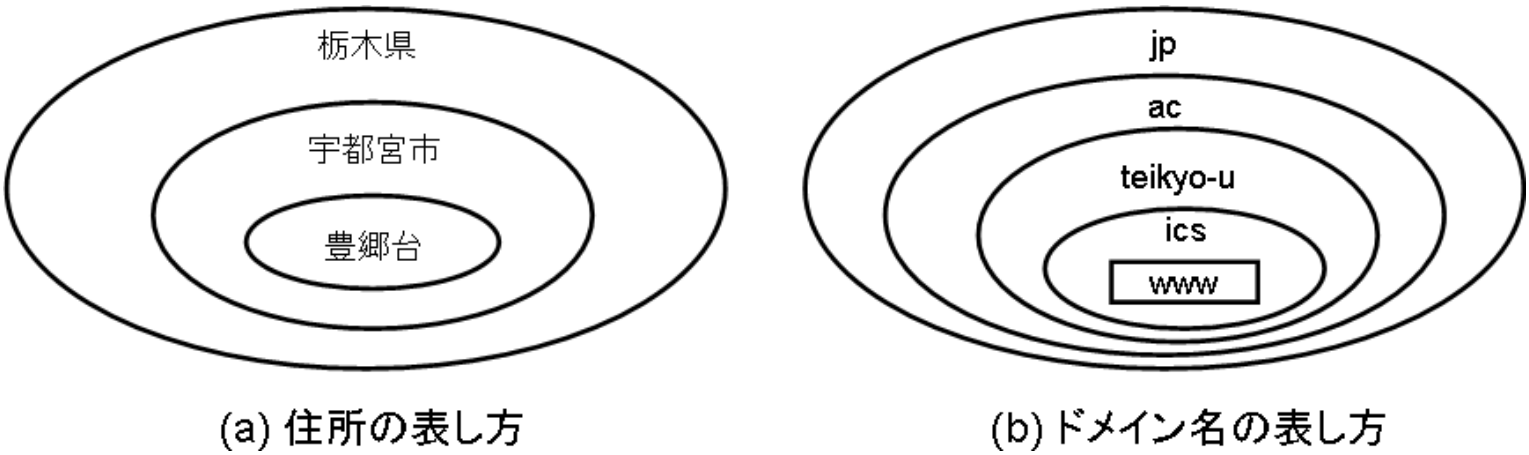

図**1** 住所とドメイン名における，領域の表し方

図1の，"jp"や"ac"などの，"."(ドット)で区切られた部分が，それぞれ「日本」や「学術関連機関」などの領域(あるいは範囲)を表しています．これらのそれぞれの領域が，インターネットでは「ドメイン」と呼ばれています．したがって，ics.teikyo-u.ac.jpは，jpドメインの中の，acドメインの中の，teikyo-uドメインの中のicsドメイン，ということになります．また，wwwは領域ではなく，icsドメインの中になる1台のサーバマシンを表しています．インターネットにつながれたサーバのようなコンピュータ等は，「ホスト」と呼ばれていて，この場合wwwは「ホスト名」です．www.ics.teikyo-u.ac.jpは，icsドメインの中にあるwwwというホストを表しており，www.ics.teikyo-u.ac.jp がこのホストを表すドメイン名です．あるホストを表す(wwwだけではなく，ドメインの情報すべてを表記した) www.ics.teikyo-u.ac.jp のような表記のことを，FQDN(Fully Qualified Domain Name，完全修飾ドメイン名)と呼びます(図2)．

また，acドメインはjpドメインの中のドメインで，teikyo-uドメインはacドメインの中のドメインです．このように，あるドメインの中にあるドメインのことを「サブドメイン」と呼びます．acドメインはjpドメインのサブドメインであり，teikyo-uドメインはacドメインのサブドメインです．

※ホスト名を含んだwww.ics.teikyo-u.ac.jpをドメイン名と呼ぶ場合と，ics.teikyo-u.ac.jpのように，ドメインを表す部分のみをドメイン名と呼ぶ場合があります．ここでは，FQDNがホスト名も含んでいる概念であることから，ホスト名を含んだものもドメイン名と呼ぶことにします．

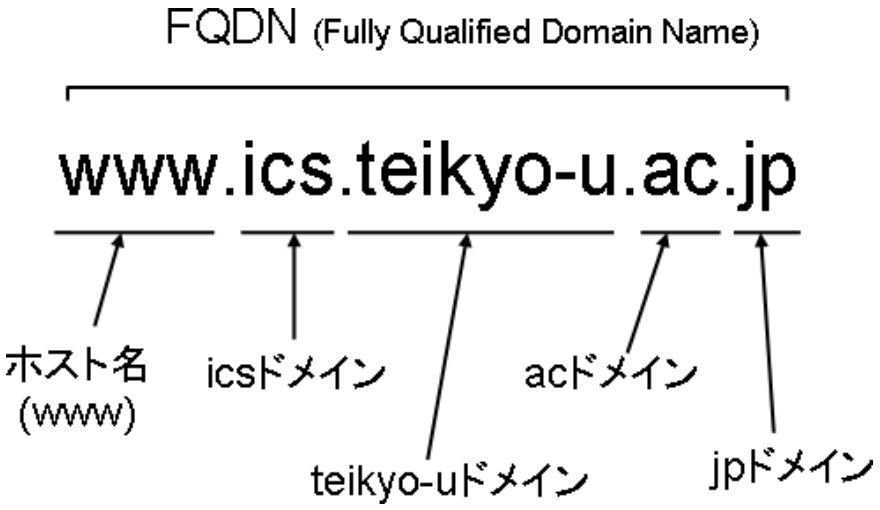

図**2** ドメイン名，ホスト名と**FQDN**

ドメインの階層構造

ドメイン名は，www.ics.teikyo-u.ac.jp という形をしていました．ここで，いちばん外側のドメインは，右端のjpです．jpと同じように，ドメイン名の右端に来るものとして，uk(英国)，tw(台湾)，cn(中国)などのように国を表すものや，com(営利機関)，org(組織)などがあります．また，jpのすぐ左側に来るものとしては，ac(研究機関)，co(営利機関)，go(政府機関)などがあります．さらに，acの左側には，例として挙げたteikyo-u(帝京大学)，u-tokyo(東京大学)などが続きます．これらのドメインの構成は，図3のような木構造(ツリー構造)で表すことができます．図3のようにツリー構造で構成されたドメイン名全体を，「ドメイン名前空間(Domain Name Space)と呼びます．また，ドメイン名のツリー構造を「ドメインツリー」と呼びますが，ドメインツリーでは，jpやacなどのドメイン名のところで枝分かれしています．この枝別れの部分をツリー構造では「ノード」と呼びます．すなわち，ドメインツリーのノードの名前がドメイン名である，と言うこともできます．

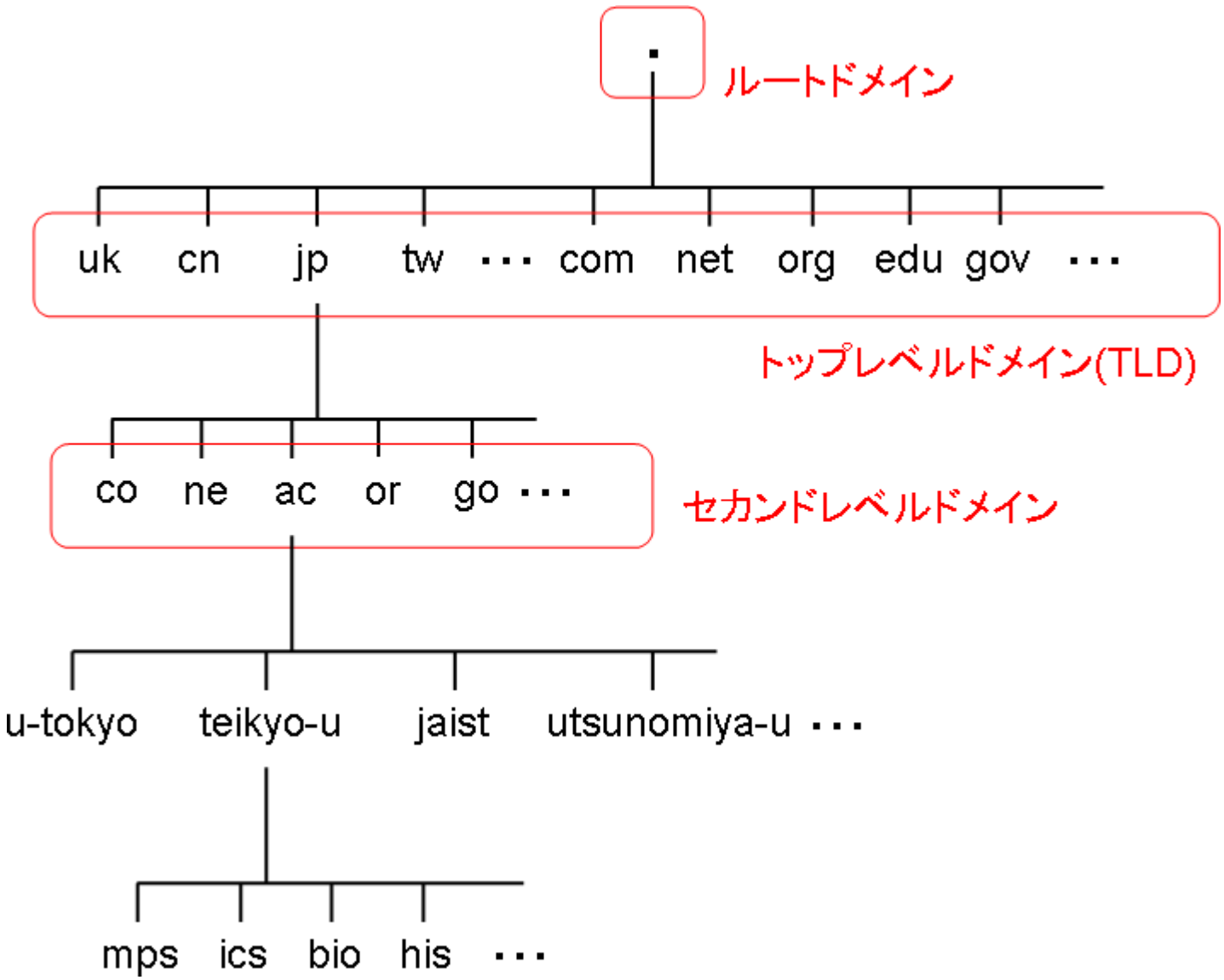

図3 ドメインのツリー構造

ドメインの階層構造

ツリー構造の一番上にある，jpやuk, comなどをトップレベルドメイン(TDL：Top Level Domain)と呼びます．トップレベルドメインの下にある，acやcoなどをセカンドレベルドメインと呼びます．ツリー構造では，上の層にあるものを親，下の層にあるものを子と呼びますので，あるドメインがあるドメインの下に来る場合，上に位置しているドメインを「親ドメイン」，下に位置しているドメイン

を「子ドメイン」と呼びます．(サブドメインと子ドメインは同じことを意味しています．)

図3には，トップレベルドメインの上に”.”(ドット)があります．トップレベルドメインの親ドメインとして，「ルートドメイン」が存在し，”.”(ドット)で表します．ドメイン名は，実際はこのルートドメインを含んだ形 www.ics.teikyo-u.ac.jp. でも表すことができます．DNSを設定する際には，ドメイン名を，ルートドメインを含んだFQDNで表記します．

DNSでは，図3のようなツリー構造をもつドメインの情報を管理しています．ただし，1台のDNSサーバがすべての情報を持っているわけではありません．DNSサーバが管理しているのは，自分の子ドメイン(あるいはその子ドメイン･・・)の情報です．たとえば，jpドメインを管理するDNSサーバは，jpドメインのサブドメインであるacドメインやcoドメインを管理するDNSサーバの情報を持っていて，acドメインを管理するDNSサーバは，teikyo-uドメインやu-tokyoドメインを管理するDNSサーバについての情報を持っています．このように，DNSは，全体として，階層的にドメイン名を分散して管理する，分散型データベースシステムになっています．通常，DNSサーバはドメインツリーのあるノード(ドメイン)，あるいはその子ドメインを管理しています．DNSサーバの管理する，ドメイン名前空間の一部を「ゾーン」と呼びます．DNSサーバが管理しているのは，ゾーンの情報であるゾーンデータベースであると言えます．

ドメイン名からIPアドレスを調べることを「名前解決(Name Resolution)」といいます．ドメイン名からIPアドレスを取得することを「正引き」といい，これとは逆に，IPアドレスからドメイン名を取得することを「逆引き」といいます．

DNSのしくみ

DNSでは，たくさんのDNSサーバが分散してゾーンの情報を管理している，ということでした．このようなドメイン名前空間に存在する，あるドメイン名に対応するIPアドレスを調べる(名前解決を行う)手順を見ていきましょう．

図4に，あるクライアントから，www.ics.teikyo-u.ac.jp の名前解決をする手順を示します．

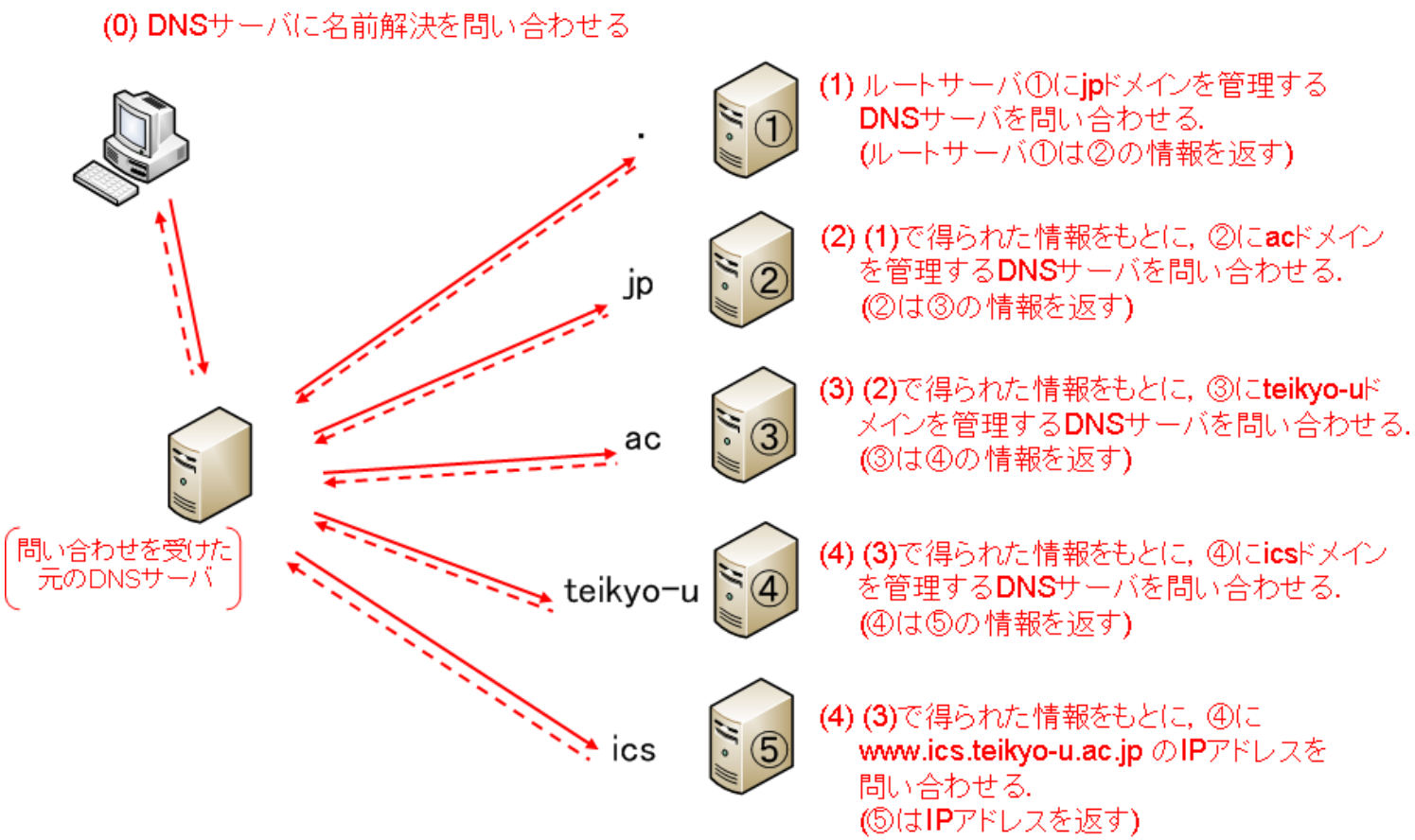

図4 DNSサーバにwww.ics.teikyo-u.ac.jp の名前解決を問い合わせた場合の処理

(0) クライアントは，クライアントから利用するように設定してあるDNSサーバに対して，www.ics.teikyo-u.ac.jp　の名前解決を要求します(図4の(0))．名前解決の要求を「問い合わせ」といいます．

(1) 問い合わせを受けたDNSサーバは，別のDNSサーバに問い合わせます．では，どのDNSサーバに問い合わせたらいいでしょう．ドメインツリーの最上位はルートドメインでしたが，ルートドメインを管理しているDNSサーバを「ルートサーバ」といいます．インターネット上には，世界に13台のルートサーバがあります．名前解決を要求されたDNSサーバは，まずルートサーバ(図4の①)のうちのどれかに，トップレベルドメイン(ここではjp)を管理するDNSサーバの情報を問い合わせます．すると，ルートサーバが，jpドメインを管理するDNSサーバ(図4の②)の情報を，元のDNSサーバに返します．

(2) 元のDNSサーバは，(1)で得られたDNSサーバ(図4の②)に対して，acドメインを管理するDNSサーバの情報を問い合わせます．②のDNSサーバはacドメインを管理するDNSサーバの情報(図4の③)を元のDNSサーバに返します．

(3) 元のDNSサーバは，(2)で得られた③のDNSサーバに対して，teikyo-uドメインを管理するDNSサーバの情報を問い合わせます．③のDNSサーバはteikyo-uドメインを管理するDNSサーバの情報(図4の④)を元のDNSサーバに返します．

(4) 元のDNSサーバは，(3)で得られた④のDNSサーバに対して，icsドメインを管理するDNSサーバの情報を問い合わせます．④のDNSサーバはicsドメインを管理するDNSサーバの情報(図4の⑤)を元のDNSサーバに返します．

(5) 元のDNSサーバは，(4)で得られた⑤のDNSサーバに対して，icsドメインにあるwwwというホストのIPアドレスを問い合わわせます．⑤のDNSサーバは，www.ics.teikyo-u.ac.jp のIPアドレスを元のDNSサーバに返します．

DNSサーバは，問い合わせがあったドメイン名を，ルートサーバから始めて，下層のゾーンを管理するDNSサーバの情報を再　帰的に問い合わせていきます．これを，求めるドメイン名のIPアドレスが取得できるまで繰り返します．このとき，jpドメイン，ac.jpドメイン，teikyo-u.ac.jpドメインを管理するDNSサーバの情報は，元のDNSサーバに一時的に保存されます．DNSサーバに保存されている，問い合わせの結果の情報を「キャッシュ」といいます．キャッシュを使うことで，同じドメインに関する問い合わせを減らし，トップレベルドメインやセカンドレベルドメインのDNSサーバへの負荷を低減しています．

ローカルDNSサーバの構築

通常DNSサーバを構築しようとする場合は，図4の④や⑤のような，インターネットに公開された，あるゾーンの情報を管理するDNSサーバを構築することになります．この場合，teikyo-uドメインを④のDNSサーバが管理しているという情報が，③のacドメインを管理する③のDNSサーバに登録されていなければなりません．また，icsドメインを⑤のDNSサーバが管理している棟情報が，④のDNSサーバに登録されていなければなりません．

この演習では，インターネットに公開できるドメイン名やIPアドレスを使っていませんので，図4の④や⑤のようなDNSサーバを構築することはできません．その代りに，図5に示す，次のような役割を持ったDNSサーバを構築します．

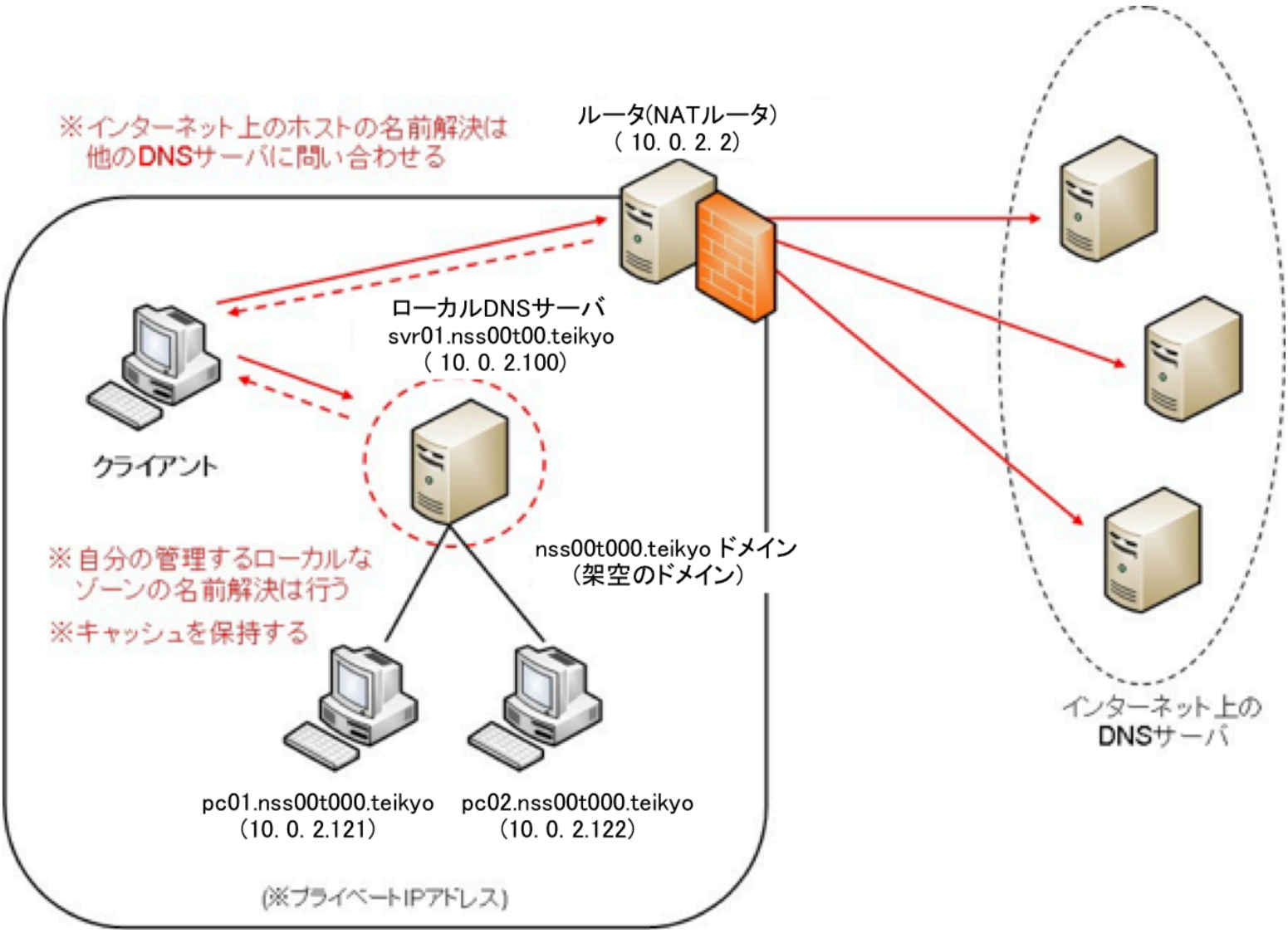

図**5** 演習で構築する**DNS**サーバの概要

○構築するローカルDNSサーバの役割
- ローカルドメイン(ゾーン)の管理
- キャッシング機能

演習環境のネットワークは，インターネットでは利用できない「プライベートネットワークアドレス(※1)」で構築されています．インターネットへは，NAT(IPマスカレードという場合もあります)(※2)という仕組みで，外部に接続するときは，ルータのグローバルIPアドレス(インターネットで使うことのできるIPアドレス)を利用しています．ルータはファイア

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

ウォールも兼ねており，セキュリティの関係上，HTTPなど一部を除いてLANの外側とは直接通信ができないようになっています．したがって，この演習で構築するDNSサーバは，ルートサーバへ問い合わせをすることができません．そのためインターネット上のホスト名の名前解決には外部のDNSサーバを利用することにします．このため，クライアントには複数のDNSサーバを登録することにします．

※**1** プライベートネットワークアドレス

インターネットに直接接続されていない(このIPアドレスがインターネットに出ていくことのない)，ローカルなネットワークで自由に用いることができるように，あらかじめ用意されているIPアドレスです．次のアドレスを使うことができます

```
Aクラス：10.0.0.0. ~ 10.255.255.255
Bクラス：172.16.0.0 ~ 172.31.255.255
Cクラス：192.168.0.0 ~ 192.168.255.255
```

プライベートアドレスに対して，インターネットで利用できるIPアドレスを「グローバルアドレス」といいます．

※**2 NAT**

NAT (Network Address Translation，ナットと読む)は，ネットワークアドレスを変換するための技術です．プライベートアドレスからグローバルアドレスへ変換するときによく用いられます．複数のプライベートアドレスを1つのグローバルアド　レスに対応