

ご購入はこちら

パケットづくりではじめる ネットワーク入門

第51回 応答も中継して簡易DNSプロキシを仕上げる

坂井 弘亮

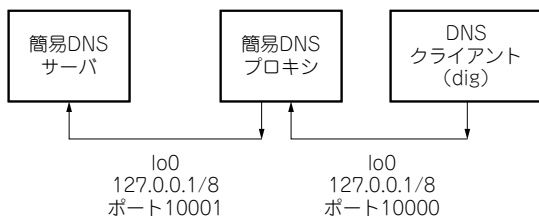


図1 サーバとクライアントの中継機能を持たせた簡易DNSプロキシの実験環境

本連載はネットワーク上を流れるパケットを直接扱うようなツールを自作しつつ、ネットワークの仕組みを勉強していきます。テーマは「自作」、「現物ベース」、「動く感動」の3つです。ネットワークにはイーサネットとIPを想定しています。

● 今回行うこと

前回まではUDPで最もよく利用されているサービスであろうDNSを題材として、簡易的なDNSサーバを作成し、さらにDNSプロキシの第1段階として、クライアントからの要求を中継する機能を実装しました。

今回は、サーバからの応答をクライアントに中継する機能を実装します(図1)。これにより、DNSプロキシとして動作させることが可能になります。

DNSプロキシとは

DNSはDomain Name System(ドメイン・ネーム・システム)の略で、www.cqpub.co.jpのようなホスト名からIPアドレスを取得するための、インターネット上に構築された分散型データベースです。

インターネット上での実際の通信のためにはIPアドレスが必要ですが、IPアドレスは例えば192.168.1.1というような、単なる数字の羅列になっています。

そこで「ホスト名」という、我々にとってより覚えやすい別名を定義し、ホスト名からIPアドレスを対応づけることができれば、通信先の指定はホスト名によって行えます。この名前解決を行うサービスが

DNSです。

● その1：高性能フルサービス・リゾルバ

DNSサーバは、例えばwww.sample.jpというホスト名に対する名前解決を行う場合、まずルート情報を持つDNSサーバからjpドメインのDNSサーバの情報を取得し、次にjpドメインのDNSサーバからsample.jpドメインのDNSサーバの情報を取得し、さらにsample.jpドメインのDNSサーバからwww.sample.jpの情報をとるように、段階的に名前解決を行います。

このようなことを行うDNSサーバはフルサービス・リゾルバと呼ばれますが、これらの処理は高負荷となり、安価な家庭用ルータなどで実現・管理することは負担が大きくなります。

● その2：簡易的DNSプロキシ

このためDNSの問い合わせをフルサービス・リゾルバに中継し、応答は問い合わせを行ったノードに中継するような機能が実現できれば、見かけ上は中継サーバをDNSサーバに見せかけて、各ノードに登録することができます。

このような中継サービスを、一般にDNSプロキシと呼びます。DNSプロキシにより、以下のようなことが低いコストで実現できます。

- 自身に登録されている情報ならば自身が答えることで、個別の名前解決が行える。
- 応答情報をキャッシュすることができれば、通信量を削減できる。
- 各ノードにはDNSプロキシをDNSサーバとして登録することで、中継先のDNSサーバが変更されても全ノードを設定変更することを避けられる。

プログラム

今回はDNSプロキシの実装の第1段階として、ノードからの名前解決の要求をDNSサーバに中継する機能を実装しています。