ファイアウォール内におけるDNS設定に関する一考察

7F－5

久保 孝弘　飯作 俊一　浅見 徹
国際電信電話株式会社 研究所

1. はじめに

社内LANをインターネットに接続する場合、セキュリティを確保するためにはファイアウォールを構築する必要がある。ファイアウォールを構築した場合には社外向きと社内向きのDNS(Domain Name System)サーバを設定する必要がある。その時社内向きDNSサーバがインターネットへ直接アクセスできないためアドレス解決に時間がかかる障害が発生し得る。本稿では、ファイアウォール環境下におけるDNSサーバの設定について調査したので報告する。

2. Domain Name System

DNSは、インターネットにおけるIPアドレスとドメイン名とを関係付けるシステムである。[1][2][3]

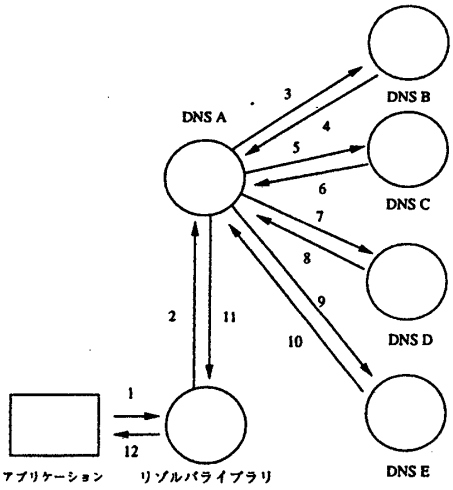

図 1: DNSの動作

ユーザアプリケーションからの問い合わせは

(1) まず端末のリゾルバライブラリがローカルのDNSサーバAに問い合わせを行なう。(図1中の2)

(2) 問い合わせの内容がDNS内に存在していれば応答する。(図1中の11) 存在していなければ、キャッシュ情報の中で一番情報を知っていると思われるDNSサーバに問い合わせを行なう。その際、ローカルのDNSサーバAの起動直後は、ルートキャッシュに登録されているDNSサーバBに問い合わせを行なう。(図1中の3)

DNSサーバBに問い合わせの内容が存在していれば応答し存在していなければ、次に一番知っていると思われるDNSサーバを問い合わせ元に通知する。(図1中の4)

(3) ローカルDNSサーバAでは、受けとった応答が、別のDNSサーバを指していたときは、そのDNSサーバに同じ問い合わせを行なう。(図1中の5,7,9)

インターネット環境では、上記の動作を繰り返すことによりアドレスを解決することができる。

3. ファイアウォール

ファイアウォールは、インターネット上でセキュリティを確保するための技術である。ネットワークを、インターネットに接続した場合、インターネットからのアタックに対してネットワークを守る必要がある。このためネットワークをインターネット接続用のバリアセグメントと、ローカルネットワークに分けルータによるパケットフィルタリングにより、インターネットからのパケットはバリアセグメントまで到達するが、ローカルネットワークには到達しないようにする。また、ローカルネットワークのパケットは、バリアセグメントには、到達するが、インターネットには、出ていかないようにする。(セキュリティを強化するために、ローカルネットワークからバリアセグメントに接続できる端末を限定する場合もある)

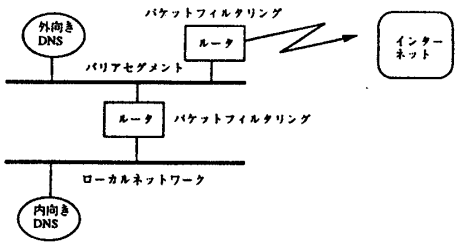

図 2: ファイアウォール環境

4. ファイアウォール環境におけるDNS

ファイアウォール環境においては、DNSサーバを外向きと内向きに分けて構築する必要がある。外向きDNSサーバは、バリアセグメントに設置され、インターネッ

"A Study on DNS setting inside the Firewall Network"
Takahiro KUBO, Shun-ichi IISAKU, and Tohru ASAMI
KDD R & D Laboratories

トに対して、自ドメインの情報を提供し、また、インターネットにドメイン情報の問い合わせを行なう。内向きDNSサーバは、ローカルネットワークの情報を保持しておりローカルネットワークの端末からの問い合わせに応答する。

この場合、ローカルネットワークの端末は、インターネットに直接アクセスできないので一般に図1に示した手続きによってインターネットのアドレスを解決することはできない。アドレスを解決できるようにするには次の方法が考えられている。[4]

- 方式1
  ローカルネットワークの端末のDNS設定を内向き、外向きDNSサーバ双方を参照するようにする。インターネットへの問い合わせは、外向きDNSサーバが行なう。
- 方式2
  内向きDNSが外向きDNSに問い合わせを行なう。

上記方法には、それぞれ以下のような問題がある。

- 方式1の問題
  ファイアウォールによっては、ローカルネットワークの端末が直接外向きDNSサーバにアクセスできない場合があり、アドレス解決ができない。また、外向きDNSサーバを変更したときには、全ての端末の設定を変更する必要があり、IBM-PC互換機やMacintosh等のクライアント端末使用ユーザにDNS設定の変更を強制することになる。

  DNSは、ドメイン名を各管理ゾーン別に分散管理するために開発されたシステムである。外向きDNSサーバが変更されてもローカルネットワークのDNSサーバの変更だけで対処できるようになっていなければ分散管理とは言えない。
- 方式2の問題
  内向きDNSサーバがインターネットにあるDNSサーバをキャッシュしてしまい、直接アクセスしようとしてタイムアウトしてしまう。これは、内向きDNSサーバが、インターネットに直接アクセスできないために起こる。

5. 解決方法

図3に示すように、各ローカルネットワーク上に外向きDNSサーバに唯一アクセスできる「問合せDNSサーバ」を構築し、各ローカルネットワーク上のDNSクライアント端末では、このDNSサーバと、内向きDNSサーバとを参照するようにする。

この場合は、問合せDNSサーバは、キャッシュのみのサーバにする。また、ローカルネットワークの他のDNSサーバが、このサーバの2次サーバになったり、このサーバをルートキャッシュやフォワーダに入れたりしないようにする。この方法を採用することにより、インターネットのセキュリティを保ちながら、ローカルネットワークのドメイン名の分散管理を行なうことができる。

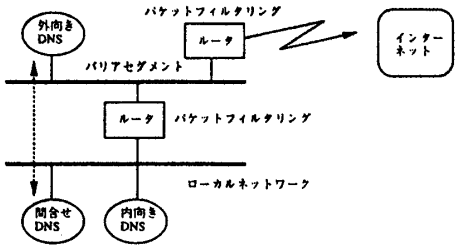

図 3: ファイアウォール内 DNS サーバの分散管理

6. 考察

図3の場合は、ローカルネットワークの各サブドメインに問合せDNSサーバを構築する必要があり計算機リソースを無駄使いしてしまうことと、問合せDNSサーバの台数分だけルータのフィルタを解放するため、セキュリティが弱体化する問題がある。

このため、以下のような方法でインターネット側とローカルのドメイン名も分散管理できるような実装を行なうことが今後の課題である。

(1) ローカルドメインとその他のインターネットドメインとを区別して管理する。
(2) 端末からの問い合せに対して、ローカルドメインの時は、内向きDNS情報を用いて応答し、インターネットドメインの時は、外向きDNSサーバに問い合せる。
(3) 他のDNSからの応答についても、内向きDNSと外向きDNSとを区別してキャッシュに格納する。

7. おわりに

本稿では、ファイアウォール環境でのDNS設定について報告した。最後に日頃御指導頂くKDD研究所 浦野所長、福光次長に感謝します。

参考文献

[1] M.Lottot, "DOMAIN ADMINISTRATORS OPERATIONS GUIDE," RFC-1033, IETF, Nov. 1987.
[2] P.Mockapetris, "DOMAIN NAMES - CONCEPTS AND FACILITIES," RFC-1034, IETF, Nov. 1987.
[3] P.Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION," RFC-1035, IETF, Nov. 1987.
[4] P.Albits and C Liu, "DNS and BIND," 319-326, O'Reilly & Associates INC., 1992.