ダイヤルアップ型 ADSL のための DNS 支援手法

力武 健次　菊地 高広　永田 宏　濱井 龍明　浅見 徹

株式会社 KDDI 研究所 高信頼 IP ネットワーク技術プロジェクト

ADSL(非対称デジタル加入者線) のインターネット接続では、多くの場合ダイヤルアップ型、つまり IP アドレスの割り当ては動的に変化することが前提である。本稿ではダイヤルアップ型 ADSL 接続機器を外部から接続可能にする時起こる DNS 上のセキュリティ問題を考察し、既存の DNS サーバーを利用した解決手法を示す。

Practical DNS Support for Dialup ADSL

Kenji Rikitake, Takahiro Kikuchi, Hiroshi Nagata, Tatsuaki Hamai and Tohru Asami

High Quality Internet Project, KDDI R&D Laboratories Inc.

In most installations of ADSL (Asynchronous Digital Subscriber Link), the Internet connectivity is treated as a dialup link, which means the assigned IP address to the connected equipment dynamically changes. In this paper, we analyze the DNS security issues when connecting to the equipment over a dialup ADSL, and propose a method to solve the issues using the existing DNS servers.

1　はじめに

個人や小規模事業所のインターネットへの安価な常時接続アクセス手段として、ADSL（非対称デジタル加入者線）が 2001 年に入って爆発的に普及している。

総務省 [1] によれば、DSL（デジタル加入者線）の加入者数は、2000 年 12 月末には 9723 回線だったのに対し、2001 年 8 月末には 510339 回線と指数関数的な伸びを示している。この伸びを受け、個人向けの ADSL サービスを提供する ADSL 回線事業者や ISP (Internet Service Provider) 間では、2001 年 9 月から月額 3017 円で加入者収容局から利用者への下り速度が最大で 8Mbps に達するサービス（Yahoo!BB）の登場により、月額 2400〜4500 円程度の価格帯のサービスが一般的な状況となった [2]。この価格は世界各国の中でも最も安価な部類に入る。

一方、より高品質な企業向け ADSL サービスをインターネットアクセス回線として提供する業者も増えている [3]。これらは既存のデジタル専用回線の置き換えを狙っているため、価格は月額 1 万円〜5 万円程度であり、個人向けサービスに比べ 5〜10 倍程度の価格となっている。

個人向けと企業向け ADSL サービスの価格の違いには、利用者への IP (Internet Protocol) アドレスの割り当て方法の違いが反映されていると考えられる。個人向けサービスの多くは、IP アドレスを利用者に動的に割り当てるダイヤルアップ型であるため、外部から利用者の機器に接続する形

での利用が困難である。これは ISP にとってはアドレス管理の手間を省け経費を節減できるが、利用者から見れば双方向接続を前提とするインターネット技術の利便性を著しく損う。一方、企業向けサービスでは、IP アドレスの固定ブロックを割り当てることが前提であり、外部から接続する際の問題はない。しかし、すでに固定アドレスの割り当てを受けている利用者にとっては、固定アドレスのためだけに従来のデジタル専用回線の場合とほぼ同等の費用を払わねばならず、新規導入の利点が薄れる。

仮にダイヤルアップ型 ADSL サービスに接続した機器に対し、既存の DNS (Domain Name System) サーバを利用して外部から安全に利用できる方法が実現できれば、既存のインターネット環境に個人向け ADSL 回線を新たに追加することで、安価に利用可能帯域を増やし利便性を向上させることができる。本論文では、ダイヤルアップ型 ADSL サービスに接続した機器への外部からの接続を可能にする際に起こるセキュリティ上の問題を考察すると共に、既存の DNS サーバを利用して外部接続を行う方式を提案する。

2 ダイヤルアップ接続固有の問題

2.1 動的 IP アドレスの一般的利用形態

一般的なダイヤルアップ型接続では、ISP から IP アドレスを一つだけ割り当てられる。このアドレスは切断や再接続、一定時間以上の同一アドレス占有などの場合に、ISP が一方的に変更する。利用者側では、割り当てられた IP アドレスの値は知ることができるが、それがいつ変わるかを事前に知ることはできない。

このような環境下では一般的な機器接続方法として、NAT (Network Address Translation) と NAPT（Network Address Port Translation, IP Masquerade とも呼ばれる）が使われる。

NAT では IP パケット内の送受信アドレスを付け替える。静的 NAT では対応付けを固定して変換する。動的 NAT では必要に応じて変換前後のアドレスの対応付けを変えることで、 ISP から割り当てられたアドレスを利用者側の複数のプライベートアドレス [11] を持つ機器で共有する。ただし、NAT 単独では複数の利用者側機器で同時に外部接続はできない。アドレスの対応付けができなくなるからである。

NAPT では、IP アドレスに加えてポート番号も変換する。動的な NAPT では、複数の利用者側の機器が同時に外部との通信をできるようになる。ただし、この方法では利用者側から外部への TCP (Transmission Control Protocol) 接続は（16bit 長のポート番号が枯渇しない限り）自由にできるが、逆はできない。外部から利用者側機器への TCP 接続をするには、あらかじめ静的な対応付けをしておく必要がある。UDP (User Datagram Protocol) を使う場合も同様である。

2.2 動的 IP アドレスでの外部接続

動的 NAT や NAPT では、一つの IP アドレスを複数の機器で共有することが目的である。しかし、これらの方法は利用者側から外部への接続を行う場合には適用できても、外部から利用者側の機器に接続するためには利用できない。

外部から利用者側の機器を利用可能にする最も単純かつ明確な方法は、利用者側で接続する機器を一つに限定し、ISP から割り当てられる IP アドレスをその機器に対応させることである。他の利用者側の機器はこの機器を中継用機器として利用する。この場合、ISP からは中継用機器だけが接続しているように見える。外部からの接続要求はこの中継用機器で受け付けることで対応できる。また、途中で静的 NAT が行われていても、アドレスの対応付けは固定であるため、外部から見たプロトコル上の透過性は高い。利用者側機器からの外部への通信要求は、代理サーバ (proxy server) などアプリケーション層での中継技術を使えば対応できる。

他の方法例としては、外部接続用ルータで最低限必要なプロトコルだけ静的 NAT および NAPT による対応付けを行うやり方がある。しかし、この方法では利用者側の機器と外部接続のポート番号との対応付けが複雑になり、セキュリティ上重要なポート番号などによるアクセス制限が行いにくくなるため、本研究では採用しないこととした。

2.3 動的 IP アドレス情報の取得

ダイヤルアップ型接続の場合、ISP から割り当てられる IP アドレスの情報をどのようにして取得するかという問題が生じる。解決方法としては、ISP からのアドレス変更要求を検知して情報を得るか、あるいは定期的に割り当てられているアドレスの値をポーリングして確認するかの 2 つがある。前者は PPPoE (PPP over Ethernet) [14] など、接続機器が直接アドレス情報を得られる場合に適している。一方、ADSL 接続専用のルータなどを介して接続している場合は、ISP からのアドレス情報はルータが持っているため、後者を適用し、接続機器からルータを定期的にポーリングしてアドレス情報を調べるのが現実的である。本研究では、後者を採用した。

3 システム設計

3.1 システム構成と前提条件

本研究では図 1 に示す接続形態を前提としてシステム設計を行った。この図のホスト X と Y には FreeBSD 4.3-STABLE を OS として使用している。これは FreeBSD が実験に必要なネットワーク設定上の柔軟性を備えていることによる。

図 1 で、ネットワーク B は固定アドレスブロックを持つ既設のネットワークである。これにホスト X を ADSL ISP との dual-home gateway として接続する。ADSL ルータは、割り当てられたアドレス A1 とホスト X の ADSL ISP 向けアドレス P2 との間の静的 NAT のみを行う。ホスト X は、ADSL ISP からの IP パケットを受信し、必要なプロトコルに対してのみ処理を行う。また、ネットワーク B から ADSL ISP へ向かう接続要求に対して、代理サーバなどでアプリケーション層の中継を行う。IP パケットの中継は行わない。ホスト X のデフォルト経路は ADSL ISP 側へ向ける。

この構成では、ホスト X をネットワーク B からの HTTP (HyperText Transfer Protocol) 代理サーバとして使用したり、ssh (secure shell) [16] を使いホスト X にログインしてから、さらに外部のホストへ ADSL 回線を通して接続するなど、一般的な dual-home gateway によるファイアウォールとして使うことができる。最近は家庭利用者の常時接続回線へのセキュリティ攻撃も頻繁に発生している [6]。本論文執筆時も頻繁に不正アクセスの試みが観測された。このような状況下では、防衛上の観点からも図 1 のような構成が適切であると考えられる。

3.2 DNS サーバの運用と情報更新

動的に変化する IP アドレスを持つ機器へ外部から接続するためには、その機器に固定したホスト名を割り当て、DNS サーバで IP アドレスと対応付ける必要がある。図 1 の構成では、アドレス A1 がホスト X に対応している旨知らせるための DNS サーバが必要になる。この DNS サーバのアドレスは上位サーバへ登録されるため固定されていることが必要で、ホスト X 自身では DNS サーバを動かすことはできない。この問題はネットワーク B 上の固定アドレスを持つ別のホスト Y で DNS サーバを動かすことによって解決できる。

実際の DNS サーバの運用と情報更新は、以下の手順で行う。

- ホスト Y は本研究の実験と直接関連しない DNS サーバ (アドレス B2) も運用しているため、実験用のサーバはアドレス B3 で別途動かす。このサーバはホスト X に関する情報のみを提供する。
- ホスト X とアドレス A1 の対応付けを行うには、ホスト X から ADSL ルータを定期的にポーリングしてアドレス A1 の値に変化がないか、あるいは回線切断などの異常が起きていないかどうかを確認する。実際に検知する情報は、アドレス A1 の値（あるいは未割り当ての状態）と、直前のポーリングの際とアドレスが同じか違っているかどうかの 2 つである。これらの情報はホスト X で保持する。
- ホスト X はアドレス A1 の状態に変化が生じたことを検知したら、ホスト Y 上の DNS サーバ (アドレス B3) の登録情報を更新する。この DNS サーバはホスト X の情報のみを保持しているため、更新には登録情報ファイル

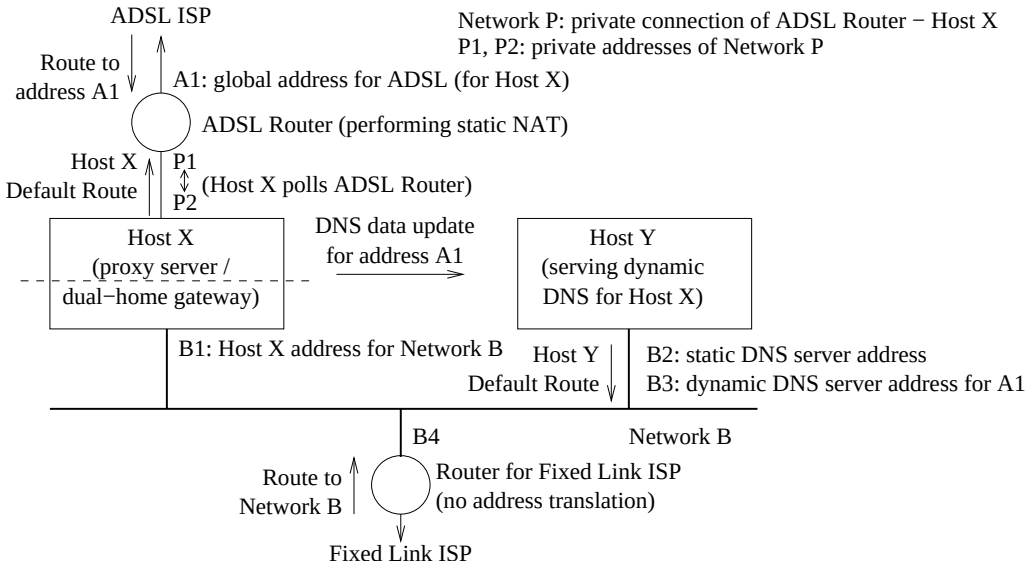

図 1: ADSL 回線と既存ネットワークの接続図

を書き換えれば良い。

DNS サーバは、djbdns [9] 中の tinydns を使用した。tinydns は特定アドレスの UDP ポート 53 への DNS 処理要求に対して、高速検索できるデータベース cdb [7] を参照し応答する単機能のプログラムであり、安全性も高い。データベースの情報更新は、ホスト Y 上の更新プログラムをホスト X から ssh で起動することで行っている。セキュリティ事故の可能性を減らすため、ホスト X のアドレス監視プロセスと、ホスト Y の DNS サーバとデータベース更新プログラムは、それぞれ専用の非特権ユーザで動かしている。

4 実装と考察

4.1 実験環境と実装評価

筆者の一人力武は自宅からテレワークの際に生じる技術的・社会的問題に関する研究を行っている [10]。本論文の実験はこの研究のテレワーク環境構築作業の一部として行った。

力武自宅のネットワーク構成は図 1 に準拠している。ADSL 回線では PPPoA (PPP over AAL5/ATM) [13] を採用しており、ADSL ルータにアドレス A1 が割り振られる。この ADSL ルータでは ISP が NAT による利用を要請しているため、静的 NAT を行いホスト X はアドレス P2 で受けている。また、ネットワーク B の外部接続には既設の専用回線を使い、ネットマスク/28（ホスト 16 個分）の固定アドレスブロックの割り当てを受けている。

実験ではホスト X から ADSL ルータに約 30 秒に 1 度ポーリングを行い、アドレス A1 に変動があれば、変動後のアドレス（あるいは接続が切れたという情報）をホスト Y 上のアドレス B3 で動いている DNS サーバのデータベースに逐一反映している。実際にはホスト X の名前に対応した DNS の A リソースレコードを提供することで、ホスト X へ ADSL 経由で外部から到達できるようにしている。接続が切れた場合は、A リソースレコードを消去する。これは、以前のアドレスへ別の機器が割り当てられた場合の誤接続の可能性を減らすためである。ホスト X の名前に対応する DNS サーバはアドレス B3 で動いているものだけであるため、DNS 情報の伝播遅延の問題は生じない。

リソースレコードの有効期間 (TTL) は 30 秒に設定している。これは上記のポーリング間隔を反

映したものである。また、ADSL 回線は一度接続が切れると再接続が完了しアドレスが確定するまで実測で 30〜40 秒かかる。これらの理由から、ポーリング間隔は現状程度で問題ないと考えられる。ADSL ルータの電源を切って入れ直すことで切断状況を作り出した限りでは、リソースレコードの消去から 4 回のポーリング、つまり 2 分程度でリソースレコードが復帰している。また、ADSL 回線のアドレスの変更頻度は長い場合は数日に一回、短くても数十分に一度と頻度は少ないため、実用上は問題ないものと思われる。

実際に DNS サーバの動作を確認するため、外部からホスト X の名前で TCP 接続を試みた限りでは、毎回失敗なく接続できた。これにより、本研究の最初の目標である外部接続性の実現は達成できたものといえる。

本研究では一つの ADSL 接続に対して単独の DNS サーバを対応させることで、複数の更新要求が同時に発生した場合の排他制御の問題を回避している。複数の接続に対して単独の DNS サーバでデータベースを共用するためには、内容更新の際に排他制御が必要になる。この方法の実装は今後の課題である。

4.2 類似手法とその評価

本研究と類似の機能と目的を持つプログラムとして、DHIS (Dynamic Host Information System) [8] がある。DHIS では UDP 上の専用プロトコルで IP アドレスの変動するホストから専用サーバが定期的にポーリングを受けて相手ホストを認証することで、アドレスとホスト名の対応付けを行う。しかし、DHIS を DNS 情報の更新に使うためには、BIND (Berkeley Internet Name Domain) [4] の DNS UPDATE プロトコル [12] を使う必要があった。BIND はセキュリティ上多くの問題を抱えており [5]、本研究の実験環境には不適当と判断した。そのため DHIS も本研究では評価していない。ただし、DHIS の仕組み自身はすでに運用実績があり、今後の研究用素材としては有望と思われる。

DNS UPDATE は、Microsoft の Active Directory で使われるなど普及しつつある。しかし、DNS UPDATE では原理的に外部からの DNS パケットだけで DNS データベースの更新ができるため更新要求の認証が必要だが、実際の認証手順はまだ発展途上である [15]。本研究ではまず単独のダイヤルアップ型接続に対応できる仕組みを作ることが目標であり、DNS UPDATE ほどの大規模かつ複雑な仕組みは必要ないと判断した。本研究での DNS データベース更新方式は ssh の公開鍵認証と暗号化で安全性を確保しており、DNS UPDATE に比べ問題は少ないといえる。

4.3 ダイヤルアップ接続の本質的な問題

一般的には一定範囲のアドレスブロックを複数の利用者が共用する場合は、DNS のホスト名と IP アドレスの対応に依存した認証は安全ではない。相手が知らない間に別のホストに変わっている可能性があるからである。ssh など公開鍵認証の応用では、各ホストが秘密鍵を持つことで、クライアントと相互に認証してホストのなりすましを防いでいる。今後は IP アドレスに依存しない認証方式の普及が必要であろう。

本研究の実装方式でも、動的 IP アドレスが変わった瞬間の接続性を迅速に確保することはできていない。これを実現するためには、ISP から利用者へアドレス変更の際の通知を明示的に行う仕組みが必要である。本研究の環境では実験できなかったが、例えば PPPoE で直接ホスト OS のインターフェースにアドレスが割り当てられる事例では、OS カーネルで情報が把握できるのでより迅速な対応が可能と考えられる。

仮にダイヤルアップ接続の場合でも、各利用者に固定 IP アドレスを割り振ることができるとすれば、本研究の課題とした問題はほぼ解決する。しかし、IPv4 ではアドレスは有限の資源であり、その利用は技術的側面よりも社会的また経済的理由で現在は決まっている。また IPv6 でアドレス空間が広がっても動的 IP アドレス割り当ては必要に応じて使われることが予想されるため、本研究の提案は応用可能であると考えられる。

5 まとめ

本研究では、ダイヤルアップ型 ADSL 接続の際の動的に変化する IP アドレスを、既設の固定 IP アドレスネットワーク上にある DNS サーバで対応づけるための実装方式を提案し、単独の ADSL 回線に対して提案方式が有効であることを示した。本研究の方式は、基本的に ADSL だけでなくダイヤルアップ型接続全てに応用が可能であるため、ISDN やケーブルテレビなどの個人向け常時接続サービスの利用でも有効であると予想される。

今後の検討課題としては、多数の動的 IP アドレスを処理する際のスケーラビリティの確保、また割り当てアドレスの変化への迅速な追従を可能にすることがある。

謝辞

本研究を進めるにあたり、ご助力いただいた株式会社 KDDI 研究所インターネットアプリケーショングループ主任研究員 松本一則氏、また同研究所ネットワークエンジニアリンググループ主査堀田孝男氏に深く感謝する。

参考文献

[1] 総務省総合通信基盤局電気通信事業部電気通信技術システム課：DSL 普及情報公開ページ、http://www.joho.soumu.go.jp/whatsnew/dsl/

[2] 阿蘇和人：ADSL インターネット値下げの波紋 Yahoo!追随で事業者は疲弊 展望なきまま我慢比べに突入、日経コミュニケーション 2001 年 9 月 3 日号、日経 BP 社、No. 349, pp. 67–69 (2001).

[3] 阿蘇和人：企業向け ADSL サービス 専用線並みの高品質タイプも登場 IP アドレスの配布方法に注意、日経コミュニケーション 2001 年 9 月 3 日号、日経 BP 社、No. 349, pp. 112–119 (2001).

[4] Internet Software Consortium: BIND, http://www.isc.org/bind/

[5] CERT/CC: Multiple Vulnerabilities in BIND, CERT Advisory CA-2001-02 (last revised: August 07, 2001). http://www.cert.org/advisories/CA-2001-02.html

[6] CERT/CC: Continuing Threats to Home Users, CERT Advisory CA-2001-20 (last revised: July 23, 2001). http://www.cert.org/advisories/CA-2001-20.html

[7] Daniel J. Bernstein: cdb, http://cr.yp.to/cdb.html

[8] Dynamic Host Information System, http://www.dhis.org/dhis/

[9] Daniel J. Bernstein: djbdns, http://cr.yp.to/djbdns.html

[10] 力武健次、菊地高広、永田宏、橋本和夫、浅見徹：インターネット VPN による安価なテレワーク環境の構築とその問題点の解決、ヒューマンインターフェース学会 HIS2001 シンポジウム論文集 (2001).

[11] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear: Allocation for Private Internets, RFC1918 (Also BCP5) (1996).

[12] P. Vixie (Editor), S. Thomson, Y. Rekhter, J. Bound: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC2136 (1997).

[13] G. Gross, M. Kaycee, A. Lin, A. Malis, J. Stephens: PPP Over AAL5, RFC2364 (1998).

[14] L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, and R. Wheeler: A Method for Transmitting PPP Over Ethernet (PPPoE), RFC2516 (1999).

[15] B. Wellington: Secure Domain Name System (DNS) Dynamic Update, RFC3007 (2000).

[16] Daniel J. Barrett, and Richard E. Silverman: *SSH, The Secure Shell: The Definitive Guide*, O'Reilly & Associates (2001).