ビジネス開発者必須講座

P2P/ブロードバンド時代の新・TCP/IP入門

村上 健一郎　法政大学ビジネススクール イノベーション・マネジメント研究科　教授

第9回　Skypeの呼制御とNAT越えを学ぼう

前回は、Skypeと従来のIP電話の代表であるSIPとの違いを中心に、その構造について説明しました。今回は、Skypeの呼制御やどのようにNATやファイアウォールを越えて音声を伝えるかを説明します。

[Q1]

Skypeはどのように呼制御を行っているのですか？

[A1]

コンタクトリストをクリック

Skypeでは、ログイン時にネットワーク環境やコンタクトリストに入っている相手の状態などを収集します。また、相手の状態は、随時このコンタクトリストに反映されます。

コンタクトリストとは電話帳のようなもので、仲間の名前を登録しておきます。こうすると、クリックするだけで電話をかけることができます。また、相手が電話に出られる状態かどうかについても、電話をする前にこのリストでわかります。コンタクトリストの表示例を図1に示します。

なお、これまでは、コンタクトリストは自分のパソコンに保存されていましたが、これでは、パソコンごとに登録するという不便さがあるので、Skypeのソフトウェアバージョン1.2では、ネットワーク側にそれを保持し、ログイン時にダウンロードするように改められました。

200のスーパーノードを持つ一般ノード

呼制御では、どの電話サービスでも、まず「電話番号」あるいは「識別子」が必要となります。Skypeの場合は、ソフトウェアをインストールする時に、他の人と重複することのないユーザー名（Skype名）とパスワードを登録します。このSkype名が自分の電話番号になるのです。たとえば図1の‘skype-lover’や‘catherine’などです。Skypeソフトウェアを起動するごとに、ログインサーバーで認証を受けますが、この時には、このSkype名とパスワードが使用されます。認証されると、暗号化のための鍵（の種）が渡されます。というのは、呼制御や音声データの転送は暗号化されるからです。

以前は、Skypeでは唯一のログインサーバーが用意されており、これにすべてのユーザーがログインしていました。しかし、これがダウンしてしまうとまったく使えなくなる危険性があるため、現在では、ログインサーバーの分散を図っているようです。

ログイン直後には、自分の状態を中継ノードである「スーパーノード」（一般ノー

図1　コンタクトリスト表示例
（http://www.skype.com/intl/ja/products/より引用）

ドから選択されたノード）を介してネットワークに通知します。これで、自分をコンタクトリストに登録しているすべての仲間に、状態の変化が伝わります。

また、自分のパソコンがどのような種類のNAT（IPアドレス変換機能付きルーター、後述）やファイアウォールを介してインターネットに接続されているかについても判別しておきます。たとえば、スーパーノードからUDP（User Datagram Protocol）を当該パソコン（自分のパソコン）へ送ってみて、もし、当該パソコンが何も受信できなければ、これはUDPがフィルターされたファイアウォールを介しているものと判断します。この情報は、後の呼制御の時に使用されることになります。

なお、ログイン後は、一般ノードは少なくとも1つのスーパーノードと常にTCPで接続されています。また、一般ノードは約200のスーパーノードのリスト（IPアドレスやサービスを受け付けるポート番号など）を保持しています。これをHC（Host Cache、ホストキャッシュ）と呼びます。リストは2時間ごとに更新され、平均のスーパーノードの生存時間は2.5時間と言われています※1。

Skype名（ユーザー名）の検索

コンタクトリストでは、相手がどのような状態にあるか、たとえば「オフラインである」「電話を受けることができる」などがわかるようになっています。なお、設定によっては、相手に状態を通知しないようにすることも可能です。

これらの状態を、ログイン時に把握してコンタクトリストに表示します。図1では、Skype名の左にアイコンでこれが示されています。

この状態を把握するため、一般ノードはスーパーノードに対して検索を依頼するためのノード群を要求します。これに対してスーパーノードは、4つのスーパーノードのIPアドレスを示し、それらへ分散して検索要求を送るように指示します※2。

検索要求を受けるスーパーノードは、一般ノードの機能である電話をかけたり受けたりする機能に加え、Skype名とそのパソコンの実際のIPアドレスとの対応表、つまり、電話番号簿を保持しています。しかし、SIPのように集中して記憶するのではなく、ネットワーク中のスーパーノードで分散して保持しています。

Skypeの呼制御を見てみよう

Skypeでは、一般ノードが発呼する時には、すでに、相手の状態やIPアドレス、どのような装置（NATやファイアウォール）を介して相手がインターネットに接続されているかなどがわかっています。ですから、もし発呼側のパソコンと着呼側のパソコンが両方ともグローバルIPアドレスを持つならば、呼制御は簡単です。発呼側は着呼側に直接TCPのコネクションを確立して接続要求を送り（①）、それが受理されれば、会話が始まります（②）。この音声はUDPを使用して送られます〔図2（a）〕。

もし、片方がNATやファイアウォールで接続されている場合には、そちら側から先に音声のためのUDPパケットを送ればよいのです。これは、スーパーノードがTCPで指示します。

しかし、もし相手がNATを介して接続されていれば、着呼時にはスーパーノードの手を借りてブロックされているUDPのポートに音声通信用の穴をあけなければなりません。このとき、着呼側の一般ノードには、それが接続しているスーパーノードからTCPで着呼要求が送られてきます〔図2（b）①、②〕。これによって、NATの穴あけがはじまります。実際の穴あけは、介在する装置の種類によって方法が違いますから、後で詳しく説明することにしましょう。

穴をあけることができない場合には、スーパーノードが音声を中継して発呼側と着呼側の間で音声通信を行います〔図2（b）③〕。また、UDPをまったく通さないファイアウォールなどの場合には、TCPで音声を運びます。

なお、Skypeのプロトコルは公開されておらず、ソフトウェアのアップデートに伴って変更されています。したがって、ここでの記述が正確ではない場合があることを、お断りしておきます。

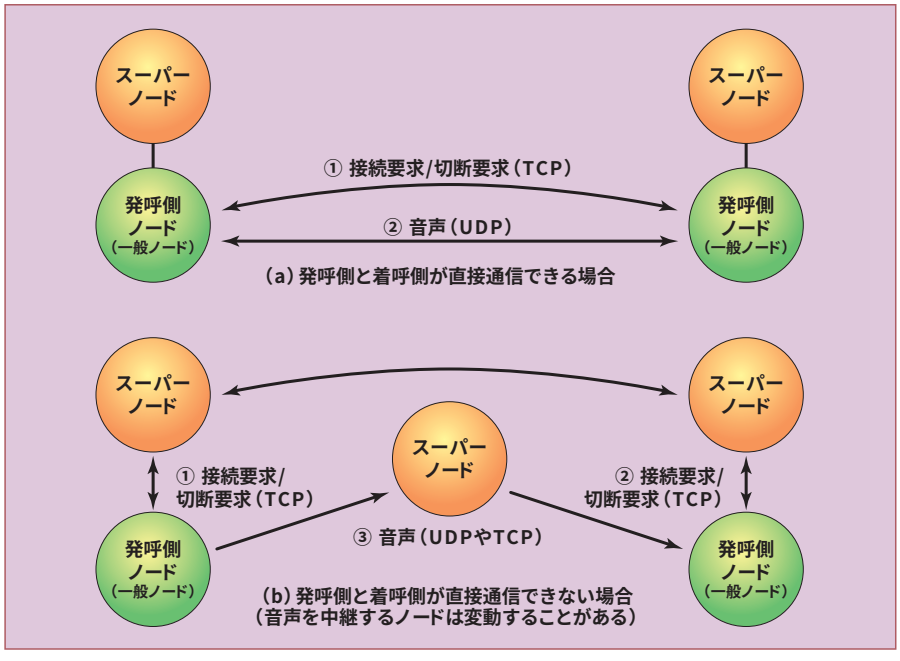


図2　Skypeにおける呼制御と音声の転送経路

[Q2]

IPアドレスの変換やファイアウォールの穴あけの制御は、どのように行うのでしょうか？

[A2]

P2Pアプリの使えないインターネットアーキテクチャー

NAT（Network Address Translation、IPアドレスの変換）やファイアウォールの制御を理解するには、まず、現在のインターネットアーキテクチャーを整理しておきましょう。

インターネットが作られた当初は、すべてのコンピュータは、直接インターネットに接続されていました。しかし、アドレスの有効利用やセキュリティーの確保のために、現在では、多くの企業や家庭が、NATやファイアウォールを通して接続されています。つまり、当初は、インターネットは1つのネットワークだったのが、今では、中心のインターネットバックボーンと、その外側にNATやファイアウォールで接続されたイントラネット群との2階層で構成されたネットワークアーキテクチャーに変わりました（図3）。

NATやファイアウォールのために、インターネット側からイントラネット側へはアクセスできません。しかし、ほとんどの利用者は困りません。なぜならば、インターネット上にあるサーバーで提供されるウェブや電子メールのサービスを利用するだけだからです。

ところが、IP電話のようにインターネット経由でパソコン同士が直接通信する必要が生じた場合には、これが障害となってサービスが実現できません。それでは、Skypeなどのような P2P アプリケーションは、どのようにしてこれを回避しているのでしょうか？

表1　4種類のNAT

	NATの種類	処理の軽さ	セキュリティーの堅さ
1	full core	↑ 軽い	↓ 堅い
2	restricted core		
3	port restricted core		
4	symmetric		

P2Pを可能にする2つの方法

P2P通信を可能にするには、次のような方法があります。

(1) バックボーンに直接接続されたサーバーを用意し、それが音声を中継する方法

(2) RFC 3489で規定されたSTUN（Simple Traversal of UDP through NATs）に代表されるNATを巧みに制御して、ピンポイントで直接通信するための穴をあける方法、あるいは、NAT自身に穴を制御する機能を入れるUPnP（Universal Plug and Play）という方式を利用する方法

(1)には、サーバーを経由するために、遅延が増大してスループットが落ちるという問題があります。(2)で挙げたUPnPは、必ずしもすべてのNATが実装しているわけではありません。そこで、SkypeはSTUNと同じような方法で穴あけを試み、それが駄目であればスーパーノードが音声を中継するというアプローチを採っています（なお、現在のバージョンでは、UPnPも使えるようです）。

他のIP電話やファイル転送などのP2Pアプリケーションの中にも同様のアプローチを採るものがあります。たとえば、検索サービスを提供しているグーグルは、Skypeのような電話サービスをGoogle Talkというインスタントメッセンジャーで提供しています。

NATによるP2P通信

現在のNATは、アドレスの変換方式によって表1のように4つの種類に分けられます。このうち、STUNでUDPポートに穴をあけることができるのは、1～3のNATです。この場合には、図2(a)のように、発呼側と着呼側のノードは直接音声を送ることができます。

一方、4のsymmetric NATやUDPをまったく通さないファイアウォールの場合には、直接音声を送れないため、Skypeは図2(b)のように、スーパーノードを介して音声を送ることになります。このとき、一般ノードは、音声を中継しているスーパーノード以外に、常に4、5個のスーパーノードと通信しており、それぞれの接続遅延や負荷の情報を得ています。そして、状態の良いものがあれば、次第に中継ノードを変更していきます。たとえば、135分間の会話中に4回

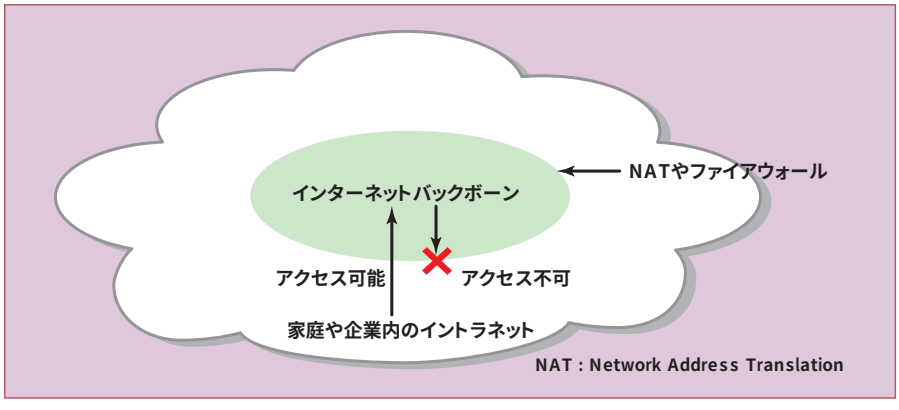


図3　現在の2階層のインターネットアーキテクチャー

の切り替わりがあったことも報告されています※2。

この仕組みのおかげで、中継ノードが突然停止したり、そこまでのネットワークが切れたりしても、次善のスーパーノードへ中継を引き継ぐことができるのです。

実際の穴あけを見てみよう

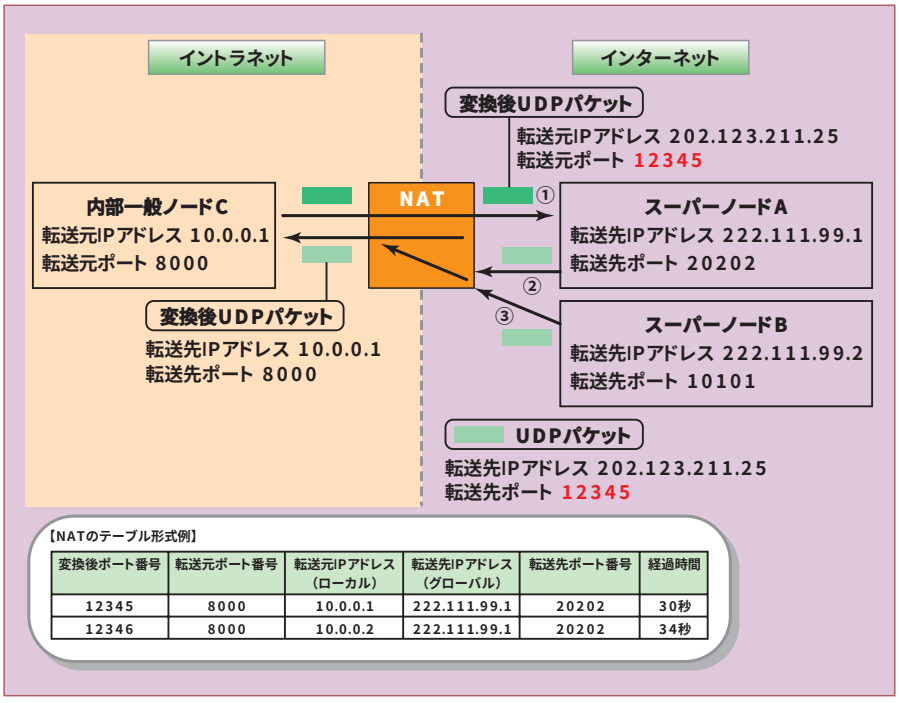
UDPの穴をあけ、その穴のIPアドレスとUDPポート番号を、外部のノードが知るためには、NATの内側のノード(家庭内や企業内の一般ノードC)から外のスーパーノードAへパケットを送ればよいのです(図4の①)。NATは、インターネット側へUDPパケットを転送する時には、(内部ノードCの)転送元IPアドレスと転送元ポート番号を書き換えます。

ここでは、図4の例で説明します。書き換え後の転送元IPアドレスは、常にNATの持つグローバルIPアドレス(202.123.211.25)です。書き換え後の転送元ポートは、このパケットに対する応答を受信した時に、ローカルIPアドレスを持つオリジナルの転送元に渡せるようにポート(12345)を割り振り、テーブルに記憶しておきます(図4中の表)。表1に示した「full core」「restricted core」、そして「port restricted core」は、転送先IPアドレスにかかわらず、転送元が同じローカルIPアドレスからの場合には、同じポート番号(12345)へ変換します。ですから、図4のノードCへ外部のスーパーノードAからパケットを送る時には、ポート番号12345を転送先ポートとしたパケットをNATへ送れば(図4の②)、NATはオリジナルのローカルアドレス(10.0.0.1)とポート番号(8000)に変換してノードCへ渡してくれます。

(1)full core

上記のように、変換後のポート番号さえわかれば、どの外部ノードからでもその番号に対応したローカルアドレスを持つ内部ノードへUDPパケットが送れます。

図4　full core NATの場合の穴あけ



変換後ポート番号	転送元ポート番号	転送元IPアドレス(ローカル)	転送先IPアドレス(グローバル)	転送先ポート番号	経過時間
12345	8000	10.0.0.1	222.111.99.1	20202	30秒
12346	8000	10.0.0.2	222.111.99.1	20202	34秒

(2)restricted core

一度転送した先のIPアドレスからでないと応答パケットを受理しません。ですから、CからはAだけでなくBにも、あらかじめパケットを送っておく必要があります。そうすれば、Bからのパケットも受理します(図4の③)

(3)port restricted core

IPアドレスに加え、これまでパケットを送ったことのある転送先ポート番号からのパケットしか受理しません。ですから、それ以外のポートを利用したいのであれば、それらを転送先ポートとして持つUDPパケットを、外部ノードへ送っておく必要があります。

表1に示したように、full core、restricted core、port restricted coreの順にセキュリティーが堅くなっていますので、穴をあける処理も同じ順番で複雑さが増しているというわけです。しかし、少なくとも穴をあけることは可能です。

一方、symmetric NATは、他の3つの種類のNATと大きく異なり、転送先のIPアドレスごとに変換するポート番号も異なるものになります。したがって、そのIPアドレスを転送元アドレスに持ち、しかも、それぞれの外部ノードごとに異なったポート番号を持つパケットしか受理しません。つまり、ポート番号はそれぞれの外部ノードごとに異なるので、特定のポート番号で一意に内部のホストを特定することができません。これではスーパーノードと協力してあけた穴はスーパーノード以外が利用できないので、スーパーノードが音声を中継することになります。

なお、NATで注意しなければならないのは、一定時間内に変換テーブルに該当するパケットが送られない場合、当該エントリーが消去されてしまうことです。そこでSkypeでは、定期的にkeep-alive(接続確認)パケットを転送することによって、その穴を開けたままにしておきます。

【参考文献】

※1　An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, Salman A. Baset and Henning Schulzrinne, Columbia University, http://www1.cs.columbia.edu/~salman/publications/baset_schulzrinne_04_01.pdf, September, 15, 2004
※2　Final Project : Skype, Frank Bulk, http://www1.cs.columbia.edu/~salman/skype/frank.pdf, May 5, 2004

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp