小≪ ○ ○ ○ ◉ ≫大 サイズ変更

検証 > ネットワーク管理者のためのSkype入門 第2回

検証
ネットワーク管理者のためのSkype入門 第2回

2. Skypeの高い接続性の秘密

デジタルアドバンテージ＋海津 智宏
2005/07/15

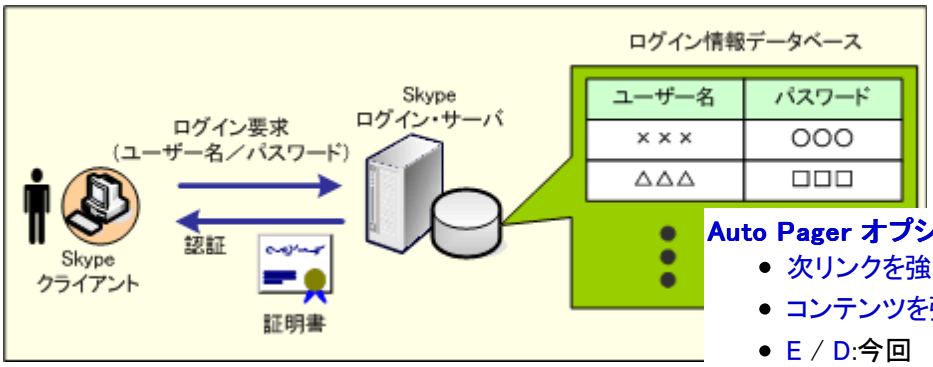
ログイン・サーバでのユーザー認証

Skypeネットワークに参加し、ほかのクライアントと通話するには、ログイン・サーバに接続して、ユーザー名とパスワードの認証を受ける必要がある。

ユーザー名は、Skypeネットワークでノードを識別する名前であり、システム全体でユニークであることが保証されている。Skypeを最初にインストールしたときには、適当な名前を指定してユーザー登録を行う必要があるが、この理由からすでに登録されている名前は使えない。

ログイン・サーバは、Skypeネットワークに登録されたすべてのユーザー名とパスワードの対応を一元管理している。ただし管理しているのはユーザー名とパスワードだけで、それ以外の個人情報（住所やメールアドレスなど）は保持しない。前回ご紹介したとおり、Skypeではユーザーごとにアイコン・ビットマップを指定したり、名前や性別、生年月日、住所、電話番号などを個人のプロフィールとして保存しておき、ほかのユーザーがこれらを検索できるようにしたりできる。しかしこれらの個人情報は、ログオン・サーバではなく、各Skypeクライアントのレジストリおよび設定フォルダ内に保存されるようになっている（プライバシー情報の扱いについては、次回に詳しく述べる）。

Skypeログイン・サーバに送信されたユーザー名とパスワードが正しければ、ログイン・サーバはSkypeによってデジタル署名された時間制限付きの証明書をSkypeクライアントに送り返す。Skypeのデジタル署名では、1536bitのRSA鍵が使用される。こうして返送される証明書により、Skypeユーザーは、Skypeネットワーク内で本人であることが識別可能になる。この証明書に対して、Skypeによる有効なデジタル署名が付けられていることを確認すれば、中央のサーバに問い合わせなくても、それが正しいユーザーであることを識別できるようになる。



Skypeログイン・サーバ

Skypeネットワークの唯一の中央サーバであるログイン・サーバは、たユーザーのユーザー名とパスワードを保持し、クライアントから応える。Skypeのログイン・サーバが保持しているのはユーザー

で、そのほかのプロフィール情報などは保持しない。認証に成功すると、Skypeネットワークでそのユーザーを識別可能にする証明書が返送される。証明書に加えられたSkypeのデジタル署名を確認することで、証明書が正しい(ユーザーが間違いなく本人であること)が識別できる。

必要なら、一度ログオンに成功したユーザー名/パスワードを使用して、次回からSkypeの起動時に自動ログオンさせる設定も可能である。ただし、複数のユーザーで共用するコンピュータなどではこのオプションを有効にしてはいけない。

Skypeの高い接続性の秘密 —— NATルータ越えのテクニック

ログイン認証を受けてSkypeネットワークに接続したら、適当な相手と接続して音声通話やチャットによる会話が可能になる。しかしここで問題がある。現在では、企業はもちろん、個人でも多くのユーザーが、インターネットの接続部分にNATルータやファイアウォールを設置し、プライベート・ネットワークを構成したり、外部から内部へのパケットをフィルタリングしたりしている。この目的の1つは、インターネットから内部ネットワークに対する不正アクセスを阻止することだが、代わりにVoIPシステムなど、特殊な通信がこれらによって制限される場合がある。

Skype最大の特徴は、ファイアウォールやNATルータの存在によって、ほかのメッセンジャー・ソフトウェアやVoIPソリューションでは通信不可能な環境においても、外部と接続して会話できることだ。接続性を向上させるため、Skypeはファイアウォールや NATルータを越えるためのさまざまな接続手段を持っており、環境によってそれらを切り替えている(コラム「NATルータとUDP」を参照)。

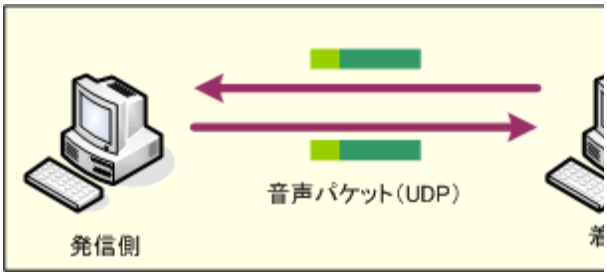
関連記事 Windows Server INSIDER
基礎から学ぶWindowsネットワーク(UDPプロトコル)

なお、必ずしも通信に100%の信頼性を必要としないVoIPソリューションでは、「信頼性はない」が、軽量で高速なプロトコルであるUDPが一般に使用される。信頼性がない、とは、送信したパケットが必ずしも相手に確実に届くという保証がなく(ネットワークが混雑していると欠落する可能性がある)、また送信した順番どおりに届くという保証もない(パケットの順番が入れ替わることがある)、ということを指す。しかしその分複雑な制御が一切不要なので、処理が簡単であり、システムへの負荷も少なくて済む。音声通信では、少々データが欠落しても問題にならないので(音質が多少劣化する程度)、UDPでも構わない。またUDPは、TCPでの接続が不可能な場合でも、後述するUDPホール・パンチングと呼ばれる手法によって、ファイアウォール/NATルータ越えが可能になる場合があるという特徴もある。Skypeの音声通話においても、基本的にはこのUDP接続が利用される。ただしSkypeは、UDP接続が不可能な環境においては、TCP接続を利用した音声パケットのルーティングも行う(詳細は後述)。

以後、ネットワーク環境のパターン別にSkypeの通信方法を述べる。まずはNATルータの存在について考慮し、ファイアウォールについては別途最後に言及する。

NATルータが存在しない場合(発信側/着信側コンピュータがグローバルIPを持つ場合)

これは最も簡単なケースで、Skypeに限らず、すべてのTCP/IPアプリケーションが何の障害もなく自由に通信できる。この場合、発信側/着信側双方のコンピュータにグローバルIPアドレスが割り当てられているので、インターネット内で双方が相手を識別し、通信パケットを直接相手に送信できる。



発信側／着信側の双方がグローバルIPを持つ場合

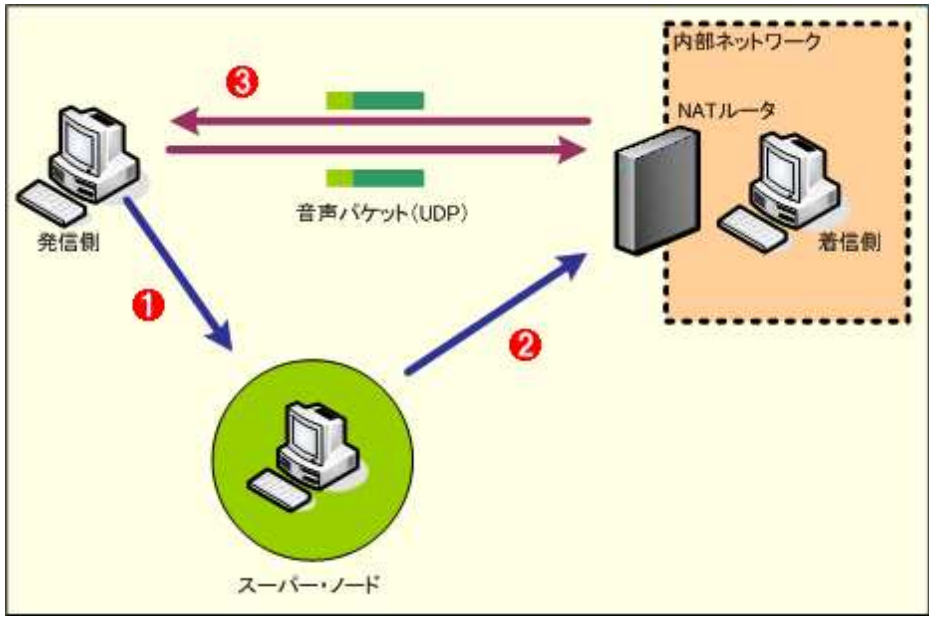
この場合は何の障害もないので、Skypeに限らずどのアプリケーションも相手と接続できる。発信側からUDPで着信側を呼び出し、着信側がこれに応答する。

着信側がNATルータの内側にいるとき／発信側がNATルータの内側にいるとき

着信側がNATルータの内側にいる場合、発信側は直接着信側コンピュータを呼び出すことができない。従ってこの場合発信側コンピュータは、着信側コンピュータを直接呼び出すのではなく、スーパー・ノードに依頼して着信側コンピュータを呼び出してもらう。スーパー・ノードは、制御用としてSkypeクライアントとのTCP接続を維持しているので、このルートを使えば、NATの内側にいるコンピュータを呼び出すことが可能だ。

この際着信側コンピュータには、スーパー・ノードから発信側コンピュータのグローバルIPアドレスと使用ポートが通知される。次に着信側コンピュータは、自分から発信側コンピュータに対してUDPプロトコルを使用して音声パケットを発信する。こうすれば、NATルータのNATテーブルにパケット通過用のエントリが作成され、着信側コンピュータもパケットを受信できるようになる。

これとは逆に、着信側コンピュータがグローバルIPアドレスを持っている場合には、問題なく発信側から着信側に向けてパケットを送出できる。



着信側がNATの内側に存在する場合

着信側がNATの内側に存在する場合、発信側はこれを直接呼び出すことはできない。スーパー・ノードは、SkypeクライアントとのTCPコネクションを持っているので、スーパー・ノードを経由して、着信側に呼び出しパケットを転送してもらう。続いて着信側が発信側に向けて音声パケットを送出させれば、NATがあっても問題なく双方向のパケット送受信が可能になる。

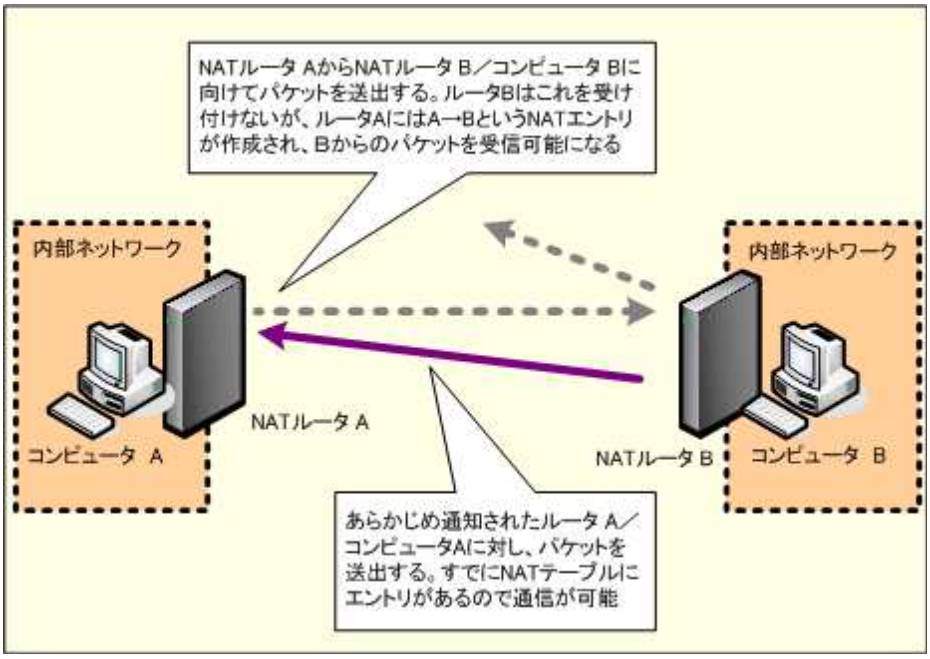
1. 直接呼び出すことができないので、発信側はまずスーパー
   る。
2. スーパー・ノードは、制御用としてすでに確立しているTCP
   て、着信側コンピュータへコマンドを送る。この際には、発
   グローバルIPアドレスとポート番号を通知する。
3. 通知されたIPアドレス:ポート番号を使って、着信側から発
   パケトを送出する。以後は双方向の送受信が可能になる。

発信側／着信側とも、NATルータの内側にいる場合

一方だけがNATルータの内側にいる場合の接続は比較的容易だったが、接続する双方がNATルータの内側にいる場合はこうは簡単にいかない。この状況で双方のコンピュータを接続するため、SkypeではUDPホール・パンチング（UDP hole punching）と呼ばれる手法を使って接続を試みる。

そもそもNATルータが使われている場合には、任意の2台のコンピュータ間で簡単に通信が行われてはまずいのだが（セキュリティが維持できなくなるから）、NATの仕組みをうまく使い、双方のノードが協調して動作すれば、UDPで通信を行うことが可能になる（UDPが通るなら、カプセル化などの手法を併用してTCP通信を行うことも不可能ではないだろうが、ここでは特に触れない）。このための1つの手法がUDPホール・パンチングである。ただし、あらゆる種類のNATルータに対してこの方法が適用できるわけではなく、ある特定のアルゴリズムを使っている、一部のNATルータにのみ対応可能な手法である。

UDPホール・パンチングの原理はこうだ。仮にコンピュータAとコンピュータBがそれぞれNATルータA、Bによってプライベート・ネットワーク内部にいるとする。



UDPホール・パンチングの原理

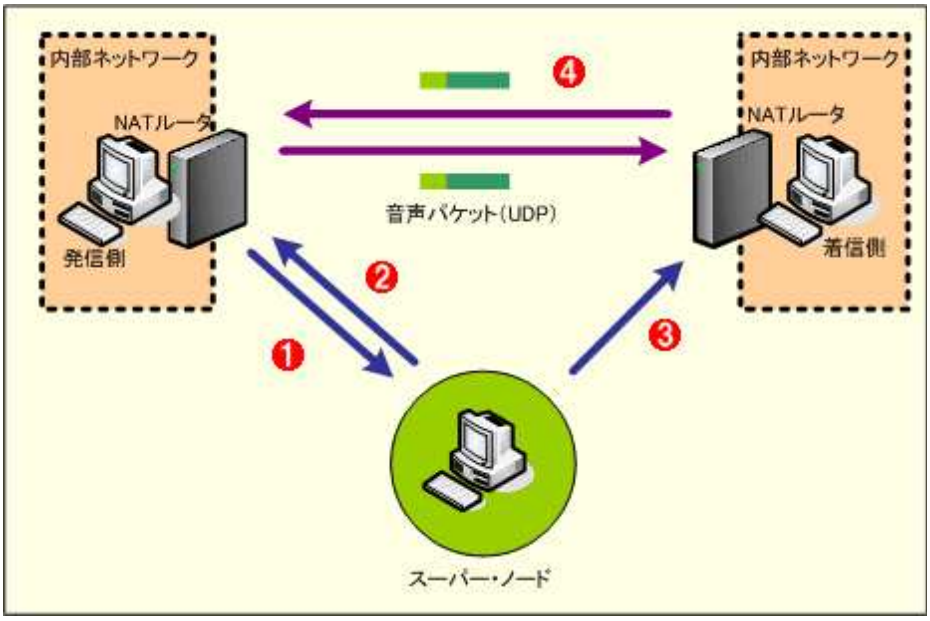
UDPホール・パンチングでは、まず一方が相手に向けてパケットを送出する。相手先はNATルータの内側なので、このパケットは相手に届かないが、NATルータAのNATエントリにAからBへのエントリが作成され、Bからのパケットを受信可能な状況ができる。次にコンピュータBは、あらかじめ知っているコンピュータAに対してパケットを送信する。今度はルータAのNATテーブルにエントリがあるので、パケットはコンピュータAに到着する。つまり、コンピュータAから送信されたUDPパケットに対する応答パケットを、コンピュータBが偽装することにより（送信されたパケットと同じポート番号を持つように、コンピュータB側でパケットを組み立てる）、あたかもUDPパケットの送信と、それに対する応答であるかのように見せ掛けている。

ここで一方（例えばコンピュータA）が、コンピュータB（NATルータB）に向けてU
ケットは、ルータBにとっては許可されていない未知のパケットなのでそれをブロ
はコンピュータBには到着しない。しかしこの際、ルータAのNATテーブルにはA
パケットを受信可能な状態になる（BからAに送られたUDPパケットのうち、送信
なっているものを許可するようなエントリが作成される）。

そこで今度は、コンピュータBからコンピュータA（NATルータA）に向けてパケッ

はエントリが作られているので、パケットはコンピュータAに到着する。もちろんルータBにも、ルータAとのUDP通信を許可するエントリが作成されるので、以後は、AからB、BからAのいずれも通信が可能となる。「ホール・パンチング」という名前の由来は、このようにNATルータに作成したエントリ(＝穴＝ホール)に向けて逆側からパケットを送信して接続するためだと思われる。

Skypeでは、このUDPホール・パンチングのしくみを発信側、着信側の双方で使用して互いに通信を開始する。互いに接続するための情報は、スーパー・ノードがすでに確立されているTCP接続を経由して双方に通知する。



発信側／着信側双方がNATの内側にある場合

発信側／着信側双方がNATの内側にある場合には、スーパー・ノードが発信側／着信側双方に相手のIPアドレス:ポートを通知し、UDPホール・パンチングを利用して直接通信を行う。

1. 発信側はまずスーパー・ノードを呼び出す。
2. スーパー・ノードが着信側コンピュータのアドレス:ポート番号を通知する。
3. スーパー・ノードが発信側コンピュータのアドレス:ポートを知らせる。
4. 発信側／着信側双方がUDPホール・パンチングを利用して通信を開始する。

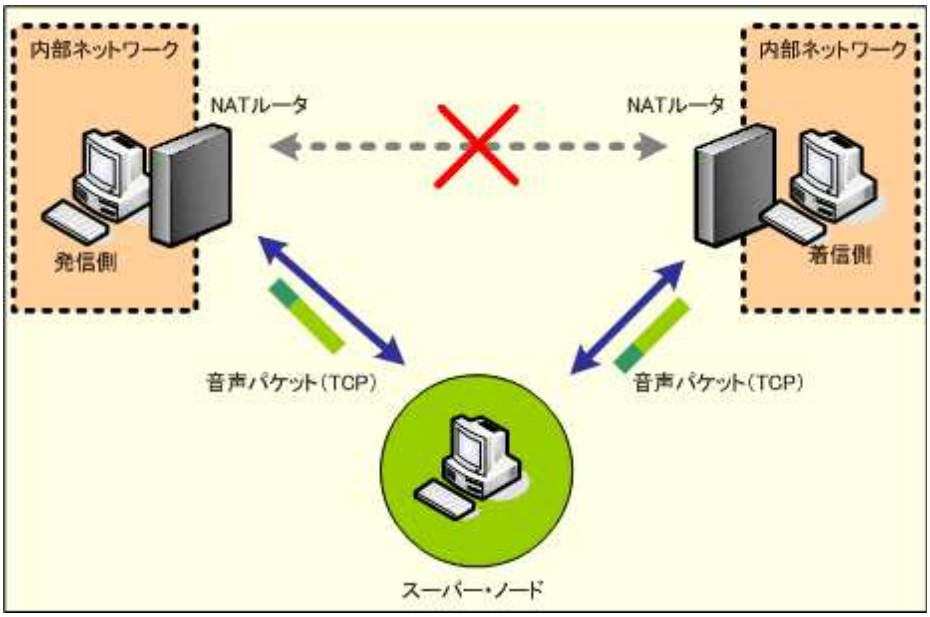
ファイアウォールなどによって通信できない場合

これまでSkypeがNATルータを越えて通信するためのしくみをパターン別に見てきた。発着信側双方がNATルータの内側にいる場合を含め、接続できる可能性は高い。しかしNATルータの作りによっては、UDPホール・パンチングを利用できないケースがある。

またNATルータに加えて、パケットを厳密に制御するファイアウォールがあり、これで厳しくパケットがフィルタリングされている場合は、NATルータは越えてもファイアウォールで通信が阻止される可能性もある(例えば、UDPでの接続が全面的に禁止されているなど)。一般的な家庭／SOHO向けブロードバンド・ルータでは、UDPパケットを送信すると、それに対する逆方向の(戻りの)UDPパケットの通過も自動的に(一定時
が企業向けの高機能ファイアウォールでは、通過させるためのポート番号や、
を厳密に設定しておかなければならず、許可されていないパケットは送信も受
い。

このようなファイアウォールが利用されている場合、Skypeは、最後の手段と
ノードとのTCP接続を利用して、音声パケットを中継する。ただしこの方法では、
に、システムやネットワークに負担がかかるし、遅延時間も大きくなるので音声

る。



スーパー・ノードによる音声パケットの中継

UDPホール・パンチングを使った直接のUDP通信が不可能な場合には、各Skypeクライアントとスーパー・ノードとの TCP接続を利用して音声パケットを中継してもらう。

■

今回は、Skypeによる音声通話の内部について見てきた。次回はSkypeのセキュリティ機能や分散インデックスを利用したユーザー検索のしくみについて解説する。

◀前のページへ　　次のページへ▶

INDEX

[検証]ネットワーク管理者のためのSkype入門

第2回　Skypeの通信メカニズム

1. Skypeの通信開始処理
2. Skypeの高い接続性の秘密

コラム: NATルータとUDP

インデックス　「検証」