2003－UBI－2 (16)
2003／11／18

NAT Traversal Technology

山田育矢[1)] 佐藤 大介[2)] 荒木 英士[3)] 須之内雄司[4)] 木野瀬友之[5)]
Ikuya YAMADA Daisuke SATO Eiji ARAKI Yuji SUNOUCHI Tomoyuki KINOSE

1) 株式会社ニューロン（〒252-0804 藤沢市湘南台 1-7-4 綴ビル 4F E-mail: ikuya@newrong.com）
2) 株式会社ニューロン（〒252-0804 藤沢市湘南台 1-7-4 綴ビル 4F E-mail: daisuke@newrong.com）
3) 株式会社ニューロン（〒252-0804 藤沢市湘南台 1-7-4 綴ビル 4F E-mail: eiji@newrong.com）
4) 株式会社ニューロン（〒252-0804 藤沢市湘南台 1-7-4 綴ビル 4F E-mail: sunouchi@newrong.com）
5) 株式会社ニューロン（〒252-0804 藤沢市湘南台 1-7-4 綴ビル 4F E-mail: kinose@newrong.com）

ABSTRACT. Computers connected to the internet through connection such as ADSL uses broadband routers as their gateway, and use private network addresses allocated by the router. Because they only have private network address, many computers are unable to accept connection from outside of their network, and unable to establish P2P communication such as transferring a file. Solutions such as STUN and UPnP exist, but they do not function in some NAT equipments. Our "NAT Traversal Technology" uses combination of existing technologies and our original technology to enable all computers with private addresses communicate peer-to-peer.

1．背景

P2P 型通信と NAT 問題

ADSL 等のブロードバンド接続の多くはルータに内蔵された NAT 装置[1]によって変換されたプライベート IP アドレスを用いて通信を行っている．このため多くのブロードバンド環境下において外部のネットワークからの参照が不可能な状況であり，ファイル転送を始めとした P2P 型の通信が妨げられているのが現状となっている．

従来，この問題への対処手法はグローバル IP アドレスを持つ中継サーバを設け，データを中継しながら転送を行う TURN 型通信と呼ばれるものを採用してきた．

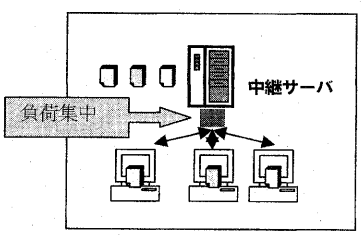

Fig. 1 TURN 型通信

各端末の間にサービサーが提供するグローバルアドレスを持ったサーバをおくことで，データを中継するものである．これによりプライベート IP アドレスを持った端末同士での通信が可能となるが，中継サーバに多くのトラフィックが集中するという事態が発生する．ブロードバンド接続が普及するとともに NAT 環境下の端末は増えていく傾向にあるため，大量のデータを流すプライベート IP 端末が増加していくのに対しこの対処法は極めて効率的ではないことがうかがえる．また，中継サーバが停止することでサービス全体，或いは一部が停止してしまうボトルネックにもなりかねない．P2P 型通信を行うアプリケーションの例としてマイクロソフト社の Windows メッセンジャー[2] が挙げられるが，このシステムではプライベート端末が通信を行う際には中継サーバを通過してメッセージが交換される．負荷対策として中継を利用している時にはファイルの送受信や音声通信ができなくなっている．MSN メッセンジャー[2]においてはファイル交換を中継サーバ経由で行うことが可能になったが転送速度が低速に抑えられている．Yahoo! サイトで配布されている Yahoo メッセンジャー[3] に搭載されているボイス通信は複数の中継サーバを設置した上で半二重での通信のみを許可している．このように TURN 型の解決手法は大容量，或いはリアルタイムなデータ転送には適さない．

2．目的

この問題を抜本的に解決するために 2 通りの解決アプローチが存在する．1 つはルータ自体の設定を端末から自動的に行う UPnP[4] 技術の利用，もう一つがルータの設定を変えずに NAT 機能の特徴を利用する手法である．前者においては UPnP 対応のルータでなければ対処することができないこと，また各ルータの UPnP の実装に揺らぎがあることから全てのルータに対応することが困難であるのが現状である．そこで後者のアプローチをベースとして全ての NAT 装置に対応するために開発された技術が本技術，NAT Traversal Technology である．

3．NAT Traversal Technology

（1）開発内容

今回開発した NAT Traversal Technology（特許申請中）は NAT 環境下の全ての端末同士が直接 P2P 型通信を行うことを可能にする．本技術のベースとなるオープンな既存技術として IETF にて 2003 年 3 月に RFC 化された STUN[5] があるが弊社での実証実験により多くの NAT 装置下において通信が行えないことが確認された．

STUN の規格の中で，ルータの NAT 実装形態は以下の 4 種類に分類される．

List.1 NAT 種類

種類	動作内容
Full Cone	NAT 内端末 I のポートαとルータのポート A が関連付けられた後，どのホストからのポート A 宛のパケットでも NAT 内端末 I のポートαに届く．ポートαからのパケットは常にポート A が利用される．
Restricted Cone	NAT 内端末 I のポートαとルータのポート A が関連付けられた後，一度何らかのパケットを送信したホストからのパケットであればポート A 宛のパケットはポートαに送られる．ポートαからのパケットは常にポート A が利用される．
Port Restricted Cone	NAT 内端末 I のポートαとルータのポート A が関連付けられた後，一度何らかのパケットを送信したホストの送信先ポートからのパケットであればポート A 宛のパケットはポートαに送られる．ポートαからのパケットは常にポート A が利用される．
Symmetric	上記 3 種類以外のルータ．NAT 内端末 I のポートαとルータのポート A が関連付けられた後，送信先端末ごとにポートαに対応するルータのポート番号が変化する．

STUN ではこのうち Symmetric 型ルータへの対応ができないことが明記されている[6]．弊社で様々なルータでの実証実験を行い NAT の種類判別を行ったところ多くのルータにおいて Symmetric 型の動作が確認され STUN では通信できなかった．さらにこの実験において Symmetric 以外のルータにおいても様々なセキュリティ機能の副作用により STUN では通信が行えないケースが多々発見された．そこで NAT Traversal Technology では Symmetric 型ルータへの対応，セキュリティ機能の副作用による通信阻害への対応を行うため，UPnP 技術，STUN 技術を含めながら独自開発技術を複数組み込み，全ての NAT 装置に対応することを実現した．また、その他通信の安定化の仕組みを組み込むことで接続後の通信のサポートも行っている．

（2）成果

弊社の NAT 越え技術との評価比較のために,コンシューマゲーム機 X のネットワーク対戦プラットフォーム技術との通信確立の比較を行った．X では STUN、UPnP をベースとした NAT 越え機能が実装されておりプライベート IP を保持するゲーム機同士が通信対戦を行うことが可能となっている．弊社にてほぼ全ての家庭用ルータメーカを網羅して NAT 越えの実証実験を行った結果，Symmetric 型のルータにおいて，X では接続確立に失敗，弊社の技術では接続に成功し安定的な通信を行うことができた．また，Symmetric 以外のルータにおいても、セキュリティ機能の副作用から X では接続できなかった全ての組み合わせにおいて安定通信に成功した．

4．NAT Traversal SDK

弊社ではこの技術を用いたアプリケーション開発を容易に行えるよう SDK 化を行い，ネットワークアプリケーション開発ライブラリ「NAT Traversal SDK」の提供を行っている．NAT Traversal SDK は NAT Traversal Technology を利用するためのライブラリファイルとサーバシステムから構成される．

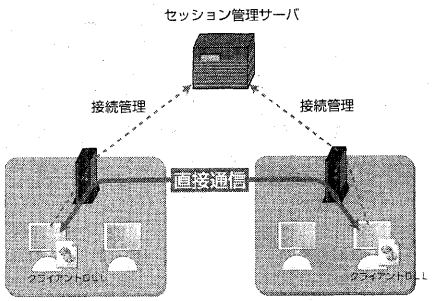

Fig. 2 NAT Traversal SDK 構成図

ライブラリファイル内の API をアプリケーションから呼び出すことで、通常のソケットプログラミングとほぼ同じ手法でアプリケーション開発が可能である．通信プロトコルは UDP を用いるが，通常の UDP 通信が利用できるのはもちろんのこと，TCP 通信と同じ信頼性のある Reliable-UDP 通信もサポートしている．そのため TCP 通信を行う要領でプログラムをコーディングするだけでファイル転送等の信頼性が必要となる通信を行うことが可能となる．また，ライブラリファイルの他にセッション管理サーバが含まれる．このサーバは本 SDK が組み込まれたアプリケーション同士が接続を行う際，セッションのイニシエーションを行うためのみに存在する．セッションが確立された後にはデータ通信はサーバを経由することなく直接端末間で行われることとなるため，セッション管理サーバに負荷が集中するということがない．これにより,これまでのようにブロードバンド対応 P2P 型アプリケーションサービスの提供時に多額な運営コストをかける必要がなくなり，ソフトウェアの構築の手間も大幅に削減することが可能となった．

5．参考文献

[1] Network Address Translation：RFC1631
http://www.ietf.org/rfc/rfc1631.txt
[2] MSN Messenger：.NET Messenger Service
http://messenger.msn.co.jp/
[3] Yahoo メッセンジャー：Yahoo!メッセンジャー
http://messenger.yahoo.co.jp/
[4] UPnP：http://www.upnp.org
[5] STUN : RFC3489 Simple Traversal of UDP Through NATs
http://www.ietf.org/rfc/rfc3489.txt
[6] RFC3489 1 章" Applicability Statement"内