

SIPを用いた音声通話に対する NAT 通過手法の提案とその実装

大竹 八洲孝[†] 但 馬 康 宏^{††} 寺 田 松 昭^{††}

本論文は, SIP (Session Initiation Protocol) を呼制御プロトコルとした音声通話に対して, ファイアウォール/NAT (Network Address Translator) と SIP サーバを統合することにより, プライベートネットワーク内外の音声通話を可能にする手法を提案している. 提案方式の特徴は (1) 従来の NAT ではできなかったパケット内部のアドレス変換や, 外部から内部への NAT 通過をファイアウォール/NAT と SIP サーバの統合により可能にし (2) SIP メッセージの中継機能, 音声パケットの NAT 通過機能, マッピングテーブルによる動的ファイアウォールのポリシー変更機能をアプリケーションレベルゲートウェイとして, SIP サーバに持たせたことである. 提案方式に基づき, 上記機能を PC 上に実装し, 実験ネットワークにおいて実測により評価を行った. この結果, 最大ホスト数 254 台とする小規模ネットワークに対応できる見通しを得た.

A Proposal and an Implementation of a NAT Traversal Method for SIP Based VoIP Communications

YASUTAKA OTAKE,[†] YASUHIRO TAJIMA^{††} and MATSUAKI TERADA^{††}

In this paper, we propose a technique which makes voice communication realize a NAT (Network Address Translation) Traversal using SIP (Session Initiation Protocol) as a signaling protocol by integrating a Firewall/NAT and SIP server. The advantageous characteristics of this system are the introduction of integrating Firewall/NAT and SIP server that translates addresses in data packets though existing NATs do not translate them, and that traverses packets from external network to internal network, the SIP server of proposal has proxying function of SIP Messages and voice packets, and function of dynamically changing policy rules of Firewall by mapping tables as a application gateway. Based on this proposal method, we implement these functions on the PC and evaluate the performance of a prototype system by the actual measurement in the experiment network. Consequently, we show that it is applicable to small network into 254 maximum hosts.

1. はじめに

現在の ADSL (Asymmetric Digital Subscriber Line) や FTTH (Fiber To The Home) などによる広帯域ネットワークの普及にともない, ネットワークサービス加入者に対する VoIP (Voice over IP) によるリアルタイム音声通信が提供されはじめている.

しかし, インターネットを利用した VoIP 通信を利用するためには, グローバル IP アドレスが必要であり, かつ NAT (Network Address Translator) およびファイアウォール環境を持たないことが一般的となっ

ている.

これは, NAT およびファイアウォールを利用した環境では, 以下のような問題点が存在することによる.

- グローバルネットワークから内部ローカルアドレス内の個々のホストに直接アクセスできない.
- パケットのペイロード (データ本体) に含まれるネットワークアドレスやポート番号は NAT では, 変換できない.

そこで本論文において, SIP (Session Initiation Protocol)^{1),2)} を呼制御プロトコルとした音声通話に対して, ファイアウォールと SIP サーバを統合した「アプリケーションレベルゲートウェイ機能付き SIP サーバ」による NAT 通過手法を提案し, 同時に試作機による評価を行う.

SIP は HTTP (Hyper Text Transfer Protocol) に似たテキストベースのプロトコルであり, マルチメディアセッション, 呼の確立, 終了を行うアプリケーション

[†] 東京農工大学大学院工学研究科

Graduate School of Technology, Tokyo University of Agriculture and Technology

^{††} 東京農工大学工学部情報コミュニケーション工学科

Department of Computer, Information and Communication Sciences, Tokyo University of Agriculture and Technology

ン層のコントロールプロトコルである。SIP は、ユーザを識別するために SIP アドレスという電子メールアドレスに似たアドレスを用いる。さらに、SIP アドレスをもとに、ユーザの位置を登録する機能を提供している。

本手法により、現在のローカルネットワークによる運用を変更せずに音声通信経路を確立することができる。

2. NAT およびファイアウォール越しの音声通話の問題点と解決方法

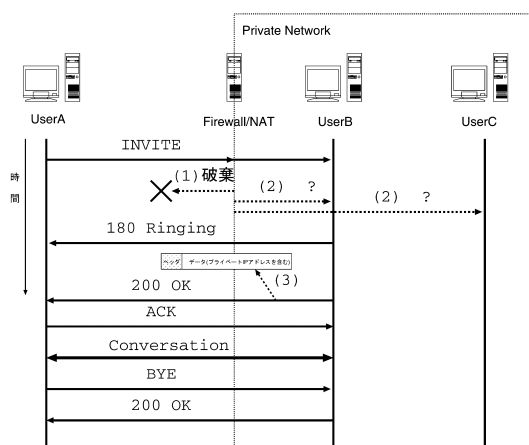
ローカルネットワーク通話例による問題点を図 1 に示す。実線は SIP における一般的な呼の確立から終了までの例である (1) UserA から、UserB に通話を行う場合、まず呼を発する UserA は INVITE という要求を UserB へ送信する。INVITE 要求には UserA の音声通信に用いられる UserA の IP アドレスやポート番号、音声符号化方式などの情報を記述した SDP (Session Discription Protocol)³⁾ が含まれる (2) INVITE 要求を受信した UserB は 180 Ringing という応答を返す。この応答は最終的な応答ではなく、進行状況を示すために使用する応答で通知応答と呼ばれる (3) UserB が電話に対応すると、UserB は 200 OK という応答を返す。この応答は INVITE 要求が成功し受理されたことを表す。また、この応答には UserB の音声通信に用いられる UserB の情報が含まれている (4) 200 OK を UserA が受信すると、INVITE に対する最終確認応答として ACK を UserB へ送る (5) ここでセッションが確立され、両方のクライアントは SDP をもとに音声通話の準備処理を行い、音声パケットの送受信を行う (6) UserA が通話を終了したい場合は、BYE 要求を UserB へ送信する (7) BYE 要求を受信した UserB は要求に対する肯定応答 200 OK を UserA へ送信し、それぞれのクライアントはセッションを終了し、音声通信の終了処理を行う。

ここで、クライアントの一方もしくは、両方が NAT およびファイアウォール環境の内部にある場合、以下のような問題点がある。

- ファイアウォールのセキュリティポリシー (方針) による、呼制御パケット、音声パケットの破棄。
- データ本体であるペイロードに含まれる IP アドレス、ポート番号は変換できない。
- 外部から内部の個々のホストにアクセスできない。

図 1 において点線はローカルネットワークを介したときの問題点を示した例である。

(1) ファイアウォールのセキュリティルールが SIP メッ



- (1)セキュリティルールによる破棄
(2)宛先決定不能
(3)NAT通過によるペイロード内のアドレス変換不能

図 1 ローカルネットワーク通話例による問題点

Fig. 1 A problem by the example of a local network call.

セージの着信するポート番号やトランスポートプロトコルを許可していない場合、グローバルネットワークにある UserA が INVITE 要求を送信し、SIP メッセージがファイアウォールに到着すると、ファイアウォールは SIP メッセージヘッダを参照し、セキュリティルールによりそのメッセージを破棄するかどうかを決定する。図 1 の (1) の場合は許可していないので、破棄される。

- (2) 仮に SIP メッセージを着信できるようにセキュリティルールを変更した場合、ファイアウォールまで SIP メッセージを届けることが可能である。しかし、この SIP メッセージが内部のどのクライアント宛なのか、またはこのファイアウォール自身宛なのかを判断することができず、結局宛先不明なメッセージとして処理される。
- (3) 仮に外部からの INVITE 要求がローカルネットワーク内のプライベート IP アドレスを持つ UserB に届いたとする。UserB は通話を許可する場合、200 OK 応答を UserA へ送信する。この SIP メッセージが NAT を通過する際、NAT によってこのパケットのヘッダ部分を書き換えられる。しかし、プライベート IP アドレスを含むデータ領域は NAT で変換できないため、データ領域は変更されず UserA へ送られる。UserA は受信した応答メッセージのデータ内容をもとに応答するため、不正なアドレスとしてうまく応答をすることができない。

NAT は IPv4 の 32 bit アドレスの枯渇問題を解消するのみでなく、外部から内部ローカルネットワーク

のホストへのアクセス制限を行えるという、セキュリティ上の利点をもたらす。しかしこれは、ローカルネットワーク内部への直接アクセスが不可能であることを示している。

またファイアウォール環境では、ローカルネットワーク内外からの通信要求を適切に処理することにより、必要なサービスをユーザに提供しつつ、セキュリティを確保している。ここでどのような通信要求に対して制限をかけるかは、組織のセキュリティポリシーによって大きく異なる。

一方、一般的な VoIP における音声パケットは、通話ごとに動的に割り当てられたポートを用いた UDP/RTP/RTCP⁴⁾ 通信によって搬送される。したがって、ファイアウォールのセキュリティポリシーを低く設定しなければ、ローカルネットワークとグローバルネットワーク間の通話を行えない。

さらに、通話ごとに動的にポートを割り当てる操作は、音声データの通信に先立ってアプリケーション層の呼制御プロトコルを用いて行われるのが一般的である。ところが、呼制御データの中には IP アドレスなどアプリケーション層よりも下層のデータが含まれているために、NAT は下層のデータに含まれる IP アドレスやポート番号を変換することができない。すなわち、NAT 越しの音声通話では、呼制御プロトコルさえ正しく機能させることができない。

一般に、NAT およびファイアウォールを利用する環境では、それらの機能を 1 台の機器（ゲートウェイ）として集約し、ローカルネットワーク内部の機器が外部と通信する場合は必ずゲートウェイを介した通信となるようにネットワークを設計する場合が多い。したがって、ゲートウェイに前述の問題点を解決する機能を取り込むことにより、セキュリティを確保しつつ、音声通話を行うことができる。

本手法によるシステムは、

- (1) SIP メッセージやセッション情報を解釈することにより、マッピングテーブルを作成し、
 - (2) そのマッピングテーブルをもとにファイアウォールのルールを動的に変更する、
- ことにより、音声パケットが NAT を通過できるようにしている。

したがって、SIP に準拠しているクライアントソフトウェアまたはハードウェアであれば、それらを改造する必要はなく、ファイアウォールをまたいだ通話を行うことができる。

本手法の持つ制約条件としては (1) 複数のゲートウェイが存在する場合には対応できない点 (2) サブ

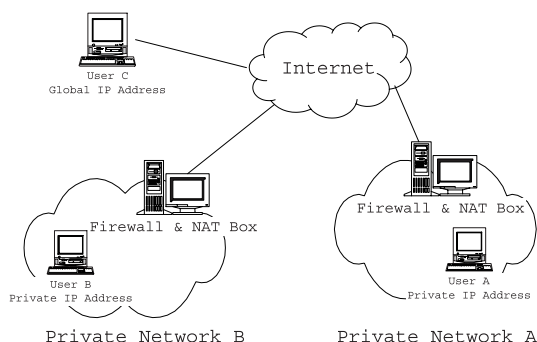


図 2 ネットワーク構成

Fig. 2 Network configuration.

ネットの出口は唯一、本ゲートウェイでなければならない点である。

しかし、本システムを作るうえで、導入している考え方は、単一のゲートウェイを持つネットワークに容易に適用でき、ユーザにファイアウォールや NAT があることを意識させずに音声通信ができるという利点がある。

3. 「アプリケーションレベルゲートウェイ機能付き SIP サーバ」の設計

図 2 に本システムを利用する場合の典型的なネットワーク構成図を示す。

ここで、ゲートウェイとして動作するマシンは一般的なファイアウォール/NAT に比べ、以下の機能が追加されている。

(1) SIP サーバ機能

SIP サーバには、プロキシサーバ（SIP メッセージの中継）、登録サーバ（ユーザの位置情報をデータベースまたはロケーションサービスに登録）、ロケーションサーバ（ユーザの位置情報をデータベースに格納または取得）、リダイレクトサーバ（リダイレクトレスポンスのみを返すサーバ）が定義されている。これらの 4 つのサーバ機能は、SIP メッセージの NAT 通過には必須の機能である。

- (2) SIP メッセージの解釈
 - (3) SIP メッセージの転送
 - (4) SIP メッセージ内に含まれる、SIP より下層のネットワークに関する情報の書き換え
 - (5) セッション確立後の音声データ NAT 通過許可
 - (6) セッション終了後の音声データの NAT 通過拒否
- 次にこれらの機能が、一般的な SIP による通話確立の過程においてどのように利用されるかを示す。

図 3 は、SIP サーバを介したときの、呼の確立から

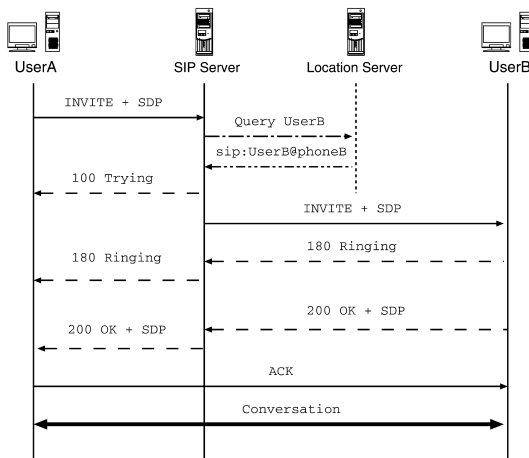


図3 一般的な SIP による通話確立過程

Fig. 3 A telephone call established process by general SIP.

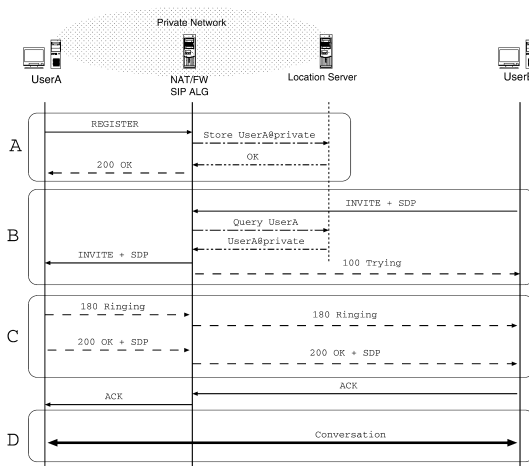


図4 本システムによる通話確立過程

Fig. 4 A telephone call established process by this system.

終了までの例である。

UserA から SIP サーバを経由して UserB に通話を行う場合、UserA は INVITE 要求を SIP サーバへ送信する。UserA からの INVITE 要求が SIP サーバに到着すると、SIP サーバは INVITE のリクエスト URI やヘッダをもとに UserB の位置情報をロケーションサーバに問い合わせ、UserB の現在位置を取得する。取得できなければ、UserA にエラー応答を返す。

UserB の位置情報を取得すれば、SIP サーバはリクエスト URI を取得した UserB の位置情報に書き換え、UserB へ INVITE を転送する。さらに、SIP メッセージのヘッダ情報をもとに処理状態を保存しておく。他は一般的な呼の確立と同じ動作を行う。

図4は、本システムによる通話確立の過程を示した

表1 本システムに必要な SIP/SDP ヘッダ

Table 1 SIP/SDP headers which are necessary for the prototype system.

SIP/SDP ヘッダ	説明
Call-ID(*) (**)	セッション識別子
Contact(*)	現在位置の SIP アドレス
Content-Type(**)	メッセージボディに含まれる内容
Content-Length(**)	メッセージボディのサイズ
From(*) (**) (tag を含む)	送信元の SIP アドレス (tag を含む)
Record-Route(*)	メッセージ経路の記録
Route(*)	メッセージ経路
To(*) (**) (tag を含む)	送信者の SIP アドレス (tag を含む)
Via(*)	要求を処理したパス
c(*) (**) (tag を含む)	送信者の IP アドレス
m(*) (**) (tag を含む)	受信ポート番号、コーデックの種類

*書き換えが必要な SIP/SDP ヘッダ

**マッピングテーブル作成に必要な SIP/SDP ヘッダ

ものである。以下、図4を用いて、通話確立過程を説明する。

(1) 初期登録

Aの部分において、プライベートネットワーク内のクライアントの情報が本システムのロケーションサーバに登録される。これは SIP メッセージの到着に先立って、登録しておかなければならない。登録は REGISTER 要求を使って行われる。

(2) 外部からの着信

Bの部分において、外部から INVITE 要求(通話要求)が本システムに到着すると、リクエスト URI に記述されている SIP アドレスと本システムのロケーションサーバ機能を用いて、メッセージを転送する。ロケーションサーバ機能は SIP に定義されているが、SIP サーバとの連携方法のプロトコル仕様については定義されていないため、本システムでは SIP サーバに内蔵する。

このロケーションデータベースを用いる利点は、前述の初期登録により、内部ホストの位置を登録されたアドレスをキーとして、取得できることである。

(3) 内部から外部への SIP メッセージの中継

Cの部分において、内部から外部へ SIP メッセージを中継する場合、SIP メッセージの中にプライベートアドレスが記述されている部分があるので、これをグローバルアドレスに書き換え、送り出す。表1に書き換える SIP/SDP ヘッダの一覧を示す。

以上の操作によりセッションを確立することができる。次に、音声通信のための設定を行う。

(4) 音声データの NAT 通過

Dの部分で音声データの NAT 通過が行われる。SIP による音声通信では、SDP を使用してコーデックなどを決定している。さらにこのプロトコルには、SIP

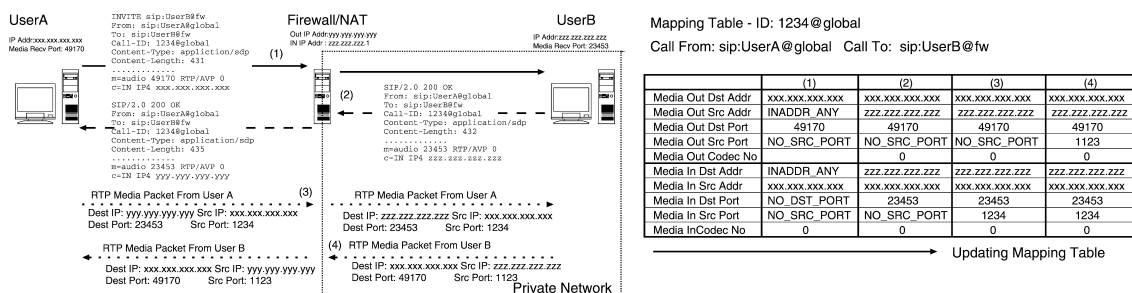


図 5 マッピングテーブル更新

Fig. 5 Updating a mapping table.

表 2 マッピングテーブルへの情報の対応づけ

Table 2 Matching of the required information on a mapping table.

項目	マッピングテーブル情報
Call-ID	マッピングテーブル作成 ID 例: Call-ID:214abe@domain.com
Content-Type	セッション情報が含まれるか調査用 例: Content-Type:application/sdp
Content-Length	セッション情報のサイズチェック用 例: Content-Length:321
From	セッション開始者 SIP アドレス
To	通話先 SIP アドレス
c	送信者の IP アドレス 例: c=IN IP4 192.168.0.31
m	受信ポート番号, コーデックの種類 例: m=audio 49170 RTP/AVP 0
送信元ポート番号	音声パケットを送り出す際のポート番号

メッセージ送信者の音声データを受信する IP アドレス, ポート番号などの情報が記述してある。音声データの NAT 通過およびマッピングテーブル作成に必要な SIP/SDP ヘッダを表 1 に示す。

図 5 のように, SDP メッセージ内にある c フィールド, および m フィールドのセッション情報を取得し, SIP メッセージのセッション識別子である Call-ID をキーとし, マッピングテーブルを作成し, その状態を記憶しておく。SDP メッセージ付きの SIP メッセージが NAT を通過するごとにこの処理を行い, マッピングテーブルの項目を埋める。マッピングテーブルへのヘッダ情報の対応付けを表 2 に示す。

すべてのマッピングテーブルの項目を満たし, どちらかのクライアントの初めの音声パケットがファイアウォールに到着したら, NAT はこのパケットの IP ヘッダ, UDP ヘッダや RTP ヘッダの音声コーデックの種類を参照し, マッピングテーブルの内容と比較する。一致すれば, このパケットの送信元ポート番号, 宛先ポート番号, マッピングテーブルをもとに, OS のファイアウォール機能にアクセスし, パケットを許可/拒否する規則を動的に適用する。さらに, マッピ

ングテーブルには音声通信に必要なすべての情報がそろっているため, それをもとに音声データの NAT 通過を実現することができる。

(5) 終了処理

BYE 要求により, セッションが終了する場合, 本方式では (a) BYE 要求のあとの, 200 OK 応答が返ったときに設定したルールを削除する方式と (b) どちらかの音声パケットを送り出してから, 一定時間過ぎた場合, 設定したルールを削除する方式とを併用している。これは, BYE 要求を見てルールを削除する方式のみにした場合, クライアントソフトウェアの異常終了により BYE 要求が送信されなかったときに, ルールが削除されないことを防ぐためである。

(6) エラー処理

INVITE 要求や, その要求に対する肯定応答 (200 OK) がファイアウォールを通過する際に, SIP メッセージを解析できるように改良した NAT は, 必ず SIP ヘッダの Content-Type ヘッダを参照し, SIP メッセージ内に SDP メッセージが含まれているかどうかを調べる。さらに, SIP メッセージ内のメッセージボディのサイズを調べ, Content-Length ヘッダのサイズと等しいか検査する。これらのヘッダが存在しないか, ヘッダのサイズが不正な場合, マッピングテーブル作成処理を行わない。また, SDP 内にマッピングテーブル作成に必要な情報が記載されていないければ, マッピングテーブルを作成しない。

さらに, 本システムの SIP メッセージ送受信に使用するトランスポートプロトコルは, SIP において標準で推奨されている UDP を用いている。UDP には信頼性がないため, メッセージ再送処理およびメッセージの要求と応答の正しい対応付けや正しい通話処理順序制御を行う必要がある。本システムでは, 同一通話の識別を, 送受信者の IP アドレス, ポート番号, 表 1 に示す SIP ヘッダで判別する。たとえば, 通話者の最終確認応答 ACK 要求が相手へ到達した後に, 通話者

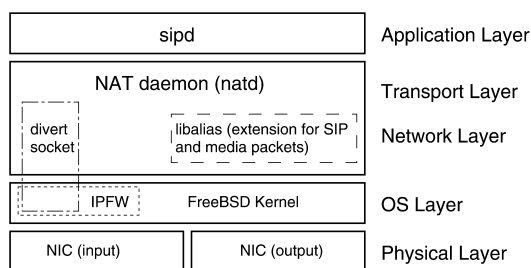


図 6 ソフトウェア構成

Fig. 6 A software architecture of this system.

が同じ Call-ID を持つ INVITE 要求を再び送信するようなことがあった場合、SIP サーバは通話の状態を調べ、この INVITE 要求を破棄する。

また、通話者の最終確認応答 ACK 要求が相手へ到達せず、セッションが確立されない場合、作成されたマッピングテーブルは一定時間後に破棄され、この通話の処理状態も破棄される。

以上の動作をする NAT デモンの改良を行うことにより、音声パケットの NAT 通過を実現している。

4. 実 装

作成した評価システムは、アプリケーション層で SIP メッセージの中継、管理、登録、SIP メッセージの書き換えを行う、新規に作成した“sipd”、ネットワーク層、トランスポート層において、プライベート/グローバルアドレスを相互に変換する FreeBSD の標準機能である NAT デモンの 2 つから構成されている。本システムのソフトウェア構成を図 6 に示す。

“sipd”は 2 つのネットワークインタフェースのアドレスでバインドを行い、SIP メッセージが到着するのを待機する。SIP メッセージが到着すると、“sipd”の待機プロセスはメッセージ処理プロセスを生成した後、以降のメッセージ処理のために待機する。メッセージ処理プロセスは、SIP メッセージをスタートライン、ヘッダ、メッセージボディの 3 つの項目に分割する。次に 3 つの項目についてそれぞれ RFC2543¹⁾ に準拠した解析処理を行う。解析処理を終えれば、SIP トランザクションを作成および取得し、ヘッダのパラメータを構造体に格納する。その後は、要求/応答メッセージに応じた処理を行う。

FreeBSD の NAT デモンは“libalias”とよばれるパケットエイリアス(パケットのアドレス変換)を行うライブラリを使用している。このライブラリに SIP/SDP および音声パケットの NAT 通過を実現できるような改良を施す。

音声パケットが NAT 通過を実現するために、既存

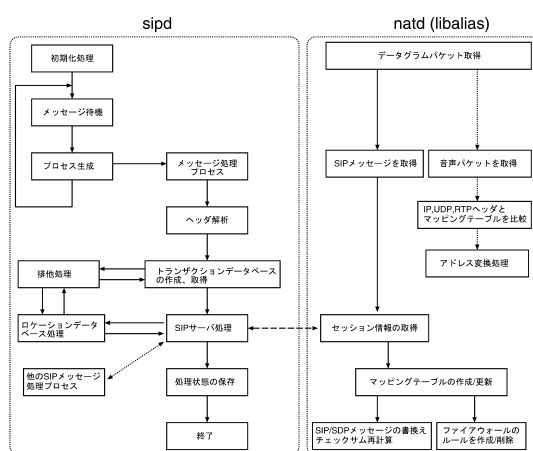


図 7 流れ図

Fig. 7 A flow chart of this system.

の NAT デモンから下記の点について改良を施している。

- (1) SIP/SDP メッセージからセッション情報を取得
- (2) マッピングテーブルの作成/更新
- (3) SIP/SDP メッセージの書き換え
- (4) 動的なファイアウォールのルールを作成、削除

マッピングテーブルの 4 つの情報(送信元 IP アドレス、送信元ポート番号、NAT 内部宛先 IP アドレス、宛先ポート番号)をもとにして、FreeBSD のカーネルに組み込まれているファイアウォール機能にアクセスし、パケットを許可する規則を作成し適用する。

図 7 に本システムの流れ図を示す。

5. 評 価

5.1 評価方法

VoIP において、音声ストリームは短い間隔の音声パケットの列で構成されている。これらのパケットはすべて NAT 上を通過するため、複数のセッション間で音声通信を行う場合、NAT には十分なパフォーマンスが要求される。SIP メッセージ処理および音声パケットのアドレス変換処理などには CPU 負荷がかかり、CPU 使用率が 100% 近くに上昇し、これらの処理が間に合わなくなると、通話要求受け付け不能に陥るか、または音声パケットの損失が発生する。

そこで本論文では「アプリケーションレベルゲートウェイ機能付き SIP サーバ」の性能を評価した。評価に用いたクライアントソフトウェアはマイクロソフト社の Windows RTC (Real-Time Communication) クライアントサンプルプログラムを使用した。評価に用いた実験機器の構成を表 3 に示す。

評価システム構成を、図 8 に示す。ファイアウォー

表 3 評価システムのスペック

Table 3 Specification of prototype system and clients.

項目	仕様
サーバ OS	FreeBSD 4.7-STABLE
Firewall/NAT	ipfw + natd
SIP サーバ	sipd
CPU	Intel Pentium III 450 MHz
メモリー	256 MB
NIC	Intel PRO/100+ Ethernet Card
クライアント OS	Windows XP Professional
SIP クライアント	Windows RTC Client Sample
プロトコル	SIP:UDP/IP, 音声: RTP/UDP/IP
音声コーデック	G.711 (PCMU)
サンプリングレート	8,000 Hz
ビットレート	64 Kbps
音声パケット化間隔	20 ms
音声パケットサイズ	172 バイト (RTP ヘッダ含む)

表 4 SIP メッセージの処理時間

Table 4 The processing time of SIP messages.

メッセージの種類	処理時間 (ミリ秒)
INVITE	18
180 Ringing	4.7
200 OK (INVITE)	3.8
ACK	2.4
BYE	4.6
200 OK (BYE)	2.9
CANCEL	4.9
REGISTER	3.6
OPTIONS	14

想定した。

評価システムの想定値から、下記の項目について本システムの評価を行った。

- SIP メッセージ処理時間
- 1 秒間あたりの接続要求数と CPU 使用率
- セッション数と CPU 使用率
- セッション数と NAT における転送時間

5.2 SIP メッセージの処理時間

SIP メッセージを受信してから SIP メッセージを中継または応答処理終了までの、“sipd” における SIP メッセージ処理時間を `gettimeofday` 関数を使用して 100 回測定し、平均した結果を表 4 に記す。単位はミリ秒である。

INVITE 要求および OPTIONS 要求において、他と比べて処理時間を要するのは、ロケーションデータベースにアクセスするために時間がかかるか、またはこれらの要求を中継した際に相手からの応答を待つために時間がかかるものと考えられる。

5.3 1 秒間あたりの接続要求数と CPU 使用率

図 9 は、“sipd” における 1 秒間あたりの接続要求数と CPU 使用率の関係を表したグラフである。縦軸は CPU 使用率を表し、横軸は 1 秒間あたりの接続要求数を表す。

図 9 より、仮に想定するセッション数分のクライアントから接続要求が同時にあったとしても、CPU 使用率は約 40% 以下であり、他のデータトラフィックおよび、音声トラフィックの転送にも対応できると考えられる。

5.4 セッション数と CPU 使用率

セッション確立後、最大何セッションの音声通信が可能かを測定するためには、多くの PC が必要になるため、実測は難しい。5 セッション以上からは、音声データをダミーパケットとして送信して評価を行った。セッション数と CPU 使用率の関係を表したグラフを図 10 に示す。縦軸は CPU 使用率を表し、横軸は音

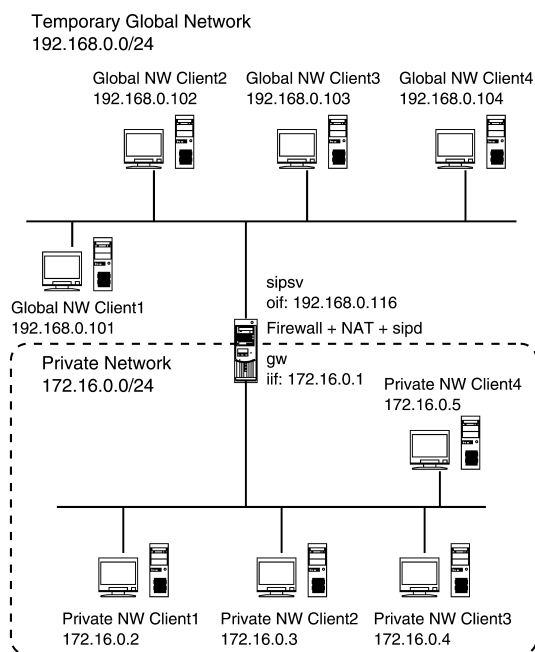


図 8 評価システム構成

Fig. 8 An experiment network for the evaluation.

ルの設計値はクラス C の IP アドレスを持つようなネットワークとし、プライベートネットワーク内の最大ホスト数を 254 台と設定した。また、評価システムの構成は大規模ネットワークではなく、最大ホスト数を 254 台とする小規模ネットワークを想定している。さらに、本システムではゲートウェイとして動作するため、他のデータトラフィックおよび接続要求数に対するトラフィックを考慮した。最も音声通信が集中する時間帯において、最大ホスト数 254 台のうち、10～20% のホストが音声通信を行っている仮定すれば、同時通話数および最大接続数を 40～50 セッションと

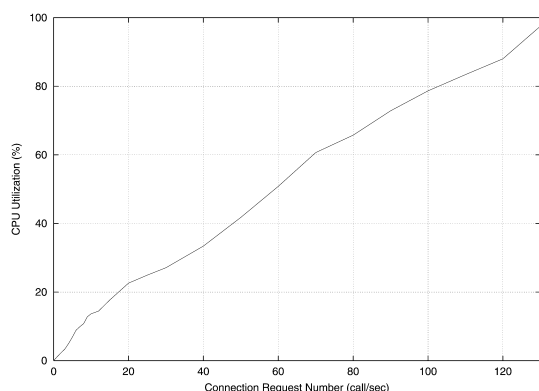


図 9 1 秒あたりの呼接続要求数と CPU 使用率

Fig. 9 The numbers of call request for per second and CPU utilization.

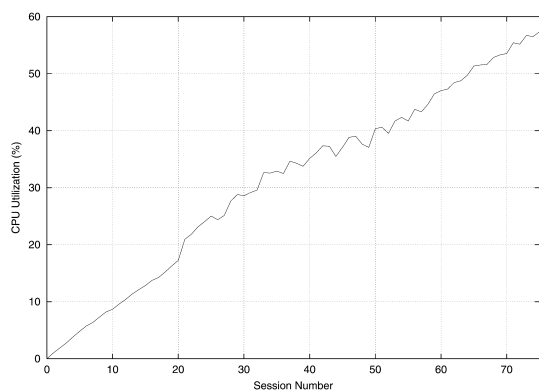


図 10 セッション数と CPU 使用率

Fig. 10 Session numbers and CPU utilization.

声通信を行っているセッション数を表す。

仮に平均 3 分間の通話をするとした場合、接続要求 (INVITE 要求, BYE 要求) の処理時間は表 4 の合計値より、約 40 ミリ秒であり、音声パケットの転送における処理時間は 3 分なので、接続要求の CPU 処理時間は相対的に無視することができる。よって、CPU はほとんど音声パケットの転送に使われ、セッション数により CPU 負荷が決まると考えられる。

このことから、図 10 より、想定値である 40~50 セッションの通話が十分に可能であると考えられる。この性能があれば、小規模ネットワークで用いる際には実用上問題ないと考えられる。

5.5 NAT 通過における音声パケットの遅延

FreeBSD の NAT デモンは、DoAliasing 関数により、到着したパケットを取得し、パケットのアドレス変換を行い、各方向へパケットを転送する。この DoAliasing 関数において、パケット入力から、アドレス変換、パケット出力まで、gettimeofday 関数を用

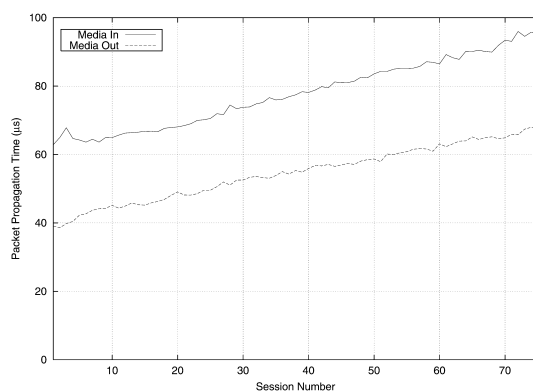


図 11 セッション数と NAT のパケット転送時間

Fig. 11 The numbers of sessions and the packet propagative time of NAT.

いて、マイクロ秒単位で測定を行った。gettimeofday 関数を使用して測定した結果を図 11 に記す。

図 11 の MediaIn はグローバルネットワーク側からプライベートネットワーク、MediaOut はプライベートネットワークからグローバルネットワークへ流れる音声パケットの転送時間を表す。

リアルタイム音声通信において、片方向での遅延時間の合計が 150 ミリ秒以内であることが望ましい⁵⁾。本システムで発生するアドレス変換、パケット転送による遅延は、図 11 から、遅延時間の合計 150 ミリ秒のうち 1%未満である。

5.6 他の NAT 通過手法との比較評価

SIP を利用した音声通話に対する NAT 通過手法はいくつか提案されている。しかし、いくつかの NAT 通過手法は提案および草案レベルの状態であるため、本システムとのパフォーマンス上での比較評価を行うことができない。本節では、他の NAT 通過手法と本提案方式の機能的な違いについて述べる。

NAT 通過手法は機能的な違いから、下記の 4 通りに分類することができる。

(1) NAT のバインディングを利用

プライベートネットワークから UDP パケットをグローバルネットワークへ送信した際にできる NAT のバインド関係 (グローバルアドレスとプライベートアドレスの変換テーブル) を利用した方法である。既存の NAT/ファイアウォールを利用することが可能という利点がある。また、SIP のトランスポート層のプロトコルとして UDP を使用した場合、NAT のバインディングを保持するために、SIP 端末/サーバが頻繁にメッセージを送信しなくてはならないという欠点がある。ユーザにバインディング先を知らせる必要がある。NAT を意識する必要がある。しかも、セッショ

表 5 各方式の比較評価
Table 5 Comparison evaluation of other NAT Traversal methods.

比較項目	STUN/TURN	UPnP	Midcom	静的ポート フォワーディング	提案方式
NAT 通過手法の種類	NAT Binding	外部 NAT 制御	内部 NAT 制御	Port Forwarding	ALG*
SIP 端末改良の必要性	要/要	要	不要	不要	不要
NAT の種類に依存	する/しない	しない	しない	しない	しない
NAT の改良	不要/不要	要	要	不要	要
制御プロトコルの必要性	要/要	要	要	不要	不要
外部機器の必要性	要/要	不要	要	不要	不要
外部から内部への着信	○/○		○		○
ユーザへ NAT の意識度	高/高	中	低	中	低
管理の容易さ	○/○	×	×	×	
処理手順の容易さ	/	×	×	○	○
汎用性	○/○	○	○	○	×

*ALG (Application Level Gateway)

ン数が増えた場合、バインディングメッセージによる NAT パフォーマンス低下が懸念される。内部と外部に SIP サーバを設置することを除き、外部から内部 SIP 端末への着信ができない。

(2) NAT/ファイアウォールを外部から制御

NAT/ファイアウォールを制御する外部のエージェントを NAT/ファイアウォール内外に配置し、NAT/ファイアウォールとエージェント間の通信プロトコルにより、NAT/ファイアウォールを制御する方法である。SIP 端末はこれらの制御プロトコルの通信を知る必要はない。しかし、NAT/ファイアウォールに制御プロトコルの実装が必要であり、プロトコルの盗聴の可能性も考えられる。また、SIP 端末に制御プロトコルを組み込む方法もある。前者の場合、ユーザは NAT を意識する必要はないが、後者は意識する必要がある。制御プロトコルが増える分、NAT/ファイアウォールの設定項目が増える。

(3) NAT が SIP および音声パケットを認識

NAT を通過するデータの内容を調査し、アクセス制御を行う方法である。アプリケーションレベルゲートウェイと呼ばれ、本手法はこの方法に属する。新たなアプリケーション、プロトコルへの対応やアプリケーション、プロトコルのバージョンアップへの対応が難しく、そのつど対応させなければならないという欠点を持つ。

(4) ポート番号ごとに内部ホストを静的に割り振る

グローバル IP アドレスのポート番号ごとに NAT 内部の端末へ転送する方法である。既存の NAT/ファイアウォールを利用することが可能である。しかし、音声通信のポート番号が動的に割り当てられる端末の場合は対処できない。さらに、ポートと内部ホストの割当て設定が煩わしいという欠点を持つ。

6. 関連研究

本章では、5.6 節で述べた他の NAT 通過手法について、関連研究との比較を行った。既存システムの改良の必要性、機器コスト、処理手順、利用者/管理者にとっての違いを比較項目とした。表 5 に示す。

NAT のバインディングを利用した STUN (Simple Traversal of UDP Through Network Address Translators ^{6)~8)} /TURN (Traversal Using Relay NAT ⁹⁾) 方式では、既存の NAT を利用しつつ、NAT のバインド関係を維持するため、それぞれ STUN/TURN メッセージの実装が必要であり、内部または外部に STUN/TURN サーバの機器が必要になる。さらに、SIP 端末に STUN/TURN プロトコルの実装が必要になり、処理手順も複雑になる。

NAT/ファイアウォールを内部から制御する UPnP (Universal Plug and Play) 方式では、SIP 端末自体に NAT を制御するプロトコルを実装することにより、NAT の制御を行う。そのため、SIP 端末および NAT に UPnP の実装が必要であり、外部からの着信には対応できない。

NAT/ファイアウォールを外部から制御する Midcom (Middlebox Communication ^{10)~12)}) 方式では、NAT を制御するエージェントと NAT 間のプロトコルの定義が必要であり、さらに NAT を改良する必要がある。利用者にとっては、通常の SIP 端末で対応が可能である。

ポート番号ごとに内部ホストを静的に割り振る方式¹³⁾においては、管理者にとって、ポートごとの割当て作業が必要であり面倒である。さらに、通話ごとに音声通信のポートを動的に割り当てる端末の場合は対応できない。

アプリケーションゲートウェイ方式を採用した本方式は他の方式と比べ、利用ユーザから見れば、NATがあることを意識せず、さらに端末に特別な改良をせずに、SIPに準拠した端末のみで通信ができるという利点もある。管理者の視点から見れば、NAT/ファイアウォールの設定のみで、本システムを動作させることができる。

7. ま と め

本論文では、SIPを利用した音声通話に対し、SIPメッセージおよび音声パケットのNAT通過を実現するための手法を提案した。提案方式は、ファイアウォール/NATとSIPサーバを統合化することにより、既存のNATでは実現できなかった、(1)パケットのペイロードにあるSIP/SDPメッセージの認識およびアドレスの書き換えを行う機能、(2)SIPメッセージからセッション情報を取得し、マッピングテーブルを作成する機能、(3)マッピングテーブルをもとに音声パケットを動的に許可/拒否する機能を有するものである。これらの機能を実装することにより、実験ネットワーク上で提案した方式の性能測定を行った。

トランスポートプロトコルとしてUDPを使用したSIPメッセージの中継および、NATにおける音声パケットの通過を確認した。また、クラスCのIPアドレスを持ち、最大ホスト数が254台の実験ネットワーク上において、プロトタイプシステムを用いた性能評価を行い、想定したセッション数の会話を処理することが可能であることを明らかにした。

さらに、関連する他のNAT通過手法との比較を行った。本提案方式は他の方式と比べ、SIP端末の改良、制御プロトコル、外部機器は必要はなく、処理手順が容易という利点がある。

今後の課題としては、IPv6環境におけるNATへの対応、エンドツーエンドにおけるSIPセキュリティへの対応についても検討していく必要がある。

参 考 文 献

- 1) Handley, M., Schulzrinne, H., Schooler, E. and Rosenberg, J.: SIP: Session Initiation Protocol, RFC2543 (1999).
- 2) Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, RFC3261 (2002).
- 3) Handley, M. and Jacobson, V.: SDP: Session Description Protocol, RFC2327 (1998).
- 4) Schulzrinne, H., Casner, S., Frederic, R. and

Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications, RFC1889 (1996).

- 5) 総務省：IPネットワーク技術に関する研究会報告書 (2001).
- 6) Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: STUN — Simple Traversal of UDP Through Network Address Translators, Internet Draft (2002).
- 7) Rosenberg, J., Mahy, R. and Sen, S.: NAT and Firewall Scenarios and Solutions for SIP, Internet Draft (2002).
- 8) 伊藤洋輔, 福田芳巳：STUNの適用に関する一考察, B-6-111, 電子情報通信学会ソサイエティ大会 (2002).
- 9) Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: Traversal Using Relay NAT (TURN), Internet Draft (2002).
- 10) Sen, S., Sollee, P. and March, S.: Midcom-unaware NAT/Firewall Traversal, Internet Draft (2002).
- 11) Davies, S., Read, S. and Cordell, P.: Traversal of non-Protocol Aware Firewalls & NATS, Internet Draft (2001).
- 12) 近藤 誠, 中村宏之：SIPメッセージのNAT通過方式に関する一考察, B-6-8, 電子情報通信学会ソサイエティ大会 (2001).
- 13) 福元徳広, 山田秀昭, 遠藤俊樹, 清水 徹：NAT環境におけるVoIPプロトコル制御に関する一検討, B-6-204, 電子情報通信学会総合大会 (2002).
- 14) Camarillo, G.: *SIP Demystified*, pp.90-157, McGraw-Hill TELECOM (2001).
- 15) Thernelius, F.: SIP, NAT and Firewalls, Master's thesis, Department of Teleinformatics, Kungl Tekniska Hogskolan (2000).
- 16) 大竹八洲孝, 但馬康宏, 寺田松昭：VoIPにおけるNAT通過の実現, マルチメディア, 分散, 協調とモバイルシンポジウムDICOMO2002, IPSJ Symp. Seri., Vol.2002, No.9, pp.1-4 (2002).

(平成 15 年 3 月 10 日受付)

(平成 15 年 12 月 2 日採録)



大竹八洲孝 (学生会員)

1976年生。2002年東京農工大学大学院工学研究科電子情報工学専攻修士課程修了。現在、同大学院工学研究科電子情報工学専攻博士課程に在学中。VoIPアプリケーション、コンピュータネットワークの研究に従事。



但馬 康宏 (正会員)

1994 年電気通信大学電気通信学部電子情報学科卒業。1996 年同大学大学院博士前期課程修了。同年石川島播磨重工業(株)入社。2001 年電気通信大学大学院博士後期課程修了。同年東京農工大学情報コミュニケーション工学科助手。現在に至る。博士(工学)。ネットワークにおける知的処理の研究, 計算論的学習理論の研究に従事。EATCS, 電子情報通信学会, 人工知能学会各会員。



寺田 松昭 (正会員)

1970 年岡山大学工学部電気工学科卒業。同年(株)日立製作所入社。同社システム開発研究所において, 制御用分散処理システム, LAN, プロトコル高速処理, VoIP, 次世代インターネットの研究に従事。工学博士。著書『制御用計算機におけるリアルタイム技術』(共著, コロナ社), 『デジタルサービス革命』(共著, 日刊工業新聞社)。1999 年 4 月より東京農工大学工学部情報コミュニケーション工学科教授。IEEE, ACM, 電子情報通信学会各会員。