ファイアウォールを通過できる IP 電話の研究

伊藤　将志　　渡邊　晃

現在，IP 電話はインターネットのブロードバンド化による“低価格固定料金”，“常時接続環境”，“通信帯域の確保”によって著しい普及を遂げるに至った．しかし，まだ課題は残っており，ファイアウォール・NAT・プロキシサーバなどにより外部との通信に制限を受けている企業内ネットワークからでは外部の IP 電話端末と通話を行うことはできない．この課題を解決すべくいくつかのシステムが既に実現されている．しかし，まだ完璧と言えるシステムは無く，新たに様々な課題が発生してしまうことがほとんどである．本論文ではそれらの課題を最小限に抑えられるようなシステムを提案し，その詳細について述べ，他の既存の VoIP 技術と比較した結果を報告する．

Proposal of voice over IP system passing through Firewall

MASASHI ITO　AKIRA WATANABE

In recent year,IP telephone achieved remarkable spread by the "low price fixed charge","regular connection environment", and "reservation of a communication zone"by the formation of a broadcloth band of the Internet. However, yet, the subject remains and it cannot telephone to external IP telephone terminal from the local network which has received restriction in communication with the exterior by the fire wall, NAT, the proxy, etc. Some systems are already realized that this subject should be solved. However,There is no perfect system for the system , and In almost all cases, various subjects will newly occur. In this paper, the system which can suppress those subjects to the minimum is proposed, and the details are given, and it reports the result compared with other existing VoIP technology.

1．はじめに

近年では ADSL，CATV，FTTH 等のブロードバンドの普及や ISP 間のバックボーンの整備により，ネットワークの伝送容量が大幅に増加されてきたため，これまで IP 電話の大きな課題の一つであった実用レベルの品質保証が可能となった．また，2002 年秋から総務庁より IP 電話専用番号“050-”の事業者受付が開始となり，IP 電話が公衆回線網の電話機からのダイアルを受信することを可能にした．これによって，それ以降多くの ISP が従来の電話に対し低額固定料金である IP 電話サービスを提供するようになり，IP 電話の普及は著しく進んできた．

しかし，この著しい普及に伴い VoIP（Voice over Internet Protocol）[1]に様々な課題が浮かび上がってきた．これらの課題を発生させる要素として，セキュリティ向上を目的に IP アドレスやポート番号を指定し，パケットをフィルタリングするファイアウォール[2]，インターネット上のアドレスを透過的に相互変換し，外部から内部のアドレス環境を特定できなくする NA(P)T[3]，内部ネットワークから外部ネットワークへ代理で接続を中継するプロキシ[4]がある．これらの装置のためインターネットへ直接接続することができず，外部との通信が制限されてしまっている企業ネットワークがほとんどである[5].

VoIP とは“コーデック技術”，“シグナリング

“Proposal of voice over IP system passing through Firewall”
Masashi Ito & Akira Watanabe
Faculty of Science and Technology, Meijo

技術”, “IP パケット処理技術” の３つからなるインターネットプロトコルを利用して音声通信を行う伝送技術全般のことを指し, IP 電話はこの VoIP によってインターネットを介して電話をすることができる.

VoIP に関連するプロトコルとしては，早い時期に International Telecommunication Union – Telecommunication（ITU-T）によって標準化された H.323 という既存の電話仕様をベースにして IP 電話サービス用に拡張されたシグナリングプロトコルがある[6]．また，現在では Internet Engineering Task Force（IETF）によって標準化された Session Initiation Protocol（SIP）[7]が実装も容易で拡張性に優れているとして様々なメディア通信で注目されており，現在 ISP が提供している IP 電話は大抵この SIP プロトコルによりシグナリングを行っている[8] [9].

しかし，この SIP というプロトコルはダイアル開始時には相手端末の IP アドレス，または相手端末の情報が登録されている SIP プロキシの IP アドレスが DNS から特定できることが必須となり, NA(P)T により相手の IP アドレスが外部から特定不可能な場合, その内部の相手へパケットを宛てることはできない. これに関しては将来 IPv6 によって解決することだが[10]，その普及は順調ではなく期待できない. また，企業などのファイアウォールは大抵，外部からの通信ほぼ全てと, 内側からの通信もさえも HTTP 通信のための 80 番ポートなど，必要とされるポート以外は通過できないように設定されているため，SIP によるダイアルやその後の音声データは遮断されてしまう場合がほとんどである（図１）．このように外部との通信に制限を受けたネットワークにおいて SIP による IP 電話を導入する場合，ファイアウォールの設定の変更が必要な上, セキュリティ低下にも繋がってしまう.

これらの問題に対してルータを UPnP に対応させることによってポートを自動的に開閉する方法[11]や，ルータに導入することによって NA(P)T 内部のホストの IP アドレスを特定可能とする NATS[12]などがあるが，それだけでは IP 電話がファイアウォールを超えて自由に通信する上での根本的解決には至らない.

しかし，近年では IP 電話システムとして NA(P)T，ファイアウォールなどによって電話としての機能を制限されることなく通過するためのシステムが既にいくつか開発されている．これらのシステムに HCAP[13]，Skype[14]などがあるが, これらにもまだ多くの課題が残っている．また，VoIP に限らず全てのアプリケーションが制限なくファイアウォールの通過をすることを目的とした SoftEther[15]があるが, 本来ファイアウォールに守られているはずのネットワークを危険にさらしてしまうシステムとして問題視されている.

これらのシステムに対し本提案システムでは, SIP をベースとし，プライベートネットワークの内部と外部にリレーエージェントを配置し，その２台の間の通信を HTTP[3]でトンネルすることによって解決する方式を提案する. また, 他のシステムと性能の比較を行い, 提案システムの機能を SoftEther に見立てて測定を行った結果から, 提案システムの実装により起こるディレイの見積もりの計算を行い検討する.

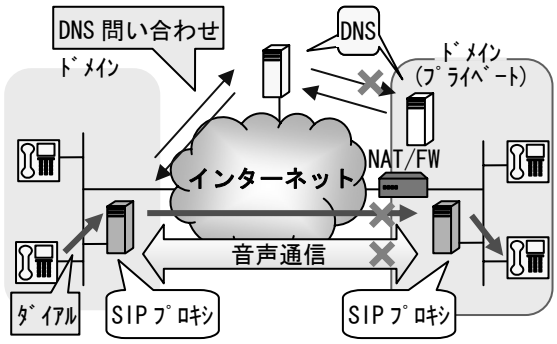

図１．SIP による NAT/FW の問題

2．既存の対応技術とその課題

ファイアウォール・NAT などの問題に対して前述で紹介した HCAP では端末から予め TCP でグローバル環境上に設置されたサーバへ接続を確立しておくことで NAT を通過する．そして, ダイアルや音声ストリームを HTTP に埋め込むことで, Web を観覧することのできる環境であれば，HTTP の 80 番ポートによりファ

イアウォールを通過することも可能としている．しかし，音声端末側にそれぞれ HCAP という専用のプロトコルをインストールする必要があり，DMZ 上に HTTP 中継サーバという特殊なサーバを配置し，そこへファイアウォール内の複数の専用音声端末から常時 TCP による接続が行われているため，ファイアウォール上に不要なトラヒック流がれてしまう(図2)．

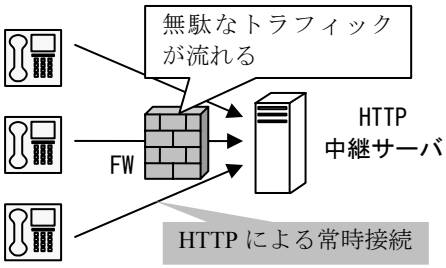

図２．複数の常時接続による無駄なトラフィック

続いて Skype では 80 番ポートを利用した独自のアプリケーションによりファイアウォールを通過する．また，NAT の通過には HCAP と同じ方法を利用して解決している．しかし，80 番ポートを使った独自のアプリケーションを使用しているため，ネットワークが HTTP プロキシサーバを通してでしか外部へパケットを送信できない環境になっている場合，HTTP プロキシを通過することができない上，セキュリティ的にも信頼性が低く，企業などのネットワーク管理者はこのシステムの使用を禁止することが予想される（図 3)．

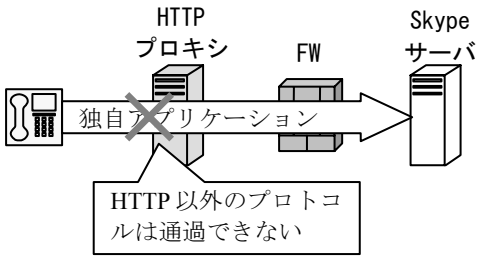

図３．HTTP プロキシを通過できない Skype

そして，グローバル環境上に設置した仮想 HUB に仮想 LAN カードを組み込んだ PC から HTTPS によって接続することにより，仮想的な LAN を作る SoftEther というシステムがある．このソフトは仮想 HUB に接続している PC 同士ならどのようなアプリケーションでもファイアウォール，NAT，プロキシのほとんどを通過して通信することができてしまう．この仮想的なネットワーク上で SIP を利用し，IP 電話を導入することもできる．しかし，使用の方法によっては企業内の LAN をそのまま外部のネットワークとファイアウォール無しで繋いでいるのと同じ状態にもなってしまい，ネットワークは不正アクセスの危険にさらされることになるという課題が指摘されている．

3. 提案システム

本提案システムでは，特殊な機能を追加した SIP サーバをプライベートネットワークの内部と外部にそれぞれ 1 台ずつ設置する．これらの 2 台の特殊な SIP サーバは，ダイアルの際，プライベートアドレスとグローバルアドレスの２つのインターフェースを持ち合わせて仮想的な１つの SIP プロキシとしての機能を持つ．この 2 台の特殊な SIP サーバを Half Relay Agent（HRA）と呼び，プライベートネットワークの内部に設置するものを HRA クライアント，外部に設置するものを HRA サーバと呼ぶ．

この２つの HRA は図４のようにダイアルや音声ストリームを HTTP に埋め込み，２つの間でダウンロードやアップロードによりデータのやり取りを行い NAT・ファイアウォールを通過することができる．

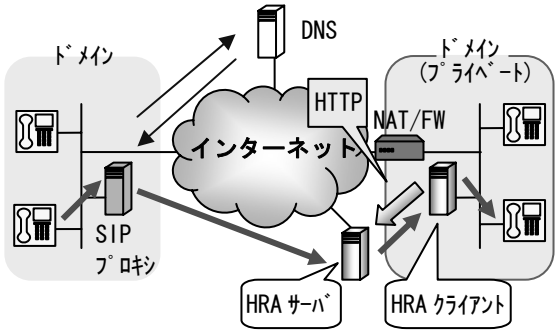

図４．HRA による解決法

3.1. HTTP によるトンネリング

本提案システムの基本動作は図５のように，まずプライベートネットワーク内部の HRA クライアントから外部の HRA サーバに向けて，あらかじめ十分に大きなサイズのデータをダウンロードする GET メソッドを発行しておく．

このとき，1 回のみの GET メソッド発行では TCP の機能により接続が切断してしまうので，HRA サーバから定期的に HRA クライアントに向けて通信を行うようにして，HRA 間の HTTP 接続を維持する．つまり，外部から内部の端末へ向けられたダイアル情報を持つメッセージや音声パケットが HRA サーバに到達すると，それを HRA クライアントが HRA サーバから先に発行していた GET メソッドにより，ダウンロードを開始する．そして，HRA クライアントはダイアル情報を持つメッセージを受け取った場合は HTTP から既存の SIP のメッセージを取り出し，音声データを含む HTTP パケットを受け取った場合は HTTP から音声データを取り出し，それを UDP により宛先の端末に向けて中継する．また，内部の端末からのダイアル情報を持つメッセージや音声パケットは POST メソッドにより，HRA サーバへアップロードされ，HRA サーバにより UDP に変換され，外部の相手端末に送信される．

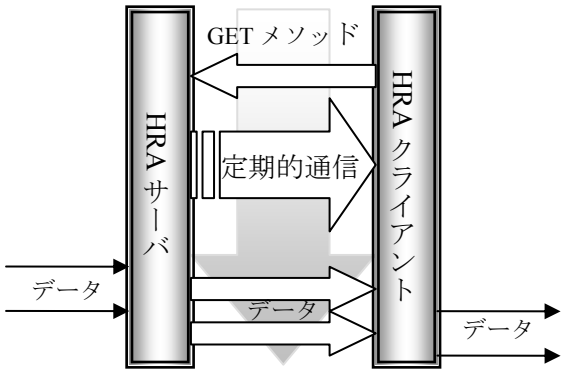

図５．データの中継

3.2. 音声データの中継

本来の SIP では音声データの通信は SIP プロキシを介さず UDP で直接端末同士で行う．しかし、本提案システムではファイアウォールを通過させるため音声データも HRA を中継させなければならない．そのため端末が音声データを HRA 宛に送信するような仕組みにする．これには，ダイアルの際に SIP メッセージに含まれる Contact ヘッダ利用する．この Contact ヘッダは送信側の端末の IP アドレス情報を含む URI を持っている．SIP では本来，メッセージを受信した端末がこの Contact ヘッダを参照することにより，相手端末の IP アドレスを知り，端末同士直接通信を行うことができるようになる．

図６のように本提案システムでは HRA から端末にメッセージを中継する前に Contact ヘッダに記述されている送信元の IP アドレス情報を HRA の IP アドレス情報に書き換えることにより，端末に通信相手の端末が HRA であるようにだまし，端末が音声データを HRA に送信するようにする．

また，複数の通信が確立する場合，HRA サーバと HRA クライアントの間で通信を識別することと端末情報を保持することを目的に，ダイアルのパケットが HRA に到着する際，２つの HRA で通信を一意に識別する SIP メッセージに含まれるヘッダである Call-ID・From・To を参照し，それとその HRA 側の端末の IP アドレスの対応させたものに Call-No という番号を付けたテーブルをそれぞれに作成する．なお，１回のダイアルのやり取りの際この３つの SIP メッセージのヘッダは常に変わらないので HRA サーバと HRA クライアントでは同じ IP アドレスと Call-No の関連付けが記録される．そして，音声データが端末から HRA へ送信された際，HRA では自分の持っている対応表から受信したパケットの IP アドレスに対応する Call-No を参照し，HTTP ヘッダに載せて次の HRA に HTTP によって中継する．そのパケットを受け取った HRA は対応表からその HTTP ヘッダに加えられた Call-No と対応する IP アドレスを参照し，その IP アドレスを音声データを中継すべき端末の宛先としてパケットを送信する．つまり，２つのユーザエージェントの IP アドレスは HRA 間で中継される Call-No によってリンクされることになる（図７）．

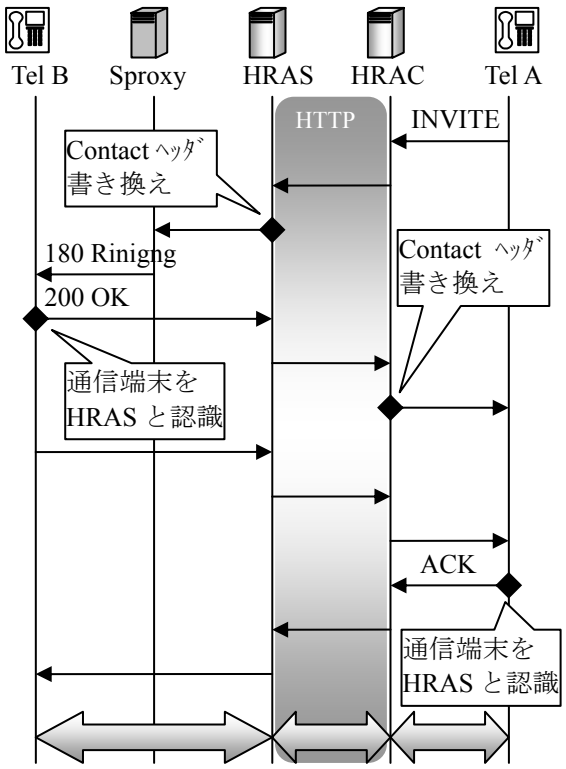

図６．HRA への中継

4. 評価

本提案システムの評価を行うために，既存の IP 電話システムの調査を行った．さらに，セッション確立の方法とシステムの導入の簡易さなどについて本提案システムと比較し，SoftEther のディレイを測定し，提案システムに見立てることでシステム導入によって起こるディレイの見積もりを行った．

4.1. セッション確立の方式

まずセッションの確立方式についての評価を行った．システムごとに，それぞれファイアウォール・NAT・プロキシが通過可能であるか，SIP との互換性，システムを導入することによって起きるディレイという５つの項目で比較を行い，その結果を表１に示す．

表１．セッション確立方式のシステム比較

	FW 通過	NAT 通過	ﾌﾟﾛｷｼ 通過	SIP の 互換	ﾃﾞｨﾚｲ
Linphone	×	×	×	○	○
HCAP	○	○	○	×	△
Skype	○	○	×	×	△
提案ｼｽﾃﾑ	○	○	○	○	△

ここでは，比較システムの一つに，既存の SIP 技術を利用した IP 電話としてフリーソフトである Linphone を挙げた．Linphone ではファイアウォールや NAT などは通過できないが，導入するには SIP サーバと端末を用意するのみでよいので容易である．そしてディレイに関しても UDP で音声通信を行うため，他のシステムに比べ小さい．

また，HCAP・Skype・SoftEther については先の第２章で詳しいことは述べているが，HCAP ではファイアウォール・NAT・プロキシを通過することができる．しかし，セッションの確立方法に HTTP の CGI を利用しているので，SIP との互換性は低く，導入に関しても容易とは言えない．その上，ファイアウォール上に無駄なトラフィックが発生する．

Skype では HTTP プロキシを通過することができず，SIP との互換性も低い．

これらのシステムに対して，提案システムのダイアルでは，ファイアウォール，NAT，プロキシを通過できる上，SIP プロキシ間の通信を

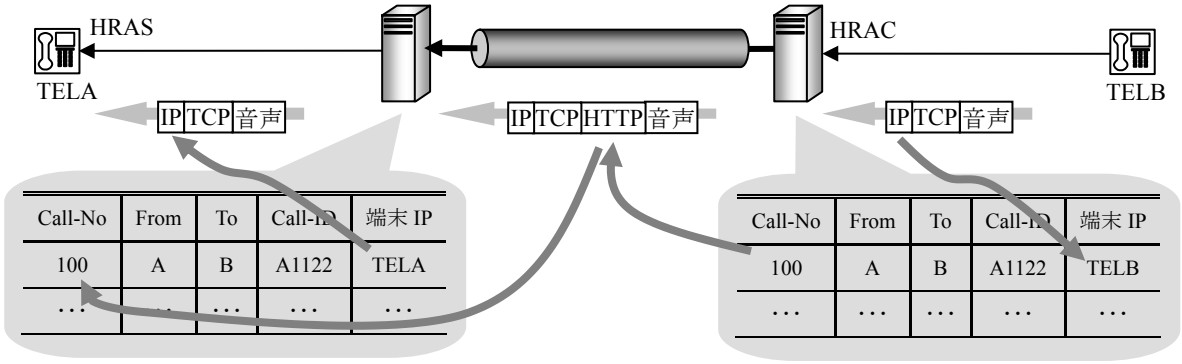

図８．独自ヘッダと変換表

ダイアルメッセージから音声データまで全て HTTP でトンネリングするシステムなので, SIP との互換性は高く， HTTP の機能を利用して通信を行うので HTTP プロキシの通過も可能となる．また，本提案システムでは，既存のファイアウォールシステムに全く影響を与えない上, ファイアウォール上を流れるのはファイアウォールを挟む外部と内部に存在する HRA 同士の 1 対 1 の通信のみとなるため, ファイアウォールを通るトラヒックは少なくなる. そして，HCAP や Skype など端末がデータを HTTP に埋め込む機能を持っているシステムに対し，本システムでは HRA クライアントがその機能を持つため，電話端末から HRA までの通信は既存の SIP 技術をそのまま利用すればよい. そのため, 特別な機能をインストールした電話端末を導入する必要はなく，標準の IP 電話に対応したものを利用すれば良い.

4.2. 音声遅延の評価

前述ではセッションの確立方式について比較を行ったが, 次は音声通信を行う際のディレイについて評価を行う. 本提案システムを導入した場合, 導入によって起こるディレイがどれ程なのか, 提案システムの装置を既存のシステムと同等の機能を持つ装置にあてはめて想定されるディレイを見積もることにした. 見積もりは既存のシステムで単純なネットワーク構成を作り，端末から端末への音声遅延を計り，提案システムに置き換え, さらに後から実際のネットワークに導入した際に想定されるルータによる遅延などを考慮することで行った.

まず比較のためファイアウォール・NAT・プロキシなどの通過をすることのできない単純な VoIP クライアントを利用し，UDP による音声通信を確立して測定を行った. ネットワーク構成は図９のようにごく単純な形で, 両端末の LAN カードでパケットをキャプチャした.

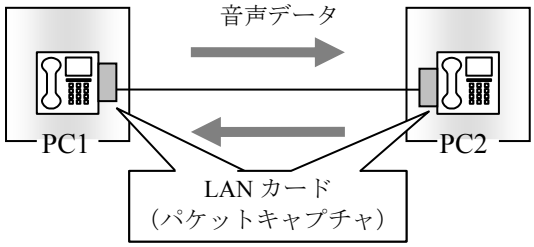

図９．単純な音声通信

次に，提案システムの各構成要素のディレイを見積もるために，ファイアウォール・NAT・プロキシを超えることのできる SoftEther を利用した場合の音声遅延の測定を行った．まず SoftEther を導入し，仮想 LAN を構築した上で既存の VoIP を利用することでファイウォール･NAT･プロキシを超える VoIP を実現した. 実験を行ったネットワークの構成は図 10 の通りである.

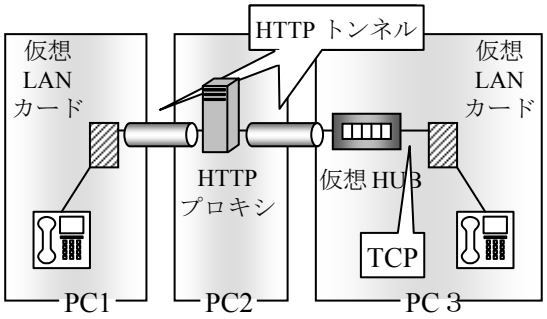

図 10. SoftEther による VoIP

SoftEther では仮想 LAN カードをクライアントにインストールし, グローバル環境上の仮想 HUB へ接続しておく. PC1 には仮想 LAN カードと VoIP 端末を導入した．また，SoftEther は HTTP の接続を利用する際はプロキシサーバのアドレスを設定しなければならないため，PC２には HTTP プロキシを導入してある. そして, PC３には仮想 HUB と仮想 LAN カードを導入し，PC1 の仮想 LAN カードからは HTTP プロキシを介して仮想 HUB へ，PC３の仮想 LAN カードからは直接 TCP で仮想 HUB へ接続するように設定されている．ただし，今回の実験ではシステムの導入によって起こるディレイを測定することを目的とするため全ての構成要素をローカルアドレス上に置いている.

SoftEther では直接 TCP，プロキシ，SOCKS

サーバ，SSH サーバに繋ぐ方法があるが，このようなネットワーク構成にしたのは本提案システムの構成に機能を当てはめ比較を行うためである．この構成を本提案システムに当てはめたイメージを図で表すと，図 11 のようになる．

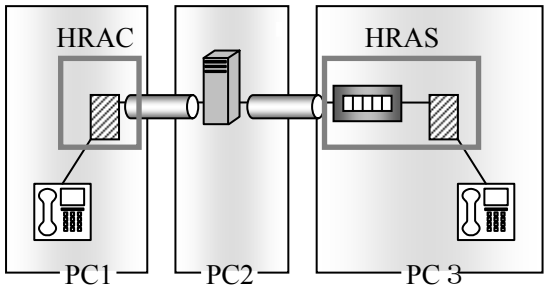

図 11．SoftEther による VoIP

このように仮想 HUB で MAC アドレスと IP アドレスを管理する SoftEther とネットワークレイヤーの違いはあるが，SoftEther の要素を機能ごとに次の表２のように提案システムの要素に置き換えることができる．

表２．構成要素の置き換え

要素	機能	置き換え
HRAS	・ データを HTTP にカプセリング ・ カプセリング解除 GET，POST メソッドの受信	仮想 HUB ＋ 仮想 LAN
HRAC	・ データを HTTP にカプセリング ・ カプセリング解除 GET，POST メソッドの送信	仮想 LAN

また，図７からはあらかじめセッションを確立し，HTTP でファイアウォールを通過する本提案システムと SoftEther は同様の方式のように見えるが，SoftEther は全てのプロトコルに対応することによって，ファイアウォールの利点を全く無効にしてしまうという危険性があるが，SIP と音声通信の特性のみに合わせ，途中で UDP に変換できるようにし，他のプロトコルには対応しない本提案システムとは方針が異なる．

この測定では PC1 の仮想 LAN カードと PC3 の仮想 LAN カードに到着するパケットをキャプチャし端末間の双方向の通信の遅延の計算を単純な直接 UDP 通信の測定と同様にして行った。また，本提案システムの構成要素のみによるディレイも見積もりたい．そこで，図１におけるエンドトゥエンドのディレイから HTTP プロキシによるディレイを引くために，HTTP に埋め込まれた音声データが HTTP プロキシを通過する際のディレイの測定も行った．この測定は HTTP プロキシの LAN カードに到着するパケットをキャプチャし，同一のパケットが HTTP プロキシに到着する時間と新たに作成された中継パケットの出発時間の差を求め HTTP プロキシを通過する際のディレイとした．通常 VoIP エンドトゥエンドの結果を加えたこれらの測定結果は以下の表３の通りである．

表３．測定結果

	遅延(sec)
SoftEther エンドトゥエンド	0.01613120
HTTP プロキシ	0.01499205
ルータ	0.00035500
通常 VoIP エンドトゥエンド	0.00019650

この SoftEther によるエンドトゥエンドの遅延から HTTP プロキシの遅延を引いた値が提案システムの HRAC と HRAS を導入した際に起こるディレイとしての見積もりは以下のようになる．

$$\begin{matrix}\text{HRAC} \\ + \\ \text{HRAS}\end{matrix} = \begin{matrix}\text{SoftEther} \\ \text{エンドトゥエンド}\end{matrix} - \begin{matrix}\text{HTTP} \\ \text{プロキシ}\end{matrix}$$

$$= 0.00113915$$

これに実際のネットワークでは 20～40 のルータが存在すると考えられるので，ルータの遅延を加算すると以下の表４のようになる．また HTTP プロキシを利用する場合も計算した．

表４．提案システムでのディレイの見積もり

	ディレイ
プロキシあり	0.00823915～0.01533915sec
プロキシなし	0.02323120～0.03033120sec

現在，総務省によって IP 電話の評価尺度がクラス A～C まで決められているが，エンドトゥエンドのディレイはクラス A が 100msec 以下，B が 150msec 以下，C が 400msec 以下とされている．このようにルータを通した上で，更にプロキシがあってもパケットのディレイは 100msec 以下のクラス A にあたり，充分なディレイが得られていると思われる．しかし，この評価尺度はパケットを UDP で送信することを前提としている．よって，今回の提案システムのように TCP を利用する場合にはネットワーク品質の保障された環境ならまだ良いが，ネットワークの状態によってはパケット・ロスからの再送，パケットの揺らぎ（ジッター）などにより，TCP を利用する本提案システムはパケットの平均ディレイは充分であっても音声通信の性能は著しく影響を受けることが予測される．良い音声品質を得るには最終的により短いディレイに加え，ジッター，およびパケット・ロス値が必要となる[16]．これについては次の段階でシステムの実装を行った際に解決しなければならない課題として検討を行っていく予定である．しかしながら，提案方式や SoftEther と同じように HTTP によるファイアウォール・NAT・プロキシの通過を解決している HCAP では音声品質の測定の結果，直接 UDP により通信する方式と同等の通信品質が得られたという報告がある[17]．この報告は提案システムの実装を行う上での通信品質に期待できるものとなる．

5．おわりに

本論文では，IP 電話が課題とするファイアウォール・NAT・プロキシを越えることのできる新しいシステムを提案し，その詳細について説明した．また，既存の VoIP と提案システムを複数の項目に分けて比較することにより，システムを導入することによって得られる利点について考察し，既存システムの測定値から提案システムを導入した際に生じるディレイについても見積もりを出してその結果を報告した．

今後はこの提案システムの実装を行い，その測定結果を出し，また既存技術と比較することにより，実際に既存技術と比べてセッション確立による有効性と，実用的な音声品質が得られるかを評価する．ただし，本提案方式では TCP 通信を利用するのでネットワークの状況によって影響を大きく受けることが予測されるので，それについても検討を行っていく．また，今回は NAT・ファイアウォール以下にある内部ネットワークと通信する相手はグローバル環境上における端末であると言う制限された環境で検討を行ってきたが，その実装が上手くいけば，同時に相手端末が同じように NAT・ファイアウォールの存在する環境であった場合でもセッション確立，音声通信ができるように検討を行っていく予定である．

参考文献

[1] 星 徹:VoIP の最新動向,情報処理学会誌, Vol.42 No.02 - 008

[2] N.Freed : Behavior of and Requirements for Internet Firewalls , IETF RFC 2979 (2000.10).

[3] K. Egevang, P. Francis:The IP Network Address Translator (NAT),IETF RFC 1631(1994.5).

[4]Berners-Lee,T.,Fielding,R.T.and Nielsen,H.:Hyper-TextTransfer Protocol-HTTP/1.0, IETF RFC (1994.11).

[5] 大田:Colum 本当のインターネットをめざして，Vol.6，インターネットと電話（２），情報処理学会誌，Vol.40,No9,pp922 923

[6] 千村保文，村田利文“SIP 教科書”IDG ジャパン

[7] J. Rosenberg,et all”SIP: Session Initiation Protocol”IETF RFC3261(2002.6)

[8]Petri Koskelainen,Henning Schulzrinne,Xiaotao Wu:VoIP:A SIP-based conference control framework,ACM press 53-61(2002.5).

[9] Stefan Berger,Henning Schulzrinne,Stylianos Sidiroglou,Xiaotao

Wu:Conferencing:Ubiquitous computing using SIP,ACM press 82-89(2003.6)
[10] S. Deering, R. Hinden: Internet Protocol, Version 6 (IPv6) Specification,RFC 2460(1998.12).
[11] UPnP Forum:
" http://www.upnp.org/"
[12] NATS Project:
"http://www.nats-project.org"
[13] 宮内信二"多様な環境で利用できるインターネットプロトコル"情報処理学会論文誌 Vol.44 No.3
[14] Skype:
" http://www.skype.com/home.html"Kazaa
[15] 登大遊"SoftEther による Ethernet の仮想トンネリング通信"
[16] AVAYAlobs"AVAIYA IP VOICE QUALTY NETWORK REQUIREMENTS"
[17] 宮内信二，他"ブロードバンド時代のインターネットに適した HTTP による VoIP 方式" CSVC2001-13,pp.39 43,7(2001.4.5).

伊藤　将志（渡邊研究室 B4）
2004 年名城大学理工学部情報科学科卒業．同年，同大学院理工学研究科情報科学専攻修士課程進学．マルチメディアネットワークの研究に従事．2003 年度情報科学科 Web コンクール優秀賞．同大学 TEC 所属．情報処理学会会員．

渡邊　晃（教授）
1974年慶応大学電気工学科卒業．1976年同大学院修士課程修了．同年三菱電機（株）入社．以来，同社情報技術総合研究所にてLAN，ネットワークセキュリティ等の研究開発に従事．新エネルギー・産業技術総合開発機構（NEDO）を経て，現在，名城大学理工学部教授．情報処理学会会員．電子情報通信学会会員．