社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（19）
2005－CSEC－28（19）
2005／3／22

ファイアウォールを通過できるIP電話の提案と実装

伊藤将志　渡邊晃

名城大学理工学研究科

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てきた．しかし，ファイアウォール・NA(P)T・プロキシサーバなどにより外部との通信に制限のある企業ネットワークでは外部の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我々はSIPから音声通話までをHTTPトンネルを用いて，外部と内部のIP電話通信を可能とするシステムSoFW（SIP over FireWall）を提案してきた．本稿ではSoFWの機能と実装方式について報告する．

A Proposal and an Implementation of Voice over IP System Passing Through FireWall

Masashi Ito　Akira Watanabe

Graduated School of Information and Science, Meijo University

In recent years, IP telephone has achieved remarkable progress on the Internet through "low priced charge", "continuous connection environment", and "high-speed communication band". However, it is not easy to use IP telephone over firewall and NA(P)T because of their restrictions of the communication. We have proposed the system called SoFW that suppresses the problem. In this paper, detailed functions and its implementation method of SoFW are described.

1．はじめに

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たことで，これまでIP電話の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IP電話専用番号“050-”の事業者受付が開始となり，公衆回線網の電話機からのダイヤルを受信することが可能になった結果，多くのISPがIP電話サービスを提供するようになった．

しかし，VoIP（Voice over Internet Protocol）[1]の利用範囲を制限してしまうファイアウォール（以下FWと記述）[2]やNA(P)T[3]の介在により，VoIPによる外部ネットワークとの通信ができない企業ネットワークがほとんどである[4]．IP電話の普及を進めるには，企業ネットワークへの浸透が不可欠であり,これらの装置が介在しても安全に通話できることが必要である．

VoIPに関連するプロトコルとしては，早い時期にITU-T（International Telecommunication Union – Telecommunication）によって標準化された H.323[5]という既存の電話仕様をベースにしたシグナリングプロトコルがあるが,現在ではIETF（Internet Engineering Task Force）によって標準化されたSIP（Session Initiation Protocol）[6]が実装も容易で拡張性に優れているとして様々なマルチメディア通信で注目されている．現在はISPが提供しているIP電話の多くがSIPを採用している[7] [8].

しかし，SIPはダイヤル開始時に相手端末のIPアドレスが特定できるか，相手端末の属するSIPサーバのIPアドレスが特定できることが必須である．そのため，NA(P)Tが介在するような環境ではプライベートアドレス側のIPアドレスが特定できず，ダイヤルできない．また，企業などのFWは多くの場合，メールや内部から外部へのWebサーバへのアクセスなどに通信を限定しており，それ以外の通信を遮断してしまう．このような制限を受けたネットワークにSIPを適用したIP電話を導入しようとすると，FW再設

定のために企業のセキュリティポリシーの変更が必要になる上, それに伴うセキュリティ低下の恐れが発生する.

そこで, FW ／NA(P)T などによって IP 電話としての機能を制限されることのないシステムがいくつか提案されている. 代表的なシステムとして HCAP[9], Skype[10]などがあり, VoIP に限らずプロトコルフリーで FW の通過を可能にする方式として SoftEther[11]がある. HCAP は端末とグローバルアドレス環境に置かれた中継サーバとの間で HTTP トンネルを作り FW を越えることができる. しかし, 端末に特殊な機能が要求されたり, FW 上には無駄なトラヒックが流れるという課題がある. Skype は IP 電話機能を 80 番ポート上で実行することにより FW を越えるが, 独自アプリケーションであるため HTTP プロキシサーバ[12]などが介在すると中継できない. SoftEther は端末と中継装置の間をイーサネット・フレームごと HTTPS に埋め込んで中継することで FW をまたがって仮想的なイーサネットを作ることができる. しかし, この方式では本来 FW 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可能性がある. また, 仮想ネットワーク内のアドレスを統一的に管理する必要があるという課題がある.

そこで著者らは, FW の内部と外部にリレーエージェントを配置し, 端末からの SIP メッセージと音声データを HTTP でトンネルすることで, 既存ネットワークに影響を与えない IP 電話システム, SoFW（SIP over FireWall）を提案してきた[13]. 本稿では SoFW の機能を整理し, かつ実装方式について検討したので報告する.

以下, 2 章で既存のファイアウォール通過技術とその問題点について述べる. 3 章では提案システム SoFW の概要を, 4 章では実装方法を説明し, 5 章でまとめとする.

2. 既存の技術とその課題

FW を通過する既存のシステムとして SoftEther と HCAP をとりあげ, その方式と課題について簡単に説明する. なお SoftEther は IP 電話に限らず全てのアプリケーションで FW ／NA(P)T を通過できるシステムのため, SoftEther を導入したネットワーク上で IP 電話を利用する場合を想定した.

2.1. SoftEther

SoftEther は FW 内部の端末に仮想 LAN カードと呼ばれる機能を, 外部の端末に仮想 HUB と呼ばれる機能を組み込む. 仮想 LAN カードと仮想 HUB は HTTPS などの FW を越えられるプロトコルでトンネルを作っておく. アプリケーションはこのトンネルを使って外部とのやり取りを行う. この仮想ネットワーク上に IP 電話を導入するには端末接続型とネットワーク接続型の 2 通りの方法が考えられる.

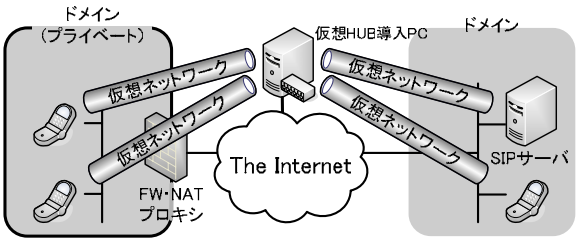

図 2.1 端末接続型の構成

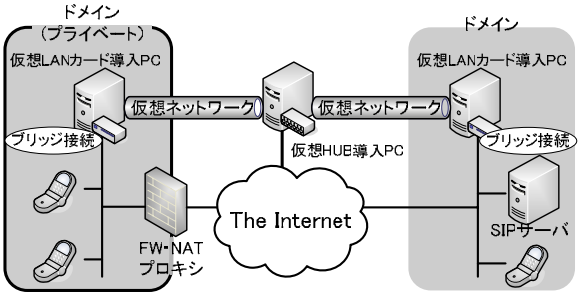

図 2.2 ネットワーク接続型の構成

端末接続型の構成を図 2.1 に示す. 仮想 LAN カードを導入した端末それぞれから仮想 HUB に接続して仮想ネットワークを形成する. 仮想ネットワーク上の端末はあたかも同一の LAN 上にあるように見える. 仮想ネットワーク上で SIP サーバと電話端末を導入すれば FW を越えた IP 電話が構築できる.

ネットワーク接続型の構成を図 2.2 に示す. 仮想 LAN カードを導入したゲートウェイにより仮想ネットワークと実際の LAN をブリッジ接続する. これにより, 二つの LAN を仮想的ネットワークで繋げ, 一つの LAN にすることができ, 仮想 LAN カードを導入していない端末からでも FW を越えた通信が可能となる.

しかし, SoftEther を用いた方法は電話端末の IP アドレスを全て同じアドレス空間上で管理することを必要とする. 端末接続型では仮想アドレスを, ネットワーク接続型では異なる LAN 同士で実アドレス空間を統一する必要がある. また, 全てのアプリケーションに FW の通過を許して

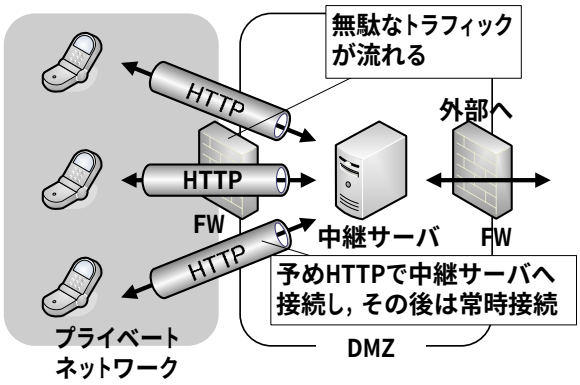

図 2.3 HCAP の構成

しまうことから, セキュリティ的にも問題が発生する.

2.2. HCAP

HCAP では図 2.3 のように FW の DMZ 上に中継サーバが設置され，内部には HCAP 対応機能を内蔵した端末が設置される. 端末立ち上げ時に端末から中継サーバへ HTTP で接続して，トンネルを作り, 以後は接続を維持する. ダイヤルや音声データは HTTP の GET メソッドに対するレスポンスと POST メソッドに埋め込んで中継する．HCAP は外部の Web サイトを閲覧できる環境であれば，FW／NA(P)T を通過できる．しかし, 音声端末側にそれぞれ専用のプロトコルをインストールする必要がある．また, 中継サーバに FW 内の複数の専用端末から常時 HTTP による接続を行うため, FW 上に不要なトラヒック流れる.

3. 提案方式の概要

図 3.1 に SoFW ネットワーク構成を示す. SoFW の構成要素には HRAC と HRAS があり, 企業ネットワーク内部の端末は既存のものを利用する. 外部には通常の SIP を用いた IP 電話の環境があることを想定する. 企業ネットワークのプライベートアドレス環境には HRAC，外部のグローバルアドレス環境に HRAS を設置する. この２つの装置の間に HTTP トンネルを張り, 内部に対してプライベートアドレス, 外部に対してグローバルアドレスのインターフェースを持った２つで１つの仮想的な SIP サーバとしての役割を持たせる．また音声通話時もこの HTTP トンネルを利用して, 音声ストリームを中継する.

HRAC は主に HTTP への埋め込み・解除を担当するのみで，HRAS が HTTP への埋め込み・

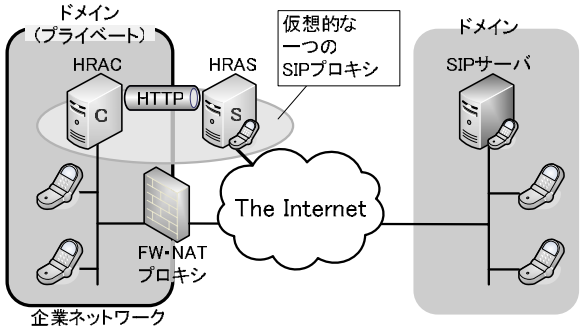

図 3.1 SoFW の構成

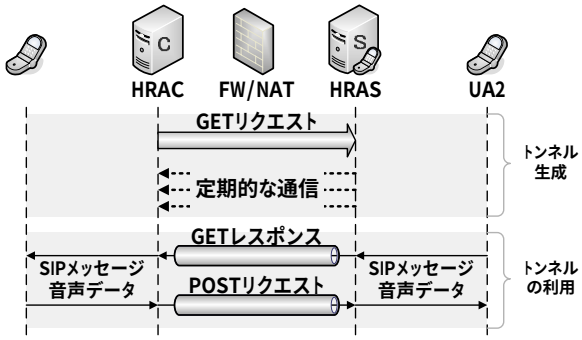

図 3.2 HTTP トンネル生成

解除や SIP サーバ・RAT 管理・SDP 修正（後に説明）などの主要な機能を担う.

以下では HRAC と HRAS の機能をシステム立ち上げから通話終了まで過程に沿って説明する.

(1) HTTP トンネル生成

HTTP トンネルの生成は既存技術と同様の方式を利用する. SoFW ではシステム立ち上げ時に HRAC と HRAS の間で HTTP トンネルを生成し, 以後の通信は全てこのトンネルを通す. このシーケンスを図 3.2 に示す.

SoFW では HRAC に HTTP クライアントとして，HRAS に HTTP サーバとしての機能を持たせる．まず，HRAC から HRAS へ接続し，GET リクエストを送信し待機する. 待機中は接続維持のため HRAS から HRAC へ定期的通信を行う. 端末間の通信が始まると, 外部から内部への SIP メッセージ・音声ストリームは GET レスポンスに，内部から外部への SIP メッセージ・音声ストリームは POST リクエストに埋め込み，中継する.

(2) 端末情報の登録

ダイヤルに先立ち，あらかじめ SIP の端末情報を HRAS に登録しておく必要がある．ユーザ

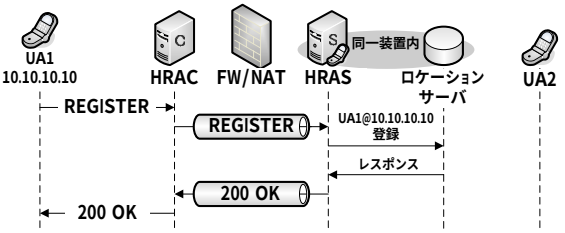

図 3.3 登録処理

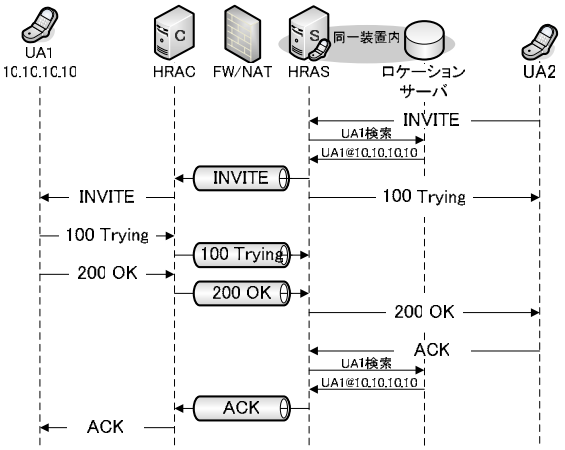

図 3.4 ダイヤルのシーケンス

識別子：UA１，IP アドレス：10.10.10.10 の端末が登録を行うシーケンスの例を図 3.3 に示す. 従来の SIP では，端末は SIP サーバが管理するロケーションサーバへ自身の IP アドレス・ユーザ識別子などの情報を登録する. ロケーションサーバは SIP サーバにユーザ情報を提供するデータベースであり, SIP サーバと同一の装置に組み込まれている場合が多い．本システムの HRAS の持つ SIP サーバ機能もロケーションサーバを SIP サーバ内に組み込んでいる. SoFW では端末は SIP サーバの代わりに HRAC の IP アドレスまたはホストを指定し，REGISTER メッセージを送信する．HRAC はトンネルを用いて REGISTER メッセージを HRAS へ中継する. メッセージを受け取った HRAS はロケーションサーバに端末情報を登録し, 登録が完了するとトンネルを用いて 200OK メッセージを端末に返す.

(3) ダイヤル

外部端末 UA2 から内部端末 UA1 へダイヤルを行う場合のシーケンスの例を図 3.4 に示す.

UA2 は INVITE メッセージを HRAS へ送信する．HRAS の SIP サーバ機能は INVITE メッセージの宛先（UA1）のユーザ識別子からロケーションサーバに UA1 の IP アドレスを問合せ，そ

表 3.1 RAT の内容

内容	説明
To	ダイヤルを識別するためのダイアログ ID の一つ
From	同上
Call-ID	同上
IIP	内部ネットワーク端末の IP アドレス
IPort	内部ネットワーク端末のポート番号
OIP	外部ネットワーク端末の IP アドレス
OPort	外部ネットワーク端末のポート番号

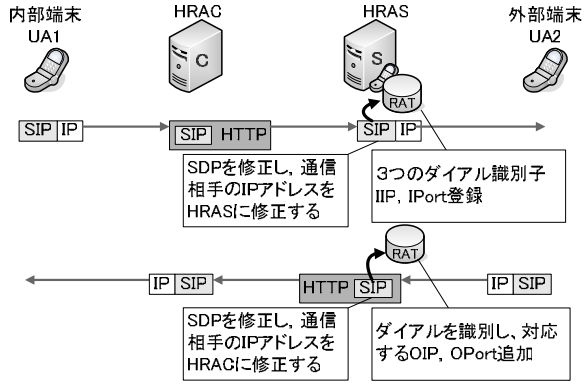

図 3.5 RAT 生成と SDP 修正

の IP アドレスと INVITE メッセージを HTTP トンネルに通して HRAC へ送信する．HRAC は UA1 へ INVITE メッセージを送信する．以後の SIP メッセージも同様に HTTP トンネルを用いて中継する.

HRAS では SIP メッセージを中継しながら，RAT 生成と SDP 修正処理を行う. 内部端末から通信が始まる RAT 生成と SDP 修正の例を図 3.5 に示す. RAT 生成では, 後に音声データを HTTP トンネルで中継するのに必要なユーザ情報を集め RAT（Relay Agent Table）と呼ぶテーブルを生成する．このユーザ情報は SIP メッセージボディ部に含まれる SDP(Session Description Protocol）[14]から参照される．SDP は端末が音声通信に利用する IP アドレス・ポート番号などの情報を記述するためのプロトコルである. RAT の内容を表 3.1 に示す．RAT ではダイアログ ID と呼ばれる SIP のパラメータである To，From，Call-ID の３つを格納するフィールドとそのダイアログ ID に対応した内部端末・外部端末の IP アドレス･ポート番号を格納するフィールドを持つ. HRAS は内部端末の UA1 から SIP メッセージを受け取ると，ダイアログ ID と UA1 の IP アドレス･ポート番号を RAT に登録する. そして，外部端末の UA2 から SIP メッセージを受信する

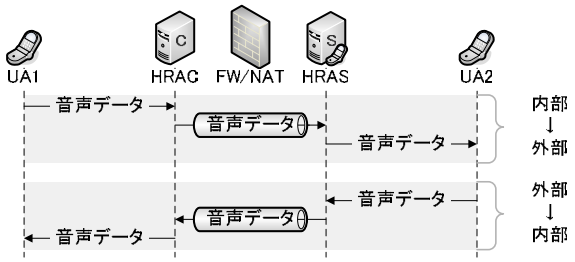

図 3.6 音声データのシーケンス

と, ダイアログ ID に対応するレコードを検索し, UA2 の IP アドレス・ポート番号を追加する.

次に SDP 修正の機能を説明する. 通常の SIP 手順ではダイヤルが完了すると音声端末は相手端末と P2P で通信を行う. しかし, SoFW では図 3.5 のように, 音声通信の際, 端末に音声ストリームをトンネル中継させるため, 内部端末には通信相手端末を HRAC であるように, 外部端末には通信相手端末を HRAS であるように認識させる処理を行う. HRAS は内部端末 UA1 から SIP メッセージを受信すると, SDP の解析を行い, 相手端末が音声通信に利用する IP アドレスを記したパラメータを HRAS の IP アドレスに書き換える. また, HRAS が外部端末 UA2 から SIP メッセージを受信した場合は, 上記パラメータを HRAC の IP アドレスに書き換える.

(4) 音声通信

ダイヤルが完了すると音声データのやり取りが可能となる. 音声データのやり取りのシーケンスを図 3.6 に示す.

音声データにはユーザ情報が含まれていないため, データ部に RA（Relay Agent）ヘッダを定義する. この一連の流れを図 3.7 に, RA ヘッダの構成を図 3.8 に示す.

内部端末 UA1 から外部端末 UA2 へ音声データを送信する場合, まず UA1 は修正された SDP に従って, 音声データを HRAC へ送信する. HRAC では受信した音声データの送信元 IP アドレスとポート番号を元に RA ヘッダを生成して音声データに付加し, それを HTTP トンネルに埋め込み HRAS へ中継する. HRAS は RA ヘッダから取り出した IP アドレス・ポート番号を IIP・IPort として RAT を参照し, 対応する OIP・OPort を宛先とし, UA2 へ送信する.

逆に外部端末 UA2 から音声データが送信される場合, まず UA2 は HRAS へ音声データを送信する. HRAS では送信元の IP アドレス・ポート番号を OIP・OPort として RAT を参照する.

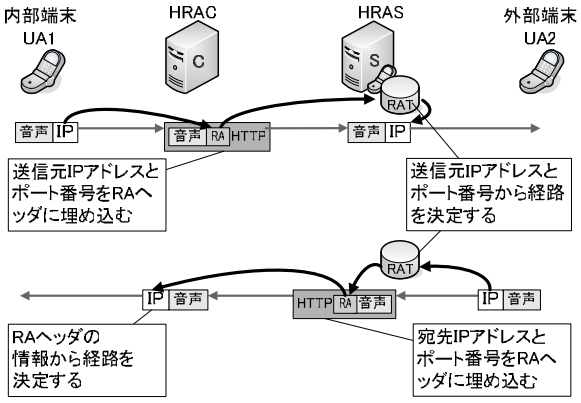

図 3.7 RAT を利用した音声データの中継

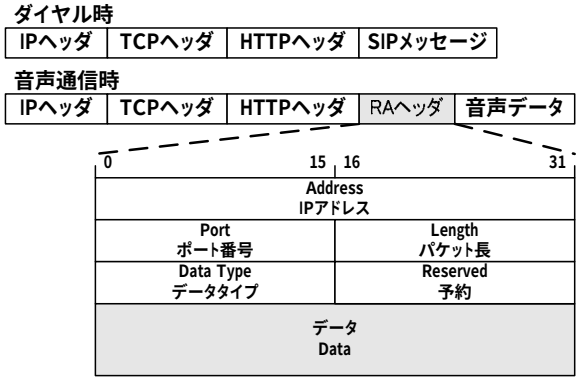

図 3.8 RA ヘッダの構成

HRAS は対応する UA1 の IP アドレス・ポート番号である IIP・IPort を元に RA ヘッダとして音声データに付加し, HRAC へ送信する. HRAC は RA ヘッダから宛先の IP アドレスとポート番号を取り出し, 送信する.

(5) 切断

通話を切断すると端末は BYE メッセージを相手端末に向けて送信する. 本システムではこのメッセージを HRAS が受信すると, その通信に関する端末情報を RAT から削除する.

4. 実 装

本システムを LinuxRedhat9.0 上のアプリケーションに実装中である. HRAS の SIP サーバはフリーソフトである SER[15]を利用する. SER はシステムが立ち上がると SIP 端末に対してソケットの生成を行い, 端末から SIP メッセージが届くまで待機する. SIP メッセージを受信するとそれを解析し, メッセージのタイプに応じて RFC3261 に準じた登録・中継などの処理を行う. ここで, HRAS の SIP サーバ機能を担う SER に

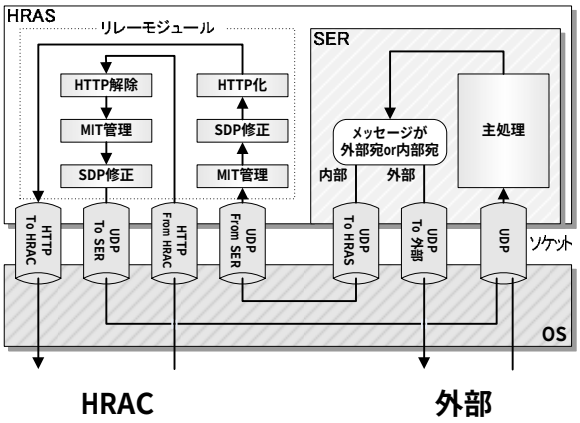

図 4.1 HRAS と SER の関係

対してそれ以外の機能を担うプログラムをリレーモジュールと呼ぶ.

SER とリレーモジュールを連携させるため, SER の外部端末に対する SIP メッセージの出力部分にメッセージの宛先が外部宛か内部宛かにより, 以後のプロセスを分岐するための変更を施す. HRAS のリレーモジュールと SER はソケットを介して接続する. SER の主処理の部分は修正を施さず, そのまま利用する.

HRAS と SER の間のデータと処理の流れの関係を図 4.1 に示す. HRAS のリレーモジュールは SER と１つの装置上で互いに送受信用のソケットを生成する. SER が外部端末から SIP メッセージを受信すると, SER の主処理が実行される. この SIP メッセージは内部宛であるため, リレーモジュール宛てのソケットへ送信される. リレーモジュールが SER に対して開いていたソケットから受信した上記 SIP メッセージは, RAT 管理・SDP 修正・HTTP 化などの処理を経て, HRAC へ送信される. 逆にリレーモジュールが HRAC から受信した SIP メッセージは HTTP のデカプセル･RAT 管理･SDP 修正の処理を経て, SER 宛のソケットへ送信される. SER では SIP メッセージを受信後, 主処理が実行されて上記で追加された分岐処理によって外部へ向けて送信される.

5. おわりに

本稿では SoFW の機能の詳細と実装方法を報告した. 今後は実装を完了させ, 動作検証と評価を行う予定である.

また, 本稿では SIP で扱うマルチメディア・データを音声データに限定して説明したが, SIP は様々な用途に対して, その将来性が注目されており, IP 電話以外への応用もして行く.

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] 大田 昌孝: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

[5] H.323,Packe Based Multimedia Communications Systems, ITU-T Recommendation,1998.

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

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

[8] Stefan Berger,Henning Schulzrinne,Stylianos Sidiroglou,Xiaotao Wu:Conferencing:Ubiquitous computing using SIP,ACM press 82-89(2003.6)

[9] 情報処理学会論文誌, Vol.44, No.3, 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”

[10] Skype: ” http://www.skype.com/home.html”Kazaa

[11] 登大遊“SoftEther による Ethernet の仮想トンネリング通信”

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

[13] 情報処理学会研究報告, 2004-DPS-120, Vol2004, No107

[14] Handley,M. and Jacobson, V.:SDP:Session Description Protocol,IETF RFC2327(1998)

[15] SER:“http://www.iptel.org/ser/”