ファイアウォールやNATを通過できるIP電話の提案と評価

伊藤将志[†] 鹿間敏弘[††] 渡邊晃[†]

通信基盤の発達により，IP電話は実用レベルの品質を確保できるようになった．しかし，グローバルネットワークと企業ネットワークの間には，ファイアウォールやNATが存在し，自由かつ安全にIP電話を利用することは困難である．本論文では2台のリレーエージェントをグローバルネットワーク環境と企業ネットワーク環境に設置し，HTTPトンネルを生成することによりVoIP通信のファイアウォールやNATを通過できるIP電話システムSoFW（SIP over FireWall）を提案する．これまでの類似の研究や解決方法では，専用端末が必要であったり，アドレス空間の統一的管理が必要であったりするなどの課題があった．SoFWは既存のSIP端末を利用することができ，アドレス空間の統一的管理が必要なく，導入が容易であるという特長がある．SoFWをLinux上に実装し，評価実験を行った結果，その有用性を確認することができたので報告する．

Proposal and Its Evaluation of IP Telephone That Can Pass through a Firewall and a NAT

Masashi Ito,[†] Toshihiro Shikama[††] and Akira Watanabe[†]

Due to development of communication infrastructure, IP telephone has reached a level of practice use. However, it is difficult to use IP telephone freely and safely, because there exist a firewall and a NAT between a global network and enterprise networks. In this paper, we propose a system called SoFW (SIP over Firewall) that enables passing through a firewall and a NAT by placing two relay agents on a global network and a private network, and generating an HTTP tunnel. Though there exist similar technologies, however, they need special terminals or integrated control of IP addresses. SoFW can use normal SIP terminals, and does not need integrated control of IP addresses, and it is easy to setup. We have implemented SoFW on Linux machines and confirmed the effectiveness.

1. はじめに

ブロードバンドの普及や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し，IP電話は十分な通信品質を確保できるようになった．これにともない，多くの企業は通話料金の削減や，IP電話特有の機能，アプリケーションとの連携による生産性向上を期待して社内LANへのIP電話導入を進めてきた．

しかし，企業ネットワークには外部ネットワークとの間にファイアウォール[1]やアドレス変換装置（Network Address Translator：以下NAT）[2]が存在するため，企業ネットワークとその外部のネットワークに接続した端末どうしで自由にVoIP（Voice over IP）を利用することができない[3]．企業ネットワークと外部のネットワーク間においてVoIPが自由かつ安全に利用できるようになればIP電話の利便性はさらに向上するものと考えられる．

VoIPのセッション開始プロトコルとしては，電話仕様をベースとして早期にITU-T（International Telecommunication Union - Telecommunication）によって標準化されたH.323[4]がある．しかし，現在はIETF（Internet Engineering Task Force）によって標準化されたSIP（Session Initiation Protocol）[5]が実装も容易で拡張性に優れており，様々なマルチメディア・サービスに利用できるため注目されている．現在，ISPが提供しているIP電話のほとんどがSIPを採用している．SIPは主にユーザエージェントとSIPサーバで構成されており，SIPサーバにユーザエージェントの位置情報を登録し，この位置情報をもとに呼設定のためのメッセージの中継を行う機能を提供する．しかし，SIPは呼設定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

† 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†† 三菱電機株式会社情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation

の IP アドレスが特定できることが必須である．そのため，NAT が介在するような環境では呼設定を開始できないという課題がある．また，企業などのファイアウォールは多くの場合，メールや内部から外部への Web サーバ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 IP 電話を導入し，外部との通話に利用しようとすると，企業のセキュリティポリシの変更が必要になり，ファイアウォールの設定変更の稼動やセキュリティ上のリスクが増加する．

そこで，ファイアウォールや NAT 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．これらはファイアウォールの許可する通信を動的に操作する方法と，HTTP などのあらかじめファイアウォールが通信を許可しているプロトコルを利用して通信する方法の 2 種類に分けられる．前者は IETF でもいくつかの関連技術が提案されている[6)~7)]．この方式はピンホール・ファイアウォールと呼ばれ，例として文献 8) ではファイアウォールが SIP による呼設定を監視し，その呼設定によって開始される音声通信のみを許可するようにフィルタ処理を動的に変更する．しかし，音声通信では不特定多数の IP アドレスとポート番号を使った UDP の通信が利用されるため，ピンホール・ファイアウォールは企業によってはセキュリティポリシの変更が必要となる．また，ファイアウォールへのモジュール追加や新規の VoIP 専用ゲートウェイ設置が必要とされるため，導入には手間がかかる．後者の代表的なシステムとして HCAP[9)]，Skype[10)] などの IP 電話専用システムと，全アプリケーションに適用できる SoftEther（現在では PacketiX VPN と名称が変更されている）[11)] がある．HCAP や Skype はファイアウォールの外側に設置された中継サーバと電話端末間で HTTP トンネルを張ることにより，Web を閲覧できる環境であれば IP 電話による通話が可能になる．しかし，端末に特殊な機能が必要なため，企業ネットワークに導入するには IP 電話端末の総入替えが必要である．

SoftEther はファイアウォール外部の仮想 HUB というソフトウェアとファイアウォール内部の仮想 LAN カードというソフトウェア間で HTTPS などのトンネルを張り，仮想的なイーサネット環境を構築することができる．しかし，この方法は仮想的なイーサネット内での IP アドレスと MAC アドレスの統一的管理を要すること，内部のネットワークが外部にさらされる危険があるなどの課題があり，企業ネットワークの IP 電話として利用するには適していない．

現時点で市場に出ているファイアウォール対応 SIP appliance や SIP-NAT 対応ファイアウォールとしては下記のようなものがある．

文献 12) では 2 台の中継装置によって SIP 通信のファイアウォール越えを可能にする．2 台の中継装置間では NAT を通過するために UDP ホールパンチング[13)] を用いた音声の経路を生成する．このため，ファイアウォールには UDP を通過させるための設定変更が必要になり，企業のセキュリティポリシに影響を与える．文献 14) ではルータとして設置された装置が SIP に含まれる情報から，アドレス変換の操作やピンホール・ファイアウォールの設定を動的に変更して音声の通過を可能にする．しかし，UDP ホールパンチングの場合と同様に UDP を通過させるため，企業のセキュリティポリシの変更が必要となる．また，ルータの取替えが必要で，導入には手間がかかる．

本論文ではファイアウォールの内部と外部に 1 台ずつリレーエージェントと呼ぶ装置を設置し，その間に呼設定用と音声ストリーム用に HTTP トンネルを張り，すべての端末からの SIP メッセージと音声ストリームをこのトンネルに通す SoFW（SIP over FireWall）を提案する．これを実現するために，呼設定時の SIP のメッセージボディを書き換え，SIP 端末が音声ストリームをトンネルに向けて送信するように誘導する．SoFW は既存のネットワーク機器に影響を与えないため導入が容易であり，既存の SIP 端末をそのまま利用できる．また，IP アドレス管理にもいっさい影響を与えない．将来的には，音声通信に限らず，様々な SIP 端末への応用が可能である．SoFW を実装し性能評価を行った結果，実用に耐えうる性能を発揮できることを確認した．以下，2 章で既存技術とその課題について説明し，3 章で SoFW の概要と実現方法について述べる．4 章では実装方式について説明し，5 章で評価，6 章でまとめとする．

2. 既存技術とその課題

ファイアウォール（以下 FW）を通過する既存技術として HCAP と SoftEther 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 はすべ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であるため，SoftEther により形成された仮想的なイーサネット環境上に IP 電話に必要な装置を設置する場合を想定した．

2.1 HCAP

HCAP の概念図を**図 1** に示す．HCAP では FW の DMZ（DeMilitarized Zone）上などのグローバルな

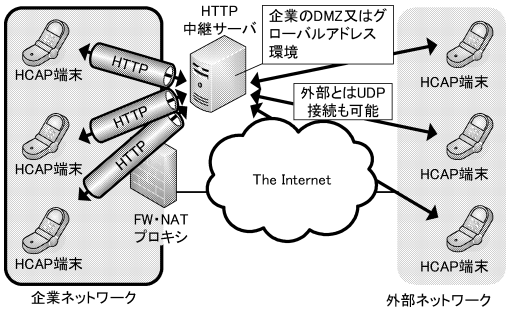

図 1 HCAP の概念図
Fig. 1 A concept of HCAP.

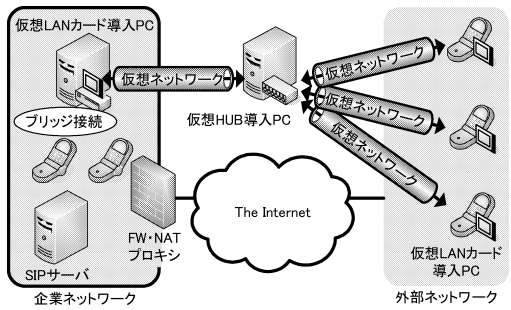

図 2 仮想的なイーサネット上での IP 電話ネットワーク構成例
Fig. 2 Example of composing an IP telephone network using SoftEther.

アドレス空間に中継サーバを設置し，プライベートアドレス空間となる企業ネットワーク内には HCAP 対応機能を内蔵した端末を設置する．HCAP 端末立ち上げ時に端末から中継サーバへ HTTP で接続して，トンネル経路を作る．HTTP の CGI（Common Gateway Interface）の機能を利用して，セッションの開始を行い，Inbound の音声ストリームは HTTP の GET メソッドに対するレスポンスに，Outbound の音声ストリームは POST メッセージ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/NAT を通過できる．また，グローバルアドレス空間上の端末に対しては UDP の利用もできる．HCAP は，個々の端末が HCAP 機能を保持するか，回線交換タイプの既存電話機をアダプタにより収容する方法がある．HCAP は電話端末が FW を越えて通信できるようにすることが目的であり，呼設定および音声通信とも中継サーバを経由した通信となるように独自の手順が定義されている．そのため，SIP 端末との互換性は考慮されていない．SIP 端末対応のアダプタを準備しようとすると，プロトコル変換が必要となるため処理が煩雑になる．

2.2 SoftEther

図 2 に SoftEther による仮想的なイーサネット上で SIP による IP 電話ネットワークを構築した例を示す．SoftEther は FW 内部の端末に仮想 LAN カードと呼ばれる機能を，外部のサーバ端末に仮想 HUB と呼ばれる機能を組み込む．通信に先立ち仮想 LAN カードは仮想 HUB に対して HTTPS や SSH などの FW を越えられるプロトコルで接続し，トンネルを作る．このとき仮想 LAN カードには仮想 MAC アドレスと仮想 IP アドレスが割り当てられる．仮想 LAN カードはトンネルにイーサフレームごと埋め込んで送信し，仮想 HUB がイーサフレームの経路決定を行い，該当する端末に転送することにより仮想的なイーサネット環境を作る．各端末はこの仮想的なイーサネット環境を利用して，FW/NAT の有無にかかわらずあらゆる通信を自由に行うことができる．また，仮想 LAN カードを導入した端末と通常のイーサネットをブリッジ接続することにより，ネットワークごと外部につなぐことも可能である．仮想的なイーサネット環境上で IP 電話を利用するには仮想的なイーサネット環境上に IP 電話要素を導入すればよい．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ため FW の意味がなくなる．また，仮想的なイーサネット環境上の IP アドレスや MAC アドレスを統一的に管理する必要があり，企業ネットワークの IP 電話として利用するのは難しい．

3. SoFW

3.1 SoFW の概要

SoFW は標準の SIP 対応の音声端末を対象とする．SIP 端末は LAN に直結され，音声端末としてだけでなく様々なアプリケーションを実行できる．SoFW は，このような SIP で構成された既存のネットワーク環境にいっさい手を加えないまま，FW を越えた通信が可能になる．本論文では音声に着目しているが，将来的にはそれ以外の様々な SIP 端末への応用が想定できる．

SoFW の構成を**図 3** に示す．SoFW では SIP サーバの代わりに内部のプライベートアドレス環境上に HRAC（Half Relay Agent Client），外部のグローバルアドレス環境上に SIP サーバ機能を備えた HRAS（Half Relay Agent Server）を設置する．システム立ち上げ時において，HRAS と HRAC は SIP メッセージと音声ストリームを中継するためのトンネルを生成する．呼設定時において HRAS および HRAC は SIP 端末からグローバル IP アドレスとプライベート IP アドレスのインタフェースを持つ仮想的な 1 つの SIP サーバのように見える．音声通信時は SIP メッセー

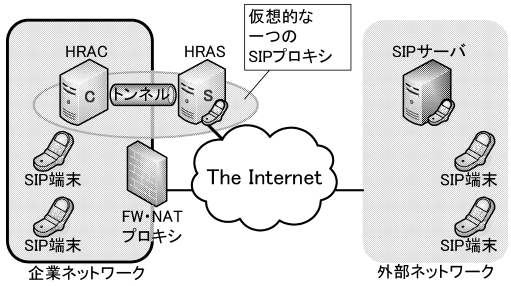

図 3 SoFW の構成
Fig. 3 Structure of SoFW.

ジから得た情報から音声ストリームのグローバル IP アドレスとプライベート IP アドレスおよびそれらのポート番号を変換して中継する．SoFW では，端末とは独立して HTTP トンネルを設置するため，既存の SIP 端末をそのまま利用することができる．これは企業がすでに SIP ネットワークを構築していた場合，特に有効である．さらに IP アドレスの管理形態をまったく変える必要がなく，SIP に限定した安全な通話ができる．

SIP 対応の音声端末では，呼設定後の音声通信を SIP サーバを介さずにエンドツーエンドで実行する．そのため，FW を越えるためには，音声ストリームをエンド端末宛てでなく，HRAS/HRAC に向けて誘導する必要がある．SoFW ではこれを実現するために，呼設定時に SIP のメッセージボディ（SDP）を HRAS/HRAC が書き換え，エンド端末に対して通信相手が HRAS/HRAC であるかのように見せかける．このようにしてエンド端末は音声データを HRAS/HRAC に送信することになり，音声ストリームが FW を越えられるようになる．以下の記述においては，3.2 節は FW を越える多くのシステムが採用しているトンネル生成に係わる方式の説明であり，3.3 節，3.4 節はこれを前提に音声ストリームを HRAS/HRAC に導く SoFW 独自の技術の説明である．

3.2 システム開始から通話までの流れ

外部端末から呼設定を開始し，内部端末が通話を終了する場合を例にとって，システム起動時から通話終了までのシーケンスを**図 4** に示す．

システムを起動すると HRAS と HRAC は 2 点間でトンネル生成を行う．HRAC は HRAS に対して HTTP（RFC2616）に準拠する GET リクエストと POST リクエストメッセージを送信する．HRAS は GET リクエストを受け取ると 200 OK レスポンスのヘッダ部を返す．この後，HRAS と HRAC は端末から SIP メッセージが送信されるまで TCP コネクション

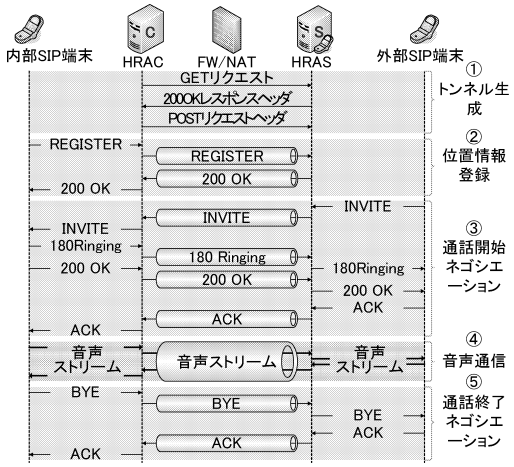

図 4 HTTP トンネル生成から通話終了までのシーケンス
Fig. 4 Sequence from generation of an HTTP tunnel to termination of a call.

ンを維持したまま待機する．以降，SIP メッセージまたは音声ストリームを受信すると HTTP のボディ部としてこれらを中継することができる．内部の SIP 端末は自身の情報を HRAS の SIP サーバに登録するため REGISTER リクエストを HRAC に送信する．HRAC は HTTP トンネルを介してリクエストを HRAS に中継し，HRAS から返信される 200 OK レスポンスを内部 SIP 端末に返す．上記処理により外部 SIP 端末からの通話開始ネゴシエーションが可能となる．外部 SIP 端末は INVITE リクエストを HRAS の SIP サーバ宛に送信する．HRAS の SIP サーバは内部 SIP 端末を特定し HTTP トンネルを介して端末に INVITE リクエストを転送する．INVITE メッセージを受けた内部 SIP 端末は呼び出し中を意味する 180 Ringing レスポンスを返し，フックオフすると 200 OK レスポンスを返す．呼び出し側はこれを受けて，応答確認の ACK メッセージを返す．通常の SIP ネゴシエーションは初めのリクエストが端末に届いた後は端末間で直接 SIP メッセージを交換しようとする．ネゴシエーションが終わると音声通信が開始される．音声ストリームは以下に述べる方法により，外部端末は HRAS へ，内部端末は HRAC へ送信し続ける．HTTP トンネルはその音声ストリームを対応する端末へ中継する．最後に通話終了ネゴシエーションはフックオンを告げる BYE メッセージと確認応答 ACK が HTTP トンネルによって中継され，通話が終了する．

3.3 SDP の修正による音声ストリーム誘導

SoFW では音声ストリームも HRAS/HRAC 間の HTTP トンネルを中継させなければならない．しか

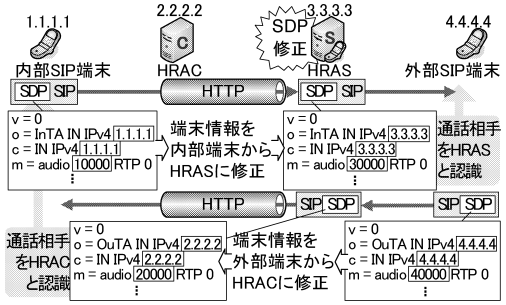

図 5 SDP の修正
Fig. 5 Modification of SDP.

し，通常の SIP 端末の仕様では音声ストリームはエンド端末どうしで直接交換される．SoFW では通常の SIP 端末から送信される音声ストリームを HTTP トンネルに誘導するために，SIP メッセージの INVITE リクエストとその 200 OK レスポンスが HRAS に到達すると，メッセージボディ部の SDP [15] で記述されるタイプ値の修正を行う．この処理により，内部端末は HRAC を，外部端末は HRAS を通信相手と見なすこととなり，端末の機能を変更することなく音声ストリームを HRAS/HRAC に誘導することが可能となる．

SDP 修正の手順を**図 5** に示す．SDP にはそのセッションの音声通信に必要とされる送信側ユーザエージェントの様々な情報がタイプ値として記述される．タイプ値にはメッセージ送信側の端末が音声通信に使用する IP アドレス・ポート番号やコーデック方式などがあり，端末は SDP を SIP メッセージのボディに記述することにより，音声通信に先立ち互いの音声通信情報を交換する．HRAS は，内部ネットワーク端末から送信された SDP の IP アドレス・ポート番号の値を HRAS の IP アドレス・ポート番号に，また外部ネットワーク端末から送信された SDP の IP アドレス・ポート番号の値を HRAC の IP アドレス・ポート番号に書き換える．修正された SDP を受け取った内部端末は音声ストリームの宛先を HRAC，外部端末は HRAS と認識して音声通信を開始する．

3.4 RAT による音声ストリーム経路決定

前節で記述したように，端末は音声ストリームの宛先 IP アドレス・ポート番号を HRAC もしくは HRAS に指定するよう誘導されるため，実際に通信相手となる端末の IP アドレス・ポート番号の情報を持っていない．HRAS/HRAC では宛先端末の IP アドレス情報を持たない音声ストリームに対して適切な通信相手へ送信する経路決定を行う方法が必要になる．

SoFW では呼設定時に両方向の SIP メッセージの

表 1 RAT の内容
Table 1 Structure of RAT.

内容	説明
To	受信者情報（ダイアログ ID）
From	送信者情報（ダイアログ ID）
Call-ID	セッション識別子（ダイアログ ID）
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

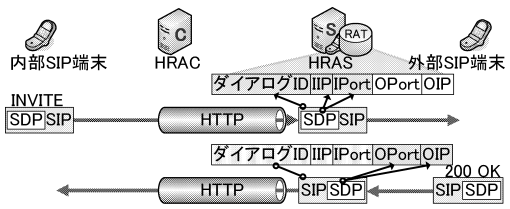

図 6 RAT の生成
Fig. 6 Generation of RAT.

SIP ヘッダと SDP の情報から SoFW 特有の RAT（Relay Agent Table）と呼ぶテーブルを HRAS で生成し，音声通信時にはこのテーブルを参照して音声ストリームの経路決定を行う．RAT は音声通信を行う両端末を対応させた情報を保持する．RAT の内容を**表 1** に示す．To，From，Call-ID は SIP メッセージのヘッダ情報であり，この 3 つを合わせて通信を識別するダイアログ ID となる．IIP・IPort は SDP から得られる内部端末の IP アドレス・ポート番号，OIP・OPort は外部端末の IP アドレス・ポート番号の値が書き込まれる．

図 6 に内部ネットワーク端末から呼設定を開始する場合の RAT 生成の流れを示す．SDP は SIP の発呼側の開始メッセージである INVITE リクエストと受信側の応答である 200 OK レスポンスのボディ部に記述される．HRAS は INVITE リクエストを受信すると，メッセージのヘッダ部からダイアログ ID を RAT レコードに書き込み，SDP からは IP アドレス・ポート番号を IIP・IPort フィールドに書き込む．次に 200 OK レスポンスを受信するとメッセージのダイアログ ID が一致する RAT レコードを検索し，SDP に記述されている IP アドレス・ポート番号を OIP・OPort として追記する．このようにして RAT には内部端末と外部端末の IP アドレス・ポート番号を対応させた情報ができる．

呼設定が完了し，音声通信が開始されると HRAS の RAT と RA（Relay Agent）ヘッダと呼ぶ独自のヘッダを利用して音声ストリームの経路決定を行う．

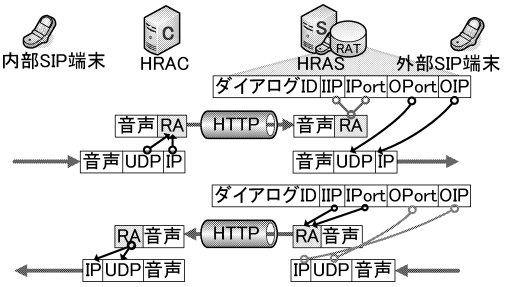

図 7 音声ストリーム処理の流れ
Fig. 7 Processing flow of voice streams.

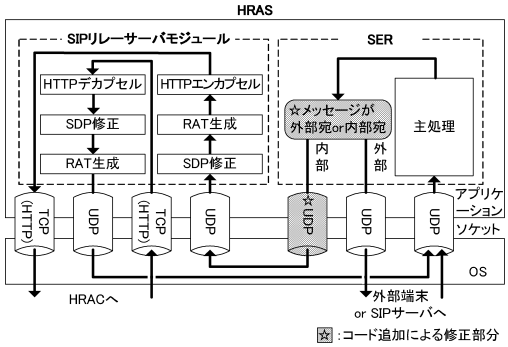

図 8 HRAS のモジュール構成と主要な処理
Fig. 8 Connections between SER and a SIP relay server module.

RA ヘッダは HRAS・HRAC 間のアプリケーションレベルの中継によって失われる IP レベル情報を保持するためのヘッダである．

音声ストリームの処理の流れを**図 7** に示す．音声ストリームが内部端末から外部端末へ向けられている場合，HRAC はこれを受信すると送信元 IP アドレスとポート番号を RA ヘッダとして音声データに付加し，HRAS へ送信する．HRAS では受け取った RA ヘッダの IP アドレス・ポート番号から RAT で対応する外部端末の IP アドレス・ポート番号を検索し，これを宛先に指定し，音声ストリームを中継する．外部から内部へ向けられた音声ストリームの場合，HRAS がこれを受信すると送信元 IP アドレスとポート番号から RAT によって対応する内部端末の IP アドレス・ポート番号を検索し，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 ヘッダに含まれる IP アドレス・ポート番号を宛先に指定して音声ストリームを中継する．

最後に，通話を切断する際には RAT からセッションの情報を削除する．HRAS が SIP の切断要求である BYE メッセージを受信すると，そのダイアログ ID から該当する RAT のレコードを検索して該当レコードの内容を削除する．

4. 実 装 方 式

3 章で述べた実現方式を HRAS/HRAC として，それぞれ 1 台の FedoraCore3.0（linux2.6.9）上のアプリケーションとして実装した．HRAS の SIP サーバ機能の部分はフリーソフトの SIP サーバである SER（SIP Express Router）[16] と連携することによって実現した．

HRAS のモジュール構成と主要な処理を**図 8** に示す．HRAS の SER 以外の SIP メッセージ処理に関する処理を SIP リレーサーバモジュールと呼ぶ．SER には SIP メッセージを SIP リレーサーバモジュールとやりとりするために少量のコード修正を加えた．SER で SIP メッセージがソケットに出力される前に，外部ネットワーク端末宛のものか内部ネットワーク端末宛のものかを判別し，外部宛であれば通常どおり外部へ送信し，内部宛であれば SIP リレーサーバモジュールの生成したソケットに送信するように修正した．このように，HRAS では SER と SIP リレーモジュールが連携して動作する．

また，SoFW では複数の SIP メッセージおよび音声パケットを同時に扱うため，並行処理を行う必要がある．Linux で並行処理を行うにはマルチプロセス方式とマルチスレッド方式がある．マルチプロセスでは処理単位ごとにメモリ空間が用意されるためプロセス間の独立性が高いという利点があるが，RAT をプロセス間で共有するにはプロセス間通信処理が必要になり効率が悪くなる．そのため，各処理単位が RAT を共有できるマルチスレッド方式を採用した．

5. 評 価

5.1 IP 電話の規格と評価システムの構成

総務省発行の IP ネットワーク技術に関する研究会報告書[17] によると，エンドツーエンド遅延についてはクラス A（固定電話並）が 100 ms，クラス B（携帯電話並）が 150 ms，クラス C（許容範囲）が 400 ms として分類されている．遅延についての数値は 95%の確率で満足させる必要があり，呼損率はすべてのクラスにおいて 0.15 以下とされている．また，ITU-T 勧告[18] によると IP パケット損失率はすべてのクラスにおいて 1×10^{-3} が目標値とされている．上記規格を参考に，本提案システムの評価においては，クラス C の実現を目指し，HRAS/HRAC と FW 部分の合計遅延が 95%以上の確率で 70 ms 以下（400 ms の 5 分の 1 以下）であること，IP パケットの損失が 0.1%以

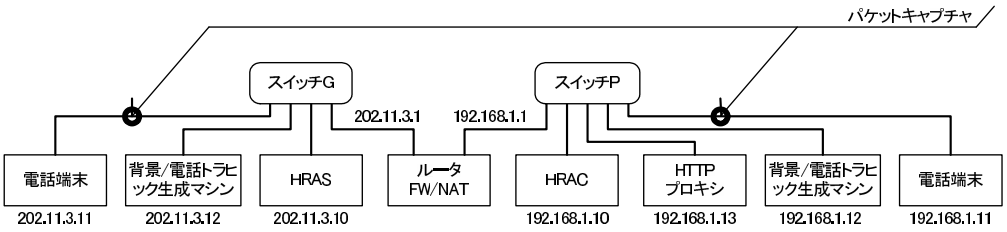

図 9 評価システムの構成
Fig. 9 Configuration of the evaluation system.

下であること，SIP による呼損失が 0.15 以下であることをもって実用に耐えうる性能であると判断する．

評価システムの構成を**図 9** に，SoFW を構成する各装置の性能を**表 2** に示す．100BASE-TX 対応のスイッチ G，スイッチ P をそれぞれ外部ネットワーク側用とプライベートネットワーク側用に位置づけ，スイッチ G に外部用端末，HRAS，背景/音声トラヒック生成マシン，ルータのグローバルインタフェース側を接続し，スイッチ P に内部用端末，HRAC，HTTP プロキシ，背景/音声トラヒック生成マシン，ルータのプライベートインタフェース側を接続した．スイッチ G に接続するインタフェースにはグローバルアドレスを，スイッチ P に接続するインタフェースにはプライベートアドレスを割り当てた．ルータには FW と NAT の機能を実装した．また，背景/音声トラヒック生成マシンは実験ごとに用途を変え，背景トラヒックや音声トラヒックを生成する．背景トラヒックの生成にはトラヒックジェネレータ D-ITG [19] を用いた．FW には内側から外側への HTTP 以外の通信を遮断するルールと TCP レベルのステートフル・インスペクションを設定した．また，SIP 端末は X-Lite，音声コーデックは G.711 を使用した．

5.2 実験結果と考察

(1) パケット処理遅延の測定

SoFW の純粋な処理速度を評価するため，SoFW を構成する各装置の処理時間が音声パケットに与える遅延を測定する実験を行った．SoFW を利用する環境では必ず FW，NAT および HTTP プロキシを通過させるため，HRAS，HRAC に加え，FW，NAT および HTTP プロキシが音声パケットに対して行う処理時間の合計を測定した．

外部用端末からの呼設定により音声通信を開始した後，モニタマシンによって送信直後の音声パケット，受信直前の音声パケットをキャプチャし，Outbound（内部端末から外部端末へ）と Inbound（外部端末から内部端末へ）の音声ストリームの平均遅延と分布を計算した．サンプルとなる音声パケットは計 100,000 パケットの平均とした．

表 2 評価システムの性能
Table 2 Specifications of the evalutation system.

装置	仕様	
HRAS /HRAC	CPU	Intel PentiumIV 2.8 GHz
	メモリ	512 MB
	NIC	Broadcom Tigon3 100BASE-TX
FW/NAT /Proxy	CPU	Intel PentiumIII 600 MHz
	メモリ	256 MB
	NIC	Global: Silicon Integrated System crop 100BASE-TX
		Privete: ADMtek FNW-9803-T 10/100BASE-TX
外部用端末	CPU	Intel PentiumIV 3.4 GHz
	メモリ	1 GB
	NIC	Broadcom NetXtreme57xx 100BASE-TX
内部用端末	CPU	Intel PentiumM 1.80 GHz
	メモリ	512 MB
	NIC	Realtek RTL8139/810x 100BASE-TX

遅延時間の測定値を**表 3** に，遅延時間の分布を**表 4** に示す．実験結果では Outbound および Inbound ともに平均 1 ms 以下であり通話に影響を与えない範囲であるといえる．最大値は約 50，70 ms であるが，表 4 から分かるように，1.9 ms 以上の遅延を持つパケットが全体に占める割合は 0.01%程度である．このことより SoFW 構成装置の音声パケットに対する処理時間は音声通話に影響しない範囲であるといえる．また，Outbound と Inbound で遅延時間が異なるのは，パケットの処理工程数の多い HRAS において，RA ヘッダに対する処理が生成と参照で異なるためである．

(2) 同時通話に対する性能評価

HRAS/HRAC が対応できるセッション数を測定する実験を行った．複数台の端末装置を接続するのは現実的に困難であるため，あらかじめ HRAS では手動で RAT を生成し，外部と内部に位置する両音声パケット生成マシンから擬似的に複数台分の音声パケットを HRAS および HRAC に送信し，実際に通常の IP 電話端末で SoFW を利用するのと同様の負荷を与えた．

表 3 遅延時間の測定値
Table 3 Measurement results of delay.

	Outbound	Inbound
average	0.95 ms	0.97 ms
max	52.0	73.8

表 4 遅延の分布
Table 4 Distribution of delay.

遅延	～ 0.7 ms	0.7～ 1.3 ms	1.3～ 1.9 ms	1.9 ms ～
Outbound	0.4%	98.3%	1.3%	0.01 %
Inbound	1.1	98.0	0.8	0.01

音声パケット発生装置は G.711 の音声通信を擬似的に生成する．1 台分の出力音声トラヒックは UDP で 172 Byte のデータを 20 ms 間隔で送信する．これをランダム間隔で複数台分立ち上げ，1 対の音声通信に加えられる遅延時間とパケットロス率を測定した．

図 10 にセッション数に対する遅延時間の増加，**図 11** にセッション数に対するパケットロスの増加を示す．それぞれ縦軸が遅延時間およびパケットロス率，横軸が端末数を表している．Outbound が Inbound よりも遅延時間，パケットロス率の両方において多数の端末数に耐えられているのは，(1) で述べたように RA ヘッダ処理負荷の違いがより顕著に現れたためであると考えられる．また，遅延時間が一定の値で収束するのは，遅延時間が所定の値以上になるとバッファ量の制限から処理待ちのパケットが溢れて廃棄され，一定以上の処理待ち時間は起こらないためと考えられる．30 セッション程度であればパケットロスは発生せず，平均遅延時間も 20 ms 以下を示している．また，**表 5** の 30 セッション時の遅延の分布から，30 セッションの通話が行われているとき，Outbound，Inbound がともに 95%以上の確率で 70 ms 以下の遅延を維持していることが分かる．この結果から通常使用される PC を用いて構成した HRAS および HRAC は少なくとも 30 セッション程度の負荷まで絶えうることが分かった．

(3) 呼設定と音声通信が互いに及ぼす影響

呼設定と音声通信の負荷が混在するときの本システムの有用性を確認するために，呼処理と音声ストリーム処理を同時に実行させ，相互に及ぼす影響を調査した．呼処理の評価にあたっては，呼の接続と切断を，平均間隔 t の指数分布に従って連続的に発生させるプログラムを作成した．

SoFW は同時 30 セッションの音声負荷に耐えられるので，ユーザの通話時間を平均 1 分と仮定すると，音声とバランスをとるには，平均毎分 30 以上の呼処理に対応できる必要があると考えられる．以下の評価では，呼の平均間隔 t を 300 ms と設定した．これは，同時に受付可能な呼数に換算すると，平均毎分 198 呼に相当するため評価としては十分な余裕を見ているといえる．

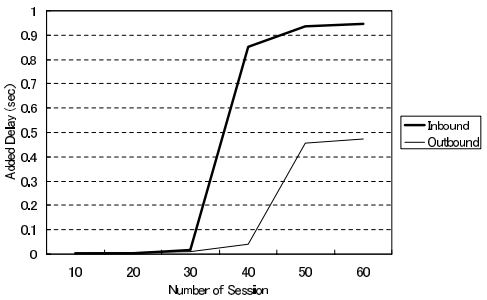

図 10 セッション数に対する SoFW による追加遅延
Fig. 10 Additional delay for the number of sessions.

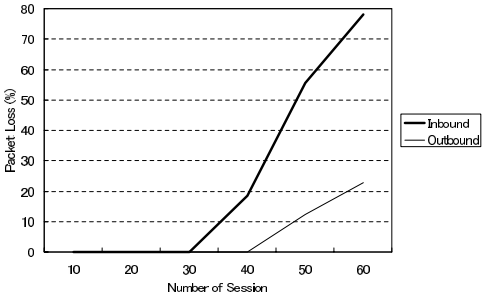

図 11 セッション数に対する SoFW によるパケットロス
Fig. 11 Packet loss for the number of sessions.

表 5 30 セッション時の遅延の分布
Table 5 Distribution of delay in case of 30 session.

遅延 (ms)	～ 10	10～ 30	30～ 50	50～ 70	70 ～
Outbound(%)	74.0	13.7	6.8	1.6	3.8
Inbound(%)	48.8	26.7	17.7	4.3	2.5

システム構成としては，SIP 端末間に SIP サーバのみが存在する場合（Normal 構成）と，SIP 端末間に FW および HRAS/HRAC が存在する場合（SoFW 構成）を想定した．なお，SoFW 構成においては，HRAS が SIP サーバの機能を包含している．

SIP で使用される各パケットが，Normal 構成において SIP サーバを通過する時間，SoFW 構成において FW と HRAS/HRAC を通過する時間をそれぞれ計測した．ただし，Register においては SIP 端末が SIP サーバへ Register メッセージを送信し，200 OK メッセージが返ってくるまでの時間とした．SoFW 構成においては，さらに呼処理の情報だけを流した場合と，30 セッションの音声を同時に流した場合を計測した．この結果を**表 6** に示す．表中の値は 100 回の平均値

表 7 呼設定が音声パケットに与える影響
Table 7 Effects on voice packets with a call process.

遅延		～10 ms	10～30 ms	30～50 ms	50～70 ms	70 ms	平均
音声	Inbound	52.3%	43.9%	3.68%	0.05%	0.06%	11.4 ms
	Outbound	66.3	16.7	9.1	7.8	0.03	12.5
音声+呼処理	Inbound	44.8	49.3	5.9	0	0	12.3
	Outbound	60.4	20.8	10.1	8.7	0.03	13.8

表 6 SIP メッセージの処理時間
Table 6 Processing time of SIP messages.

	メッセージの種類	Normal 構成	SoFW	SoFW+30 セッション
接続処理	INVITE	0.42 ms	2.7 ms	5.6 ms
	Ringing	0.24	3.1	3.8
	200 OK	0.32	2.6	4.8
	ACK	0.25	1.6	2.5
	合計	1.23	10	16.7
切断処理	BYE	0.25	1.7	5.2
	200 OK	0.18	1.5	2.1
	合計	0.43	3.2	7.3
登録処理	Register	0.32	3.6	6.3

である．

Normal 構成と SoFW 構成が呼接続時間および呼切断時間に与える遅延は，それぞれ INVITE から ACK までのメッセージの処理時間の合計，BYE から 200 OK（BYE）までのメッセージの処理時間の合計となる．また，端末情報の登録時間に与える遅延は Register の処理時間となる．表 6 に示すように，SoFW 構成においては Normal 構成に比べ HRAS/HRAC の分だけ接続処理時間と切断処理時間および登録処理時間は増大するものの，音声セッションの処理を同時に実行させた場合においても，ユーザ心理には影響を与えない十分小さな値であるといえる．ここで，SoFW 構成で呼と音声 30 セッションを同時に流した場合において，1,000 回の呼処理を連続実行させたが，呼損はまったく発生しなかった．これから SoFW が呼損率を劣化させる要因とはならないことを確認した．以上の結果より，音声データが呼処理に与える影響は十分小さいと判断できる．

次に，呼処理によって音声パケットがどのように影響を受けるかを評価するため，音声 10,000 パケットの遅延時間の変化を測定した．**表 7** にその結果を示す．本実験では，音声のセッション数が 25 の時点での測定を行った．表 7 から分かるように，呼処理を加えることによって Outbound，Inbound とも平均遅延時間と分布の偏りが若干増加するが，いずれの場合においても遅延時間が 95%以上の確率で 70 ms 以下を維持している．以上の結果より，呼設定が音声パケットに与える影響も十分小さいと判断できる．

(4) TCP 再送制御による影響の評価

本システムでは UDP 通信を行う 2 台の音声端末の間に，TCP 通信の経路が挟まれるという構造になっている．このような構造では，TCP 経路上でパケットロスが起こった場合に実行される TCP の再送制御によって通話に影響を及ぼすことが懸念される．そこで，HRAS と HRAC 間の TCP の経路が通過するルータに背景負荷となるトラヒックを与えて，故意にパケットロスを発生させ，音声パケットの遅延時間に与える影響を評価する実験を行った．トラヒックジェネレータによりプライベートアドレス側からグローバルアドレス側へ背景トラヒックを発生させ，ルータ部でパケットロスを発生させる．背景トラヒックのデータサイズは 200 Byte，送信間隔はランダムとし，単位時間（1 秒）あたりの送信パケット数を調節することによりトラヒック量を変更しながら測定を行った．音声通信を開始した後，モニタマシンによって送信直後のパケット，受信直前のパケットをキャプチャすることにより Outbound と Inbound の音声ストリームの平均遅延時間（50,000 パケットの平均）を算出した．また，通常の音声通信と比較するために SoFW を利用せず，ルータの FW と NAT 機能をオフにして通信する実験も同様の方法で測定した．

図 12 に Outbound における背景負荷と遅延時間の関係を，**図 13** に Inbound における背景負荷と遅延時間の関係を，**図 14** に Outbound における背景負荷とパケットロス率の関係を，**図 15** に Inbound における背景負荷とパケットロス率の関係を示す．また **表 8** に Outbound における遅延時間の分布を，**表 9** に Inbound における遅延時間の分布を示す．SoFW を利用せず，ルータの FW と NAT 機能をオフにして直接通信した実験を Normal モード，SoFW を利用した実験を SoFW モードとして比較した．図 12，図 13 の縦軸は音声パケットに加えられた遅延時間を示し，図 14，図 15 の縦軸はパケットロス率を示す．横軸はいずれも背景トラヒック量で 1 秒間の平均パケット送信回数である．図 12，図 13 から SoFW モードでは平均パケット送信回数 23,000 パケット/秒の背景トラヒック量を与えるまでは十分小さい平均遅延時間を示

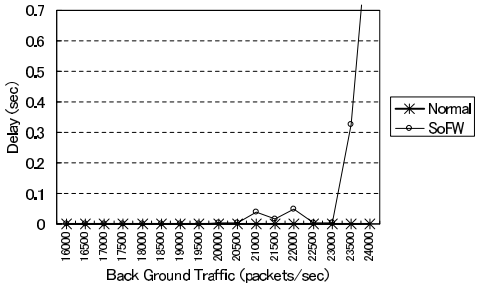

図 12 Outbound トラヒックにおける遅延時間の比較
Fig. 12 Comparison of delays in case of Outbound traffic.

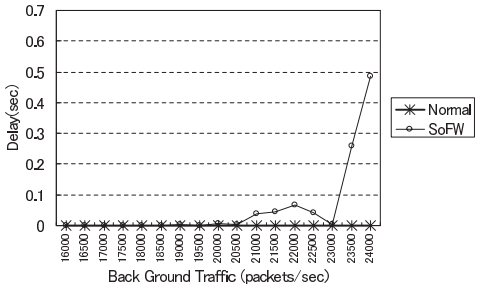

図 13 Inbound トラヒックにおける遅延時間の比較
Fig. 13 Comparison of delay in case of Inbound traffic.

すが，それ以降は急激に遅延時間が増加することが分かる．また，表 8，表 9 からも分かるように背景負荷が 23,000 パケット/秒までは 95%以上の確率で 70 ms 以下の遅延に収まっている．それに対し Normal モードでは背景トラヒックに対して遅延時間の影響はさほど大きくならないことが分かる．次に，図 14，図 15 から SoFW モードではパケット送信回数 23,000 パケット/秒の背景トラヒックまでは実用的なパケットロス率の範囲に収まっているが，それ以降は急激にロス率が増加することが分かる．それに対し Normal モードでは 23,000 パケット/秒の時点ですでにパケットロス率が 0.1%を超えている．すなわち，Normal モードでは背景トラヒックの影響は遅延にはさほど現れないかわりにパケットロスに現れる．それに対し SoFW モードでは再送制御がパケットロスを補う代わりに，遅延時間に影響が現れることが分かる．また，23,000 パケット/秒以降で SoFW モードの遅延時間が急増しているのは再送制御によりデータ送信が遅れ，TCP の送信待ち行列がオーバフローして，データが破棄されてしまうためである．このように，SoFW を利用した音声通信では所定の負荷までは十分実用に耐えうる性能を示すが，それを超えると急激に遅延時間が増加して使用できない状態になる．これに対し，UDP を利用した一般の音声通信では，上記と同様の負荷が与えられた段階で，すでにパケットロスが許容範囲を超えた状態になっている．以上の結果より，SoFW はそれを用いない場合に比べ，同等かそれ以上の背景負荷に耐えられるということができる．

ただし，負荷が大きくなっていくと，Normal モード

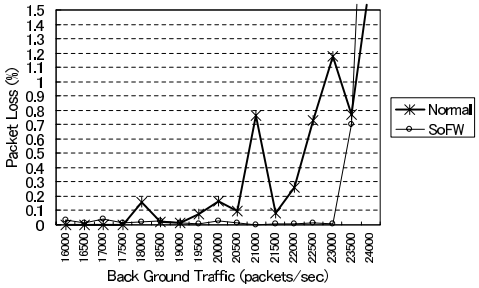

図 14 Outbound トラヒックにおけるパケットロス率の比較
Fig. 14 Comparison of packet loss rate in case of Outbound traffic.

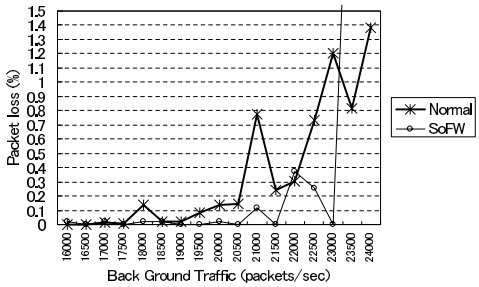

図 15 Inbound トラヒックにおけるパケットロス率の比較
Fig. 15 Comparison of packet loss rate in case of Inbound traffic.

表 8 Outbound トラヒックにおける遅延時間の分布
Table 8 Distribution of delay in case of Outbound.

背景負荷＼遅延	～ 10 ms	10～ 30	30～ 50	50～ 70	70 ～
19,000 (pkt/s)	99.7%	0.2	0.0	0.1	0.1
21,000	97.4	0.3	0.2	0.1	1.9
22,000	96.0	0.4	0.2	0.3	3.2
23,000	99.2	0.2	0.2	0.1	0.4
23,500	94.8	0.5	0.4	0.5	3.7
24,000	92.3	0.4	0.3	0.4	6.6

表 9 Inbound トラヒックにおける遅延時間の分布
Table 9 Distribution of delay in case of Inbound.

背景負荷＼遅延	～ 10 ms	10～ 30	30～ 50	50～ 70	70 ～
19,000 (pkt/s)	99.0%	0.3	0.1	0.1	0.5
21,000	95.7	0.5	0.4	0.3	3.0
22,000	94.9	0.7	0.3	0.4	3.7
23,000	97.7	0.4	0.3	0.2	1.4
23,500	91.4	1.3	0.9	0.8	5.6
24,000	91.9	0.7	0.5	0.5	7.3

ではパケットロスが大きくなって徐々に許容範囲を超えるのに対し，SoFW では HRAS/HRAC 間で TCP の再送制御が働き，あるトラヒックを超えた時点で SoFW がまったく使えない状態になる．これはエンド音声端末に対して TCP の輻輳制御が伝わらないためである．これを防止するには，FW において IP 電話を優先する QoS 制御を行い，かつ IP 電話のセッション数に制限を設けるなどの対策が必要と考えられる．

6. おわりに

ファイアウォールの外部と内部にそれぞれ 1 台のリレーエージェントを設置し，その間に HTTP トンネルを作ることによってファイアウォールを越えられる IP 電話システム SoFW の実現方法を提案した．SoFW は既存の方式に対して，既存ファイアウォールの取替え，セキュリティポリシの変更が不要なため導入が容易であることや，既存の SIP 端末がそのまま利用できること，アドレス空間の統一的管理の必要がないという利点を持っている．

評価実験では背景トラヒックや同時通信による負荷をかけ性能を測ることにより，SoFW が IP 電話システムとして実用に耐えうる性能を持つことを示した．

本論文では SIP で扱うデータを音声データに限定したが，SIP は様々な用途のメディア通信に対して，その将来性が注目されており，今後は SoFW の IP 電話以外への対応も検討していく．

参考文献

1) Freed, N.: Behavior of and Requirements for Internet Firewalls, RFC 2979 (2000).
2) Egevang, K. and Francis, P.: The IP Network Address Translator (NAT), RFC 1631 (1994).
3) 大田昌孝：本当のインターネットを目指して：インターネットと電話 (2)，情報処理学会誌，Vol.40, No.9, pp. 922–923 (1999).
4) ITU-T Recommendation H.323: Visual Telephone Systems and Equipment for Local Area Networks which Provide a Non-guaranteed Quality of Service (1996).
5) Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, RFC 3261 (2002).
6) Peterson, J.: Application-layer Policy Enforcement at SIP Firewalls, IETF Internet-Draft (2000).
7) Thernelius, F.: SIP Firewall Solution, IETF Internet-Draft (2000).
8) 大竹八洲考，但馬康宏，寺田松昭：SIP を用いた NAT 通過手法の提案とその実装，情報処理学会論文誌，Vol.45, No.3, pp.813–823 (2004).
9) 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, pp.553–560 (2003).
10) Skype. http://www.skype.com/home.html
11) 登大遊：SoftEther の内部構造，情報処理学会誌，Vol.45, No.10, pp.1057–1062 (2004).
12) Asgent Apostra. http://www.asgent.co.jp/Products/Apostra_Tunnel/tunnel.html
13) UDP Hole Punching. http://www.brynosaurus.com/pub/net/p2pnat/
14) NEC UNIVERGE IX seriese. http://www.sw.nec.co.jp/ix2k3k/index.html
15) Handley, M. and Jacobson, V.: SDP: Session Description Protocol, RFC 2327 (1998).
16) SER. http://www.iptel.org/ser/
17) 総務省：IP ネットワーク技術に関する研究会報告書 (2001).
18) ITU-T Recommendation Y.1541: Network Performance Objectives for IP-Based Services (2003).
19) D-ITG. http://www.grid.unina.it/software/ITG/

(平成 18 年 5 月 19 日受付)
(平成 18 年 11 月 2 日採録)

伊藤 将志（学生会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．現在，同大学院理工学研究科電気電子・情報・材料工学専攻博士後期過程に在学中．VoIP，無線ネットワーク等の研究に従事．

鹿間 敏弘（正会員）

1976 年東工大・総合理工学研究科・電子システム専攻修了．現在，三菱電機（株）情報技術総合研究所勤務．衛星利用コンピュータネットワーク，高速リング型 LAN，ATM，ネットワークセキュリティ，高速 PLC 等に関する研究開発に従事．電子情報通信学会，IEEE 各会員．情報学博士．

渡邊 晃（正会員）

1974 年慶應義塾大学工学部電気工科学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．