異なる企業間のファイアウォールを通過できる IP 電話の提案

若原宏太

通信基盤の発達により IP 電話の普及が進んでいる．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や NAT が存在するため, 両者の間で VoIP による通信ができない場合が多い．我々は，この問題を解決するため SoFW（SIP over FireWall）を提案してきた．しかし，これまでの SoFW は企業内とインターネット上の VoIP だけを想定していた．本稿では，SoFW を拡張し異なる企業をまたがる VoIP と，同一企業内の VoIP を安全に行える方式を検討した．

Proposal of IP Telephone system That Can Pass through Firewalls of Different Enterprises.

KOTA WAKAHARA

The spread of IP telephones is progressing by development of a communication base. However, since a firewall and NAT exist between a enterprise network and an external network, communication by VoIP cannot be performed among both in many cases. We have proposed SoFW(SIP over FireWall) in order to solve this problem. However, old SoFW assumed only VoIP the inside of a enterprise, and on the Internet. This paper examined the system which can perform safely VoIP which straddles a enterprise which extends SoFW and is different, and VoIP in the same enterprise.

1. はじめに

通信基盤の発達により，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，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（以下 FW）[1]や 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同士では VoIP（Voice over IP）による通信ができない．

VoIP のセッション開始プロトコルとして IETF（Internet Engineering Task Force）によって標準化された SIP（Session Initiation Protocol）[3]は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・サービスで利用できるとして注目されている．現在の IP 電話の多くが SIP を利用している[4][5]. 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 サーバにユーザの位置を登録し，この位置情報を元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課題がある．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，企業のセキュリテポリシ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/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として，我々は FW 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，全ての端末からの 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）を提案してきた[6]. SoFW は既存のネットワーク機器に影響を与えないので導入が容易であり，既存の SIP 端

末をそのまま利用できる．

しかし，これまでの SoFW では，異なる企業をまたがる端末同士の通信が考慮されていない．また，企業内にある端末の情報を FW の外部にある HRAS に登録しなくてはならず，企業内端末同士の通信時にも HRAS を経由した呼設定になるという課題がある．

そこで，本稿では SoFW を拡張し異なる企業をまたがる VoIP と，同一企業内の VoIP を安全に行える方式を提案する．

2. SoFW の概要

SoFW の構成を図 1 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．これは企業が既に 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全く変える必要がなく，SIP に限定した安全な通話ができる．

2.1 SDP の修正による音声ストリームの誘導

SoFW では SIP メッセージだけではなく，音声ストリームも HRAC/HRAS 間の HTTP トンネルを中継させなければならない．しかし，通常の SIP 端末の仕様では音声ストリームはエンド端末同士で直接交換される．SoFW では音声ストリームを 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 200OK レスポンスが HRAS に到達すると，SIP メッセージのボディ部の SDP[7]で記述されるタイプ値の修正を行う．

SDP 修正の手順を図 2 に示す．SDP にはそ

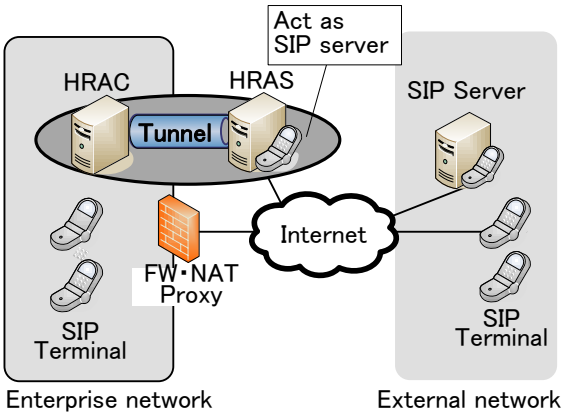

図 1 SoFW の構成

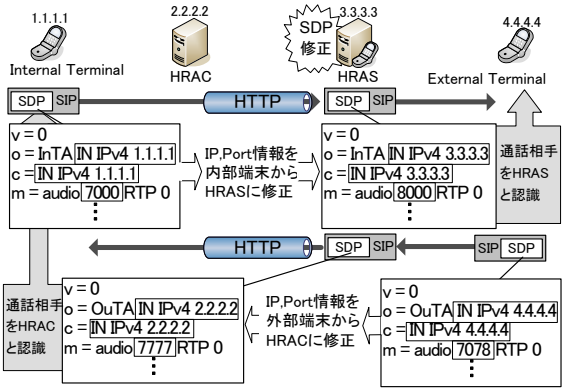

図 2 SDP 修正の手順

のセッションの音声通信に必要な様々な情報がタイプ値して記述される．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含めることで，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ことになり，音声ストリームは HTTP トンネルに誘導される．

2.2 RAT による音声ストリーム経路決定

呼設定時においては，SIP によりアプリケーションレベルでエンド端末の宛先情報を保持しており，HRAC/HRAS 間ではこれを利用して中継を行う．しかし，音声ストリームは宛先

IP アドレス情報を IP ヘッダのみに持つ．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．HRAC/HRAS 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 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，IP・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 3 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 と受信側の応答である 200OK メッセージのボディ部に記述される．HRAS は INVITE メッセージを受信すると，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 200OK 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．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 4 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．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 HRAS が受信すると，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．

表 1 RAT の内容

内容	説明
To	送信者情報（ダイアログ ID）
From	受信者情報（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
Port	外部ネットワーク端末のポート番号

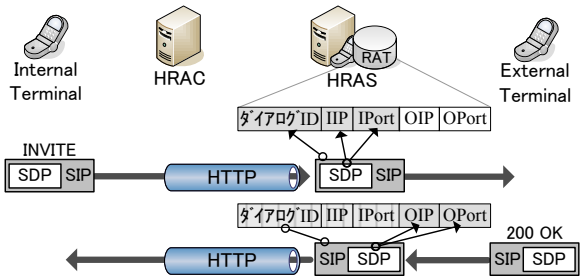

図 3 RAT 生成の流れ

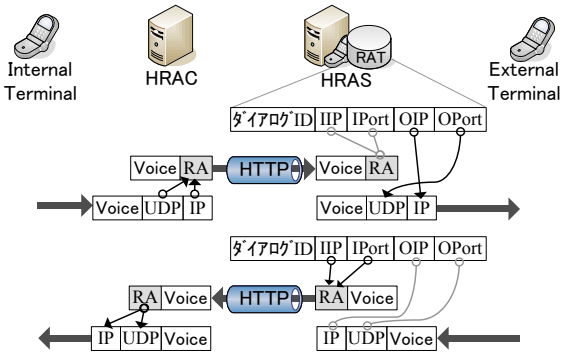

図 4 音声ストリーム処理の流れ

3. SoFW の拡張

3.1 同一企業内の VoIP

提案方式では，新たに HRAC にも SIP サーバ機能を組み込む．これにより企業内端末同士の通信は HRAC のみで行える．図 5 に内部ネットワーク端末から同一企業内の端末に呼設定を開始する場合の流れを示す．HRAC は内部端末 A から送信された INVITE メッセージを受信すると，メッセージのヘッダ部の宛先の URI が内部端末 B の場合，HRAC 内部の SIP サーバ機能へ中継する．HRAC の SIP サーバは，内部端末 B へメッセージを中継する．内部端末 B はこれを受信すると，200OK レスポンスを HRAC の SIP サーバに送信する．HRAC の SIP サーバは，内部端末 A へメッセージを中継する．内部端末 A がこれを受信すると呼設定が完了し，内部端末 A と内部端末 B は音声ストリームをエンド端末同士で直接交換する．

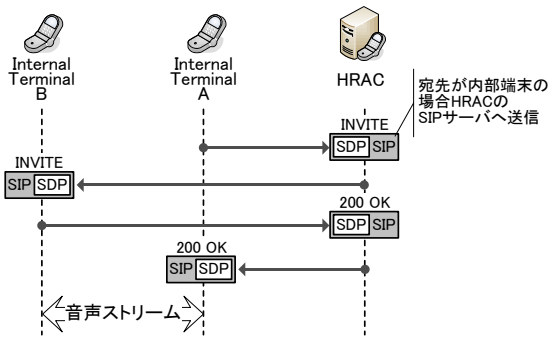

図 5 同一企業内の VoIP

3.2 企業内端末情報の隠蔽

既存の SoFW では，本来外部ネットワークに隠蔽されているはずである企業内の端末の情報を FW の外部にある HRAS に登録しなくてはならなかった．企業内の端末の情報を外部に隠蔽するため，HRAC は端末情報の登録メッセージである REGISTER を受信すると端末 IP アドレスを仮想 IP アドレスに書き換えて，HRAS には仮想 IP アドレスを登録する．このとき HRAC は端末の IP アドレスと，その IP アドレスから生成した仮想 IP アドレスを対応させる IPTT（IP address Translation Table）と呼ぶテーブルを生成する．図 6 に端末情報の登録動作と IPTT 生成の流れを示す．HRAC は，REGISTER メッセージを受信すると HRAC の SIP サーバに端末の IP ドレス登録する．また，メッセージのヘッダ部から端末の IP アドレス，仮想 IP アドレスを生成し IPTT レコードに書き込む．次に REGISTER メッセージのヘッダ部の端末の IP アドレスを仮想 IP アドレスに書き換え HRAS へ中継する．HRAS は REGISTER メッセージを受信すると HRAS の SIP サーバに仮想 IP ドレスを登録する．

以降，SIP メッセージの内部端末の IP アドレスを仮想 IP アドレスに書き換えることで，企業内端末情報を外部に隠蔽することが可能となる．

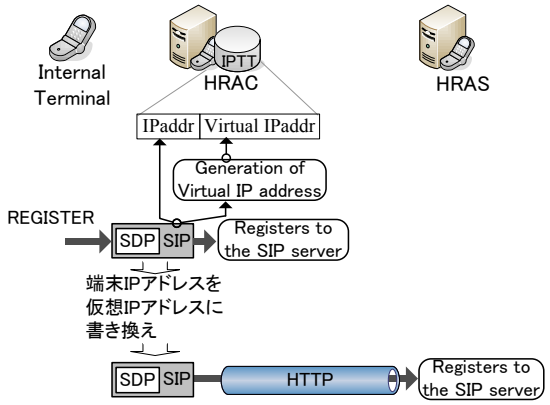

図 6 REGISTER，IPTT 生成の流れ

3.3 拡張 RAT による音声ストリーム経路決定

既存の SoFW では，異なる企業をまたがる端末同士の通信が考慮されていなかった．そのため，HRAS のポート番号が固定であり相手企業内の端末からの音声ストリームの経路決定ができなかった．HRAS の音声通信時に使うポート番号を相手端末ごとに動的に生成する．次に RAT を拡張し，従来の情報にこの音声通信用ポート番号（以下 SrcPort）を追加する．RAT を拡張し，異なる企業をまたがる呼設定の場合の RAT 生成の流れを図 7 に示す．図 7 は企業 A の端末から企業 B の端末に呼設定を開始する場合の例を示している．企業 A の HRAC_A は，内部端末 A からの INVITE メッセージを受信すると，メッセージのヘッダ部の内部端末 A の IP アドレスから IPTT で対応する仮想 IP アドレスを検索し，これを内部端末 A の IP アドレスと書き換え，企業 A の HRAS_A へ中継する．HRAS_A は外部宛ての INVITE メッセージを受信すると，メッセージのヘッダ部からダイアログ ID を RAT レコードに書き込む．SDP からは IP アドレス・ポー

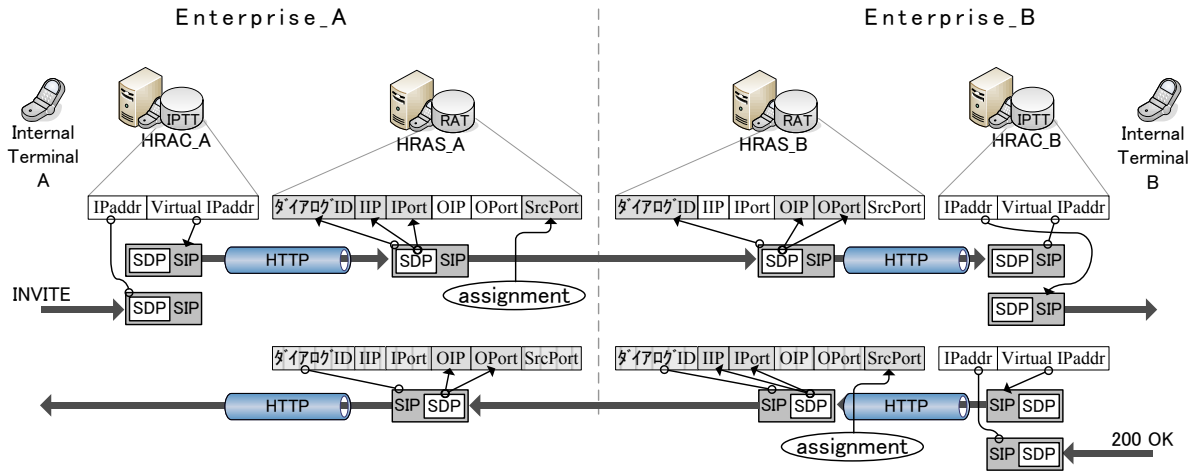

図 7 異なる企業をまたがる場合の拡張 RAT 生成の流れ

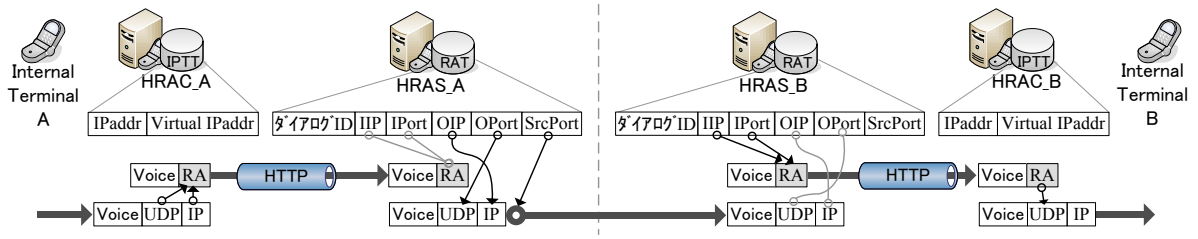

図 8 異なる企業をまたがる場合の音声ストリームの処理の流れ

ト番号，音声通信時に使うポート番号を生成し IIP・IPort・SrcPort フィールドに書き込み，企業 B の HRAS_B に中継する．この音声通信用ポート番号は相手端末ごとに動的に生成され，相手企業内の端末を識別可能にする．HRAS_B が内部宛ての INVITE メッセージを受け取ると，メッセージのヘッダ部からダイアログ ID，SDP からは IP アドレス・ポート番号を RAT の OIP・OPort フィールドに書き込み，HRAC_B に中継する．HRAC_B は，メッセージの宛先の仮想 IP アドレスが一致する IPTT レコードを検索し内部端末 B の IP アドレスに修正して，宛先内部端末 B まで INVITE メッセージを中継する．

次に内部端末 B の 200OK レスポンスを HRAC_B が受信すると，メッセージのヘッダ部の内部端末 B の IP アドレスから IPTT で対応する仮想 IP アドレスを検索し，これを内部端末 B の IP アドレスと書き換え，HRAS_B へ中継する．HRAS_B は外部宛ての 200OK 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，音声通信時に使うポート番号を生成し，IIP・IPort・SrcPort として追記し，HRAS_A へ中継する．HRAS_A が内部宛の 200OK 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 として追記し，HRAC_A へ中継する．HRAC_A は，メッセージをそのまま宛先内部端末 A まで中継する．

次に異なる企業をまたがる場合の音声ストリームの処理の流れを図 8 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，これまでの SoFW と同様に送信元 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・ポート番号と音声通信用ポート番号を検索し，外部端末情報を宛先にして指定のポートから音声データを中継する．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これまでの SoFW と同様に，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．

4. 実装

4.1 実装環境

既存の SoFW の HRAC と HRAS は，FedoraCore3.0 上のアプリケーションとして実装している．HRAS の SIP サーバ機能の部分はフリーソフトの SIP サーバ SER（SIP Express Router）[8]との連携によって実現している．

3 章で述べた方式を FedoraCore4.0 上のアプリケーションとして実装した．HRAC の SIP サーバ機能の部分は HRAS と同様に SER を使用した．

4.2 モジュール構成

HRAC/HRAS の機能とデータの流れを図 9 に示す．SER 以外の機能を総称して SIP リレーモジュールと呼ぶ．

4.2.1 SIP メッセージの処理

内部ネットワークから外部ネットワークへ向けられた SIP メッセージは HRAC の SIP リレーモジュールで SIP メソッド，レスポンスの判別を行う．

- 判別結果が REGISTER メッセージであった場合，メッセージを 2 つに複製し一方を HRAC の SER へ登録し，もう一方のメッセージの内部端末の IP アドレスから仮想 IP アドレスを生成[9]し，IPTT 生成機能，内部端末の IP アドレスを仮想 IP アドレスに書き換える SIP 修正機能，HTTP エンカプセル機能によって HRAS へ送信する．
- 判別結果がリクエストメッセージであった場合，メッセージのリクエスト URI が“HRAS”か“その他”かを判別する．HRAS であれば，HRAC の SER へ送信し，SER はメッセージを内部端末に送信する．その他であれば，HTTP エンカプセル機能によって HRAS へ送信する．
- 判別結果がレスポンスであった場合，HTTP エンカプセル機能によって HRAS へ送信する．

HRAS では SIP リレーモジュール，SER によって処理され外部へ中継する．

外部ネットワークから内部ネットワークへ向けられた SIP メッセージは HRAS の SER で処理した後，SIP リレーサーバモジュールで処理し HRAC へ送信する．HRAC では HTTP デカプセル機能，仮想 IP アドレスであれば元の内部端末の IP アドレスに修正する SIP 修正機能によって内部端末へ送信する．

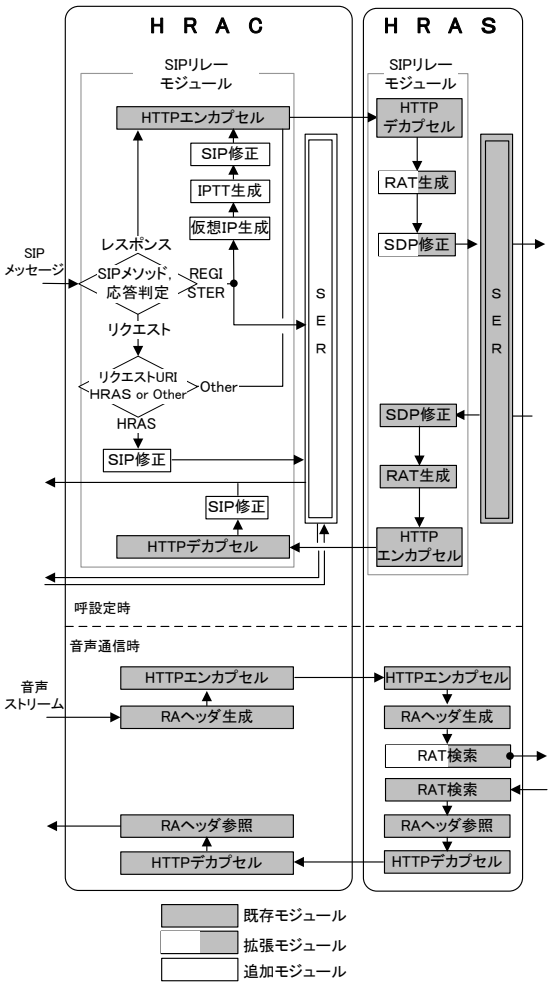

図 9 HRAC/HRAS の機能とデータの流れ

4.2.2 音声ストリームの処理

内部ネットワークから外部ネットワークへ向けられた音声ストリームは HRAC で RA ヘッダ生成，HTTP エンカプセル機能の順に処理し，HRAS へ送信する．HRAS では HTTP デカプセル，RA ヘッダ参照，RAT 検索機能の順に処理し指定のポートから外部ネットワークへ中継する．外部ネットワークから内部ネットワークへ向けられた音声ストリームは HRAS で RAT 検索，RA ヘッダ生成 HTTP エンカプセル機能の順に処理し，HRAC へ送信する．HRAC では HTTP デカプセル，RA ヘッダ機能の順に処理し，内部ネットワークへ中継する．

4.3 仮想 IP アドレスの生成

仮想 IP アドレスは内部端末の IP アドレスに

対応して割り当てられる．仮想 IP アドレスを“A.B.C.D”と表記した場合, 各バイトには以下に示す値が設定される．A には企業内ネットワークのネットワークアドレス上位 1 バイト目と異なる値を設定する．プロトタイプシステムでは，A には実験的目的のために予約されているクラス E にあたる 240 を設定した. B は初期値として 0 が設定される．C は内部端末の IP アドレスのハッシュ値，D は内部端末のユーザ名のハッシュ値が設定される．ハッシュ関数の出力値の範囲は 1～254 とした．このように仮想 IP アドレスを割り当てることにより，仮想 IP アドレス，外部ネットワークアドレス，企業内ネットワークアドレスであるかを識別することができ HRAC の SIP リレーモジュールで仮想 IP アドレスを内部端末 IP アドレスに修正する処理, HRAS の SER で SIP メッセージが外部ネットワーク端末宛のものか企業内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，企業内宛であれば HRAS の SIP リレーサーバモジュールに送信する処理を可能とする．ハッシュが衝突した場合は，B を異なる値に設定することにより，IPTT の端末の IP アドレスと仮想 IP アドレスは一意に対応する．

5. まとめ

異なる企業をまたがる端末同士の VoIP，および同一企業内の端末同士の VoIP を安全に行うために SoFW の拡張を提案した.

拡張 SoFW を実装し, その動作を確認した.

参考文献

[1] N.Freed,Behavior of and Requirements for Internet Firewalls,IETF RFC 2979 (2000).

[2] K. Egevang, P. Francis:The IP Network Address Translator (NAT),IETF RFC 1631(1994).

[3] J. Rosenberg,et all”SIP: Session Initiation Protocol”IETF RFC3261(2002)

[4] Petri Koskelainen,Henning Schulzrinne,Xiaotao Wu:VoIP:A SIP-based conference control framework,ACM press 53-61(2002).

[5] Stefan Berger,Henning Schulzrinne,Stylianos Sidiroglou,Xiaotao Wu:Conferencing:Ubiquitous computing using SIP,ACM press 82-89(2003).

[6] 伊藤将志，鹿間敏弘，渡邊晃：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，情報処理学会論文誌, Vol.48，No.2，pp.644-655，(2007).

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

[8] SER:“http://www.iptel.org/ser/”

[9] 鈴木秀和，宇佐見庄五，渡邊晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌, Vol.48, No.12, pp.3949-3961, (2007).