

ファイアウォールを通過できる IP 電話の実現方式と実装

伊藤 将志 渡邊 晃

名城大学大学院理工学研究科

A Realization method and its Implementation of Voice over IP System Passing Through FireWall

Masashi Ito Akira Watanabe

Graduate School of Science and Technology, Meijo University

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し、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り、企業や一般家庭に IP 電話が普及しつつある。

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 (FireWall; 以下 FW) [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同士では VoIP (Voice over IP) [3] による通信ができない[4]。企業・外部ネットワーク間において VoIP が安全に利用できるようになれば、IP 電話の普及がさらに促進され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、早期に 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ベースのプロトコルがあるが、現在は 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おり、様々なマルチメディア・サービスに利用できるとして注目されている。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[7][8]。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ダイヤルメッセージの中継を行う機能を提供する。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、NAT が介在するような環境ではダイヤルできない。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、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 /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既に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]などの IP 電話システムや、IP 電話に限らず、どのようなアプリケーションでも FW の通過を可能にする SoftEther[11]がある。

HCAP や Skype はプライベートアドレス側の端末とグローバル IP アドレス環境に置かれた中継サーバとの間で HTTP トンネルを張る。ダイヤルには CGI や独自のアプリケーションを利用し、音声ストリームは HTTP の GET メソッドに対するレスポンスと POST メッセージに埋め込んで中継する。このようにして外部の 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、端末に特殊な

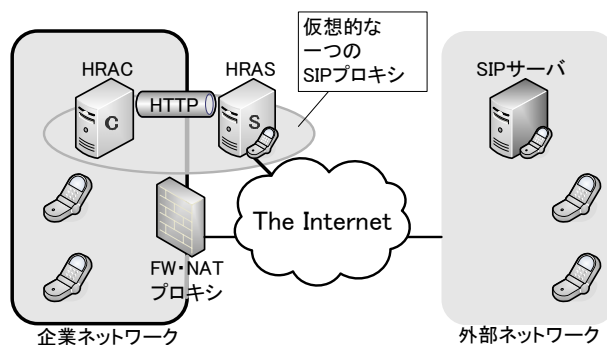


図 1. SoFW の構成

機能が必要であったり、FW 上には HTTP の常時接続による無駄なトラフィックが流れるという課題がある。また、SoftEther では、プライベートアドレス側の PC に仮想 LAN カードと呼ぶソフトウェアを搭載し、グローバルアドレス側に仮想 HUB と呼ぶソフトウェアを搭載した PC を準備する。接続の際に仮想 LAN カードには仮想的な IP アドレス・MAC アドレスが割り当てられる。仮想 LAN カードと仮想 HUB は HTTPS や SSH などの FW を通過できるプロトコルにイーサネットフレーム埋め込むことにより、両者の間で仮想イーサネットを構築する。この仮想イーサネットにより接続端末は FW を越えて自由に通信をできる。仮想イーサネット上で IP 電話を利用するには仮想イーサネットに繋がっている端末に IP 電話要素を導入する。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という課題があるうえ、仮想ネットワーク内のアドレスの統一的な管理の必要性が発生する。

そこで著者らは FW の内部と外部に 1 台ずつリレーエージェントを設置し、その間にダイヤル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[12]。SoFW は HRAC と HRAS の導入のみで FW 越えを実現するため、既存の SIP 端末の機能に依存しない。また、常時接続による FW 上のトラフィックが少ないという特徴を持つ。本稿では SoFW の実装方式の機能とプロセスの連携について詳しく検討したので報告する。

以下、2 章で提案システム SoFW の概要について述べる。3 章では実装方式を説明し、4 章でまとめとする。

2. SoFW の概要と実現方法

2.1. SoFW の概要

SoFW の構成を図 1 に示す。SoFW では通常の SIP ネットワークに対して、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 (Harf Relay Agent Client)、外部

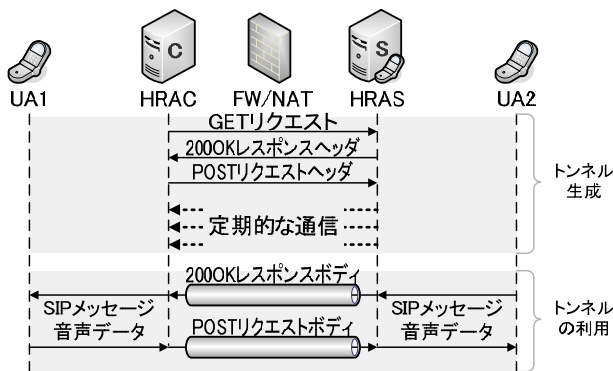


図2. HTTP トンネル生成から中継までのシーケンス

のグローバルアドレス環境上に HRAS (Half Relay Agent Server) を設置する。SIP 端末からのメッセージに先立ち、HRAC・HRAS 間で HTTP トンネルを張り、メッセージを中継させることにより 2 つの装置をグローバル/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一つの SIP サーバとして機能させる。音声ストリームに対しても同様に予め HTTP トンネルを張り中継する。これらのトンネルを利用して、端末間の SIP による登録からダイヤル、音声通信まで IP 電話の一連のやり取りを中継する。

2.2. HTTP トンネル

SoFW ではシステムの起動時に HRAC と HRAS の間で HTTP トンネルを生成する。トンネル生成からメッセージ中継までのシーケンスを図2に示す。HRAC は HRAS に GET リクエスト・POST リクエスト用に 2 つの TCP コネクションを確立し、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 200OK レスポンスのヘッダ部を返す。この処理が終わると、HRAC と HRAS は端末から SIP メッセージが送信されるまで待機し、メッセージを受信すると HRAC はそれをアプリケーションレベルで POST リクエストのボディ部に埋め込み HRAS へ、HRAS は 200OK レスポンスのボディ部に埋め込み HRAC へ送信する。複数ある端末からの SIP メッセージは全てこの 2 つの HTTP コネクションへ渡され中継される。ここで、HRAC と HRAS が端末からのメッセージ待ちで待機している間、メッセージのやり取りがないまま特定の時間が経過すると TCP のタイムアウト機能によりコネクションが切断されてしまう。そのため、待機中も一定時間ごとに Time Arrival と呼ぶメッセージのやり取りを行う。音声ストリームに対する HTTP トンネルも上記同様に生成し接続を維持する。

2.3. SDP の修正による音声ストリーム誘導

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る。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、ダイヤル時に SIP メッセージが HRAS に到達すると、SIP メッセージのボディ部に含まれる SDP[13]で記述されるタイプ値の修正を行う。SDP 修正の手順を図3に示す。SDP にはそ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として記述される。タイプ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

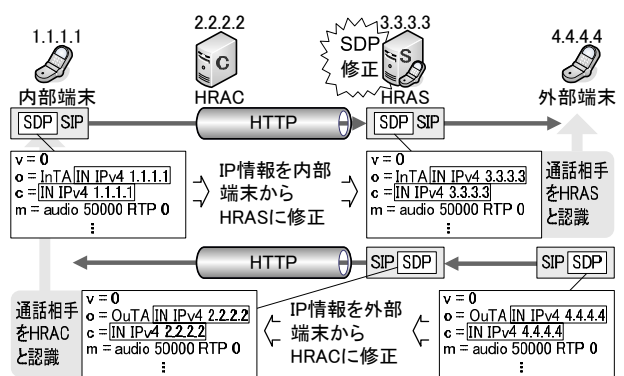


図3. SDP 修正の手順

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
OPort	外部ネットワーク端末のポート番号

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 における修正処理では、内部ネットワークの端末から送信された SDP の IP アドレスタイプの値を HRAC の IP アドレスに、また外部ネットワークの端末による SDP の IP アドレスタイプの値を HRAS の IP アドレスに書き換える。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。

2.4. RAT による音声ストリーム経路決定

ダイヤル時においては、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。2.2 章で記述したように、端末は音声ストリームの宛先 IP アドレスを HRAC もしくは HRAS に指定するよう誘導されるため、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 SIP メッセージの通信時に 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4に内部ネットワーク端末からダイヤルを開始する場合の 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

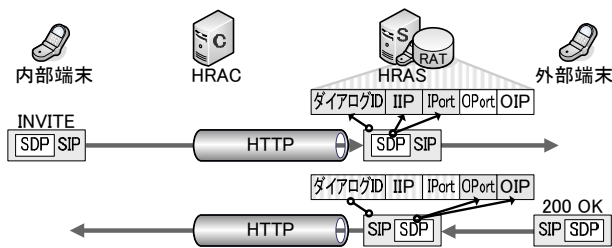


図4. RAT 生成の流れ

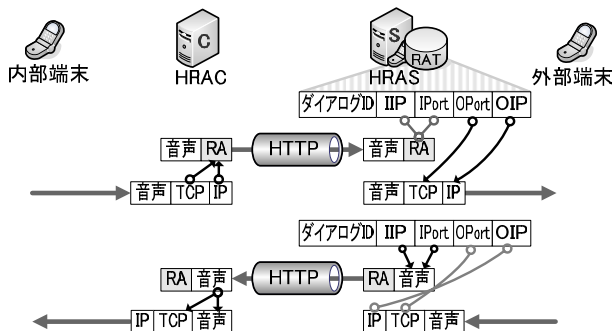


図5. 音声ストリーム処理の流れ

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IIP・IPortフィールドに書き込む。次に200OKを受信するとメッセージのダイアログIDからRATの同一通信の記録を検索し、SDPのIPアドレス・ポート番号をOIP・OPortとして追記する。

ダイヤルが完了し、音声通信が開始されるとHRASのRATとHRAC・HRAS間で生成するRA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。

音声ストリームの処理の流れを図5に示す。音声ストリームが内部から外部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の記録を検索して該当記録の内容を削除する。

3. 実装方式

HRACとHRASは、それぞれ一台のFedoraCore3.0 (linux2.6.9) 上のアプリケーションとして実装する。

HRASのSIPサーバ機能はフリーソフトのSIPサーバであるSER[14]との連携によって実現する。

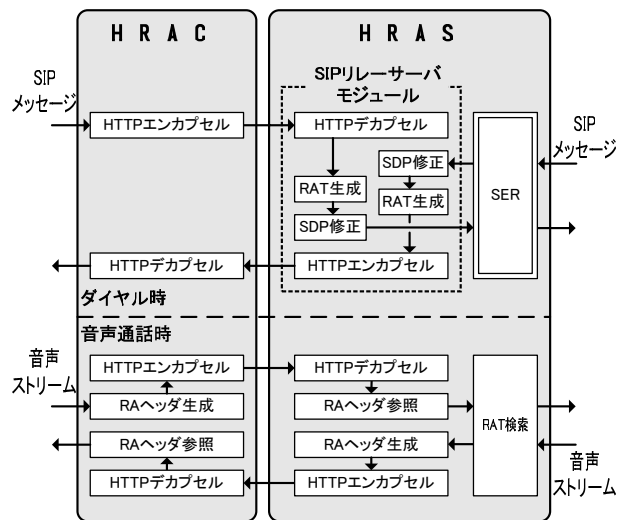


図6. HRA の機能とデータの流れ

表2. HRAC・HRAS の機能

	実現方式	機能
HRAS	HTTPトンネル	HTTPエンカプセル HTTPデカプセル
	音声ストリーム誘導	SDP修正
	音声ストリーム経路決定	RAT生成 RAT検索 RAヘッダ参照 RAヘッダ生成
	SIPサーバとの連携	SER
HRAC	HTTPトンネル	HTTPエンカプセル HTTPデカプセル
	音声ストリーム経路決定	RAヘッダ参照 RAヘッダ生成

2章で述べた実現方式をHRAC・HRASの機能として実装する。機能とデータの流れを図6に示し、表2に実現方式とHRAC・HRASの機能の対応を示す。HRASにおけるSER以外の機能を総称してSIPリレーサーバモジュールと呼ぶ。ダイヤル時、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でSERに処理された後、SIPリレーサーバモジュールでSDP修正・RAT生成機能、HTTPエンカプセル機能によってHRACへ送信される。HRACではHTTPデカプセル機能によって内部ネットワークへ中継される。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HTTPエンカプセル機能によってHRASに送信され、HRASではSIPリレーモジュール・SERによって処理され、外部へ中継される。音声通話時、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され、HRACへ送信される。HRACではHTTPデカプセル・RAヘッダ機能の順に処理され、内部ネットワークへ中継される。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され、HRASへ送信される。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され外部ネットワークへ中継され

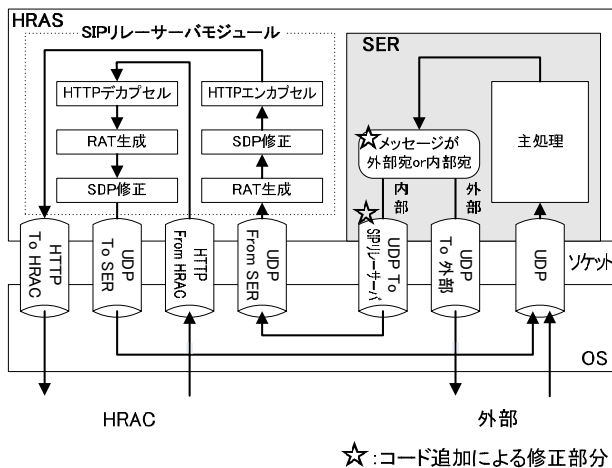


図7. SER と SIP リレーサーバモジュールの連携

る。

SIP リレーサーバモジュールと SER との間の連携にはソケット通信を利用する。SIP メッセージに対する SER と SIP リレーサーバモジュールの処理を順に個別で行うことによって、HRAS に SER の機能を組み込む方法を単純にした。SER と SIP リレーサーバモジュールのソケットによる連携を図7に示す。図7は図6の SER と SIP リレーモジュールの境界を詳しく示したものである。外部ネットワーク側の SIP サーバ、または SIP 端末から HRAS に送信された SIP メッセージは SER の生成したソケットへ到達し、SER の SIP リレーサーバモジュール用ソケットから SIP リレーサーバモジュールの SER 用ソケットに送信される。SIP リレーサーバモジュールでは HRAC 用ソケットから HRAC へ送信される。一方、内部ネットワーク側から HRAC を通って HRAS に到達した SIP メッセージは SIP リレーサーバモジュールの生成した HRAC 用ソケットへ到達し、SER 用ソケットから SER の SIP リレーサーバモジュール用ソケットに渡され外部端末用ソケットから送信される。ただし、内部ネットワークの端末から送信される SIP の登録メッセージのように次のドメインの SIP サーバに中継する必要がなく、端末に対して応答を返すメッセージは再び SIP リレーサーバモジュールに返し、登録要求を出した端末へ中継する。以上の流れは、SER に少量の修正を加えることで実現できる。図8で示すように SER によって一連の処理を終えた SIP メッセージがソケットに出力される前に、メッセージが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通り外部へ送信し、内部宛であれば SIP リレーサーバモジュールへ送信するように修正を加える。

SoFW では複数のセッションによる SIP メッセージと音声ストリームを一つの装置上で並列して処理するため、それぞれを別のプロセスで起動するように実装する。さらに HRAS では別にコンパイルした SER とソケット通信で連携するために SER を実行するためのプロセスも起動する。図8に各プロセスの親子関係を示す。HRAS・HRAC は起動すると HRAS メインプロセス・HRAC メインプロセスがそれぞれ SIP メッセージ処理用の SIP リレープロセスと音声ストリーム用の音声リレープロセスを FORK 関数によって起動する。HRAS では SER を実行するための SER プロセスも立ち上げる。また SIP リレープロセスと音声ストリームプロセスは

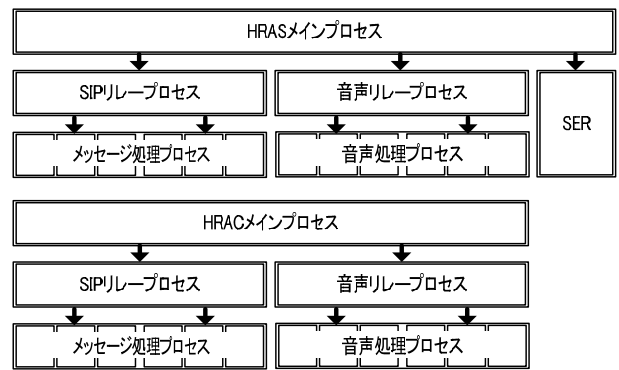


図8. プロセスの親子関係

HTTP トンネルに関する初期処理を行った後、できるだけリアルタイムで複数の端末からの SIP メッセージを処理できるようにするために複数の処理プロセスを立ち上げる。

4. おわりに

本稿では SoFW の実現方式と実装について報告した。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 で扱うデータを音声データに限定して説明したが、SIP はさまざまな用途に対して、その将来性が注目されており、IP 電話以外への対応も検討していく。

参考文献

- [1] N.Freed: Behavior of and Requirements for Internet Firewalls, IETF RFC 2979 (2000.10).
- [2] K. Egevang, P. Francis: The IP Network Address Translator (NAT), IETF RFC 1631 (1994.5).
- [3] 星 徹: VoIP の最新動向, 情報処理学会誌, Vol.42 No.02 - 008
- [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, Packet Based Multimedia Communications Systems, ITU-T Recommendation, 1998.
- [6] J. Rosenberg, et al: "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 Sidiropoulos, 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] 情報処理学会研究報告, 2005-DPS-122, Vol2005, No33
- [13] Handley, M. and Jacobson, V.: SDP: Session Description Protocol, IETF RFC2327 (1998)
- [14] SER: "http://www.iptel.org/ser/"

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

名城大学大学院理工学研究科

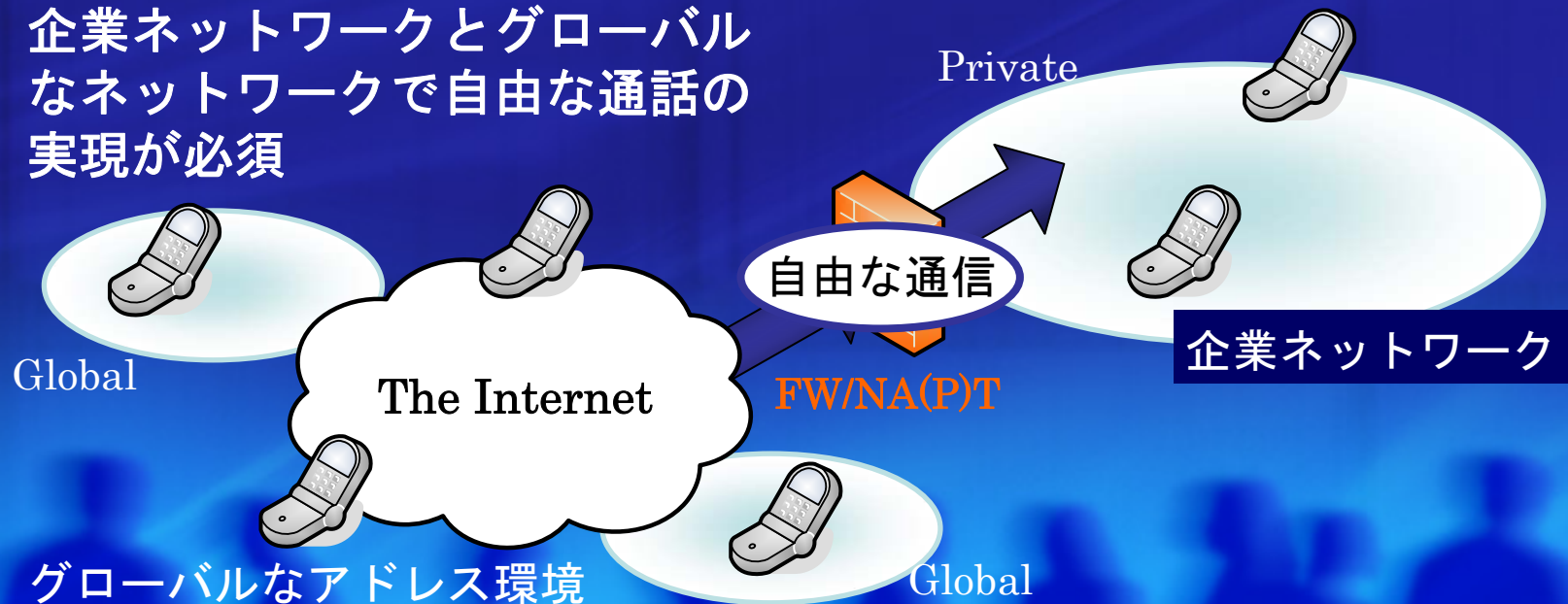
はじめに

- インターネットのブロードバンド化
- IP電話専用番号”050-”の事業者受付の開始

➡ 多くのISPがIP電話を提供

IP電話の更なる利便性の向上のためには・・・

企業ネットワークとグローバルなネットワークで自由な通話の実現が必須

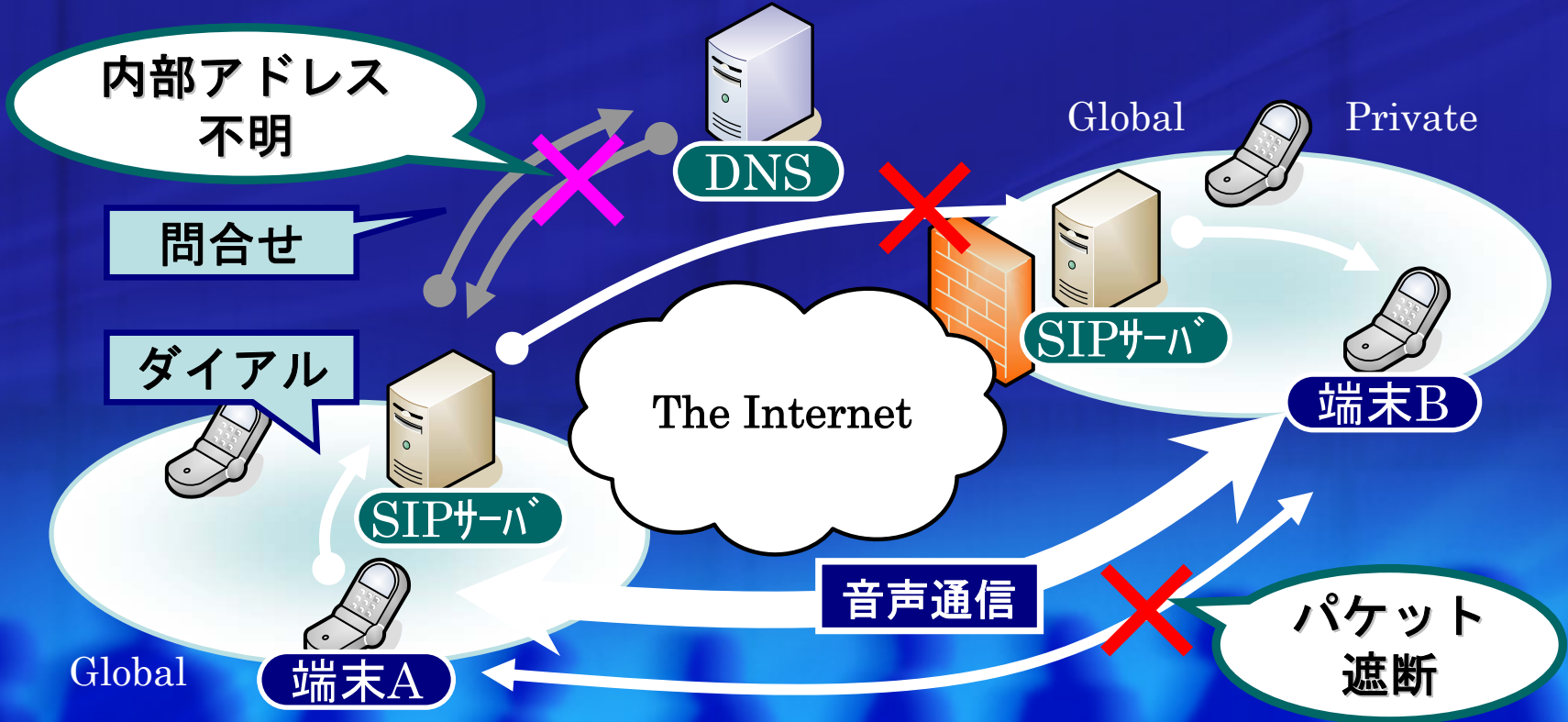


SIPとFW／NATの問題

SIP (Session Initiation Protocol)

拡張性・導入の容易さから、様々なメディア通信のセッション開始プロトコルとして期待されている

FW／NA(P)Tがあると・・・



既存のFW越え技術

■ ファイアウォールに実装するシステム

ポート番号やアドレス管理を動的に行えるように
ルータに実装するシステム

UPnP, VoIPセキュアGW, Connect-VPnP, IP - NAT, etc...



セキュリティポリシーの変更が必須

■ 専用端末、サーバなどに実装するシステム

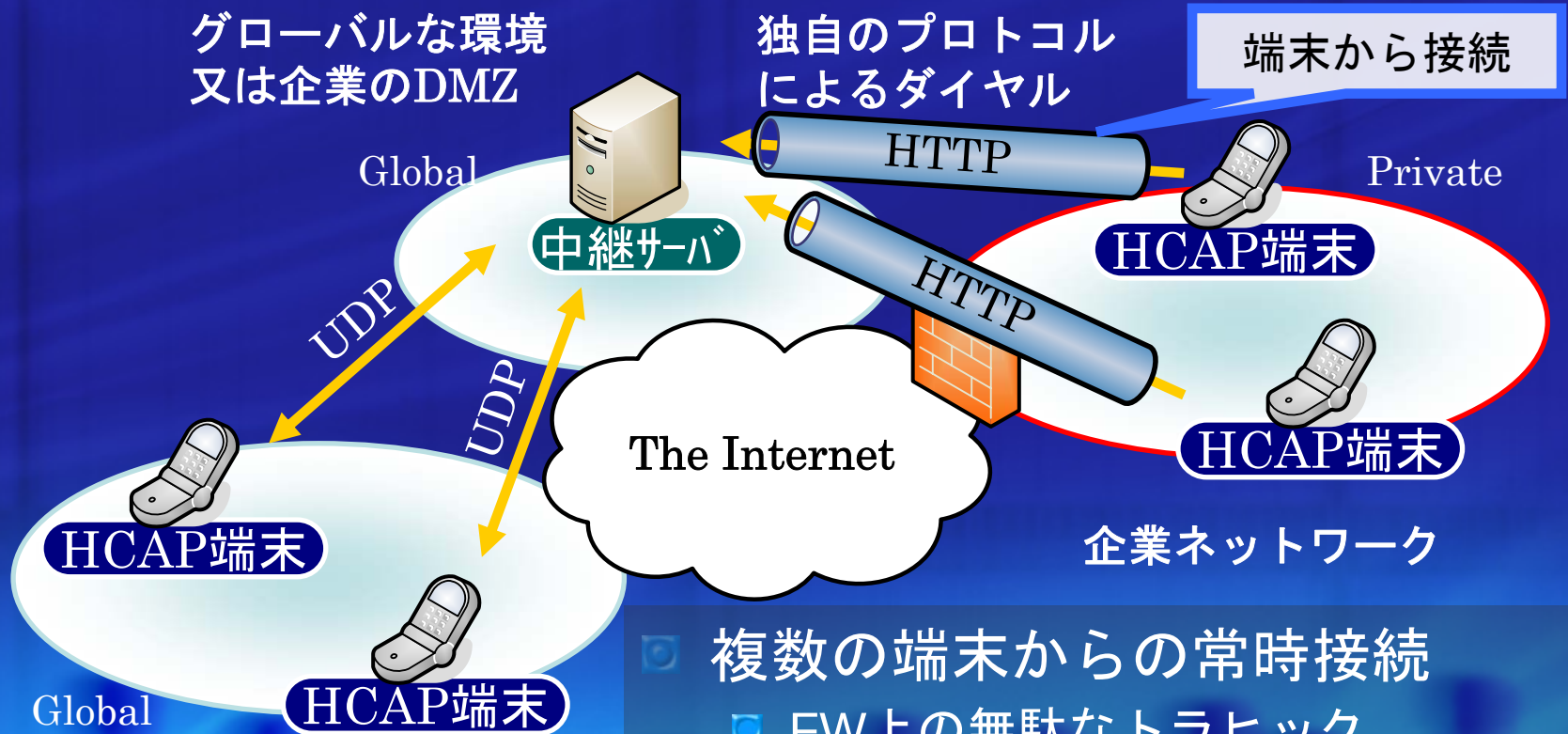
■ Skype

■ HCAP

■ SoftEther（プロトコルフリー）

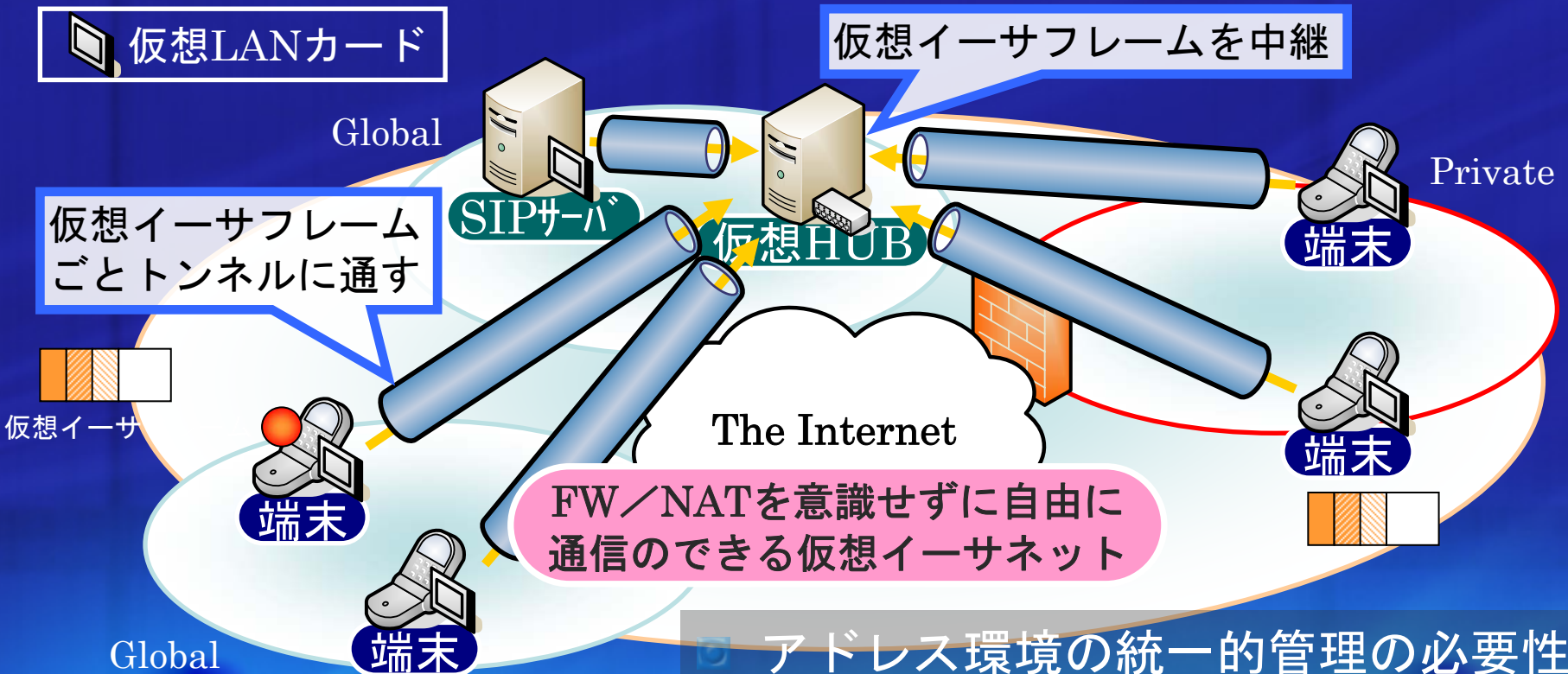
HCAP

専用端末とHTTP中継サーバ間でトンネルを生成し、ダイヤル・音声ストリームを中継する



- 複数の端末からの常時接続
 - FW上の無駄なトラフィック
 - 専用端末を導入する必要がある

端末に実装した仮想LANカードから仮想HUBと呼ばれる中継サーバにHTTPSで接続し、仮想ネットワークを作る



Global
端末には仮想MAC・IP
アドレスが割り当てられる

- アドレス環境の統一的管理の必要性
- 通信相手と同じアドレス環境に置かれるためセキュリティ的に問題

提案システム

システムの目的

- 導入の容易性
- FW上の無駄なトラフィック削減
- 独立したアドレス空間の保持
- 外部ネットワークに対する安全性

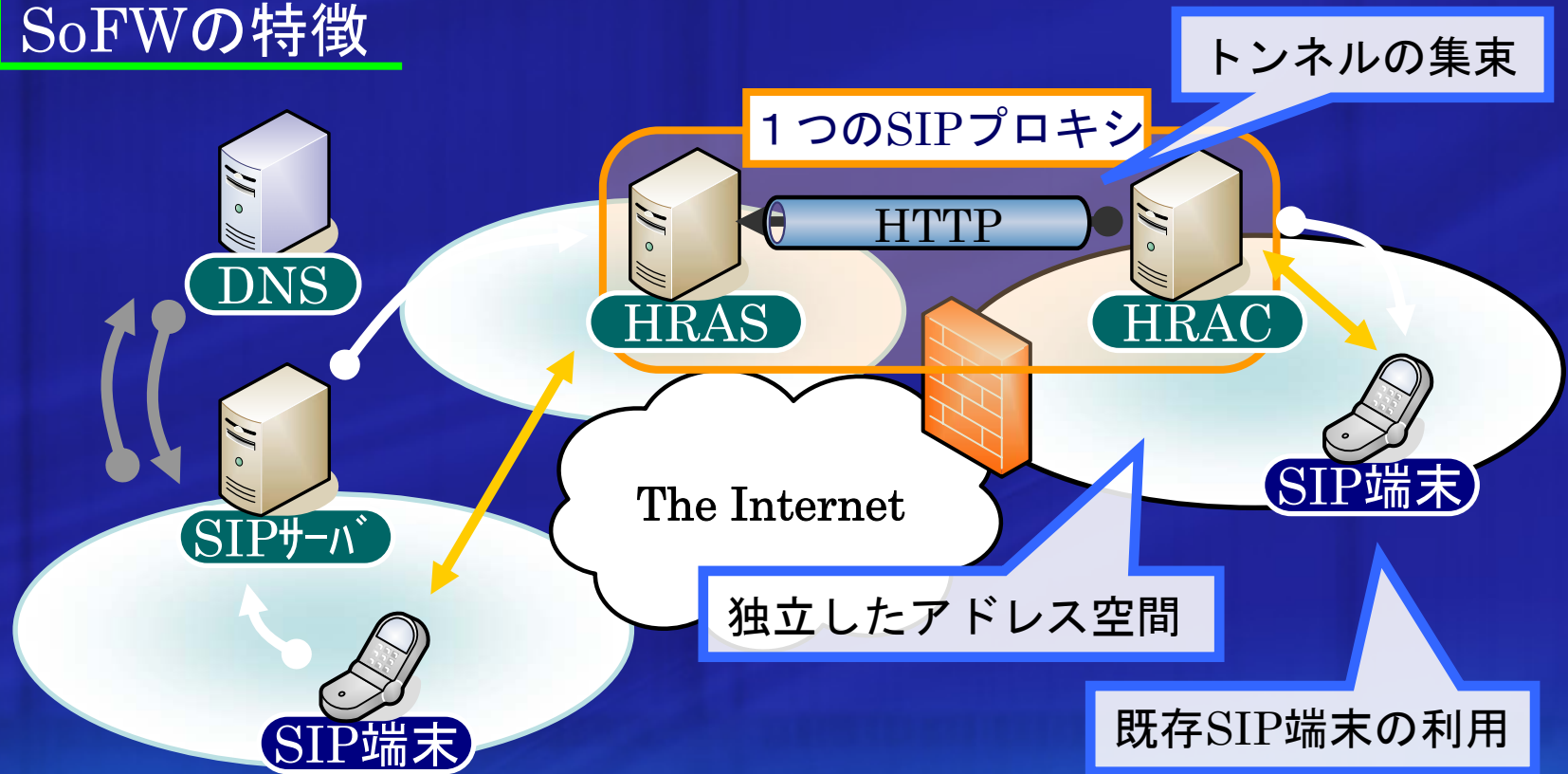


SoFW(SIP over Fire Wall)

内部と外部のネットワークに中継装置を設置し、2台の間にHTTPトンネルを張り、SIP、音声进行中継する。

SoFWの構成

SoFWの特徴



HRAS (Half Relay Agent Server) : 外部に設置

HRAC (Half Relay Agent Client) : 内部に設置

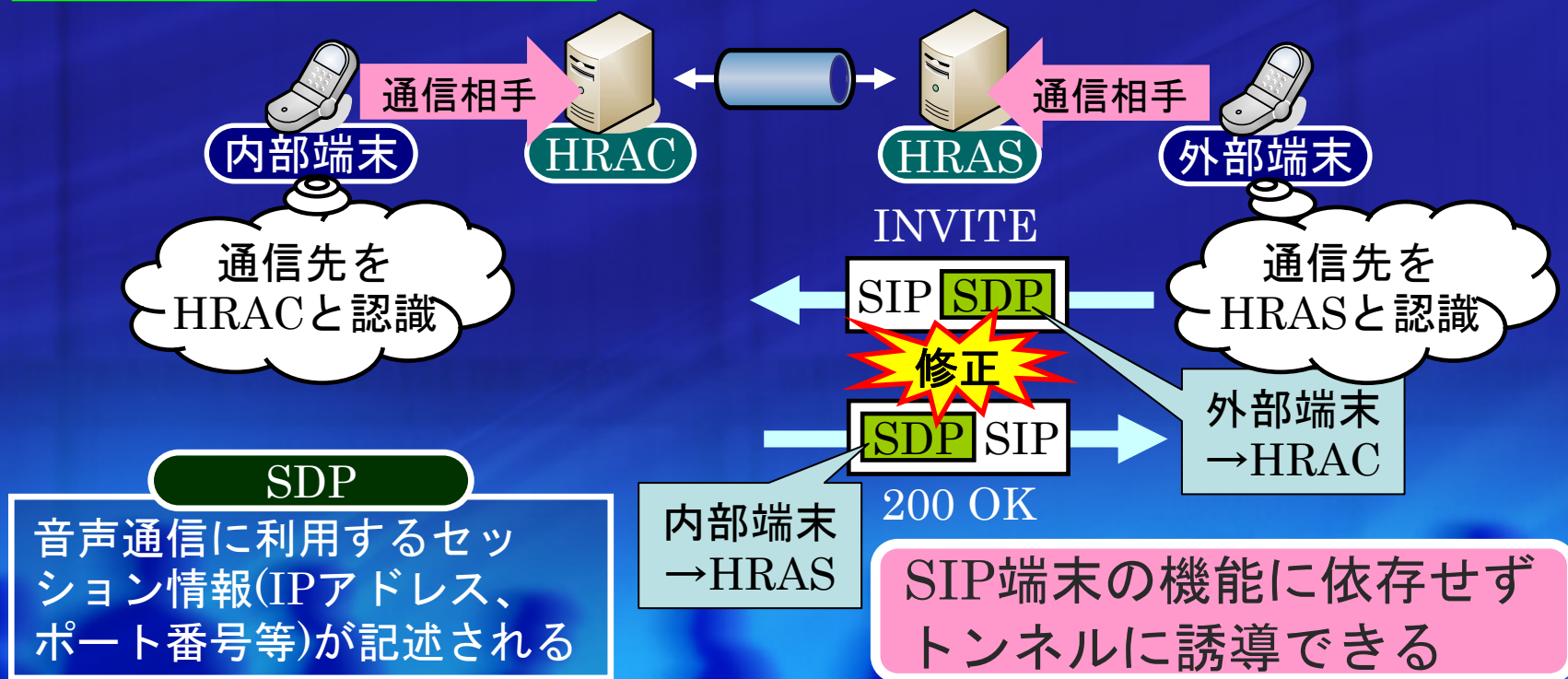
トンネルへの音声ストリーム誘導

通常のSIP端末は音声データを直接相手端末に送信する

通常SIP端末を利用してトンネルへパケットを通すには端末をだまし、HRAC・HRASを通信相手と認識させる必要がある

通信情報のすり替え

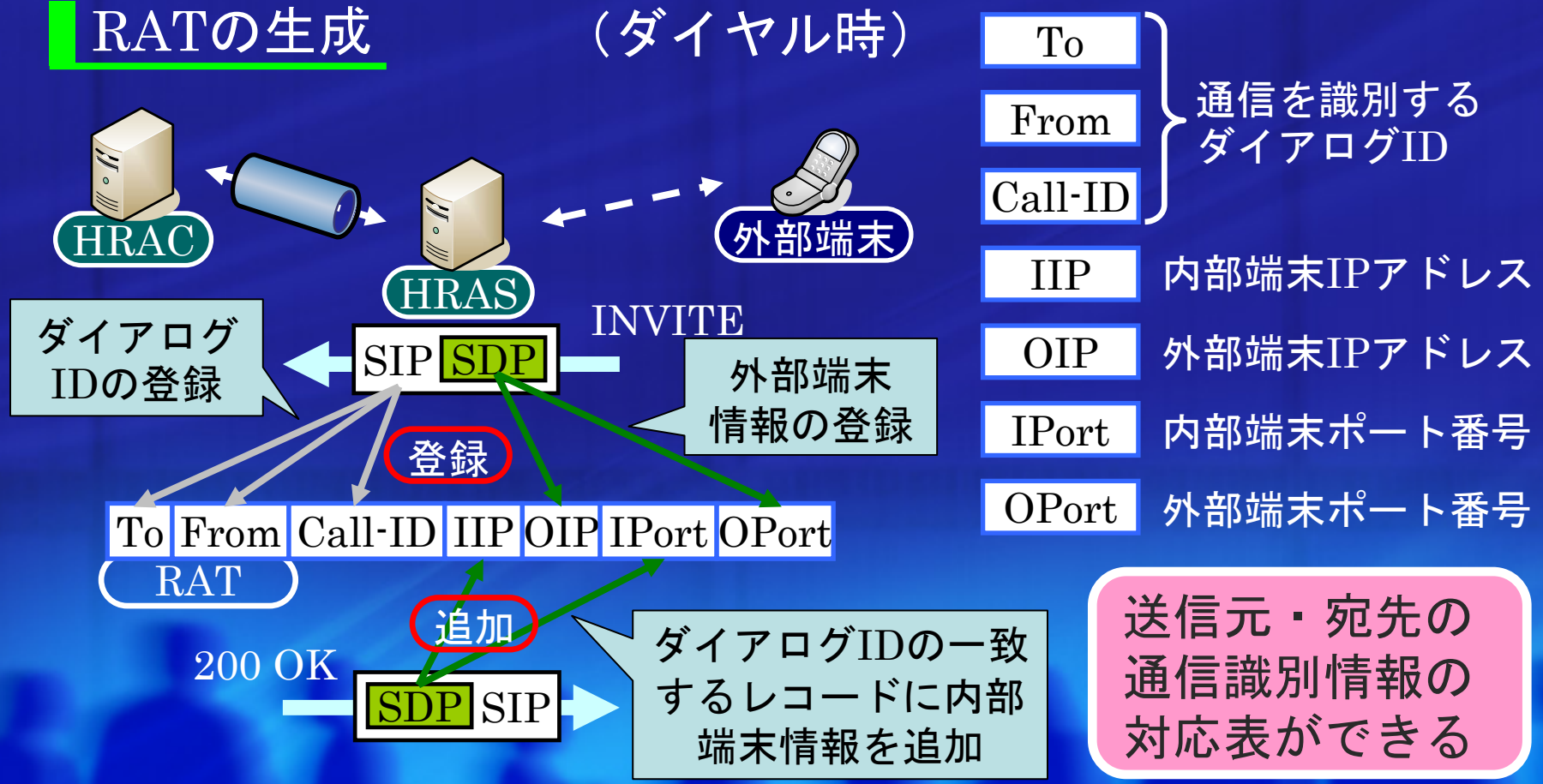
(ダイヤル時)



中継テーブルを利用した経路決定

HRASにRAT (Relay Agent Table) を設置し、宛先を変換して中継することで経路決定を行う

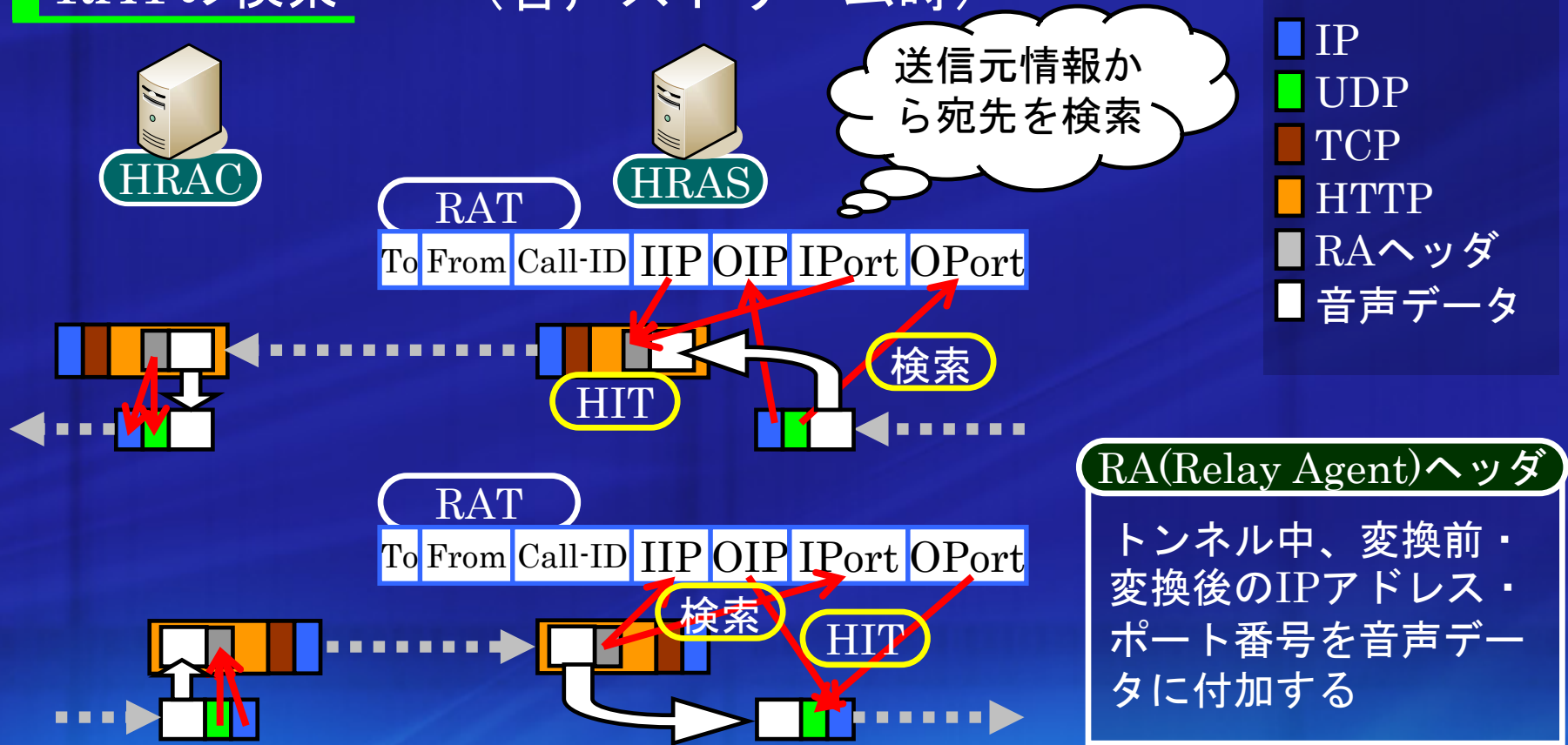
RATの生成 (ダイヤル時)



中継テーブルを利用した経路決定

RATの検索

(音声ストリーム時)

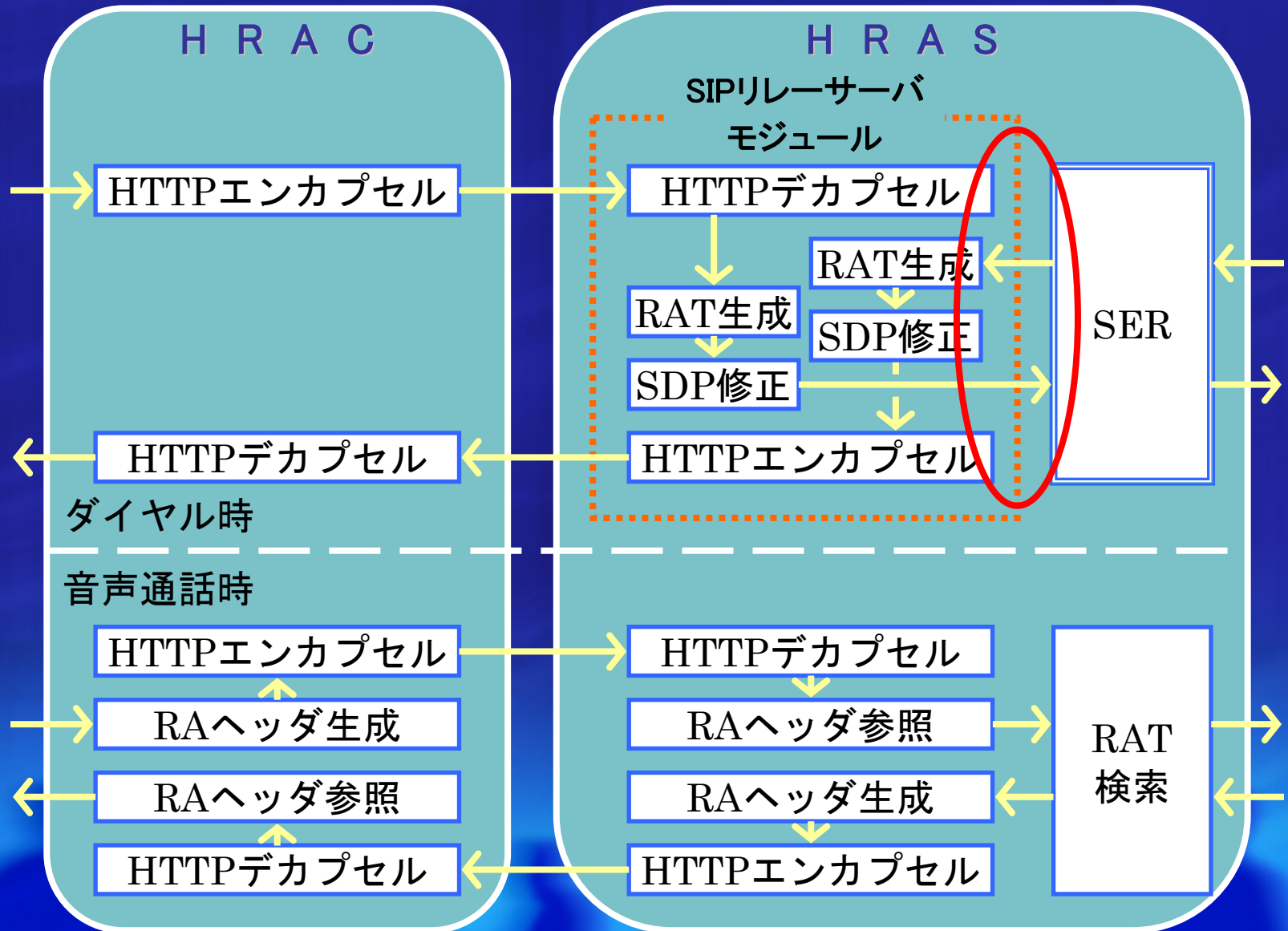


中継テーブルを利用することによって、相手ネットワークと独立したアドレス空間を維持する

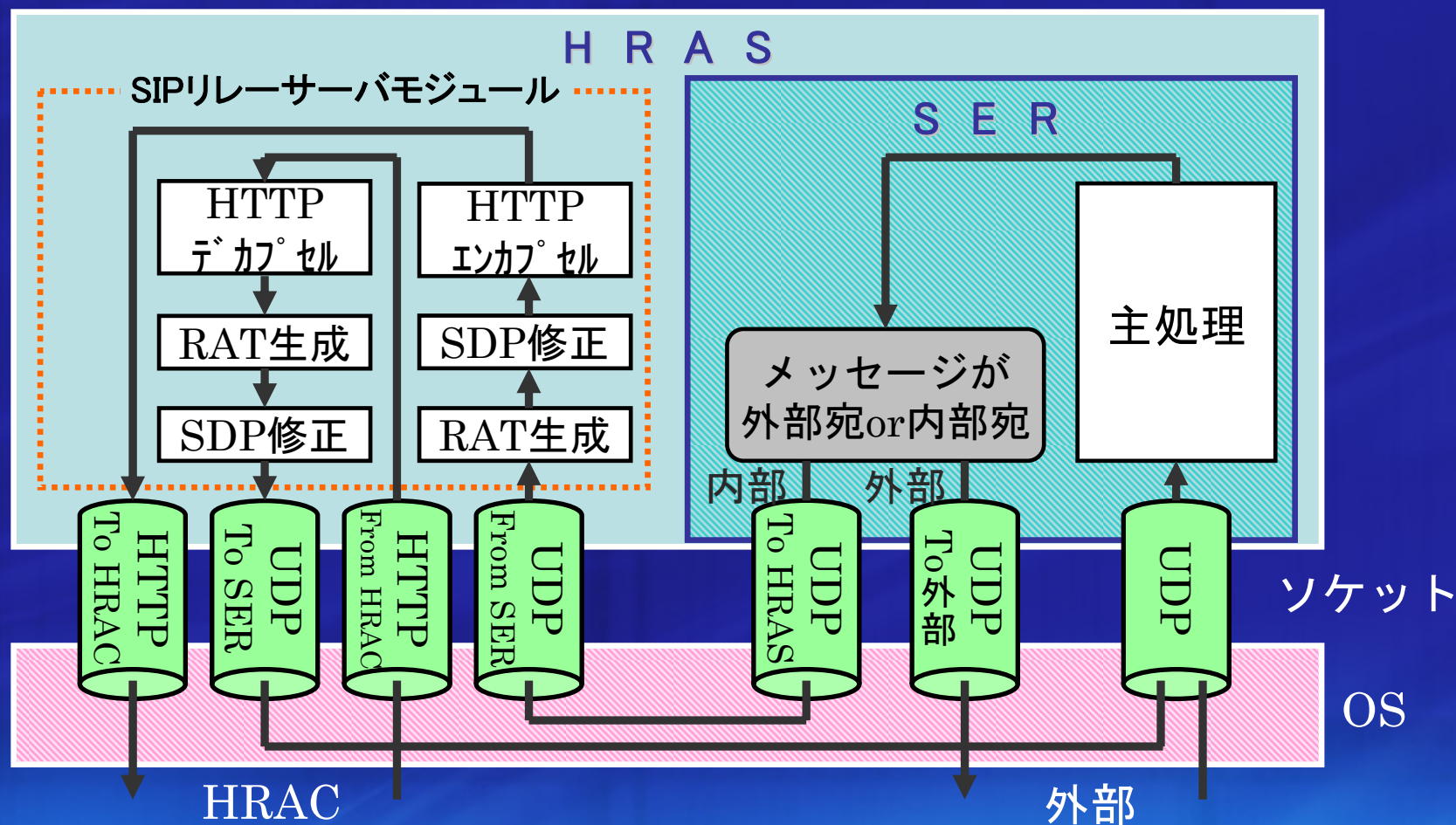
実装 1

- Fedora core3.0のアプリケーションとして実装
- HRASのSIPサーバ機能はフリーのSIPサーバSERと連携することで実現する
- HRASに主処理、HRACには中継に必要最小限な機能のみを実装する

実装 1



実装 2



- SIPリレーサーバモジュール・SERで互いにソケットを開き、メッセージのやり取りを行う
- SERのメッセージ送信部にメッセージが内部・外部宛かでリレーモジュール・外部端末へ送信させる分岐を加える

おわりに

■ まとめ

- ファイアウォール通過システムSoFWの提案
- HRAC・HRASの詳細

トンネルへの音声ストリーム誘導

中継テーブルを利用した経路決定



- 外部に対する安全性
- 独立したアドレス管理
- ファイアウォール上のトラヒックの改善
- 導入の簡単化

■ 今後

- 実装の完了
- ファイアウォール上のトラヒックの評価
- エンドトゥエンドのディレイの評価

おわり

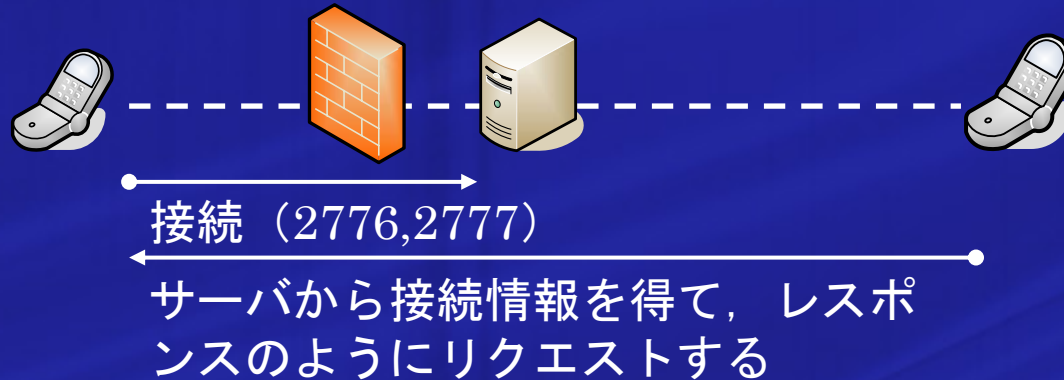


補足 1. その他のFW通過システム 1

- VoIPセキュアゲートウェイ（富士通）
VoIPを通過させるゲートウェイ
- Connect-VPnP（ソルフォン株式会社）
内部端末からFWの開放ポートを操作
- SIP-NAT（ヤマハ株式会社）
SIPとVoIPを通過させるゲートウェイ

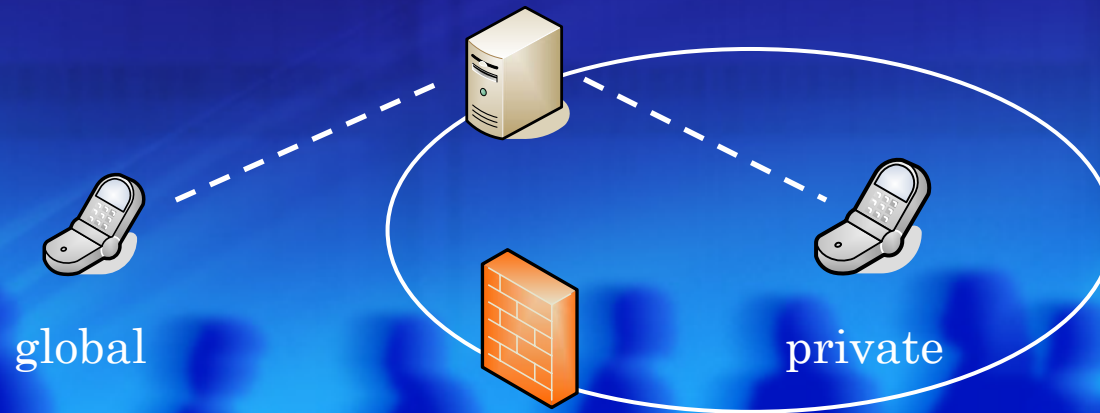
補足 2. その他のFW通過システム

■ IPFreedom (TANDBERG社)



■ OnDo SIPサーバ

SIPサーバがグローバル&プライベートのNICを持つ



補足 3. トンネル中継の基本的な流れ

HTTPトンネルを生成、その後は内部・外部から受信するSIPメッセージ・音声データをトンネルに埋め込み中継する

