ファイアウォールを通過できる IP 電話の実装と評価

043432004　伊藤将志
渡邊研究室

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 電話は十分な通信品質を確保できるようになった．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（Firewall：以下 FW）やアドレス変換装置（Network Address Translator：以下 NAT）が存在し，これらは企業ネットワーク内と外部の端末間の VoIP（Voice over IP）の利用を困難にする．VoIP が FW/NAT を越えて安全に利用できるようになれば IP 電話の利便性は更に向上されるものと考えられる．

現在，IP 電話のダイヤルには，SIP （Session Initiation Protocol）[1]が導入の容易性と優れた拡張性から注目されている．SIP は既に広く普及しており，SIP 端末/サーバの開発には多くのベンダーが着手し，固定電話，携帯型，ソフトフォンと形態や機能も多種多様である．

SIP は SIP 端末と SIP サーバで構成されており，SIP サーバに SIP 端末の位置情報を登録し，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，ダイヤル開始に先立ち相手端末，または相手端末の属する 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，内部のアドレス情報を隠蔽してしまう NAT が介在するような環境ではダイヤルを開始できない．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いる．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，本稿では FW の内部／外部に設置した 2 台の中継装置間で作った HTTP トンネルを利用して FW 越えを実現するシステム SoFW（SIP over Firewall）を提案する．また SoFW の実装と評価を行ったので，その結果を報告する．

2. 既存技術とその課題

FW/NAT が介在しても IP 電話が可能なシステムは既にいくつか提案されている．これらは FW の許可する通信を動的に操作する方法と，HTTP などの予め FW 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．

前者はピンホール・ファイアウォール方式と呼び，FW がダイヤルを監視するか，端末が FW に情報を提供することで，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，ピンホール・ファイアウォールを利用した音声通信では不特定多数の UDP 通信を許可するため，企業によっては

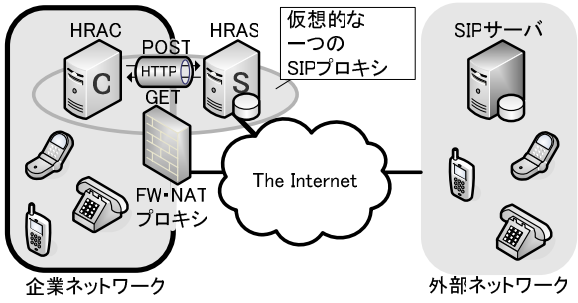


図 1．SoFW の構成

セキュリティポリシィの変更が必要となり，FW 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，導入には手間とコストがかかる．

後者の代表的なシステムとして HCAP，Skype などの IP 電話専用システムと，全アプリケーションの FW の通過を可能にする SoftEther がある．

HCAP は FW の外側に接続し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，外部との通話を可能にする．Skype も同様に端末から HTTP トンネルを張るが，中継はスーパーノードと呼ばれる一定の性能基準を満たしたインターネット上の不特定な端末が行う． HCAP や Skype は端末に特殊な機能が必要なため，利用可能な電話端末は専用のものに限定され，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．また Skype は不特定な中継ノードを利用するという点で安全面の信頼が薄い．

SoftEther は FW 外部の仮想 HUB というソフトウェアと内部の仮想 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，仮想イーサネット環境を構築する．仮想イーサネットに接続することによりアプリケーションに依存しない通信が可能となるが，仮想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，外線用 IP 電話として企業ネットワークへ導入することは難しい．

3. 提案システム SoFW

SoFW は FW の外部と内部に 2 台の中継装置を設置し，2 点間で HTTP トンネルを作る．既存のネットワーク構成に変更を加えない容易な導入を可能にし，既存の SIP 端末の機能をそのまま利用できる．また，IP アドレス管理にも一切影響を与えない．

SoFW の構成を図 1 に示す．プライベートアドレス側の中継装置を HRAC（Half Relay Agent Client），グローバルアドレス側の中継装置を HRAS（Half Relay Agent Server）と呼ぶ．HRAS には SIP サーバが組み込まれており，HRAS と HRAC が HTTP トンネルで接続

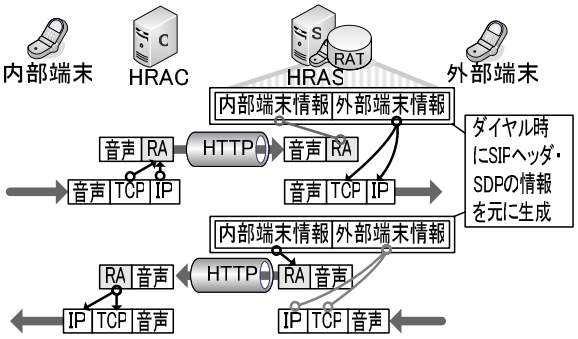


図 2．RAT を用いた経路決定

される．HRAC/HRAS はグローバルアドレスとプライベートアドレスのインタフェースを持つ仮想的な 1 台の SIP サーバとなる．端末は HRAC/HRAS を SIP サーバと見なしてダイヤルを行う．HRAS はその際 SIP メッセージから外部/内部端末の対応テーブル RAT（Relay Agent Table）を作る．音声通信時には端末はトンネルへ音声ストリームを送り，HRAS は RAT に従って音声ストリームを中継する．

3.1 音声ストリームの誘導と経路決定

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 のセッション開始メッセージとそのレスポンスメッセージが HRAS に到達すると，そのボディ部に記述されるセッション情報のタイプ値の修正を行う．HRAS が内部端末に対して外部端末のセッション情報を通知するセッション情報を HRAC の情報に，外部端末に対して内部端末のセッション情報を通知するセッション情報を HRAS のセッション情報に修正する．これにより内部端末は HRAC を，外部端末は HRAS を通信相手とみなすこととなり音声ストリームは HTTP トンネルへ誘導される．

3.2 音声ストリームの経路決定

SoFW は HRAC/HRAS の 2 点をアプリケーションレイヤで中継するという構造のため，エンド端末の IP レイヤ情報をアプリケーションで保持する必要がある．ダイヤル時は，SIP が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．音声通信時は RA（Relay Agent）ヘッダと呼ぶ IP アドレス・ポート番号をメンバとする独自のヘッダを利用する．図 2 に経路決定の概念図を示す．RAT はダイヤル時に HRAS が両方向の SIP ヘッダとボディ部に記述されるセッション情報を組み合わせて生成されている必要がある．音声通話時，INBOUND の音声ストリームは HRAS が送信元の情報に対応する外部端末情報を RAT から参照し，外部端末情報を RA ヘッダとして音声データに付加し，HRAC に中継する．HRAC は RA ヘッダの内容を宛先にして音声データを送信する．OUTBOUND の音声ストリームは HRAC が送信元情報を RA ヘッダとして音声データに付加し，HRAS に中継する．HRAS は RA ヘッダの情報に対応する外部端末情報を宛先にして音声データを送信する．

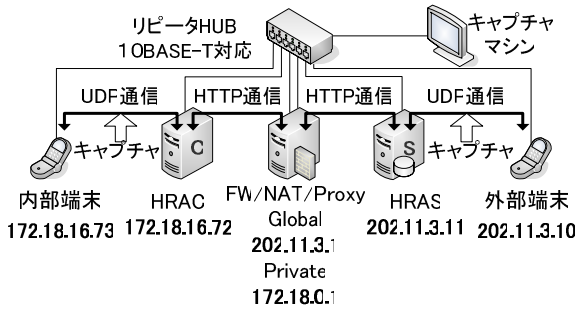


図 3．実験構成

表 1．実験結果

ストリーム方向	SoFW 構成装置の処理遅延
OUTBOUND	1.641msec
INBOUND	2.087msec

4. 実験と評価

HRAC/HRAS を 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 サーバ機能はフリーソフトの SER（SIP Express Router）とのソケットを利用した連携によって実現した．

今回は音声通話の際に HRAC/HRAS と FW，NAT，Web プロキシの処理遅延合計を計測する実験を行った．

実験構成を図 3 に示す．リピータ HUB に FW，NAT，HTTP プロキシを一台に実装した装置と，外部端末，HRAS，HRAC，内部端末，キャプチャマシンを接続している． SIP 端末には X-Lite というソフトフォンを採用し，音声コーディックは G.711 である．図 3 の環境で，音声通信を行わせ，片方のエンド端末から送信される直後の音声パケットと，もう片方のエンド端末が受信する直前の音声パケットをキャプチャし，その差を計算した．音声パケットのサンプル数は 10000 とした．結果を表 1 に示す．

IP 電話ではネットワークを介した端末間の音声遅延が 400msec 以内であれば音声通信を行うサービスとして認められる[2]．実験結果では両方向共に 2msec 前後の平均遅延であった．400msec に対して SoFW による遅延は約 0.5%程度であり通話にはほとんど影響を与えないと言える．

5. おわりに

ファイアウォールを通過できる IP 電話 SoFW を提案し，実装と実験結果を報告した．SoFW の処理によって加算されるエンドツーエンドの遅延は十分小さいことが分かった．

今後は HRAS/HRAC 間の TCP の再送制御がエンドツーエンド遅延に与える影響，エンド端末のペア数が複数ある場合の性能を測定していく．

参考文献

[1] J.Rosenberg, et all: ”SIP:Session Initiation Protocol”, IETF RFC3261(2002,6)

[2] 総務省: ”IP ネットワーク技術に関する研究会　報告書”, (2002,2)

ファイアウォールを通過できるIP電話の実装と評価

Implementation and Evaluation of Voice over IP System Passing Through Firewall and its Implementation

渡邊研究室

043432004　伊藤 将志

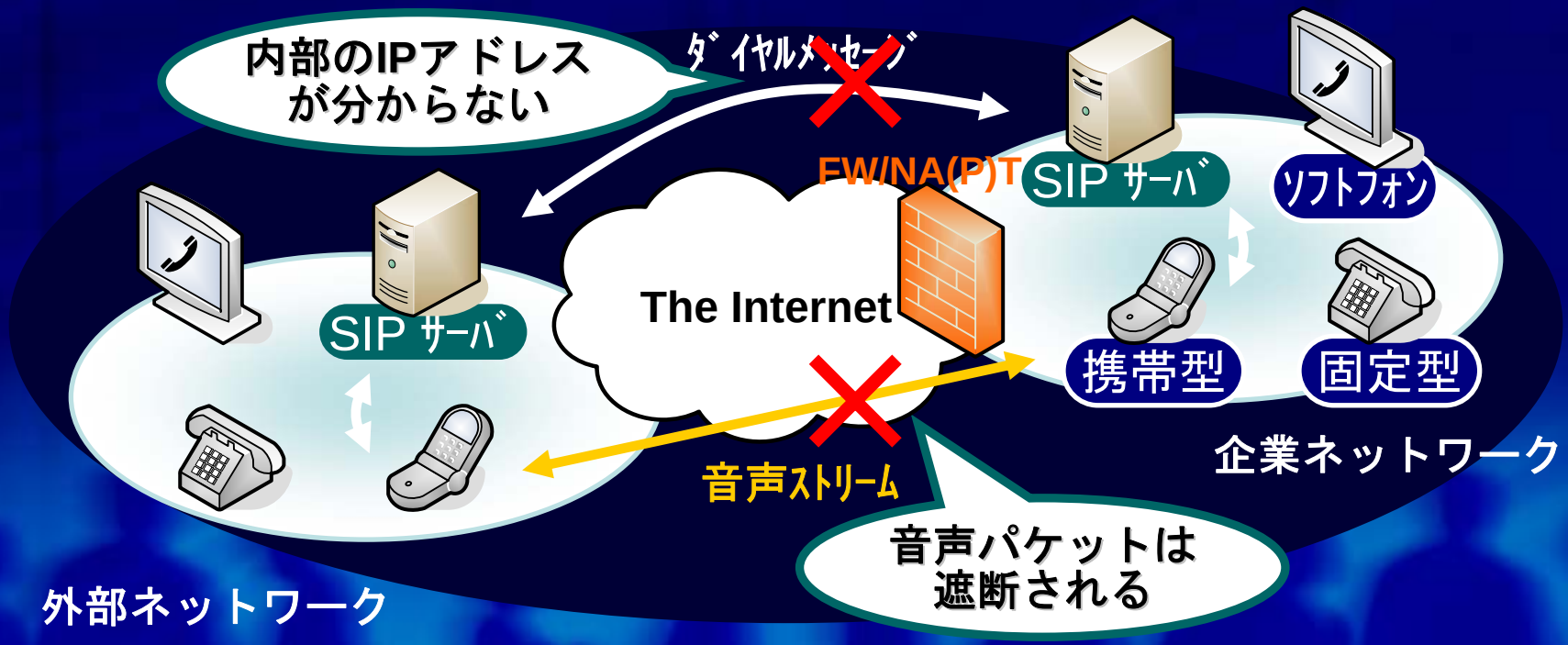
はじめに

IP電話を導入する企業の増加

- 通話料金のコスト削減
- 生産性向上

SIP（Session Initiation Protocol）の普及

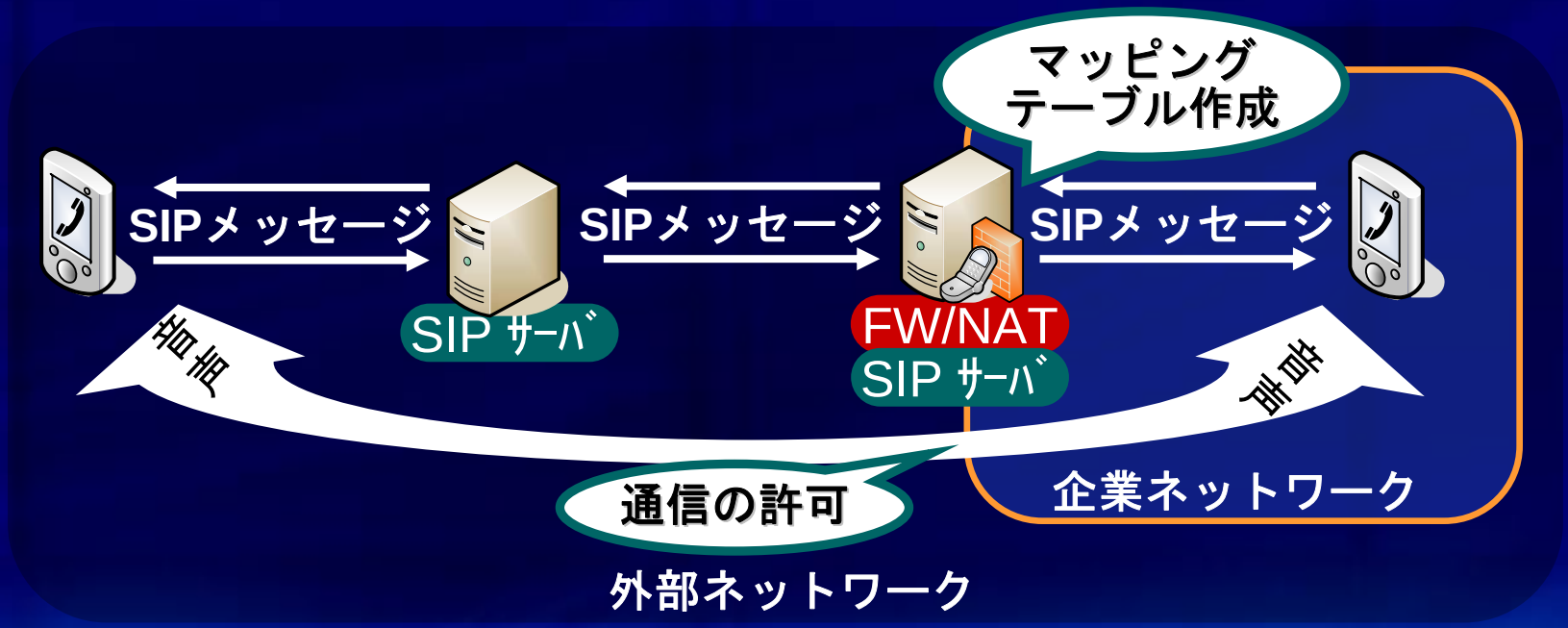
様々な形態・機能を持つSIP端末・SIPサーバが開発されている



既存技術　ピンホール・ファイアウォール方式

ダイヤルを監視し，動的にファイアウォールの開閉を行う

アプリケーションレベルゲートウェイ付きSIPサーバ

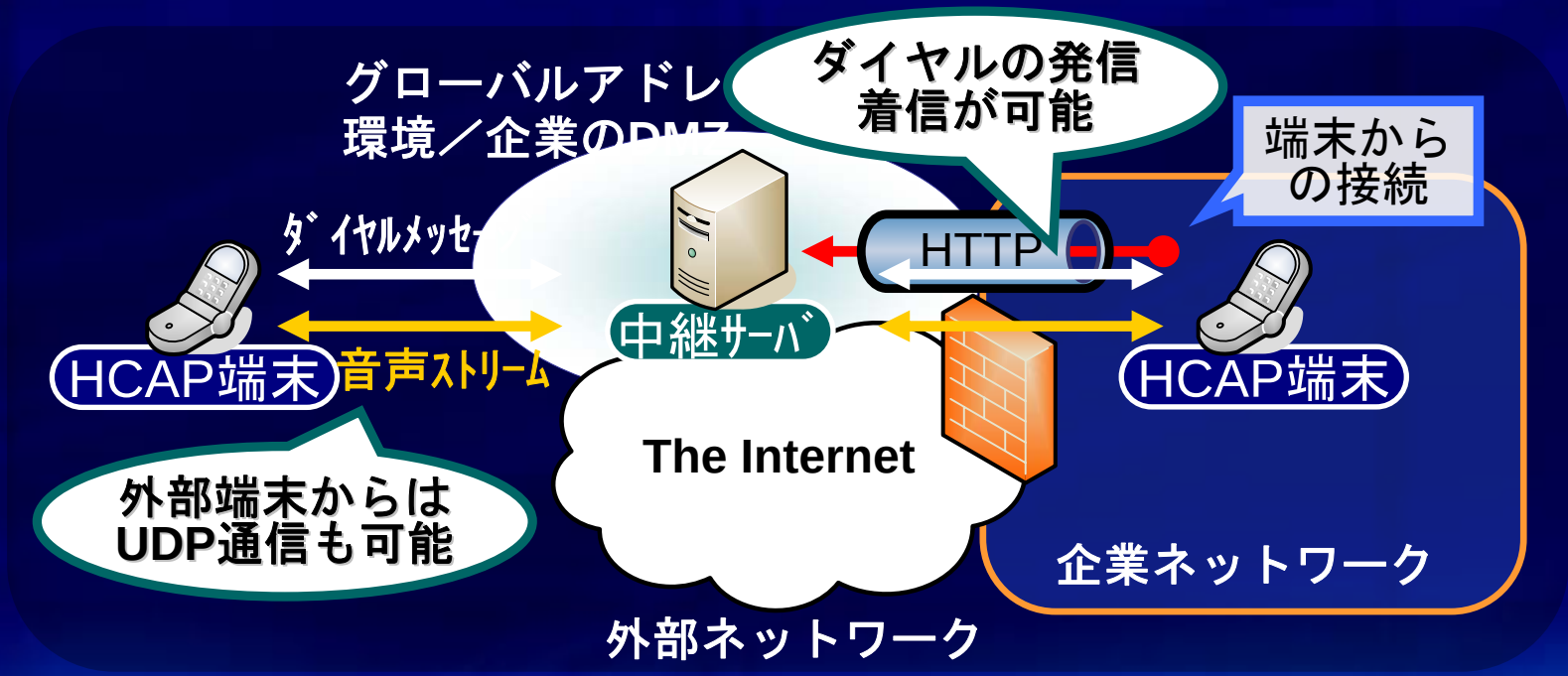


- 外部へのゲートウェイが唯一の場合に限定
- ファイアウォールにモジュールの追加，もしくは新規にゲートウェイの導入が必要

既存技術　HTTPトンネル方式（HACP，Skype）

端末と中継サーバの間にHTTPトンネルを張る方式

HCAP(HTTP-based Conference Application protocol)

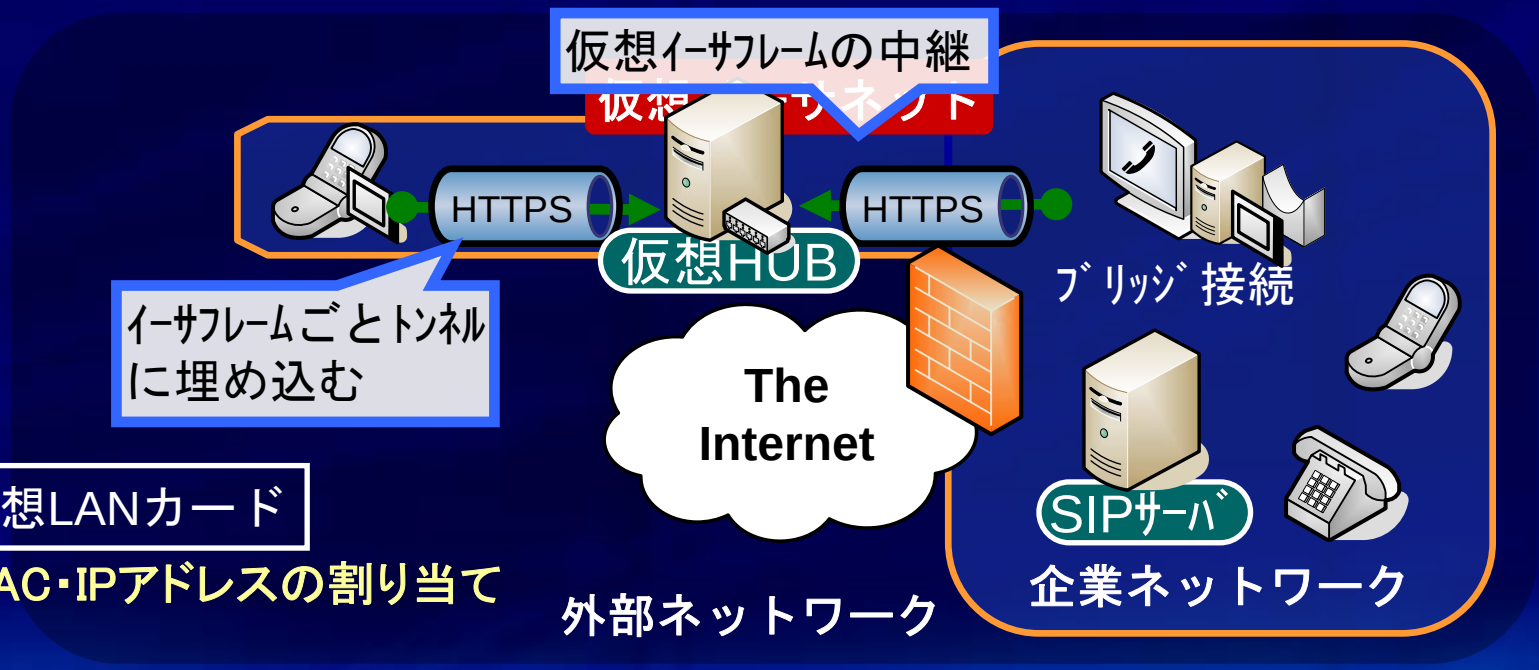


- 端末に特殊な機能が必要
  - 既存のSIP端末では使用できず，企業にて既存のSIPネットワークを構築済みの場合は総入れ替えが必要

既存技術　ファイアウォールを越えるVPN

SoftEther (現在の名称はPacketiX VPN)

仮想HUB/仮想LANカードと呼ばれるソフトウェア間で生成したトンネルで仮想イーサフレームを中継し仮想イーサネットを形成する



- IPアドレスの統一的管理が必要
  - 内線用電話としては利用できるが，外線用電話として利用すると外部に内部ネットワークをさらすことになる

提案システム

SoFW（SIP over Fire Wall）

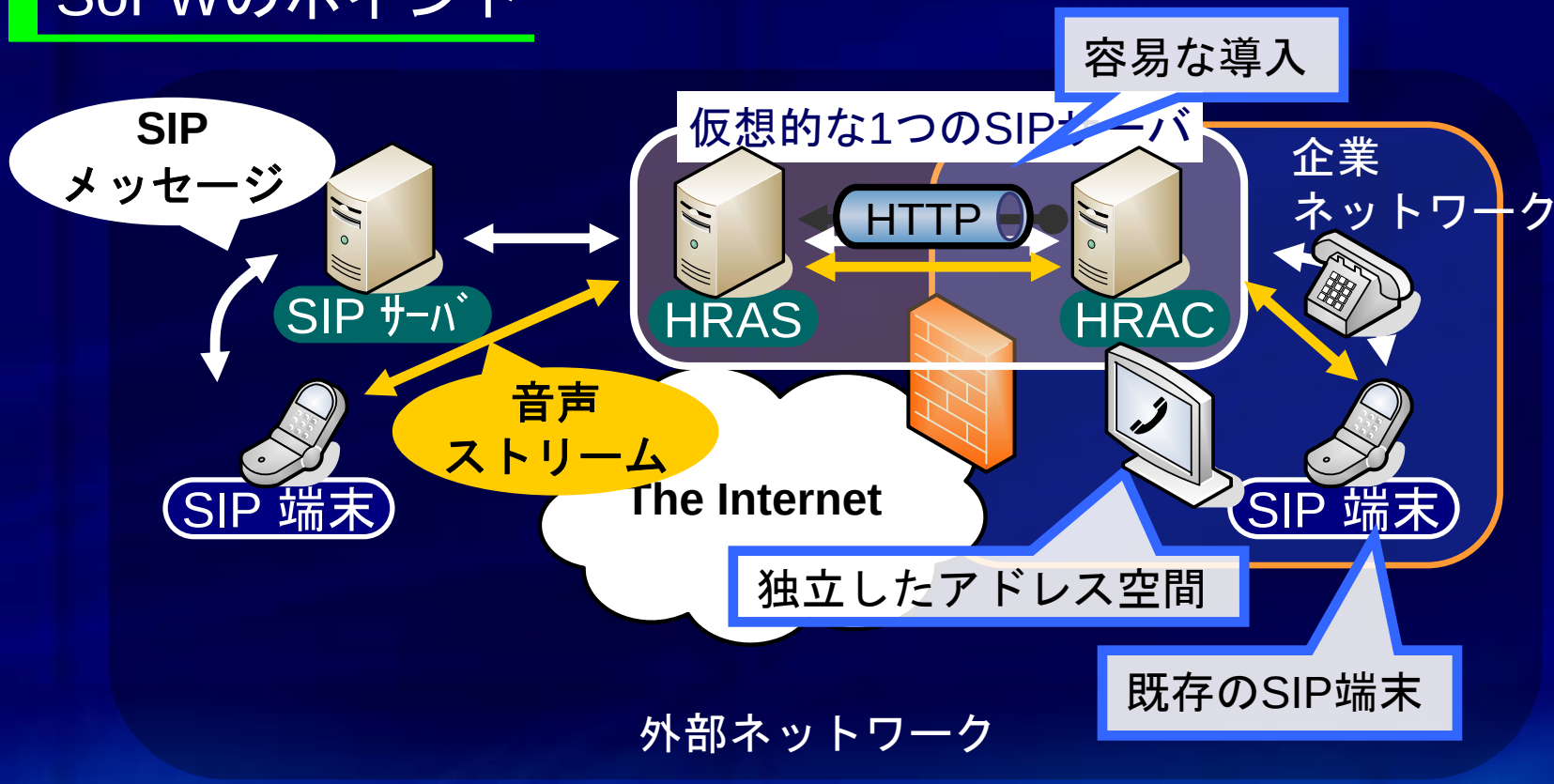
ファイアウォール**内部/外部に設置した中継装置間**で
HTTPトンネルを作成し，**アプリケーションレベル**
でSIPメッセージ/音声ストリームを中継する

システムの利点

- 導入が容易にできる
- 既存のSIP端末が利用できる
- アドレス環境の統一的管理を必要としない

提案システムSoFW　システムの構成

SoFWのポイント



HRAS (Half Relay Agent Server)：外部に設置，SIPサーバの機能

HRAC (Half Relay Agent Client) ：内部に設置

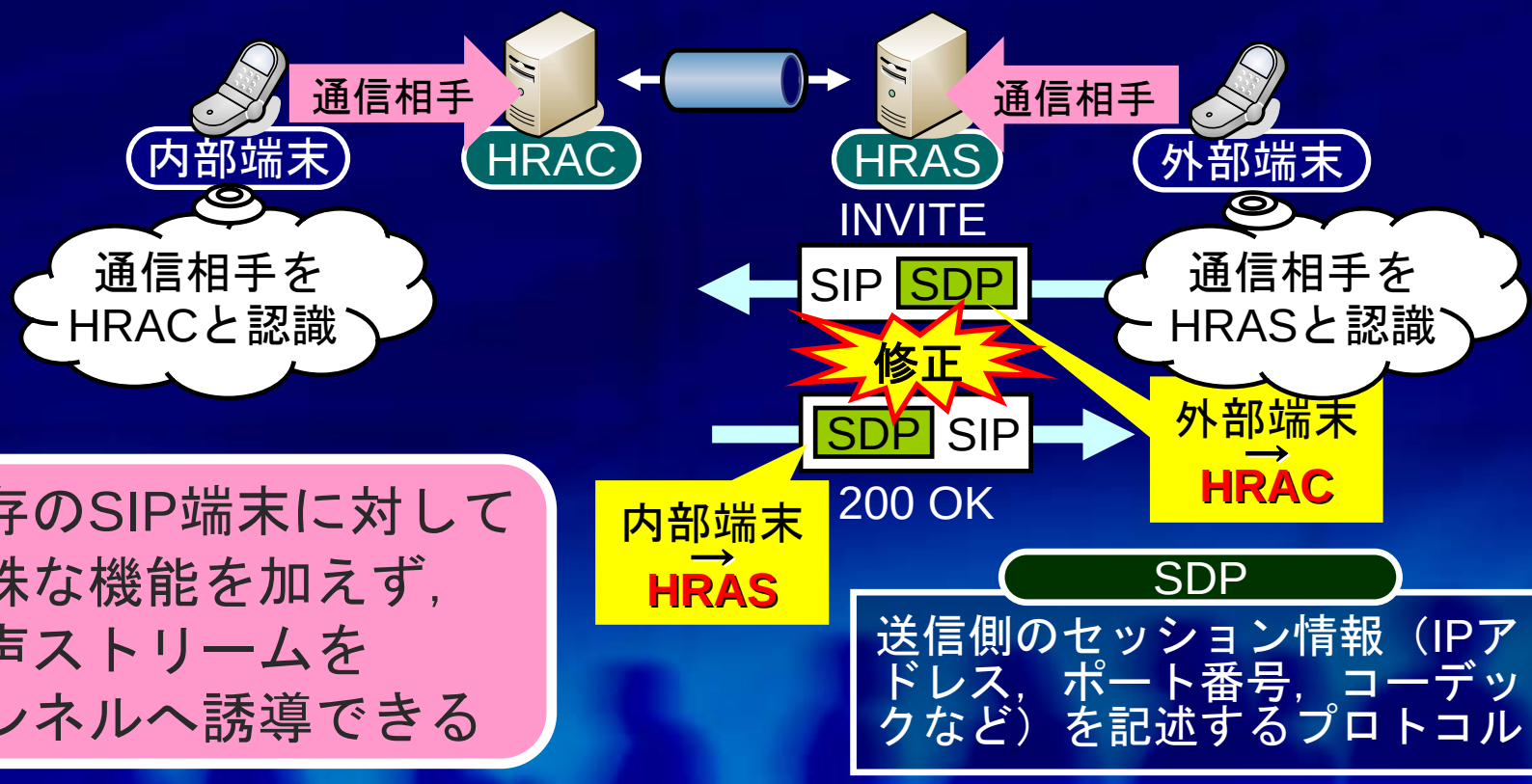
提案システム SoFW

音声ストリームの誘導

通常のSIPでは，音声通話時は端末間で直接通信を行う

HTTPトンネルに音声ストリームを誘導する必要がある

セッション情報の修正（ダイヤル時）



既存のSIP端末に対して特殊な機能を加えず，音声ストリームをトンネルへ誘導できる

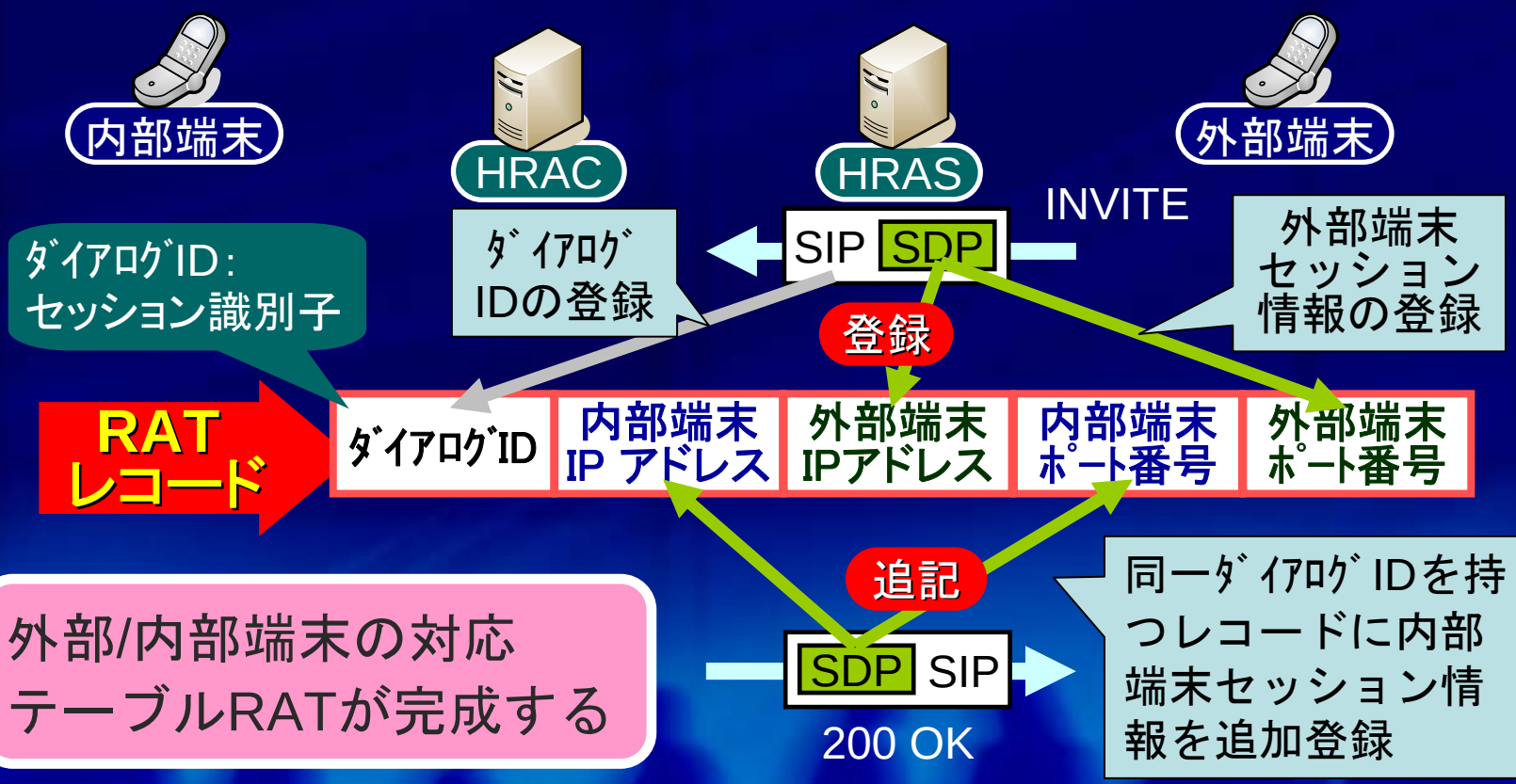
SDP

送信側のセッション情報（IPアドレス，ポート番号，コーデックなど）を記述するプロトコル

提案システムSoFW　経路決定

HRASは**RAT (Relay Agent Table)**を生成して音声ストリームの経路決定を行う

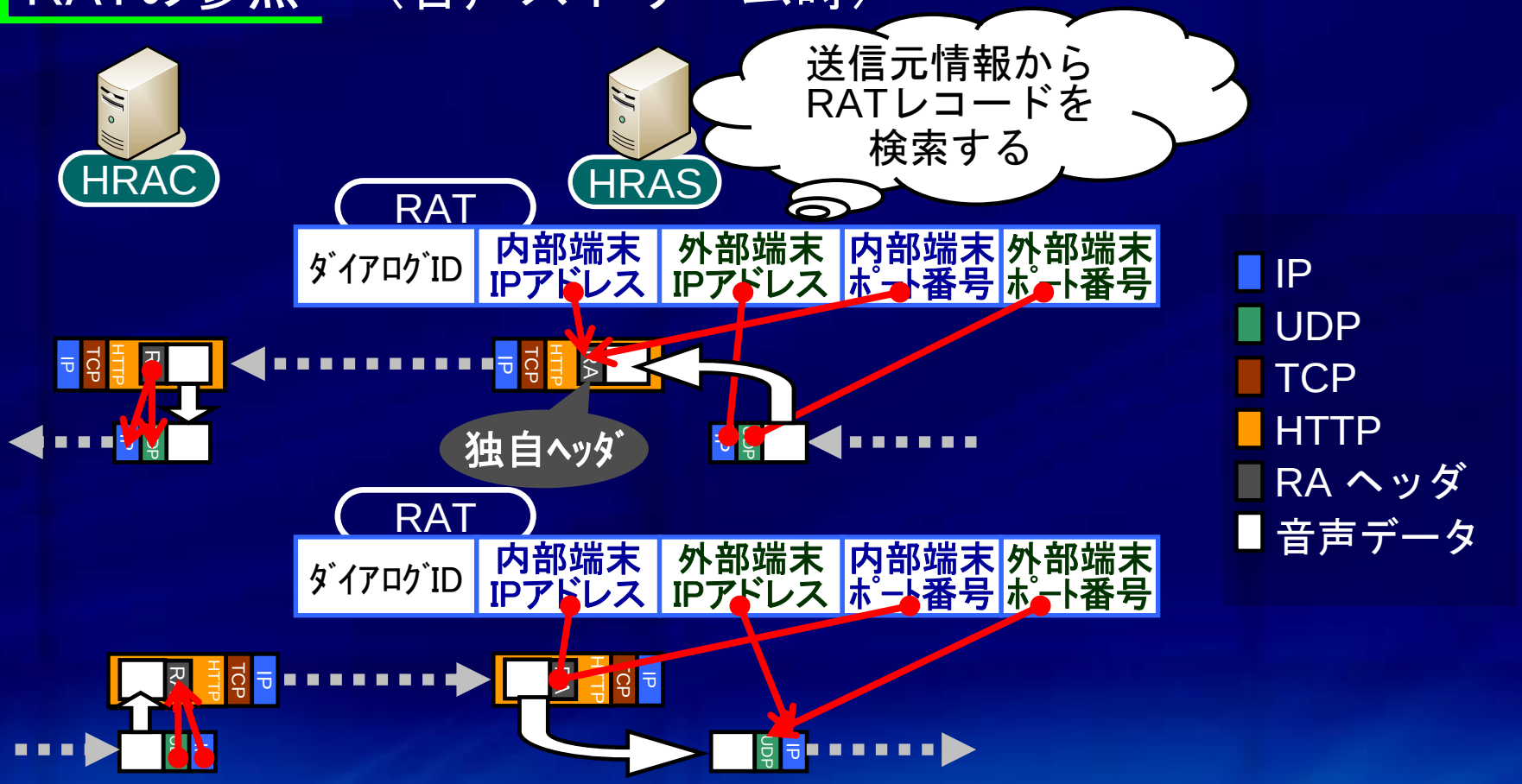
RATの生成　（ダイヤル時）



外部/内部端末の対応テーブルRATが完成する

提案システムSoFW　経路決定

RATの参照　（音声ストリーム時）



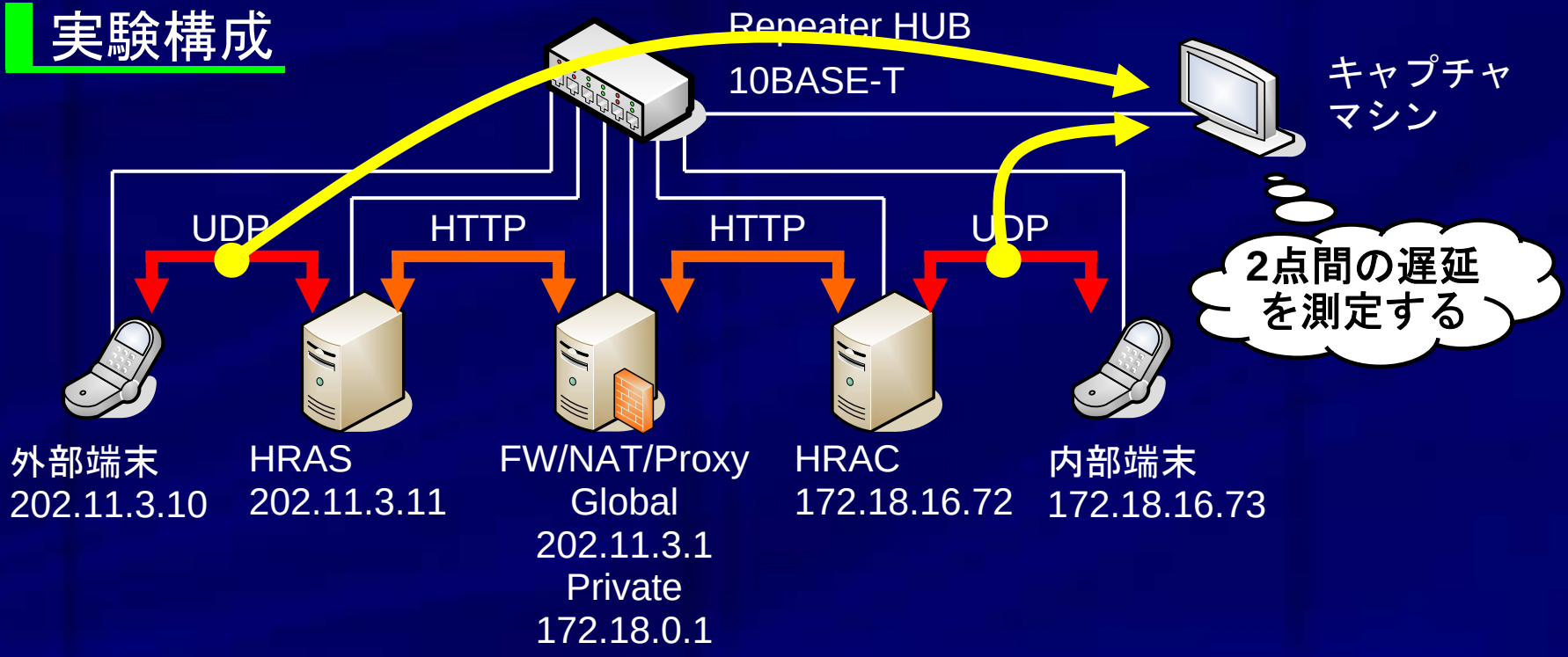
RATの利用と，アプリケーションレベルの中継によって，
ネットワークアドレス空間を独立したまま通信が可能となる

実装

- Fedora core3.0 (Linux 2.6.9)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ソフトSER(SIP Express Router) とソケットで連携することで実現する
- メモリアクセスを効率化するために並行処理にはマルチスレッドを用いる

実験と評価

実験構成



SoFWの各装置の処理時間の合計を測定

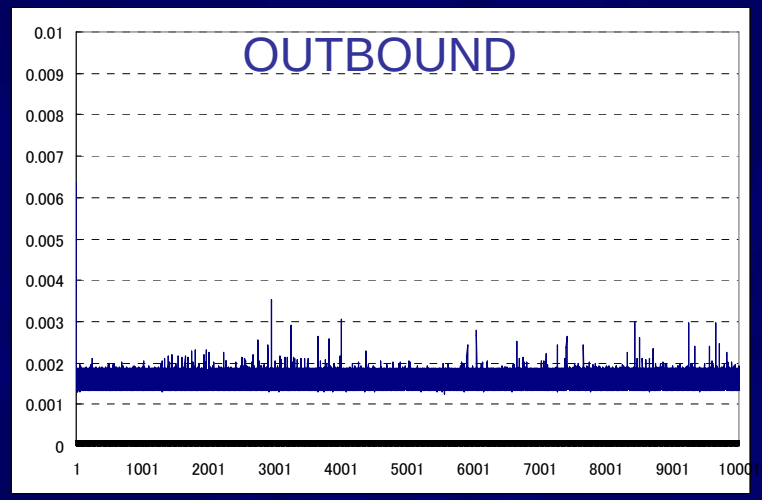
- SIP端末にはX-Liteを使用
- 音声コーデックにはG.711を使用
- 余計なトラヒックを発生させるような装置は接続しない

実験と評価

測定結果

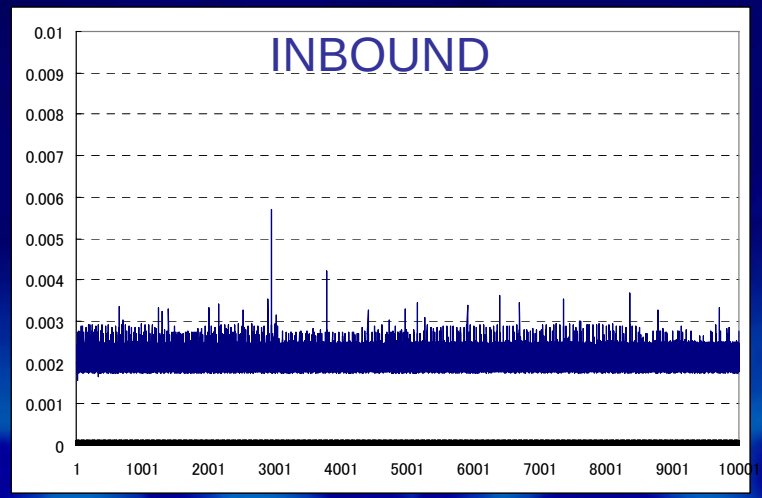
音声ストリームの方向	SoFW構成装置の処理遅延の平均
Outbound	1.641msec
Inbound	2.087msec

Number of sample packet: 10000



電話サービスとして認められる遅延は200～400msec

SoFW構成装置による処理遅延は音声通信に影響を与えない範囲



おわりに

- まとめ
  - ファイアウォールを通過できるIP電話SoFWの提案
  - SoFWを実現するための機能

音声ストリームのトンネル誘導

RATを利用した経路決定

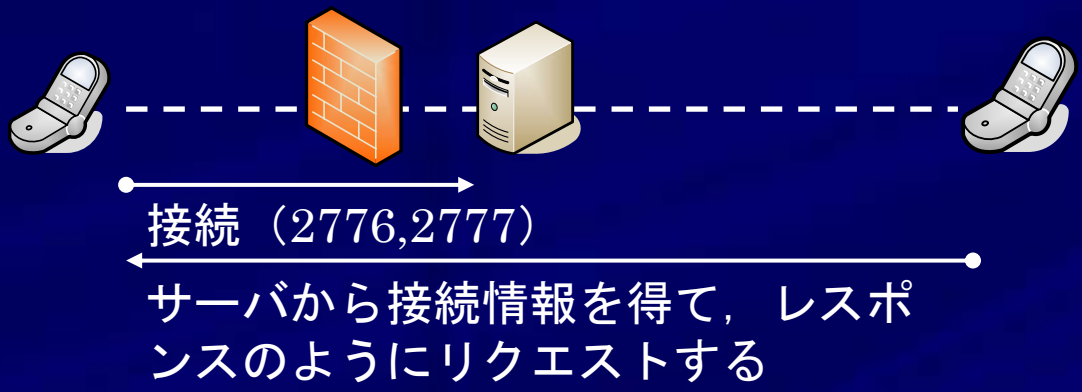
    - 容易に導入できる
    - 既存のSIP端末が利用できる
    - アドレス空間の独立性は損なわない
  - SoFW構成要素の処理遅延は音声通信に影響を与えない
- 今後について
  - パケットロス発生時のTCPの再送制御による影響の評価
  - 端末のペア数を増やした場合の性能評価

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
- IETFインターネットドラフト
  ピンホール・ファイアウォール関連

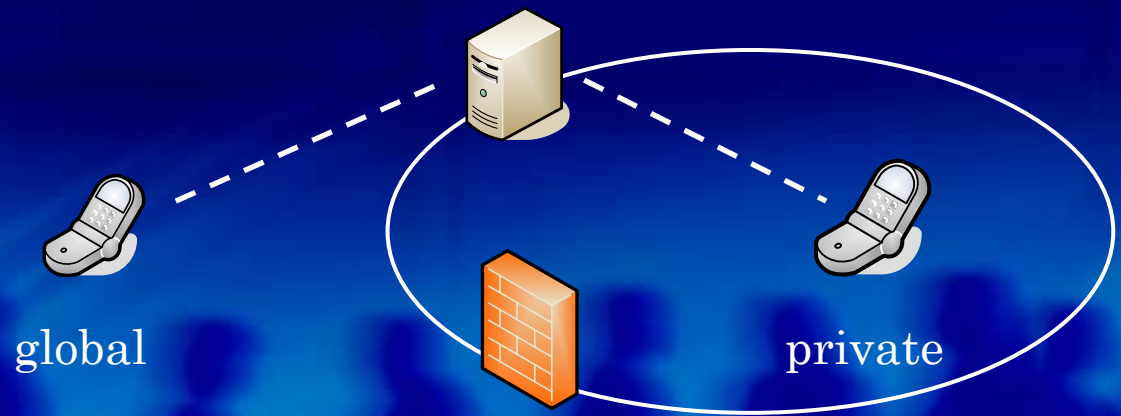
補足２．その他のFW通過システム

- IPFreedom（TANDBERG社）



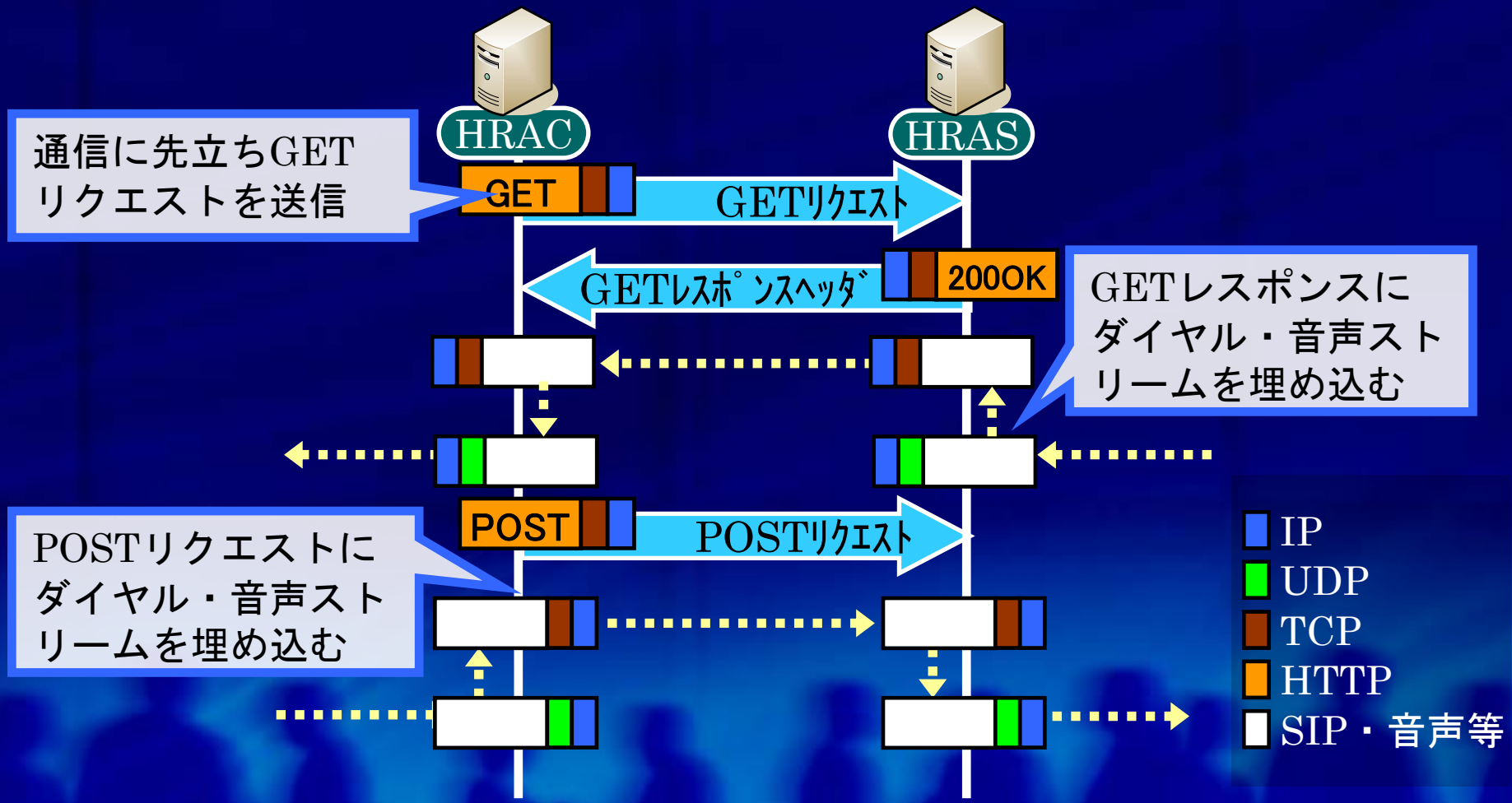
- OnDo SIPサーバ

  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

OUTBOUNDのデータはHTTPのアップデート，
INBOUNDのデータはダウンロードを利用して中継する

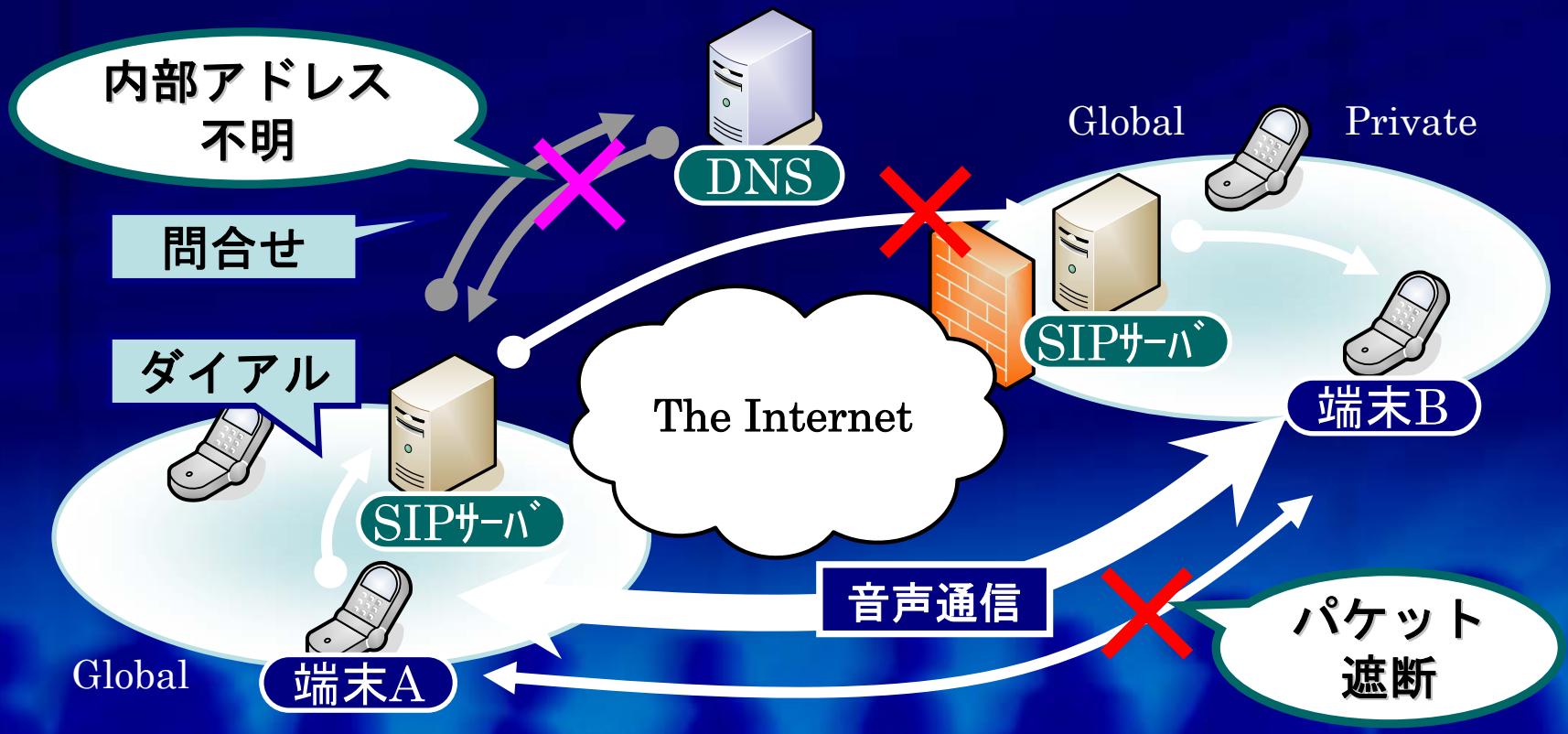


補足４．SIPとFW／NATの問題（詳細）

SIP（Session Initiation Protocol）

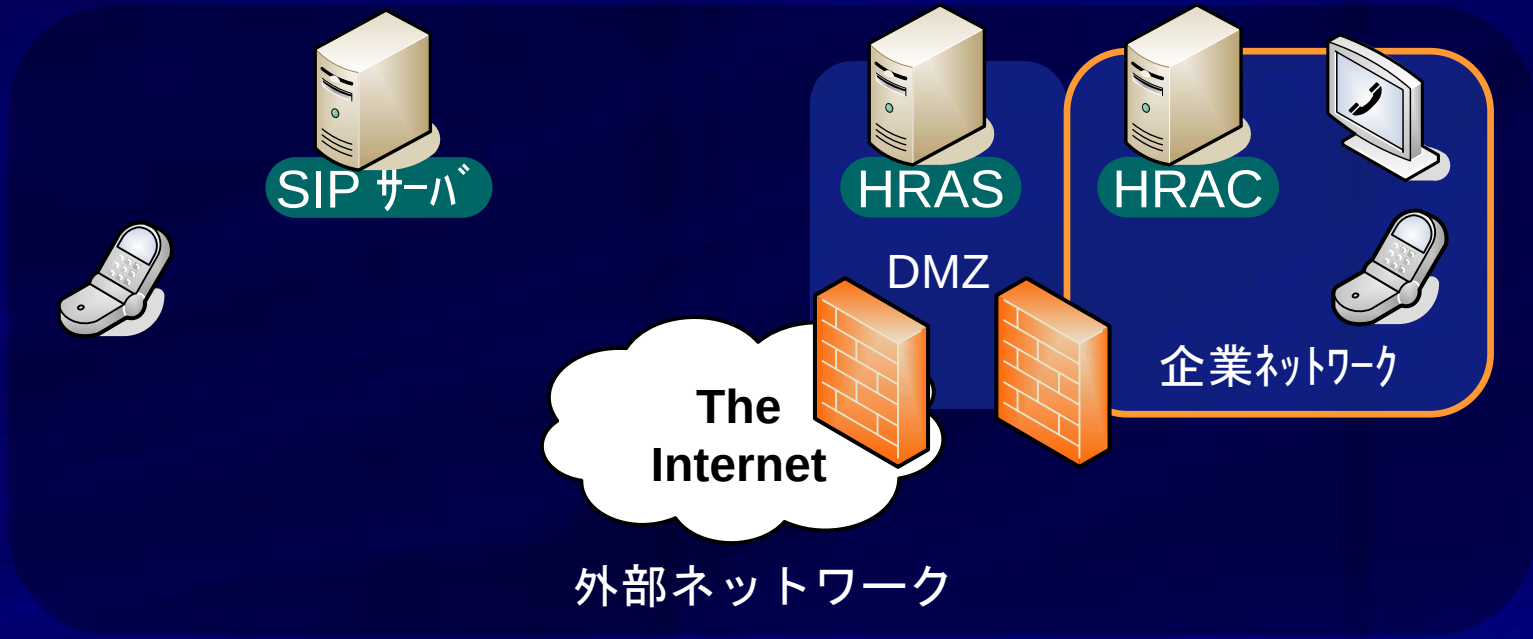
拡張性・導入の容易さから、様々なメディア通信の
セッション開始プロトコルとして期待されている

FW／NA(P)Tがあると・・・



補足5.1. HRASの設置場所 1

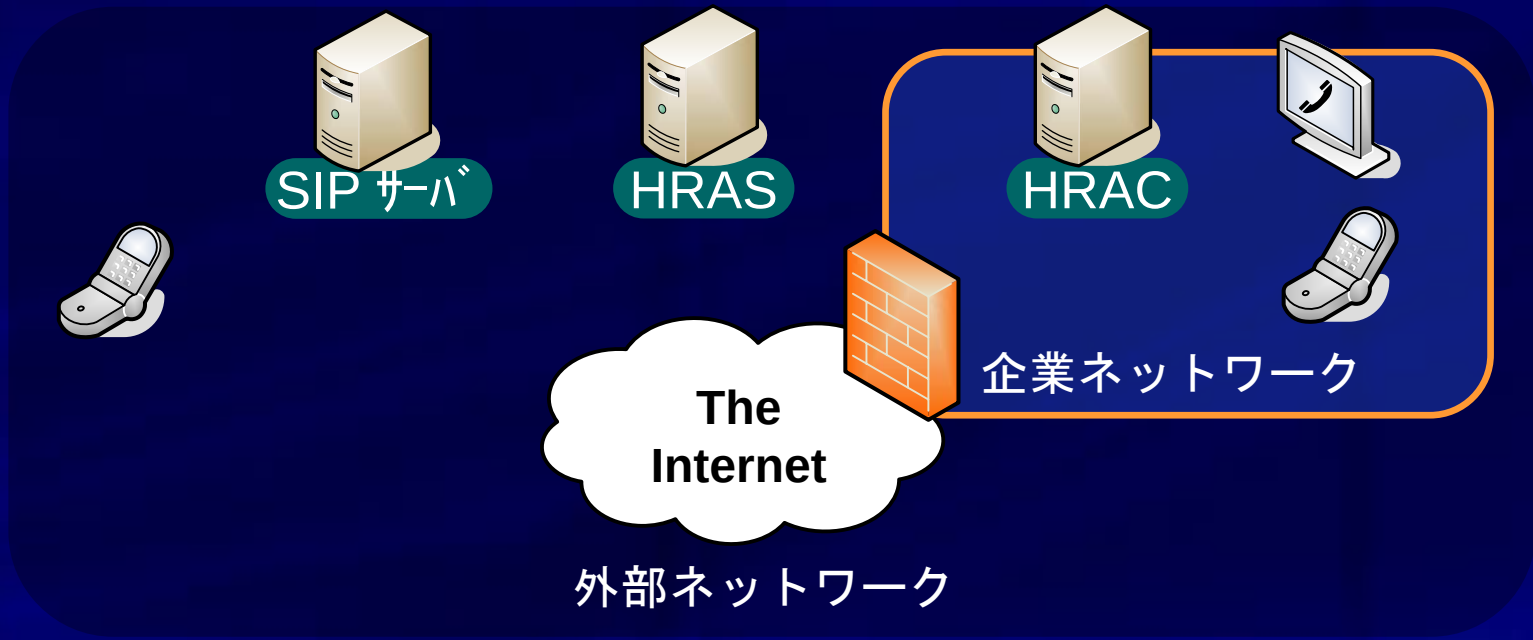
企業のDMZ



DMZと外部ネットワークの間のFWでは，HRASが利用するSIP通信とUDP通信は全て許可するように設定する.

補足5.2. HRASの設置場所２

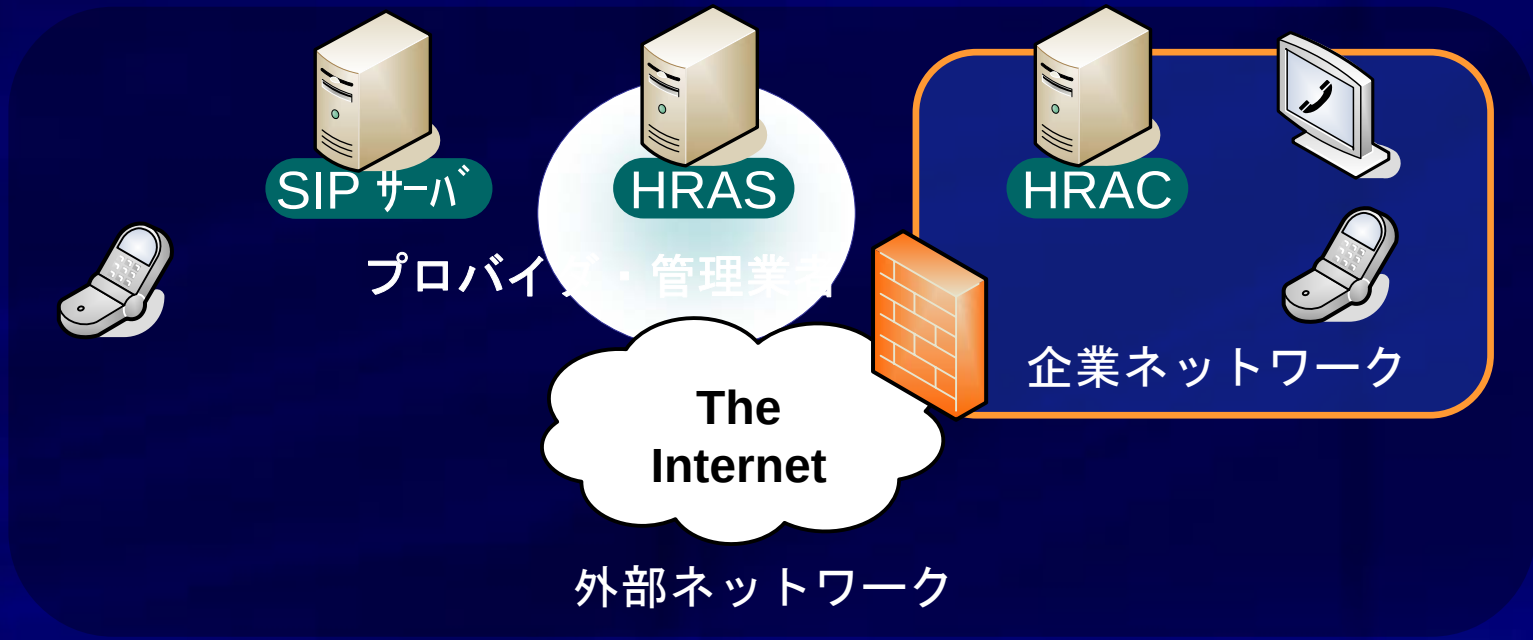
インターネット上に汎用的に公開されたもの



DMZのFWの変更が難しい場合に有効．汎用的に公開されたもの以外にも，企業がグローバルアドレスを企業ネットワークとは別に１つ用意すればよい

補足5.3. HRASの設置場所３

サービスプロバイダや管理業者による運用



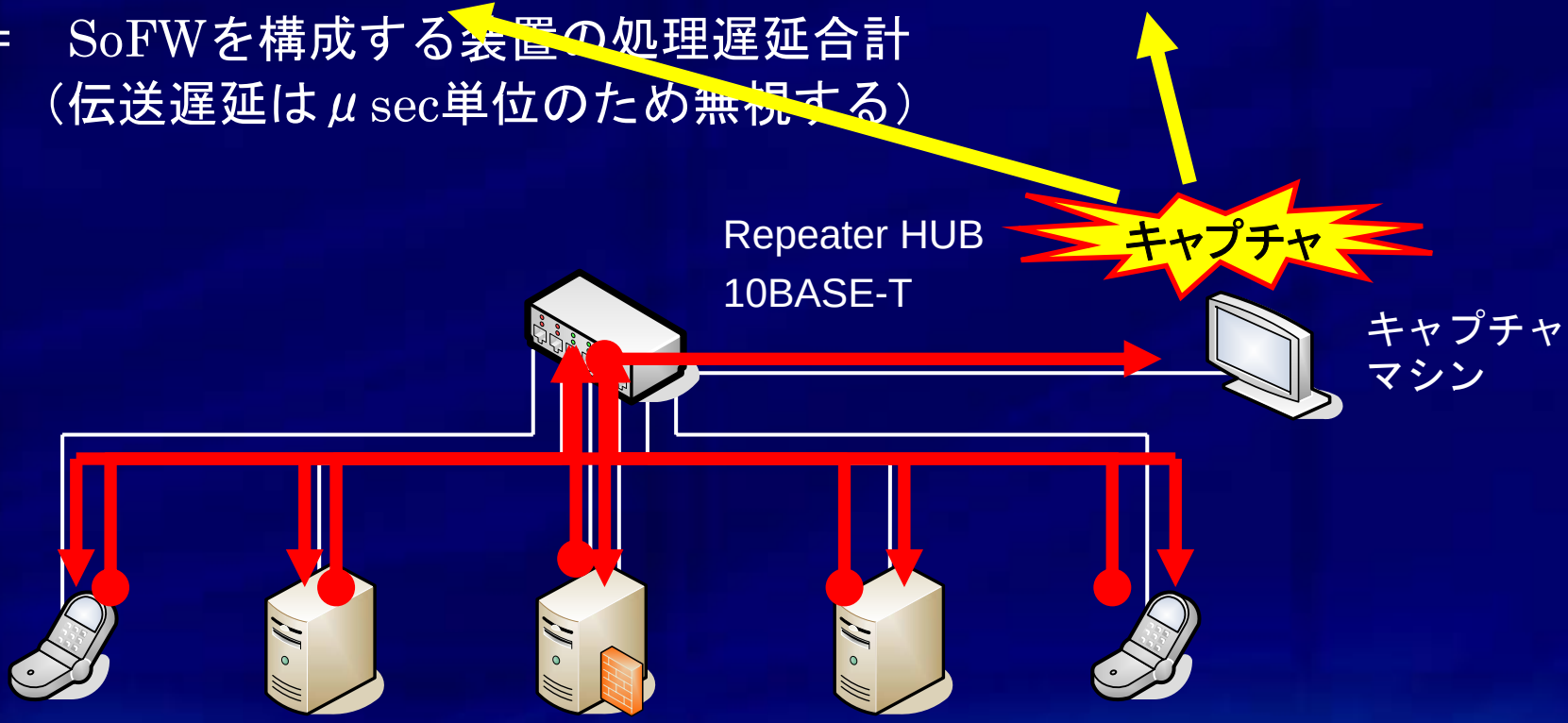
HRASの運用をプロバイダや管理業者に委託する.
企業ネットワークにはHRACを設置するだけ

補足6. 実験と評価

内部端末送信直後時間　－　外部端末受信直前時間

＝　SoFWを構成する装置の処理遅延合計

（伝送遅延はμsec単位のため無視する）



外部端末
202.11.3.10

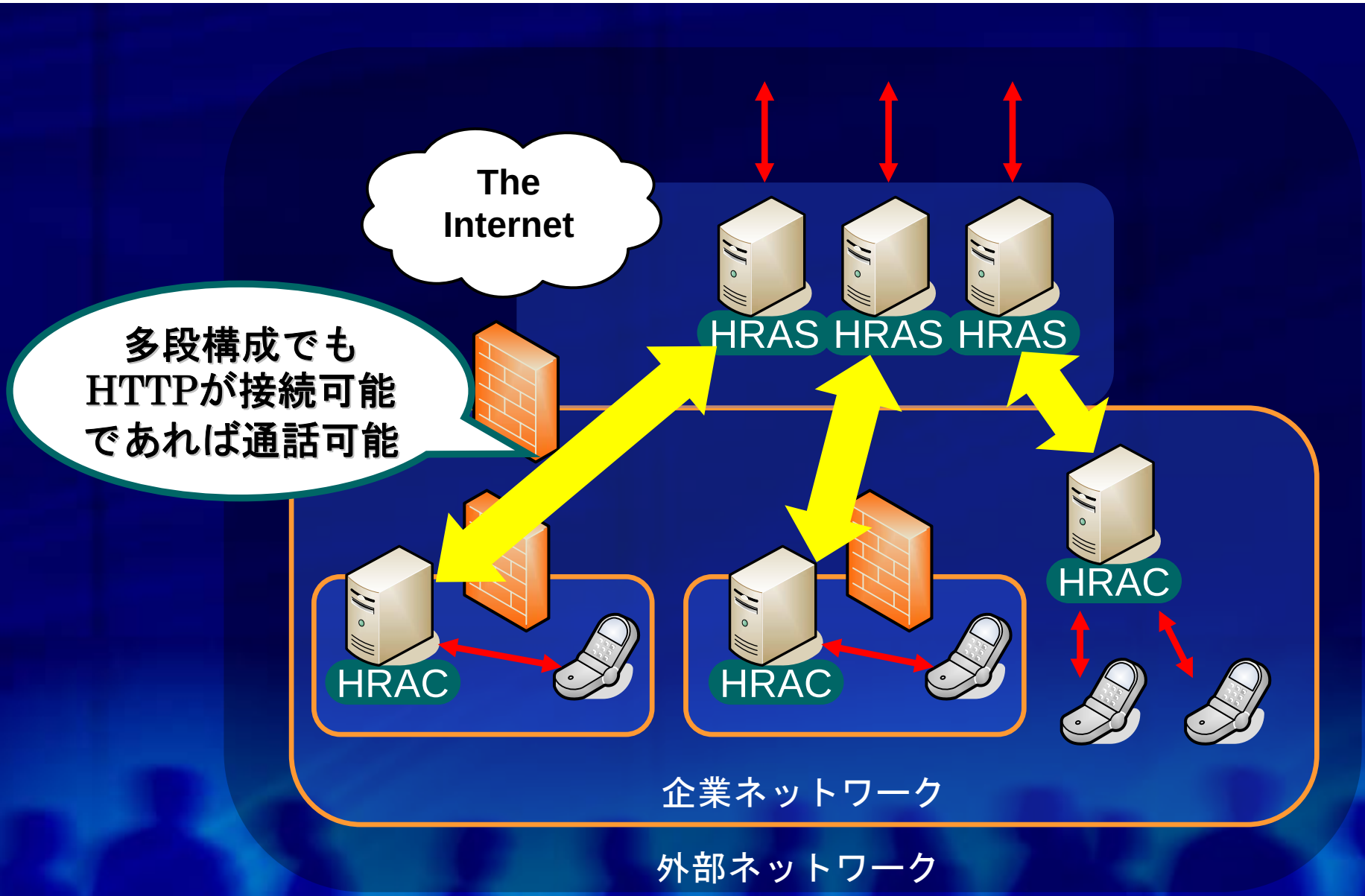
HRAS
202.11.3.11

FW/NAT/Proxy
Global
202.11.3.1
Private
172.18.0.1

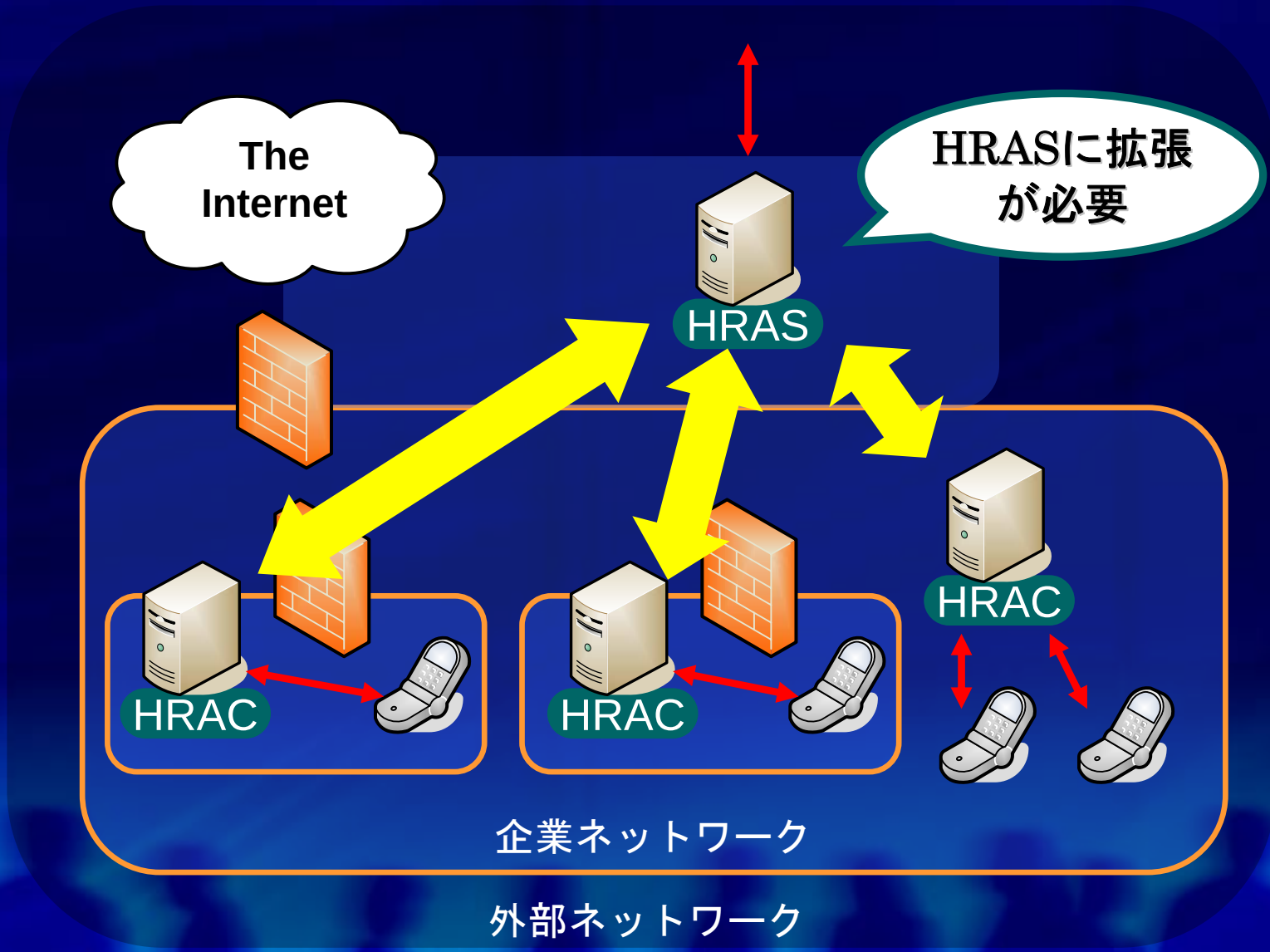
HRAC
172.18.16.72

内部端末
172.18.16.73

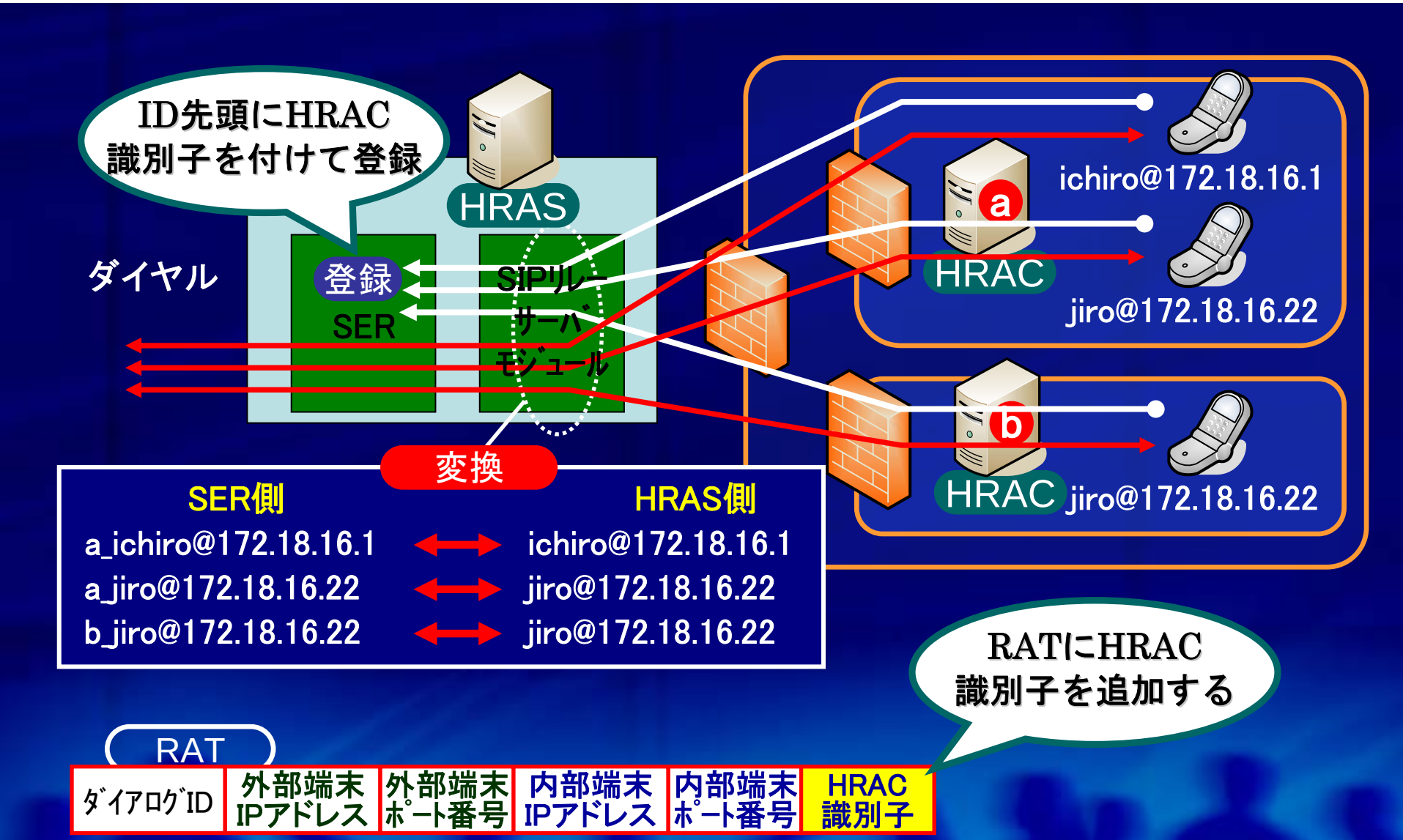
補足7.1. FW/NAT多段構成の検討



補足7.2. FW/NAT多段構成の検討

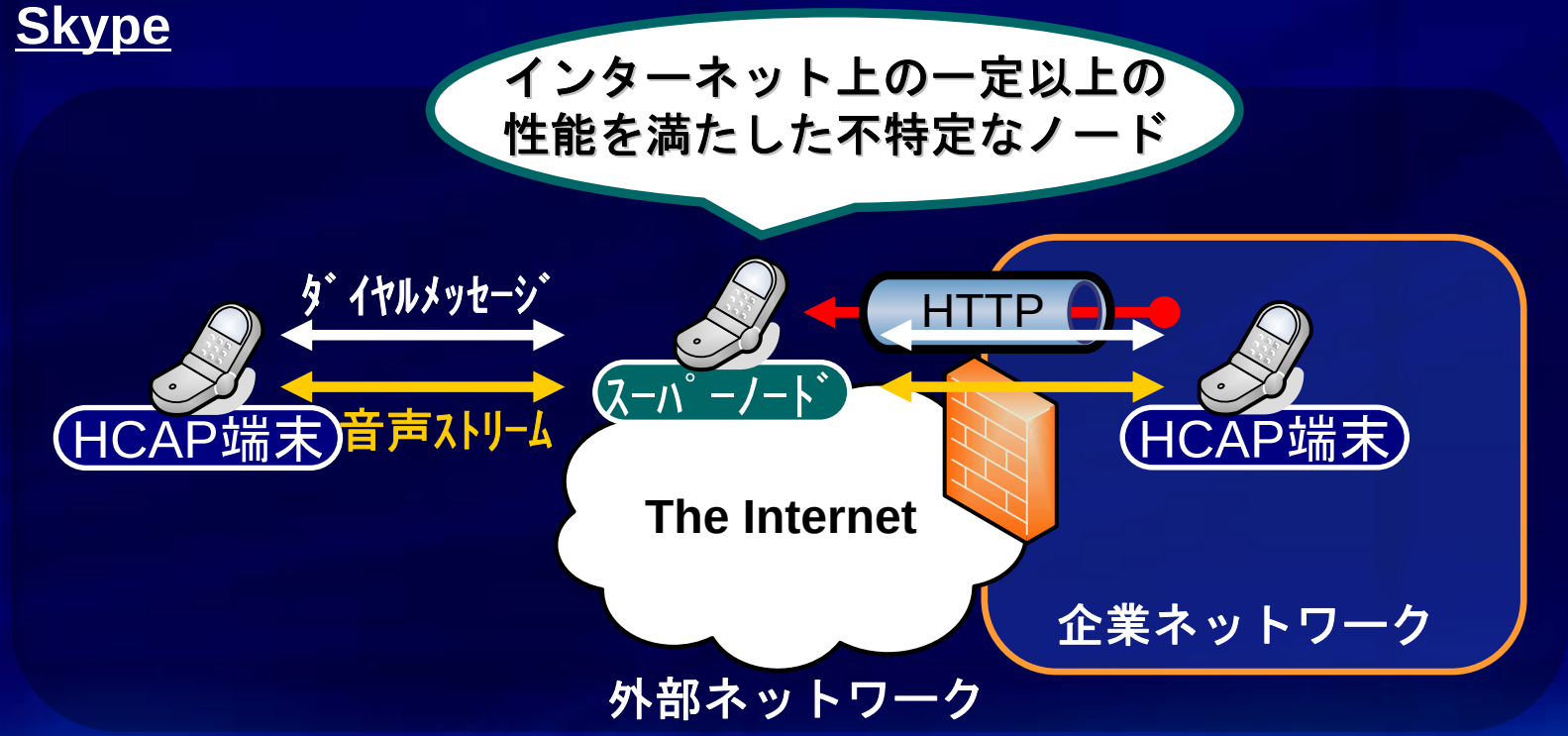


補足7.3. HRASの拡張



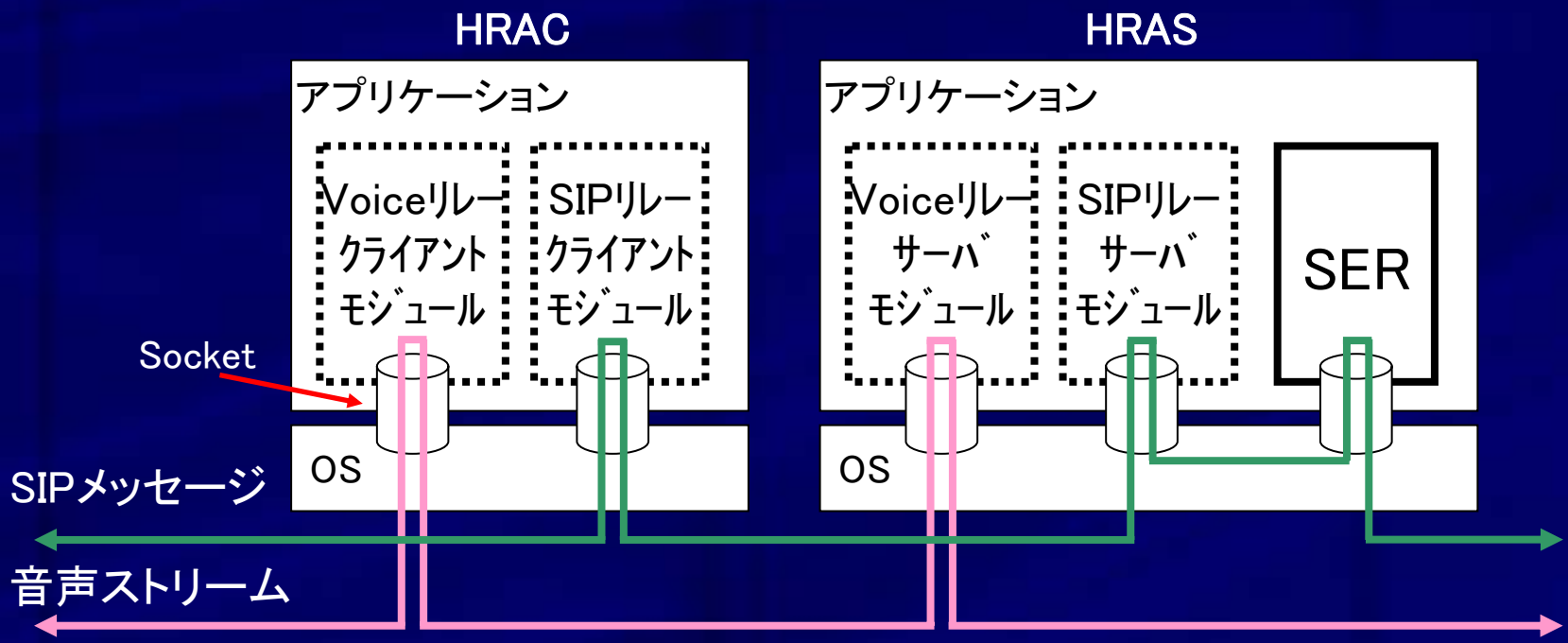
補足 8. Skype

端末と中継サーバの間にHTTPトンネルを張る方式



- インターネット上の不特定なノードの中継
  - セキュリティなど信頼性に欠けるため，それを重視する企業であれば導入を拒む

補足９．実装



- Fedora core3.0 (Linux 2.6.9)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ソフトSER(SIP Express Router) とソケットで連携することで実現する
- メモリアクセスを効率化するために並行処理にはマルチスレッドを用いる