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

040427315　若原宏太
渡邊研究室

1. はじめに

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（以下 FW）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[1]．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．そこで，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．

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空間上に HRAC（Half Relay Agent Client）を，外部のグローバルアドレス空間上に SIP サーバ機能を備えた HRAS（Half Relay Agent Server）を設置する．HRAC/HRAS 間は SIP メッセージと音声ストリームを中継するための HTTP トンネルを生成する．HRAC/HRAS はプライベート／グローバル IP アドレスのインターフェースを持つ仮想的な一つの SIP サーバとなる．SIP 端末は HRAC/HRAS を SIP サーバと見なして呼設定を行う．

SoFW では音声ストリームを HTTP トンネルに誘導するため，呼設定時に HRAS が SIP メッセージを受信すると，SIP のメッセージボディ（SDP）を書き換え，エンド端末に対して通信相手があたかも HRAC/HRAS であるように見せかける．音声通信時には誘導した音声ストリームをトンネルを経由して中継する．また，呼設定時に HRAS は内部/外部端末情報を対応させる RAT（Relay Agent Table）を生成する．そして，音声通信時はこの RAT と 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し音声ストリームの経路決定を行う．

しかし，現状の 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．

3. SoFW 拡張方式

従来の SoFW に提案方式を加えた動作を図 2 に示す．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．企業内の端末の情報を外部に隠蔽するため端末情報の登録時に，HRAC は REGISTER の SDP の IP アドレスを仮想 IP アドレス（以下 VIP）に書き換えて HRAS へ中継する．HRAS は VIP を登録する．このとき HRAC は IP アドレスと VIP を対応させる IPTT（IP address Translation Table）を生成する．

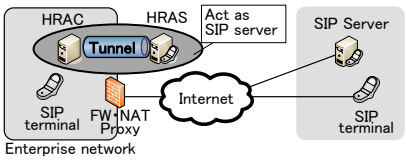


図 1.SoFW の構成

次に RAT を拡張し，従来の情報に音声通信用ポート番号を追加する．HRAS は外部宛ての SIP メッセージを受けると，音声通信時に使うポート番号を生成し，SIP メッセージに含まれるダイアログ ID と SDP に含まれる内部端末情報と共に RAT に追加する．この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 が内部宛ての SIP メッセージを受け取ると，ダイアログ ID が一致するレコードに外部端末情報を追加し，HRAC へ中継する．HRAC は SIP メッセージの VIP を IPTT から検索し元の IP アドレスに修正して，宛先端末まで SIP メッセージを中継する．

音声通信時，HRAC は外向けの音声ストリームの送信元情報を RA ヘッダに記述し，HRAS に中継する．HRAS は RA ヘッダの情報に対する外部端末情報とポート番号を RAT から検索し，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送信する．内向けの音声ストリームは HRAS が送信元情報に対する内部端末情報を RAT から検索し，RA ヘッダに記述して HRAC に中継する．HRAC は RA ヘッダの情報を宛先にし，音声データを送信する．

拡張 SoFW を実装し，その動作を確認した．

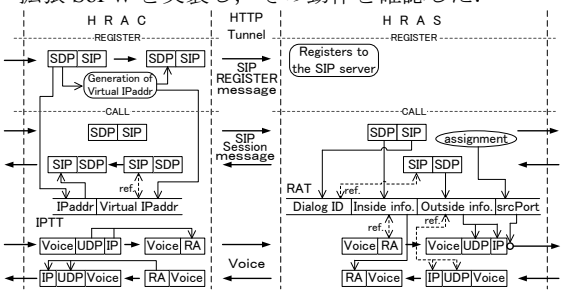


図 1.拡張した HRAC/HRAS の動作

4. 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．

参考文献

[1] 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).

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

渡邊研究室

040427315　若原 宏太

研究背景

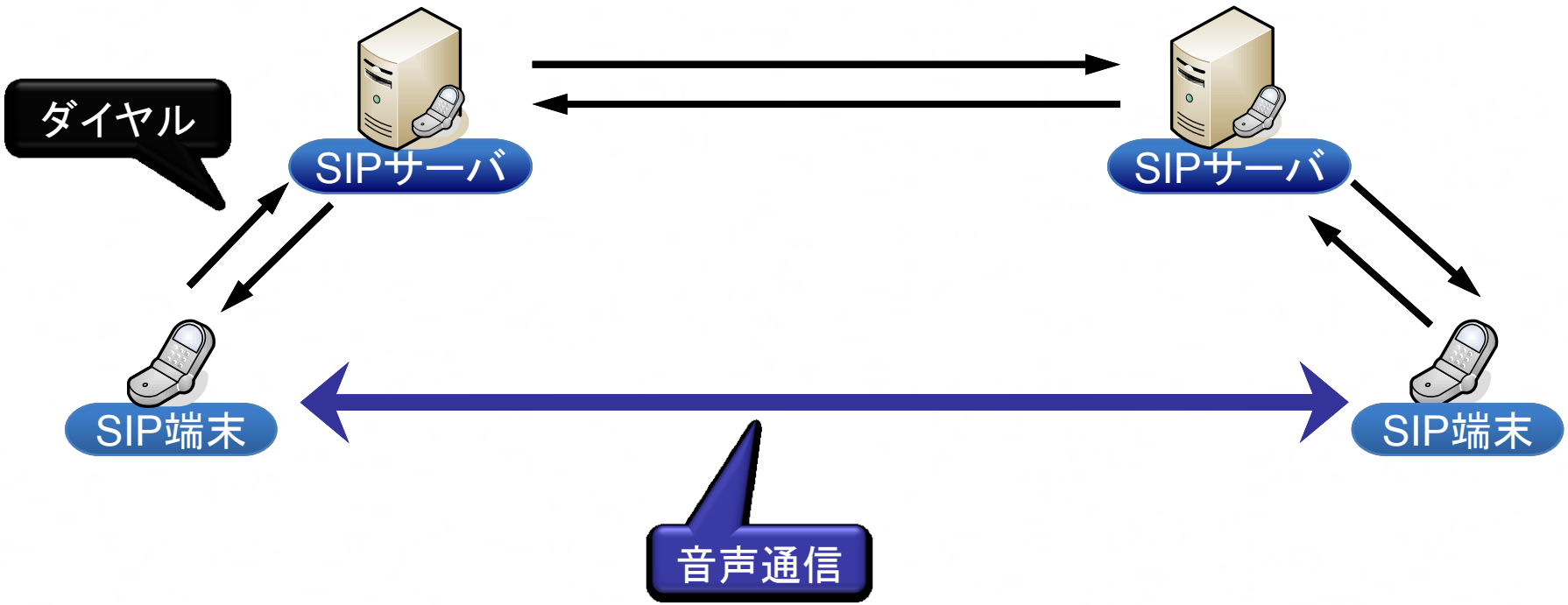
- 通信基盤の発達によるIP電話の普及
- IP電話は今後，SIP(Session Initiation Protocol)による通信が中心になる

- 企業ネットワークと外部ネットワークとの間にファイアウォール(FW)やNATが存在
  ⇒企業のFWは，企業内から外部へのWebアクセスとメールだけが許可されているためSIP/音声のパケットは遮断される.

企業ネットワークと外部ネットワークでの安全なIP電話を実現

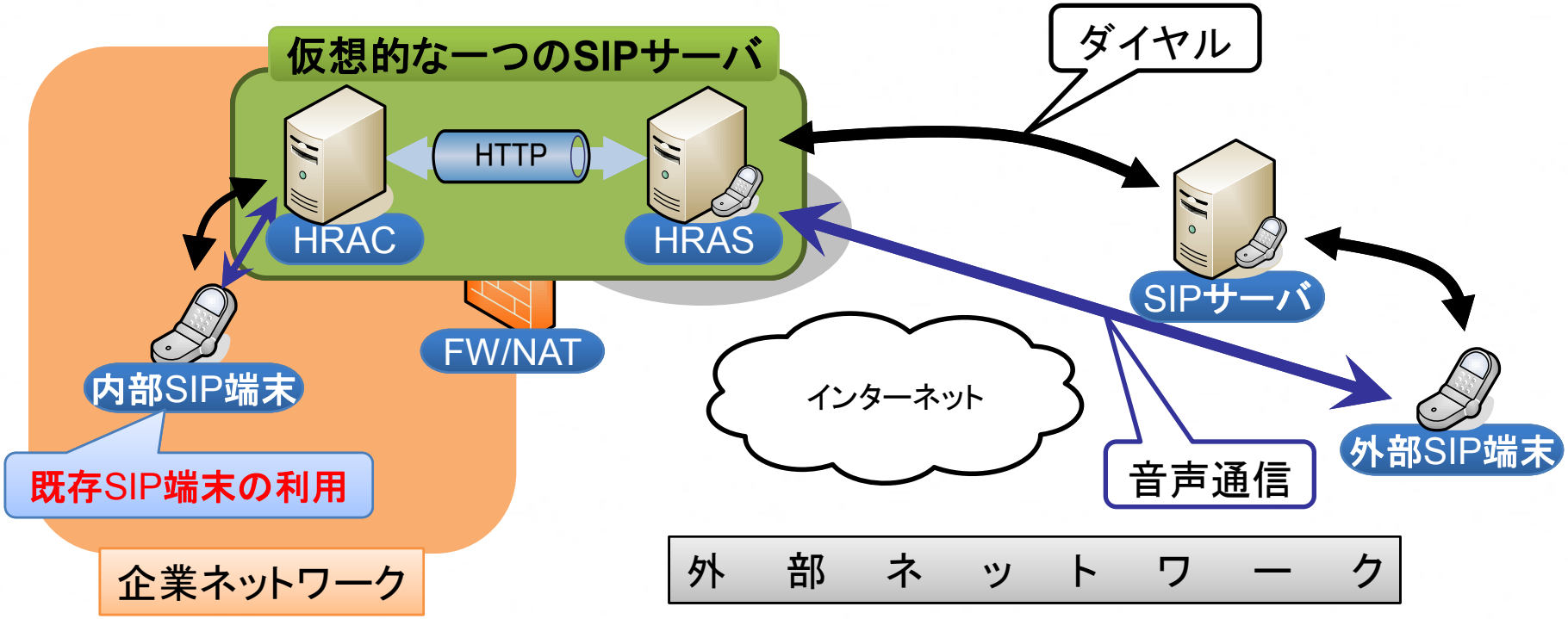
SIP(Session Initiation Protocol)による通話

- ダイヤル
  - SIPサーバを介して行う
- 音声通信
  - SIP端末がエンド - エンドで音声データを通信し合う



SoFW（SIP over FireWall）の概要

- 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トンネルを生成し，全てのSIP/音声をHTTPでカプセル化し中継する.



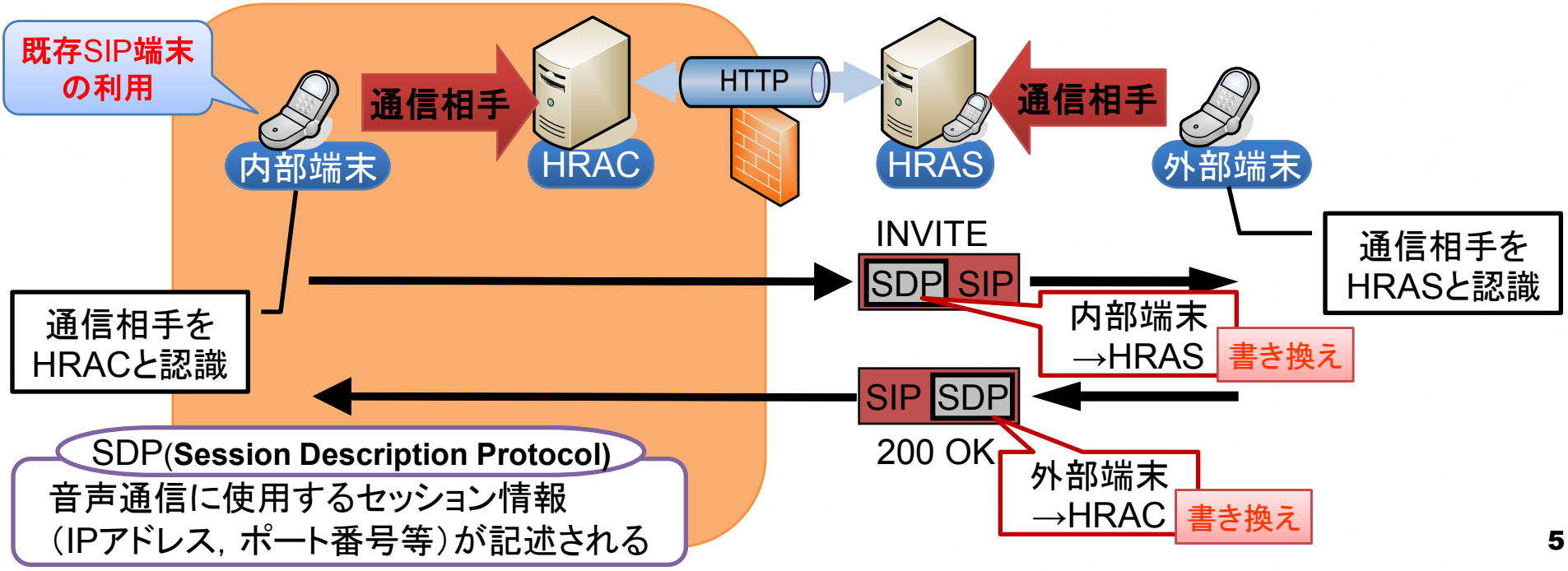
HRAC （Half Relay Agent Client）：プライベートアドレス環境上に設置
HRAS （Half Relay Agent Server)：グローバルアドレス環境上に設置・SIPサーバ機能

SoFW　トンネルへの音声データの誘導

通常のSIP端末は音声データをエンド-エンドで通信し合う

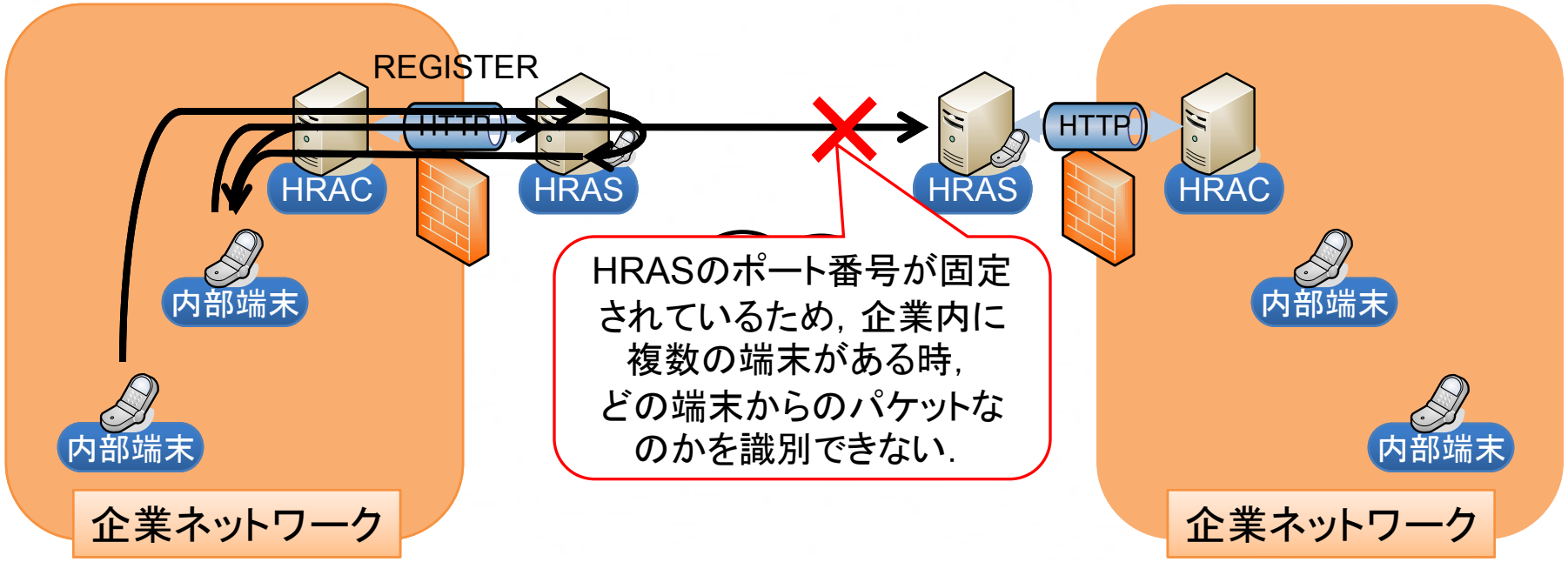
通常のSIP端末を利用して音声データをトンネルへ通すには
端末にHRAC/HRASを通信相手と認識させる必要がある

セッション情報の修正　（ダイヤル時）



SoFWの課題

- 企業内にある端末情報をFWの外部にあるHRASに，登録しなければならない
- 企業内の通話もHRASを経由する
- 異なる企業間での音声通信ができない



SoFW拡張方式の概要

HRASへの端末情報の登録は仮想アドレスで登録する

- →企業内の端末情報を外部に登録しなくてもよい

HRACにSIPサーバ機能を組み込む

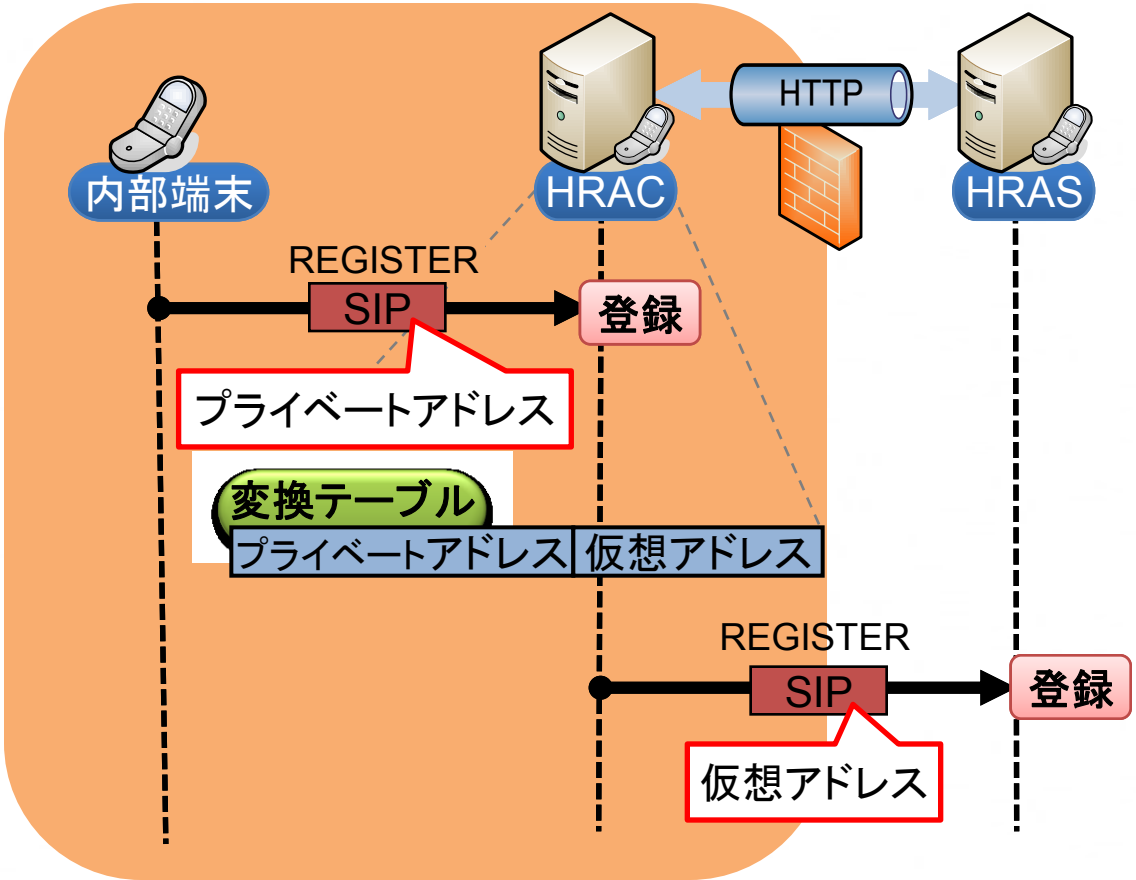
- →企業内の通信はHRACのSIPサーバを利用
  企業内通信を企業内のみで実現

HRASの音声中継時に使用するポート番号を相手端末ごとに動的に割り当てる

- →異なる企業内の端末が識別でき音声通信が可能

SoFW拡張方式 端末情報のHRAC/HRASへの登録

HRACへは通常のIPアドレス，HRASへは仮想IPアドレスに変換し端末情報を登録する．HRACではIPアドレス変換テーブルを保持する．

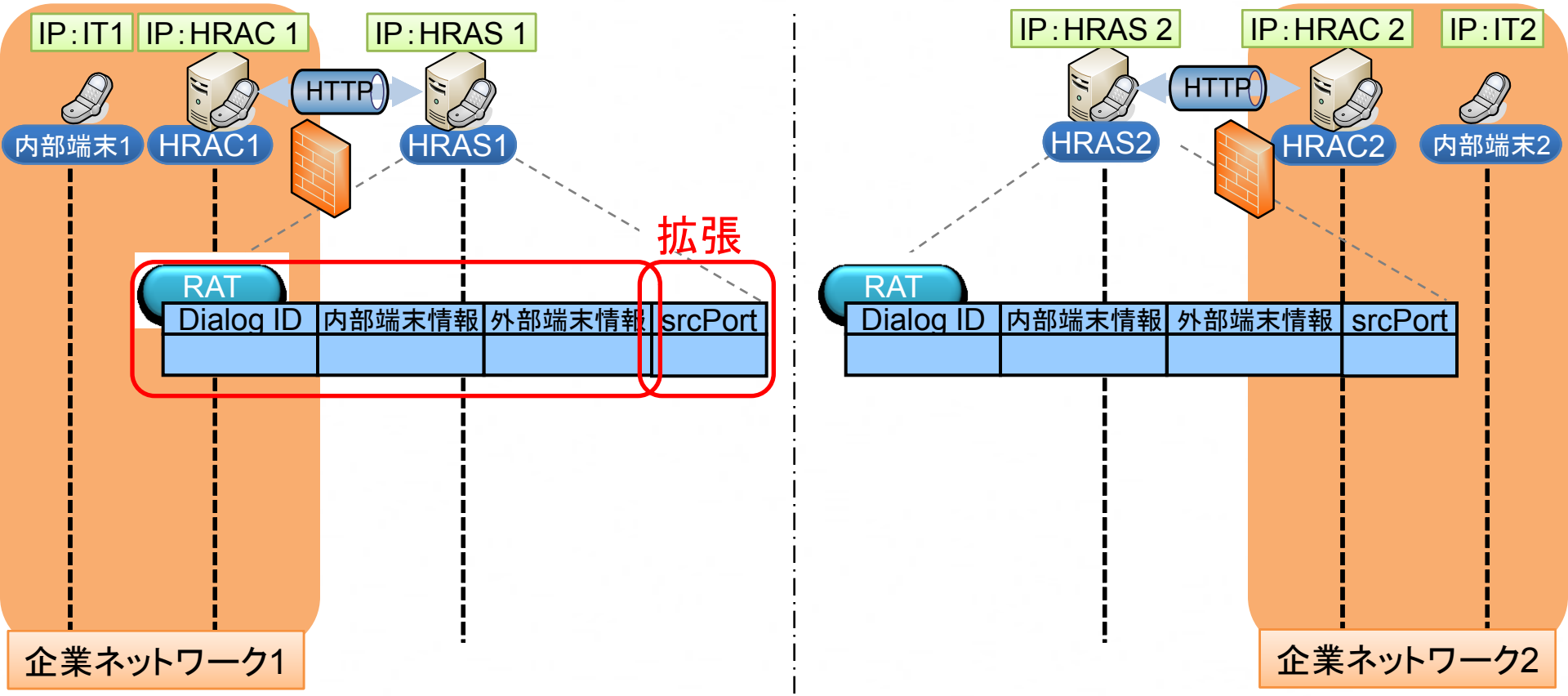


企業内の端末情報を
FWの外部に登録しない

SoFW拡張方式　異なる企業間での通信
中継テーブル(RAT)を利用した経路決定

音声データの経路決定のため，従来のSoFWから使用される
内部/外部端末情報とを対応させるHRASにあるRAT（Relay Agent Table）に，
新たに音声通信用ポート番号の情報を拡張する

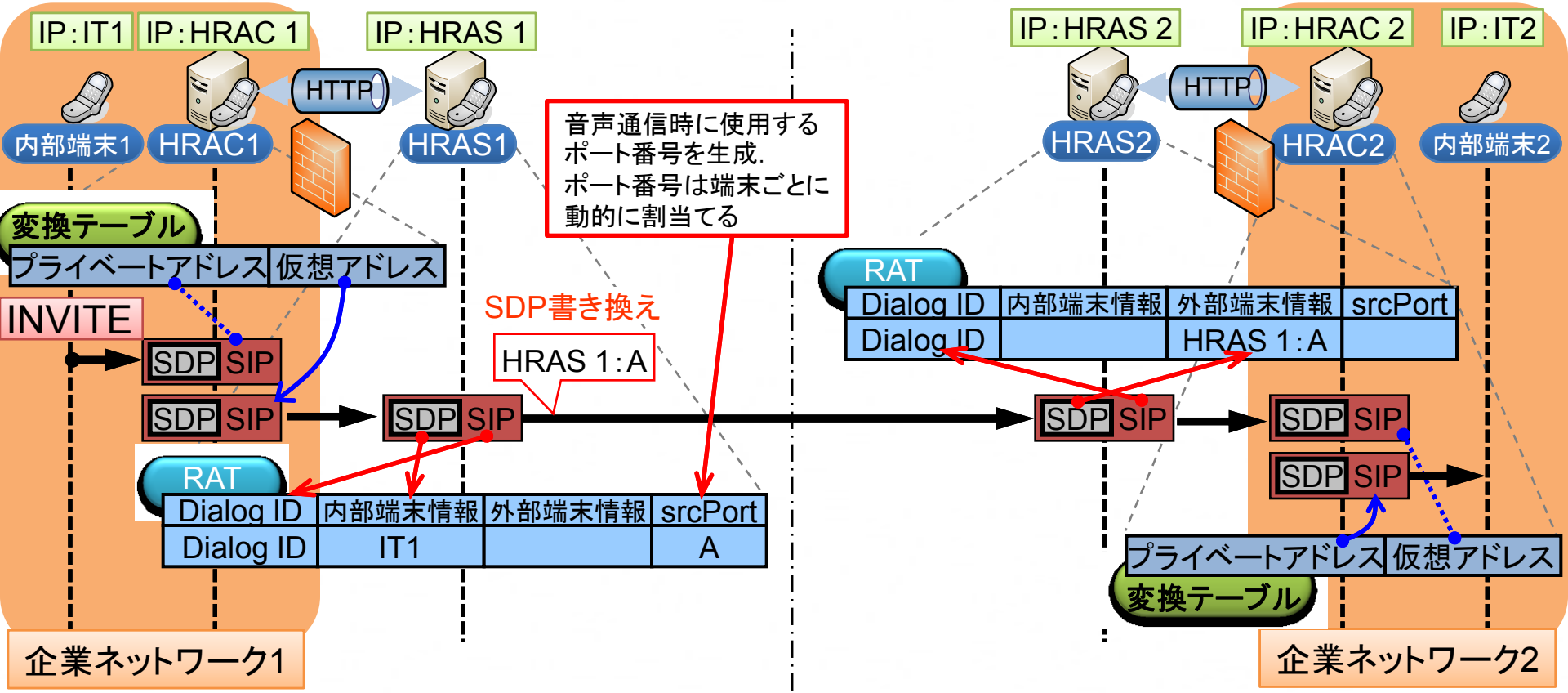
RATの生成　（ダイヤル時）



SoFW拡張方式　異なる企業間での通信 中継テーブル(RAT)を利用した経路決定

音声データの経路決定のため，従来のSoFWから使用される
内部/外部端末情報とを対応させるHRASにあるRAT（Relay Agent Table）に，
新たに音声通信用ポート番号の情報を拡張する

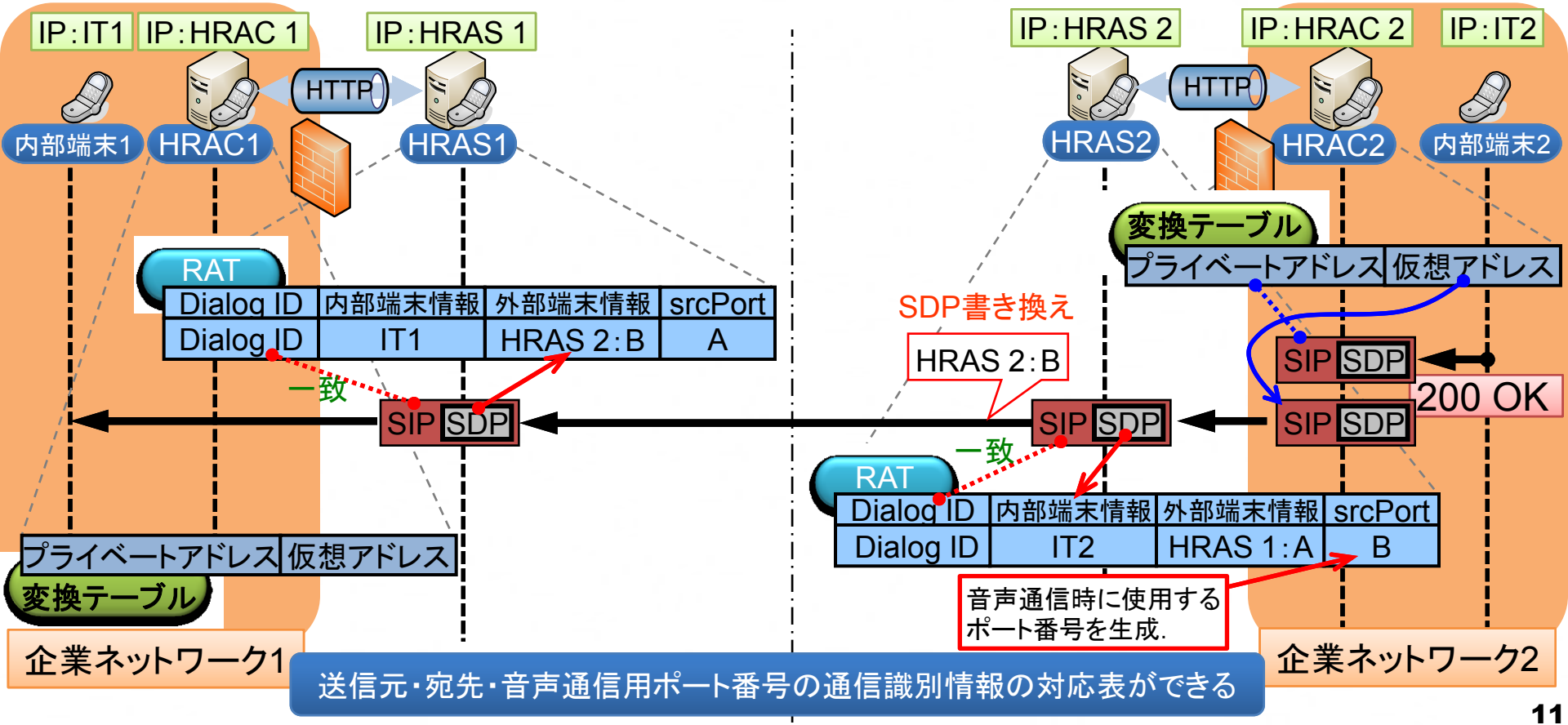
RATの生成　（ダイヤル時）



SoFW拡張方式　異なる企業間での通信 中継テーブル(RAT)を利用した経路決定

音声データの経路決定のため，従来のSoFWから使用される
内部/外部端末情報とを対応させるHRASにあるRAT（Relay Agent Table）に，
新たに音声通信用ポート番号の情報を拡張する

RATの生成　（ダイヤル時）

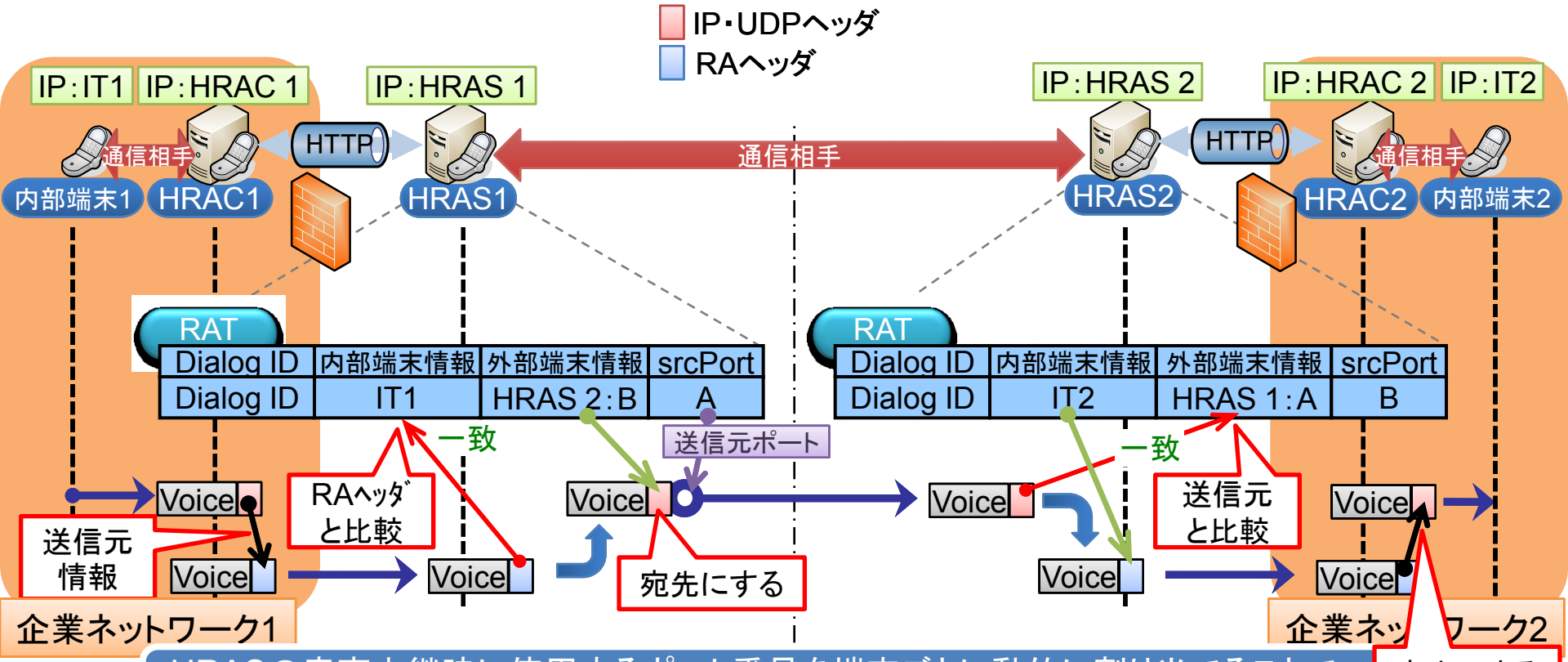


送信元・宛先・音声通信用ポート番号の通信識別情報の対応表ができる

SoFW拡張方式　異なる企業間での通信 中継テーブル(RAT)を利用した経路決定

RATの検索　（音声通信時）

従来のSoFWから使用される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



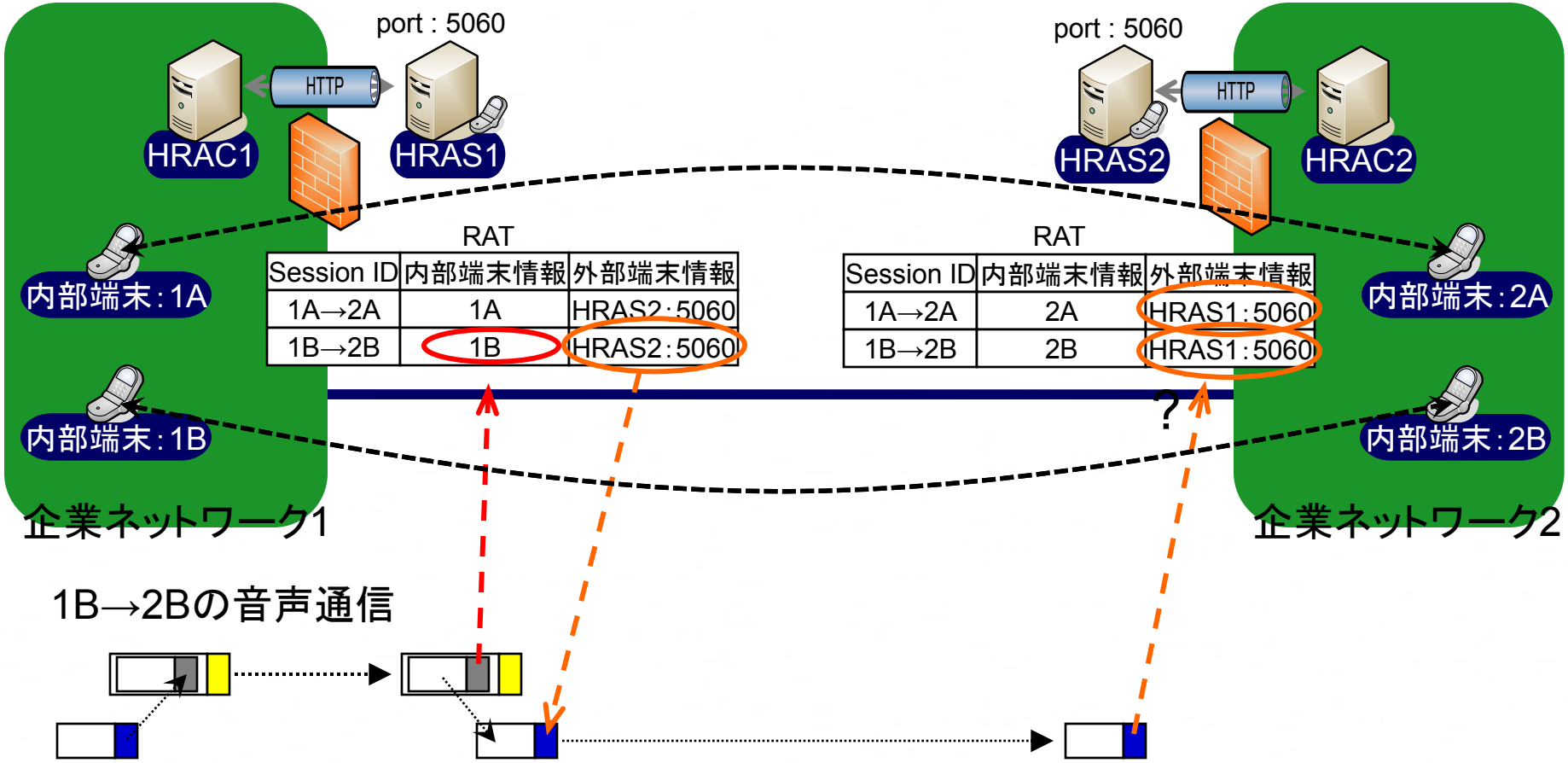
HRASの音声中継時に使用するポート番号を端末ごとに動的に割り当てることで，
送信元ポート番号から異なる企業内の複数の端末を識別することができる

異なる企業間での通話を実現

むすび

- まとめ
  - SoFWを拡張し，以下のシステムを提案
    - 異なる企業間での通話
    - 企業内の通話を，企業内だけで実現
    - 企業内の端末情報を外部に登録しない
  - 拡張SoFWを実装し，動作を確認
- 今後
  - 提案システムの評価

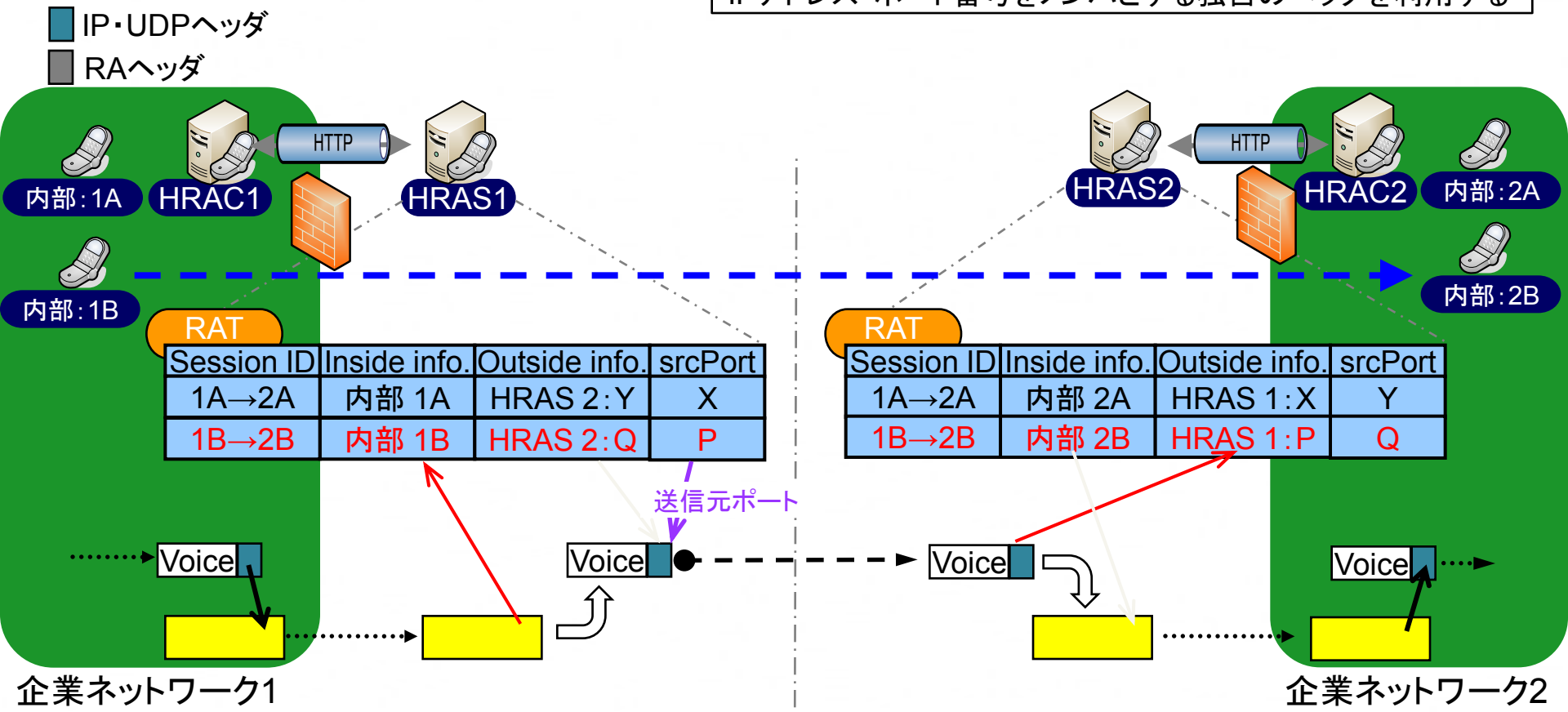
既存SoFW　異なる企業間の通信



SoFW拡張方式　異なる企業間での通信 中継テーブルを利用した経路決定

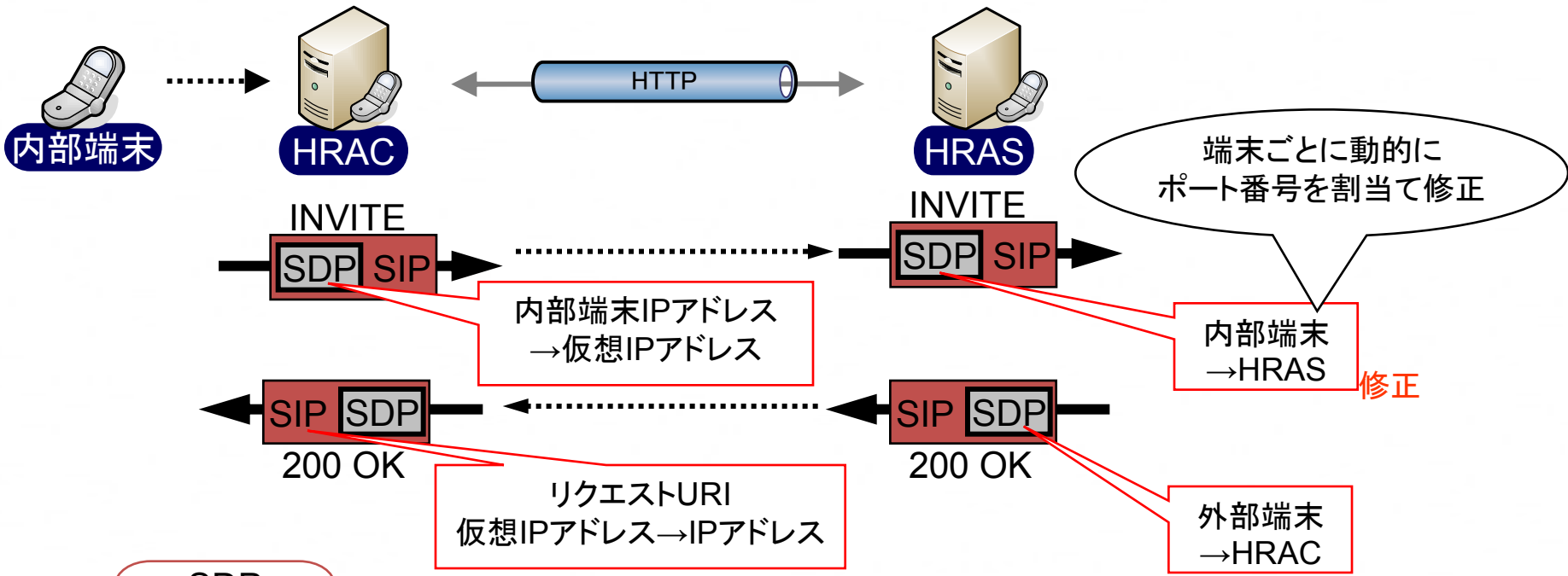
RATの検索　（音声通信時）

従来のSoFWから使用される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



SoFW拡張方式 トンネルへの音声ストリームの誘導

セッション情報の修正　（ダイヤル時）



SDP

音声通信に使用するセッション情報（IPアドレス，ポート番号等）が記述される

仮想アドレス

IPアドレス

192.168.0.1

A . B . C . D

A : 240（クラスE.「実験的」な目的に予約）
B : 0（ハッシュが衝突した場合異なる値にする）
C : 内部端末のIPアドレスハッシュ値（1～254）
D : 内部端末のユーザ名のハッシュ値（1～254）

HRAS内部のSIPサーバ機能にメッセージがプライベートアドレス・グローバルアドレス宛かでリレーモジュール・外部端末へ送信させる機能があるため，実際に使用されないIPアドレスを仮想アドレスにすることで．仮想アドレスと識別させるため．

REGISTERのヘッダ

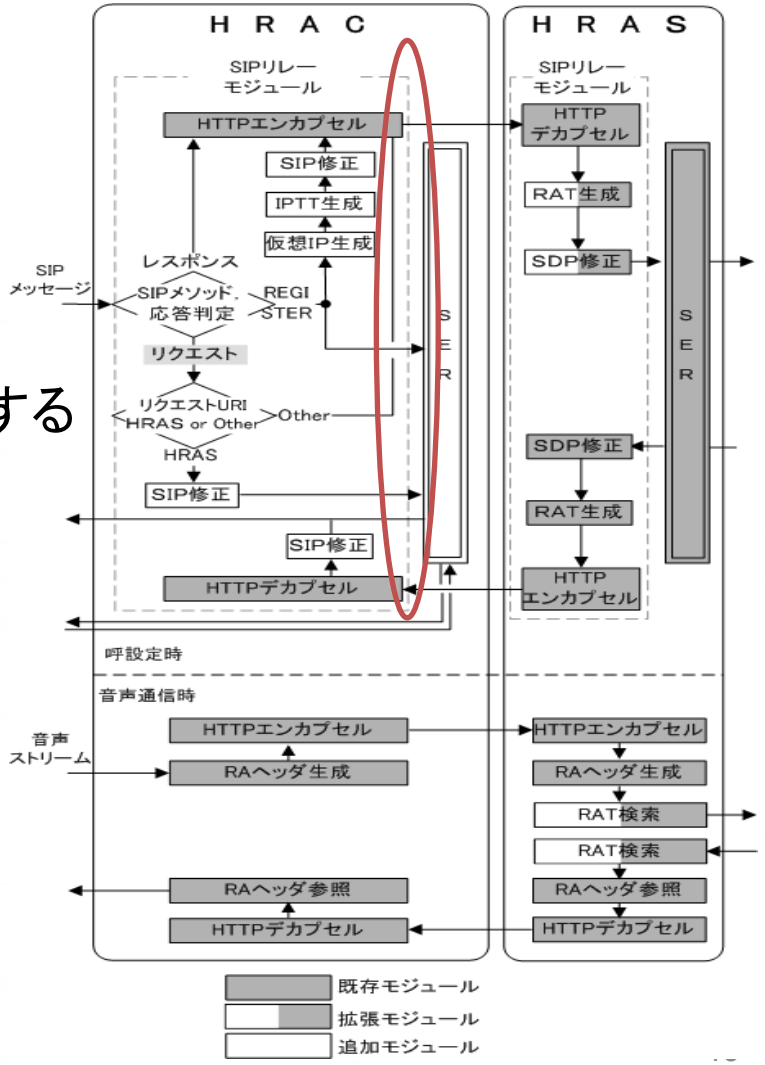
```
REGISTER sips:wata.com SIP/2.0
 Via: SIP/2.0/TLS
From: ua1 <sip:ua1@wata.com>
To: ua1 <sip:ua1@wata.com>
Call-ID: 1j9FpLxk3uxtm8tn@wata.com
CSeq: 1 REGISTER
Contact: <sips:ua1@192.168.0.1>
Content-Length: 0
```

ua1@192.168.0.1

実装

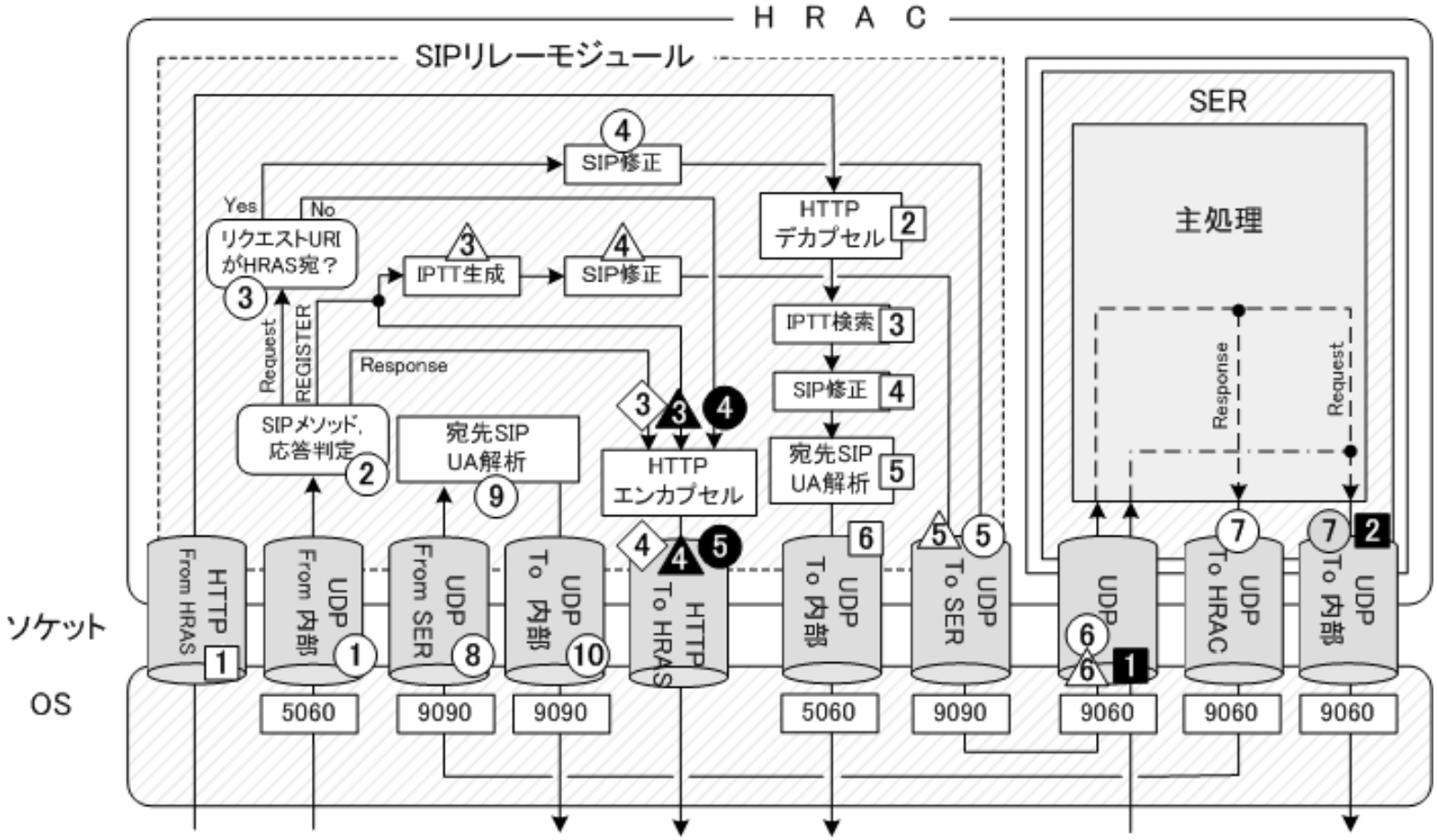
- Fedora core4.0のアプリケーションとして実装
- HRACのSIPサーバ機能はHRASと同様に

フリーのSIPサーバSERと連携することで実現する



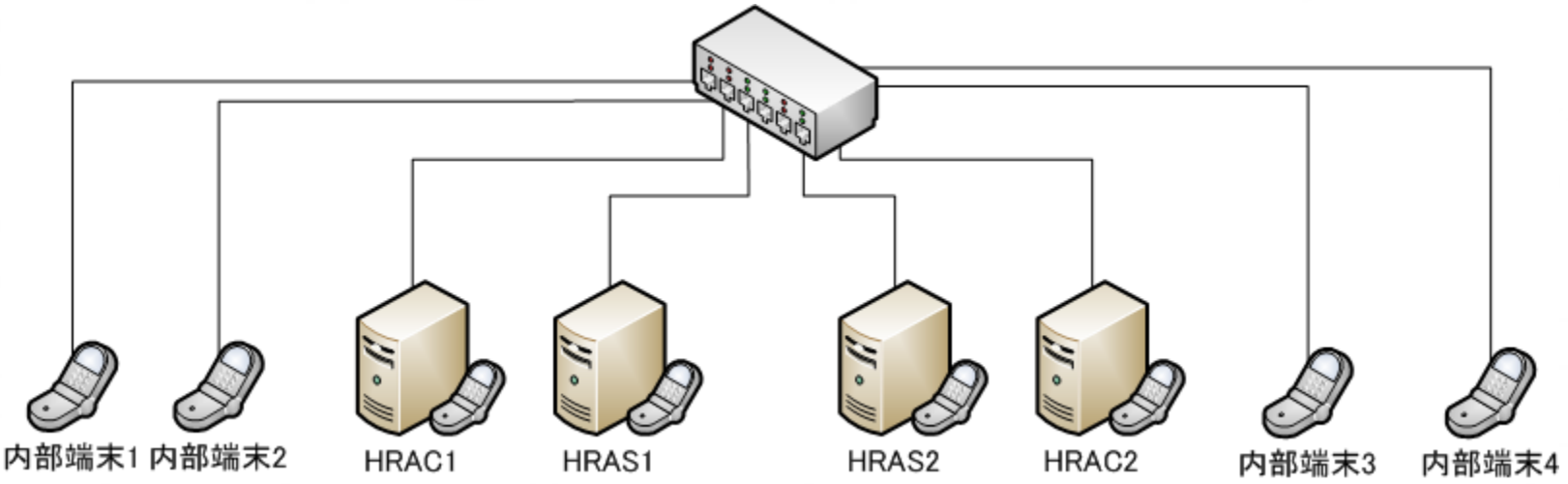
実装

SIPリレーモジュール・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



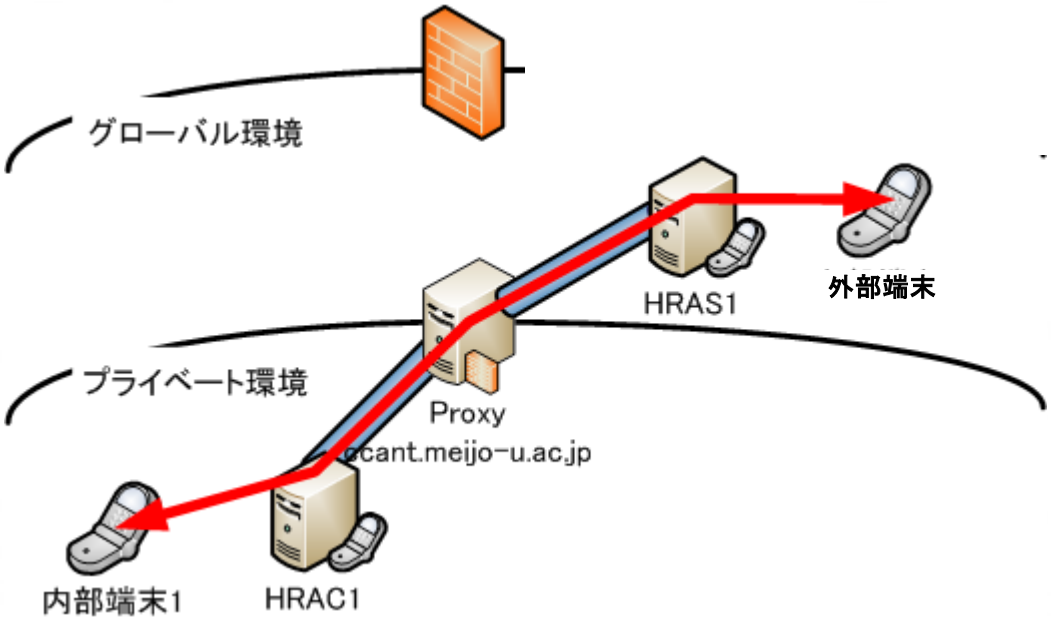
実験

- 拡張SoFWを実装
  - ローカル環境で実験し，動作を確認

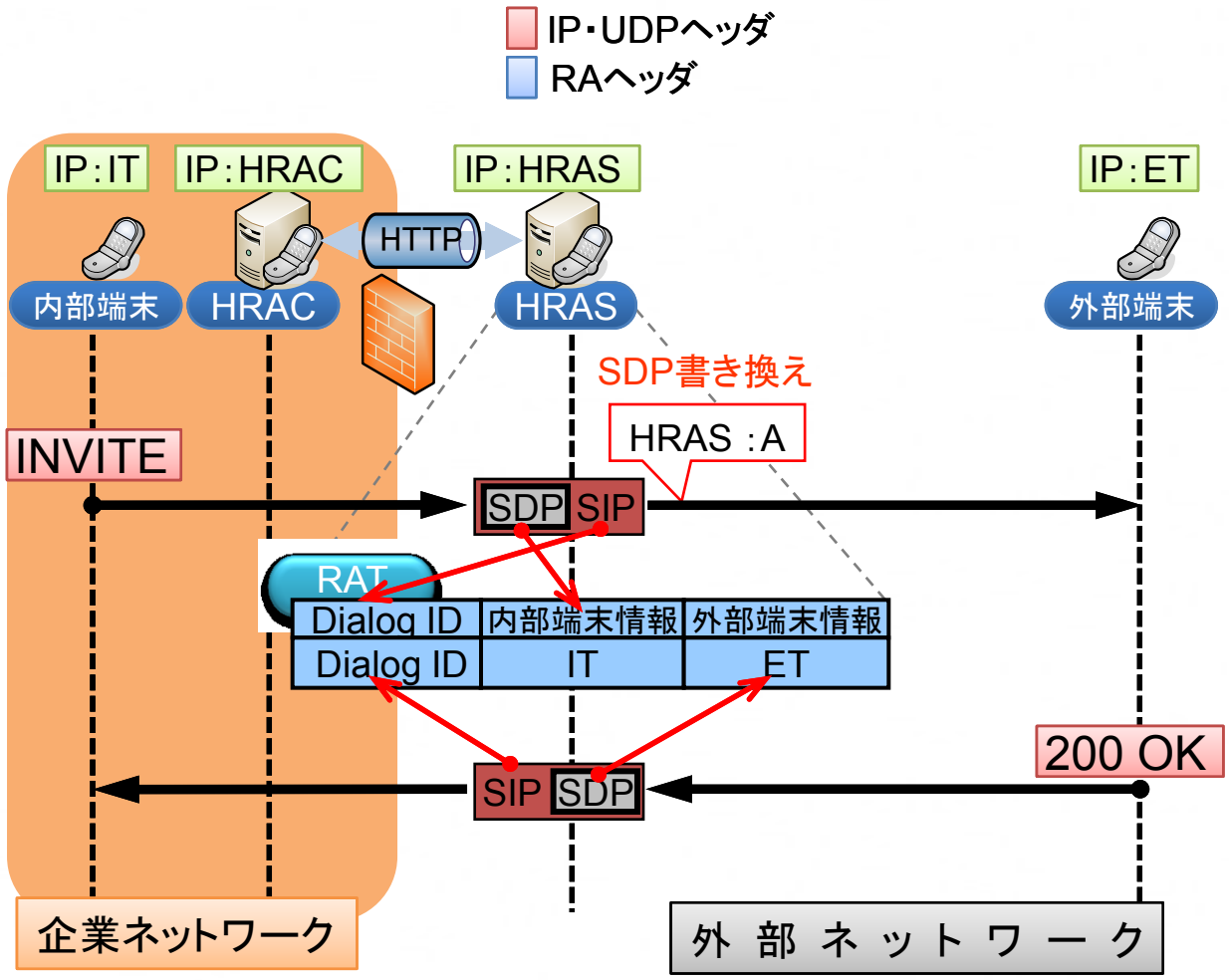


実験

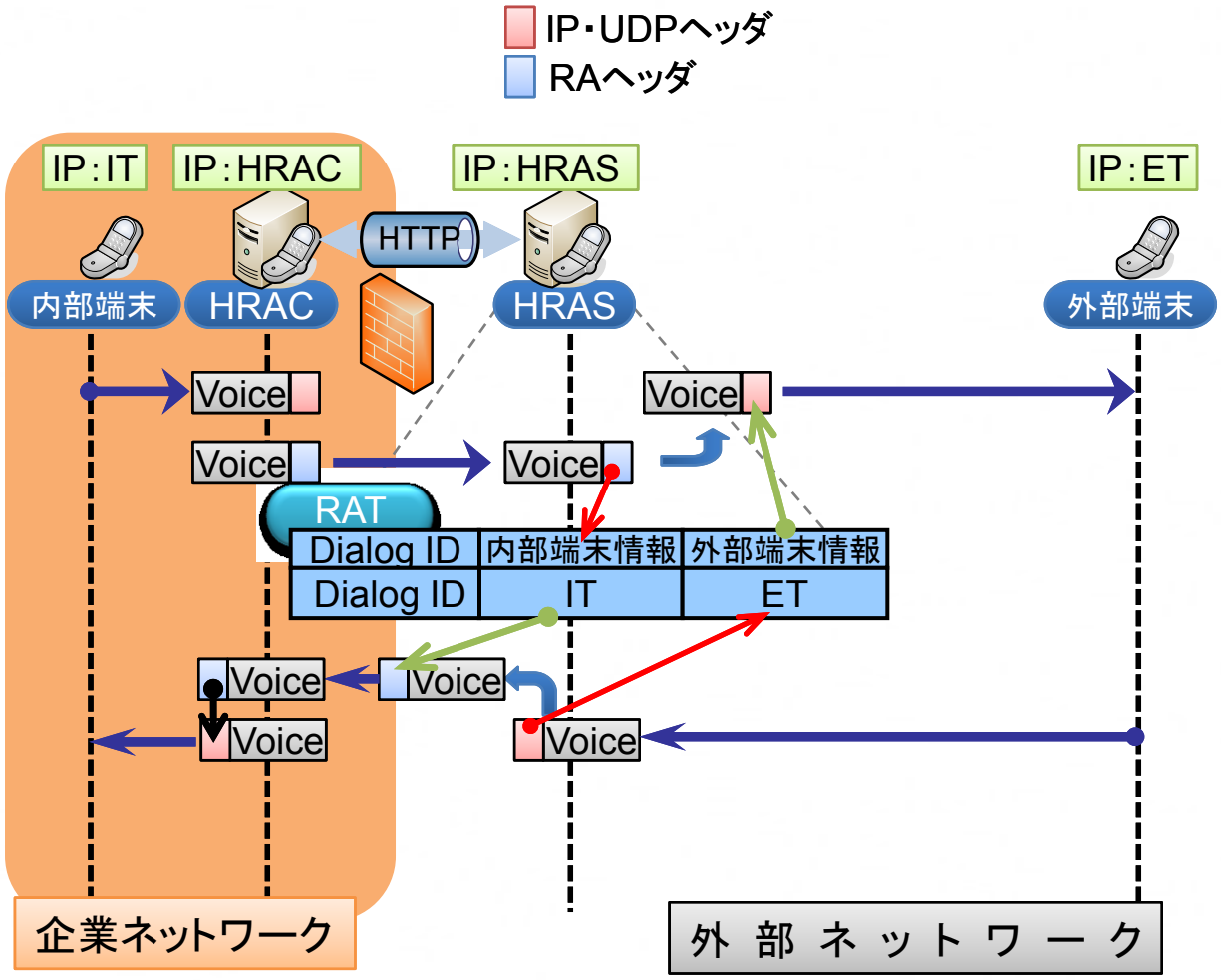
- 拡張SoFWを実装
  - 実在のプロキシを通過しての実験をし，動作を確認



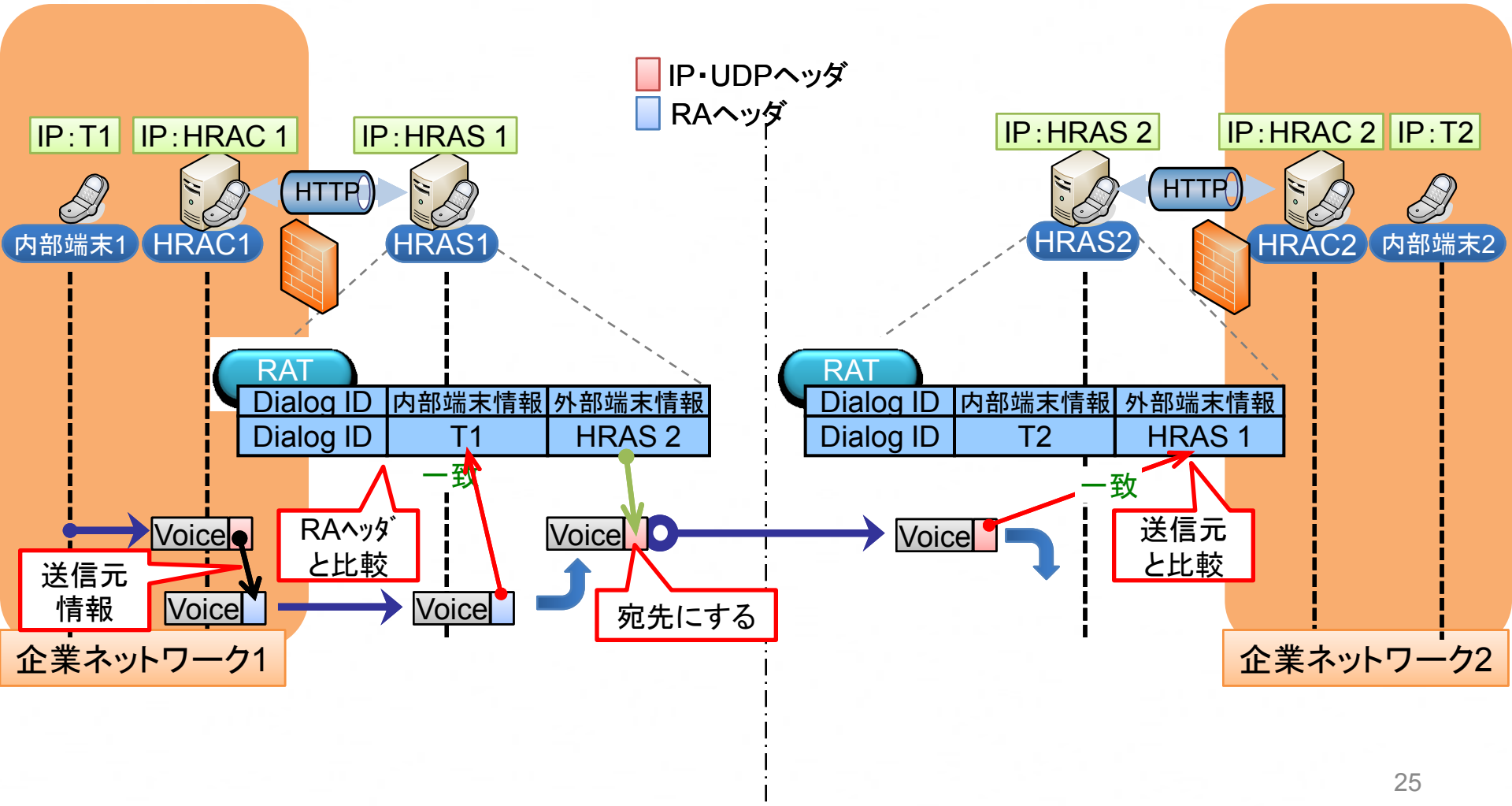
SoFW　経路決定


IP・UDPヘッダ
RAヘッダ
IP：IT
IP：HRAC
IP：HRAS
IP：ET
HTTP
内部端末
HRAC
HRAS
外部端末
SDP書き換え
HRAS ：A
INVITE
SDP
SIP
RAT
Dialog ID
内部端末情報
外部端末情報
Dialog ID
IT
ET
200 OK
SIP
SDP
企業ネットワーク
外 部 ネ ッ ト ワ ー ク

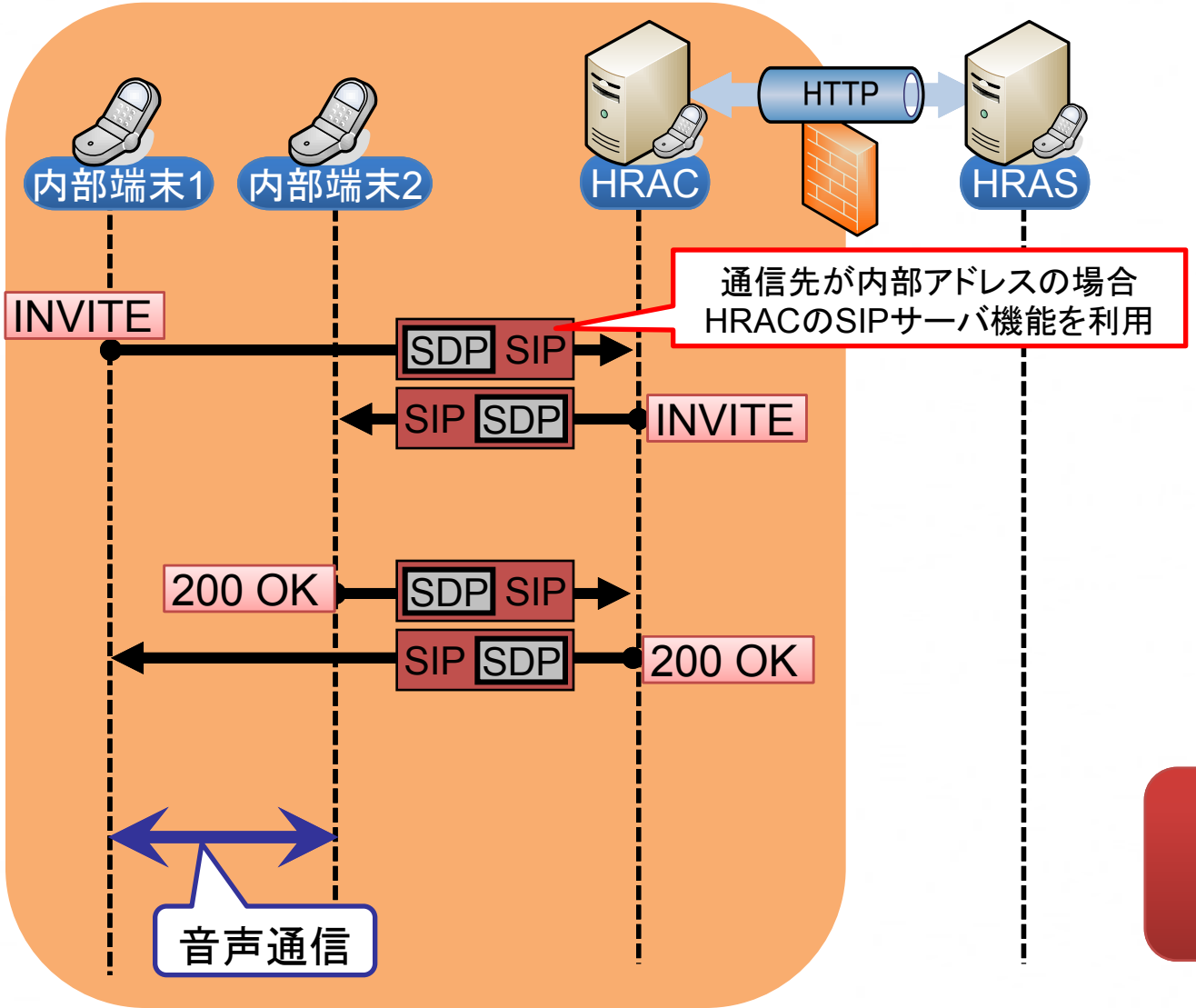
SoFW　経路決定


IP・UDPヘッダ
RAヘッダ
IP：IT
IP：HRAC
IP：HRAS
IP：ET
HTTP
内部端末
HRAC
HRAS
外部端末
Voice
Voice
Voice
Voice
RAT
Dialog ID
内部端末情報
外部端末情報
Dialog ID
IT
ET
Voice
Voice
Voice
Voice
企業ネットワーク
外 部 ネ ッ ト ワ ー ク

SoFW　経路決定


IP・UDPヘッダ
RAヘッダ
IP：T1
IP：HRAC 1
IP：HRAS 1
IP：HRAS 2
IP：HRAC 2
IP：T2
HTTP
HTTP
内部端末1
HRAC1
HRAS1
HRAS2
HRAC2
内部端末2
RAT
Dialog ID
内部端末情報
外部端末情報
Dialog ID
T1
HRAS 2
RAT
Dialog ID
内部端末情報
外部端末情報
Dialog ID
T2
HRAS 1
一致
一致
Voice
Voice
Voice
Voice
Voice
RAヘッダ
と比較
送信元
と比較
送信元
情報
宛先にする
企業ネットワーク1
企業ネットワーク2

SoFW拡張方式 企業内通話



企業内の通話を
企業内のみで実現