ファイアウォールを通過できる IP 電話の研究

伊藤　将志　　渡邊　晃

現在，IP 電話はインターネットのブロードバンド化による“低価格固定料金”，“常時接続環境”，“通信帯域の確保”によって著しい普及を遂げている．しかし，ファイアウォール・NAT・プロキシサーバなどにより外部との通信に制限のある企業ネットワークでは外部の IP 電話端末と通話を行うことはできない．この課題を解決すべくいくつかのシステムが既に実現されているが，まだ実用に耐え得るシステムは無いのが現状である．本論文ではこれらの課題を最小限に抑えられるシステムの提案と，既存技術の比較結果を報告する．

Proposal of voice over IP system passing through Firewall

MASASHI ITO　AKIRA WATANABE

In recent years,IP telephone has achieved remarkable progress with the benefit from "low priced fixed charge","always-online environment", and "high-speed communications " However, it is not easy to use IP telephone between an external terminal and a local terminal, because there are restrictions in communications due to firewalls, NAT, and proxy servers. Some systems have been proposed to solve the problem however, they are still unpractical In this paper, IP telephone passing through firewall in safey is proposed, and the the results of　the comparisons with other existing VoIP technologies are shown.

1．はじめに

近年，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されてきたため，これまで 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った．また，2002 年秋から IP 電話専用番号“050-”の事業者受付が開始となり，IP 電話が公衆回線網の電話機からのダイアルを受信することが可能になった結果，多くの ISP が IP 電話サービスを提供するようになった．

“Proposal of voice over IP system passing through Firewall”
Masashi Ito & Akira Watanabe
Graduate School of Information and Science,
Meijo University

しかし，この普及に伴い VoIP（Voice over Internet Protocol）[1]の様々な課題が浮かび上がってきた．これらの課題を発生させる要素として，セキュリティの向上を目的としたファイアウォール[2]，プライベートアドレス空間からのインターネットアクセスを可能とするための NA(P)T[3]などの存在が上げられる．そのため VoIP による外部ネットワークとの通信ができない企業ネットワークがほとんどである[5].

VoIP に関連するプロトコルとしては，早い時期に ITU-T （International Telecommunication Union – Telecommunication）によって標準化された H.323 という既存の電話仕様をベースにしたシグナリングプロトコルがある[6]．しかし，現在では IETF （Internet Engineering Task

Force）によって標準化された SIP （Session Initiation Protocol）[7]が実装も容易で拡張性に優れているとして様々なメディア通信で注目されている．現在 ISP が提供している IP 電話は多くの場合，SIP を採用している[8] [9].

しかし，SIP はダイアル開始時には相手端末の IP アドレスが特定できるか，または相手端末の情報が登録されている SIP プロキシの IP アドレスが DNS から特定できることが必須であり，NA(P)T により相手端末や SIP プロキシの IP アドレスが外部から特定できない場合には適用できない．また，企業などのファイアウォールは多くの場合，メールおよび内部から外部への Web アクセスなどに限定されており，SIP によるダイアルやその後の音声データは遮断されてしまう．このように外部との通信に制限を受けたネットワークにおいて SIP による IP 電話を導入すると，ファイアウォールの設定の変更が必要な上，セキュリティ低下にも繋がる恐れがある．

これらの課題を解決するため，NA(P)T，ファイアウォールなどによって IP 電話としての機能を制限されることなく通過するためのシステムが既にいくつか開発されている．それらの代表的なシステムに HCAP[11], Skype[12]などがある．HCAP は端末側でデータを HTTP に埋め込み外部に設置されているサーバに中継することで，ファイアウォール越えを実現するが，端末側に特殊な機能を要求することや，ファイアウォール上に無駄なトラフィックが流れるなどの課題がある．Skype は 80 番ポートを利用して外部のサーバに接続することでファイアウォールを越えるが，独自のアプリケーションで 80 番ポートを利用しているため HTTP プロキシサーバなどが介在すると通過できない．また，VoIP に限らずプロトコルフリーでファイアウォールの通過を可能とした SoftEther[13]がある．SoftEther はファイアウォールの内部または外部に仮想 LAN カード機能を導入した端末と，外部に仮想 HUB 機能を導入した端末を用意する．仮想 LAN カードはデータを仮想的なイーサネット・フレームごとに HTTPS に埋め込み，仮想 HUB でそのパケットを中継し，宛先端末の仮想 LAN カードによってデータを取り出すことができる．しかし，この方式では本来ファイアウォール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可能性がある．

本稿では， SIP をベースとし，プライベートアドレスネットワークの内部と外部にリレーエージェントを配置し，その２台の間の通信を HTTP でトンネルし，端末からの通信を中継することで，従来の SIP ネットワーク，ファイアウォールシステムに全く影響を与えない IP 電話方式を提案する．

2. 既存の対応技術とその課題

ファイアウォール／NAT 越えができる代表的な既存技術として HCAP, SoftEther の２つをあげ，その課題を整理する．SoftEther については仮想ネットワーク上に VoIP を導入した場合を想定する．

（1）HCAP

HCAP では図１のように外部に中継サーバが設置され，内部には HCAP 対応機能を内蔵した端末が設置される．セッションを確立するには，まず端末から予め中継サーバへ HTTP で接続を確立し GET メソッドを送信しておく．その後は HTTP の接続を維持し，ダイアルが開始するまで待機する．ダイアルや音声ストリームは，中継サーバから端末へは GET に対するレスポンス，端末から中継サーバへは POST メソッドに埋め込むことでデータの中継を行う．このような方式で外部の Web サイトを観覧することのできる環境であれば，ファイアウォール，NA(P)T を通過することができる． しかし，HCAP では音声端末側にそれぞれ専用のプロトコルをインストールする必要がある．また，ファイアウォールの DMZ 上に HTTP 中継サーバという特殊なサーバを配置し，そこへファイアウォール内の複数の専用音声端末から常時

HTTP による接続が行われているため，ファイアウォール上に不要なトラヒック流がれるという課題がある．

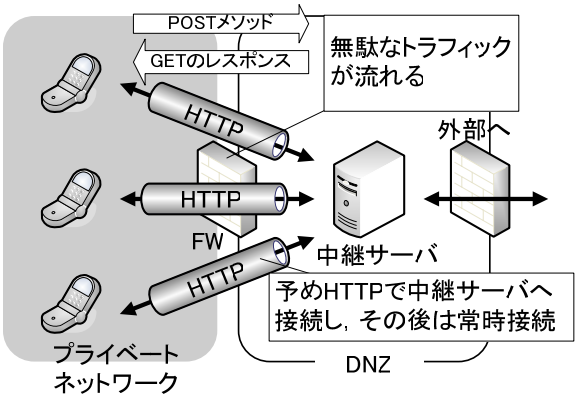


図 1.HCAP の方式

（2）SoftEther

SoftEther はグローバル環境上に設置した仮想 HUB に仮想 LAN カードを導入した PC から HTTP によるリンクを張りイーサネット・フレームをトンネルし，仮想的な LAN 環境を作る．仮想 LAN カードはデータを仮想的イーサネット・フレームごと HTTPS などに埋め込み，仮想 HUB は受け取った仮想イーサネット・フレームを転送する機能を持つ．SoftEther は仮想 HUB に接続している PC 同士ならどのようなアプリケーションでもファイアウォール，NAT のほとんどを通過して通信することができる．SoftEther を利用して外部の組織と通話をするには図２と図３の 2 通りの構成が考えられる．図２では仮想的なネットワーク上で SIP を利用している．この方式では SoftEther のブリッジ接続を利用してネットワーク同士を一つのブリッジで繋いだ構成になるため，両ネットワークのアドレス環境を統一せねばならず，異なる企業ネットワーク同士で通信を行うことのある IP 電話には都合が悪い．

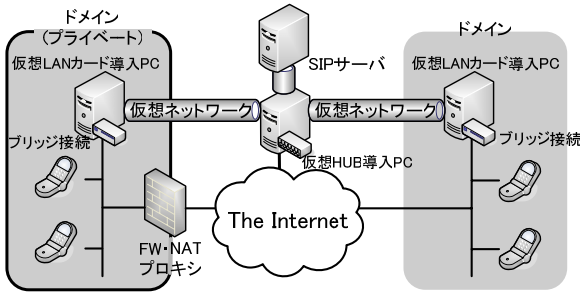


図 2.ブリッジ接続による仮想ネットワーク

図３では全ての端末に仮想 LAN カードを導入し，仮想ネットワークに直接繋ぐ構成となっている．この場合，端末には仮想 IP アドレスが割り振られるので，ネットワークの物理アドレス環境を心配する必要はないが，仮想アドレスの統一的な管理が必要となる．

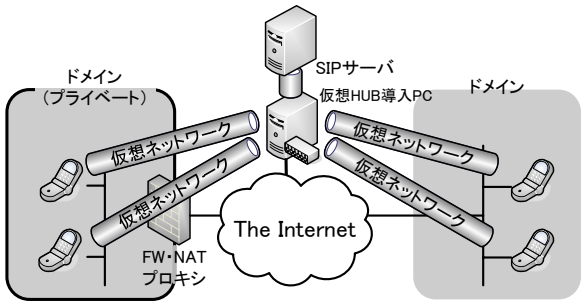


図 3.端末による仮想ネットワーク

また，SoftEther では内部のネットワークと外部のネットワークを無条件に接続してしまうことによって，内部ネットワークを危険にさらしてしまうことが大きな課題である．

3. 提案システム VoFW

本提案システム VoFW は従来の SIP ネットワーク，ファイアウォールシステムに影響を与えず，SIP メッセージ，音声データを中継サーバ間でそのまま HTTP に埋め込む．以下提案システムの詳細について説明する．

3.1. VoFW の構成

提案システムでは，図４のようにファイアウォールを越えるための機能を持つ装置をプライベートネットワークの内部と外部にそれぞれ 1 台ずつ設置する．これらの 2 台の装置は，プライベートアドレスネットワークとグローバルアドレスネットワークにそれぞれ１つずつインターフェースを持つ仮想的な１台の SIP

プロキシとしての機能を持つ．この 2 台の装置を Half Relay Agent（HRA）と呼び，プライベートネットワークの内部に設置するものを HRA クライアント（以下 HRAC），外部に設置するものを HRA サーバ（以下 HRAS）と呼ぶ．

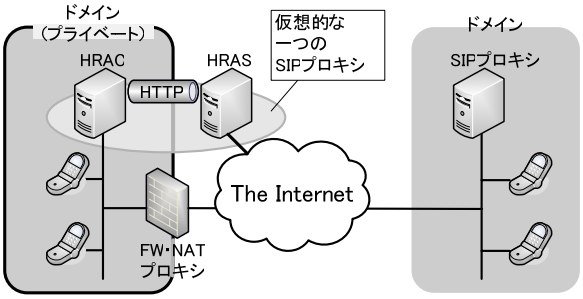


図 4 VoFW の構成

3.2. HTTP によるトンネリング

図 5 に提案システムの基本動作を示す，HRAC は電源立ち上げ時に HRAS に向けて，あらかじめ GET メソッドを発行し，HTTP のセッションを確立する．以降は，HRAS から定期的に HRAC に向けてダミー通信を行い，HRA 間の HTTP 接続を維持する．HRAS はダイアルや音声データを外側から受信すると，そのデータをそのまま GET メソッドのレスポンスに埋め込み HRAC に返すことで HRAS 中継を行うことができる．逆に HRAC は内側の端末からダイアルや音声データを受け取ると POST メソッドにそのデータを埋め込むことで HRAC に中継を行うことができる．

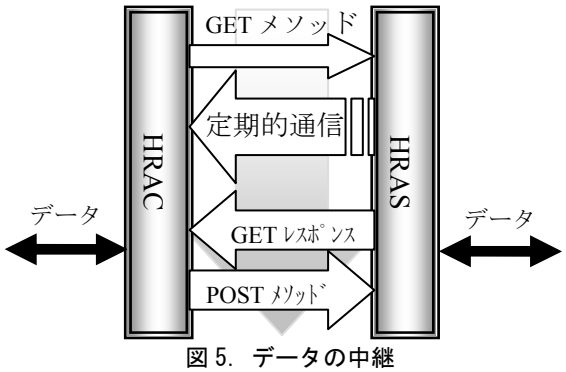


図 5. データの中継

3.3. ダイアルの中継

HRAS は音声データが HRA 間を中継される際に端末同士の通信情報を管理するためのテーブルを保持する．このテーブルを音声通信情報テーブル（VCIT）と呼ぶ．VCIT は表 1 のような内容を持つ．

表 1.音声通信情報テーブル（VCIT）

内容	説明
To	SIP メッセージの通信を識別する 3 つのヘッダの一つ．
From	同上
Call-ID	同上
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 に VCIT の生成手順を示す．HRAS はダイアルの際， SIP メッセージの To，From，Call-ID の 3 つのヘッダから通信を識別し，両方向からの SIP メッセージから通信に利用する両端末の IP アドレスやポート番号を VCIT に加えていく．ポート番号は音声通信の際，同じ端末の音声データの識別に利用できる．

端末から送信する音声データを HRA 宛に送信させるため，HRAC は外部からの SIP メッセージに含まれる端末情報の IP アドレスを HRAC の IP アドレスに，HRAS は内部からの SIP メッセージの端末情報の IP アドレスを HRAS の IP アドレスに修正する．この端末情報は SIP メッセージのボディ部に付加されている SDP というプロトコルに記述されている．

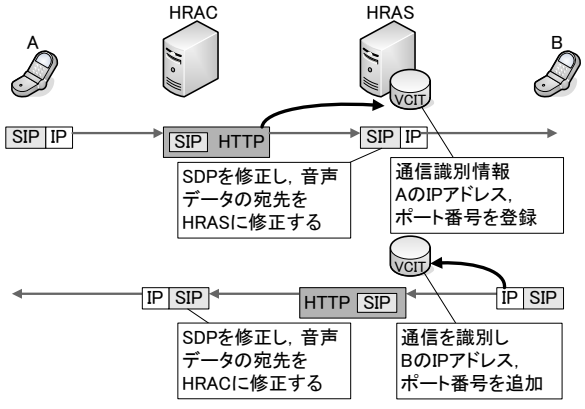


図 6.VCIT 生成

3.4. 音声データの中継

音声データの中継では HRA 間で HTTP に音声データをカプセリングするが，その際に経路を決定するために HRAS の VCIT を利用する．図

７のように外側のネットワークから内側へ音声データが送信されてきた場合，HRAS ではその音声データの送信元 IP アドレス，ポート番号から VCIT を参照し，宛先 IP アドレス，ポート番号を決定し，データと共に HTTP でカプセル化して HRAC に中継する．それを受け取った HRAC はカプセルを解除し，宛先 IP アドレス，ポート番号を読み取りデータの送信を行う．逆に内側から外側のネットワークへ音声データが送信された場合は，HRAC はデータとその送信元の情報を HTTP でカプセル化して，HRAS に中継し，HRAS では VCIT から宛先を決定する．

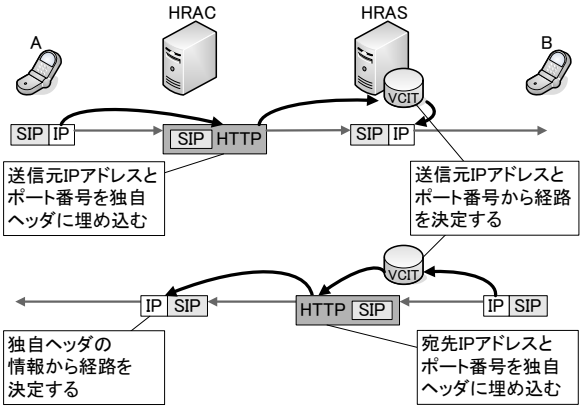


図 7.VCIT での経路決定

3.5. プライベートアドレス空間同士の IP 電話

企業では内部ネットワーク内での通話が多い．内部ネットワーク内の通話の場合は HRAS で初期のダイアルの一部を処理し，図８のようにネットワークの内部のみで残りのダイアル・音声通話のやり取りを行う．この場合，セッションの確立を要求する SIP メッセージが HRAS に送られてくると HRAS では SIP アドレスのドメインから内部宛か外部宛かを判別する．セッション確立要求に対するレスポンスまでは HRA を中継するが，それ以降の確認応答，通話終了などを示す SIP メッセージ・音声データは HRA を通さないように SIP メッセージに指示し，端末同士で全て直接通信させる．

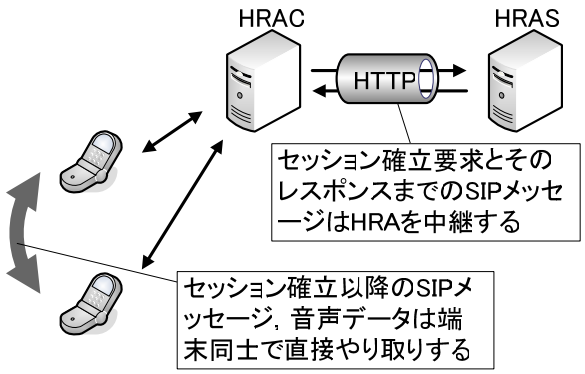


図 8．プライベートアドレス空間でのセッション確立

4．評価

VoFW と従来の SIP を利用した VoIP，他の代表的なファイアウォール通過 VoIP を比較し評価した結果を表１に示す．

表１．各方式の比較

	Linphone	HCAP	SoftEther*	VoFW
FW 通過	×	○	○	○
NA(P)T 通過	×	○	○	○
SIP の互換	○	△	○	○
導入の容易性	○	△	○	○
ディレイ	○	△	△	△
ｾｷｭﾘﾃｨ	○	○	×	○
ｱﾄﾞﾚｽ管理	○	○	×	○

*仮想ネットワーク上に VoIP を導入した場合．

Linphone はファイアウォールの通過を意識したものではないため，本提案との直接の比較対象ではないが，参考に揚げてある．Linphone は SIP サーバと端末を用意するのみでよいため導入が容易であり，ディレイに関しても UDP で直接音声通信を行うため，他のシステムに比べ小さい．

HCAP は，セッションの確立に HTTP を利用した独自の方式を採用しており，SIP との互換性はなく，端末に専用の機能が必要であり導入が容易とは言えない．また，各端末から中継サーバへ常時 HTTP の接続を行っているためファイアウォール上に無駄なトラフィックが発

生する.

SoftEther のブリッジ接続を利用する場合（図２のケース），両方のネットワークのアドレス環境などを一つの LAN になるように予め設定しておくことが必要になり, 外部のネットワークの端末と繋ぐ IP 電話には都合が悪い．端末全てに導入する場合（図３のケース）では，物理的なアドレス環境の設定はいらないが, 両ネットワークで統一した仮想 IP アドレスの管理が必要となる．また，セキュリティに関しても外部のネットワークとアドレス空間を共有してしまうため内部ネットワークが危険にさらされることになる.

VoFW のダイアルでは, SIP プロキシ間の通信をダイアルメッセージから音声データまで全て HTTP でトンネリングするシステムであるため，SIP との互換性がある．また，VoFW では, 既存のファイアウォールシステムに全く影響を与えない上, ファイアウォール上を流れるのは HRA 同士の 1 対 1 の通信のみとなるため, トラフィックの無駄が少ない．HCAP や Skype などでは, 端末がカプセリング機能を持っているのに対し，本システムでは HRAC がその機能を持つため, 電話端末は既存の SIP 技術をそのまま利用すればよく, 特別な機能をインストールする必要はない. IP アドレス管理についても既存のアドレス管理と何らかわるところはない.

5. おわりに

本論文では，IP 電話が課題とするファイアウォール・NAT・プロキシを越えることのできる新しいシステムを提案し, その詳細について説明した．また，既存の VoIP と提案システムを複数の項目に分けて比較することにより, システムを導入することによって得られる利点について考察し報告した.

今後は提案システムの実装を行い，その有効性を確認する．また，HTTP を利用することによる品質劣化の可能性についても検討を行っていく.

参考文献

[1] 星 徹:VoIP の最新動向,情報処理学会誌, Vol.42 No.02 - 008

[2] N.Freed : Behavior of and Requirements for Internet Firewalls , IETF RFC 2979 (2000.10).

[3] K. Egevang, P. Francis:The IP Network Address Translator (NAT),IETF RFC 1631(1994.5).

[4]Berners-Lee,T.,Fielding,R.T.and Nielsen,H.:Hyper-TextTransfer Protocol-HTTP/1.0, IETF RFC (1994.11).

[5] 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

[6] 千村保文，村田利文“SIP 教科書”IDG ジャパン

[7] J. Rosenberg,et all”SIP: Session Initiation Protocol”IETF RFC3261(2002.6)

[8]Petri Koskelainen,Henning Schulzrinne,Xiaotao Wu:VoIP:A SIP-based conference control framework,ACM press 53-61(2002.5).

[9] Stefan Berger,Henning Schulzrinne,Stylianos Sidiroglou,Xiaotao Wu:Conferencing:Ubiquitous computing using SIP,ACM press 82-89(2003.6)

[10] S. Deering, R. Hinden: Internet Protocol, Version 6 (IPv6) Specification,RFC 2460(1998.12).

[11] 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

[12] Skype: ” http://www.skype.com/home.html”Kazaa

[13] 登大遊“SoftEther による Ethernet の仮想トンネリング通信”

[14] AVAYAlobs”AVAIYA IP VOICE QUALTY NETWORK REQUIREMENTS”

[15] 宮内信二，他“ブロードバンド時代のインターネットに適した HTTP による VoIP 方式”CSVC2001-13,pp.39 43,7(2001.4.5).

ファイアウォールを通過するIP電話の提案

Proposal of voice over IP system passing through Firewall

名城大学大学院理工学研究科

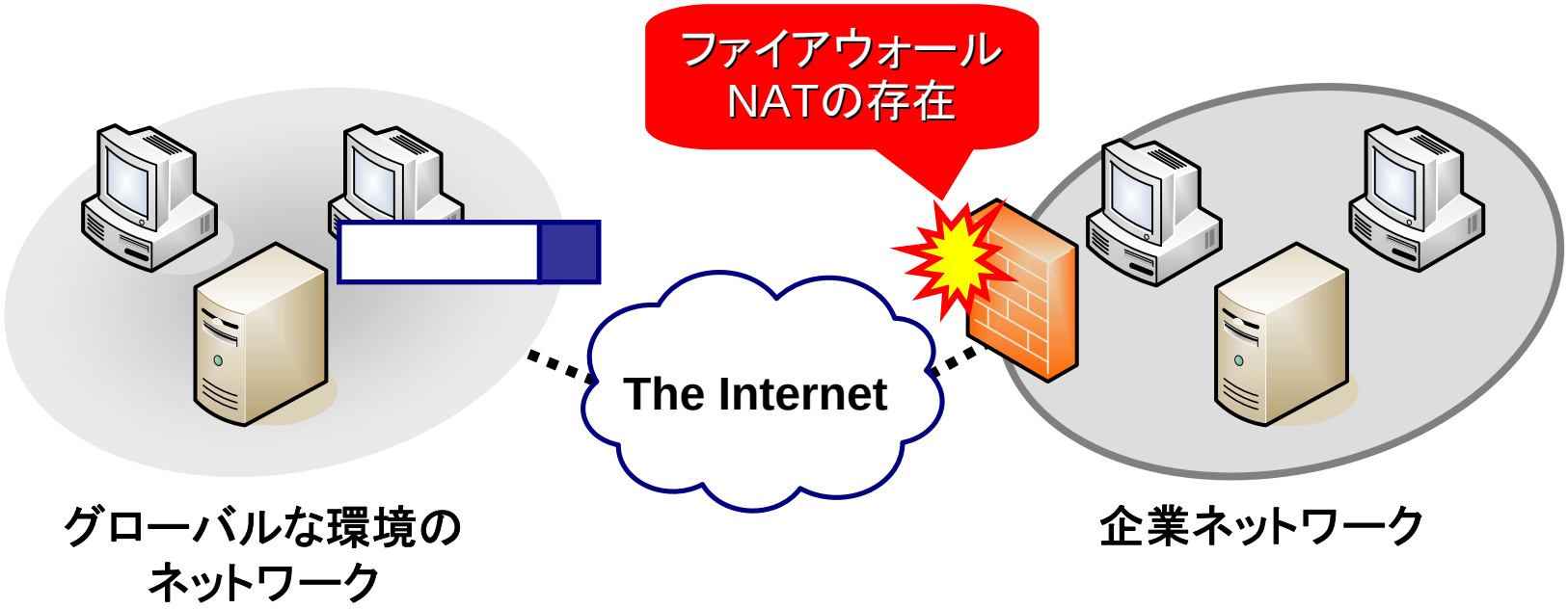
伊藤 将志　　渡邊 晃

1. はじめに

近年、IP電話はインターネットのブロードバンド化・“050-”の事業者受付により著しく普及を遂げた

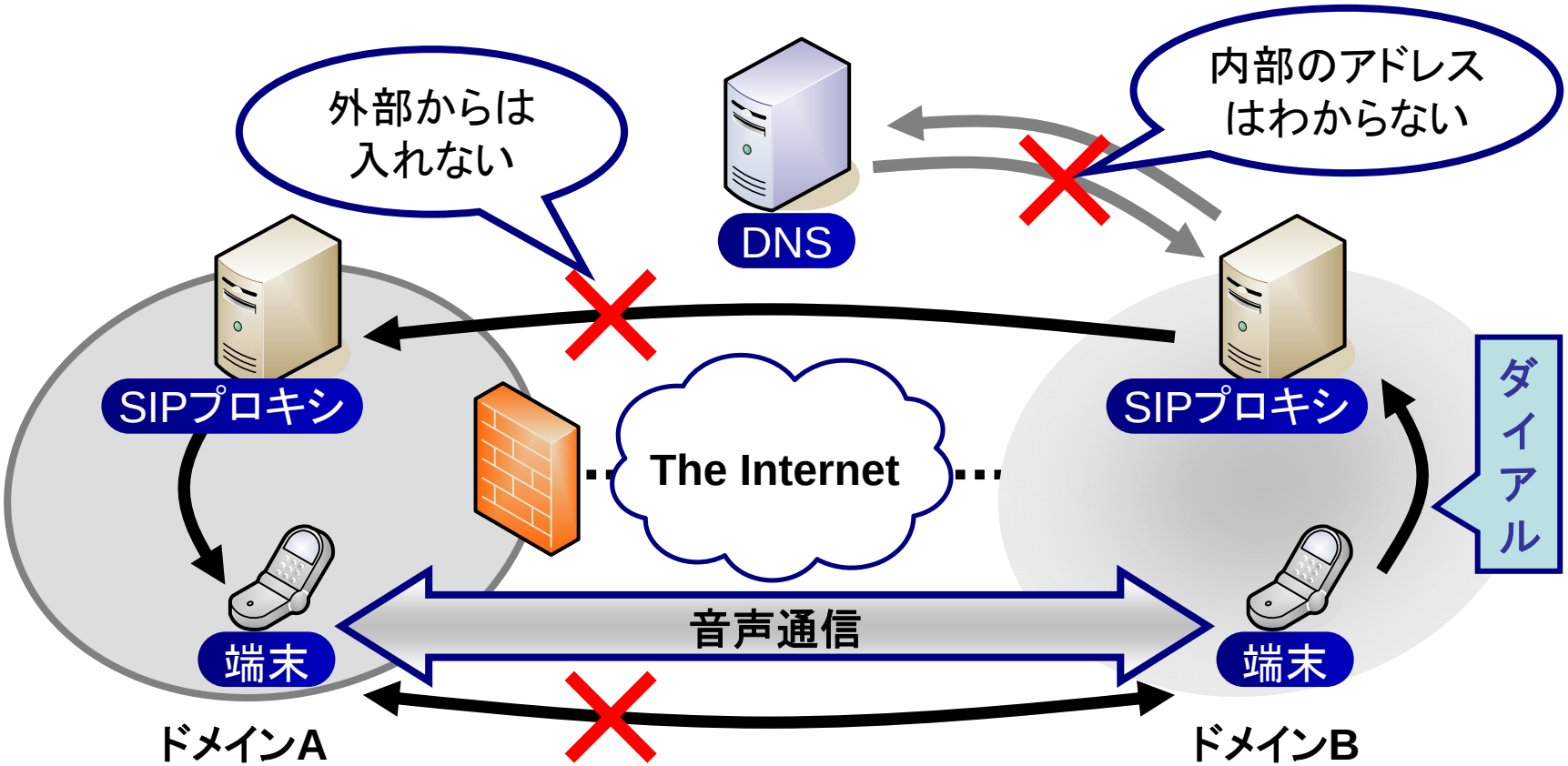
IP電話の課題

ファイアウォールのある企業ネットワークの内部からは外部と通信できない。



2. SIP（Session Initiation Protocol）

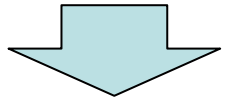
VoIPのセッション開始プロトコルとして実装の容易さと拡張性に優れたSIPが普及している



3. 既存のファイアウォール通過VoIP

- ファイアウォールに実装するシステム

  UPnPなどポート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



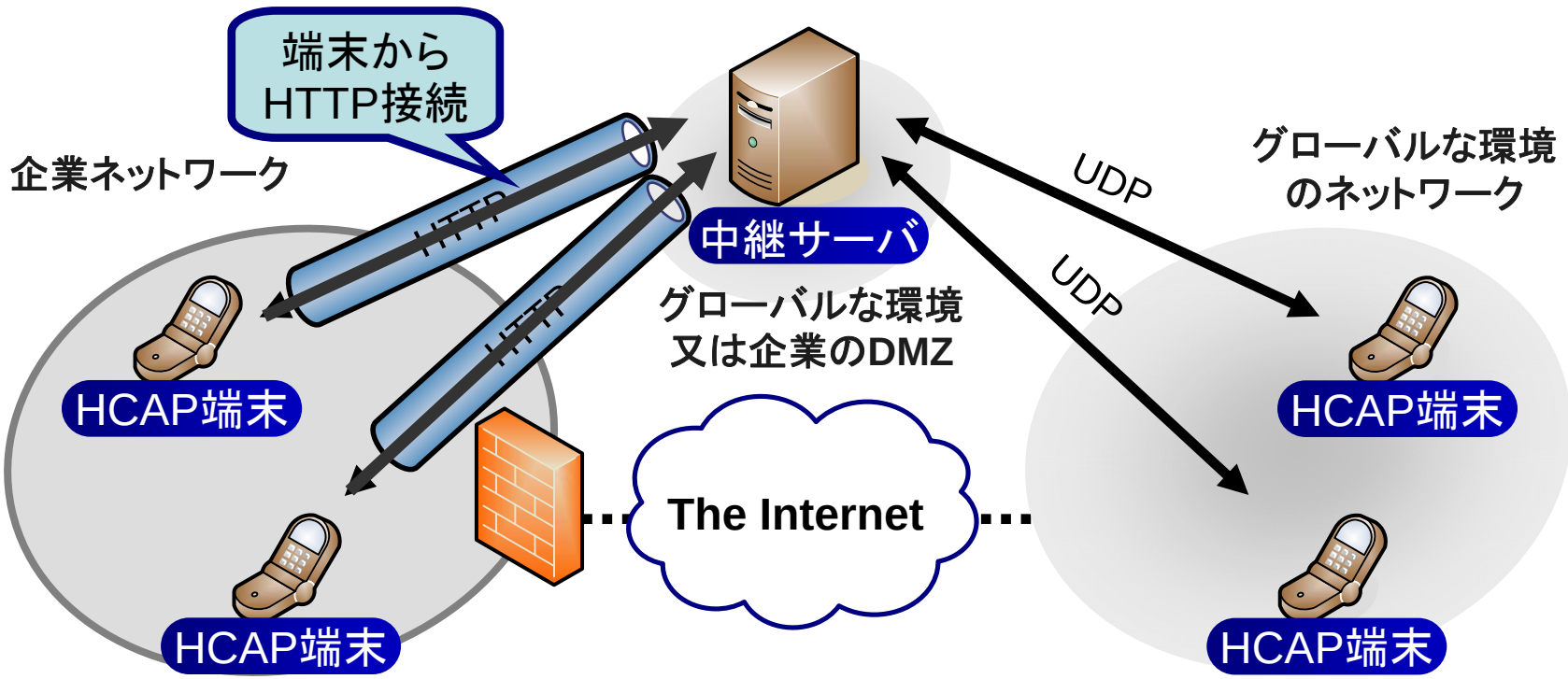
ネットワーク管理の権限が必要となり、ユーザが簡単に設置できるシステムではない。

- 専用端末、サーバなどに実装するシステム
  - Skype
  - HCAP
  - SoftEhter

80番ポートを偽装してファイアウォールを越えようとするのでHTTPプロキシが通過できない。

3．1．HCAP

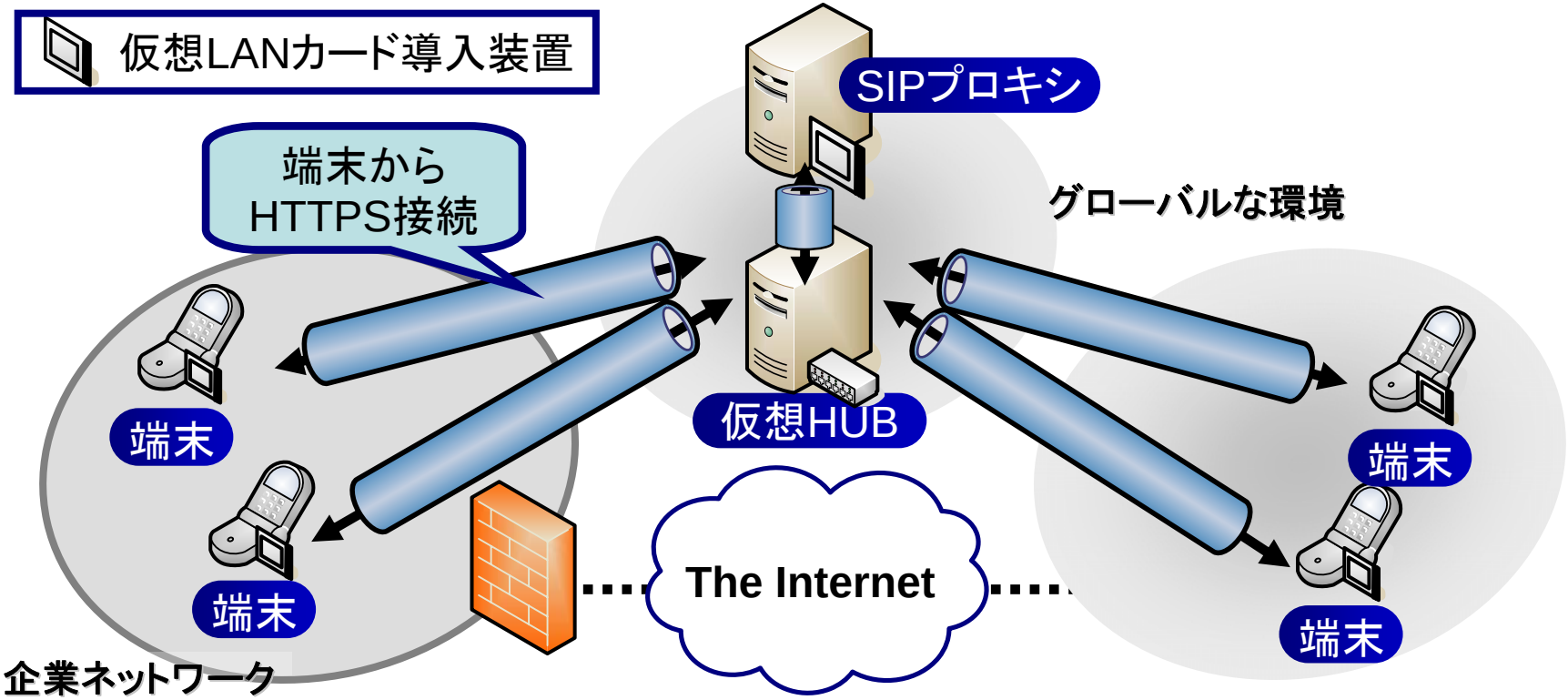
端末からHTTPで中継サーバに接続することで外部と通話可能



- 端末からの中継サーバへのHTTP常時接続
  - ファイアウォール上に無駄なトラフィックが発生
  - 専用の端末を導入しなければならない

3．2．SoftEther

仮想LANカードと呼ばれる端末から仮想HUBと呼ばれる中継サーバへHTTPSなどで接続し、仮想的なネットワークを作る



- プロトコルフリーの仮想ネットワークを作る
  - 企業ネットワークが外部にさらされる危険がある
  - 仮想的なIPアドレスの統一的な管理が必要

4. 提案システム

システムの目的

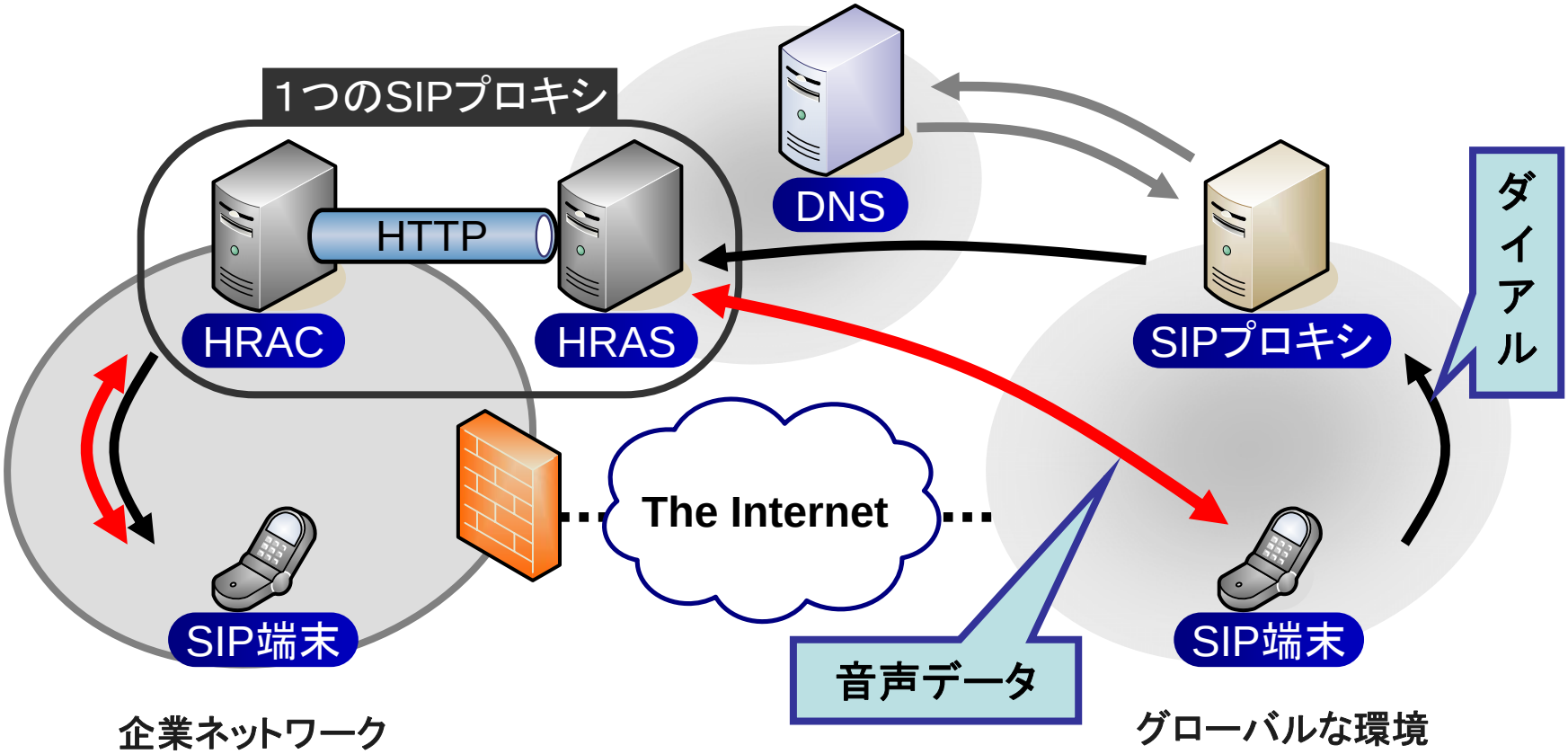
- 導入の容易さ
- 無駄なトラフィックの削減
- アドレス管理に影響を与えない

VoFW(Voice over Fire Wall)

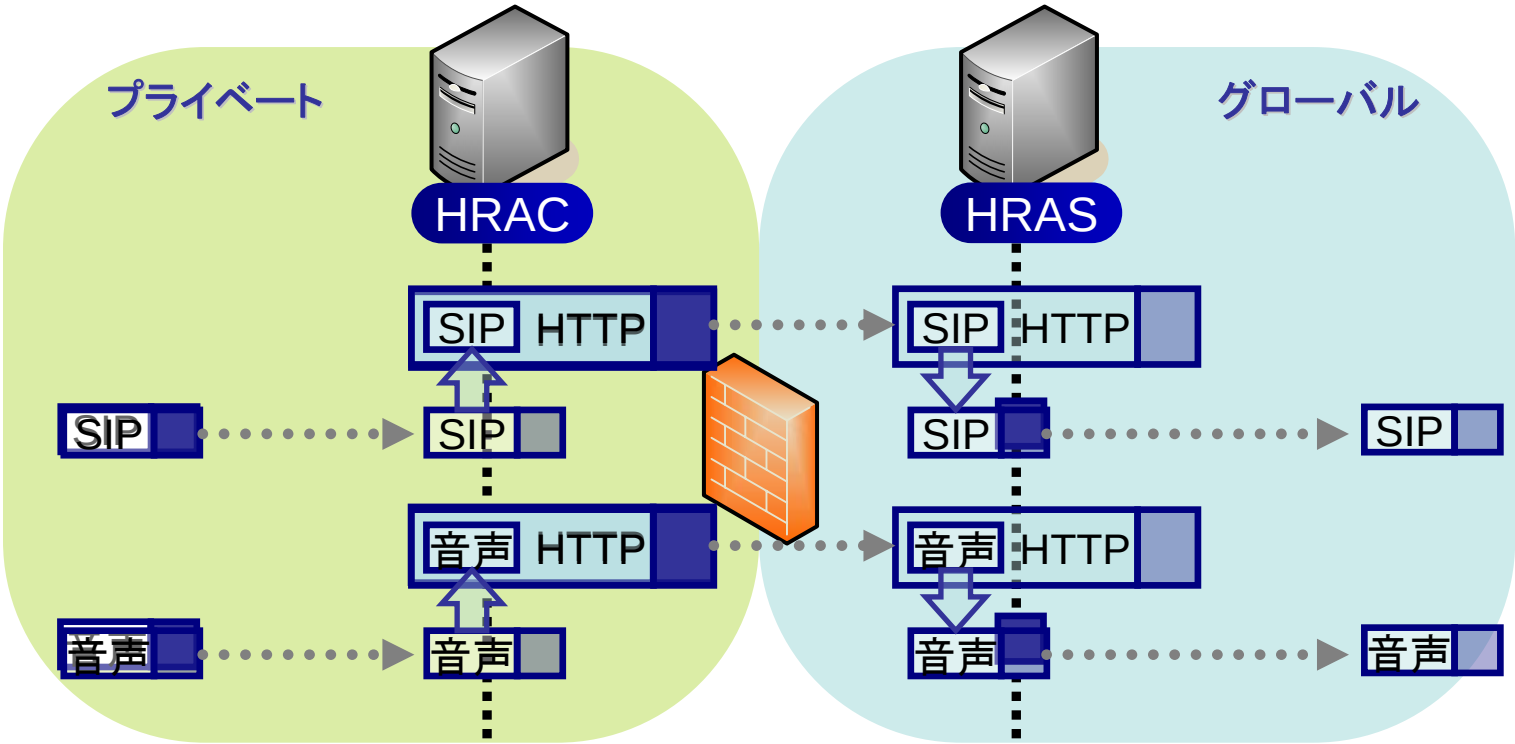
SIP・音声データをそのままHTTPに埋め込み
ファイアウォールを通過させる

4．1．VoFWの構成

ファイアウォールの内部と外部に2つのHRA（Half Relay Agent）と呼ぶ装置を設置する

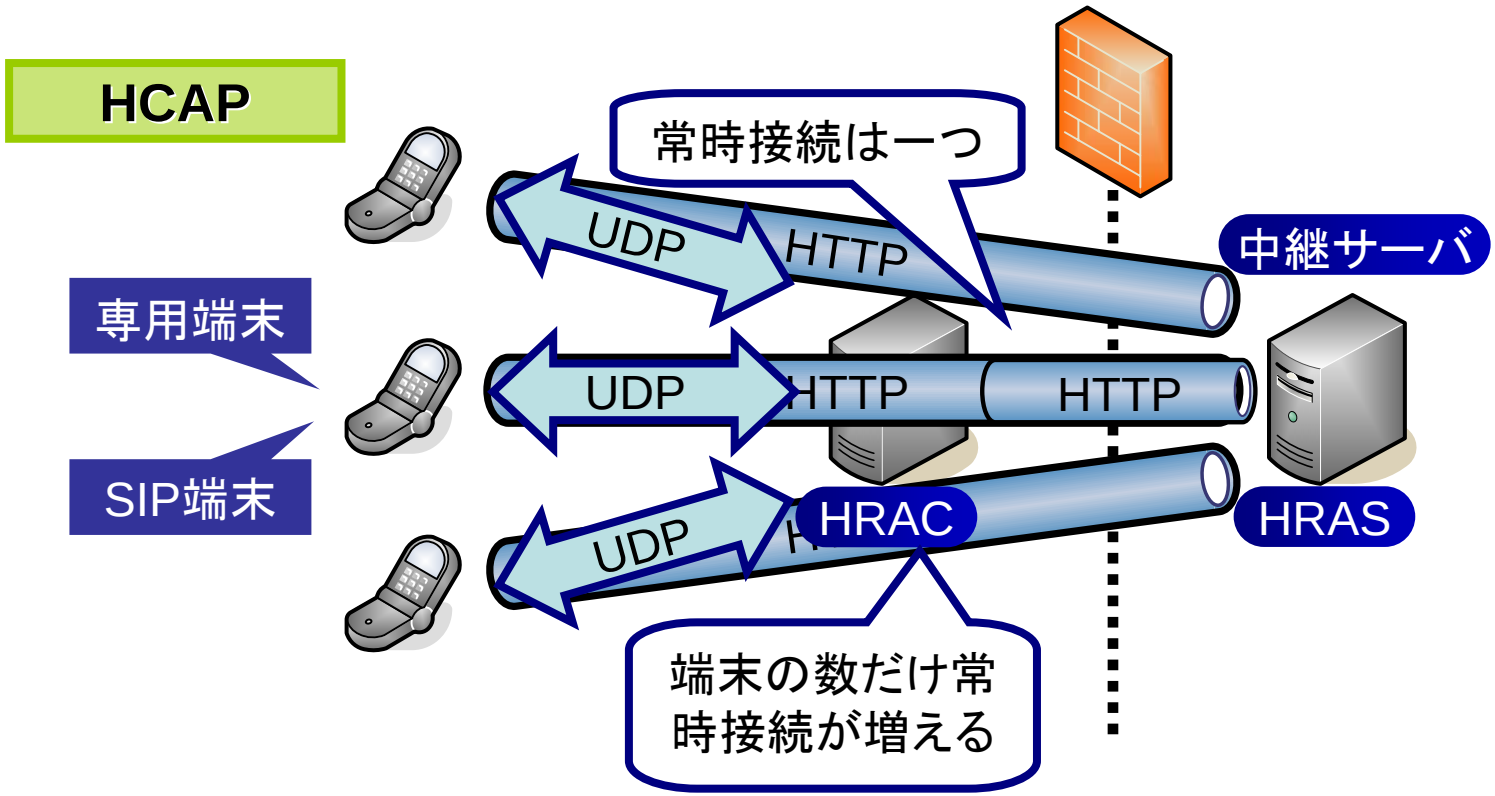


4．2．VoFWの特徴1



- SIPをHTTPに埋め込みファイアウォールを通過
  - Web閲覧の可能な環境であればどこでもダイアル可能
  - 既存のSIPネットワークをそのまま使える
- 音声データもHTTPに埋め込みファイアウォール通過

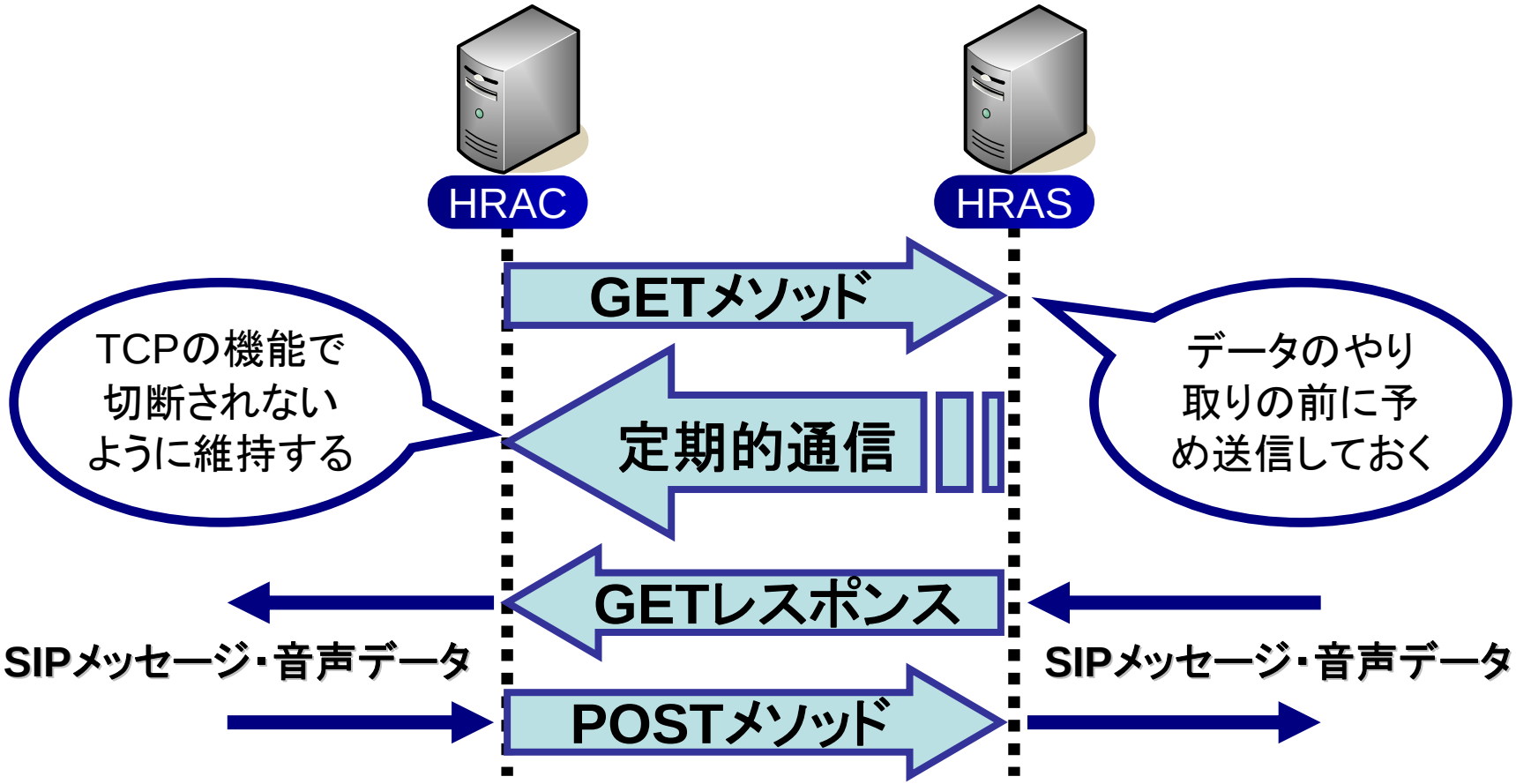
4．3．VoFWの特徴2



- ファイアウォールの内部と外部にHRAを設置
  - ファイアウォール上の無駄なトラフィックを抑えられる
  - 端末は既存のSIP対応のもので良い

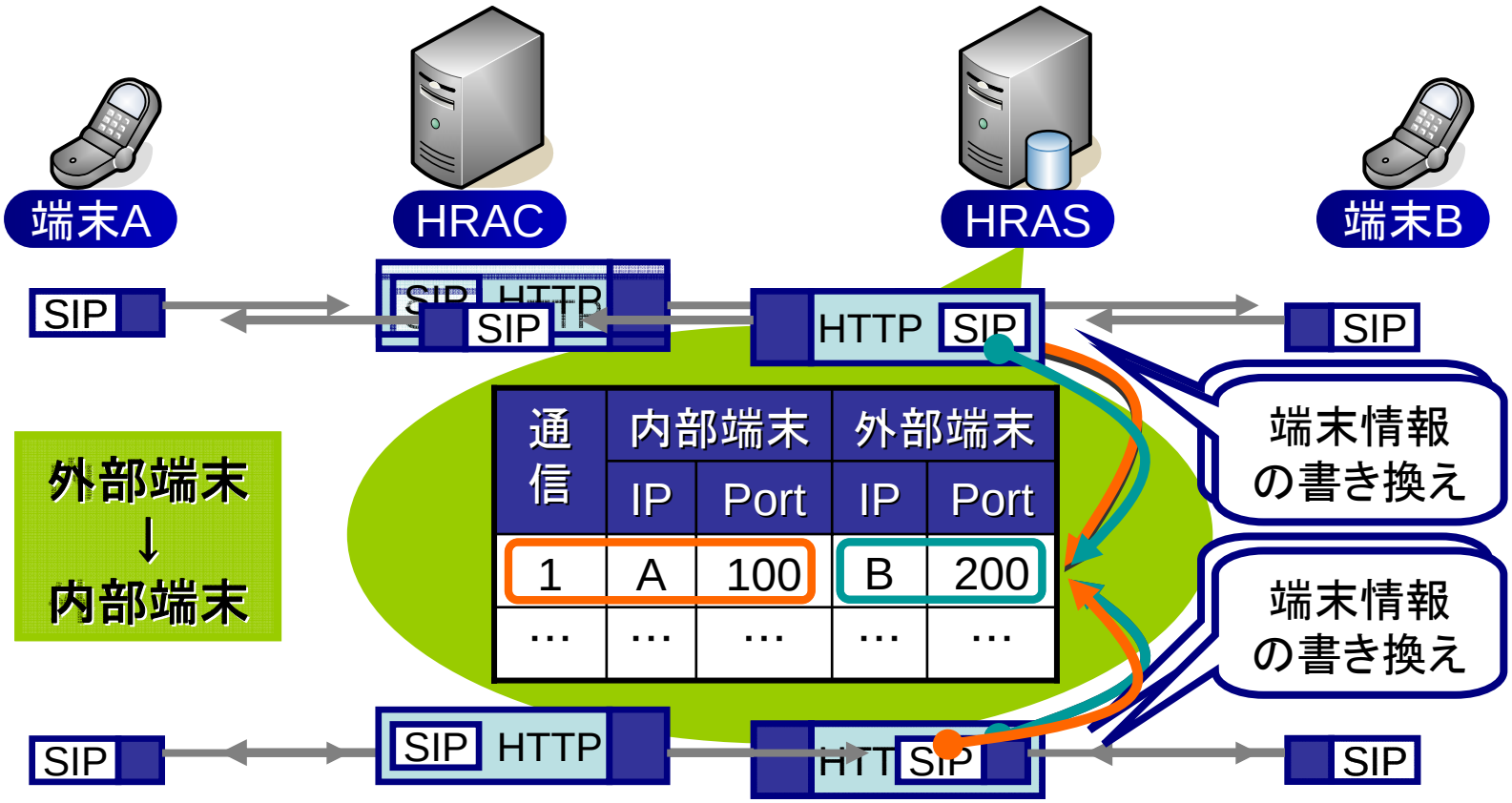
4．4．HTTPトンネルの確立

内側への送信はGETメソッドのレスポンス、外側への送信はPOSTメソッドにデータを埋め込む



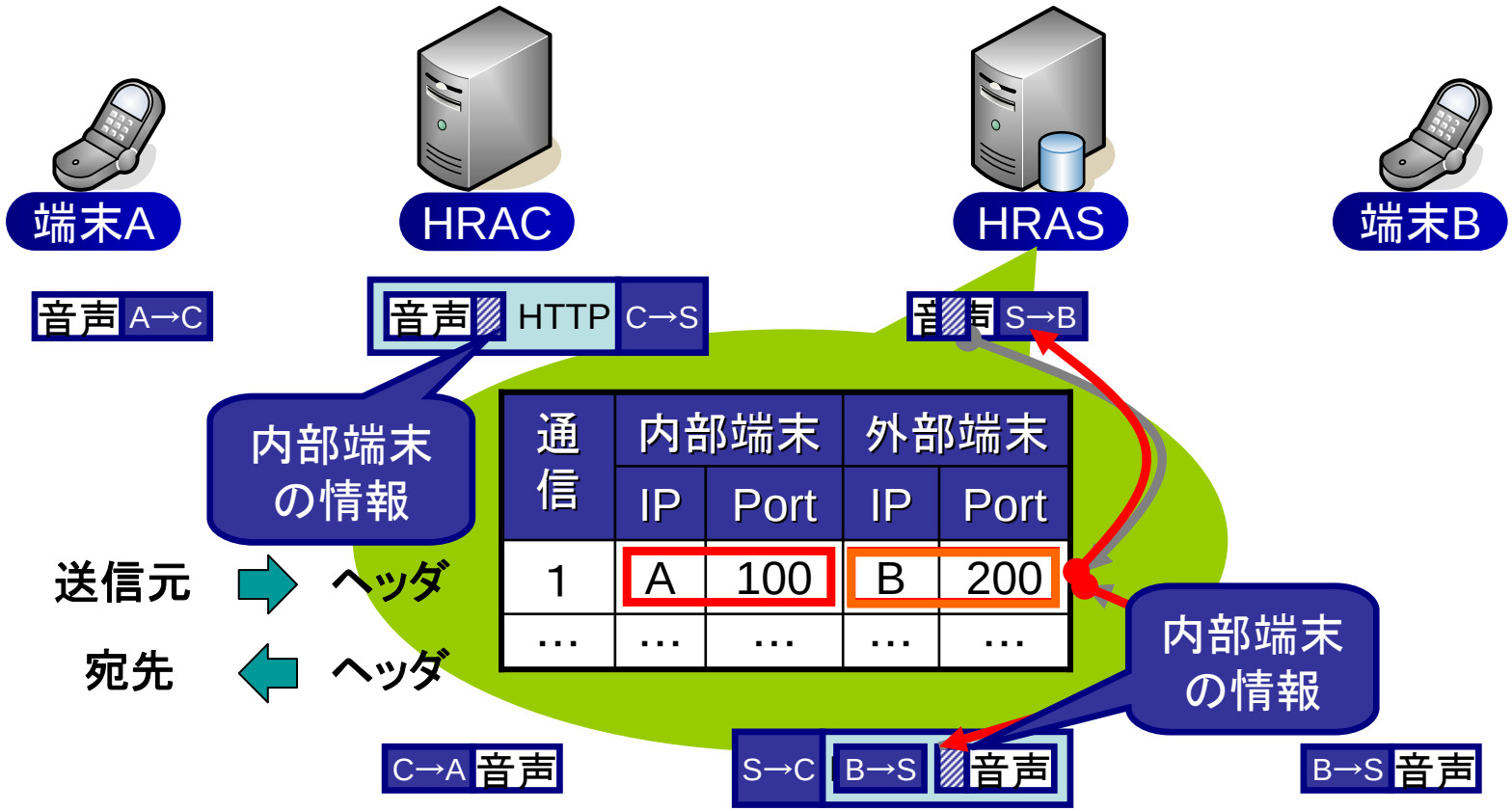
4．5．ダイアルとVCITの生成

ダイアルの際、SIPの端末情報の書き換え・VCIT（音声通信情報テーブル）の生成を行う



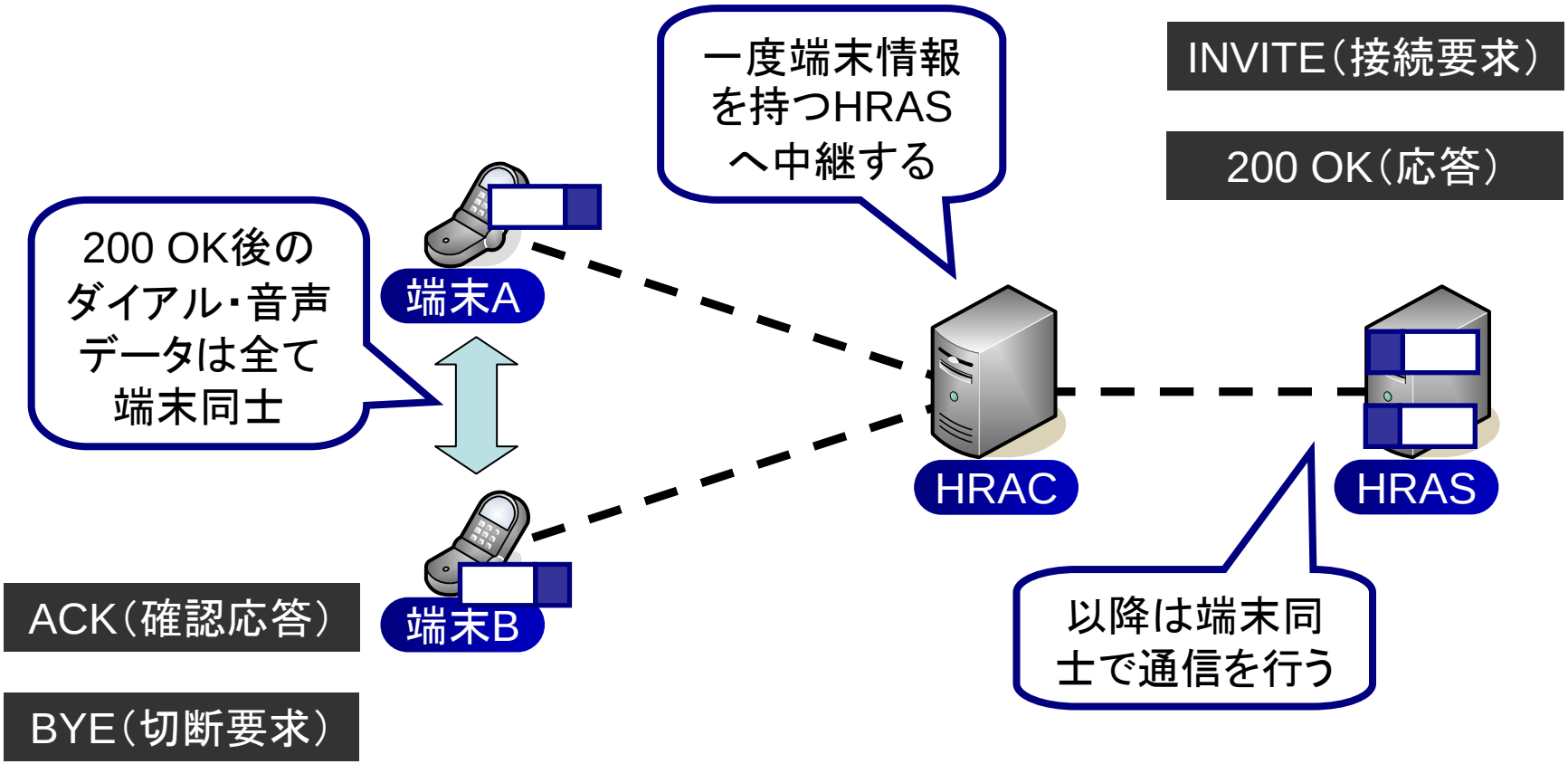
4．6．音声データの経路決定

ダイアルの際、生成したVCITを利用し、音声データの経路を決定する



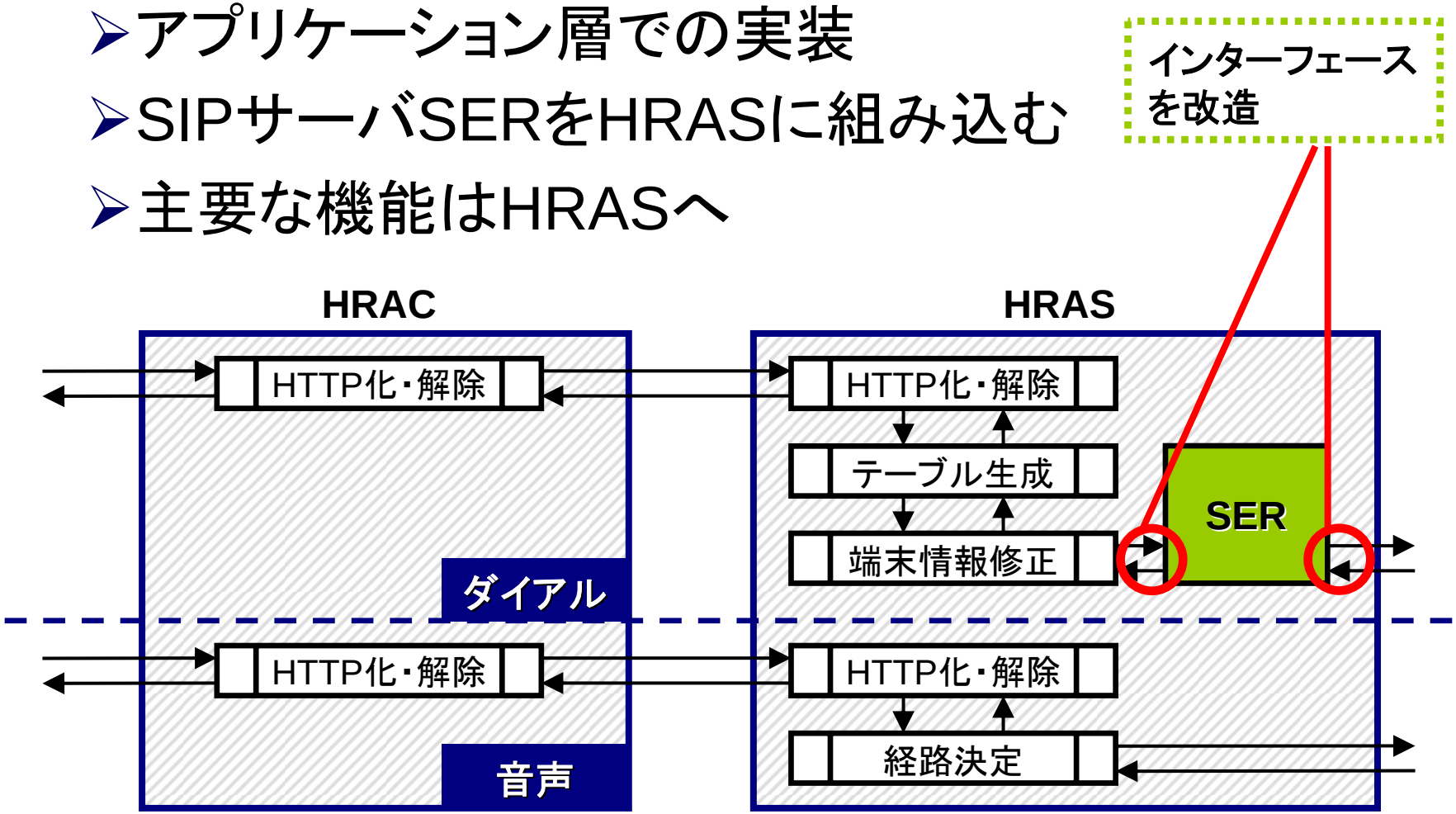
4．7．内部同士の通話

内部端末同士の通話は端末同士で直接やりとりする



4．8．実装

- 実装方式
  - アプリケーション層での実装
  - SIPサーバSERをHRASに組み込む
  - 主要な機能はHRASへ



5. 既存技術との比較

	FW通過	NA(P)T通過	SIPとの互換性	導入の容易性	ディレイ	セキュリティ	アドレス管理
Linphone	×	×	○	○	○	○	○
HCAP	○	○	△	△	△	○	○
SoftEther	○	○	○	○	△	×	×
VoFW	○	○	○	○	△	○	○

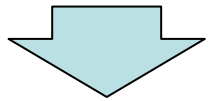
VoFWの特長

- 既存の端末・SIPネットワークがそのまま使える
- IPアドレス環境は外部からはわからない
- IPアドレス管理の必要がない

6. おわりに

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

ファイアウォールの内部と外部にHRAを置き、SIP・音声データをそのままHTTPに埋め込む方式



  - 導入性・アドレス管理・トラフィックなどの改善
  - 他のシステムとの比較
- 今後の課題
  - 実装
  - 端末間におけるパケットディレイの評価
  - ファイアウォール上のトラフィックの評価

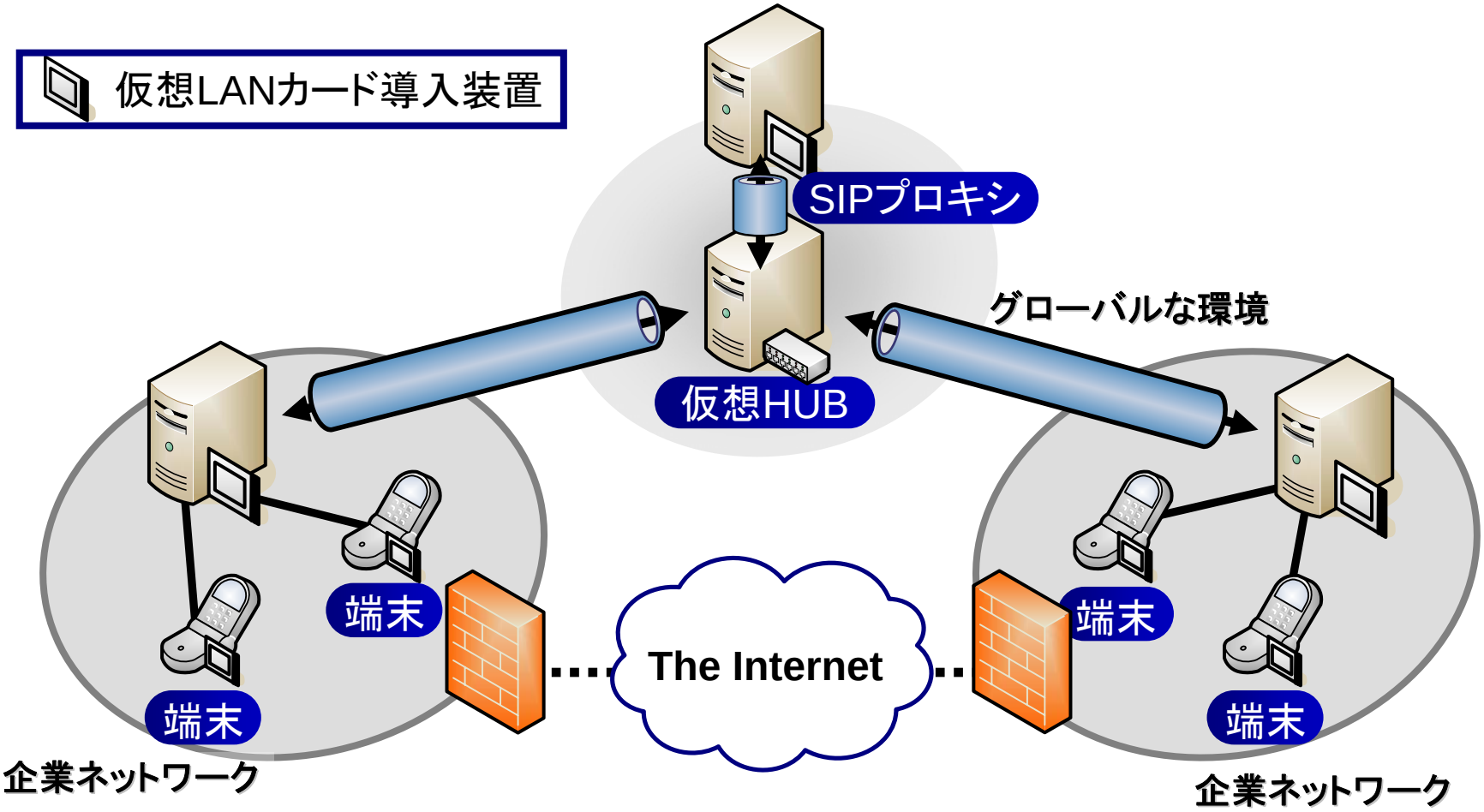
おわり

音声通信情報テーブル

VCIT（Voice Communication Information Table）

内容	説明
To	SIPメッセージの通信を識別する3つのパラメータの一つ
From	同上
Call-ID	同上
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Port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Port番号

補足資料2　SoftEtherの構成



IPアドレス環境を両ネットワークで統一しなければならない

補足資料3　Skype

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.11	192.168.11.2	TCP	3664 > 64596 [SYN] Seq=33
2	0.137415	192.168.1.11	66.98.158.185	HTTP	Continuation
3	0.327773	66.98.158.185	192.168.1.11	TCP	http > 3582 [ACK] Seq=231
4	0.847296	66.98.158.185	192.168.1.11	HTTP	Continuation
5	0.964693	192.168.1.11	66.98.158.185	TCP	3582 > http [ACK] Seq=259
6	2.279347	192.168.1.11	193.229.37.89	TCP	3665 > http [SYN] Seq=336
7	2.279692	192.168.1.11	80.162.18.157	TCP	3666 > http [SYN] Seq=336
8	2.578531	193.229.37.89	192.168.1.11	TCP	http > 3665 [SYN, ACK] Se
9	2.578667	192.168.1.11	193.229.37.89	TCP	3665 > http [ACK] Seq=336
10	2.579348	192.168.1.11	193.229.37.89	HTTP	Continuation
11	2.580495	80.162.18.157	192.168.1.11	TCP	http > 3666 [SYN, ACK] Se
12	2.580541	192.168.1.11	80.162.18.157	TCP	3666 > http [ACK] Seq=336
13	2.580844	192.168.1.11	80.162.18.157	HTTP	Continuation
14	2.887472	193.229.37.89	192.168.1.11	HTTP	Continuation
15	2.888394	80.162.18.157	192.168.1.11	HTTP	Continuation
16	2.888706	192.168.1.11	193.229.37.89	HTTP	Continuation
17	2.888941	192.168.1.11	80.162.18.157	HTTP	Continuation
18	3.187899	193.229.37.89	192.168.1.11	HTTP	Continuation
19	3.211915	80.162.18.157	192.168.1.11	HTTP	Continuation
20	3.212280	192.168.1.11	66.98.158.185	HTTP	Continuation
21	3.372384	192.168.1.11	80.162.18.157	TCP	3666 > http [ACK] Seq=336
22	3.372484	192.168.1.11	193.229.37.89	TCP	3665 > http [ACK] Seq=336

TCP の接続

80番で動くアプリケーション

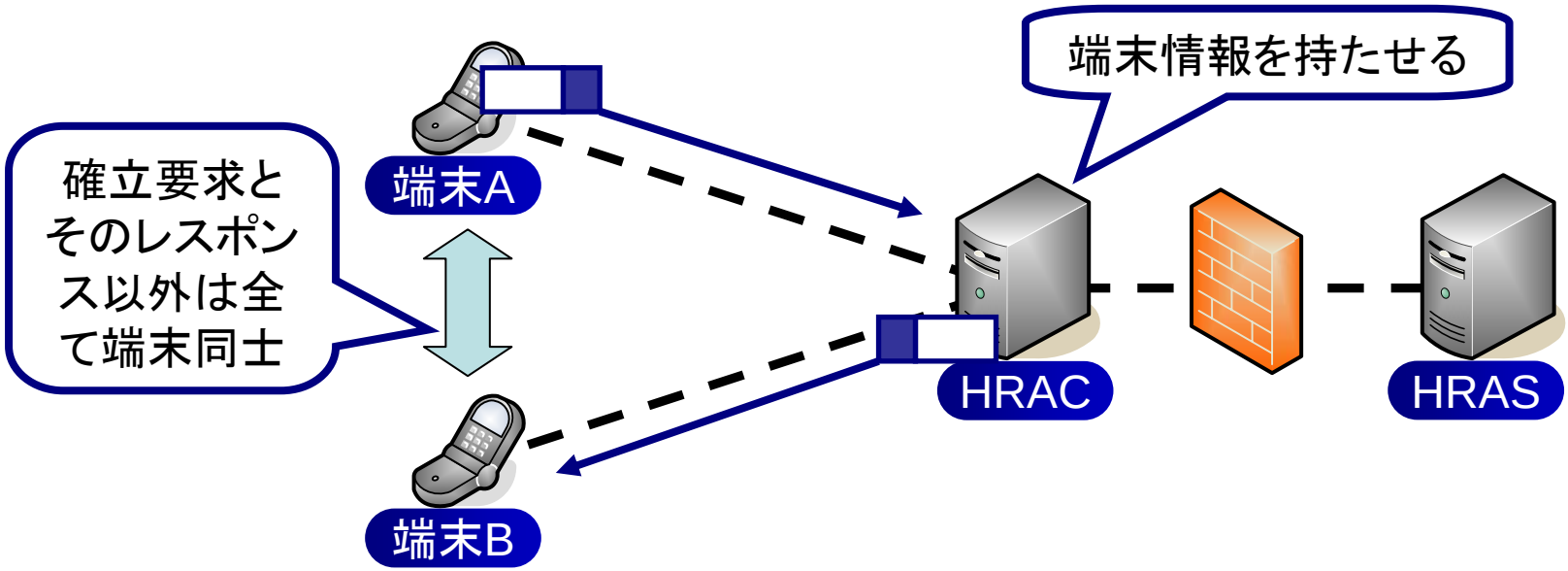
端末からSkypeのサーバへ接続する際のパケットのキャプチャ

TCP接続後、GETなどのメソッドが使われていない

↓

80番ポートで独自のアプリケーションを利用

補足資料4　内部同士の通信



HRACに端末情報を持たせて、全てのパケットがファイアウォールより外部に出ないようにすることも検討中