ファイアウォールを通過できる IP 電話

11300j011　伊藤 将志
渡邊研究室

1. はじめに

近年,ブロードバンドの普及により IP 電話の実用レベルの品質保証が実現した．また，2002 年秋より総務庁から“050-”の事業者受付も開始され，従来の電話からも受信が可能となり，多くの ISP が低額固定料金の IP 電話サービスを提供するようになった．

しかし,この普及に対し VoIP には様々な課題がある．それは，FW(Fire wall)，NAT，プロキシなどによる通信の制限である.既存 VoIP ではこの課題に対応できず,それらの存在する企業ネットワークからは外部との通話が難しい．

本稿では，この課題を解決するために，プライベートネットワークの内部と外部に特殊なリレーエージェントを配置し，それを用いて SIP[2]によるダイアルと音声データを HTTP でトンネル中継するシステムを提案する．また，その詳細を説明し，既存システムと比較した性能評価を挙げる．

2. 既存技術とその課題

SIP では，送信元の SIP プロキシが端末からダイアルメッセージを受けると，宛先の SIP プロキシの IP アドレスを DNS から取得するため，通信開始には相手 IP アドレスが DNS から特定できることが必須となる．しかし，NAT が存在すると，通話先端末の IP アドレスが外部から特定できず，通信ができない．また，企業の FW は HTTP で使用する 80 番など,必要以外のポートを通過不可にするため,SIP による IP 電話の実現には,FW 設定の変更が必要である．これはセキュリティ低下に繋がるため望ましくない．

すでにこの課題を解決している HCAP では HTTP を利用して 80 番ポートで FW を通過し，ローカルから予めセッションを確立することで NAT 問題を解決する [1]．しかし,端末に専用プロトコルを導入する必要があり,DMZ 上に特殊なサーバの設置を必要とする上，FW 内の複数の端末が常時接続するため FW に不要なトラヒックが流れるという課題がある．

また，Skype は 80 番ポートを利用した独自アプリケーションにより FW を通過する[3]．そして，端末からグローバル環境上のサーバに TCP 接続を行い，端末間のダイアルや音声をサーバが中継することで，NAT の通過も可能である．しかし，80 番ポートを独自アプリケーションで使用しているため,HTTP プロキシ通過が不可能で，セキュリティ的にも信頼性が低い．

3. 提案システム

本システムでは図１のようにプライベートネットワークの内側と外側に特殊なリレーエージェントを設置する．この２台の装置それぞれを Half Relay Agent(HRA)といい,内側に設置するものを HRA クライアント，外側に設置するものを HRA サーバと呼ぶ．通常の SIP によって中継されたダイアルメッセージや音声ストリームは HRA により HTTP に埋め込まれ､ダウンロード・アップロードにより，FW や NAT の通過を可能とする．この２台は合わせて音声中継も行う特殊で仮想的な SIP プロキシの役割を果たす．

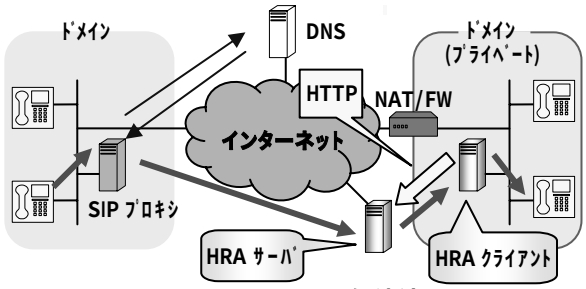


図１．HRA による解決法

4. 評価

本システムと既存の IP 電話システムを比較した結果を表にして示す．

表１．ダイアル方式等の比較

	FW 通過	NAT 通過	ﾌﾟﾛｷｼ 通過	SIP との互換	ディレイ	導入
Linphone	×	×	×	◎	◎	◎
HCAP	◎	◎	◎	×	△	○
Skype	◎	◎	×	×	△	○
提案システム	◎	◎	◎	○	△	◎

提案システムでは，FW, NAT, プロキシを通過でき，SIP プロキシ間通信を HTTP でトンネルするので，SIP との互換性も高い.また端末は標準の VoIP 対応のもので良く，プライベート環境内のユーザ個人で実装を行うことができる．さらに，FW に流れる通信は HRA 同士の１対１の通信のため,無駄なトラフィックが少ない.ただし，HTTP を利用するため，音声のディレイに関しては UDP による方式に比べ劣化する可能性がある．

5. おわりに

本稿では,ファイアウォールを通過する IP 電話を提案し，その詳細について説明した．今後はシステムの実装を行い，機能確認を行うと共に実用的な音声品質が得られるかを評価する．

参考文献

[1]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
[2] J. Rosenberg,et all ”SIP: Session Initiation Protocol ” IETF RFC3261(2002.6)
[3]Skype ”http://www.skype.com/home.html ” Kazaa

ファイアウォールを通過できるIP電話
voice over IP system passing through Firewall

渡邊研究室

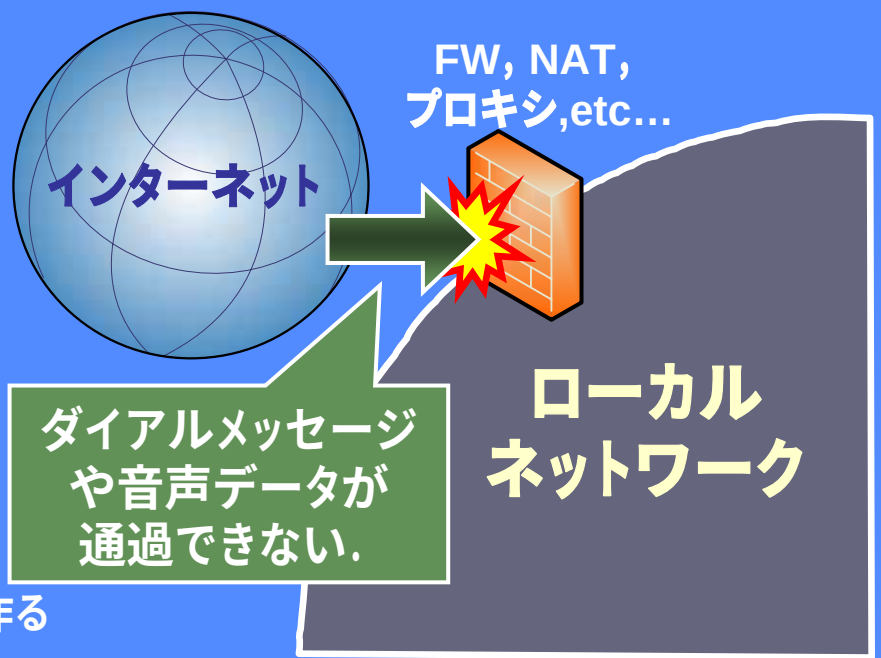
11300J011　　伊藤将志

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ー”の事業者受付により著しく普及を遂げた．

課題

外部と内部の通信に制限があるネットワークでは通信ができない



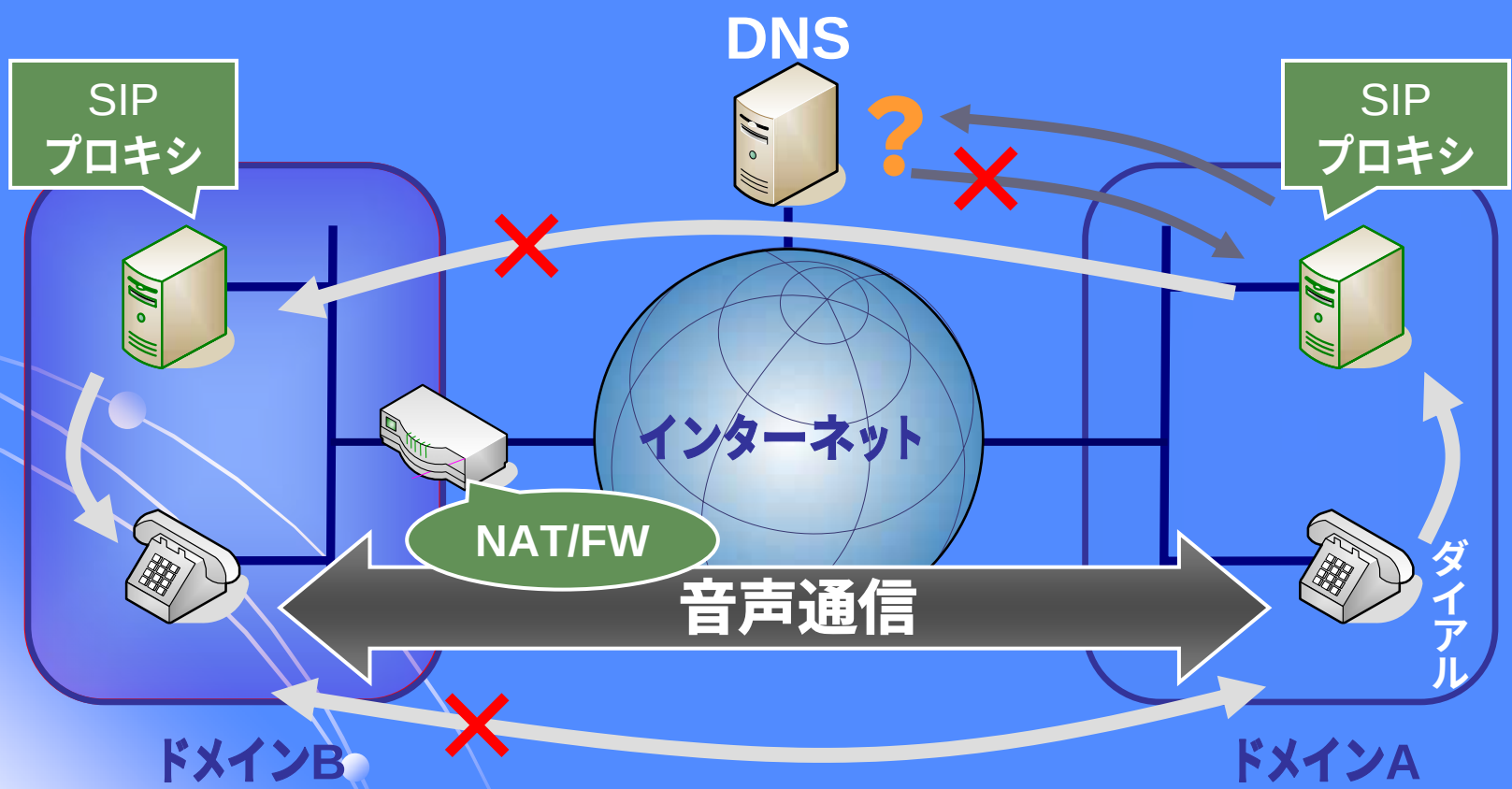
FW‥‥特定パケット以外を遮断

NAT‥‥外部から特定不能なアドレス環境を作る

ﾌﾟﾛｷｼ‥内部の端末の通信を代理で行う

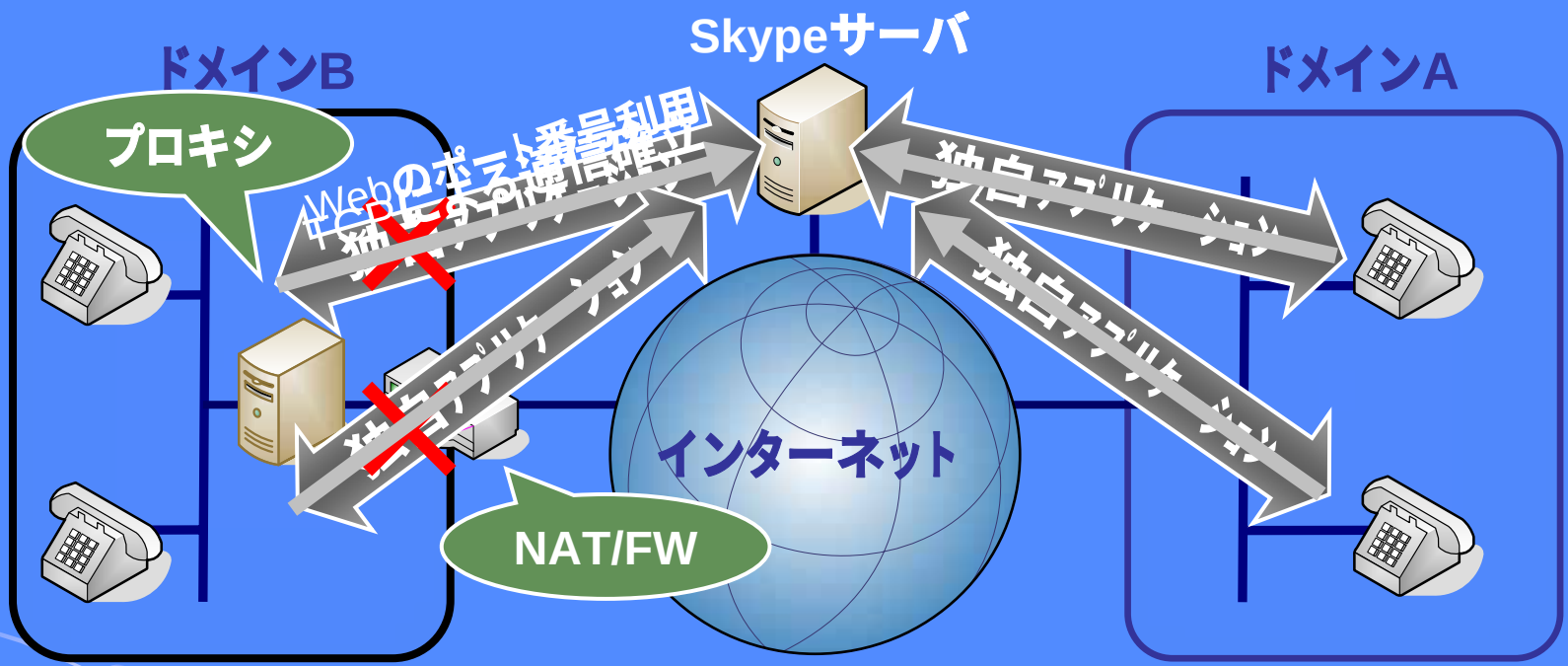
2. SIP (Session Initiation Protocol)

VoIP (音声通信技術全般) のセッション開始プロトコルとしてSIPが普及している.



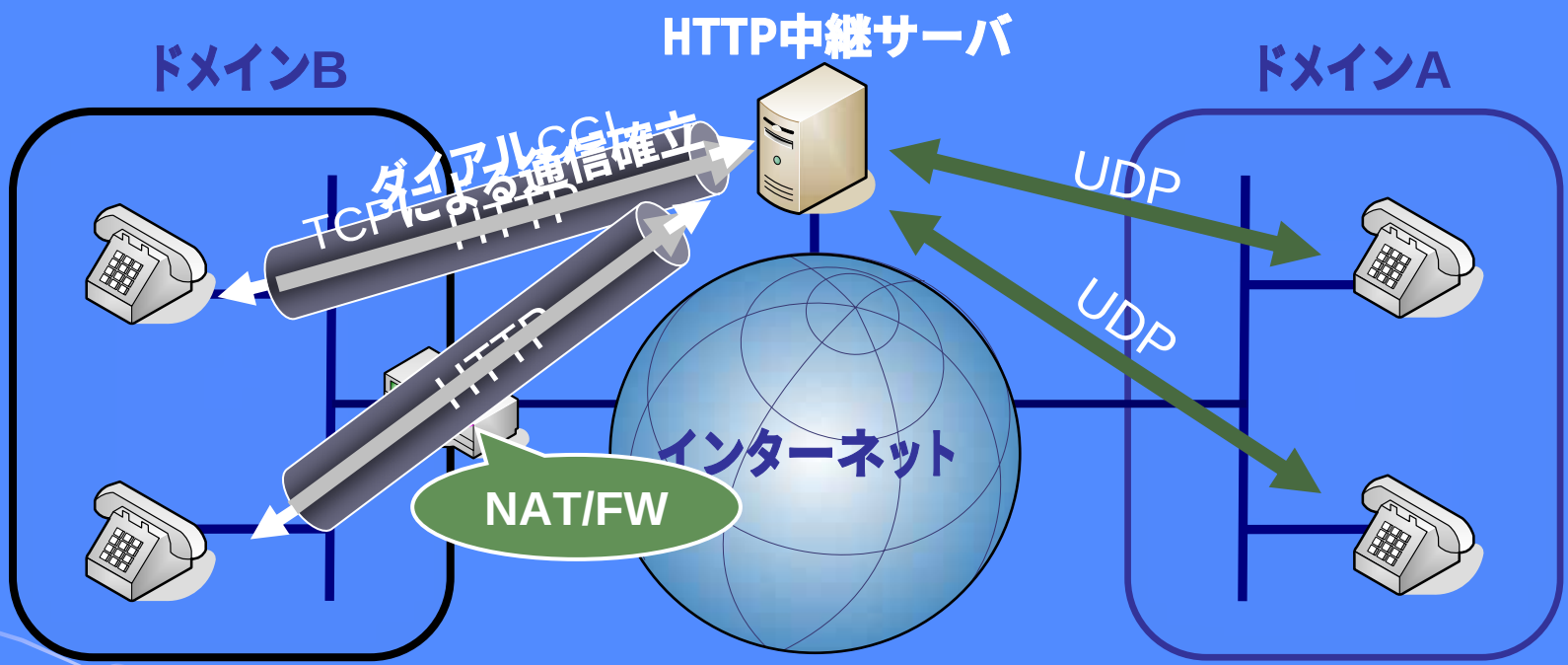
3．既存のファイアウォール通過VoIP

3．1．Skype



- 内部の端末から先にセッションを確立することでNAT解決
- 独自アプリケーションで80番ポートを利用してFW通過
  - HTTPプロキシを通過できない
  - セキュリティに信頼性がない

3．2．HCAP



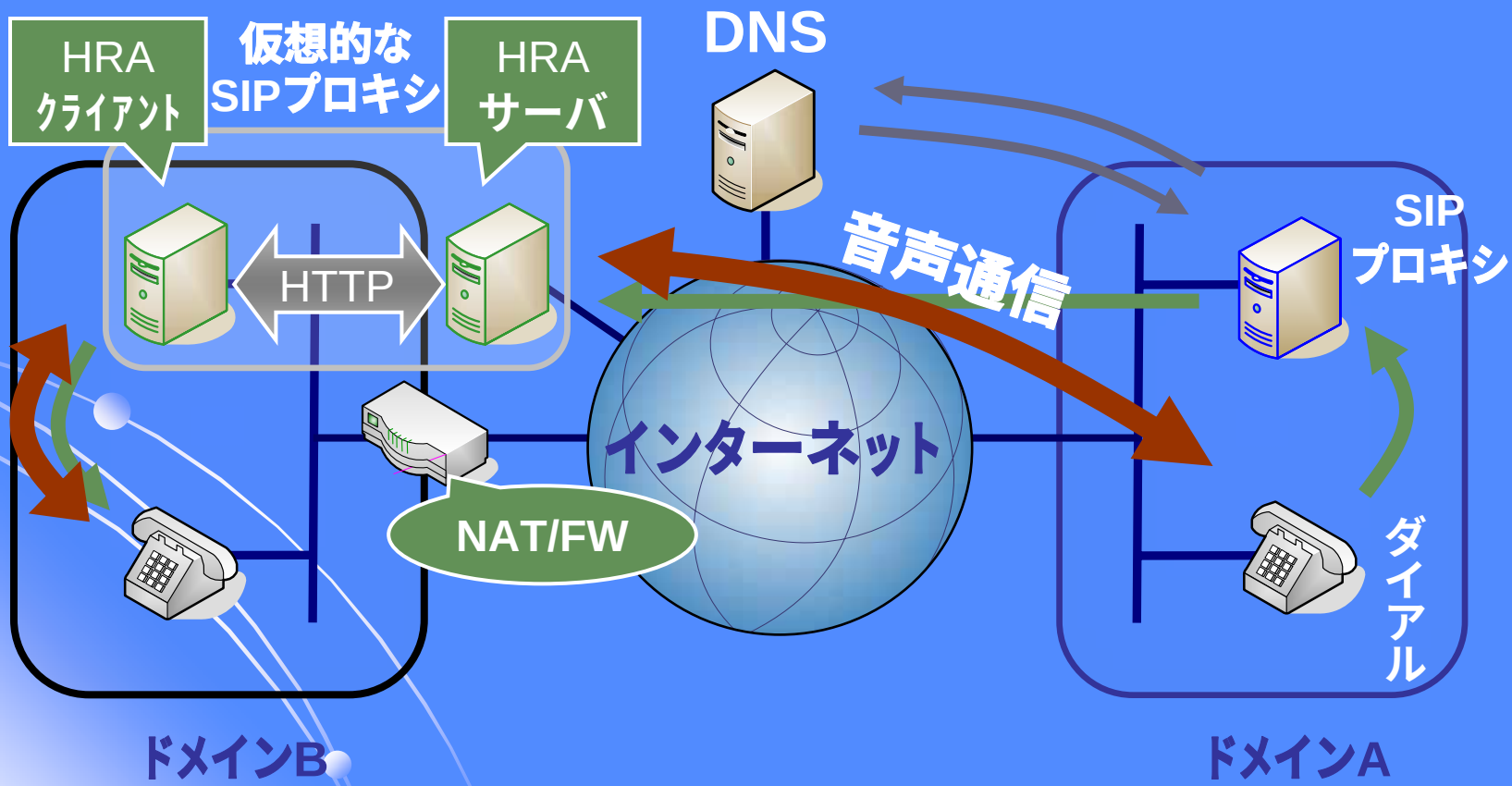
- FW・NATの無いドメインからはUDPが利用できる
- 端末それぞれからHTTP中継サーバへ常時接続を行う
  - ファイアウォール上に無駄なトラフィック
  - SIPとの互換性の問題

4．提案システム

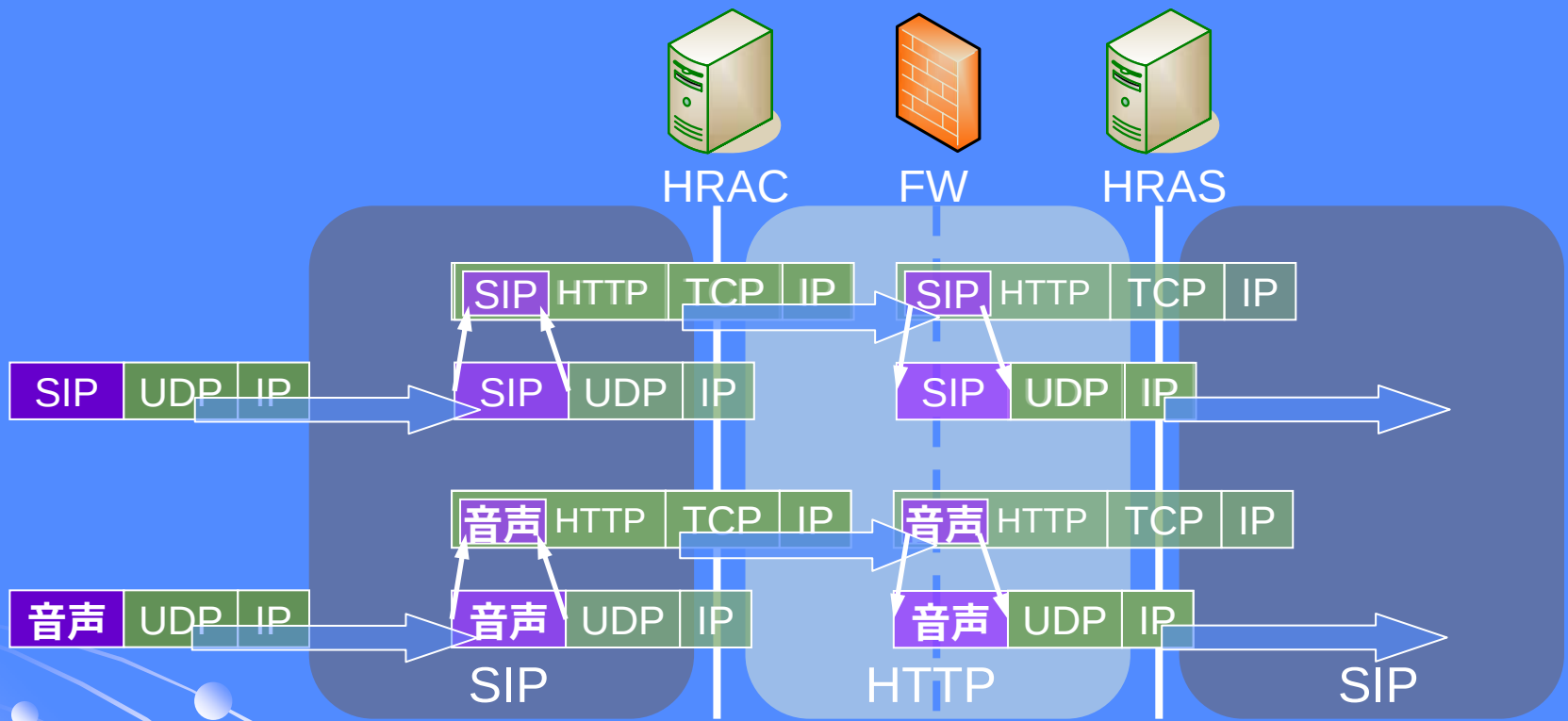
- HTTPに埋め込む方式
- ファイアウォール上のトラフィック
- SIPとの互換性

4．1．提案システムの構成

SIPベースで2つのHRA (Half Relay Agent)間に予めHTTPトンネルを作り、FW・NAT・プロキシを通過

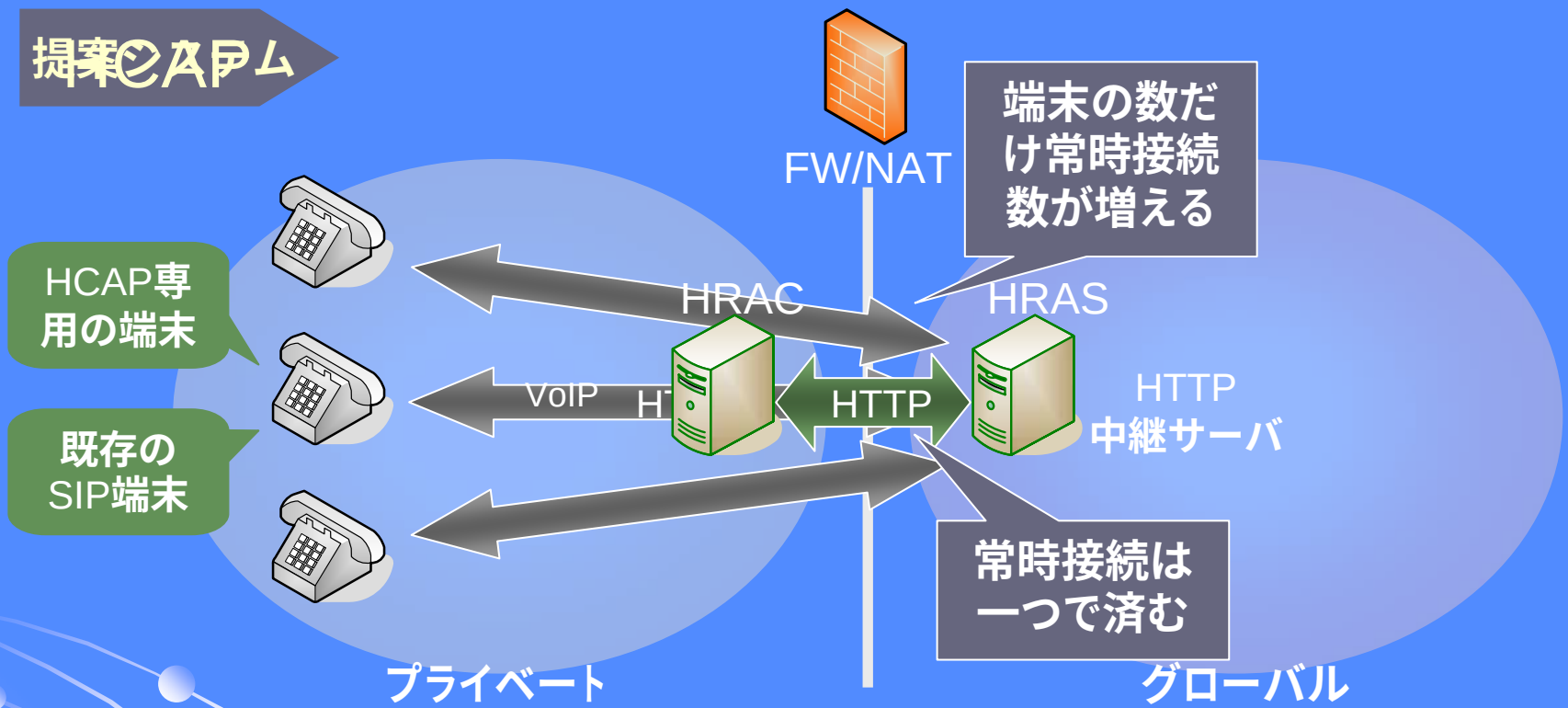


4．2．HRAその1



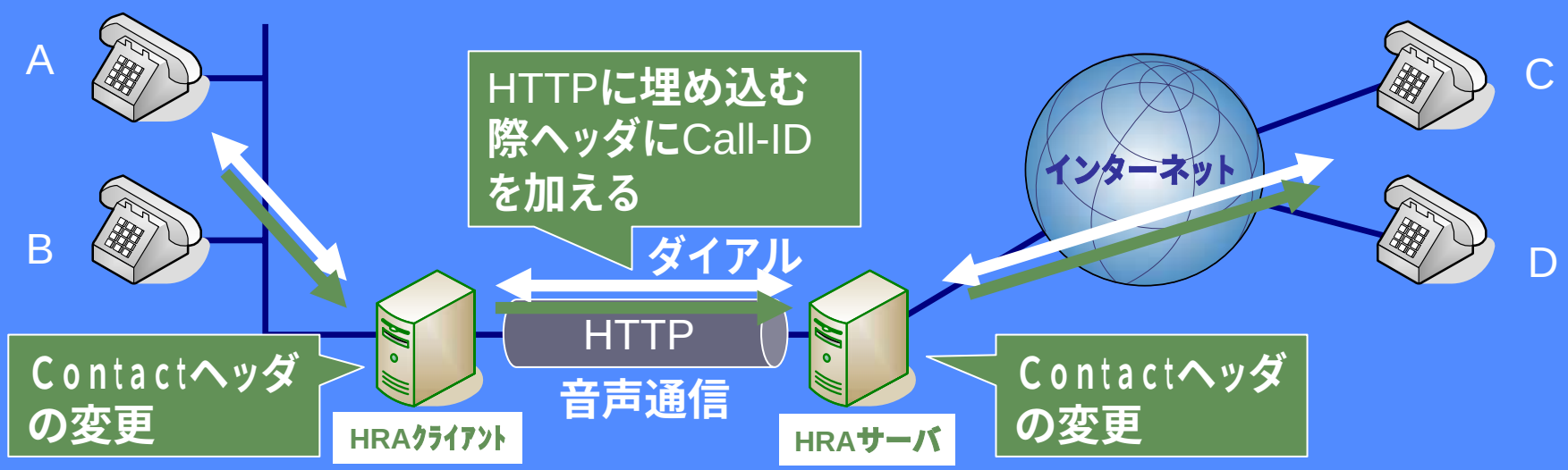
- SIPメッセージをHTTPに埋め込んでファイアウォールを通過
  - HTTPプロキシも通過できる
  - 既存のSIPとの互換性が大きい
- 音声データもHTTPに埋め込みファイアウォールを通過させる

4．3．HRAその2



- FWをまたいでHRACとHRASを設置
  - ファイアウォール上のトラフィックが最小限に抑えられる
  - 端末は既存のSIP対応のものが利用できる

4．4．音声通信の識別



Call-ID	端末情報
100	A
101	B
・・・	・・・

Call-ID	端末情報
100	C
101	D
・・・	・・・

※ダイアル時はSIPメッセージに端末情報が含まれているのでテーブル不要

テーブルをダイアル時にSIPメッセージと端末情報から作成

↓

音声パケット中継の際テーブルを利用して中継

5．セッション確立方式の比較

	FW 通過	NAT 通過	ﾌﾟﾛｷｼ 通過	SIPの 互換	ﾃﾞｨﾚｲ
Linphone (SIP)	×	×	×	○	○
HCAP	○	○	○	×	△
Skype	○	○	×	×	△
提案システム	○	○	○	○	△

提案システムの特徴

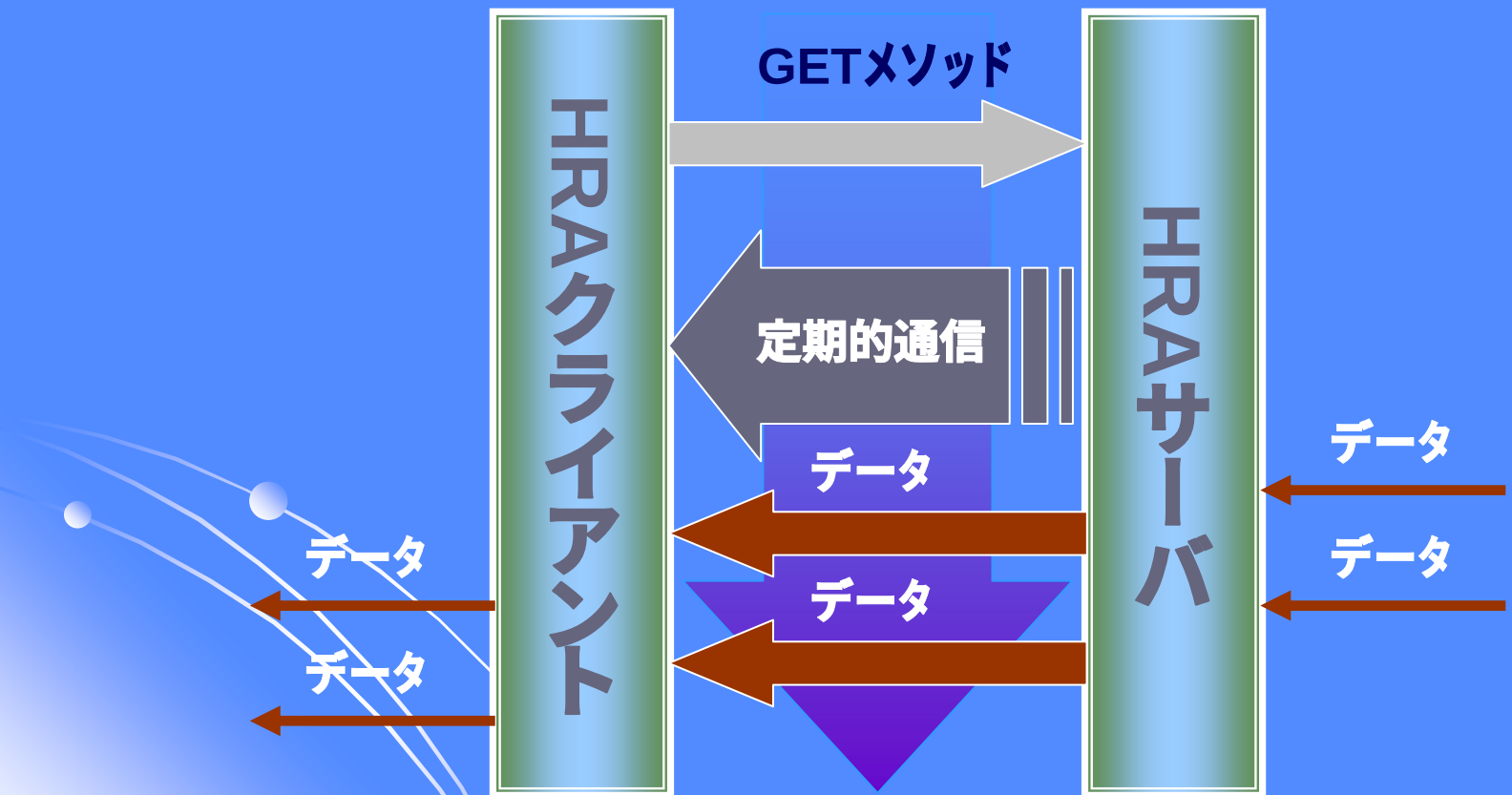
- FW･NAT･プロキシ全て通過可能
- SIPベースでSIPとの互換性が高い
- TCPを利用するためディレイは劣るが30msec以内
  （IP電話として支障なく利用できるとされるパケットディレイは400～150msec以下）

6．まとめ

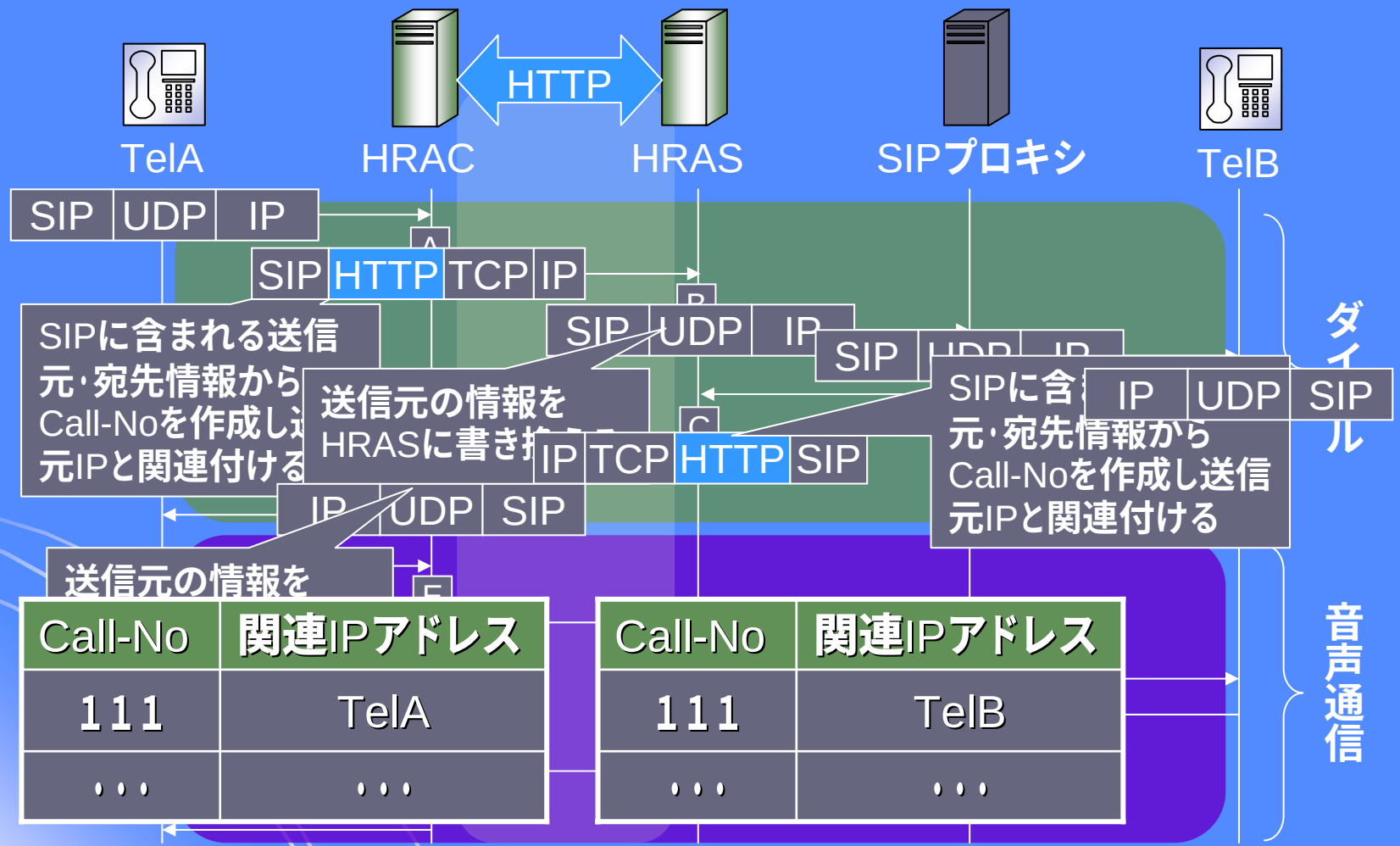
- これまで行ったこと
  - システムの提案
  - セッション確立方式の評価
  - 提案システム導入によるディレイの見積もり
- 今後の課題
  - 両端末が通信を制限された環境にある際の検討
  - TCPによる揺らぎ修正や再送による音声の劣化

おわり

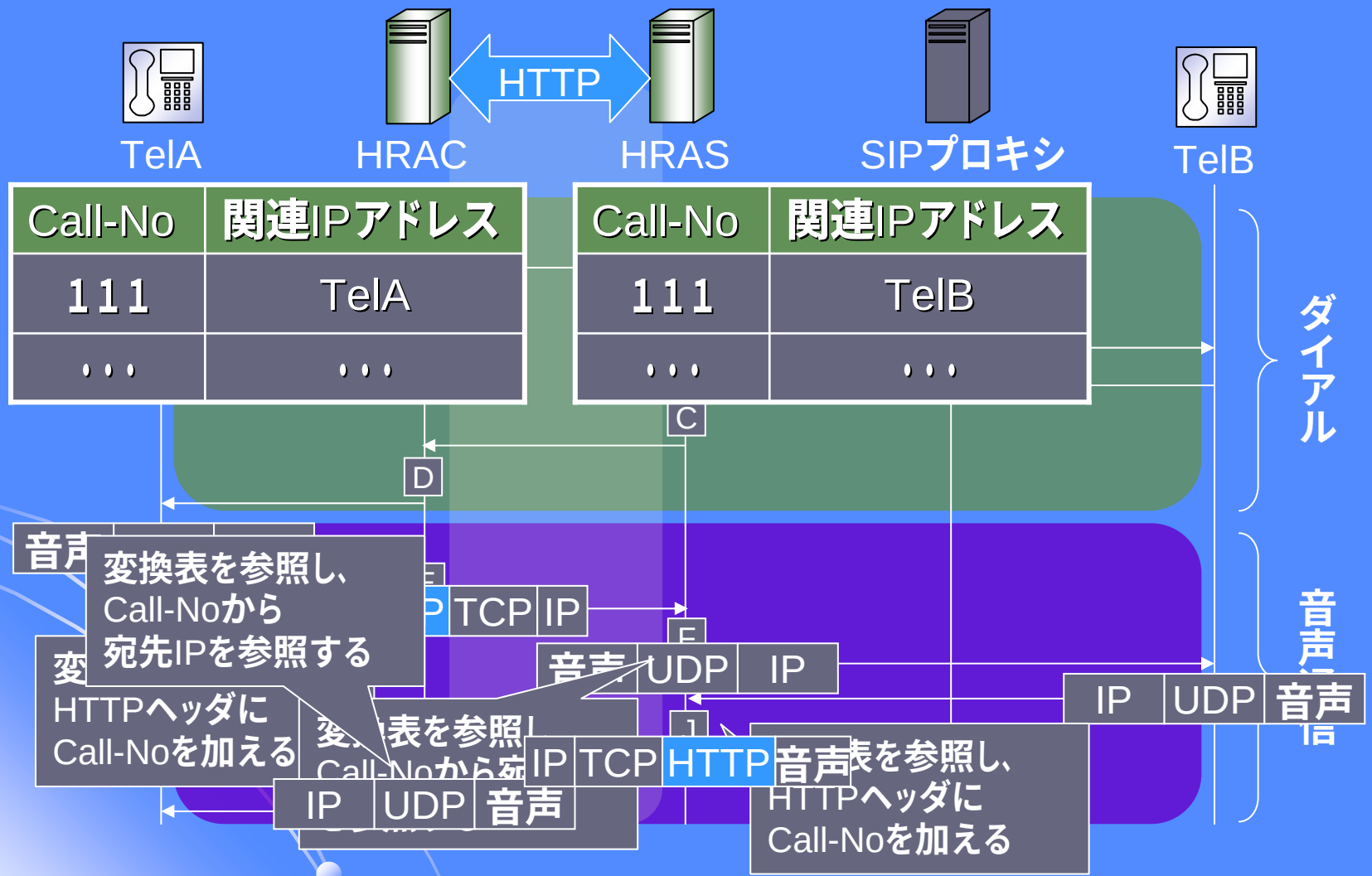
捕捉1．セッションの確立



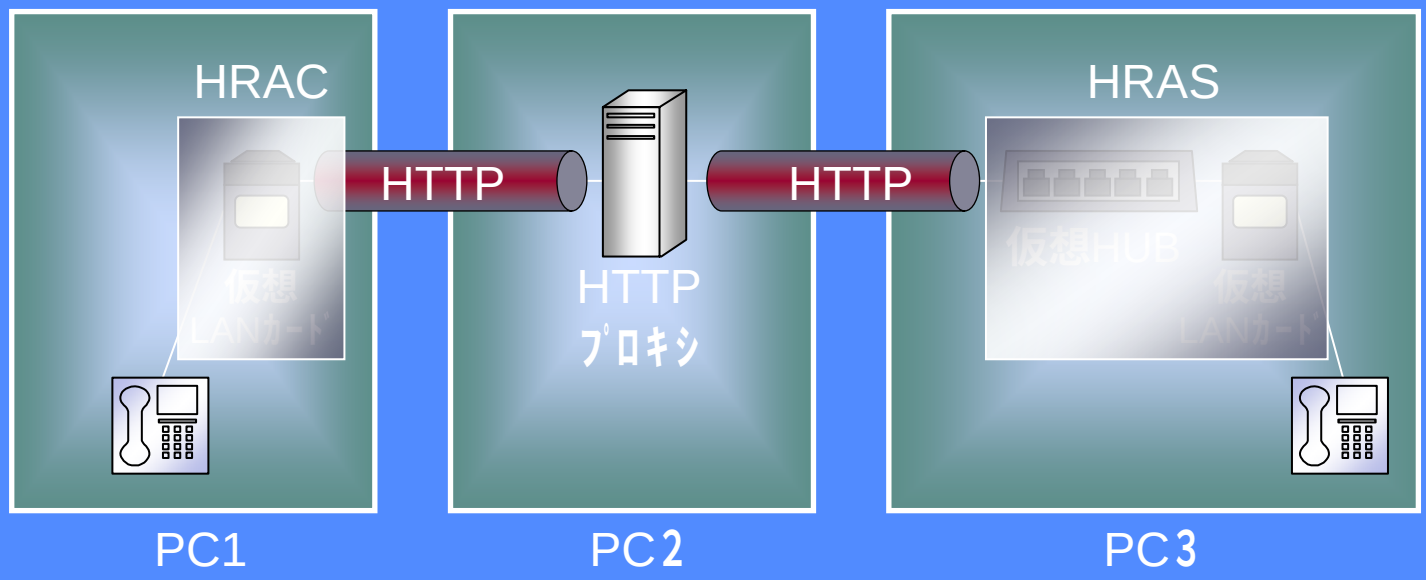
捕捉2．音声データ中継の準備



捕捉2．音声データ中継の準備

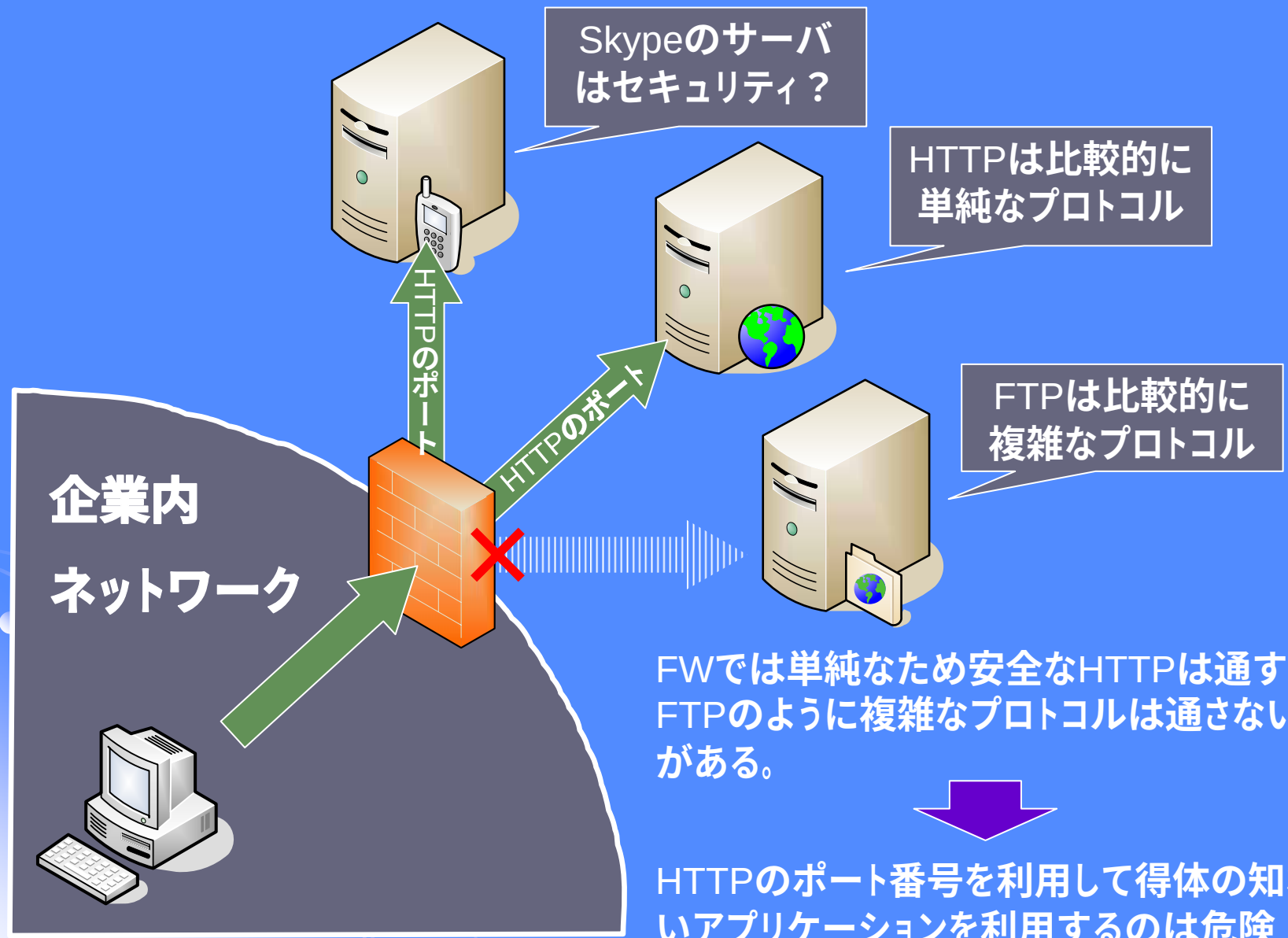


捕捉3．ディレイの見積もり



	ディレイ(sec)
エンドトゥエンド	0.01613120
プロキシ	0.01499205
ルータ	0.00035500
見積もり（プロキシあり）	0.02323120〜0.03033120
見積もり（プロキシなし）	0.00823915〜0.01533915

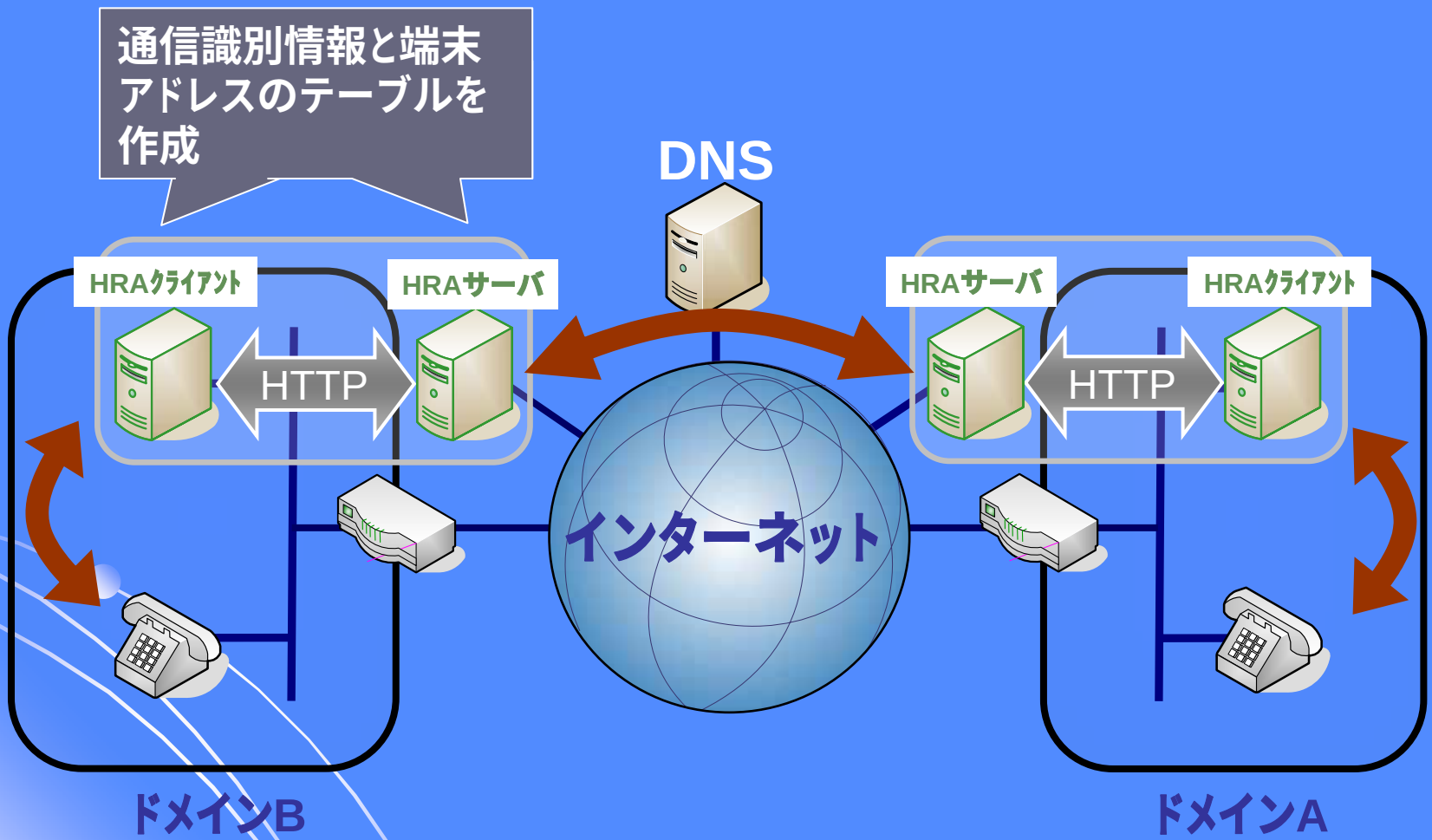
捕捉4．Skypeのセキュリティ信頼性



FWでは単純なため安全なHTTPは通すが
FTPのように複雑なプロトコルは通さない場合
がある。

HTTPのポート番号を利用して得体の知れな
いアプリケーションを利用するのは危険

捕捉5．両端末がHRAを利用する場合



捕捉6．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
ｱﾌﾟﾘｹｰｼｮﾝ

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