ファイアウォールを通過するIP電話の研究

東海ものづくり創生協議会
平成19年8月28日
名城大学　渡邊　晃

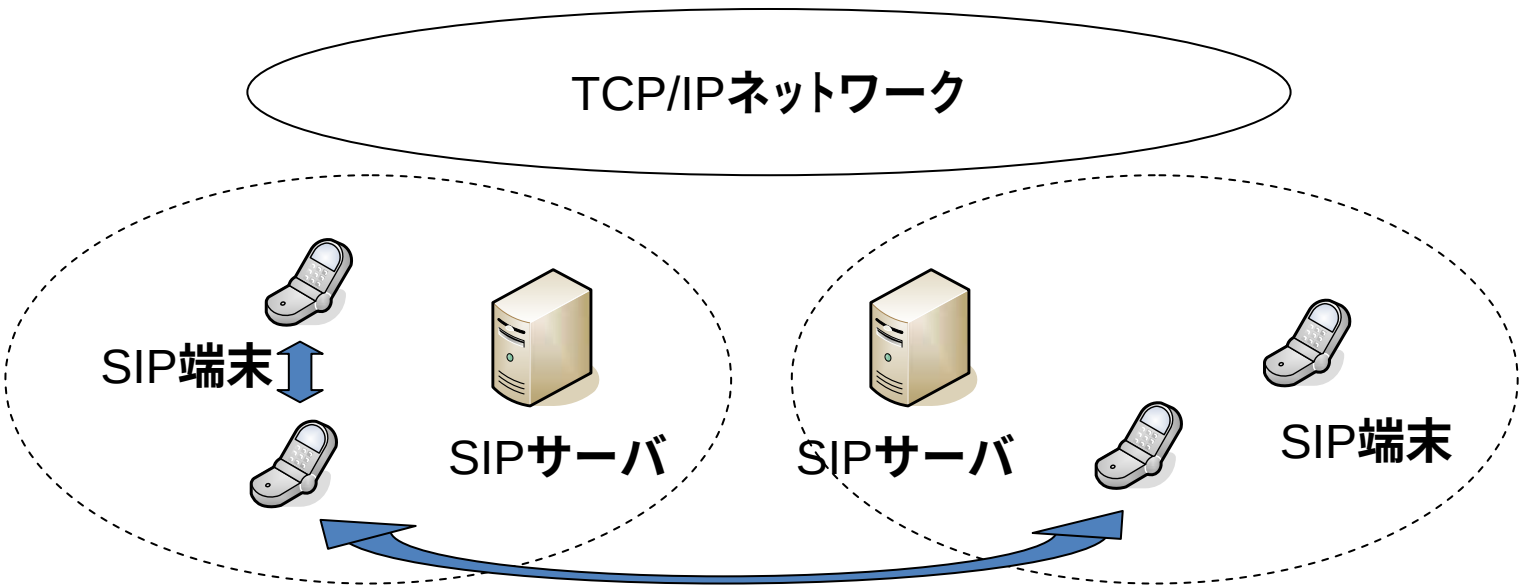
提案内容

SoFW (SIP over FireWall)

- SIP端末を前提としたVoIP通信
- 『安全に』ファイアウォール（含：NAT)を越える
- 企業のセキュリティポリシーに影響を与えない
- 既存のネットワーク設備に影響を与えない
- VoIP以外への拡張性がある

SIP ; Sesshon Initiation Protocol

- **呼設定を実現するプロトコル**、RFC3261
- WindowsXP**に標準で搭載されている**
- **次世代携帯電話のバックボーンで採用されることが決まっている**
- **コンテンツは音声、動画、テキスト**

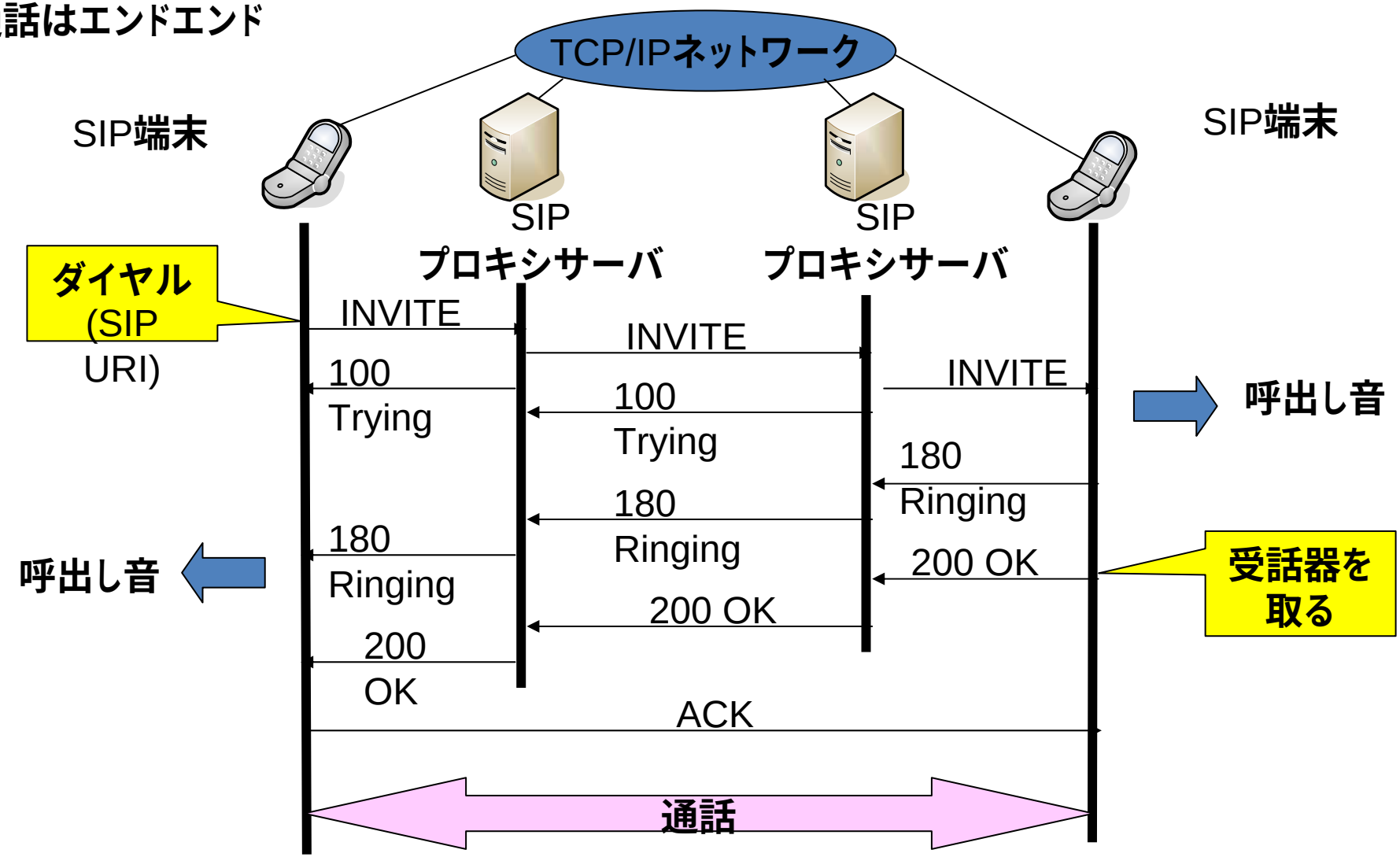


SIP URI (SIP Uniform Resource Identifier)
例 sip:wata@ccmfs.meijo-u.ac.jp

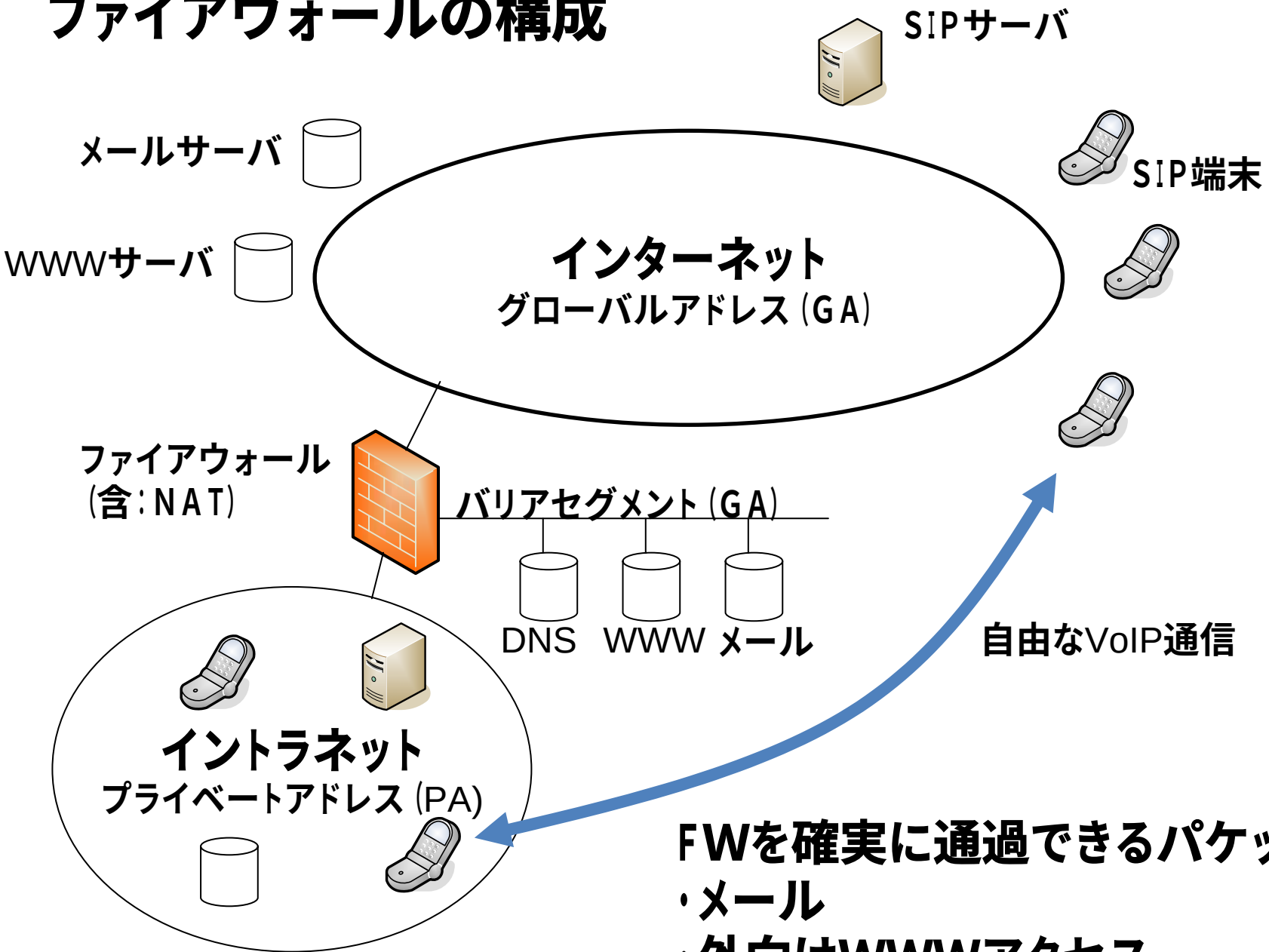
SIPの流れ

ダイヤルはSIPサーバ経由

通話はエンドエンド



ファイアウォールの構成



FWを確実に通過できるパケット

- メール
- 外向けWWWアクセス

既存のファイアウォール越えシステム

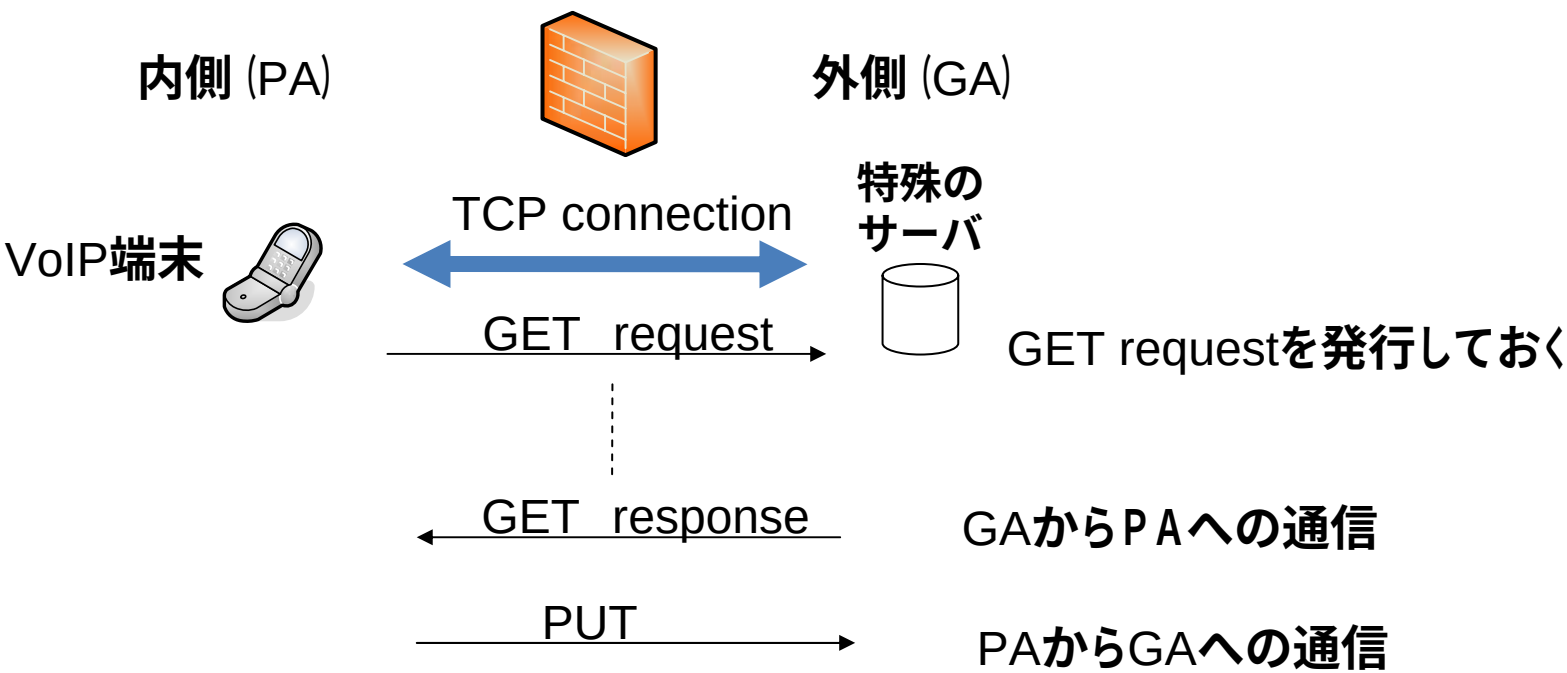
①HTTPトンネル方式

Skype、SoftEther、SoFW (SIP over FireWall)

②ファイアウォール改造方式　→既存システムに影響あり

SIP機能の組み込みなど

HTTPトンネルの実現方法



Skype

通信品質よい、使い勝手よい→企業でも注目されているIP電話

旧Skype社（現在eBay配下）

FW,NAT**通過できる**

Skype**を制約する動き**

・標準を使っていない。特定の企業に縛られる。

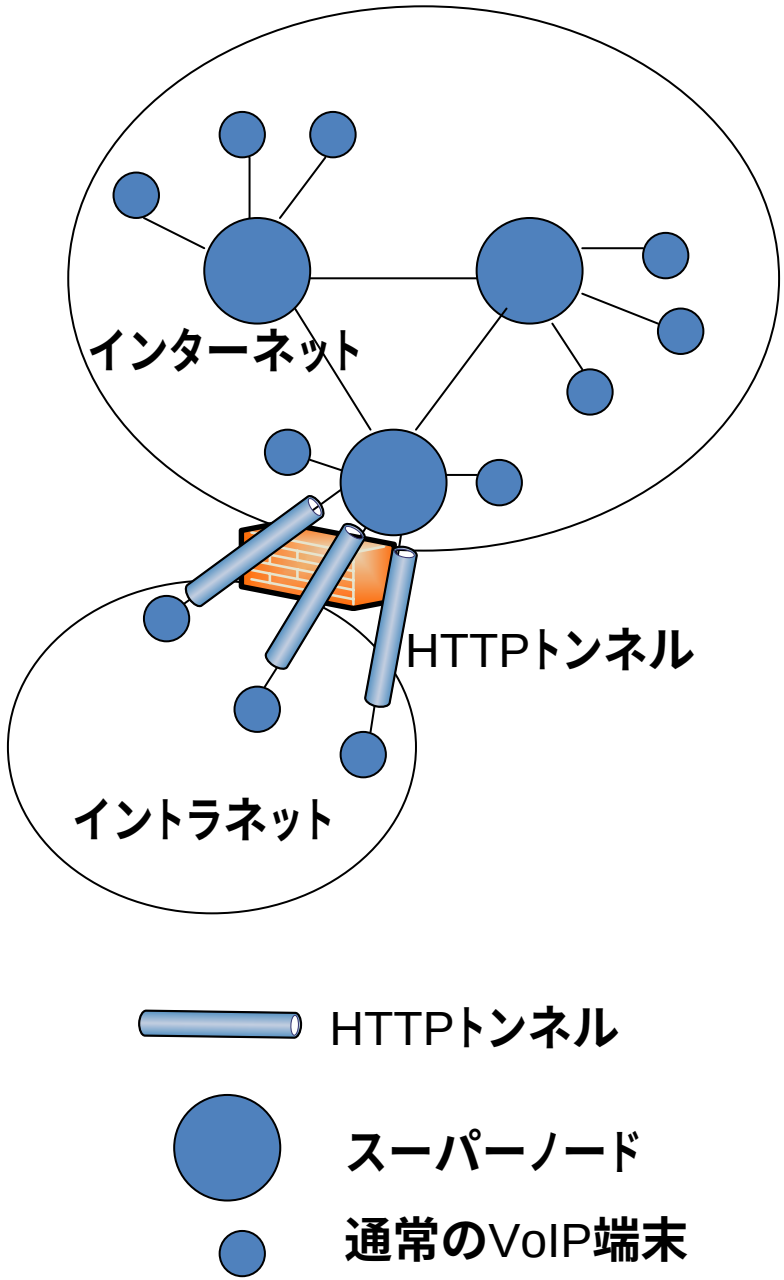
・脆弱性という観点では未知。脆弱性を悪用される可能性。

・Skypeが備えるファイル転送機能やチャット機能などが，セキュリティ・ホールになりうる

・暗号化しており利用状況が管理できない。法令順守の妨げ。機密情報の漏洩の可能性を把握できない。

・規制している国がある（中国、UAEなど、電話通信事業に痛手）。

・勝手にスーパーノードに指定される可能性。



SoftEther (PacketiX)

仮想HUBと仮想LANカードにより容易に仮想イーサネットを構築

筑波大学生が開発。

FW,NATを通過できる

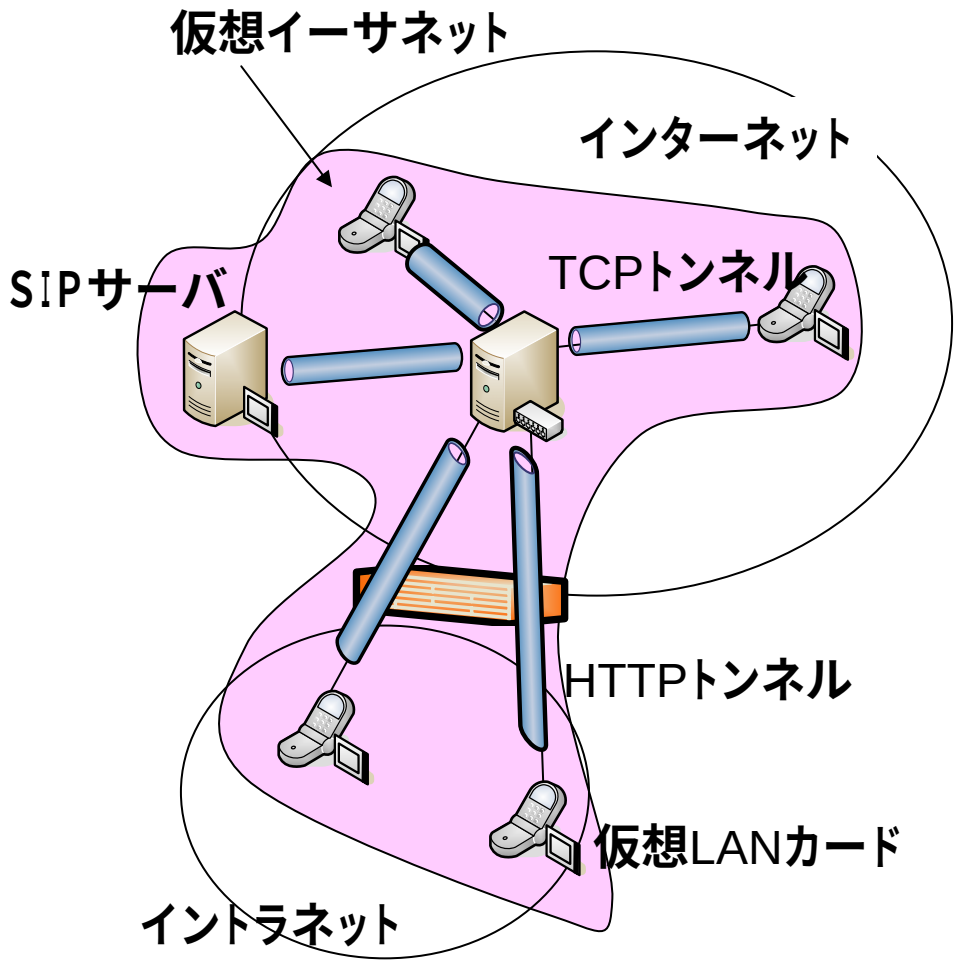
SoftEtherを制約する動き

・仮想イーサネット内で自由に通信が可能

←ファイアァイアウォールの意味がない
ネットワーク管理者から見ると脅威

・通信内容を把握できない、情報漏洩の可能性

・仮想ネットワーク内では統一したアドレス管理が必要




HTTP/TCPトンネル

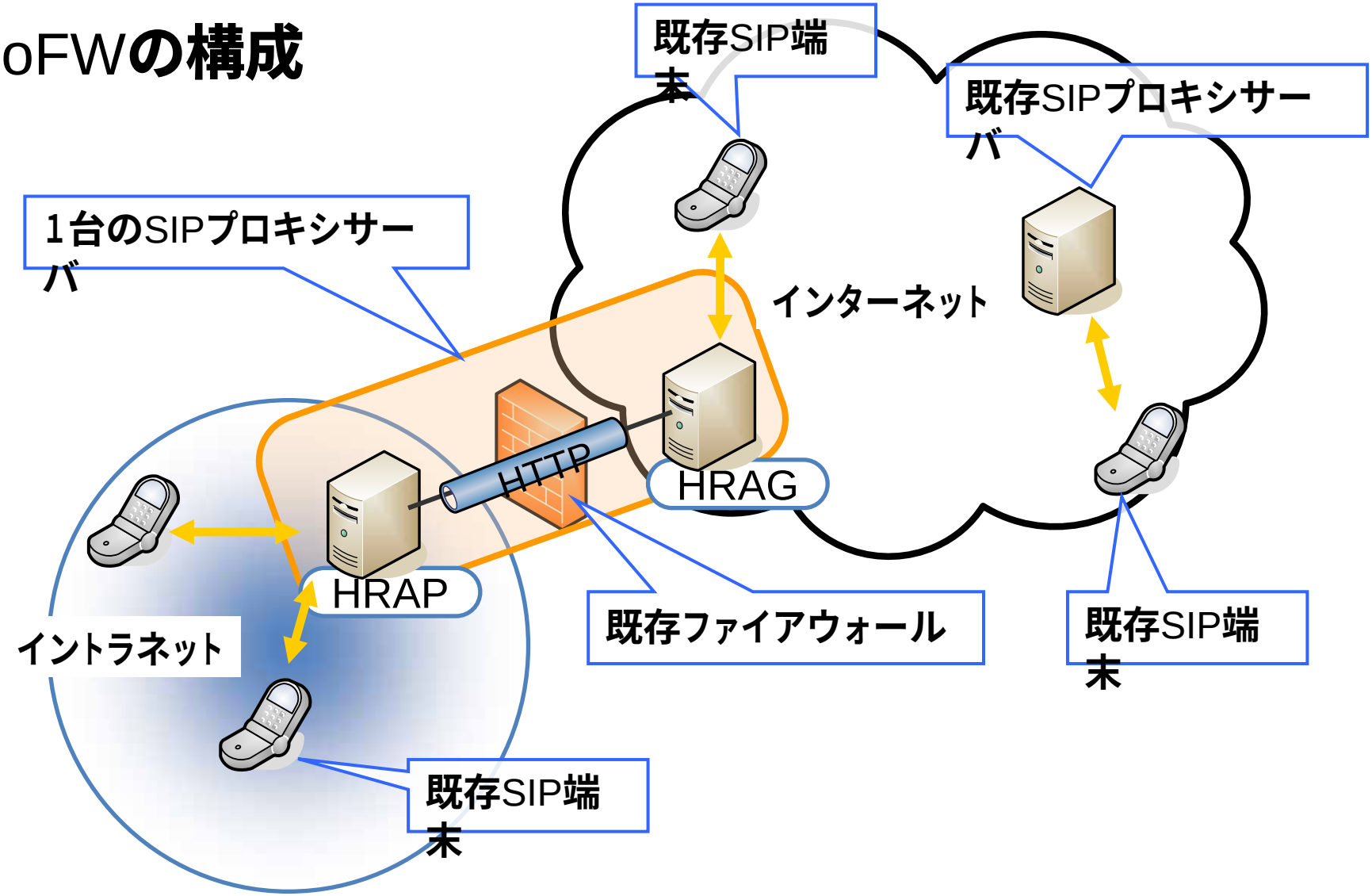

仮想LANカード


仮想HUB

SoFW (SIP over FireWall)

- SIP端末を前提としたVoIP通信
- 『安全に』ファイアウォール（含：NAT)を越える
- 企業のセキュリティポリシーに影響を与えない
- 既存のネットワーク設備に影響を与えない
- VoIP以外への拡張性がある

SoFWの構成



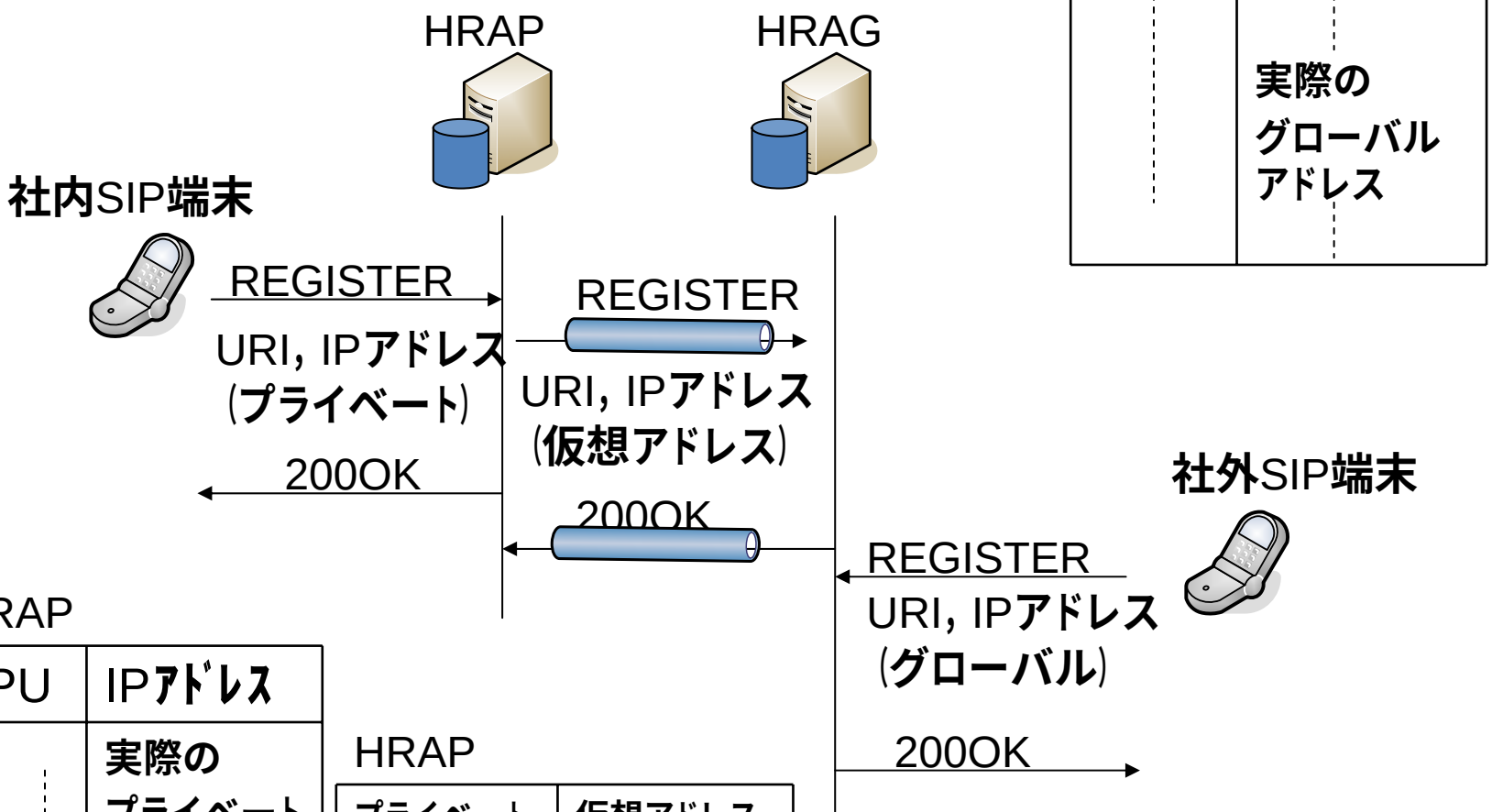
HRAG（Half Relay Agent for Global）：**グローバルアドレス空間に設置**

HRAP（Half Relay Agent for Private）：**プライベートアドレス空間に設置**

HRAP/HRAGが管理する情報

HRAG

SIPU	IPｱﾄﾞﾚｽ
RI	仮想アドレス 実際の グローバル アドレス



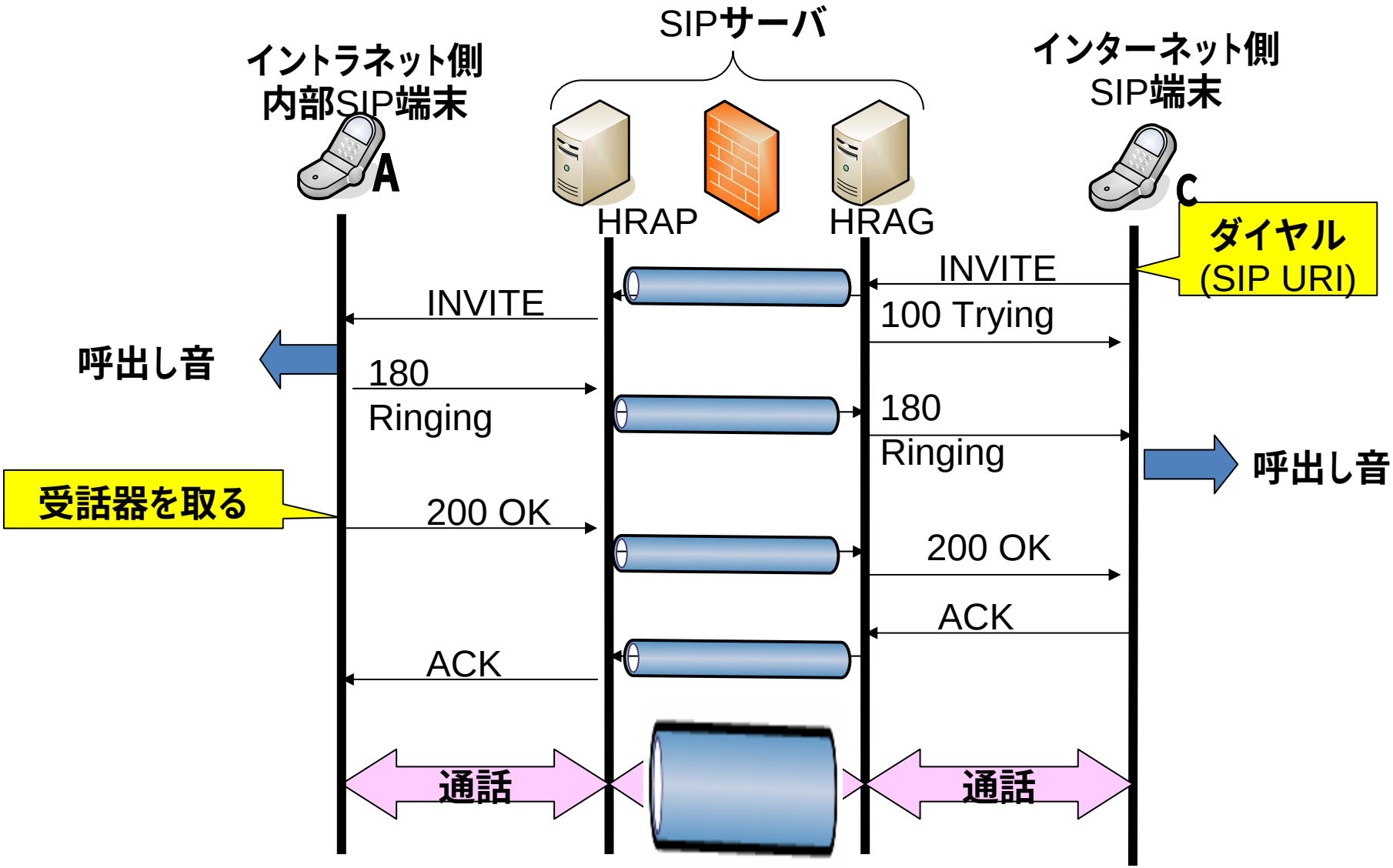
HRAP

SIPU	IPｱﾄﾞﾚｽ
RI	実際の プライベート アドレス

HRAP

プライベート アドレス	仮想アドレス

ファイアウォールを跨るVoIP（C⇒A）



HRAP/HRAGがINVITE/200OK内のメッセージを書き換える。

AはHRAPが、CはHRAGが通信相手に見える

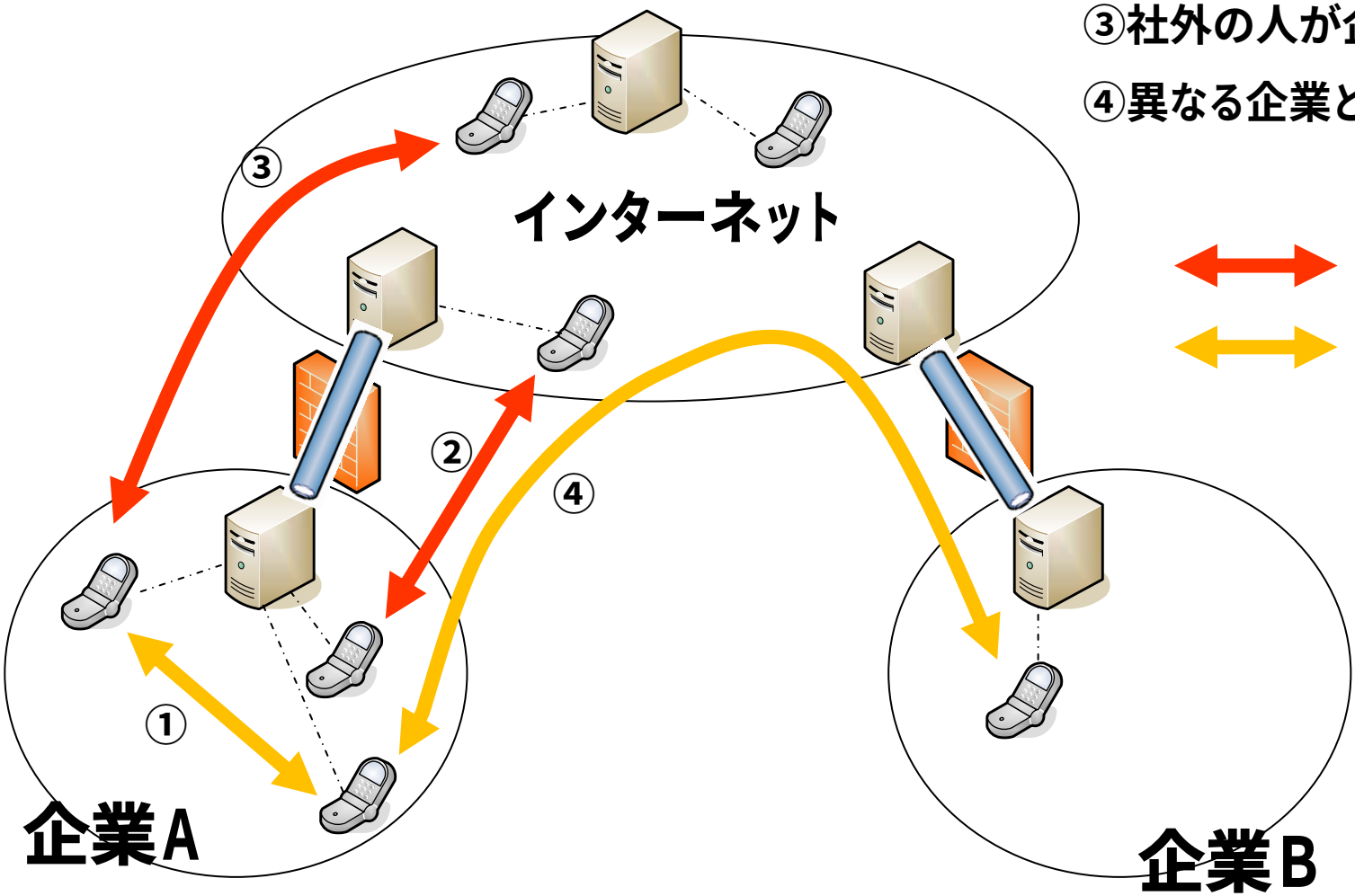
実現可能な通話形態

①企業内VoIP

②出張者が企業内とVoIP

③社外の人が企業内とVoIP

④異なる企業どうしのVoIP



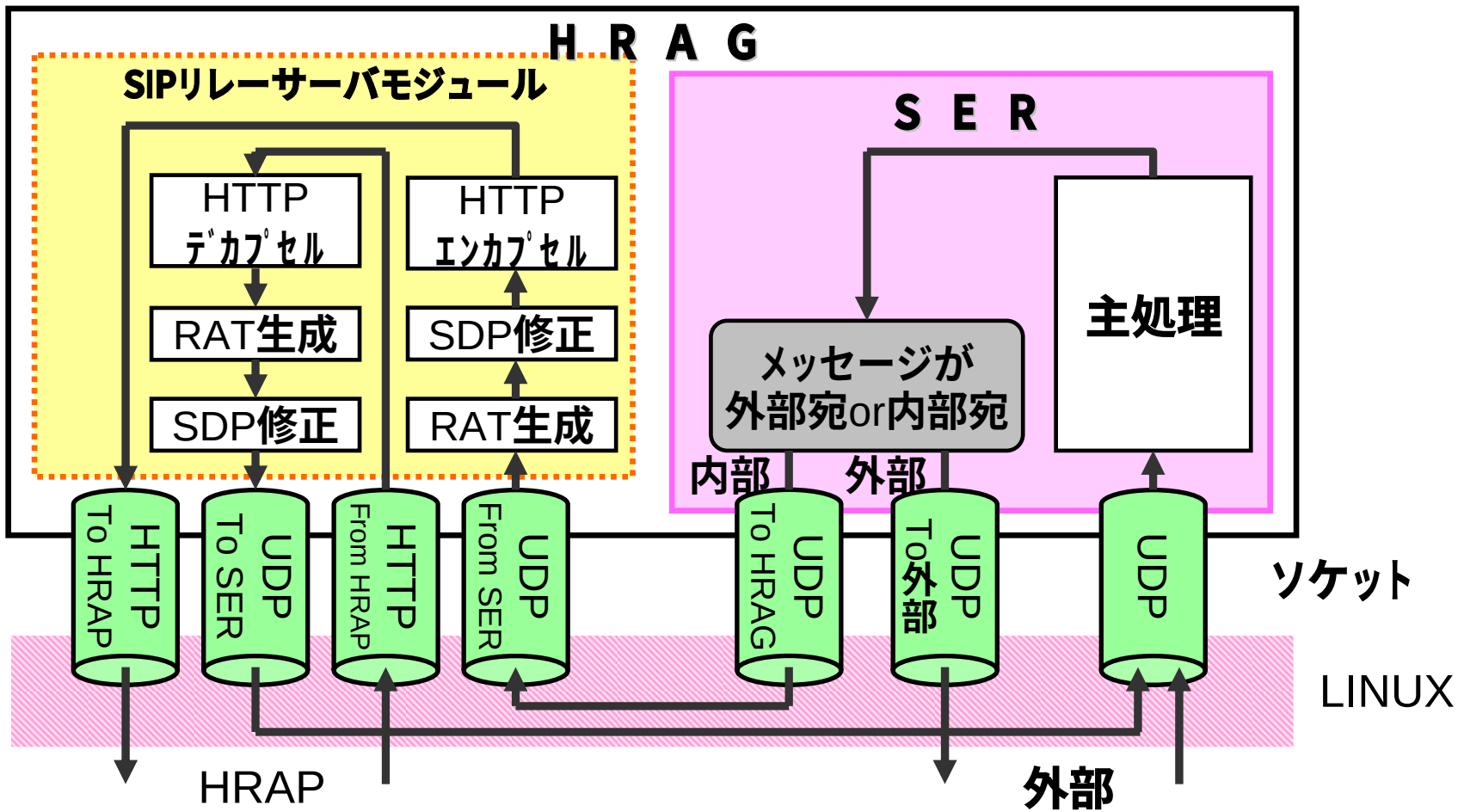
実現済み

計画

(今年度中)

実装

- Linux (Fedora core3.0)のアプリケーションとして実装
- SIPサーバとしてSER (SIP Express Router)を採用、一部書き換え



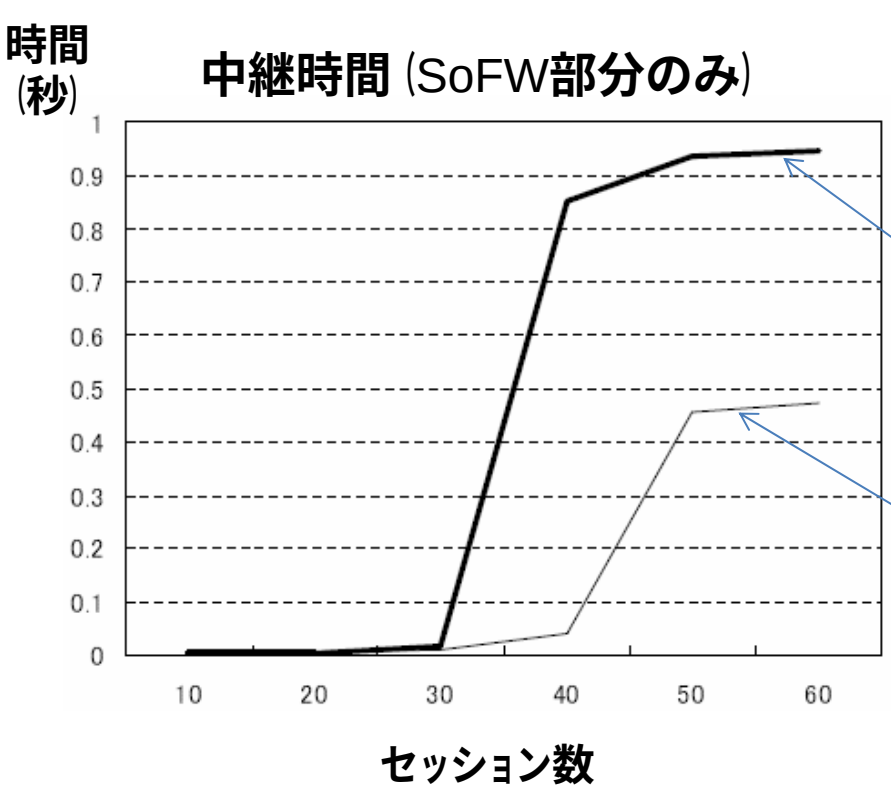
SDP; Session Description Protocol

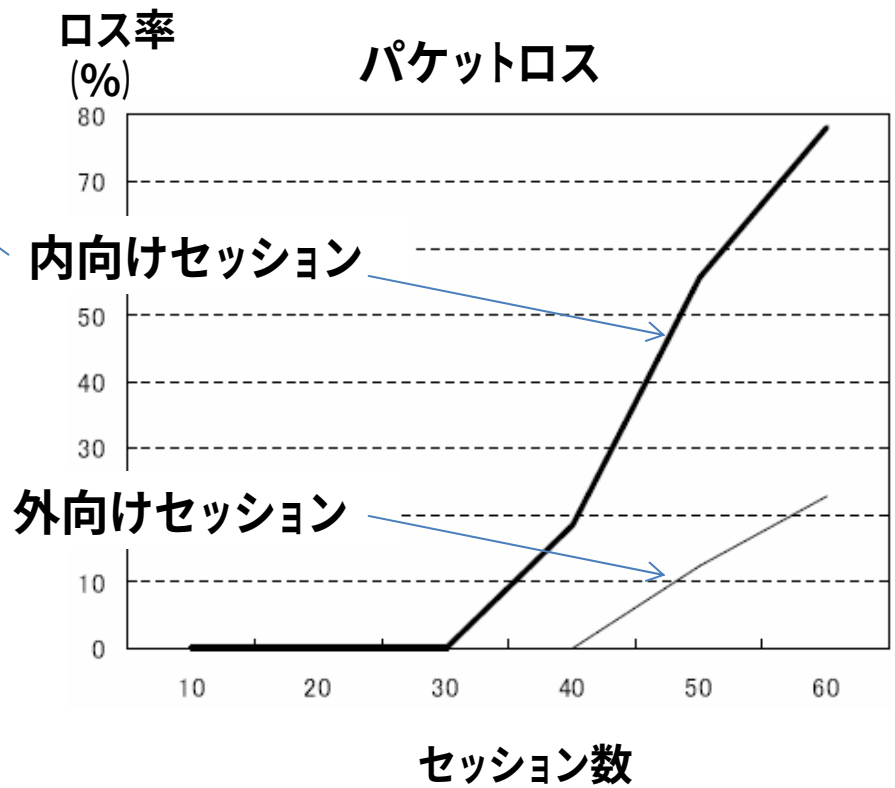
RAT; Relay Agent Table (独自)

実験データ1

・SoFW評価システムを構築し、IP電話セッション数とともにパケット中継時間とパケットロスがどのように変化するかを調査

・30セッションを越えた時点で急激に遅延、ロスが増加

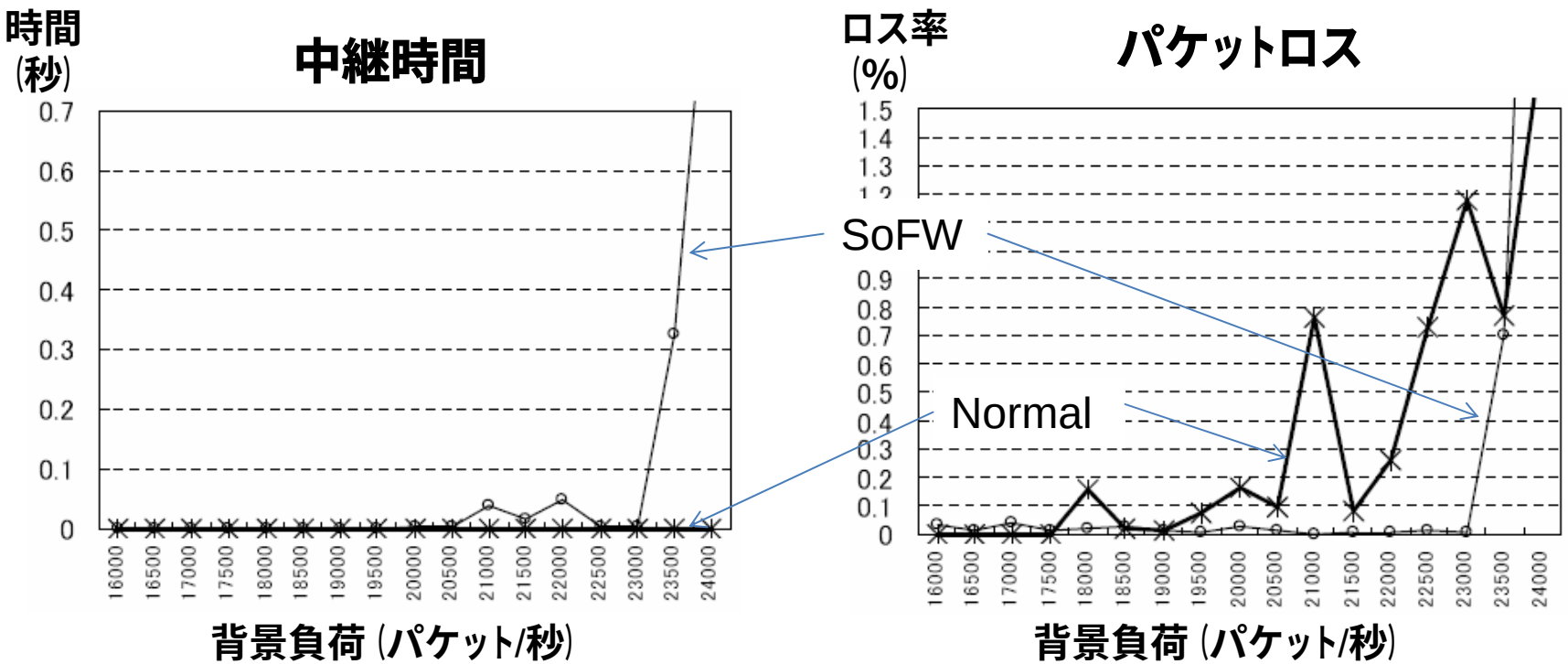




実験データ2

・背景負荷の増加とともにパケット中継時間とパケットロスがどのように変化するかを調査

・SoFWの中継時間、ロスが急激に増加する時点で、Normal（SoFWなし）のロスが許容範囲を越えている



まとめ

SoFW (SIP over FireWall)

- ファイアウォールを安全に越えるIP電話の提案
- 既存の設備には一切手を加える必要がない
- 試作完了，現在拡張開発中

参考文献:

伊藤，鹿間，渡邊，

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，

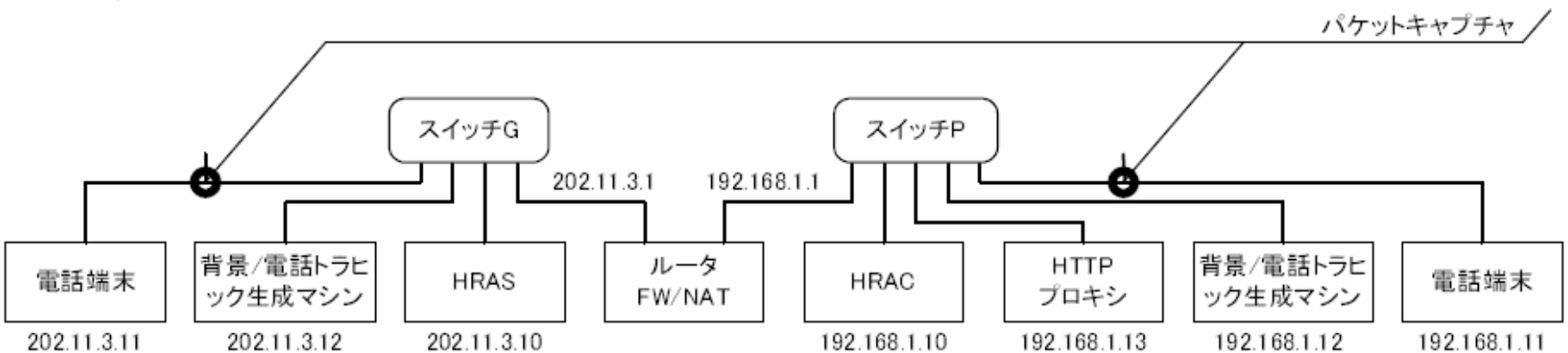
情報処理学会論文誌，Vol.48，No.2，pp.400-411，Feb.2007．

評価システムの構成

装置仕様

装置	仕様	
HRAS /HRAC	CPU	Intel Pentium 2.8GHz
	メモリ	512MB
	NIC	Broadcom Tigon3 100BASE-TX
FW/NAT /Proxy	CPU	Intel Pentium 600MHz
	メモリ	256MB
	NIC	Global: Silicon Integrated System crop 100BASE-TX
		Privete: ADMtek FNW-9803-T 10/100BASE-TX
外部用端末	CPU	Intel Pentium 3.4GHz
	メモリ	1GB
	NIC	Broadcom NetXtreme57xx 100BASE-TX
内部用端末	CPU	Intel PentiumM 1.80GHz
	メモリ	512MB
	NIC	Realtek RTL8139/810x 100BASE-TX

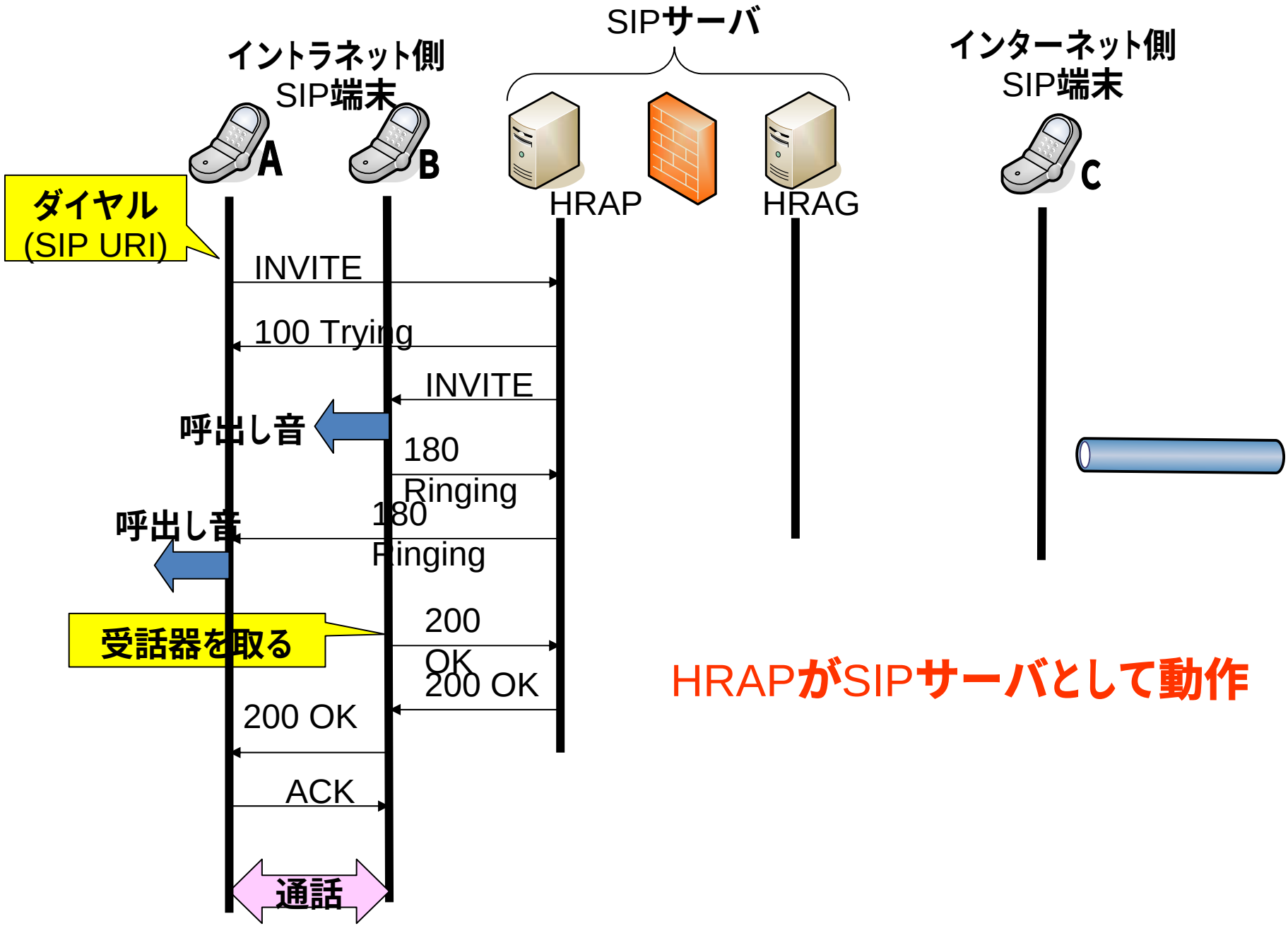
構成



IP電話の規格

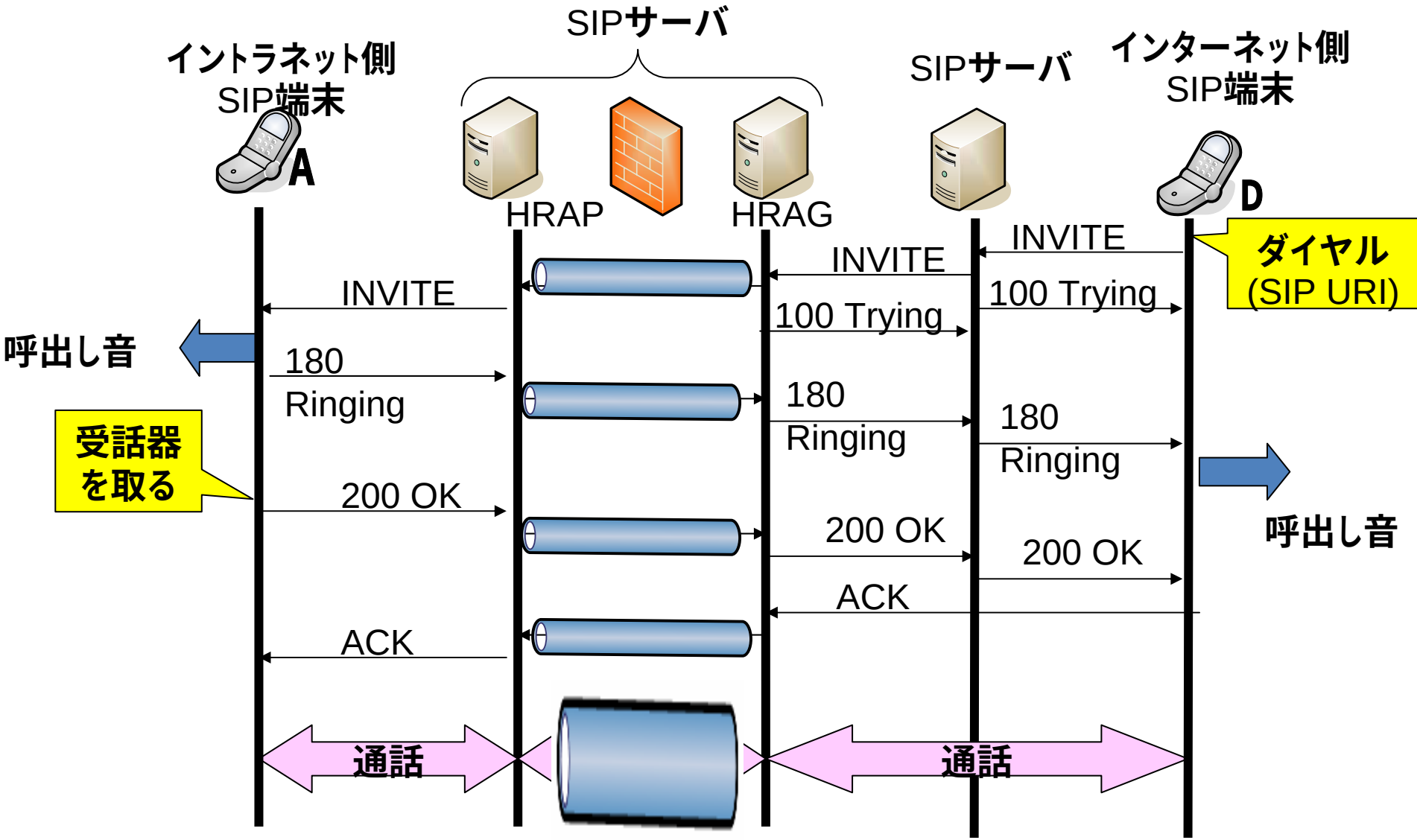
	クラスA (固定電話並)	クラスB (携帯電話並)	クラスC (許容範囲)
エンドエンド遅延 (95%確率) (総務省報告書より)	100m秒	150m秒	400m秒
パケット損失率 (ITU-T勧告より)	1×10^{-3}	1×10^{-3}	1×10^{-3}

イントラネット内のVoIP（A⇒B）



HRAPがSIPサーバとして動作

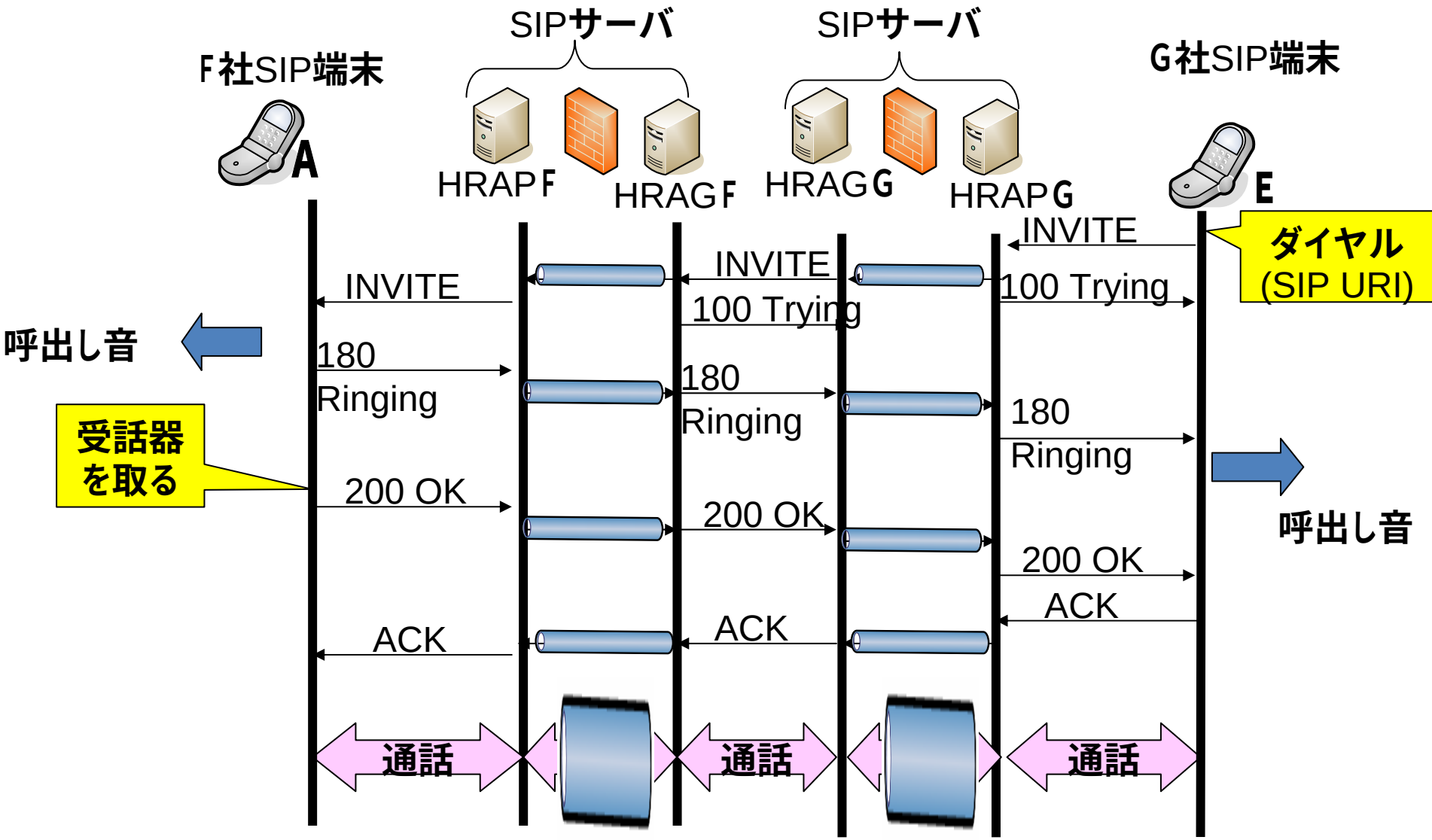
ファイアウォールを跨るVoIP（D⇒A）（SIPサーバが異なる場合）



HRAP/HRAGがINVITE/200OK内のメッセージを書き換える。

AはHRAPが、DはHRAGが通信相手に見える

異なる企業を跨るVoIP



AはHRAPFが、EはHRAPGが通信相手に見える

HRAGFはHRAGGが、HRAGGはHRAGFが通信相手に見える