本資料について

- 本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 著者：大竹八洲孝，但馬康宏，寺田松昭
- 論文名：SIPを用いた音声通話に対するNAT通過手法の提案とその実装
- 出展：情報処理学会論文誌Vol. 45 No. 3

SIPを用いた音声通話に対するNAT通過手法の提案とその実装

名城大学理工学部渡邊研究室
三浦 健吉

1. はじめに

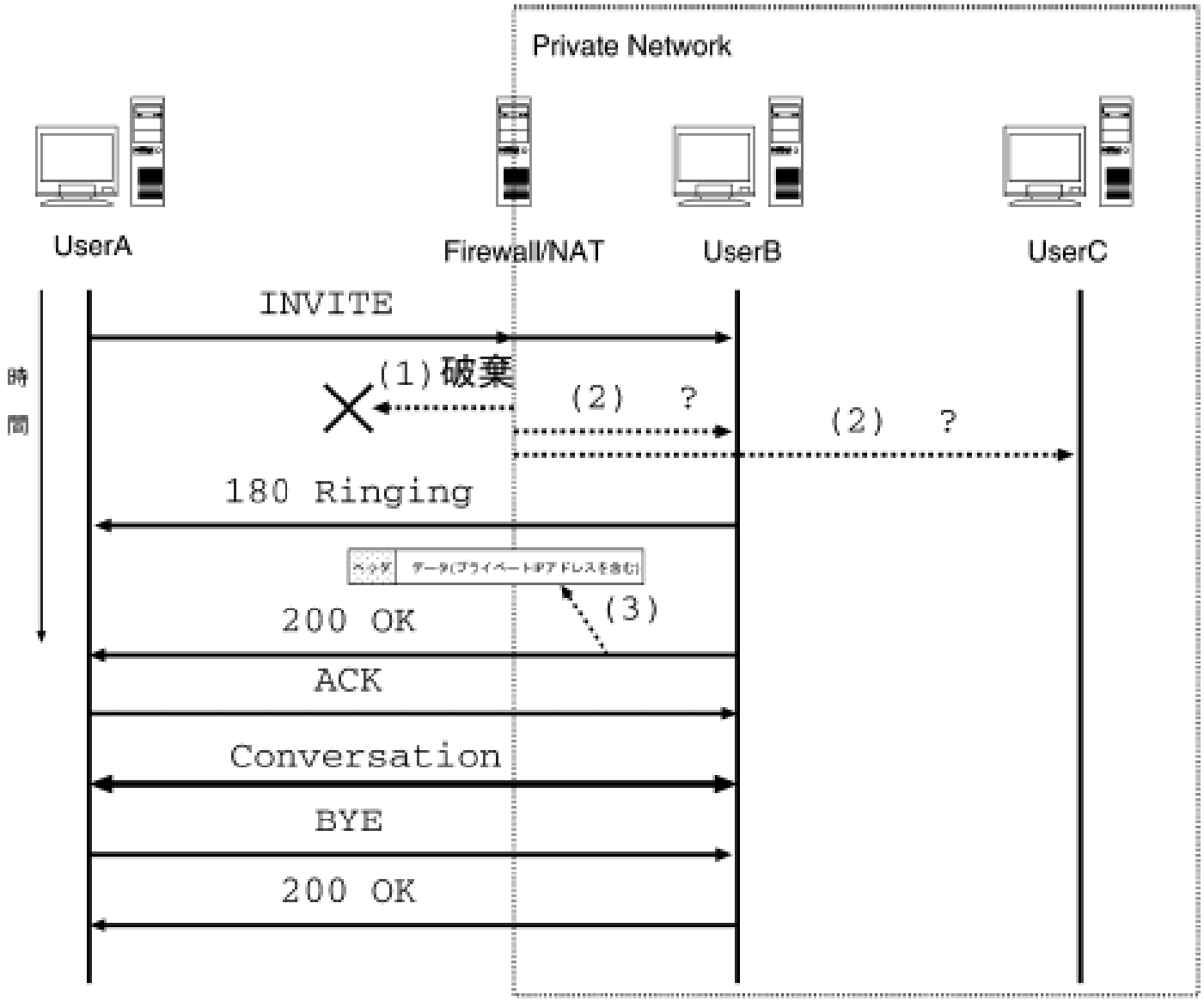
はじめに

- NAT/FW環境における問題点
  - グローバルネットワークから内部ローカルアドレス内の個々のホストに直接アクセスできない.
  - パケットのペイロード(データ部分)に含まれるネットワークアドレスやポート番号はNAT では, 変換できない.

⇒FWとSIP サーバを統合した「アプリケーションレベルゲートウェイ機能付きSIPサーバ」によるNAT 通過手法を提案

2. NAT およびファイアウォール越しの音声通話の問題点と解決方法

SIPシーケンスと問題点



(1) セキュリティルールによる破棄
(2) 宛先決定不能
(3) NAT通過によるペイロード内のアドレス変換不能

(1)セキュリティルールによる破棄

FWのセキュリティルールがSIP メッセージの着信するポート番号やトランスポートプロトコルを許可していない場合

⇒ファイアウォールはSIP メッセージヘッダを参照し，セキュリティルールによりそのメッセージは破棄される

(2) 宛先決定不能

仮にSIP メッセージを着信できるようにセキュリティルールを変更した場合

⇒ファイアウォールまでSIP メッセージを届けることが可能である

⇒しかし，このSIP メッセージが内部のどのクライアント宛なのか判断することができず，結局宛先不明なメッセージとして処理される.

(3) NAT通過によるペイロード内のアドレス変換不能

仮に外部からのINVITE 要求がローカルネットワーク内のプライベートIPアドレスを持つUserBに届いた場合

⇒通話を許可する場合，200 OK応答を返す．

⇒このSIPメッセージがNATを通過する際，パケットのヘッダ部分が書き換えられる．しかし，プライベートIPアドレスを含むデータ領域はNATでは変換されない

⇒このSIPメッセージを受け取ったUserAは，データ内容を元に応答するため，不正なアドレスとしてうまく応答できない

提案システム

- 一般的に，FW/NATを利用する環境では，それらの機能を1台の機器(ゲートウェイ)として集約する場合が多い

⇒ローカルネットワーク内部の機器が外部と通信する場合は必ずゲートウェイを介した通信となる

⇒ゲートウェイに問題点を解決する機能を取り込むことを提案

提案システム

提案システムでは

(1)SIPメッセージやセッション情報を解釈することにより，マッピングテーブルを作成し

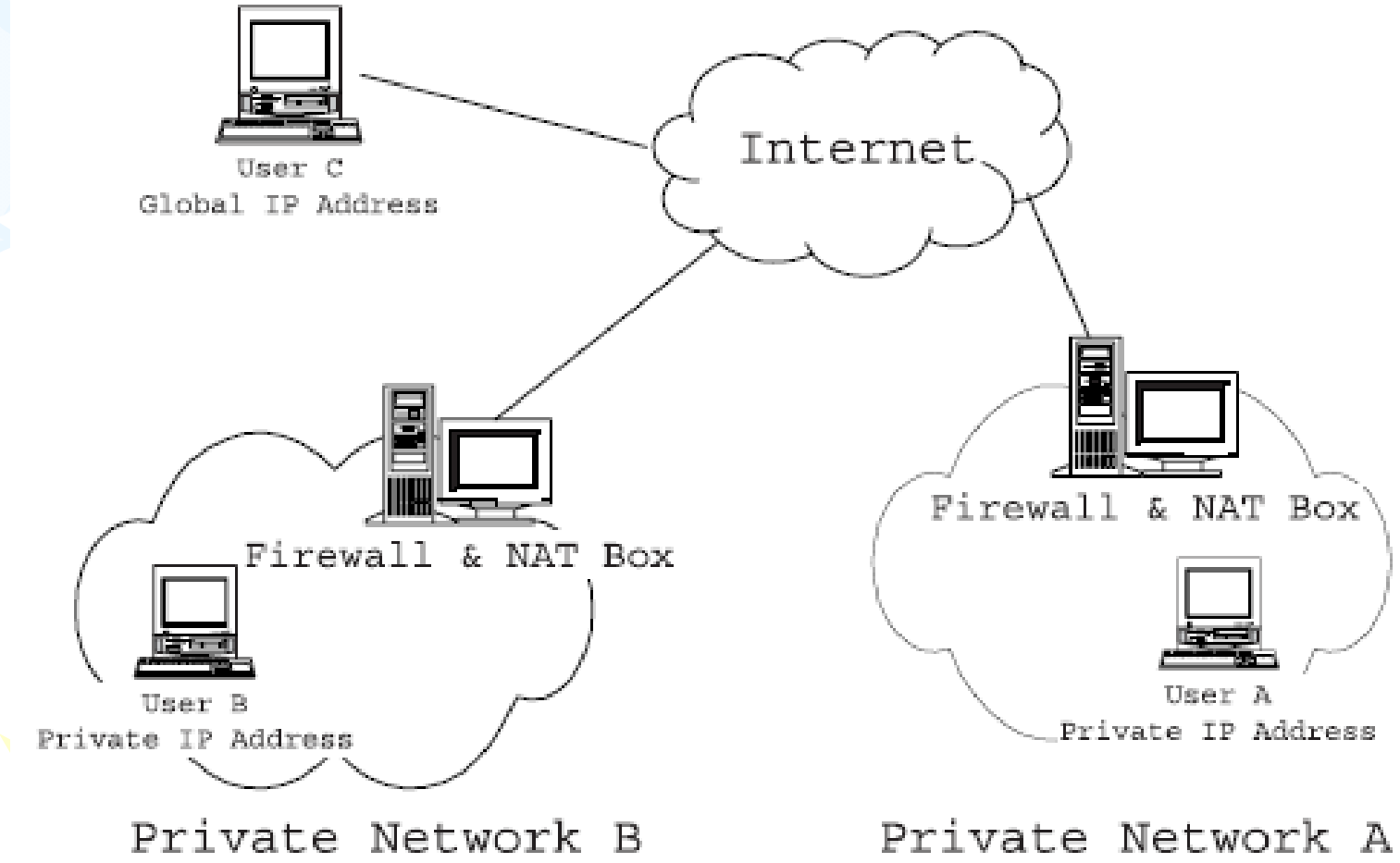
(2) そのマッピングテーブルをもとにFWのルールを動的に変更する

ことにより，音声パケットのNAT通過を実現

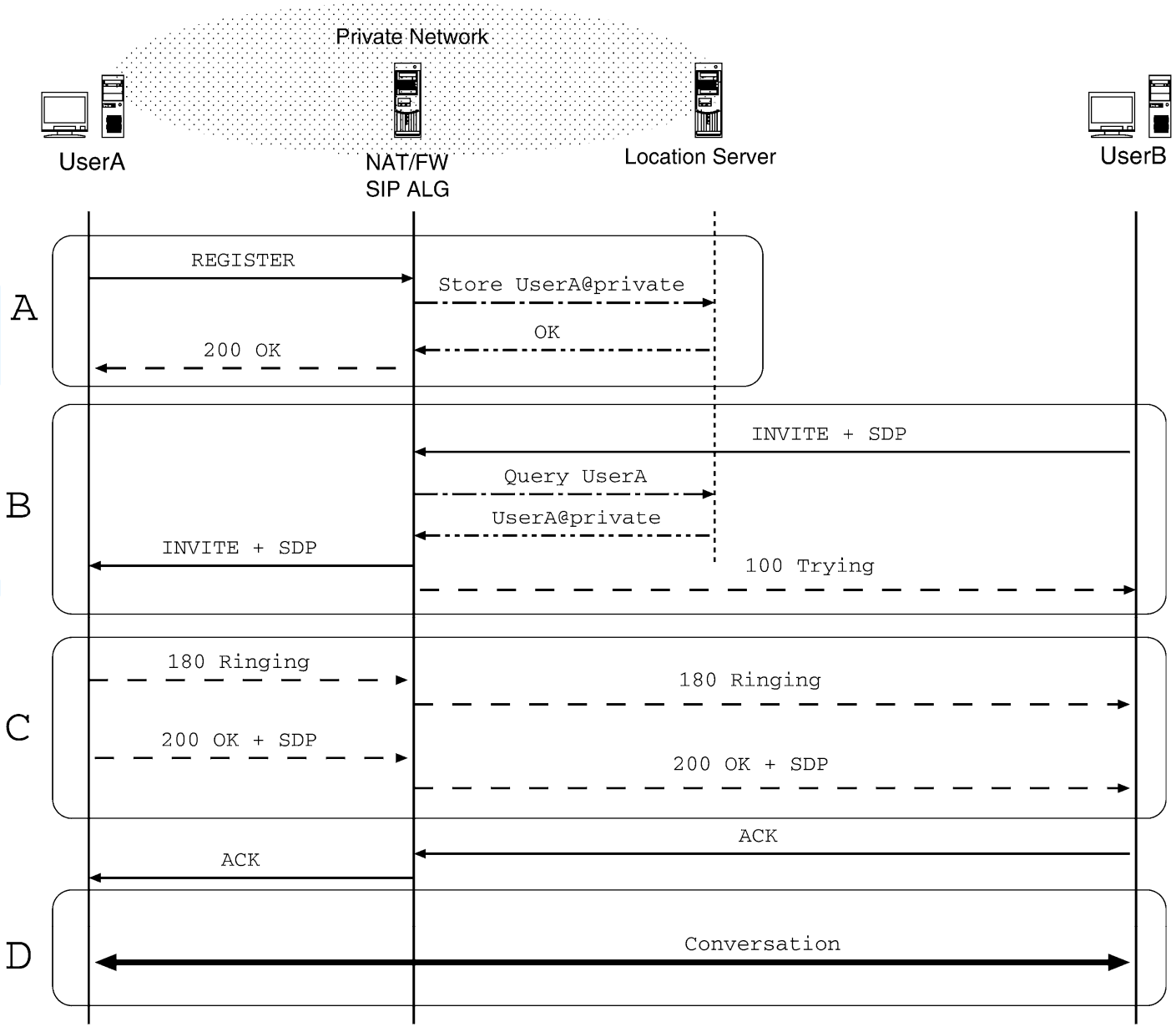
3.「アプリケーションレベルゲートウェイ機能付きSIP サーバ」の設計

ネットワーク構成

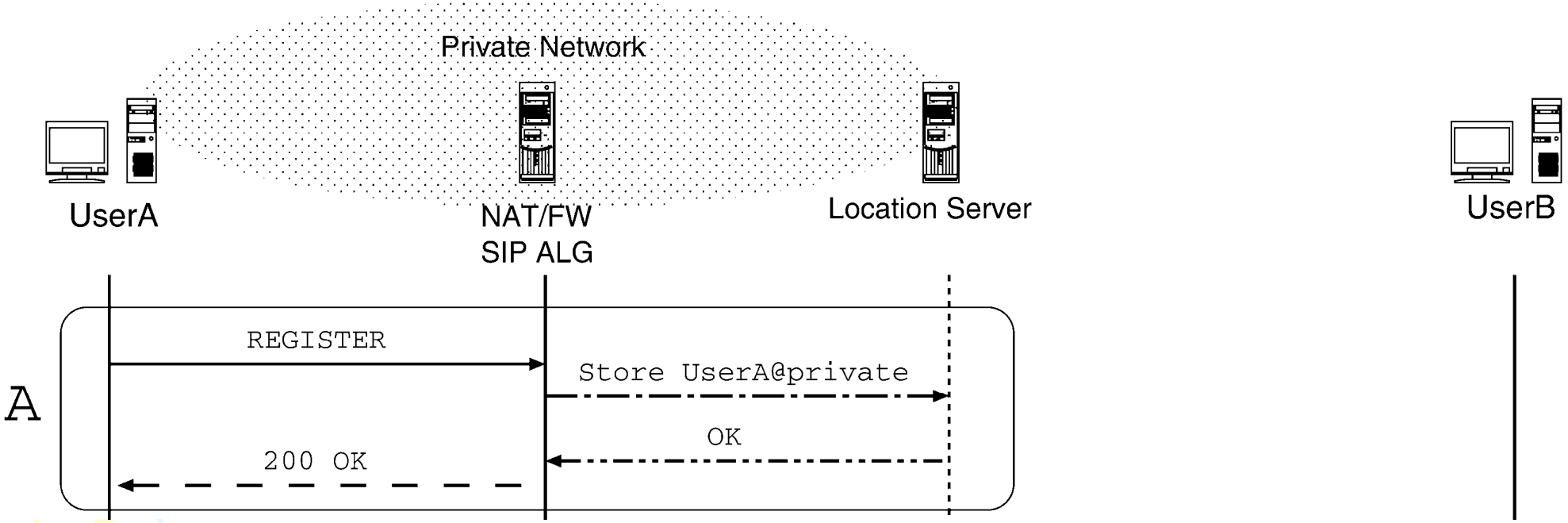
- 提案システムを利用する場合の典型的なネットワーク構成図



提案システムの通話確立過程(全体図)



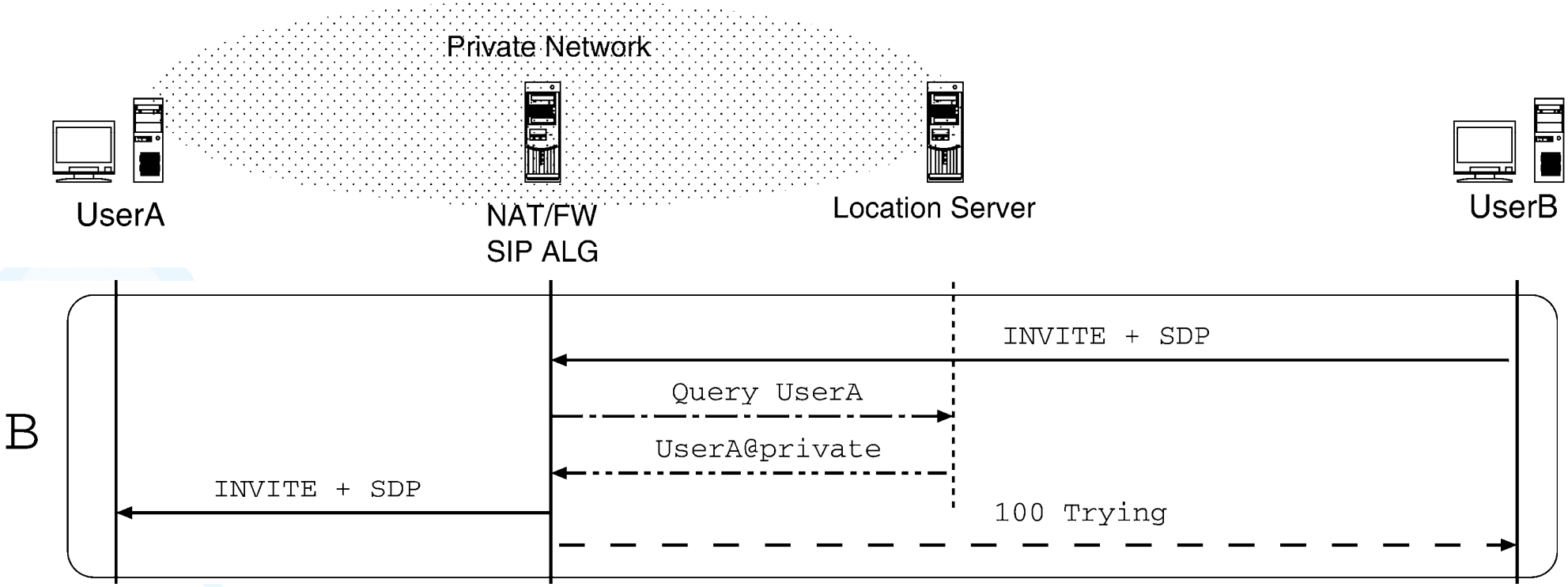
提案システムの通話確立過程(1)



(A) 初期登録

- プライベートネットワーク内のクライアントの情報(SIP URIとIPアドレス)が本システムのデータベースに登録される.
- これはSIP メッセージの到着に先立って，登録しておかなければならない.
- 登録はREGISTER 要求を使って行われる.

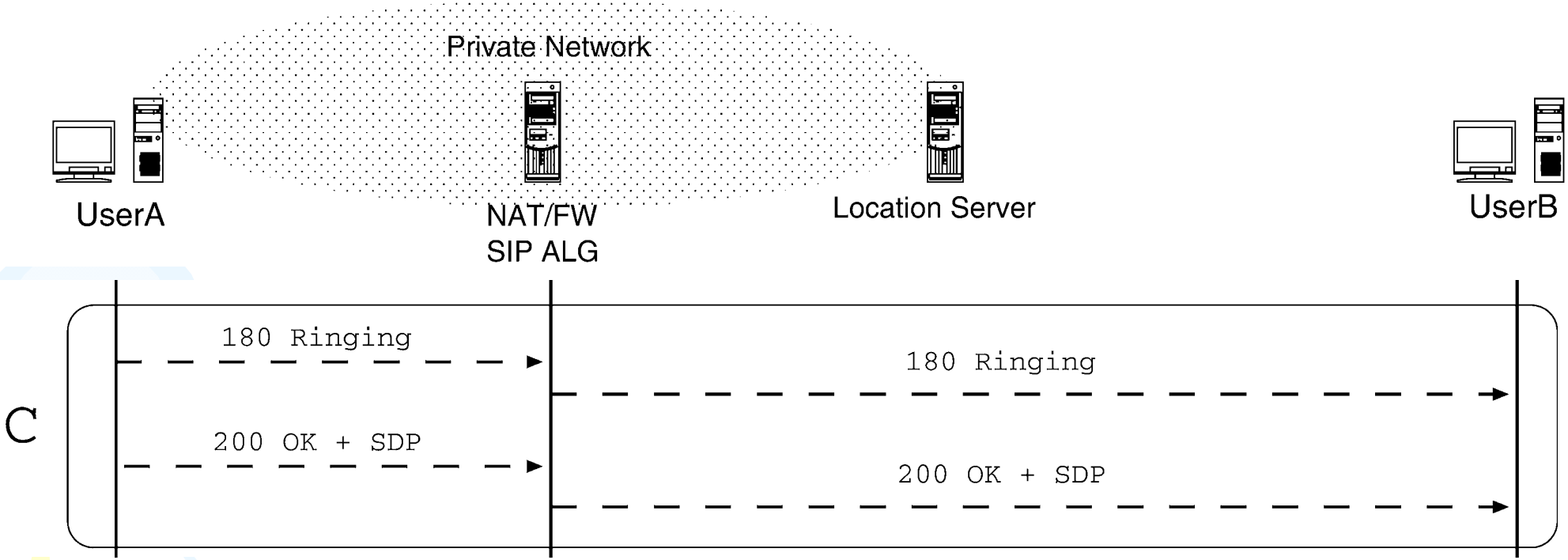
提案システムの通話確立過程(2)



(B) 外部からの着信

- 外部からINVITE 要求(通話要求)が本システムに到着すると, リクエストURI に記述されているSIP URIから転送先を調べメッセージを転送する.
- 初期登録により, 内部ホストのIPアドレスを登録されたSIP URIをキーとして, 取得できる.

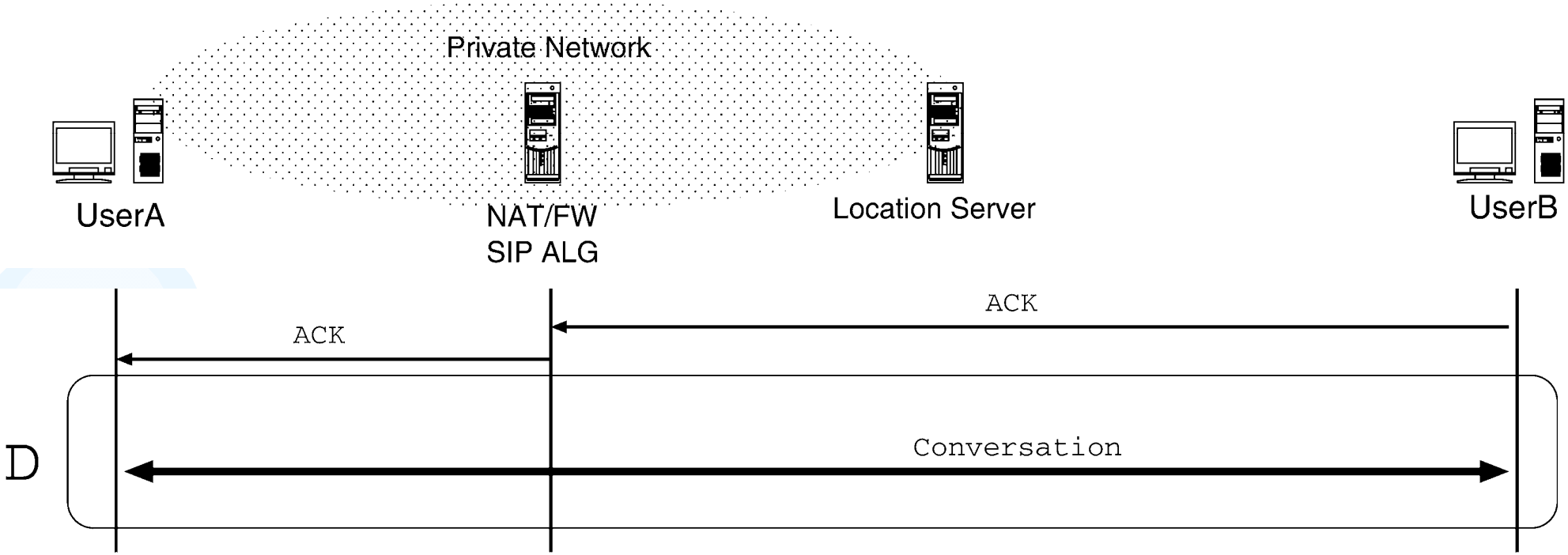
提案システムの通話確立過程(3)



(C) 内部から外部へのSIP メッセージの中継

- 内部から外部へSIP メッセージを中継する場合，SIP メッセージの中にプライベートアドレスが記述されている部分があるので，これをグローバルアドレスに書き換え，送り出す．
- 書き換えるSIP/SDP ヘッダの一覧 ⇒ 表1

提案システムの通話確立過程(4)



(D) 音声データのNAT 通過

- SIPによる音声通信では，SDP を使用してコーデックなどを決定している.
- さらにこのプロトコルには，SIPメッセージ送信者の音声データを受信するIP アドレス，ポート番号などの情報が記述してある.
- 音声データのNAT 通過およびマッピングテーブル作成に必要なSIP/SDP ヘッダの一覧 ⇒ 表

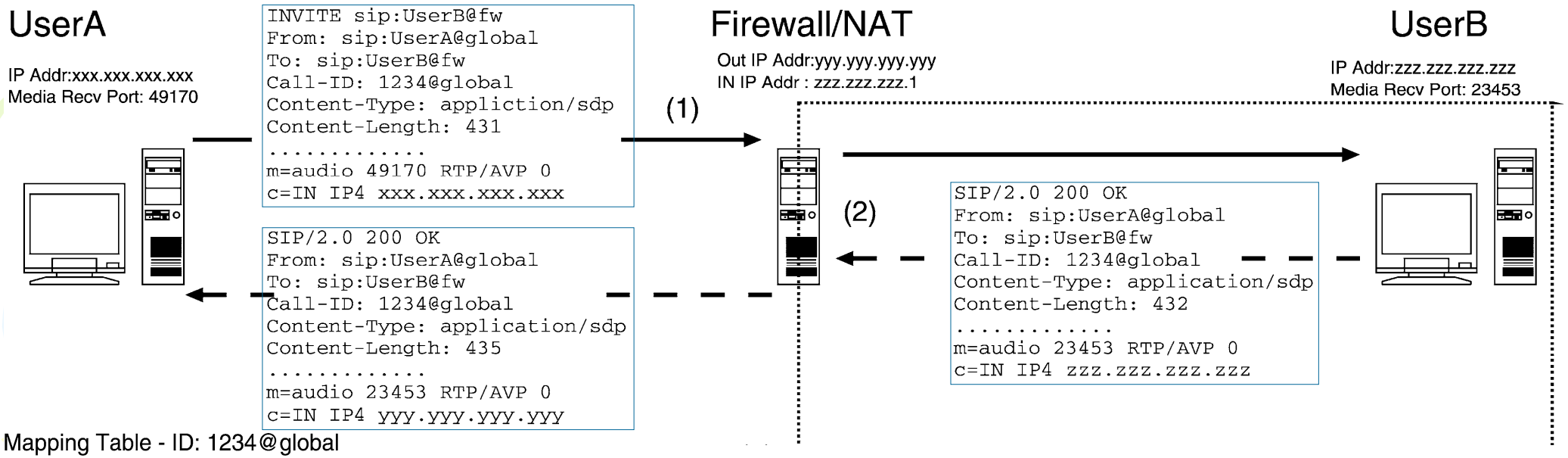
表1. 提案システムに必要なSIP/SDP ヘッダ

	ヘッダ	説明
SIP	Call-ID(*)(**)	セッション識別子
	Contact(*)	現在位置のSIP アドレス
	Content-Type(**)	メッセージボディに含まれる内容
	Content-Length(**)	メッセージボディのサイズ
	From(*)(**)	送信元のSIP アドレス（tag を含む）
	Record-Route(*)	メッセージ経路の記録
	Route(*)	メッセージ経路
	To(*)(**)	送信者のSIP アドレス（tag を含む）
	Via(*)	要求を処理したパス
SDP	c(*)(**)	送信者のIP アドレス
	m(*)(**)	受信ポート番号，コーデックの種類

*書き換えが必要なSIP/SDP ヘッダ

**マッピングテーブル作成に必要なSIP/SDP ヘッダ

マッピングテーブル更新(1)

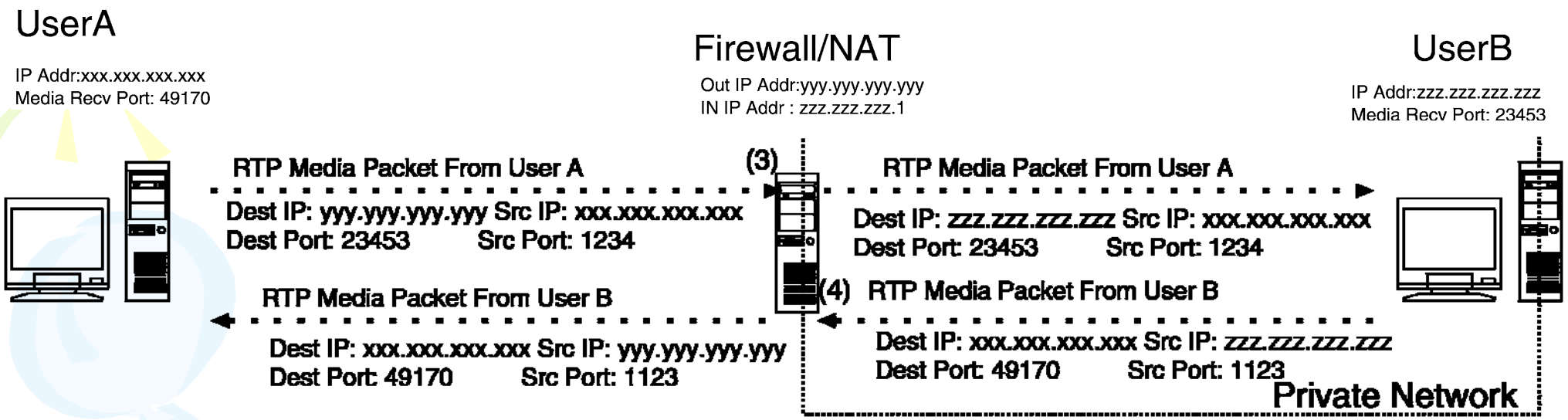


Mapping Table - ID: 1234@global
Call From: sip:UserA@global Call To: sip:UserB@fw

	(1)	(2)	(3)	(4)
Media Out Dst Addr	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
Media Out Src Addr	INADDR_ANY	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz
Media Out Dst Port	49170	49170	49170	49170
Media Out Src Port	NO_SRC_PORT	NO_SRC_PORT	NO_SRC_PORT	1123
Media Out Codec No		0	0	0
Media In Dst Addr	INADDR_ANY	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz
Media In Src Addr	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
Media In Dst Port	NO_DST_PORT	23453	23453	23453
Media In Src Port	NO_SRC_PORT	NO_SRC_PORT	1234	1234
Media InCodec No	0	0	0	0

Updating Mapping Table

マッピングテーブル更新(2)



Mapping Table - ID: 1234@global
Call From: sip:UserA@global Call To: sip:UserB@fw

	(1)	(2)	(3)	(4)
Media Out Dst Addr	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
Media Out Src Addr	INADDR_ANY	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz
Media Out Dst Port	49170	49170	49170	49170
Media Out Src Port	NO_SRC_PORT	NO_SRC_PORT	NO_SRC_PORT	1123
Media Out Codec No		0	0	0
Media In Dst Addr	INADDR_ANY	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz	zzz.zzz.zzz.zzz
Media In Src Addr	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
Media In Dst Port	NO_DST_PORT	23453	23453	23453
Media In Src Port	NO_SRC_PORT	NO_SRC_PORT	1234	1234
Media InCodec No	0	0	0	0

Updating Mapping Table

マッピングテーブルへの情報の対応付け

項目	マッピングテーブル情報
Call-ID	マッピングテーブル作成ID 例：Call-ID：214abe@domain.com
Content-Type	セッション情報が含まれるか調査用 例：Content-Type：application/sdp
Content-Length	セッション情報のサイズチェック用 例：Content-Length：321
From	セッション開始者SIP アドレス
To	通話先SIP アドレス
c	送信者のIP アドレス 例：c＝IN IP4 192.168.0.31
m	受信ポート番号，コーデックの種類 例：m＝audio 49170 RTP/AVP 0
送信元ポート番号	音声パケットを送り出す際のポート番号

FWのセキュリティルールの更新

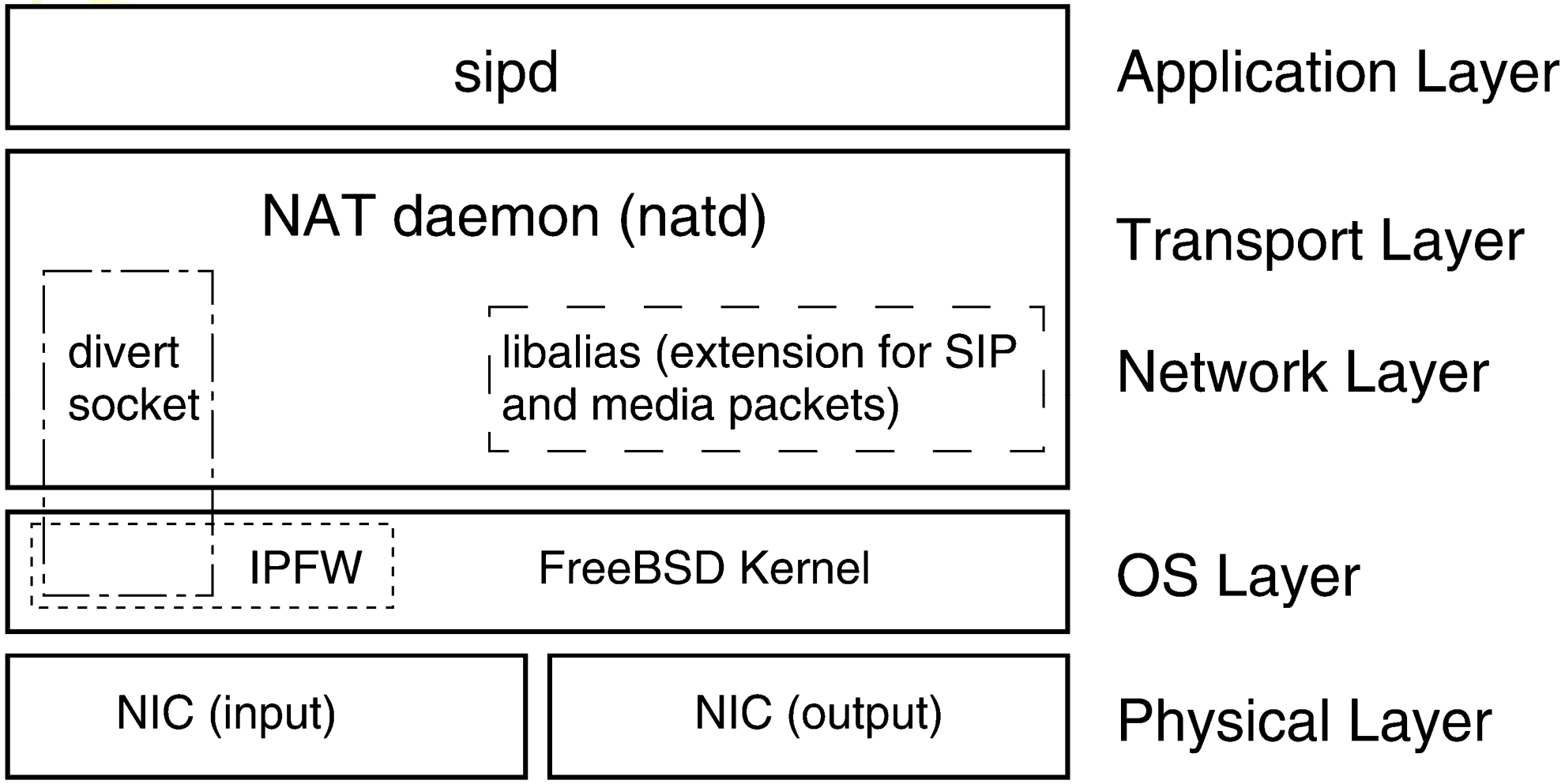
- クライアントからの初めの音声パケットがFWに到着

⇒NATはこのパケットのIPヘッダ，UDPヘッダやRTPヘッダの音声コーデックの種類を参照し，マッピングテーブルの内容と比較する

⇒一致すれば，このパケットの送信元ポート番号，宛先ポート番号，マッピングテーブルを元にFWのセキュリティルールを動的に更新する

4. 実装

ソフトウェア構成

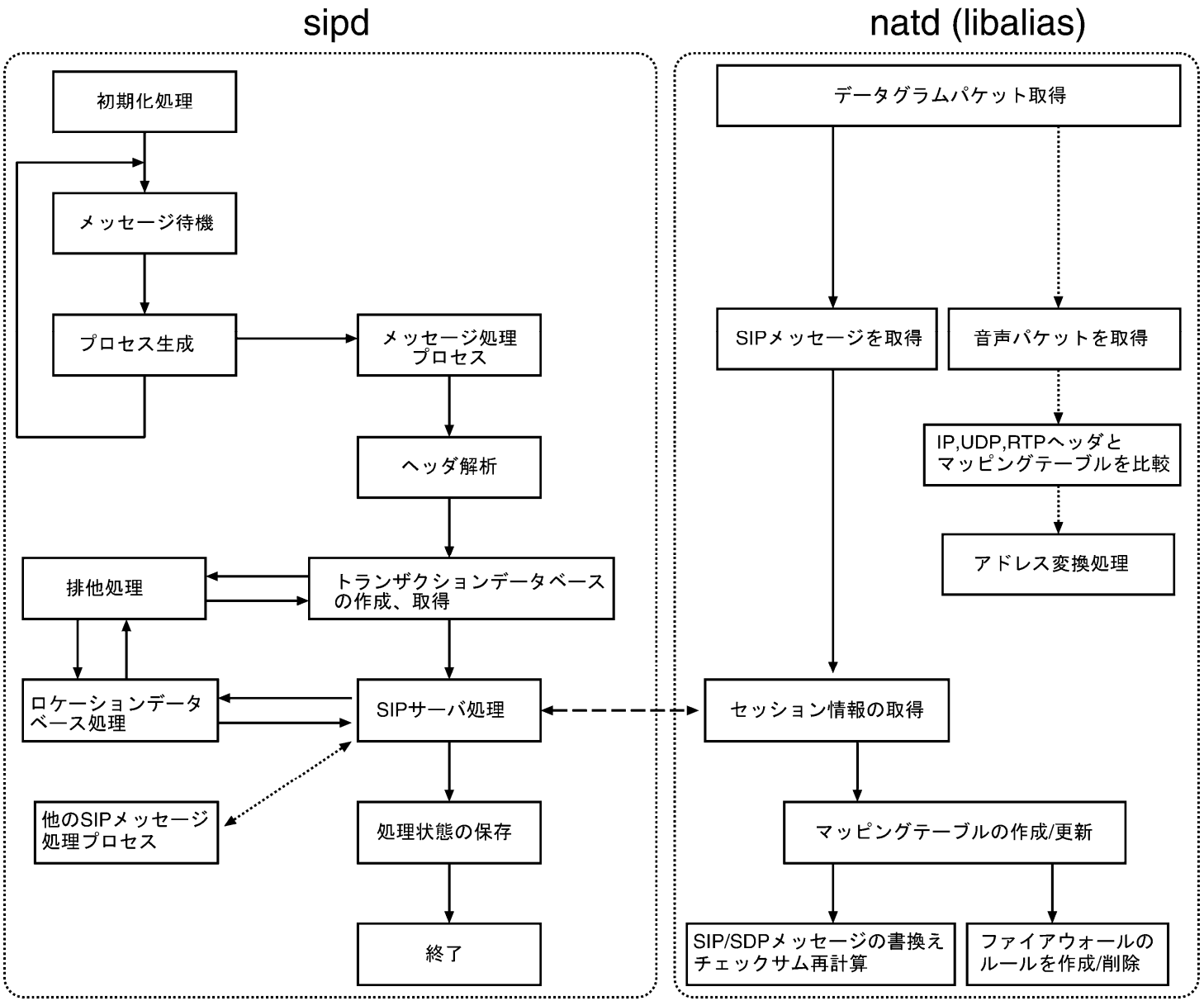

sipd
Application Layer
NAT daemon (natd)
Transport Layer
divert socket
libalias (extension for SIP and media packets)
Network Layer
IPFW
FreeBSD Kernel
OS Layer
NIC (input)
NIC (output)
Physical Layer

ソフトウェア構成

- sipd
  - 新たに作成したもの。
  - アプリケーション層でSIPメッセージの中継，管理，登録，SIP メッセージの書き換えを行う。
- natd
  - FreeBSD標準のNATデーモン。
- libalias
  - パケットエイリアス（パケットのアドレス変換）を行うnatdのライブラリ
  - 以下の改造を行う

(1) SIP/SDP メッセージからセッション情報を取得
(2) マッピングテーブルの作成/更新
(3) SIP/SDP メッセージの書き換え
(4) 動的にファイアウォールのルールを作成，削除

提案システムの流れ図


sipd
natd (libalias)
初期化処理
メッセージ待機
プロセス生成
メッセージ処理プロセス
ヘッダ解析
排他処理
トランザクションデータベースの作成、取得
ロケーションデータベース処理
SIPサーバ処理
他のSIPメッセージ処理プロセス
処理状態の保存
終了
データグラムパケット取得
SIPメッセージを取得
音声パケットを取得
IP,UDP,RTPヘッダとマッピングテーブルを比較
アドレス変換処理
セッション情報の取得
マッピングテーブルの作成/更新
SIP/SDPメッセージの書換えチェックサム再計算
ファイアウォールのルールを作成/削除

むすび

- SIP を利用した音声通話に対し，SIPメッセージおよび音声パケットのNAT 通過を実現するための手法を提案した.
- 提案方式は，FW/NATとSIP サーバを統合化することにより，既存のNAT では実現できなかった
  (1) パケットのペイロードにあるSIP/SDP メッセージの認識およびアドレスの書き換えを行う機能
  (2) SIP メッセージからセッション情報を取得し，マッピングテーブルを作成する機能
  (3) マッピングテーブルをもとに音声パケットを動的に許可/拒否する機能
  を有するものである.