異なるプライベートアドレス空間に存在する端末どうしの通信を可能とする CIPA の提案

043432041　柳沢信成
渡邊研究室

1. はじめに

ユビキタス社会とは，いつでも誰でもどこからでも自由に通信できる社会である．しかし，IPv4 の世界においては IP アドレス空間としてグローバルアドレス空間（GA 空間）とプライベートアドレス空間（PA 空間）の 2 つの空間があり，両者は自由に通信を行うことができない．具体的には，アドレス変換装置（NAT）のアドレス変換の原理に起因して GA 空間から PA 空間に対して通信を開始することができない．IPv6 が普及すればアドレス変換が不要となり，このような課題は解決される可能性はあるが，IPv4 は当面の間 IPv6 と共存しつつ使い続けられると思われる．また，IPv6 を適用したときに，内部のネットワークが見えてしまうのは問題であるとの指摘もあり，アドレス変換は IPv6 の時代でも使われる可能性がある．よって上記課題の解決を検討することは意味のあることと考えられる．

IPv4 の PA 空間と GA 空間との間にはアドレス変換装置 (Network Address Translation，以下 NAT)の設置が必須で，多くの場合ファイアウォールに内蔵される．企業ネットワークにおいてはセキュリティーポリシーによりファイアウォールを用いて自主的に通信制限をかけるため，NAT による通信の制約は表に出てこない．しかし，今後家庭にもネットワークが普及していった場合，通信の利便性の向上が要求されるため NAT による通信の制約を除去することが望まれる．

これらの課題を解決するため，本研究室では端末と NAT が強調することにより GA 空間からの通信開始を可能とする NATF（NAT Free Protocol）[1]を提案している．　本研究では，NATF の考え方を更に拡張し，グローバルアドレス環境をはさんで異なるプライベートアドレス環境にある端末同士の自由な通信を可能にする方式 CIPA（Communication between terminals in Independent Private Address areas；サイパ）を提案する．

2. 従来研究

GA 空間から PA 空間への通信の開始ができない理由は PA 空間から GA 空間に抜ける最初のパケットによってのみ NAT のアドレス変換テーブルが生成されるためである．事前に静的にテーブル内容を登録しておくことによりこの課題を解決する方法（ポートフォワーディング）もあるが，ネットワーク構成やアプリケーションに応じてテーブルを設定する必要があり，自由な通信とは言えない．

NAT を越える通信方式の研究には，GA 空間上にサーバを用意するサーバ中継方式とサーバを使用しない P2P 方式がある．

サーバ中継方式全般の欠点として，サーバを設置するためのコスト増加やサーバを中継するための遅延が生じる点があげられる．今後 P2P 通信が発展して行くことを考えると，サーバ中継方式は望ましい方式とは言えない．

P2P 方式として NATS（Network Address Translation with Sub-Address）が挙げられる． NATS は，独自のサブアドレスを定義し，DNS サーバと NAT が連携して IP in IP カプセリングにより NAT を通過する．しかし，サブアドレスを別途定義しなければならないことや，NAT がカプセル化を行うためのオーバヘッドが発生するなどの課題がある．

3. CIPA の提案

CIPA は，NATF を拡張し，グローバルアドレス環境を挟んだプライベートアドレス端末同士の通信を可能とする．CIPA では，NATF で拡張した端末の機能を 2 台の NATFBOX が実行する．提案システムの環境を図 1 に示す．CIPA では通信端末は一般端末でよく，NATFBOX 同士が NATF プロトコルを実行する．送信元の NATFBOX は NAT アドレス変換に加え FAT 変換を行う．FAT 変換とはポート番号変換のことである，図 1 のような環境では，プライベートアドレス空間のアドレスが重複する場合もあり得る。そこで本章では，端末 A と端末 B が同一のプライベートアドレスであっても通信が可能であることを示すため，実アドレスを用いて動作を説明する．端末 A,B のアドレスはともに 192.168.0.1 であるものとする．

端末 A から端末 B へ接続を開始する場合の通信の流れを図 2 に示す．初期設定として NATFBOX1 には通信先ホスト名(h)とドメイン名(natf.com)を，NATFBOX2 には内部に属する端末のホスト名(h)とプ

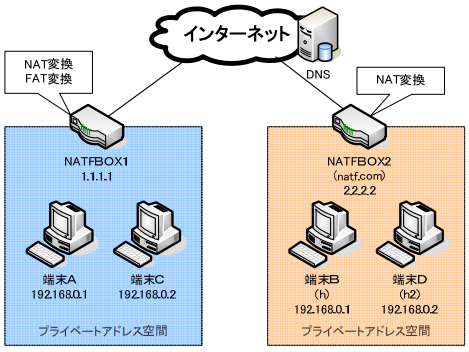


図 1　CIPA の環境

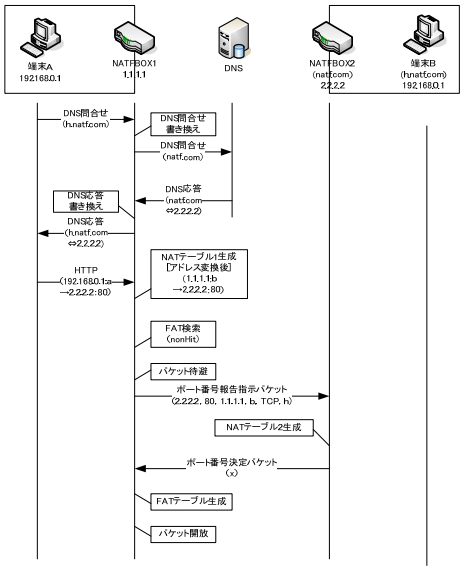


図 2　CIPA 時の NATF プロトコルの流れ

ライベート IP アドレス(192.168.0.1)を設定する．

端末 A は端末 B に関する DNS 問合せを行う．このパケットが NATFBOX1 に届いたら NAT 処理後に問合せ部のホスト名(h)+ドメイン名（natf.com）からホスト名を削除し DNS に送信する．DNS は，A レコードとして NATFBOX2 のグローバルアドレス（2.2.2.2）を返す．

NATFBOX1 は DNS 応答を受信すると，NATFBOX2 の IP アドレスを保存する．そして DNS 応答の問合せ部を元のホスト名（h）とドメイン名（natf.com）に戻し，端末 A へ転送する．端末 A は通信相手が NATFBOX2 であるものと認識し通信を開始する．

以下 IP アドレスとポート番号の関係を，順を追って示す．下記記述においてスラッシュの左側は送信元 IP アドレス：送信元ポート番号，右側は宛先 IP アドレス：宛先ポート番号である．端末 A 側の OS から動的に割り当てられた送信元ポート番号を a，端末 B を HTTP サーバと仮定し，宛先ポート番号を 80 とすると，端末 A が送信するパケットは次のようになる．

192.168.0.1：a / 2.2.2.2：80

NATFBOX1 はこのパケットを受信すると，NATF プロトコルを実行するための準備を行う．NATFBOX1 は一般の NAT の手順に従い NAT テーブル 1 を生成し，最初のパケットのアドレス変換を行っておく．NAT テーブル 1 の情報は以下のように生成される．b は NAT により動的に割り当てられたポート番号である．

{192.168.0.1：a⇔1.1.1.1：b}

したがって，アドレス変換後のパケットは

1.1.1.1：b / 2.2.2.2：80

となる．次に NATF プロトコルを実行するため，このパケットは NATFBOX1 に一時的に待避しておき，ポート番号報告指示パケットを NATFBOX2 に送る．このパケットには，送信元 IP アドレス：ポート番号（1.1.1.1：ｂ）と宛先 IP アドレス：ポート番号（192.168.0.1：80）とプロトコル（TCP）とホスト名(h)の情報が含まれる．

NATFBOX2 は上記ポート番号報告指示パケットを受信したら，このパケットの情報と予め登録した情報をもとに NAT テーブル 2 を生成する．テーブルの内容は以下の通りである．ｘは NAT により動的に割り当てられたポート番号である．

{192.168.0.1：80⇔2.2.2.2：ｘ}

NATFBOX2 はこの変換ポート番号（ｘ）を，ポート番号報告応答パケットを用いて NATFBOX1 に送る．

NATFBOX1 は変換ポート番号の情報を元に，FAT テーブルを生成する．FAT テーブルの情報は以下の通りである．

{1.1.1.1：a→2.2.2.2：80⇔1.1.1.1：a→2.2.2.2：ｘ}

ポート番号変換テーブル作成後，NATF プロトコルは終了する．

NATF プロトコル終了後の通信の流れを説明する．NATFBOX1 は，待避していたパケットを NAT テーブルにより，アドレス/ポート番号変換後，FAT テーブルから更にポート変換し，NATFBOX2 宛に送信する．このパケットの内容は次のとおりである．

1.1.1.1：b / 2.2.2.2：ｘ

このパケットを受信した NATFBOX2 では，NAT アドレス変換後，端末 B に送信する．パケットの内容は以下のように変わる．

1.1.1.1：b / 192.168.0.1：80

端末 B から端末 A への応答は，上記と逆の変換で行われる．

以下，NATFBOX1 では NAT アドレス変換とポート番号変換，NATFBOX2 では NAT アドレス変換をすることにより通信が行われる

このように，NATFBOX はアドレス変換用のポート番号をそれぞれ独立して生成し，送信側の NATFBOX は NAT 変換とポート番号変換を行う．端末 A は NATFBOX2 と，端末 B は NATFBOX1 と通信しているようにみえる．

4. まとめ

本稿では，NATF を拡張して，グローバルアドレス環境を挟んだプライベートアドレス端末同士の通信を可能とする方式 CIPA の提案を行った．CIPA は NATFBOX どうしが，通信開始に先立って情報を事前に交換し，その情報を元に通信パケットの IP アドレス変換，ポート番号変換をする．CIPA ではカプセル化／デカプセル化やパケット長を変化させる必要がなくオーバヘッドが少ない．また，異なるプライベートアドレス空間に同一のプライベート IP アドレスを持つ端末があっても CIPA を利用することにより P2P 通信が可能である．CIPA の実装を行い，NAT を越えて通信できることを確認した．また FTP を用いた性能測定ではオーバヘッドが極めて少ないことを確認した．

参考文献

[1] 加藤尚樹，柳沢信成，鈴木秀和，宇佐見庄五，渡邊晃，"インターネットから家庭ネットワークへの接続を可能とする NATF プロトコルの検討と実装", WiNF2005 論文集，pp.142-146，Sep.2005.

異なるプライベートアドレス空間に存在する端末どうしの通信を可能とするCIPAの提案

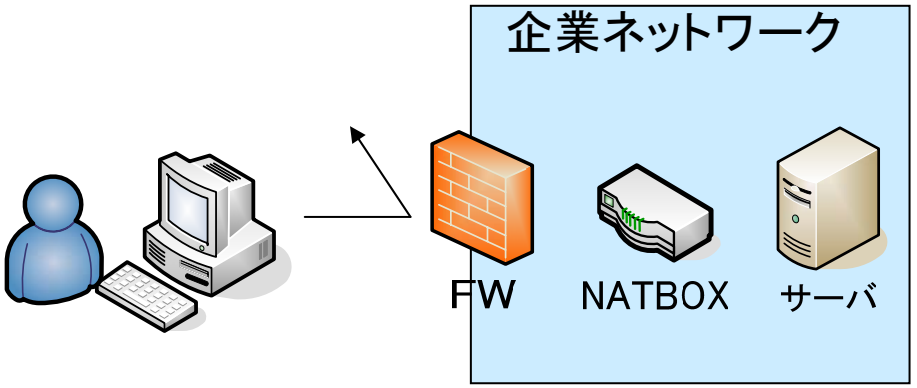
名城大学大学院理工学研究科
渡邊研究室
043432041 柳沢信成

背景

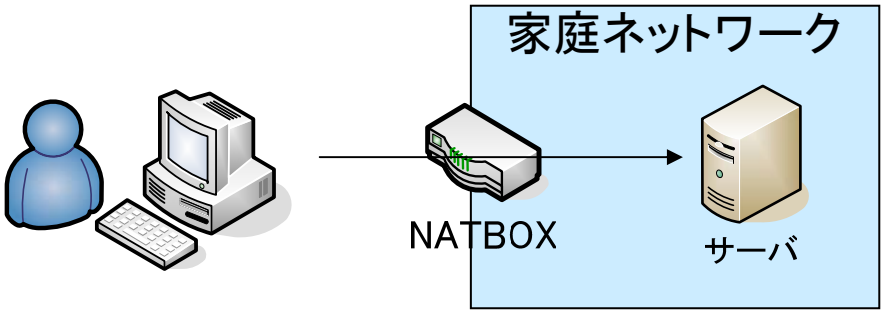
- インターネットの普及
  - ユビキタス社会
- IPアドレスの枯渇
  - プライベートアドレスの導入
    - アドレス変換装置（NAT）の設置
    - NATにより自由に通信が行えない

背景

- 企業ネットワーク
  - FW
  - 通信不可
    - NATの制約は表立って出てこない

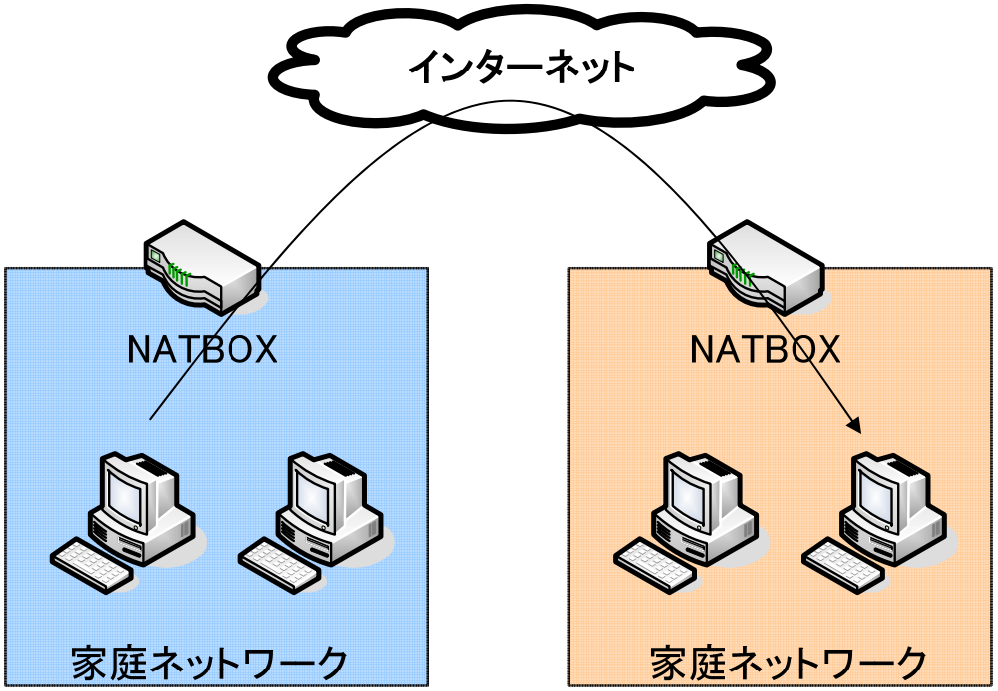


- 家庭ネットワーク
  - いつでも、どこでも接続したい
    - NATの制約を除去したい



背景

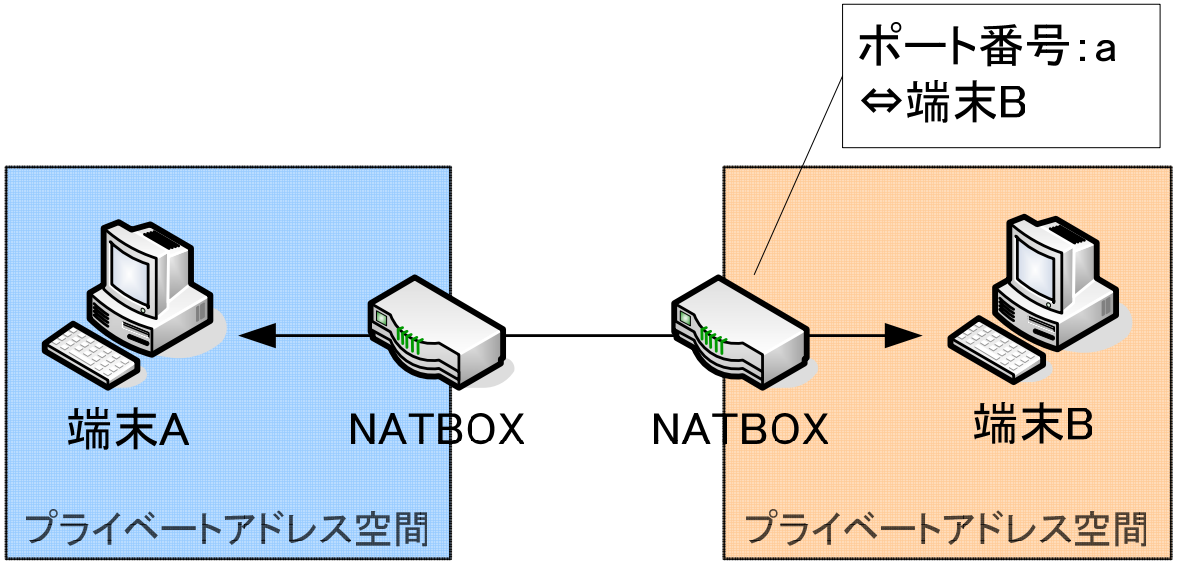
- 各家庭間で自由に通信が行いたい



異なるプライベートアドレス空間で
自由に通信可能な方式CIPAの提案

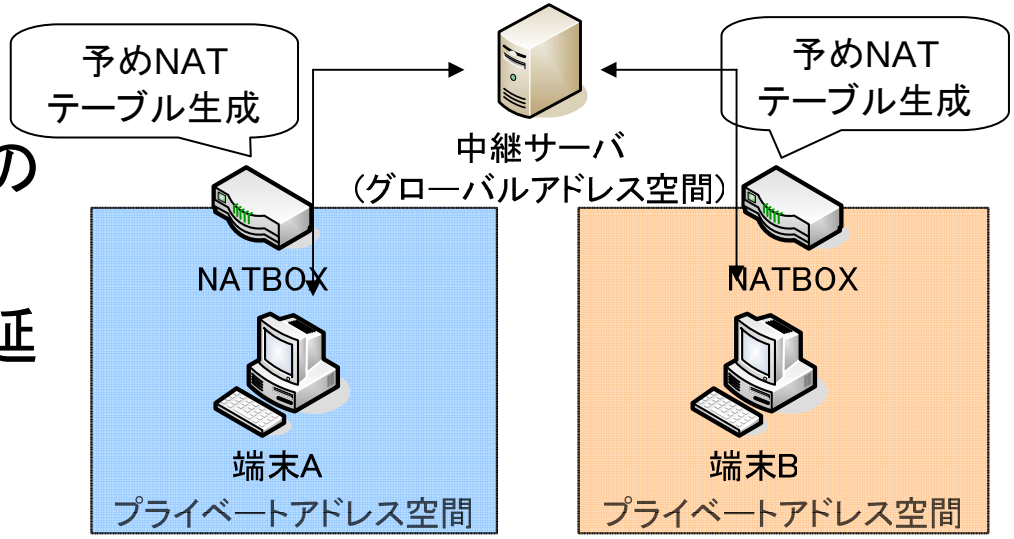
ポートフォワーディング

- 静的にNATテーブルを生成
  - ポート番号とプライベートアドレスが固定される
  - ポート番号1つに対し，サービスする端末が1台しか対応できない

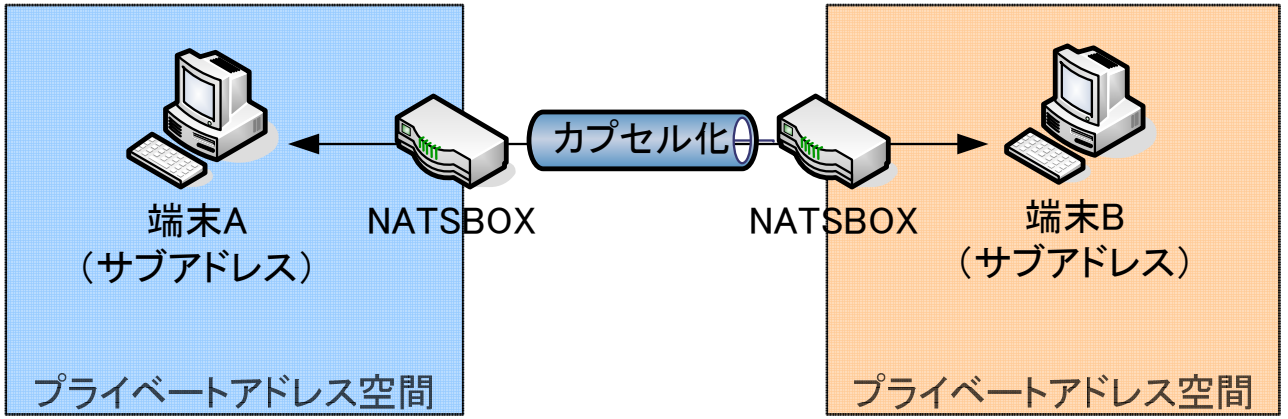


既存技術

- サーバ中継方式
  - サーバを設置するための コスト増加
  - サーバを中継による遅延

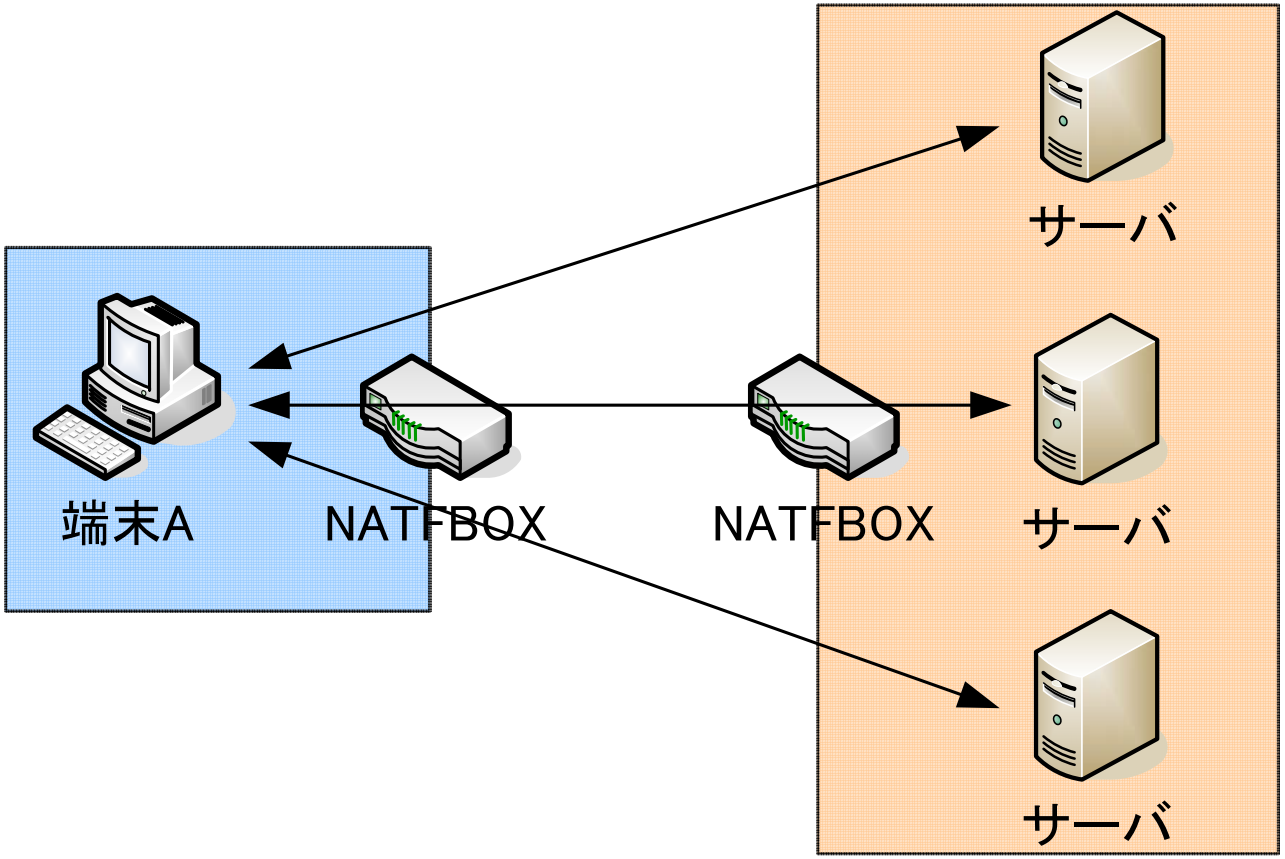


- P2P方式
  - NATS
    - 新たなアドレス空間（サブアドレス）
    - DNS改造
    - カプセル化



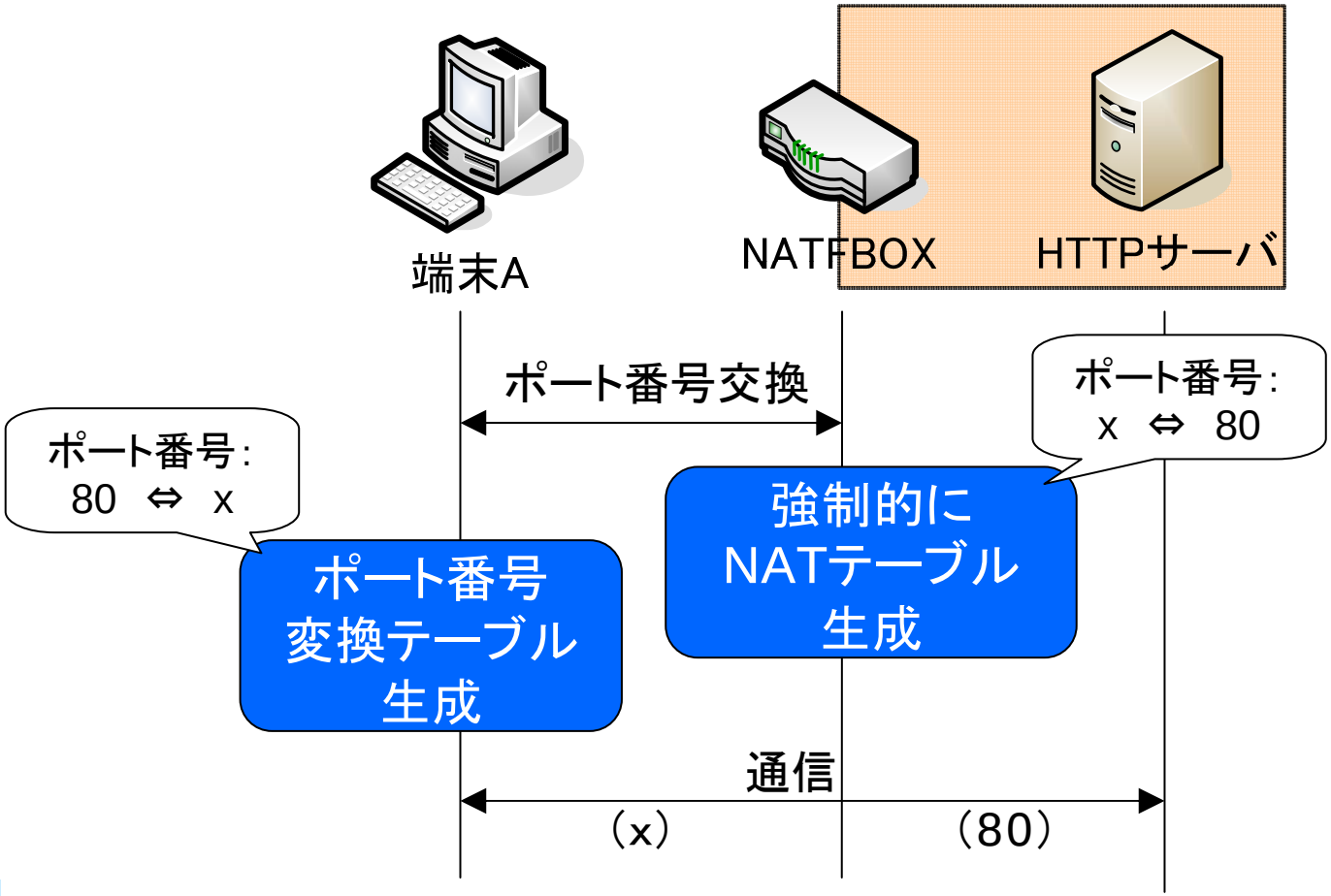
提案システム

- CIPA（Communication between terminals in Independent Private Address areas）
  - NATFを拡張



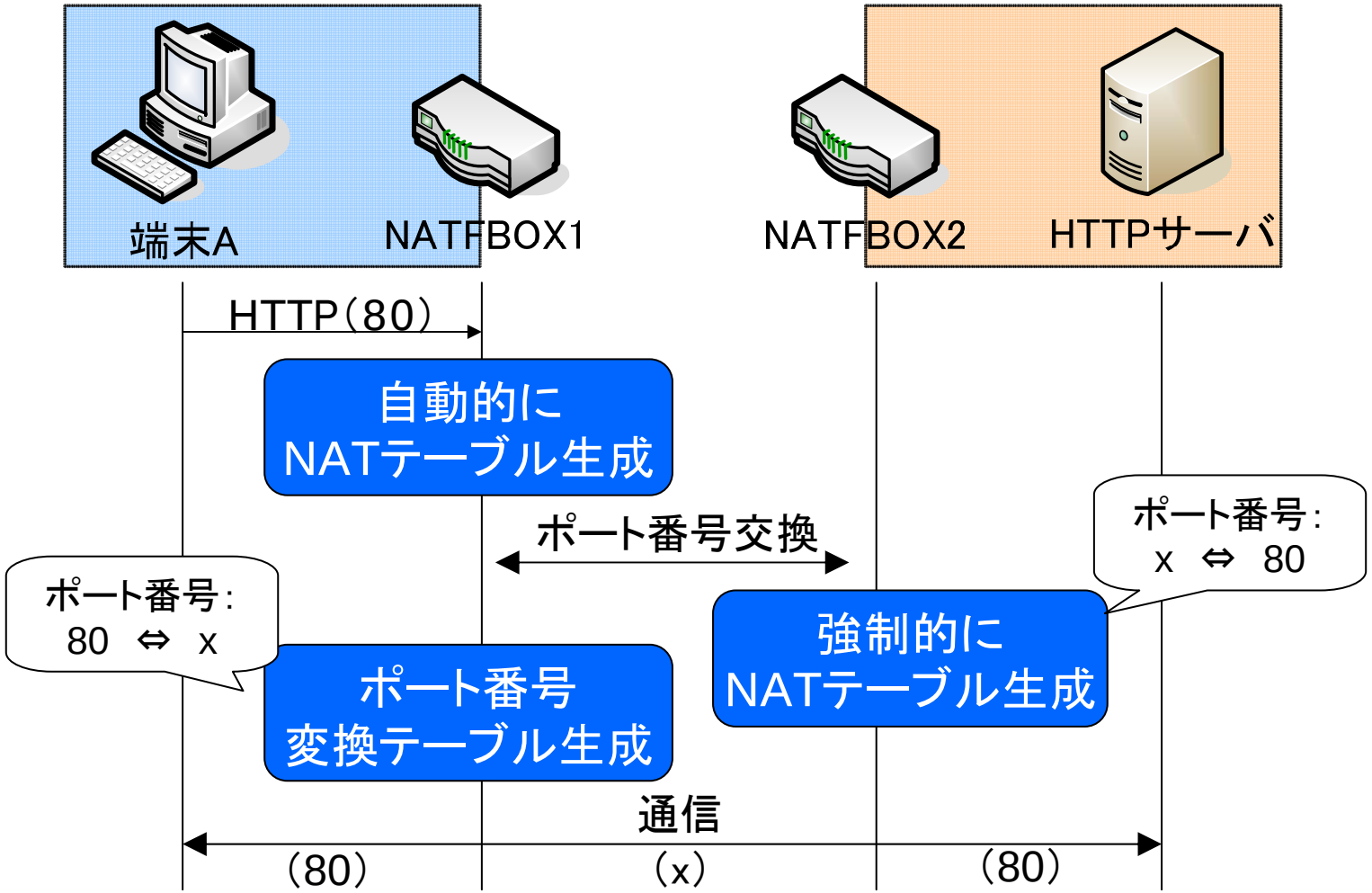
NATF（NAT Free protocol）

- グローバルアドレス空間からプライベートアドレス空間への通信を可能とするプロトコル



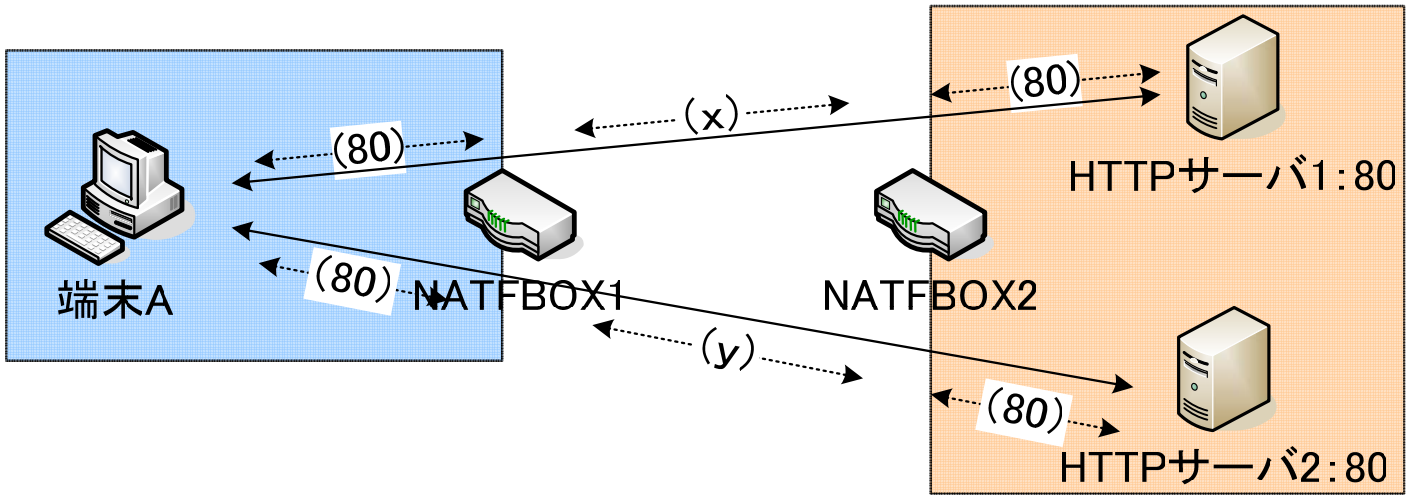
CIPA

- NATFにおける端末側の機能（ポート番号変換）をNATFが代行

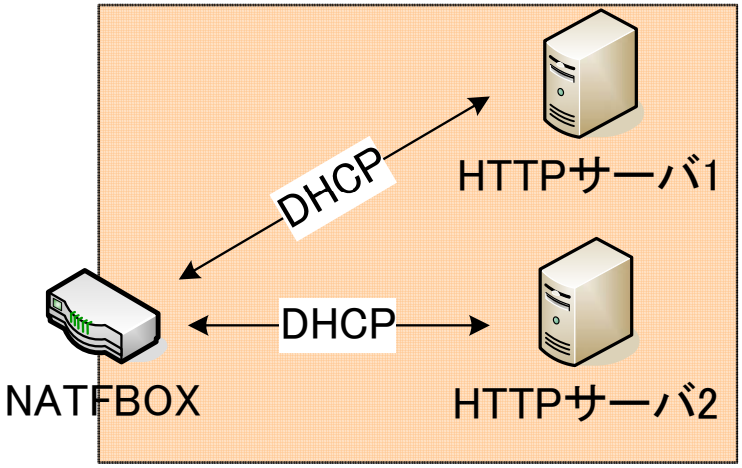


CIPAの特徴

- 同一のアプリケーションが利用可能

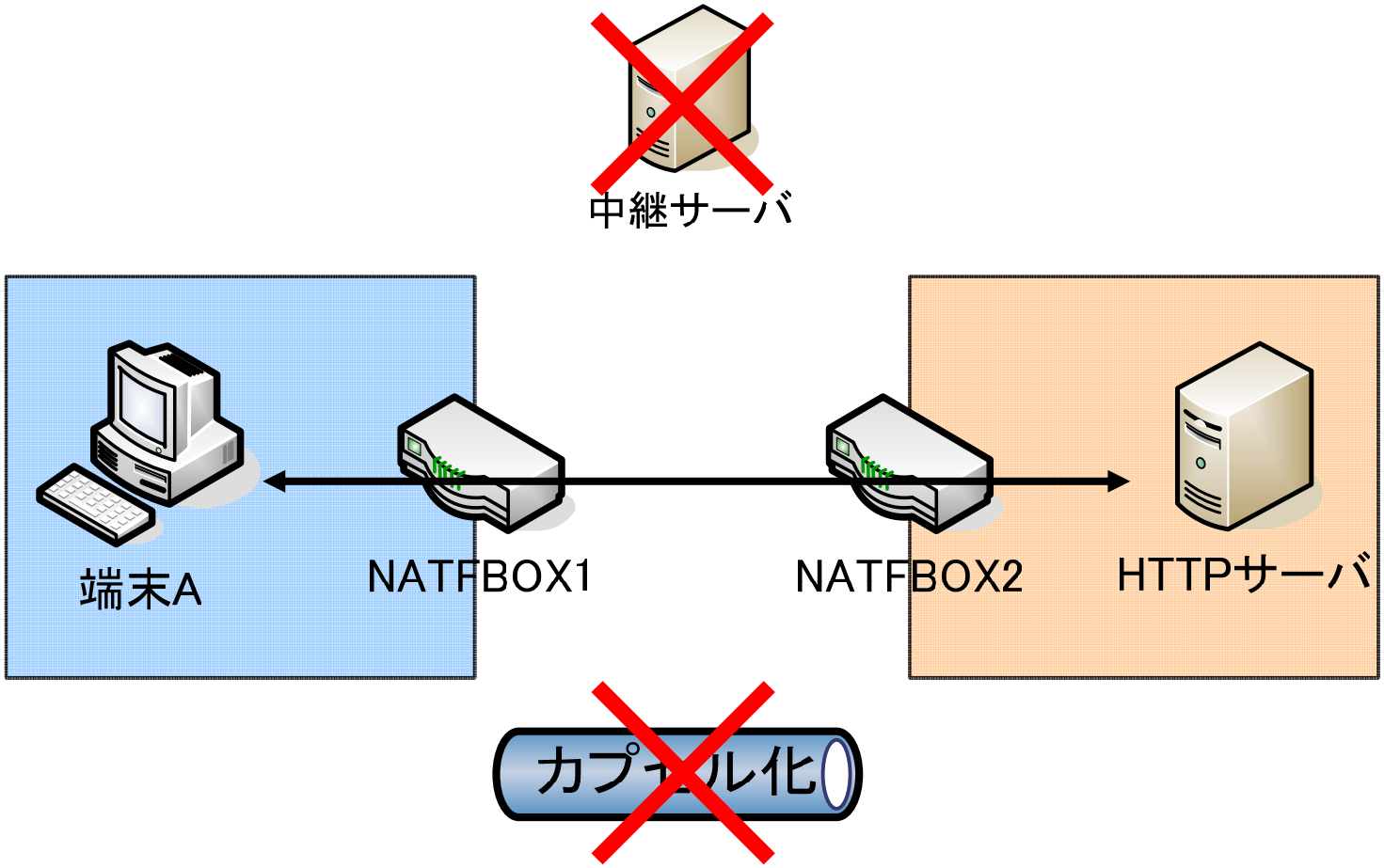


- プライベートIPアドレス:ポート番号の設定が不要

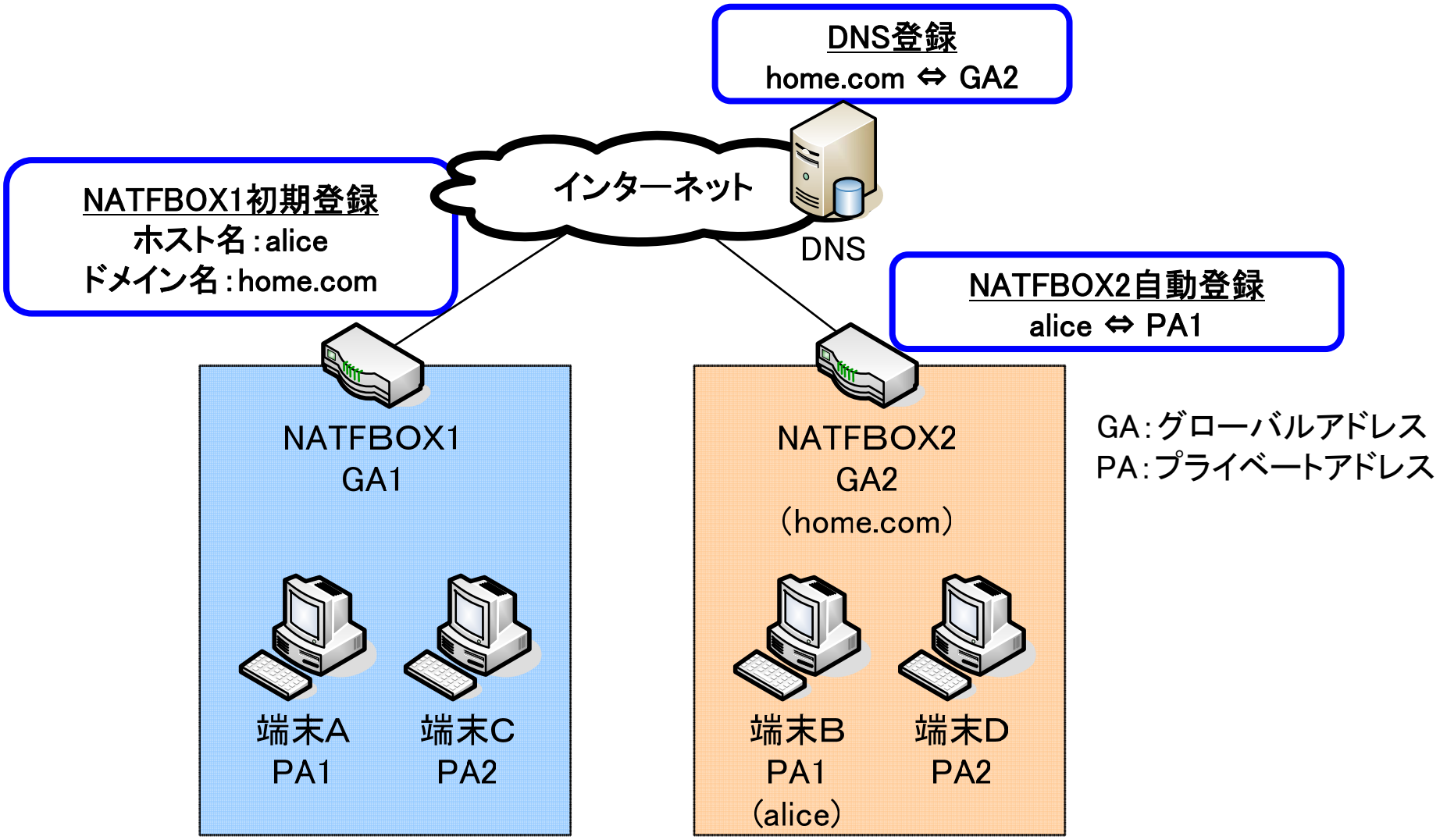


CIPAの特徴

- 通信中のオーバヘッドが少ない
  - サーバ中継やカプセル化を行わない

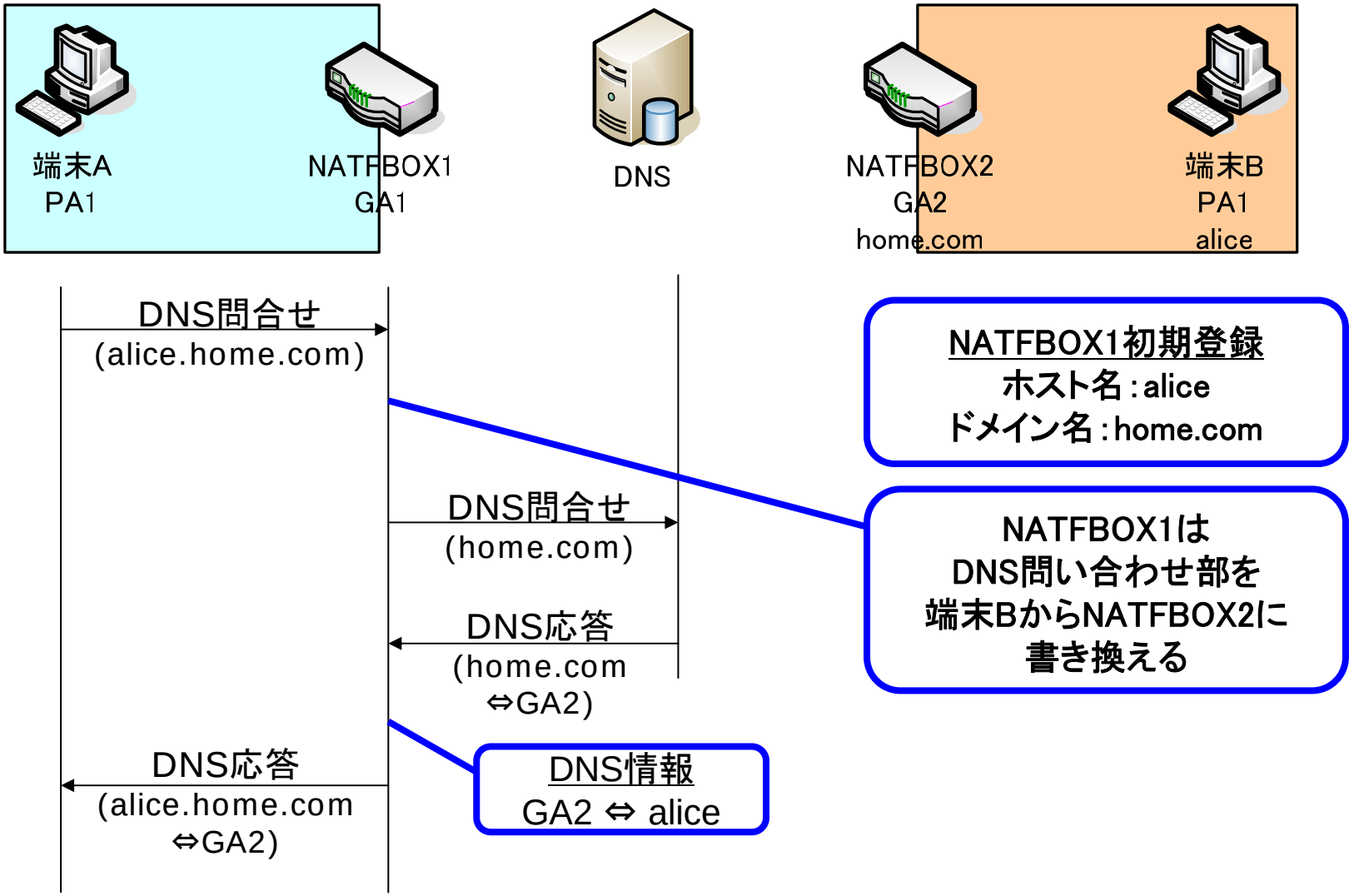


提案環境

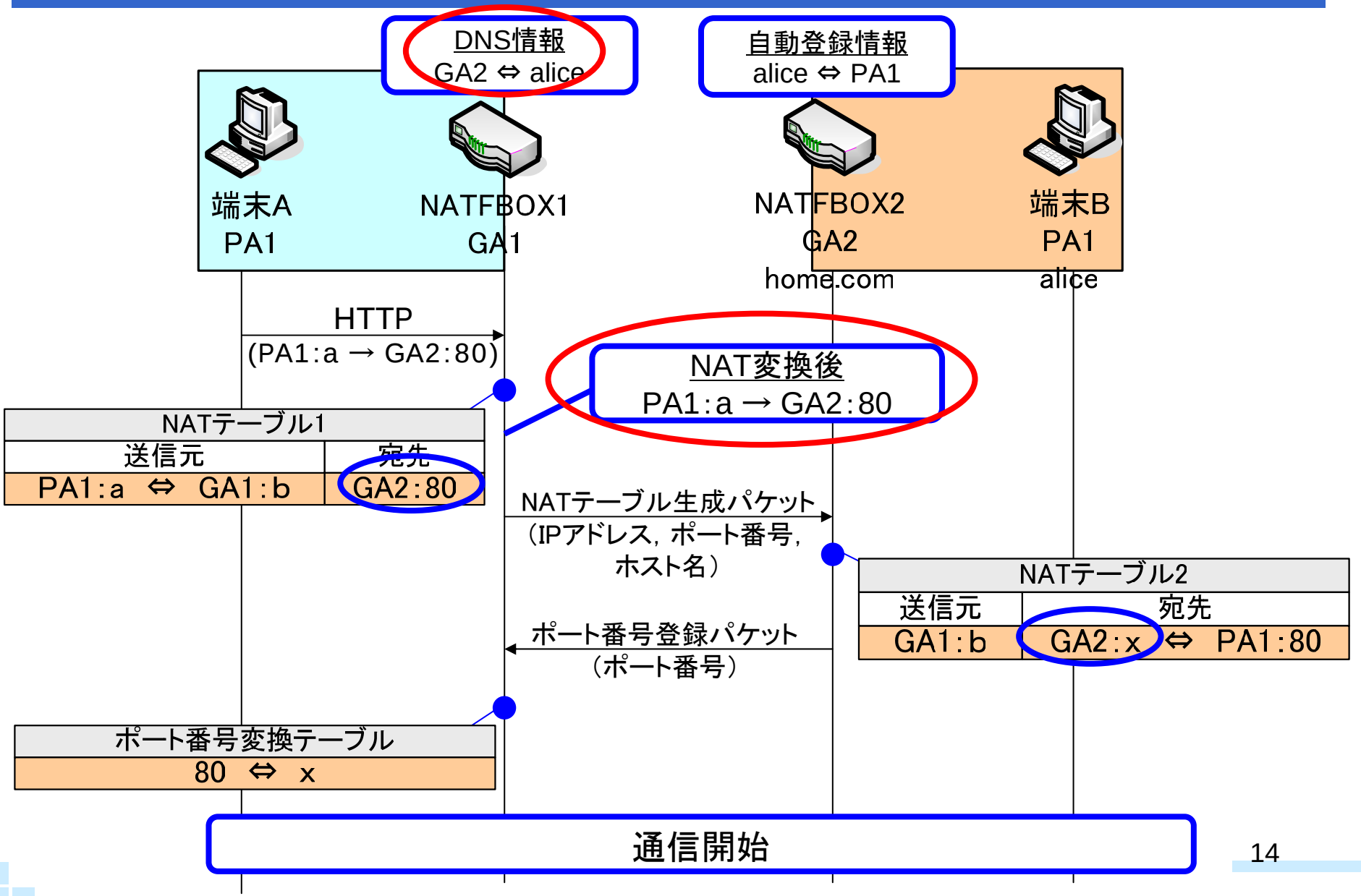


※各端末，DNS：既存
NATFBOX：NATBOXを拡張

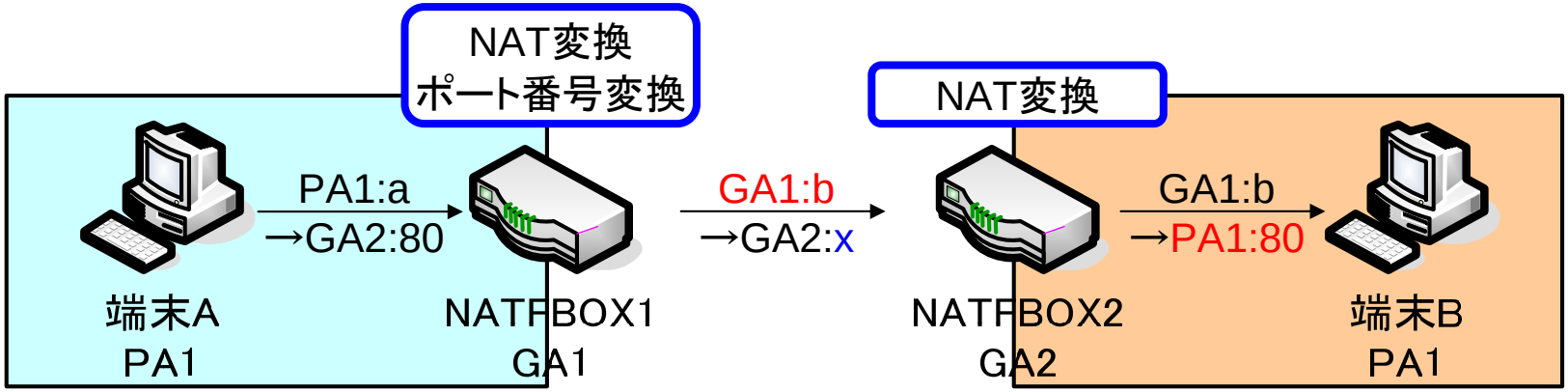
CIPAの流れ（DNS）


端末A
PA1
NATFBOX1
GA1
DNS
NATFBOX2
GA2
home.com
端末B
PA1
alice
DNS問合せ
(alice.home.com)
DNS問合せ
(home.com)
DNS応答
(home.com
⇔GA2)
DNS応答
(alice.home.com
⇔GA2)
NATFBOX1初期登録
ホスト名：alice
ドメイン名：home.com
NATFBOX1は
DNS問い合わせ部を
端末BからNATFBOX2に
書き換える
DNS情報
GA2 ⇔ alice

CIPAの流れ（NATFプロトコル）



CIPAの流れ（NATFプロトコル後）



NATテーブル1	
送信元	宛先
PA1:a ⇔ GA1:b	GA2:80

NATテーブル2	
送信元	宛先
GA1:b	GA2:x ⇔ PA1:80

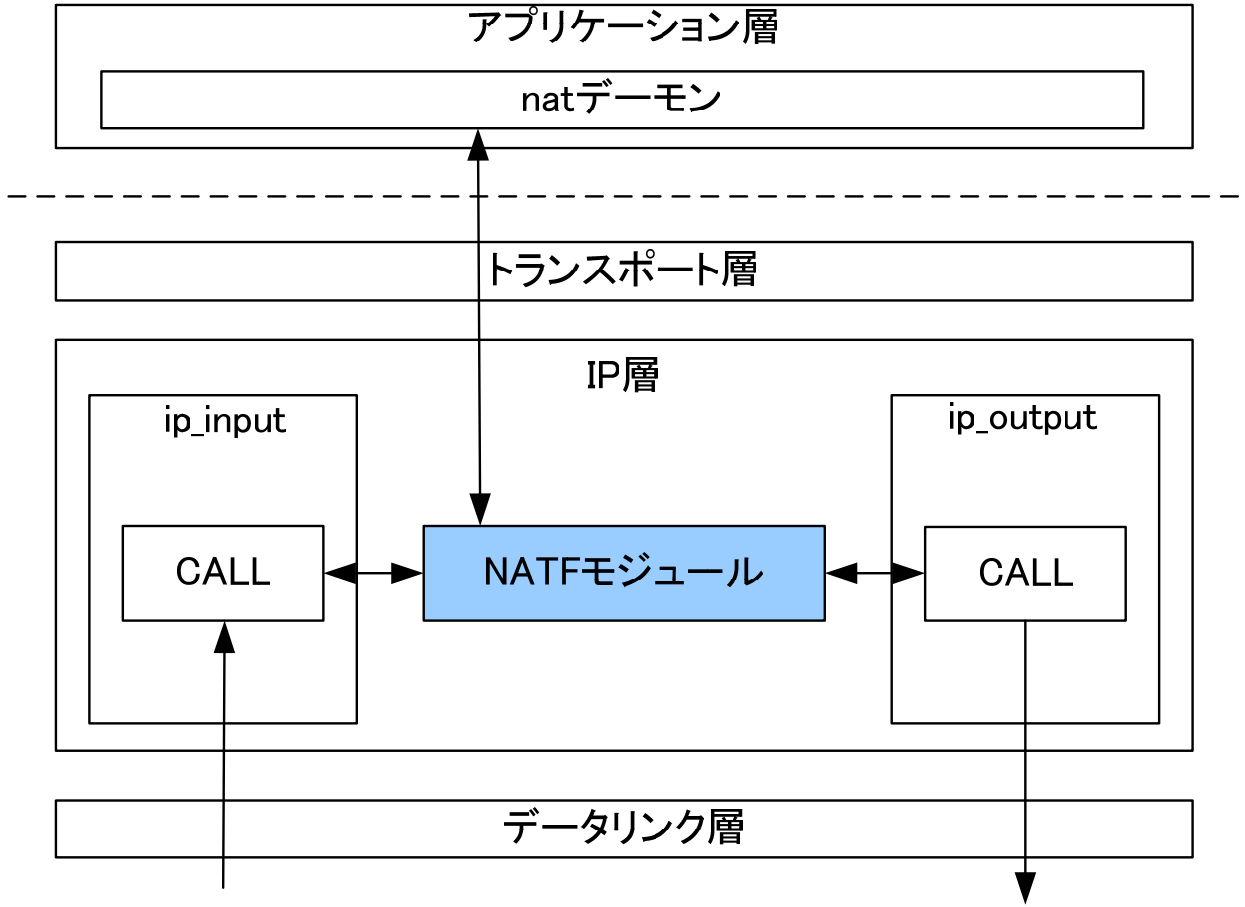
ポート番号変換テーブル
80 ⇔ x

- 端末AはNATFBOX2，端末BはNATFBOX1と通信しているように見える

異なるプライベートアドレス空間同士で通信が可能

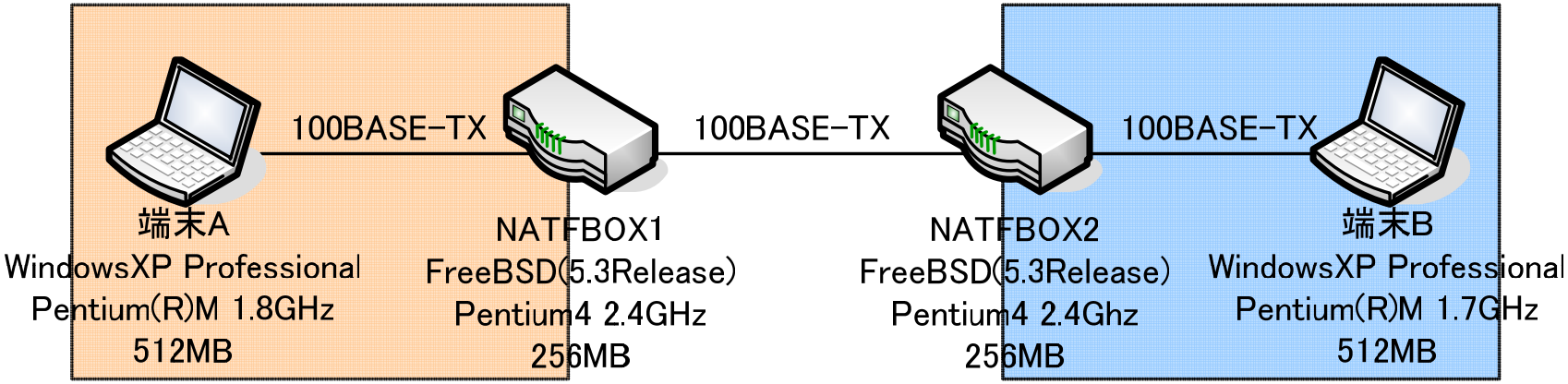
実装（NATFBOX）

- FreeBSD(5.3-R)に実装
- IP層やnatデーモンで行われる既存の処理に変更を加えない



評価実験

- CIPAとポートフォワーディングの性能を比較
  - FTPを用いて100Mbyte のファイルをダウンロードし スループットを計測
  - CIPAはDNS応答処理後のスループットを計測



評価実験

- CIPAとポートフォワーディングの性能を比較
  - FTPを用いて100Mbyte のファイルをダウンロードしスループットを計測
  - CIPAはDNS応答処理後のスループットを計測

	CIPA	ポートフォワーディング
スループット	61.1(Mbps)	62.1(Mbps)

  - CIPAはポートフォワーディングの約98.5%のスループット
  - NATFBOX1におけるポート番号変換テーブルの検索によるオーバヘッドが影響したものと考えられる

まとめ

- 異なるプライベートアドレス空間端末どうしの通信（CIPA）の提案
  - アドレスとポート番号の設定が不要
  - 複数の端末が同じポート番号を利用可能
  - 中継サーバやカプセル化不要
- 提案システムの実装
  - 通信中のオーバヘッドが少ない
- 今後の予定
  - 実環境への適用