アドレス空間の違いを意識しない通信方式の研究

11300j038　加藤尚樹
渡邊研究室

1. はじめに

ADSL をはじめとするブロードバンドの普及による高速通信とモバイル端末機器の発展に伴い，いつでもどこでも通信が行えるようになった．一方，現在 IP アドレスの枯渇，セキュリティの面から NAT をネットワーク構成に入れることが標準的である．しかし，NAT を入れることによって外部からのアクセスができなくなることが問題となっている．この問題を解決するため，グローバルネットワーク端末からプライベートネットワーク端末へのアクセスを可能とする通信方式について提案する．

2. 課題

NAT が介在すると，基本的にグローバルネットワークから通信を開始することはできない．通信開始時においては NAT がグローバルネットワーク側からくるパケットに関するアドレス変換テーブルを持っていないからである．一方，プライベートネットワーク側から通信を開始する場合，通信開始時のパケットの情報よりアドレス変換テーブルを生成することができるため正しく通信を行うことができる．

現在，この問題を解決するためにNATS[1]という技術が提案されている．NATSはプライベートネットワークの各端末のプライベートIPをサブアドレスと呼ばれる識別子としてDNSレコードに設定し，それに応じてパケットを転送する機能である．しかし，新たなDNS問い合わせシーケンスが必要でありオーバヘッドが大きい．また，IP in IPのカプセル化によるパケットの冗長が発生するという課題がある．

3. 提案方式

提案方式について図 1 を用いて説明する．図中番号は処理の順番を，実線矢印はパケットの流れを，破線矢印は処理の流れをそれぞれ表している．はじめにクライアントは DNS サーバに対して Server1 の IP アドレスの問い合わせを行う(①)．その後，DNS サーバは Server1 の IP アドレスがプライベートアドレスであるため，グローバルアドレスを持つルータの IP アドレス『GA1』に変換してクライアントに伝える(③)．それと同時に，ルータに対して問い合わせ時のパケット情報を通達することによって NAT テーブルを生成させる(②)．クライアントにおいては Server1 へ送るパケットの送信元ポート番号『z』を DNS 問い合わせ時に用いたポート番号『x』へ変換する(④，⑤)．その後パケットはルータに送られ，ルータは DNS サーバからの情報より生成した NAT テーブルを用いてパケットを Server1 へと転送する(⑥)．以後の通信に関しては通常の NAT と同様の処理が行われる(⑦，⑧)．最後にクライアントに返答パケットが送られると⑤で変換されていたポート番号を元に戻しアプリケーションへと渡す(⑨)．

4. 比較

表 1 に既存技術と本提案の比較を表に示す． 本提案方式と NATS は、ともに複数台の端末をグローバルネットワークからアクセスできる．本提案においては通信のカプセル化を行わないためパケット長に変化を与えないという利点がある．

表 1：既存技術との比較

	NATS	本提案
複数台で可能であるか	○	○
パケットの変化	△	○
DNS の特殊性	レコード追加	レコード追加

5. まとめ

本稿では端末側でポート番号の書き換えることにより，グローバルネットワーク端末からプライベートネットワーク端末へのアクセスを可能とする方法について提案した．今後は提案方式を実装し，その有効性を確認する．

参考文献

[1] 近藤 邦昭：http://www.nats-project.org/index-j.htm

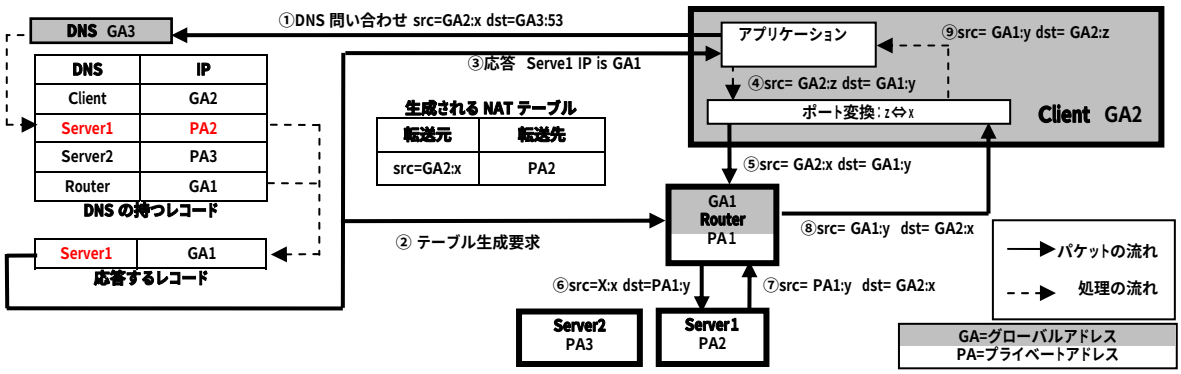


図 1：提案方式の処理の流れ

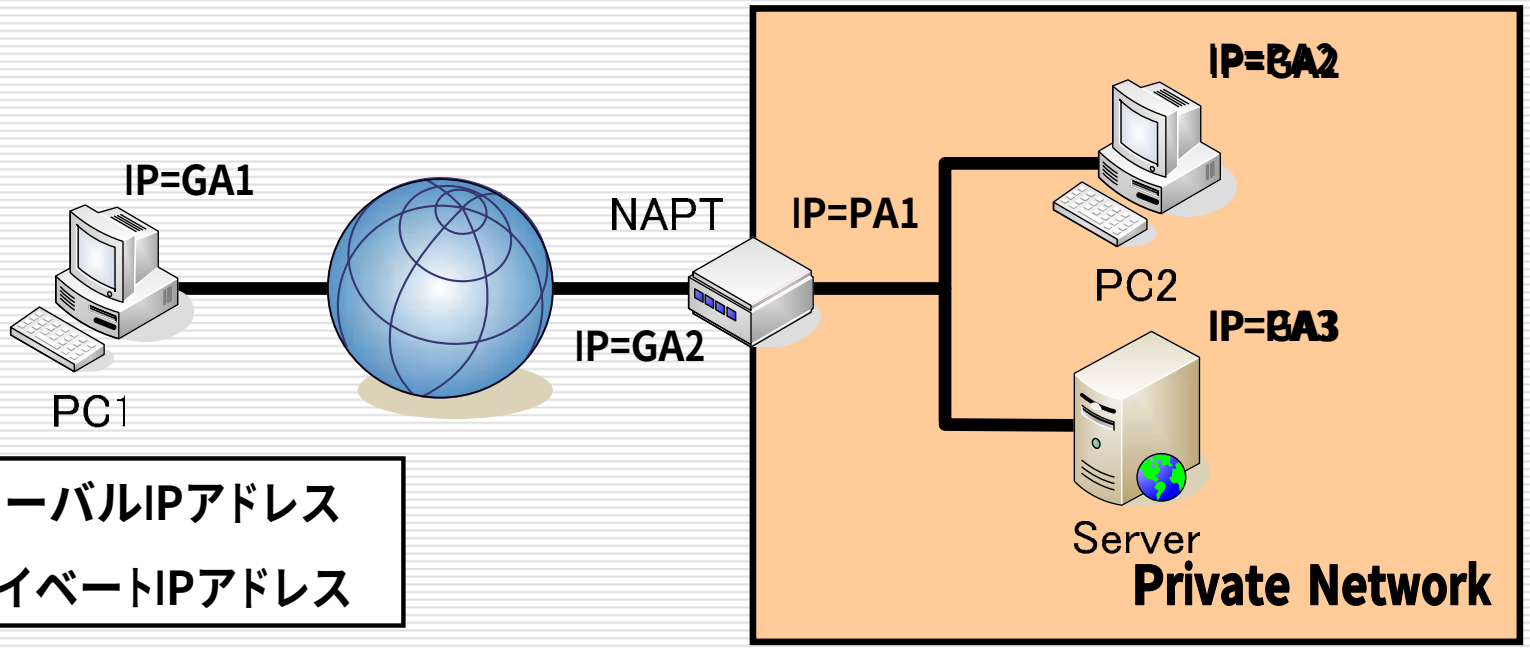
アドレス空間の違いを意識しない通信方式の研究

渡邊研究室
11300j038　加藤尚樹

研究背景

- インターネットの普及
  - いつでもどこからでもサーバに接続したいというニーズ
  - 接続機器の増加によるIPアドレスの枯渇

NAPTの利用



GA＝グローバルIPアドレス

PA＝プライベートIPアドレス

NAPTの動作概要

- NAPT (Network Address　Ports　Translator)
  - プライベートIPアドレスを用いてイントラネットを構築
    - プライベートIPアドレスはイントラネット内のみで有効

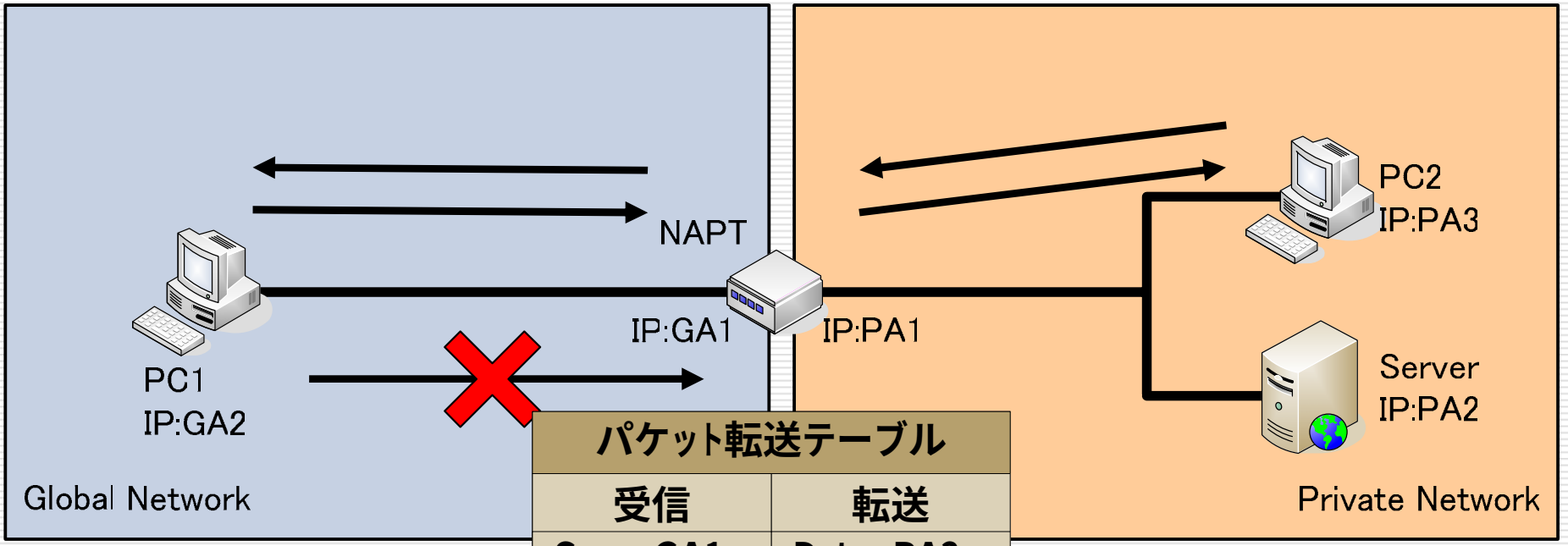
送信元	宛先	

グローバルからの送信時

GA2:y	GA1:a	

GA2:y	PA3:x	

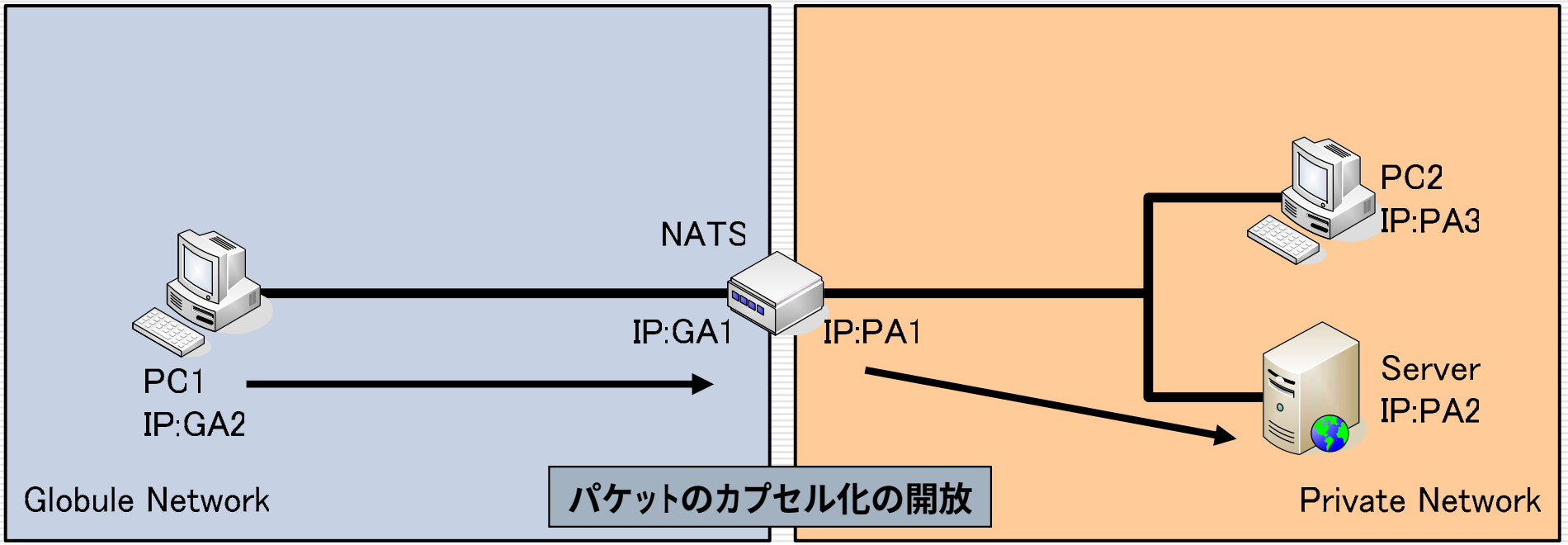
PA3:x	GA2:y	

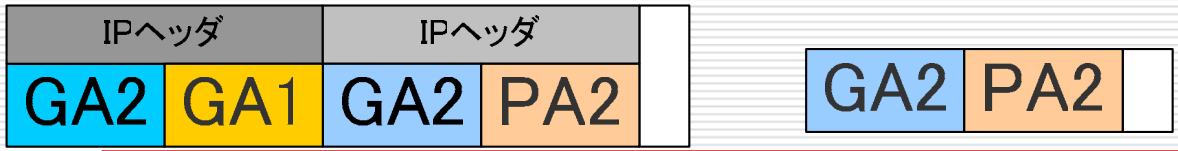


パケット転送テーブル	
受信	転送
Src = GA1:a	Dst = PA3:x

既存技術

- NATS (Network Address Translation with Sub-Address)
  - イントラネットの端末の識別子としてサブアドレスを使用
  - DNSを利用して非対応端末にも接続が可能
  - IP in IP のカプセル化が行われる



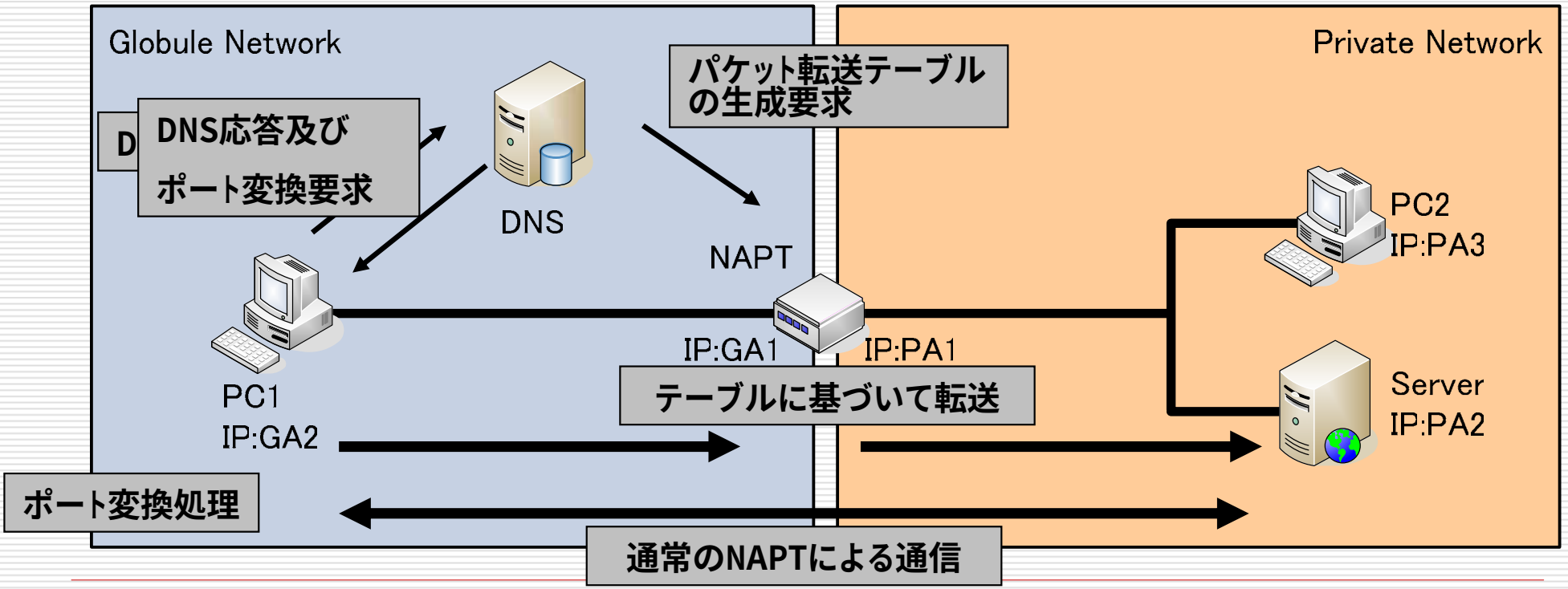


提案方式

概要

- クライアントのDNS問い合わせ時にDNSサーバが処理を要求
  - クライアントにはポート変換を要求
  - NAPTには情報とともにテーブル生成を要求

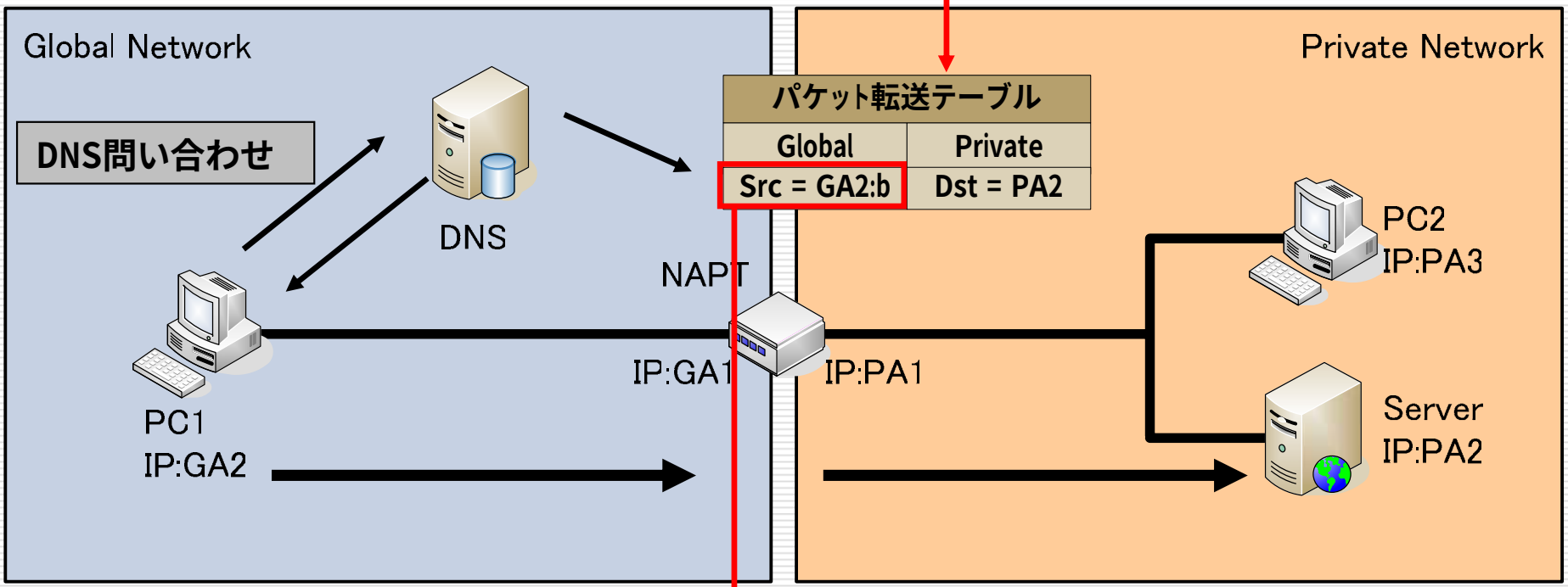
グローバルネットワークから転送可能なNAPTの転送テーブルを生成



提案方式 (詳細)

DNSレコード			
ホスト名	IPアドレス	転送先	ポート
PC1	GA2	ー	ー
PC2	PA3	GA1	a
Server	PA2	GA1	b

テーブル生成要求



送信元	宛先	
GA2:b	GA1:y	
GA2:b	PA2:y	

比較

- NATSと提案方式はともに複数台の端末にグローバルネットワークからアクセスできる。
- 本提案においては通信のカプセル化を行わないのでパケットの長さは変化しない

	NATS	本提案
複数台で 可能であるか	○	○
パケットの変化	△	○
DNSの特殊性	レコード追加	レコード追加
DNSパケットの特徴	NATSにおいてDNSパケットのフッキングを行う	サーバーにおいて レコードの変換を行う

まとめ

- DNSにレコードを追加
  - 外部からのNATのパケット転送テーブルの生成
  - クライアントによるポート番号の書き換え

  ⇒グローバルネットワーク端末からプライベートネットワーク端末へのアクセスが可能

- 今後は提案方式を実装し，その有効性を確認する．

おわり