異なるプライベートアドレス空間端末の通信（CIPA）の提案

柳沢信成　加藤尚樹　鈴木秀和　渡邊晃
名城大学大学院理工学研究科

A proposal of CIPA : Communication between terminals in Independent Private Address areas

Nobushige YANAGISAWA　Naoki KATO
Hidekazu SUZUKI　Akira WATANABE
Graduate School of Science and Technology, Meijo University

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），プライベートアドレス空間（PA 空間）[1] 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 [2] 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 NAPT [3] 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，NAPT 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 NAPT による通信の制約を除去することが望まれる．

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 NAPT 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でこの課題を解決する方法（ポートフォワーディング）[3]もあるが，ネットワーク構成の変化やアプリケーションごとにテーブルを設定し直さなければならず，自由な通信とは言えない．筆者らは端末側に新たにポート変換機能を追加することにより GA 空間からの通信開始を可能とする NATF（NAT Free Protocol）を提案してきた [4].

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通信を可能にする方式を提案する．この方式を，ここでは CIPA（Communication between terminals in Independent Private Address areas ; サイパ）と呼ぶ．一般に，異なる PA 空間ではアドレス管理が別々に行われており，アドレスの重複があり得る．したがって，このような通信を P2P で実現しようという発想はこれまでなかった．しかし，今後は各家庭内のプライベートアドレス端末同士の P2P 通信のニーズはあり得ると考えられ，これが実現できれば，今後のユビキタス社会において有益である．

CIPA では，NATF で拡張した端末の機能を NATF BOX に持たせる．すなわち，2 台の NATF BOX が，通信開始に先立って通信を行うポート番号の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，ポート番号変換を行うことにより制約のない通信を行うことが可能になる．特に本稿では異なる PA 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 を流用することにより通信が可能であることを示す．

以下，2 章に NATF，3 章に CIPA の実現方式について，4 章に実装方法，5 章に応用例である位置情報取得システム，6 章にまとめを述べる．

2.　NATF（NAT Free protocol）

NATF は，端末・DNS・NATF BOX が連携し，GA 空間の端末から PA 空間の端末への通信を可能とするプロトコルで

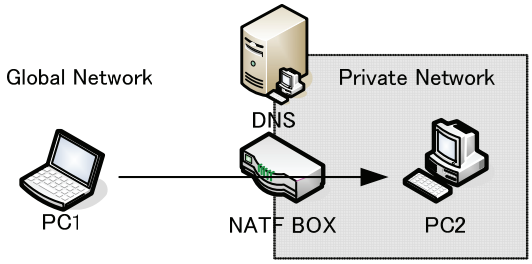


図 1　NATF の環境

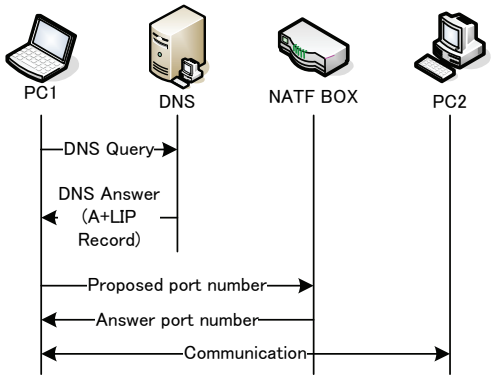


図 2　NATF のシーケンス

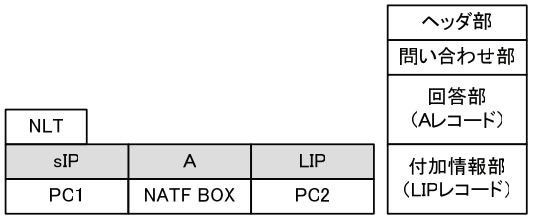


図 3　NLT と DNS 応答

ある．NATF BOX とは NATF が適用されたアドレス変換装置のことである．NATF の環境を図 1 に，NATF のシーケンスを図 2 に示す．DNS には，あらかじめドメイン内に存在する端末のプライベートアドレスを，LIP（Local IP）と呼ぶ拡張レコードとして登録しておく必要がある．DNS は，PC1 から PC2 に対する IP アドレスの問合せがあると，A レコードと共に，上記 LIP レコードを付加して応答する．ここで，A レコードは NATF BOX のグローバルアドレス，LIP レコードは PC2 のプライベートアドレスとなる．端末 PC1 の IP 層において，この DNS 応答から送信元 IP アドレス，宛先 IP アドレス，LIP アドレスを記憶する NLT(NATF List Table) を作成する(図 3)． DNS 応答を IP 層から上位層へ渡す際，LIP レコード(PC2)を削除し，A レコード（NATF BOX）のみを渡す．アプリケーションでは，通信相手はグローバルアドレスを持つ NATF BOX であると認識する．次に，PC1 は NATF BOX に対して通信を行うが，通信開始に先立ち，NATF プロトコルを実行する．PC1 は，最初のパケットを一時待避し，NATF BOX にポート番号報告指示パケットを送信する．このパケットには，PC1 が通信中に使う送信元アドレス・ポート番号，宛先アドレス・ポート番号，LIP，プロトコルの情報が含まれる． この情報を元に NATF BOX はアドレス変換テーブルを生成する．NATF BOX はここでアドレス変換用の割り当てたポート番号を，ポート番号報告応答パケットを用いて PC1 に送り返す． PC1 は，報告されたポート番号を元に，ポート番号変換テーブルを生成し，NLT を削除する．PC1 は以後の通信においては宛先ポート番号を，ポート番号変換テーブルを用いて変換する．一方，NATF BOX は上記 NAPT アドレス変換テーブルを用いて IP アドレス変換とポート番号変換を行う．以上の動作により，GA 空間から PA 空間への通信が開始可能となる．

3. CIPA の実現方式

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．提案システムの環境を，図 4 に示す．CIPA では通信端末は一般端末でよく，NATF BOX 同士が NATF プロトコルを実行する．送信元の NATF BOX は NAPT アドレス変換に加え，ポート番号の変換，即ち NATF おけるグローバルアドレス側端末が実行していたポート番号変換を行う．本章では，図 4 における PC1 と PC3 が同一のプライベートアドレスを持っているものとし，CIPA 両者が問題なく通信できることを示す．

PC1 から PC3 へ接続を開始する場合の通信の流れを図 5 に示す．PC1 は PC3 に関する DNS 問合せを行う．DNS は，A レコードとして NATF BOX Y のグローバルアドレス（200.0.0.1）を，LIP レコードとして PC3 のプライベートアドレス（192.168.0.1）の情報を載せた DNS 応答を返す．

NATF BOX Y の GA と PC3 の PA のペアは唯一無二であるため，同一のプライベート IP アドレスを持つ端末が存在しても両者の区別が可能である．

NATF BOX X がこの DNS 応答を受け取ったら NLT を作成する．次に，応答パケットから LIP レコードを分離し，A レコードのみを載せた DNS 応答を PC1 へ送る．PC1 は DNS 応答を受け取ったら通信を開始する．

以下 IP アドレスとポート番号の関係を，順を追って示す．矢印の左側は送信元 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．PC1 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，PC3 を WEB サーバと仮定し，宛先ポート番号を 80 とすると，PC1 が送信するパケットは次のようになる．

192.168.0.1：a / 200.0.0.1：80

NATF BOX X はこのパケットを受信すると，NLT を検索する．該当する NLT が存在したら NATF BOX 間で NATF プロトコルを実行するための準備を行う．NATF BOX X は一般の NAPT の手順に従い NAPT テーブルを生成し，最初のパケットのアドレス変換を行っておく．NAPT テーブルの情報は以下のように生成される．b は NAPT 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⇔60.0.0.1：b}

したがって，アドレス変換後のパケットは

60.0.0.1：b / 200.0.0.1：80

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 NATF BOX X 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 NATF BOX Y に送る．このパケットには，送信元 IP アドレス：ポート番号（60.0.0.1：y）と LIP：ポート番号（192.168.0.1：80）とプロトコル情報が含まれる．

NATF BOX Y は上記ポート番号報告指示パケットを受信したら， NATF BOX Y は NAPT テーブルを生成する．テーブルの内容は以下の通りである．c は NAPT 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⇔200.0.0.1：c}

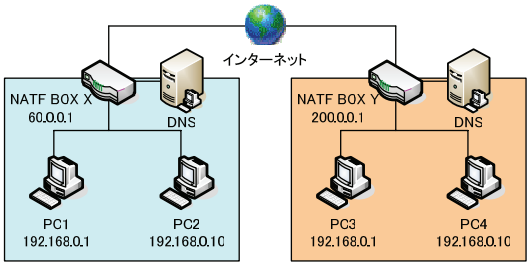


図 4 CIPA の環境

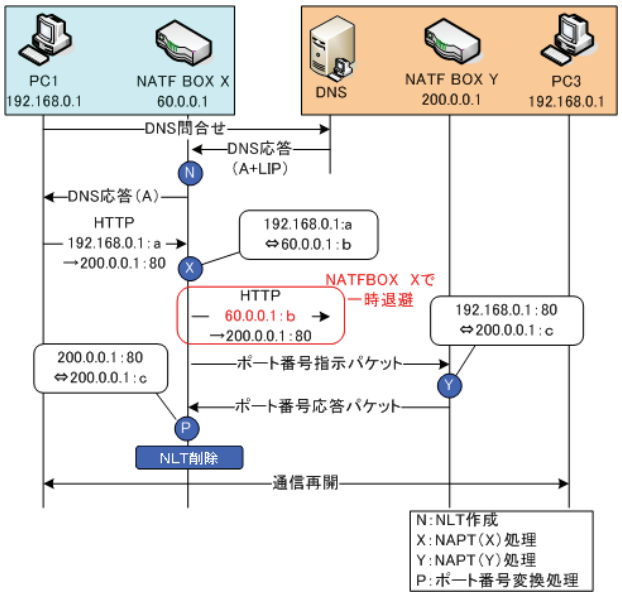


図 5 CIPA のシーケンス

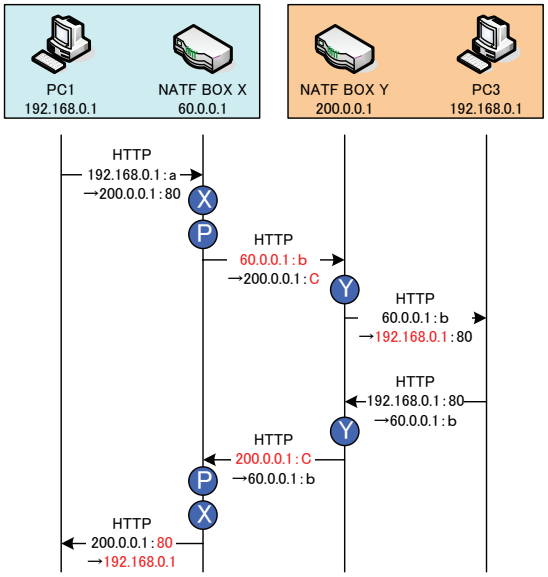


図 6　通信再開後の流れ

テーブル生成後，疑似パケットは破棄する．NATF BOX Y はこの変換ポート番号（c）を，ポート番号報告応答パケットを用いて NATF BOX X に送る．

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

{200.0.0.1：80⇔200.0.0.1：c}

ポート番号変換テーブル作成後，NLT を削除し 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図 6 に示す．NATF BOX X は，待避していたパケットを NAPT テーブルにより，アドレス/ポート番号変換後，ポート番号変換テーブルより更にポート変換し，NATF BOX Y 宛に送信する．このパケットの内容は次のとおりである．

60.0.0.1：b / 200.0.0.1：c

このパケットを受信した NATF BOX Y では，NAPT アドレス変換後，PC3 に送信する．パケットの内容は以下のように変わる．

60.0.0.1：b / 192.168.0.1：80

PC3 から PC1 への応答は，上記と逆の変換で行われる．

以下，NATF BOX X では NAPT アドレス変換とポート番号変換，NATF BOX Y では NAPT アドレス変換をすることで，通信を行う

このように，NATF BOX 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 NATF BOX が 2 つのポート番号の変換を行う．PC1 は NATF BOX Y と，PC3 は NATF BOX X と通信しているようにみえる．

4.　.実装

4.1　実装の概要

試作システムは，IP 層の詳細な処理フローに関する情報が多い FreeBSD を採用する．natd を組み込んだ FreeBSD カーネル内に，NATF モジュールを組み込むことで実現方法を検討中である．natd のアドレス変換はアプリケーション層で行われるが，NATF のポート番号変換は IP 層で行う．ポート番号変換テーブルはハッシュテーブルとして実装する．

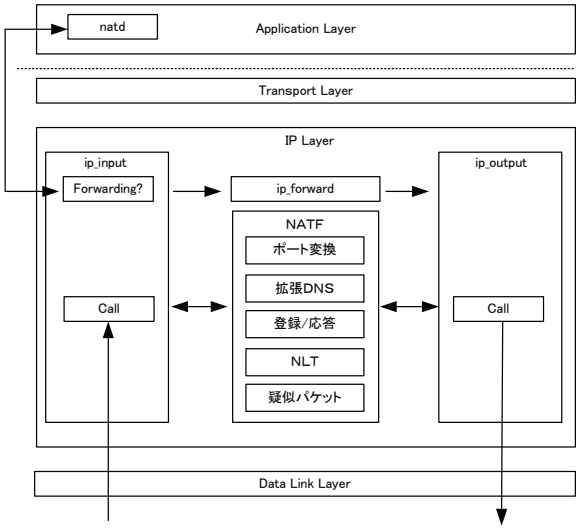


図 7　モジュール構成

ハッシュ検索アルゴリズムはチェイン法を用いる．図 7 のように，natd や IP 層で行われる既存の処理に一切の変更を加えず，IP 層の ip_input，ip_output から NATF モジュールに処理を渡し，処理を終えたら差し戻す形を採用する．

4.2　試作モジュールと機能

NATF の試作システムはポート変換モジュール，拡張 DNS モジュール，NLT モジュール，登録/応答モジュール，疑似パケットモジュールで構成される．

ポート変換モジュールは，ポート番号応答パケットの情報により，ポート番号変換テーブルを作成し，ポート番号変換処理を行う．拡張 DNS モジュールは，DNS 応答パケット受信時に A レコードと LIP レコードを分離し，端末に A レコードのみ転送する．また，A レコードと LIP レコードの情報を NLT モジュールに渡す．NLT モジュールは，拡張 DNS モジュールから受け取った情報から NLT テーブルを作成する．登録/応答モジュールは，送信時に NLT テーブル検索を行い，該当したらパケットを一時待避させ，パケットの情報（送信元 IP アドレス・ポート番号，宛先 IP アドレス・ポート番号，プロトコル）と NLT テーブルの情報（LIP）よりポート番号指示パケットを作成する．また，ポート番号指示パケット受信時には，その情報を疑似パケットモジュールに渡す．疑似パケットモジュール終了後，NAPT テーブルの情報からポート番号応答パケットを作成する．疑似パケットモジュールは，疑似パケットと呼ぶ仮想的なパケットを作成する．このパケットは，NATF BOX にプライベートアドレス空間側の端末からグローバルアドレス空間側へ通信が行われたと見せかけ NAPT テーブルを強制的に作成させる．ポート番号指示パケットから受け取った情報から，疑似パケットを作成し，NAPT テーブルを作成する．

5.　応用例

提案方式の適用事例として位置情報取得システムが考えられる．このシステムではインターネットを用いてターゲットの位置情報を別な場所から常に把握することができる．図 8 に位置情報取得システムの構成を示す．監視端末はターゲットの位置を知りたいユーザが保持する端末である．ターゲットは，子供などが保持する小型端末で，将来的にはより小型になり常時保持が可能になることを想定する．ターゲットの

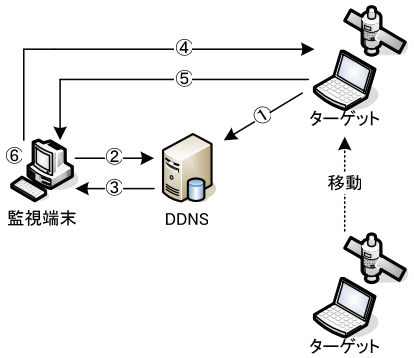


図 8 位置情報取得システムの構成

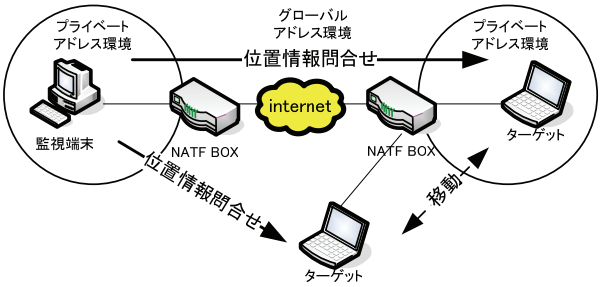


図 9 CIPA と位置情報取得システムの組み合わせ

位置情報の取得は GPS から取得する．DDNS（Dynamic DNS）はターゲットのホスト名と IP アドレスの関係をダイナミックに管理する装置である．

システムの動作は以下の通りで，図中の番号と説明の番号は同様の動作を示す．

①ターゲットが移動して IP アドレスが変化すると,ターゲットは新しい IP アドレスを DDNS サーバに通知する．

②監視端末はターゲットの位置情報を知りたいとき，DDNS サーバに対してターゲットのホスト名を基にターゲットの IP アドレスを問い合わせる．

③DDNS サーバが監視端末へターゲットの IP アドレスを渡す．

④監視端末は獲得した IP アドレスによって，ターゲットに対して位置情報を要求する．

⑤ターゲットは監視端末へ位置情報を返す．

⑥監視端末はターゲットの位置を画面に表示する．

このシステムはインターネットを用いてターゲットの位置を把握できるのが特徴であるが，図 9 のように監視者はプライベートアドレス空間におり，ターゲットは別のプライベートアドレス空間とグローバルアドレス空間を移動する可能性がある．本稿の提案方式と組み合わせることによりターゲットがどのように移動しても位置情報を取得することができる．

もし監視端末とターゲットの両者に NATF 機能を実装すれば，監視端末，ターゲットともどの空間に移動しても位置情報を取得できる．ただし，プライバシの確保が重要であり，認証技術との組合せも必要となる．

6. 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方式 CIPA の提案を行い，実装方法，応用例を述べた．異なる PA 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 を流用することにより通信が可能であることを示した．

今後は，実装を完了し，システムとしての動作検証と性能評価を行う．また，IPv6 について本手法の適用を検討する．

文　献

[1] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, “Address Allocation for Private Internets”, RFC1918, February 1996

[2] S. Deering, R. Hinden, “Internet Protocol, Version6 (IPv6) specification”, RFC2460, December 1998

[3] P. Srisuresh, M. Holdrege, “IP Network Address Translator (NAT) Terminology and Considerations”, RFC2663, August 1999

[4] 加藤尚樹，渡邊晃，“アドレス空間の違いを意識しない通信方式 NATF の提案と実装”，研究報告「マルチメディア通信と分散処理」No.2005-DPS-122 ，March 2005

[5] 柳沢信成，渡邊晃，“グローバルアドレスをはさんだプライベートアドレス端末同士の通信の提案と実装”,研究報告マルチメディア通信と分散処理」No.2005-DPS-122 ，March 2005

[6] 鈴木秀和，渡邊晃，“フレキシブルプライベートネットワークにおける動的処理解決プロトコル DPRP の実装”，研究報告「コンピュータセキュリティ」No.2005-CSEC-028 ，March 2005

[7] Kuniaki Kondo，“Capsulated Network Address Translation with Sub-Address(C-ＮＡＴS)”，Internet Draft, draft-kuniaki-cap sulated-ＮＡＴS-03.txt，December 2002

[8] 竹内元規，渡邊晃，“モバイル端末の移動透過性を実現する Mobile PPC の実装”，研究報告「モバイルコンピューティングとユビキタス通信」No.2005-MBL-032 ，March 2005

[9] P. Mockapetris，“DOMAIN NAMES- IMPLEMEN -TATION AND SPECIFICATION”，RFC1035，November 1987

[10] S. Thomson， Y. Rekhter， J. Bound，“Dynamic Updates in the Domain Name System (DNS UPDATE)”，RFC2136，April 1997

異なるプライベートアドレス空間端末の通信（CIPA）の提案

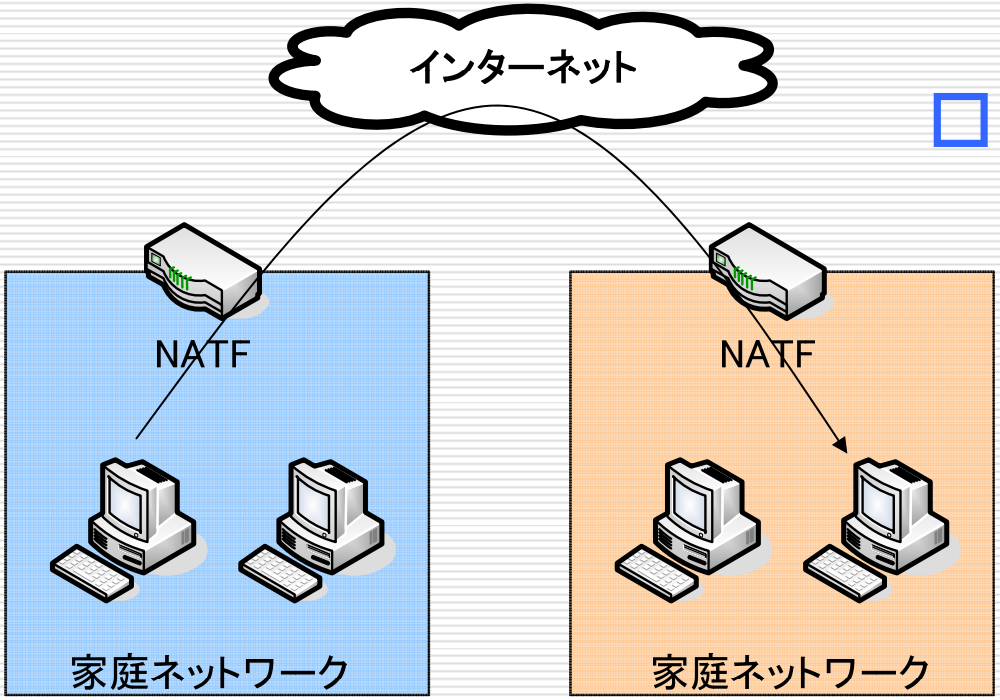
名城大学大学院理工学研究科
柳沢信成　加藤尚樹　鈴木秀和　渡邊晃

はじめに

- 家庭ネットワークの普及
  - ユビキタス社会
- IPアドレスの枯渇
  - NAT
    - 多くの端末がプライベートネットワークへ
    - 自由に通信が行えない

目的

- 異なるプライベートアドレス端末同士で通信を行う
  - 家庭ネットワークでは企業のような厳密なFWはない



- 課題
  - プライベートアドレスはインターネットで使えない
  - インターネット側からプライベートアドレス空間にアクセスを開始できない
  - プライベートアドレス空間はアドレス管理が別々

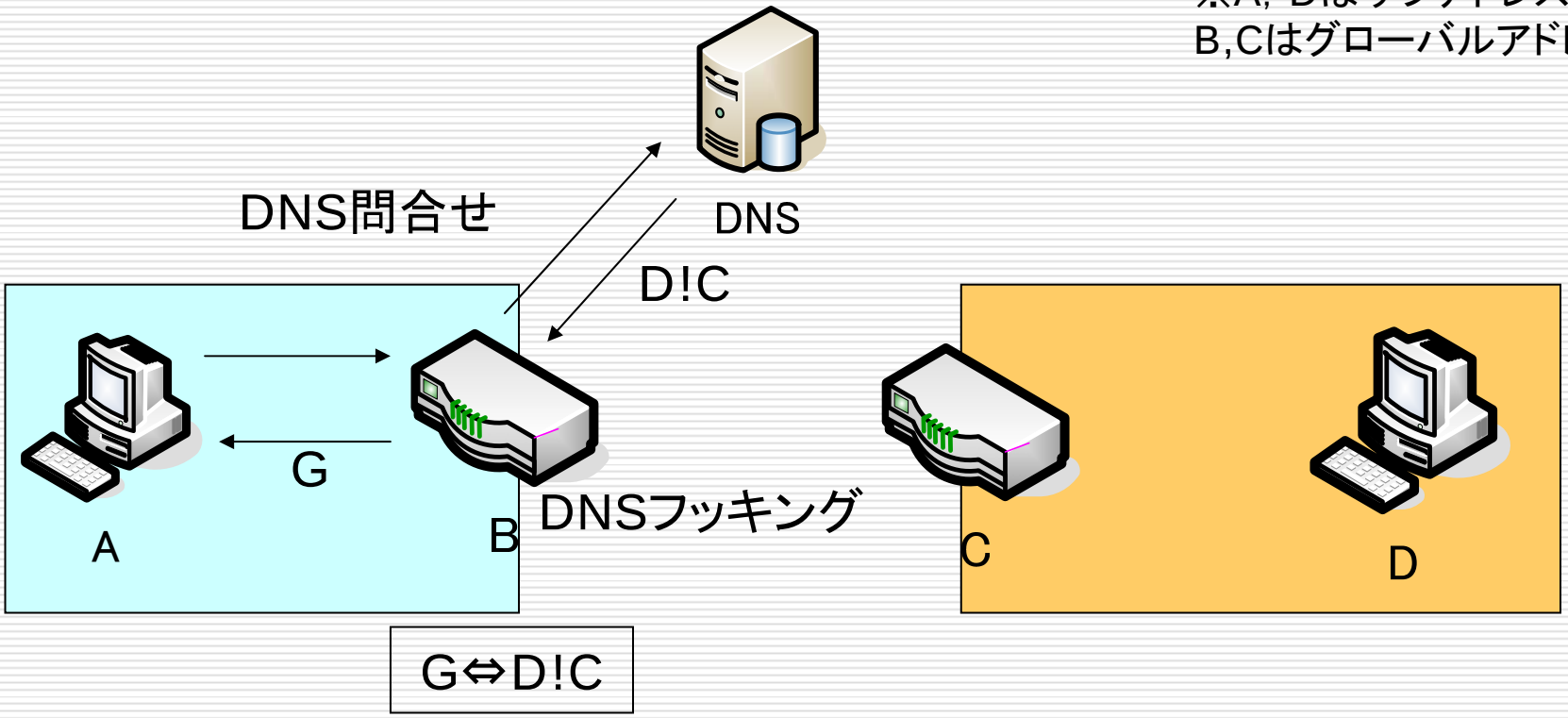
既存技術

- NATS
- SoftEther

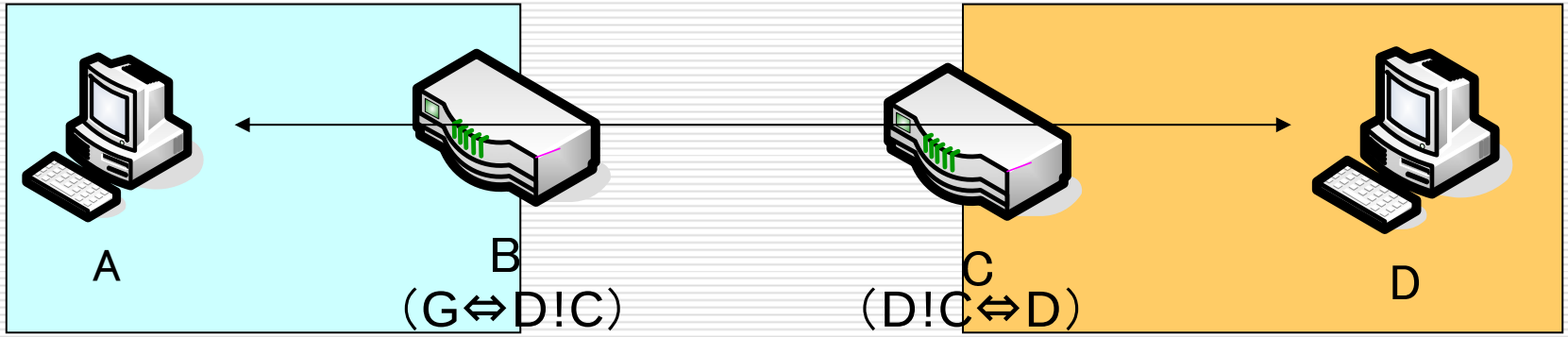
NATS(1)

- NATSとDNSが連携し，サブアドレスをIP in IPカプセリングを行い通信を行う

※A，Dはサブアドレス
B,Cはグローバルアドレス



NATS(2)

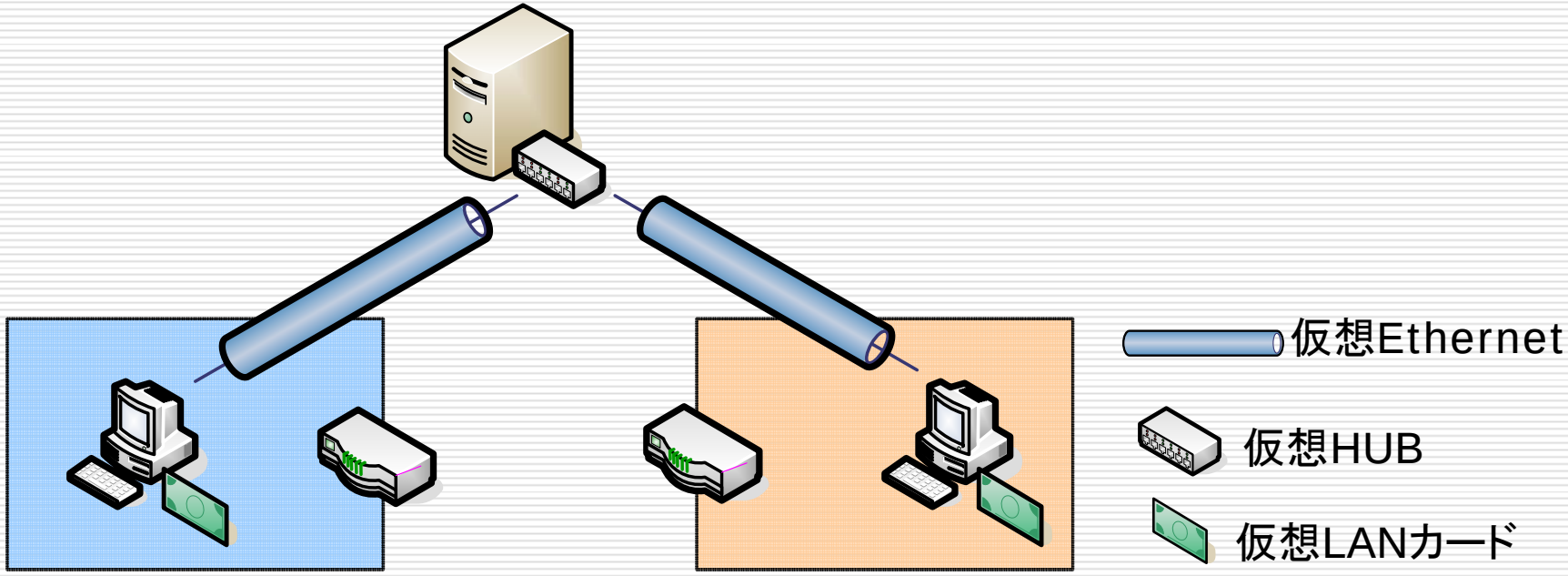


A→G	A!B→D!C	B→D
A←G	A!B←D!C	B←D

- NATS_B
  - 宛先アドレスGならば、IP in IPでカプセル化
- NATS_C
  - デカプセル化

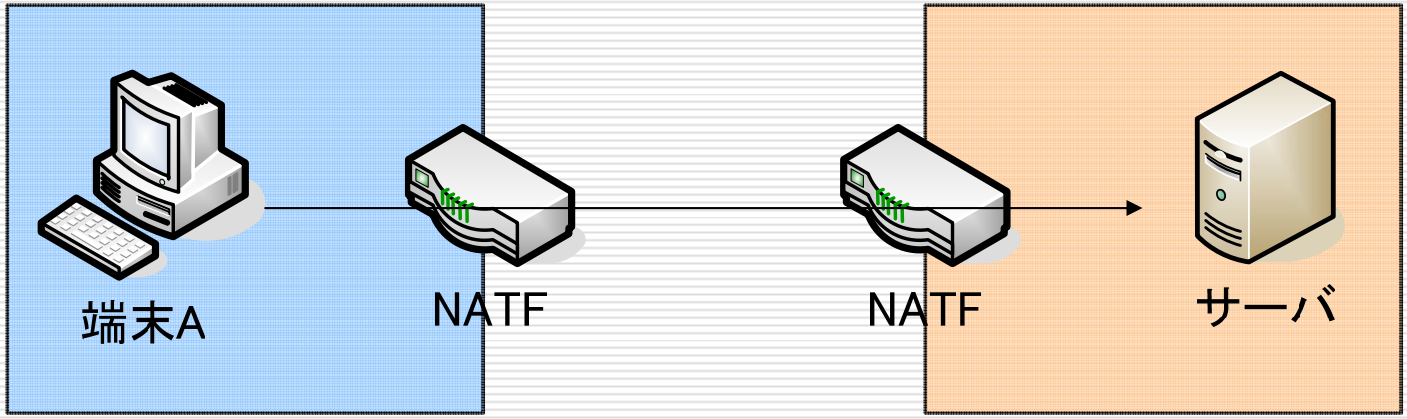
SoftEther

- 仮想HUBと仮想LANカードにより、TCP/IPネットワーク上に仮想的なEthernetネットワークを構築
  - アドレス環境の統一管理が必要
  - セキュリティ対策が別途必要



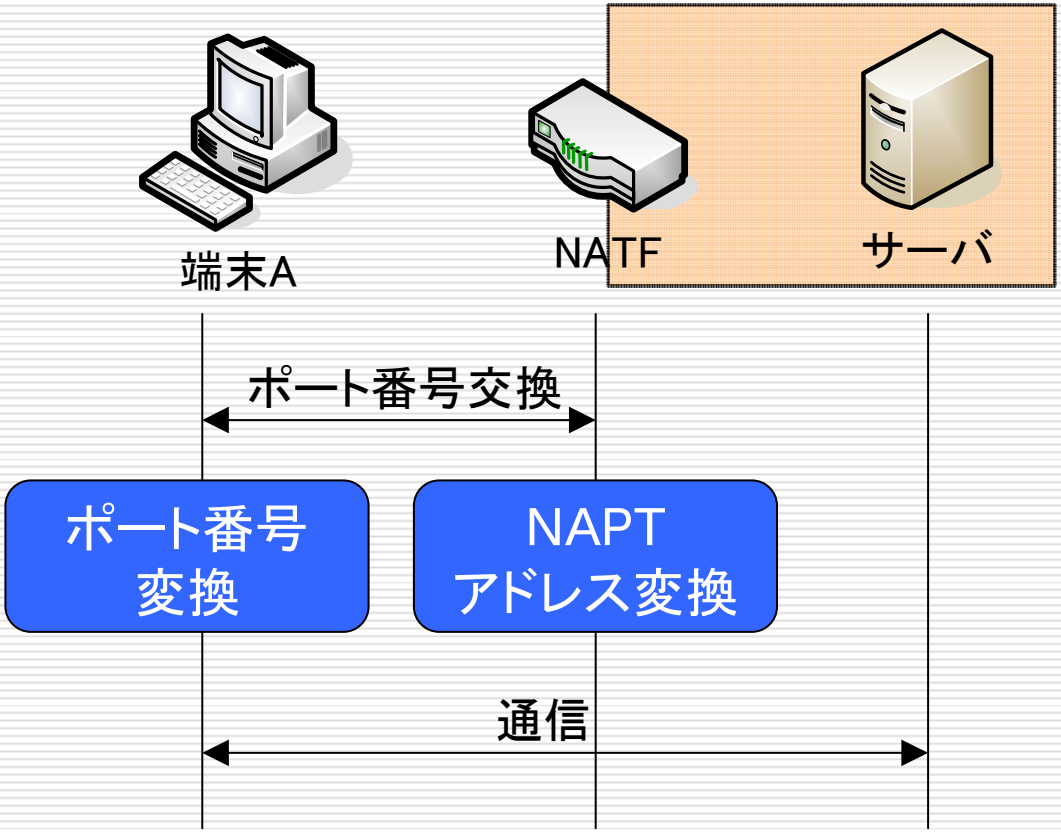
提案システム

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



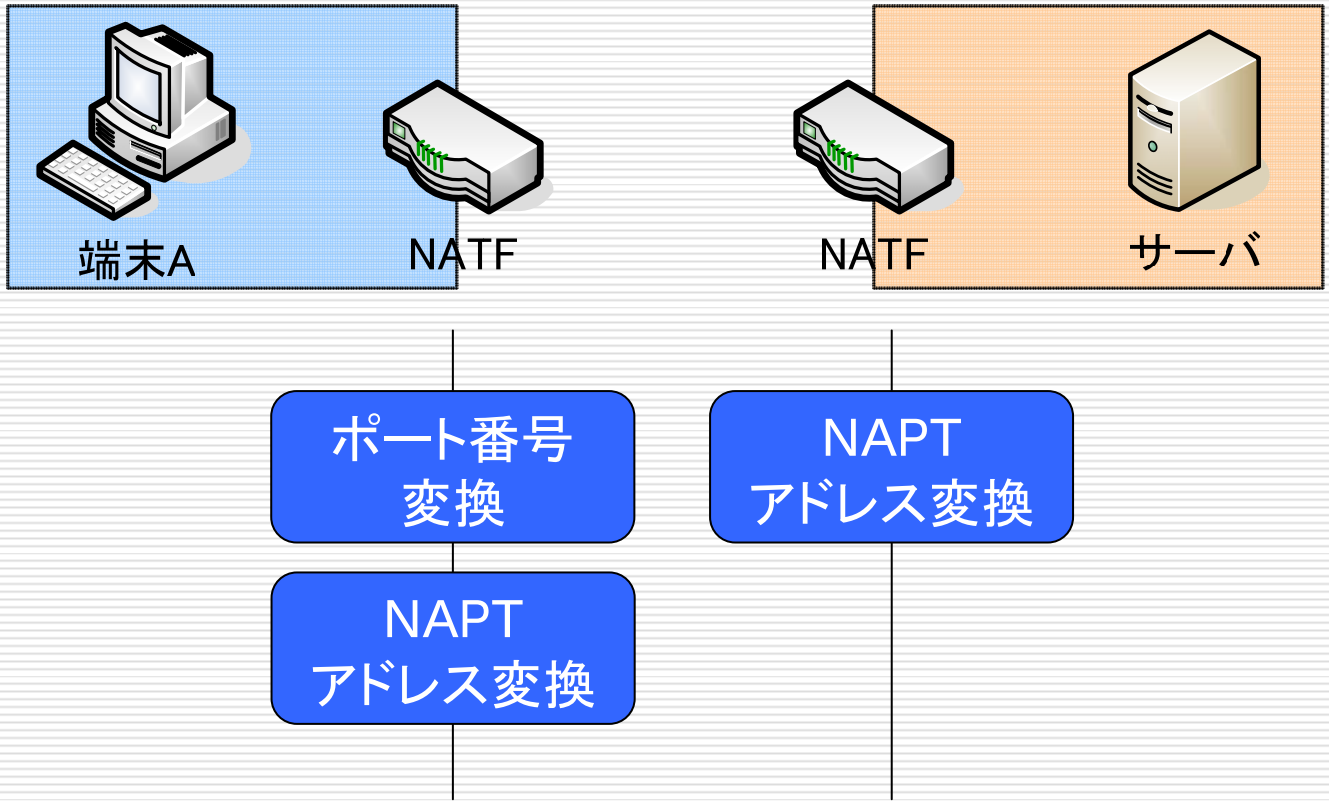
NATF（NAT Free protocol）

- 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の提案

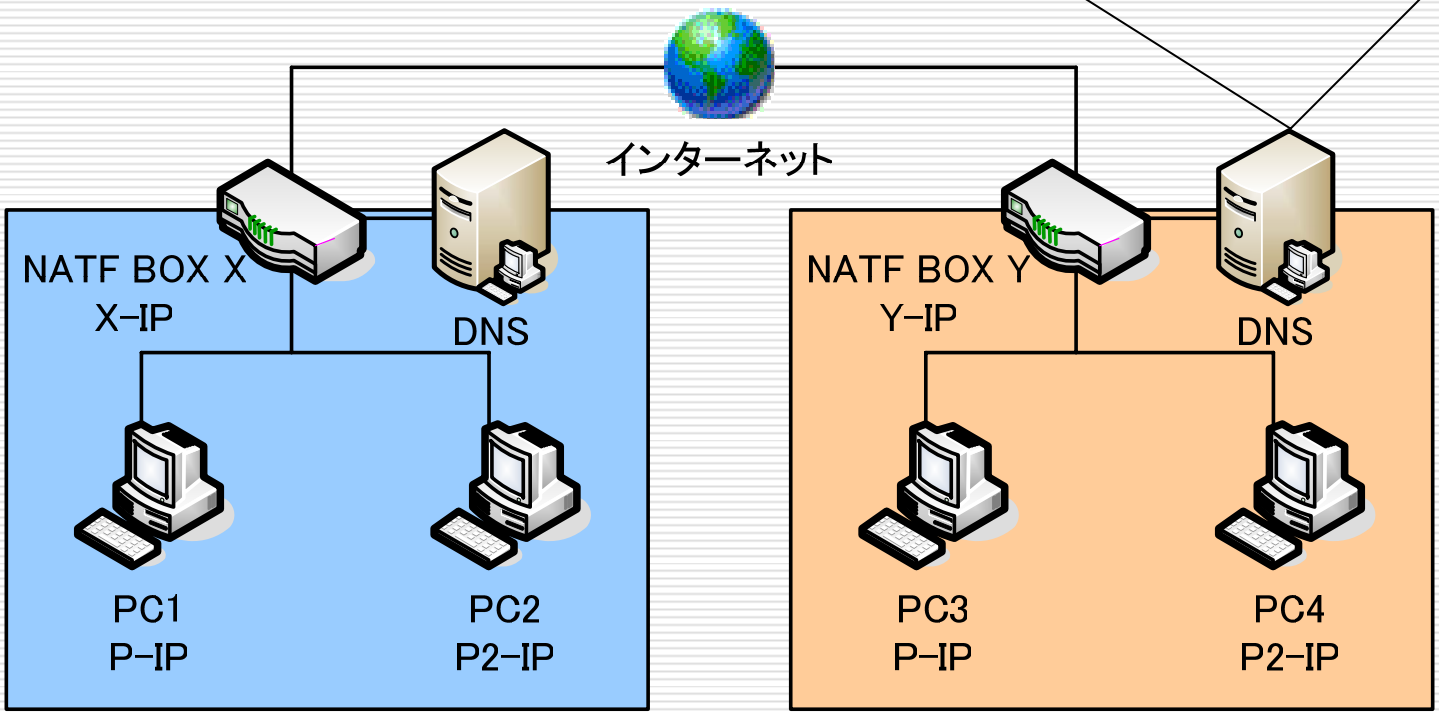
- NATFにおける端末側の機能（ポート番号変換）をNATFが代行



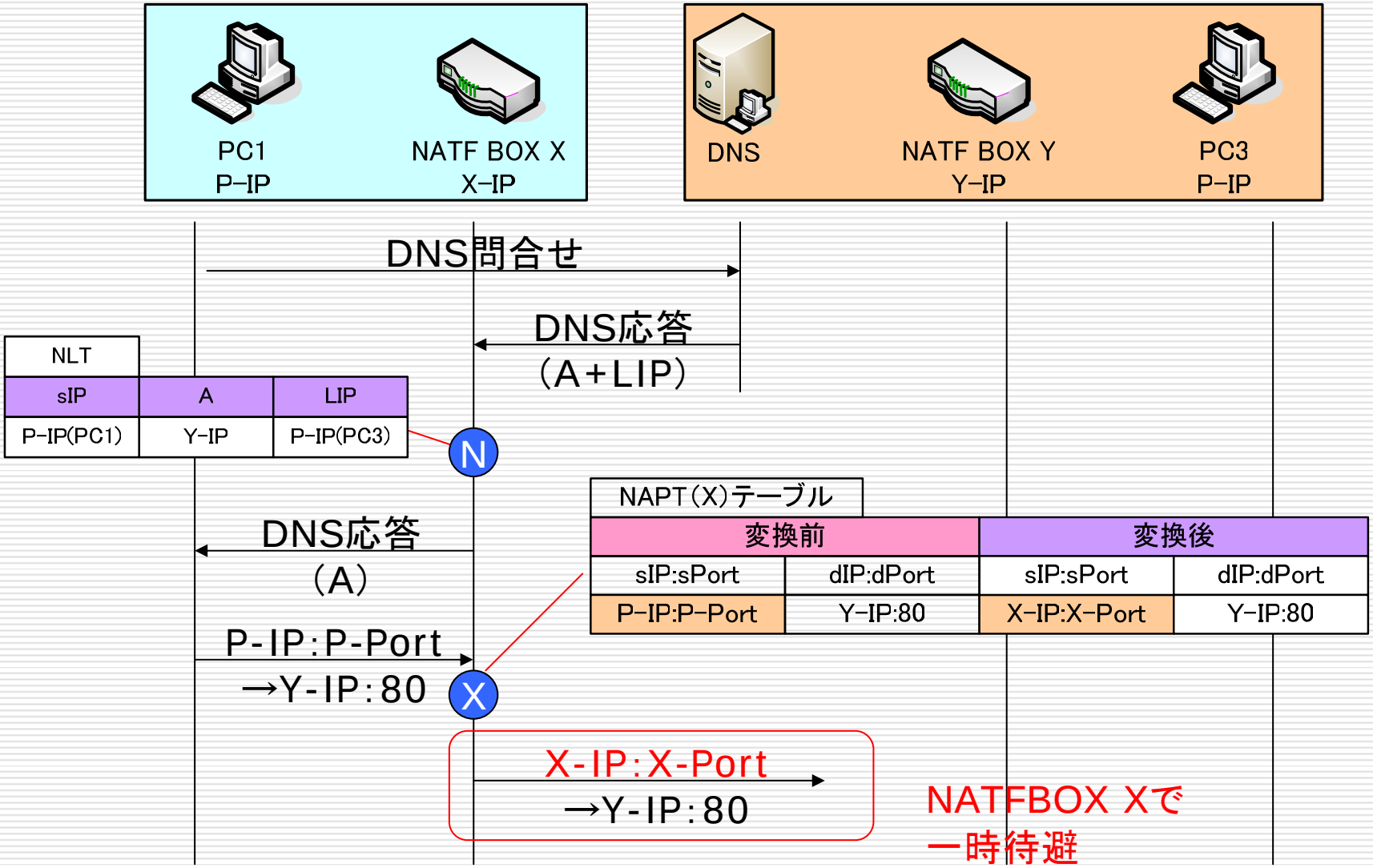
CIPA

環境

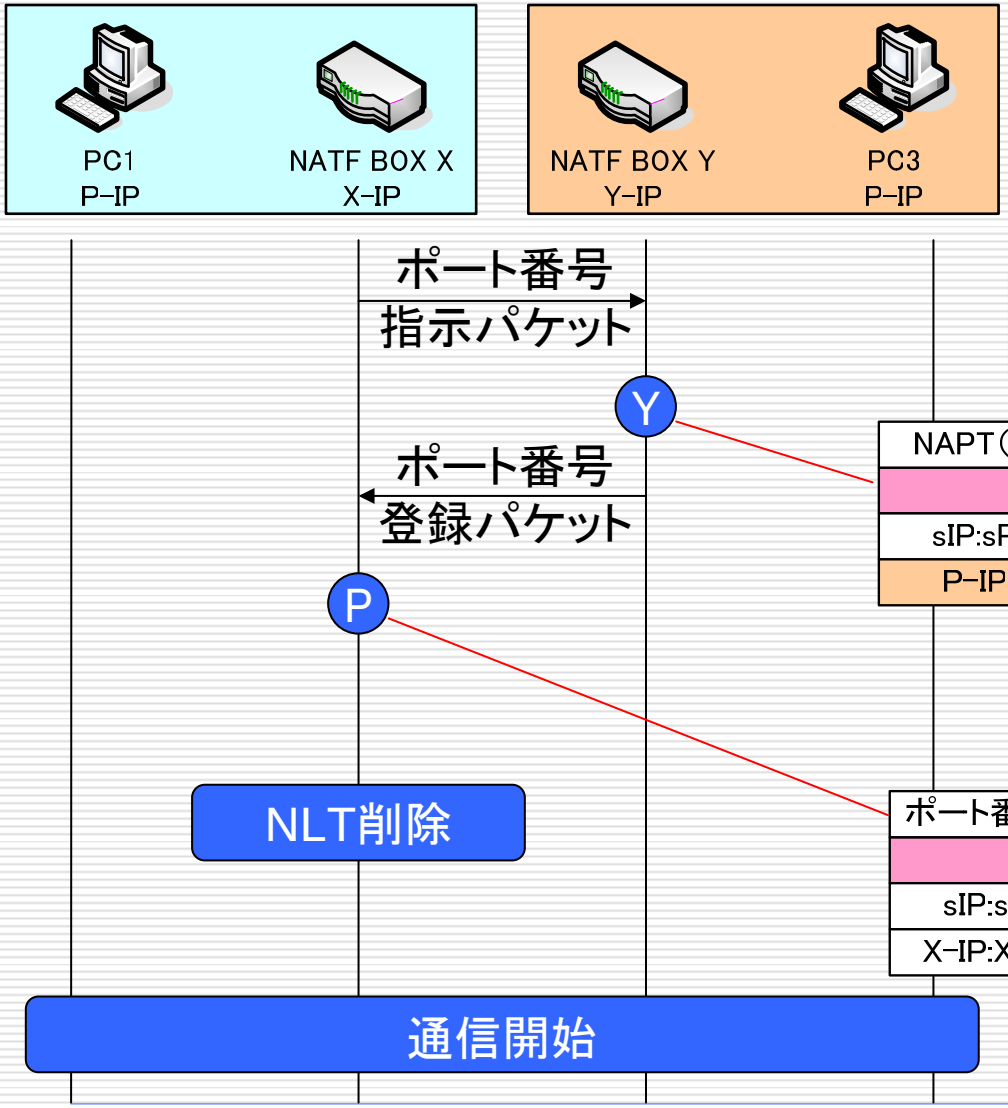
	IPAddress
NATF Y	Y-IP
PC3	P-IP
PC4	P2-IP



CIPAの流れ1


PC1
P-IP
NATF BOX X
X-IP
DNS
NATF BOX Y
Y-IP
PC3
P-IP
DNS問合せ
DNS応答
(A+LIP)
NLT
sIP
A
LIP
P-IP(PC1)
Y-IP
P-IP(PC3)
N
NAPT(X)テーブル
変換前
変換後
sIP:sPort
dIP:dPort
sIP:sPort
dIP:dPort
P-IP:P-Port
Y-IP:80
X-IP:X-Port
Y-IP:80
DNS応答
(A)
P-IP:P-Port
→Y-IP:80
X
X-IP:X-Port
→Y-IP:80
NATFBOX Xで
一時待避

CIPAの流れ2



退避パケットパケット内容
X-IP, X-Port, Y-IP, 80

NLT
P-IP(PC1), Y-IP, P-IP(PC3)

ポート番号指示パケット内容
X-IP, X-Port, Y-IP, 80, P-IP(PC3)

NAPT(Y)テーブル

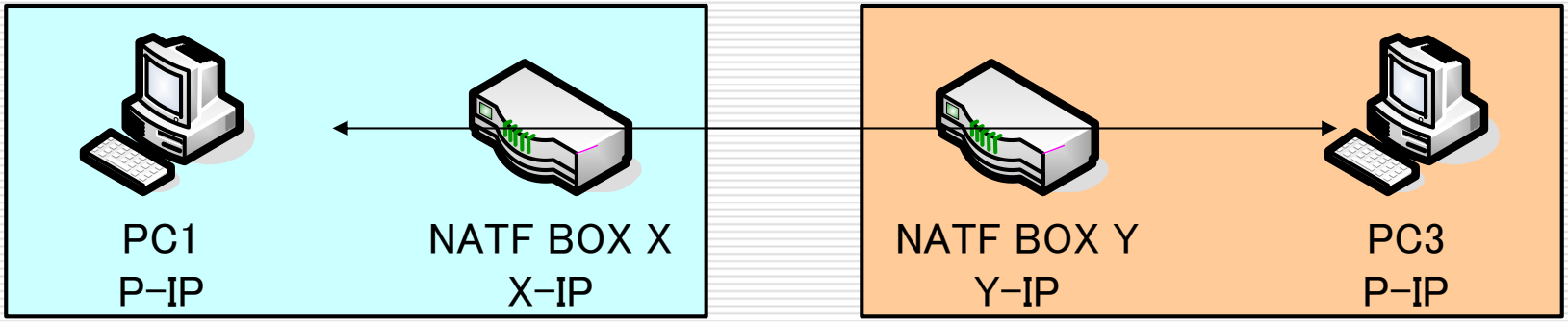
変換前		変換後	
sIP:sPort	dIP:dPort	sIP:sPort	dIP:dPort
P-IP:80	X-IP:X-Port	Y-IP:Y-Port	X-IP:X-Port

ポート番号登録パケット内容
Y-Port

ポート番号変換テーブル

変換前		変換後	
sIP:sPort	dIP:dPort	sIP:sPort	dIP:dPort
X-IP:X-Port	Y-IP:80	X-IP:X-Port	Y-IP:Y-Port

CIPAの流れ3



P-IP:P-Port → Y-IP:80　X-IP:X-Port → Y-IP:Y-Port　X-IP:X-Port → P-IP:80
P-IP:P-Port ← Y-IP:80　X-IP:X-Port ← Y-IP:Y-Port　X-IP:X-Port ← P-IP:80

※青字:NAPT変換
赤字:ポート番号変換

NATFBOX X

NAPT(X)テーブル

変換前		変換後	
sIP:sPort	dIP:dPort	sIP:sPort	dIP:dPort
P-IP:P-Port	Y-IP:80	X-IP:X-Port	Y-IP:80

ポート番号変換テーブル

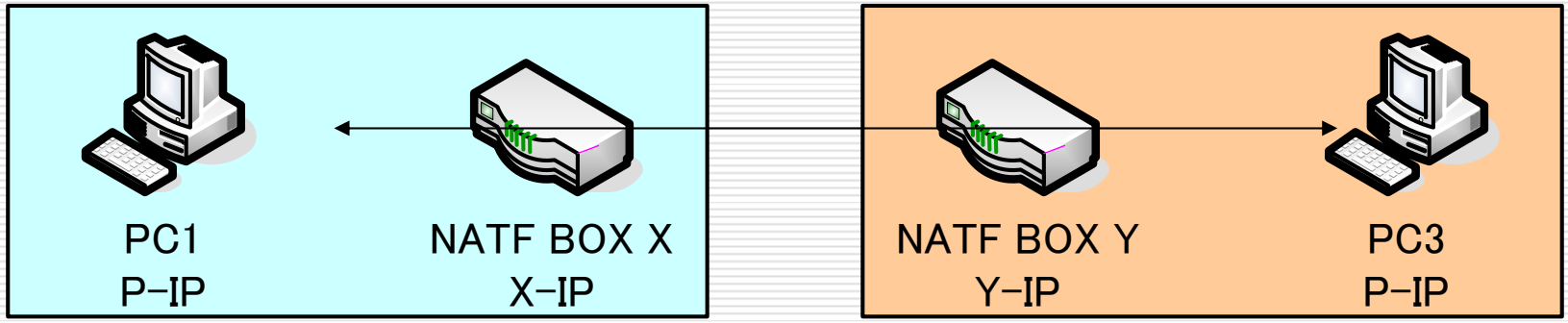
変換前		変換後	
sIP:sPort	dIP:dPort	sIP:sPort	dIP:dPort
X-IP:X-Port	Y-IP:80	X-IP:X-Port	Y-IP:Y-Port

NATFBOX Y

NAPT(Y)テーブル

変換前		変換後	
sIP:sPort	dIP:dPort	sIP:sPort	dIP:dPort
P-IP:80	X-IP:X-Port	Y-IP:Y-Port	X-IP:X-Port

CIPAの流れ3



P-IP:P-Port → Y-IP:80
P-IP:P-Port ← Y-IP:80

X-IP:X-Port → Y-IP:Y-Port
X-IP:X-Port ← Y-IP:Y-Port

X-IP:X-Port → P-IP:80
X-IP:X-Port ← P-IP:80

※青字:NAPT変換
赤字:ポート番号変換

- NATFBOX X
  - NAPT 変換とポート番号変換
- NATFBOX Y
  - NAPT 変換
- PC1はNATFBOX Y, PC3はNATFBOX X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

比較

	アドレス管理	通信中の オーバヘッド	中継サーバ	DNSの特殊性
NATS	×	×	○	×
SoftEther	×	×	×	○
CIPA	○	○	○	×

- アドレス管理
  - NATS:サブアドレス　　SoftEther:アドレス環境の統一管理
- 通信中オーバヘッド
  - NATS, SoftEthet:カプセル化
- 中継サーバ
  - SoftEther:仮想HUB
- DNS
  - NATS, CIPA:拡張レコード

まとめ

- 異なるプライベートアドレス空間端末の通信（CIPA）の提案
  - アドレス管理が不要
  - 中継サーバが不要
  - 通信中のオーバヘッドが少ない
- 今後の予定
  - 実装
  - 動作検証と性能評価

おわり