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

柳沢　信成　　渡邊　晃
名城大学大学院理工学研究科

Communication between private address terminals via a global address area

Nobushige Yanagisawa　　Akira Watanabe
Graduate School of Science and Technology，Meijo University

1.　はじめに

ユビキタス社会では，いつでも誰でもどこからでも自由に通信したいという要求が高い．しかし，現実のネットワークにおいては IP アドレス空間としてグローバルアドレス，プライベートアドレスの 2 つがあり，両者は自由に通信を行うことができない．プライベートアドレスとは組織内部のネットワークアドレスとして自由に利用できる IP アドレス空間のことであり，グローバルアドレス空間との間には NAT が設置され，多くの場合ファイアウォールも併設される．

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，今後家庭にネットワークが普及していった場合，家庭用のファイアウォールによる制約はそれ程厳しい必要はなく，NAT による通信の制約は無視できなくなると考えられる．

ＮＡＴによる通信の制約とは，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の開始ができないことである．これを解決する手段として DNS と連携してサブアドレスという新しいアドレス体系を定義する NATS[1]，端末，DNS，NAT が協調してポート番号の変換を行う NATF[2][3] などの研究がある．

本研究では，上記のような NAT 越え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だ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検討している．現時点では，このような環境下での通信方式に係わる研究はほとんどなされていない．もし実現するとすれば，プライベートアドレス空間の端末同士がグローバルアドレス空間上の HTTP サーバを介して情報を中継する方法があるが，アプリケーションが限定されるため，ユビキタス環境で適用可能な方式とは言えない．また，通信中に端末が移動することにより，結果的にグローバルアドレス環境をはさんだプライベートアドレス端末どうしの通信を可能にする研究があるが[5]，通信コネクションの維持を実現するものであり，自由な通信の開始を解決するものではない．

本稿では，NATF の考え方を拡張し，２台の NATF BOX が，通信開始に先だって DNS と連携して使用可能な空きポート番号を事前に決定し，その情報を元にデータパケットの IP アドレス，ポート番号変換を行うことで NAT による通信の制約をなくす方式を提案する．

提案方式の応用例として，インターネットを用いて第 3 者の位置情報を知ることができる位置情報取得システムを紹介する[4]．

以下，2 章に従来方式とその課題，3 章に提案方式について，4 章に実装，5 章に応用例，6 章に評価，7 章にまとめを述べる．

2.　従来の通信方式

従来，グローバルアドレス環境をはさんでプライベートアドレス環境同士の端末が通信する方法として，図 1 に示すようにグローバルアドレス空間上に中継サーバを置く方法がある．中継サーバはいわゆる WWW サーバであり，各プライベート空間の端末から中継サーバに HTTP リンクをはり，HTTP のアップロード，ダウンロードにより情報を交換することが可能である．この方法は，強固なファイアウォール，NAT が間にあっても情報交換が可能であり非常に有効な方式である．ただし，アプリケーションが HTTP に限定される，中継サーバが必要となる，中継サーバによるディレイが発生するなどの課題があり柔軟性に欠ける．

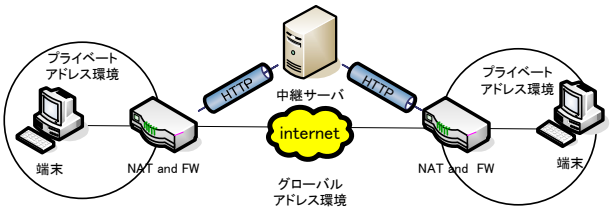


図 1　従来の通信方式

3.　提案方式

ここでは NATF で実現される NATF BOX のポート変換機能を拡張することによる通信方式を提案する．以下 3.1 で NATF について，3.2 で提案方式について説明する．

3.1　NATF（NAT Free Protocol）

図 2 に NATF の動作環境を示す．端末 A はグローバルアドレス空間，端末 B は NATF BOX 配下のプライベートアドレス空間にいる端末である．NATF BOX とは NATF 機能が追加された NAT である．DNS 機能は一般には独立して存在すべきものであるが，ここでは簡単のため DNS 機能を NATF BOX が内蔵することを前提に説明を進める．端末 A には NATF 対応機能が必要であるが，端末 B は一般端末でよい．NATF BOX に内蔵された DNS は，プライベートアドレス空間にいる端末のアドレス情報を管理している．

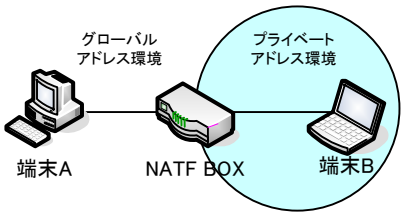


図 2　NATF の動作環境

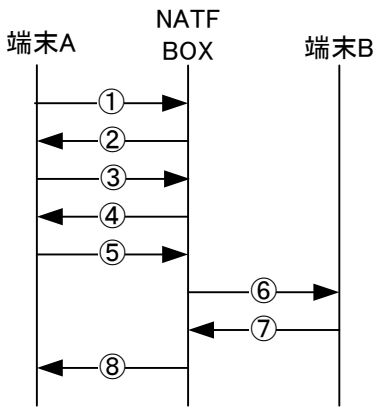


図 3　NATF の通信開始の動作

図 3 に端末 A から端末 B への通信開始時の動作の流れ，すなわちグローバルアドレス環境からプライベートアドレス環境への通信の開始手順を示す．①から④が NATF で定義されたネゴシエーションであり，⑤から⑧がデータ通信の流れである．以下の説明は，図中の番号に対応したものである．

①端末 A は NATF BOX に内蔵された DNS に対して，端末 B に関する DNS 問合せを行う．ここでは上位 DNS への問合せの動作は省略する．

②NATF BOX は端末 A にポート番号提案パケットを送付する．これは端末 A に空ポート番号を提示するパケットであり，同時に端末 A に NATF が適用されているか否かを調べるパケットである．

③端末 A に NATF が適用されていれば，提示されたポート番号の中から適当なポート番号を選択し，そのポート番号を NATF BOX に返送する．ここでポート番号 x を選択したとすると，以後端末 B との通信には端末 A 側のポート番号として x を使用しなければならない．
端末 A が NATF を適用していなかったら，②は不正なパケットとして破棄される．

④NATF BOX は端末 A に DNS 応答を返す．このとき，端末 B はプライベートアドレスなので NATF BOX のグローバルアドレスを返す．

⑤端末 A から端末 B へのデータの通信が始まる．
端末 A はパケット送信時に，送信元ポート番号をネゴシエーションで決定した送信元ポート番号 x に変換する．

⑥NATF BOX は送信元アドレスと送信元ポート番号からパケットの宛先が端末 B 宛であると判断し，宛先アドレスを B に変換して送信する．

⑦⑧以降の動作は通常の NAT と同様である．ただし，端末 A においてはポート番号の逆変換が必要である．

NATF のネゴシエーションシーケンスのうち①と④は通常 DNS シーケンスであり，②③のシーケンスが新たに追加されたシーケンスである．

このように，端末 A と NATF BOX が端末 A 側のポート番号決定のネゴシエーションをすることでグローバルアドレス環境の端末からプライベートアドレス環境の端末への通信の開始が可能となる．

3.2　提案方式

図 4 に NATF を適用した提案方式の動作環境を示す．ここで端末が所有するホスト名，IP アドレス，ポート番号は図 4 に示すとおりとする．端末 A は NATF BOX1 配下のプライベートアドレス空間，端末 B は NATF BOX2 配下のプライベートアドレス空間にいる端末である．

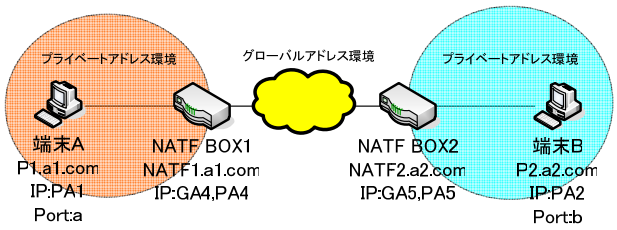


図 4　提案方式の動作環境

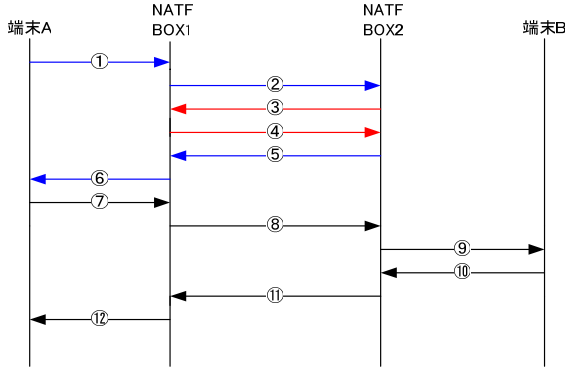


図 5　提案方式の通信開始時の動作

図 2 の場合と同様に，NATF BOX は DNS 機能を内蔵しているものとする．すなわち，NATF BOX1，NATF BOX2 はそれぞれの配下のプライベートアドレス空間にいる端末の情報を管理している．

図 5 に端末 A から端末 B への通信開始時の動作の流れを示す．①から⑥が NATF を拡張したネゴシエーションであり，⑦から⑫はデータ通信の流れである．

①端末 A は DNS を内蔵した NATF BOX1 に端末 B（P2.a2.com）に関する DNS 問合せを行う．上位 DNS への問合せの動作は省略する．

②NATF BOX1 は NATF BOX2 に端末 B に関する DNS 問合せを行う．

③NATF BOX2 は NATF BOX1 にポート提案パケットを送付する．これは NATF BOX 1 に空ポート番号を提示するパケットである．

④NATF BOX1 は提示されたポート番号の中から選択したポート番号を NATF BOX 2 にポート応答パケットとして返送する．ここでポート番号 x を選択したとすると以後端末 B との通信には端末A側のポート番号として x を使用しなければならない．

⑤NATF BOX2 は NATF BOX1 に DNS 応答を返す．このとき，端末 B はプライベートアドレス（PA2）なので NATF BOX2 のグローバルアドレス（GA5）を返す．

⑥NATF BOX1 は端末 A に DNS 応答を返す．

⑦端末 A から端末 B への実際の通信が始まる．このときの IP アドレスとポート番号は以下の通りである．
宛先アドレス：ポート　　GA5：b
送信元アドレス：ポート　　PA1：a

⑧NATF BOX1 は送信元アドレスをグローバルアドレスに，送信元ポート番号をネゴシエーションで決定した送信元ポート番号 x に変換する．
宛先アドレス：ポート　　GA5：b
送信元アドレス：ポート　　GA4：x

⑨NATF BOX 2 は送信元アドレスと送信元ポート番号から端末B宛であると判断し，宛先アドレスをBにして送信する．
宛先アドレス：ポート　　PA2：b
送信元アドレス：ポート　　GA4：x

⑩⑪⑫以降の動作は通常 NAT と同様であるため省略する．

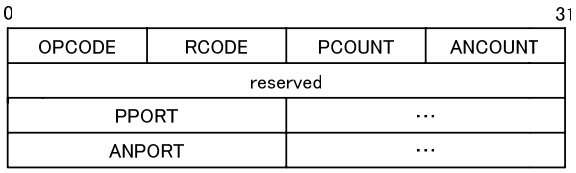


図 6　パケットフォーマット

表 1　パケットフォーマットの内容

フィールド名	bit 数	内容
OPCODE	8	Operation CODE 問合せの種類
RCODE	8	Response CODE 回答の一部でエラーなどを示す
PCOUNT	8	Proposed COUNT 提案されたポートの数
ANCOUNT	8	Answered COUNT 決定したポートの数
reserved	32	予約
PPORT	16× PCOUNT	Proposed PORT 提案されたポート番号が入る
ANPORT	16× ANCOUNT	Answered PORT 決定したポート番号が入る

NATF のネゴシエーションシーケンスのうち①②⑤⑥は通常の DNS シーケンスであり，③④が新たに追加されたシーケンスである．NATF BOX2 の動作は 3.1 で説明した NATF の動作と全く同じである．

提案方式では NATF BOX 同士がポート番号をネゴシエーションし，かつ変換するので，端末 A，B は一般の端末でかまわない．

3.3　パケットフォーマット

ポート提案パケット，ポート応答パケットのフォーマットを図 6，表 1 にパケットフォーマットの内容を示す．図中の…で示す部分は PCOUNT の数だけ同一の内容が続くことを示している．

4.　　実装

NATF モジュール構成を図 7 に示す．NATF モジュールは DNS モジュールと NAT モジュールで構成されている．表 2 に各モジュールの内容を示す．DNS モジュールは DNS 機能にポート変換提案モジュール，ポート変換応答モジュール，DNS 応答書き換えモジュール, NAT 連携モジュールを, NAT モジュールには NAT 機能に NAT テーブル書き換えモジュールを追加する．実装 OS は FreeBSD を採用し，試作システムをアプリケーションレベルで開発している．

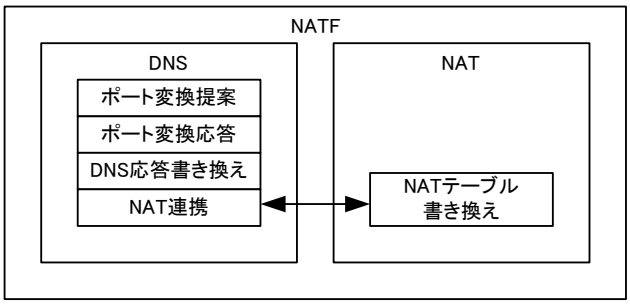


図 7　NATF のモジュール構成

表 2　追加モジュールの内容

モジュール名	説明
ポート変換提案	通信相手，またはそれが所属する NAT　BOX が NATF を適用しているかどうかを調べる. 同時に通信相手の端末の送信元ポート番号の提案を行う.
ポート変換応答	ポート提案パケットが送られてきた場合, その提案されたポート番号を選び，結果を返す.
DNS 応答書き換え	DNS 要求があった端末がプライベートアドレスであった場合，NATF BOX が持つグローバルアドレスに変換する.
NAT 連携	ポート変換提案, ポート変換応答モジュールで決定した情報を NAT モジュールに渡す.
NAT テーブル書き換え	DNS モジュールから受け取った情報より NAT テーブルを書き換える.

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を紹介する．このシステムではインターネットを用いて位置情報を別な場所から常に把握することができる．5.1 に位置情報取得システムの概要を，5.2 に提案方式と組み合わせた場合の例について述べる．

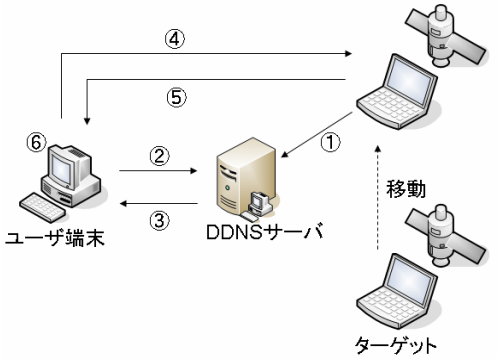


図 8　位置情報取得システムの構成

5.1　位置情報取得システム

図 8 に位置情報取得システムの構成を示す．ユーザ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している．ターゲットの位置情報の取得は GPS を想定しているが別の方式でもかまわない．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．

以下にシステムの動作を示す．図中の番号と説明の番号は同様の動作を示している．

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ユーザ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 サーバがユーザ端末へターゲットの IP アドレスを渡す．

④ユーザ端末は獲得した 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ターゲットはユーザ端末へ位置情報を返す．

⑥ユーザ端末はターゲットの位置を画面に表示する．

5.2　提案方式を適用した位置情報取得システム

位置情報取得システムの課題としてターゲットはプライベートアドレス空間に移動できない点があげられる．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グローバルアドレス空間およびプライベートアドレス空間を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（図 9）．

もしユーザ端末とターゲットの両者に NATF 機能を実装すれば，ユーザ端末，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ことになる．ただし，位置情報を扱う上でプライバシの確保は大きな課題である．ターゲットの位置情報を取得できるのは特定のユーザのみとすべきであり，更に認証技術との組合せを検討していく必要がある．

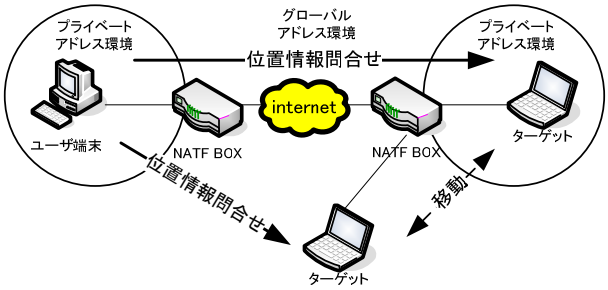


図 9　提案方式と位置情報取得システムの組み合わせ

6.　評価

表 3 に従来方式と提案方式との比較を示す．

表 3　従来方式と提案方式の比較

	従来方式	提案方式
アプリケーションの制約	HTTP のみ	制約なし
中継サーバ	必要	不要
ディレイ	大	小

従来方式ではアプリケーションが HTTP に限定されるが，提案方式ではそのような制約がない．従来方式では中継サーバが必要となるが，提案方式では不要である．また，提案方式は P2P 通信が可能であり，通信ディレイも少ない．

7.　むすび

本稿では，NATF を拡張することにより，グローバルアドレス空間をはさんだプライベートアドレス空間の端末同士の通信方式の提案を行い，更にその応用例を示した．

今後は提案方式の試作を行い，実用上での有効性を検討していく予定である．また応用例を実現しフィールドでの動作検証を行って行く．

参考文献

[1] Kuniaki Kondo : Capsulated Network Address Translation with Sub-Address(C-NATS), Internet Draft, draft-kuniaki-capsulated-nats-03.txt(December 2002)

[2] 加藤尚樹，渡邊晃：NAT を意識しない個人ネットワークを管理する Home Fire Wall の提案，情報処理学会第 66 回全国大会講演論文集 3-469 March 2004

[3] 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，情報学ワークショップ 2004 論文集 September 2004

[4] 柳沢信成，渡邊晃：DDNS を利用したターゲットの位置情報表示システム，情報処理学会第 66 回全国大会講演論文集 3-415 March 2004

[5] 清水智行，美濃導彦：NAPT を越えた端末の移動時の TCP コネクション維持による移動透過性保証プロトコル，情報処理学会研究会報告（マルチメディア通信と分散処理研究会 DPS)， vol.2002 no.032，March 2002

[6] ココセコム（http://www.855756.com/top.html）

[7] いまどこマピオン（http://imadoko.mapion.co.jp）

[8] 市村重博，二瓶克己，坂田一拓，茶園 篤，倉島顕尚：モバイルインターネット・サービス：位置情報サービスー位置情報を用いた通知サービスの発展に向けてー，情報処理学会論文誌，Vol.42，No.12，pp.1210-1215，December.2001

[9] 楯岡孝道：DNS による IP 移動透過性の実現，情報処理学会論文誌，Vol.44，No.06，pp.656-657，June.2003

[10] 渡辺恭人，竹内奏吾，寺岡文男，植原啓介，村井純：プライバシ保護を考慮した地理位置情報システム，情報処理学会論文誌，Vol.42，No.2，pp.234-242，Feb. 2001.

[11] 渡辺恭人，竹内奏吾：インターネット自動車と地理位置情報サービス，情報処理学会論文誌，Vol.43，No.04，pp.357-362，April.2002

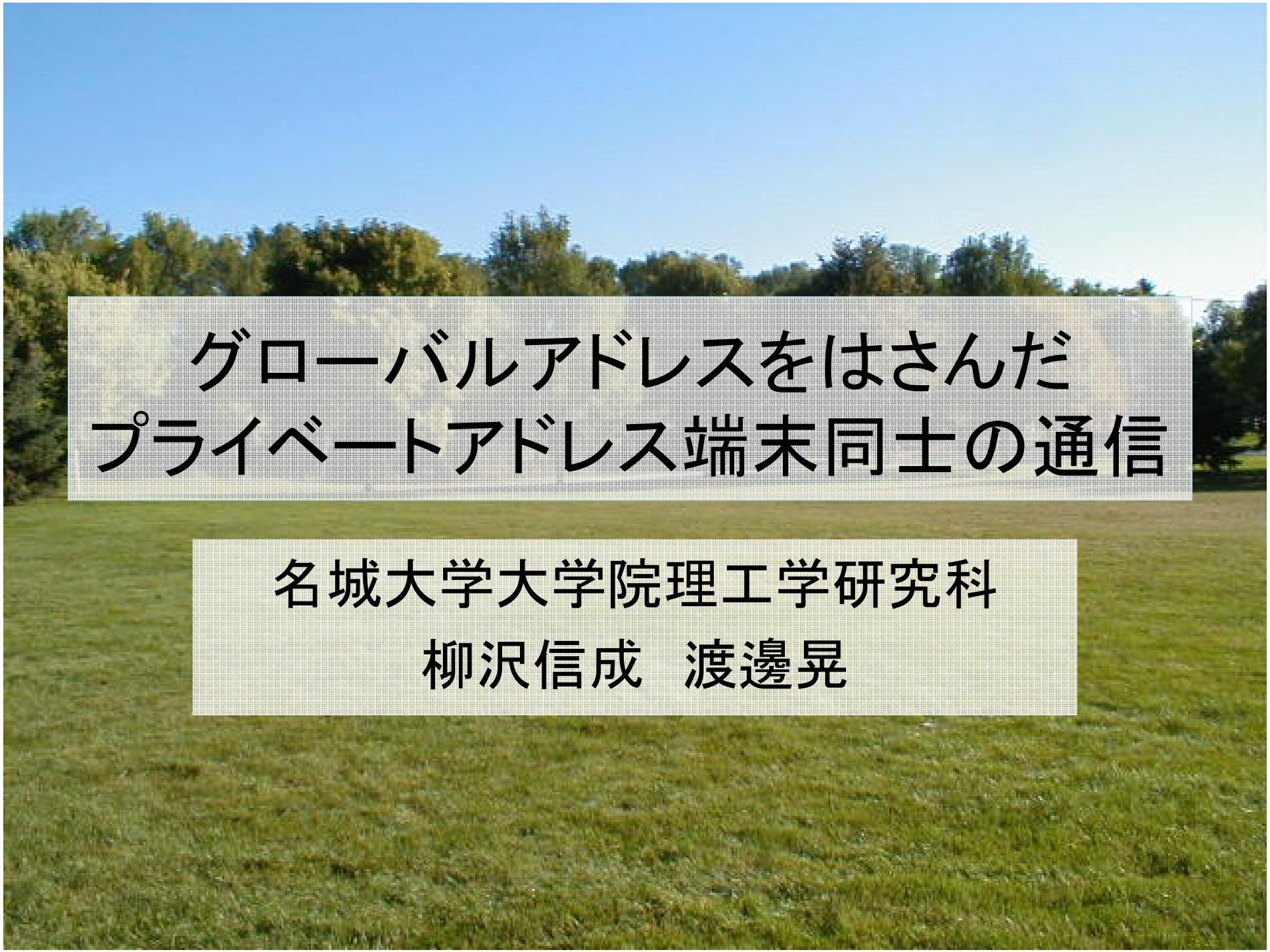
[12] 島健一：位置情報流通のプラットフォーム，情報処理学会論文誌，Vol.42，No.4，pp.362-365，April.2001

[13] 入江一成，向野誉，中川広一：地域情報 NW システム用ダイナミック DNS の開発，電子情報通信学会論文誌 B，Vol.J83-B，No.4，pp.589-596，2000 年 4 月

[14] 砂原秀樹，佐藤雅明，植原啓介，青木邦友，村井純：PCar：インターネットを利用した自動車プローブ情報システムの構築，電子情報通信学会論文誌 B，Vol.J85-B，No.4，pp.431-437， April.2002

[15] 松澤智史，山崎誠，武田正之：DHCP 環境におけるネットワーク情報更新手法，電子情報通信学会論文，Vol.J83-B No.6， pp.800-807 ，June.2000

[16] 大石晴夫，倉内政喜，桑木伸夫，長田正則，大窪政範：マルチ業務対応型作業者位置動態管理システムの開発，電子情報通信学会論文誌 D-I，Vol.J85-D-I，No.7，pp.644-652，July.2002



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

名城大学大学院理工学研究科
柳沢信成　渡邊晃

はじめに

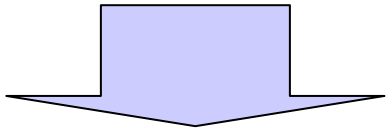
- ユビキタス社会での要求
  - いつでも誰でもどこからでも自由に通信がしたい

現実のネットワークにおいてはIPアドレス空間として、グローバルアドレス、プライベートアドレスと2つがあり、両者は自由に通信を行うことができない

グローバルアドレス空間と組織内部のプライベートアドレス空間との間にはNATが設置され、多くの場合ファイアウォールも設置される

はじめに

- 企業ネットワーク
  - セキュリティ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を制限
    →NATによる通信の制約は表に出てこない
- 家庭内ネットワーク
  - ファイアウォールによる制約は企業より厳しい必要はない
    →家庭外から家庭内へ通信は行えない



アドレス空間の違いを気にせず通信を行いたい

はじめに

- グローバルアドレス環境からプライベートアドレス環境への通信

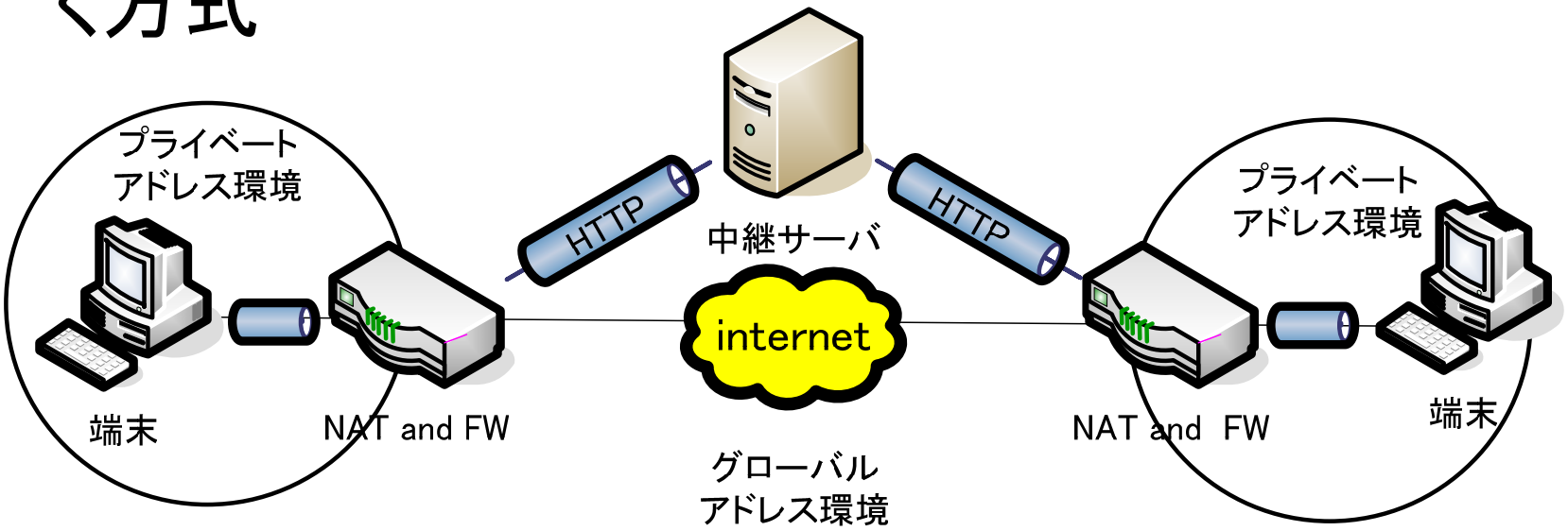
  – NATS（Network Address Translation with Sub-Address ）
    - DNSと連携してサブアドレスという新しいアドレス体系を定義する

  – NATF（ NAT Free protocol ）
    - 端末，DNS，NATが協調してポート番号の変換を行う

NATFを拡張しグローバルアドレス環境をはさんだプライベートアドレス環境端末同士の通信の提案を行う

従来の通信方式

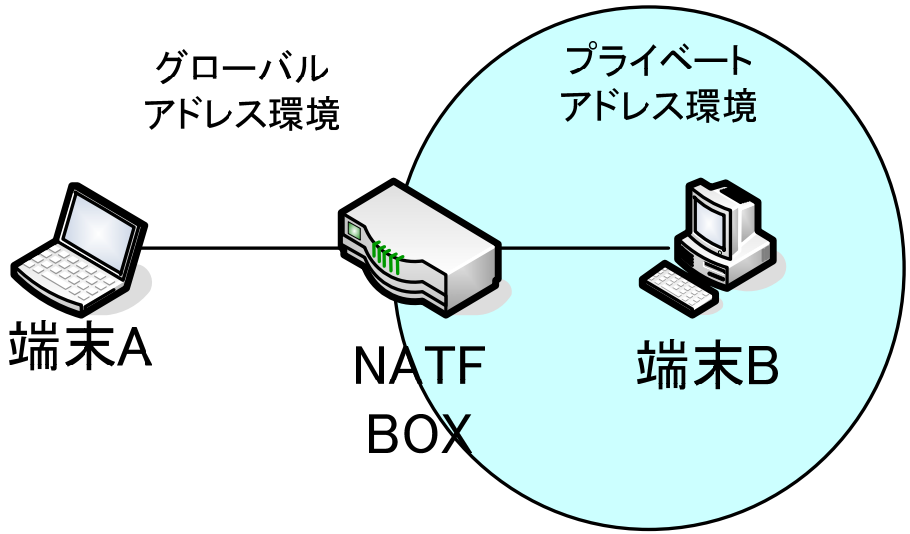
- グローバルアドレス空間上に中継サーバを置く方式



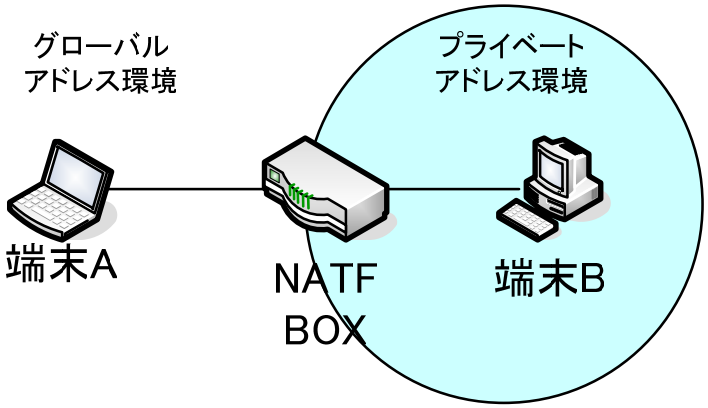
- ファイアウォールやNATが間にあっても情報交換が可能
- 特別なアプリケーションに限定
- 中継サーバが必要
- 中継サーバによるディレイ発生

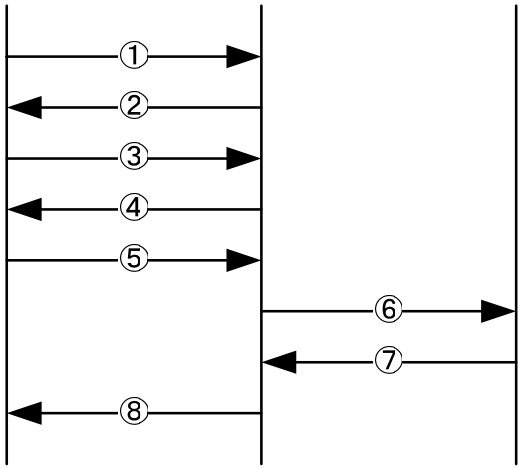
NATF（NAT Free protocol)

- 端末Aから端末Bへの通信を行う際、端末AとNATF BOXが事前に共通に空いているポート番号を決めるネゴシエーションを行い通信を行う



NATF（NAT Free protocol）





①端末Bに関するDNS問合せを行う

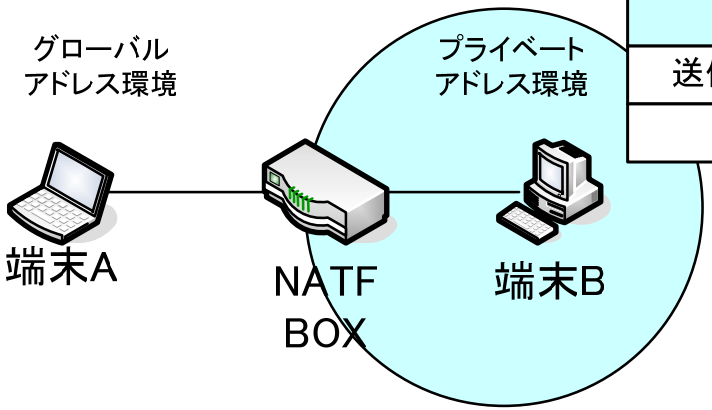
②ポート番号提案パケットを送付する

③提示されたポート番号の中から適当なポート番号を選択し，そのポート番号を返送する

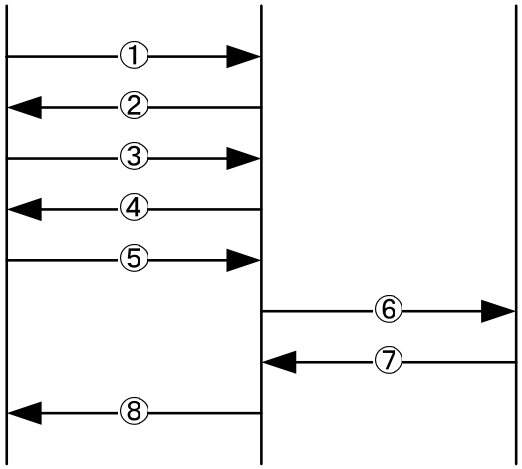
④DNS応答を返す。このとき，端末Bはプライベートアドレスなので NATF BOXのグローバルアドレスを返す

変換前		変換後	
送信元IP：Port	宛先IP	送信元IP：Port	宛先IP
端末A：a	NATFBOX	端末A：a	端末B

NATF（NAT Free protocol）



変換前		変換後	
送信元IP：Port	宛先IP	送信元IP：Port	宛先IP
端末A：a	NATFBOX	端末A：a	端末B



⑤端末Aはパケット送信時に，送信元ポート番号をネゴシエーションで決定した送信元ポート番号に変換する

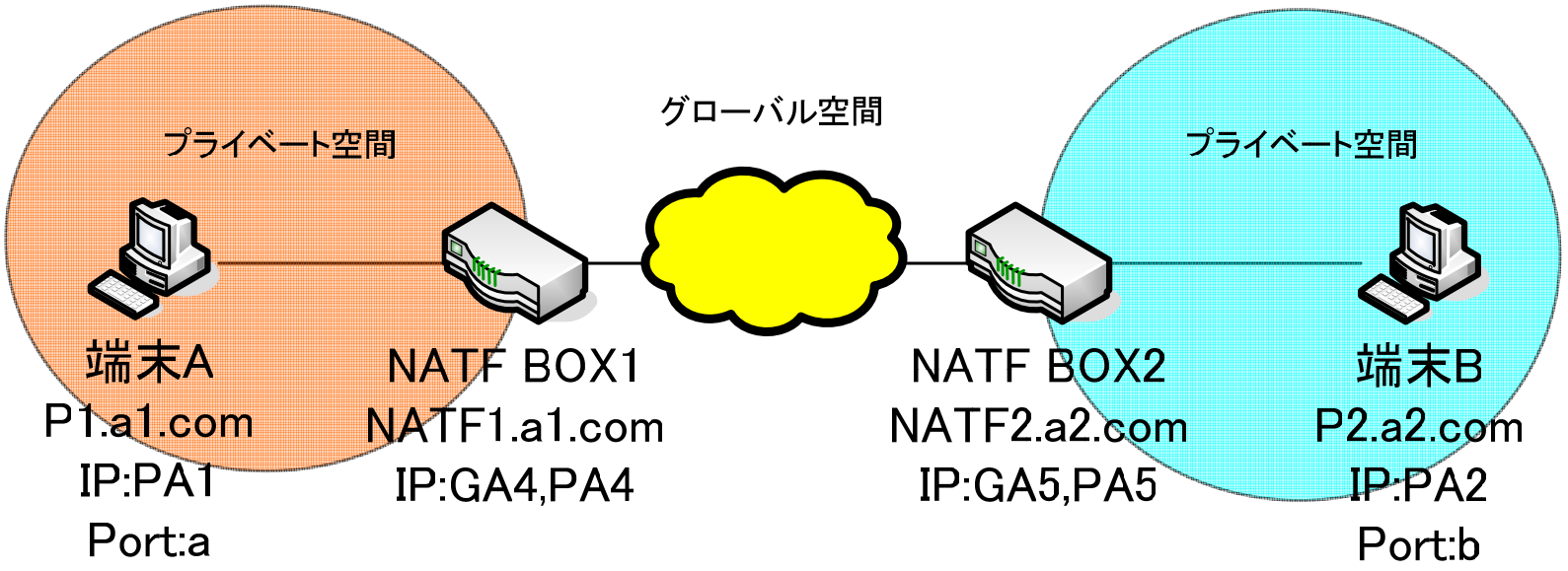
⑥NATF BOXは送信元アドレスと送信元ポート番号からパケットの宛先が端末B宛であると判断し，宛先アドレスを端末Bに変換して送信する

⑦⑧以降の動作は通常のNATと同様である

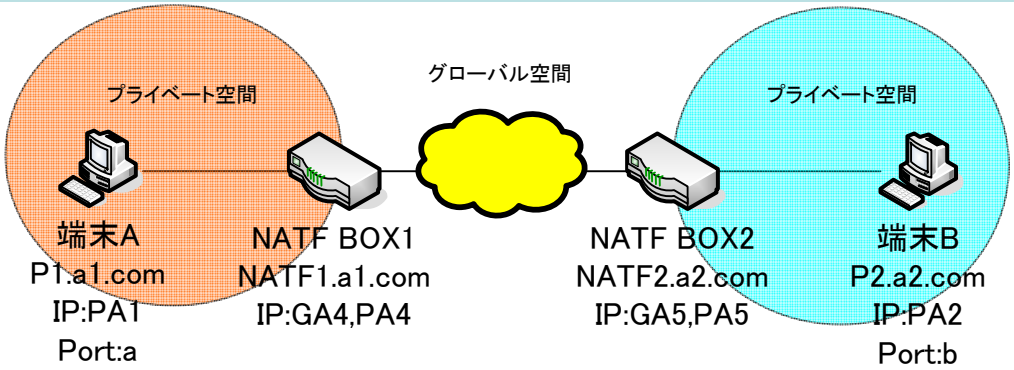
このNATFを拡張し、2台のNATF BOXを用いグローバルアドレス環境をはさんだプライベートアドレス環境端末同士の通信の提案を行う

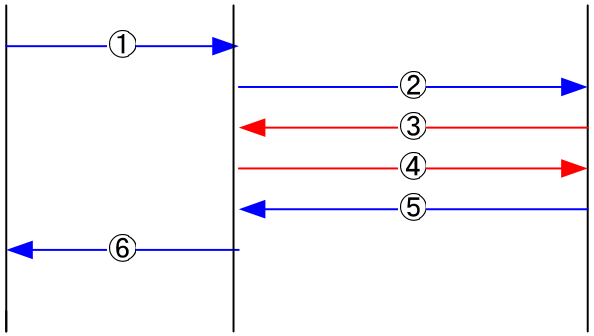
提案方式

- 端末Aから端末Bへの通信を行う際、NATF BOX同士が事前に共通に空いているポート番号を決めるネゴシエーションを行い通信を行う



提案方式





変換前		変換後	
送信元IP:Port	宛先IP	送信元IP:Port	宛先IP
PA1:a	GA5	GA4:x	GA5

NATFBOX1

変換前		変換後	
送信元IP:Port	宛先IP	送信元IP:Port	宛先IP
GA4:x	GA5	GA4:x	PA2

NATFBOX2

①②端末Bに関するDNS問合せを行う

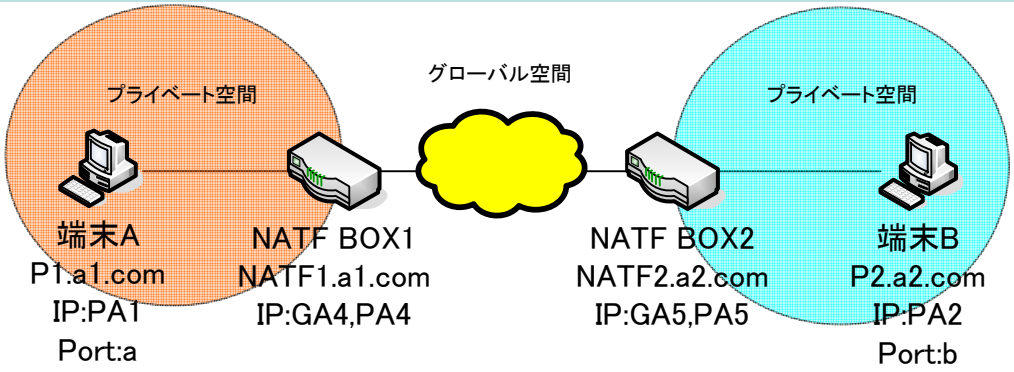
③NATF BOX2はNATF BOX1にポート提案パケットを送付する

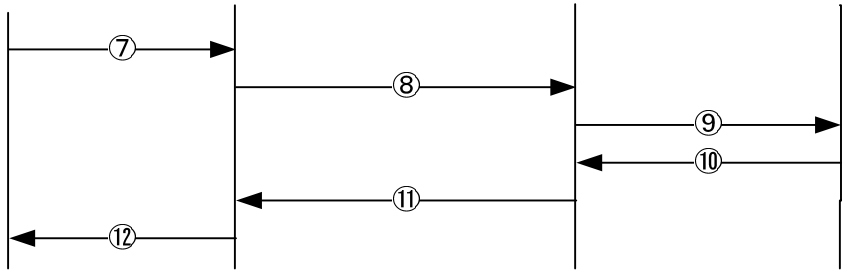
④NATF BOX1は提示されたポート番号の中から選択したポート番号をNATF BOX2にポート応答パケットとして返送する．ここでポート番号xを選択したとする

⑤NATF BOX2はNATF BOX1に DNS応答を返す．このとき，端末Bはプライベートアドレス（PA2）なのでNATF BOX2のグローバルアドレス（GA5）を返す

⑥端末Aに DNS応答を返す

提案方式





変換前		変換後	
送信元IP:Port	宛先IP	送信元IP:Port	宛先IP
PA1:a	GA5	GA4:x	GA5

NATFBOX1

変換前		変換後	
送信元IP:Port	宛先IP	送信元IP:Port	宛先IP
GA4:x	GA5	GA4:x	PA2

NATFBOX2

⑦実際の通信が始まる
宛先アドレス:ポート　GA5:b
送信元アドレス:ポート　PA1:a

⑧アドレス・ポート変換を行う
宛先アドレス:ポート　GA5:b
送信元アドレス:ポート　GA4:x

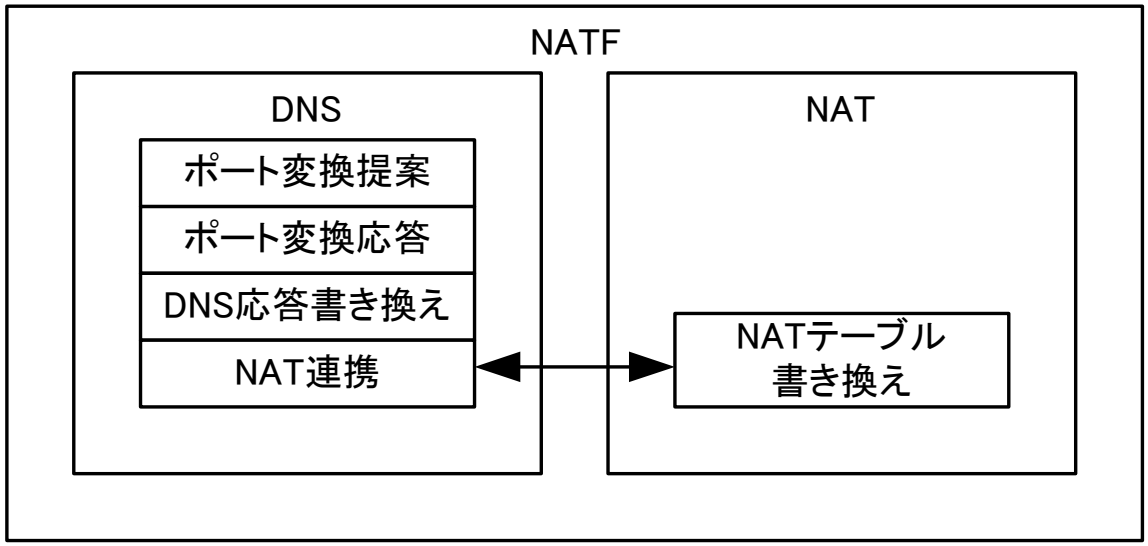
⑨テーブルより，宛先アドレスをPA2にして送信する
宛先アドレス:ポート　PA2:b
送信元アドレス:ポート　GA4:x

⑩⑪⑫以降の動作は通常NATと同様であるため省略する

・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が可能
・NATF BOX同士がポート番号をネゴシエーションし，かつ変換するので，端末A，Bは一般の端末でかまわない

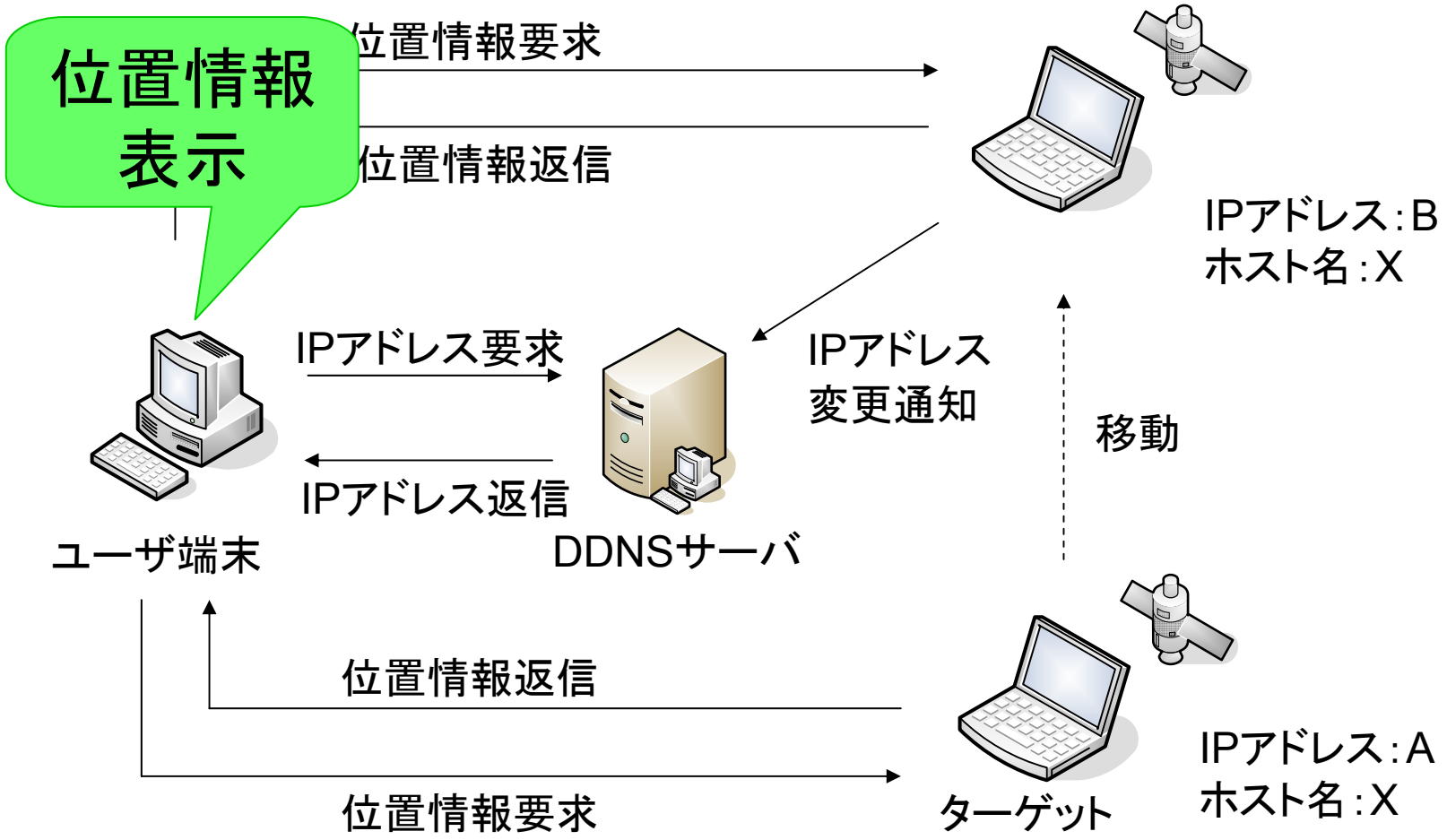
実装

- 実装OSはFreeBSDを採用し，試作システムをアプリケーションレベルで開発している
- DNSモジュールとNATモジュールで構成している

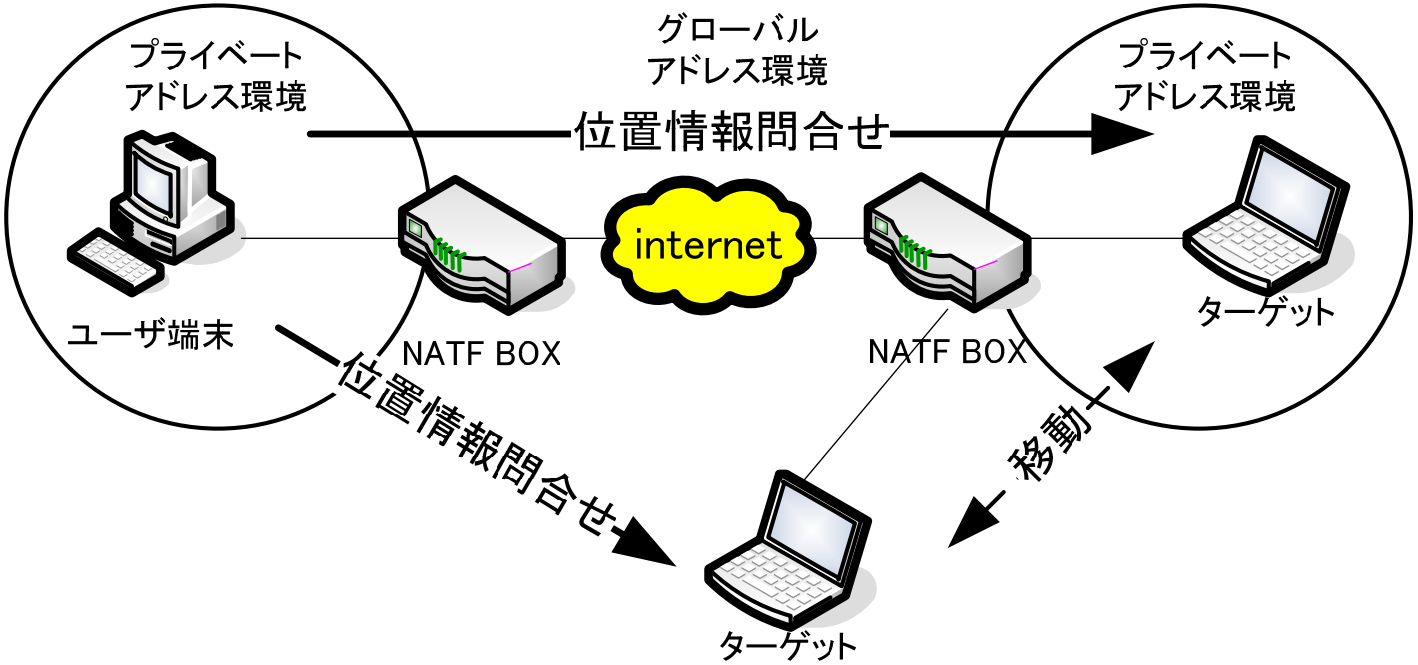


応用例-位置情報取得システム-

- インターネットを用いて位置情報を別な場所から常に把握する システム



応用例-位置情報取得システム-



- ターゲットがプライベートアドレス環境にいても検索が可能
- ユーザ端末とターゲットの両者にNATF機能を実装すれば，ユーザ端末，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

比較検討

	従来方式	提案方式
アプリケーションの制約	制約あり	制約なし
中継サーバ	必要	不要
ディレイ	大	小

・従来方式ではアプリケーションが特別なアプリケーションに限定されるが，提案方式ではそのような制約がない

・従来方式では中継サーバが必要となるが，提案方式では不要である

・提案方式はP2P通信が可能であり，通信ディレイも少ない

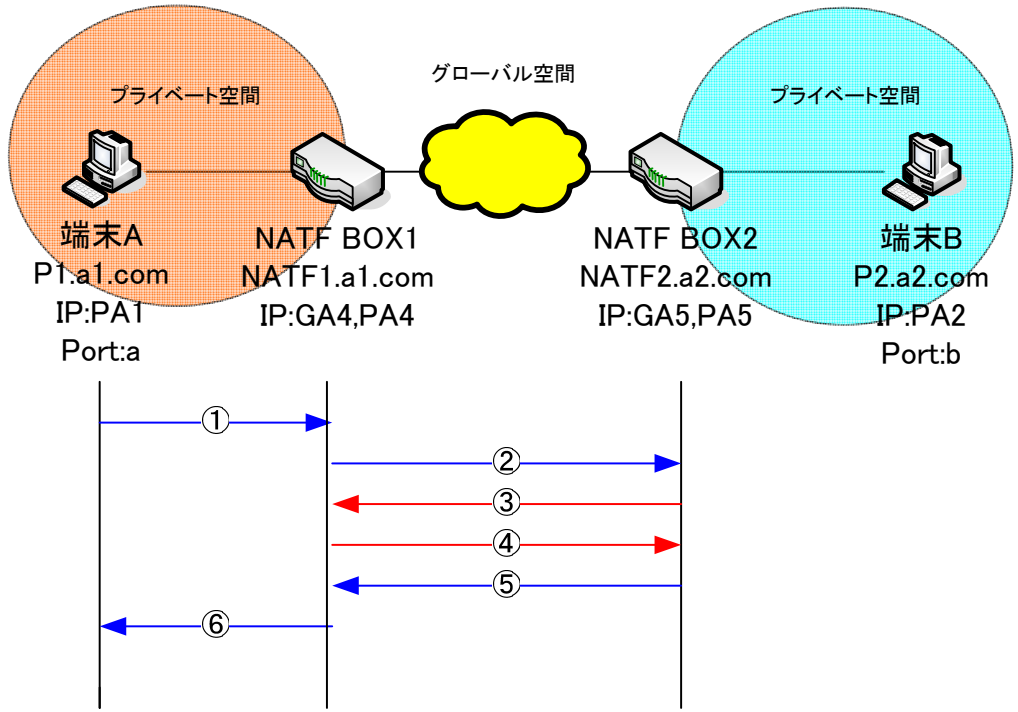
むすび

- まとめ
  - NATFを拡張することにより，グローバルアドレス空間をはさんだプライベートアドレス空間の端末同士の通信方式の提案を行った
  - 応用例（位置情報取得システム）を示した

- 今後の課題
  - 提案方式の試作を行い，実用上での有効性を検討していく
  - 応用例を実現しフィールドでの動作検証を行っていく

お わ り

NATF BOX1が通常NATであった場合



③のポート提案パケットが送られてきたら、NATでは不正なパケットと判別され破棄する

NATF BOX2には④のパケットは送られてこないので、タイムアウトとなる

⑤では通常のDNS応答のNot Foundを返す