アドレス空間の違いを意識しない通信方式 NATF の提案

加藤　尚樹　　渡邊　晃
名城大学理工学部大学院情報科学専攻

Proposal of NATF communication systems being not conscious of different address spaces

Naoki Kato　　Akira Watanabe
Graduate School of Science and Technology,　Meijo University

1.　はじめに

ユビキタス社会においてはどこにいても自由に通信できることが求められる．しかし，実際にはインターネットで用いられるグローバルアドレス空間と組織内で用いられるプライベートアドレス空間があり．両者の間にはNAT/NAPTが存在することから、通信に制約がある。NAT/NAPTは、プライベートアドレス空間に存在する端末がNAT/NATSの持つグローバルIPアドレスを利用してインターネット側の端末と通信をするためにパケットの送信元IPアドレス/ポート番号を変換する機能を持つ．しかし、アドレス変換テーブルが、プライベートアドレス空間からグローバルアドレス空間へのアクセスで始まる場合にしか生成できないため、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のアクセスで始まる通信を開始することができないという制約がある。この制約を緩和するためNAPTにはアドレス変換テーブルを静的にあらかじめ生成しておくIPフォワード機能があるが、1つのグローバルアドレスのポート番号1つに対して1台の端末しか設定できないうえ，動的に変更できないので汎用性に欠ける．

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アクセス開始を汎用的に可能にしようとする方式として，NATS(Network Address Translation with Sub-Address)[1]が提案されている.これは DNS と連携してサブアドレスと呼ばれる新しい IP アドレス体系を定義し，IP in IP Tunneling[5]を用いて NATSBOX を通過させる方式である．

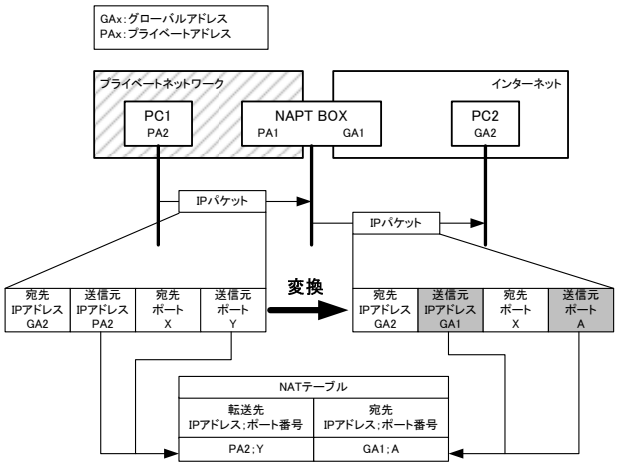


図 1　NAPT の動作
Fig1　operation of NAPT.

しかし，NATSにはパケットの冗長，DNS処理に係わる遅延などの課題がある．

本稿においてはDNS、端末、NAT/NAPTが協調してポート番号の変換を行い、NAT変換テーブルを自動生成する方式NATF（NAT Free Protocol）を提案する．NATFは既存のNAPTに若干の改造を加えることで実現可能である。

以下２章にNAPTとその課題、３章にNATSとその課題、４章にNATFの概要、５章に実装、６章に評価、７章にまとめを述べる。

2.　NAPT とその課題

NAPT は、NAPTBOX がグローバルアドレスを１つだけ保持していればよいため、グローバルアドレスが複数必要な NAT より広く用いられている。そこで、ここでは NAPT の動作概要とその課題について述べる。

図１に NAPT の動作を示す。ここでプライベートアドレス空間に属する PC1 がグローバルアドレス空間に属する PC2 へアクセスを開始するものとする。PA はプライベート IP アドレス，GA はグローバル IP アドレスを示す。はじめに PC1 は送信元 IP アドレスおよびポート番号を『PA2』,『Y』，宛先 IP アドレスおよびポート番号を『GA2』,『X』としてパケットを送信する．NAPTBOX では送信元 IP アドレスを『PA2』から『GA1』に変換し，さらに通信を判別するため送信元ポート番号を『Y』から『A』へと変換する．このとき NAPT BOX では IP アドレス『GA1』, ポート番号『A』と IP アドレス『PA2』, ポート番号『X』とを対応付けるアドレス変換テーブルを生成する．このテーブルを参照することにより逆方向のパケットも PC1 に届くようにアドレス変換を実現することが可能になる．

しかし，逆に PC2 側より通信を開始する場合は、PC1 の IP アドレスである『PA2』はインターネット上では有効でないため送信することができず、NAPT のアドレス変換テーブルを生成するタイミングがない．ゆえにグローバル空間からプライベート空間への通信開始は NAPT が介在する限りできない。ただし、NAPT に NAT テーブルを静的に生成しておくことによってグローバル空間から始まる通信を可能にする IP フォワードと呼ぶ手段がある。しかし，この方法では１つのポート番号に対して１台の端末しか設定できないことや，動的に変更することができないなど、ユビキタス社会の要求には答えることができない。

3.　NATS による解決とその課題

グローバルアドレス空間の端末からプライベートアドレス空間の端末へのアクセス開始を汎用的に可能にする方式として NATS が検討されている．図２に NATS の概要を示す。図２ではグローバルアドレス空間の端末 PC2 からプライベー

トアドレス空間の端末 PC1 へのアクセス開始を例にとって説明する。NATS ではプライベート IP アドレスとグローバル IP アドレスを組としたサブアドレス呼ばれる識別子が定義される．図 2 の例で PC1 のサブアドレスは「NATS BOX の持つグローバル IP アドレス（GA 1」｜「PC1 のプライベート IP アドレス（PA2)」という 2 つが対となったアドレスであり、DNS にはこの値が登録されている。はじめに， PC2 が PC1 の DNS 問い合わせを行うと，DNS は上記『PA2』｜『GA1』というサブアドレスを応答する．このサブアドレスを元に PC2 は IP in IP Tunneling によってカプセル化を行い，宛先 IP アドレスが『GA1』となるパケットを送信する．このパケットを受け取った NATS BOX はカプセル化を解放し，解放後の宛先 IP アドレス『PA2』にパケットを送信する．PC 1 から PC2 宛の逆方向パケットは，上記と対応する逆の動作を行う．このように NATS では常時 NATSBOX においてカプセル化／カプセル開放を行う．また，端末ごとの通信を区別するため NATS BOX では Spool Address と呼ばれる仮想の IP アドレスが用いられるため処理が複雑である．このようなことから NATSBOX の負荷が大きいという課題がある。

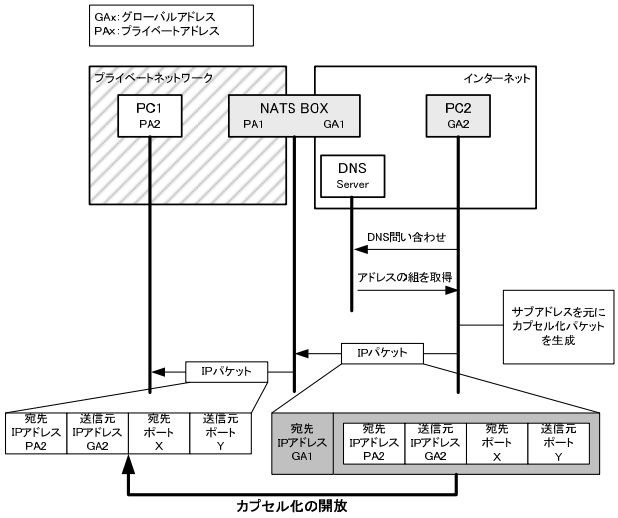


図 2　NATS の動作
Fig2　operation of NATS.

4.　提案方式

4.1.　概要

本稿では、DNS、端末、NAT が協調してポート変換を行う NATF を提案する。NATF の概要を図 3 に示す．図中の記号と意味は図 2 と同様である。DNS は、本来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 NATF BOX が DNS 機能を併せ持つものとして説明する．PC2 は通信を始めるにあたって DNS の問い合わせを行う．このとき NATF BOX は，応答すべき端末の IP アドレスがプライベート IP アドレスだった場合， PCP(Port Conversion Protocol)によって PC2 とネゴシェーションを行い，NATF と端末間で共通に使用するポート番号を決定する．そして DNS の問い合わせ内容および PC2 の IP アドレスと決定されたポート番号から NAT テーブルを生成する．DNS 応答としては NATF の持つグローバル IP アドレスを PC2 に返す．PC2 では DNS からの応答を受けて、NATF を宛先とするパケットを生成する．さらに送信元ポート番号を PCP によって決定されたポート番号になるよう変換した後，パケット

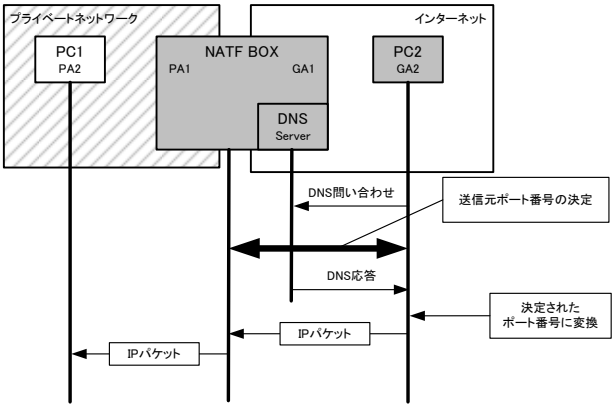


図 3　NATF の動作の概要
Fig3.　The outline of operation of NATF

を送信する．このパケットを受信した NATF BOX では、先に生成されたアドレス変換テーブルを用いてパケットの IP アドレス，ポート番号を変換し，PC1 にパケットを送信する．

4.2.　PCP シーケンス

図 4 に NATF と端末間で共通に使用するポート番号を PCP によって決定するシーケンスを示す．PCP はポート提案パケット PPR(Port PRoposal packet)とポート応答パケット PRE(Port REsponse packet)の 2 つのパケットからなる．PPR は NATF BOX が現在使用していない空きポート番号を提示するために用いられる．提示するポート番号の数は初期値によって決めることができる．図 4 の例では 3 つ提示している．PRE は PPR によって提示されたポート番号の中から端末側が使用していないポート番号を選択して応答するためのパケットである．図 4 の例では PC2 でポート番号『a』を選択した例を示している．

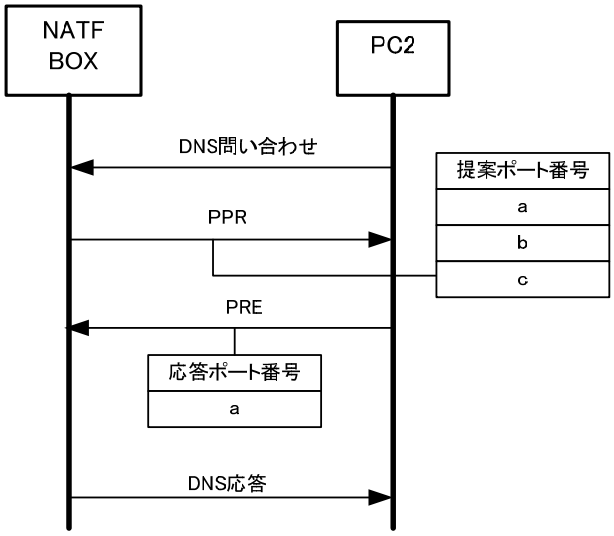


図 4　PCP のシーケンス
Fig4.　PCP sequence

4.3. PCP フォーマット

図 5 に PCP に用いられる PPR と PRE のフォーマットを、表 1 に各フィールドの内容を示す。

0 31

OPCODE	RCODE	PCOUNT	ANCOUNT
Reserved			
PPORT		・・・	
ANPORT		・・・	

図 5　パケットフォーマット

Fig5.　Packet format

表 1　各フィールドの内容

Table1.　Contents of　each field

フィールド名	概要
OPCODE(8bit)	Operation CODE パケットの種類を示す
RCODE(8bit)	Response CODE 回答の一部でエラーコードを示す
PCOUNT(8bit)	Proposed COUNT 提案したポート数
ANCOUNT(8bit)	Answered COUNT 決定したポート数
Reserved(32bit)	機能追加などのための予約
PPORT(16bit)	Proposed　PORT 実際に提案したポート番号が入り，PCOUNT の数だけ存在する
ANPORT(16bit)	Answered PORT 実際に決定したポート番号が入り，ANCOUNT の数だけ存在する

PPR ではポート番号がまだ決定していないため ANCOUNT 値は 0 であり ANPORT は存在しない．

4.4. NAT テーブルの生成

図 3 において NATF BOX では PC2 の DNS 問い合わせにより，PC2 が PC1 と通信を行おうとしていることがわかる．さらに PCP ネゴシエーションにより，この通信で用いられる共通ポート番号が『a』であることもわかる。この二つの情報より、NAT テーブルは表 3 のように決定される．これは、グローバルアドレス空間側から受信するパケットと宛先端末のプライベートアドレスを関連付けるものである。

表 2　NATF BOX で生成される NAT テーブル

Table2.　NAT table generated in NATF BOX

受信パケット		送信パケット
送信元 IP アドレス	送信元 ポート番号	宛先 IP アドレス
GA2	a	PA2

4.5. 端末側のポート番号の変換

端末側ではアプリケーションによって自動的に送信元ポート番号が決定されるため，これを PCP により決定したポート番号に変換する必要がある。この処理はアプリケーションには影響を与えないようにするため、OS の処理として変換する必要がある．また逆方向のパケットを受信した場合においてもポート番号を元の値に戻す必要がある。図 6 は図 3 における PC2 がポート変換処理を行っている様子を示したものである．PCP によって決定したポート番号は『a』としている

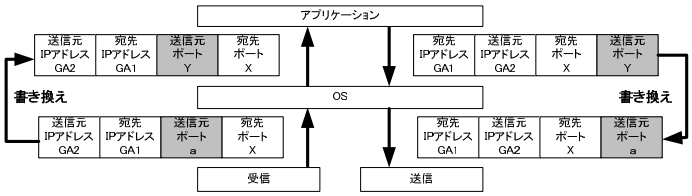


図　6　ポート番号の変換の流れ

Fig6.　The flow of　port number　conversion

5. 実装

本提案方式では NATF BOX およびインターネット側端末の両者にプログラムの実装が必要である．

5.1. NATF BOX の実装

NATF BOX にはサーバ用途として広く使われていることと、端末側の実装と開発環境を合わせるために FreeBSD を OS として採用した．また，DNS の問い合わせ内容の書き換え処理および PPR の送信処理を行わせるため DNS サーバープログラム bind を改良する．図 7 に NATF BOX の実装の概要を示す．DNS 問いあわせ時に呼び出される Send_query 関数内で NATF 関連の関数を呼び出し，PPR の送信，NAT テーブルの生成，返信 IP アドレスの書き換え処理を終えた後，通常の DNS 処理に戻る．

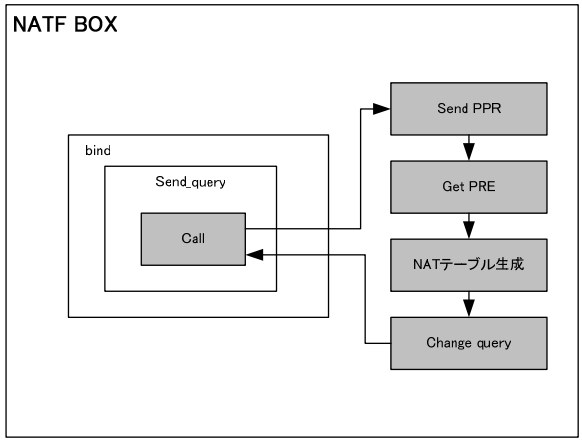


図 7　NATF BOX 実装図

Fig6.　Outline of NATF BOX implementation

5.2. 端末の実装

インターネット側端末では OS によるポート番号変換の処理が必要となる．アプリケーションが意識せずに変換を行うためには IP 層に実装を行う必要がある．よって IP 層での処理の情報の多い FreeBSD を採用した。図８に端末側の実装の概要を示す．パケットの送信時には IP 層からデータリンク層にパケットを渡す『ip_output』関数内でポート変換モジュールを呼び出し，送信元ポート番号の書き換えを行う．また，パケット受信時にはデータリンク層からデータを受信する『ip_input』関数内でポート変換モジュールを呼び出し，宛先ポート番号の書き換えを行う．この方式により IP 層より上位層ではポート番号変換の処理を意識する必要がない．

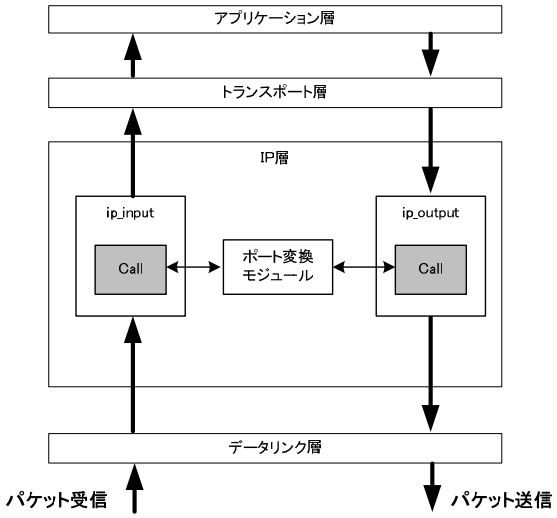


図８　端末実装図
Fig7. Outline of terminal implementation

6. 評価

NATS と NATF の比較を表 4 に示す。

表 4　NATS と NATF の比較
Table4. Comparison of NATS and NATF

	NATS	NATF
DNS レコードの特殊性	×	○
DNS の負荷	△	△
通信中の負荷	×	○

NATS ではカプセル化を行うために宛先の IP アドレスとグローバル IP アドレスの組を新しい DNS レコードとして定義しており DNS レコードが特殊である．一方，NATF ではポート番号の管理を通常の NAT テーブルに追加するだけであるため DNS レコードに特殊性はない．

NATS ではプライベートアドレス端末からグローバルアドレス端末へ通信を開始する際に NATS BOX が DNS フッキングを行うため NATS BOX に負荷がかかるが、NATF ではそのような問題はない。また，NATS では DNS フッキングをするためにすべての DNS シーケンスを監視していなくてはならないのに対して，提案方式では通常の DNS シーケンスの中で必要なときだけポート番号決定シーケンスが走る。

NATS はすべてのパケットに対して、グローバルアドレス端末側でのカプセル化、NATS BOX 側でのカプセル化の開放が常時必要であり負荷がかかる．NATF では，インターネット端末でポート変換処理を行っているものの NATF BOX 側では通常の NAPT 処理のみである．

7. むすび

本稿では DNS、NAT、端末が協調して通信開始時にポート番号を決定し、端末でポート番号変換を行うことでインターネット端末からプライベートネットワーク端末への通信開始を可能とする通信方式を提案し，その動作について示した．この方式によれば既存の NAPT に改良を加えるだけでインターネット側から通信を開始することを可能としている．今後は試作を進め，その有効性を確認する予定である．

参考文献

[1] Kuniaki KONDO，Capsulated Network Address Translation with Sub-Address(C-NATS) http://www.nats-project.org/docs/draft-kuniaki-capsulated-nats-03.txt

[2] Kuniaki KONDO，Capsulated NATS Protocol Overview http://www.nats-project.org/presentations/Capsulated-NATS-Overview.pdf

[3] Kuniaki KONDO，NATS Address Translation Practice http://www.nats-project.org/presentations/Capsulated-NATS-Overview.pdf

[4] Kuniaki KONDO，　NATS の適用範囲とプロトコルの概要 http://www.nats-project.org/presentations/NATS-exp-Generic.pdf

[5] W. Simpson, IP in IP Tunneling http://www.ietf.org/rfc/rfc1853.txt

[6] Keith Moore, Things that NATs break http://www.cs.utk.edu/~moore/what-nats-break.html

[7] 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.

[8] Flexible Private Network，Watanabe lab. Division of Information Sciences ，　Meijo University ，http://www-is.meijo-u.ac.jp/~watanabe/research/fpn1.html

アドレス空間の違いを意識しない通信方式NATFの提案

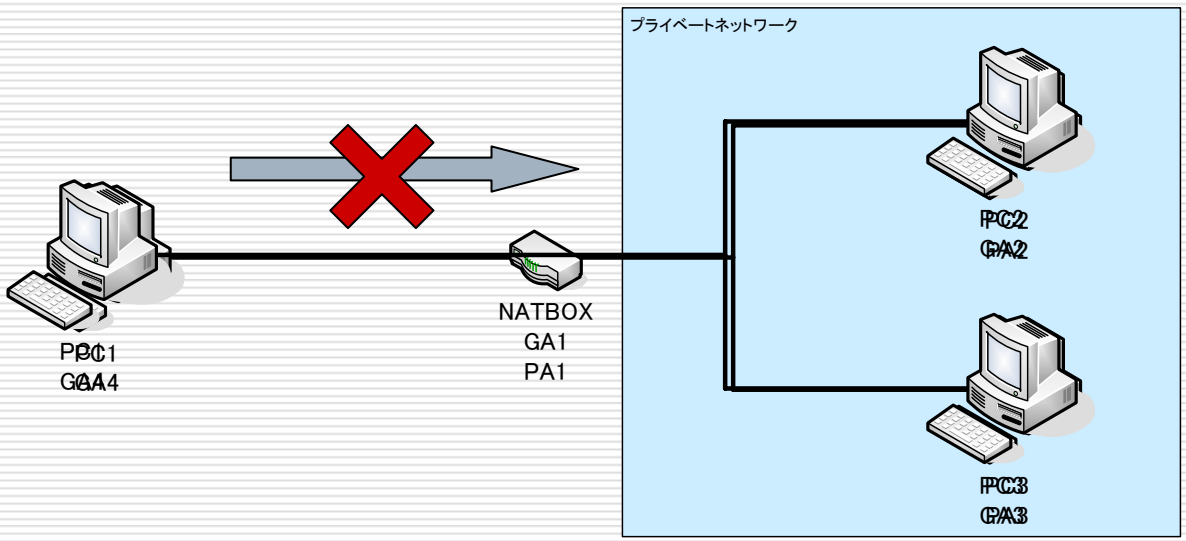
名城大学大学院理工学研究科
加藤　尚樹　　渡邊　晃

研究背景

- IPアドレスの不足からNAT/NAPTの利用が必須

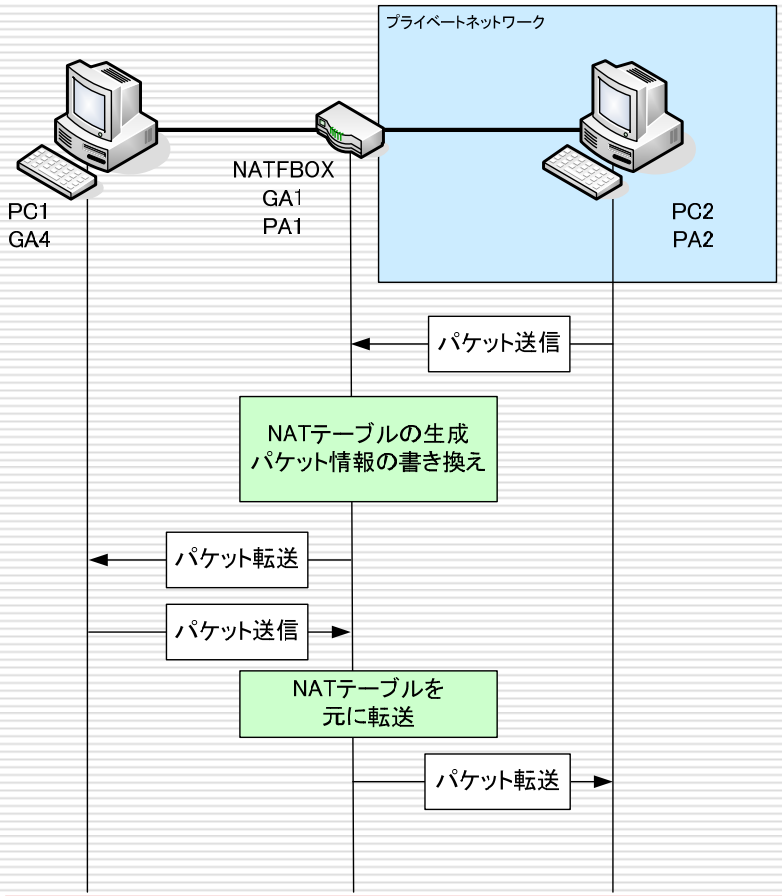
NAT/NAPTによる通信の弊害

家庭においてはプライベートIPアドレスの端末にもアクセスしたいという要求



NATの動作

- PC2がPC1のWWWにアクセスする場合



パケット情報
送信元IPアドレス：PA2
送信元ポート番号：a
宛先IPアドレス：GA4
宛先ポート番号：80

パケット情報
送信元IPアドレス：GA1
送信元ポート番号：b
宛先IPアドレス：GA4
宛先ポート番号：80

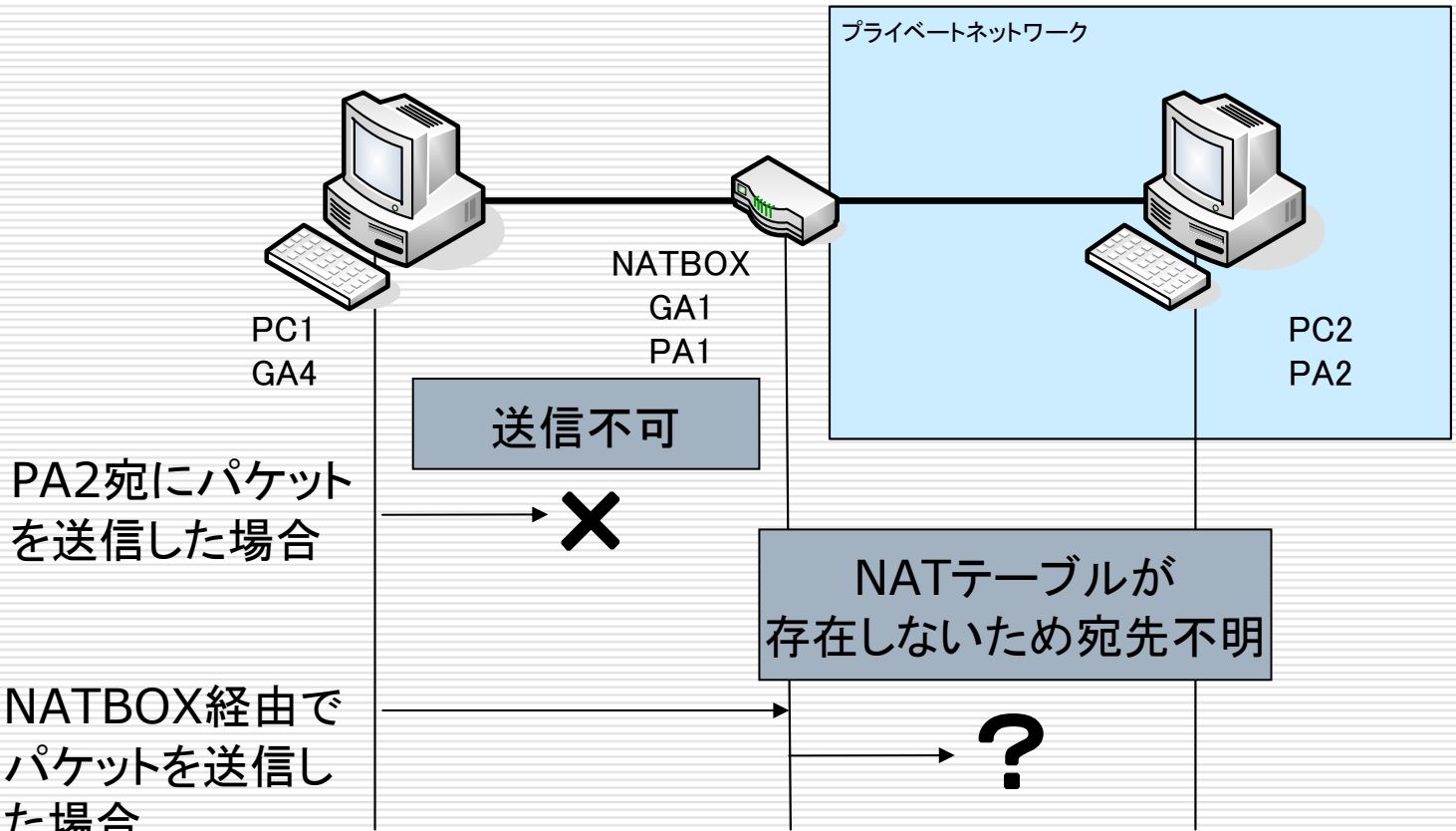
NATテーブル
受信パケットIPアドレス：GA4
受信パケット宛先ポート番号：b
転送先IPアドレス：PA2
転送先ポート番号：a

パケット情報
送信元IPアドレス：GA4
送信元ポート番号：80
宛先IPアドレス：GA1
宛先ポート番号：b

パケット情報
送信元IPアドレス：GA4
送信元ポート番号：80
宛先IPアドレス：PA2
宛先ポート番号：a

NAT/NAPTによる通信弊害

- インターネット側端末から通信を開始することが出来ない
  - プライベートIPアドレス宛にインターネットからパケットを送信できない
  - 通信端末が認識できない

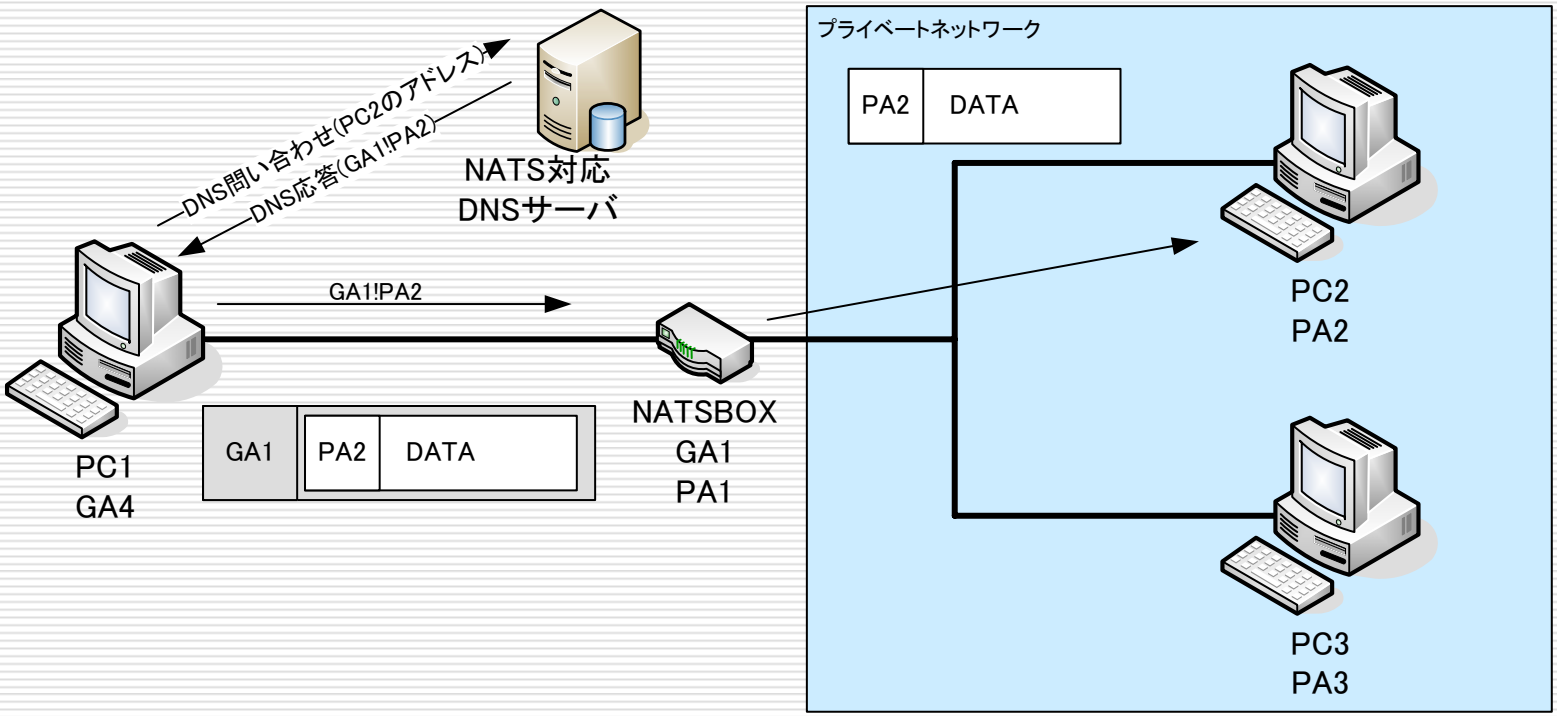


既存技術による解決

- NATS(Network Address Translation with Sub-Address)
  - DNS上でサブアドレスの利用
    - インターネット上からプライベートネットワーク側端末の識別が可能
  - IP in IPカプセリングの利用
    - インターネットではNATSBOXのIPアドレスを利用
      - インターネットで利用できるIPアドレスに変換
    - プライベートネットワークでは各個のIPアドレスを利用
- 前提条件
  - インターネット側端末およびNATSBOXに改良
  - プライベートネットワーク側端末は通常の端末

NATSの通信の流れ

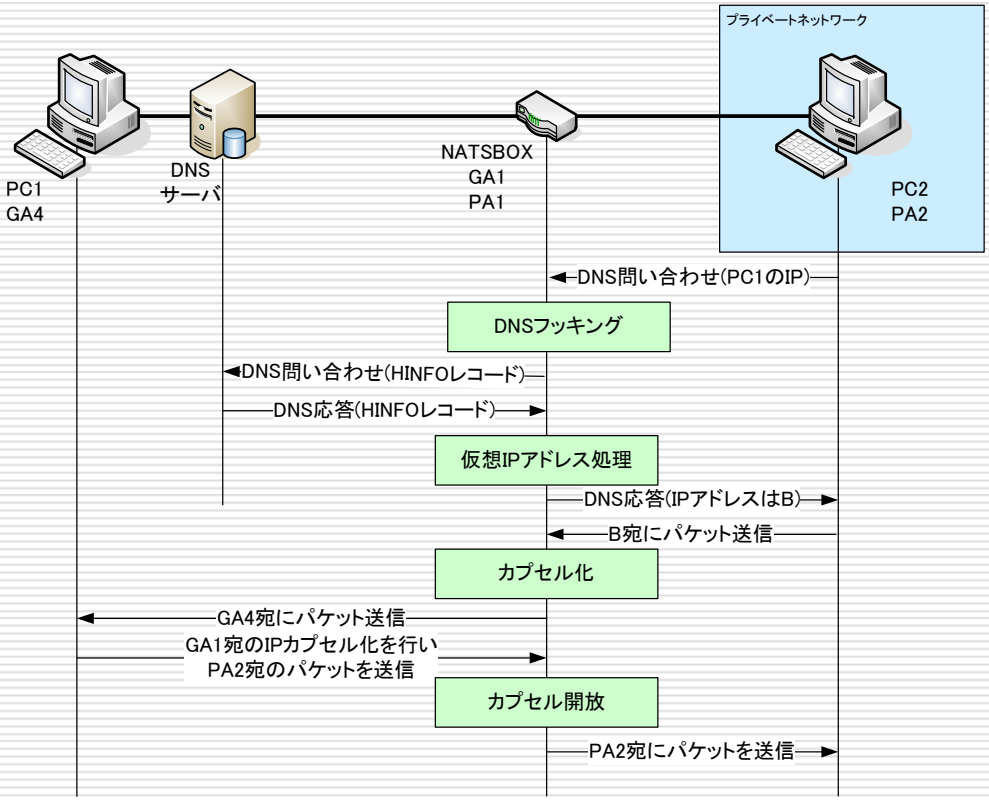
- インターネット側端末から通信を開始する場合



カプセル化によるパケットの冗長
サブアドレスの利用によるDNSレコードの特殊性

NATSの通信の流れ2

- プライベートネットワーク側から通信を開始する場合



仮想IPアドレス

NATSBOX内のみで有効なIPアドレスで通信の判別に用いる

NATSテーブル
受信パケットIP:B
送信元アドレス:GA1！PA2

仮想IPアドレスの使用とカプセル化の代行による
NATSBOXへの高負荷

提案方式による解決

- NATF(Network Address Translation Free protocol)
  DNSサーバ,NAT,端末が協調することでパケットを
  プライベートネットワーク上の端末に送信可能とする
  - **DNSでは**
    - プライベートIPアドレスを問い合わせを受けたときNATのIP
      アドレスに問い合わせ内容を変換

プライベートIPアドレスを持つ端末宛のパケットを
NATFBOXが受信することが出来る

  - **NATでは**
    - 端末とのネゴシエーションによる送信元ポート番号の決定

NATテーブルを生成し，パケットの転送を可能とする

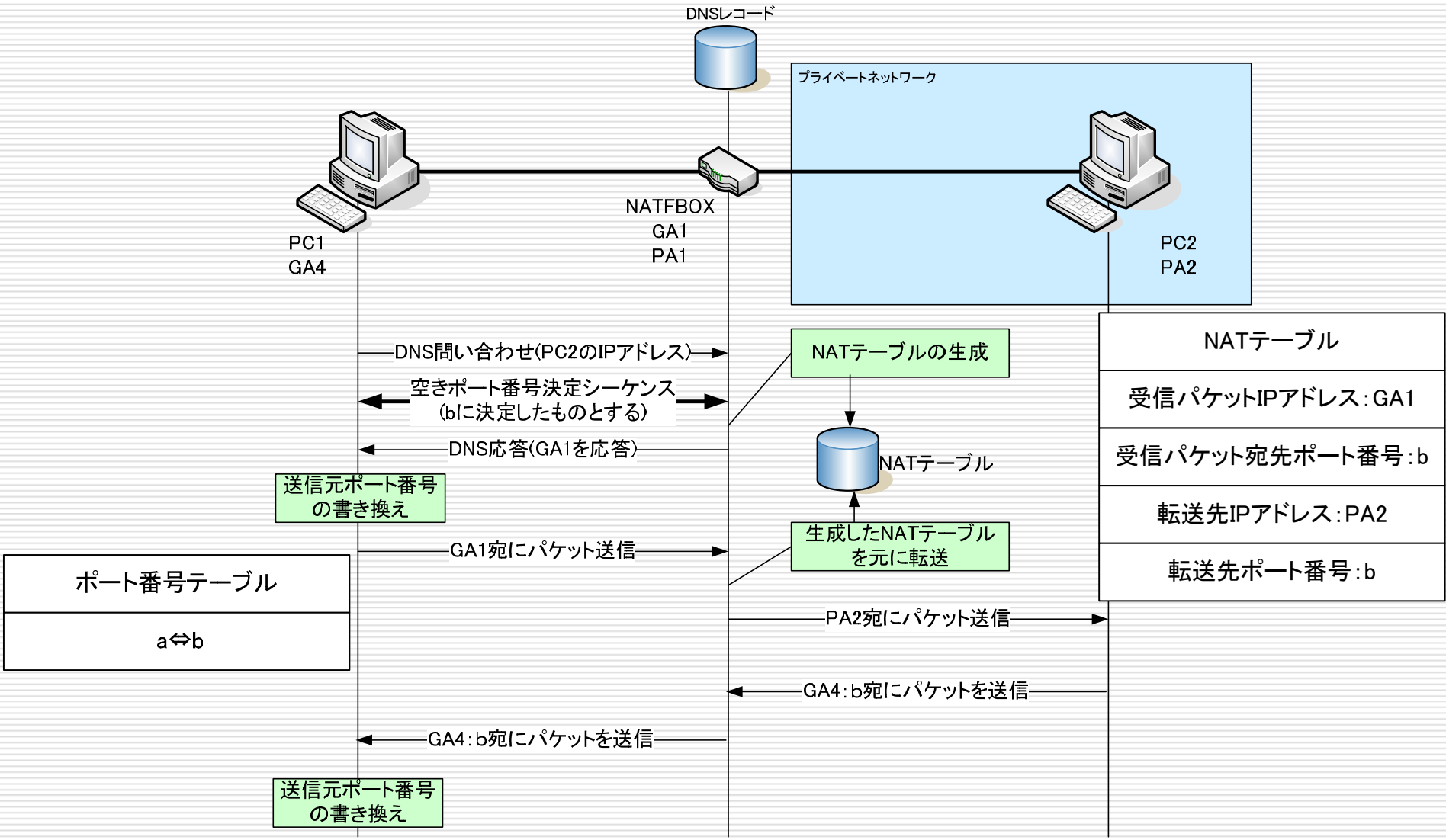
  - **端末では**
    - NATとのネゴシエーションによる送信元ポート番号の決定

NATテーブルで転送可能なパケットの生成が可能

前提条件

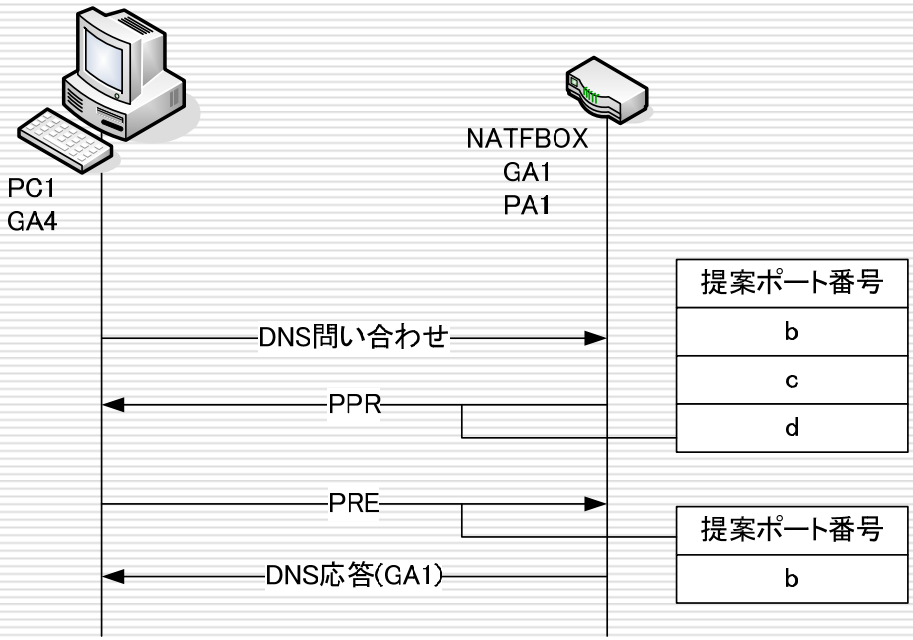
- DNSサーバ機能をNATFBOXが所有
  - 説明の簡略化，実装の簡略化のため
- NATFBOXおよびインターネット側端末を改良
- プライベートネットワーク側端末は通常の端末

提案方式の通信の流れ


DNSレコード
プライベートネットワーク
PC1
GA4
NATFBOX
GA1
PA1
PC2
PA2
DNS問い合わせ(PC2のIPアドレス)
NATテーブルの生成
空きポート番号決定シーケンス
(bに決定したものとする)
DNS応答(GA1を応答)
NATテーブル
送信元ポート番号
の書き換え
GA1宛にパケット送信
生成したNATテーブル
を元に転送
ポート番号テーブル
a⇔b
PA2宛にパケット送信
GA4:b宛にパケットを送信
GA4:b宛にパケットを送信
送信元ポート番号
の書き換え
NATテーブル
受信パケットIPアドレス:GA1
受信パケット宛先ポート番号:b
転送先IPアドレス:PA2
転送先ポート番号:b

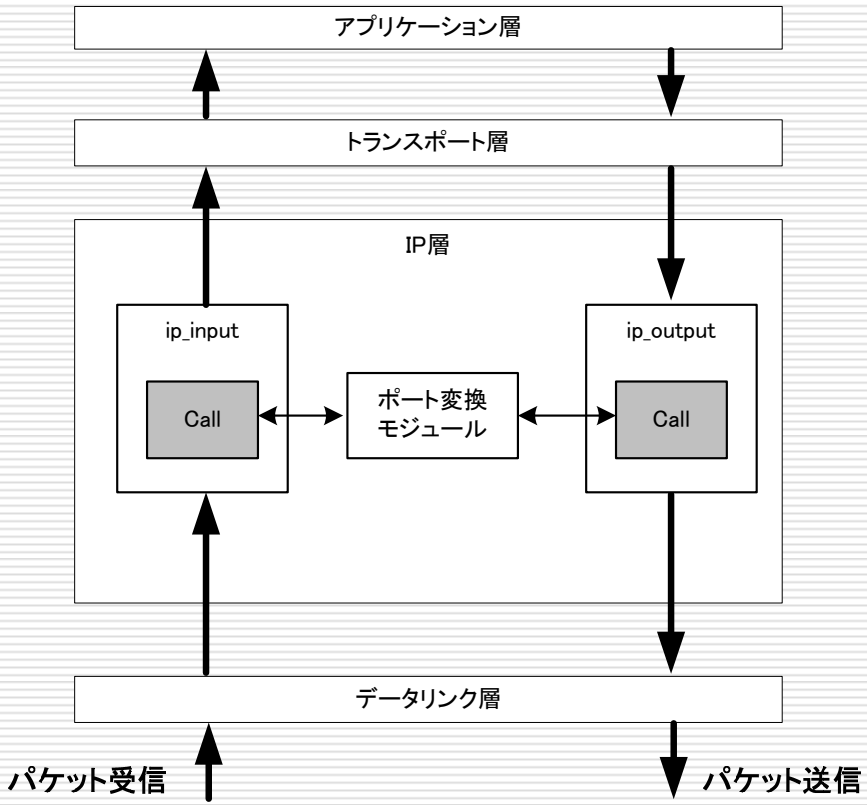
空きポート番号決定シーケンス

- 通信を区別するために空きポート番号を決定
  - NATFはランダムに未使用ポートを選び，DNS問い合わせ受付時にPPR(Port PRoposal packet)を送信
  - PPRの応答としてPRE(Port REsponse packet)を端末は送信
  - PPRに未使用ポートが存在しない場合はエラーを返し決定するまで繰り返す
  - ポート番号決定後にDNS応答をNATFBOXのグローバルIPで返す



実装について

- 現在端末側のポート変換処理を検討
  - ポート変換処理はOS側で行う
  - アプリケーションに意識させないようIP層に実装を予定
- OSはFreeBSDを利用
  - カーネルのソースコードが公開されている
  - ネットワーク研究で利用されており資料が多い



評価

	NATS	NATF
DNSレコードの特殊性	×	○
DNSに対する負荷	×	×
通信中の負荷	×	○
実装方法	○	×

- DNSレコードの特殊性
  - NATSはレコードの追加を行っている
- DNSに対する負荷
  - 双方ともにシーケンスの変更を行っているため負荷がかかる
- 通信中の負荷
  - NATSでは常時カプセル化・カプセル開放処理を行っているため負荷がかかる
  - NATFでは通信開始時に負荷はかかるが，その後の通信では通常のNATと同程度である

むすび

- DNS、NAT、端末が協調することで送信元ポート番号を決定しNATテーブルを生成する方式を提案
  - インターネット側端末からプライベートネットワーク側端末へのアクセスが可能
  - 今後は試作を進め，その有効性を確認する