

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

加藤 尚樹 柳沢 信成 鈴木 秀和 渡邊 晃

あらまし： インターネットの普及に伴い、家庭内でプライベートなネットワークを構築し、複数の端末でインターネットを接続するのが一般となりつつある。しかし、プライベートネットワークとインターネットの間にはアドレス変換装置が介在し、自由な通信をすることができない。本稿では、DNS, 端末、アドレス変換装置が連携し、課題を解決するNATF(NAT Free protocol)について提案し、その実装方法について述べる。

Proposal and implementation of NAT Free Protocol.

Naoki KATO Nobushige YANAGISAWA
Hidekazu SUZUKI Akira WATANABE

Abstract: It is not easy to communicate between a private address terminal and a global address terminal, because a Network Address Translator can not make its address translation table when the communication begins from the terminal in the global address area. In this paper, we propose a new protocol called NATF (NAT Free) to solve the problem. Implementation method of NATF is also described.

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、IPv4の世界で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/NAPT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へ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[1]があるが、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。

従来、企業ネットワークにおいてはNAT/NAPTと共にファイアウォールが併設され、内側からの通信開始のみを許可するのが一般的であった。そのため、NAPTの課題は表に出ることはなかった。しかし、今後家庭にネットワークが導入されていくと、企業のようなセキュリティポリシーは必要とならない、外出先から家庭内のネットワーク端末に自由にアクセスしたいというニーズが、十分に考えられ、NAT/NAPTの制約を除去することは有益である。

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)[2-4]が提案されている。これは

名城大学大学院理工学研究科
Graduate School of Science and Technology,
Meijo University

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、ポート変換の代わりに IP in IP Tunneling[5]を用いて NATS BOX を通過させる方式である。しかし、全パケットにカプセル化／カプセル解放処理を行うため、NATS BOX に高い負荷がかかることや、プライベートアドレス空間からの DNS 問い合わせを NATS BOX が監視し、パケットのフッキング処理を行う必要がある。

本稿では、DNS、端末、NAPT が協調することで NAPT テーブルを自動的に生成し、端末側がポート番号の変換を行うことで NAPT の制約を解決する方式 NATF (NAT Free Protocol) [6-9]を提案する。NATF は既存の NAPT BOX 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 1 つのグローバル IP アドレスで複数のプライベートアドレス空間に属する端末を同時にグローバルアドレス空間に接続できるため、同時接続台数分だけグローバル IP アドレスを必要とする NAT よりも広く用いられている。以下に、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。ここではプライベートアドレス空間に属する端末 P がグローバルアドレス空間に属する端末 G へ通信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、端末 P は送信元 IP アドレスおよびポート番号を『PA1』、『X』、宛先 IP アドレスおよびポート番号を『GA1』、『80』としてパケットを送信する(①)。NAPT BOX では送信元 IP アドレスを『PA1』から NAPT のグローバル IP アドレス『GA2』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『X』から『Y』へと変換して転送する(②)。このとき NAPT BOX では IP アドレス『GA1』、ポート番号『Y』と IP アドレス『PA1』、ポ

ート番号『X』とを対応付ける NAPT 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応答パケットも端末 P 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(③、④)。

しかし、逆に端末 G より通信を開始する場合は、端末 P の IP アドレスである『PA1』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。また、NAPT BOX へ直接にパケットを送信しても、アドレス変換テーブルがないためパケットは破棄される(⑤)。ゆえに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開始は NAPT が介在する限りできない。ただし、NAPT 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。

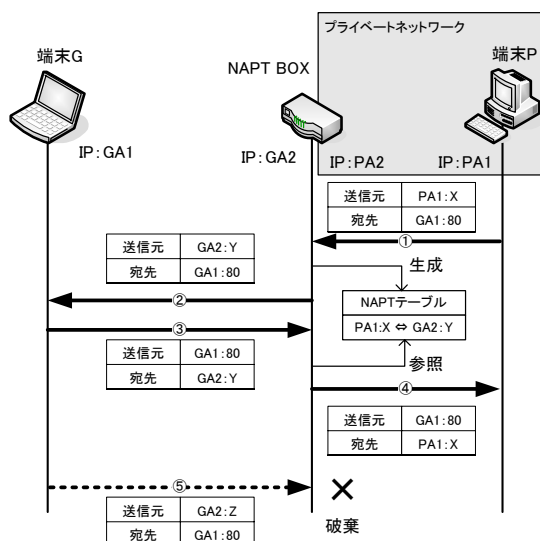


図 1 NAPT の動作

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 G からプライベートアドレス空間の端末 P 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と呼ばれる識別子が定義される。図 2 の例で端末 P のサブアドレスは『NATS BOX のグローバル IP アドレス (GA2)』 | 『端末 P のプライベート IP アドレス (PA1)』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、端末 G が端末 P の DNS 問い合わせを行うと、DNS は上記『GA2』 | 『PA1』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端末 G 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『GA2』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『PA1』にパケットを送信する。端末 P からの応答パケットは、上記と対応する逆の動作を行う。NATS において端末 P から通信を開始する場合の処理を図 3 に示す。端末 P は通常端末を想定しており、サブアドレスが扱えない。よって、NATS BOX にて DNS 問い合わせを常時監視しており、問い合わせがあったときに NATS BOX がパケットをフックキング(横取り)し、サブアドレスの解決を行う。

このように、プライベートアドレス空間からのパケットを常時 NATS BOX においてカプセル化／カプセル開放を行うため NATS BOX にかかる負荷が高い。さらに、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 IP アドレスが用いられるため処理が複雑になる。

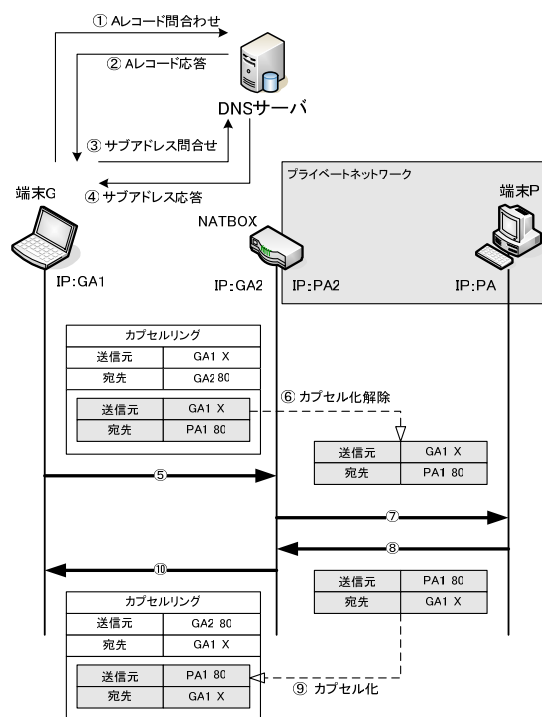


図 3 NATS の動作

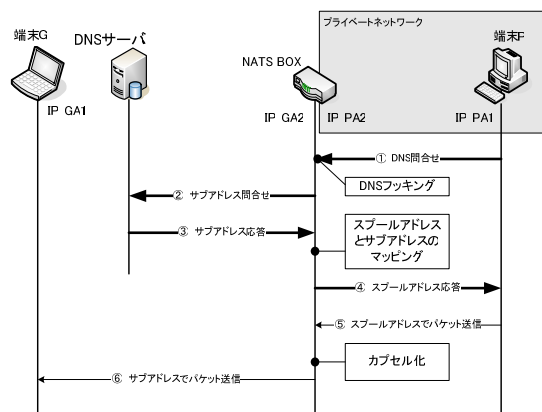


図 2 NATS におけるプライベートアドレス空間からの通信

4. NATF

本稿では DNS サーバ，端末，NAPT BOX が協調して NAPT テーブルを生成し，端末側でポート変換を行う NATF を提案する．NATF の環境を図 2 に示す．端末の位置関係，記号は図 1,図 2 と同様である．また，NATF が適用された NAPT BOX を NATF BOX と呼ぶ．

4.1. DNS 問い合わせ

NATF では，DNS にあらかじめドメイン内に存在する端末のプライベート IP アドレスを，LIP(Local IP address)と呼ぶ拡張レコードとして登録しておく必要がある．図 5 に NATF における DNS 処理の流れを示す．DNS は，端末から端末 P に対する IP アドレスの問合せ①があると，A レコードに LIP レコードを付加して応答する②．ここで，A レコードは NATF BOX のグローバルアドレス『GA2』，LIP レコードは端末 P のプライベートアドレス『PA1』となる．端末 G の IP 層では，上記 DNS 応答から送信元 IP アドレス，宛先 IP アドレス，LIP アドレスの関係を記憶しておく．DNS 応答を上位層へ渡す際，LIP レコードは削除し，A レコードのみを渡す③．従って，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．

4.2. ポート情報の交換

次に，端末 G が NATF BOX に対して通信を開始する処理を図 6 に示す．両者は通信開始に先立って，ポート情報の交換を行う．端末 G は最初の packets を一時的に退避し，NATF BOX にポート番号要求 packets を送信する ①．この packets には端末 G が通信を行うのに必要な情報(対比した packets の送信元 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 LIP)が含まれる．NATF はこれを受信するとその情報を用いて，疑似 packets を生成する ②．これは，NATF BOX に NAPT テーブルを強制的に作成させるためのもので，端末 P から

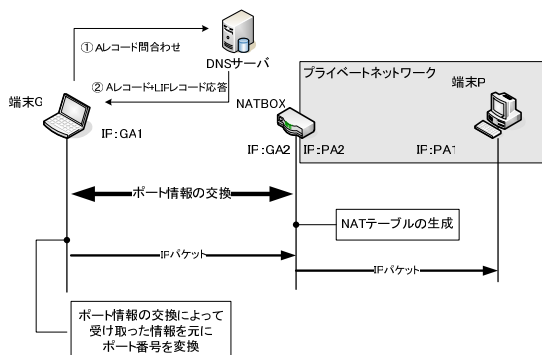


図 4 NATF の構成

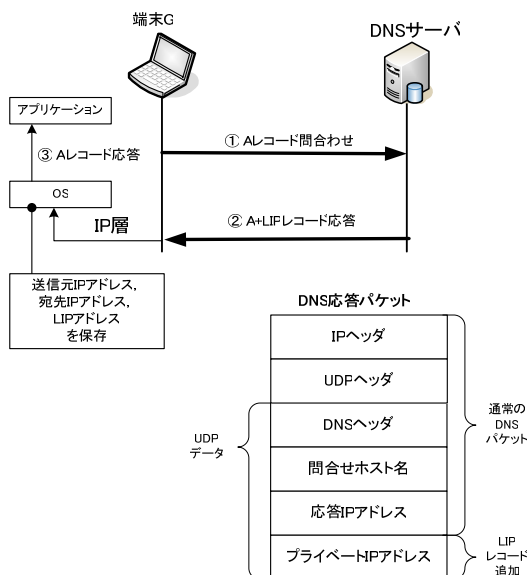


図 5 NATF における DNS 処理

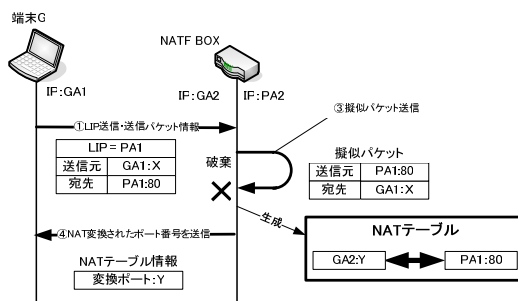


図 6 ポート情報の交換手順

端末Gへ送信されたパケットと見せかける。NATF BOXは通常のNAPTの手順に従って適当なポート番号を選択し、NAPTテーブルを生成した後、疑似パケットを破棄する。NATF BOXは選択したポート番号を、ポート番号応答パケットを用いて端末Gに送り返す(③)。端末Gは、報告されたポート番号を元に、ポート変換テーブルを生成する。端末Gは以後の通信においては宛先ポート番号を、ポート変換テーブルを用いて変換する。一方、NATF BOXは疑似パケットで生成されたNAPTテーブルを用いてIPアドレスとポート番号の変換を行う。以上の動作により、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が開始可能となる。

5. 実装方法

NATFを実装するにはDNSサーバ、グローバル端末、NAPT BOXに対して機能を追加する必要がある、そのモジュール一覧を表1に示す。

DNSに実装されるLIP付加モジュールでは、プライベートIPアドレスの応答の場合に、AレコードをNATF BOXのグローバルIPアドレスへ書き換えを行い、プライベートIPアドレスをLIPレコードとして付加する。

グローバル側端末には、LIP受信、ポート番号要求パケット送信、ポート変換テーブル生成、ポート変換処理の4つのモジュールが必要である。LIP受信モジュールは、LIPが付加されたDNS応答を受けた場合に、AレコードとLIPレコードを分割し、2つのレコードを関連付けるテーブルを生成する。ポート番号要求パケット送信モジュールは、LIPレコードと退避パケットのヘッダ情報を

NATF BOXに送信する。ポート変換テーブル生成モジュールでは、ポート番号応答パケットを元にポート番号変換テーブルを生成する。ポート変換処理モジュールは、生成されたポート変換テーブルを元に、OSから渡されるパケットのポート番号の変換処理を行う。

NAPT BOXには疑似パケット生成モジュールとポート番号応答パケット送信モジュールを実装する必要がある。疑似パケット生成モジュールは、ポート番号要求パケットを受信したときに、そのパケットの情報を元に疑似パケットを送信し、NAPTテーブルを生成する。ポート番号応答パケット送信モジュールは、疑似パケットによって生成されたNAPTテーブルのポート番号情報をポート番号応答パケットとして送信する。

図7に実装の概要を示す。問合せパケットがOSからDNSサーバプログラムに渡される前に、LIP追加モジュールに渡す。送信元IPアドレスがグローバルIPアドレスであった場合、問合せパケットのDNSヘッダ部にある問合わせIDを組として問合せ履歴テーブルに保存し、パケットをDNSサーバプログラムに渡す。送信元IPアドレスがプライベートIPアドレスであった場合は、そのままパケットをDNSサーバプログラムに渡す。DNSサーバプログラム内ではDNSの問い合わせ内容を検索し、応答パケットを生成する。これをOSに渡す直前でLIP追加モジュールに渡す。この時、問合せ履歴テーブルを検索してテーブルが存在し、なおかつ応答するIP

表 1 モジュール構成

実装部位	モジュール名称
DNS サーバ	LIP 付加
グローバル側端末	LIP 受信
	ポート番号要求パケット送信
	ポート変換テーブル生成
	ポート変換処理
NATF BOX	疑似パケット生成
	ポート情報交換

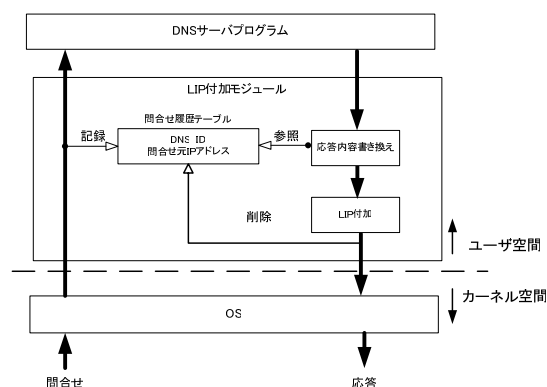


図 7 DNS 実装概要

アドレスがプライベート IP アドレスであった場合、あらかじめ設定ファイルで用意された NATF BOX のグローバル IP アドレスに応答内容の書き換えを行って、LIP レコードを付加する。グローバル IP アドレスであった場合は何もしない。その後、問合せ履歴テーブルを削除し、OS へとパケットを渡す。

6. 評価

NATS, NATF(提案方式)を4つの項目について比較した結果を表2に示す。

NATS では、通信開始時に DNS 問合せが IP アドレスとサブアドレスの2回行われる。また、通信中は全てのパケットに対してカプセル化／カプセル解放処理を行うためオーバーヘッドが発生する。さらに、通信の集中する NATS BOX でもこれらの処理が行われるため、NATS BOX にかかる負荷も大きい。DNS の特性として HINFO レコードにサブアドレスの記述を行う必要があり、端末側の改良が必要である。

NATF では、通信開始時にポート情報の交換を行うため多少のオーバーヘッドが発生する。通信中のオーバーヘッドは端末側でポート変換処理が追加されるだけであるため、性能変化は小さいと思われる。また、NATF BOX は NAPT による通常の変換処理を行うだけであるので通信中の新たな負荷は発生しない。DNS の特性は新たに LIP レコードを追加しているが、一般端末がこのレコードを受け取ったとしても未定義のレコードとして破棄されるためその影響は少ない。

表 2 既存技術との比較

	NATS	NATF
通信開始時のオーバーヘッド	○	△
通信中のオーバーヘッド	△	○
NAT BOX にかかる負荷	△	○
DNS の特殊性	△	○

7. むすび

本稿ではグローバルネットワークからプライベートネットワーク内の複数の端末へアクセスする通信方式 NATF を提案し、その実装状況について報告した。今後は実装を完了して性能評価を実施し、機能の有効性について確認する。

参考文献

- [1]P.Srisuresh, "IP Network Address Translator (NAT) Terminology and Considerations" RPC2663
- [2]Kuniaki KONDO, Capsulated Network Address Translation with Sub-Address(C-NATS), <http://www.nats-project.org/docs/draft-kuniaki-capsulated-nats-03.txt>
- [3]Kuniaki KONDO , Capsulated NATS ProtocolOverview, <http://www.nats-project.org/presentations/Capsulated-NATS-Overview.pdf>
- [4]Kuniaki KONDO, NATS Address Translation Practice, http://www.nats-project.org/presentations/NATS_Address_Translation_Practice.pdf
- [5]W. Simpson, IP in IP Tunneling, <http://www.ietf.org/rfc/rfc1853.txt>
- [6]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, pp.222-225 (2004).
- [7]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, 情報学ワークショップ 2004 論文集, pp.217-221 (2004).
- [8]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.
- [9]Flexible Private Network , Watanabe lab. Division of Information Sciences , Meijo University , <http://www-is.meijo-u.ac.jp/~watanabe/research/fpn1.html>