アドレス空間の違いを意識しない通信を可能とする NATF(NAT Free protocol)の検討と実装

加藤　尚樹[†1]　柳沢　信成[†2]　鈴木　秀和[†3]　渡邊　晃[†4]
名城大学大学院理工学研究科

Researches and its implementation on NATF (NAT Free protocol) which enables to communicate between terminals in different types of address areas

Naoki Kato[†1]　Nobushige Yanagisawa[†2]　Hidekazu Suzuki[†3]　Akira Watanabe[†4]
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，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，両者を接続するために NAT/NAPT[1] が存在し，その間の通信に制約がある．NAT/NAPT は，プライベートアドレス空間に存在する端末をグローバルアドレス空間に接続するための装置で，パケットの 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(以下 NAPT 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のみに生成されるため，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 と共にファイアー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．また，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通信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 DNS サーバ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]を用いてパケットをカプセル化することで NATS BOX を通過させる方式である．しかし，NATS BOX が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．

我々は，DNS サーバ，端末，NAPT が協調して NAPT テーブルを自動的に生成し，端末側が NAPT テーブルにあわせてポート番号の変換を行うことによって NAPT の制約を解決する方式 NATF（NAT Free Protocol）[6-9]を提案している．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．本稿では，DNS 関連の処理については試作プログラムを作成し，動作を検討したので，その結果について報告する．

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グローバルアドレス空間に同時接続できるため，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 よりも広く使われている．以下に NAPT の原理とその課題を述べる．

図 1 に NAPT の動作を示す．プライベートアドレス空間に所属するクライアントがグローバルアドレス空間に所属する WEB サーバへ HTTP 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．

はじめにクライアントは宛先を IP アドレス GA1，ポート番号を 80，送信元を IP アドレス PA1，ポート番号を X として送信する(①)．X はクライアントの OS が動的に選んだ任意のポート番号である． NAPT BOX では送信元を IP アドレス GA2，ポート番号 Y へと変換して中継する(②)．Y は NAPT BOX が動的に選んだ任意のポート番号である．このとき NAPT BOX はこの変換の関係を記した NAPT テーブルを生成する．上記パケットを受信した WEB サーバは，応答パケットを宛先 IP アドレス GA2，ポート番号 Y，送信元 IP アドレス GA1，ポート番号 80 として返信する(③)．このパケットは NAPT BOX が受信し，NAPT テーブルに従って宛先を IP アドレス PA1，ポート番号『X』に書き換えて中継し

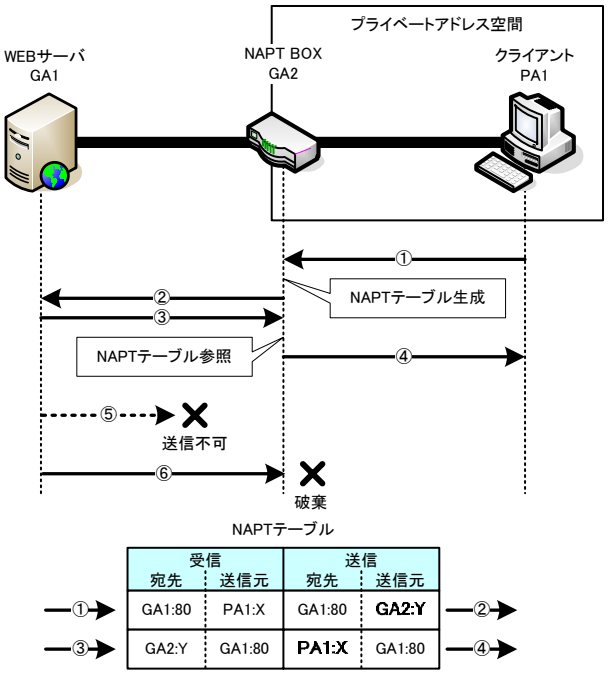

図 1　NAPT の動作とその課題

(④)，クライアントがこれを受信する．以後の通信は NAPT テーブルに従って，NAPT BOX がアドレス変換を行うことにより，通信が行われる．

次に，グローバルアドレス空間から通信を開始する場合を考える．宛先はプライベート IP アドレスとなるが，グローバルアドレス空間においては無効な値であるため送信ができない(⑤)．また，仮に NAPT BOX のグローバル IP アドレスを知ることができて，NATF BOX までパケットを送信できたとしても，NAPT BOX には，まだ NAPT テーブルが存在しないためパケットは破棄される(⑥)．即ち，プライベートアドレス空間にサーバ，グローバル空間にクライアントが存在するシステムは構築できない．NAPT では静的にあらかじめ NAPT テーブルを手動で記述しておき，グローバルアドレス空間からの通信開始を可能とする IP フォワードと呼ぶ機能がある．しかしこの方法では，1 つのポートに対して 1 台しか設定できないことや動的に変更が不可能なため柔軟性に欠ける．

3. NATF

3.1. 概要

図 2 に NATF の構成と概要を示す．NATF ではグローバルアドレス空間にクライアントと DNS サーバ，プライベートアドレス空間に WEB サーバ，その間に NATF BOX を配置する．クライアント，NATF BOX 及び DNS サーバには NATF 対応の機能の実装が必要となる．DNS サーバには，あらかじめドメイン内に存在する WEB サーバのプライベート IP アドレスと NATF BOX のグローバル IP アドレスを登録しておく必要がある．

以下に，クライアントが WEB サーバに対し，通信を開始する場合について動作を示す．クライアントは，通信に先立って DNS サーバに WEB サーバの名前解決を依頼する．DNS サーバでは，A レコードを NATF BOX のグローバル IP アドレスとし，WEB サーバのプライベート IP アドレスを LIP(Local IP address)レコードとして新しく定義した拡張フィールドに載せて応答する．クライアントの OS では，LIP レコードを含む DNS 応答を受け取ると，通信に先立って NATF BOX とネゴシエーション(以下 NATF ネゴシエーション)を行う．このネゴシエーションでは，クライアントでは FAT(natF Address Translation)テーブルの作成，NATF BOX では NAPT テーブルの作成をそれぞれ行うため，それに必要な情報の交換を行う．ネゴシエーションを終了するとクライアントの OS は，LIP レコードを除去した DNS パケットをアプリケーションに渡す．アプリケーションは A レコードから NATF BOX のグローバル IP アドレスを取得し，NATF BOX にパケットを送信する(①)．OS では FAT テーブルを参照して，①のパケットの宛先ポート番号を書き換えて送信する(②)．NATF BOX がこのパケットを受信すると NAPT テーブルに従ってパケットを転送し，パケットは WEB サーバへ到達する(③)．応答パケット(④)は NATF BOX 通過時に通常の NAPT 同様，NAPT テーブルを参照してアドレス変換されクライアントへ転送される(⑤)．クライアントでは応答のパケットを OS にて FAT テーブルを参照し，ポート番号を元に戻してアプリケーションに渡す (⑥)．以後の通信はクライアントでポート変換処理を，NATF BOX では通常の NAPT によるアドレス変換処理行うことで，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可能になる．

3.2. DNS 問合せ

通常の DNS 問合せでは，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の端末のホスト名に問合せがあった場合，プライベート IP アドレスを返すためグローバルアドレス空間では無効な値である．しかし，NATF で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の端末の問い合わせがあった場合，図 3 に示すような応答を行う．以下に，WEB サーバのホスト名を『www. test. com』とした場合の処理について述べる．まず，DNS サーバは WEB サーバに関する問い合わせを受け付けると図 3 の左側に示す通常の DNS パケットを生成する．質問部とは問い合わせがどのホストに対する何のレコードを求めているかを示し，応答部では

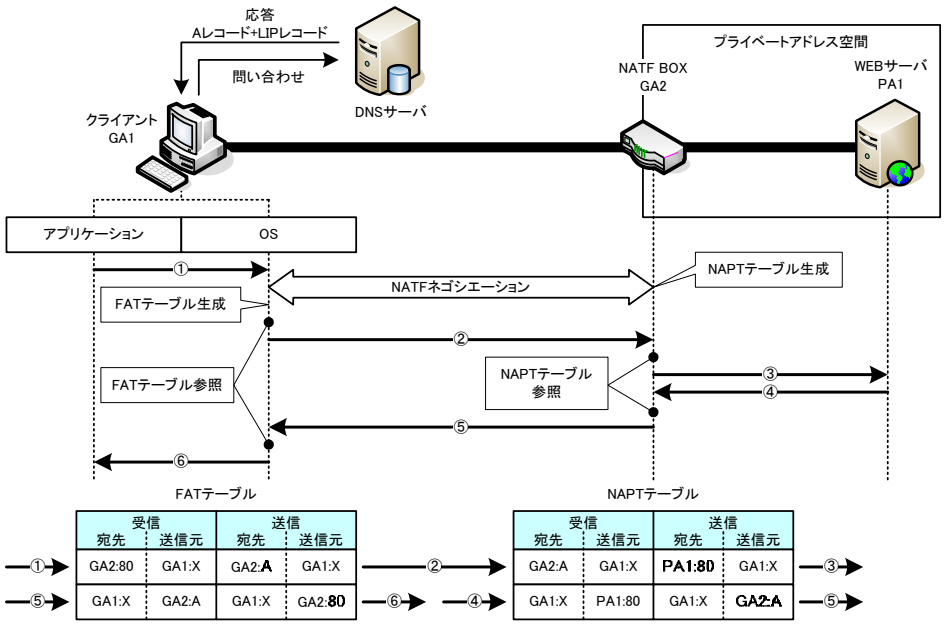

図 2　NATF の構成と概要

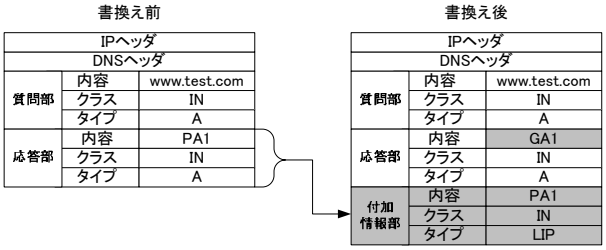

図 3　DNS パケットの書き換えと LIP レコードの付加

その質問の応答としてホストの IP アドレスを返す．次に実装された NATF によりこの応答のパケットの IP アドレスを WEB サーバのプライベート IP アドレス『PA1』から NATF BOX のグローバル IP アドレス『GA2』に書き換えを行う．さらに，書き換え前の応答部のタイプを A から LIP に書き換えて付加情報部として追加する．この書き換え後のパケットを返信することで，クライアントに通信で使うグローバル IP アドレスと通信相手を識別するプライベート IP アドレスの両方を通知することができる．

3.3.　NATF ネゴシエーション

図 4 に NATF ネゴシエーションの処理を示す．はじめにクライアントは WEB サーバのプライベート IP アドレス，パケットの送信元ポート番号及び，宛先ポート番号などの情報をポート番号支持パケットにより NATF BOX に通知する(①)．送信元ポート番号はクライアントの OS が動的に割り当てた番号である．　NATF BOX では受け取った情報を元に NAPT テーブルを生成する．このとき NAPT は自動的に送信元ポート番号『A』を選択する．その後，NATF BOX は選択されたポート番号『A』を調整ポート番号として、さらに 1 で受信したポート番号の情報をポート番号応答パケットによりクライアントに通知する(②)．これを受け取ったクライアントは通知されたパケット情報を元に，FAT テーブルを生成する．

以後の通信においては，クライアントでは FAT テーブルに従って宛先（WEB サーバ側の）ポート番号を，NATF BOX では NAPT テーブルに従って宛先（WEB サーバ側の）IP アドレスとポート番号を変換する．

4.　実装方法

4.1.　モジュール構成

図 5 にモジュール構成図を示す．DNS サーバに実装する LIP 付加モジュールは，クライアントからの問い合わせを判別し，必要に応じて応答の書き換えと LIP レコードの付加を行う．詳細は 4.3 節で述べる．クライアントには LIP 受信モジュール，ネゴシエーション処理モジュール，FAT テーブル作成モジュール，ポート変換処理モジュールを実装する．ネゴシエーション処理モジュールは，通信開始時にアプリケーションが生成したパケットを一時退避し，そのパケットの IP アドレスとポート番号の情報を NATF BOX に通知する．FAT テーブル作成モジュールは，NATF BOX から通知される調整ポート番号を利用して，FAT テーブルを生成する．ポート変換処理モジュールはアプリケーションが生成したパケットや受信パケットを FAT テーブルにしたがって変換する．NATF BOX には擬似パケット作成モジュールとネゴシエーション処理モジュールを実装する．擬似パケット作成モジュールはクライアントからポート番号と IP アドレスの通知を受け，NAPT テーブルを生成するための擬似的なパケットの作成を行う．詳細は 4.2 節で述べる．ネゴシエーション処理モジュールは生成した NAPT テーブルで利用されるポート番号をクライアントへ通知する．

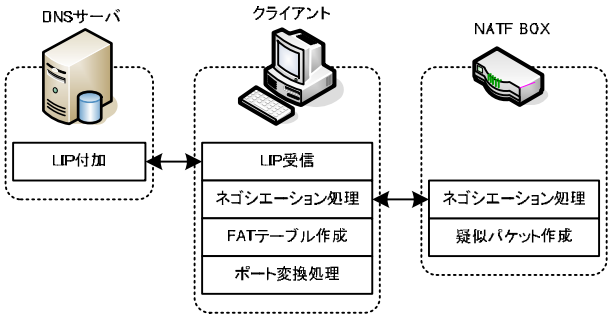

図 5　モジュール構成図

4.2.　擬似パケット作成モジュール

擬似パケットはクライアントから受信したポート番号や IP アドレスの情報を元に，あたかもクライアントから送信されてきたパケットとなるように NATF BOX のカーネル内で擬似的に作成し，NAPT テーブルを生成する．図 6 に擬似パケットによる NAPT テーブル生成の流れを示す．NATF BOX がポート番号指示パケットを受け取るとパケット情報から擬似的なパケットを生成することで NAPT テーブルを生成する．その後このパケットは NATF BOX 内で破棄され，外部に送信されることはない．疑似パケットを破棄した後，ネゴシエーション処理モジュールによりポート番号応答パケットを送信する．

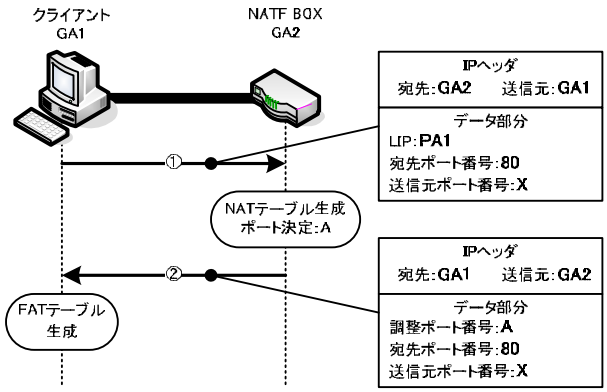

図 4　NATF ネゴシエーションの流れ

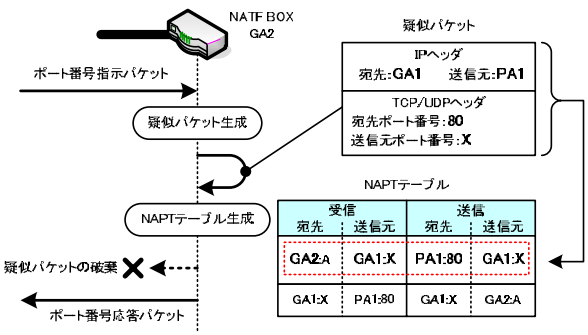

図 6　擬似パケット作成モジュールの処理

4.3. LIP 付加モジュール

LIP 付加モジュールは応答の書き換えと LIP の付加を判断し，必要に応じて処理を行うモジュールである．このモジュールは DNS サーバプログラムに代わって，53 番ポートで待ち受ける．グローバルアドレス空間から A レコードの DNS 問合せがあると DNS ヘッダ内の ID を問合せ履歴テーブルに追加する．これ以外の場合は何もしない．次にほかのポート番号(例では 10053 番ポート)に待ち受けさせている DNS サーバプログラムに対して DNS 問合せを行い，応答を受信する．応答内容書き換えを行うサブモジュールは問合せ履歴テーブルを検索し．ヒットした場合に応答書き換えと LIP 付加を行う．ヒットしない場合は LIP 付加の条件に当てはまらないため書き換えを行わない．

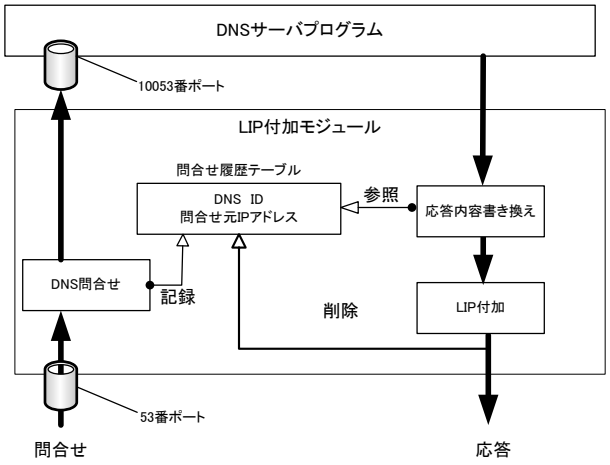

図 7　LIP 付加モジュールの処理の流れ

5. まとめ

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，DNS 実装について報告した．今後は端末部，NATF BOX 部についても実装を行い，機能の有効性について確認する．

参　考　文　献

1). P．Srisuresh, M. Holdrege: IP Network Address Translator (NAT) Terminology and Considerations, RPC2663 (1993).

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 Protocol Overview, 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，RFC1853 (1995).

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 (2004).

9). Watanabe lab．：Flexible Private Network, http://www-is.meijo-u.ac.jp/~watanabe/research/fpn1.html.