目次

概要

家庭内で利用される PC の増加に伴い，プライベートアドレスで構築した家庭内ネットワークを，NAT（アドレス変換装置）を介してインターネットと接続する通信形態が一般的になりつつある．しかし，このような環境では NAT の原理に起因して，インターネット側の外部端末から家庭内の内部端末に対して通信の開始ができないという制約がある．そこで，本研究では，外部端末と NAT が協調することにより，上記制約を解決する NATF(NATF Free Protocol)を提案する．NATF では，外部端末が DNS サーバから NAT のグローバル IP アドレスを取得後，通信に先立って外部端末と NAT がネゴシエーションを行うことにより，NAT のアドレス変換テーブルを強制的に生成する．また，外部端末ではネゴシエーション情報を元に NAT のアドレス変換テーブルに対応したポート番号変換テーブルを生成する．NATF を実装し，動作が可能であることを確認した．また，性能測定の結果，NATF のオーバヘッドは十分に小さく，通常の通信にほとんど影響を与えないことを確認した．

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アドレス変換装置(以下 NAT(Network Address Translation))が存在し、その間の通信に制約がある．NAT 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，端末のプライベート IP アドレスと NAT の持つグローバル IP アドレス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のみ生成されるため、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の通信を開始することができない．この制約を緩和するため，NAT 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、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．

これまで, 企業ネットワークにおいては NAT と共にファイアーウォールが設置され，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，NAT 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厳しいセキュリティポリシーは必要とならない．よって，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，上記のような NAT 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, STUN[1]や AVES[2], IPv4+4[3], NATS[4,5,6,7,8]などがある．

STUN(Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators)はあらかじめプライベート空間側の端末がインターネット上に公開された SUTN サーバに NAT のグローバル IP アドレスと利用可能なポートを登録し，グローバル空間側の端末が通信開始時にこの内容を問合せることによって NAT の制約を除去する方式である．しかし，インターネット上に第 3 のサーバをおく必要があり，UDP 通信に限定されるという課題がある．

AVES（Address Virtualization Enabling Service）は NAT BOX,DNS サーバを改造し，さらに waypoint と呼ぶ装置をインターネット上に設置する．グローバル空間側の端末がプライベート空間側の端末と通信を行う場合, 改良された DNS サーバはプライベート空間側の端末の IP アドレスの代わりに waypoint の IP アドレスを通知する．パケットを受け取った waypoint は NAT BOX と協調することによって

プライベート空間側の端末へパケットを転送する．しかし，STUN 同様，第三の機器をインターネット上に配置する必要があり，DNS に改造を加える必要がある．

IPｖ4+4 は，端末と NAT BOX に改造を加える．端末は DNS サーバより通信相手及び NAT BOX の IP アドレスを得て，IP ヘッダを多重化し，必要に応じて複数の IP ヘッダを入れ替えることで通信を可能とする．この方式では全ての NAT BOX に IPv4+4 を実装する必要がある．また，カプセル化によるオーバヘッドも問題になると考えられる．

NATS(Network Address Translation with Sub-Address)は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[9]を用いてパケットをカプセル化し NAT BOX を通過させる方式である．しかし，NATS 非対応端末と通信を行う際には，全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， NAT 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 NAT 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，端末と NAT BOX が協調して NAT テーブルを強制的に生成し，端末側がポート番号の変換を行うことによって外部からの通信開始を可能とする NATF（NAT Free Protocol）[10,11]を提案する．NATF は，第３の機器を必要とせず，DNS の改造が不要であり導入が容易であると考えられる．また，端末および既存の NAT BOX に改造を加えることにより NATF を実現し，有用なシステムになりうることを確認した．

以下 2 章で NAT の動作とその問題点を示し，3 章で既存技術による解決方法，4 章で NATF の概要を説明する．5 章では NATF の実装方法を示し，6 章で測定結果とその考察を行い，7 章でまとめる．

2. NAT の動作

NAT には，IP アドレスのみを変換する NAT と IP アドレス変換に加え，ポート番号変換も行う NAPT(Network Address Port Translation)がある．NAT は，ポート番号による通信の判別を行わないので，同時にグローバルアドレス空間上の端末と通信ができるのは NAT の保持するグローバル IP アドレスの数だけに制限される．一方，NAPT はポート番号を用いて通信の判別を行うため， NAPT に 1 つだけグローバル IP アドレスを割り当てれば, 複数のプライベートアドレス空間の端末がグローバルアドレス空間の端末と同時に接続できる．NAPT は NAT より汎用性が高いので多く使われているが，NAPT は広義の NAT に含まれるため，以後 NAPT を含めて NAT と呼ぶ．ただし，本稿における NAT の動作説明は全て NAPT のそれをさすものとする．

図 1 に NAT の動作を示す. プライベートアドレス空間に所属する端末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. NAT BOX は NAT 機能が搭載された装置である. 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．NAT BOX では送信元を NAT BOX の 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 NAT BOX が動的に選んだ任意のポート番号である．このとき NAT BOX はこの変換の関係を記した NAT 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，宛先ポート番号 Y，送信元 IP アドレス GA1，送信元ポート番号 80 として返信する(③)．このパケットは NAT BOX が受信し，NAT 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(④)， クライアントがこれを受信する．以後の通信は NAT テーブルに従って，NAT 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の例を図 2 に示す．グローバルアドレス空間に所属する端末がプライベート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．まず,WEB サーバはプライベート IP アドレスであるため，グローバルアドレス空間から見ると無効な値であり，インターネット上に送信ができない(①)．また，仮に NAT BOX のグローバル IP アドレスを知ることができて，NAT BOX までパケットを送信できたとしても，NAT BOX には, まだ NAT テーブルが存在しないためパケットは破棄される(②). 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一般的に構築できない．ただし，NAT で静的にあらかじめ NAT テーブルを手動で記述しておく IP フォワードと呼ぶ機能を利用すればこの限りではない．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.

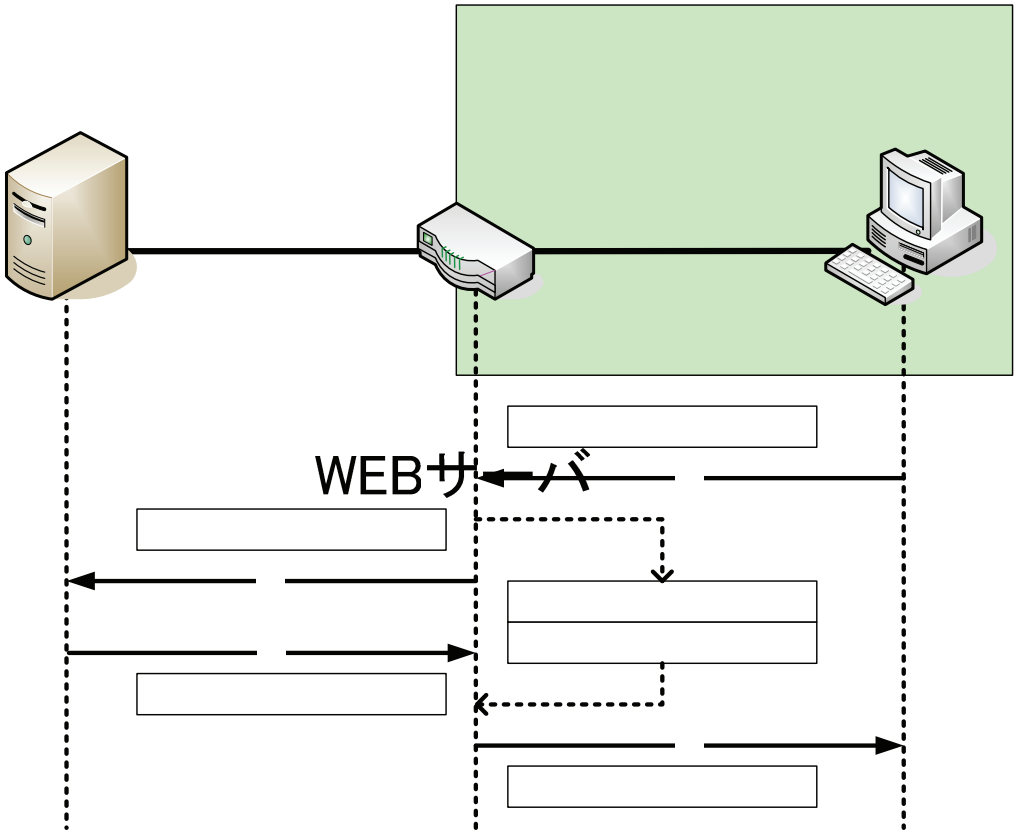

図 1　NAT の動作 1

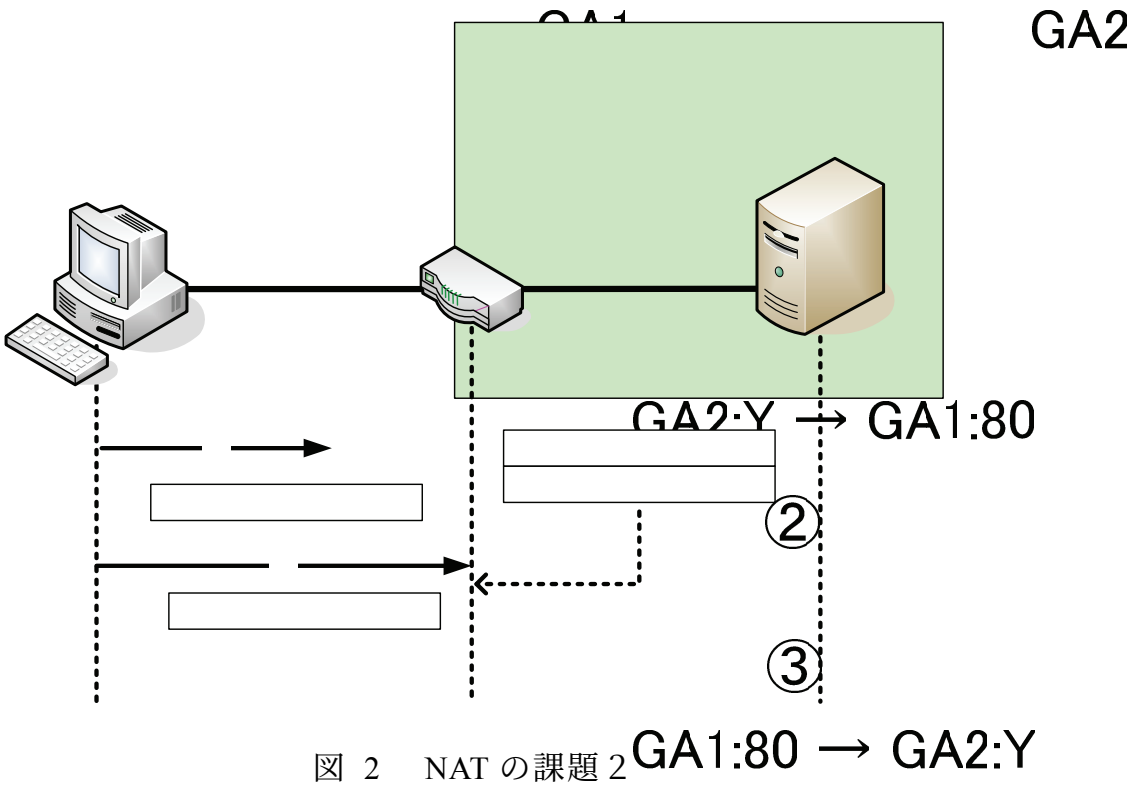

図 2　NAT の課題 2

3. 従来研究による解決とその課題

インターネット側からプライベートネットワーク内の端末へ通信を開始することを実現するために様々な研究が行われている．STUN や AVES では第 3 の装置をインターネット上に置く必要があり，これは大きな課題である．また IPv4+4 は全ての NAT に機能追加しなければならないなど課題がある．本章ではインターネット上に第三の機器を必要とせず，既存システムに影響少ない方式として NATS を取り上げ，その解決法と課題を詳細に述べる．

図 3 に NATS の動作を示す．グローバル空間に端末，プライベート空間に WEB サーバ，その間に NATS 機能を搭載した装置(以後 NATS BOX)が配置され，IP アドレスは端末に『GA1』,NATS BOX のグローバルアドレス空間側に『GA2』,WEB サーバに『PA1』が割り当てられているものとする．また NATS 機能を利用するにあたって，端末，DNS サーバ，NATS BOX に機能が追加される．通信に先立って端末は DNS による名前解決を行う(①)．このとき通常の A レコード問合せによる IP アドレスの取得とともに，NATS 独自のアドレス体系であるサブアドレスの取得を行う(②)．取得したサブアドレスを元に宛先 PA1，送信元 GA1 のパケットを宛先 GA2，送信元 GA1 の IP ヘッダでカプセル化し送信する(③)．これを NATS BOX が受信するとカプセル解放処理を行い，WEB サーバへと転送する(④)．WEB サーバは応答パケットを宛先 GA2,送信元 PA1 として送信する(⑤)．このパケットを NATS BOX が受け取ると，送信元を PA1 から GA2 へと書き換えた IP ヘッダでカプセル化し，端末へと転送する(⑥)．以後の通信は同様の処理によって行われる．

NATS は，NATS 非対応端末に代わり，NATS BOX がパケットのカプセル化，カプセル解放，サブアドレスの解決処理を行う必要があるなど，処理が NATS BOX に集中する．また，サブアドレスを DNS サーバに登録する必要があり，これを取得するため DNS シーケンスに変更を加える必要がある．

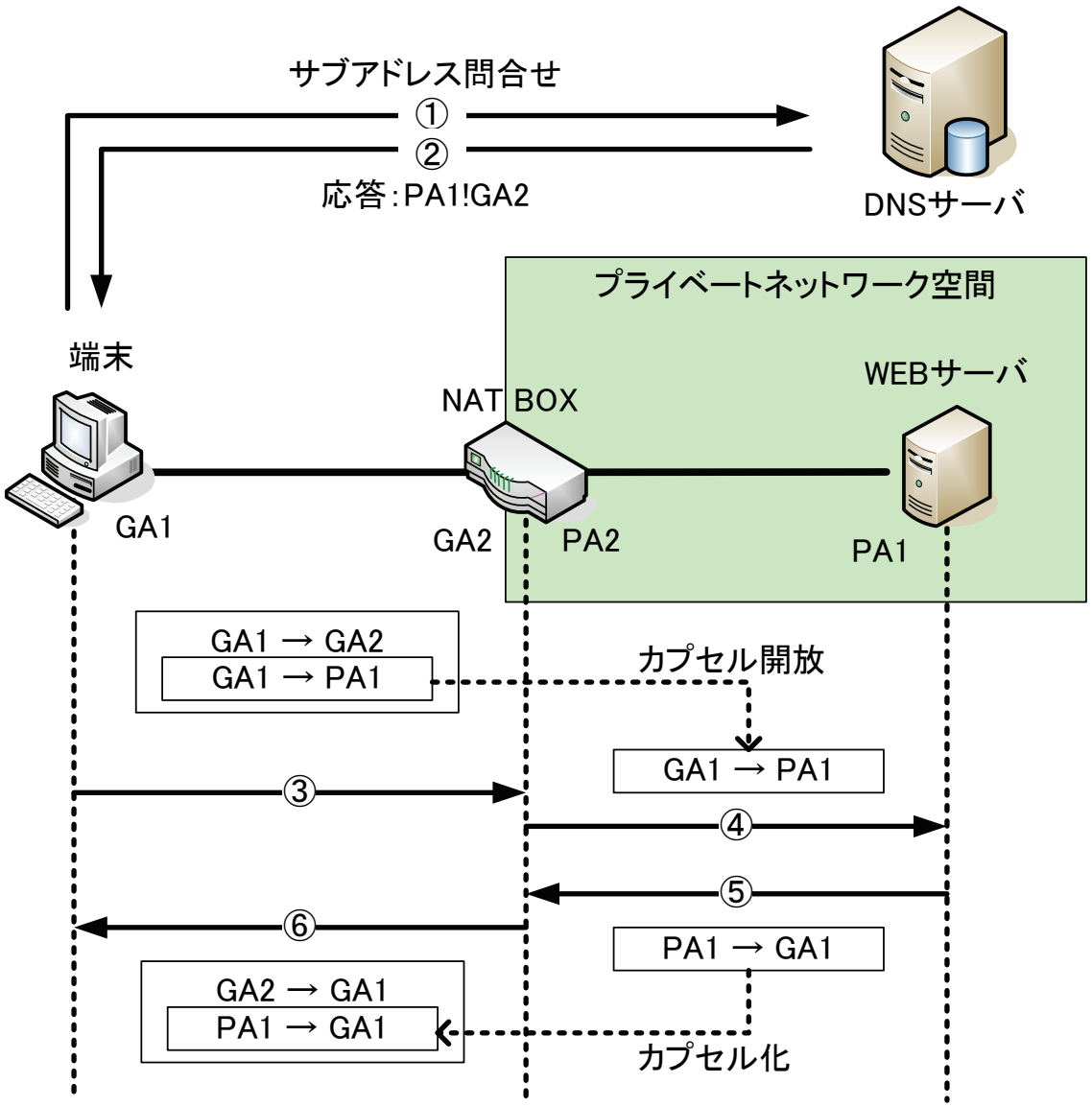
サブアドレス問合せ
①
②
応答:PA1!GA2
DNSサーバ
プライベートネットワーク空間
端末
WEBサーバ
NAT BOX
GA1
GA2
PA2
PA1
GA1 → GA2
GA1 → PA1
カプセル開放
GA1 → PA1
③
④
⑤
⑥
PA1 → GA1
GA2 → GA1
PA1 → GA1
カプセル化

図 3　NATS の動作

4. NATF

4.1. コンセプト

本稿では，自宅のインターネット環境を整え，ネットワークを構成できる程度のユーザがインターネット上から自宅のネットワークへの機器へアクセスすることを想定している．

図 4 に現在の家庭ネットワーク構成を示す．ブロードバンドルータは光ケーブルや ADSL などのブロードバンドを利用してインターネットへ接続するインターフェースを持ち合わせた NAT BOX である．ユーザは家庭内ネットワークに存在する端末をインターネットへ接続するために，ブロードバンドルータにダイヤルアップの設定を行ってインターネットへ接続する．また，近年のブロードバンドルータには DHCP と呼ばれる接続した機器に自動的にプライベート IP アドレスを割り当てる機能が備わっており，簡単な設定を行うだけで家庭内ネットワークを構築することができる．

当初，NATF の実現方式として，DNS サーバとブロードバンドルータ及び端末を改造する方法が考えられる．しかしながら，DNS サーバは通常プロバイダ提供するものを利用できることが望ましく， DNS サーバへ改造を加える方法は普及しづらいと考えられる．そこで，NATF ではユーザが設定可能なブロードバンドルータと外部から接続する端末のみを改造することによってインターネット側から家庭内ネットワーク内端末への通信を可能にした．

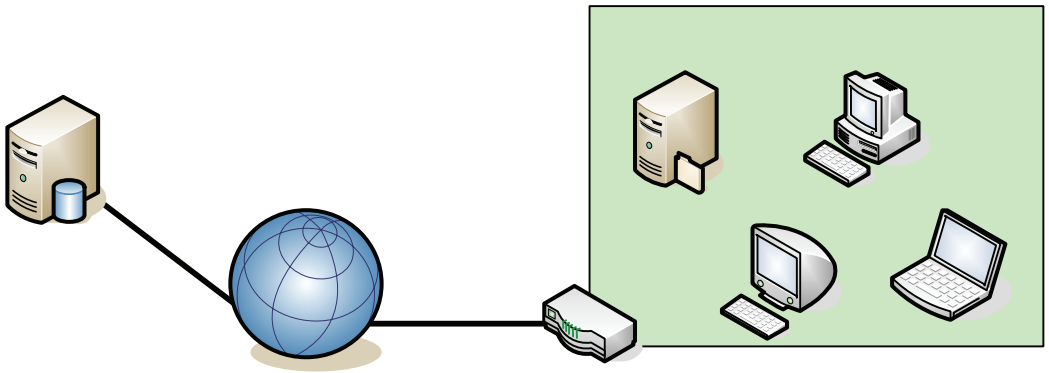

図 4　現在の家庭ネットワーク構成

4.2. NATF の構成と初期情報の設定

NATF の構成を図 5 に示す．グローバルアドレス空間に端末，プライベートアドレス空間に WEB サーバ, その間に NATF 機能を搭載した装置(以下 NATF BOX)が配置されている．IP アドレスは端末に『GA1』,NATF BOX のグローバル空間側に『GA2』,WEB サーバに『PA1』が割り当てられているものとする．DNS サーバには『home.com』として NATF BOX のグローバル IP アドレス『GA1』が登録されている．端末と NATF BOX はあらかじめ下記のような初期情報の設定が必要である．即ち，端末には，NATF BOX 配下のプライベート空間の端末のホスト名『www』とその IP アドレス『PA1』を組とした NRDB(Name Resolution Data Base)を登録する．NATF BOX には，WEB サーバのホスト名『www』とその IP アドレス『PA1』を組とした APDB(Access Permission Data Base)を登録する．

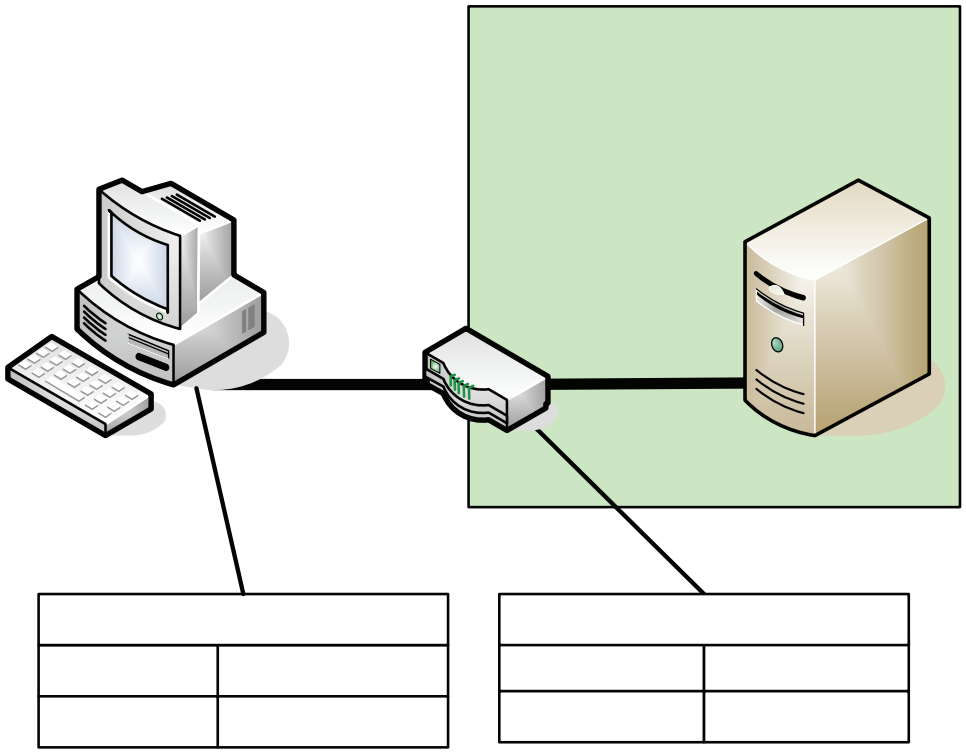

図 5　NATF の構成と初期情報

4.3. 動作概要

NATF の動作概要を図 6 に示す．端末は，通信に先立って DNS による名前解決を行い， NATF BOX のグローバル IP アドレスである GA2 を得る．名前解決の詳細については，4.4 で述べる．次に，端末と NATF BOX 間で NATF ネゴシエーションを行う. このネゴシエーションでは, 以後の通信に必要な情報を交換し, NATF BOX で NAT テーブルを強制的に生成する. NATF ネゴシエーションが終了すると，端末ではネゴシエーションで得た情報を元に宛先ポート番号変換テーブルを生成する．NATF ネゴシエーションの詳細は 4.5 で述べる．以後の通信は端末でのポート番号変換処理と NATF BOX での通常の NAT 処理によって行われる．

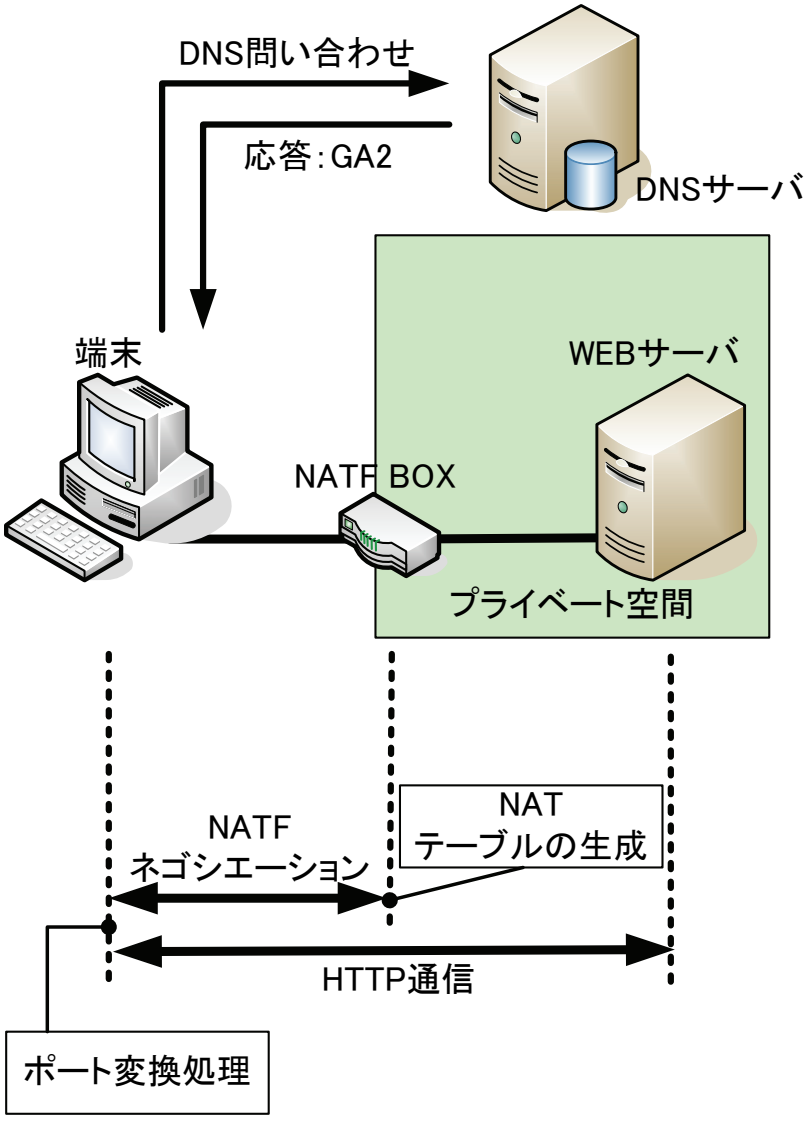

図 6　NATF の動作概要

4.4. DNS による名前解決

グローバルアドレス空間の端末がプライベートアドレス空間の WEB サーバと通信したい場合，端末は NATF BOX のグローバルアドレスを知る必要がある．DNS サーバにはドメイン名とそれに対応した NATF のグローバルアドレスが登録されている．そこで，端末側は DNS 問合せ時に図 7 のような動作を行う．

端末のアプリケーションは OS に対し『www.home.com』の問合せを依頼する．OS では問合せ依頼を受けると事前に登録されていた NRDB 検索を行う．問合わせ内容が NRDB 内のホスト名+ドメイン名とヒットした場合，問合わせ内容からホスト名を除去し，ドメイン名のみで DNS サーバへ問い合わせを行う．DNS サーバはこの問合せに対して，NATF BOX の IP アドレスを返答する．この動作により，アプリケーションは NATF BOX の IP アドレスを『www.home.com』の IP アドレスであるものとして認識する．NRDB の検索にヒットしなかった場合は NATF を利用しない問合せであることを示すため，そのままの内容で DNS 問い合わせを行う．端末側ではこの動作を実現するために OS の改造を行う．

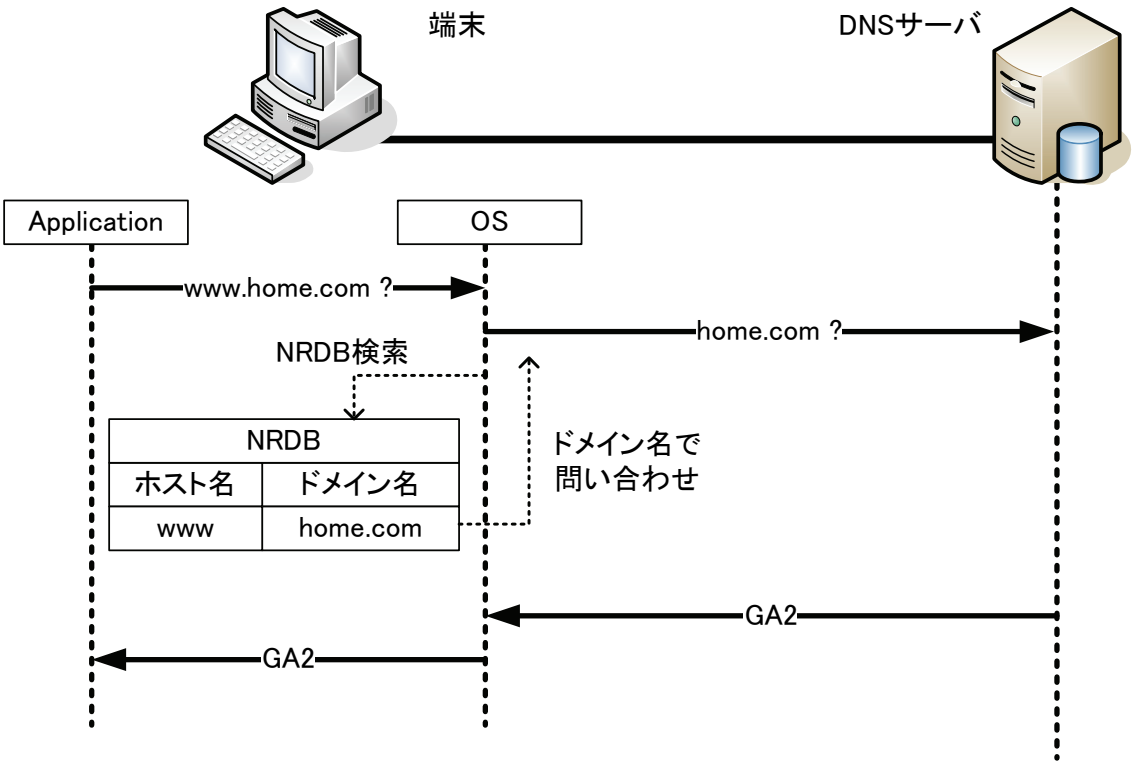

図 7　端末における名前解決の動作

4.5. NATF ネゴシエーション

NATF ネゴシエーションは NATF BOX での NAT テーブルを強制的に生成することと，端末側に利用可能なポート番号変換テーブルを生成することを目的としている．図 8 に NATF ネゴシエーションの動作を示す．NATF ネゴシエーションは端末側でアプリケーションからの第 1 パケットを OS が受信したところから開始する． このとき受け取った第 1 パケットは OS 内部に退避しておく．次に第 1 パケットの宛先，送信元の IP アドレスとポート番号，プロトコルタイプ及び，宛先のホスト名をポート番号指示パケットとして NATF BOX 宛に送信する．NATF BOX では上記パケットを受信すると，この内容から擬似パケットと呼ぶ仮想のパケットを生成し自分宛に送信する．擬似パケットは，宛先 IP アドレス『GA1』，宛先ポート番号『X』とする．擬似パケットを受信すると NATF BOX 内の NAT 処理により強制的に NAT テーブルが生成される．生成された NAT テーブルにより，擬似パケットの送信元ポート番号８０は Y に変換される．NATF BOX はポート番号通知パケットと呼ぶ応答パケットを生成し，端末へ変換ポート番号『Y』を通知する．上記パケットを受信した端末では，その内容から宛先ポート番号変換テーブルを生成し，NATF ネゴシエーションが終了する．

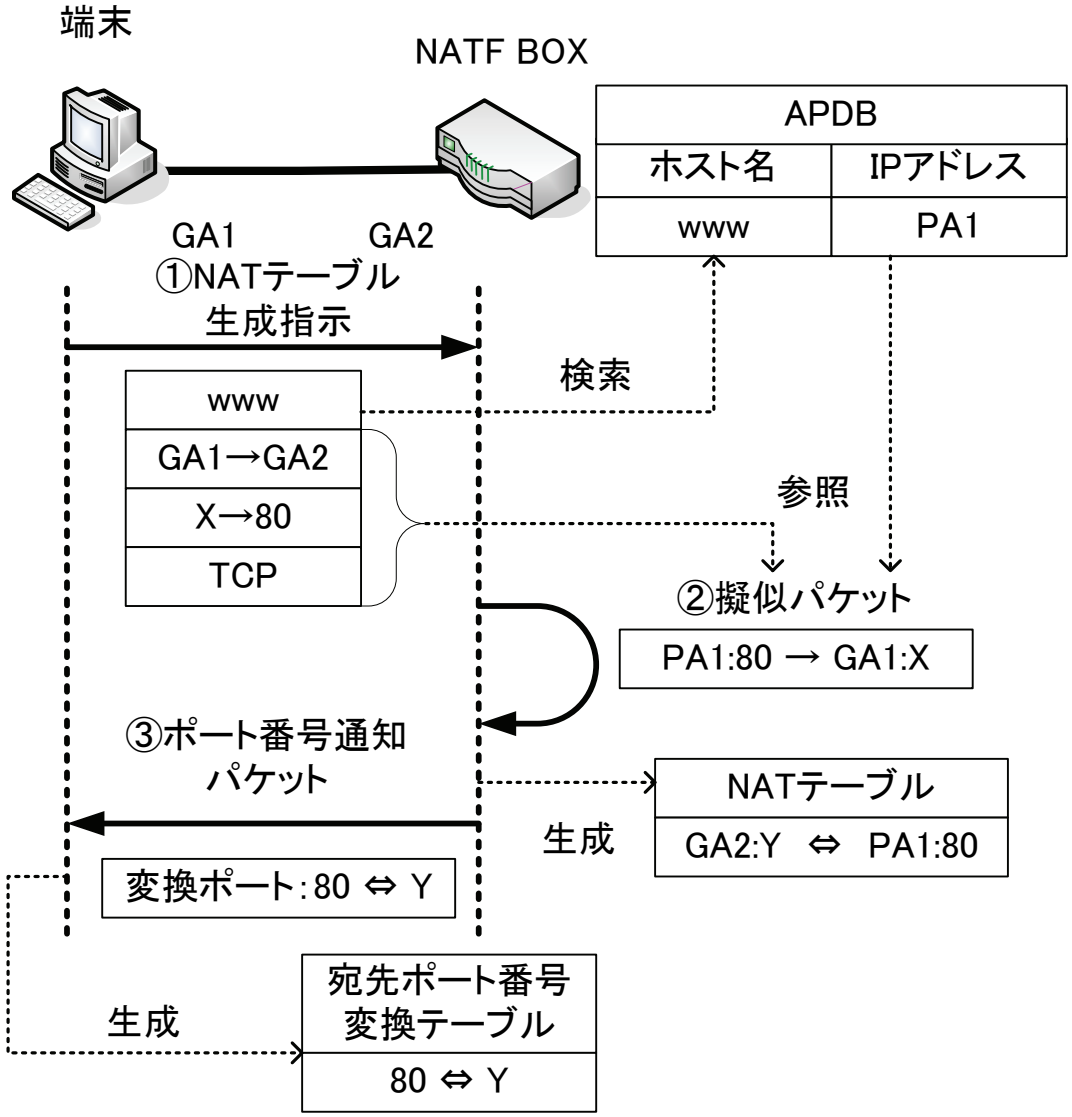

図 8　NATF ネゴシエーションの動作

5. 実装

NATF は端末及び NATF BOX の IP 層に実装される．実装に利用した OS は IP 層の情報が豊富な FreeBSD である．図 9 に NATF の実装概要を示す．この実装図は端末及び NATF BOX に共通なものである. NATF モジュールは IP 層の入出力関数 ip_input，ip_output から呼び出して処理を行う．NATF モジュール内さらに適切なサブモジュールが呼び出され，処理を行う．NATF モジュールで処理された通信パケットは元の位置に戻される．既存の IP 層の処理には一切影響を与えない．

natd は既存の NAT のモジュールであり，パケットのアドレス変換，ポート番号変換，及び NAT テーブルの管理を行う．また，ip_foward 関数は，ip_input で受信したパケットが自分宛のパケットではない場合に転送処理を行う関数である．NATF は, これらの NAT 処理の前に NATF モジュールは呼び出されて処理を行う．以下 5.1 に NATF のモジュール構成，5.2 に端末における動作，5.3 で NATF BOX における動作を示す．

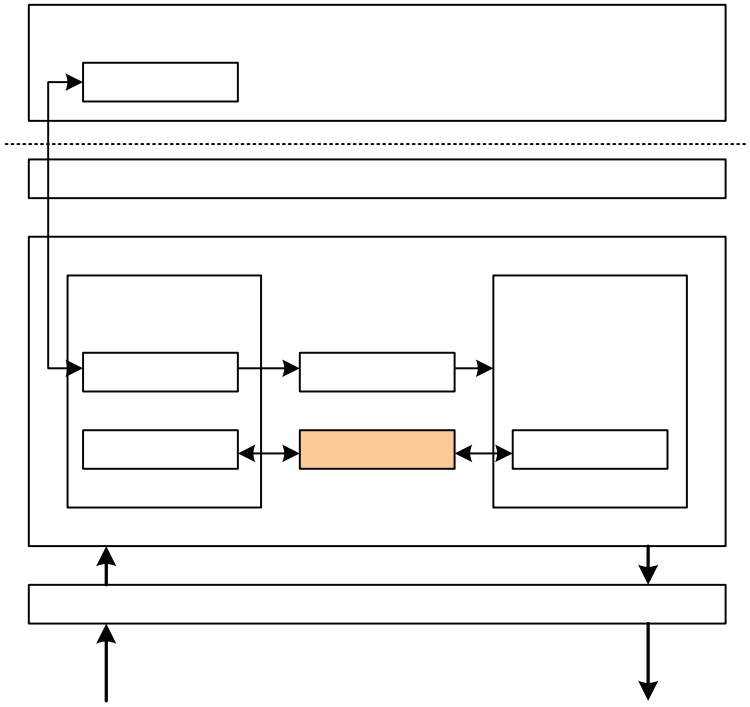

図 9　NATF の実装概要

5.1. モジュール構成とその機能

NATF モジュールの構成を図 10 に示す．初期設定モジュールは APDB 及び NRDB の追加,検索，削除を行うモジュールである．ネゴシエーションモジュールは NATF ネゴシエーションに必要な NAT テーブル生成指示パケット, 擬似パケット及びポート番号通知パケットを生成するモジュールである．ポート番号変換モジュールはポート番号変換テーブルを管理し，これに基づいてパケットのポート番号を書き換えるモジュールである．DNS 書き換えモジュールは初期設定モジュールで登録された NRDB を参照し DNS の問い合わせ内容の書き換えを行うモジュールである．

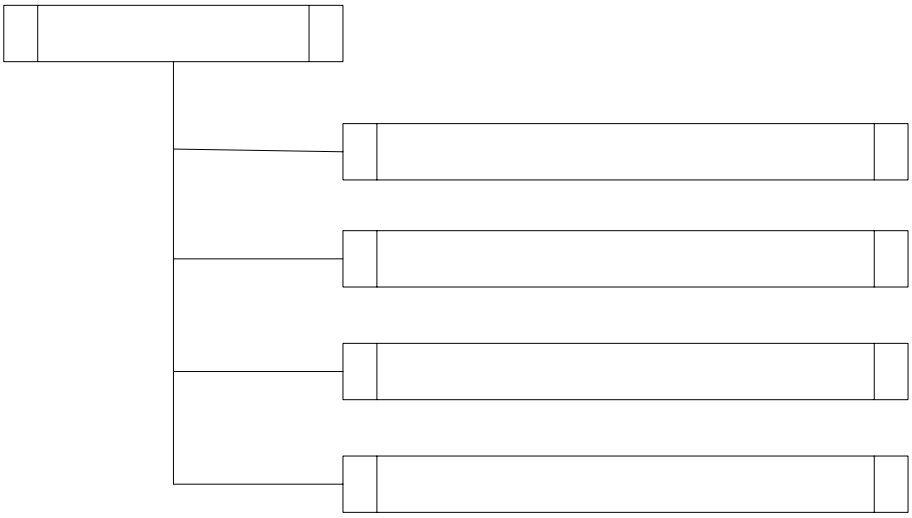

図 10　モジュール構成

5.2. 端末における処理

図 11 に端末における NATF モジュールがデータを受け取った後の処理フローを示す．受信パケットの UDP が 53 番ポートであった場合，DNS に関する通信パケットであるため，DNS 書き換えモジュールが呼び出され，NRDB（端末への登録情報）を検索する．NRDB にヒットした場合，問い合わせ内容が書き換えられ，そうでない場合は通常の問合せであるため何もせずに処理を戻す．次に ICMP パケットであった場合，ポート番号通知パケットかどうかを判別する．ポート番号通知パケットであった場合，ポート番号変換テーブルに生成情報を追加する．ポート番号通知パケットでなかった場合は何もせずに処理を戻す．TCP または UDP パケットであった場合は，ポート番号変換モジュールによってポート番号変換テーブルを検索する．ヒットした場合はそのテーブルに従いポート変換を行い，そうでなかった場合は何もせずに処理を戻す．

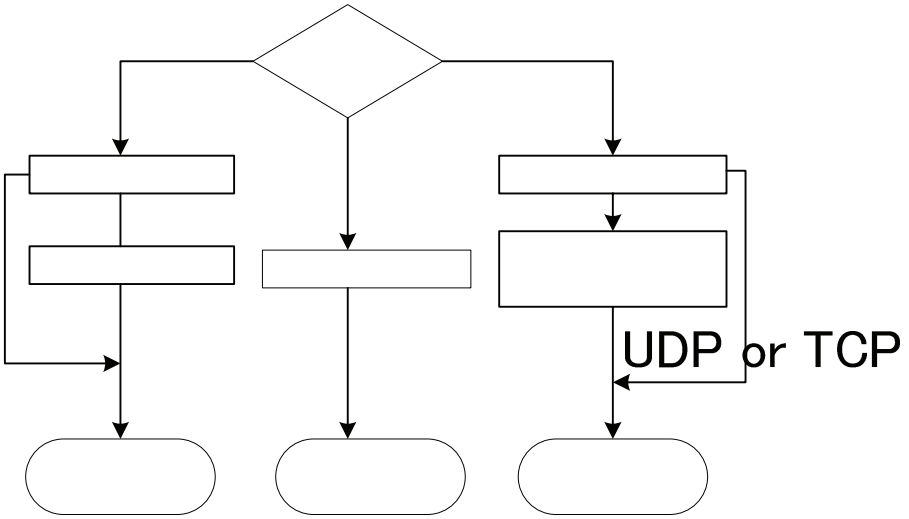

図 11　端末における NATF 処理フロー

5.3. NATF BOX における処理

図 12 に NATF BOX における処理のフローを示す．受信パケットが ICMP であった場合，ポート番号指示パケットかどうかを判別する．ポート番号指示パケットであった場合ネゴシエーションモジュールを呼び出し，擬似パケットを生成する．ポート番号指示パケットでなかった場合は何もせずに処理を戻す．TCP または UDP パケットであった場合は擬似パケットかどうかを判別する.擬似パケットであった場合はパケットを破棄し，ネゴシエーションモジュールにより擬似パケットの情報からポート番号通知パケットを生成する．擬似パケットでなかった場合はそのままパケットを送信する．

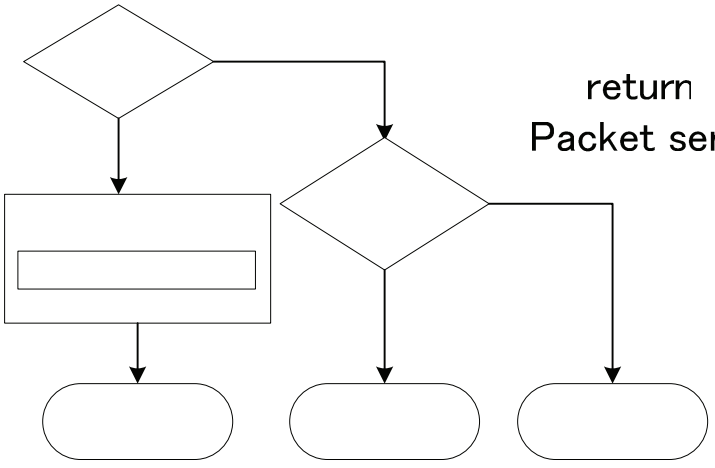

図 12　NATF BOX における NATF 処理フロー

6. 評価

6.1. 評価方法

実験環境を図 13, 図 14 に示し, 各機器のスペックを表 1 に示す. 図 13 は NATF を利用した場合のネットワークで, 以下構成 A と呼ぶ. 通信開始端末, NATF BOX にはそれぞれ NATF モジュールの組み込みを行い，実験サーバには FTP サーバデーモンと測定ツール Netperf[12]をインストールした. 図 14 は比較のために構築した通常の NAT を利用したネットワークで以下構成 B と呼ぶ．通信開始端末は改造を加えていない構成 A と同スペックものを利用し，NAT BOX は FreeBSD に NATD をインストールしたものを利用する．上記二つの構成を用いて，FTP によるファイルのダウンロード時間と，スループット測定ツール NetPerf によるスループット測定を実施した.

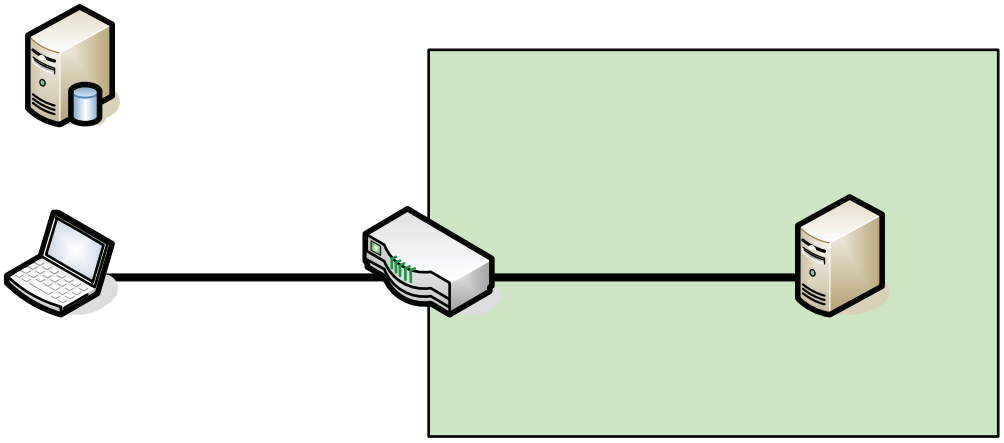

図 13　NATF BOX を用いたネットワーク構成 (構成 A)

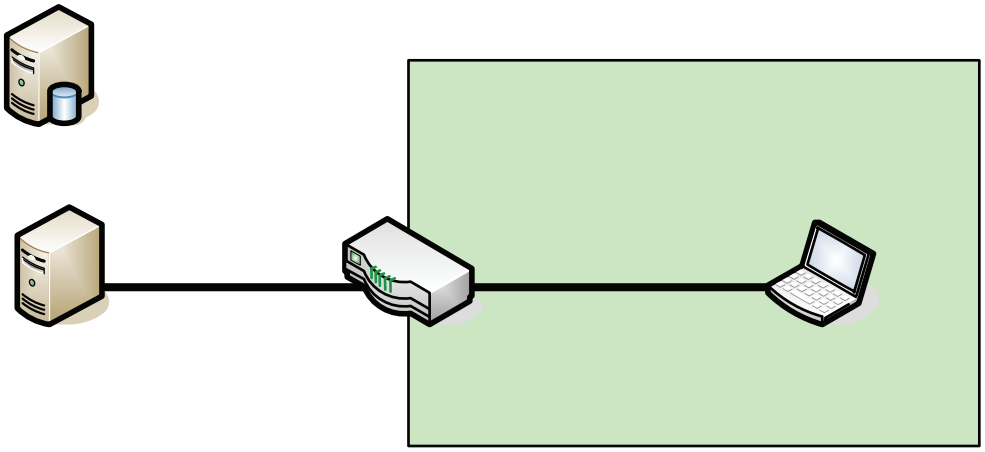

図 14　NAT BOX を用いたネットワーク構成 (構成 B)

DNSサーバ

表 1　実験機器の仕様

	通信開始端末	NATF BOX	実験サーバ
CPU	Pentium4 2.4GHz	Pentium4 2.4GHz	Pentium(R)M 1.8GHz
メモリ	256MB	256MB	512MB
NIC	100BASE-TX	100BASE-TX	100BASE-TX
OS	FreeBSD5.3	FreeBSD5.3	Windows XP Professional

6.2. 測定結果

Netperf によるスループットの測定値を表 2 に示す．この測定は，100BASE の環境において送信するメッセージサイズとスループットの関係を示したものであり, 測定値は各メッセージサイズにおける 10 回の測定値の平均値である. 構成 A, 構成 B とも，どのメッセージサイズにおいてもスループットは 90～91MBps 程度であり，理論限界値に近い値が実現された．両者の間には有意差が認められず，同等のスループットが得られていることが分かる．

次に，FTP で 500MB,100MB,50MB のファイルをそれぞれダウンロードするのに要した時間を比較したものを図 14 に示す．各値は 10 回の測定結果の平均値である．50MB,100MB のファイルのダウンロード時間はほぼ一緒であった．また，500MB のファイルについては 1%程度の遅れがあるがオーバヘッドは小さい．

FTP では接続時に DNS の問合せが行われるため DNS の書き換え処理は含まれない，よって，このオーバヘッドは端末におけるポート変換によるものだと考えられる．しかしながら，NATF のオーバヘットは非常に小さく，通常の通信に影響を与えないものであり，実用的であると考えられる．

表 2　Netperf によるスループット測定値

メッセージサイズ(MB)	構成 A(Mbps)	構成 B(Mbps)
64	90.565	90.05
128	92.361	91.837
256	91.054	91.274
512	90.977	91.383
1024	90.977	90.835

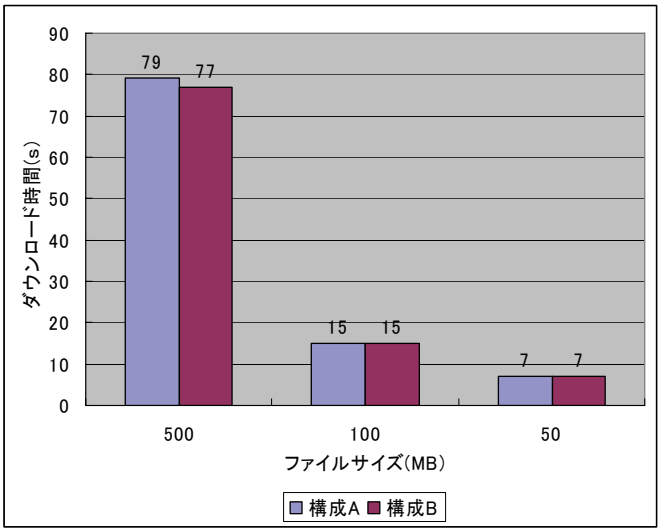

図 15 FTP におけるファイルのダウンロード時間

7. まとめ

本稿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内の複数の端末へアクセスする通信方式 NATF を提案した. 本方式では DNS の問合せによって NATF BOX のグローバルアドレスを得て, 通信に先立ちネゴシエーションを行う. これによって, NATF BOX で NAT テーブルを強制的に生成し, 端末側でポート変換を行うことによって通信を可能としている.

NATF を利用することによって, 家庭内ネットワークの機器へ自由にアクセスが可能となる. プライベート IP アドレスは自由に割り当てることができ, アドレス数も十分に確保できることからインターネット家電への活用なども考えられる. また, NATF BOX を複数台利用することにより異なるプライベートアドレス空間間で相互に通信を行う CIPA[13]も可能となり, より自由な通信環境が実現できる. 実装については IP 層の情報が豊富な FreeBSD を利用し, 端末, NATF BOX ともに同じモジュールを利用することによって簡単にすることができた. また, Netperf によるスループット測定と ftp によるダウンロード時間の計測を行い, 性能を評価した. 既存の NAT と NATF の比較から NATF のオーバヘッドは小さく, 通常の通信にほとんど影響を与えないため. 実用性は高いものと考えられる.

今後, 実際に運用し, 実利用における問題点の検証を行っていく必要がある.

謝辞

本研究にあたって，御指導をして下さった渡邊晃教授には，様々な助言をもらい非常に研究の励みとなり，また多くの事を学習する事ができ，心より感謝しています．また，同研究室で研究をともに行った仲間にもアドバイス，意見を活発に出していただいたことに深く感謝します．

参考文献

1 J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy,"STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489 (2003)

2 T.S.Eugene Ng, I.Stoica, H.Zhang, "A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces", USENIX 2001 (2001).

3 Z. Turanyi, A. Valko, "IPv4+4", ICNP2002 (2002).

4 Kuniaki Kondo, "Capsulated Network Address Translation with Sub-Address(C-NATS)", Internet Draft (2002).

5 Kuniaki Kondo, "Possibility of NATS Communications Summary", http://www.nats-project.org/com-possibility-sum.html

6 Kuniaki Kondo, "Capsulated NATS Protocol Overview", http://www.nats-project.org/presentations/Capsulated-NATS-Overview.pdf

7 Kuniaki Kondo, "NATS Address Translation Practice", http://www.nats-project.org/presentations/NATS_Address_Translation_Practice.pdf

8 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

9 W. Simpson, “IP in IP Tunneling”, RFC 3489(1995)

10 加藤尚樹，柳沢信成，鈴木秀和，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"，情報技報，2005-DPS-122，pp.351-356 (2005).

11 加藤尚樹，柳沢信成，鈴木秀和，宇佐見庄五，渡邊 晃，"インターネットから家庭ネットワークへの接続を可能とする NATF プロトコルの検討と実装", 情報学ワークショップ 2005，pp.，論文集(2005)

12 NetPerf, http://www.netperf.org/netperf/NetperfPage.html

13柳沢信成，加藤尚樹，鈴木秀和，渡邊晃，

発表実績

平成 15 年度　電気関係学会東海支部連合大会
"DDNS を用いた移動体通信における IP アドレス解決方法"
電気関係学会東海支部連合大会，Oct. 2003.

情報処理学会　第 66 回全国大会
"NAT を意識しない個人ネットワークを管理する Home FireWall の提案"
情報処理学会　第 66 回全国大会，Mar.2004.

第 2 回　情報学ワークショップ 2004（WiNF2004）
"アドレス空間の違いを意識しない通信方式 NATF の提案"
WiNF2004 論文集，Vol.2，pp.222-225，Sep. 2004.

第 122 回　DPS 研究発表会
"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"
情報処理学会研究報告，　2005-DPS-122.

情報処理学会　DICOMO2005 シンポジウム
"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"
DICOMO2005 シンポジウム論文集，Vol.2005，No.6，pp.373-376，Jul.2005.

情報学ワークショップ 2005（WiNF2005）
"インターネットから家庭ネットワークへの接続を可能とする NATF プロトコルの検討と実装"
WiNF2005 論文集，pp.142-146，Sep.2005.

受賞暦

情報処理学会　DICOMO2005 シンポジウム　　ヤングリサーチャ賞 受賞

付録

1. 過去技術

1.1. STUN

SUTN は NAT BOX の持つ NAT テーブル情報を事前にグローバルネットワーク空間上に配置された登録サーバ(以下 STUN サーバ)へ登録し，通信開始端末が通信に先立って NAT テーブル情報を STUN サーバへ問い合わせることで NAT テーブルで転送可能なパケットを生成し，通信を可能とする方式である．図 A に端末が TFTP サーバと通信を行う場合の SUTN の動作を示す．グローバルネットワーク空間には端末，STUN サーバ，NAT BOX を配置し，NAT BOX 配下のプライベートネットワーク空間には WEB サーバを配置している．IP アドレスは，端末『GA1』，STUN サーバ『GA3』，NAT BOX『GA2』『PA2』，WEB サーバ『PA1』が割り当てられている．端末，WEB サーバには STUN クライアントモジュールが組み込まれており，STUN サーバとの通信を担っている．

はじめに TFTP サーバは STUN サーバに送信元ポート番号を TFTP プロトコルの待ち受けポート番号の 69 番とするパケットを送信する（①）．①のパケットを NAT BOX が受信すると NAT テーブルを生成し，送信元のポート番号及び IP アドレスを変換し，STUN サーバへ転送する(②)．STUN サーバでは受信したパケットの送信元 IP アドレスと送信元ポート番号をマッピング情報として登録する．

次に端末が，STUN クライアント機能によって，通信に先立ち STUN サーバへマッピング情報の問合せを行う(③)．STUN サーバは②によって登録されたマッピング情報を端末へ応答する(④)．端末では④受け取ったマッピング情報の IP アドレスとポート番号を宛先とするパケットを送信する(⑤)．⑤のパケットを NAT BOX が受信すると①によって生成された NAT テーブルを参照し，宛先 IP アドレス『PA1』，宛先ポート番号『69』に変換して送信する．これによって TFTP サーバへパケットが到達し，通信が可能となる(⑥)．

STUN における課題は，インターネット上に第三の装置として STUN サーバ設置しなければならないことや NAT BOX の実装方式には様々な種類があるため，その種類によっては利用できないことである．また，UDP でのみ利用が可能で，基本的には TCP に対応していない．TCP に対応させるために，UDP でカプセリングを行う方式が提案されているが，パケットの冗長が発生する課題がある．

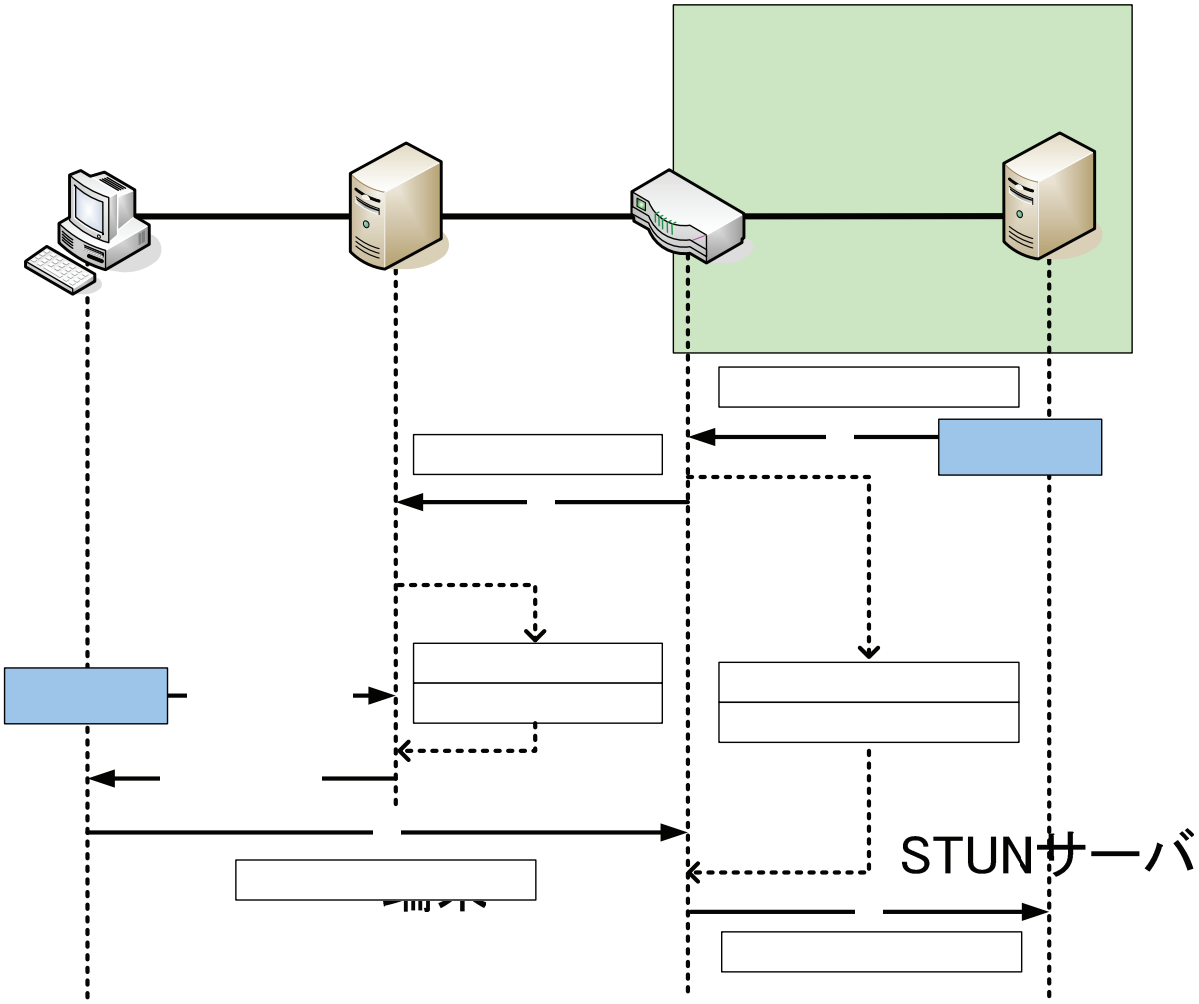

図 A　STUN の動作

GA1　　GA3

GA2:Y

1.2. AVES

AVES は IPｖ４のプライベートネットワーク空間やグローバルネットワーク空間，IPv6 ネットワークなど，様々なネットワーク空間の相互接続を目的としたアーキテクチャであり，waypoint と呼ばれる機器を配置し，NAT 及び DNS を拡張している．

図 B は IPｖ４のプライベートネットワーク空間とグローバルネットワーク空間の相互接続を行い，端末がサーバ www.home.com と通信を行う場合の例である．端末，DNS サーバ，waypoint がグローバルネットワーク空間に存在し，www.home.com の FQDN を持つサーバがプライベートネットワーク空間に存在している．また，グローバルネットワーク空間とプライベートネットワーク空間の間に NAT BOX がゲートウェイとして存在する．IP アドレスは端末『GA1』，waypoint『GA3』，NAT BOX『GA2』，『PA2』，www.home.com には『PA1』を割り当てる．このとき GA で始まるアドレスはグローバル IP アドレスであり，PA で始まるアドレスはプライベート IP アドレスである．また DNS サーバには www.home.com が『PA1』であることが登録されている．

はじめに，端末は www.home.com の DNS 問合せを DNS サーバに送信する(①)．DNS サーバは，①を受信すると端末が www.home.com と通信可能であるかの確認要求を waypoint へ送信する(②)．waypoint は②に含まれる端末の IP アドレス，NAT BOX の IP アドレス，www.home.com の IP アドレスより通信が可能であるかどうかを判断し，可能であれば OK を応答として返す(③). DNS サーバは，waypoint から OK の応答を受信すると，端末に対し，waypoint の IP アドレス『GA3』を応答する(④)．端末は宛先を『GA3』としてパケットを送信する(④)．waypoint は④を受信すると送信元 IP アドレス及び②で受け取ったルート確認情報を利用し，送信元『GA2』，宛先『PA1』とした，プライベートネットワーク空間で用いる IP ヘッダを生成する．さらに，送信元『GA3』，宛先『GA2』とした，グローバルネットワーク空間で用いる IP ヘッダを生成して IP in IP カプセリングを行い，送信する(⑤)．⑤を受信した NAT BOX は，カプセル解放を行い，送信元『GA2』，宛先『PA1』としてパケットを転送する(⑥)．www.home.com サーバは応答として送信元『PA1』，宛先『GA1』のパケットを送信し(⑦)，通常の NAT 処理によって送信元『GA2』，宛先『GA1』へ書き換えを行い，転送されて端末へ到達し通信が可能となる(⑧)．以後は⑤，⑥，⑦，⑧に示す経路をたどり，通信が行われる．

AVES における課題は，グローバルネットワーク空間上に waypoint を設置しなければならないことや，NAT や DNS といった普及しているシステムに変更を加えなければならないことから，普及に時間がかかる．また，パケットを waypoint に中継させるため，三角経路が発生し，経路が冗長することも挙げられる．さら

に，waypoint - NAT BOX 間では IP in IP カプセリングを利用しているためパケットが冗長する．

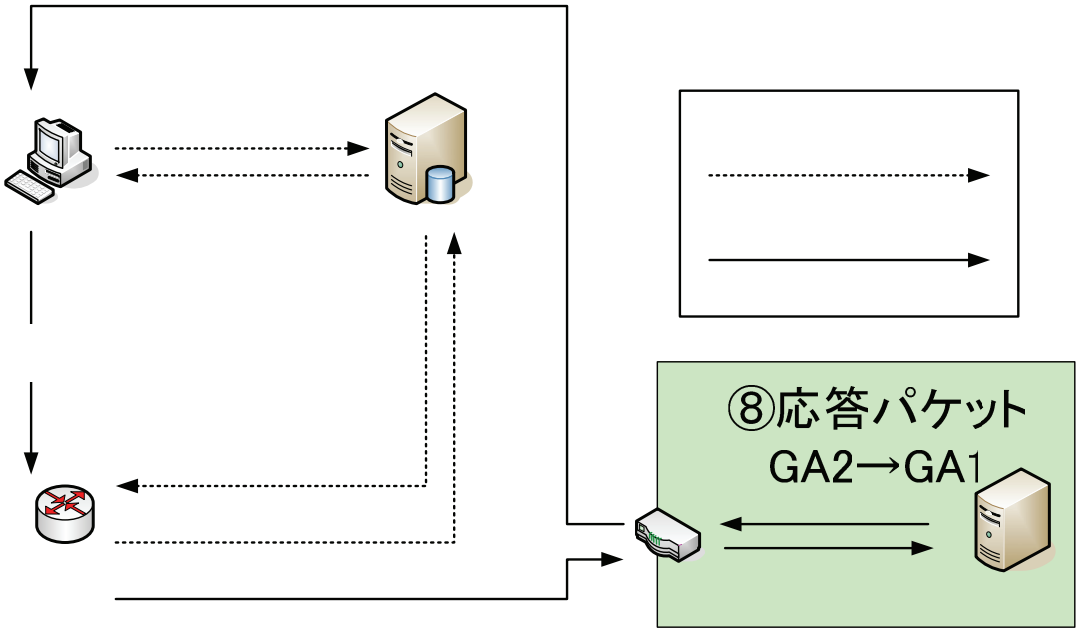

図 B　AVES の動作

1.3. IPv4+4

IPｖ4+4 は IPv4 ヘッダを拡張し，IP アドレスを複数扱えるようにすることで，パケットの存在するアドレス空間で有効なアドレスに変換して通信を行う技術である．図に IPｖ４+4 の動作を示す．端末，ルータ，および WEB サーバそれぞれに IPｖ４+4 機能が追加される．IPｖ４+4 では IP アドレスの代わりに，端末と端末が所属するネットワークのゲートウェイの IP アドレスを組とした IP4+4 アドレスが用いられる．IP4+4 アドレスは IP アドレスを『.』で区切った形で表記される．通信に先立って DNS 問合せにより DNS サーバから宛先 IP4+4 アドレス『GA1. PA1』を取得する(①,②)．次に送信元『GA1.0』，宛先『GA1. PA1』としてパケットを送信する(③)．送信元 IP4+4 アドレスの後半部が 0 であるのは，端末がグローバルアドレス空間存在し，ゲートウェイが存在しないからである．これをルータが受信すると宛先の IP4+4 アドレスを入れ替え『PA1. GA1』として送信する(④)．このようにしてパケットは WWW サーバへ到達する．以後の通信は同様の処理によって行われる．IPｖ４+４における課題は通信を行う全ての機器に対して機能の追加を行う必要があるため導入が難しい点である．

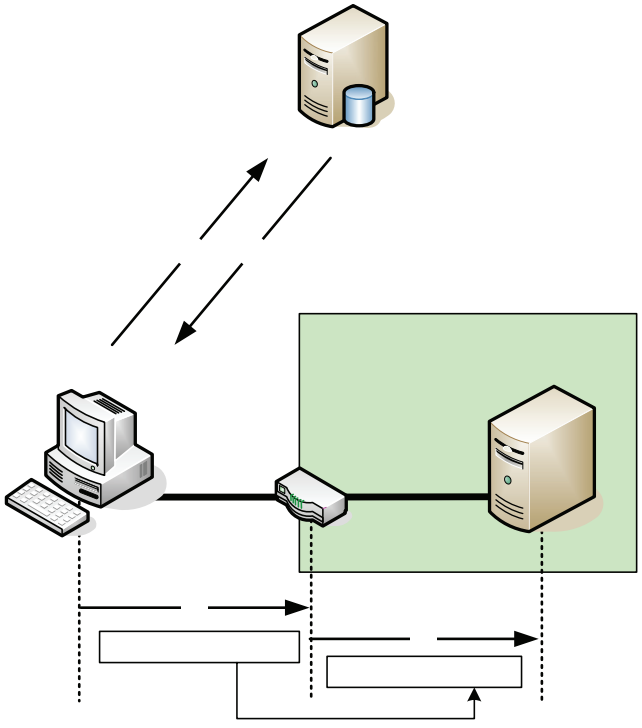

図 C　IPv4+4 の動作