平成25年度　修士論文

邦文題目

端末の変更が一切不要な NAT越え通信システムの提案

英文題目

Proposal of a NAT traversal Communication System Requiring No Changes in the Terminal

情報工学専攻専攻

(学籍番号: 123430037)

松尾　辰也

提出日: 平成26年1月31日

名城大学理工学研究科

内容要旨

IPv4 グローバルアドレスが枯渇したため，家庭内や企業のネットワークの端末はプライベートアドレスで実現するのが一般的である．しかし，NAT が存在するとインターネット側の端末からプライベートアドレス側の端末へ通信を開始できない NAT 越え問題が存在する．NAT 越え技術としてこれまで様々な方式が提案されているが，多くの方式では端末に特殊な機能を実装する必要がある．この課題を解決するために，本研究室では端末の改造が不要な NAT 越え技術 NTSS（NAT Traversal Support System）を提案しているが，端末の登録変更が必要という課題が残されていた．そこで本論文では，NTSS を更に改良を加え，登録変更も不要とした NTSSv2 を提案し，その実装方法を述べる．また，NTSS の測定結果を基にルータの負荷を予測した結果，問題なく動作できることが確認できた．

目 次

第1章　はじめに

2011 年 4 月に IPv4 グローバルアドレスが枯渇 [1] し，家庭内や企業などのネットワークはプライベートアドレスで構築するのが一般的となっている．プライベートアドレスはインターネット上では利用できないため，両ネットワークの間には NAT（Network Address Translation）[2] [3] [4] を設置し，アドレス変換を行う必要がある．しかし，NAT はグローバル側の端末からプライベート側の端末へ通信を開始できないという課題があり，これを NAT 越え問題と呼ぶ．以前のインターネットの利用形態は Web ページの閲覧やメールの利用など，一般にグローバルアドレス空間に設置されたサーバに対してプライベートアドレス側の端末から通信を開始していたため，NAT 越え問題が表面化することはなかった．しかし，近年ではネットワークの普及に伴い，企業だけでなく一般家庭にもネットワークを構築していることが一般的となっている．そのため，グローバル側からプライベートアドレスを持つサーバなどに自由にアクセスしたいというニーズは十分にあると考えられる．

NAT 越え問題を解決するためにこれまで様々な解決手法が提案されてきたが，その特徴により以下のように分類することができる．すなわち，既存の NAT 装置をそのまま使えることを目的としたアプリケーションレベル改造方式，既存のアプリケーションをそのまま使えることを目的としたネットワークレイヤ改造方式，端末の改造を不要とすることを目的とした端末非依存方式である．

アプリケーションレベル改造方式は，エンド端末のアプリケーションとインターネット上に設置したサーバが NAT テーブルの情報を交換し，NAT に生成された NAT テーブルに合わせて，外部端末からパケットを送信する点が特徴である．この方式は，アプリケーションが限定されることと，新たな専用装置が必要になるという課題がある．代表例として，STUN（Simple Traversal of UDP through NATs）[5] [6]，TURN（Traversal Using Relay NAT）[7]，UPnP（Universal Plug and Play）[8]，NAT-PMP（NAT Port Mapping Protocol）[9] などがある．

ネットワークレイヤ改造方式は，アプリケーションを限定しないために，外部端末のカーネルや NAT などのネットワーク機器に手を加える．外部端末と NAT が協調してパケットを内部に転送する点が特徴である．この方式は，端末の OS ごとに異なる対応が必要となる．代表例として，4+4 [10]，NAT-f（NAT-free protocol）[11]，NATS（NAT with Sub-Address）[12] などがある．

端末非依存方式は，DNS（Domain Name Server）[13] [14]，NAT，あるいはインターネット上のサーバなどが情報交換し，一般端末が送信するパケットを通信経路上でアドレス変換し，プライベートアドレス空間の中に転送する点が特徴である．この方式は研究事例がそれほど

多くないため，研究途上であるといえる．端末非依存方式の AVES（Address Virtualization Enabling Service）[15] では，第三の装置が必要であること，通信経路が冗長になること，送信元アドレスが実際と異なるため経路上のルータで廃棄される可能性があるなどの課題がある．

これらの NAT 越え技術を用いると，共有サーバをプライベートアドレス空間に設置できるので，グローバルアドレスを大幅に節約することができる．このとき，情報家電やモバイル端末の多様化により，今後はユーザが自由に端末に機能を追加できない場合が考えられる．例えば，情報家電の組み込みシステムにおいて独自 OS を使用している場合，システムをそのまま適用させることが難しいと考えられる．そこで，本論文では一般ユーザが容易に共有サーバを利用できるようにするため，端末に改造が不要な端末非依存方式に着目する．

本研究室では，これまで端末非依存方式として NTSS（NAT Traversal Support System）[16] を提案してきた．NTSS はグローバル側の端末が名前解決のために使用する DNS キャッシュサーバ，及び NAT を改造し，それぞれを協調させることにより，NAT 越えを実現する．新たな専用装置が不要でエンドエンドで NAT 越え通信を行うことができ，AVES が抱えていた課題を解決できる．しかし，NTSS ではグローバル側の端末において DNS キャッシュサーバの登録変更をしなければならず，誰でも利用できる訳ではなかった．

そこで本論文では，DNS キャッシュサーバには一切改造を加えず，プライベート側の端末のアドレスを管理する DNS 権威サーバを改造するように機能を見直した NTSSv2 を提案する．この方式により，両エンドの端末の変更及び登録変更が一切不要な NAT 越えシステムを実現する．

提案方式で使用するサーバとルータの実装検討を行った．サーバはプライベート側の端末を管理する DNS サーバを改造するため，送信元の DNS サーバからの反復問合せをトリガにするように変更した．また，反復問合せには EN のアドレス情報が含まれていない為，ルータとのネゴシエーションメッセージの内容に変更を加えた．ルータにおいても，この変更に対応させるために，処理動作と NAT テーブル生成方法に変更を加えた．

また，NTSS の測定結果を基にルータの負荷予測を行った．予め利用端末の種類や RTT などを想定し，ルータの設定を適切な値にすることで，問題なく動作できることが予測できた

以降, 2 章で既存の端末非依存方式である AVES の概要と課題, 3 章で要素技術となる NTSS の概要と課題，4 章で本論文の提案方式である NTSSv2 を説明し，5 章で実装について述べ，6 章で提案方式におけるルータの負荷予測について述べる．最後に 7 章でまとめる．

第2章　既存の端末非依存方式の概要と課題

既存の NAT 越え技術の１つとして AVES がある．AVES は AVES 対応の DNS と NAT，第三の装置である Waypoint と呼ばれる中継器を設置し，これらが協調動作を行うことで NAT 越えを実現する．以降, EN（External Node）をグローバル側からアクセスする端末, IN（Internal Node）をプライベートアドレス空間に存在し，EN からアクセスされる端末とする．

2.1　AVES の概要

図 2.1 に AVES の動作を示す．AVES 対応の DNS と NAT をそれぞれ ADNS サーバ，ANAT ルータと呼ぶ．事前設定として，IN は ADNS サーバに自身の FQDN とプライベート IP アドレス（PA1）に加え，ANAT ルータのグローバル IP アドレス（GA2）を関連付けて登録しておく．また，EN は ADNS サーバを自身のプライマリ DNS として登録変更しておく必要がある．以下，EN から IN（alice）へ通信を開始する場合を例として説明する．

EN が ADNS サーバに alice の名前解決を行うと，ADNS サーバは Waypoint に Setup メッセージを送信する．Setup メッセージには EN のグローバル IP アドレス（GA1），ANAT ルータのグローバル IP アドレス（GA2）及び alice のプライベート IP アドレス（PA1）が含まれる．これを受信した Waypoint は経路変換テーブルを生成し，ADNS サーバに Accept メッセージを応答する．そして，ADNS サーバは Waypoint のグローバル IP アドレス（GA3）を EN に応答する．このため，EN は alice 宛の通信パケットを Waypoint に対して送信することになる．

Waypoint は EN からのパケットを受信すると，経路変換テーブルに基づいて宛先アドレスを alice のプライベート IP アドレス（PA1）に変換する．さらに ANAT ルータ宛の IP ヘッダで変換したパケットをカプセル化して，ANAT ルータへ送信する．これを受信した ANAT ルータは，カプセル化を解除し alice へ転送する．これに対し，alice からの応答パケットは Waypoint を経由せず，ANAT ルータから EN へ直接送信される．ここで，ANAT ルータは送信元 IP アドレスを Waypoint の IP アドレスとなるように変換する．このようにして EN から IN の通信は Waypoint を経由し，IN から EN への応答は直接通信という三角経路となる．

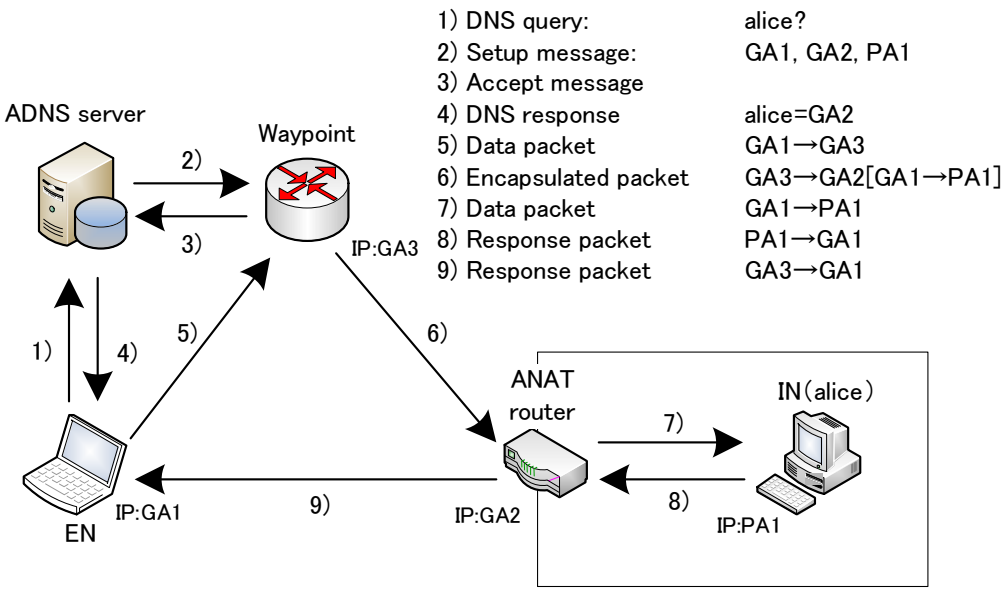

図 2.1　AVES の動作

2.2　AVES の課題

AVES は Waypoint という第三の装置が必要であるため，この装置が故障した場合の対策を別途考える必要がある．また，経路が冗長になることや，カプセル化によるパケット冗長が発生し，スループットが低下するなどの課題がある．更に，IN からの応答パケットの送信元アドレスが ANAT ルータではなく Waypoint の IP アドレスとなるため，ネットワーク上のルータにイングレスフィルタリング [17] などのセキュリティが設定されている場合，パケットが経路途中で破棄される可能性がある．

第3章　NTSSの概要

本章では要素技術となる NTSS について，その実現手法の詳細と課題を示す．以後の説明では，DNS サーバが提供する機能の違いにより，ホスト名を管理する DNS サーバを権威サーバ，ホスト名を問い合わせる DNS サーバをキャッシュサーバと呼ぶ．NTSS では，EN のキャッシュサーバと NAT を改造し，そこに NTSS を実現させるための NTS プロトコルを実装していた．改造したキャッシュサーバを NTS サーバ，改造した NAT を NTS ルータと呼ぶ．NTS ルータは NTS サーバと協調し，外部から送信されてくるパケットに合わせて NAT テーブルをオンデマンドに生成する特徴がある．

この方式により，AVES の課題であった第三の装置の設置と経路の冗長化を解決できる．しかし，EN においてキャッシュサーバの登録変更をしなけれならないという課題がある．これにより，登録変更を行っていないユーザは NTSS を利用することができない．

3.1　構成と事前設定

図 3.1 に NTSS の構成を示す．インターネット上に EN のキャッシュサーバとなる NTS サーバと，IN の権威サーバとなる DDNS（Dynamic DNS）[18][1]を設置する．DDNS は既存の ISP[2]が使用しているものを利用できる．事前設定として，EN はあらかじめ，NTS サーバをキャッシュサーバとなるように登録変更しておく．また，DDNS には IN の FQDN と NTS ルータのグローバル IP アドレスの対応関係を DNS レコードに登録する．NTS ルータには IN の FQDN とプライベート IP アドレスの対応関係を独自のテーブル PHL（Private Host List）に登録する．

EN，NTS ルータのグローバル IP アドレスをそれぞれ GA1，GA2 とし，IN（alice）のプライベート IP アドレスを PA1 とする．

EN から IN（alice）へ通信を開始する場合を例として，NTSS の動作を名前解決と通信開始時に分けて説明する．

[1] IP アドレスとホスト名の対応関係を動的に登録・管理するサーバ
[2] インターネットサービスプロバイダ

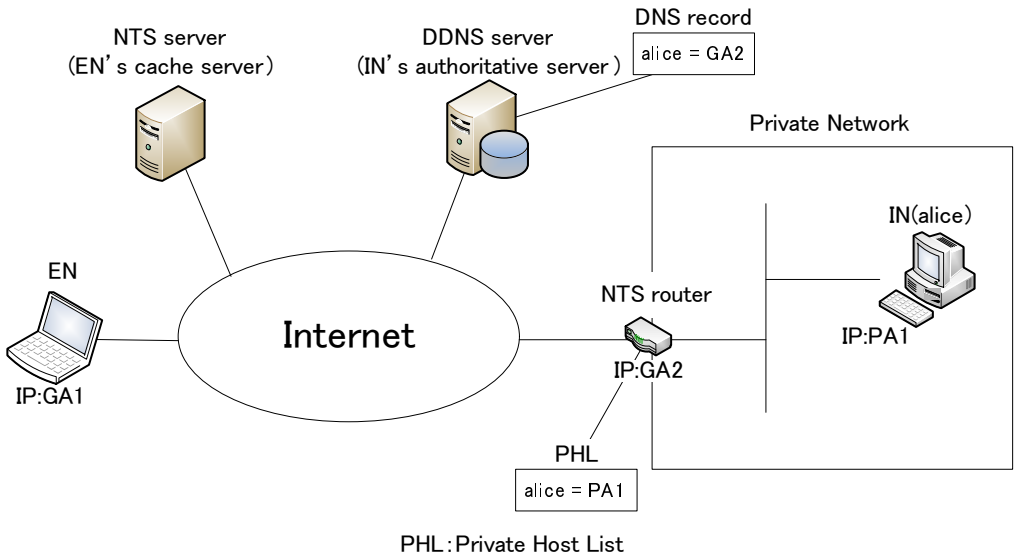

図 3.1　NTSS の構成

3.2　名前解決

図 3.2 に NTSS の名前解決シーケンスを示す．EN は通信を開始するに当たり，alice の名前解決を NTS サーバへ依頼する．NTS サーバは通常の DNS の仕組みにより，反復問合せを行い，alice の権威サーバである DDNS サーバより NTS ルータのグローバル IP アドレス（GA2）を取得する．図 3.2 は簡単のため NTS サーバの反復問合せの部分は省略して記述している．NTS サーバはこの名前解決を EN へ返信する前に，EN から alice への接続要求があることを通知する NTS リクエストを NTS ルータに送信する．このメッセージには，EN の IP アドレス（GA1）と alice の FQDN が含まれている．この通知を受け取った NTS ルータは事前に設定しておいた PHL を参照し，alice のプライベート IP アドレス（PA1）を取得する．その後，EN と IN の IP アドレスの関係を RC（Request Cache）と呼ぶ独自のキャッシュへ記憶し，NTS サーバへ NTS レスポンスを返信する．これを受信した NTS サーバは，先ほど取得した名前解決結果（GA2）を EN に返信する．

3.3　通信開始

図 3.3 に名前解決後の通信開始シーケンスを示す．EN は名前解決の結果，alice の IP アドレスを“ GA2 ”と認識しているため，NTS ルータに向けて通信を開始する．ここで，

$$GA1 : s \rightarrow GA2 : d \tag{3.1}$$

は送信元 IP アドレス GA1，送信元ポート番号 s，宛先 IP アドレス GA2，宛先ポート番号 d のパケットであることを示す．s は EN のカーネルが選択した任意のポート番号であり，d は

IN がサービスを提供しているポート番号である．

NTS ルータはインターネット側からパケットを受け取ると，送信元 IP アドレスをキーとして RC を参照する．RC に該当するデータがあれば，NTS ルータは受信したパケットと RC の内容から次のような NAT テーブルを動的に生成する．

$$GA1 : s \leftrightarrow \{GA2 : d \Leftrightarrow PA1 : d\} \tag{3.2}$$

上記 NAT テーブルの意味は，NTS ルータから見た外側トランスポートアドレス“ GA1 : s ”との通信では NAT のトランスポートアドレス“ GA2 : d ”と IN のトランスポートアドレス“ PA1 : d ”が対応していることを意味する．即ち，“ GA1 : s ”から“ GA2 : d ”へ送信されたパケットは，NTS ルータの NAT 機能において宛先が“ PA1 : d ”に変換されて alice へ転送される．これに対する alice からの応答パケットは上記と逆の変換を行い，EN へ送信される．RC は NAT テーブルを生成した時点で削除する．

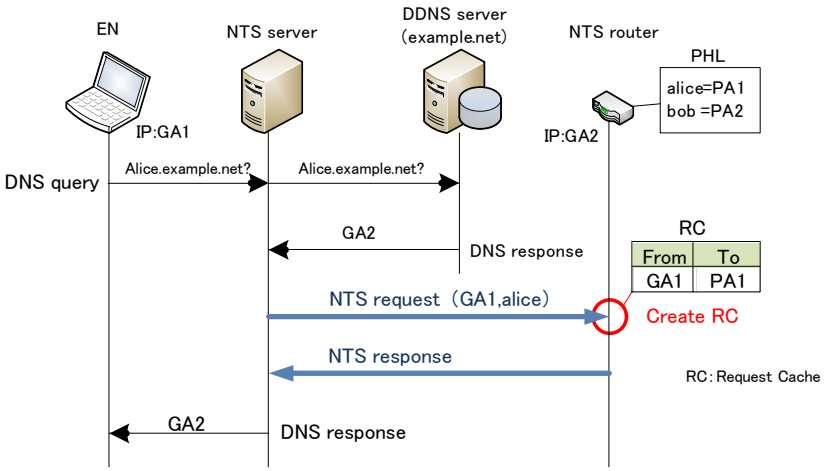

図 3.2　NTSS の名前解決シーケンス

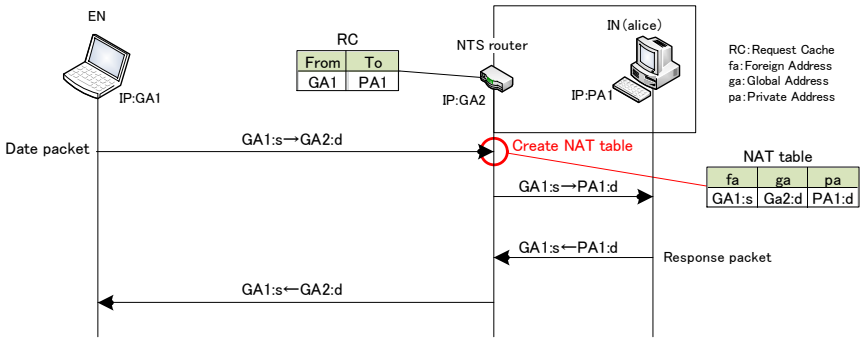

図 3.3　NTSS の通信開始シーケンス

3.4 NTSS の課題

上記の手順により，EN は IN へ NAT を越えて通信を開始することができる．しかし，NTSS を実際のインターネット環境に適用する場合，EN に当たるユーザは，各自で使用するキャッシュサーバの設定を NTS サーバに変更する必要がある．例えば，EN が Windows7 の OS を使用している場合，ネットワーク接続のインターネットプロトコルバージョン 4 のプロパティである図 3.4 の黒枠内に NTS サーバの IP アドレスを直接入力する必要がある．しかし，今後は情報家電やモバイル端末の多様化により，ユーザが故意に設定変更ができない可能性が考えられる．そのため，利用するユーザが限定されるという課題がある．

そもそも，NTSS において EN 側のキャッシュサーバを改造の対象とした理由は，NTS ルータへ “ GA1 から alice へ通信要求がある ” ということを NTS リクエストで通知する時，EN の IP アドレス（GA1）も同時に通知できるためである．しかし，本論文では EN は一般端末であることから登録変更が必要であることは望ましくない．EN の登録変更を不要とするためには，通常利用しているキャッシュサーバを NTS サーバに置き換える方法があるが，この方法は一般ユーザが利用する全てのキャッシュサーバを置き換える必要があり現実的ではない．

そこで，キャッシュサーバではなく権威サーバを改造する方法を考えた．権威サーバはプライベート空間を管理する ISP などの管理者が設置すれば可能である．ただし，DNS の仕組みから，RC の From が不明となり通信の不具合が発生する可能性がある．そのため，これを解決手段が必要となる．これを解決すればあらゆる EN を対象にできるため，応用範囲を広げることができる．

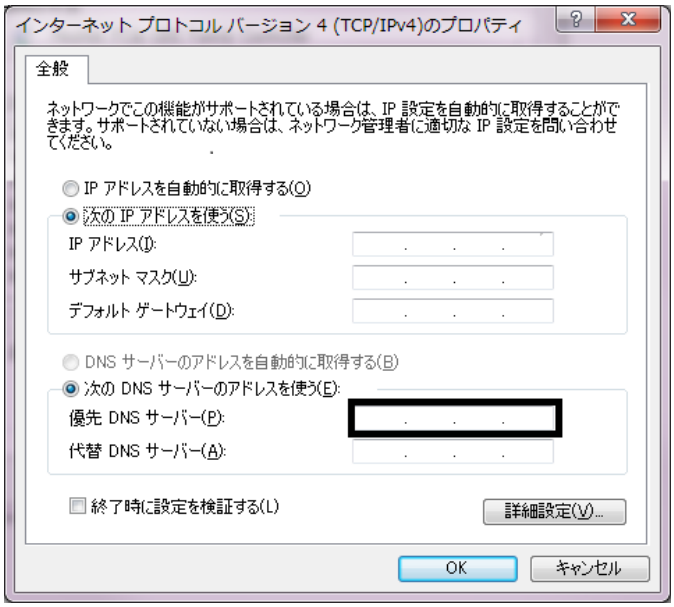

図 3.4　Windows におけるキャッシュサーバの設定

第4章　提案方式

本章では，3.4 節の課題を解決するために，NTSS を実現する構成機器の見直しを行った NTSSv2 を提案する．NTSSv2 では EN のキャッシュサーバは改造せず，代わりに IN 側の権威サーバとなる DDNS を NTSv2 サーバとして改造する．権威サーバはプライベートアドレス側の装置であるため，改造は１ヶ所で良いという利点がある．これに伴い，NTS ルータの処理動作と RC の仕様の見直しを行い，これを NTSv2 ルータと呼ぶ．

4.1　構成と事前設定

図 4.1 に NTSSv2 の構成を示す．NTSv2 サーバは，キャッシュサーバからの反復問合せをトリガとし，NTS サーバと同等の処理を行う．NTSv2 ルータも，処理動作に変更を加えているが，NTS ルータと同等の機能を持つ．そして，EN は既存のキャッシュサーバをそのまま使うので登録変更が不要である．

NTSS と同様に，EN から IN（alice）へ通信開始する場合を例として，名前解決と通信開始時に分けて説明する．事前設定は，キャッシュサーバの登録変更以外 NTSS と同様なので省略する．

4.2　名前解決

図 4.2 に NTSSv2 の名前解決シーケンスを示す．EN はキャッシュサーバに IN の名前解決を依頼する．キャッシュサーバは通常の DNS の仕組みにより，IN の権威サーバとなる NTSv2 サーバを反復問合せにより名前解決を行う．NTSv2 サーバはこの問合せを受け取ると，alice への接続要求を通知するために NTS リクエストを NTSv2 ルータに送信する．この時，NTSv2 サーバが受信する DNS 問合せには，問合せを依頼したノードの情報が含まれていないため，EN の IP アドレスを特定することができない．そのため，NTSv2 サーバが生成する NTS リクエストは，ソースアドレスの情報を無くして宛先の FQDN のみを載せるように変更している．NTSv2 ルータはこれを受け取ると，ソースアドレスである From のエントリ部分を無くし，宛先である To を alice とした RC を生成しておく．この RC は，「誰かからの alice への通信要求」ということであり，不特定の EN からの通信要求に対応するという意味を持つ．RC 生成後は名前解決結果として，EN に NTSv2 ルータのグローバル IP アドレス（GA2）が返信される．

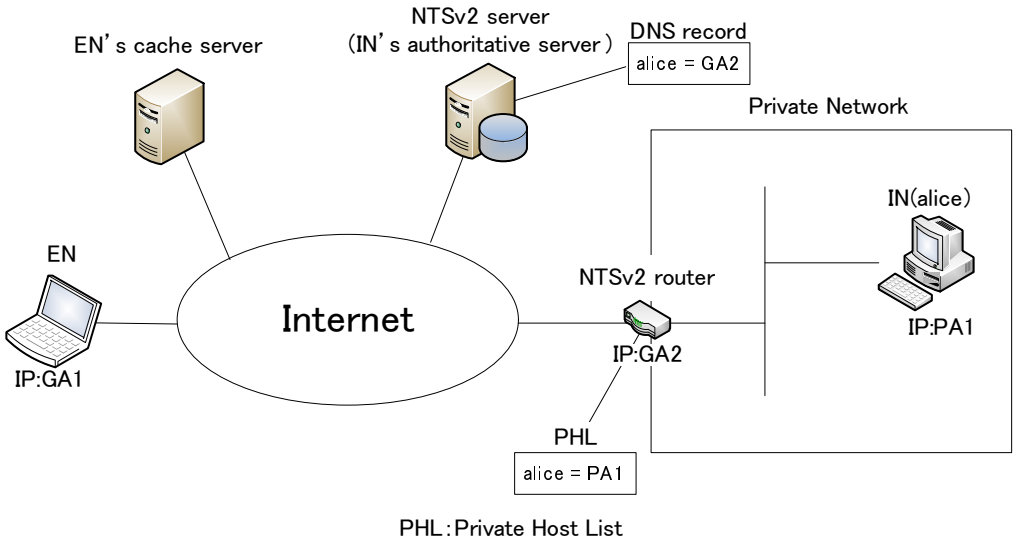

図 4.1　NTSSv2 の構成

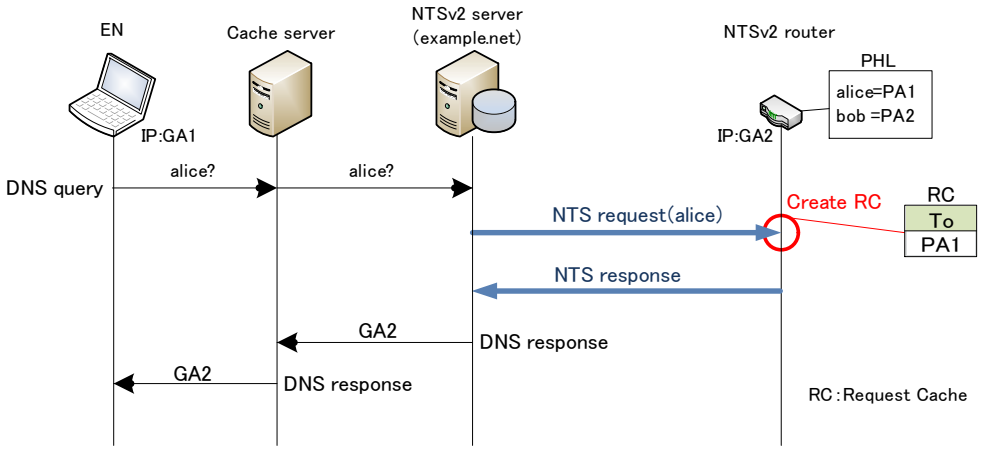

図 4.2　NTSSv2 の名前解決シーケンス

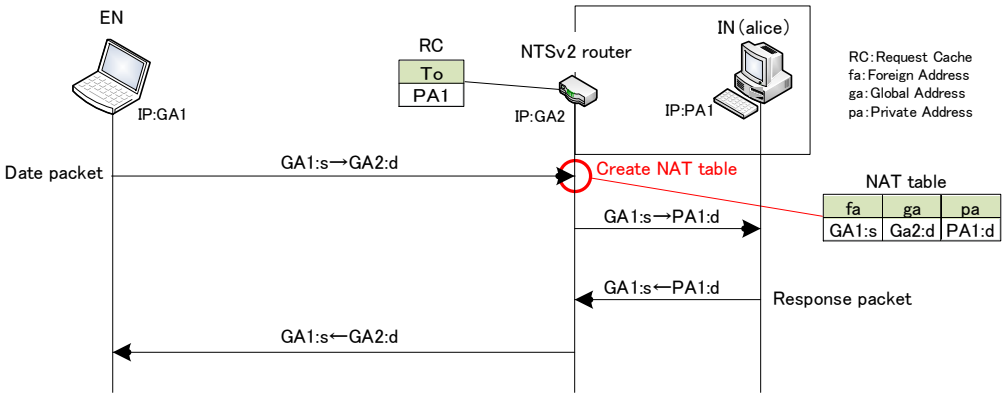

図 4.3　NTSSv2 の通信開始シーケンス

4.3　通信開始

図 4.3 に NTSSv2 の通信開始シーケンスを示す．EN は名前解決後，NTSv2 ルータに向けて通信を開始する．NTSv2 ルータはデータパケットを受け取ると，既に生成されている RC の内容を参照する．ここで，RC の宛先である To が alice となっているため，以下のように

$$GA1 : s \leftrightarrow \{GA2 : d \Leftrightarrow PA1 : d\} \tag{4.1}$$

NTSS と同様の NAT テーブルを生成する．しかし，RC の仕様が変更されているため，その生成方法は NTSS とは異なる．その生成方法とは，NTSv2 ルータは送られてきたパケットのヘッダから送信元 IP アドレスを抽出し，これをソースアドレスとする NAT テーブルをオンデマンドに生成することである．これにより，NTSS と同様にパケットの宛先 IP アドレスが変換されるため，EN は IN に通信を開始することができる．

4.4 権威サーバ改造による影響とその解決策

NTSS ではキャッシュサーバを改造することにより，NTSv2 ルータに EN の IP アドレスを通知することができた．しかし，権威サーバにおいては通常の DNS の仕組み上，NTSv2 ルータに EN の IP アドレスを通知することができない．そのため，NTSv2 ルータはソースアドレスである From のエントリを無くした RC を生成させている．ゆえに，複数の EN が同時問合せした場合と第三者が通信に介入した場合においては，システムが正常に動作しない可能性がある．以下，これらの課題を解決する手法について説明する．

4.4.1 同時問合せ時の動作

同時問合せとは，2 つ以上の EN がほぼ同時に名前解決を開始し，NTSv2 ルータに対して通信開始する場合を示す．この場合，ネットワークの遅延などの影響でパケット到着順が変わると，宛先を誤って NAT テーブルを生成してしまう可能性がある．この問題を解決するために，NTSv2 ルータは以下のように処理をシリアライズする．

図 4.4 に NTSSv2 の同時問合せ時のシーケンスを示す．EN1 が alice，EN2 が bob と通信を行いたい場合を例として説明する．EN1 が名前解決を行うと，NTSv2 ルータに EN1 の NTS リクエストが届く．NTSv2 ルータは alice と “ any を ” 対応付けた RC を生成する．図 3.4 では，直後に EN2 からの問い合わせで EN2 の NTS リクエストが届いているが，NTSv2 ルータはこのリクエストを待機状態とし，RC は生成しない．EN1 からのデータパケットが到着して EN1 のテーブルが完成した時点で EN2 の RC を生成し，NTS レスポンスを返信する．この他の問合せ要求があっても同様に先着順で待機させる．このように，NTSv2 ルータは NTS リクエストを先着順で処理することにより，同時問合せに対応することができる．DNS 問合せに対する処理が遅れる可能性があるが，既に NAT テーブルが生成されている通信には影響しない．

また，DNS 問い合わせが大量に NTSv2 ルータにストックされ，DNS 処理のタイムアウトが発生した場合には，DNS の再送処理により再度問い合わせを行う．DNS の問い合わせが成功した場合，応答できなかった古い NTS リクエストをリフレッシュさせて新しい NTS リクエストとして更新する．失敗した場合は再送処理を繰り返す．これも失敗した場合は，該当する NTS リクエストをすべて削除し，名前解決が失敗する．この時，NTSv2 ルータは名前解決の成否判断としてタイマーを使用するが，再送処理の回数は DNS によって異なるため，実際の利用環境においての最悪値を取る必要がある．

4.4.2 通信の妨害に対する処置

通信の妨害とは，EN1 の通信開始シーケンスに EN2 の通信開始シーケンスが介入する場合を示す．この場合，EN2 のデータパケットが EN1 より先に NTS ルータに到着すると，RC

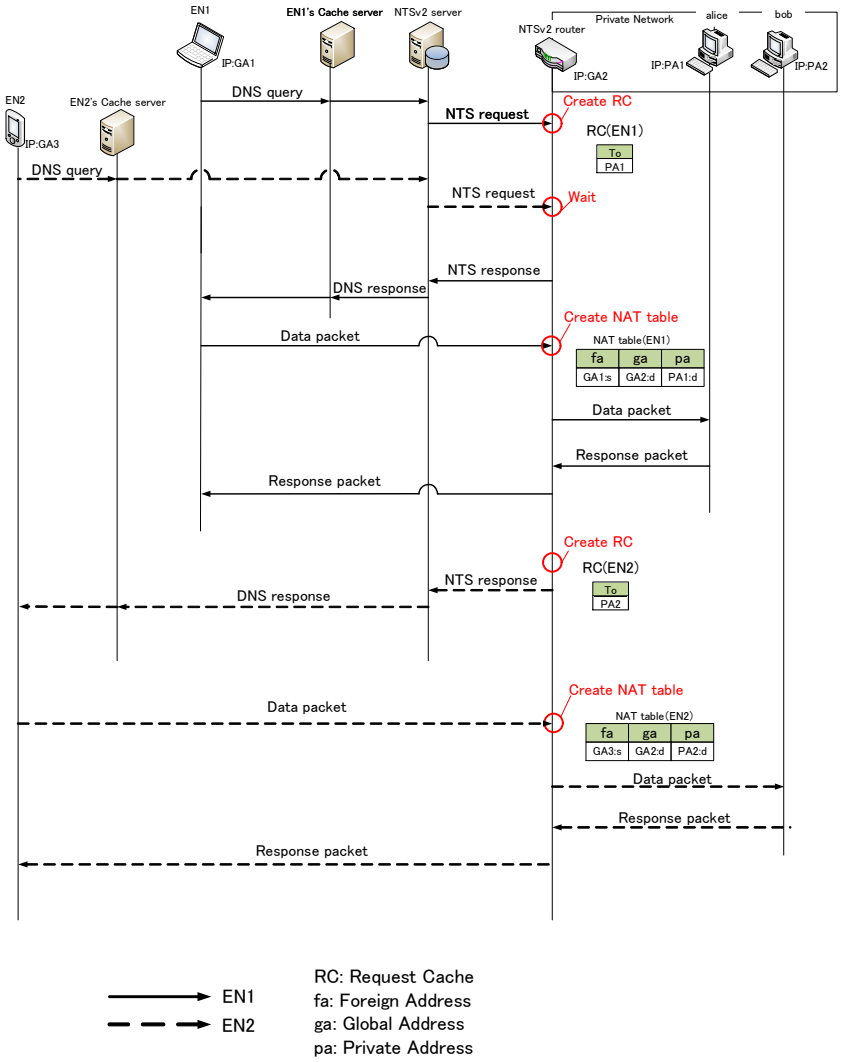

図 4.4　同時問合せ時の動作シーケンス

が削除される可能性がある．これは，NTSS では NAT テーブルを生成した時点で削除していたため発生する．この問題を解決するために，NTSv2 ルータは NAT テーブルを生成した時点で RC を削除せず，所定の時間保持しておくようにした．具体的な数値については 6 章で説明する．

図 4.5 に第三者による通信の妨害を示す．EN1 が alice に通信を行いたい時，第三者である EN2 が通信に介入した場合を例として説明する．EN2 は NTSv2 ルータの IP アドレス（GA2）を既に知っているものとする．EN1 は名前解決により NTSv2 ルータの IP アドレス（GA2）を取得し．NTSv2 ルータにデータパケットを送信する．このとき，図 4.5 のように EN2 は NTSv2 ルータにデータパケットを送信する．NTSv2 ルータはパケットを受け取ると EN1 用，EN2 用の NAT テーブルをそれぞれ生成する．EN1 と EN2 は両者とも NAT を越えて通信することができる．この方法では，EN2 による不正パケットが内部ネットワークに流れることになるが，EN1 による正常な通信が阻害されることはない．

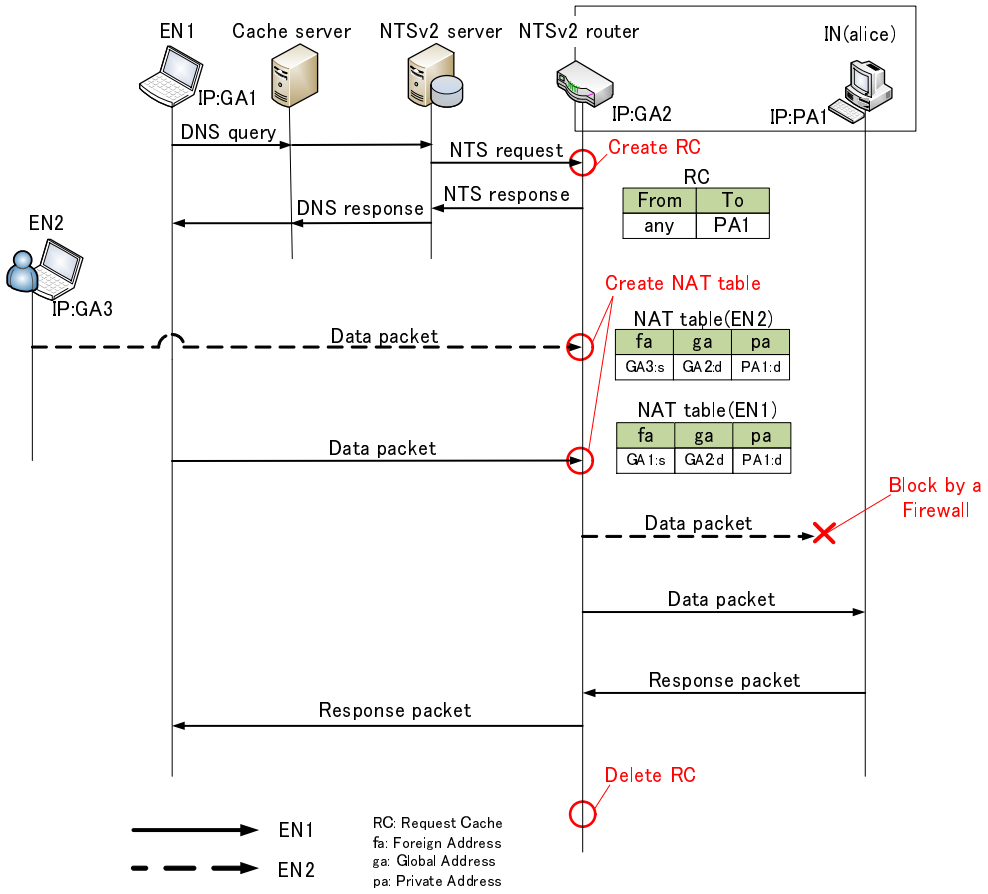

図 4.5　第三者による通信の妨害

NAT はその仕様上，ネットワーク構成が外部ネットワークから見えなくなる性質があるので，NAT をセキュリティ装置として考える場合がある．この観点から見ると図 4.5 に示す方法は，不正なパケットをネットワーク内部に流すことになるため，セキュリティホールになるという指摘がある．しかし，NAT は本来 IPv4 アドレス枯渇に対処するためのものであり，セキュリティは IN の PSW（Personal Firewall）などの別の方法でも確保することができる．また，NAT が存在しないネットワークの場合，不正なパケットは IP アドレスを直接指定して送信することができるため，不正なパケットが送られて来ることは特別な問題ではないとも考えられる．

第5章　実装

5.1　NTSv2サーバの実装

図5.1にNTSv2サーバの実装概要を示す．NTSv2サーバには，DNSアプリケーションであるBINDをインストールし，これを10053番ポートでリッスンするように設定する．代わりに，NTSサーバモジュールを53番ポートでリッスンするように設定する．NTSサーバモジュールは，通常の名前解決処理はBINDに受け渡し，その処理結果を基にNTSルータとネゴシエーションを行う．ネゴシエーションが完了すると，ENのキャッシュサーバに名前解決結果を返す．このような手順により，NTSv2サーバは通常の権威サーバの様に振る舞う．

5.2　NTSv2ルータの実装

図5.2にNTSv2ルータの実装概要を示す．NTSv2ルータは，natd（NATデーモン）と呼ぶNAT機能を持つFreeBSDのデーモンにNTSルータモジュールを内蔵させる．NTSルータモジュールは，divertソケットからパケットを受信すると，送信元IPアドレスと宛先IPアドレスを入れ替えたダミーパケットを生成する．更に，PATテーブルという独自の変換テーブルにより，ポート番号の整合性を解消させ，natdにEN用のNATテーブルを強制的に生成させる．提案方式では異なるENからの同時問合せ時対応するため，処理をシリアライズに行わせる必要がある．そのため，NTSリクエストを保存させるネゴキャッシュを新たに用意する．

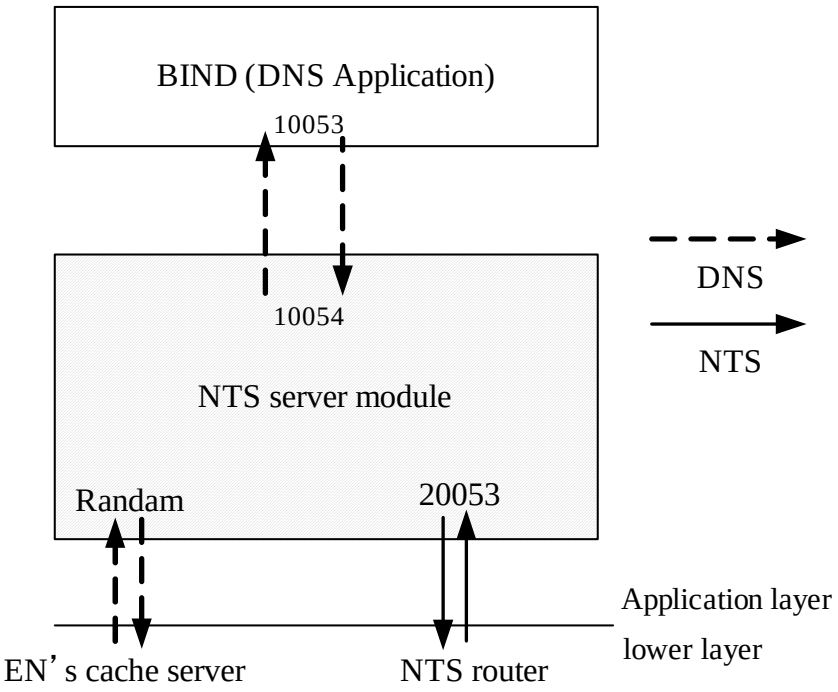

図 5.1　NTSv2 サーバの実装概要

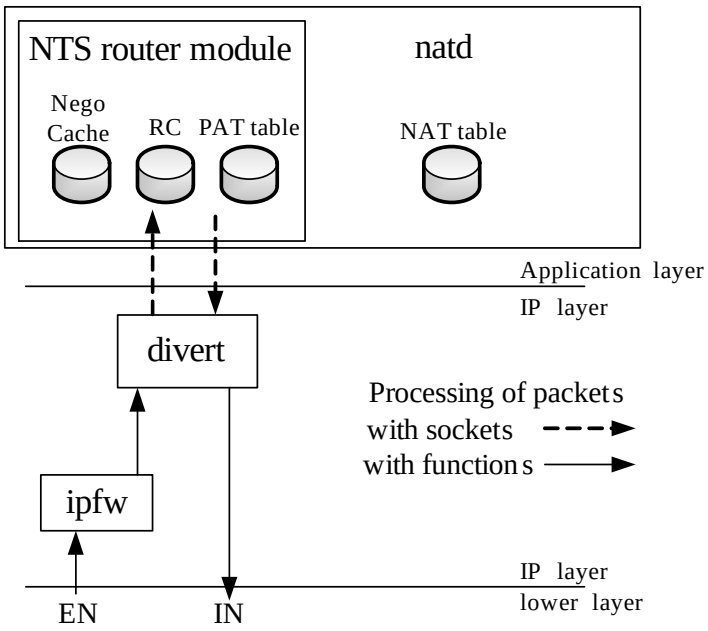

図 5.2　NTSv2 ルータの実装概要

第6章　ルータの負荷予測

NTSv2 ルータの NAT テーブル生成処理をシリアライズしたため，この処理が NTSSv2 のネックになる懸念がある．そこで NTSv2 ルータの負荷予測を行った．この時間と DNS 要求のタイムアウト値から，NTSv2 ルータの処理負荷を予測する．ここでいう NTSv2 ルータの処理負荷とは，NTSv2 ルータが同時にどのくらいの NTS リクエストを待機させることができるかを表す．

図 6.1 に NTSSv2 における DNS 問合せに要する時間を示す．EN と DNS サーバ，および NTSv2 サーバと NTSv2 ルータは通信遅延が無視できるような近隣のネットワークに設置できるものとする．図中のハッチング部分は他のリクエストを処理できないため，1 回のリクエストに対する NTS ルータの処理時間に相当する時間とし，この時間を t とする．また，EN は別々の IN に通信要求を行うものとし，名前解決後に即座に通信開始することを前提とする．

NTSS の測定結果によると，NTSS の処理に要する時間は NTS サーバで 360.2μs，NTS ルータで 265.2μs であった．NTSSv2 では処理内容が大きく変わることがないので，同等の時間を要するものと想定できる．一方，実際のシステムにおいて ping の RTT を測定すると 10ms〜400ms ぐらいである．この値は NTSS の処理時間に比べて大きな値と言える．このようなことから，NTSS の処理時間は無視できる程小さいと考えられるので，t の値は RTT により見積ることができる．つまり，t の値を RC の有効時間とすることができる．これらのことから，DNS タイムアウトをデフォルトの 5s，EN と NTSv2 ルータ間の RTT を 20ms[1]とすると，同時に 250 個までの DNS リクエストを処理できることになる．

実際には，DNS タイムアウト及び RTT は各々の環境により異なるので，正確な性能値を示すことはできない．しかし，RTT は RC の保持時間と見積もることができるため，最悪値をとる必要がある．また，一般ユーザが DNS タイムアウトをデフォルトより低く設定を変える可能性は考えられないため，値はあらかじめ予想できる．そのため，事前に NTS ルータの負荷予測が可能となる．

以上のことから，予めユーザが利用する端末や利用シーンを想定することで，問題なく動作できることが予測できる．

[1]EN が LinuxOS を使用し，EN と NTSv2 ルータが東京-大阪間で 100Mbps の WAN 接続されていることを想定

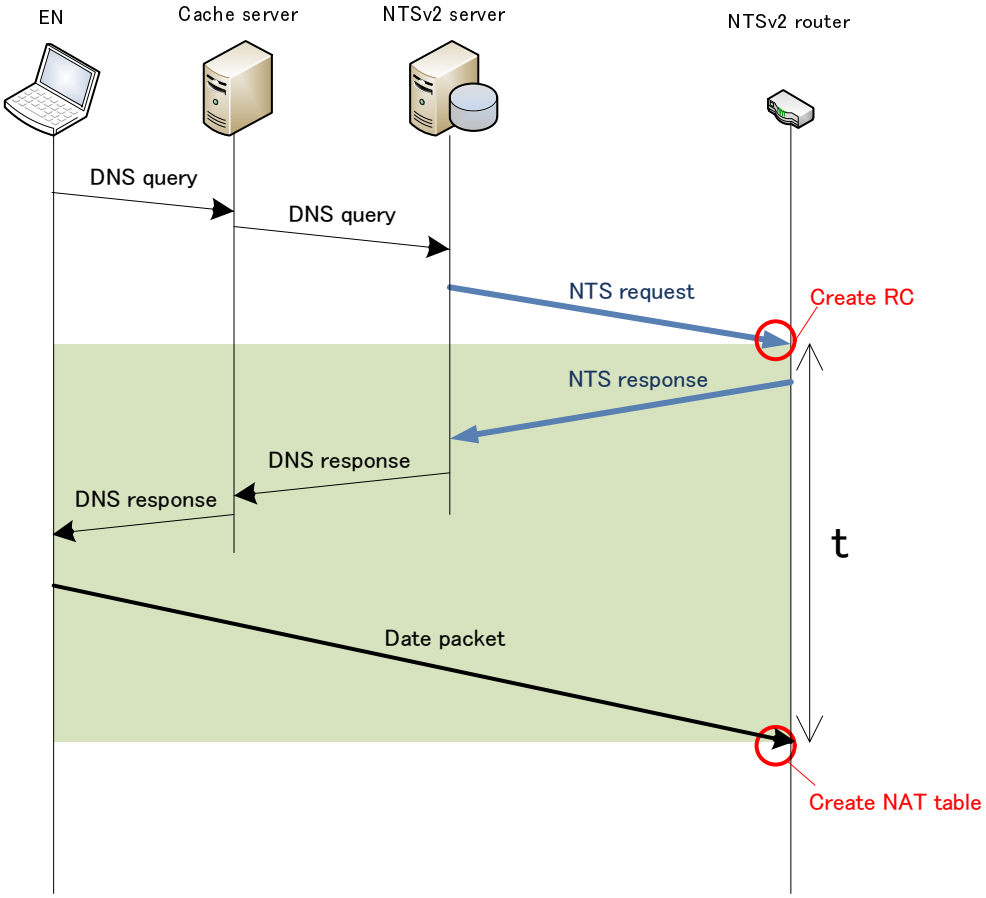

図 6.1　DNS 問合せに要する時間

第7章　まとめ

NTSS は端末の改造が不要であるが，キャッシュサーバの改造や EN の設定の変更が必要であった．そこで，これらの課題を解決するために，IN の権威サーバを NTSv2 サーバとして改造した NTSSv2 を提案した．NTSSv2 サーバが受信する DNS 問合せにはノードの情報が含まれていないため，EN の IP アドレスを特定することができない．そこで，NTSv2 ルータは送信元 IP アドレスを “ any ” とし，これを宛先と対応付けした RC を生成をすることにより，NTSv2 ルータはデータパケットはデータパケットを受け取ると，送られてきたパケットの送信元 IP アドレスを抽出し，それをソースアドレスとする NAT テーブルを生成する．これにより，NTSS と同様の通信を可能とした．また，同時問い合わせや通信の妨害時の動作を再検討することにより課題を解決した．NTSv2 サーバと NTSv2 ルータの実装概要及び処理の流れを示した．また，ルータの負荷予測によって，あらかじめユーザが利用する端末や利用シーンを想定することで，問題なく動作できることが確認できた．今後は，NTSSv2 の実装を完成し評価を行う予定である．

謝辞

本研究に関して，研究の方向や進め方など終始御熱心な御指導とご教示を賜りました，大学院理工学研究科情報工学専攻　渡邊晃教授に心より厚く御礼申し上げます.

本論文を作成するにあたり，快く査読を引き受けてくださり，熱心にご指導を頂きました，大学院理工学研究科情報工学専攻　柳田康幸教授に心より厚く御礼申し上げます.

本研究を進めるにあたり，研究内容に関して終始御熱心な御指導とご教示を賜りました，大学院理工学研究科情報工学専攻　宇佐見庄五准教授に心より厚く御礼申し上げます.

本研究を進めるにあたり，研究内容に関して終始御熱心な御指導とご教示を賜りました，大学院理工学研究科情報工学専攻　鈴木秀和助教に心より厚く御礼申し上げます.

最後に，本研究を行うにあたり，適切なご検討を頂いた，大学院理工学研究科情報工学専攻渡邊研究室並びに鈴木研究室の皆様に心より感謝致します.

参考文献

[1] JPNIC News letter for JPNIC Members, No.48 (2011)
https://www.nic.ad.jp/ja/newsletter/No48/NL48_ all.pdf

[2] K.Egevang and P.Francis: The IP Network Address Translator (NAT), RFC 1631 (1994).

[3] Srisuresh, P. and Holdrege, M.: IP Network Address Translator (NAT), Terminology and Considerations, RFC 2663 (1999).

[4] Nishitani, T. and Miyakawa, S.: Carrier Grade Network Address Translator (NAT) Behavioral Requirements for Unicast UDP, TCP and ICMP, Internet-draft, IETF (2008). draft-nishitani-cgn-00.txt.

[5] Rosenberg, J.,Weinberger, J., Huitema, C. and Mahy, R.: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC 3489, IETF (2003).

[6] Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).

[7] Rosenberg, J., Mahy, R. and Matthews, P.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), Internet- draft, IETF (2009). http://tools.ietf.org/id/draft-ietf-behave-turn-16.txt

[8] UPnP Forum: Internet Gateway Device (IGD) *Italic Standardized Device Control Protocol V 1.0* (2001). http://www.upnp.org/standardizeddcps/igd.asp

[9] Cheshire, S., Krochmal, M. and Sekar, K.: NAT Port Mapping Protocol (NAT-PMP), Internet-draft, IETF (2006). draft-cheshire-nat-pmp-02.txt.

[10] Turanyi, Z., Valko, A. and Campbell, A.: 4+4: An Architecture for Evolving the Internet Address Space Back Toward Transparency,*Italic ACM SIGCOMM Computer Communication Review*, Vol.33, No.5, pp.43-54 (2003).

[11] 鈴木秀和，宇佐見庄五，渡邊　晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌， Vol.48, No.12, pp.3949-3961 (2007).

[12] Kondo, K.: Capsulated Network Address Translation with Sub-Address (C-NATS), Internet-draft, IETF (2003). draft-kuniaki-capsulated-nats-05.txt.

[13] P.Mockapetris: DOMAIN NAMES - CONCEPTS AND FACILITIES, RFC 1034 (1987).

[14] P.Mockapetris: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, RFC1035 (1987).

[15] Ng, T., Stoica, I. and Zhang, H.: A Waypoint Service Approach to Connect Heterogeneous Internet Address Spaces, *Italic Proc. USENIX Annual Technical Conference*, pp.319-332 (2001).

[16] 宮崎悠，鈴木秀和，渡邊晃．端末の改造が不要な NAT 越え通信システム NTSS の提案と評価, 情報処理学会論文誌, Vol. 51, pp.1873-1880, Sep.2010.

[17] Ferguson, P. and Senie, D.: Network Ingress Filtering : Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, IETF (2000).

[18] Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, IETF (1997).

研究業績

学術論文

なし

国内会議（査読あり）

1. 松尾辰也, 鈴木秀和，旭健作，渡邊晃, “端末の変更が一切不要な NAT 越え通信システムの提案”, マルチメディア, 分散, 協調とモバイル (DICOMO2012) シンポジウム論文集，Vol.2012，No.1，pp.1155-1161，Jul.2012.

研究会・大会等

1. 松尾辰也, 鈴木秀和，旭健作，渡邊晃, “プライベートアドレスを持つ無線メッシュネットワークとインターネットの接続方法”, 平成 23 年度電気関係学会東海支部連合大会論文集，Sep.2011.
2. 松尾辰也, 鈴木秀和，旭健作，渡邊晃, “双方向通信が可能な無線メッシュネットワークのインターネット接続方法”, 情報処理学会第 74 回全国大会講演論文集，Mar.2012.
3. 松尾辰也, 鈴木秀和，旭健作，渡邊晃, “端末の変更が一切不要な NAT 越え通信システムの提案”, 情報学ワークショップ 2013（WiNF2013）論文集，WiNF2013，Vol.2013，Dec.2013.

付 録A　セキュリティ対策

提案方式では，不正なパケットも許可することになるため，別にセキュリティ対策を取る必要がある．その方法として，IN に PSW を導入する方法とルータの動的パケットフィルタリングを利用する方法が考えられる．

A.1　PSW を導入する方法

PSW とは，インターネットの外部から侵入してくるウイルス (ワーム) やクラッカーをシャットアウトするソフトウェアことである．昔は企業向けの高価な製品が主流であったが，現在ではブロードバンドで常時接続するユーザが増えたため、機能を限定して低価格にした個人向けの製品が増加している．そのため，ユーザが比較的導入しやすいセキュリティ製品の 1 つだと言える．

PSW の種類としては，PSW 単体の製品と統合セキュリティソフトウェアに組み込まれている製品がある．これらは，各ユーザがインストールすることで利用できる．また，OS に組み込まれている製品もあり，これは設定を有効にするだけで利用できる．

PSW の機能は，送受信されるパケットを監視して不正なパケットを遮断することである．これは IN 上で処理されるということから，提案方式との共用は可能であると考えられる．しかし，情報家電などの場合はインストールすることが困難なため，利用できないという問題がある．

A.2　動的パケットフィルタリングを利用する方法

ルータにおいて，通信セッションの状態を記録し，その中から不正なパケットを遮断する方法である．これを動的パケットフィルタリングと呼ぶ．一般的な NAT では、通過させるか遮断させるかをポート番号のみで判断しているため，第三者により通信妨害を受ける可能性がある．提案方式においても同様となるため，別にフィルタリング機能が必要となる．そこで，動的フィルタリングは通信セッションの状態をフィルタリングテーブルという独自のテーブルに記録しているため，その内容から不正なパケットを動的に遮断することができる．しかし，最初は動的パケットフィルタリングは外側から内側の通信を完全に遮断されているため，これを回避できるように設定する必要がある．