ネットワーク空間を意識しない通信方式の研究

加藤　尚樹　　渡邊　晃

ブロードバンドの普及により一般家庭においても複数台の端末によるインターネットが標準的にとなり, モバイル機器の発達によりいつでもどこでも通信を行えるようになった. これに伴い, 外出先から家庭内ネットワークにアクセスを行いたいというニーズが増えてきたが，IP アドレスの不足，セキュリティの面から NAT が介在するのが標準的であり，これによって通信することができない場合がある．そこで本稿では，DNS によって家庭内ネットワーク上の端末を検知し，ポート変換によって上記の問題を解決する方式を提案する．本方式では通信開始時にのみポートを変換し，その後の通信に影響を与えないことを可能とする．

Research of a communication system which is not conscious of network space

Naoki　Kato　and　Akira Watanabe

It became common to perform the Internet at general home using plural terminals. On the other hand, It can communicate now always anywhere by development of mobile apparatus. Consequently, the needs of wanting to access a domestic network from a going-out place have increased. However, it is standard that NAT intervenes from shortage of an IP address and the field of security, and it may be unable to communicate by this. Then, the terminal on a domestic network is detected by DNS, and the system which solves the above-mentioned problem by port conversion is proposed. By this system, a port is changed only at the time of a communication start, and it makes it possible not to affect subsequent communication.

1. はじめに

ADSL をはじめとするブロードバンドの普及により高速で快適なインターネット通信を行うことができるようになった．また，機器コストの低下により一般家庭においても，複数台の PC を利用するようになり，家庭内で LAN を形成している．よって、現在は家庭内 LAN をインターネットへ接続し，一般家庭においても複数台の端末で快適なインターネット通信を行えるようになった.

しかしその反面, 近年増加するネットワーク犯罪の脅威に家庭内ネットワークがさらされているのが現状である．そこで，我々は家庭内ネットワークを管理し, 外部からの攻撃から守る Home Fire Wall(以下 HFW)の設置を検討している．HFW の機能は，外部からの攻撃を防ぐパーソナルファイアーウォール機能, 接続時に自動的に IP アドレスを与える DHCP 機能、各端末にホスト名を割り当て, 端末が移動した際に更新を行うことのできる Dynamic Domain Name System (以下 DDNS)機能，そして、外部から接続可能なルーティング機能などが上げられる. これらの機能のうちパーソナルファイアーウォール，DHCP，DDNS においては既存技術を用いることによって解決が出来る. しかし外部から接続可能なルーティング機能は既存技術である NAPT(Network Address Ports Translator)では実現していない.

現在、グローバル IP アドレスが枯渇しているため，ISP から配られるグローバル IP アドレスは１つである．よって，直接複数台の PC をインターネットに接続することは不可能で

ある．しかし，NAPT を用いることで家庭内ネットワークの複数の端末からインターネットへの接続を 1 つのグローバル IP アドレスで可能としている．また，NPAT を用いた場合，グローバル IP アドレスを 1 つしか持たないことからインターネット側からは見かけ上 1 台しかないように見えるため, 家庭内のネットワーク構成を隠蔽することができる．よって，NAPT はセキュリティ対策としても幅広く利用されており，IPv6 が普及して IP アドレスの枯渇が解消されたとしても今後も使われる技術である．

NAPT の介在するネットワークにおいては，家庭内ネットワーク（以下プライベートネットワーク）の端末から，インターネットに通信を行うために，NAPT で IP アドレスを NAPT の持つグローバル IP アドレスに変換し，通信を行う．しかし，プライベート IP アドレスを用いてインターネットで通信を行うことができないため, インターネットからプライベートネットワーク内の端末にインターネットからアクセスを行うことはできない．

この問題を解決するために NAPT はポートフォワードと呼ばれる機能を持っている. これはあらかじめポート番号とプライベート IP アドレスを 1 つの組としてパケット転送テーブルを作成し, インターネットからパケットが送られてきた場合, そのテーブルをもとにしてパケットをプライベートネットワーク内の端末に転送する機能である．しかし，ポートフォワード機能ではひとつのポート番号に対して，1 台の端末しかテーブルを作成することができない．よって，ひとつのグローバル IP アドレスを用いて通常の 80 番ポートを利用して 2 台以上の WEB サーバを立てるといったことや，Telnet によってプライベートネットワーク内の端末にアクセスできないなど、複数のプライベートネットワークの端末と通信できないのが問題である．

また NAT の拡張として NATS(Network Address Translator with Sub-address)が提案されている．これは IP ヘッダの前にもう 1 つ IP ヘッドをつけることによって IP in IP のカプセルかを行うことで，通信を行う．この際，プライベート IP アドレスとグローバル IP アドレスを組としてサブアドレスと呼ばれる識別子を用いてアドレス表記を行っている. サブアドレスは IP アドレスを模しており，非対応機器があったとしても通信が可能となっている. しかし，その動作は DNS シーケンスが複雑化や IP in IP のカプセル化などオーバーヘッドが大きくなるのが課題である．

本稿においてはこれらの問題を解決するため DNS 問い合わせ時に NAT に対してパケット転送テーブルを作成し, それと同時にクライアントでポート番号を変換することによって通信を可能とする方式を提案する．

2. NAPT における課題

2.1. 動作

NAPT はプライベートネットワーク内の端末がインターネットの端末にアクセスすること可能とする. プライベートネットワークに属する PC1 がインターネットに存在する PC2 に対してアクセスを行う際の NAPT の動作を図 1 に示す．

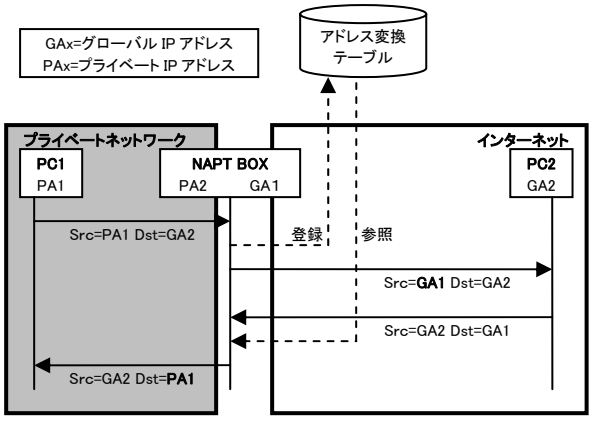

図 1　NAPTの動作
Fig 1　operation of NAPT.

はじめに PC 1 は送信元を自分の IP である『PA1』，宛先を PC2 の IP である『GA2』としてパケットを送信する．このパケットは NAT を通過する際, 宛先 IP を NAT 自身の持つグローバル IP である『GA1』へと変換する．それと同時にアドレス変換テーブルを生成する．

PC2 がパケットを受信し, その応答パケットが返される場合, 受信したパケットに含まれる送信元 IP を参照して応答パケットの宛先 IP が決定される．よって，応答パケットは宛先 IP を『GA2』として送信される．

応答パケットを NAT が受信するとアドレス変換テーブルをもとに宛先 IP が『GA2』から『PA1』へと変換されて転送されるので，パケットは正しく PC1 へと送信され通信を行うことができる．

2.2. 課題

NAPT における課題はインターネット側からプライベートネットワーク側の端末にアクセスが不可能なことである. アクセスが不可能

になる理由として２つ挙げられる.

まず 1 つはインターネットにおいてプライベート IP を指定することが不可能な点である. プライベート IP はプライベートネットワーク内においてプライベートネットワーク管理者が任意で与えた IP アドレスであり，インターネットでは使用することができないので, インターネット上をプライベート IP に当たる値を用いたパケットが流された場合, 破棄されるためである.

もう１つはアドレス変換テーブルが生成されていないためパケットの転送先がわからないためパケットが破棄される点である. これは何らかの方法によって NAPT のグローバル IP アドレスを知り, NAPT に対してパケットが送信できた場合, NAPT のアドレス変換テーブルが登録されていないため宛先がわからないためである．(図２).

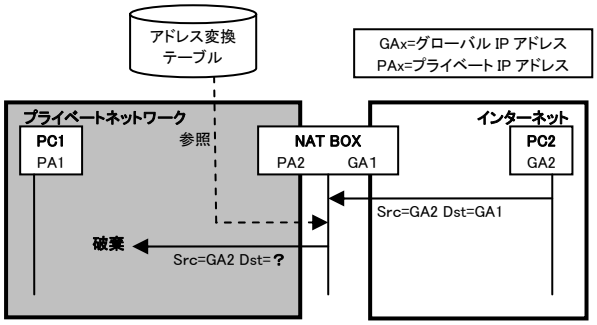

図 2 NAPT における問題点
Fig 2 The problem in NAPT

3. 従来の解決方法とその問題点

3.1. ポートフォワード

ポートフォワードは NAT の機能の１つであり, あらかじめアドレス変換テーブルを設定しておき, それに基づいてパケットを転送させる方式である. 図 3 は 80 番ポートと 53 番ポートについて静的にアドレス変換テーブルを設定した場合のパケットの流れを示している. NAT に対して 80 番ポートに送信されたパケットはアドレス変換テーブルにより『PA１』のアドレスを持つ PC1 へと転送される．同様にして 53 番ポートに送信されたパケットは PC3 へと転送される. しかしこの機能では 1 つのポートに対して 1 台しか設定することができないという課題を持つ.

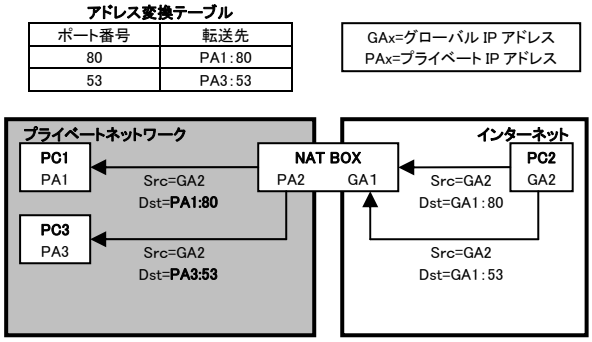

図 3 ポートフォワード機能によるパケットの流れ
Fig 3 The flow of the packet by the port forward function

3.2. NATS

ポートフォワードでは 1 つのポートに対して 1 台しか設定することができない. この問題を解決するため NATS(Network Address Translation with Sub-Address)[1]が提案されている．NATS では，サブアドレスいう識別子を用いて通信を行う. サブアドレスはプライベートネットワーク内の端末でもインターネットから識別できるため通信が可能である.

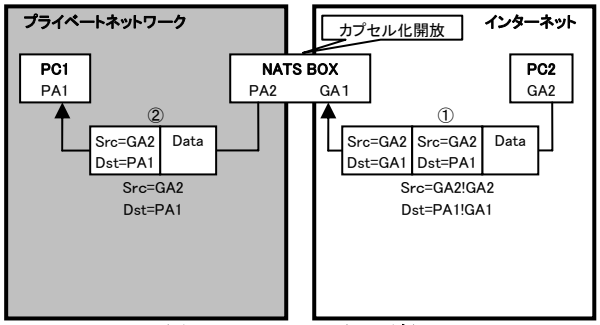

図 4 NATS における通信
Fig 4 Communication in NATS

3.2.1. サブアドレス

サブアドレスは“プライベート IP！グローバル IP”の形で示される．これはサブアドレスが用いられている NATS 対応機器間において IP in IP のカプセル化が行われているためである.『！』の前者に書かれる IP はプライベートネットワーク内で用いられるプライベートネットワーク内の端末の IP アドレスであり，NATS BOX によってカプセル化の開放が行われた後, 通常の IP ヘッダとして用いられる. 後者に書かれる IP アドレスはカプセル化の際, 外側のヘッダにつけられるもので, インターネット上での IP アドレスを意味する.

3.2.2. NATS によるパケットの流れ

図４は NATS を用いた端末 PC2 から NATS BOX を通過しプライベートネットワーク上に

ある NATS に対応していない PC1 にパケットを送信する様子である．まず PC2 は送信元アドレスとしてサブアドレス『GA2!GA2』，宛先アドレスとしてサブアドレス『GA1!PA1』を設定してパケットを送信する. このパケットはサブアドレスによって IP in IP のカプセル化が行われる．よって送信元 IP アドレスが『GA2』，宛先 IP アドレスが『GA1』として送信される(同①)．次にこのパケットが NATS BOX に受信されるとカプセル化の開放が行われる. 開放された後のパケットは通常の IP パケットとなり，送信元 IP アドレスが『GA2』，宛先 IP アドレスが『PA１』のパケットとして PA1 の IP アドレスを持つ PC1 へと正しく送信される(同②)．このパケットの応答パケットの宛先 IP アドレスは GA2 になるので応答も正しく行われる．

3.2.3. NATS における課題

NATS における課題は，NATS を介した通信が行われるたび IP in IP のカプセル化が行われるため，パケットの冗長，また処理にかかるオーバーヘッドなどがあげられる．また，非対応機器が存在する場合においても NAT を介して通信を可能とするために，NATS 常に DNS パケットを監視，及び変換を行っているため，この処理によるオーバーヘッドの増加，DNS の遅延なども懸念される．

4. 提案システム

4.1. 概要

前章でも述べたとおりインターネットから NAT の介在するプライベートネットワークに対してアクセスができないのはプライベートネットワーク内に存在する端末が認識できないからである．よって，本提案方式においては DNS を利用してプライベートネットワーク内の端末を検知する．DNS のレコードとしてポート変換フラグレコードを新たに定義する. このレコードが OFF の場合は通常の DNS として処理されるが，ON の場合，続いて NAT の IP アドレスを検索し，そのアドレスを DNS の応答として返答する．同時に NAT に対して DNS レコードと問い合わせのあったプライベート IP と受信パケットの送信元 IP からアドレス変換テーブルを生成するよう要求を出す.

次に，DNS の返答を受け取ったクライアントでは, 通信開始に送られるパケットの送信元ポート番号を DNS 問い合わせ時に用いた送信元ポート番号に変換し送信する．送信先は DNS によって変換された NAT のアドレスとなっている.

NAT に届いたパケットは，DNS からのテーブル生成要求によって生成されたテーブルに基づいて転送される．このとき，生成されたテーブルの条件とクライアントでポート番号変換を行ったパケットは一致するので目的の端末へ転送することができる. パケットを転送した後，このテーブルは即座に破棄される.

パケットを受信した端末はアプリケーションによる処理を終えた後, 応答パケットとして送信される．このパケットは通常の NAT と同様にしてクライアントへと転送される.

応答パケットを受信したクライアントでは送信時に行われたポート変換処理を元に戻す. このようにすることによってアプリケーションは送信時と同じポート番号でパケットを受け取ることができ，正しい通信が行われる.

4.2. ポート変換フラグレコード

このレコードは, クライアントでのポート変換処理及び，NAT に対してアドレス変換テーブルの生成要求を行うかどうかのフラグを設定するレコードであり，対象のレコードの IP アドレスによって決定される．IP アドレスがプライベート IP である場合，本提案方式を用いて処理を行う必要があるため, このフラグを ON とする．グローバル IP であった場合は，通常通りに通信ができる端末であるため OFF とする.

また，本提案方式では，アドレス変換テーブル生成要求を NAT に対して送る必要があるため，NAT のグローバル IP を知る必要がある．これを判別するため，NAT のレコードに対して設定を R とする．（表１）.

フラグの表記	レコードに書かれる IP	フラグの内容
ON	プライベート IP	クライアントにポート変換を要求する
OFF	グローバル IP	通常の DNS の応答を行う
R	NAT グローバル IP	NAT ルータを示す

表 1 ポート変換フラグレコード
Table 1 Port conversion flag record

4.3. システム構成と実際の処理

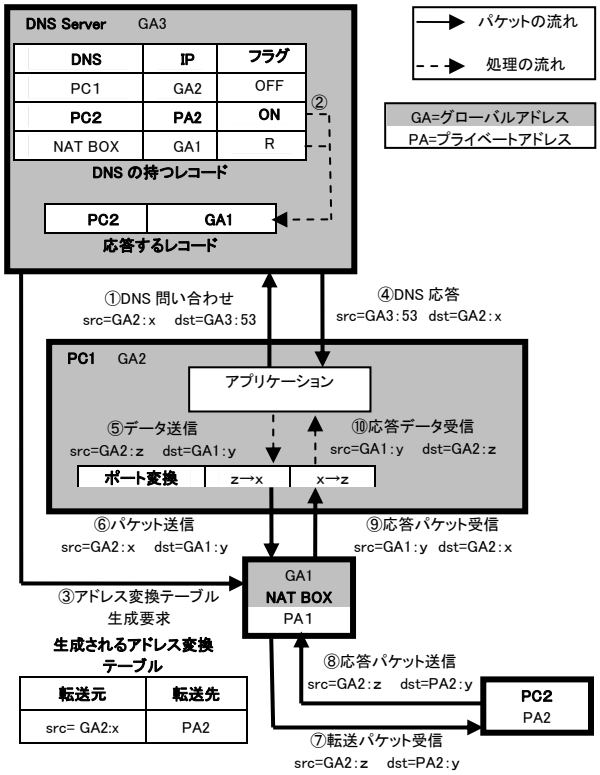

図 5 提案システムの構成と処理の流れ
Fig 5 The composition of a proposal system, and the flow of processing

図５に提案システムのシステム構成と PC1 から PC2 へ通信を開始する場合の処理の流れを示す．灰色で示された端末 DNS Server,PC2 はインターネット上に存在するものでグローバル IP アドレスがそれぞれ『GA3』『GA2』に割り当てられている．白色で示された端末 PC2 はプライベートネットワーク上に存在し，プライベート IP『PA2』が割り当てられている．NAT BOX はルータであり，グローバル IP として『GA1』が，プライベート IP として『PA１』が割り当てられている．

また，実線の矢印はパケットの流れを示し，破線の矢印は端末内における処理の流れを示す．

はじめに PC１は通信を開始するに当たって DNS サーバに対し，名前解決のために DNS 問い合わせを行う(同①).

DNS サーバは問い合わせ内容である PC2 のレコードを検索する．PC２のポート書き換えフラグは ON であるので，次にフラグが R であるレコードを検索し，その結果である IP アドレス『GA1』に変換を行って DNS 応答レコードを生成する（同②）.

以上のことが行われると同時に，ポート書き換えフラグのうち，『R』を持つ NAT BOX に対してアドレス変換テーブルの生成を情報とともに送信する（同③）．これを受信した NAT BOX では，受信した情報を元にテーブルを生成する．その後②で生成された DNS 応答レコードは PC1 に送信される(同④).

PC1 においてはアプリケーションよりデータパケットが送信される(同⑤)．このとき送信されたパケットの送信元ポート番号『ｚ』を DNS 問い合わせ時に使用した送信元ポート番号『ｘ』へと変換を行い，送信する(同⑥).

送信されたパケットを NAT BOX が受信すると④の要求によって生成されたテーブルによって宛先 IP アドレスを GA2 から PA1 へと変換され，PC２へ転送される(同⑦)．このパケットが転送された直後，生成されたテーブルはパケットの誤転送を防ぐため，即座に破棄される．

PC2 で⑦のパケットが受信されるとアプリケーションによって処理が行われ応答パケットが送信される（同⑧）.

応答パケットを受信した NAT BOX では通常の NAT と同様にしてテーブルを生成し，パケットの送信元 IP を『GA1』へと変換し，PC1 へと転送する(同⑨).

NAT によって転送された応答パケットは PC1 に受信される(同⑨)．受信されたパケットは送信時とは逆に宛先ポート番号『ｘ』を『ｚ』へ変換され，アプリケーションに渡される．アプリケーションの受け取るパケットは通常の通信と同様のパケットを受けるとることになるので正しく処理される．

これ以後の通信は⑧のパケットが通過することよって生成されたアドレス変換テーブルが存在するため，通常の NAT と同様に通信することができる．

5. 比較

既存技術と提案方式の比較を表 2 にまとめる．

	ポート フォワード	NATS	提案方式
複数台でアクセス可能か？	×	○	○
DNS の特殊性	なし	レコードの追加	レコードの追加
DNS シーケンス	-	×	△
ポート変換の有無	必要	不要	必要
特定ポートの有無	不要	必要	不要
ネットワークの柔軟さ	×	○	△

表 2 既存技術との比較
Table 2 Comparison with the existing technology

ポートフォワードでは複数台することはできないが，NATS，及び提案方式では可能である．

DNS レコードは NATS では HINFO と呼ばれるサブアドレス用のレコードの追加があり，提案方式ではポート変換フラグレコードを追加している．HINFO は通信をする端末の組み合わせの数だけレコードが存在するのに対して，ポート変換フラグレコードは端末の数だけ登録すればよいのでレコード数は少なくてすむ．また書き換え頻度は，HIFO のほうは機器が 1 つ移動するとサブアドレスが組み合わせの数だけ変更されるため，ポート変換フラグテーブルよりも多くなる．

DNS シーケンスについては NATS が DNS フックを行うため DNS に関するパケットをすべて監視，必要に応じて変換を行っているのに対し，提案方式は通信開始時にのみ特殊な処理を行えばよいので，提案方式のほうがオーバヘッドは少ないといえる．

ポート変換は提案方式では行われるが，NATS では必要がない．しかし，送信元のポート番号は応答パケットを送り返すためだけのものであり，通信にそれほど影響を与えるものではない．また，応答パケット受信時にクライアント側で元のポート番号に戻すことからクライアント側での問題はない．また，ポート変換を行うのは 1 だけなのでオーバーヘッド大きくない．

NATS においては NATS 機器間でサブアドレス情報をやり取りするため，UDP のポートを使用する．これは FW が存在するネットワークにおいて，ポートあけなくてはならず，セキュリティ面からデメリットである．提案方式では DNS を用いて情報をやり取りするため特殊なポートは必要としない．

ネットワークの柔軟性は DNS フッキングによって非対応機器までサポートする NATS のほうが高いといえる．しかし家庭内ネットワークなど，小規模なネットワークにおいてはネットワーク管理者の管理する DNS で十分カバーできると考えられるため本提案方式は有効である．

6. むすび

本稿ではポート番号の書き換えによる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方法を提案し，その動作方法について示した．また，既存技術による解決方法と比較しその有効性についても考察した．これにより既存システムに改良を加えることのみでインターネットからのアクセスを可能とすることができる．今後は提案方式を実装し，その有効性を確認する．また，本提案方式では DNS の情報が重要なものとなってくるため，そのセキュリティについても考える必要がある．

参 考 文 献

[1] 近藤 邦昭：Capsulated Network Address Translation with Sub-Address(C-NATS), http://www.nats-project.org/index-j.html

[2] 近藤 邦昭：Capsulated-NATS, http://www.nats-project.org/presentations/Capsulated-NATS-Overview.pdf

[3] 近藤 邦昭：NATS Address Translation Practice, http://www.nats-project.org/presentations/NATS_Address_Translation_Practice.pdf

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

[6] W. Simpson： IP in IP Tunneling, RFC 1853

[7] K. Egevang： The IP Network Address Translator (NAT), RFC 1631

[8] P. Srisuresh： NAT Terminology and Considerations,RFC 2663

[9] 竹下隆史／村山公保／荒井 透／苅田幸雄：マスタリング TCP/IP, オーム社、2002 年