NAT-fを利用したSIPのNAT越え通信の検討

三　浦　健　吉

いつでもどこからでもネットワークにアクセスできるユビキタスネットワークの需要が広まっている．ユビキタスネットワークでは，個人同士の通信が重要になるため，IP 電話や情報家電などで利用される SIP が注目されている．ホームネットワークは一般にプライベートアドレスで構築されるため，インターネット側の外部ノードからホームネットワーク内の内部ノードに対して通信を開始できないという NAT 越え問題が存在する．我々は，外部ノードと NAT ルータが連携することにより，NAT 越え問題解決する NAT-f（NAT-free protocol）を提案している．しかし，現在の NAT-f は SIP（Session Initiation Protocol）に対応できないという課題があった．そこで本論では，この NAT-f を利用し，SIP の NAT 越えを実現する手法について検討する．

"Researches on NAT traversal for SIP utilizing NAT-f"

Kenkichi Miura

The demand of ubiquitous network that can be accessed from henever and anywhere is spreading. In the ubiquitous network, a communication of the individual becomes important. Therefore, SIP used by the Internet protocol telephone and information appliances is paid to attention. In general, a communication cannot start from a node on the Internet side to a node in the home network because the home network is constructed with private addresses. This problem called the NAT traversal problem. We have proposed NAT-f protocol that modifies the NAT router and the external node to solves the problem. However, NAT-f cannot handle SIP(Session Initiation Protocol). In this paper, We propose the NAT traversal for SIP utilizing NAT-f.

1. はじめに

IPv4 ネットワークでは IP アドレスの枯渇を回避するため，家庭内や企業内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である．それらのネットワークとインターネットの間には NAT(Network Address Translator) が必要である．しかし，このような環境ではインターネット側の端末からプライベートアドレス空間の内部が見えなくなるため，NAT 外側の端末から内側の端末へ通信を開始することができないという制約がある．これは NAT 越え問題と呼ばれている．これまでのインターネットの利用形態は WWW 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空間に存在する端末側から通信を開始していた．ファイアウォールでもこのような通信形態のみを許可するのが一般的であったため，NAT の制約が表面化することはなかった．しかし，今後は家庭にもネットワークが導入されるようになり，外出先から家庭内の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る．このため IPv4 ネットワークにおいて NAT 越え問題を解決することは有益である．

我々は，外部ノードと NAT ルータが連携することにより，NAT 越え問題を解決する NAT-f（NAT-free protocol）[1] を提案している．しかし，NAT-f は，今後，IP 電話や情報家電で多く使用されると考えられているシグナリングプロトコルである SIP（Session Initiation Protocol）[2] に対応できないという課題があった．そこで本論文では，NAT-f を利用した SIP の NAT 越え手法について提案する．

以降，第 2 章で SIP と SIP における NAT 越え問題について説明する．第 3 章で SIP の NAT 越えを実現する既存技術について簡単に説明する．第 4 章で NAT-f の動作について説明し，第 5 章で提案方式について説明する．そして第 6 章でまとめる．

2. SIP

2 台の UA（User Agent）が 2 台の SIP Proxy を経由してシグナリングを行う場合について述べる．

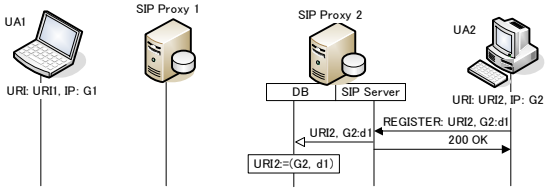

図 1 端末情報の登録シーケンス

2.1 端末情報の登録

図 1 に SIP サーバに対する端末情報登録時のシーケンスを示す．UA2 は SIP Proxy 2 に対して REGISTER により自身の URI（Uniform Resource Identifier）である URI2 と SIP メッセージを受信する際に使用するトランスポートアドレス G2:d1 の登録を要求する．SIP Proxy 2 は受信した URI とトランスポートアドレスを DB（Data Base）に登録し，UA2 に対して正常応答を意味する 200 OK を返答する．

2.2 動 作 概 要

2.2.1 SIP の基本シーケンス

図 2 に SIP の基本シーケンスを示す．通信開始時，UA1 は INVITE により UA2 とのセッションの確立を要求する．INVITE には，UA2 とのセッションを確立する際に UA1 が使用するトランスポートアドレス G1:s2 が記載されており，SIP Proxy 1 を中継し，SIP Proxy 2 に転送される．SIP Proxy 2 は，URI2 の名前解決を行い，INVITE を UA2 へ転送する．INVITE を受信した UA2 は，200 OK を返答する．200 OK には，UA2 が使用するトランスポートアドレス G2:d2 が記載されており，2 台の SIP Proxy を経由して UA1 まで転送される．UA1 は ACK を返答した後，交換したトランスポートアドレスを用いて，UA2 と直接メディアセッションを確立する．

セッション終了時は，セッション切断要求を意味する BYE とそれに対する正常応答 200 OK によってセッションが切断される．

2.2.2 IP 電話のシーケンス

2 台の UA がそれぞれ IP 電話であった場合，シーケンス図は**図 3** に示すようになる．SIP Proxy 1 は INVITE を転送すると，UA1 に対して暫定応答を意味する 100 Trying を返答する．SIP Proxy 2 も同様に，INVITE を転送すると，SIP Proxy 2 に対して 100 Trying を返答する．

UA2 は INVITE を受信すると，電話のベルを鳴らし，同時に，UA1 に対して呼出し中であることを伝えるため，180 Ringing を返答する．180 Ringing は 2 台の SIP Server を経由し，UA1 まで到着する．

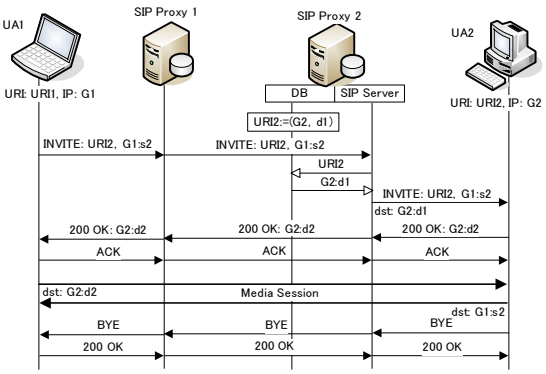

図 2 SIP の基本シーケンス

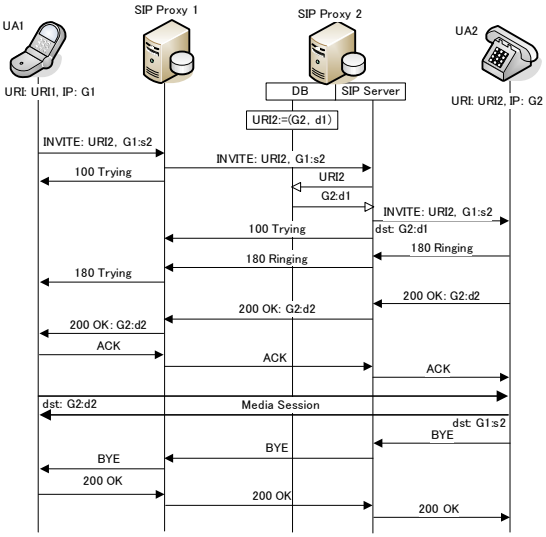

図 3 IP 電話のシーケンス

UA2 は受話器を持ち上げられると同時に，200 OK を送信する．

以後の処理については 2.2.1 と同様である．

2.3 SIP における NAT 越え問題

NAT が存在する環境で SIP を使用する場合，以下の 2 つの問題がある．1 つは，通常の NAT 越え問題に係るもので，NAT の外部から内部に向けてシグナリングを開始できないことである．もう 1 つは，SIP は IP ペイロード内に IP アドレスが埋め込まれるため，NAT を通過すると IP ヘッダ内の IP アドレスとの間で IP アドレスの不整合が生じる．

2.3.1 端末情報登録時に生じる問題

図 4 に UA が NAT 配下にある場合に発生する問題を示す．なお，破線で示されているのは失敗時の動作である．UA2 は NAT 配下にあり，プライベート IP アドレスが割り当てられている．UA2 は SIP Proxy

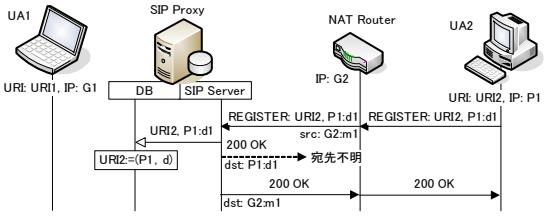

図 4 端末情報登録時に生じる問題

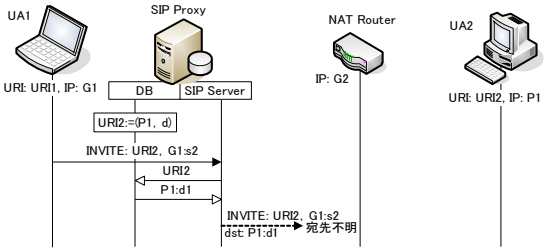

図 5 INVITE 時に生じる問題

に対して，REGISTER により SIP メッセージを受け取る際に使用するトランスポートアドレス P1:d1 の登録を要求する．SIP Proxy は受信した URI とトランスポートアドレスを DB に登録し，200 OK メッセージを P1:d1 宛に送信する．しかし，P1 はプライベート IP アドレスであるため，200 OK は宛先不明として処理されてしまい，UA2 には到達しない．

これを解決するため，RFC3581[3] では，REGISTER の送信元 IP アドレス・ポート番号に向けて，応答を返す方法が規定されている．図 4 では，NAT により変換された REGISTER の送信元 G2:m1 に向けて，200 OK を返答し，UA2 まで到達させることができる．これにより，SIP Proxy に端末情報を登録することができる．RFC3581 は NAT 配下にいる UA から開始されるシグナリングの場合，全ての SIP メッセージについて NAT 越え可能である．しかし，以下に示すケースには対応できない．

2.3.2 INVITE 時に生じる問題

図 5 に INVITE 時に生じる問題を示す．SIP Proxy は，UA1 から UA2 に向けた INVITE 受信すると，DB から URI2 の転送先のトランスポートアドレス P1:d1 を取得する．しかし，P1 はプライベート IP アドレスであるため，SIP Proxy 1 が INVITE を P1:d1 宛に送信しても，宛先不明として処理されてしまい，UA2 には到達しない．

2.3.3 セッション確立時に生じる問題

UA1 は受信した 200 OK に記載されている UA2 のトランスポートアドレスに基づき，セッションを確立する．しかし，P1 はプライベート IP アドレスであるため，UA1 からセッションを確立することはできない．また，セッションには SIP とは別のポート番号が使われるので，そのための NAT 越え対策が必要である．

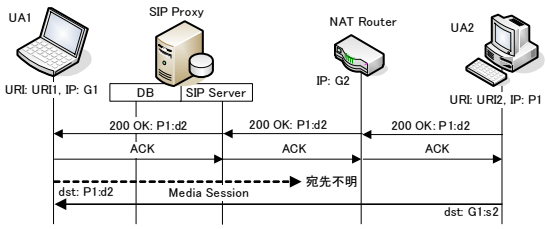

図 6 セッション確立時に生じる問題

3. 既存技術

ここでは，既存の SIP の NAT 越え技術をアドレス埋め込み型，アドレス書き換え型，サーバ中継型，3 種類に分類し，それぞれについて簡単に説明する．

3.1 アドレス埋め込み型

アドレス埋め込み型は，SIP メッセージを送信する際に，予め NAT 越え問題が解決済みの IP アドレス・ポート番号を埋め込んでおく方式である．ここでは，UPnP と STUN について述べる．

3.1.1 UPnP

図 7 に UPnP（Universal Plug and Play）[4] の動作概要を示す．機能の実装が必要になるのは NAT と NAT 配下の UA である．

SIP メッセージの送信に先立ち，UA と NAT の間で UPnP のネゴシエーションを行い，UA は NAT 外側の IP アドレス・ポート番号を取得する．UA は，この IP アドレス・ポート番号を SIP メッセージに埋め込んで送信する．UPnP のネゴシエーションは，SIP メッセージを受信するためのポートと，メディアセッションを確立する際に使用するポートについてそれぞれ実行する必要がある．

UPnP の機能が実装されている NAT ルータ（ブロードバンドルータ）は数多く存在するが，UA 側のポートと NAT 側のポートが一致していない設定が施せないものや，UPnP の実装が正しく行われていない場合などがあり，上手く動作しない場合がある．

3.1.2 STUN

図 8 に STUN（Simple Traversal of UDP through Network Address Translators）[5] の動作概要を示す．機能の実装が必要になるのは NAT と NAT 配下の UA である．また，第 3 の端末として STUN サーバが必要である．

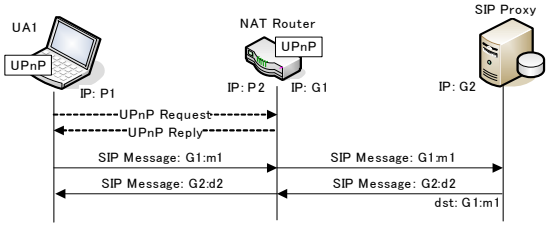

図 7 UPnP の動作概要

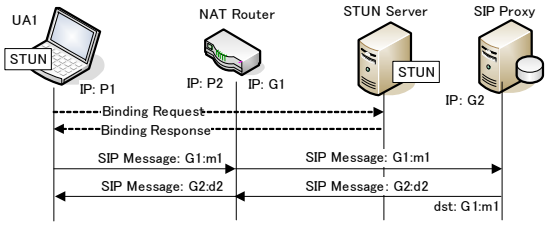

図 8 STUN の動作概要

SIP メッセージの送信に先立ち，UA は SIP メッセージを送信する際に使用するのと同じポート番号を使用し，STUN サーバに対して Binding Request を送信し，NAT 上に NAT テーブルを生成する．STUN サーバは，このとき STUN サーバ側から見た送信元 IP アドレス・ポート番号を Binding Response として返答する．そして，UA は，この IP アドレス・ポート番号を SIP メッセージに埋め込んで送信する．

しかし，この方式には STUN そのものの制約が引き継がれている．即ち，Symmetric NAT には使用できない．また，通信は UDP に限定される．

3.2 アドレス書き換え型

アドレス書き換え型は，NAT が SIP メッセージ中の IP アドレス・ポート番号の書き換える方式である．代表例として，SIP ALG と B2B UA について述べる．

3.2.1 SIP ALG

図 9 に SIP ALG（Application Level Gateway）[6] の動作概要を示す．機能の実装が必要なのは NAT の箇所だけである．NAT の機能を拡張し，プライベートネットワーク側からグローバルネットワーク側に送信された SIP メッセージの中身を参照し NAT 外側の IP アドレスとポート番号へ書き換える．

改造が必要になるのは NAT だけだが，NAT に負荷がかかることや，SIP メッセージが暗号化されていた場合に対応できないなどの課題がある．

3.2.2 B2B UA

図 10 に B2BUA（Back to Back User Agent）の動作概要を示す．機能の実装が必要なのは NAT の箇所だけである．B2B UA はネットワークの境界面である NAT 上で動作し，プライベートアドレス側とグローバルアドレス側にそれぞれ UA が存在するように振舞う．プライベートアドレス側の UA で SIP メッセージを受信すると，グローバルアドレス側の環境に合わせて SIP メッセージ生成し，グローバル側の UA で送信することにより，NAT を超えている．逆方向についても同様である．

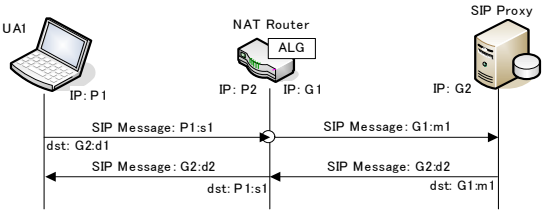

図 9 SIP ALG の動作概要

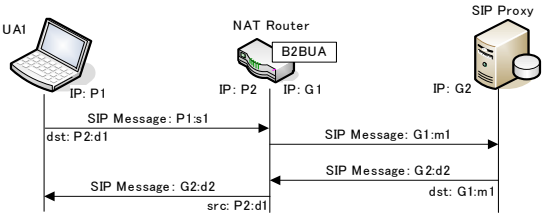

図 10 B2BUA の動作概要

3.3 サーバ中継型

サーバ中継型は，グローバルネットワークに設置されたサーバを中継し，通信を行うことで，NAT 越えを実現する方式である．

3.3.1 TURN

図 11 に TURN（Traversal Using Relay NAT）の動作概要を示す．機能の実装が必要になるのは NAT 配下の UA である．また，第 3 端末として TURN サーバが必要である．

UA は通信開始に先立ち，TURN サーバに対して Allocate Request を行う．これに対して，TURN サーバは，自身のポートを割り当て，Allocate Response により UA に通知する．この後，UA は TURN サーバとの間でセッションを維持し続ける．UA は，TURN サーバ上に割り当てられた IP アドレス・ポート番号を SIP メッセージに埋め込み，パケットをカプセル化して TURN サーバに送信する．TURN サーバは SIP メッセージを取り出し，送信する．TURN サーバが受信した SIP メッセージについては，カプセル化し，UA まで転送する．

TURN は NAT の種類に依存せず，NAT 越えが可能であるが，全ての通信が TURN サーバを中継するた

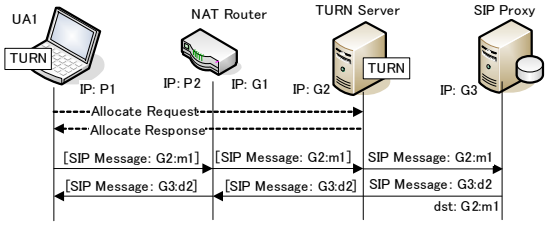

図 11 TURN の動作概要

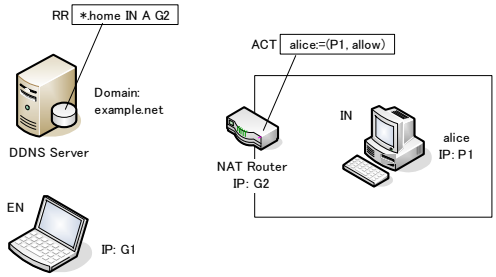

図 12 NAT-f 事前設定

め，TURN サーバに対する負荷が大きいことと，セッションのスループットが低下するという課題がある．

4. NAT-f

NAT-f は外部ノード EN（External Node）と NAT ルータが連携することにより NAT 越えを実現する技術である．以下に，NAT-f の概要について説明する．

4.1 事 前 設 定

図 12 にシステムの構成と初期設定情報を示す．外部ノード EN（External Node）と NAT ルータには NAT-f 機能が実装されており，内部ノード IN （Internal Node）及び DDNS（Dynamic DNS）[7] サーバは既存のものを利用する．

DDNS サーバには，IN の名前とそれに対応する NAT ルータの IP アドレスを登録しておく．

また，IN の名前，プライベート IP アドレス，及び外部からのアクセス許可情報を NAT ルータの ACT（Access Controll Table）に対して

$$alice := (P1, allow)$$

のように関連付けて，登録しておく．

4.2 動 作 概 要

図 13 に NAT-f の通信シーケンスを示す．NAT-f における通信は以下の 3 フェーズから構成される．

4.2.1 DNS 名前解決

EN は IN へ通信を開始する際，DDNS サーバへ名前解決を依頼する．DDNS サーバは NAT ルータの IP アドレス G2 を返答する．EN は IP 層において取得し

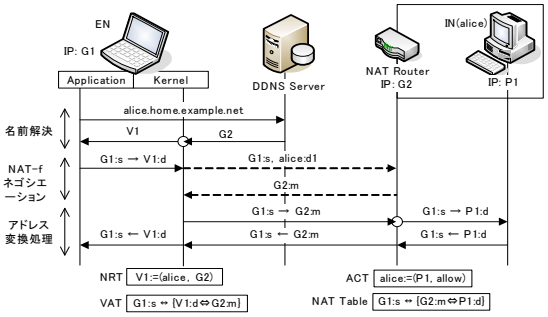

図 13 NAT-f の通信シーケンス

た NAT ルータの IP アドレスを仮想アドレス V1 へ書き換えてアプリケーションに渡す．このとき，NAT ルータの IP アドレス，仮想 IP アドレス，及び IN の名前の関係を NRT(Name Relation Table) に

$$V1 := (alice, G2)$$

のように関連付けて，保存する．以上の処理により，EN は通信相手の IP アドレスを V1 として認識する．

4.2.2 NAT-f ネゴシエーション処理

EN は宛先 IP アドレスが V1 である最初の TCP/UDP パケットを送信する際，一時的にこのパケットをカーネル内に待避させ，NAT ルータとの間で NAT-f ネゴシエーションを実行する．NAT ルータは，ACT を参照し，EN と IN 間の通信に必要な NAT テーブルを

$$G1 : s \leftrightarrow \{G2 : m \Leftrightarrow P1 : d\}$$

のように生成する．これは，IP アドレス・ポート番号が G1:s から G2:m に送信されたパケットの宛先 G2:m を P1:d へ変換することを意味している．そして，NAT ルータは，自身の IP アドレス G2 とマッピングされたポート番号 m を EN に返答する．EN はこの応答を元に VAT（Virtual Address Translation）テーブルを

$$G1 : s \leftrightarrow \{V1 : d \Leftrightarrow G2 : m\}$$

のように生成する．

4.2.3 通信中の仮想アドレス変換処理

以後，EN は VAT テーブルに従い，送信するパケットの宛先 IP アドレスを V1 から G2 へ，宛先ポート番号をマッピングされたポート番号 m に変換する．NAT に届けられたパケットの宛先 IP アドレス・ポート番号は NAT テーブルに従って変換され，IN に届けられる．逆方向の通信についても同様のアドレス・ポート変換を行う．

以上の処理により，NAT を超えて End-to-End で通信を開始できる．

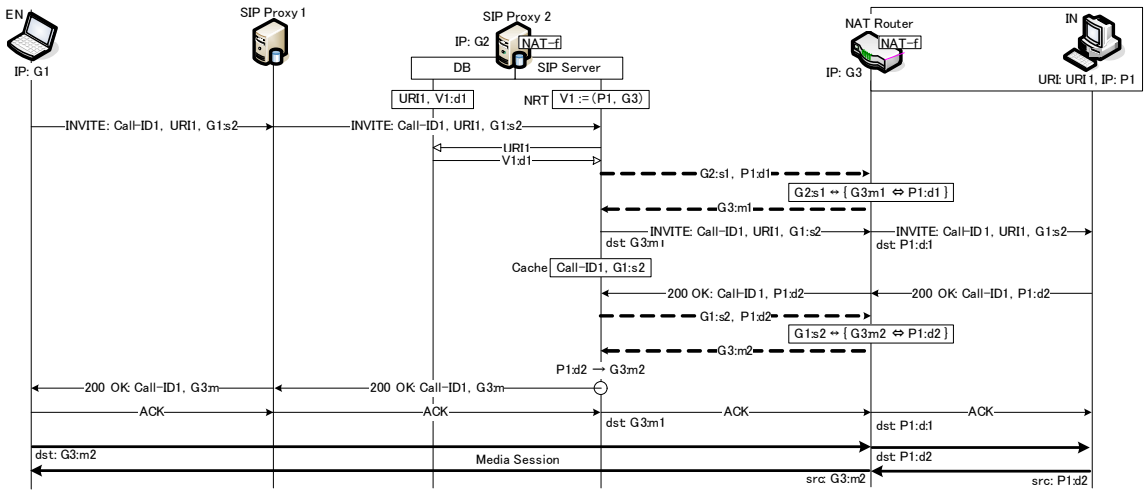

図 14 提案方式のシーケンス

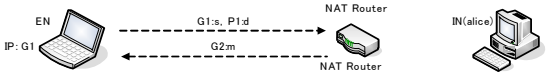

図 15 NAT-f ネゴシエーションの仕様拡張

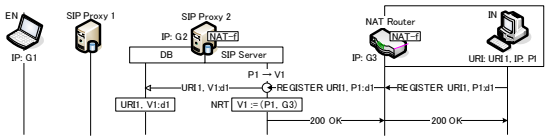

図 16 端末情報登録時のシーケンス

5. 提 案 技 術

ここでは，提案技術について説明する．本提案を実現するために NAT-f ネゴシエーションを拡張したため，拡張箇所について述べる．そして，提案技術の動作について説明する．

5.1 NAT-f ネゴシエーションの拡張

本提案を実現するために拡張を加えた NAT-f ネゴシエーションを**図 15** に示す．NAT 配下の端末を指定するための情報として，IN のホスト名の代わりに IN の IP アドレスを送信している．いずれも，NAT 配下の端末を指定するための情報であるため，本質的には変更はない．しかし，通信プロトコルとしては，実際にやり取りする情報に変更が加えられている．

5.2 動 作 概 要

EN 及び IN は SIP 機能を持つ一般端末とする．SIP Proxy 2 及び NAT ルータに拡張 NAT-f 機能を実装する．

5.2.1 端末情報の登録

図 16 に端末情報登録時のシーケンスを示す．EN は SIP Proxy 2 に対して REGISTER により自身の URI と SIP メッセージを受信する際に使用するトランスポートアドレス P1:d1 の登録を要求する．SIP Proxy 2 は REGISTER 受信時に，記載されている IP アドレスを P1 から仮想アドレス V1 へ書き換えて DB に登録する．この時，SIP Proxy 2 は V1，P1，G3 の関係を NRT に保存し， 200 OK を IN に返答する．

5.2.2 通信開始時の動作

図 14 に通信開始時のシーケンスを示す．EN からの通信開始時，SIP Proxy 2 は EN からの INVITE を受信すると DB の内容により，INVITE の転送先となる V1:d1 を取得する．ここで，宛先 IP アドレス V1 が仮想アドレスであるため，SIP Proxy 2 と NAT ルータ間で NAT-f ネゴシエーションを実行する．SIP Proxy 2 は INVITE の送信元トランスポートアドレス G2:s1，宛先ポート番号 d1，及び NRT に保存した IN のアドレス P1 の情報を NAT ルータに送信する．NAT ルータはこれらの情報を用いて，SIP Proxy 2 と IN の SIP ネゴシエーションに必要な NAT テーブルを生成後，マッピングされた G3:m1 を返答する．SIP Proxy 2 はこのマッピングされたポートに向けて INVITE を送信する．また，SIP Proxy 2 は一連のシーケンスで共通する Call-ID と EN が使用するトランスポートアドレス G1:s2 を対応付けてキャッシュする．SIP Proxy 2 は，INVITE に対する 200 OK を受信すると，先ほど作成したキャッシュの情報を Call-ID1 で検索し，NAT ルータに対して再度 NAT-f ネゴシエーションを実行する．SIP Proxy 2 は EN のトランスポートアドレス G1:s2 と IN のトランスポートアドレス P1:d2 を通知して EN と IN 間の通信で必要な

NAT テーブルを生成する．即ち，SIP Proxy 2 の指示により，NAT ルータ内に EN と IN 間の通信に必要となる NAT テーブルが生成される．SIP Proxy 2 は 200 OK に記載されているトランスポートアドレスを P1:d2 から G3:m2 へ書き換え，転送する．

200 OK を受け取った EN は，ACK 返答した後，交換したトランスポーアドレスに従い，メディアセッションを確立することができる．

6. ま と め

本論文では，NAT-f を利用した SIP の NAT 越えに手法ついて検討した．

SIP Server による NAT 外部から内部の IN に対する INVITE に先立ち，SIP Proxy が NAT ルータに対して NAT-f ネゴシエーションを実行し，SIP Proxy と IN 間の通信に必要な NAT テーブルを生成する手法を提案した．

また，SIP Proxy が EN と IN 間のセッションの確立に先立ち，NAT ルータに対して NAT-f ネゴシエーションを実行し，EN と IN 間の通信に通信に必要な NAT テーブルを生成する手法を提案した．

今後は，実装と動作確認を行う．

参 考 文 献

1) 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 越えを実現する NAT-f の提案と実装，情報処理学会論文誌， No.12, pp.3949–3961.
2) J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, M.Handley and E.Schooler: SIP: Session Initiation Protocol, RFC3261 (2002).
3) J.Rosenberg and H.Schulzrinne: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing, RFC3581 (2003).
4) Forum, U.: Internet Gateway Device (IGD) Standardized Device Control Protocol V 1.0, http://www.upnp.org/ (2001).
5) J.Rosenberg, J.Weinberger, C.Huitema and R.Mahy: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (2003).
6) A.Johnston, S.Donovan, R.Sparks, C.Cunningham and K.Summers: Session Initiation Protocol (SIP) Basic Call Flow Examples, RFC3665 (2003).
7) P.Vixie, S.Thomson, Y.Rekhter and J.Bound: Dynamic Updates in the Domain Name System (DNS UPDATE) (1997).