解説

ISPへのNAT導入によるユーザ影響評価

Evaluation of Impacts on Users When ISPs Adapt a Large-scale NAT

屏　雄一郎　大岸智彦　勝野　聡

Abstract

IPv4アドレス枯渇対策の一つとして，ISPのネットワークにNAT装置を導入することで，一つのIPv4アドレスを不特定な複数のユーザで共有する方法が検討されている．ISPに適用されるNAT装置は大規模なものになるため，このようなNAT装置はラージスケールNAT（LSN：Large Scale NAT）と呼ばれている．しかし，LSN環境下では，特定のアプリケーションが使えなくなるなど，エンドユーザに少なからず影響が出ると考えられている．本稿では，LSNの導入形態について最初に説明する．次に，LSN導入時のユーザへの影響，及び影響低減のために既存のNAT越え手法のLSN環境における有効性について考察した結果を述べる．最後に，実際の大手ISPにおけるトラヒック解析結果に基づき，LSN環境下でセッション制限が行われた場合のユーザに対する影響について評価した結果を紹介する．

キーワード：IPv4アドレス枯渇，ラージスケールNAT，NAT越え，トラヒック解析

1. はじめに

現在，インターネット接続事業者（ISP：Internet Service Provider）においては，IPv4アドレス枯渇問題への対策が急務となっている．IPv6への移行手法を含む，IPv4アドレス枯渇問題対策全般については，本会誌2月号の解説[1]で述べられている．

本稿では，IPv4アドレス枯渇問題への対策手法の一つである，限定的な範囲で利用可能なプライベートIPv4アドレスから，インターネットでの接続に利用可能なグローバルIPv4アドレスへのアドレス変換機能（NAT：Network Address Translation）を，ISPのような大規模ネットワークに適用する方法を取り扱う．ISPに適用されるNAT装置は，ラージスケールNAT（LSN：Large Scale NAT）と呼ばれている．LSNは，家庭用ルータ（HGW：Home Gateway）などの一般的なNAT装置と比較して，収容される機器数や装置が保持するアドレス変換テーブルなどの情報が大量であるという点が異なる．

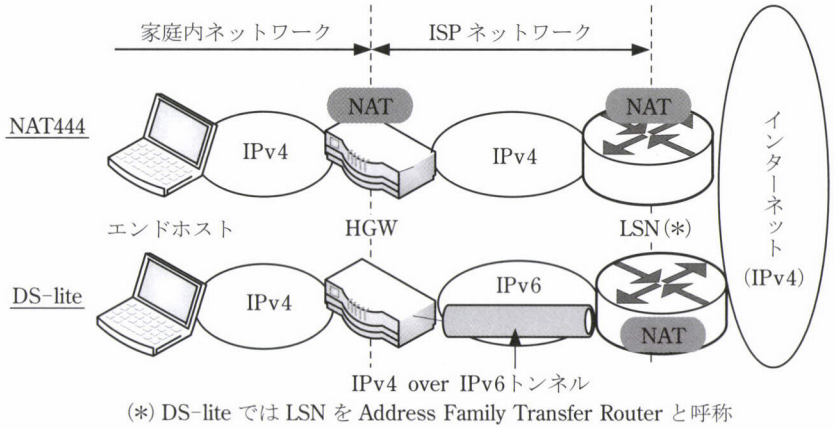
ISPネットワークへのLSN導入に対する影響として，ISPのネットワーク運用に与える影響と，ISPネットワークを利用するユーザに与える影響がある．今回は，後者に焦点を当て，LSN導入におけるユーザへの影響，及び影響低減のための既存のNAT越え手法の適用可能性について考察を行う．また，実際の大手ISPにおけるトラヒック解析結果に基づき，LSN環境下でセッション制限が行われた場合のユーザに対する影響について評価した結果を紹介する．

2. LSNのISPへの導入形態

図1に，ISPがLSNを導入する場合の代表的な導入形態であるNAT444[2]とDS-lite（Dual-Stack lite）[3]を示す．これらは，現在IETF（Internet Engineering Task Force）で議論されている．なお，図1では家庭内でネットワークに接続する機器（エンドホスト）が複数あることを想定し，エンドホストはHGW及びISPが構築するLSNを介してIPv4でインターネットに接続する場合のみを考慮している．

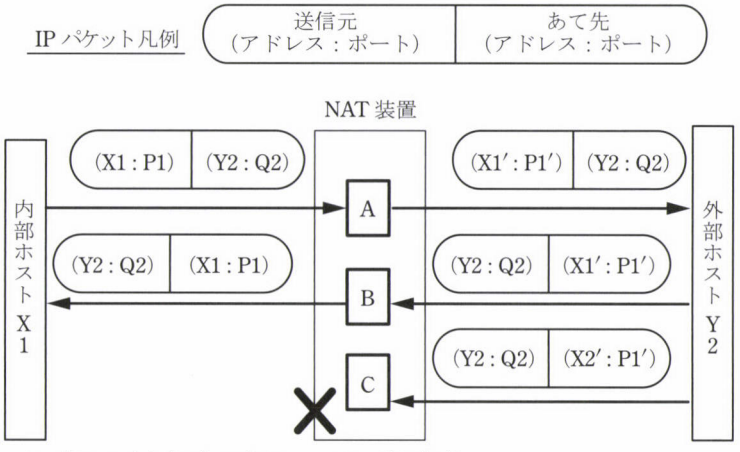
NAT444は，ISPネットワークにおいて，ISP内でのみ一意性が保証されているプライベートIPv4アドレスを利用する形態である．そのため，エンドホストからイ

屏　雄一郎　正員　（株）KDDI研究所ネットワークインテグレーショングループ
E-mail　hei@kddilabs.jp
大岸智彦　正員　（株）KDDI研究所ネットワークインテグレーショングループ
E-mail　ogishi@kddilabs.jp
勝野　聡　正員　KDDI株式会社技術統括本部
E-mail　sa-katsuno@kddi.com
Yuichiro HEI, Tomohiko OGISHI, Members (Network Integration Laboratory, KDDI R&D Laboratories, Inc., Fujimino-shi, 356-8502 Japan), and Satoshi KATSUNO, Member (Technology Sector, KDDI Corporation, Tokyo, 102-8460 Japan).
電子情報通信学会誌　Vol.93 No.6 pp.473-478 2010年6月



(*) DS-lite では LSN を Address Family Transfer Router と呼称

図 1　NAT444 と DS-lite　NAT は，NAT444 では 2 段，DS-lite では 1 段となる．



A：(X1 : P1) と (X1′ : P1′) のマッピングを作成
B：マッピングに従って (X1′ : P1′) あてのパケットを (X1 : P1) に転送
C：X2′に対するマッピングが存在しないため，転送不可

図 2　NAT の基本動作　内部ホストから開始される通信は NAT を通過するが，外部ホストから開始される通信は NAT を通過しない．

ンターネットに向かう IPv4 パケットは，少なくとも HGW と LSN で 2 段の NAT を行う必要がある．どのような IPv4 アドレスを HGW に割り当てるかは各 ISP にゆだねられるが，NAT 実施時にアドレス変換テーブルで混乱が生じないために，家庭内で利用している IPv4 アドレス空間と重複しないような対策が必要である．

一方，DS-lite は ISP ネットワークが IPv6 であることを前提とした形態であり，HGW には IPv6 アドレスが割り当てられる．エンドホストからの IPv4 パケットは LSN まで IPv4 over IPv6 トンネル上で転送され，LSN で NAT されてインターネットに送られる．したがって NAT444 とは異なり，NAT は LSN での 1 段のみとなる．

3.　ユーザへの影響

3.1　NAT による一般的な影響

アプリケーションが NAT による影響を受ける場合，その原因の多くは，外部ホストから NAT 装置内部にあるホストにはアクセスできないことにある（図 2）．そのため，例えば P2P アプリケーションなど，双方のホストから通信が開始される場合は，NAT が存在すると正常に動作しない場合が多い．この問題を解決するための「NAT 越え」という外部ホストから内部ホストへの通信を可能とする手法が存在する（詳細は 3.3 を参照）．

また，他の要因として，NAT 装置が保持可能な変換前後のアドレスやポート番号の対応などの情報量が挙げられる．NAT 装置の情報保持量を超えた通信が発生した場合，超えた分の通信は正常な NAT 処理が行われないため，インターネットへの接続障害が発生する場合がある．

3.2　ISP での LSN 導入による影響

ISP に LSN が導入された場合のユーザへの影響は，基本的には NAT による一般的な影響と同様である．LSN 固有の影響としては，同時通信数の制限がある[1]．

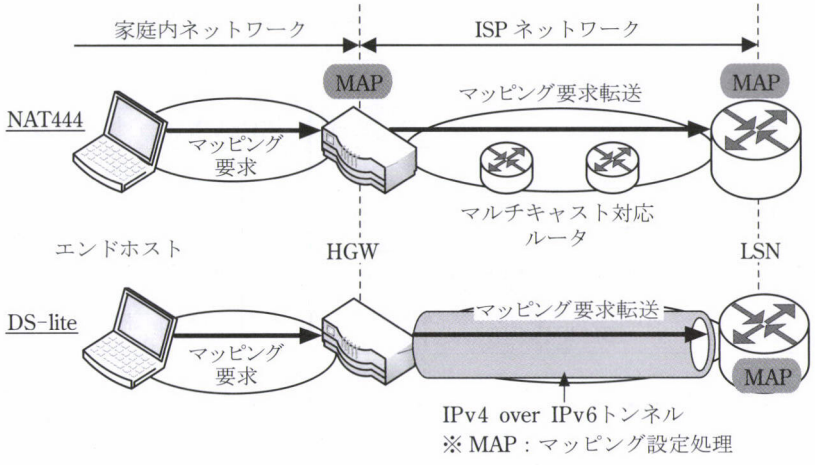


図 3　LSN 導入環境における UPnP の動作　NAT444 では HGW と LSN にマッピング設定が必要で，かつ HGW と LSN 間はマルチキャスト転送への対応が必要である．DS-lite では LSN のみでマッピング設定が行われる．

LSN 環境下では IP アドレスのポート数や機器性能などの制限，またユーザ間の公平性の観点から，1 ユーザ当りの同時通信数を制限することが検討されている[4]．しかし，アプリケーションによっては，同時に 100 以上の通信を行う場合もあることから，LSN での同時通信数制限により，アプリケーションが正常に動作しなくなるなどの影響が出ると考えられる．

3.3　NAT 越え手法の LSN 環境への適用可能性

現在の NAT 越え手法の中には，エンドユーザの近くで適用することを想定している手法が存在する．そのため，NAT が ISP 内で行われる LSN 環境では，NAT 越え手法によっては，有効に動作しない可能性がある．

そこで，一般的な NAT 越え手法の例として，既に多くのアプリケーションで実装されている，ポートマッピングと UDP ホールパンチングを取り上げ，これらが LSN 環境下でも有効な手法となり得るか考察する．

（1）　ポートマッピング

ポートマッピングは，特定の外部アドレス／ポート番号あてのパケットを，特定の内部ホストのアドレス／ポートに転送するためのマッピングを，あらかじめ NAT 装置に設定しておくことで，外部ホストから内部ホストへの通信を可能とする手法である．マッピングの設定方法として，NAT 装置に静的に設定する方法と，UPnP（Universal Plug and Play）等を利用して動的に設定する方法がある．

LSN へのポートマッピング静的設定の方法として，ユーザからの申請により ISP が設定を投入する方法や，設定画面を Web 等で公開してユーザに直接設定を投入してもらう方法などが考えられる．しかし，これらの方法では ISP が LSN のマッピング設定をユーザに開放する必要があるため，静的設定手法が適用可能かどうかは ISP の事情によるところが大きい．また，仮に開放したとしても，LSN 環境では多数のユーザで IP アドレス／ポート番号を共有することから，特定のポート番号を利用するアプリケーションを使用できるユーザ数が制限される可能性が高い．

UPnP によるマッピングの動的設定では，エンドホスト上で動作するアプリケーションが，特定のマルチキャストアドレスあてのマッピング要求パケットを用いて，NAT 装置に対してマッピング設定を要求する．LSN 環境で UPnP によるマッピングの動的設定が動作するためには，NAT444 モデルの場合，HGW と LSN が NAT を行うことから，それぞれでマッピング設定が必要である．また，マッピング要求パケットはマルチキャストで送信されるため，HGW と LSN の間のルータがマルチキャスト転送に対応している必要がある．一方，DS-lite モデルでは，HGW では NAT を行わないために，LSN のみのマッピング設定でよいが，HGW はエンドホストからのマッピング要求パケットを LSN に転送する必要がある．しかし，HGW と LSN は IPv6 トンネル経由で通信するため，HGW と LSN の間のルータがマルチキャスト転送に対応していなくてもよい（図 3）．

（2）　UDP ホールパンチング

UDP ホールパンチングの基本原理は，内部ホストから外部ホストへの通信を開始して NAT 装置にマッピング状態を保持させることで，外部ホストから内部ホストへの通信が NAT 装置を通過できる状態とすることである．図 4 に NAT444 モデルにおける UDP ホールパンチングの動作の一例として，別の LSN，HGW 配下にあるホスト A とホスト B 間通信の動作を示す．図 4 において，LSN と HGW におけるマッピング情報作成は，①，①′の手順で外部サーバに接続して自身の IP アドレス／ポート番号（LSN で変換後のアドレス／ポート番号）

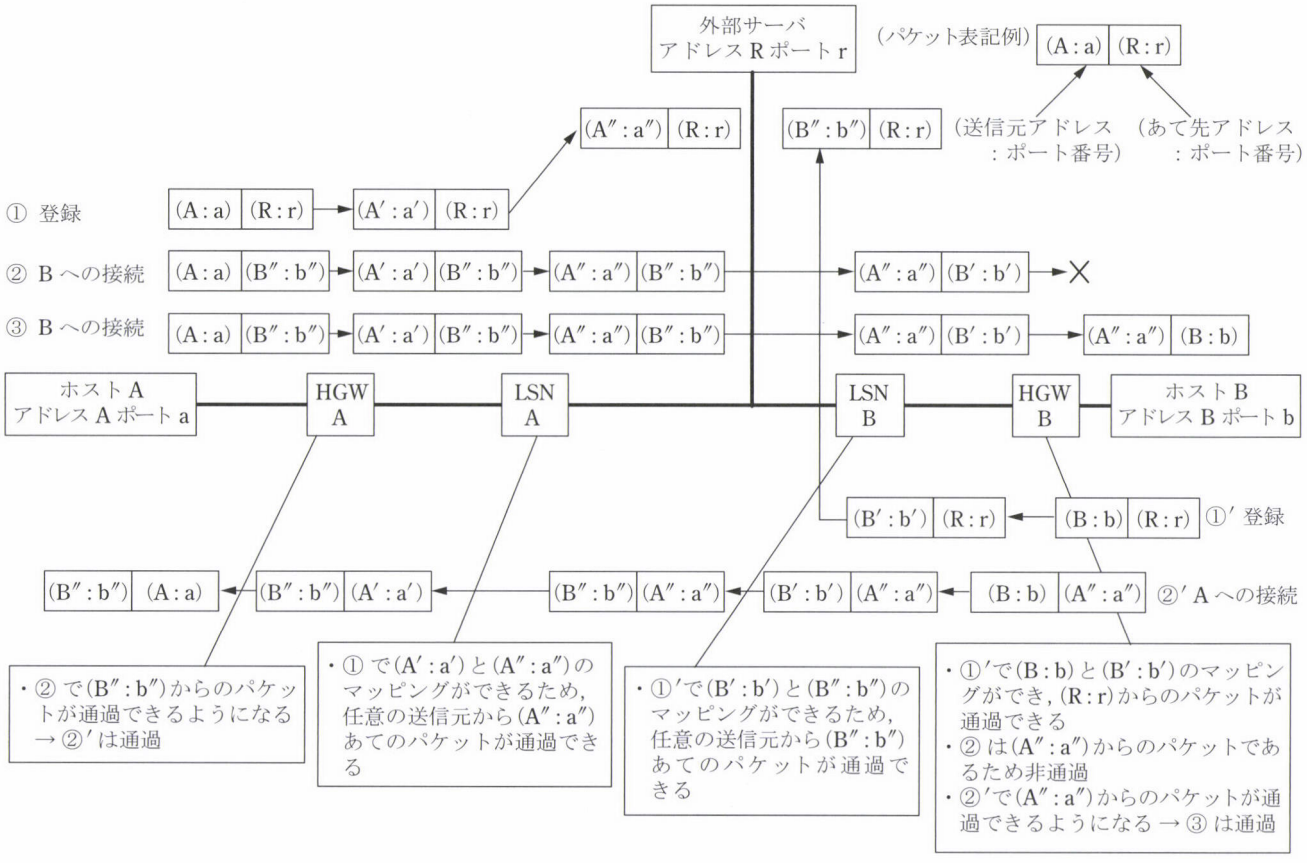


図4　NAT444におけるUDPホールパンチング　UDPホールパンチングでは，NATの内部ホストから外部ホストへの通信を開始してNATにマッピング状態を保持させることで，外部ホストから内部ホストへの通信がNATを通過できる状態とする．

を登録するとともに，通信相手ホストのIPアドレス／ポート番号を取得することで行う．

次に，図4②，②′，③のUDPパケット到達性を検証する．なお，NATのフィルタリング挙動によりパケットフローは若干異なるが，今回はLSNは端末非依存のフィルタリングを行い，HGWはアドレス・ポート依存フィルタリングを行う場合を示している．すなわち，LSNでは，LSNが割当て済みの外部アドレス／ポート番号あてのパケットは，送信元に関係なく通過する．一方，HGWでは，内部から開始された通信に対応する外部からのパケットのみ通過する．

- ホストAからBへの最初のパケット②は，LSN Bは通過し，HGW Bで遮断されるが，パケット②の情報でHGW Bにマッピングが作成される．
- ホストBからAへの最初のパケット②′はHGW Aも通過してホストAに到達する．
- パケット③は，パケット②′によりHGW Bにマッピングが作成されているため，今度はHGW Bも通過してホストBに到達する．以降，ホストA，Bからのパケットとも相手側のHGWを通過し，双方向で直接通信することが可能となる．

以上より，UDPホールパンチングは，原理上はNATが2段でも動作する．しかし，NAT装置の挙動により動作が異なる場合も十分考えられるので，実環境で動作検証することが重要である．

4.　実トラヒック解析によるLSN導入のユーザへの影響評価

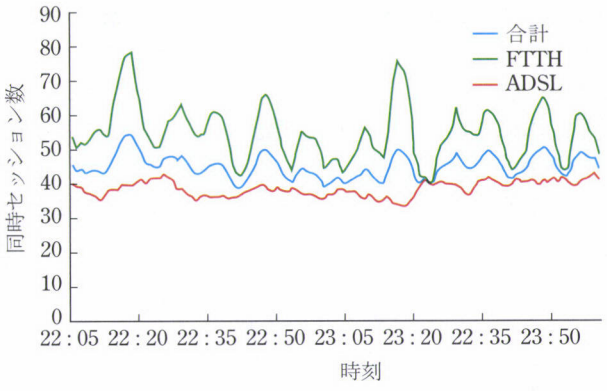
3.で述べたLSN導入によるアプリケーションへの影響のうち，セッション数制限による影響に関して，実際の商用トラヒックデータの解析により評価を行った．

4.1　評価条件

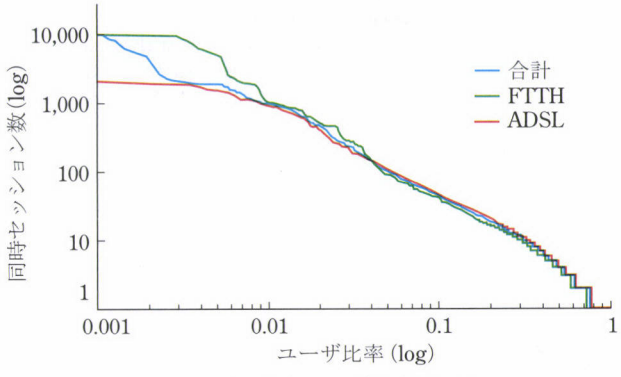
本評価で用いたトラヒックデータは，2008年に大手ISPにおいてTCP/UDPヘッダを収集したものであり，あるルータ配下の約20,000ユーザ（ADSLユーザが69.5%，FTTHユーザが30.5%）の，ユーザからインターネット向け通信である．解析対象期間は，1週間で最もトラヒック量が多い週末の夜間約2時間である．

以降で用いている用語の意味は次のとおりである．

- セッション：発着IPアドレス，発着ポート番号，プロトコルの組合せが同じパケットの集合

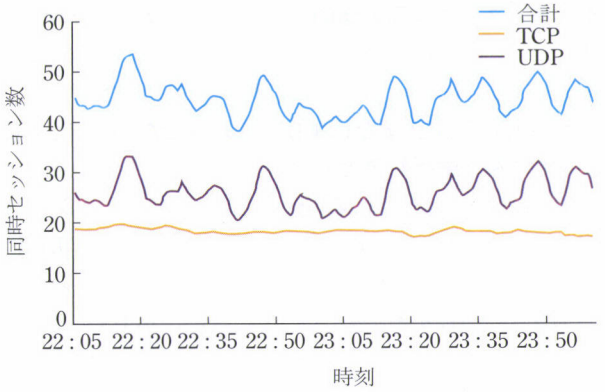


(a) 時間変動

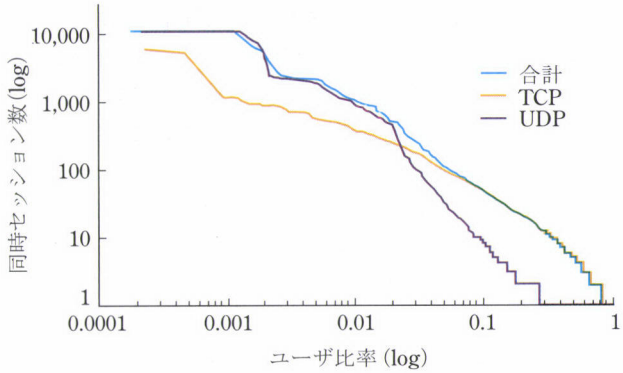


(b) ユーザごとの分布

図5 アクセス回線別の同時セッション数の傾向 FTTHユーザの比率が増加すればユーザ当りの平均使用セッション数が増える．また，ユーザごとにセッション数制限を行う場合，ユーザの使用セッション数をある程度多く見積もっても，少数のヘビーユーザには影響を与える可能性がある．



(a) 時間変動



(b) ユーザごとの分布

図6 プロトコル別の同時セッション数の傾向 UDPの方が時間変化が激しく，ユーザごとのセッション数の制限をすると特定のユーザは影響を受けやすい．

- 同時セッション数：ある一時刻に同時に存在するセッション数
- 合計セッション数：ある時間範囲において存在した延べセッション数
- アクティブユーザ：ある一時刻に少なくとも一つのセッションを発生させているユーザ

なお，解析において，セッション終了は以下のように判断した．

- TCPセッションの場合，FINまたはRSTフラグが立ったパケットが含まれる場合に正常終了セッションと判断し，最終パケットの観測時刻をセッション終了時刻とする．
- TCPセッション正常終了以外では，5分間該当セッションのパケットがない場合，セッションが終了したものとし，最終パケットの観測時刻に5分を加算した時刻をセッション終了時刻とする．

4.2 アクセス回線種別での傾向

まず，アクセス回線種別での同時セッション数の傾向を述べる．図5 (a)は，1アクティブユーザ当りの同時セッション数の1分ごとの時間変動を示したものである．本結果では，FTTHユーザは平均40～79セッション，ADSLユーザは平均33～43セッションを使用していた．このことから，FTTHユーザの方が平均的にセッションを多く使用し，時間ごとのセッション数の変動が激しいことが分かった．なお，FTTH及びADSLの平均アクティブユーザ率は，それぞれ30.9%，20.4%であり，FTTHの方がアクティブユーザ率は高かった．

図5 (b)は，解析時間内のある一時刻におけるユーザごとの分布であり，横軸は全アクティブユーザを1としたときの占有率(値が小さいほど当該ユーザ数は少ない)を示している．10,000セッションを使用するユーザもいたが，99%のユーザは使用セッション数が1,000セッション以下であった．また，1%のヘビーユーザについては，FTTHの方がより多くのセッション数を使用していることが分かった．

これらの結果より，FTTHユーザの比率が増加すれば平均使用セッション数が増えることが分かった．また，ユーザごとにセッション数制限を行う場合，セッション数の制限値をある程度多く見積もっても，少数のヘビーユーザには影響を与える可能性があることが分かった．

4.3 プロトコル別の傾向

次に，プロトコル別での同時セッション数の傾向について述べる．今回の評価条件では，観測されたセッションの約99%がTCPまたはUDPであったため，TCP及びUDPのみを解析対象とした．

図6 (a)は1アクティブユーザ当りの同時セッション数の1分ごとの時間変動を示しており，TCP，UDPはそれぞれ17～20セッション，20～33セッションであり，UDPの割合が多いことが分かった．これは，UDPがTCPのような正常終了判定ができないためと考えられる．なお，TCPでは85%のセッションにおいて正常終了判定が可能であった．また，UDPの方が時間ごとのセッション数の変動が大きいことが確認された．図6 (b)は，解析時間内のある一時刻におけるユーザごとの分布であり，TCPに比べてUDPの方が，特定のユーザが多数のセッションを使用する傾向が強いことが分かった．

以上の結果より，アクセス回線種別の場合と同様に，ユーザごとのセッション数の制限をすると，特定のユーザは影響を受けやすい傾向がある．また，TCPと比較するとUDPセッションの方がユーザごとのセッション制限値の見積もりに影響を与える可能性が大きいことが分かった．

5. 今後の導入に向けて

本稿では，ISPへのラージスケールNAT (LSN) 導入によるユーザへの影響について，既存のNAT越え手法の有効性と，実トラヒック解析に基づきLSNでセッション数制限が行われた場合の影響について解説した．NATの挙動については，LSNはなるべく既存のアプリケーションに影響を与えない実装とすることが推奨されているが[4]，実際には機器により細かな挙動が異なる場合も考えられるため，今後所望のアプリケーションが使えるかどうかを実環境で検証することも重要となるであろう．また，トラヒック解析では，セッション終了時刻の推定方法を変えた場合に，同時セッション数の傾向が変わることなども確認しており，LSNの実運用時のパラメータ設計についてはなお慎重な検討が必要と考えられる．本稿で紹介した解析結果は，トラヒックデータ収集時点のものではあるが，一つのデータとして，LSNの設計や運用方法を将来検討する際に活用されることを期待する．

文　献

(1) 宮川　晋，“大規模NAT技術とIPv6，”信学誌，vol.93, no.2, pp.145-151, Feb. 2010.
(2) Y. Shirasaki, S. Miyakawa, A. Nakagawa, J. Yamaguchi, and H. Ashida, “NAT444 with ISP shared address,” draft-shirasaki-nat444-isp-shared-addr-02, Sept. 2009.
(3) “Dual-stack lite broadband deployments post IPv4 exhaustion,” A. Durand, ed., draft-ietf-softwire-dual-stack-lite-02, Oct. 2009.
(4) T. Nishitani, I. Yamagata, S. Miyakawa, A. Nakagawa, and H. Ashida, “Common functions of large scale NAT (LSN),” draft-nishitani-cgn-03, Nov. 2009.

(平成22年2月15日受付　平成22年3月1日最終受付)

屏　雄一郎（へい　ゆういちろう）（正員）
平8東大・工・電子情報卒．平10同大学院修士課程了．同年KDD（株）入社．以来，研究所にてIPネットワーク管理・制御の研究に従事．現在，（株）KDDI研究所ネットワークインテグレーショングループ研究主査．

大岸　智彦（おおぎし　ともひこ）（正員）
平4東大・工・電気卒．同年KDD（株）入社．以来，研究所にて通信システムの試験，IPネットワーク管理・制御の研究に従事．現在，（株）KDDI研究所ネットワークインテグレーショングループリーダー．博士（工学）．

勝野　聡（かつの　さとし）（正員）
平元東大・工・電気卒．平3同大学院修士課程了．同年KDD（株）入社．以来，研究所にて画像通信，IPネットワーク運用に関する研究に従事．現在，KDDI（株）IPネットワーク部課長．