LTA6：IPv6固定アドレスを介した軽量IP機器への位置透過なアクセス手法

黒木　秀和[†,††a)]　井上　博之[†††]　荻野　司[†]　石原　進[††]

LTA6 : Location Transparent Access Scheme to Lightweight IP Devices through IPv6 Fixed Addresses

Hidekazu KUROKI[†,††a)], Hiroyuki INOUE[†††], Tsukasa OGINO[†], and Susumu ISHIHARA[††]

あらまし　近年，IP通信機能が搭載された様々な機器が製品化されている．これらの機器は，機器ユーザのネットワークに設置されると任意のアドレスが付与されるが，それとは別の固定のIPアドレスでこれらの機器と通信できれば，遠隔から機器の保守，操作，監視を行うことが容易になる．本論文では，双方向のアドレス変換機構をもつアドレス変換装置を用い，固定IPv6アドレスを用いた機器と他ノードの通信を可能とする手法を提案する．本手法では，IPトンネル処理や特殊なヘッダの処理など，機器の処理負荷を増大させる機能の実装を不要としている．また，固定IPv6アドレスを利用した通信が常にアドレス変換装置を経由するように動作することで，機器に対する不正アクセスをアドレス変換装置で防ぐことを可能にしている．

キーワード　遠隔機器管理，固定アドレス，IPv6，アドレス変換，軽量機器

1. まえがき

近年，家電，センサデバイス，監視カメラなどの機器にIP通信機能が搭載され，機器を製造したベンダ（機器ベンダ）による遠隔からの機器の保守，操作，監視などに利用されるようになっている．遠隔からの機器へのアクセスを実現するには，機器の現在のIPアドレスを常に把握する必要がある．しかし，機器が設置されるネットワークやその上位ネットワークは，機器ユーザごとに異なり，機器ユーザの引っ越しや利用するISP（Internet Service Provider）の変更によって変化する．これに伴って，機器のアドレスも変化する．このため，機器ベンダは，変化する機器のアドレスを機器の出荷前に知ることは困難である．

機器ベンダが，機器の設置場所とは独立した固定の接続情報を機器に割り当てて出荷し，この接続情報を用いて機器と通信できれば，機器のアドレスが変化するたびに機器への接続情報を変更する必要がなくなる．こうすることで，機器ベンダによる機器の保守，操作，監視などが低コストで実現可能となる．ただし，機器ベンダが機器に割り当てた固定の接続情報を用いて機器に対する不正アクセスが行われた場合，機器ベンダの責任が問われる可能性がある．このため，機器ベンダは接続情報を用いた通信を常に監視・制御できる必要がある．

常に固定の接続情報で機器にアクセス可能な技術として，Dynamic DNS [1], [2]，Mobile IP（IP Mobility Support for IPv4（MIP4）[3]，IP Mobility Support in IPv6（MIP6）[4], [5]）などがある．Dynamic DNSを用いると，機器に固定のFQDN（Fully Qualified Domain Name）でアクセス可能となる．しかし，機器のアドレスはそれぞれ異なるネットワークプレフィックスをもつために経路集約は不可能であり，各機器へのすべての通信を監視・制御するノードを設置することはできない．このため，機器ベンダは，自身が管理

† （株）ユビテックユビキタス研究所，東京都
Ubiquitous Labs., Ubiteq, Inc. Gotanda-NT Bldg. 6F, 1–18–9 Nishi-gotanda, Shinagawa-ku, Tokyo, 141–0031 Japan
†† 静岡大学創造科学技術大学院，浜松市
Graduate School of Science and Technology, Shizuoka University, 3–5–1 Johoku, Hamamatsu-shi, 432–8051 Japan
††† 広島市立大学情報科学研究科，広島市
Graduate School of Information Sciences, Hiroshima City University, 3–4–1 Ozukahigashi, Asaminami-ku, Hiroshima-shi, 731–3194 Japan
a) E-mail: hidekazu@ubiteq.co.jp

するノードで，機器への不正アクセスを遮断することができない．Mobile IP を用いると，機器は常に固定の IP アドレスで通信可能となり，機器の設置場所を意識する必要がなくなる．しかし，Mobile IP では，機器に IP トンネル処理などの負荷のかかる処理が必要となり，機器の実装を複雑にしてしまう．

本論文では，機器ベンダのネットワークに設置したアドレス変換装置で，固定アドレスと機器の設置場所におけるアドレスの相互変換を行うことで，固定アドレスで機器にアクセスすることを可能とする手法 Location Transparent Access to a lightweight IP device through an IPv6 fixed address（LTA6）を提案する．本手法では，機器は通常の IPv6 機能とアドレス変換装置にアドレスを登録する機能をもてばよく，機器の通信相手は通常の IPv6 機能のみをもてばよい．固定のアドレスを用いた機器との通信は常にアドレス変換装置を経由するため，ここで通信の監視・制御を行うことで機器への不正アクセスを防ぐことができる．

以下，**2.** では本論文で提案する LTA6 について述べ，**3.** ではその検討を行う．**4.** では関連技術との比較を行い，**5.** では LTA6 の実装とその評価を行う．最後に，**6.** でまとめを行う．

2. LTA6

LTA6 は，図 1 のように，機器ベンダネットワークのネットワークプレフィックスに含まれるアドレスを固定アドレスとして機器ベンダネットワーク上のアドレス変換装置に設定し，このアドレス変換装置上で受信する通信パケットのあて先アドレス（以下，あて先）及び送り元アドレス（以下，送り元）を変換することにより，固定アドレスで機器にアクセスすることを可能とする．LTA6 は以下の二つの特徴をもつ．

(i) 機器に必要な追加機能が少なく，処理負荷も少ない．

(ii) 通信は機器ベンダが管理するノードを経由するため，不正な通信の遮断が可能．

2.1 LTA6 のシステム構成

LTA6 のシステムは，図 2 に示すように，機器ノード（Device Node：DN），遠隔ノード（Remote Node：RN），アドレス変換装置（Address Translator：AT）の各ノードで構成される．

DN は，機器ベンダから出荷される機器であり，機器ユーザのホームネットワーク（Home Network：HN）に接続されている．HN はインターネットに接続され，LTA6 に対応した一つ以上の DN 及びそれ以外の IP ノードが接続される．RN は，DN と通信を行うインターネット上の遠隔に設置された任意の IP ノードである．DN と RN には，それぞれインターネット上の任意のノードと通信可能な IPv6 アドレス $\mathsf{Addr}_{\mathsf{DN}}$ 及び $\mathsf{Addr}_{\mathsf{RN}}$ が設定されている．AT は，アドレスを変換と通信監視を行うための装置であり，機器ベンダに割り当てられた IPv6 ネットワークプレフィックスをもつ機器ベンダネットワーク（Vendor Network：VN）に接続される．VN 及び AT は，機器ベンダごとに独立して存在する．

2.2 固定アドレス及び一時アドレス

LTA6 では，$\mathsf{Addr}_{\mathsf{DN}}$ と $\mathsf{Addr}_{\mathsf{RN}}$ 以外に，以下の 2 種類の IPv6 アドレスを使用する．

- DN に固定で割り当てる IPv6 アドレス（固定アドレス）$\mathsf{FixAddr}_{\mathsf{DN}}$
- RN–DN 間の組合せに一時的に割り当てる IPv6 アドレス（一時アドレス）$\mathsf{TmpAddr}_{\mathsf{RN,DN}}$

これらは，機器ベンダが割当を受けた IPv6 ネットワークのプレフィックスをもち，すべて AT のアドレスとして設定される．すなわち，これらのアドレスをあて先とするパケットは，AT（VN）にルーチングされる．

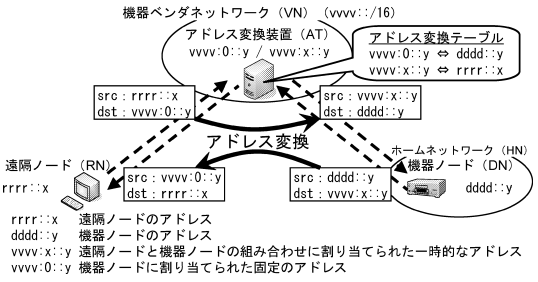

図 1 LTA6 の概要
Fig. 1 Overview of LTA6.

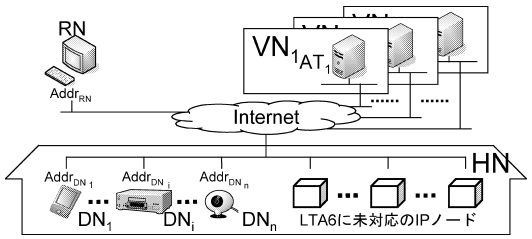

図 2 LTA6 のシステム構成
Fig. 2 System overview of LTA6.

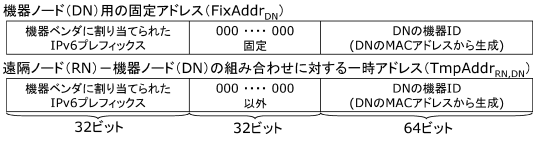

図 3　固定アドレス及び一時アドレスの例
Fig. 3　Example of a fixed address and a temporary address.

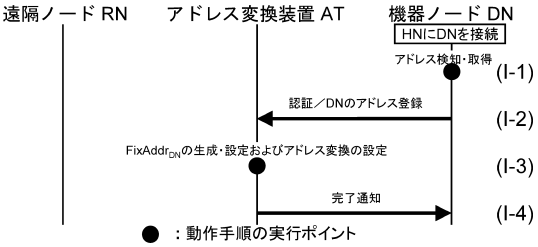

図 4　DN を HN へ接続する時の初期動作
Fig. 4　Initial procedure of connecting DN to HN.

機器ベンダに割り当てられた IPv6 ネットワークのプレフィックス長を 32 ビットとした場合の固定アドレス及び一時アドレスの構成を図 3 に示す．それぞれの下位 64 ビットは，DN の機器 ID である．DN の機器 ID は，IPv6 アドレス仕様 [6] のインタフェース ID であり，DN のネットワークインタフェースの MAC アドレスから生成される．中間の 32 ビットは，固定アドレスの場合はすべてのビットで 0 であり，一時アドレスの場合は 0 でないビットを少なくとも一つ含んでいる．一時アドレスは，異なる RN–DN の組合せごとに $\mathsf{TmpAddr}_{\mathsf{RN,DN}}$ が異なるように中間の 32 ビットがラウンドロビンで割り当てられる．

2.3　LTA6 の動作手順

LTA6 の動作手順を以下の三つに分けて述べる．

- DN を設置するときの初期動作
- RN から通信を開始するときの動作
- DN から通信を開始するときの動作

なお，以下に述べる動作手順において，アドレス変換の前後でパケットのサイズに増減はない．

2.3.1　DN を設置するときの初期動作（図 4）

DN には，AT の FQDN などの AT へアクセスするための情報（以下，AT アクセス情報）が出荷時に機器ベンダによって設定されている．HN に DN が接続され，ルータ広告 [7] や DHCPv6 [8] などにより，DN に新しい IPv6 アドレスが設定されると，以下の処理が行われる．

(I-1)　DN は，$\mathsf{Addr}_{\mathsf{DN}}$ とネットワークインタフェースの MAC アドレスを取得する．

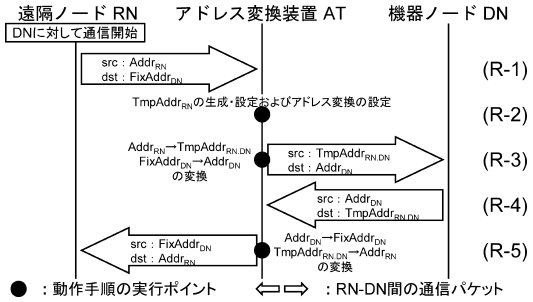

図 5　RN から通信を開始する場合の動作
Fig. 5　Procedure of communication from RN to DN.

(I-2)　DN は，AT アクセス情報を用いて AT に接続し，AT–DN 間で適切な認証を行った後に $\mathsf{Addr}_{\mathsf{DN}}$ 及び MAC アドレスを AT に送信して DN のアドレス登録を行う．この通信の方法についてはここでは問わない．

(I-3)　AT は，DN の MAC アドレスから DN に割り当てる固定アドレス $\mathsf{FixAddr}_{\mathsf{DN}}$ を決定して自身に設定し，$\mathsf{Addr}_{\mathsf{DN}} \leftrightarrow \mathsf{FixAddr}_{\mathsf{DN}}$ のアドレス変換を設定する．

(I-4)　AT は，DN のアドレス登録に対する完了通知を DN に送信する．

2.3.2　RN から通信を開始するときの動作（図 5）

(R-1)　RN は，$\mathsf{FixAddr}_{\mathsf{DN}}$ をあて先とするパケットを送信する．このパケットは VN にルーチングされ，AT に $\mathsf{FixAddr}_{\mathsf{DN}}$ が設定済みの場合は AT が受信し，未設定の場合は RN に到達不能エラーが返される．

(R-2)　AT は，送り元が $\mathsf{Addr}_{\mathsf{RN}}$，あて先が $\mathsf{FixAddr}_{\mathsf{DN}}$ のパケットを受信すると，$\mathsf{Addr}_{\mathsf{RN}}$ と $\mathsf{FixAddr}_{\mathsf{DN}}$ に対応する一時アドレス $\mathsf{TmpAddr}_{\mathsf{RN,DN}}$ が自身に設定済みか確認する．未設定の場合，AT は，一時アドレス $\mathsf{TmpAddr}_{\mathsf{RN,DN}}$ を決定して自身に設定し，$\mathsf{TmpAddr}_{\mathsf{RN,DN}} \leftrightarrow \mathsf{Addr}_{\mathsf{RN}}$ のアドレス変換を設定する．

(R-3)　AT は，受信パケットの送り元が $\mathsf{Addr}_{\mathsf{RN}}$ あて先が $\mathsf{FixAddr}_{\mathsf{DN}}$ である場合，送り元を $\mathsf{TmpAddr}_{\mathsf{RN,DN}}$ あて先を $\mathsf{Addr}_{\mathsf{DN}}$ に変換し，DN に送信する．また，このとき ICMPv6，TCP，UDP ヘッダ内のチェックサムを更新する．

(R-4)　DN は，受信したパケットに対する応答として，その送り元である $\mathsf{TmpAddr}_{\mathsf{RN,DN}}$ をあて先とするパケットを送信する．このパケットは VN にルーチン

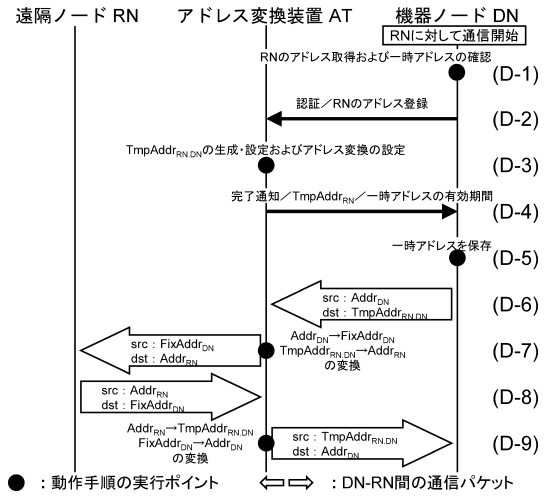

図 6　DN から通信を開始する場合の動作
Fig. 6　Procedure of communication from DN to RN.

グされ，AT が受信する．

(R-5)　AT は，受信パケットの送り元が Addr_{DN} あて先が $\mathsf{TmpAddr}_{RN,DN}$ である場合，送り元を $\mathsf{FixAddr}_{DN}$ あて先を Addr_{RN} に変換し，RN に送信する．また，このとき ICMPv6，TCP，UDP ヘッダ内のチェックサムを更新する．

2.3.3　DN から通信を開始するときの動作（図 6）

(D-1)　DN は，DNS などで Addr_{RN} を取得する．DN は，Addr_{RN} をキーとして有効期限内の $\mathsf{TmpAddr}_{RN,DN}$ が存在するか確認する．存在する場合は，(D-6) 以降の処理を行う．

(D-2)　DN は，AT アクセス情報を用いて AT に接続し，AT–DN 間で適切な認証を行った後に Addr_{RN} 及び Addr_{DN} を AT に送信して RN のアドレス登録を行う．この通信の方法についてはここでは問わない．

(D-3)　AT は，Addr_{DN} をキーとして (I-3) で設定した $\mathsf{FixAddr}_{DN}$ を割り出し，Addr_{RN} と $\mathsf{FixAddr}_{DN}$ に対応する一時アドレス $\mathsf{TmpAddr}_{RN,DN}$ が自身に設定済みか確認する．未設定の場合，AT は，一時アドレス $\mathsf{TmpAddr}_{RN,DN}$ を決定して自身に設定し，$\mathsf{TmpAddr}_{RN,DN} \leftrightarrow \mathsf{Addr}_{RN}$ のアドレス変換を設定する．

(D-4)　AT は，RN のアドレス登録に対する完了通知と $\mathsf{TmpAddr}_{RN,DN}$ 及び一時アドレスの有効期間を DN に送信する．

(D-5)　DN は，$\mathsf{TmpAddr}_{RN,DN}$ を Addr_{RN} と対応づけて，現在日時に一時アドレスの有効期間を加算した有効期限とともに自身に記録する．

(D-6)　DN は，$\mathsf{TmpAddr}_{RN,DN}$ をあて先とするパケットを送信する．このパケットは VN にルーチングされ，AT が受信する．

(D-7)　(R-5) に同じ．

(D-8)　RN は，受信したパケットに対する応答として，その送り元である $\mathsf{FixAddr}_{DN}$ をあて先とするパケットを送信する．このパケットは VN にルーチングされ，AT が受信する．

(D-9)　(R-3) に同じ．

3. 検　　討

3.1　チェックサム再計算と IPSec

LTA6 では，AT においてアドレス変換を行うパケットに ICMPv6，TCP，UDP のヘッダが含まれる場合，これらのヘッダ内のチェックサムを再計算して置き換える必要がある．なぜならば，これらのヘッダ内のチェックサムの計算には送り元とあて先のアドレスを利用しており，アドレス変換によりチェックサムも変わるためである．チェックサムが正しくないと，変換後のパケットを受け取る RN や DN によってパケットが破棄される．

IP Security（IPSec）によって暗号化されたパケットや認証情報が付加されているパケットは，通信途中でその中に含まれる ICMPv6，UDP，TCP の各ヘッダ内のチェックサムを変更するのは不可能である．このため，LTA6 を用いた場合，RN–DN 間の IPSec 通信は不可能であり，RN–AT 間と AT–DN 間で別々に IPSec 通信を行う必要がある．

3.2　一時アドレスの回収と再利用

一時アドレス $\mathsf{TmpAddr}_{RN,DN}$ は，RN–DN 間で通信を行う際に一時的に用いられるアドレスであり，RN–DN 間の通信を終えた後，AT から削除する必要がある．このため AT は，各一時アドレスについて，このアドレスを使用した通信パケットの受信を監視し，一定期間以上受信しなければこの一時アドレスを削除して回収する．この一定期間は，(D-4) で AT から DN に通知される一時アドレスの有効期間より長くする．回収された一時アドレスは新たな RN–DN 間の通信を開始するときに再び利用される．

3.3　セキュリティ

LTA6 で特徴的なのは，AT，固定/一時アドレスの導入である．そこで本論文では，AT のもつアドレス（固定/一時アドレス，AT の本来のアドレス）への非正規ユーザからの接続と DoS 攻撃に絞って議論する．

LTA6 では，RN 及び DN のアドレスと固定/一時アドレスが用いられる．このうち，RN 及び DN のアドレスあてに対する不正アクセスについては，RN 及び DN において一般的なセキュリティ対策を行えばよい．固定/一時アドレスあてに対する不正アクセスについては，双方とも AT に設定されるアドレスであるため，AT において以下のセキュリティ対策を行うことで，AT または AT を介した RN または DN への不正アクセスと AT への DoS を防ぐ．

3.3.1 不正な固定/一時アドレスの設定の防止

固定アドレスの設定は，DN からの DN のアドレス登録で行われる．また，一時アドレスの設定は，DN からの RN のアドレス登録または RN から固定アドレスあてへの通信パケットによって行われる．一つの DN に対して複数の固定アドレスや，一つの RN–DN の組合せに対して複数の一時アドレスが設定されることはない．そこで，(I-2) や (D-2) で DN または RN のアドレス登録を行う前に，チャレンジ・レスポンス認証や Kerberos 認証など DN に対する実装や負荷が少ない認証手法を用いて，AT が DN の認証を行って正常な DN からのアドレス登録のみ受け付けるようにする．更に，RN は DN の保守，操作，監視を行うための端末やサーバであり，そのノード数とアドレスは限定され，あらかじめ知ることができる．そこで，これらのアドレス以外を送り元とする固定アドレスあての通信パケットはすべて遮断するアクセス制限を行う．こうすることで，不正なリクエストや通信パケットによる固定/一時アドレスの設定や，それらが大量に行われることによる DoS 攻撃を防ぐことができる．

3.3.2 不正な送り元からの通信パケットの遮断

上記のアクセス制限により，固定アドレスにはあらかじめ限定されたアドレスをもつ RN からのみアクセス可能となる．更に，一時アドレスを設定するときに，一時アドレスに対応する RN–DN の組合せをなす DN 以外からこの一時アドレスあての通信パケットはすべて遮断するアクセス制限を行う．こうすることで，固定アドレスあて及び一時アドレスあての不正な送り元からのアクセスや，そのようなパケットを大量に送信することによる DoS 攻撃を防ぐことができる．

上記の対策を行ったとしても，LTA6 で発生し得るセキュリティ上の問題をすべてを解決することはできない．例えば，正規の DN や RN によって AT に固定/一時アドレスが設定された後，この DN や RN が他の機器に置き換えられるすり替えが起こり得る．この機器が，置き換えられる前の正規の DN や RN と同じアドレスをもち，固定/一時アドレスに対してパケットを送信した場合，AT が正規の DN や RN からのパケットであるか否かを判別することは困難である．また，RN–AT 間及び AT–DN 間でのパケット盗聴・書換えによる中間者攻撃も LTA6 単体で防ぐことは困難である．これらに対処するには，RN–AT 間及び AT–DN 間でそれぞれ IPSec 通信を行うことが考えられる．

3.4 スケーラビリティ

$\mathsf{Addr}_{\mathsf{DN}}$ または $\mathsf{Addr}_{\mathsf{RN}}$ の登録を除き，LTA6 で行う処理の大半は AT での RN–DN 間の通信パケットのアドレス変換とパケットの転送であるため，AT に注目してスケーラビリティについて検討する．

機器ベンダが出荷した DN の総数を n，DN と通信をする RN の総数を m とすると，AT に設定される固定アドレスの最大数は n，一時アドレスの最大数は nm になる．また，AT におけるアドレス変換は，固定アドレスと一時アドレス一つに対して一つ設定されるため，その総数は固定アドレスと一時アドレスの個数の合計と同じである．LTA6 では，RN として DN の保守，操作，監視を行うための端末やサーバを想定しているため，m は定数であり，DN の監視や制御による通信トラヒック量はすべての DN で同程度だと考えられる．したがって，DN の総数に比例して使用アドレス数及び通信トラヒックが増大するため，機器ベンダは出荷した DN の総数に応じて AT と VN の増強を行うとよい．

また，**3.2** で述べたように，使用されていない一時アドレスを適時回収することで，AT に設定されるアドレス数とアドレス変換の設定数を減少させることができる．

3.5 負荷分散

AT の増強を行う方法として，一つの高性能な AT を用意するのではなく，VN 上に複数の AT を設置する方法が考えられる．この場合，特定の AT に処理が集中しないようにする方法について検討する．

DN に埋め込む AT アクセス情報を FQDN とし，機器ベンダの DNS サーバは，この FQDN の問合せに対して，複数の AT のアドレスをラウンドロビンで返答することで負荷分散が実現できる．また，DN に埋め込む AT アクセス情報を特定の AT を指し示す情報とし，複数の異なるアクセス情報のいずれかが DN に埋め込まれようにすることでも負荷分散が実現できる．

複数の AT を動作させる場合，AT は，DN のアドレス登録を行った DN が他の AT に登録されていないことを，DN の固定アドレス $\mathsf{FixAddr}_{\mathsf{DN}}$ に対する Duplicate Address Detection（DAD）[7] を行って確認し，複数の AT に同一の固定アドレスが設定されないようにする必要がある．また，AT は，自身の負荷が高い場合，DN からの DN のアドレス登録を拒否することで，自身の負荷が高くならないようにすることも重要である．この場合，拒否された DN は，他の AT に登録をやり直し，成功した AT を利用する．

一方，DN からの RN のアドレス登録を受け付ける AT は，それ以前に DN から DN のアドレス登録を行った AT である必要がある．固定アドレスが登録されていない AT では，一時アドレスの設定及びアドレス変換が不可能なためである．このため，複数の AT を動作させる場合，DN は，DN のアドレス登録をしたときに AT のアドレスを記憶し，RN のアドレス登録をするときはこのアドレスを利用するように動作する必要がある．

以上のように動作することで，複数の AT 間で負荷分散が可能である．

3.6 冗 長 性

AT が停止すると，その AT に $\mathsf{FixAddr}_{\mathsf{DN}}$ の登録を行った DN は RN と $\mathsf{FixAddr}_{\mathsf{DN}}$ を用いた通信ができなくなる．このため，複数の AT を設置し，DN は定期的に登録を行った AT を確認して，停止している場合は別の AT に登録を行うことで冗長性をもたせる必要がある．

また，Mobile IP において複数の Home Agent（HA）間で情報共有することで HA の冗長性を確保する技術として，Local HA to HA protocol [9] や Home Agent Reliability Protocol [10] が提案されている．これらを応用し，LTA でも複数の AT 間で情報共有が可能である．これにより，ある AT が停止しても他の AT を利用して RN–DN 間通信の継続できる．

一方，すべての AT は同一の VN に接続されていなければならないため，VN は上位ネットワークとの接続を多重化しておく必要がある．

4. 関連技術との比較

固定の IP アドレスまたは FQDN を用いたアクセス技術に，Dynamic DNS，Mobile IP（MIP4，MIP6）がある．また，アドレス変換の代表的な技術に Network Address Translation（NAT）[11] がある．更に，機器における複雑な処理を不要とする技術に，Proxy Mobile IPv6（PMIP6）[12]，Network Address Translation - Protocol Translation（NAT-PT）[13] などがある．以下，これらの技術と LTA6 を比較する．

4.1 Dynamic DNS

Dynamic DNS は，アドレスと FQDN の対応を動的に管理するシステムであり，機器のアドレスが変化した場合は，リアルタイムに DNS サーバ上の登録アドレスを更新することで，常に固定の FQDN で機器にアクセスすることを可能とする．しかし，機器のアドレスは設置場所によって変化するため，通信が特定のノードを常に経由するとは限らない．LTA6 は，すべての通信が機器ベンダが管理する AT を通過する．このため，機器ベンダが機器に対する通信を監視・制御して不正なアクセス（DoS アタック，ブルートフォースアタック，ポートスキャンなど）の検知と遮断を行う場合，LTA6 の方が容易である．

4.2 Mobile IP

Mobile IP（MIP4 及び MIP6）は，IP の移動透過性を提供する技術であり，機器設置した場所におけるアドレスを HA に登録することで，常にホームアドレスと呼ばれる固定のアドレスで通信することを可能とする．しかし，Mobile IP では機器に複雑な IP 処理（IP トンネル処理，特殊なヘッダの処理など）が必要で，機器の実装コストや処理負荷が増大してしまう．LTA6 は，固定のアドレスで通信するために必要な処理の大半は AT で実行され，機器に複雑な仕組みを実装する必要はない．このため，LTA6 は，機器の開発コストが大きく増大せず，機器の処理負荷も増大しないという利点をもつ．

一方，LTA6 は **3.1** で述べたように末端同士の IPSec 通信ができない欠点をもつが，Mobile IP では末端同士の IPSec 通信が可能である．また，Mobile IP では，LTA6 に比べて使用するアドレス数が少なくて済む．Mobile IP の HA における使用アドレス数は 1 で，トンネルの設定数は MN の総数である．トンネルの設定をアドレス変換の設定と考えると，RN の総数を定数，MN の総数と DN の総数が同数とした場合，LTA6 におけるアドレス変換の設定数は Mobile IP の HA におけるトンネルの設定数に比較して (RN の総数 + 1) 倍となり，LTA6 の AT の方がアドレスの設定数，アドレス変換の設定数とも大幅に多い．

機器に複雑な IP 処理の実装が不要となるように MIP6 を拡張した技術として，PMIP6 が存在する．し

かし，PMIP6 は機器が接続されるネットワーク上のすべてのアクセスルータに特殊な機能をもたせる必要があるため，普及へのハードルが高い．LTA6 では，機器ベンダが自身の出荷する機器に AT にアドレスを登録する小さい特殊機能を搭載するだけでよく，機器ユーザ及び機器ユーザが利用するネットワーク事業者は，機器とは別に特別な装置を用意する必要がないため普及へのハードルが低い．

4.3 NAT

プライベートアドレスを設定した複数のノードで共通のグローバルアドレスを共有する IPv4 のアドレス変換技術に NAT が存在する．NAT では，パケットの送り元，あて先のどちらか一方のアドレス変換を行うが，LTA6 では，パケットの送り元，あて先ともに同時に変換する点が異なる．

NAT の機能を IPv6 に対応させ，MIP6 と併用すると，LTA6 と同様に HA でのアドレス変換処理，トラヒック監視が実現できる．しかし，この場合も MN は MIP6 の機能を搭載する必要があるので，LTA6 に比べて実装は複雑となる．NAT と MIP6 を併用した場合の使用アドレス数及びアドレス変換の設定数ともに HA の管理する MN の総数である．RN の総数を定数，MN の総数と DN の総数が同数とした場合，LTA6 におけるアドレスの設定数とアドレス変換の設定数はともに NAT と MIP6 を併用する場合に比較して (RN の総数＋1) 倍となり，LTA6 の AT の方がアドレスの設定数，アドレス変換の設定数とも大幅に多い．

NAT に IPv4–IPv6 間のプロトコル変換の機能を追加し，IPv4 から IPv6 への移行期において，IPv4 のみのネットワークと IPv6 のみのネットワークの橋渡しを行うために考案された技術として，NAT-PT が存在する．NAT-PT は，IPv4 プライベートアドレスとこのアドレスを下位 64 ビットに埋め込んだ IPv6 アドレスの間のアドレス変換を行う．IPv6 アドレスのプレフィックスは NAT-PT をサポートしたルータが設置される IPv6 ネットワークと同じである．機器ベンダは，NAT-PT をサポートしたルータを運用することで，機器に対して機器ベンダネットワーク内から固定の IPv4 プライベートアドレスで通信可能となる．しかし，NAT-PT では固定アドレスが IPv4 プライベートアドレスであるため，機器ベンダネットワーク内に存在しないノードから固定アドレスを用いて機器と通信することは不可能である．

5. 実装と評価

Linux 2.6 上で LTA6 の実装を行った．これをもとに，MIP6 との実装コストの比較を行う．また，遅延測定結果をもとに，LTA6 の利用に伴う遅延増加が実用的範囲内に収まることを示す．

なお，RN–AT 間及び AT–DN 間で通信可能なパケットの最大サイズ Path MTU（Maximum Transmission Unit）より大きいサイズのパケットを RN/DN から送信すると，送信時にパケットのフラグメントが発生する．この場合，AT では，フラグメントされたパケットの断片をすべて受信してもとのパケットを再構成し，その後にアドレス変換を行う必要がある．しかし，DN の保守，操作，監視にかかわる情報を含むパケットのサイズは，通常 Path MTU より小さいと想定される．このため，実装はフラグメントされたパケットに対する AT の処理を除いており，RN/DN 上でフラグメントが発生しない条件下で評価を行う．

5.1 実　　装

AT と DN にそれぞれ以下に示す機能を実装し，LTA6 の稼動環境を構築した．RN には，LTA6 特有の処理がなく，特別な実装は不要である．なお，以下に列挙する各機能の括弧内は，相当する動作手順，または詳細を明記した節である．

［AT へ実装した機能］

- 固定/一時アドレスの生成，設定，管理（(I-3)，(R-2)，(D-3)）
- DN からの登録の受付（(I-2)，(D-2)）
- RN からのパケット監視（(R-2)）
- Packet ソケット（PF_PACKET）を用いたパケットの取得とそのアドレス変換（(R-3)，(R-5)，(D-7)，(D-9)）
- ICMPv6，TCP，UDP ヘッダのチェックサム再計算（(R-3)，(R-5)，(D-7)，(D-9) 及び **3.1**）
- ハッシュ関数に MD5 を用いた DN とのチャレンジ・レスポンス認証（(I-2)，(D-2) 及び **3.3**）
- 不正なパケットの遮断（**3.3**）
- 一定期間未使用の一時アドレスの回収（**3.2**）

［DN へ実装した機能］

- $\mathsf{Addr}_{\mathsf{DN}}$ と MAC アドレスの取得（(I-1)）
- AT への $\mathsf{Addr}_{\mathsf{DN}}$ と MAC アドレスの登録（(I-2)）
- AT への $\mathsf{Addr}_{\mathsf{RN}}$ の登録と $\mathsf{TmpAddr}_{\mathsf{RN,DN}}$ の取得（(D-2)）

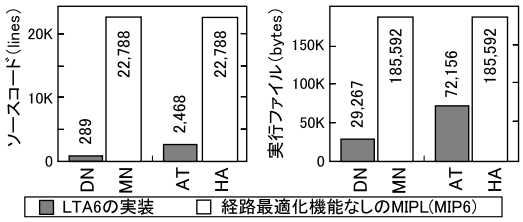

図 7　LTA6 の実装，MIPL のソースコード及び実行ファイルのサイズの比較
Fig. 7　Comparison of source code and binary file size of an implementation of LTA6 and MIPL.

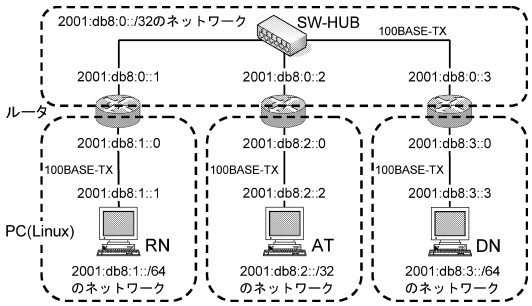

図 8　LTA6 の実装の評価環境
Fig. 8　Network topology for the evaluation of the implementation of LTA6.

表 1　図 8 の評価環境のスペック
Table 1　Specifications of the network presented in Fig. 8.

ルータ		YAMAHA RTX1000, 100BASE-TX
SW-HUB		BUFFALO LSW10/100-5NWP, 100BASE-TX
PC	AT	Intel モバイル Celeron 1.33 G, 128 M, 100BASE-TX
	RN,DN	Intel PentiumIII-M 1.20 G, 384 M, 100BASE-TX

- ハッシュ関数に MD5 を用いた AT とのチャレンジ・レスポンス認証（(I-2)，(D-2) 及び **3. 3**）
- 一時アドレス保存と有効期間チェック（(D-1), (D-5)）

この LTA6 の実装は，ユーザランドで行っており，カーネルの変更は不要である．

5. 2　評　　価

LTA6 の実装と Linux2.6 における MIP6 の実装 MIPL [14], [15] で，ソースコードの行数と実行ファイルのバイト数を比較し，LTA6 の実装コストが MIP6 より少ないことを示す．なお，**4.** の MIP6 以外の技術については，潤沢なアドレスをもつ IPv6 を用いること，機器ベンダが管理するノードで通信の監視・遮断ができること，任意ノードに対して固定アドレスを用いた機器との通信を許可できることなどが LTA6 の利点であるため，実装のサイズによる比較は行わない．LTA6 と MIP6 の比較は，ネットワークトポロジー的に同位置の LTA6 の DN と MIP6 の Mobile Node（MN），LTA6 の AT と MIP6 の HA で行った．

各実装のソースコードの行数及び実行ファイルのバイト数を図 7 に示す．なお，LTA6 の実装との比較を公平に行うため，MIPL からは経路最適化の機能を削除してある．また，MIPL はユーザランド以外にカーネル内の処理も必要であるが，ユーザランドに限定して比較を行った．なぜならば，LTA6 の実装はカーネル内の処理を加えないユーザランドのみの MIPL より明らかに小さいためである．図 7 より，次のことが分かる．

- LTA6 の DN は，ソースコードが MIP6 の MN に必要なソースコードの 1%強，実行ファイルが MIP6 の MN の実行ファイルの 16%弱である．したがって LTA6 は，MIP6 に較べて機器の実装コストを抑えつつ，固定アドレスを用いた機器との通信が実現可能といえる．
- LTA6 の AT は，ソースコードが MIP6 の HA に必要なソースコードの 11%弱，実行ファイルが MIP6 の HA の実行ファイルの 39%弱である．今回の LTA6 の実装は基本的な機能のみとし，エラー処理はないため厳密な比較は困難だが，AT の実装コストは MIP6 の HA より抑えることが可能といえる．また，LTA6 はユーザランドで実装可能で，カーネルの拡張を要する MIP6 より開発は容易である．

次に，図 8，表 1 に示すネットワーク環境で，LTA6 の実装の動作検証を行った．各ノード間を接続するケーブルの長さは 1.5 m で，ケーブルによる伝搬遅延は無視できるため，各ノード間の往復通信遅延（Round Trip Time：RTT）は各ノードやルータ上で，パケット処理やルーチング処理に要する時間にほぼ等しい．

100回のICMPv6 ECHO REQUEST/RESPONSE の送受信で測定した各ノード（AT と DN，AT と RN）間の RTT を表 2 に示す．また，RN と DN が LTA6 を用いて AT 経由で通信する場合と，RN と DN が直接通信する場合において，同様に測定した RTT を表 3 に示す．

LTA6 を用いた場合の RN–DN 間の平均 RTT は，RN–AT 間と AT–DN 間の平均 RTT の合計より 0.496 ms 長い．これは，AT におけるパケットのアドレス変換と転送の処理時間と考えられる．ところが，

表 2　図 8 の評価環境における各ノード間の RTT
Table 2　RTT between function nodes in the network presented in Fig. 8.

		最小（ms）	平均（ms）	最大（ms）
RN–AT 間	(2001:db8:1::1 ⇔ 2001:db8:2::2)	1.761	1.925	2.354
AT–DN 間	(2001:db8:2::2 ⇔ 2001:db8:3::3)	1.837	1.927	2.416

表 3　RN–DN 間の RTT の測定結果
Table 3　Measurement results of RTT between DN and RN.

		最小（ms）	平均（ms）	最大（ms）
RN–DN 間（LTA6）	(2001:db8:3::3 ⇔ 2001:db8:1::1)	4.104	4.348	5.453
RN–DN 間（直接）	(2001:db8:3::3 ⇔ 2001:db8:1::1)	1.827	1.922	2.350

表 4　トンネル処理による遅延の測定結果
Table 4　Measurement results of delay for tunneling processing.

		最小（ms）	平均（ms）	最大（ms）
トンネル処理なし	(2001:db8::1 ⇔ 2001:db8::2)	0.186	0.277	0.308
トンネル処理あり	(2001:db8:1:: ⇔ 2001:db8:2::)	0.222	0.355	0.452

この値は，表 2，表 3 の各行における RTT の最大値と最小値の差（0.523 ms から 1.349 ms）比べて小さい．したがって，LTA6 による RN–DN 間の通信遅延の増加は，AT の中継による経路長の増加が支配的といえる．LTA6 では，RN として DN の保守，操作，監視を行うための端末やサーバを想定している．これらは，機器ベンダによって運用され，VN 内に設置される場合が多いと考えられる．この場合，RN–DN 間の直接通信と LTA6 を用いた通信の経路の違いは，VN 内で AT を経由するかしないかである．RN–AT 間にルータを設置しないことで，LTA6 による通信遅延の増加は更に抑えることができる．したがって，この通信遅延の増加は，実用上問題とはならない．

DN が AT 対して行う DN のアドレス登録及び RN のアドレス登録に要する通信コストは問題とならない．DN のアドレス登録は，DH に DN が接続されたときや DN のアドレスが変化したときに実行され，頻繁に実行されることはない．RN のアドレス登録は，(D-1) と (D-5) の手順により，一度 AT から取得した一時アドレスが有効である間は実行されない．また，RN として DN の保守，操作，監視を行うための端末やサーバを想定しているためその数は固定である．このため，RN のアドレス登録は，一時アドレスの有効期間内に最大でも RN の数しか実行されない．したがって，DN のアドレス登録及び RN のアドレス登録ともに実行頻度は低く，実用上問題とはならない．

最後に，トンネル処理を行わないことによる LTA6 の遅延面での MIP6 に対する優位性を示す．図 9 に示すネットワーク環境で，RN/DN として用いたものと

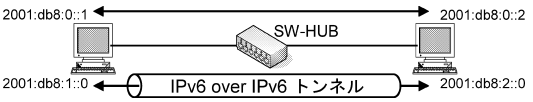

図 9　トンネル処理の遅延の評価環境
Fig. 9　Network topology for the evaluation of the delay for tunneling processing.

同一スペックの 2 台の PC を使い，トンネル処理に要する処理時間の測定を行った．トンネルを経由した場合と直接通信した場合で，100 回の ICMPv6 ECHO REQUEST/RESPONSE の送受信で測定した RTT を表 4 に示す．トンネル処理がある場合は，ない場合に比べて平均で 0.078 ms 余分に時間を要している．この時間は，2 台の PC それぞれがトンネル処理に要した時間の合計であり，2 台の PC は同一スペックであることから，単一の PC で送信と受信の双方のトンネル処理に要した時間の合計は 0.039 ms である．今回は PC を用いて評価を行ったが，PC ほどの処理能力をもたない機器の場合，より多くの処理時間を要すると考えられる．LTA6 は，MIP6 とは異なり，トンネル処理が不要であるため，このような処理時間は発生しない．

6. むすび

本論文では，機器ベンダが管理するネットワークにアドレス変換装置を設置して双方向のアドレス変換を行うことで，遠隔から機器に常に固定の IPv6 アドレスで通信可能とする手法 LTA6 を提案した．本手法では，固定アドレスで機器と通信するための処理の大半をアドレス変換装置で実行し，機器に対する大きな機

能追加や処理負荷なしに，遠隔からの機器の保守，操作，監視を容易に実現可能としている．また，固定のIPv6 アドレスを利用した通信は常にアドレス変換装置を経由するため，機器ベンダは機器に対する一元的なセキュリティ対策を実施可能である．

Linux 上で LTA6 を実装し，MIP6 を機器に実装する場合に比べて，機器に必要な実装コストを低く抑えられることを確認した．

なお，LTA6 では，アドレスの変換を伴うため末端のノード間で直接 IPSec 通信を行うことはできない．今後の課題として，末端のノード間で直接 IPSec 通信が可能な手法の検討が挙げられる．

文　献

[1] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, “Dynamic updates in the domain name system (DNS UPDATE),” RFC 2136, April 1997.

[2] B. Wellington, “Secure domain name system (DNS) dynamic update,” RFC 3007, Nov. 2000.

[3] C. Perkins, “IP mobility support for IPv4,” RFC 3344, Aug. 2002.

[4] C.E. Perkins and D.B. Johnson, “Mobility support in IPv6,” Proc. 2nd Annual International Conference on Mobile Comuputing and Networking (MobiCom’95), pp.22–37, Nov. 1996.

[5] D. Johnson, C. Perkins, and J. Arkko, “Mobility support in IPv6,” RFC 3775, June 2004.

[6] R. Hinden and S. Deering, “IP Version 6 addressing architecture,” RFC 4291, Feb. 2006.

[7] S. Thomson and T. Narten, “IPv6 stateless address autoconfiguration,” RFC 2462, Dec. 1998.

[8] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, “Dynamic Host configuration protocol for IPv6 (DHCPv6),” RFC 3315, July 2003.

[9] V. Devarapalli, R. Wakikawa, and P. Thubert, “Local HA to HA protocol,” Internet-Draft draft-devarapalli-mip6-nemo-local-haha-01, March 2006.

[10] R. Wakikawa, “Home Agent Reliability Protocol,” Internet-Draft draft-ietf-mip6-hareliability-03, Nov. 2007.

[11] P. Srisuresh and K. Egevang, “Traditional IP Network Address Translator (Traditional NAT),” RFC 3022, Jan. 2001.

[12] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6,” Internet-Draft draft-ietf-netlmm-proxymip6-12, April 2008.

[13] G. Tsirtsis and P. Srisuresh, “Network address translation - Protocol translation (NAT-PT),” RFC 2766, Feb. 2000.

[14] Go-Core Project, “MIPL:Mobile IPv6 for Linux,” http://www.mobile-ipv6.org/

[15] USAGI Project, “UMIP:USAGI-Patched mobile IPv6 for linux,” http://www.linux-ipv6.org/memo/mipv6/

（平成 19 年 12 月 21 日受付，20 年 5 月 7 日再受付）

黒木　秀和　（正員）

平 8 東工大・工・情報卒．平 10 同大大学院修士課程了．平 15（株）インターネット総合研究所入社．平 16（株）IRI ユビテック（現（株）ユビテック）入社，現在に至る．現在，静岡大創造科学技術大学院在学中．IPv6 とその応用に関する研究に従事．情報処理学会，IEEE 各会員．

井上　博之　（正員）

昭 62 阪大・工・電子卒．平元同大大学院修士課程了．同年住友電気工業（株）入社．平 12 奈良先端大学院大学博士後期課程了．平 12（株）インターネット総合研究所入社．平 16（株）IRI ユビテック（現（株）ユビテック）入社．平 19 広島市立大大学院情報科学研究科講師，現在に至る．IPv6，センサネットに関する研究に従事．情報処理学会，IEEE 各会員．

荻野　司

昭 61 長岡技術科学大大学院修士課程了．同年キヤノン（株）入社，平 7 ファストネット（株）出向．平 12（株）インターネット総合研究所入社．平 15TAU 技研（株）（現（株）ユビテック）代表取締役社長，現在に至る．現在，静大創造科学技術大学院及び同大情報学部客員教授．

石原　進　（正員）

平 6 名大・工・電気卒．平 11 同大大学院工学研究科博士後期課程了．平 10 日本学術振興会特別研究員．平 11 静岡大学情報学部助手．平 13 同大工学部助教授．現在，静岡大学大学院創造科学技術研究部准教授．博士（工学）．平成 9 年電気通信財団テレコムシステム技術学生賞．モバイルコンピューティング，無線環境用 TCP/IP，モバイルアドホックネットワークに関する研究に従事．情報処理学会，IEEE，ACM 各会員．