情報処理学会論文誌 Vol. 49 No. 6 1763–1777 (June 2008)

LTAEAv6：軽量IP機器に埋め込まれたIPv6アドレスへの位置透過なアクセス手法

黒木秀和[†1,†2] 井上博之[†3]
荻野司[†4] 石原進[†2]

近年，IP 通信機能が搭載された様々な機器（情報家電，センサデバイス，監視カメラなど）が出荷されている．機器に固定の IP アドレスを埋め込み，このアドレスで機器とつねに通信できれば，機器の現在のアドレスを別途管理，把握する必要がなく，遠隔の場所から機器の保守，操作，監視を行うことが容易になる．筆者らは，固定の IPv6 アドレスを埋め込んだ機器と任意の IP ノード間の，このアドレスを用いた通信を可能にする手法を提案する．この手法では，機器が接続されるネットワーク上のゲートウェイは Network Mobility Basic Support（NEMO BS）のモバイルルータを拡張した機能を持ち，機器はこのゲートウェイと連携して動作する．ゲートウェイは，機器に埋め込んだアドレスの位置透過を実現する処理の大半を実行し，機器に必要な機能は，固定のアドレスの設定や機器に埋め込んだ情報の通知などわずかなものに限定する．こうすることで，機器の開発コストを削減する．この手法は，固定の FQDN で通信可能な DNS や Dynamic DNS とは異なり，埋め込んだアドレス宛の不正アクセスを防ぐことができる．さらに，固定のアドレスで通信可能な IP Mobility Support for IPv4（MIP4）や IP Mobility Support in IPv6（MIP6）とは異なり，機器に複雑な処理を必要としない．

LTAEAv6: Location Transparent Access to Embedded Address for IPv6 in Lightweight IP Devices

Hidekazu Kuroki,[†1,†2] Hiroyuki Inoue,[†3]
Tsukasa Ogino[†4] and Susumu Ishihara[†2]

These days, IP communication functions are installed into various devices like information appliances, sensor devices, or monitoring cameras. If a fixed IP address is embedded in a device and can be used to communicate with other IP nodes, remote maintenance, control, and monitoring of the device is facilitated, because it is unnecessary to manage and to keep current addresses of devices. We propose a scheme for enabling a device with an embedded fixed IPv6 address to communicate with any IP node using this address. In this scheme, the gateway on the network connected to the device has extended functions as a mobile router of the Network Mobility Basic Support (NEMO BS), and the device works with the gateway. The gateway executes most processings for the location transparent of the addresses embedded in the device, and functions necessary for the device are reduced. Therefore, the development cost of the device is reduced. This scheme is different from DNS or Dynamic DNS in that illegal accesses to addresses embedded in devices are prevented. Furthermore, this is different from IP Mobility Support for IPv4 (MIP4) or IP Mobility Support in IPv6 (MIP6) in that complex processing functions are unnecessary in devices.

1. はじめに

近年，これまで IP 通信機能が搭載されることのなかった様々な機器，たとえば情報家電，センサデバイス，監視カメラなどに IP 通信機能が搭載され，これらの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きている．このような遠隔から機器へのアクセスを実現するには，機器ベンダは，機器の現在の IP アドレスや FQDN（Fully Qualified Domain Name）をつねに把握する必要がある．機器と通信を行うプログラムや機器ベンダのオペレータが，機器のアドレスや FQDN をつねに把握し，これらの情報を使って個々の機器へ接続可能とするのは困難である．また，機器のアドレスや FQDN が変化することを，機器と通信を行うプログラムやオペレータに意識させない方が良い．

機器は，機器ベンダから出荷された後，機器を所有するユーザ（機器ユーザ）のネットワークに設置される．しかし，機器ユーザごとにインターネット接続事業者（Internet Services Provider: ISP）などの上位ネットワークは異なるため，機器のアドレスや FQDN を機器

†1 株式会社ユビテックユビキタス研究所
Ubiquitous Laboratories, Ubiteq, INC.
†2 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†3 広島市立大学情報科学研究科
Graduate School of Information Sciences, Hiroshima City University
†4 株式会社ユビテック
Ubiteq, INC.

© 2008 Information Processing Society of Japan

ベンダが知ることはできない．また，機器の設置場所はつねに一定とは限らず，機器ユーザの都合，たとえば引っ越しや ISP の変更などで変化し，同時に機器のアドレスや FQDN も変化する．

機器ベンダが，あらかじめ固定のアドレスや FQDN などの一意な識別子を機器に割り当て，この識別子でつねに機器と通信可能になれば，機器ベンダが機器の保守，操作，監視を行うコストを低減可能と考えられる．なぜなら，つねに固定の識別子で機器へアクセス可能となり，機器がその設置場所において割当てられるアドレスや FQDN を管理，把握しておく必要がなくなるためである．

これを実現可能な技術として，DNS，Dynamic DNS [1),2)] がある．これらを用いると，機器ベンダはネームサーバを運用することで，機器に固定の FQDN でアクセス可能となる．しかし，DNS は，機器からネームサーバに登録されているデータを自動的に更新することはできず，Dynamic DNS は，データを自動的に更新するプログラムを機器に用意する必要がある．また，アドレスは各機器の設置場所において割り当てられたものであり，アドレスを割り当てた上位ネットワーク（ISP など）が機器ごとに異なるため，経路集約可能ではない．このため，各機器の通信をすべて監視して制御することを目的とするノードを設置することは不可能である．したがって，機器に対する不正アクセスや脆弱性への攻撃を防ぐための対策は，各機器や機器を設置するネットワークで実施する必要があり，機器ユーザのセキュリティに対する知識や機器およびネットワークの設定に依存してしまう．

また，ほかにも IP Mobility Support for IPv4 [3),4)]（MIP4），IP Mobility Support in IPv6 [5),6)]（MIP6）の技術も同じ目的のために利用できる．これらを用いると，機器はつねに固定のアドレスで通信可能となり，機器ベンダは機器の設置場所やその変化を意識する必要がなくなる．しかし，IP トンネル処理などの負荷のかかる処理を機器上で行う必要があり，機器の実装を複雑にしてしまう．なお，MIP4 の場合 FA モードを利用すると機器の実装が複雑になることはないが，MIP4 の IPv6 版である MIP6 には，MIP4 の FA モードと同等の機能は存在しない．

本稿では，機器を判別する識別子として，固定の IPv6 アドレスを機器内部に埋め込み，このアドレスを用いた機器の通信を可能とする手法—Location Transparent Access to Embedded Address for IPv6（LTAEAv6）—を提案する．本手法により以下の問題が解決する．

- 機器ベンダが，出荷した機器の管理と監視を行うには，機器に設定された IP アドレスをつねに把握する必要があるが，機器の出荷時に埋め込んだ固定の IPv6 アドレスで接続可能とする．
- MIP6 など，固定の IP アドレスで機器にアクセス可能な既存の手法では，機器に複雑で負荷のかかる処理を実装する必要があったが，これを低減させて少ない追加ソフトウェアと負荷を実現する．
- 機器に埋め込んだ固定の IPv6 アドレスを用いた通信でセキュリティ上の問題が発生すると，機器ベンダの責任となる可能性があるが，機器ベンダによるこの通信の監視と制御を可能とする．

本手法において，IPv6 アドレスを識別子として選んだ理由は，大量の機器に一意に割当て可能な量のアドレスを容易に確保することができ，アドレスの維持管理コストが安価だからである．

一般に，機器ベンダが機器を出荷する時点で，その機器がどこに設置されるかは不明である．したがって，機器に埋め込んだ IPv6 アドレスは，機器の設置場所におけるアドレスとは無関係である．このため，埋め込んだ IPv6 アドレスを用いた通信の機器宛パケットが，機器の設置場所へルーティングされる経路は存在せず，機器に埋め込んだ IPv6 アドレスは，通信に使用できない孤立したアドレスになる．

この問題を解決するために，本手法は，Network Mobility Basic Support [7),8)]（NEMO BS）技術を応用している．NEMO BS は，モバイルルータと呼ばれる装置に接続される固定のネットワークプレフィックスを持つネットワーク（モバイルネットワーク）の移動透過性を実現する技術である．本手法では，固定のネットワークプレフィックスに相当する情報を埋め込んだ機器が，その設置場所のゲートウェイと連携し，ゲートウェイをモバイルルータ，機器とゲートウェイの 2 つで構成されるネットワークをモバイルネットワークとした，NEMO BS と同様の動作をする．

本手法により，機器が，複雑な処理を行うことなく，任意のノードとつねに固定の IPv6 アドレスで通信可能とする．機器に複雑な処理が必要な MIP4，MIP6 に比べて，機器のソフトウェア量を少なくすることができる．さらに，機器の処理コストを低減させ，機器の開発コストも削減することができる．また，本手法による任意のノードと機器との固定の IPv6 アドレスを用いた通信は，機器ベンダによって設置される管理ポイントをつねに経由する．この管理ポイントで，固定の IPv6 アドレス宛に対する不正アクセスの検知と遮断を行うことで，機器に対して機器ベンダによる一括したセキュリティ対策を適用可能とする．さらに，本手法では，機器の通信相手は IPv6 の基本機能以外の特別な機能を必要としない．

以下，2 章では関連する技術とその問題点について述べ，3 章では本稿で提案する手法

© 2008 Information Processing Society of Japan

LTAEAv6 について述べるとともに，関連技術との比較を行う．さらに，4 章では LTAEAv6 の実装とその評価を行い，5 章でまとめを行う．

2. 関 連 技 術

特定の IP ノードに対してつねに固定の識別子でアクセス可能にする既存技術として，FQDN を識別子とした DNS，Dynamic DNS[1),2)]，アドレスを識別子とした Mobile IP（MIP4[3),4)]，MIP6[5),6)]），IP ノードを識別する情報を個体識別用と位置識別用に分離して個体識別用の情報で通信可能とするいくつかの技術がある．本章では，これらの既存技術について概観する．

2.1 DNS，Dynamic DNS

DNS および Dynamic DNS は，アドレスと FQDN の対応を管理するシステムである．ノードのアドレスが変化した場合，ネームサーバ上のノードの FQDN に対応したアドレスを更新する．こうすることで，つねに固定の FQDN でノードにアクセスすることが可能となる．DNS は，ネームサーバの管理者によってアドレスを更新する必要があるが，Dynamic DNS は，リモートからリアルタイムにアドレスを更新することが可能である．

一般に，設置場所が変わることのあるノード（ノート PC，PDA など）は，設置場所ごとに接続するネットワークやその上位ネットワーク（ISP など）も変わるため，そのアドレスはつねに同じとはならない．アドレスが一定でない場合，アドレスごとにその経路情報が異なるため，ノードの通信が特定の中継ポイントをつねに経由するとは限らない．すなわち，ノードのすべての通信が通過し，ノードに対する不正アクセス（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）の検知と遮断が可能な中継ポイントは存在しない．

機器ベンダにより出荷前に固定のアドレスや FQDN が埋め込まれた機器に対して，これらの情報を基に外部から機器に対して不正アクセスが行われた場合，これらの情報を埋め込んで機器を出荷した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，埋め込んだ情報に基づいて発生する機器の通信を監視し，場合によってはこの通信を制御できる必要がある．

DNS および Dynamic DNS の場合，各ノードの通信がつねに特定の中継ポイントを経由することは不可能なため，機器ベンダによる機器に対する不正なアクセスの検知と遮断は困難である．

2.2 Mobile IP

IP Mobility Support for IPv4（MIP4）および IP Mobility Support in IPv4（MIP6）は，ノードに移動透過性を提供する技術である．MIP4 は IPv4 用であり，MIP6 は IPv6 用である．これらの技術では，ノードに対して外部からつねに固定のアドレスでアクセスすることを可能とする．そして，通信を行っている最中にノードが移動することによって，ノードが接続されるネットワークが変化した場合でも，この通信は途切れることなく継続可能である．また，ホームエージェントにおいて，固定のアドレスを利用したノードの通信トラヒックの監視と制御を行うことも可能である．

しかし，Mobile IP を使用するには，ノードに対して MIP4 や MIP6 の複雑な IP 処理（IP トンネル処理，アドレス登録処理，経路最適化処理など）を実装する必要がある．このため，ノードの実装コストが増大してしまうという問題がある．また，MIP4 の場合 FA モードを利用することで機器の実装は複雑にしないようにできる．しかし，MIP4 の IPv6 版である MIP6 には，MIP4 の FA モードと同等の機能は存在しない．このため，本稿で前提とする IPv6 では FA モードの仕組みを利用することはできない．

MIP6 に対して MIP4 の FA モードの仕組みを導入した場合を考えると，単一ノードを対象とするか，あるいはネットワークを対象とするかの相違はあるが，NEMO BS と同等になると考えられる．

2.3 そ の 他

上記にあげた以外にも，固定のアドレスまたは FQDN を用いた他ノードとの通信を実現する手法として，Location Independent Network Architecture[9)]（LINA），Location Independent Networking for IPv6[10)]（LIN6），Host Identity Protocol[11)]（HIP），Locator/ID Separation Protocol[12)]（LISP），Level 3 Multihoming Shim Protocol[13)]（Shim6）などの技術が存在する．これらは，ノードを識別するための情報を位置識別用と個体識別用の情報に分離して扱う．そして，ノードが接続されるネットワークやノードに割り当てられるアドレスが変化した場合は，位置識別用の情報は変化するが個体識別用の情報は変化しないという特長を持つ．このため，通信を行う双方のノードが個体識別用の情報を用いることで，各ノードの設置場所がどこであってもつねに個体識別用の情報のみで相手ノードの識別し，通信可能とする．

しかし，これらの手法では，通信を行う双方のノードに同一の手法が実装されている必要がある．このため，通信を行うどちらか一方にこれらの手法が実装されていないか，双方で異なる手法が実装されている場合は通信が不可能となる問題がある．

© 2008 Information Processing Society of Japan

3. LTAEAv6

本章では，本稿で提案する手法である LTAEAv6 について述べる．LTAEAv6 は，固定のアドレスを埋め込んだ機器が，特別なゲートウェイの下位ネットワークに接続され，任意のノードとつねに固定のアドレスで通信可能とする．本手法では，機器メーカが出荷前の機器に対して固定のアドレスを埋め込むことを想定している．このアドレスを用いた機器の通信を実現し，機器に必要な処理の実装を必要最小限にして，機器ベンダによる機器の開発コストを削減することを目的としている．さらに，機器ベンダが，機器に埋め込んだアドレス宛に対する不正アクセスの検知と遮断を行えるようにする．

本手法では，IPv6 ネットワークの移動透過性を実現する NEMO BS の技術を応用し，NEMO BS のモバイルルータを拡張した機能を持つゲートウェイにおいて，ゲートウェイにつながる機器と任意のノードの，固定のアドレスを用いた通信を可能としている．このゲートウェイは，自身につながる機器よりネットワーク情報を通知され，このネットワーク情報に基づいて各機器ごとに複数の異なるネットワークを構成する点が，NEMO BS におけるモバイルルータとは異なる．機器およびゲートウェイは，次のように動作する．機器は，自身に埋め込まれたアドレスやネットワークプレフィックス長などをゲートウェイに通知する．このアドレスとネットワークプレフィックス長をもとに，機器とゲートウェイは，この 2 つのみで構成されるネットワークを構築する．ゲートウェイは，このネットワークをモバイルネットワークとして，NEMO BS のモバイルルータと同様の動作を行う．

以下，まず初めに，LTAEAv6 のベースとなる NEMO BS について説明し，さらに，LTAEAv6 の詳細について述べる．その後，関連技術との比較を行う．

3.1 NEMO BS

LTAEAv6 が利用している NEMO BS は，ノード単体の単一の IPv6 アドレスに対して移動透過性を提供する MIP6 を拡張し，移動するネットワーク上の全 IPv6 アドレスに対して移動透過性を提供する技術である．なお，図および本文中のホームリンク（Home Link: HL），出先リンク（Foreign Link: FL），モバイルネットワーク（Mobile Network: MN），モバイルルータ（Mobile Router: MR），モバイルネットワークノード（Mobile Network Node: MNN），通信相手ノード（Correspondent Node: CN），モバイルネットワークプレフィックス（Mobile Network Prefix: MNP），ホームエージェント（Home Agent: HA），ホームアドレス（Home Address: HoA），気付けアドレス（Care-of Address: CoA）の各用語の意味は，文献 6)，文献 8)，文献 14)，および文献 15) に記載されているため，ここでは省略する．

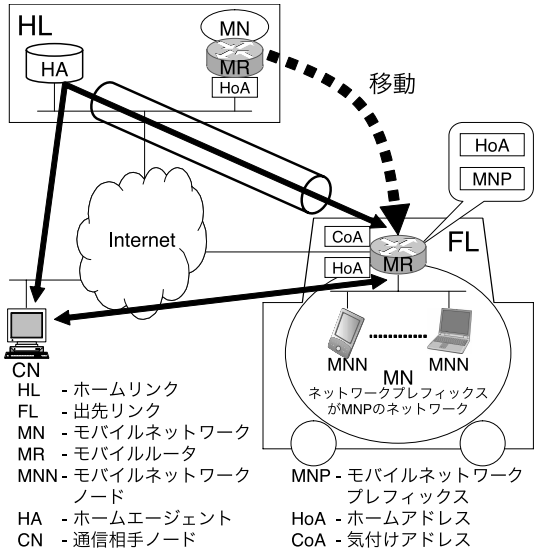

図 1　NEMO BS のシステム構成
Fig. 1　System overview of NEMO BS.

図 1 に示すように，NEMO BS では，MR の下位ネットワークのネットワークプレフィックスとして，MR に一意の MNP を割り当てる．MR は，自身に割り当てられた MNP を管理対象とする HA との間に IP トンネルを構築する．そして MR は，MNP に含まれるアドレスを送り元とする通信パケットを，IP トンネルを介して HA に転送する．また HA は，MNP に含まれるアドレスを宛先とする通信パケットを，IP トンネルを介して MR に転送する．このように動作することで，MR に接続された下位ネットワーク上の各ノードが，任意のノードとつねに MNP をネットワークプレフィックスとして含む固定の IPv6 アドレスで通信可能とする．

FL において，MN に接続された MNN が，MR に設定された MNP をネットワークプレフィックスとして含むアドレスを用い，CN と通信を開始するための動作手順を**図 2** および以下に示す．

まず，MNN を含む MN を下位ネットワークとして持つ MR が FL に接続され，FL に接続されている側の MR のネットワークインタフェースに対して FL におけるアドレスで

© 2008 Information Processing Society of Japan

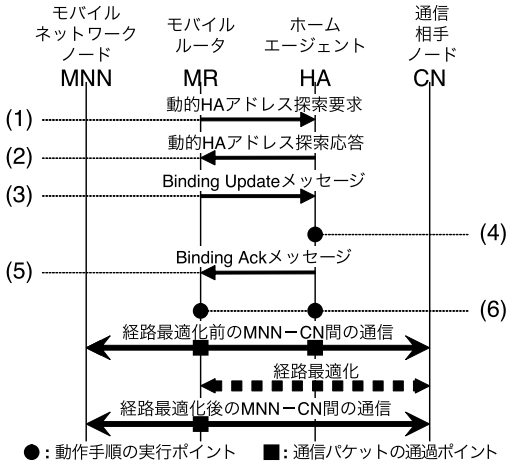

図 2　NEMO BS の動作手順
Fig. 2　Operating procedures of NEMO BS.

ある CoA が設定されているものとする．また，MR は，あらかじめ HoA および MNP が設定されており，MN 上の全 MNN に対して MNP をネットワークプレフィックスとするルータ広告[16]（RA）メッセージを送信しているものとする．すなわち，MN 上のすべての MNN は，MNP をネットワークプレフィックスとして含む IPv6 アドレスが設定されているものとする．

(1)　MR は，動的 HA アドレス探索要求メッセージを HoA に対応する予約された動的 HA アドレス探索用のエニーキャストアドレス[17] 宛にユニキャスト送信する．

(2)　HA は，自身のアドレスを含む動的 HA アドレス探索応答メッセージを MR 宛にユニキャスト送信する．

(3)　MR は，自身の HoA と自身の FL におけるアドレス CoA と MNP を含む Binding Update メッセージを，判明した HA のアドレス宛にユニキャスト送信する．

(4)　HA は，受信した Binding Update メッセージに含まれる HoA と CoA と MNP を用いて MN の登録を行う．

(5)　HA は，MR に Binding Ack メッセージをユニキャスト送信し，MN の登録が完了したことを通知する．

(6)　HA と MR は，HA–MR 間の IP トンネルを構築する．さらに，HA は，MR の HoA 宛に対する近隣発見[18] の要求に対し，MR の代わりに自身が応答するように設定する．

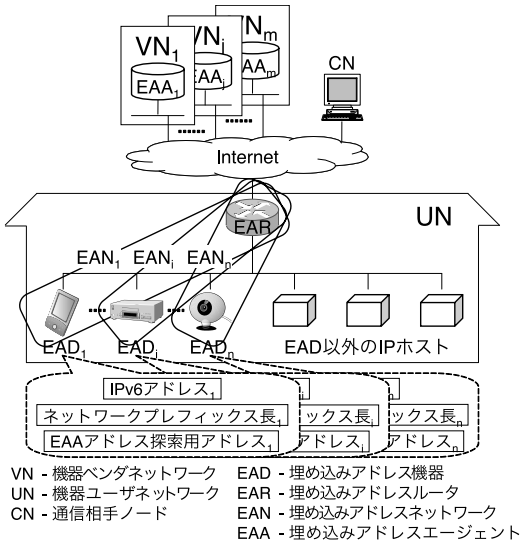

図 3　LTAEAv6 のシステム構成
Fig. 3　System overview of LTAEAv6.

以上の動作手順により，MN 上の各 MNN は，MNP をネットワークプレフィックスとして持つ固定のアドレスを用いて任意の CN と通信することができる．この通信は，MR と HA の間に構築された IP トンネルを通過して，HA を経由する．HA を経由する MNN–CN 間の通信は，経路が冗長になる．これを避けるため，NEMO BS では HA を経由しないように MR–CN 間の経路を最適化する仕組みも持つ．

NEMO BS は，MIP6 とほぼ同じ動作をするが，末端のノードではなくルータとその下位ネットワーク全体に移動透過性を実現する点が MIP6 と異なる．末端のノードである MNN には，基本的な IPv6 通信機能があればよい．

3.2　LTAEAv6 の詳細

3.2.1　LTAEAv6 のシステム構成

LTAEAv6 のシステム構成を**図 3** に示す．LTAEAv6 では，埋め込みアドレス機器（Embedded Address Device: EAD），埋め込みアドレスルータ（Embedded Address Router:

© 2008 Information Processing Society of Japan

EAR），埋め込みアドレスエージェント（Embedded Address Agent: EAA），CN が存在する．EAD は EAR に接続され，EAR，EAA および CN は，インターネットに接続される．以下，EAD，EAR，EAD と EAR で構成される埋め込みアドレスネットワーク（Embedded Address Network: EAN），EAA，CN について説明する．

EAD は，機器ベンダから出荷される機器であり，情報家電，センサデバイス，監視カメラなどである．EAD は，NEMO BS における MNN に相当する．EAD は，そのネットワークインタフェースが，機器ユーザネットワーク（UN）に接続されている．EAD には，機器ベンダによって出荷時に一意の IPv6 アドレス，ネットワークプレフィックス長および EAA アドレス探索用アドレスが埋め込まれている．その詳細は 3.2.2 および 3.2.3 項で述べる．

EAR は，内側と外側の 2 つのネットワークインタフェースを持ち，UN と上位ネットワーク（ISP など）を接続するためのゲートウェイとして機能する．EAR は，NEMO BS における MR に相当する．EAR の外側ネットワークインタフェースは，上位ネットワークを介してインターネットに接続されている．さらに，EAR の内側ネットワークインタフェースは，UN に接続されている．上位ネットワークより EAR の外側ネットワークインタフェースに割り当てられるアドレスが，EAR の CoA である．なお，NEMO BS における MR は，CoA とは別に HoA や MNP を持つが，EAR は，HoA および MNP に相当する情報を EAD より通知される．

EAD のネットワークインタフェースと EAR の内側ネットワークインタフェースは同一リンクローカルネットワークで接続され，EAR と EAD のペアで UN の物理ネットワークの構成によらない仮想的なネットワークである EAN を構成する．EAN は，NEMO BS における MN に相当する．EAR は，複数の EAD が同時に接続されてもよく，それぞれの EAD ごとに異なる EAN を構成するとともに，EAN ごとに独立した MR として動作する．EAD および EAR は，UN の物理ネットワークを構成する一部でもあり，EAR は UN のゲートウェイである．すなわち，EAD は，UN と EAD ごとに EAR と構成される EAN の 2 つのネットワークに属する．また，EAR は，UN と EAD ごとに EAR と構成される複数の EAN のすべてのネットワークに属する．なお，UN には，EAD 以外の IP ホストも接続され，これらは，EAR をゲートウェイとしてインターネット上の任意のノードと通信可能である．

EAA は，機器ベンダネットワーク（VN）に接続され，EAD を出荷する機器ベンダによって管理される．EAA は，NEMO BS における HA に相当する．また，EAA は，機器ベンダが出荷する各 EAD に一意となるように埋め込まれている IPv6 アドレスと，この IPv6 アドレスおよび各 EAD に埋め込まれているネットワークプレフィックス長から生成される埋め込みアドレス（詳細は 3.2.2 項で述べる）のすべてを包含するアドレスブロックを管理する．さらに，EAA は，EAR の CoA とこのアドレスブロックに含まれる EAN のネットワークプレフィックスのペアの登録を EAR から受け付ける．機器ベンダが異なると EAA も異なる．このため，EAR は，EAD の機器ベンダごとにそれぞれ異なる EAA に対して EAR の CoA と EAN のネットワークプレフィックスの登録を行う．

CN は，EAD の通信相手となるインターネットに接続された任意のノードで，NEMO BS における CN と同等である．

3.2.2　埋め込みアドレス

EAD を製造する機器ベンダによって，EAD には EAD ごとに一意の IPv6 アドレスとネットワークプレフィックス長が埋め込まれている．これらから，EAD が CN との通信で用いる埋め込みアドレスおよびこの通信を実現するために EAR で利用される埋め込みアドレスが生成される．EAD に埋め込まれているネットワークプレフィックス長は，EAD と EAR で構成される EAN のネットワークプレフィックスの長さである．

現在広く普及している IPv4 アドレスではなく，IPv6 アドレスを埋め込む理由は，各機器を個別に識別するために一意のアドレスを機器に埋め込む必要があり，大量のアドレスが必要となるためである．このため，アドレスの枯渇が懸念される IPv4 ではなく潤沢なアドレスを持つ IPv6 を利用する．また，アドレス 1 つあたりの維持管理に要するコストは IPv6 のほうが安価であり，多くの機器に対して一意となるアドレスを埋め込むために必要なコストを低減させることが可能である．

EAD に埋め込まれている IPv6 アドレスおよびネットワークプレフィックス長と，EAN のネットワークプレフィックスおよび埋め込みアドレスの関係を**図 4** に示す．EAD に埋め込まれた IPv6 アドレスおよびネットワークプレフィックス長から，EAN のネットワークプレフィックスと，EAN で EAR 側に割り当てるアドレス（EAR 側埋め込みアドレス）および EAD 側に割り当てるアドレス（EAD 側埋め込みアドレス）がそれぞれ生成される．このうち，EAR 側埋め込みアドレスは，EAD に埋め込まれた IPv6 アドレスと同一である．少なくとも EAD と EAR の 2 つに埋め込みアドレスを割り当てるため，EAD に埋め込まれているネットワークプレフィックス長は 127 以下である．EAD が必要とする EAD 側埋め込みアドレスの数に応じて，EAD に埋め込まれるネットワークプレフィックス長は変化する．複数生成された EAD 側埋め込みアドレスはすべて EAD に設定され，EAD 上で動作するプログラムによって使い分けられる．

© 2008 Information Processing Society of Japan

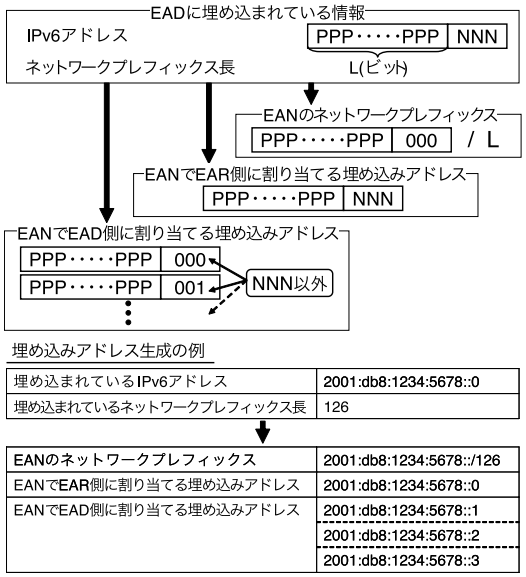

図 4　EAD に埋め込まれている情報による埋め込みアドレスの生成
Fig. 4　Generation of embedded addresses from informations embedded in an EAD.

埋め込みアドレスは，EAR や EAD を個別に識別するために一意である必要がある．したがって，機器ベンダは，生成されるすべての EAR 側埋め込みアドレスとすべての EAD 側埋め込みアドレスで重複が生じないように，IPv6 アドレスおよびネットワークプレフィックス長を，各 EAD に埋め込む必要がある．

3.2.3　EAA のアドレスの探索

EAR は，EAA に関する情報（アドレスなど）は保持せず，EAD より EAA のアドレスを探索するためのアドレス（EAA アドレス探索用アドレス）の通知を受ける．EAR が EAA アドレス探索用アドレスを保持しない理由は，EAR に接続される EAD の機器ベンダは一定ではなく，機器ベンダが異なるごとに EAA も異なるためである．また，EAA アドレス探索用アドレスは，EAA に実際に設定されているアドレスではなく，EAA のアドレスを探索するためのアドレスである．その理由は，機器ベンダによる EAA のアドレス変更や，動的 HA アドレス探索を前提とした HA を高信頼化する技術[19] を使った EAA の安定した運用などに柔軟に対応可能とするためである．

EAR は，EAA のアドレスを取得するために，EAA アドレス探索用アドレスを宛先として NEMO BS における動的 HA アドレス探索と同様の手順を実行し，EAA のアドレスを取得する．しかし，探索の宛先が NEMO BS の動的 HA アドレス探索処理とは異なる．NEMO BS の動的 HA アドレス探索処理は，MR に設定された HoA と MR が接続される HL のネットワークプレフィックス長から生成され，予約された動的 HA アドレス探索用のエニーキャストアドレス[17]（HA アドレス探索用アドレス）の形式に合致したアドレスが宛先である．一方，LTAEAv6 の EAA のアドレス探索では，EAD より EAR に通知された EAA アドレス探索用アドレスを宛先とする．

この EAA アドレス探索用アドレスは，機器ベンダが自身の管理するアドレスブロックから適切に割り当てたアドレスでよく，IETF（Internet Engineering Task Force）によって決められた HA アドレス探索用アドレスの形式に合致する必要はない．機器ベンダは，出荷する機器すべてに対して同一の EAA アドレス探索用アドレスを埋め込む．

EAA のアドレスを探索するため情報は，IP アドレスでなくてもよい．たとえば，EAA アドレス探索用アドレスの代わりに，EAA の FQDN（Fully Qualified Domain Name）でもよい．この場合，DNS からこの FQDN に対するアドレスを取得して EAA のアドレスを知ることが可能である．

3.2.4　LTAEAv6 の動作手順

図 5 に従って，埋め込みアドレスを用いた EAD と CN の通信を可能にする動作手順を説明する．この手順より前に，EAR が UN と UN の上位ネットワークを接続するゲートウェイとして設置済みとする．さらに，EAR の外部ネットワークインタフェースには，UN の上位ネットワークよりアドレスが割当て済みとし，このアドレスを EAR の CoA とする．また，EAA は，EAA アドレス探索用アドレス宛の動的 HA アドレス探索要求メッセージを受け付け，自身のアドレスを含む動的 HA アドレス探索応答メッセージを返すように，EAA アドレス探索用アドレスをエニーキャストアドレスとして自身に設定済みとする．

EAR の発見と EAD に埋め込まれた情報の通知

(1)　EAD は，ルータ要請[16]（RS）をリンクローカルスコープの全ルータマルチキャストアドレス（FF02::2）[20] 宛にマルチキャスト送信する．

(2)　EAR は，自身のルータ広告[16]（RA）を EAD 宛にユニキャスト送信する．この RA に含まれるネットワークプレフィックスは，EAR が上位ネットワークから UN 用としして割り当てられたネットワークプレフィックスとする．

(3)　EAD は，EAR から受信した RA に含まれるネットワークプレフィックスに基づい

© 2008 Information Processing Society of Japan

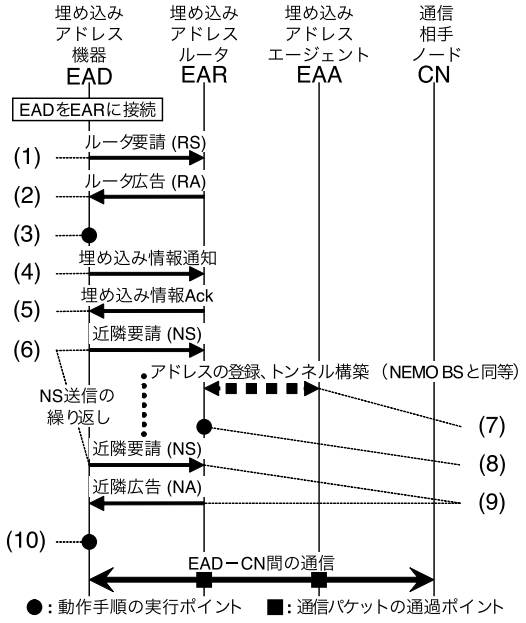

図 5　LTAEAv6 の動作手順
Fig. 5　Operating procedures of LTAEAv6.

て生成されるアドレスを，自身のネットワークインタフェースへ設定する．また，自身のデフォルトルータを EAR に設定する．これにより，EAD は，UN において割り当てられたアドレスで通信可能となる．

(4)　EAD は，自身に埋め込まれている IPv6 アドレス，ネットワークプレフィックス長および EAA アドレス探索用アドレスを格納した埋め込み情報通知を EAR 宛にユニキャスト送信する．この EAD から EAR への埋め込み情報通知は，EAD が EAR の特定の TCP ポート宛にアクセスするなど，あらかじめ決められた独自の通信手順に基づいて行われる．

(5)　EAR は，埋め込み情報 Ack を EAR 宛にユニキャスト送信する．これによって，IPv6 アドレス，ネットワークプレフィックス長および EAA アドレス探索用アドレスを受け取ったことを EAD に伝える．

EAR 側埋め込みアドレスの有効確認

(6)　EAD は，自身に埋め込まれている IPv6 アドレスを対象とした近隣要請[18]（NS）を EAR 宛にユニキャスト送信する．EAD は，NS に対する応答である近隣広告[18]（NA）を EAR から受信するまで，一定時間ごとにこの処理を繰り返す．

EAR の CoA および EAN の登録処理

(7)　EAR は，EAD から受け取った IPv6 アドレスとネットワークプレフィックス長から EAN のネットワークプレフィックスを生成する．さらに，EAR は，EAR 側埋め込みアドレスを MR の HoA，自身の CoA を MR の CoA，EAN のネットワークプレフィックスを MN の MNP として，3.1 節で示した NEMO BS の動作手順 (1)〜(6) に相当する以下の処理を行う．

- 3.2.3 項で示した EAA のアドレスの探索．
- EAR の CoA と EAN のネットワークプレフィックスのペアを EAA に登録．
- EAA–EAR 間の IP トンネルの構築．
- EAR の CoA と EAN のネットワークプレフィックスに含まれるすべてのアドレス宛に対する近隣発見の要求を，EAA で応答するように設定．

NEMO BS で HA が，近隣発見の要求に自身が応答するアドレスとして設定するのは，登録された MN のゲートウェイである MR の CoA だけである．一方，LTAEAv6 では，EAA は，近隣発見の要求に自身が応答するアドレスとして，登録された EAN のネットワークプレフィックスに含まれるすべてのアドレスを設定する．

埋め込みアドレスの設定処理

(8)　EAR は，EAD から受け取った IPv6 アドレス（EAR 側埋め込みアドレスに同じ）およびネットワークプレフィックス長を，自身の内部ネットワークインタフェースへ設定する．

(9)　EAR は，(6) において EAD から定期的に送信されている NS を受信し，その応答として自身の NA を EAD 宛にユニキャスト送信する．

(10)　EAD は，EAR から NA を受信すると，NS の送信を停止する．そして，EAD は，自身に埋め込まれている IPv6 アドレスとネットワークプレフィックス長から EAD 側埋め込みアドレスを生成する．さらに，EAD は，この EAD 側埋め込みアドレスおよび自身に埋め込まれているネットワークプレフィックス長を，自身のネットワークインタフェースへ設定する．

以上の動作により，EAD と EAR で構成される EAN が構築され，EAD は EAR，EAR–

© 2008 Information Processing Society of Japan

EAA 間の IP トンネル，EAA を経由して任意のノード CN と固定の埋め込みアドレスを用いた通信が可能となる．なお，手順の (6)，(8)〜(10) では，EAD は，EAR に EAR 側埋め込みアドレスが設定されたことを確認した後に，自身に EAD 側埋め込みアドレスを設定する．すなわち，EAD は，埋め込みアドレスで通信可能となったことを確認した後に，EAD 上のプログラムが埋め込みアドレスを利用できるようにする．さらに，EAD は，EAR が配布している RA に含まれる UN の上位ネットワークから割り当てられたネットワークプレフィックスに基づいて生成されるアドレスも持つ（手順の (3)）．したがって，このアドレスを用いた通信も可能である．

3.2.5　埋め込みアドレスルータの特長

LTAEAv6 における EAR は，NEMO BS における MR とほぼ同じ役割と動作をするが，以下の点で MR とは異なる特徴を持つ．

- EAR は，特定の IPv6 アドレスやネットワークプレフィックスをあらかじめ設定されておらず，EAD よりこれらに相当する情報の通知を受けて動作する．これにより，EAR は，EAD に埋め込まれる IPv6 アドレスや EAD を製造する機器ベンダに非依存である．
- EAR は，NEMO BS の MR と同様の動作をするが，MR のように単一のモバイルネットワークではなく，複数のネットワークのルータとして動作する．すなわち，EAR には複数の EAD が同時に接続されてもよい．これら複数の EAD の機種や製造する機器ベンダは EAD ごとに異なっていてもよい．また，EAR が EAN の登録を行う EAA は EAD ごとに異なっていてもよい．
- EAR は，EAA と同一のネットワークに設置されることはなく，HoA を持たない．ただし，EAR–EAA 間の EAN の登録処理では，EAR 側埋め込みアドレスを EAR の HoA として扱う．
- EAR は，CN との間で経路最適化処理を行わない（詳細は 3.2.6 項で述べる）．
- EAR は，設置場所のゲートウェイであり，上位ネットワークより割り当てられる下位ネットワークのネットワークプレフィックスを広報するルータとしても動作する．すなわち，EAD に対しては NEMO BS の MR およびゲートウェイの両方として動作し，EAD 以外の IP ホストについては通常のゲートウェイとして動作する．

3.2.6　経路最適化の未サポート

LTAEAv6 では，機器ベンダが自身の管理するアドレスブロックに含まれる固定の IPv6 アドレスを埋め込んだ機器を出荷し，そのアドレスから生成される埋め込みアドレスを用いた機器の保守，操作，監視を遠隔で行うことを想定している．固定の IPv6 アドレスの埋め込みは，機器の出荷時など機器ユーザの管理外で行われる．したがって，埋め込みアドレスを介して機器に不正アクセスが行われた場合，固定の IPv6 アドレスを埋め込んだ機器ベンダが責任を問われる可能性がある．このため，機器ベンダが，埋め込みアドレスを利用した通信について，不正アクセスの検知と遮断を行うことができる仕組みが必要不可欠である．

これを実現するため，LTAEAv6 では NEMO BS とは異なり，経路最適化を行わない．すなわち，EAD–CN 間の通信はつねに EAA を経由する．

3.2.7　セキュリティ

LTAEAv6 におけるセキュリティについて検討を行う．LTAEAv6 において，セキュリティ上の脅威となる点は以下の 4 点である．

(a)　EAD や EAR に設定される埋め込みアドレスを宛先とした外部のノードからの不正アクセス
(b)　EAA に対して，正規の EAD（この EAA を管理する機器ベンダが出荷した EAD）以外からの不正な EAN の登録
(c)　EAN が EAA に登録された後の，正規の EAD のすり替え
(d)　(b) または (c) によって発生する，不正なノードによる EAD へのなりすましと他ノードへの攻撃

(a) については，埋め込みアドレスを利用した通信のパケットがすべて通過する EAA において，埋め込みアドレスを宛先とした不正なアクセスの監視と遮断を，以下の方法で行う．

まず，EAA が埋め込みアドレスを宛先とするパケットを受信した場合について考える．受信したパケットの宛先アドレスが，EAR を経由して EAD から EAA に登録された EAN のネットワークプレフィックスのいずれにも含まれない場合は，このパケットを処理する必要のないパケットであるか不正なパケットであると判定できる．このため，このパケットを EAA において遮断することが可能である．また，EAA に対して EAN の登録を行う EAD は，この EAA を管理する機器ベンダが出荷した機器である．このため EAA は，EAD がどのような通信を受け付けるかについての情報（TCP，UDP 通信のポート番号など）をあらかじめ知ることが可能で，これに合致しないパケットを不正なパケットであると判定できる．このため，このパケットも EAA において遮断することが可能である．

さらに，埋め込みアドレスを用いて EAD へアクセス可能な CN が，機器ベンダが管理する監視端末などに限定される場合について考える．この場合，EAA が埋め込みアドレスを宛先とするパケットを受信すると，そのパケットの送り元アドレスがあらかじめ決められた特定の監視端末のアドレスでないならば，このパケットを不正なパケットであると判定でき

© 2008 Information Processing Society of Japan

る．このため，このパケットも EAA において遮断することが可能である．

EAA が以上のように動作することで，埋め込みアドレスを利用した通信のパケットがすべて通過する EAA において，埋め込みアドレスを宛先とした EAD および EAR に対する不正アクセスを，EAA で防ぐことができる．また，EAA は，自身を通過する埋め込みアドレスを利用した通信のパケットをつねに監視し，埋め込みアドレスを宛先とした DoS 攻撃などを検知して遮断することも可能である．これにより，EAD および EAR は，埋め込みアドレスを用いた通信の監視と制御の必要がなくなり，その処理負荷を低減させることができる．

(b) については，EAA に対する EAN の登録は，EAA を管理する機器ベンダが出荷した EAD から EAR を介して行われなければならない．このため EAA では，EAR からの EAN の登録要求が，EAA を管理する機器ベンダが出荷した EAD に基づいた要求であることを確認する必要がある．これを実現する 1 つの方法として，EAR を経由して EAD と EAA の間でチャレンジ・レスポンス認証を行うことが考えられる．この方法について，以下に述べる．

各 EAD には，あらかじめ埋め込みアドレスとともに認証用パスワードが埋め込まれて出荷される．また EAA は，EAA を管理する機器ベンダが出荷した EAD に埋め込まれた認証用パスワードを保持している．この場合，LTAEAv6 の動作手順 (7) において，EAA が EAR から EAN の登録要求を受け付けてから EAN の登録を自身に行うまでの間で，以下の手順を追加する．

(1’)　EAA は，チャレンジ文字列を生成する．
(2’)　EAR は，EAA よりチャレンジ文字列を受信する．
(3’)　EAR は，EAD にチャレンジ文字列を送信する．
(4’)　EAD は，チャレンジ文字列と埋め込まれている認証用パスワードからレスポンス文字列を生成し，EAR に送信する．
(5’)　EAR は，EAA にレスポンス文字列を送信する．
(6’)　EAA は，チャレンジ文字列と EAA に保管されている EAD の認証用パスワードから生成した文字列と受信したレスポンス文字列を比較する．一致した場合，EAA は LTAEAv6 の動作手順 (7) の動作を続行し，一致しなかった場合，EAA は EAR からの EAN の登録を拒否する．

このように動作することで，EAR からの EAN の登録要求に対して，EAA は EAR を介して EAD を認証し，EAA を管理する機器ベンダが出荷した EAD であった場合のみ，EAR からの EAN の登録を受け付けるように動作する．

(c) については，EAD のすり替えを防ぐ方法として，EAN の登録時だけでなく登録後も EAA と EAD の間で (1’)〜(6’) で述べたようなチャレンジ・レスポンス認証を定期的に実行することが対策として考えられる．ただし，EAD が設置されるネットワークが悪意ある第三者によって通信内容が盗聴されやすい無線 LAN などである場合，チャレンジ・レスポンス認証を定期的に実行することで発生する通信の内容を収集して解析することでパスワードが推測される可能性がある．このようなネットワークに EAD を設置する場合，このネットワーク内における通信を安全に暗号化する技術（無線 LAN では，Protected Extensible Authentication Protocol [21]（PEAP）など）を併用することで，パスワードが容易に推測されるのを防ぐことができる．

しかし，定期的に EAA と EAD の間でチャレンジ・レスポンス認証を行ったとしても，EAD のすり替えを完全に防ぐことはできない．これを完全に防ぐには，EAA と EAD の間，または通信の末端どうしである CN と EAD の間で IP Security [22]（IPSec）などのつねに認証がともなう通信を行う必要がある．

(d) については，(b) または (c) の結果として生じる脅威であり，(b) および (c) の脅威に対する対策を行うことで回避することができる．

3.2.8　EAD に必要な追加機能

LTAEAv6 によって EAD には，IPv6 ノードとして必要な通常の機能に加えて以下の機能の追加が必要となる．

- 自身に埋め込まれた情報を EAR に通知する処理
- EAD 側埋め込みアドレスを計算する処理
- EAA との間で行うチャレンジ・レスポンス認証の処理

これらの処理のうち，初めの 2 つの処理のソフトウェア量および処理負荷は明らかに小さい．チャレンジ・レスポンス認証の一連の処理で EAD に必要な処理は，EAR より送られてきたチャレンジ文字列と EAD に埋め込まれた認証パスワードの文字列を連結した文字列のハッシュ値を，あらかじめ決められた 1 方向性ハッシュ関数で計算し，この値をレスポンス文字列として送信することである．代表的な 1 方向性ハッシュ関数の 1 つである MD5 [23] の実装は，一般的には数百行程度でかつ高速に動作することから，チャレンジ・レスポンス認証のソフトウェア量および処理負荷も小さい．したがって，LTAEAv6 によって EAD の処理負荷が大きく増大することはなく，同一ネットワーク上の EAR や他の EAD 設置数に依存して処理負荷が増大することもない．

© 2008 Information Processing Society of Japan

3.2.9　スケーラビリティおよび冗長性

LTAEAv6 において，EAR および EAA は，それぞれ EAR の下位ネットワークに接続される EAD の個数および EAA を管理する機器ベンダが出荷した EAD の総数に比例して，処理負荷が増大する．

EAR において，その下位ネットワークに同時に接続される EAD の個数は，たかだかその EAR を設置した機器ユーザの所有する機器の総数である．1 人の機器ユーザが所有する機器の個数が無制限に増加することはない．このため EAR は，あらかじめ決められた個数の EAD が同時に接続されても大丈夫な処理性能を持たせればよい．大量のセンサデバイスを設置するなどして EAD の個数が大量になった場合，機器ユーザは，既存の EAR を自身が保有する EAD の個数に適した処理性能を持つ新しい EAR に置き換えることで対処可能である．

EAR を介して EAA に EAN の登録を行う EAD の個数は，たかだかその EAA を管理する機器ベンダが出荷した EAD の総数である．このため機器ベンダは，自身が出荷した EAD の総数に比例して，自身の管理する EAA を増強すればよい．また，EAA は複数設置することで負荷分散を行うことが可能である．

また EAA は，実装および機能が NEMO BS の HA とほぼ同一である．このため，NEMO BS において検討されている Home Agent Reliability Protocol [19] などの HA の負荷分散や冗長性に関する技術をそのまま適用することが可能である．

3.3　関連技術との比較

関連技術と比較して，LTAEAv6 は次の利点を持つ．

- DNS や Dynamic DNS を用いる場合，機器に対する不正アクセスの検知と遮断は，機器や機器の設置場所のゲートウェイで行う必要がある．一方，LTAEAv6 の場合，機器ベンダで不正アクセスの検知と遮断を行うことが可能である．したがって，機器の処理負荷を低減可能である．
- MIP4 や MIP6 では，基本 IP 機能以外の負荷の高い処理が機器に必要である．一方，LTAEAv6 の場合，機器は，機器の設置場所のゲートウェイに対する自身に埋め込まれた情報の通知やアドレスの設定など負荷の少ない処理のみが必要であり，他の処理はゲートウェイが行う．
- LINA，HIP，LISP，Shim6 では，通信する双方が同一の技術に対応する必要がある．一方，LTAEAv6 の場合，機器の通信相手は IPv6 の基本機能に対応すればよく，任意の IPv6 ノードと埋め込みアドレスを使った通信が可能である．

4.　実装と評価

LTAEAv6 の実装を行った．この実装に基づき，MIP6 や NEMO BS などと実装コストの観点から比較を行う．また実環境での動作時間の測定値を示すことで動作の確認を行う．

4.1　実　　装

Linux 上の NEMO BS の実装である NEPL [24),25)] をベースにし，LTAEAv6 の実装を行った．NEPL は，Linux 上の MIP6 の実装である MIPL [26),27)] を拡張することで NEMO BS の機能を実現している．

LTAEAv6 における EAD，EAR および EAA について，ベースとなる NEPL に対する変更箇所を以下に述べる．

EAD

EAD は，NEMO BS では MNN に相当する．MNN は通常の IPv6 ノードであるため，NEPL に MNN 用の実装は存在しない．NEPL に含まれる RS，RA，NS，NA の各処理の実装を参考にして，LTAEAv6 の EAD に必要な以下の処理の実装を行った．

- EAR の探索．
- EAR 側および EAD 側埋め込みアドレスの生成．
- EAR へ IPv6 アドレス，ネットワークプレフィックス長および EAA アドレス探索用アドレスの通知．
- EAR 側埋め込みアドレスの有効性確認．
- EAD へ EAD 側埋め込みアドレスの設定．
- EAR を EAD のデフォルトルータとして設定．

EAR

EAR は，NEMO BS では MR に相当する．NEPL 内の MR の処理の箇所に以下の処理の拡張を行った．

- EAD から IPv6 アドレス，ネットワークプレフィックス長および EAA アドレス探索用アドレスを受信し，EAR に新しい EAN を動的に追加．
- EAN のネットワークプレフィックスの生成．
- EAA アドレス探索用アドレスを用いた EAA のアドレスの探索．
- EAR へ EAR 側埋め込みアドレスの設定．

EAR は，複数の EAD に対して同時に NEMO BS における MR として動作する．このため，EAR として動作するために必要なデータや状態などを EAD ごとに個別に管理する

© 2008 Information Processing Society of Japan

ように NEPL を変更した．また，EAR には不定期に EAD が接続されるため，設定ファイルにあらかじめ設定された情報に対応した動作のみを行う NEPL に対して，EAD からの要請をうけて動的に EAN の情報を追加するように拡張した．

EAA

EAA は，NEMO BS では HA に相当する．NEPL 内の HA の処理の箇所に以下の拡張を行った．

- EAD に EAA アドレス探索用アドレスとして埋め込んだアドレス宛に対する動的 HA アドレス探索要求への応答．
- EAR より登録された EAR の CoA だけでなく，EAN に含まれるすべてのアドレス宛の近隣発見の要求に対する代理応答．

なお，NEMO BS における MR–CN 間の経路最適化処理に相当する処理を行わないため，LTAEAv6 の実装では NEPL に含まれる経路最適化処理や CN としての処理は不要である．しかし，NEPL に対して LTAEAv6 を実現するため行ったソースコードの変更量を正確に知るため，これらの処理の削除は行わず，NEPL に備わっている経路最適化を無効にする設定を利用している．

上記の NEPL に対する変更は，ユーザランドのプログラムの作成または修正のみで，カーネルの修正は不要であった．これは，LTAEAv6 を実装するために必要なカーネル内の処理は，NEPL が対象とする Linux カーネルに対して，NEPL で提供されている変更を適用することで実現可能なためである．

4.2 評　　価

LTAEAv6 の実装，NEPL，MIPL の各実装のソースコードの行数および実行ファイルのバイト数の比較によって，LTAEAv6 の実装コストが少ないことを示す．なお，比較はネットワークトポロジ的に同じ位置づけであるモバイルノードと MNN と EAD，MR と EAR，HA と EAA のそれぞれで行った．経路最適化を行わないため，CN は通常の IPv6 ノードであり，これらの各実装で CN に必要な部分は存在しない．

各実装のソースコードの行数および実行ファイルのバイト数を，**図 6** に示す．なお，NEPL および MIPL はモノリシックな構造をしているため，NEPL の場合は MR と HA で，MIPL の場合はモバイルノードと HA で同一の実行ファイルであり，設定ファイルや起動時の指定で動作を変化させる．このため，NEPL の MR と HA，MIPL のモバイルノードと HA でソースコードの行数および実行ファイルのバイト数は同一となる．

図 6 より，次のことが分かる．

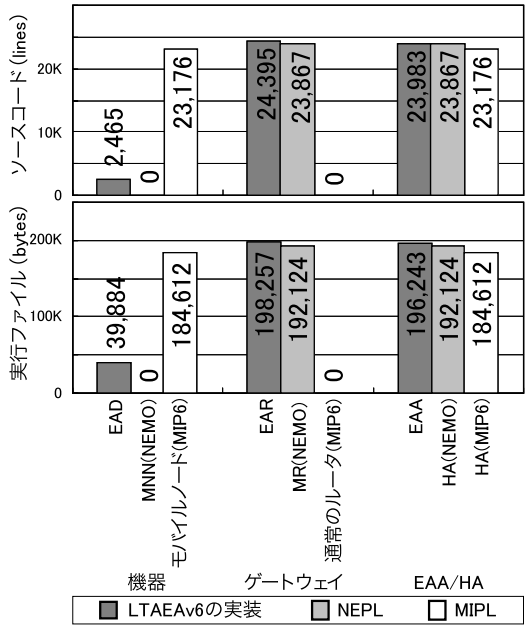

図 6　LTAEAv6 の実装，NEPL，MIPL のソースコードおよび実行ファイルのサイズの比較
Fig. 6　Comparison of source code and binary file size for an implementation of LTAEAv6, NEPL, and MIPL.

- EAD には，2,465 行の実装が新たに必要であるが，MIP6 のモバイルノードに比べてソースコード，実行ファイルとも大幅に少ない．したがって，LTAEAv6 を適用すると，MIP6 に比較して実装コストを大幅に抑えて，固定のアドレスを用いた通信が実現可能であるといえる．軽量な実装が求められるセンサデバイスなどの機器において，この実装コスト削減効果は重要である．
- MR に対し，EAR のソースコードの行数，実行ファイルのバイト数とも増加は数%である．
- HA に対し，EAA のソースコードの行数の増加は 116 行で，実行ファイルのバイト数の増加もわずかである．

次に，LTAEAv6 の実装の動作評価を行った．**図 7** および**表 1** は，動作評価に用いたネットワーク環境を示している．EAD から CN までのケーブル長さは最大でも 7.5 メートル

© 2008 Information Processing Society of Japan

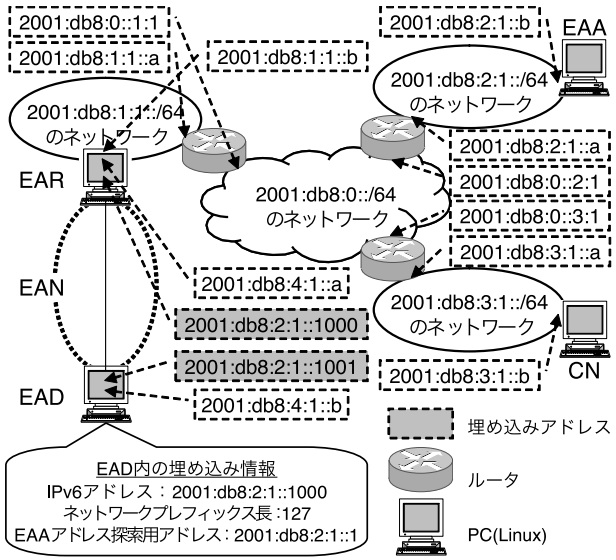

図 7　LTAEAv6 の実装の評価環境
Fig. 7　Network topology for evaluation of the LTAEAv6 implementation.

表 1　図 7 の評価環境のスペック
Table 1　Specifications of network presented in Fig. 7.

ネットワーク	
ルータ	YAMAHA RTX1000 CPU:MIPS32 150 MHz RAM:16 MBytes 100BASE-TX ポート × 3
SW-HUB	BUFFALO LSW10/100-5NWP 100BASE-TX ポート × 5 （2001:db8:0::/64 のネットワークで使用）
ケーブル	カテゴリ 5 100BASE-TX（1.5 メートル）

ノード（EAA/EAR/EAD/CN）	
EAA/EAR	CPU:Intel モバイル Celeron 1.33 GHz RAM:128 MBytes NET:100BASE-TX
EAD/CN	CPU:Intel PentiumIII-M 1.20 GHz RAM:384 MBytes NET:100BASE-TX

表 2　図 7 の評価環境における各ノード間の RTT
Table 2　RTT between function nodes in network presented in Fig. 7.

		最小 (msec)	平均 (msec)	最大 (msec)
EAD–EAR 間	(2001:db8:4:1::b ⇔ 2001:db8:4:1::a)	0.187	0.262	1.026
EAR–EAA 間	(2001:db8:1:1::b ⇔ 2001:db8:2:1::b)	1.868	1.984	2.407
EAR–CN 間	(2001:db8:1:1::b ⇔ 2001:db8:3:1::b)	1.847	1.960	2.672
EAA–CN 間	(2001:db8:2:1::b ⇔ 2001:db8:3:1::b)	1.763	1.960	2.368

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

	最小 (msec)	平均 (msec)	最大 (msec)
LTAEAv6 あり			
(2001:db8:2:1::1001 ⇔ 2001:db8:3:1::b)	3.791	4.016	5.153
LTAEAv6 なし（埋め込みアドレスを用いない）			
(2001:db8:4:1::b ⇔ 2001:db8:3:1::b)	2.001	2.143	2.845

（1.5 メートル × 5 本）であるため，ケーブルによる伝搬遅延は無視できる．このため，各ノード間の往復通信遅延（Round Trip Time: RTT）は各ノード（EAD/EAR/EAA/CN）やルータにおけるパケット処理やルーティング処理に要する時間と考えられる．

100 回の ICMPv6 ECHO REQUEST/RESPONSE の送受信で測定した各ノード（EAD, EAR，EAA，CN）間で直接通信を行った場合の RTT を**表 2** に示す．

このようなネットワーク環境において，EAD と CN が，LTAEAv6 ありで埋め込みアドレスを利用して EAR および EAA を経由して通信を行う場合と，LTAEAv6 なしで埋め込みアドレスを用いずに直接通信を行った場合の RTT を 100 回の ICMPv6 ECHO REQUEST/RESPONSE の送受信で測定した．その結果を**表 3** に示す．

表 2，表 3 より，LTAEAv6 ありの場合，EAD–CN 間の平均 RTT は，EAD–EAR 間，EAR–EAA 間，EAA–CN 間の平均 RTT の和にほぼ等しい．これらの差は 0.190 msec である．一方，LTAEAv6 なしの場合，EAD–CN 間の平均 RTT は，EAD–EAR 間，EAR–CN 間の平均 RTT の和にほぼ等しい．これらの差は 0.079 msec である．ICMPv6 ECHO REQUEST/RESPONSE の送受信による RTT の測定における最大値と最小値の差には，0.538 msec（EAR–EAA 間）から 1.362 msec（LTAEAv6 ありの EAD–CN 間）の幅がある．これらに比べ，先に示した EAD–CN 間の RTT と，各中継ノード間の RTT の和との差（0.079 msec および 0.190 msec）は十分に小さい．したがって，LTAEAv6 導入による

© 2008 Information Processing Society of Japan

EAD–CN 間の通信における遅延の増加は，中継ノードの増加によるものが支配的であるといえる．

5. ま と め

NEMO BS を応用して，固定の IPv6 アドレスを用いた機器と任意のノードの通信を可能とする手法 LTAEAv6 の提案を行った．本手法により，機器ベンダが固定の IPv6 アドレスで機器にアクセスすることを可能にし，遠隔からの機器の保守，操作，監視を容易にした．また，本手法では，機器に複雑な IP 処理を実装しないことで機器の処理コストの低減や開発コストの削減をした．また，固定の IPv6 アドレスを用いた通信について，機器ベンダが不正アクセスの検知と遮断を行うことを可能とした．さらに，Linux 上の NEMO BS の実装である NEPL を拡張することで LTAEAv6 を実装し，ソースコードの行数および実行ファイルのバイト数で実装コストの評価を行った．この結果，MIP6 を機器に実装する場合に比べて，LTAEAv6 では機器に必要な実装コストを低く抑えられ，NEMO BS の実装に対して大幅な変更が不要であることを示した．

本手法では，機器の設置場所の既存ゲートウェイを置き換える必要がある．今後の課題として，既存ゲートウェイの置き換えを必要としない手法や，機器の設置場所に機器以外の特殊な装置を必要としない手法の検討があげられる．

参 考 文 献

1) Vixie, P., Thomson, S., Rekhter, Y. and Bound, J.: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136 (1997).
2) Wellington, B.: Secure Domain Name System (DNS) Dynamic Update, RFC 3007 (2000).
3) Perkins, C.E.: Mobile IP, *IEEE Communications Magazine*, Vol.35, No.5, pp.84–99 (1997).
4) Perkins, C.: IP Mobility Support for IPv4, RFC 3344 (2002).
5) Perkins, C.E. and Johnson, D.B.: Mobility support in IPv6, *Proc. 2nd Annual International Conference on Mobile Comuputing and Networking* (*MobiCom'95*), pp.22–37 (1996).
6) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support in IPv6, RFC 3775 (2004).
7) Ernst, T., Castelluccia, C. and Lach, H.-Y.: Extending Mobile IPv6 with Multicast to Support Mobile Networks in IPv6, *Proc. 1st IEEE European Conference on Universal Multiservice Networks* (*ECUMN'00*), pp.114–121 (2000).
8) Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, P.: Network Mobility (NEMO) Basic Support Protocol, RFC 3963 (2005).
9) Ishiyama, M., Kunishi, M., Uehara, K., Esaki, H. and Teraoka, F.: LINA: A New Approach to Mobility Support in Wide Area Networks, *IEICE Trans. Comm.*, Vol.E.84-B, No.8, pp.2076–2086 (2001).
10) Kunishi, M., Ishiyama, M., Uehara, K., Esaki, H. and Teraoka, F.: LIN6: A New Approach to Mobility Support in IPv6, *Proc. 3rd International Symposium on Wireless Personal Multimedia Communications* (*WPMC'2000*) (2000).
11) Nikander, P., Ylitalo, J. and Wall, J.: Integrating Security, Mobility, and Multi-Homing in a HIP Way, *Proc. Network and Distributed Systems Security Symposium* (*NDSS'03*), pp.87–99 (2003).
12) Farinacci, D., Fuller, V., Oran, D. and Meyer, D.: Locator/ID Separation Protocol (LISP), Internet-Draft draft-farinacci-lisp-02 (2007).
13) Nordmark, E. and Bagnulo, M.: Shim6: Level 3 Multihoming Shim Protocol for IPv6, Internet-Draft draft-ietf-shim6-proto-08 (2007).
14) Manner, J. and Kojo, M.: Mobility Related Terminology, RFC 3753 (2004).
15) Ernst, T. and Lach, H.-Y.: Network Mobility Support Terminology, RFC 4885 (2007).
16) Thomson, S. and Narten, T.: IPv6 Stateless Address Autoconfiguration, RFC 2462 (1998).
17) Johnson, D. and Deering, S.: Reserved IPv6 Subnet Anycast Addresses, RFC 2526 (1999).
18) Narten, T., Nordmark, E. and Simpson, W.: Neighbor Discovery for IP Version 6 (IPv6), RFC 2461 (1998).
19) Wakikawa, R.: Home Agent Reliability Protocol, Internet-Draft draft-ietf-mip6-hareliability-02 (2007).
20) Hinden, R. and Deering, S.: IP Version 6 Addressing Architecture, RFC 4291 (2006).
21) Palekar, A., Salowey, J., Josefsson, S. and et al.: Protected EAP Protocol (PEAP) Version 2, Internet-Draft draft-josefsson-pppext-eap-tls-eap-10 (2004).
22) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301 (2005).
23) Rivest, R.: The MD5 Message-Digest Algorithm, RFC 1321 (1992).
24) Helsinki University of Technology Go-Core Project: NEPL:NEMO Platform for Linux (online). available from ⟨http://www.mobile-ipv6.org/⟩ (accessed 2007-09-01).
25) WIDE Project Nautilus6 working group: NEPL patch for UMIP (online). available from ⟨http://software.nautilus6.org/NEPL-UMIP/⟩ (accessed 2007-09-01).

© 2008 Information Processing Society of Japan

26) Helsinki University of Technology Go-Core Project: MIPL:Mobile IPv6 for Linux (online). available from ⟨http://www.mobile-ipv6.org/⟩ (accessed 2007-09-01).
27) USAGI Project: UMIP:USAGI-Patched Mobile IPv6 for Linux (online). available from ⟨http://www.linux-ipv6.org/memo/mipv6/⟩ (accessed 2007-09-01).

(平成 19 年 9 月 2 日受付)
(平成 20 年 2 月 5 日採録)

黒木　秀和（正会員）

平成 8 年東京工業大学工学部情報工学科卒業．平成 10 年同大学大学院理工学研究科修士課程修了．平成 12 年株式会社エコス入社．平成 15 年株式会社インターネット総合研究所入社．平成 16 年株式会社 IRI ユビテック（現株式会社ユビテック）転籍，現在に至る．修士（工学）．現在，静岡大大学院創造科学技術教育部在学．IPv6 とその応用，ユビキタスネットワークに関する研究に従事．電子情報通信学会，システム制御情報学会，IEEE 各会員．

井上　博之（正会員）

昭和 62 年大阪大学工学部電子工学科卒業．平成元年同大学大学院工学研究科修士課程修了．同年住友電気工業株式会社入社．平成 12 年奈良先端大学院大学情報科学研究科博士後期課程修了．平成 12 年株式会社インターネット総合研究所入社．平成 16 年株式会社 IRI ユビテック（現株式会社ユビテック）転籍．平成 19 年広島市立大学大学院情報科学研究科講師，現在に至る．博士（工学）．ネットワークアーキテクチャ，センサネットに関する研究に従事．電子情報通信学会，IEEE 各会員．

荻野　　司

昭和 61 年長岡技術科学大学大学院工学研究科修士課程修了．同年キヤノン株式会社入社．平成 7 年ファストネット株式会社出向．平成 11 年同社取締役．平成 12 年株式会社インターネット総合研究所入社．同年株式会社インターネットシーアンドオー（現株式会社ブロードバンドセキュリティ）代表取締役．平成 14 年株式会社インターネット総合研究所取締役．平成 15 年 TAU 技研株式会社（現株式会社ユビテック）代表取締役社長，現在に至る．修士（工学）．現在，静岡大学大学院創造科学技術研究部客員教授および同大学情報学部客員教授．

石原　　進（正会員）

平成 6 年名古屋大学工学部電気工学科卒業．平成 11 年同大学大学院工学研究科博士後期課程修了．平成 10 年日本学術振興会特別研究員．平成 11 年静岡大学情報学部助手．平成 13 年同大学工学部助教授．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．無線環境用 TCP/IP，モバイルアドホックネットワーク，センサネットワークに関する研究に従事．電子情報通信学会，IEEE，ACM 各会員．

© 2008 Information Processing Society of Japan