XD-AUTH：インターネットモビリティにおけるドメイン間移動時の事前認証方式

川口裕樹[†1] 海沼義彦[†1] 張亮[†2]
林秀樹[†2] 寺岡文男[†1]

インターネットは複数のドメイン（インターネットサービスプロバイダなど）から構成されるマルチドメイン構成であり，このような環境においてノードの移動時に高速に認証が行われるシステムが求められている．本論文では移動先アクセスルータアドレス解決プロトコルである CARD と認証メッセージを運ぶプロトコルである DIAMETER/PANA を組み合わせて拡張利用した，ドメイン間ノード移動時の高速認証プロトコル XD-AUTH を提案する．通常の認証手順ではドメイン間でのメッセージ交換の処理を含むため多くの処理時間がかかるが，XD-AUTH では同一ドメイン内の移動ノードと移動先アクセスルータ間でのメッセージ交換のみで認証することができる．XD-AUTH を FreeBSD に実装し，実験ネットワークで処理時間を測定したところ，ドメイン間移動時の認証処理を 10.22 msec で完了できることが分かった．

"XD-AUTH": Proposal of Pre-authentication in Case User Moves Across Domains At Internet Mobility

Hiroki Kawaguchi,[†1] Yoshihiko Kainuma,[†1] Ryo Tyo,[†2]
Hideki Hayashi[†2] and Fumio Teraoka[†1]

The Internet is a multi-domain environment that consists of a lot of administrative domains such as Internet Service Providers. In such an environment, fast authentication is required when a mobile node changes its attachment point to the Internet. This paper proposes a fast authentication protocol called XD-AUTH that supports inter-domain handover. XD-AUTH combines CARD (a protocol resolving the address of the next access router) and DIAMETER/PANA (protocols transferring authentication data). In conventional protocols, authentication processing takes long time because it includes message exchanges between different domains. In XD-AUTH, authentication processing requires message exchanges between the mobile node and the access router. XD-AUTH was implemented on FreeBSD. The measurement results in our test network show that the authentication time is 10.22 msec when a mobile node executes an inter-domain handover.

1. はじめに

インターネット上でインターネットへの接続サービスを提供するプロバイダを ISP（Internet Service Provider）もしくはドメインと呼び，現在のインターネットは複数のドメインの集合により構成されるマルチドメイン構成をとっている．私たちがインターネットを利用するためには通常 1 つのドメインと契約を結び，契約したドメインを経由してインターネットにアクセスする．

一方，近年インターネットの普及，無線環境の充実，機器類の小型化そして Mobility support for IPv4/v6（MIPv4/v6）[1),2)] を代表としたモビリティプロトコルが標準化されたことによりあらゆる場所でコンピュータをインターネットに接続できる環境が整いつつあり，このような環境下では契約外のドメインを介してインターネットに接続したいという要求が発生する．

各ドメインはインターネットにアクセスするユーザを認証し（Authentication），サービスを利用するための権限を委譲し（Authorization），サービスの利用状況を把握するための情報を収集する（Accounting）ことでどのユーザにも公平にサービスを提供すること

†1 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University
†2 ソフトバンクモバイル株式会社技術総合研究室ワイヤレスシステム研究開発センター
Wireless System R & D Center, Research Laboratory, SOFTBANK MOBILE Corp.

が可能となる．この Authentication，Authorization，Accounting の一連の処理のことを AAA 処理という．AAA を行わない場合，不正なサービス利用を容易に許してしまい，またその不正なサービス利用が誰によって行われたのかの特定が困難となってしまう．そのためネットワーク上で商用目的のサービスを提供する場合，AAA の実現が必要不可欠とされている．

移動端末のユーザ（Mobile Node，以下 MN）が契約外のドメインを介してインターネットに接続するという状況を想定した場合，各ドメインは MN を直接認証することができないため，MN が直接契約を結んでいるドメイン（home domain）への問合せが必須となる．この問合せは MN の home domain から離れれば離れるほど処理に時間がかかる．また MN はアクセスルータ（以下 AR）に接続することで通信が可能となる．MN が移動すると接続する AR が切り替わるが，接続する AR が切り替わるたびに AAA のため home domain への問合せが必要となる．そのため MN が移動した直後から通信を再開するまでに時間がかかるという問題がある．こうした背景から認証を含めた AAA の高速化は必須である．

MN が AR を切り替える際，異種通信媒体間（たとえば WiFi と Cellular 間）で行う場合と同一通信媒体間（たとえば WiFi どうし）で行う場合の 2 つの場合が考えられる．異種通信媒体間移動の場合は，移動前に現在通信に利用していないネットワークインタフェースで移動先の AR に接続し，事前に AAA 処理を済ませておくことができる．一方，同一通信媒体間移動の場合，ハードウェアの制約から MN のネットワークインタフェースは 1 つであると想定されるため，上記のような方法は利用できず，新たな高速事前 AAA 処理方式が必要となる．そこで本論文では同一通信媒体間で移動する場合を考え，MN のネットワークインタフェースが 1 つであることを想定する．

また，MN の移動には 2 つの場合が想定される．MN が移動後に接続する AR が移動前と同じドメインの管轄にある場合とそうでない場合である．MN の移動が同一のドメイン内なのかドメイン間の移動なのかによって状況は異なる．MN の移動が同一のドメイン内であれば，FPANA [3] のような高速認証手法が有効である．FPANA は移動前後の AR 間に信頼関係があることを仮定する．そして認証完了後に得られる情報を移動前に接続している AR（PAR: Previous Access Router）から移動後に接続する AR（NAR: New Access Router）に直接転送する．こうすることにより，移動後に MN の home domain への問合せを省くことができ AAA の高速化を実現できる．しかし，MN の移動がドメイン間である場合，基本的には移動前後の AR 間に信頼関係はなく FPANA のような手法は適用できない．また，ドメイン間移動時の高速認証方式の具体的な提案はほとんどされていない．本論文はドメイン間移動時における AAA の高速化のための事前認証方式 XD-AUTH を提案する．XD-AUTH では MN が移動する前に MN の認証を home domain の AAAs において行い，認証完了後に得られる情報を安全な経路を介して AAAs から移動先のアクセスルータである NAR に転送する．これにより移動後は，MN と NAR の間のやりとりで MN の認証をすることができ，home domain への問合せを省ける．これにより AAA の高速化を実現する．

本論文の構成は以下のとおりである．2 章では AAA アーキテクチャ全体に関する説明を行い，3 章では高速認証方式の関連研究について説明する．4 章では本論文で提案する XD-AUTH についての詳細設計を述べ，5 章で実装，6 章で評価について述べる．最後に 7 章で本論文をまとめる．

2. AAA アーキテクチャ

2.1 AAA アーキテクチャの概要

インターネットにおけるモバイル環境では以下のような使用例が想定される．MN はある 1 つの管理ドメイン（たとえば ISP，Internet Service Provider）と契約しているものとする．この管理ドメインを home domain と呼ぶこととする．インターネットは複数の管理ドメインから構成されており，MN ごとに home domain が異なる．home domain の認証サーバには契約している MN の認証情報，権限委譲情報などが安全に管理されており，契約している MN が home domain を介してインターネット接続要求を行う際には，home domain の認証サーバがこの MN の認証や権限委譲処理を行う．

home domain 以外の管理ドメインを visited domain と呼ぶこととする．MN は移動先において visited domain を経由してインターネット接続要求を行う場合もある．このとき，visited domain の認証サーバはこの MN の認証情報や権限委譲情報を保持していないため，この MN の home domain に認証処理や権限委譲処理を依頼する必要がある．このように，MN と複数の管理ドメイン間で AAA 情報をやりとりするための基盤を AAA 基盤と呼ぶ．

IETF（Internet Engineering Task Force）では MN と AR 間で AAA 情報をやりとりするプロトコル

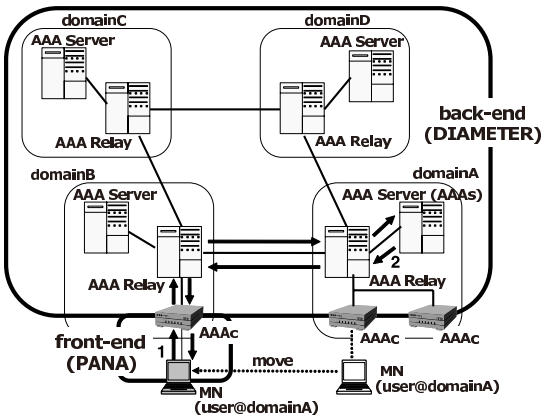

図 1 AAA アーキテクチャ
Fig. 1 AAA architecture.

を front-end プロトコルと呼び，PANA（Protocol for carrying Authentication for Network Access）[4] が標準化されつつある．また管理ドメイン間で AAA 情報をやりとりするプロトコルを back-end プロトコルと呼び，Diameter Base Protocol（DIAMETER）[5] が標準化されている．

図 1 に IETF における AAA アーキテクチャを示す．AAA back-end においては，各ドメインに AAA 情報のやりとりや認証処理などを担当する AAA ノードが設置され，これらがオーバレイネットワークを構成する．大きく分けて，AAA ノードには役割に応じて 3 種類のタイプがある．1 つ目は AAAs（AAA server）である．AAAs はそのドメインの契約ユーザ（MN）の AAA 情報を管理し，認証処理などを行う．負荷分散のため，契約ユーザごとに AAAs を分けることも可能だが，ここでは簡単のため各ドメインには AAAs は 1 台設置されているものとする．2 つ目は AAAr（AAA relay）である．AAAr はドメイン間で AAA 情報を中継する．3 つ目は AAAc（AAA client）である．AAAc は AAA front-end と AAA back-end の間で AAA 情報を中継する．

MN は接続を希望するドメインの AAAc に接続要求を送信する．この接続要求は AAAc や AAAr を介して，この MN の home domain の AAAs まで配送され，認証処理が行われる．すなわち，MN が移動して接続地点（たとえばアクセスポイント）を変更するごとに MN と AAAs 間で AAA 情報のやりとりが発生するため，移動後の通信再開に時間がかかるという問題が発生する．

MN の認証のためのプロトコルとしては EAP（Extensible Authentication Protocol）[6] が利用される．AAA front-end と AAA back-end によって MN とこの MN の home domain の AAAs 間で EAP メッセージをやりとりする．

AAA back-end を構成する AAA ノード間には互いに信頼関係があり，AAA ノード間には IPsec [7] などによる安全な通信路が確立されていることが定められている．また，MN と AAAc 間には MN の認証処理が完了したあとに信頼関係が確立され，両者の間の通信は IPsec などにより保護される．

2.2 Extensible Authentication Protocol（EAP）

EAP とは，もともとは Point to Point Protocol（PPP）を拡張し認証の機能を持たせた方式として IETF により標準化されたプロトコルであるが，現在では PPP とは独立したプロトコルとして利用されている．EAP そのものは様々な認証方式（method）をサポートするフレームワークとして定義されており，認証に関する処理は各 method により定義されている．文献 6) には代表的な method として MN の ID を取得するための EAP-Identity method，challenge/response 型の認証を行う EAP-MD5 method，証明書を利用した相互認証や鍵生成を行う EAP-TLS method，事前共有鍵（Pre-Shared Key，PSK）を利用して相互認証や鍵生成を行う EAP-PSK method などが定義されている．

2.3 Diameter Base Protocol（DIAMETER）

DIAMETER は現在認証プロトコルとして広く世に普及している Remote Authentication Dial In User Service（RADIUS）[8] の後継プロトコルとして開発された．RADIUS と比較し DIAMETER は Failover の仕組みが仕様として定義されている，メッセージの送受信を信頼性向上のために TCP で行う，クライアント主導だけではなくサーバ主導のメッセージも定義されているなどをはじめとした様々な利点があり，マルチドメイン環境における認証システムの基盤としての利用が期待されている．

DIAMETER はそれ自体には認証を直接行う機能はなく，DIAMETER ノード間でオーバレイネットワークを構成し，それぞれが Realm based routing というルーティング手法を用いてルーティングを行い AAA のためのメッセージを転送するプロトコルである．また DIAMETER ノード間には IPsec をはじめとしたセキュリティプロトコルにより保護されているコネクション（Security Association，以下 SA）が存在していることが前提となっている．

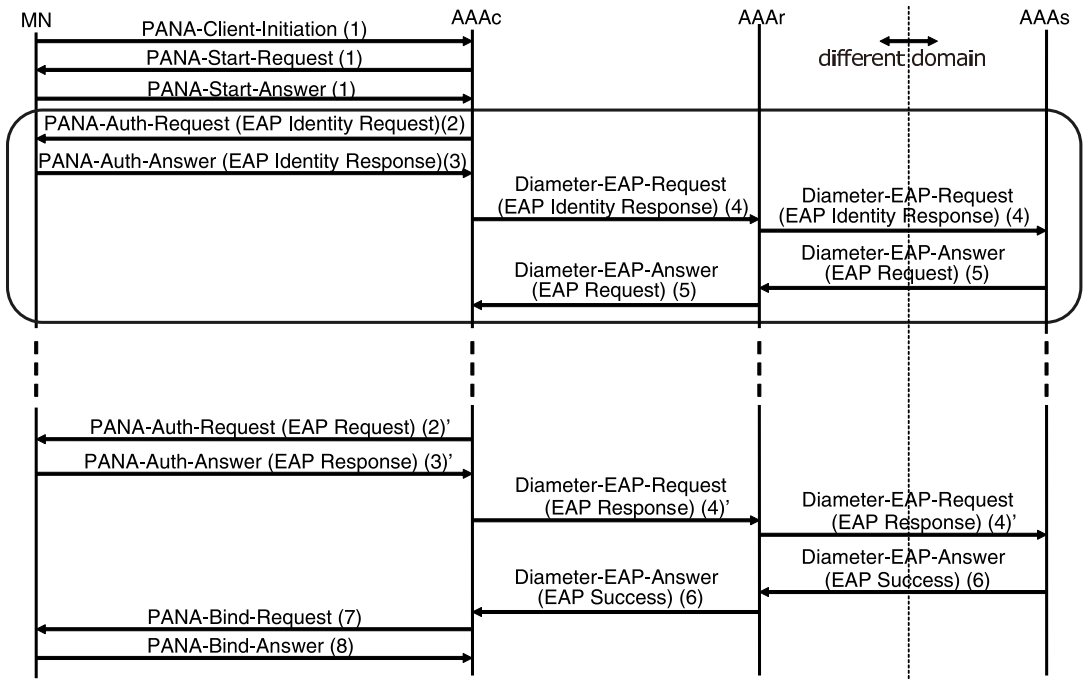

図 2 DIAMETER/PANA EAP Application における認証の流れ
Fig. 2 Authentication flow in DIAMETER/PANA EAP Application.

2.4 Protocol for carrying Authentication for Network Access（PANA）

PANA は EAP パケットをはじめとした認証情報をエンドノードと AAAc 間で転送するプロトコルとして提案されている．DIAMETER と同様に PANA 自体には認証機能はない．

PANA の大きな利点として認証情報をトランスポート層で転送すること，認証エージェントとアクセスコントロールを行うモジュールが別々に定義されていること，AVP（Attribute Value Pairs）の追加により容易に拡張が行えることがあげられる．

2.5 DIAMETER/PANA EAP Application

DIAMETER や PANA 自体には認証機能はなく，DIAMETER や PANA メッセージ中に EAP などの認証プロトコルのデータを載せることで認証機能を実現している．以下 EAP を PANA と DIAMETER 上のアプリケーションとして動作させたときの認証について説明する．

DIAMETER メッセージと PANA メッセージはそれぞれ 1 つの DIAMETER ヘッダ，PANA ヘッダと複数の AVP から構成されている．この AVP は用途に応じて定義することができ，拡張性を実現している．EAP を利用して認証機能を実現するために EAP パケットを格納する EAP Payload AVP，通信をセキュアにするための鍵情報である Master Session Key（MSK）AVP，MSK の識別子を格納する EAP Key Name AVP が定義されている．認証の流れは**図 2** のようになる．図 2 において，MN/AAAc/AAAr と AAAs は異なるドメインに属しているものとする．

まず MN と AAAc の間で PANA メッセージを交換するための PANA session を確立する (1)．次に AAAc が EAP Identity の Request を生成し MN に送信する（PANA-Auth-Request）(2)．MN から EAP Identity の Response が返ってくると (3)，この EAP Identity の Response を EAP Payload AVP とし，さらに EAP Identity の Response 内の “ユーザ名@ドメイン名” という形をとる Network Access Identifier（NAI）を User Name AVP として Diameter EAP Request に添付する．Diameter EAP Request は EAP Identity の Response に格納されていた NAI のドメイン名部分を利用して AAAr を介して AAAs までルーティングされる (4)．この時点で AAAc-AAAs 間の Diameter EAP Application のためのセッションが確立する．Diameter EAP Request を受け取った AAAs は適当な method（認証方式）を選択し EAP Request パケットを生成する．その EAP Request パケットを EAP Payload AVP として Diameter EAP Answer に添付する．Di-

ameter EAP Answer は AAAs から AAAr を介して AAAc に返信される (5)．AAAc は受け取った Diameter EAP Answer から EAP Request パケットを取り出し MN に送信する．以降 AAAs が選択した method による認証が終了するまで EAP Request/Response の交換が続く（図 2 の中の枠で囲った部分が繰り返される）．代表的な認証方式である EAP-PSK method を利用した場合，枠で囲った部分が 3 回繰り返される．最終的に AAAs が EAP Success/Failure を EAP Payload AVP として Diameter EAP Answer に添付して AAAc に送信するところで終了する (6)．AAAc は Diameter EAP Answer の Result Code AVP の中身が DIAMETER MULTI ROUND AUTH であれば引き続き EAP の認証が行われると判断し，DIAMETER SUCCESS であれば EAP の認証が成功したと判断し，それ以外の値であれば EAP の認証が失敗したと判断する．EAP が成功した場合は EAP Success パケットを格納した EAP Payload AVP の他に MSK を格納した EAP Master Session Key AVP と MSK の識別子を格納した EAP Key Name AVP が送られる．その後 AAAc が MN に PANA-Bind-Request を送り (7)，MN から PANA-Bind-Answer を受信する (8) ことで認証が完了し，MN が通信できる状態になる．

MN が移動し，接続する AR を変えるたびに以上のようなメッセージ交換を行い認証される．しかしこの処理ではメッセージ交換数が多く，特に AAAr と AAAs は異なったドメインに属するためこの間のメッセージ交換には時間を要する．そのため MN が新たに AR に接続されてから通信できるまでに時間がかかるという問題がある．

3. 関 連 研 究

3.1 ドメイン内移動時の高速 AAA 処理（FPANA）

MN の移動にはドメイン内移動とドメイン間移動の 2 種類の場合が考えられる．ドメイン内移動においての高速 AAA 処理として我々は FPANA という方式を提案している[3]．PAR と NAR 間において，MN と PAR が共有していた情報を転送するプロトコルとして Context Transfer Protocol（CT）[9] が提案されており，FPANA はこの CT を利用している．**図 3** で示すように FPANA は，visited domain においてすでに認証が完了している MN が同一ドメイン内で移動を行う際（1. detect New AR），CT を用いて PAR と MN の間に確立されている PANA session を NAR に移動させること（2. context transfer）で認証の高速化を実現している．つまり PANA session の移動により MN の認証された状態を継続し，back-end の AAA システムへの問合せを省略している．MN の移動時には FMIPv6 [10] で得られる情報を用いることで MN の移動に先立って NAR の IP アドレスや MAC アドレスを取得可能とし，MN が移動する前に AR 間で MN の認証情報の受け渡しが可能となる．さらに PANA でやりとりするメッセージを FMIPv6 のメッセージに付加することで冗長なメッセージのやりとりを減らし，さらなる高速な認証を可能としている．また情報をやりとりする AR 間はセキュアであることが前提となっている．

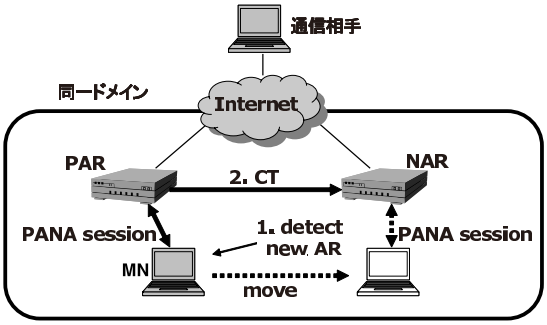

図 3 FPANA の動作
Fig. 3 Procedure of FPANA.

ここでドメイン間移動時に FPANA の適用を仮定してみる．FPANA を利用するには，PAR は NAR の IP アドレスを取得可能であり，PAR と NAR の間の通信はセキュアであることを前提としている．しかし NAR が PAR とは異なるドメインに所属している場合，この前提には無理がある．よって FPANA をドメイン間移動の場合に利用することは現実的ではない．

3.2 MPA: Media Independent Pre-Authentication

MPA は特定のリンクレイヤや特定のモビリティマネージメントプロトコルに依存しない事前認証プロトコルとして提案されており処理の手順は以下のようになる．ここではモビリティマネージメントプロトコルとして MIPv6 を例にあげ説明を行う．

まず MN は移動先になりそうなネットワーク（Candidate Target Network，CTN）を発見するとそのネットワーク内にある認証エージェント（authentication agent，AA），MN の IP アドレスを得るための構成エージェント（configuration agent，CA），AR のそれぞれの IP アドレスをなんらかの方法で取得する．そして MN と AA との間で認証が行われ，認証に成功

すると MN-CA key，MN-AR key が生成され各 key は CA，AR，MN それぞれに送られる．

次に MN がリンクレイヤの情報から移動先になりそうな CTN を検知すると，MN は CA とのやりとりから移動後の new care-of address を得る．また MN と移動後の AR との間では tunnel management protocol を用いて proactive handover tunnel（PHT）を生成する．

そしてなんらかの方法を用い MN が CTN に移動することを決定すると MN は MIPv6 での binding update メッセージを Home Agent に送信する．これにより MN は実際に CTN に移動する前に PHT を介してパケットを受信する．最後に実際に MN が CTN に接続されると PHT は消去される．

MPA は移動先のネットワークの agent の IP アドレスを発見する方法などの詳細は定められていないフレームワークの提案になっている．

3.3 関連研究のまとめ

FPANA は MN のドメイン内移動を想定し移動前後の AR どうしに信頼関係があることを前提として認証情報を移動前後の AR どうしで共有することで認証の高速化を実現している．MPA は MN の移動を検知すると実際に移動する前に認証を行い，鍵を共有することで認証の高速化を実現している．

しかし FPANA は MN がドメイン間を移動することは想定しておらず，MPA はフレームワークの提案のみで具体的な詳細が定められていない．また，情報転送に必要な NAR の IP アドレスを MN が取得する手段を FPANA も MPA も定めてはいない．

4. 設　　計

4.1 XD-AUTH の概要

XD-AUTH の動作概要を**図 4** に示す．XD-AUTH は MN が移動する前に MN の認証情報を NAR に送り，MN の移動後の認証を MN と NAR のメッセージ交換のみで行うことで認証の高速化を実現する．まず MN は NAR の IP アドレスを CARD（Candidate Access Router Discovery）[12] プロトコルを利用して取得する (1)．次に MN は AAAs に認証要求を送信する (2)．AAAs は認証の結果得られる MN の認証情報を DIAMETER back-end 上で NAR まで転送する (3)．認証情報の転送を DIAMETER back-end 上で行うためこの処理はセキュアであることが保証される．この認証情報転送により実際に MN が移動し (4)，その後の認証が MN-NAR 間のメッセージ交換のみで行われ高速化が実現できる (5)．

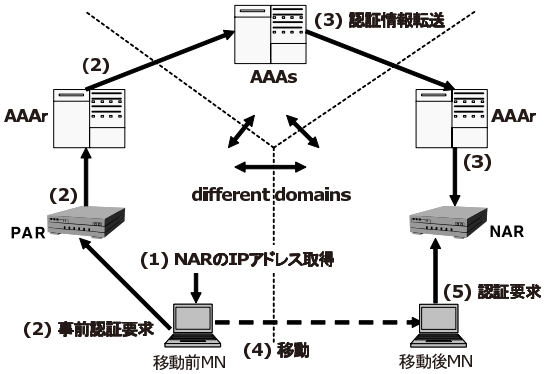

図 4 XD-AUTH の動作概要
Fig. 4 Procedure of XD-AUTH.

以上のような認証システムを実現するために CARD と DIAMETER/PANA を拡張利用する．詳細を以下で説明する．

4.2 NAR の識別

IEEE802.11 のような無線 LAN においては，アクセスポイント（AP）は定期的に自身の存在を知らせるためにビーコンを送信している．本論文では議論を簡略化するため，1 台の AR（アクセスルータ）には 1 台の AP が接続しているとする．ビーコンには AR の L2 アドレスの情報が含まれているが IP アドレスの情報は含まれていない．MN が移動先の AR に近づくにつれてビーコンの強度が強まり，MN は接続する AR を切り替えることを決定する．

移動先候補の AR が複数ある場合についてはレイヤ間制御情報伝達機構 LIES [11] を用いて周辺の AP の電波強度を知り，最も強いものを移動先 AR とする．

元々の CARD は各 AR が近隣 AR の L2 アドレスと IP アドレスを対応付けることのできるテーブルを保持し，MN が IP アドレスを取得したい AR の L2 アドレスを含めた CARD Request を AR に送るとその L2 アドレスに対応する IP アドレスを含めた CARD Reply が返ってくるという仕組みになっている．

XD-AUTH において図 4 の “(1)NAR の IP アドレスの取得” を実現するために CARD のオプションの機能として提案されている CARD Server の利用，拡張を行う．元々の CARD では，CARD Server は MN が移動する可能性のあるすべての AR の L2 アドレスと IP アドレスとを対応付けるテーブルを保持していることが前提となっており，機能を一極集中的に実現するアプローチである．しかし本論文で想定している MN の移動がドメイン間である場合，異なるドメインに所属している AR の情報を 1 つの CARD Server が保持しているという仮定には無理がある．そこで本論

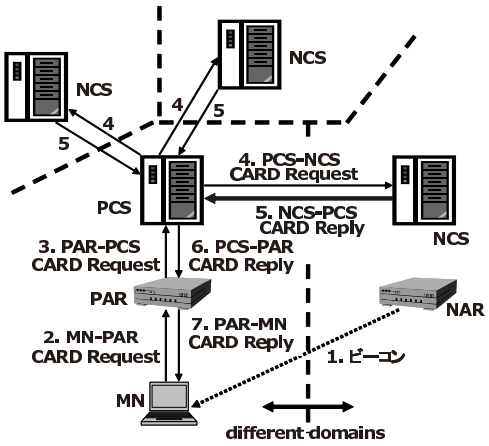

図 5 NAR の IP アドレス取得までの流れ
Fig. 5 Procedure to acquire NAR's IP address.

文では各ドメインにはそのドメインに所属するすべての AR の情報を保持している CARD Server（または CARD Server 群）が存在することを仮定する．通常，各ドメインは運用上，自身のドメイン内にある機器の情報を管理する必要があると考えられるためこの仮定は妥当であると考えられる．そのうえで，隣接する各ドメインの CARD Server どうしのメッセージ交換を新たに定義することにより，MN による NAR の IP アドレスが取得可能となる．

また，CARD Server 間が隣接していることを知る方法や隣接関係情報の更新方法については現在はネットワーク管理者が設定し固定的に利用することを想定している．今後これらを自動的に行うプロトコルを定義することも可能であり，今後の課題である．

図 5 に NAR の IP アドレス取得までの流れを示す．MN はまず NAR の L2 アドレスを受信し（1. ビーコン），PAR に受信した L2 アドレスを送信する（2. MN-PAR CARD Request）．PAR は自分が持つ L2 アドレスと IP アドレスを対応付けるテーブルに MN から送られてきた L2 アドレスのエントリがあるかを探す．もしあれば対応する IP アドレスを MN に返すが，ここでは MN の移動先が別のドメインであることを仮定しているため，このテーブルには送られてきた L2 アドレスのエントリはない．そこで PAR は自ドメインの CARD Server（Previous CARD Server, PCS）に MN から送信されてきた L2 アドレスを転送する（3. PAR-PCS CARD Request）．PCS は PAR の動作と同様に，自分の持つテーブルに PAR から送られてきた L2 アドレスのエントリがあるかを探す．もしあれば対応する IP アドレスを PAR に返すが，MN の移動先が別のドメインであることを仮定している

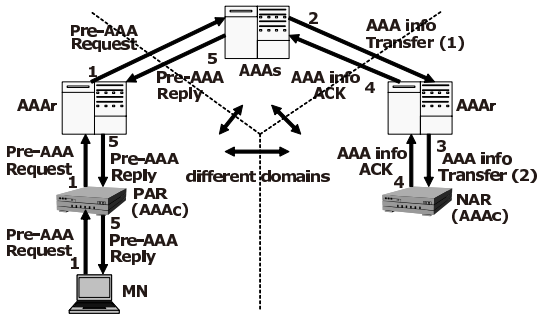

図 6 NAR への認証メッセージ転送
Fig. 6 Procedure to transfer authentication information to NAR.

ため，このテーブルにも送られてきた L2 アドレスのエントリはない．この場合近隣に存在する複数のドメインの CARD Server に L2 アドレスを送信する（4. PCS-NCS CARD Request）．このメッセージを受信した CARD Server はテーブル中に対応する L2 アドレスのエントリがあれば，その L2 アドレスに対応する IP アドレスとその CARD Server（Next CARD Server, NCS）が所属するドメイン名を PCS に返す（5. NCS-PCS CARD Reply）．PCS は NCS から受信した IP アドレス，移動先のドメイン名を PAR に送信する（6. PCS-PAR CARD Reply）．このとき，移動先が別ドメインであることを MN に知らせるために CARD ヘッダ中に移動先が別ドメインであることを示すフラグを新たに定義し，このフラグを立てることをあわせて行う．PAR は受信した IP アドレス，移動先のドメイン名，移動先が別ドメインであることを示すフラグの情報を MN に転送する（7. PAR-MN CARD Reply）．これらのやりとりにより MN は移動先の AR の IP アドレス，移動先のドメイン名，そして移動がドメイン間であることを知ることができる．

4.3 認証情報の事前転送

XD-AUTH において図 4 の “(2) 事前認証”，“(3) 認証情報転送” を実現するために DIAMETER を拡張する．**図 6** に NAR に認証情報を転送するまでの流れを示す．

まず，“(2) 事前認証” において NAR の IP アドレス，移動先のドメイン名を格納する新たな AVP を定義する．また XD-AUTH を行うことを示すフラグも定義し，認証要求メッセージの中にこれらを含めたものを Pre-AAA Request として MN から PAR，AAAr を経由して AAAs に送信する（1: Pre-AAA Request）．AAAs は Pre-AAA Request 中の XD-AUTH であることを示すフラグから，XD-AUTH での認証であることを判断し，認証を行う．認証に成功すると AAAs か

らNARへの“(3) 認証情報転送”が行われる．AAAsは鍵などの認証完了後に得られる情報を含んだAAA info transferメッセージを移動先ドメインのAAArを介してNARまで送る（2, 3: AAA info transfer）．ここでAAAr，NARのアドレス解決はPre-AAA Request中に含まれる新たに定義したAVPである移動先ドメイン名，NARのIPアドレスから行われる．情報の転送が成功したことをNARから移動先のAAArを経由してAAAsへ伝える（4: AAA info ACK）．認証応答メッセージにNARへの情報転送が成功したことを示すフラグを加えたPre-AAA ReplyをAAAsから移動前に所属しているドメインのAAAr，PARを経由してMNへと送信する（5: Pre-AAA Reply）．こうすることでAAAシステムのback-endでセキュアに認証完了後に得られる情報をMNとNARで共有することができる．

4.4 移動後の認証

本節では図4においてのMN移動後の“(5) 認証要求”について説明する．通常の認証では図2のようなメッセージ交換が必要であるが，XD-AUTHではNARに認証情報がすでに転送されているためMNとNARの間のメッセージ交換だけで認証を行うことができる．具体的にはPANAメッセージ中にXD-AUTH用のフラグを定義し，NARに認証情報の転送が完了していることが確認できた場合にMNはこのフラグをセットしてPANAメッセージを送る．NARはこのフラグからXD-AUTHであることを判断し，PANAメッセージ中のUser Name AVPとOrigin Realm AVPの値が一致したら，認証が成功したと見なす．こうすることでMNとNARの間のメッセージのやりとりだけで，認証を行うことができ，通信が再開できるまでの時間を短縮することができる．**図7**に通常の認証の場合とXD-AUTHを実行した場合のMN移動後における認証の様子を示す．この図においてAAArとAAAsの間の通信にかかる時間はMNが契約しているドメインから離れれば離れるほど長くなり，EAPにおいて使用する認証methodによって異なるが，通常認証が完了するまでに複数往復のメッセージ交換を必要とするためこの差は顕著なものになると考えられる．

もし，MNが認証完了後に得られる情報がNARに転送されたことを示すPre-AAA Replyを受信する前に移動を完了した場合は，MNは通常の認証を行う．この場合，実際に使用されないにもかかわらず，MNの認証完了後に得られる情報をNARに渡してしまうことになるが，NARが信頼できるという前提においては悪用されることはない．MNがNARを介して通信するにはそのMNとNAR間で共通鍵を持たなければならないが，NARに事前認証によって得られた共通鍵が残ったところでその共通鍵を悪意のあるMNが持ちえないためである．また，NARが攻撃されると共通鍵が盗まれる可能性もあるため，ライフタイムを持たせている．

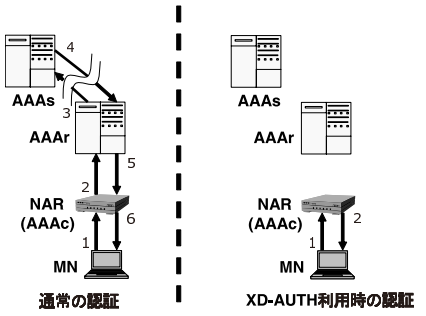

図7 MN移動後の通常時の認証とXD-AUTH利用時の認証
Fig. 7 Authentication procedure after MN's movement in normal case and in XD-AUTH.

4.5 XD-AUTHの動作

XD-AUTH全体を通してのメッセージシーケンスを**図8**に示す．移動前の事前認証プロセスのところで，MN-AAAs間でのメッセージ交換が1回で認証が完了している例をあげているが，通常はAAAs-NAR間で情報転送をする前にMN-AAAs間で2〜3往復のメッセージ交換が行われる．MN移動後の認証は通常図2に示したメッセージ交換全部を行うが，XD-AUTHではMN-PAR間での最初の5つのメッセージ交換をMN-NAR間で行うだけで実現している．

5. 実　　装

本論文で提案するXD-AUTHを実現するにあたりAAAプロセス，CARDプロセスをFreeBSD6.1-Release上に実装した．AAAプロセスの実装にあたり，WIDEプロジェクトが公開しているDIAMETERのライブラリであるWIDE Diameterを拡張することでXD-AUTHの機能を実現した．

5.1 CARD機能の実装

図9のように我々が開発したPANAライブラリ，WIDE Diameterを利用するのと同時にMN，PAR，各CARD Server上でCARD functionを新たに実装した．

5.2 情報転送機能の実装

既存のWIDE DiameterライブラリではAAA ServerはMNからの認証要求メッセージを受信し，認証した後，応答メッセージをMNに送り返す機能が実装されている．しかし，認証の結果得られる情報を

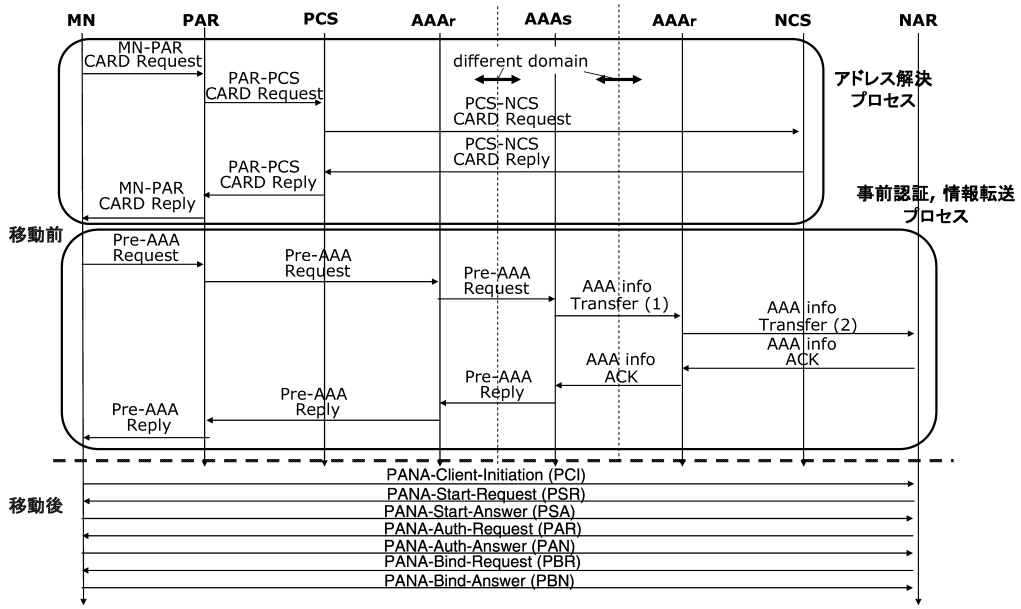

図 8 XD-AUTH 全体のメッセージシーケンス
Fig. 8 Total message sequence in XD-AUTH.

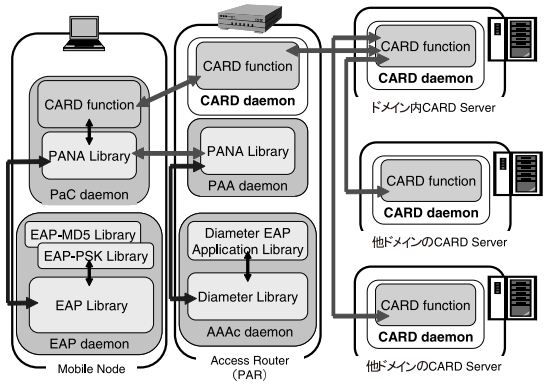

図 9 CARD 機能の実装
Fig. 9 Implementation of CARD function.

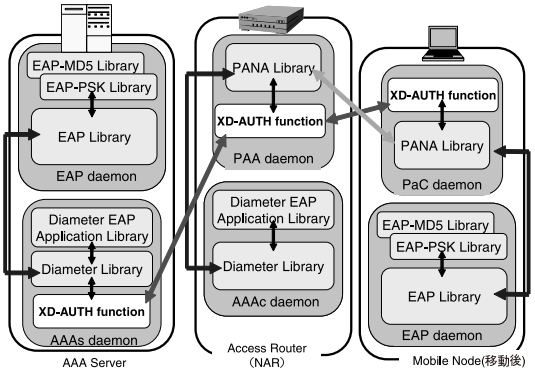

図 10 DIAMETER における情報転送機能の実装
Fig. 10 Implementation of information transfer in DIAMETER.

認証要求メッセージ送信者以外に送る仕組みは実装されていない．XD-AUTH を実現するためには AAAs は MN の移動先ドメインの AAAr，NAR に情報を転送することが必須である．そのためメッセージ送信者以外にもメッセージを転送できる機能を新たに実装し，WIDE Diameter を拡張した．また，MN 移動後の高速認証を行うための機能を実装することで我々が開発した PANA ライブラリも拡張した．**図 10** の XD-AUTH function の部分がライブラリを拡張した部分に相当する．

6. 評　　価

図 11 のようなネットワークを組み XD-AUTH にかかる各時間を測定した．各マシンのスペックは**表 1** のとおりである．ここでは AAAr を省略しているが，AAAr はメッセージ自体の処理はせず転送のみ行うため本質的には問題ない．XD-AUTH の各処理のうち，アドレス解決プロセスを**図 12**，事前認証，情報転送プロセスを**図 13**，移動後の認証プロセスを**図 14** に示す．また MN が移動した後，通常の認証を行った場合の処理時間もあわせて測定し，測定結果を**図 15** に示す．各数値はそれぞれ 30 回の試行を行い，その平均値を計測値とした．

6.1 実 行 時 間

同一リンク内 RTT を RTT_{link}，同一ドメイン内

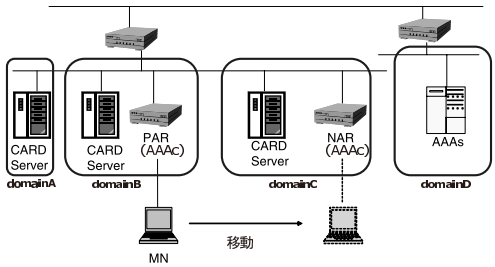

図 11 構成したネットワーク
Fig. 11 Test network.

表 1 各マシンのスペック
Table 1 The specification of each machine.

マシン	CPU	メモリ
AAAs	VIA C3 800 MHz	512 MB
CARD Server	VIA C3 800 MHz	512 MB
PAR, NAR	VIA C3 800 MHz	512 MB
MN	VIA C3 800 MHz	512 MB

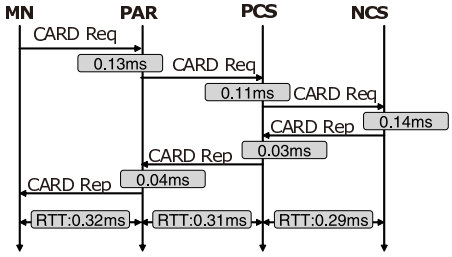

図 12 アドレス解決プロセスにおける処理時間
Fig. 12 Processing time of address resolution.

RTT を RTT_{intra}，ドメイン間 RTT を RTT_{inter} とする．図 12 からアドレス解決にかかる時間が 0.45 msec+$1RTT_{link}$+$1RTT_{intra}$+$1RTT_{inter}$，図 13 から事前認証，情報転送にかかる時間が 16.11 msec+$5RTT_{link}$+$4RTT_{inter}$ であることが分かる．ここで XD-AUTH を実環境で利用することを想定し，文献 13) に基づき RTT_{link} を 1 msec，RTT_{intra} を 3 msec，RTT_{inter} を 23 msec と仮定すると XD-AUTH において MN が移動前の処理にかかる時間は 140.56 msec となる．この値は MN が移動先のビーコンを受信してからハンドオーバ開始までに行うべき処理にかかる時間であり，XD-AUTH を実環境で利用するうえで問題のない値といえる．

MN が移動した後，通常の認証にかかる時間は図 15 から 22.2 msec+$5RTT_{link}$+$3RTT_{inter}$，XD-AUTH の認証にかかる時間は図 14 から 9.29 msec+$3RTT_{link}$ であることが分かる（本論文の実験環境では MN 移動後の XD-AUTH すべての処理に 10.22 msec かかった）．上述と同様に RTT_{link} を 1 msec，RTT_{inter}

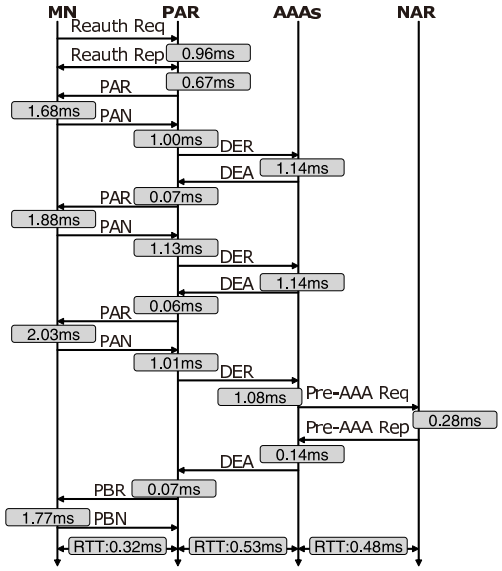

図 13 事前認証，情報転送プロセスにおける処理時間
Fig. 13 Processing time of pre-authentication and information transfer.

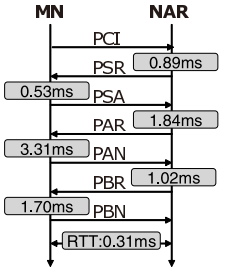

図 14 MN 移動後の XD-AUTH 認証にかかる各処理時間
Fig. 14 Processing time of XD-AUTH authentication after MN's movement.

を 23 msec と仮定すると通常の認証にかかる時間が 96.2 msec であるところを XD-AUTH 認証では 12.29 msec に短縮できる．以上の結果から MN が移動した後 MN が通信を再開できるまでの時間，つまり MN が通信できない時間を XD-AUTH は短縮できていることが分かる．リアルタイム音声通信での許容切断時間 50 msec [14] を考えても XD-AUTH における認証時間短縮は有用であることが分かる．

6.2 安全性の考察

XD-AUTH は利用する認証方式そのものや IPsec といった安全な通信路を提供する方式には変更を加えていないため，既存の認証方式や暗号化方式に脆弱性を加えることはない．したがって，認証方式自体や IPsec の耐攻撃性に関する考察は本論文の対象外である．そこで本節では XD-AUTH における情報交換が安全に行われているかに焦点を当てて考察する．

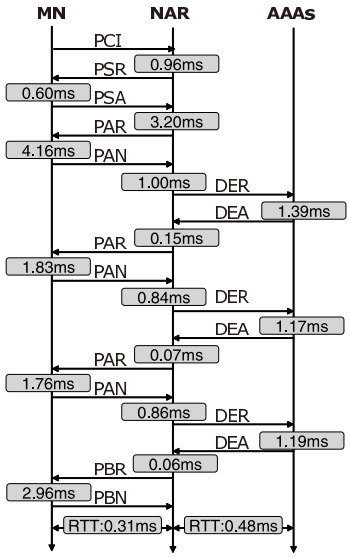

図 15 MN 移動後の通常の認証にかかる各処理時間
Fig. 15 Processing time of normal authentication after MN's movement.

XD-AUTH は図 8 の事前認証，情報転送プロセスで示すとおり，MN が移動する前に事前認証を行い，認証の結果得られる鍵などの MN の認証情報を NAR まで転送する．このとき MN と PAR の間の通信は XD-AUTH を開始するときにすでに存在している MN-PAR 間の PANA session によりセキュアに保たれる．PAR-AAAr 間，AAAr-AAAs 間，AAAr-NAR 間の通信は DIAMETER back-end 上での通信であり，DIAMETER の仕様上セキュアに保たれることが保証されている．よって XD-AUTH での情報転送において盗聴される心配はない．

NAR に事前に User Name AVP，MSK AVP といった MN の認証情報を送ること自体の安全性に関しては，NAR は AAAc であり通常の認証においてもこの情報は AAAc に送られるため問題はない．また NAR に MN の認証情報が転送されたにもかかわらず，実際は MN が移動しなかった場合においても悪意のある MN が MN の認証情報を持ちえないため悪用はできず，NAR が攻撃され認証情報が盗まれる可能性を考えて，ライフタイムを持たせている．

7. ま と め

マルチドメイン構成のインターネット環境において MN の移動時に高速に認証が行われるシステムが求められている．MN の移動がドメイン内の場合だけではなく，ドメイン間である場合も想定する必要がある．本論文では MN のドメイン間移動時，認証を高速に行うために移動先 AR のアドレス解決を行う CARD プロトコルと認証メッセージを転送する DIAMETER/PANA プロトコルを拡張利用した XD-AUTH を提案した．XD-AUTH を FreeBSD に実装し，実験ネットワークで処理時間を測定したところ，ドメイン間移動時に通常の認証では 22.2 msec+$5RTT_{link}$+$3RTT_{inter}$ かかるところを XD-AUTH では 9.29 msec+$3RTT_{link}$ で完了できた．上述のとおり RTT の値を仮定すると 96.2 msec から 12.29 msec に認証時間を短縮でき，リアルタイム音声通信での許容切断時間 50 msec を考えても XD-AUTH が有用であることが分かる．

参 考 文 献

1) Patil, B., Roberts, P. and Perkins, C.E.: IP Mobility Support for IPv4, RFC3344, IETF (Aug. 2002).
2) Johonson, D.B., Perkins, C.E. and Arkko, J.: Mobility Support in IPv6, RFC3775, IETF (June 2004).
3) 海沼義彦，小野夏子，木村 徹，張 亮，林 秀樹，寺岡文男：FMIPv6 における PANA を用いた高速杷証方式の設計と実装及び評価，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO 2005）シンポジウム論文集 (July 2005).
4) Forsberg, D. and Ohba, Y. (Eds.), Patil, B., Tschofenig, H. and Yegin, A.: Protocol for Carrying Authentication for Network Access (PANA), Internet draft, IETF (Sep. 2007). (Work in progress).
5) Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and Arkko, J.: Diameter Base Protocol, RFC3588, IETF (Sep. 2003).
6) Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H.: PPP Extensible Authentication Protocol (EAP), RFC3748, IETF, (June 2004).
7) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC4301, IETF (Dec. 2005).
8) Rigney, C., Willens, S., Rubens, A. and Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC2865, IETF (June 2000).
9) Koodli, R., Loughney, J., Nakhjiri, M. and Perkins, C.: Context Transfer Protocol, Internet draft, IETF (Aug. 2004).
10) Koodli, R.: Fast Handovers for Mobile IPv6, RFC4068, IETF (July 2005).
11) 後郷和孝，寺岡文男：動的なネットワーク環境に適応するためのクロスレイヤシステムの設計と実装，電子情報通信学会論文誌（掲載予定）.

12) Chaskar, H., Funato, D., Liebsch, M., Shim, E. and Singh, A.: Candidate Access Router Discovery (CARD), RFC4066, IETF (July 2005).
13) 菊池 豊，藤井資子，山本正晃，永見健一，中川郁夫：遅延計測による日本のインターネットトポロジーの推定，情報処理学会研究報告，2007-DSM-46, 2007-QAI-24, pp.103–108 (July 2007).
14) Shirdokar, R., Kabara, J. and Krishnamurthy, P.: A QoS-based Indoor Wireless Data Network Design for VoIP Applications, *Proc. IEEE Vehicular Technology Conference 2001 Fall*, pp.2594–2598 (2001).

(平成 19 年 7 月 29 日受付)
(平成 19 年 12 月 4 日採録)

川口 裕樹

2006 年慶應義塾大学理工学部情報工学科卒業．2006 年同大学大学院入学．現在，在学中．AAA 基盤の研究に従事．

海沼 義彦

2005 年慶應義塾大学理工学部情報工学科卒業．2007 年同大学大学院修士課程修了．

張 亮

2003 年立命館大学大学院理工研究科前期博士課程修了．2004 年日本テレコム（株）（現ソフトバンクテレコム（株））入社．以来，無線ネットワークのモビリティ制御技術とセキュリティ技術の研究開発に従事．2006 年ボーダフォン（株）（現ソフトバンクモバイル（株））ワイヤレスシステム研究開発センターに出向．現在，無線ネットワーク制御技術に関する研究開発に従事．電子情報通信学会会員．

林 秀樹（正会員）

1988 年大阪大学工学部通信工学科卒業．1990 年同大学大学院工学研究科博士前期課程修了．同年日本テレコム（株）（現ソフトバンクテレコム（株））入社．2002 年から 2004 年まで通信・放送機構高知通信トラヒックリサーチセンター研究員として出向．2004 年高知工科大学大学院・工学研究科博士後期課程修了．同年日本テレコム（株）情報通信研究所（現ソフトバンクテレコム（株）研究所）に復帰．2006 年ボーダフォン（株）（現ソフトバンクモバイル（株））ワイヤレスシステム研究開発センターに出向．現在に至る．博士（工学）．QoS およびモビリティネットワークに関する研究に従事．本会第 66 回全国大会大会優秀賞受賞．電子情報通信学会会員．

寺岡 文男（正会員）

慶應義塾大学理工学部教授．1984 年慶應義塾大学大学院修士課程修了．同年キヤノン（株）入社．1988 年（株）ソニーコンピュータサイエンス研究所入社．2001 年 4 月から現職．博士（工学）．1991 年日本ソフトウェア科学会高橋奨励賞受賞．1993 年元岡記念賞受賞．2001 年情報処理学会平 12 年度論文賞受賞．コンピュータネットワーク，オペレーティングシステム，分散システム等の研究に従事．2000 年 5 月から 2002 年 5 月まで情報処理学会理事．2005 年 4 月から日本ソフトウェア科学会理事．著書に『ワイヤレス LAN アーキテクチャ』（共著，共立出版），“Wireless IP and Building the Mobile Internet”（共著，Artech House Publishers）．監訳に『詳解 Mobile IP』（共監訳，プレンティスホール出版）．ACM，IEEE，日本ソフトウェア科学会，電子情報通信学会各会員．