情報処理学会論文誌 Vol. 51 No. 1 163–173 (Jan. 2010)

IP データ通信用フェムトセルを用いた移動体ネットワーク接続におけるプロキシ型 MOBIKE ハンドオフ方式とその高速化手法に関する研究

千葉恒彦[†1] 小森田賢史[†1] 横田英俊[†1]

近年，移動体ネットワークを構成する要素として，フェムトセルやピコセルなどの携帯電話の小型基地局が注目されている．フェムトセルは，高層ビルや地下など広域基地局からの電波が十分に到達しないエリアに配置し，通信エリアを拡充するために用いられるが，その他のメリットとして，少数ユーザで専有的に無線帯域を利用することによる通信容量の増加や移動体アクセスネットワークの負荷軽減などもあげられる．通信エリア拡充のため，オフィス内にフェムトセルを複数配置した場合，ユーザが移動しながらデータ通信を継続するためには，フェムトセル間のハンドオフ技術が要求される．とりわけ VoIP などのリアルタイムアプリケーションでは，フェムトセル間の高速なハンドオフ技術が重要な課題となる．本論文では，複数のプロトコル実装にともなうフェムトセルの負荷増大を軽減し，かつフェムトセル間ハンドオフを実現するプロキシ MOBIKE 方式について提案し，実装評価によりその有効性を検証する．

Study on Proxy-based MOBIKE Handoff and its Fast Method for IP Data Communication in Femtocell Integrated Mobile Network

Tsunehiko Chiba,[†1] Satoshi Komorita[†1] and Hidetoshi Yokota[†1]

Recently, small base station such as femtocell and picocell are drawing attention as new components of wireless access networks. These small base stations are used not only to expand the wireless area in a high-rise building or basement, where the signal strength from macrocell base stations is not often strong enough, but also to increase bandwidth capacity for IP data communication and reduce the load on the core network. If multiple femtocells are deployed in an office building to expand the wireless area, a handoff mechanism between femtocells is required to support the continuity of IP data communication. Especially, real-time applications such as VoIP require a seamless handoff mechanism. In this paper, we propose Proxy MOBIKE mechanisms that can realize an efficient handoff between femtocells and mitigate the complexity of femtocell implementation resulting from supporting multiple protocols. We also implement our proposed mechanism to verify and compare their effectiveness.

1. はじめに

移動体ネットワークにおける TCP/IP の利用が普及するにつれて，ネットワーク全体を IP 化するオール IP 化の流れが加速している．これに呼応して，第 3 世代移動通信の標準化においても IMS（IP Multimedia Subsystem）[1] および MMD（Multimedia Domain）[2] が規定され，SIP（Session Initiation Protocol）[3] を用いたマルチメディアアプリケーション制御基盤が整いつつある．一方，移動体基地局機能の集積化技術により，フェムトセルと呼ばれる屋内設置が可能な小型の基地局が実現可能となり，移動端末の新しい収容形態として注目されている[4]．フェムトセルは，高層ビルや地下など広域基地局からの電波が十分に到達しないエリアに配置し，通信エリアを拡充するために用いられるが，フェムトセルを用いるメリットとして，少数ユーザで専有的に無線帯域を利用することによる通信容量の増加，一般のブロードバンド回線を介してフェムトセルを移動体通信事業者のコアネットワークと直接通信させることによる，移動体アクセスネットワークの負荷軽減などもあげられる[5]．フェムトセルは，一般的に携帯電話の音声通信に用いられるが，IP データ通信に用いることも可能である．IP データ通信を提供する場合，ブロードバンド回線を利用したアクセス方式として，汎用の無線 LAN を利用して移動体コアネットワークへ接続する形態は 3GPP2（Third Generation Partnership Project 2）における無線 LAN とのインターワーク標準文書[6] により規定されているものの，フェムトセルを利用した移動体コアネットワークへの接続形態は十分に検討されていない．たとえば，基地局を小型化し，その送信電力を小さくすると 1 基地局あたりの収容エリアも狭くなるため，オフィスなどの比較的広いエリアに設置して隈なく通信を可能にするにはフェムトセルを複数台設置する必要がある．このような環境下でユーザが移動しながら通信を行う場合，アプリケーションの IP データ

†1 株式会社 KDDI 研究所
KDDI R&D Laboratories, Inc.

通信継続のためにはフェムトセル間のハンドオフを実現する必要がある．とりわけ，VoIP（Voice over IP）やテレビ電話などのリアルタイムアプリケーションでは，通信の断時間を極力短縮した高速ハンドオフ技術が要求される．なお，フェムトセルと広域基地局間の IP データ通信継続のためのハンドオフ方式としては，モバイル IP [7),8)] などの方式を用いることで実現可能である．よって，本論文ではフェムトセルと広域基地局間のハンドオフは対象外とし，フェムトセル間のハンドオフ評価を対象とする．

本論文では，まず IP データ通信におけるフェムトセル間のハンドオフを実現する既存の移動管理方式として，汎用の無線 LAN のネットワーク間ハンドオフに用いられる MOBIKE（IKEv2 Mobility and Multihoming）[9)]，およびネットワーク主導でハンドオフを制御するプロキシモバイル IP [10),11)] について説明する．次に，フェムトセル上の実装プロトコル数をより低減させたプロキシ MOBIKE 基本方式を提案するとともに，IPSec のセッション情報をフェムトセル間で転送することによるプロキシ MOBIKE の高速ハンドオフ方式についても提案し，実装評価によりその有効性を検証する．なお，コンテキスト転送方式としては，無線リンクの切替え後にハンドオフ先のフェムトセルの基地局情報を取得するリアクティブ型，無線リンクの切替え前にハンドオフ先のフェムトセルの基地局情報を取得し，あらかじめその情報をネットワークへ通知するプロアクティブ型の 2 方式について検証する．

2. 既存の移動管理方式

2.1 無線 LAN 接続のケース

図 1 に，文献 6) で規定されている，無線 LAN を経由した移動体コアネットワークへの接続形態を示す．ここで，移動体コアネットワークでは，通信事業者により秘匿性が確保されるためセキュアとする．一方，無線区間，ブロードバンドアクセス回線およびインターネットは非セキュアとする．端末は，これら非セキュアのネットワークを介した通信を暗号化するため，移動体コアネットワークに配置されるセキュリティゲートウェイの PDIF（Packet Data Interworking Function）と IKEv2 （Internet Key Exchange version 2）[12)] により IPSec を確立する．また，ネットワーク間ハンドオフの実現には MOBIKE を用いる．ここで，IPSec トンネルの終端装置である端末が用いる IP アドレスとして，PDIF と通信を行うための外側 IP アドレスを TOA（Tunnel Outer Address），アプリケーションのデータ送受信に用いる内側 IP アドレスを TIA（Tunnel Inner Address）と定義する．MOBIKE では，端末がハンドオフ後に変更された TOA を PDIF へ通知することにより，IPSec のセッションを継続させる．

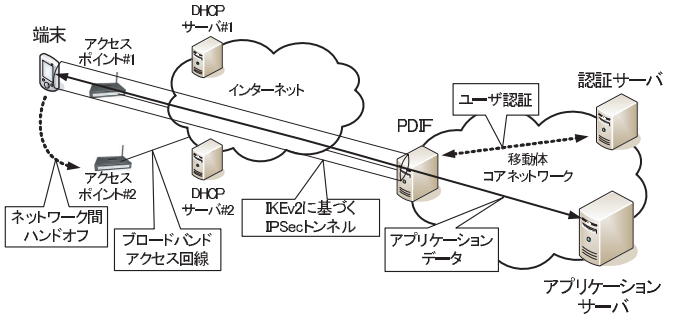

図 1　無線 LAN の接続形態
Fig. 1　Architecture for wireless LAN.

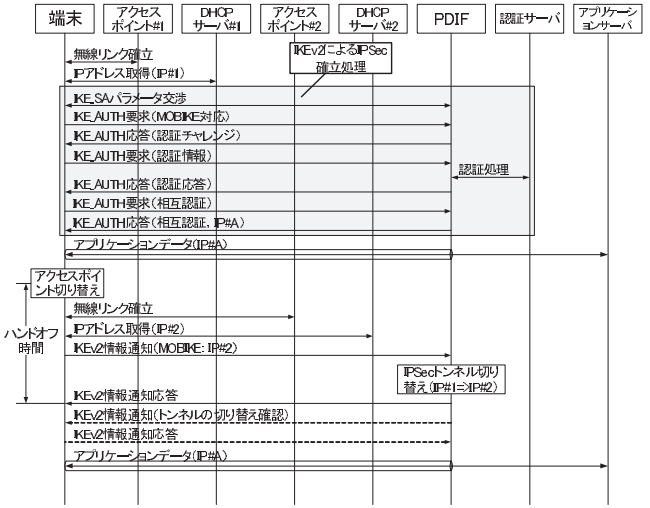

図 2　MOBIKE を用いたハンドオフ手順
Fig. 2　Handoff procedure using MOBIKE.

図 2 に無線 LAN を利用した接続形態の処理手順を示す．端末は，アクセスポイント#1 との無線リンク確立に引き続き，DHCP サーバ#1 より IP アドレス（IP#1）を取得する．その後，端末は PDIF との間で IKEv2 手順に基づき IPSec トンネルを確立する．この IKEv2 手順の中で，PDIF は認証サーバと連携してユーザの認証処理を行うとともに，端末に TIA

である IP#A を割り当てる．なお，端末と PDIF は，MOBIKE 対応可否の交渉も IKEv2 手順の中で行う．その後，端末は IP#A を用いてアプリケーションデータの送受信を行う．端末はアクセスポイント#2 へ移動し，無線リンクの確立に引き続き，DHCP サーバ#2 より IP アドレス（IP#2）を取得する．端末はハンドオフ前後で DHCP サーバより取得した TOA に用いる IP アドレスが異なるため，IKEv2 情報通知を用いて MOBIKE に基づく IPSec トンネルの終端変更（IP#1 から IP#2）を PDIF へ通知する．PDIF は，端末における IPSec トンネルの切替え完了の確認を行うため，IKEv2 情報通知を送信してもよい．ただし，アプリケーションに用いる TIA の IP アドレス（IP#A）は変更されないため，通信は継続される．

2.2　プロキシモバイル IP の利用

一方，携帯電話の小型基地局であるフェムトセルを利用した接続の場合，既存端末は暗号化通信のための IKEv2 や MOBIKE などのプロトコルをサポートしていない．よって，CDMA（Code Division Multiple Access）方式などにより物理層のセキュリティが十分確保されていると見なすことができる場合には，端末ではなくフェムトセルで IPSec トンネルを終端する方が望ましい．これにより，暗号化通信による無線区間の IP パケットのオーバヘッド増大を回避することができるとともに，端末への IKEv2 や MOBIKE の実装にともなう処理負荷を軽減できるという利点も得られる．

図 3 に，cdma2000 HRPD（High Rate Packet Data）のフェムトセルを利用した移動体ネットワークへの接続形態を示す[13]．図 3 の構成において，フェムトセルである FAP（Femto Access Point）間のハンドオフを実現するための手法として，端末が介在せずにハンドオフ前後で同一の IP アドレスを割り当てることが可能なプロキシモバイル IP[10),11)] の利用が考えられる．プロキシモバイル IP では，モバイル IP の登録要求を MAG（Mobile Access Gateway）が端末の代わりに LMA（Local Mobility Anchor）へ送信することにより端末の移動管理を行う．ここでは，FAP が MAG として動作することにより，ハンドオフ前後で同一の IP アドレスを端末へ割り当てる．

2.3　既存の移動管理方式の課題

しかしながら，プロキシモバイル IP を用いた場合，FAP は FGW（Femto Gateway）との IPSec 確立のための IKEv2 や移動管理のためのプロキシモバイル IP を実装する必要があり，FAP 上のプロトコル数増加による処理負荷増大や LMA 配置による設備数増加といった問題が残る．また，厳密なセキュリティ管理のためには，端末ごとに IPSec トンネルを確立できる仕組みが要求される．既存の移動管理方式として，2.1 節に述べた MOBIKE,

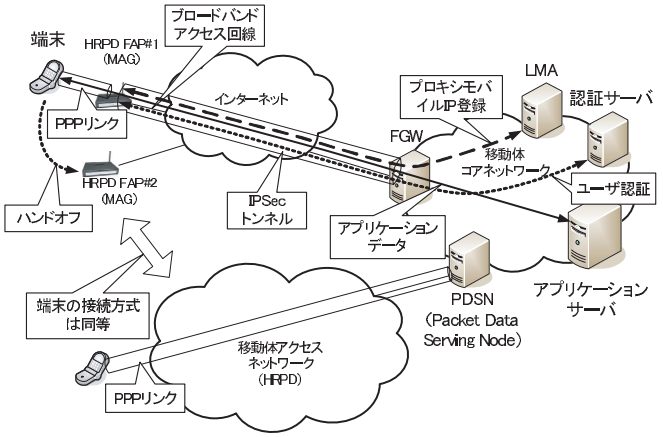

図 3　プロキシモバイル IP を用いたフェムトセルの接続形態
Fig. 3　Proxy Mobile IP based architecture for femtocell.

2.2 節に述べたプロキシモバイル IP のほかに，端末がネットワークのハンドオフを検知して HA（Home Agent）へ登録するモバイル IP，ハンドオフにより変更された IP アドレスを用いて SIP などのセッションを再確立することにより通信の継続性を実現するアプリケーションベースのハンドオフ方式がある．しかしながら，モバイル IP の場合には，HA が追加設備として必要，端末のモバイル IP プロトコル実装による負荷増大および HA を経由することによるアプリケーションデータの冗長経路といった課題が残る．また，アプリケーションベースのハンドオフ方式の場合には，個々のアプリケーションがハンドオフに対応しなければならないため，利用可能なアプリケーションに制約が生じる．そこで，これらの問題を解決するため，FAP が端末ごとに IPSec トンネルを確立し，FGW が IKEv2 手順の中で移動管理を行うプロキシ MOBIKE 方式を 3 章で提案する．

3.　プロキシ MOBIKE の提案と概要

図 4 に，プロキシ MOBIKE による FAP の接続形態を示す．プロキシ MOBIKE では，端末と FAP 間のデータリンク設定手順，および FAP と FGW 間の IKEv2 手順を連携させることにより，ハンドオフ前後で同一の IP アドレスを端末へ割り当てる．よって，本方式では，プロキシモバイル IP で用いた LMA は不要となる．また，端末は通信事業者で認証および管理されており，信頼できるものとする．

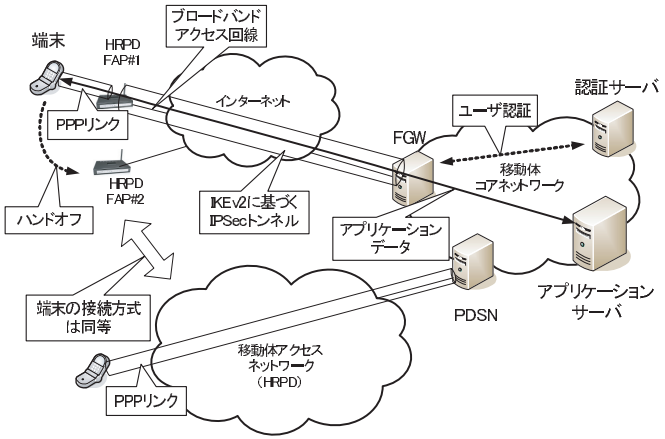

図 4　プロキシ MOBIKE を用いたフェムトセルの接続形態
Fig. 4　Proxy MOBIKE based architecture for femtocell.

3.1　プロキシ MOBIKE 基本方式

図 5 に，cdma2000 HRPD のフェムトセルを利用した場合のプロキシ MOBIKE 基本方式によるセッション確立手順およびハンドオフ手順を示す．フェムトセル端末は，FAP#1 との無線リンク確立に続き，PPP（Point-to-Point Protocol）[14] リンクの設定を行う．PPP リンクは，LCP（Link Control Protocol）による下位リンクの設定，CHAP（Challenge Handshake Authentication Protocol）などに基づくユーザ認証，NCP（Network Control Protocol）によるネットワークアドレスやヘッダ圧縮の設定の順に交渉が行われる．代表的な NCP として，IPCP（IP Control Protocol）や IPv6CP（IPv6 Control Protocol）が定義されており，それぞれ IPv4 用の制御と IPv6 用の制御に用いられる．FAP#1 は LCP 設定手順の実行後，IKEv2 手順に基づいて FGW との鍵交換を保護するための SA（Security Association）である IKE_SA の算出を行う．その後，FAP#1 は，認証処理に用いるユーザ識別子を取得するため，認証チャレンジを端末へ送出する．FAP#1 は認証情報を端末から取得し，ユーザ識別子を IKEv2 の認証要求に含めて送信する．FGW は当該ユーザ名用の認証チャレンジを生成し，そのチャレンジ値を含めた IKEv2 の認証応答を FAP#1 へ返信する．FAP#1 は FGW から取得した認証チャレンジを再度端末へ送信する．FAP#1 は，端末から受信した認証情報を IKEv2 の認証要求に設定して FGW へ送信する．FGW は，認証サーバと RADIUS（Remote Authentication Dial In User Service）[15] などを用

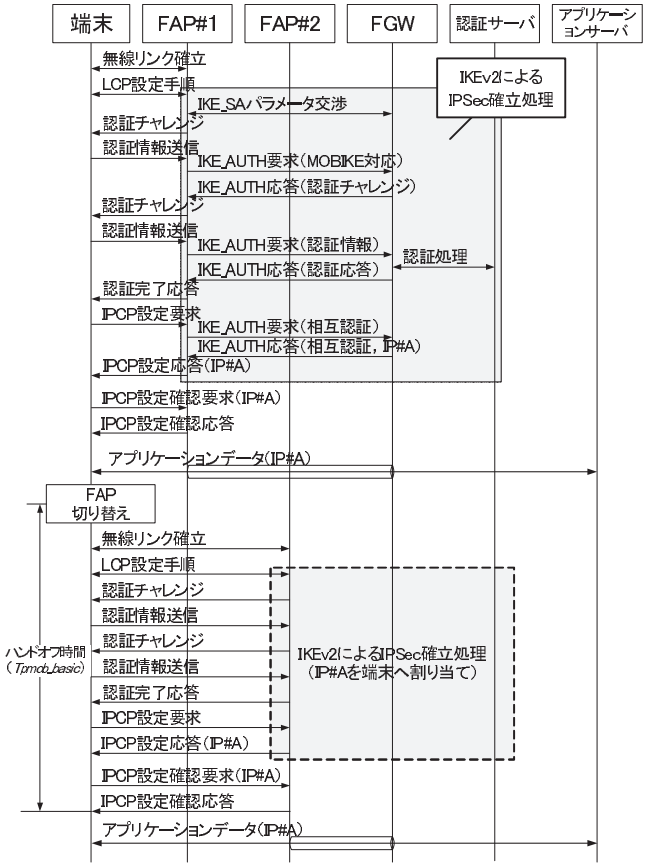

図 5　プロキシ MOBIKE 基本方式の確立及びハンドオフ手順
Fig. 5　Setup and handoff procedure with basic Proxy MOBIKE.

いてユーザの認証を行い，認証応答を FAP#1 へ返信する．FAP#1 は認証応答を端末へ返信後，端末からの IPCP 設定要求受信を契機に，FGW に対して端末に割り当てる IP アドレス（IP#A）を要求する．FAP#1 は，FGW から IKE_AUTH 応答で取得した IP#A を IPCP 設定応答に含めて返信する．端末は指定された IP#A を用いてアプリケーションデータの送受信を行う．端末が FAP#2 へ移動した場合，FGW は IKEv2 の認証手順の中

でハンドオフ前と同一の IP アドレス（IP#A）を割り当てるため，アプリケーションの通信は継続される．

ここで，無線リンクの確立時間を T_w，端末と FAP 間のメッセージ転送時間を T_1，FAP と FGW 間のメッセージ転送時間を T_2，FGW と認証サーバ間のメッセージ転送時間を T_3 とすると，T_1 が影響するメッセージ数が LCP の設定交渉で 2 メッセージ，PPP の CHAP 認証処理で 5 メッセージ，IPCP の設定交渉で 4 メッセージの計 11 メッセージとなり，T_2 が影響するメッセージ数が IKEv2 による IPSec 確立処理の 8 メッセージ，T_3 が影響するメッセージ数が認証処理の 2 メッセージであることから，プロキシ MOBIKE 基本方式を用いた場合のハンドオフ時間 T_{pmob_basic} は次の式で表される．

$$T_{pmob\_basic} = T_w + 11T_1 + 8T_2 + 2T_3 \quad (1)$$

3.2　プロキシ MOBIKE コンテキスト転送方式

3.1 節で示したプロキシ MOBIKE 基本方式では，ハンドオフ後に再度 IPSec の確立を行うため，ハンドオフに時間を要する．リアルタイムアプリケーション通信の場合には，より高速なハンドオフが要求されるため，このハンドオフ時間が問題となることがある．そこで，プロキシ MOBIKE を拡張し，コンテキスト転送の概念を適用した方式を提案する．本論文におけるコンテキスト転送は，IPSec などのリンク設定情報をハンドオフ前のフェムトセルからハンドオフ後のフェムトセルへ転送する機能と定義する．また，そのコンテキスト転送に用いられる，フェムトセル上の IPSec のセッション情報を一意に特定する識別子を IPSec セッション識別子と定義する．**図 6** にプロキシ MOBIKE コンテキスト転送方式のハンドオフ手順を示す．端末はハンドオフ後の LCP 設定要求にハンドオフ前のフェムトセルの識別子（FAP#1）および FAP#1 上に存在する当該端末用の IPSec セッション識別子を含めて送信する．FAP#2 は，この LCP 設定要求を受信すると，FAP#1 に対して IPSec セッション識別子を含めたコンテキスト転送要求を送信する．FAP#1 は IPSec セッション識別子によって特定した当該端末の IPSec セッションの情報（IP#A，IPSec 設定情報，FAP#1 の IP アドレス）を FAP#2 へ転送する．FAP#2 は FAP#1 から取得した当該端末の IPSec セッションの情報に基づいて IPSec セッションを復元し，MOBIKE による IPSec トンネルの終端変更（FAP#1 の IP アドレスから FAP#2 の IP アドレス）を FGW に通知する．FAP#2 は MOBIKE による IPSec トンネルの終端変更の処理後，端末に対して認証を不要とした LCP 設定応答を返信する．FAP#2 は端末からの IPCP 設定要求に対し，すでに FAP#1 から取得した IP#A を含めて IPCP 設定応答を返信する．よって，プロキシ MOBIKE 基本方式と同様，端末に割り当てる IP#A は変更されないため，アプリケーションの通信は継続される．なお，近隣の FAP 間は事前に IPSec を設定しておくものとし，セキュリティは十分に確保されているものとする．

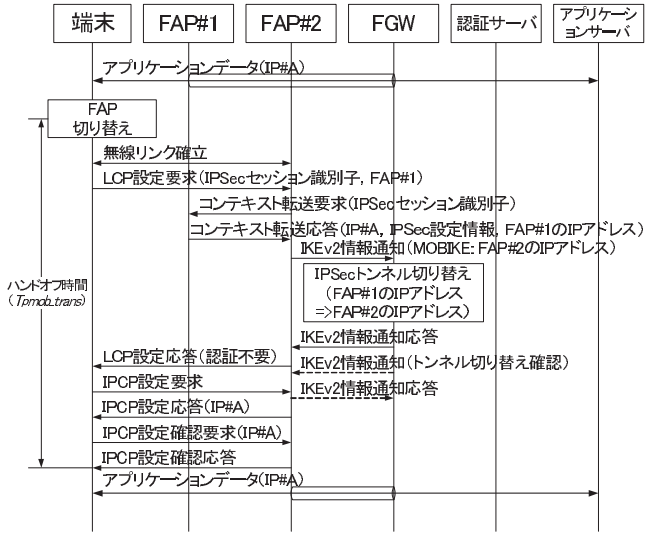

図 6　プロキシ MOBIKE コンテキスト転送方式のハンドオフ手順
Fig. 6　Handoff procedure with context transfer method of Proxy MOBIKE.

ここで，プロキシ MOBIKE コンテキスト転送方式の場合のハンドオフ時間 T_{pmob_trans} は，FAP 間のメッセージ転送時間を T_4 とすると次の式で表される．

$$T_{pmob\_tran} = T_w + 6T_1 + 2T_2 + 2T_4 \quad (2)$$

よって，プロキシ MOBIKE 基本方式とプロキシ MOBIKE コンテキスト転送方式のハンドオフ時間の差 T_{diff1} は，次の式で表される．

$$T_{diff1} = (1) - (2) = 5T_1 + 6T_2 + 2T_3 + 2T_4 \quad (3)$$

式 (3) において，インターネット上の転送時間（T_2）や認証サーバと FGW 間の認証メッセージ送受信に要する時間（T_3）が大きくなるほど，FAP 間のメッセージ送受信に要する時間（T_4）の影響は小さくなり，コンテキスト転送方式によるハンドオフ時間の短縮効果も大きくなる．このように，コンテキスト転送方式では，IPSec のセッション情報をハンドオフ前後の FAP で引き継ぎ，MOBIKE を実行することにより，認証処理や IPSec の再確立処理が不要となり，プロキシ MOBIKE 基本方式に比べ，高速なハンドオフが実現できる．

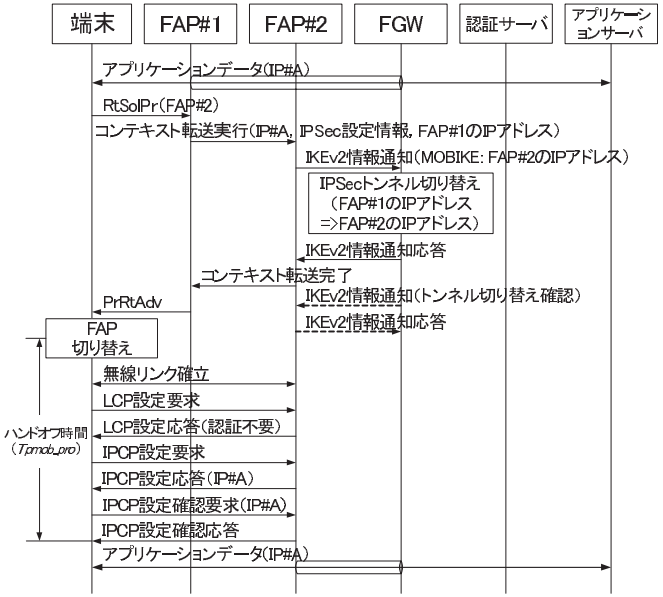

図 7　プロアクティブ型のプロキシ MOBIKE コンテキスト転送方式のハンドオフ手順
Fig. 7　Proactive handoff procedure with context transfer method of Proxy MOBIKE.

次に，さらなるハンドオフ高速化のため，端末が FAP を切り替える前にハンドオフ先の FAP が検知可能な無線方式に適用可能なプロアクティブ型のプロキシ MOBIKE コンテキスト転送方式を提案する．なお，図 6 に提案したコンテキスト転送方式は，FAP を切り替えた後にハンドオフ先の FAP を検知するため，リアクティブ型のプロキシ MOBIKE コンテキスト転送方式とする．**図 7** にプロアクティブ型のプロキシ MOBIKE コンテキスト転送方式のハンドオフ手順を示す．プロアクティブ型のプロキシ MOBIKE コンテキスト転送方式の場合，前提条件として FAP#1 には近隣ノードのリストとして FAP#2 の識別子および IP アドレスが設定されているものとする．端末はハンドオフの実行の必要性を検知すると，接続している FAP#1 に対し，FMIPv4 [16] に規定されている RtSolPr（Router Solicitation for Proxy Advertisement）メッセージを送信する．FAP#1 は当該端末の IPSec セッションの情報を FAP#2 へ転送する．FAP#2 はリアクティブ型のコンテキスト転送方式と同様，IPSec セッションの復元および MOBIKE による IPSec トンネルの終端変更の処理後，FAP#1 へコンテキスト転送応答を返信する．FAP#1 は RtSolPr に対して PrRtAdv（Proxy Router Advertisement）メッセージを返信する．端末は PrRtAdv を受信すると FAP を切り替え，無線リンクの確立と PPP 交渉処理を行う．このように，端末の FAP 切替え前に FAP 間のコンテキスト転送が完了し，PrRtAdv メッセージが通知される状況では，FAP 間のメッセージ送受信に要する時間（T_4）がハンドオフ時間に影響せず，省略することが可能である．また，プロアクティブ型のコンテキスト転送方式は，リアクティブ型のコンテキスト転送方式とは異なり，IKEv2 の交渉メッセージがハンドオフ時間に影響しない．なお，プロアクティブ型の場合もリアクティブ型のコンテキスト転送方式と同様，端末に割り当てる IP#A は変更されないため，アプリケーションの通信は継続される．

ここで，プロアクティブ型のプロキシ MOBIKE コンテキスト転送方式の場合のハンドオフ時間 T_{pmobi_pro} は，次の式で表される．

$$T_{pmob\_pro} = T_w + 6T_1 \tag{4}$$

よって，基本方式およびリアクティブ型のコンテキスト転送方式に対する，プロアクティブ型のコンテキスト転送方式のハンドオフ時間の差をそれぞれ T_{diff2}，T_{diff3} とすると次の式で表される．

$$T_{diff2} = (1) - (4) = 5T_1 + 8T_2 + 2T_3 \tag{5}$$

$$T_{diff3} = (2) - (4) = 2T_2 + 2T_4 \tag{6}$$

式 (5) および式 (6) より，式 (3) と同様，インターネット上の転送時間（T_2）が大きくなるほど，プロアクティブ型のコンテキスト転送方式によるハンドオフ時間の短縮効果も大きくなる．特に基本方式との差（T_{diff2}）はリアクティブ型のコンテキスト転送方式との差（T_{diff3}）に比べて急速に大きくなる．

4. 評価実験と考察

4.1 実 装 機 能

3 章に提案したプロキシ MOBIKE の実装評価を行うため，端末，FAP，FGW および認証サーバを Linux ベースの PC で実装した．実験システムでは FAP を模擬するため，PC に無線 LAN アクセスポイントを接続したものを仮想 FAP として動作させた．端末と FAP 間には，PPPoE（Point-to-Point Protocol over Ethernet）を用いることで，cdma2000 HRPD システムをエミュレーションし，FAP の IKEv2 の実装には，Racoon2 [17] をベースに PPPoE との連携機能，MOBIKE 機能およびハンドオフ時のコンテキスト転送機能を実装した．

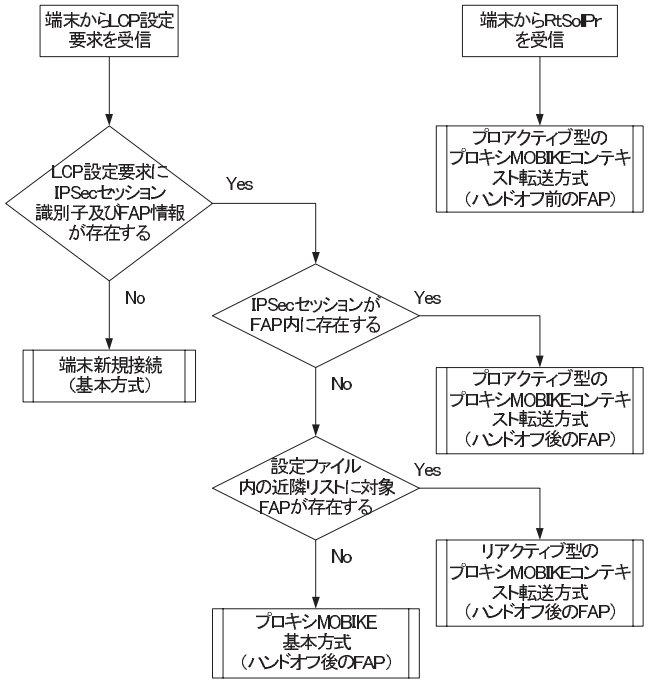

図 8　FAP のハンドオフ方式判定
Fig. 8　Decision algorithm of handoff method on FAP.

FAP 間のコンテキスト転送メッセージには FMIPv4 に規定されている FBU（Fast Binding Update）および FBA（Fast Binding Acknowledgement）メッセージのフォーマットを用い，必要となるパラメータをオプションフィールドに規定した．FGW では strongSwan [18] をベースに認証サーバとの連携機能やプロキシ MOBIKE 基本方式におけるハンドオフ後の同一 IP アドレス割当て機能を実装した．なお，認証サーバには FreeRADIUS [19] を用いた．

また，端末にはハンドオフ動作モードとして，リアクティブモードとプロアクティブモードを実装し，プロアクティブモードの場合には，ハンドオフの際にハンドオフ後の FAP 情報を入力することにより，ハンドオフ前にハンドオフ後の FAP 情報を提供できるように実装した．なお，FAP では，**図 8** のとおり，端末から受信したメッセージと各状態に応じてハンドオフ方式を識別する仕組みを実装した．

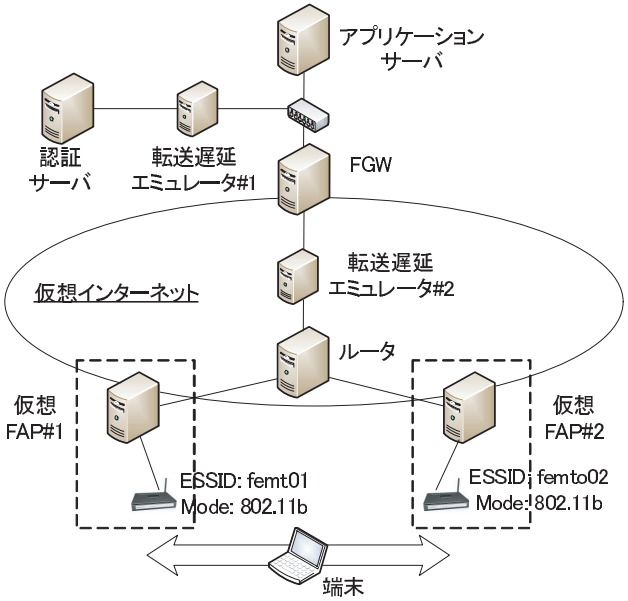

図 9　プロキシ MOBIKE の実験システム
Fig. 9　Experimental system for Proxy MOBIKE.

4.2　ハンドオフ実験

図 9 に示す実験システムを構築し，各方式におけるプロキシ MOBIKE のハンドオフ時間の測定を行った．**表 1** に各装置の諸元を示す．端末における仮想 FAP のアクセスポイント切替えは，Linux の iwconfig コマンドによる手動切替えとし，PPPoE の開始メッセージであり，無線リンク確立後の最初のメッセージである端末からの PADI（PPPoE Active Discovery Initiation）送出時間から IPCP 設定確認応答メッセージ受信時間までをハンドオフ時間とした．無線の切替え時間（T_w）については，各方式で共通であることや電波状況によってネットワーク間のハンドオフ時間へ影響を及ぼすことなどから測定範囲からは除外することとした．なお，ハンドオフ実行中，端末はアプリケーションサーバから継続的に UDP データを受信する．

最初に，FGW と認証サーバ間の転送遅延や認証サーバの応答遅延（T_3）を模擬するため，図 9 に示した転送遅延エミュレータ#1 を稼働させ，その遅延が各方式のハンドオフ時

表 1　実験装置の仕様
Table 1　Specification of components.

装置 / スペック	端末	FAP, FGW, 認証サーバ, アプリケーションサーバ, ルータ, 転送遅延エミュレータ	アクセスポイント
OS	Fedora Core 6	Fedora Core 7 (転送遅延エミュレータ: Fedora Core 4)	Corega WLAPGMN
CPU	Intel Core 2/ 2.10 GHz	Intel Core 2/ 2.13 GHz	
メモリ	2 GB	2 GB	
ネットワークアダプタ	MELCO WLI-PCM-L11 (Mode: 802.11b)	Intel PRO/1000MT	

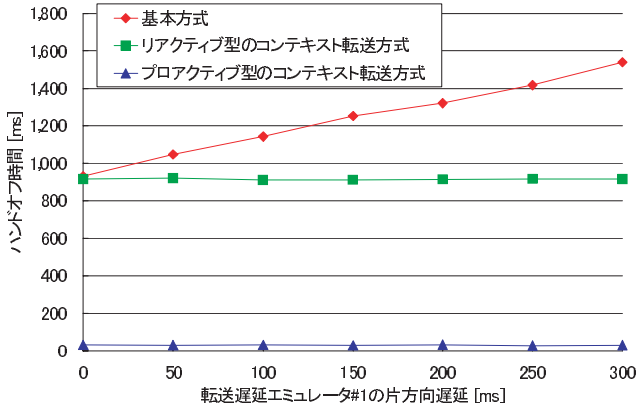

図 10　認証サーバの応答遅延の影響
Fig. 10　Handoff time along with response delay from authentication server.

間に及ぼす影響を調べた．測定は，双方向に遅延を加え，片方向遅延を 50 ミリ秒間隔で 0 から 300 ミリ秒まで増加させた．各ハンドオフ方式においてそれぞれ 5 回実施した測定結果の平均値を**図 10** に示す．図 10 より，プロキシ MOBIKE のハンドオフ時間の平均値が，転送遅延エミュレータ#1 の片方向遅延が 0 の場合，基本方式では 932 ミリ秒，リアクティブ型のコンテキスト転送方式では 916 ミリ秒，プロアクティブ型のコンテキスト転送方式では 30 ミリ秒であった．また，転送遅延エミュレータ#1 の片方向遅延が 100 ミリ秒の場合，基本方式では 1,144 ミリ秒，リアクティブ型のコンテキスト転送方式では 911 ミリ秒，プロアクティブ型のコンテキスト転送方式では 31 ミリ秒であり，片方向遅延が 300 ミリ秒の場合，基本方式では 1,540 ミリ秒，リアクティブ型のコンテキスト転送方式では 916 ミリ秒，プロアクティブ型のコンテキスト転送方式では 30 ミリ秒であった．測定結果において片方向遅延が 0 の場合，プロアクティブ型のコンテキスト転送方式が最も高速にハンドオフを実行可能であったものの，リアクティブ型のコンテキスト転送方式では，基本方式とほぼ同等であった．これは，式 (3) において，FGW と認証サーバ間の転送遅延や認証サーバの応答遅延，インターネット上の遅延が小さい場合には，コンテキスト転送方式における IPSec のセッション情報の抽出および転送に要する時間が無視できず，基本方式の IPSec 確立時間と PPP 確立における認証メッセージの送受信に要する時間を加えた値とほぼ同じであることを示している．また，FGW と認証サーバ間のパケット転送遅延や認証サーバの応答遅延が大きくなるにつれ，基本方式に比べてコンテキスト転送方式の方がより高速にハンドオフを実現できることが確認された．なお，前述のとおり，無線の切替え時間（T_w）については，各方式で共通のパラメータであるためハンドオフ時間の結果に含まれていないものの，この値が小さいほど，プロアクティブ型のコンテキスト転送方式による，無線も含めたハンドオフ時間の短縮効果が大きくなる．

次に，転送遅延エミュレータ#1 の遅延を 0 とし，図 9 に示した転送遅延エミュレータ#2 を稼働させ，インターネットの転送遅延（T_2）が各方式のハンドオフ時間に及ぼす影響を調べた．測定は，双方向に遅延を加え，片方向遅延を 50 ミリ秒間隔で 0 から 300 ミリ秒まで増加させた．それぞれ 5 回実施した測定結果の平均値を**図 11** に示す．

図 11 に示したとおり，プロキシ MOBIKE のハンドオフ時間の平均値が，転送遅延エミュレータ#2 の片方向遅延が 100 ミリ秒の場合，基本方式では 1,758 ミリ秒，リアクティブ型のコンテキスト転送方式では 1,067 ミリ秒，プロアクティブ型のコンテキスト転送方式では 29 ミリ秒であった．また，片方向遅延が 300 ミリ秒の場合，基本方式では 3,305 ミリ秒，リアクティブ型のコンテキスト転送方式では 1,512 ミリ秒，プロアクティブ型のコンテキスト転送方式では 31 ミリ秒であった．この結果は，基本方式では，インターネットを通過する IKEv2 交渉メッセージの転送遅延がハンドオフ時間に大きく影響を及ぼしているが，コンテキスト転送方式では影響を受けにくいことを示している．特にプロアクティブ型のコンテキスト転送方式では，転送遅延の影響を受けないことが確認された．

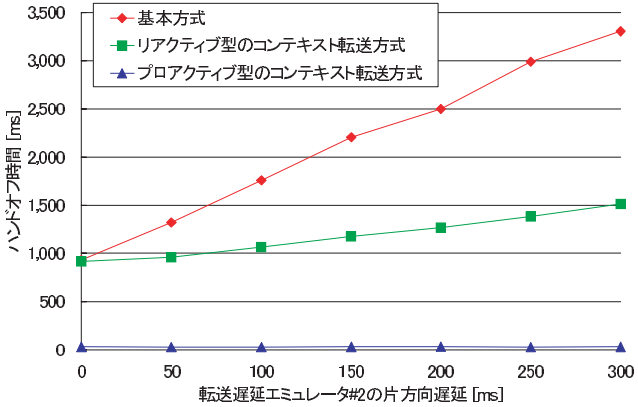

図 11　インターネットにおける転送遅延の影響
Fig. 11　Handoff time along with transit delay in the Internet.

4.3　評価結果からの考察

3GPP（Third Generation Partnership Project）の次世代移動体システムである EPS（Evolved Packet System）の要求条件文書[20] では，ハンドオフにともなうリアルタイムアプリケーションの通信断時間は 300 ミリ秒以内と規定されている．よって，4.2 節に示したハンドオフ実験結果より，VoIP やテレビ電話などのリアルタイムアプリケーションでは，インターネットの転送遅延の影響を受けずに高速なハンドオフが実現可能なプロアクティブ型のプロキシ MOBIKE コンテキスト転送方式が実用的である．また，ファイル転送などの非リアルタイムアプリケーションの場合には，再認証処理を行わず，かつインターネットの転送遅延の影響も低減させながらハンドオフを実現可能なリアクティブ型のコンテキスト転送方式でも実用化が可能といえる．プロキシ MOBIKE 基本方式の場合，接続ユーザ数が少なく，インターネットの転送遅延もほぼ無視できる場合には，リアクティブ型のコンテキスト転送方式と同様に非リアルタイムアプリケーションのハンドオフ方式として実用的であるといえる．

4.4　既存の移動管理方式との比較

本節では，提案方式であるプロキシ MOBIKE と，2.2 節において既存の移動管理方式として示したプロキシモバイル IP を利用した場合のハンドオフ時間の比較を行う．**図 12** にプロキシモバイル IP によるハンドオフ処理手順を示す．なお，厳密なセキュリティ管理のため，FAP と FGW 間の IPSec はプロキシ MOBIKE と同様に端末ごとに確立するものとする．端末は，FAP 切替え後，FAP#2 との無線リンク確立に続き，PPP リンクの設定を行う．FAP#2 はプロキシ MOBIKE 基本方式と同様の手順により，FGW と IPSec を確立するが，端末に割り当てる IP アドレスはプロキシモバイル IP 登録手順により，LMA から取得する．端末は，FAP#2 から IPCP 設定応答で取得した，ハンドオフ前の IP アドレスと同様の IP#A を用いて，アプリケーションデータの通信を継続する．なお，アプリケーションデータは LMA を経由して送受信される．

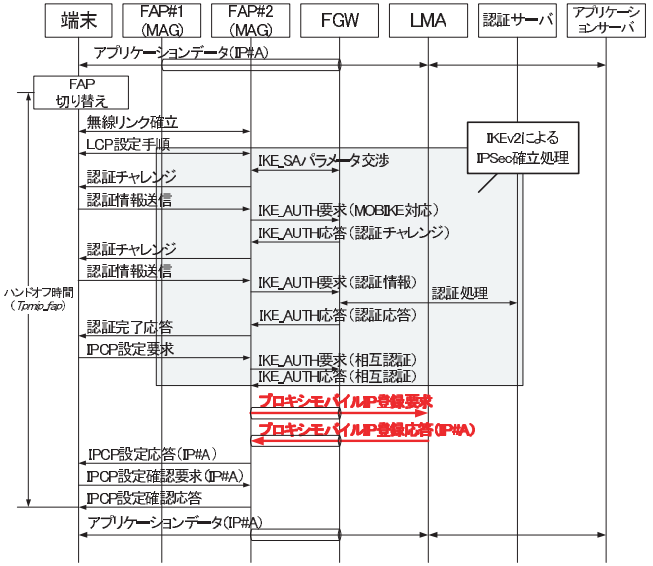

図 12　プロキシモバイル IP のハンドオフ手順
Fig. 12　Handoff procedure using Proxy Mobile IP.

ここで，FGW と LMA 間のメッセージ転送時間を T5 とするとプロキシモバイル IP を利用した場合のハンドオフ時間 T_{pmip_fap} は，次の式で表される．

$$T_{pmip\_fap} = T_w + 11T_1 + 10T_2 + 2T_3 + 2T_5 \quad (7)$$

よって，プロキシモバイル IP に対する，プロキシ MOBIKE 基本方式，リアクティブ型のコンテキスト転送方式，プロアクティブ型のコンテキスト転送方式のハンドオフ時間の差 T_{diff4}，T_{diff5}，T_{diff6} はそれぞれ次の式で表される．

表 2　プロキシモバイル IP との比較
Table 2　Comparison with Proxy Mobile IP.

移動管理方式＼比較項目		近隣FAPリストの管理	FGWの負荷	追加設備	アプリケーションデータの経路	ハンドオフ時間
プロキシMOBIKE	プロキシMOBIKE基本方式	○ 近隣FAPリストの管理が不要	× 端末移動時のIPSec再確立処理，移動管理が必要	○ なし	○ LMA不要のため冗長経路は軽減	× インターネットの転送遅延の影響を大きく受ける
	リアクティブ型コンテキスト転送方式	× 近隣FAPリストの管理が必要	△ 移動管理が必要	○ なし	○ LMA不要のため冗長経路は軽減	△ インターネットの転送遅延の影響をさほど受けない
	プロアクティブ型コンテキスト転送方式	× 近隣FAPリストの管理が必要	△ 移動管理が必要	○ なし	○ LMA不要のため冗長経路は軽減	○ インターネットの転送遅延の影響を全く受けない
プロキシモバイルIP（既存方式）		○ 近隣FAPリストの管理が不要	△ 端末移動時のIPSec再確立処理が必要	× LMAが必要	△ LMA経由による冗長経路の可能性	× インターネットの転送遅延の影響を大きく受ける

$$T_{diff4} = (7) - (1) = 2T_2 + 2T_5 \tag{8}$$
$$T_{diff5} = (7) - (2) = 5T_1 + 8T_2 + 2T_3 + 2T_5 - 2T_4 \tag{9}$$
$$T_{diff6} = (7) - (4) = 5T_1 + 10T_2 + 2T_3 + 2T_5 \tag{10}$$

式 (8) より，プロキシ MOBIKE 基本方式では，インターネット上の転送時間（T_2）や FGW と LMA 間のメッセージ転送時間（T_5）が大きくなると，プロキシモバイル IP に比べてハンドオフ時間が短くなる．また，式 (9) より，リアクティブ型のプロキシ MOBIKE コンテキスト転送方式では，FAP 間のメッセージ送受信に要する時間（T_4）が小さいほど，プロキシモバイル IP に比べてより高速にハンドオフを行うことができる．プロアクティブ型のプロキシ MOBIKE コンテキスト転送方式では，式 (10) よりプロキシモバイル IP とのハンドオフ時間の差がさらに大きく，最も高速にハンドオフを行うことができる．

次に，プロキシ MOBIKE の各方式と既存方式であるプロキシモバイル IP を利用した場合の総合的な比較を行う．**表 2** に FAP での近隣 FAP リストの管理，FGW の負荷，追加設備，アプリケーションデータの経路およびハンドオフ時間に関する比較を示す．プロキシ MOBIKE コンテキスト転送方式では，高速なハンドオフを実現するために，FAP において近隣 FAP リストを保持する機能が必要となる．一方，LMA などの移動管理プロトコル専用のノードが不要なこと，またそれを経由することによる経路の冗長化が回避可能なこと，そしてコンテキスト転送を FAP 切替え前に完了させることで実効的なハンドオフ時間が短縮されることなどの効果が得られる．

5. おわりに

本論文では，フェムトセルを含む移動体ネットワークにおいて，フェムトセル上の実装プロトコル数をより低減することが可能なプロキシ MOBIKE 基本方式を提案した．また，IPSec のセッション情報をフェムトセル間で転送することにより，より高速なハンドオフを実現するプロキシ MOBIKE コンテキスト転送方式についても提案し，実験による各方式のハンドオフ時間の比較を行った．その結果，プロキシ MOBIKE 基本方式に比べ，リアクティブ型のコンテキスト転送方式やプロアクティブ型のコンテキスト転送方式の方が，認証応答の遅延やインターネットの転送遅延の影響を受けにくく，高速にハンドオフが可能であった．特に，プロアクティブ型のプロキシ MOBIKE コンテキスト転送方式は，インターネットの転送遅延の影響を受けず，最も高速にハンドオフが可能であることが示された．

謝辞　日ごろご指導いただく KDDI 研究所秋葉所長，鈴木執行役員に，謹んで感謝の意を表する．本研究の一部は，情報通信研究機構からの委託研究「新世代ネットワークの構築に関する設計・評価手法の研究開発」に基づき実施されたものである．

参考文献

1) 3GPP: IP Multimedia Subsystem (IMS); stage 2 (Release 8), TS23.228 v8.5.0 (2008).
2) 3GPP2: All-IP Core Network Multimedia Domain: IP Multimedia (IMS) Session Handling; IP Multimedia (IM) Call Model - Stage 2, X.S0013-003-B v1.0 (2007).
3) Rosenberg, J., Schulzrinne, H., Camarillo, G., et al.: SIP: Session Initiation Protocol, IETF RFC 3261 (2002).
4) Femto Forum. http://www.femtoforum.org/
5) Chandrasekhar, V., Andrews, J. and Gatherer, A.: Femtocell Networks: A Survey, *IEEE Communication Magazine*, pp.59–67 (Sep. 2008).
6) 3GPP2: cdma2000 Packet Data Service: Wireless Local Area Network (WLAN) Interworking – Access to Operator Service and Mobility for WLAN Interworking, X.S0028-200-A v1.0 (June 2008).
7) Perkins, C.: IP Mobility Support for IPv4, IETF RFC 3344 (2002).
8) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support in IPv6, IETF RFC 3775 (2004).
9) Eronen, P.: IKEv2 Mobility and Multihoming Protocol (MOBIKE), IETF RFC 4555 (2006).
10) Leung, K., Dommety, G., Yegani, P., et al.: WiMAX Forum/3GPP2 Proxy Mobile

IPv4, IETF draft-leung-mip4-proxy-mode-09, work in progress (2008).
11) Gundavelli, S., Leung, K., Devarapalli, V., et al.: Proxy Mobile IPv6, IETF RFC 5213 (2008).
12) Kaufman, C.: IKEv2 Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306 (2005).
13) 3GPP2: Femto Network Overview and List of Parts (X.P0059-000-0), work in progress, X50-20080721-015r2 (2008).
14) Simpson, W.: The Point-to-Point Protocol (PPP), IETF RFC 1661 (1994).
15) Rigney, C., Willens, S., Rubens, A., et al.: Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865 (2000).
16) Koodi, R., Perkins, C.: Mobile IPv4 Fast Handovers, IETF RFC 4988 (2007).
17) Racoon2. http://www.racoon2.wide.ad.jp/w/
18) strongSwan. http://www.strongswan.org/
19) FreeRADIUS. http://freeradius.org/
20) 3GPP: Service requirements for the Evolved Packet System (EPS) (Release 9), TS22.278 v9.3.0 (2009).

(平成 21 年 4 月 7 日受付)
(平成 21 年 10 月 2 日採録)

千葉　恒彦（正会員）

平成 12 年北海道大学工学部電子工学科卒業．同年第二電電株式会社（現 KDDI 株式会社）入社．現在，株式会社 KDDI 研究所モバイルネットワークグループ研究主査．モビリティや IMS，コアネットワークアーキテクチャを中心としたモバイルネットワークの研究および標準化活動に従事．平成 20 年電子情報通信学会学術奨励賞受賞．電子情報通信学会会員．

小森田賢史

平成 16 年東京大学工学部電子工学科卒業．平成 18 年同大学院情報理工学系研究科電子情報工学専攻修士課程修了．同年 KDDI 株式会社入社．現在，株式会社 KDDI 研究所モバイルネットワークグループ研究員．SIP，IMS の高度化技術の研究に従事．電子情報通信学会会員．

横田　英俊（正会員）

平成 2 年早稲田大学理工学部電子通信学科卒業．平成 4 年同大学院修士課程修了．同年国際電信電話株式会社（現，KDDI 株式会社）入社．平成 7〜8 年米国スタンフォード研究所客員研究員．現在，株式会社 KDDI 研究所モバイルネットワークグループリーダー．博士（国際情報通信学）．コンピュータネットワーク，インターネット QoS，モバイルネットワークの研究・標準化に従事．平成 10 年電子情報通信学会学術奨励賞受賞，平成 17 年情報処理学会山下記念研究賞受賞，平成 18 年情報処理学会論文賞受賞，電子情報通信学会，IEEE 各会員．