

フェムトセルを用いた メディアデータの経路最適化手法の提案と評価

千葉 恒彦^{†1} 横田 英俊^{†1}

近年、携帯電話などの移動体ネットワークにおいて、数十メートル程度のごく小さいエリアをカバーするフェムトセルが注目されている。フェムトセルをブロードバンドアクセス回線やインターネットなどの公衆網に接続する場合、通信の暗号化のためにフェムトセルと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との間に IPSec トンネルを確立してメディアデータを送受信する。このため、フェムトセルどうしが近距離に配置されていた場合、セキュリティゲートウェイとフェムトセル間の距離が大きくなるとメディアデータの経路が冗長となる問題がある。また、メディアデータの暗号化処理にともなうセキュリティゲートウェイの処理負荷増大も懸念される。本論文では、オール IP ネットワークの呼制御基盤である IMS の情報を利用し、セキュリティゲートウェイを介さずにフェムトセル間でメディアデータの送受信を行うことにより、その経路を最適化する方式を提案するとともに、実機フェムトセルを用いてその有効性を検証する。

Proposal and Evaluation of Media Path Optimization Using Femtocell

TSUNEHICO CHIBA^{†1} and HIDETOSHI YOKOTA^{†1}

Recently, a femtocell, which covers several tens of meters cell area, is attracting higher attention in mobile communications. When a femtocell is connected to the public network such as broadband access network or the Internet, media data is sent and received over IPSec tunnel between the femtocell and the security gateway located in the mobile core network for data encryption. Therefore, if the security gateway is far away from femtocells, and if those femtocells are nearby each other, the routing path for media data between users becomes redundant. Moreover, the intensive processing due to encryption and decryption for media data may impact on the load of the security gateway. In this paper, we propose efficient media path optimization mechanisms by sending and receiving media data directly between femtocells in coordination with IMS (IP Multimedia Subsystem), which is expected as a core technology for the ses-

sion control in all-IP network, and evaluate the proposed mechanisms using a commercial femtocell.

1. はじめに

近年、オール IP ベースのモバイルネットワークを構成する要素として、SIP (Session Initiation Protocol)¹⁾を用いたセッション制御基盤の IMS (IP Multimedia Subsystem)²⁾や携帯電話の小型基地局であるフェムトセルが注目されている³⁾。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、少数ユーザで占有的に無線帯域を利用することによる通信容量の増加、および一般のブロードバンドアクセス回線を介して移動体通信事業者のコアネットワークへ接続することによる広域無線アクセスネットワークの負荷軽減などもあげられる⁴⁾。ここで、フェムトセルをコアネットワークへ接続する場合、通信データはブロードバンドアクセス回線やインターネットなどの非セキュア網を介する。よって、標準方式では、フェムトセルはセキュリティ確保のためコアネットワークに配置されたセキュリティゲートウェイである FGW (Femto Gateway) との間で IPSec トンネルを確立し、通信の暗号化を行う。しかしながら、標準方式においてフェムトセルに接続した端末が音声通信などを行う場合、SIP メッセージだけでなく、アプリケーションのメディアデータについても FGW を経由するため、フェムトセルと FGW 間の距離が大きくなるとメディアデータの転送遅延も増加し、通信品質を劣化させてしまう可能性がある。また、FGW でメディアデータの packets 暗号化および復号化処理を対向フェムトセルごとに実施する必要があるため、FGW の負荷増大や処理遅延も問題となる。m2m-x⁵⁾などのように、SIP プロトコルの特徴を生かし、端末が取得した IP アドレスをメディアデータ送受信用として対向端末へ通知することで、中継サーバなどを介さずにメディアデータの送受信を行うことが可能となるが、規定のフェムトセルを利用する状況では、やはりメディアデータが FGW を経由することになる。本論文では、まず音声通信において、フェムトセルを介した標準方式のコアネットワークへの接続形態とその問題点について説明する。次に、IMS とフェムトセルで連携し、フェムトセル自身の IP アドレスと FGW から割り当てられ

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

る移動端末用の IP アドレスを使い分け, SIP メッセージは FGW を介してコアネットワークへ転送しながら, メディアデータについては FGW を経由せずにフェムトセル間で送受信を行うメディアデータの経路最適化方式を提案し, 実装評価によりその有効性を検証する.

2. フェムトセルの接続形態

図 1 に cdma2000 1X⁶⁾ を具備したフェムトセルの標準文書に規定されているコアネットワーク接続形態を示す⁷⁾. 本構成では, ブロードバンドアクセス回線やインターネットなどの非セキュア網を想定している. よって, 通信の暗号化のため, フェムトセルと FGW の間で IKEv2 (Internet Key Exchange version 2)⁸⁾ 手順に基づく IPSec トンネルを確立する. フェムトセルをコアネットワークへ接続する形態として図 1 に示すとおり, 2 形態考えられる. 1 つは広域の無線アクセスネットワークに接続される形態であり, もう 1 つは IP レイヤをフェムトセルで終端し, コアネットワークに直接接続されるオール IP の接続形態である. 本論文では広域無線アクセスネットワークの負荷をより低減させることができるオール IP 接続型について述べる. フェムトセルを用いた通信では, マクロセル利用時と同程度のセキュリティを確保することを前提として標準文書が策定されている. このため, 標準方式のフェムトセルの場合, 通信事業者がセキュリティを確保できるコアネットワークに FGW を設置し, SIP メッセージやメディアデータを含め, すべての通信をフェムトセルと FGW 間に確立した IPSec トンネルを介して行うことで全通信路のセキュリティを確保している. 音声のセッション確立には IMS が用いられ, SIP メッセージは SIP サーバである P-CSCF (Proxy-Call Session Control Function) および I-CSCF (Interrogating-Call Session Control Function) を経由し, S-CSCF (Serving-Call Session Control Function) へ登録が行われる. ここで, SIP に対応していない端末を収容するため, フェムトセルが端末の代わりに SIP メッセージを制御する.

図 2 に標準方式のセッション確立手順を示す. フェムトセル#1 およびフェムトセル#2 は, ネットワークに接続されると, DHCP などにより FGW と通信可能な IP アドレスである IP#1 および IP#2 をそれぞれ取得し, IKEv2 手順によるフェムトセルの認証の後, FGW との間に IPSec トンネルを確立する. この IKEv2 手順の中で, フェムトセル#1 は P-CSCF との通信のために TIA (Tunnel Inner Address) である IP#A を取得する. その後, 端末#1 がフェムトセル#1 に接続されると, 端末#1 とフェムトセル#1 との間に cdma2000 1X 手順による無線リンクが確立される. この無線リンク確立手順の中でフェムトセル#1 は端末#1 から, その識別子 (AT#1) を取得する. 引き続き, フェムトセル#1 は FGW との

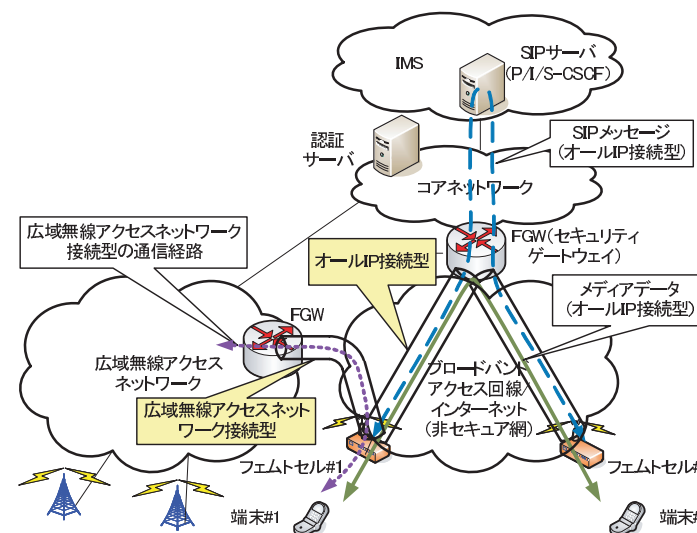


図 1 標準方式の接続形態

Fig. 1 Standard architecture for femtocell.

IPSec トンネルを経由し, P-CSCF に対して SIP REGISTER を送信することにより, 端末#1 (AT#1) を IMS へ登録する. 同様に端末#2 がフェムトセル#2 へ接続されると, IP#2 と IP#B の取得および IMS への登録が行われる. 次に, 端末#1 が端末#2 へ音声通信のために発信を行うと, フェムトセル#1 はその発信信号を SIP INVITE へ変換し, P-CSCF へ送信する. この SIP INVITE の SDP (Session Description Protocol)⁹⁾ フィールドには, フェムトセル#2 とのメディアデータの送受信に用いる IP アドレス (IP#A) と任意に設定したポート番号 (Port#A) が含まれる. P-CSCF から SIP INVITE を受け取った S-CSCF は端末#2 (AT#2) の登録情報を特定し, 接続されているフェムトセル#2 に対して P-CSCF 経由で SIP INVITE を転送する. フェムトセル#2 は着信を端末#2 へ通知するとともに, 端末#2 を呼び出し中である状況を伝えるために 180 Ringing を P-CSCF および S-CSCF 経由でフェムトセル#1 に返信する. 端末#2 の応答を契機にフェムトセル#2 は, SIP INVITE に対する 200 OK を返信する. この 200 OK の SDP には, フェムトセル#2 がフェムトセル#1 とのメディアデータの送受信に用いる IP アドレス (IP#B) と任意に設定したポート番号 (Port#B) が含まれる. フェムトセル#1 は 200 OK を P-CSCF より

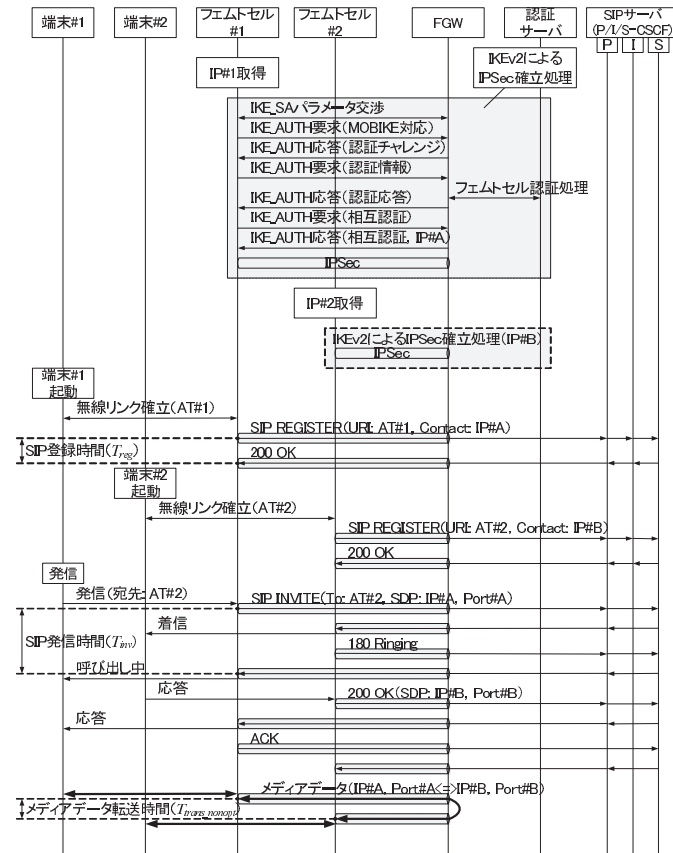


図 2 標準方式のセッション確立手順

Fig. 2 Session setup procedure of standard mechanism.

受信すると端末#2の応答を端末#1へ通知するとともにACKをP-CSCFへ送信する。この時点でセッションが確立し、端末間でそれぞれのフェムトセルを経由し、メディアデータの送受信が開始される。なお、メディアデータの送受信には、フェムトセル#1ではIP#AおよびPort#A、フェムトセル#2ではIP#BおよびPort#Bがそれぞれ用いられる。

ここで、図2に示した標準方式において、フェムトセル#1とFGW間の転送時間を T_{femto1_fgw} 、フェムトセル#2とFGW間の転送時間を T_{femto2_fgw} 、フェムトセルの

ケット暗号化および復号化処理時間をそれぞれ T_{femto_enc} および T_{femto_dec} 、FGWのケット暗号化および復号化処理時間をそれぞれ T_{fgw_enc} および T_{fgw_dec} とすると、端末#1が接続しているフェムトセル#1と端末#2が接続しているフェムトセル#2間のメディアデータ転送時間 T_{trans_nonopt} は次の式で表される。

$$T_{trans_nonopt} = T_{femto1_fgw} + T_{femto2_fgw} + T_{femto_enc} + T_{femto_dec} + T_{fgw_enc} + T_{fgw_dec} \quad (1)$$

また、セッションの確立数を N 、FGWの1セッションあたりに要するメディアデータのケット暗号化および復号化処理負荷をそれぞれ P_{fgw_enc} および P_{fgw_dec} とすると、FGW上の暗号化および復号化処理負荷 P_{fgw_sec} は次の式で表される。

$$P_{fgw_sec} = N(P_{fgw_enc} + P_{fgw_dec}) \quad (2)$$

よって、式(1)および式(2)より、フェムトセルとFGW間の距離(T_{femto1_fgw} , T_{femto2_fgw})が大きくなるとメディアデータの転送遅延も増加し、アプリケーションの品質を劣化させてしまう。また、セッションの確立数(N)が増加するとFGWにおけるケット暗号化および復号化処理(P_{fgw_sec})の負荷増大にともない、処理遅延(T_{fgw_enc} , T_{fgw_dec})が増加し、パケット損失が発生する可能性がある。ここで、SIPメッセージについては、コアネットワークの上位に接続されたIMSで処理されるため、FGWを経由してコアネットワークへ転送する必要があるが、メディアデータについては、通信路のセキュリティが確保できれば、FGWを経由せずにフェムトセル間で直接通信させることでその経路を最適化することが可能である。よって、既存の移動端末への変更を加えないという条件の下でこれらの問題を解決するため、フェムトセルにおいてSDPで指定されたメディアデータの経路を対向のフェムトセルへ切り替えて経路の最適化を図ることにより、メディアデータの転送遅延とFGWの処理負荷を低減する方式を提案する。

3. 提案方式

3.1 メディアデータの経路最適化

図3に提案方式であるメディアデータの経路最適化を実現する接続形態を示す。提案方式では、IMSとのSIPメッセージについては、コアネットワークに配置されるFGWを介して送受信されるものの、メディアデータについてはFGWを経由せずにフェムトセル間に直接送受信される。

図4に提案方式のセッション確立手順を示す。フェムトセル#1およびフェムトセル#2

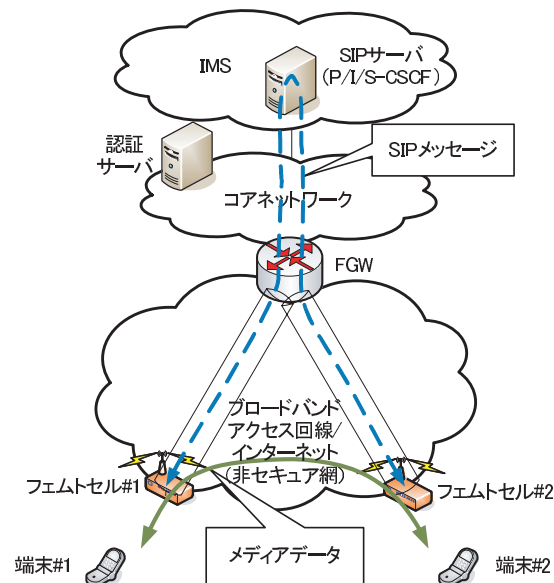


図 3 提案方式の接続形態

Fig. 3 General architecture of proposed mechanism.

は、ネットワークに接続されると、図 2 と同様の手順で FGW と通信可能な IP#1 および IP#2 の IP アドレス、P-CSCF と通信可能な IP#A および IP#B の IP アドレスをそれぞれ取得する。また、端末#1 および端末#2 の接続要求を受け、フェムトセル#1 およびフェムトセル#2 は、それぞれ FGW との IPSec トンネルを経由し、P-CSCF に対して SIP REGISTER を送信し、端末#1 (AT#1) および端末#2 (AT#2) を IMS へ登録する。次に、端末#1 が端末#2 へ音声通信のために発信を行うと、フェムトセル#1 はその発信信号を SIP INVITE へ変換し、P-CSCF へ送信する。この SIP INVITE の SDP フィールドには、FGW との通信に用いる IP#1、任意に設定した Port#1 およびメディアデータの暗号化に用いる暗号鍵 K#1 が設定される。S-CSCF は P-CSCF から SIP INVITE メッセージを受信し、端末#2 (AT#2) の登録情報を特定し、端末#2 が接続しているフェムトセル#2 に対して SIP INVITE を P-CSCF 経由で転送する。フェムトセル#2 は着信情報を端末#2 へ通知するとともに端末#2 を呼び出し中である状況を伝えるために 180 Ringing を P-CSCF および S-CSCF 経由でフェムトセル#1 に返信する。端末#2 の応答を契機にフェ

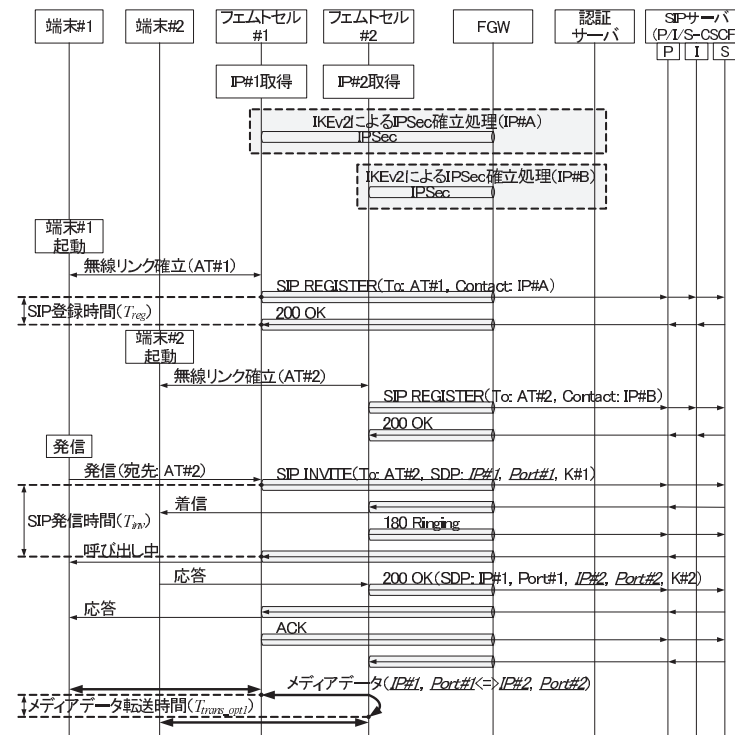


図 4 提案方式のセッション確立手順

Fig. 4 Session setup procedure of proposed mechanism.

ムトセル#2 は、SIP INVITE に対する 200 OK を P-CSCF へ返信する。この 200 OK の SDP フィールドには、FGW との通信に用いる IP#2、任意に設定した Port#2 およびメディアデータの暗号化に用いる暗号鍵 K#2 が設定される。フェムトセル#1 は 200 OK を受信すると、端末#2 の応答を端末#1 へ通知するとともに P-CSCF に対して ACK を送信する。この時点でセッションが確立され、端末間でそれぞれのフェムトセルを経由し、メディアデータの送受信が開始される。なお、メディアデータの送受信には、フェムトセル#1 は IP#1 および Port#1、フェムトセル#2 は IP#2 および Port#2 をそれぞれ用いる。よって、標準方式とは異なり、FGW を経由せずに直接フェムトセル間でメディアデータの送受信が可能となる。なお、フェムトセル間のメディアデータの暗号化には、あらかじめ IPSec

トンネルをフェムトセル間で設定しておく、もしくは SIP メッセージの SDP フィールドを用いて暗号鍵を交換したうえで SRTP (Secure Real-time Transport Protocol)¹⁰⁾ などの手法を用いる。ここで、IMS およびコアネットワークが通信事業者により管理され、通信の安全性が確保されている場合、フェムトセルと FGW 間の IPSec トンネルを利用することにより、SIP INVITE および 200 OK メッセージなどを用いて暗号鍵 (K#1, K#2) を安全に転送することができるため、暗号鍵交換のための追加メッセージが省略可能となる。

図 4 に示した提案方式において、フェムトセル#1 とフェムトセル#2 間の転送時間を T_{btw_femto} とし、フェムトセル#1 およびフェムトセル#2 のパケット暗号化および復号化処理時間が標準方式の場合と同等であるとすると、端末#1 が接続しているフェムトセル#1 と端末#2 が接続しているフェムトセル#2 間のメディアデータ転送時間 T_{trans_opt1} は次の式で表される。

$$T_{trans_opt1} = T_{btw_femto} + T_{femto_enc} + T_{femto_dec} \quad (3)$$

また、式 (1) および式 (3) より、標準方式と提案方式のメディアデータ転送時間の差分 T_{diff} は次の式で表される。

$$\begin{aligned} T_{diff} &= (1) - (3) \\ &= T_{femto1_fgw} + T_{femto2_fgw} + T_{fgw_enc} + T_{fgw_dec} - T_{btw_femto} \end{aligned} \quad (4)$$

よって、式 (4) より、フェムトセルと FGW 間の距離 (T_{femto1_fgw} , T_{femto2_fgw}) および FGW におけるメディアデータのパケット暗号化および復号化処理遅延 (T_{fgw_enc} , T_{fgw_dec}) が大きいほど、提案方式によるメディアデータの転送時間の低減効果が大きくなる。同様に、フェムトセル間の距離 (T_{btw_femto}) が小さいほど提案方式によるメディアデータの転送時間の低減効果が大きくなる。

なお、提案方式において、広域無線アクセスネットワークに接続された端末とフェムトセルに接続された端末間で通信を行う場合、図 5 のようにコアネットワークからインターネットゲートウェイを介して通信可能である。ここで、シグナリング/メディアゲートウェイはフェムトセルと同様、端末からの発信信号を SIP シグナリングへ変換するとともにメディアデータの暗号化を行う。よって、提案方式は標準方式と同等以上の適用範囲を有し、フェムトセルを介した端末間通信の状況が増加するほど、提案方式の適用範囲が広がるといえる。また、実運用において通信傍受などのためにメディアデータをコアネットワークに転送させる必要がある場合においても、対象となる音声セッションの確立処理の検知時に IMS からフェムトセルに対して標準方式による接続を再要求するなどの手法を用いることで対応

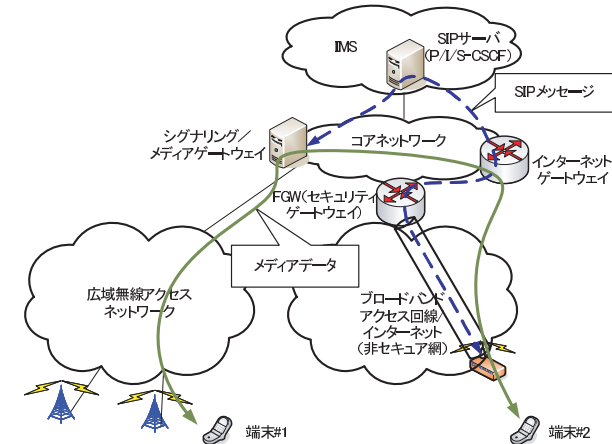


図 5 広域無線アクセスネットワークとの通信経路

Fig. 5 Communication path with radio access network.

可能である。

3.2 プライベートアドレスへの対応

一般にフェムトセルを自宅やオフィスなどに設置する場合、IP アドレスの有効利用やセキュリティの観点から、図 6 のようにプライベートアドレスの利用のため、NAT (Network Address Translation) 配下に設置される。提案方式を NAT に対応させるためには、ブロードバンドアクセス回線やインターネットとの通信に用いるグローバルアドレスおよび接続端末ごとに使用されるポート番号を取得するため、フェムトセルが STUN (Simple Traversal of UDP through NATs)¹¹⁾ もしくは UPnP (Universal Plug and Play)¹²⁾ を利用することが考えられる。UPnP は、NAT 上のアドレスマッピングを直接制御することから、セキュリティ上の課題が指摘されていること^{13)–15)}、および UPnP に対応していない NAT も対象とするため、本論文では、STUN を中心とした方式を提案する。なお、STUN を利用した場合においても、すべての形式の NAT に対応することはできないため、その適用範囲を広げるための手法として STUN を拡張した TURN (Traversal Using Relays around NAT)¹⁶⁾ や ICE (Interactive Connectivity Establishment)¹⁷⁾ などの方式が提案されている。本論文では、これら拡張方式の基本となる STUN を用いた方式で評価を行う。

図 7 に提案方式を NAT に対応させた場合のセッション確立手順を示す。フェムトセル

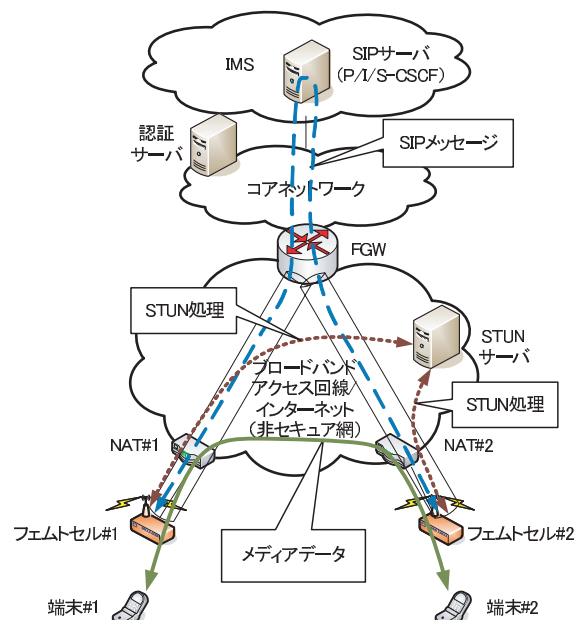


図 6 提案方式の NAT への対応
Fig. 6 General architecture of NAT support.

#1 およびフェムトセル#2 は、ネットワークに接続されると DHCP などの手順により、それぞれプライベートアドレスである PrvtIP#1 および PrvtIP#2 を取得する。続いて、FGW と IKEv2 手順に基づきフェムトセルの認証および IPSec トンネルを確立する。この手順の中で、P-CSCF との通信のためにフェムトセル#1 は TIA である IP#A、フェムトセル#2 は IP#B を取得する。ここで、フェムトセルは、FGW から割り当てられた TIA (IP#A, IP#B) が、自身の IP アドレス (PrvtIP#1, PrvtIP#2) と重複していることを検知すると、異なる TIA の割当てを FGW へ要求することで、プライベートアドレスの重複を回避する。その後、端末#1 の接続要求を受け、端末#1 のメディアデータの送受信に用いる IP アドレス (PrvtIP#1) およびポート番号 (PrvtPort#1) の NAT 変換後の IP アドレス (GlobIP#1) とポート番号 (GlobPort#1) を取得するため STUN 要求を送信し、STUN サーバよりこれらの情報を含んだ STUN 応答を受信する。その後、フェムトセル#1 は FGW との IPSec トンネルを経由し、SIP REGISTER を P-CSCF へ送信して

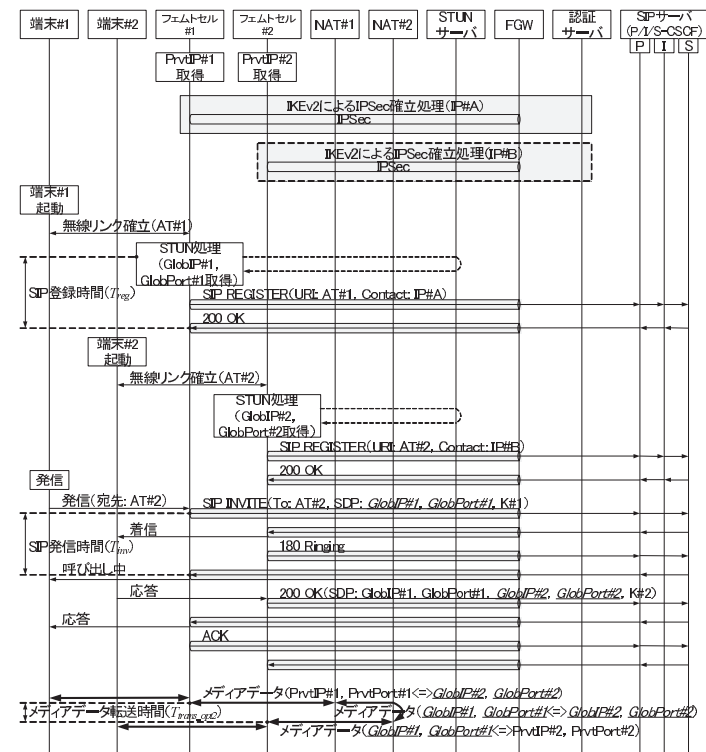


図 7 NAT 対応の提案方式のセッション確立手順
Fig. 7 Session setup procedure of NAT support.

IMS へ端末#1 (AT#1) を登録する。また、端末#1 と同様に端末#2 についてもフェムトセル#2 を介して STUN 処理および IMS への登録が実施される。次に、端末#1 が端末#2 へ音声通信のために発信を行うと、フェムトセル#1 はその発信信号を SIP INVITE へ変換し、P-CSCF へ送信する。この SIP INVITE の SDP フィールドには、STUN 処理で取得した NAT 変換後の IP アドレス (GlobIP#1) およびポート番号 (GlobPort#1) を設定する。また、同様にフェムトセル#2 からの 200 OK に含まれる SDP フィールドには、NAT 変換後の IP アドレス (GlobIP#2) および (GlobPort#2) が設定される。このように、NAT 配下に設置された場合においても、FGW を経由せずに直接フェムトセル間にて

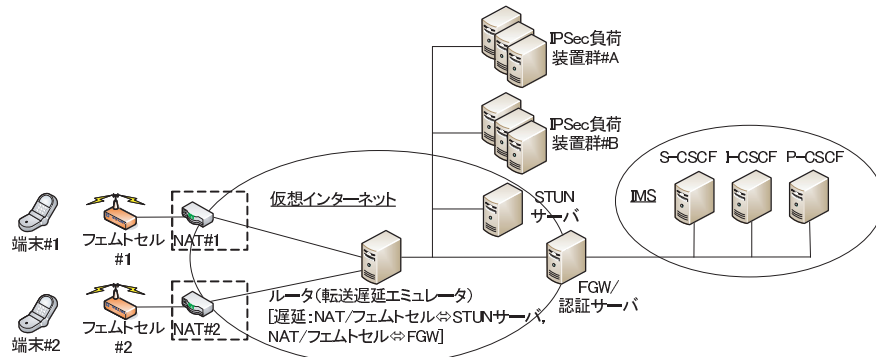


図 8 実験システムの構成
Fig. 8 Experimental system.

メディアデータを送受信することが可能となる。

図 7 に示した NAT 対応の提案方式において、NAT におけるアドレス変換処理時間を T_{nat} とすると、端末#1 が接続しているフェムトセル#1 と端末#2 が接続しているフェムトセル#2 間のメディアデータ転送時間 T_{trans_opt2} は次の式で表される。

$$T_{trans_opt2} = T_{btw_femto} + T_{femto_enc} + T_{femto_dec} + 2T_{nat} \quad (5)$$

4. 実装評価

4.1 実験システム

3 章に述べた提案方式の有効性を検証するため、メディアデータの経路最適化機能を実装した Airvana 製の cdma2000 1X フェムトセルを用いて、図 8 に示す実験システムを構築した。実験システムの仕様を表 1 に、使用したフェムトセルおよび携帯電話の外観を図 9 に示す。実運用上は数千万規模のユーザ数を収容する必要があるため、複数台の FGW で分散処理を行ったとしても 1 台あたりで処理する必要があるユーザ数は数十万から数百万と想定される。表 1 の諸元に関して、IPSec 負荷装置については被験システムに十分な負荷をかけられるよう Intel Core 2 を用いたが、模擬可能な音声セッション確立数が後述のとおり最大 1,200 程度であったため、被験システムについては負荷に対する性能の見極めが可能なよう Intel Pentium IV を選定した。また、音声のコーデックには EVRC (Enhanced Variable Rate Codec)¹⁸⁾ を用い、平均 UDP パケット長 22 バイト、パケットの送信間隔は 20 ミリ秒とした。ネットワークは IPv4 で構築し、端末とフェムトセル間は高周波ケーブルで接

表 1 実験システムの仕様

Table 1 Specification of components.

装置 スペック	FGW, P/I/S-CSCF, ルータ, STUNサーバ	IPSec負荷装置	端末	フェムトセル	NAT
OS	Fedora Core 6 (ルータ: Fedora Core 4)	Fedora Core 7	SANYO au E02SA	Airvana cdma2000 v.2.0.1.55	IO-DATA NP-BBRM
CPU	Intel Pentium IV/ 2.8 GHz	Intel Core 2/ 2.13 GHz			
メモリ	2 GB	2 GB			
ネットワーク アダプタ	Intel PRO/1000MT	Intel PRO/1000MT			

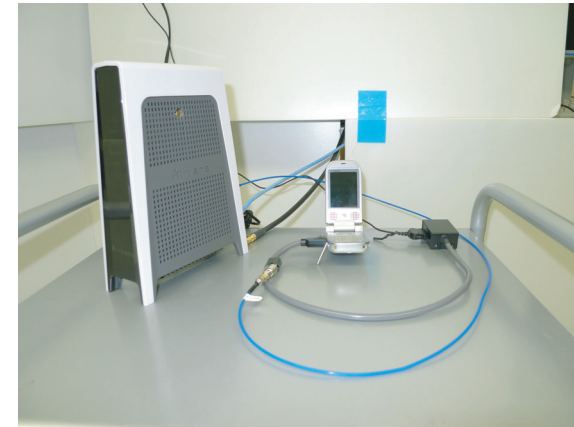


図 9 実験に用いたフェムトセルと携帯電話
Fig. 9 Femtocell and cell phone used for the experiment.

続した。また、FGW には認証サーバ機能を具備した strongSwan¹⁹⁾ を用い、IMS を構成する P-CSCF、I-CSCF および S-CSCF には、NIST-SIP²⁰⁾ をベースに必要な認証や SIP ルーティング制御機能を盛り込んだ。さらに、FGW とフェムトセル#1 および FGW とフェムトセル#2 の転送遅延 (T_{femto1_fgw} , T_{femto2_fgw}) を模擬するため、ルータ内に遅延エミュレータを動作させるとともに、FGW の処理負荷 (P_{fgw_sec}) の増大による処理遅延 (T_{fgw_enc} , T_{fgw_dec}) がパケット損失率に及ぼす影響を検証するため、strongSwan ベースの IPSec 負荷装置を 6 台配置し、3 台ずつ IPSec 負荷装置群#A と IPSec 負荷装置

表 2 処理時間 (エミュレータ遅延なし)
Table 2 Processing time (no delay at emulator).

時間 [ms]	SIP登録時間	SIP発信時間	メディアデータ 転送時間
方式	T_{reg}	T_{inv}	T_{trans_nonopt} T_{trans_opt1} T_{trans_opt2}
標準方式	100.74	2,398.13	0.25
提案方式 (NATなし)	104.32	2,512.23	0.03
提案方式 (NATあり)	114.11	2,432.87	0.22

群#Bに分けた．なお，図8に示すNAT#1およびNAT#2は，NAT対応の提案方式の測定時のみルータとフェムトセル間に配置した．

4.2 測定結果

4.1節の実験システムにおいて，ルータ内の遅延エミュレータの遅延を0とし，IPSec負荷装置なしの状態では，端末#1のSIP登録時間(T_{reg})，端末#1から端末#2への発信時間(T_{inv})，メディアデータ転送時間(T_{trans_nonopt} ， T_{trans_opt1} ， T_{trans_opt2})をそれぞれ5回測定し，その平均値を表2に示す．測定はNATを配置しない場合と配置した場合についてそれぞれ実施した．なお，図2，図4および図7に示したとおり，SIP登録時間とは，フェムトセル#1がSIP REGISTERを送信してから200 OKを受信するまでの時間とする．また，SIP発信時間とは，フェムトセル#1がSIP INVITEを送信してから180 Ringingを受信するまでの時間とする．ここで，フェムトセルにおける暗号鍵(K#1，K#2)生成の内部処理時間は，SIPによるセッション確立にかかる全体の時間に比べて十分に短いため，フェムトセル間のセキュアな通信路の確立処理がSIPによるセッション確立時間へ与える影響は無視でき，それににかかる時間は0とする．

次に，海外ローミングやインターネット上の一部狭帯域区間の状況も考慮し，遅延エミュレータの片方向遅延を0から200ミリ秒まで50ミリ秒間隔で変化させ，それぞれ5回測定し，SIP登録時間，SIP発信時間およびメディアデータ転送時間の平均値を図10，図11，図12に示す．図10および図12にそれぞれ示したSIP登録時間およびメディアデータ転送時間については，遅延エミュレータの遅延値に対して線形的な増加が確認された．一方，図11に示したSIP発信時間については，一部のSIPメッセージに再送が見られ，線形的な増加とはなっていない．また，SIP登録時間とSIP発信時間については，SIP発信時間の

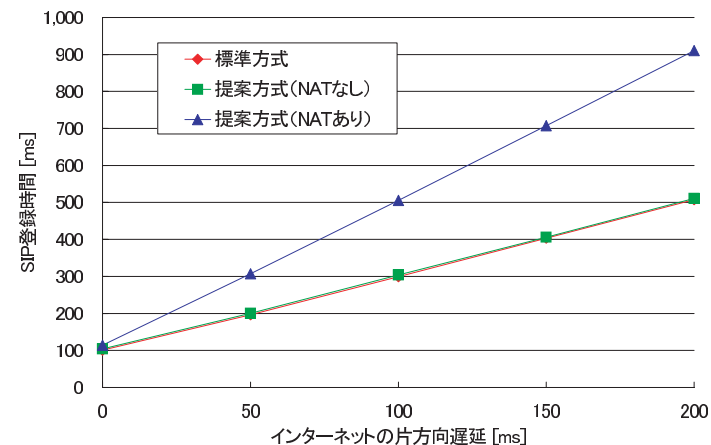


図 10 転送遅延にともなう SIP 登録時間
Fig. 10 SIP registration time along with transit delay.

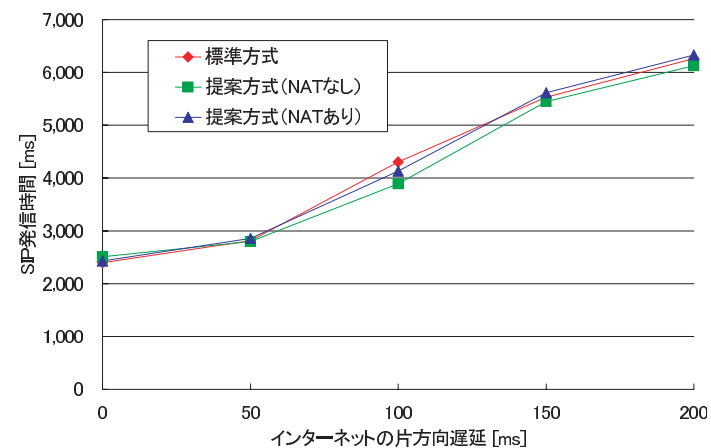


図 11 転送遅延にともなう SIP 発信時間
Fig. 11 SIP call setup time along with transit delay.

方がその交渉メッセージ数が多いため，遅延の影響を受けやすいことが確認された．なお，SIP登録時間において，NATが存在する場合の提案方式の方が，存在しない場合に比べて時間を要するのは，STUN処理によるものである．メディアデータの転送時間については，

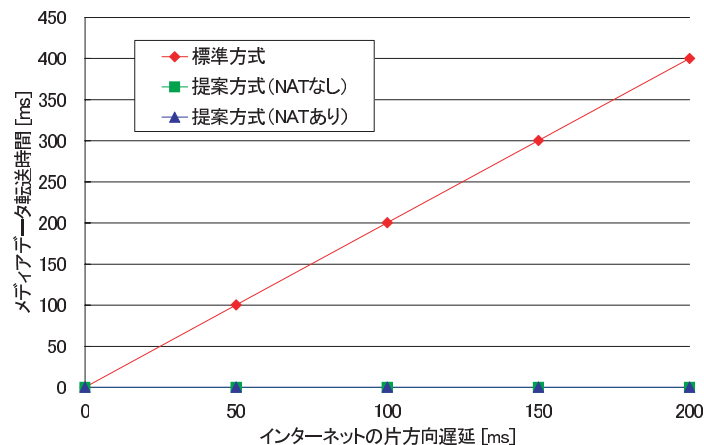


図 12 転送遅延にともなうメディアデータ転送時間

Fig. 12 Media data transit time along with transit delay.

標準方式では NAT と FGW 間の往復のインターネット転送遅延の影響を受けるのに対し、提案方式では NAT の有無にかかわらず、フェムトセル間のインターネット転送遅延の影響のみであり、品質状態を維持することが可能であった。

さらに、NAT なしの状態では遅延エミュレータの遅延を 0 とし、IPSec 負荷装置を動作させ、FGW の負荷増大にともなう端末間の音声パケットの損失率について検証した。測定は FGW における UDP バッファサイズを Linux の標準設定値である 105 キロバイトとし、図 8 に示した IPSec 負荷装置群#A と FGW、ならびに IPSec 負荷装置群#B と FGW の間で音声セッション確立数に応じた複数の IPSec トンネルを確立した状態で、それぞれの音声セッションに対して IPSec 負荷装置群#A と IPSec 負荷装置群#B の双方から、22 バイトの UDP パケットを 20 ミリ秒間隔で送信した。なお、パケット損失の測定対象となる音声セッションについては、事前に確立した状態で IPSec 負荷装置からの負荷を増加させた。具体的には、音声セッション確立数の増加にともない、同一フェムトセルに端末が 5 台接続している環境を想定し、IPSec 負荷装置では 1 台あたり最大 80 の IPSec トンネルと 400 の音声セッションを確立させた。測定はそれぞれ 5 回実施し、音声セッション確立数を 200 セッションずつ 1,200 セッションまで増加させたときの、端末間の音声パケットの損失率の平均値を図 13 に示す。測定結果より、提案方式では FGW の負荷増大によるパケット損失が発生しないのに対し、標準方式では音声セッション確立数が 800 付近から大幅なパ

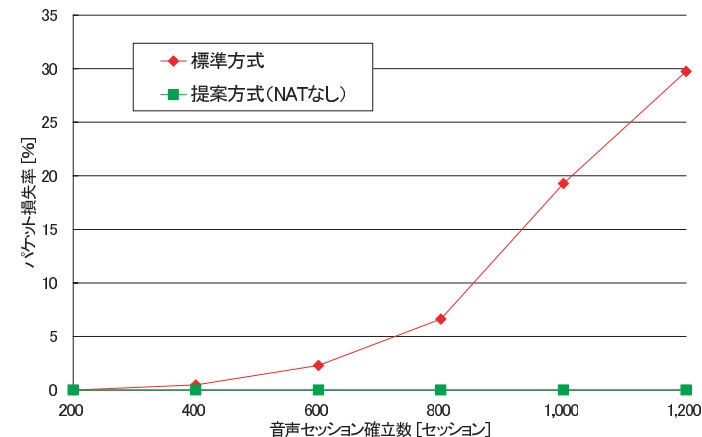


図 13 FGW の負荷増大にともなうパケット損失率

Fig. 13 Packet loss along with FGW load.

ケット損失が発生した。800 セッションでは何とか聞き取れる状況であったものの、1,000 セッションではパケット損失率が 20 パーセント付近まで増加し、音飛びが大きく会話の継続が困難な状況となり、端末間の音声品質に大きな影響を与えることが確認された。

5. おわりに

本論文では、携帯電話の新しい接続形態として注目されているフェムトセルを用いた構成方式を精査し、FGW (Femto Gateway) を介した通信における品質面からの課題について提起した。本課題に対して、IP ベースの音声通信で利用される IMS とフェムトセルを連携し、フェムトセル自身の IP アドレスと FGW から割り当てられる移動端末用の IP アドレスを使い分け、SIP メッセージは FGW を介してコアネットワークへ転送させながら、メディアデータについては FGW を経由せずにフェムトセル間で直接送受信を行う方式を提案した。また、現在 ISP (Internet Service Provider) を介したインターネット接続で広く利用されているプライベートアドレスを用いた通信環境にも対応するために、NAT が介在した状況でもフェムトセル間の通信を可能とする方式の拡張についても提案を行った。提案方式のフェムトセルにより、SIP や STUN などの機能が実装されていない携帯電話を収容しながら、セキュアにメディアデータの経路を最適化することができる。さらに、これらの提案方式を実機のフェムトセルを用いて実装評価を行い、その有効性について検証を行っ

た．実験結果より，提案方式では，NAT の設置有無にかかわらず，メディアデータの転送時間を，標準方式と比べて大幅に低減することが可能であった．よって，FGW に接続するネットワーク帯域の有効利用も利点としてあげられる．また，接続端末数と FGW で行われるパケットの暗号化・復号化にかかる CPU 処理負荷に起因するパケット損失に関する実験結果より，FGW における処理負荷の観点からも提案方式の有効性を確認した．

謝辞 本研究において，実機フェムトセルの実装評価のためにフェムトセルの開発にご協力いただいた Airvana 社の皆様，および日頃ご指導いただく 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．

参 考 文 献

- 1) Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnstone, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, IETF RFC 3261 (2002).
- 2) 3GPP: IP Multimedia Subsystem (IMS); stage 2 (Release 8), TS23.228 V8.8.0 (2009).
- 3) Femto Forum. <http://www.femtoforum.org/>
- 4) Chandrasekhar, V., Andrews, J. and Gatherer, A.: Femtocell Networks: A Survey, *IEEE Communication Magazine*, pp.59–67 (Sep. 2008).
- 5) m2m-x. <http://www.v6.ntt.net/data/m2m-x.html>
- 6) 3GPP2: Signaling Link Access Control (LAC) Standard for cdma2000 Spread Spectrum Systems, C.S0004-D v2.0 (2005).
- 7) 3GPP2: Femto Network Overview and List of Parts, X.P0059-000-0 (2009).
- 8) Kaufman, C.: IKEv2 Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306 (2005).
- 9) Handley, M., Jacobson, V. and Perkins, C.: SDP: Session Description Protocol, IETF RFC 4566 (2006).
- 10) Baugher, M., McGrew, D., Naslund, M., Carrara, E. and Norrman, K.: The Secure Real-time Transport Protocol (SRTP), IETF RFC 3711 (2004).
- 11) Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.: Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), IETF RFC 3489 (2003).
- 12) UPnP Forum. <http://www.upnp.org/>
- 13) Whai-En, C., Ya-Lin, H. and Han-Chieh, C.: NAT Traversing Solutions for SIP Applications, *EURASIP Journal on Wireless Communications and Networking*, Vol.2008, Article ID 639528 (June 2008).
- 14) Khelifi, H., Gregoire, J.-C. and Phillips, J.: VoIP and NAT/firewalls: Issues, traver-

sal techniques and a real-world solution, *IEEE Communication Magazine*, pp.93–99, (July 2006).

- 15) Aoun, C., Davies, E., Tschofenig, H. And Thiruvengadam, S.: Interaction of firewalls and network address translators with internet applications, *Proc. 8th International Conference on Telecommunications*, pp.364–374 (2005).
- 16) Rosenberg, J., Mahy, R. and Matthews, P.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), IETF work in progress (2009).
- 17) Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, IETF Work in Progress (2007).
- 18) Li, A.: RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV), IETF RFC 3558 (2003).
- 19) strongSwan. <http://www.strongswan.org/>
- 20) NIST-SIP. <http://snad.ncsl.nist.gov/proj/iptel/>

(平成 21 年 5 月 18 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．



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．
