社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－MBL－45（2）
2008/5/22

携帯電話をキーデバイスとしたユーザ主導サービス構築プラットフォームのための認証方式

松中 隆志† 蕨野 貴之† 岸 洋司† 中内 清秀†† ベドカフレ††
井上 真杉††

† （株）KDDI研究所 〒356-8502 埼玉県ふじみ野市大原2-1-15
†† （独）情報通信研究機構 〒184-8795 東京都小金井市貫井北町4-2-1
E-mail: †{ta-matsunaka,warabino,kishi}@kddilabs.jp, ††{nakauchi,kafle,inoue}@nict.go.jp

あらまし 多様なデバイスが多様なアクセスシステムによってネットワークに接続されている環境下では，ユーザが，楽しみたいサービスを，ユーザの現在の環境（アクセスシステム，利用デバイス）に応じて，ユーザ主導で柔軟に構築することができるような仕組みが求められている．筆者らは，ユーザが，ユーザの現在の状況および要求するサービスに応じて，関連するデバイスが連携して構成される仮想ネットワークを，動的にかつ簡易に構築することを可能とするユーザ主導サービス構築プラットフォームを提案している[1]．本稿では，上記プラットフォームにおける簡易なデバイス認証・登録方式として，携帯電話をキーデバイスとした簡易なデバイス認証・登録処理を提案する．提案方式によって，ユーザは，利用するデバイスに事前に設定を行わなくても，上記プラットフォームに対して登録を行い，サービスを利用することが可能となる．
キーワード モバイルネットワーク，モバイルコンピューティング，Personal Network

An Authentication Method for a User-driven Service Creation Platform Assisted by Cellular Systems

Takashi MATSUNAKA†, Takayuki WARABINO†, Yoji KISHI†,
Kiyohide NAKAUCHI††, Ved P. KAFLE††, and Masugi INOUE††

† KDDI R&D Laboratories Inc. Ohara 2-1-15, Fujimino, Saitama, 356-8502 Japan
†† National Institute of Information and Communications Technology Nukui-Kitamachi 4-2-1, Koganei, Tokyo, 184-8795 Japan
E-mail: †{ta-matsunaka,warabino,kishi}@kddilabs.jp, ††{nakauchi,kafle,inoue}@nict.go.jp

Abstract Devices and access systems which they are connected are becoming diverse. Under such circumstances, a mechanism is required that users can flexibly construct user-oriented services by themselves according to their circumstances, such as access systems and devices in use. The authors proposed an User-driven Service Creation Platform in [1]. The platform allows users to construct a virtual network which realizes services users wish and where devices related to the services are interacted with each other considering users' circumstances. This paper proposes an authentication and registration approach in the platform with assistance by cellular systems. This approach enables users to register devices which they want to use on the platform and to use devices for services briefly without any preliminaries on the devices.
Key words mobile network, mobile computing, personal network

1. はじめに

昨今，携帯電話をはじめとするモバイル端末の爆発的な発展・普及や，ネットワークへの接続機能をもつ家電製品（情報家電）の普及など，ネットワークに接続されるデバイス・端末の種類の多様化がみられる．また，ネットワークアクセス方式におい

ても，従来のISDN（Integrated Services Digital Network），xDSL（Digital Subscriber Line）などの電話線を利用したアクセス方式やEthernetによるアクセスに加えて，携帯電話，無線LANなどの移動通信用アクセス方式の普及，FTTH（Fiber To The Home），PLC（Power Line Communications）などの高速かつ大容量な固定網通信を実現するアクセス方式の台頭など多様化がみられる．さらに，Web2.0やP2P（Peer-to-Peer）アプリケーションなど，ユーザが自ら情報を積極的に発信するユーザ主導型サービスが登場しており，今後ますます発展・普及していくことが予想される．筆者らは，上述した現状を鑑み，ユーザがサービスを自由に構築・享受できるような仮想環境を，簡易にかつ安全に構築する技術が必要であると考え，ユーザの要求するサービスに応じて，ユーザの現在の状況を鑑みた上で，当該サービスに関連するデバイスが連携して仮想ネットワーク（Personal Network）を動的に構築するユーザ主導サービス構築プラットフォーム（以下，USCP）を提案している[1]．上記プラットフォーム実現のための重要な課題の一つとして，デバイス間の通信内容の秘匿性，デバイスへの不正アクセス対策など，利用デバイスにおけるセキュリティの課題がある．本プラットフォームでは，対象とするデバイスとして，デバイスのネットワークアクセス方式，端末の種類の多様性を許容し，なおかつ事業者の通信基盤によって認可されていないデバイスを利用することも許容している．このようなプラットフォームにおいて，ユーザの利便性を鑑み，簡易にデバイスの正当性を保証する仕組みが必要となる．本稿では，携帯電話をキーデバイスとし，IMS（IP Multimedia Subsystem）/MMD（MultiMedia Domain）[2], [3]のといった事業者通信基盤を活用することで簡易なデバイス認証・登録方式を実現する方式を提案する．

IMS/MMDでは，ユーザの所有する端末に対してUSIM（Universal Subscriber Identity Module）と呼ばれる認証用モジュールを配布する．ユーザは，USIM内の情報を用いてネットワーク側と認証を実施する．本稿では，USIMを持つ携帯電話をキーデバイスとして，USIMを持たないデバイスの認証を行う．この際，デバイスの認証処理をユーザが所有する携帯電話で代理することで，USIM内に保持されている秘密情報を他のデバイスに露呈することなく，デバイスの認証・登録を行うことを可能にした．また，事業者通信基盤のユーザ情報を，所有するデバイス単位で頻繁に変更・追加することなく，安全にデバイス認証を実施することを可能とした．

以下に本稿の構成について述べる．2.では本稿に関連する技術およびユーザ主導サービス構築プラットフォームについて述べる．3.では本稿で提案する認証方式について述べ，4.で提案方式の考察を行う．最後に5.で本稿をまとめる．

2. 背　　景

2.1 IMS/MMD

IMS/MMDは，従来の回線交換技術による移動・固定通信サービスとパケット交換技術による移動・固定通信サービスを、IP技術で統合させる通信方式であり，それぞれ3GPP/3GPP2（3rd Generation Partnership Project）[4], [5]で検討されている．IMS/MMDでは，ユーザの所有する端末に対してUSIM（Universal Subscriber Identity Module）と呼ばれる認証用モジュールを配布する．USIM内にはプライベートなユーザ識別子（IMPI：IP Multimedia Private Identity），パブリックなユーザ識別子（IMPU：IP Multimedia Public Identity），長期保存鍵（K）などが格納されている．またIMS/MMD内のHSS（Home Subscriber Server）にも同様の情報が格納されている．当該端末はネットワークアクセスおよびサービスを要求する際に，当該端末のUSIM内に保持された情報を用いてIMS/MMDへ認証・登録を行う[6]．認証・登録が完了すると，当該端末とIMS/MMD内のP-CSCF（Proxy-Call Session Control Function）との間でIPsec[7]による安全な通信路が確立され，以降のサービス制御用メッセージを安全にやり取りすることができる．

2.2 ユーザ主導サービスプラットフォーム

ユーザ主導サービスプラットフォーム[1]とは，ユーザによる自発的なサービスの構築を支援するためのプラットフォームである．当該プラットフォームでは，ユーザが要求するサービスに応じて，ユーザが認可するデバイス間で閉じたネットワークであるPersonal Network（以下，PN）を構成し，その上でサービスを享受する．その際，各デバイスが接続されているアクセス体系は特に問わない．ユーザによる自由なサービス構築を可能とするためには，サービス提供のためのPNをユーザが動的にかつ簡単に構築できることが求められる．今までPNの実現に関していくつか提案がなされているが[8], [9]，簡易性，柔軟性，自由度の面で実現に課題がある．そこで当該プラットフォームでは，(1) フラットなネットワーク構造，(2) 事業者通信基盤を活用したデバイス認証の2つの特徴を有するプラットフォームを構築し，ユーザによる自由なサービス構築を可能とする．

（1） フラットなネットワーク構造

当該プラットフォームでは，デバイスは全てフラットに管理される．フラットなデバイス管理構成にすることで，Personal Network内におけるデバイス間のスムーズな連携が可能となる．また，フラットな構造によって，ユーザが受けたいサービスに応じた柔軟なネットワーク構築が可能となる．

（2） 事業者通信基盤を活用したデバイス認証

ユーザがサービスを安全に享受するためには，ネットワーク内データの秘匿性，不正なデバイスによるネットワークアクセスの防止などのセキュリティ対策が必要となる．上述したようなフラットな構造をもつネットワークでは，上述した利点の反面，一般的に中央集権的なノードが存在しないため，デバイス管理が煩雑になり，それに付随して認証アーキテクチャーの構築も困難になるという欠点がある．事業者通信基盤をデバイスの信頼性の根幹とすることで，上記の煩雑さを伴わない認証アーキテクチャーを構築することが可能となる．事業者通信基盤を活用するにあたり，世の中に広く普及している携帯電話をプライベートネットワーク構築におけるキーデバイスとすることで，ユーザが初期導入時に行う設定を簡略化できる．

図1に，本稿で想定するシステムの構成概要図を示す．各デ

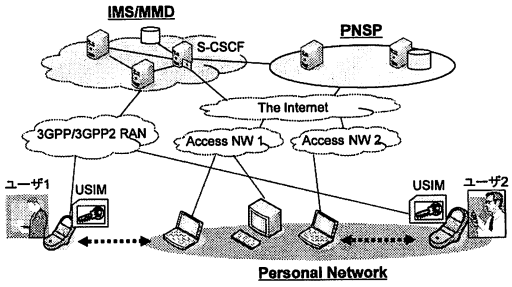

図 1　ユーザ主導サービス構築プラットフォーム

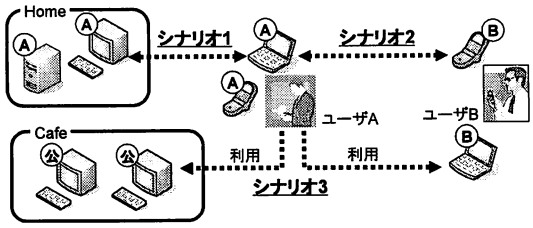

図 2　Personal Network 構成シナリオ

バイスは，固定・移動によらず様々なアクセス体系に接続されている．ネットワーク側には，PN 構築のためのサービスプロバイダ（PNSP: Personal Network Service Provider）を設置する．PNSP は IMS AS（Application Server）として，IMS 内の S-CSCF（Serving-CSCF）に接続される．また PNSP は Internet からのアクセスも可能である．PNSP は，USIM を持たないデバイスの登録，デバイス間鍵交換の仲介，IMS へのアクセスの仲介を担う．

PNSP では，Personal Network を構成するデバイス間の関係，およびユーザ—デバイス間の関係として，以下のシナリオを想定する．図 2 に，以下のシナリオを図示する．

シナリオ 1: 両デバイスがともに同じユーザの所有物である場合．例えば，あるユーザがノートパソコンを利用して，外出先から自宅のデスクトップパソコンのファイルを参照する場面が考えられる．

シナリオ 2: 各デバイスがそれぞれ別のユーザの所有物である場合．例えば，友人同士で写真を共有する場面が考えられる．

シナリオ 3: ユーザが公共デバイス，もしくは他のユーザのデバイスを利用する場合．例えば，あるユーザがネットカフェにあるデバイスを利用して，自宅のデスクトップパソコンのファイルを参照する場面が考えられる．

PNSP によるサービス構築例として遠隔診断サービスについて記載する．対応する利用シナリオをサービスに併記する．図 3 に適用例について示す．

(PN-1)　ユーザ A は，会社で自宅で療養している母親の様子を監視する．その際，自宅のカメラの映像を，会社のパソコンへ転送して映像を見る（映像配信サービス）（シナリオ 1，3）．

(PN-2)　ユーザ A は，自宅の母親の診察を要求する．その結果，診察対応可能な医師 B が検索される（診察依頼サービス）（シナリオ 2）．

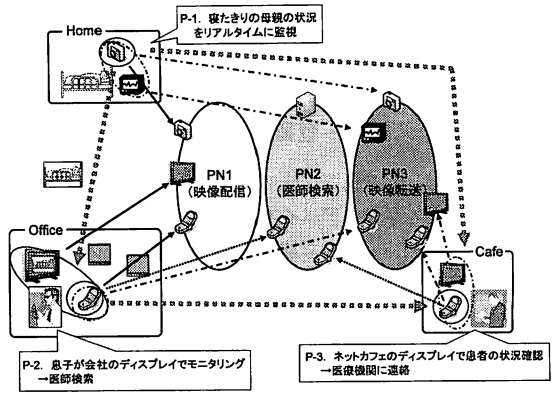

図 3　ユーザ主導サービス構築プラットフォーム適用例

(PN-3)　ユーザ A は診察のため，医師 B に自宅の母親の映像，バイタルデータを転送する（情報転送サービス）．医師 B は送られたデータを参照して，診察を実施する（シナリオ 2，3）．

2.3 関連研究

3GPP では，携帯電話を利用して Personal Network を実現する PNM（Personal Network Management）が提案・検討されている [9]．PNM では，携帯電話など USIM をもつデバイスをゲートウェイとして，他の USIM を持たないデバイスの IMS へのアクセスを可能とすることで，通話のリダイレクトサービスなど，ユーザが所有するデバイスでの IMS サービスを可能とする．しかしながら PNM では，IMS 側にあらかじめ全てのデバイス情報を保存しておく必要がある，IMS に直接接続できないデバイスは，常に USIM をもつ携帯電話を経由して，サービスを享受しなければならない．

伝宝ら [10] は，USIM を持つ携帯端末の情報を用いて，周辺の端末間で PAN を構成する手法を考案した．携帯端末が，周辺端末の情報を IMS 側に登録し，同時に周辺端末に認証情報を送付することで，周辺端末は IMS に対して認証を行うことができる．そして周辺端末を，IMS に接続された PAN 管理サーバに問い合わせることで，例えば動画配信サービスを継続しながらの端末切替，PAN の状況に応じたネットワーク主導のハンドオーバが可能となる．しかしながら，当該手法は，IMS に直接接続できない端末はサポートされない，また当該手法は，携帯端末が HSS などの IMS 網内の認証サーバの情報を書き換えることができるという前提上動作する手法であり，一般的ではない．

Bhargava ら [11] は，携帯電話網を認証用，ルーティング情報伝送用のようなネットワーク制御用通信路とすることで，アドホックネットワークの認証，およびルーティングをセキュアに行うシステム CAMA（Cellular Aided Mobile Ad Hoc Network）を考案した．CAMA では，ネットワーク側に端末の認証を司るサーバを設置する．各端末は，当該サーバに携帯電話網を用いてアクセスすることで認証を行う．また経路制御を行う場合，各端末は携帯電話網を用いて互いに情報をやり取りすることで，

正しい経路の構築が可能となる．このようにCAMAでは，携帯電話網は，制御メッセージ転送のための通信路という役割のみを担う．

3. デバイス認証・登録方式

ユーザ主導サービス構築プラットフォームでは，多様なアクセス体系，多様な種類のデバイスを対象とする．その際，全てのデバイスにUSIMのような認証情報が含まれた媒体を配布して，デバイスの正当性を担保するのは，プラットフォームのスケーラビリティという観点から現実的ではない．セキュリティを考慮したPNを構築するために，事業者通信基盤に登録されていないデバイスの管理方法が重要である．以下，本節ではプラットフォームのスケーラビリティを考慮し，携帯電話をキーデバイスとした簡易なデバイス認証・登録方式について述べる．

3.1 準　　備

要求条件 PNSPにおけるデバイス認証・登録方式の要件を以下にまとめる．

要求1: 認証・登録の対象となるデバイスには，基本的には本認証・登録方式のための機能を追加しない．

要求2: IMSには，本認証・登録方式のための機能を追加しない．また，IMS内へのユーザプロファイル編集などの処理をデバイス単位で行わない．

要求3: PNSP側での共有鍵など秘密情報管理コストを極力少なくする．

要求4: 認証・登録処理の結果，デバイスはIMSサービスの享受が可能となる．

要求5: 認証・登録処理の結果，デバイスとそれを利用するユーザとの対応付けができるようにする．

要求1，2に関しては，2.2節のシナリオ3のような利用シーン，およびプラットフォームの実現性を考慮すると必要な条件であると考えられる．要求3は膨大なデバイス数への対応のため必要である．要求4は実際のサービスおよびデバイス間の鍵共有がIMSを介して実行できるように設定した．要求5はPersonal Networkにおけるデバイスに対するユーザ単位でのアクセス制限が可能なように設定した．

前提条件 認証・登録処理を検討するにあたり，本稿では，以下の内容を前提とし，事前に設定・配布済みとする．

前提1: TEは，事前にPNSP利用のためのIMPU（$IMPU_{\mathrm{TE}}$）と，PNSPとの共有鍵（K_{PF}）を取得している．

前提2: nTEは，IMSに直接アクセスできない．

前提3: 事業者は，特定のrealm（例: xxx@pncp.net）宛のメッセージを全てPNSPに転送する．

前提4: IMS–TE間，IMS–PNSP間の通信は秘匿性，完全性が保証されている．

上記の前提1に関して，例えばPNSPの提供を一つのサービスと見なし，以下のようなシナリオを想定すると，妥当であると考えられる．(1) ユーザがTEを使ってオンラインで，もしくは店頭などでPNSPの利用を申し込む，(2) PNSPからIMPUおよび共有鍵が送付される．また前提2に関しては，全てのデバイスに対してPDG/PDIF（Packet Data Gateway/Packet Data Interworking Function）[12], [13]を通したIMSアクセスを許可するのは，DDoS（Distributed Denial of Service）などの脅威に対するセキュリティの観点から現実的ではない，またPDG/PDIFのアクセス許可のための認証情報を全てのデバイスに配布し，管理するのは，スケーラビリティの観点から困難であるという仮定から設定した．

表1　記　　法

TE_x	ユーザXのIMS登録携帯電話
nTE_x	ユーザXのIMS非登録デバイス
$ID_{\mathrm{nTE},x}$	nTE_xの識別子（例: MACアドレス，製造番号）
$IMPU_{\mathrm{TE},x}$	ユーザXのTE用IMPU
$IMPU_{\mathrm{nTE},x}$	ユーザXのnTE用IMPU
$E(k,m)$	mをkで暗号化
$D(k,c)$	cをkで復号化
$h(x)$	一方向関数
$a\|\|b$	aとbの連結
$A \oplus B$	AとBのビットごとの排他的論理和
$PK_{\mathrm{PF}}, SK_{\mathrm{PF}}$	PNSPの公開鍵，秘密鍵
MK_{PF}	PNSPのマスター鍵
$K_{\mathrm{PF},x}$	PNSPとTE_xとの共有鍵
	$K_{\mathrm{PF},x} = h(MK_{\mathrm{PF}} \oplus IMPU_{\mathrm{TE},x})$

次節以降で説明の際に用いる記法について表1にまとめる．

3.2 認証・登録方式概要

本提案手法は，PNSPにおいてIMSに登録されていないデバイス（以下，nTE）の認証およびデバイス間での鍵共有を実現するものである．図4に概要を図示する．各デバイスは，Personal Networkに参加する前に，PNSPに対して認証およびデバイス情報の登録を行う．その際，対象となるnTEのユーザの所有するIMSに登録済の携帯電話（以下，TE）が代理で認証・登録を実施することで，安全性が担保された通信路を用いてのメッセージの送受を可能とする．TEおよびPNSPでは，IMS経由でのメッセージ到達を確認することで，互いがIMSに認可されたエンティティであることを確認できる．デバイス認証および登録処理によって，TEは当該nTEのためのIMS用識別子$IMPU_{\mathrm{nTE}}$とPNSPとの事前共有鍵K_{nTE}を生成し，これらを当該nTEに渡す．ここで，$IMPU_{\mathrm{nTE}}$にK_{nTE}の生成に必要な情報を埋め込むことで，PNSP側でK_{nTE}を管理・保存しなくても，必要なときに当該nTE用のK_{nTE}を生成することができるため，PNSP側の管理負荷の軽減ができる．以降，当該nTEは，$IMPU_{\mathrm{nTE}}$およびK_{nTE}を用いて，PNSP経由でIMSにアクセスすることが可能となり，TEとのIMS経由での通信およびIMSサービスの享受が可能となる．

実際にPersonal Networkをデバイス間で構築する場合，デバイス間で共通の鍵を共有する必要がある．当該鍵を用いて，Personal Network内でやり取りするデータを秘匿化することで，そのPersonal Network内で閉じたサービスの提供・享受が可能となる．デバイス間での鍵共有を実施する際，各デバイスは，上述の登録処理でPNSPと共有されたK_{nTE}を用いて，PNSP経由で二者間で鍵共有を実施する．利用する鍵共有プロトコルとして，例えばMIKEY（Multimedia Internet

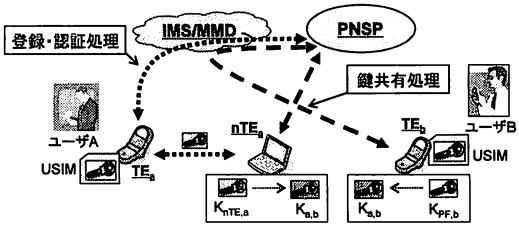

図 4　登録・認証，鍵共有処理概要図

KEYing) [14] の PSK（Pre-Shared Key）モードが挙げられる．

3.3 デバイス登録処理

以下，ユーザ A のデバイス nTE_a を PNSP に登録する場合を想定する．デバイス登録処理手順を図 5 に示す．

TE_a は，nTE_a の識別子 $ID_{\mathrm{nTE},a}$ を取得すると，INVITE メッセージにて PNSP に対してデバイス登録の要求を行う．その際，当該メッセージの From フィールドにおいて tag=$ID_{\mathrm{nTE},a}$ として，デバイスの識別子を当該メッセージに付加する．

INVITE メッセージを受け取った PNSP は，当該メッセージが IMS 経由で到達したことから，送信者が正規の IMS ユーザであることを確認する．そして，PNSP は TE_a との間で nTE_a の共有鍵 $K_{\mathrm{nTE},a}$ を共有するために，Proxy Authentication Request メッセージを TE_a 宛に返信する．その際、認証方式を示す情報を Proxy-Authenticate フィールドに例えば “PNSP-auth” のような形で追加する．さらに，当該メッセージ内に，$K_{\mathrm{nTE},a}$ の生成に必要な乱数情報等を，TE_a との共有鍵 $K_{\mathrm{PF},a}$ で暗号化したもの（c_1）を追加して送付する．c_1 は次のようにして算出される．乱数 r_0，$IMPU_{\mathrm{TE},a}$，$ID_{\mathrm{nTE},a}$ と MK_{PF} から，$c_0 = E(MK_{\mathrm{PF}}, r_0||H_0)$，$H_0 = h(IMPU_{\mathrm{TE},a} \oplus ID_{\mathrm{nTE},a})$ を生成し，$c_1 = E(K_{\mathrm{PF},a}, c_0||H_1)$，$H_1 = h(K_{\mathrm{PF},a}||c_0)$ を得る．

TE_a は，Proxy Authentication Request メッセージを受け取ると，当該メッセージ内の c_1 を復号して c_0，H_1 を導出し，$H_1 = h(K_{\mathrm{PF},a}||c_0)$ の検証を行う．そして TE_a は乱数 r_1 を生成して，$IMPU_{\mathrm{nTE},a} = E(PK_{\mathrm{PF}}, c_0||r_1||IMPU_{\mathrm{TE},a}||ID_{\mathrm{nTE},a})$，$K_{\mathrm{nTE},a} = h(c_0||r_1||IMPU_{\mathrm{TE},a}||ID_{\mathrm{nTE},a}||K_{\mathrm{PF},a})$ を生成する．

これによって PNSP は $IMPU_{\mathrm{nTE},a}$ 内の情報から $K_{\mathrm{nTE},a}$ を導出することが可能となる．まず，PNSP は自身の秘密鍵 SK_{PF} を用いて c_0，r_1，$IMPU_{\mathrm{TE},a}$，$ID_{\mathrm{nTE},a}$ を導出する．c_0 を復号し，$H_0 = h(IMPU_{\mathrm{TE},a} \oplus ID_{\mathrm{nTE},a})$ を検証した後，PNSP は $IMPU_{\mathrm{TE},a}$ から $K_{\mathrm{PF},a}$ を生成し，最終的に $K_{\mathrm{nTE},a}$ を得る．したがって，PNSP は秘密鍵 SK_{PF} のみ管理すればよいこととなり，鍵情報の管理コストを軽減することができる．

TE_a は，鍵生成後，PNSP に対して再度 INVITE メッセージを送付し，生成した共有鍵 $K_{\mathrm{nTE},a}$ および $IMPU_{\mathrm{nTE},a}$ の完全性を検証する．PNSP 側で鍵の完全性が検証されると，PNSP は 200 OK メッセージを TE_a に対して送付する．鍵共有後，nTE_a は IP アドレスなどの位置情報，提供可能サービスなどサービスに係る情報を，PNSP に登録する．その際，当該情報は共有された $K_{\mathrm{nTE},a}$ を用いて秘匿化される．

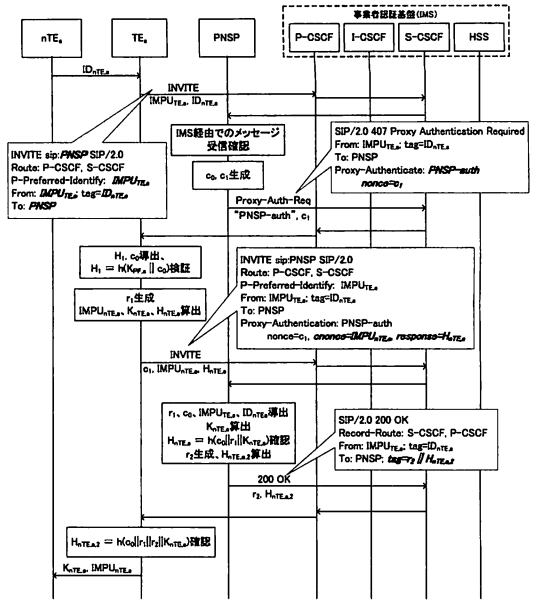

図 5　デバイス登録処理

3.4 デバイス間鍵共有処理

デバイス間の鍵共有処理は，まず二者間で IMS を経由したセッションを確立し，当該セッションの上で鍵共有のためのメッセージを送受することで実現する．

セッション確立処理　デバイス間のセッション確立は，PNSP を介して行われる．以下に，nTE_a が実際に PNSP 経由でユーザ B の TE（TE_b）とセッションを確立する場合を例示する．図 6，7 にメッセージ例を示す．

nTE_a から TE_b へセッション確立を行う場合：　nTE_a からのメッセージを IMS に通過させるために PNSP で $IMPU_{\mathrm{nTE},a}$ を $IMPU_{\mathrm{TE},a}$ に変換させる必要がある．そのために，nTE_a は Route ヘッダに PNSP を指定する．nTE_a—PNSP 間のメッセージの秘匿性，完全性に関しては，例えば共有鍵 $K_{\mathrm{nTE},a}$ を用いた S/MIME （Secure/Multipurpose Internet Mail Extensions）によって保証する方法が挙げられる [15]．メッセージを受け取った PNSP は，To フィールドの $IMPU_{\mathrm{nTE},a}$ を $IMPU_{\mathrm{TE},a}$ に変換して，TE_b へ転送する．

TE_b から nTE_a へセッション確立を行う場合：　TE_b は，Request-URI に nTE_a を指定して IMS へメッセージを送付する．その際，nTE_a に特定の realm（xxx@pncp.net）が付加されていることによって，IMS は 3.1 節の前提 3 より，当該メッセージを PNSP に転送する．PNSP は，$IMPU_{\mathrm{nTE},a}$ から $IMPU_{\mathrm{TE},a}$ および $K_{\mathrm{nTE},a}$ を導出し，nTE_a の位置情報を検索して，当該メッセージを nTE_a に転送する．

鍵共有処理　二者間で鍵共有を実施するプロトコルとして，MIKEY [14] が挙げられる．MIKEY は，1 ラウンドのメッセージの送受で二者間で鍵共有を実現するプロトコルであり，SIP (Session Initiation Protocol) [15] との親和性も高い．MIKEY の PSK モードでは，二者間が事前に共有した秘密情報を利用し

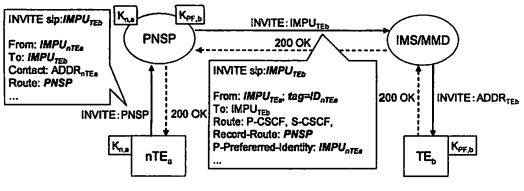

図 6 nTE から TE へのセッション確立

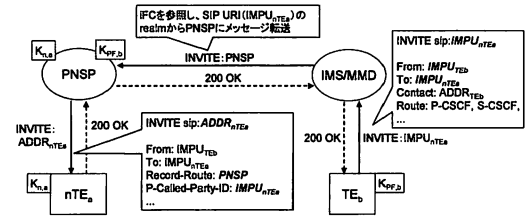

図 7 TE から nTE へのセッション確立

て，コンテンツ暗号化のための鍵情報を共有する．事前に共有した秘密情報から，お互いメッセージ秘匿化用の鍵（encr_key）とメッセージ完全性検証用の鍵（auth_key）を生成し，これらを用いて一方がランダムに生成した共有鍵を秘匿化してもう一方に送付する．この際，当該メッセージの完全性検証のために MAC（Message Authentication Code）を付与する．

デバイス間鍵共有処理では，登録済みの TE および nTE は，各々PNSP と共有鍵（$K_{\mathrm{PF},x}$，$K_{\mathrm{nTE},x}$）を共有していることから，上述したような事前共有鍵を用いた鍵共有プロトコルをデバイス—PNSP 間で適用し，PNSP を介して両デバイス間で鍵共有を実施することを考える．最終的に，両デバイス間で共通鍵 $K_{a,b}$ が共有され，以降 $K_{a,b}$ で両者間でやり取りされるコンテンツ，メッセージを秘匿化することで PN を実現する．

4. 考　　察

まず 3.1 節の要件との整合性について述べる．本方式は，認証・登録処理に関しては nTE 側は特に処理を必要としないため要求 1 を満たす．また，本方式は，ユーザが PNSP の利用を要求した際に，事業者内に 3.1 節の前提 3 のための設定を行う以外は，事業者側のユーザプロファイルに編集を加えないため要求 2 を満たす．本方式は，nTE 用に生成する $IMPU_{\mathrm{nTE}}$ に，利用者の $IMPU_{\mathrm{TE}}$ および PNSP との共有鍵 K_{nTE} 導出のための情報が内包されているため，PNSP は $IMPU_{\mathrm{nTE}}$ から当該 nTE のユーザおよび共有鍵が導出できる．よって要件 3，5 を満たす．nTE は，登録処理後に PNSP を経由することで IMS へのアクセスが可能となるため，要件 4 を満たす．

次に本方式の安全性について $IMPU_{\mathrm{nTE}}$，K_{nTE} の安全性に着目して述べる．$IMPU_{\mathrm{TE},a}$ および PK_{PF} を取得した攻撃者 $\mathcal{A}$ が，$IMPU_{\mathrm{nTE},a}$ を偽造し，PNSP 経由で IMS にアクセスすることを想定する．攻撃者 $\mathcal{A}$ は，PNSP–TE$_a$ との共有鍵 $K_{\mathrm{PF},a}$ および PNSP のマスター鍵 MK_{PF} を知らないため，$c_0 = E(MK_{\mathrm{PF}}, r_0||H_0)$（$H_0 = h(IMPU_{\mathrm{TE},a} \oplus ID_{\mathrm{nTE},a})$）を生成できない．よって $IMPU_{\mathrm{nTE},a} = E(PK_{\mathrm{PF}}, c_0||r_1||IMPU_{\mathrm{TE},a}||ID_{\mathrm{nTE},a})$，$K_{\mathrm{nTE},a} = h(c_0||r_1||IMPU_{\mathrm{TE},a}||ID_{\mathrm{nTE},a}||K_{\mathrm{PF},a})$ を生成できない．また，ユーザ A が登録処理を行わずに別の nTE 用の $IMPU'_{\mathrm{nTE},a}$ および $K'_{\mathrm{nTE},a}$ を生成する場合を想定する．この場合，ユーザ A は同様に $c'_0 = E(MK_{\mathrm{PF}}, r'_0||H'_0)$（$H'_0 = h(IMPU_{\mathrm{TE},a} \oplus ID'_{\mathrm{nTE},a})$）を生成できないため，$IMPU'_{\mathrm{nTE},a}$ および $K'_{\mathrm{nTE},a}$ を生成できない．

5. ま と め

本稿では，ユーザが，ユーザ主導サービスを自由に構築・享受できるような仮想環境を，簡易にかつ安全に構築することを可能にするユーザ主導サービス構築プラットフォームにおける安全なデバイス間連携のためのデバイス認証・登録方式について提案した．デバイス認証の簡略化のために，IMS/MMD といった事業者通信基盤を活用する，具体的には，デバイスの認証処理をユーザが所有する携帯電話で代理することで，USIM を持たないデバイスの認証を行う方法を考案した．この方式を用いることで，USIM 内に保持されている秘密情報を他のデバイスに露呈することなく，また，事業者通信基盤のユーザ情報を，所有するデバイス単位で頻繁に変更・追加することなく，安全にデバイス認証・登録を実施することができる．現在，本方式の実用性を評価するためのシステムを試作中である．

文　　献

[1] 中内, カフレ, 井上, 松中, 蕨野, 岸：“携帯電話をキーデバイスとしたユーザ主導サービス構築プラットフォームの基本設計”, 信学技報, MoMuC2008-1 (2008).

[2] 3GPP: “IP Multimedia Subsystem (IMS) Stage 2 (Release 8)”, TS 23.228.

[3] 3GPP2: “All-IP Core Network Multimedia Domain – Overview”, X.S0013-000-B.

[4] “3rd Generation Partnership Project”, http://www.3gpp.org/.

[5] “3rd Generation Partnership Project 2”, http://www.3gpp2.org/.

[6] 3GPP: “3G Security; Access security for IP-based services (Release 7)”, TS 33.203.

[7] S. Kent and K. Seo: “Security Architecture for the Internet Protocol”, RFC 4301 (2005).

[8] “MAGNET Beyond”, http://www.ist-magnet.org/.

[9] 3GPP: “Service requirements for Personal Network Management (PNM); Stage 1”, TS 22.259.

[10] 伝宝, 藤野, 秋好：“All IP Network における Personal Area Network サポート”, 電子情報通信学会 2005 年ソサイエティ大会, BS-2-10 (2005).

[11] B. Bhargawa, X. Wu, Y. Lu and W. Wang: “Integrating Heterogenious Wireless Technologies: A Cellular Aided Mobile Ad Hoc Network (CAMA)”, MONET, **9**, 4, pp. 393–408 (2004).

[12] 3GPP: “3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 7)”, TS 23.234.

[13] 3GPP2: “cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services”, X.S0011-002-D.

[14] J. Arkko, E. Carrara, F. Lindholm and M. Naslund: “MIKEY: Multimedia Internet KEYing”, RFC 3830 (2004).

[15] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Juhnston, J. Peterson, R. Sparks, M. Handley and E. Schooler: “SIP: Session Initiation Protocol”, RFC 3261 (2002).