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

2008－MBL－45（1）
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基本設計

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

† 情報通信研究機構 新世代ネットワーク研究センター, 〒184–8795 東京都小金井市貫井北町 4–2–1
†† KDDI 研究所, 〒356–8502 埼玉県ふじみ野市大原 2–1–15
E-mail: †{nakauchi,kafle,inoue}@nict.go.jp, ††{ta-matsunaka,warabino,kishi}@kddilabs.jp

あらまし デバイスの多様化，高機能化，無線通信方式の多様化，高速化など，デバイスや無線通信技術の個々の技術革新は進んでいるものの，デバイス管理負荷の増加，デバイス間連携の複雑化，及びデバイスへの不正アクセス，個人情報漏洩などが大きな課題となっている．結局，高機能デバイス同士を簡単に接続することは相変わらず困難である．そこで，オペレータ通信基盤を活用することにより，ユーザやユーザグループに閉じたセキュアなプライベートネットワークをユーザが簡易な操作で構築できるユーザ主導サービス構築プラットフォーム (USCP) を提案する．USCP は，シグナリングパスとデータ通信パスの分離，フラットな仮想ネットワーク構造という特徴をもつ．本稿では，USCP の基本設計について述べる．

キーワード パーソナルネットワーク，パーソナルエリアネットワーク，セルラネットワーク，ユーザセントリックネットワーク，仮想ネットワーク

Basic Design of A User-driven Service Creation Platform Assisted by Cellular Systems

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

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

Abstract In spite of recent advances of personal communication devices and access network technology, users are still facing the issues such as high device maintenance costs, complication of inter-device cooperation, illegal access to devices, and leakage of personal information. Consequently, it is difficult for users to securely network local as well as remote personal devices. We propose a User-driven Service Creation Platform, USCP, which enables users to construct a secure private network in a simple and intuitive way, making the most of the authentication mechanism in cellar networks. USCP separates signaling and data paths in a flat structure of a virtual network topology. In this paper, we describe the basic design of USCP.

Key words Personal Network, Personal Area Network, Cellular Network, User-centric Network, Virtual Network

1. はじめに

携帯電話や情報家電などネットワーク機能をもつデバイスの多様化，高機能化が進んでいる．一方，通信技術に目を向けても，3G 以降のセルラ通信技術，WiMAX (IEEE802.16)，WiFi (IEEE802.11)，Bluetooth，IrDA などの無線技術が実用

化，または実用化に向けて開発されており，無線通信方式の多様化，高速化も進行している．しかしながら，このようなデバイスや無線通信技術の技術革新は，ユーザに対するデバイス管理負荷の増加，デバイス及びアクセスシステムの多様化に伴うデバイス間通信・連携の複雑化，及びデバイスへの不正アクセス，個人情報漏洩などの課題をより大きくしている．結局ユーザにとっては，高機能デバイス同士を簡単に接続したり，高機能デバイスと既存デバイスを簡単に連携させてネットワーク化したりすることが相変わらず困難である．

例えば，デジタルカメラの中にある数 GB の写真データを友人達に送りたい場合，まずデータを PC にコピーし，そこから FTP サーバや Web サーバにアップロードして一時的に公開するか，オンラインストレージサービスを利用するしかなく，技術的に万人にとって使い勝手が良い方法はない．(最悪の場合は記憶メディアをオフラインで配送する.) 別の例として，数名によるオフライン会議において会議資料を共有したい場合，各参加者が資料を電子メールで全員に送ったり，USB メモリを全員に回したりするような原始的で面倒な方法しかない．

本研究の目的は，ユーザの多様な接続環境（アクセスシステム，利用デバイス）やサービス要求に柔軟に対応でき，ユーザやユーザグループに閉じたセキュアな情報共有空間をユーザが動的に構築するための要素技術の実現である．

上記のような情報空間は，パーソナルネットワーク (Personal Network, PN) [9] と呼ばれる．PN は，遠隔にあるデバイス同士で論理的に構成されるプライベートな仮想ネットワークである．PN は VPN (Virtual Private Network) [6] と形態が似ているが，次の点で根本的に異なる．VPN が LAN 間接続またはリモート端末からの LAN 接続といった LAN の拡張を目的とするのに対し，PN はサービスに応じて選定された特定のリモート端末だけで仮想ネットワークを構築することを目的とする．

PN のビジョンは，MAGNET / MAGNET Beyond プロジェクト [8], [10]，3GPP2 (Third Generation Partnership Project) [2], [3]，UIA [4], [5], [10] などで提唱されているが，実現には至っていない．

本稿では，PN の実現をより容易にし，かつユーザが簡易な操作で PN の構築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 (USCP: User-driven Service Creation Platform) を提案する．USCP では，広く普及している携帯電話を PN 構築におけるキーデバイスとして利用し，オペレータ通信基盤を活用することで，PN の構築・運用を簡略化する．

USCP の第一の特徴は，シグナリングパスとデータ通信パスの分離である．すなわち，強固なセキュリティが要求されるユーザ認証・デバイス認証（シグナリング）には IMS (IP Multimedia Subsystems) / MMD (MultiMedia Domain) [1] というオペレータ通信基盤を活用し，データ通信にはインターネットなどの高速回線を利用する．これにより，認証プロセスの簡略化，強固なセキュリティ，データ通信の高速化を両立させる．第二の特徴は PN の仮想ネットワーク構造のフラット化である．最初からユーザや管理ドメインをまたがった PN の構造を想定し，デバイスやユーザの信頼性の根幹であるオペレータ通信基盤に PN 管理機能を集約する．これによりユーザ単位，もしくは管理ドメイン単位での PN 管理が不要となり，迅速かつ少ない手順での効率的な PN 構築が可能となる．

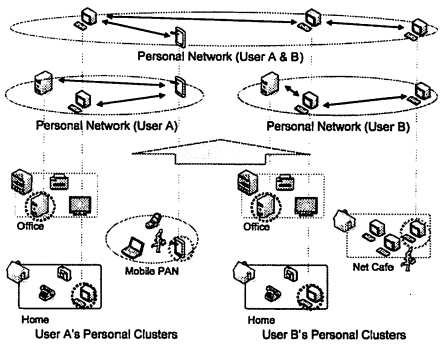

図 1　パーソナルネットワークの概要
Fig. 1　Overview of Personal Networks

本稿では，デバイスの能力に加え，機能のクリティカル度，PN 構築手順の効率を考慮して，PN 構築に必要な機能を PNSP，オペレータ，ユーザデバイスに適切に配置することにより USCP の基本設計を行う．

本稿の構成は以下の通りである．2 章において，パーソナルネットワークの概要及びアプリケーションシナリオについて説明する．3 章では，USCP の概要を述べ，4 章においてその基本設計を説明する．5 章において，USCP を用いた PN の設計手順を簡単に説明する．

2. パーソナルネットワーク

2.1 PN 概 要

PN は，PAN（Personal Area Network）の概念を拡張させたものであり，関連するデバイスがネットワークをまたがって連携することにより構築されるユーザやユーザグループに閉じたセキュアでユーザセントリックなプライベート情報共有である．PAN がユーザを中心として Bluetooth などの近距離無線技術を用いて複数のデバイスが構成するプライベートな物理ネットワークであるのに対し，PN はユーザを中心として，遠隔にあるデバイス同士が管理ドメインをまたいで論理的に構成する，いわばプライベートな仮想ネットワークである．PN の実現により，異なるユーザが所有するデバイス同士が，互いのアクセスシステムや所属ドメインに制約されることなく，オンデマンドでセキュアな通信が可能となる．

PN の概要を図 1 に示す．PN を構成するメンバとして，目的のサービスを提供または享受するデバイスだけが選定され，そのデバイスだけで PN が構成される．また，IPsec 技術などを利用してメンバとなるデバイス間にセキュアなチャネルを確立することにより，プライベートな環境を構築する．PN 構築後，必要に応じてデバイスの新規参加や，メンバデバイスの脱退が可能である．PN では利用するアクセスシステムを問わず，デバイスは無線，有線のどちらの接続形態をとってもよい．

PN のビジョンは，すでに MAGNET / MAGNET Beyond や 3GPP PMN で提案されてはいるものの，実現の目処は立っていない．本研究では PN の実用化を見据え，実現可能な PN 構築方式を提案する．

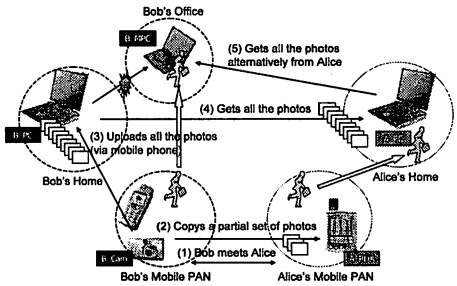

図 2 アプリケーションシナリオ: 遠隔ファイルアクセス
Fig. 2 Application Scenario: Remote File Access

2.2 アプリケーションシナリオ

図 2 に示すように，異なるサブネットに接続されたデバイスへの遠隔アクセスを考える．

1. Bob が友人の Alice に出会い，Bob のデジタルカメラ (B_Cam) 内の写真の共有を合意．
2. B_Cam 内の写真の一部を Alice の PDA (A_PDA) にコピー．(B_Cam と A_PDA でファイル共有 PN を構築)
3. B_Cam 内のすべての写真を，リモートアクセスのために Bob の自宅 PC (B_PC) にアップロード．(B_PC をファイル共有 PN に追加)
4. Alice は帰宅後，残りの写真を閲覧するために，Alice の自宅 PC (A_PC) から Bob の自宅 PC (B_PC) にアクセス．(A_PC をファイル共有 PN に追加)
5. Bob は外出中，モバイル PC (B_MPC) から B_PC へのアクセスがネットワーク障害により不可能であったため，代わりに A_PC にアクセスし，写真をダウンロード．(B_MPC をファイル共有 PN に追加)

2.3 技術的課題

パーソナルネットワークを実現するためには下記のような技術的課題を解決する必要がある．

- ユーザ認証

正規ユーザの判別や，認証基盤の正当性の保証ができなければならない．また，ユーザ毎に，PN 上で利用または構築できるサービスの認証ができなければならない．

- デバイス認証

デバイスの正当性や，メッセージの正当性の保証 (改ざん，ID 詐称の検出) ができなければならない．さらに，PN を構成する各デバイスの間で，セキュアな鍵共有方式が必要である．この時，対応する通信メディアに依存しない，即ち USIM (Universal Subscriber Identity Module) という認証用モジュールの有無に依存しない認証方式が求められる．併せて，デバイスとそれを使用するユーザとの紐付けが必要である．

- PN 管理

PN の生成，維持，解散に関する基本的運用・管理が必要である．具体的には，PN そのもののプロパティの管理 (対応サービス，セキュリティポロシー，期限など)，PN のメンバデバイスリストの管理 (デバイスの参加，脱退)，メンバデバイスのプロパティやネットワーク情報の管理が必要である．NAT 越えやモビリティを柔軟にサポートできるようデバイス間のセキュアコネクションの確立，管理を行わなければならない．

- リソース管理

各デバイスがもつコンテンツや，各デバイスが提供できるサービスの管理を行わなければならない．また，リソース単位，サービス単位 (もしくはデバイス単位) のアクセス制御を行わなければならない．

リソースやサービスの記述方式を定義し，その定義を用いたスケーラブルなリソース発見方式が必要である．このとき，既存のリソース記述方式 (Web サービスや SOA など) やリソース発見方式 (Bluetooth SDP，UPnP，SLP など) とそれぞれ連携ができることが望まれる．

- ネーミング

ユーザ，デバイスの ID を上記の各種制御が実現できるよう定義しなければならない．また，ユーザ，デバイスに対して，ユーザフレンドリな名前を付与できる仕組みが必要である．

2.4 関連研究

3GPP では，IMS (IP Multimedia Subsystems) [1] の一機能として，PNM (Personal Network Management) [2], [3] という仕様が策定されている．PNM では，IMS 対応デバイス (携帯電話) の認証情報を利用して PNM サーバと IMS 非対応 PAN デバイス間で認証を行い，PAN デバイスによる PN 構築を許可する．しかし，標準設定として USIM を具備する携帯電話が固定的に PAN のゲートウェイとなるよう設計されている．そのためシグナリングとデータ通信がともに IMS を経由することになり，PN 構築の柔軟性に欠ける．

MAGNET / MAGNET Beyond プロジェクトでは，特定のユーザ所有のデバイス同士で PN を構築するための包括的な PN アーキテクチャ [8], [10] に加えて，他のユーザ所有のデバイスまで対象を広げ，所有者の異なる複数の PN 間の相互接続を行う PN Federation 技術 [7], [11] に関する検討が進められている．また，UIA (User Information Architecture) [5]/MyNet [4] では，HIP (Host Identity Protocol) を用い，ユーザがデバイスに独自に付与する user-relative name と HIP における EID (endpoint identifier) をバインディングするネーミング方式を提案し，異なるユーザのデバイス間での PN 構築を可能としている．

MAGNET / MAGNET Beyond と UIA に共通して言えることは，認証プロセスにおいて認証基盤が脆弱なインターネットをシグナリングにも利用することを前提とするため，システムの複雑化を招いてしまっていることである．

以上のように，3GPP PNM ではシグナリングとデータ通信がともに IMS を経由し，また MAGNET / MAGNET Beyond や UIA ではそれがともにインターネットを経由することが根本的な問題となっている．提案する USCP では，シグナリングパスとデータ通信パスの分離し，シグナリングは強固なセキュリティを特徴とするオペレータ通信基盤 (IMS) に委ね，一方でデータ通信に関してはユーザ環境に応じて IMS や相対的に安価で高速なインターネットを使い分ける．すなわち，USCP は 3GPP PNM と MAGNET / MAGNET Beyond の長所を併せもつ．

また，MAGNET / MAGNET Beyond では，PN は個々のユーザの所有デバイスだけで構築される PN をベースとしてい

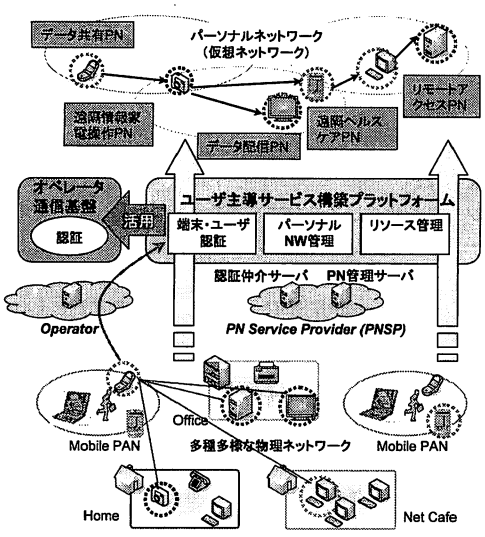

図 3 ユーザ主導サービス構築プラットフォーム (USCP)
Fig. 3 User-driven Service Creation Platform (USCP)

るため，複数のユーザ間で PN を構築する場合は，まず個々のユーザで PN を構築し，その後 PN 間を相互接続するという階層型トポロジーを構築しており，構築手順が冗長である．

それに対し，USCP でははじめから複数のユーザ間で PN を構築することを想定し，PN のネットワーク構造をフラット化している．ユーザ単位，もしくは管理ドメイン単位での PN 管理ではなく，最初からユーザや管理ドメインをまたがった構成を想定した構造にすることにより，迅速かつ少ない手順で効率的な PN 構築が可能となる．

さらに MAGNET / MAGNET Beyond では，IPsec トンネル (VPN) 構築にルータ支援を想定としている．つまり，PN を構成するデバイスが所属する両端のクラスタのエッジルータ間で IPsec トンネルを確立することにより，非力なデバイスの負荷を軽減している．しかしながら，この方式では PN の実現のためにはエッジルータに VPN 機能を追加導入する必要があり，ユーザの利便性という観点では望ましくない．USCP ではこのようなインフラ支援を必要としない．

3. ユーザ主導サービス構築プラットフォーム

本章では，ユーザ主導サービス構築プラットフォーム USCP を提案する．

3.1 要　　件

PN を実用化するためには，筆者らは USCP には下記のような要件が必要であると考えている．

(1) ユーザの負担にならない操作性，ユーザ利便性
(2) デバイス間通信の秘匿性，及びプライバシーの保護
(3) ユーザ主導で自在にサービス構築・設定ができる柔軟性
(4) デバイス間のスムーズな連携と相互接続性
(5) 対応通信メディアや機種に依存しないデバイス透過性

3.2 USCP 概要

USCP は，(1) デバイスに組み込まれる PN ソフトウェア，(2) パーソナルネットワークサービスプロバイダ (PNSP)，及び (3) オペレータ通信基盤内の PN 対応拡張認証システムの 3 つのコンポーネントから構成される．図 3 に USCP の概要を示す．

USCP では PNSP という ASP を導入する．PNSP は 認証仲介サーバと PN 管理サーバから構成される．認証仲介サーバは，PN 構築のためのユーザ認証・デバイス認証に関して，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．PN 管理サーバは PN のメンバ管理やセッション管理などの PN の基本的制御を行う．

PNSP は IMS AS (Application Server) として IMS 内の S-CSCF (Serving-CSCF) に接続されるとともに，インターネットにも接続される．PNSP が複数存在する場合は，PN 管理サーバは各 PNSP に設置され，PN 管理サーバ間で PN 管理情報の相互参照を行う（PNSP 間ローミング）．

USCP の主な利点は次の 2 つである．まず，USCP ではシグナリングパスとデータ通信パスを分離し，強固なセキュリティが要求されるユーザ認証・デバイス認証（シグナリング）には IMS / MMD を利用し，データ通信には利用可能であればインターネットなどのより高速な回線を利用する．これにより，認証プロセスの簡略化，強固なセキュリティ，データ通信の高速化を両立させる．

次に，USCP では PN の仮想ネットワークをフラット構造化（単一階層化）する．PN は単一ユーザまたは限られた数のユーザだけで構成されることが一般的であるため，階層構造の構築には手間がかかる．具体的には，ユーザ単位，もしくは管理ドメイン単位で PN 管理サーバを設置するのではなく，最初からユーザや管理ドメインをまたがった構造を想定し，デバイスやユーザの信頼性の根幹であるオペレータ通信基盤に PN 管理機能を集約する．さらに，USCP ではルータの支援を要求せず，ユーザデバイス間でダイレクトにセキュアコネクションを確立する．このようなフラット化により迅速かつ少ない手順で効率的な PN 構築が可能とする．

以上より，USCP の特徴をまとめると以下のようになる．

- 携帯電話利用によるユーザ利便性の向上
- シグナリングパスとデータ通信パスの分離
- オペレータ通信基盤による強固なユーザ・デバイス認証
- フラット構造化による PN 構築手順の簡略化
- PNSP の導入によるインフラとサービスの分離
- データ通信パスの適応的選択による高性能化
- インフラ支援を前提としないセキュアコネクション確立

3.3 PN 構成シナリオ

USCP では，PN を構成するデバイスの性質により，構成シナリオは以下のように分類できると考えられる．

- シナリオ 1: すべてのデバイスが同じユーザの所有物である場合

図 4(a) に示すように，単一ユーザが所有するデバイスのみで PN を構築する．複数のデバイスをどのように単一の携帯電話に紐付けるかが課題となる．

- 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

図 4(b) に示すように，異なるユーザが所有する複数のデバイスで PN を構築する．異なる携帯電話に紐付けられた複数のデ

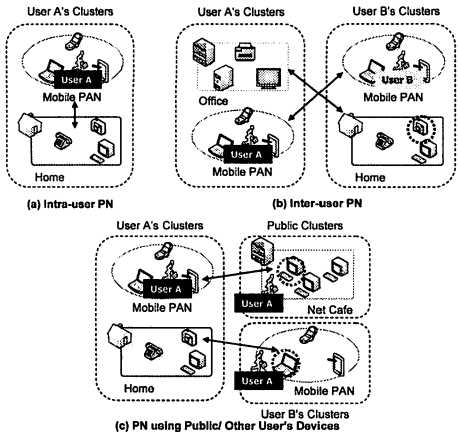

図 4　構成シナリオ
Fig. 4　Organization Scenarios

バイス間の認証が課題となる．

- シナリオ 3: 公衆デバイス，もしくは他のユーザのデバイスを利用する場合

図 4(c) に示すように，他ユーザが所有するデバイスや，ネットカフェの PC などの公衆デバイスを利用して PN を構築する．ユーザの携帯電話に紐付けられていない他ユーザデバイスや信頼性の低い公衆デバイスの認証が課題となる．

4. 基本設計

本章では，USCP の機能モデルを示し，続いて USCP の各機能ブロックについて簡単に説明する．

4.1 機能モデル

図 5 に USCP の機能モデルを示す．USCP の機能モデルは，以下の 3 つのレイヤから構成される．

- PN サービスレイヤ

サービス構築，サービス記述，コンテキスト管理，トラスト管理などの PN サービス構築のためのユーティリティを提供する．本研究ではまずは下記 2 つのレイヤの検討を優先する．

- PN 制御レイヤ　(4.2, 4.3, 4.4)

ユーザとデバイスの認証・管理，PN の生成・解散，メンバ管理，リソースの発見・管理など，PN の運用に関する基本的制御を行う．

- PN コネクションレイヤ　(4.5, 4.6)

デバイスやリソース，サービスに対するアクセス制御を行うとともに，仮想ネットワークのトポロジ，コネクション管理を行う．

4.2 ユーザ・デバイス認証機能

PN サービスを享受する権利をもつユーザの正当性を判別するためにユーザ認証を行う．PN サービスはオペレータからオプショナルサービスとしてユーザに提供されるため，ユーザ認証はオペレータ通信基盤により行われる．

また，PN にデバイスを参加させるためにデバイス認証を行う．PN では USIM をもつ IMS 対応デバイス (TE) だけでなく，USIM をもたない 非 IMS 対応デバイス (nTE) までを対象としてデバイス認証を行う．

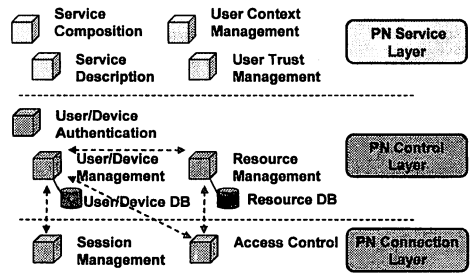

図 5　機能モデル
Fig. 5　Function Model

ユーザ認証及びデバイス認証により，IMS 対応/非対応，デバイスの所有者に依存することなく，ユーザとデバイスとの紐付け及び 2 つのデバイス間での共有鍵の生成，共有が可能となる．

筆者らは上記のデバイス認証の一実現手法として代理デバイス認証方式 [14] を提案している．具体的には，TE としてユーザが所有する携帯電話を利用し，nTE の認証処理を携帯電話が代理する．USIM 内に保持された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・登録を行うことが可能である．本機能は，PNSP 内の認証代理サーバとオペレータ通信基盤に設置される．

4.3 ユーザ・デバイス管理機能

同時に，ユーザとデバイスの名前や属性，ネットワーク情報，所属 PN リストなどのユーザプロファイル・デバイスプロファイルをデータベース (DB) として管理する．また，PN の参加デバイスリスト，サービス種別，存続期間，セキュリティポリシーなどの PN プロファイルを DB として管理する．本機能により，現在どのような PN が生成されており，その PN にどのユーザがどのデバイスを利用して参加しているかが把握される．本機能は PNSP 内の PN 管理サーバに設置される．

デバイス ID は，ヒューマンリーダブルでかつグローバルユニークなものが求められるため，例えばユーザが自由に定義するデバイス名とユーザ ID を組み合わせ，「デバイス名＠ユーザ ID」という形で表現する．代理デバイス認証方式における nTE_x の識別子 $ID_{nTE;x}$ がこれに相当する．

4.4 リソース管理機能

PN に参加するデバイスがもつリソースを，デバイス単位で管理する．本研究では，リソースを，ファイルやコンテンツ，もしくはより広義に特定のアプリケーション機能やサービス機能と定義する．アクセス権やハッシュ値などのリソース記述を定義するとともに，デバイス毎にリソースリスト（リソースインデックス）を DB として保持する．また，PN 内でのリソース検索機能を提供する．

本機能はの配置先としては，PN 管理サーバ，TE（携帯電話），nTE，ユーザドメイン内の専用サーバなどいくつか可能性が考えられ，現在検討を進めている．

4.5 アクセス制御機能

ユーザ・デバイス DB を参照し，正当性が保証されたデバイスの PN への参加，脱退を許可する．また，リソース DB を参照し，リソース DB で設定されたアクセス権に基づいて，デ

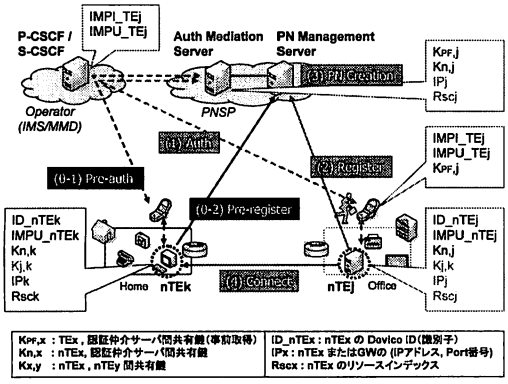

図 6 PN 構築手順
Fig. 6 PN Creation Procedure

バイス毎にリソースに対するアクセス制御を行う．本機能は PNSP 内の PN 管理サーバに設置される．

4.6 セッション制御機能

4.2 で示した共有鍵を用いてデータを暗号化することによりデバイス間のセキュアコネクションを確立する．デバイスが複数のデータ通信メディアを利用可能な場合，アプリケーション要求やネットワーク状況に応じて適切な通信メディアを選択する．3 つ以上のデバイスが PN に参加する場合，仮想ネットワークトポロジー制御を行う．本機能は PNSP 内の PN 管理サーバ及び PN デバイスに設置される．

2 つのデバイスがともに NAT の内側にいる場合は，TCP であれば UPnP (Universal Plug and Play) [13] NAT Traversal を，UDP であれば UDP ホールパンチングをそれぞれ適用することでコネクションを確立できる．最近では家庭用ブロードバンドルータの 70% 以上が UPnP に対応，90% 以上が UDP ホールパンチングが可能（STUN [12] の分類における Symmetric NAT 以外の NAT である）という統計情報もある．

5. 構築手順

本章ではユーザによる PN 構築リクエスト生成から実際に PN が構築されるまでの手順を示す．なお，ここではリソース管理（リソースポインタ管理）は PN 管理サーバで集中的に行うものとする．

図 6 に PN 構築の略式手順を示す．ここでは，2 つの非 IMS デバイス nTE_j, nTE_k で PN を構築する．

(手順 0) 前提：nTE_k は事前に手順 1,2 と同様の手順で，デバイス認証（鍵共有），リソース登録を完了していると仮定する．

(手順 1) デバイス認証：代理デバイス認証方式を用いて，nTE_j と認証仲介サーバの間で共有鍵 K_{PFj} を共有する．

(手順 2) リソース登録：nTE_j は共有鍵 K_{PFj} を用いて認証仲介サーバとの間にセキュアコネクションを確立し，認証仲介サーバ経由で PN 管理サーバにリソースインデックス Rsc_j を登録する．

(手順 3) PN 構築：nTE_j は nTE_k に接続するために PN 構築リクエストを PN 管理サーバに送信する．PN 管理サーバは，nTE_k へのアクセスに対してアクセス制御を行う．PN 管理サーバはアクセス許可後，nTE_j と nTE_k をメンバとする PN を構築し，両デバイスに共有鍵 K_{jk} と互いのデバイスプロファイルを通知する．

(手順 4) コネクション確立：nTE_j は共有鍵 K_{jk} 及び，nTE_k のデバイスプロファイルに記載されたネットワーク情報 IP_k をもとに，nTE_k との間に IPsec によるセキュアチャネルを確立する．

6. おわりに

本稿では，ユーザの接続環境（アクセスシステム，利用デバイス）及び要求するサービスに応じて，ネットワークをまたがって関連するデバイスが連携し，ユーザやユーザグループに閉じたセキュアなプライベートネットワークをユーザが動的に構築することを可能とする USCP を提案し，その基本設計について述べた．現在，USCP の詳細設計の検討を進めている．

文 献

[1] 3GPP. IP Multimedia Subsystem (IMS); Stage 2. *3GPP TS 23.228 V8.4.0 (2008-03).*

[2] 3GPP. Personal Network Management (PNM); Procedures and Information Flows; Stage 2. *3GPP TS 23.259 V8.0.0 (2008-03).*

[3] 3GPP. Service requirements for Personal Network Management (PNM); Stage 1. *3GPP TS 22.259 V8.4.0 (2007-12).*

[4] Z. Antoniou and D. Kalofonos. MyNet: a Platform for Secure P2P Personal and Social Networking Services. *Proc. PerCom'08*, Mar. 2008.

[5] B. Ford, J. Strauss, C. Lesniewski-Laas, S. Rhea, F. Kaashoek, and R. Morris. Persistent Personal Names for Globally Connected Mobile Devices. *Proc. OSDI'06*, Nov. 2006.

[6] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, and A. Malis. A Framework for IP Based Virtual Private Networks. *IETF RFC 2764*, Feb. 2000.

[7] J. Hoebeke, G. Holderbeke, I. Moerman, M. Jacobsson, V. Prasad, N. C. Wangi, I. Niemegeers, and S. H. de Groot. Personal Network Federations. *Proc. 15th IST Mobile and Wireless Communications Summit*, June 2006.

[8] M. Jacobsson, J. Hoebeke, S. H. de Groot, A. Lo, I. Moerman, I. Niemegeers, L. Munoz, M. Alution, W. Louati, and D. Zeghlache. A Network Architecture for Personal Networks. *Proc. 14th IST Mobile and Wireless Communications Summit*, June 2005.

[9] A. Lo, W. Lu, M. Jacobsson, R. V. Prasad, and I. Niemegeers. Personal Networks: An Overlay Architecture for 4G Mobile Communication Networks. *Teletronikk Journal*, 16(1):045–058, 2007.

[10] R. Prasad and K. E. Skouby. Personal Network (PN) Applications. *Wireless Personal Communications*, 33(3/4):227–242, June 2005.

[11] R. V. Prasad, M. Jacobsson, S. H. de Groot, A. Lo, and I. Niemegeers. Architectures for intra-personal network communication. *Proc. WMASH'05*, 2005.

[12] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy. STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). *IETF RFC 3489*, Mar. 2003.

[13] UPnP Forum. http://www.upnp.org/.

[14] 松中隆志, 蕨野貴之, 岸洋司, 中内清秀, ベドカフレ, and 井上真杉. 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. **信学技報** *MoMuC2008-2*, May 2008.