個人識別符号に IPv6 アドレスを使用するシステムの提案

菅野信†，　大橋秀樹†，　森英悟†

様々な知的デバイスがネットワークを通じて結合される、いわゆるユビキタスコンピューティングを実現する基盤技術として IPv6 が浸透しつつあり、IPv6 対応の家電製品などが各メーカから発表されている。ユビキタスコンピューティングにおいてユーザを識別するユーザ情報は重要なコンテキスト情報の一つであり、各デバイスはユーザ情報を簡潔かつ的確に知る必要がある。我々はユビキタスコンピューティングにおけるユーザ識別の手法として IPv6 アドレスを直接使用する方法を提案する。本稿では提案手法の詳細を説明し、実際に提案手法を用いて構築したシステム上で行った実証実験の結果を報告する。

A proposal of a system where IPv6 address is used as the user identification symbol

Makoto Sugano†, Hideki Ohhashi†, Eigo Mori†

In ubiquitous environment, various kinds of intelligent devices will be connected to network and IPv6 is expected to support the communications among them. Based on this background, some home electronic appliances, which are capable of IPv6 networking, have started to appear. These intelligent devices are supposed to know user information since it is one of the most important contexts in ubiquitous computing. We have developed a system where IPv6 address is used as the user identification symbol and confirmed that the authentication application on the system can easily be developed.

1. はじめに

ユビキタスな世界（[1]）においては、様様な知的デバイスがネットワークにつながる必要があり、IPv6 はその通信を支える技術として期待されている （[2]）。IPv6 技術の膨大なアドレス空間を利用して個々のデバイスにアドレッシングが可能となり、peer to peer コミュニケーションが容易に実現できるためである。事実この流れに沿った IPv6 対応の家電、デバイスが各社から発表されはじめている。2003 年の Interop では IPv6 対応のエアコンおよび電子レンジが展示され、おおいに注目を集めた（[3] ）。

これらのデバイスは無条件に単調な作業を繰り返せば良いわけではなく、その時々における状況を理解した上でコンテキストアウェアなサービス（[4]）をユーザに提供する必要がある。例えば、上記のエアコンは在室する人が誰であるかを特定して、その個人に応じた温度設定を行うことが好ましい。個人識別情報は重要なコンテキストの一つであり、ユビキ

† ノキア・ジャパン株式会社　ノキア・リサーチセンター
100-0014 東京都千代田区永田町 2-13-5 赤坂エイトワンビル 6F
Nokia Research Center, Nokia Japan Co., Ltd.
2-13-5, Nagata-cho, Chiyoda-ku, Tokyo 100-0014, Japan
E-mail: {makoto.sugano, hideki.ohhashi, eigo.mori}@nokia.com

タスなデバイスはこの情報を簡潔かつ的確に知る必要がある。
UNIX に代表される多くのオペレーティングシステムではユーザ ID を個人の識別符号として使用している。ユーザは UID をキーボードでタイプし、システムはこの情報をもとに個人識別を行い、各ユーザに応じた作業環境を提供する。一方で同じコンピュータ上で利用するアプリケーションサービス、例えばオンラインショッピングでは別のユーザ ID を使うのが一般的であり、個人識別符号の書式および手法は統一されていない。現状では、プラットフォームやアプリケーションごとに個人識別符号を用意する必要性があり、認証アプリケーション開発の効率化を妨げている。

2. 個人識別符号に IPV6 アドレスを使用するシステムの提案

我々は以下の理由から IPv6 が個人識別のメソッドとしてのポテンシャルを持つと考え、個人識別符号に IPv6 アドレスを使用するシステム（図 1）を提案する。

- IPv6 は巨大なアドレス空間を擁し、各個人に対する ID の付与が可能である。
- 既存の IPv6 技術を個人識別に応用することにより、個人認証作業の共通化が可能となる。

今回我々が提案するシステム上のユーザ認証アプリケーションは、個人識別符号に IPv6 アドレスを使用する。そのため、認証アプリケーション開発時には独自の認証メカニズムを用意する必要がなく、開発の効率化が期待される。システムの詳細を次章で紹介する。

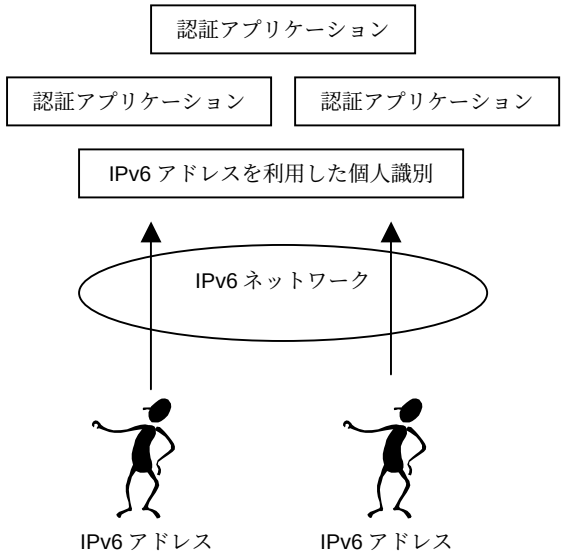

図 1: 提案システム

3. 個人識別符号に IPV6 を利用するシステムの実装

3.1 概要

本システム（図 2）では、個人の識別手法として、通常のIPv6の拡張版であるモバイルIPv6を利用する。以下に述べるように、モバイルIPv6を利用することによってネットワークを選ばず同じアドレスを使いつづけることができるからである。また、セキュリティ確保のためにはIPv6に付随するIPSecを利用する。
本システムでは、個人の識別に、端末本体とは別に個々のユーザが持ちうる外部アクセスキーを使用する。実験においては、ユーザの利便性を高めるために、その外部アクセスキーとして、RFID技術を利用した。この個人識別符号として利用するIPv6アドレスおよびセキュリティキーをRFIDタグに埋め込み、人間がそのタグを持ち運ぶことを想定する。
システムにおけるクライアント端末は、個人の所有する RFID タグから IPv6 アドレスおよび、セキュリティキーを取得する。クライアント端末はこの情報をもとに自身のネットワークの設定を行った後

に、他のノードに接続要求を行う。接続要求を受けたノードは、クライアント端末の IPv6 アドレスより個人識別を行う。

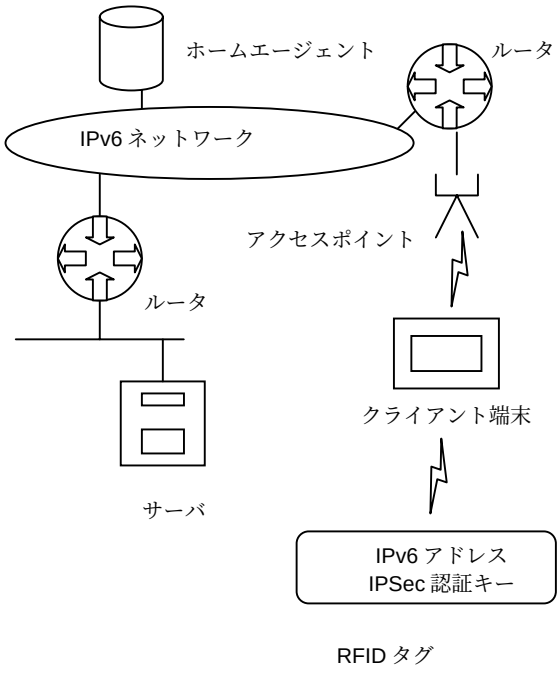

図 2: システムの概要

以下に要素技術として使用されるモバイル IPv6、IPSec および RFID の概要を示す。

3.1.1 モバイル IPv6

モバイル IPv6 は、モバイル機能をサポートするための IPv6 を拡張するプロトコルで、あり、the Internet Engineering Task Force （IETF） の中のモバイル IP Working Group で、開発が進められている。通常の IPv6 において、あるノードが異なるネットワークに移動した場合、ネットワークアドレスの変更に対応できず、同じアドレスを使いつづけることができない。モバイル IPv6 では、ホームアドレス、ケアオブアドレスおよびアドレス対応表を使って、この問題を解決し、ノードは同じアドレスを複数のネットワーク間で使いつづけることが可能となる。
そもそもモバイル IPv6 では IP 携帯電話のように、等しいハードウェアが複数のネットワークをまたいで移動することを念頭においている。本システムでは、個人がどのネットワークに移動しても、同じアドレスを使い続ける必要があり、この機能を実現するためにモバイル IPv6 を利用した。
モバイル IPv6 は、現在、ドラフトの段階であり、本開発時は、バージョン 15 をもとにその実装を行った。

3.1.2 IPSec

IPSec とは、インターネット上で、一般に広く柔軟に、安全な IP 通信を可能とするように設計された一連のプロトコルであり、the Internet Engineering Task Force （IETF） の中の IP security Working Group で、開発が進められている。IPSec を利用することにより、IP を利用する全てのアプリケーションにおいて、機密性の確保、完全性の確保、送信元の認証 が可能となる。
本システムにおいては以下の観点からある一定のセキュリティの確保を目指した。

- サーバは接続元アドレスをもとに個人識別を行っているため、なりすましを防ぐ認証メカニズムが必要である。
- サーバ、クライアント間通信の機密性を保証する必要がある。

セキュリティのためのプロトコルにはいくつかの選択肢があるが、本研究においては、システムに高い移植性を求め、**IPv6** に付随する **IPSec** を使用した。
モバイル IPv6 と IPSec の同時利用に関しては、問題（[5]）が報告されており、未だ解決に至っていない。我々はプロトコルの最終的な実装は標準化を待つことにし、IPSec の AH および、プリシェアードキー方式を使用してシステムを構築した。

3.1.3 RFID

RFID（Radio Frequency Identification）とは、電子データを RF タグの中に保存し、RF タグに、RF リーダー装置から非接触で電力を供給すると同時に、RF タグと RF リーダーとの間でデータの交換を行う

技術のことである。この非接触の電力供給とデータ交換は、磁界、電磁界、マイクロ波を用いて行われる。RFID は磁気テープのクレジットカードなどに比べ、汚れなどに強く、また、多くの情報をいれることができる。メモリや小型のプロセッサを搭載したものもあり、多機能でありながら、電池などによる電力供給が必要ない。
本システムにおいては、なるべく人間が意識しないまま IPv6 のアドレスを持ち運ぶ必要があり、上記の特徴をもつ RFID の中でも標準化されていて、容易に入手可能な ISO15693 準拠のもの使用する。

3.2 実装

個人識別符号に IPv6 アドレスを使用するシステム（図 2）にはクライアント、サーバ、ホームエージェントおよびルータが存在する。以下にそれぞれの実装手法について述べる。

3.2.1 クライアント

モバイル性を考慮した結果、クライアントのハードウェアとして、当ノキア・リサーチセンターで開発された携帯端末を利用した。端末のハードウェアの仕様を表 1に示す。本端末は、IEEE802.11b 準拠の無線 LAN 機能及び、RFID リーダーを併せもつことを特徴とする。RFID リーダー機能によって、外部にある RFID タグに書き込まれた情報へのアクセスが可能となる。
クライアントの、ソフトウェアの仕様を表 2に示す。開発の容易さを検討した結果、クライアントには、オペレーティングシステムにオープンソースである Linux の 2.4.18 版を採用した。モバイル IPv6 および IPSec プロトコルを実装しており、無線 LAN を通して、IPv6 を基盤とするインターネットへのアクセスが可能である。
なお、クライアントには後述の HTTP アプリケーションに必要となる、WEB ブラウザを搭載している。

これらの機能を併せ持つことにより、本端末は RFID タグから IPv6 アドレスおよび IPSec の認証キーを取得し、使用される RFID タグ毎に異なったネットワーク設定で、無線 LAN を介したネットワークアクセスを行う。
クライアント端末および RFID のタグの外観を図 3に示す。

表 1: クライアント端末ハードウェア

機能	説明
PC カード	Type II x 1 スロット （無線 LAN カードに使用）
RFID	RFID リーダー（ISO15693 標準、周波数 13.56MHz）
電源	ＡＣアダプタまたは内部バッテリー
サイズ	141mm（W）x 80mm（D）x 41mm（H）

表 2: クライアント端末ソフトウェア

機能	説明
OS	Linux 2.4.18
ネットワークプロトコル	モバイル IPv6 および IPSec
主なアプリケーション	WEB ブラウザ

図 3: クライアント端末および RFID タグの外観

端末における RFID タグの処理手順を以下のフローチャートを示す。（図 4）

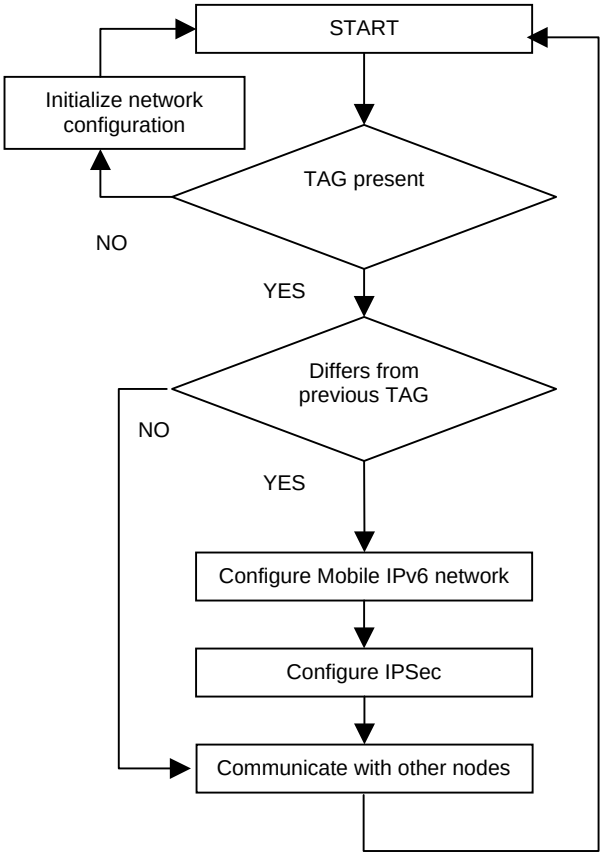

図 4: 端末における RFID タグ処理

クライアント端末は周期的に、RFID タグが端末の側にあるかを確認する。RFID タグが存在した際、そのタグが前回認識したものと同じかどうかを確認する。異なる場合には、まず、タグからネットワーク情報（モバイル IPv6 のホームアドレスおよび IPSec 用途の共有鍵）を取得する。次に、得られたアドレスを用いて、新たに端末におけるネットワークの設定を行う。引き続き、IPSec の設定を行い、ネットワークへのアクセスを開始する。同じタグを利用し続ける際には、ネットワークの再設定は行われない。

3.2.2 サーバ

サーバではモビリティーを要求しない設定とし、ハードウェアは汎用的な PC を利用した。ソフトウェアの仕様を表 3に示す。

クライアント端末と同様の理由でオープンソースである Linux の 2.4.18 版を採用した。サーバも端末と同様にモバイル IPv6 および IPSec プロトコルを実装しており、有線ケーブルを通して、IPv6 を基盤とするインターネットへのアクセスが可能である。また、サーバには後述の HTTP アプリケーションに必要となる、HTTP サーバを搭載している。

表 3: サーバＰＣソフトウェア

機能	説明
OS	Linux 2.4.18
ネットワークプロトコル	モバイル IPv6 および IPSec
主なアプリケーション	HTTP サーバ

サーバにおける端末の認証過程を図 5を示す。

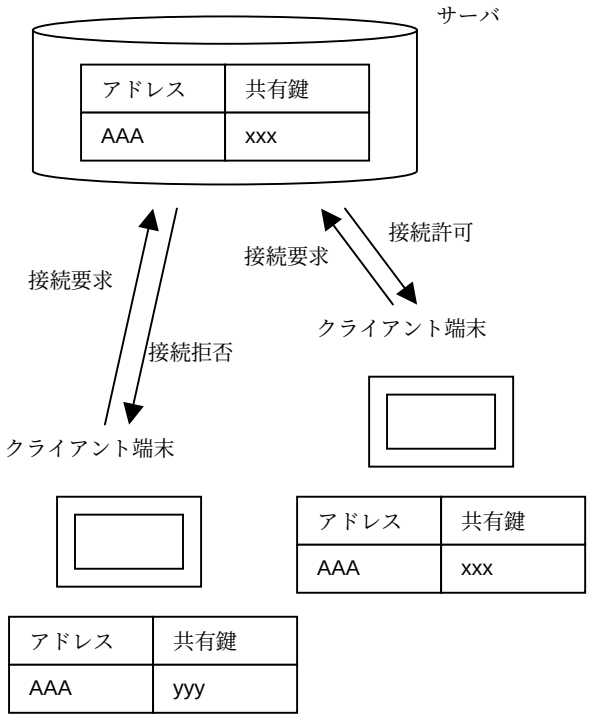

図 5: サーバにおける個人認識処理

サーバは事前にクライアント端末の IPv6 アドレスとそれに対応する IPSec 共有鍵を持つ。クライアント端末からのアクセ

ス要求があると、この情報を利用してクライアント端末の認証を行う。

3.2.3 ホームエージェントおよびルータ

ホームエージェントおよびルータではサーバ同様モビリティーを要求しない設定とし、ハードウェアは汎用的な PC を利用した。
ソフトウェアの仕様を表 4に示す。クライアント端末と同様の理由でオープンソースである Linux の 2.4.18 版を採用した。これら中間ノードでは IPSec を利用しないため、モバイル IPv6 のみを実装した。

表 4: ホームエージェントおよびルータソフトウェア

機能	説明
OS	Linux 2.4.18
ネットワークプロトコル	モバイル IPv6

3.3 HTTP アプリケーション

本システムをベースに HTTP を利用した認証アプリケーションを開発した。以下にその概要を述べる。
サーバサイドでは接続要求を行うクライアントの IPv6 アドレスによってサービスを決定する。図 6のサーバは、あらかじめクライアント端末の IP アドレスとコンテンツの対応表を持つ。サーバに用意された CGI はクライアント端末の IPv6 アドレスを確認した後、しかるべき HTML をクライアント端末に送信する。

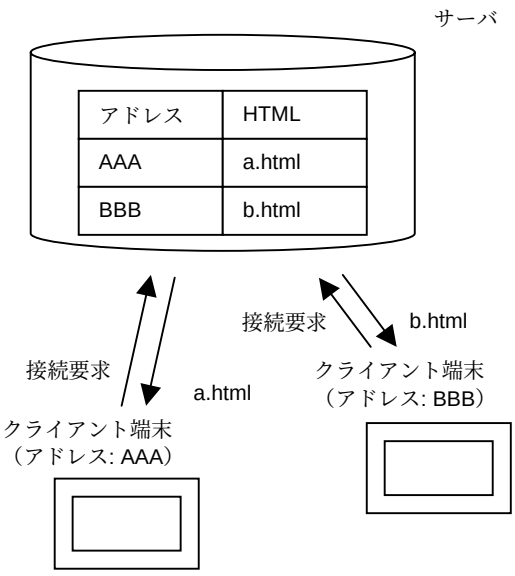

図 6: HTTP アプリケーション

3.4 評価

IPv6 アドレスを個人識別符号として利用した結果、認証アプリケーション開発において次に挙げる改善が見られた。

- 本システム上の認証アプリケーションは既存の IPv6 プロトコルを認証作業に利用するため、アプリケーション毎の認証手法を開発する必要がなくなった。

- 本システム上の認証アプリケーションは接続要求を行うノードの IPv6 アドレスをもとに個人識別行うため、クライアントに対して個人識別符号の送信を明示的に要求する必要がなくなった。

3.5 応用

個人情報をコンテキストとして使用するユビキタスシステムとしては BAT システム（[6]）が存在する。このシステムでは室内における個人やデバイスの位置はリアルタイムにトラックされ、アプリケーションはこれらの位置情報を利用する。例えば、自分にかけられた電話は、自分にとって一番身近な電話端末に転送される。しかしながら、正確な位置情報を取

得するシステム構築は非常にコスト高であるため、本システムを上記のようなアプリケーションの基盤技術として利用できるのではないかと期待している。

4. おわりに

4.1 まとめ

本稿では個人識別符号に IPv6 を使用するシステムを提案し、実際にそのシステムを構築して行った実証実験の結果を報告した。実証実験によってモバイル IPv6 および IPSec という既存のプロトコルを利用して、容易に個人識別が可能であることを示すことができた。

4.2 今後の課題

ユビキタス環境が熟成するにつれ、複数のデバイスが協調してユーザにサービスを提供するアプリケーションの登場が予想される。
一方、現状の提案システムではユーザが特定のデバイスに自らを同定するための IPv6 アドレスを与え、そのデバイスを「自分の代理」として使用するため、複数デバイスの協調アプリケーションを実現することは困難である。今後、こうした協調アプリケーションに対応するためのメカニズムを考案し、提案システムに実装することを計画している。

4.3 謝辞

本研究は NTT コミュニケーションズ株式会社と共同で行われたものであり、ここに感謝の意を表します。

参考文献

[1] M. Weiser; “The computer for the 21st century”, Scientific American, vol. 265, no. 3, Sept. 1991, pp. 94-104

[2] Lee, D.C., Lough, D.L., “The Internet Protocol version 6 Potentials”, IEEE, Volume: 17 Issue: 2, April-May 1998 Page（s）: 11 –12

[3] http://www.zdnet.co.jp/broadband/0307/04/lp15.HTML

[4] Schilit, B, Adams, N., Want, R., “Context-aware computing applications”, Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on , 8-9 Dec. 1994 Page(s): 85 -90

[5] **湧川隆次**, **植原啓介**, **村井純**, "**移動体通信プロトコル** Mobile IPv6 **の実装および評価** ", **インターネットコンファレンス** 2000 **論文集**, pp.95--pp.102, Nov2000

[6] Andy Harter, Andy Hopper, Pete Steggles, Andy Ward, Paul Webster, “The Anatomy of a Context-Aware Application”, Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, MOBICOM'99, Seattle, Washington, USA, August 1999, pp. 59-68.