

## ユビキタス環境におけるネットワーク資源提供モデルの提案

和泉 順子<sup>†</sup> 森島 直人<sup>††</sup> 砂原 秀樹<sup>†††</sup>

† 奈良先端科学技術大学院大学 情報科学研究科 〒630-0192 奈良県生駒市高山町 8916-5  
†† 奈良先端科学技術大学院大学 附属図書館研究開発室 〒630-0192 奈良県生駒市高山町 8916-5  
††† 奈良先端科学技術大学院大学 情報科学センター 〒630-0192 奈良県生駒市高山町 8916-5  
E-mail: †michi-i@is.aist-nara.ac.jp, ††naoto@dl.aist-nara.ac.jp, †††suna@itc.aist-nara.ac.jp

あらまし 移動体通信環境の普及と整備により、空間を限定することなく通信に連続性を与えるための技術がさかんに研究開発されている。しかし、これらの技術は主に IP 層における通信の連続性を確保するためのものであり、利用者の認証やアカウントおよびアクセスの管理に基づいたサービスの連続性に関してはあまり議論されていない。そのため、管理形態や運用ポリシーの異なるサービスドメイン間を移動すると、インターネットへの接続性が断たれたり資源が利用できなくなったりする可能性がある。したがって本研究では、現状の問題点を抽出・分類し、その要求項目について議論した上で、ユビキタスコンピューティング環境におけるネットワーク資源提供モデルを提案する。このモデルは、公開鍵暗号基盤のクライアント証明書などの個人識別情報や一時属性証明書を用いることを検討しており、外部で定義されたエンティティを移動先（内部）の資源へのアクセス制御や権限などにマッピングすることで柔軟なネットワーク資源提供を行う特徴を持つ。

キーワード ユビキタスコンピューティング, ネットワーク資源, 本人認証

## A Proposal of providing model for network resources over the ubiquitous environment

Michiko IZUMI<sup>†</sup>, Naoto MORISHIMA<sup>††</sup>, and Hideki SUNAHARA<sup>†††</sup>

† Graduate School of Information Science, Nara Institute of Science and Technology, Japan 8916-5,  
Takayama-cho, Ikoma, Nara, 630-0192, Japan  
†† Digital Library R&D Division, Nara Institute of Science and Technology, Jalan 8916-5,  
Takayama-cho, Ikoma, Nara, 630-0192, Japan  
††† Information Technology Center, Nara Institute of Science and Technology, Jalan 8916-5,  
Takayama-cho, Ikoma, Nara, 630-0192, Japan  
E-mail: †michi-i@is.aist-nara.ac.jp, ††naoto@dl.aist-nara.ac.jp, †††suna@itc.aist-nara.ac.jp

**Abstract** With the rapidly evolution of computing and wireless technologies, there are a variety patterns of the way to connect to the Internet. Mobile users will be able to access the Internet via multiple wireless networks and they will also have to choose pricing options, routes on the Internet, QoS, and security levels. In this paper, we proposed a resource providing model based on some certificates brought with users over the ubiquitous environment. This model has intended to design to adapt to user preference seamlessly, in which network protocols, service, and applications are integrated to provide the optimal solution.

**Key words** Ubiquitous computing, Network resources, Service access right granting, Authentication

### 1. はじめに

#### 1.1 情報通信基盤とモバイルコンピューティング

近年、計算機の小型化、軽量化、高機能化と低価格化にともなう多様な場所への計算機の導入により、情報の電子化が進んで

きた。その電子化された情報を流通させるための情報通信基盤としてインターネットが爆発的に普及し、現在では、学術機関や軍事施設での情報のやりとりだけでなく、社会的、または行政的なサービスを支えるようになった。行政サービスのオンライン化、電子政府に関する議論だけでなく、NTTグループによる

B フレッツのような光通信による FTTH(Fiber to the Home) 高速常時接続のサービスが提供されるようになり、家庭でもオンラインバンキングやチケット予約、オークションなどの様なサービスが利用可能となった。このように、インターネットは一般生活にも広く利用されるようになり、社会基盤として認知されつつある。

また、携帯電話網を利用したローミングサービスや IEEE802.11b/a/g 企画<sup>(注1)</sup>による無線 LAN 技術、Bluetooth<sup>(注2)</sup>、DSRC (Dedicated Short Range Communications: 狭域無線通信) や RFID (Radio Frequency IDentification: 無線周波数による非接触自動識別) タグなどの無線通信技術の発展により、利用者が「計算機を持ち歩くモバイルコンピューティング」が普及し、環境の構築と整備・普及が行われてきた。カフェや駅構内などからインターネットへの接続性を提供する HotSpot サービスや情報コンセントシステム [10] などの環境構築と普及が進み、利用者が携帯電話や PDA、ノート PC などのモバイル端末を持ち歩くことによって、どこにいてもインターネット上のサービスが利用可能な仕組みが実現しつつある。これらのサービスにより、会社や大学や家庭などの固定点だけでなく、移動先や移動中でもインターネット上のサービスを利用する機会が飛躍的に拡大した。このように、インターネットが社会・行政サービス提供側から社会的な通信情報基盤として認識されているだけでなく、そのサービスを利用する一般の人にも広く求められた結果、インターネット上のサービスに対するモバイルコンピューティングを利用したサービスに関する市場が拡大していると云える。

### 1.2 ユビキタスコンピューティング環境へのシフト

現在では、これらの無線技術の発達とインターネット上で提供されるサービスの拡充、計算機資源の遍在化に伴い、ネットワークに接続された遍在する計算機を利用するユビキタスコンピューティングの環境構築に関する研究開発および議論がされつつある。

モバイルおよびユビキタスコンピューティング環境の構築に対する技術的要請の一部として、空間を限定することなく通信に連続性を与えるための MoileIP [14] や MANET(Mobile Ad-hoc Networks) [15] などの技術がさかんに研究されてきた。しかし、これらの技術は主に IP 層における通信の連続性を確保するためのものであり、利用者の認証やアカウントおよび資源へのアクセス制御に基づいたサービスの連続性に関してはほとんど議論されていない。そのため、管理形態や運用ポリシーの異なるサービスドメイン間を移動すると、サービス、あるいは、通信自体の連続性が失われる可能性がある。

また、ブローブ情報システムのような新しいサービスモデルの発現と共に顕在化した、サービス利用者や情報発信者の個人情報保護や場所や時間などの動的に変化する実空間情報の正当性や完全性の保証といった問題についても、議論の余地が残されている。

### 1.3 研究の位置づけ

以上の点を考慮して、本稿では、ユビキタスコンピューティング環境におけるネットワーク資源提供モデルを提案する。このモデルは、公開鍵暗号基盤のクライアント証明書などの個人識別情報や一時属性証明書を基盤に構築されており、外部で定義されたエンティティを移動先(内部)の資源へのアクセス制御や権限などにマッピングすることで柔軟なネットワーク資源提供を行う。

ネットワーク資源とは、インターネットへの接続性を提供するための情報や各サービスドメイン内で管理されているサービス機器などを指す。普段利用していない場所に移動した場合でもインターネットへの接続性が提供される場合は、IMAP [12], [13] や VNC(Virtual Network Computing) [8], VPN(Virtual Private Network) [9], PPPoE(Point-to-Point Protocol over Ethernet) [16] などの技術を用いることで、日常利用している環境へのアクセスやある程度の再現が可能となると考える。

従来インターネット接続性の提供は、事前のアカウント登録とそれに対応するアクセス制御に依存しているが、ユビキタスコンピューティング環境では、事前のアカウント登録・削除などの運用管理コストが増加する。また、動的に変化する利用者の特性や実空間の情報を反映させることができないため、運用ポリシーに即した形での柔軟サービス提供や対応を行うことが困難である。したがって、本提案では、公開鍵暗号基盤で利用されているクライアント証明書や属性証明書をを用いた認証とアカウント管理およびアクセス制御技術に着目した。外部でエンティティを定義することができるクライアント証明書をを用いた個人認証技術と、内部でのアクセス制御や権限委譲を表現できる属性証明書をを用い、エンティティと資源の利用権限とのマッピングを行うことで、サービスドメイン内外を移動しながらシームレスにサービスを利用するユビキタス環境において、サービス提供側の運用ポリシーに沿った段階的かつ動的なサービスが選択可能になると考える。

まず、第2章では、移動を前提としていない既存のインターネットからユビキタスコンピューティング環境構築への移行の際に問題となる点を具体的な例を用いて議論し、整理する。第3章では、2章で議論した問題を解決するための機能要件をまとめ、サービスモデルを提案し、その概要をのべる。第4章では、このモデルに即したシステムを設計するにあたり、実運用の際に必要なシステムの評価項目について検討し、議論する。最後に、今後の研究の方向性を述べ、研究のまとめを行う。

## 2. ユビキタスコンピューティング環境への移行に際した問題点の整理

既存のインターネットの構造や設計は、利用者や計算機の移動を前提としていない。したがって、ユビキタスコンピューティング環境を利用したサービスを検討する際に、通信およびサービスの連続性と、新しいサービスモデルへの対応において問題が生じる。本章では、これらの問題を議論するために、通信およびサービスの連続性に注目し、モバイルコンピューティング環境のための代表的なサービスおよび既存技術を二つ挙げ、それ

(注1) : <http://www.ieee.org/wireless/>

(注2) : <http://www.bluetooth.com/>

それぞれについて利点と欠点をまとめる。また、プローブ情報システムのような新しいサービスモデルへの対応についても触れ、ユビキタスコンピューティング環境の構築の際に検討する必要のある問題点について整理する。

## 2.1 通信およびサービスの連続性

現在のモバイルコンピューティング環境利用のための代表的なサービスおよび既存技術として、以下の二つを例に挙げることができる。

- (1) 携帯電話網を用いたローミングサービス
- (2) IEEE802.11b などの無線 LAN を利用した情報コンセントシステム

### 2.1.1 携帯電話網を用いたローミングサービス

日本通信株式会社による高速 PHS データ通信サービスの b モバイル<sup>(注3)</sup>や DDI ポケット株式会社による AirH<sup>(注4)</sup>、株式会社 NTT ドコモによる @FreeD<sup>(注5)</sup> のように、既存携帯電話網を用い、特定アクセスポイントへ接続することによるインターネットへの接続性提供サービスは既に実現している。これらのサービスでは、携帯電話網のローミングを用いた連続的な通信の提供を行うことができる。また、特定アクセスポイントに接続してインターネット上のサービスを利用するため、移動先サービスドメインの運用およびセキュリティポリシーに依存または影響しない。つまり、携帯電話の電波が入るところであればいつでもどこでも使えるサービスであるといえる。しかし、ユビキタスコンピューティング環境での利用を考えると、以下のような制限や問題点が含まれている。

- 移動先の資源利用に対する制限
- 移動中は電波強度が変化するため不安定
- 有線/無線 LAN 接続と比較して、狭帯域、高遅延
- 通信コストが割高

つまり、携帯電話網を用いた接続サービスは、場所に依存することなく利用可能であるが狭帯域高遅延であり、サービスが限定される場合が多い、と云うことができる。

### 2.1.2 無線 LAN を利用した情報コンセントシステム

IEEE802.11b 規格などの無線 LAN 環境を利用した HotSpot サービスや公衆端末からのインターネットへの接続性を提供する情報コンセントシステムでは、通信コストや通信帯域の面では快適に利用可能であると云える。しかし、

- 運用およびセキュリティポリシーに強く依存する
  - 事前のアカウント登録と、ポリシー管理が必要
  - サービスが点在しており、連続性が保たれない
  - 有線接続に比べて盗聴などの可能性は高い
  - 用意されている計算機やネットワークの信頼性が保証されない
  - Cookies やプロキシなどの利用時に個人情報としての足跡が残る
- などの問題点が挙げられる。

つまり、無線 LAN 環境や情報コンセントシステムの利用は利用場所に依存するため、「点 (Spot)」としてのサービスは快適に提供されるが、その場でのポリシーに強く依存するため、移動した先々で同一サービスを連続して利用することができない。また、提供された計算機やネットワークの安全性に関しても問題が残る、と云える。

以上より、携帯電話網を用いたモバイル端末用のインターネット接続サービスや、無線 LAN を利用した情報コンセントシステムでは、以下のような制限や問題が独立または複合的に生じるため、利便性が損なわれていると云える。

- 通信コストや帯域、遅延に対する利用要求が満たせない
- インターネットへの接続性の提供が携帯電話網の電波範囲内に限定される
- 物理的に近い位置にある資源でも、運用ポリシーの異なるドメインで管理されているものは利用できない
- 特定の範囲内 (Spot) に限定したサービス
- 利用者に対する認証情報の互換性がない

これにより、利用者は地下や電波強度の弱い場所ではインターネットへの接続性が断たれる、移動先の運用ポリシーに沿って管理されているプリンタが利用できない、Spot から移動した場合に連続したサービスが受けられない、移動するごとに認証やアクセス制御処理が繰り返される、ゲストアカウント取得などの事前処理がなければ資源を利用できない、などの不便を強いられることになる。

このように、ユビキタスコンピューティングやモバイルコンピューティングという移動体通信環境は、計算機が遍在し、利用者が移動することを前提としているため、異なるサービスドメイン間での連携や協調などを考慮していない既存のインターネット構築技術や運用では対応困難になってきている。

また、物理的な位置情報や時刻など、利用状態や状況などの情報が動的に変化する場合にも、各サービスドメインのセキュリティポリシーや運用ポリシーに沿った柔軟なサービスの提供を行うためには、インターネット上の分散システムの構築と運用に関して、従来の手法に囚われない新しい概念が必要となる。

## 2.2 新しいサービスモデルへの対応

ユビキタスコンピューティング環境では、プローブ情報システム [7] や AutoID センター [11] のなどの応用アプリケーションやフレームワークの構築に関して研究開発が進んでおり、新しいサービスの提供モデルが発現しつつある。このようなサービスでは、移動する計算機やセンサが情報発信を行い、インターネット上で情報が有機的に集約・加工され、有用なサービスとして提供される。つまり、情報提供者とサービス提供者 (情報加工者) が異なっている。これに特有の問題として、情報発信時は、本当にその場所から、その人によって送信された情報かどうかを保証および検証不可能であることが挙げられる。つまり、従来の情報送信技術だけでは、実空間に依存する動的な情報の正当性を検証または保証することができないため、この問題に対する対応が求められる。

(注3) : <http://www.j-com.co.jp/prepaid/>

(注4) : <http://www.ddipocket.co.jp/ps/service/airh/index.html>

(注5) : <http://www.at-freed.com/fla.html>

## 2.3 問題点の整理

以上より、ユビキタスコンピューティングへの環境構築と移行を行う場合、以下の項目に対する検討が必要になる。

### ● 通信の連続性

通信メディアを複合的に利用する等の安定性向上

### ● サービスの連続性と利用者の利便性

組織内の運用ポリシーに沿ったサービス提供の必要性和  
利用者の利便性

### ● 受発信情報の正当性の証明と機密性および完全性の保証

新しいサービスモデルへの対応

### ● 情報発信者/利用者の個人情報の保護

- 個人情報をどこで蓄積、利用するか
- 個人情報の受発信における正当性の証明および機密性、完全性の保証

つまり、場所や時間に依存することなくインターネットへの接続性やローカルな資源の利用などのサービスを利用する場合、利用者は複数の通信メディアを用いることが可能であり、かつ、その利用者に対して、移動先の組織での運用ポリシーが的確に反映された資源へのアクセス制限および権利の委譲が行われる仕組みが必要となると云える。また、通進路の安全性や、個人情報の蓄積および開示場所について慎重に検討する必要がある。

これらの問題を解決するために、本研究では、ユビキタスコンピューティング環境におけるネットワーク資源提供モデルとして、公開鍵暗号基盤におけるクライアント証明書および一時属性証明書を用いることで、移動先のサービス提供組織内の運用ポリシーを反映させた適切なサービスを利用者に提供する仕組みを提案する。特に、外部空間で定義されたエンティティが内部空間のサービスを利用する権利をどのように付与するか、という点について検討し、実際のシステムを設計のための議論を行う。

## 3. ネットワーク資源提供モデルの提案

ここでは前章の問題提起を受け、ユビキタスコンピューティング環境におけるネットワーク資源提供モデルのための機能要件を整理する。また、これらの機能要件を満たすモデルとしてシステムの構成要素とその特性を概説し、提案モデルから設計できるシステムアーキテクチャについて述べる。

### 3.1 ネットワーク資源提供モデルの機能要件

前述の問題点抽出により、検討項目を以下の4つに分類し、それぞれについてユビキタスコンピューティング環境におけるネットワーク資源提供モデルが満たすべき機能要件を述べる。

- 通信の連続性
- サービスの連続性と利用者の利便性
- 受発信する情報の正当性の証明と機密性および完全性の保証
- 情報発信者/利用者の個人情報の保護

### 3.1.1 通信の連続性

移動を前提とした環境で、通信コストや通信帯域、遅延、異なるサービスドメイン間での通信のローミングの問題をすべて解決する通信メディアは存在しない。したがって、通信とサービスの連続性を保つためには通信メディアの複合的な利用、つまり、通信メディアの切り替え[17]や同時利用をする必要がある。利用する通信メディアが変更された場合にも通信の移動透過性は保証される必要がある。

### 3.1.2 サービスの連続性と利用者の利便性

移動によりサービスドメインが変更された場合や通信メディアを切り替えた瞬間も、サービス断が起きない仕組みが必要となる。また、ユビキタスコンピューティング環境で適切なネットワーク資源を利用するためには、利用者は個人を識別できる情報を安全に持ち歩き、適宜それを提示する必要がある。ネットワーク資源は、移動先のサービスドメインの運用ポリシーに沿った形で提供されるべきであり、必要に応じて移動先でも日常利用している環境をある程度再現できる必要がある。

### 3.1.3 受発信する情報の正当性の証明と機密性および完全性の保証

ユビキタスコンピューティング環境における新しいサービスモデルへの対応として、通進路の安全性の確保、および受発信した情報の正当性が証明可能であるような構造が必要となる。また、時刻や場所などの実空間の情報を送信する場合は、それ自体がプライバシーを含む情報となる。これらの情報の機密性および完全性を保証し、個人情報を保護する必要があると同時に、発信した情報の身元がシステム管理者には検証可能であることが望まれる。

### 3.1.4 情報発信者/利用者の個人情報の保護

個人情報の保護のため、個人を識別するための情報はインターネット上に格納するのではなく、利用者と共に移動することが望まれる。個人を識別するための情報とは、日常利用している環境や信頼できる第三者、つまり外部において定義された情報であり、個人に一つではなく、所属や立場などによって複数の情報を使い分けることが予想される。したがって、どの状況でどの情報を使うか、という選択を利用者が随時検討する自己情報制御機能が必要である。満たすべき自己情報制御機能は、第4章の議論に詳述する。

### 3.2 提案モデルの構成要素と特性

上記の機能要件を満たすシステムを検討するために、抽象化した構成要素とその特性を図1に示す。

- エンティティ
  - サービス利用者に該当
  - 移動することが前提
  - 個人を識別する情報を持ち歩く
  - 動的に変化する実空間情報の発信者でもあり得る
- ネットワーク資源
  - インターネットへの接続性を提供するための情報
  - プリンタや共有ファイルなどの内部（各サービスドメイン内）で管理されているサービス機器

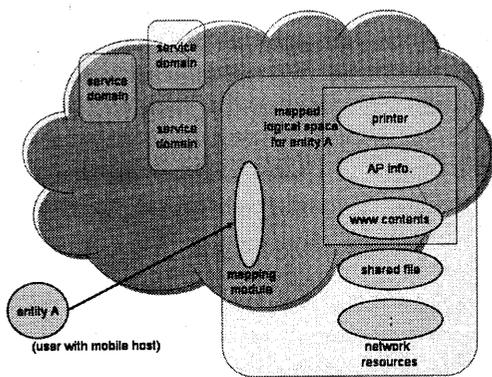


図1 ネットワーク資源提供モデル

Fig.1 a providing model of network resources

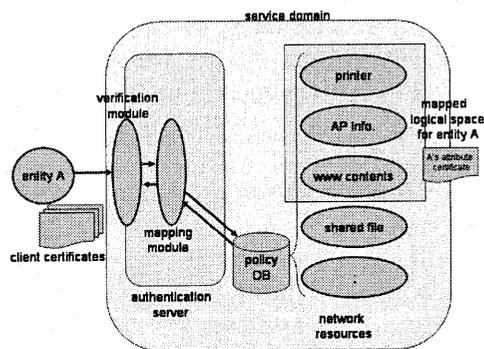


図2 システムアーキテクチャの例

Fig.2 sample of system design

● 外部定義と内部ポリシとのマッピング機構

- ネットワーク資源とエンティティのインタフェース
- 外部で定義された利用者の識別情報を一元的に管理する
- 内部で適応されるアクセス制御または権限委譲構造に対応づけられている
- 内外部の利用者の区別が必要となるため、内部での検証は可能

このモデルでは、ネットワーク資源として、サービスを構成するコンポーネント（情報、サーバ、メモリやディスクスペースなど）が分離されており、かつ、それぞれに利用のための権限が記されていると考える。このように、内部の運用ポリシによって定義された権限と外部で定義（証明）された情報を持つ利用者の権限との対応づけを、動的に定義することが目的である。

ネットワークレイヤ的には、通信メディアや経路制御などのネットワーク的に下位にあるレイヤに影響することなく、運用ポリシまたはセキュリティポリシなどの上位レイヤを柔軟に反映させることのできる汎用的な認証ミドルウェアとして検討する。

3.3 システムアーキテクチャと処理の流れ

提案モデルに基づき、システムを設計する場合のシステムアーキテクチャの例を図2に示す。

エンティティは個人識別情報を持ち歩く。移動した先で認証サービスを検索し、応答した認証サービスに向けて個人識別情報を提示する。つまり、エンティティは個人情報格納するソフトウェアのまたはハードウェア的なセキュリティデバイスを保持しており、また、サービス発見プロトコルなどを用いて移動先での認証サービスを問い合わせる機能を持つ。その後、状況に応じて利用する個人識別情報を選択し、応答したサーバに向けて発信する。サーバとエンティティの間の通信は、SSL(Secure Socket Layer)/TSL(Transport Layer Security)などを用いて保護される必要がある。

個人識別情報は、日常利用している環境や信頼できる第三者、つまり外部において定義されている。移動先、つまり内部の認証サーバは、この個人識別情報を用いてサービス利用を要求するエンティティを確認または検証する。利用者が保持する個人

識別情報がいつも移動先で検証可能であるとは限らないため、検証後、外部定義と内部ポリシとのマッピング機構によってエンティティが内部の一時的な論理空間にマッピングされ、この論理空間を記述した一時的な属性証明書などが付与される。この論理空間では、内部で定義されたポリシ適用の構造を基にした、利用可能なネットワーク資源や権限委譲の集合を扱う。これにより、外部で定義されたエンティティが、内部での特定のネットワーク資源を利用するためのアクセス制御または権限委譲を一時的に許可された空間にマッピングされる。内部で許可される空間は時限つきであるため、外部に移動する際に利用者が属性署名書を破棄/返却しなくても、一定時間経過後に無効となる。実際のシステム設計例としては、特定のサービスドメイン内で限定されたネットワーク資源へのアクセス管理や権限委譲を行うために、そのサービスドメインで独自に作成したプライベートCA(Certificate Authority)やプライベートRA(Registration Authority)を作成し、サーバの証明書や属性証明書の発行または失効処理を行う、といったことが考えられる。

これにより、エンティティは自分の保持する個人識別情報を選択的に提示するだけで、事前登録や申請をすることなく移動先でも適切なサービスを利用することが可能である。また、外部定義と内部ポリシとのマッピング機構を設けることにより、外部で定義されたエンティティに対して内部のポリシに沿った形でネットワーク資源を提供する構造が可能となる。

4. システム設計および運用に対する議論

ここでは、提案したモデルおよびシステムアーキテクチャがユビキタスコンピューティング環境におけるネットワーク資源提供サービスの機能要件を満たすことを検証するための評価項目について議論する。また、提案モデルに基づくシステムを設計した場合のスケーラビリティと、本人識別情報の種類や携帯方法、自己情報制御機能についても検討する。

4.1 提案モデルの有効性の評価

4.1.1 各機能要件について

ユビキタスコンピューティング環境におけるネットワーク資

源提供サービスを考える上で挙げた問題点を元に、以下のよう  
な検討項目に基づく機能要件を提示した。

- 通信の連続性の確保
- サービスの連続性と利用者の利便性の確保
- 受発信する情報の正当性の証明と機密性および完全性の保証
- 情報発信者/利用者の個人情報の保護

通信の連続性については、ネットワークインタフェース層に  
影響をおよぼさないレイヤでのミドルウェアとしてモデルを検  
討したため、通信メディアの複合的な利用を前提としている。そ  
こで、通信メディアの切り替えにかかる処理時間の計測や有効  
性の検証を行う必要がある。セッションの連続性については IP  
層における移動透過性を保証した Mobile IPv6 を用いた実装を  
行うことで対応する。

サービスの連続性については、クライアント証明書を用いた  
本人識別および外部と内部とのマッピング機構を用いることで  
解決を図った。この評価としては、プロトタイプシステムを構  
築した上でエンティティが移動先で認証サーバを発見する処理  
やクライアント証明書の検証処理、運用ポリシーとネットワーク  
資源割り当ての折衝にかかる処理を計測し、実用に耐えるかど  
うかを検討する必要がある。

受発信する情報の正当性に関しては、ネットワーク資源を利  
用する際にエンティティは状況に応じた個人識別情報を提示し、  
サービス提供側はその識別情報を元にアクセス制御や権限委譲  
処理を行うため、ローカルに検証可能であると云える。また、エ  
ンティティは自己情報制御を行うため、状況によっては匿名に  
近い形でネットワーク資源を要求したり厳密な認証を経た権限  
委譲を要求したりすることも可能である。これには SSL/TLS  
や IPSec などの技術を用いて通信路の安全性を確保することで、  
情報の機密性や完全性を保ったシステムを実装する必要がある。

最後に、情報発信者および利用者の個人情報保護については、  
エンティティの個人識別情報をインターネット上のどこかで蓄  
積・管理するのではなく、エンティティが常にセキュリティデ  
バイスを用いて持ち歩き、必要に応じて選択的に提示を行うこ  
とで確保する。これらの個人識別情報は、外部と内部とのマッ  
ピング機構で利用され、一時属性証明書が発行された後はシス  
テム上では参照されない。

#### 4.1.2 スケーラビリティ

提案モデルを基にシステムを設計した際のスケラビリティ  
についてを検証する場合、比較対象は、属性証明書をを用いたネ  
ットワーク資源提供モデルおよび従来のアカウント発行に基づく  
資源提供モデルであり、処理可能なエンティティの数と拠点数  
を軸とした整理と評価が必要である。しかし、属性証明書や本  
提案で用いるクライアント認証などにおいては、性能は証明書  
発行頻度に依存する。つまり、証明書発行頻度はポリシーに依  
存することになるが、性能のばらつきを吸収するための正規化が  
必要となるといえる。

また、柔軟性や拡張性の高いシステムを設計しても、導入、管  
理、および運用コストの高いものは淘汰される。大規模なポリ  
シデータベースとの連携や個人識別情報の処理時間短縮などに

関して工夫するための検討が必要である。

#### 4.2 個人識別情報の種類と携帯方法

個人識別時に用いる情報の種類とその携帯および保管場所  
についても議論をする必要がある。提案モデルでは、公開鍵暗号基  
盤で提供されるクライアント証明書個人識別情報として扱った  
が、バイOMETRICS 技術やパスワードの付加的な利用など、  
これに限定されない汎用性が求められる。また、IC カード  
や 2 次元バーコードのようなハードウェア的セキュリティデバ  
イスを持ち歩いたり、Netscape 7 などで利用されているソフト  
ウェアで実装されたセキュリティデバイスを利用することは、  
自己情報制御機能を満たす上では必要であるが、従来の認証機  
能と同様にそのデバイスの紛失や盗難によるなりすまし脅威は  
避けられない。これらのトラブルが生じた場合でも他人になり  
すますことが困難である仕組みを検討する必要がある。

#### 4.3 自己情報制御機能

現実世界では、一個人に対して割り当てられる識別子は複数存  
在するため、所有する証明書も複数ある。例えば、財布の中を探  
すだけで、社員証、診察券、運転免許証、定期券、会員カード、複  
数のクレジットカード等の身分やステータスを示す証明書を見  
つけることができる。利用者は、サービス利用時や状況などに  
応じてクレジットカードを選択したり、社員証を提示したり、診  
察券を提示したりすることで、これらの証明書を意識的、または  
無意識のうちに使い分けている。つまり、本人識別情報（自己  
情報）をプライバシーに関わる情報としてこれらの情報を自ら選  
択し、提示している。したがって、提案モデルにおいても、一  
個人に対してクライアント証明書などの複数の本人識別情報の使  
い分けが想定する場合、「自己に関わる情報について一定のコン  
トロールをおよぼす権利（自己情報制御権）」[6]に関する検  
討が必要になる。自己情報制御をプライバシーの権利として扱  
う研究としては、プライバシーを重視したアクセス制御機構の  
提案 [5] や NTT サイバーソリューション研究所の提供者の意  
思に基づく情報流通のための開示制御技術 [1]~[4] が挙げられ  
る。しかし、これらの提案技術には、認証とアクセス制御との機  
能分離を行ったため、構成要素や処理が増加し規模性に問題が  
ある、流通させる情報やサービスを限定している、などの課題が  
残っている。

個人識別情報には身分を曖昧にした証明書、つまり匿名性を  
保つものも存在する。これらの複数の本人識別情報を利用者  
自らが場合に応じて選択することにより、運用ポリシーの異なる  
サービスドメイン間を移動しても匿名性（識別子の曖昧さ）を  
保ちながらサービスを利用したり、厳密な認証のあとに権限を  
要求したりすることが可能になる。また、サービス提供者にとっ  
ては、日時や接続場所、年齢や個人のステータスなどを用いるこ  
とで、より細やかな資源アクセスへの制限や運用が可能となる。

以上より、今後の研究の方向性としては、提案モデルに基づい  
たプロトタイプシステムを設計し、これらの項目について評価  
を行う。その評価により、実用性を検証すると同時に、実運用を  
検討する際の注意点や改善点を考察する。また、サービスを構  
成するコンポーネントの構造に対する定義や権限との関係、個

人識別情報の種類と携帯方法, 自己情報制御機能についての検討も, 引き続き検討し, 議論する。

## 5. おわりに

情報の電子化にとまいない, その電子化された情報を流通させるための情報通信基盤として, インターネットが爆発的に普及してきた。とりわけ無線通信技術の発展により, 計算機を利用者が持ち歩くモバイルコンピューティング, またはネットワークに接続された計算機が遍在するユビキタスコンピューティング, という計算機の利用形態や環境が構築・整備されつつある。しかし, ユビキタスコンピューティングやモバイルコンピューティングという移動体通信環境は, 計算機が遍在し, 利用者が移動することを前提としているため, 異なるサービスドメイン間での連携や協調などを考慮していない既存のインターネット構築技術や運用では通信およびサービスの連続性への対応が困難になってきている。各サービスドメインのセキュリティポリシーや運用ポリシーに沿った形で動的かつ確かなネットワーク資源の提供を行うためには, インターネット上の分散システムの構築と運用に関して, 従来の手法に囚われない新しい概念が必要となる。

本稿では, ネットワーク資源の利用に関して従来のインターネット環境からユビキタスコンピューティング環境への利用形態の移行に際する問題点について通信およびサービスの連続性と新しいサービスモデルへの対応の観点から抽出, および整理を行った。これにより, ユビキタスコンピューティング環境におけるネットワーク資源提供を考える上で必要となる機能要件を検討し, これを満たすモデルとして, 個人証明書および一時属性証明書を用い, 移動先のサービス提供組織内の運用ポリシーを動的に反映させたサービスを提供する仕組みを提案した。主に, 外部空間で定義されたエンティティが内部空間のサービスを利用する権利をどのように付与するか, という点について検討し, 通信やサービスの連続性や利用者に対する利便性, 個人情報保護などの要件を満たすモデルを提案し, それに基づくシステムアーキテクチャを例示した。また, 実際のシステムを設計した際に評価すべき点について議論を行った。今後は, ネットワーク資源を構成するコンポーネントを整理し, そのレイヤとそれぞれの権利の構造を定義する。その上で, ユビキタスコンピューティング環境に適したネットワーク資源提供システムとしてプロトタイプを実装し, 認証やアクセス制御, 通信の処理の負荷について評価するとともに, 時刻や物理的な位置情報など, 実世界の情報を証明すべき要素の一つとして検討する。

## 謝辞

本提案モデルの構築にあたり, 奈良先端科学技術大学院大学 情報科学研究科 山口英教授に大変貴重な意見を頂きました。心より感謝を申し上げます。

## 文 献

- [1] 高倉 健, 山本 太郎, 難波 功次, 西田 玄, “提供者の意思に基づく情報流通のための開示制御技術,” NTT 技術ジャーナル 2002. vol.14, No.10, pp.28-31, 2002.

- [2] 寺西 裕一, 長谷川 知洋, 梅本 佳宏, 佐藤 哲司, “利用制約に基づくマルチメディアコンテンツ流通システム的设计,” 情報処理学会マルチメディア通信と分散処理研究会, pp.31-36, 1999.
- [3] 山本 太郎, 寺西 裕一, 梅本 佳宏, “医療情報システムにおける情報開示制御方式,” 情報処理学会マルチメディア通信と分散処理研究会, pp.19-24, 2000.
- [4] 田口, 須藤, 坪井, 山本, 寺西, “医療情報の連携を実現した医療コンテンツ流通システム,” NTT R&D, vol.51, No.1, pp.11-20, 2002.
- [5] 梅澤 健太郎, 齋藤 孝道, 奥乃 博, “プライバシーを重視したアクセス制御機構の提案,” 情報処理学会論文誌, vol.42, No.8, pp.2067-2076, 2001.
- [6] 浜田 良樹, “プライバシーの権利とインターネット,” Japan Cyber Security Management, vol.3,5,6, 2000.
- [7] 和田 光示, “プロープ情報システム (IPCar) プロジェクト,” 情報処理学会学会誌, vol.43, No.4, pp.363-368, 2002.
- [8] Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood and Andy Hopper, “Virtual Network Computing,” IEEE INTERNET COMPUTING, vol.2, No.1, 1998
- [9] Charlie Scott, Paul Wolfe, Mike Erwin, “Virtual Private Networks 2nd Edition,” O'REILLY, 2002.
- [10] 石橋 勇人, 坂本 晃, 山井 成良, 安倍 広多, 大西 克美, 松浦 敏雄, “利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式,” 情報処理学会論文誌, vol.42, No.1, pp.79-88, 2001.
- [11] AutoID Center Home Page, <http://www.autoidcenter.org>
- [12] J. Myers, “IMAP4 Authentication Mechanisms,” RFC 1731, 1994.
- [13] C. Newman, “Using TLS with IMAP, POP3 and ACAP,” RFC 2595, 1999.
- [14] P. Calhoun and C. Perkins, “Mobile IP Network Access Identifier Extension for IPv4,” RFC 2794, 2000.
- [15] S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,” RFC 2501, 1999.
- [16] L. Mamakos and K. Lidl and J. Everts and D. Carrel and D. Simone and R. Wheeler, “A Method for Transmitting PPP Over Ethernet (PPPoE),” RFC 2516, 1999.
- [17] 湧川 隆次, 植原 啓介, 田村 陽介, 徳田 英幸, “MIBsocket: 移動型計算機におけるネットワークエンティティの状態変化に対応する管理機構の設計と実装,” 情報処理学会, システムソフトウェアとオペレーティングシステム研究会, 1999.