情報処理学会論文誌　Vol. 49　No. 10　3588–3600 (Oct. 2008)

ユビキタス環境における自律的資源利用認証方式の提案

小林　透[†1,*1]　上野正巳[†1,*2]
近藤好次[†1,*3]　大戸健一[†1,*4]

近年，ブロードバンドネットワークや組み込み技術の発展にともない，公共空間に偏在したコンピューティング資源を利用できる環境が整備されてきている．しかし，不特定多数の利用者によるこのような資源の一時利用については，利用者の正当性に対するサービス提供者側の懸念や，資源の正当性に対する利用者側の懸念が障害となり実際には普及していない．これは，資源の一時利用時に利用者と資源の正当性を判定可能な方式が確立されていないことに起因する．そこで，本研究では，資源の一時利用時に即時かつ自律的に利用者と資源の正当性判定が可能な方式を提案する．提案方式では，資源利用の条件として利用者属性や資源属性に関連する条件が記述された電子的な利用権を導入する．利用者は，資源利用時に利用権と利用者属性を対象資源に提示する．資源は，受け取った利用権と利用者属性，および自らの資源属性を基にした行使判定により一時利用を認可する．これらの処理はすべて PKI を用いた相互認証による信頼関係の上に構成されている．これにより，サービス提供者側と利用者側双方にとって安心・安全な資源の一時利用サービスが提供できる．本提案方式の実用性評価として，無線 LAN アクセスポイントを資源とした場合の一時利用プロトタイプを開発し，利用者と資源の正当性を即時かつ自律的に判定することで無線 LAN の一時利用が可能であることを検証した．

A Proposal for A Resource Usage Authentication over the Ubiquitous Environment

Toru Kobayashi,[†1,*1] Masami Ueno,[†1,*2]
Yoshitsugu Kondo[†1,*3] and Kenichi Ooto[†1,*4]

Thanks to the progress of broadband network relating technologies and embedded technologies, a usage environment of computing resources distributed in a public space has recently become available. However, temporary usage of these computing resources has not been popularized because of service providers' fear of anonymous access and users' privacy concerns. This is due to the lack of an authentication method to justify temporary users and resources. Therefore, we are proposing an on-demand and autonomous authentication method which can be utilized to justify temporary users and resources. We introduced an electrical use-right policy token which contains user attribute conditions and resource attribute conditions as temporary resource usage conditions. A user provides the use-right policy token and user attribute to a target resource. This event triggers the target resource to verify conditions written in the use-right policy token according to the user attribute and resource attribute. Then, if the verification is successful, the user will be granted access to use the resource. All of these sequences are implemented on a trusted relationship by mutual authentication using the public key infrastructure. This approach provides a secure temporary resource usage service for both service providers and users.

1. はじめに

近年，FTTH，無線 LAN などのブロードバンドネットワーク関連技術や組み込み技術（embedded technology）の発達，普及にともない，これまで大学や企業のオフィス，家庭などが中心だったコンピューティング環境が，駅，空港，カフェなどの公共空間に整備されてきている．それにともない，公共空間に偏在した複数のコンピューティング資源（以降，資源と呼ぶ）を利用することで，個々の利用者に最適なサービス提供を目指すユビキタスコンピューティングに関する研究が活発に行われている．たとえば，利用者に対して公共の空間を一時的に占有可能な計算機環境を提供する PMAA [1] や，利用者の置かれている環境の変化に応じて利用するサービスをスムーズに切り替えることを可能とする ASAMA [2] が提案されている．また，異なる端末間で継ぎ目なく連続してサービスを継続する SSE [3] が提案されている．

†1 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories
*1 現在，NTT 研究企画部門
Presently with Research and Development Planning Department, NTT Corporation
*2 現在，NTT コミュニケーションズ株式会社
Presently with NTT Communications Corporation
*3 現在，NTT アドバンステクノロジ株式会社
Presently with NTT Advanced Technology Corporation
*4 現在，NTT 西日本株式会社
Presently with NTT WEST Corporation

© 2008 Information Processing Society of Japan

これらのユビキタスコンピューティングに関する研究では，個々の利用者に対して公共環境にある資源を割り当てたり，場合によっては他の資源にシームレスに切り替えたりすることで，公共環境の資源の状態が変化しても継続的なサービスを提供することに力点をおいている．しかしながら，公共環境の資源利用をビジネスとして展開するためには，まずその利用者を認証しサービス認可のプロセスを経る必要があるが，これらの既存研究は，資源の利用については，認証認可済みという前提をおいているものが多く，個々の資源の利用ための認証認可方式については，十分議論されていない．不特定多数の利用者が，公共環境に偏在している資源を，一時的に利用するような状況においては，これまでのような事前契約者を前提とした利用者認証は適用できない．また，利用者の観点からは，初めての場所で初めて利用するという場合が多いと想定され，対象資源の安全性や期待するサービスレベルを享受できるのかという不安が資源を利用する際の障害となっている．

本論文では，資源が公共環境に偏在していることを特徴とするユビキタス環境における資源の利用認証方式を提案する．この方式では，資源利用の条件として，利用者属性や資源属性に関連する条件が記述された電子的な利用権を導入する．利用者は，IC カードのような耐タンパデバイスに利用者属性を格納し，必要に応じて利用権を取得する．利用者は，資源利用時に利用権と利用者属性を対象資源に提示する．資源は，受け取った利用権と利用者属性，および自らの資源属性を基に行使判定を行うことで対象資源の一時利用を認可する．これにより，事前契約が不要で，未知な資源に対してもサービスレベルを保証したうえでの一時利用が可能になる．

2. 利用シーンと実現に向けた要求条件

2.1 想定される利用シーン

本論文における資源とは，コンピュータが埋め込まれた機器全般を指している．このような資源には，プリンタやコピー機などのオフィス機器や DVR，大画面 TV に代表される情報家電，さらには，開錠制御機構がある特定の場所やレンタカー（カーシェアリング*1）のように必ずしもネットワーク化が必須でない機器と，インターネット端末や公衆無線 LAN のアクセスポイントなどのようにネットワーク化を前提とした機器が含まれる．後者を特にネットワーク資源と呼ぶこととする．また，これらの資源を提供することをサービスといい，その資源を管理しサービスを提供する人をサービス提供者と呼ぶ．

現在普及しているカーシェアリングは，会員登録した利用者に IC カードを発行し，その IC カードによる認証によりサービスを提供する形態が一般的である．そのため，会員登録した IC カードで，別の事業者のカーシェアリングは利用できない．しかしながら，他の事業者のサービスであっても，利用者がその事業者と提携関係にある事業者の会員かどうかの利用者属性やカーナビやチャイルドシートが装備されているかどうかなどの資源属性に応じて利用時間や料金などを可変にしたうえで一時利用可能にできれば，カーシェアリングがビジネスとしてさらに普及すると考えられる．

また，対象資源として無線 LAN の一時利用を例にとると，従来は，そのつど，ある特定の事業者から 1 日単位や半日単位の一時利用チケットを購入する必要があった．そのため，短時間で移動して異なる事業者のアクセスポイントを渡り歩くといった使い方を難しくしていた．また，チケットの行使条件は有効なチケットかどうかだけであり，利用する人がだれでも，またどのようなアクセスポイントでもそのチケットに定義づけられた固定時間だけ無線 LAN サービスを利用できるというものである．そこで，利用者が他の提携する ISP（Internet Service Provider）の会員かどうかなどの利用者属性やそのアクセスポイントが 802.11e [4] などの品質制御機能を有しているかどうかなどの資源属性に応じてサービス提供時間を可変にしたうえで一時利用可能にできれば，無線 LAN サービスがさらに普及すると考えられる．

これらの利用シーンで共通に想定しているのは，公共空間に偏在する資源を，たとえ一時的であっても利用者属性や資源属性に応じて利用可能にするというものである．ここでの例のように，利用者属性や資源属性は，類似サービスの会員情報や資源が提供可能な機能などを想定している．これが実現できれば，利用者は，同様のサービスに対して複数の事業者と契約することなく利用することが可能になり，サービス提供者にとっては，自らの契約者でない利用者に対しても利用者の属性に合わせたサービスの提供が可能になるなど，双方にとってメリットがある．

これまで，インターネット接続サービスや無線 LAN サービスなどのネットワークサービスでは，事業者間の提携により，利用者が契約しているサービス事業者のサービスエリア外であっても，提携先の事業者のエリア内にあれば，元の事業者と同様のサービスを利用できるローミングが実用化されている．ローミングでは，サービス利用時に，利用者が契約しているサービス事業者に対してネットワークを通して認証依頼が行われることが前提となっているため，カーシェアリングのような対象資源がネットワークに接続されていないケースに

*1 ここでは，利用者が自ら自動車を所有せず，管理団体の会員となり，必要なときにその団体の自動車を借りるという形態をカーシェアリングと呼んでいる．

© 2008 Information Processing Society of Japan

は適用できない．また，現状のローミングでは，無線 LAN のようなネットワーク資源の一時利用においても，利用者の属性や資源の属性に応じて料金体系を可変にするようなことは実現できていない．

そこで，我々は，資源が他者に頼ることなく，自らが必要な情報を集めて，その情報を基に柔軟なサービス認可を可能とすることが本利用シーンを実現するために必要な要素技術の 1 つであると考え，これを自律的資源利用認証[*1]と定義している．

2.2　要 求 条 件

自律的資源利用認証に求められる要求条件を，以下のように整理した．

［要件 1］　一時利用者からも確実にサービス対価が受け取れること

今回実現したいのは，事前契約によりサービス対価の徴収方法が確定した利用者へのサービス提供ではないため，サービス提供者にとって「事前契約関係のない一時利用者からも確実にサービス対価が受け取れること」が必要である．

［要件 2］　利用者や資源の属性に合わせてサービスレベルを変えられること

2.1 節に示した現状の無線 LAN の一時利用のように，チケットの有効性確認のみによる一定時間利用というような固定的なサービス提供ではなく，たとえば，利用者が提携先の ISP の会員の場合や品質制御機能を有しないアクセスポイントなら利用時間を長くするといったように利用者や資源の属性に応じてサービスレベルを変えられる必要がある．

［要件 3］　ネットワーク化されていない資源であってもサービス認可が可能であること

本論文で対象とする資源は，広域に分散されており，必ずしもネットワーク化されているとは限らない．そのため，そのような資源であっても単独でサービス認可判断ができる必要がある．

3.　自律的資源利用認証方式

本章では，前章で示した 3 つの要求条件から自律的資源利用認証のための基本モデルとそれに基づいた実現方式を提案する．

3.1　基本モデル

一時利用者からの確実な対価受領を実現［要件 1］し，利用者の属性や資源の属性に合わせたサービス提供［要件 2］のために，利用者属性や資源属性に関連する条件などが記述された電子的な利用権を導入し，その利用権の行使判定によりサービス認可を行う電子権利技術に着目した．利用者は，サービス提供者から利用権を取得（購入）し，耐タンパ性を有した IC カードに格納する．ここで想定している IC カードは，ISO/IEC 7816[5] や 14443 タイプ B[5] に準拠したカードであり，複数のアプリケーションの搭載が可能な大容量マルチアプリケーション IC カード[6),7)] である．IC カードには，利用者の属性情報が格納されており，利用者が資源を利用する際に，利用権とともに資源に通知される．資源内の判定ハンドラは，利用権に記述された条件が利用者属性や資源属性と合致しているかどうかを判定することでサービス認可を行う（**図 1**）．つまり，資源内の判定ハンドラは，利用権に記述された条件の正しさと利用者属性，資源属性の正しさを検証し，その条件が満たされたかどうかの判定結果を根拠に利用者の資源利用資格の認証とサービス認可を行っている．またこのとき，資源は，IC カードから得られる情報と資源内の情報だけでサービス認可が可能であるため，［要件 3］を満たす．

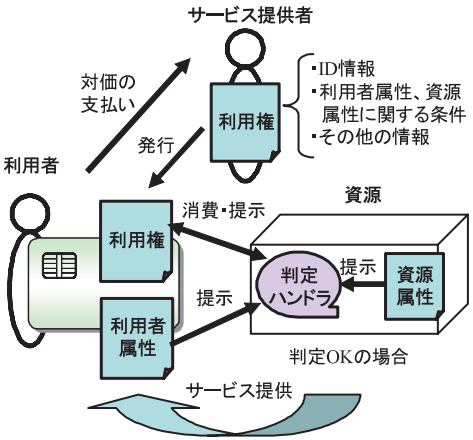

図 1　自律的資源利用認証基本モデル
Fig. 1　Basic model for autonomous resource usage authentication.

この基本モデルでは，利用権を格納する媒体として利用者が携帯する IC カードを想定している．これにより，利用者が利用権を取得するタイミングとそれを利用するタイミングが必ずしも同期する必要がないという利点がある．たとえば，対象資源のサービスエリア近くに設置された利用権発行装置を用いて取得したり，IC カードリーダを備えた自宅や会社の PC からインターネットを経由して取得したりしておき，必要なときにそれを利用するとい

*1 一般のセキュリティアプリケーションでは，認証の後にその利用者に与えられたアクセス権限により資源へのアクセスを制御するいわゆる認可が必要である．本論文で提案している「自律的資源利用認証」は，この認証と認可という 2 つの行為を含んだ言葉として定義している．

© 2008 Information Processing Society of Japan

うことが可能である．

本研究では，IC カード内の利用者属性管理機能や利用権管理機能は，それぞれ独立したアプリケーションとして IC カード発行後にダウンロードされることを想定しているため，IC カード発行主体として特定の事業者は想定していないが，2.1 節で示した無線 LAN の例では，ISP が契約者認証用に発行するような場合を想定している．これまで，1 枚の IC カードを複数の事業者が相乗りすることで，発行コストをシェアする仕組み[8] が提案されており，本研究では，このモデルを前提としている．このモデルを前提とすることで，利用者にとっては，1 枚の IC カードで，異なる事業者のサービスが利用可能になり，事業者にとっては，IC カードの発行コストを抑制できるため参入障壁を下げることができる．

3.2 実現方式

図 1 に示した基本モデルに沿って，自律的資源利用認証を実現するうえで機能上最も重要な点は，資源内の判定ハンドラが，利用権に記述された利用者属性や資源属性に関する様々な条件を判定し，条件に合致した人が，期待するサービスレベルや機能を持った資源を確実に利用することを可能とすることである．通常の OS では，利用者や利用者の属しているグループに対してファイルなどのリソースに対する読み書き許可/不許可程度のアクセス制御を提供している．しかし，我々が対象としている自律的資源利用認証のためには，たとえば，“ISP X の会員か？” といった利用者に関する条件や，“ISP X と提携関係にある公衆無線 LAN 事業者のアクセスポイントか？”，“無線区間で帯域制御が可能なアクセスポイントか？” といった資源に関する条件判断が必要であり，通常の OS が提供している程度のアクセス制御では十分でない．そこで，条件判断に利用する要素の指定や要素の設定値などを比較する演算方法が指定でき，より複雑で柔軟なアクセス制御が可能ということから，インターネット経由の情報アクセスに関する制御ポリシを表現/適用するためのマークアップ言語として，OASIS において仕様化されている XACML（eXtensible Access Control Markup Language）[9] に着目した．

XACML は，機密情報や商取引データなどを扱う Web サービスにおいて，OS やプラットフォームに依存することなく，柔軟で拡張性の高いアクセス制御を可能とすることを目的としている．そのため，XACML のデータフローモデル（**図 2**）は，Web サーバ側で事前に管理されたアクセス制御に関するポリシと，事前に登録された利用者の属性情報を基に認可決定を行うことを前提としており，このままでは，事前契約のない利用者による資源の一時利用を可能とすることを目的とする自律的資源利用認証には適用できない．そこで，XACML のデータフローモデルで定義されている各プロセスを，図 1 の基本モデルで定義

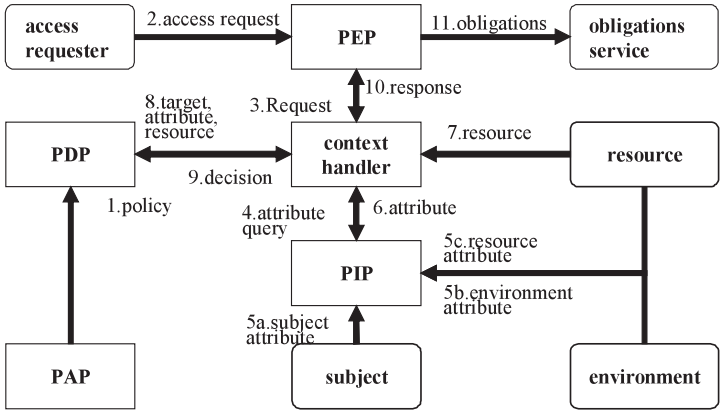

図 2　XACML のデータフローモデル
Fig. 2　XACML date flow diagram of OASIS.

した各処理主体に，その機能的役割の考え方に基づいて配置することを考えた．これにより，自律的資源利用認証のための機能配置（**図 3**）とその機能配置を前提とした処理シーケンスを明らかにした．

(1)　機能配置の考え方

図 1 の基本モデルでは，サービス提供者は，利用者属性や資源属性に関する条件を記述した利用権を発行する．この条件が図 2 のアクセス制御のルールを定義する役割を持つ PAP（Policy Administration Point）が生成するポリシ（policy）に該当すると考え，PAP をサービス提供者が運営することを想定しているサービス提供者装置に配置した．

利用者は，IC カード内に利用権を保存し，資源の一時利用時に利用者属性とともに資源に提示する．そこで，IC カードには，サービス提供者装置から取得した利用権を一時的に保存しておく利用権管理と利用者（主体：subject）の属性情報（subject attribute）を管理する利用者属性管理を配置した．

資源は，利用権や属性情報を収集し，利用権に記述された条件が各属性情報に合致しているかどうかを判定することでサービス認可を行う．そこで，属性情報を収集する PIP（Policy Information Point）と属性情報やポリシを基に行使判定を実施する PDP（Policy Decision Point），および利用者（access requester）からの要求に基づき PIP や PDP に対して属性情報の収集指示や行使判定指示をプロトコル変換のための Context handler を経由して行

© 2008 Information Processing Society of Japan

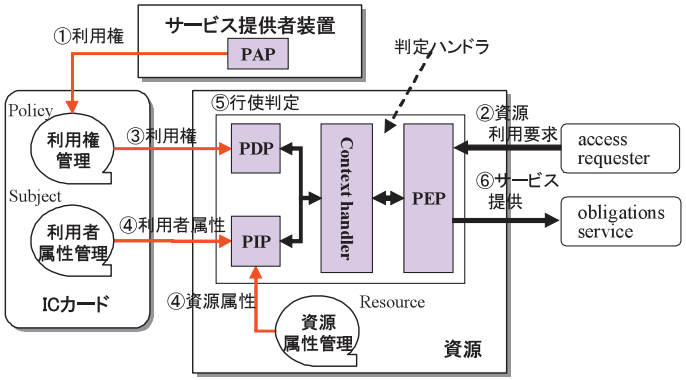

図 3　利用権の行使判定が可能な機能配置
Fig. 3　Autonomous resource usage authentication architecture.

うことでアクセス制御を行う PEP（Policy Enforcement Point）を資源に配置した．さらに，資源（resource）の属性情報（resource attribute）を管理する資源属性管理を資源に配置した．なお今回提案した基本モデルでは，図 2 の環境属性（environment attribute）の利用は前提としていないため図 3 の機能配置には含めていない*1．

(2)　処理シーケンス

図 3 で示した機能配置図を前提とした場合の処理シーケンスは以下のようになる．

① 利用者は，必要に応じてサービス提供者装置から利用権を取得して，IC カードの利用権管理により一時保管する．

② 利用者は，資源の PEP に対して資源利用要求を出す．PEP は，Context handler を経由して PDP，PIP に行使判定処理を依頼する．

③ PDP は，PEP からの依頼により IC カードの利用権管理から利用権を取り出す．

④ PIP は，PEP からの依頼により IC カードの利用者属性管理から利用者属性を，資源の資源属性管理から資源属性を収集し，PDP に通知する．

⑤ PDP は，取得した利用権内のポリシと PIP から通知された属性情報により行使判定を行う．

⑥ 判定結果は，Context handler を通じて PEP に伝達され，判定結果に応じたサービスが利用者に提供される*2．

4. システム設計

本章では，3 章で示した自律的資源利用認証方式を実装するうえでのシステム化要件を明らかにしたうえで，それに対する対応策を示す．

4.1 システム化要件

自律的資源利用認証の要求条件［要件 1〜3］を満足するために，図 3 に示したような機能配置，および処理シーケンスを採用したことにより，行使判定のために必要なポリシや利用者属性，資源属性などが異なる管理主体により分散管理されることになる．このような分散管理を前提としたうえで正しい行使判定を可能にするためには，ポリシや各属性の管理主体やその役割を明確にしたフレームワークが必要である［システム化要件 1］．さらに，行使判定時に，通常は IC カード内に管理されている利用者属性を資源に提示する必要があるため，正当なサービス提供者を装った悪意のあるサービス提供者への利用者属性の漏洩を防ぐことができる仕組みが必要である［システム化要件 2］．また，このとき，利用者属性は，無線/有線を問わず何らかの通信手段で，利用者の持つ IC カードから資源に送信されるため，通信路上での情報の盗み見を防止する必要がある［システム化要件 3］．さらに，利用権の取得や行使など利用権がサービス提供者装置，IC カード，資源間の通信路上を流通する際の盗み見による利用権の複製や偽造などの利用権の不正利用を防止できる仕組みが必要である［システム化要件 4］．

4.2 自律的資源利用認証フレームワーク

［システム化要件 1］を満足するための自律的資源利用認証フレームワークを**図 4** に，また各プレーヤの役割を**表 1** に示す．本フレームワークの特徴は，以下のとおりである．

- 利用者属性管理者やサービス提供者は他者が発行した IC カードに管理用のアプリケーションを搭載できること
- 利用者属性や資源属性を管理する主体と行使判定をする主体が異なるため適正な判定を保証できること
- それぞれのプレーヤが保証すべき情報の管理や行使判定のための機能を IC カードや資

*1 基本モデルの拡張系として，資源の利用場所や時間，温度，湿度などの情報を環境属性ととらえ，それらを行使判定の条件として判定ハンドラに取り込むことができれば，環境属性に応じた行使判定が可能になる．

*2 PEP の実行に際しては，責務（Obligation）を与えることがある．たとえば必要なメッセージを要求者に伝えなさいとか，指定した時間のみサービスを提供しなさいなど．

© 2008 Information Processing Society of Japan

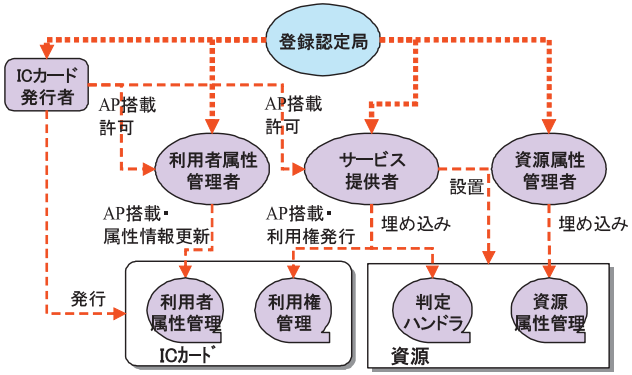

図 4　自律的資源利用認証フレームワーク
Fig. 4　Automated resource usage authentication framework.

表 1　各プレーヤの役割
Table 1　Authentication framework player.

プレーヤ	役割
登録認定局	フレームワークに登場する各プレーヤの正当性を保証する主体.
ICカード発行者	ICカードを発行する主体
利用者属性管理者	利用者属性の正当性を保証する主体.
サービス提供者	利用権を発行し，資源の一時利用サービスを提供する主体．利用権の正当性，及びその行使判定結果の正当性を保証する主体.
資源属性管理者	資源属性の正当性を保証する主体.

源に分散して搭載しても，それらは，同一の信頼ツリー下にあるため，行使判定処理に先立ち相互認証による正当性検証が可能であること

4.3　アクセス制御フレームワーク

本研究では，利用者が初めて訪れた外出先などで，資源を一時利用するような利用シーンを想定している．そのため，利用者自身がその場で対象資源のサービス提供者の良否を判断することは困難である．そこで，本研究では，[システム化要件 2] を満足するために，利用者から委任された利用者属性管理者が，利用者に代わってサービス提供者への属性情報の開示可否を制御するモデルを採用した．また，その具体的な仕組みとして，アクセス許可証を用いた属性情報へのアクセス制御フレームワーク（**図 5**）を導入した．アクセス制御フレームワークに基づいた利用者属性を開示する手順を以下に示す．

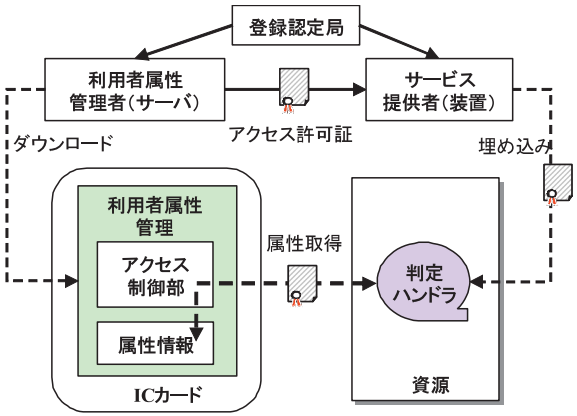

図 5　アクセス制御フレームワーク
Fig. 5　Access control framework.

① 利用者属性管理者は，サービス提供者を事前に審査することにより，属性情報を開示可能なサービス提供者を決定する．
② 開示対象となる属性情報や読み書きなどのアクセス権限情報などが記述され，利用者属性管理者の電子署名がついたアクセス許可証がサービス提供者へ発行される．
③ サービス提供者は，アクセス許可証が含まれる判定ハンドラを資源に埋め込む．
④ 行使判定時，判定ハンドラは，該当するアクセス許可証を利用者属性管理に提示する．
⑤ 利用者属性管理のアクセス制御部は，アクセス許可証の署名検証によりアクセス許可証の正しさを検証し，アクセス権限に従った属性情報へのアクセスを許可する．

このモデルは，利用者の属性情報を管理する利用者属性管理者に信頼の基点をおいており，その利用者属性管理者が信頼するサービス提供者にのみ利用者属性を開示することで，利用者属性が無制限に開示されてしまうことを防止している．これにより，利用者属性管理者から信頼されないサービス提供者は排除可能であるが，利用者属性管理者が許可した正当なサービス提供者には，利用者属性は開示される．そのため，利用者は，開示される利用者

© 2008 Information Processing Society of Japan

属性について，利用者属性管理者と合意をとることが条件となる．

4.4　オンデマンドセキュアチャネル

［システム化要件 3］を阻害するセキュリティ脅威は，行使判定の際に IC カードから資源に利用者属性が送信されるときの通信路上の情報の盗み見である．また，［システム化要件 4］を阻害するセキュリティ脅威は，利用権発行の際のサービス提供者装置と IC カード間の通信路と，行使判定の際の IC カードと資源間の通信路上の盗み見による利用権の複製などの不正利用である．そこで，これらの脅威を排除するために，サービス提供者装置—IC カード間，IC カード—資源間で，それぞれの公開鍵証明書を交換し，図 4 に示した自律的資源利用認証フレームワークに基づいた相互認証実施後，セションキーを交換することで，セキュアチャネルをオンデマンドで構成することとした．

5.　プロトタイプシステム

提案方式を無線 LAN によるインターネットアクセスサービスに適用し，公衆無線 LAN の一時利用を可能とするプロトタイプ（**図 6**）を実装した．実装したプロトタイプの概要と一時利用開始までの動作シーケンス，動作時間を以下に示す．

5.1　プロトタイプシステムの概要

各種サーバとしては，公開鍵証明書を発行する登録認定局サーバ，IC カード内の利用者属性を管理する利用者属性管理者サーバ，資源内の資源属性を管理する資源属性管理者サーバを実装した．利用者属性や資源属性は，それぞれの管理サーバにおいて電子署名が付与され，利用者属性を変更するための作業用端末に挿入された IC カードや無線 LAN アクセス制御装置に閉域網経由で設定される．また，利用者からの要求に基づいて公衆無線 LAN 利用のための利用権を発行するサービス提供者装置を実装した．

無線 LAN アクセス制御装置には，利用者からの利用権発行要求をサービス提供者装置に仲介して利用者の IC カードに利用権を発行する利用権発行機能群と利用権の行使判定を行いその結果に基づきインターネットへのアクセス制御を行う利用権行使機能群を実装した．ただし，これらの機能群は独立であり，異なる機器に別々に実装することが可能である．そのため，無線 LAN アクセス制御装置とは別の装置に利用権発行機能群を実装し，無線 LAN アクセス制御装置に利用権行使機能群のみを実装することも可能である．実際の無線 LAN 一時利用サービスにおいては，利用権を購入するタイミングや場所とそれを利用するタイミングや場所はかならずしも同じとは限らないので，異なる装置への実装が適していると考えるが，今回は，評価が目的のプロトタイプであるため，2 つの機能を無線 LAN アクセス制御装置に実装した．

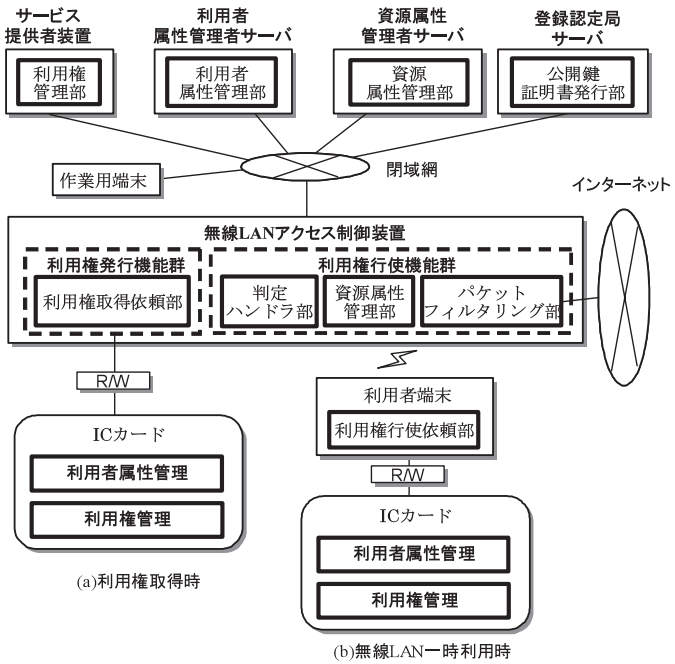

図 6　公衆無線 LAN 一時利用プロトタイプシステム
Fig. 6　Prototype system for public wireless LAN.

IC カード機能としては，マルチアプリケーション IC カードに，利用者属性管理と利用権管理をそれぞれ独立した IC カードアプリケーションとして実装した．これらの IC カードアプリケーションには，サービス提供者装置や無線 LAN アクセス制御装置と相互認証を行い，セキュアチャネル構成後，アクセス許可証によるアクセス制御機能を有している．この IC カードの発行機能や IC カードへのアプリケーションダウンロード機能，および登録認定局については，マルチアプリケーション IC カード管理プラットフォームである NICE [10)–12)] を用いた．無線 LAN アクセス制御装置には，無線 LAN アクセスポイント機能が備わり，ESS-ID と WEP キーを共有した利用者端末との無線 LAN 接続を可能としている．無線 LAN 機能を内蔵した利用者端末には，利用権行使時におけるユーザインタフェースとして利用権行使依頼部を実装した．

© 2008 Information Processing Society of Japan

利用権取得時には，図 6 (a) に示したように，利用者は，無線 LAN アクセス制御装置の IC カード R/W に IC カードを挿入し，無線 LAN アクセス制御装置を操作することで，サービス提供者装置から利用権を取得することができる．無線 LAN 一時利用時には，図 6 (b) に示したように，利用者は，利用者端末の IC カード R/W に IC カードを挿入し，利用者端末を操作することで，判定ハンドラ部で利用権の行使判定が実施され，判定結果によりパケットフィルタリング部がポートを開くことで，インターネット接続が可能となる．この際，利用される利用者属性や資源属性は，IC カード内の利用者属性管理と無線 LAN アクセス制御装置内の資源属性管理部に格納されたものが利用されるため，閉域網を経由しての利用者属性管理者サーバや資源属性管理者サーバへのアクセスは行われない．そのため，図 6 に示したように必ずしもこれらのサーバ群と無線 LAN アクセス制御装置を閉域網で接続する必要はないが，評価実験にあたっては，利用者属性や資源属性を様々なパターンに変更し，それらを効率的に IC カードや無線 LAN アクセス制御装置に設定できる必要があったため，このようなプロトタイプ構成とした．

ハードウェアとしては，サーバ群として，CPU 処理能力 1.6 GHz 相当の PC サーバを，無線 LAN アクセス制御装置として，CPU 処理能力 650 MHz 相当の PC サーバを用いた．また，IC カードとしては，暗号処理プロセッサが具備されていること，複数の IC カードアプリケーションの実装が可能なこと，複数の利用権を格納できることなどの要求条件から，非接触型大容量マルチアプリケーション IC カード（フラッシュメモリ 1 Mbyte 内蔵）である eLWISE [6),7)] カードを用いた．

5.2　動作シーケンスと動作時間

無線 LAN の一時利用を開始するまでの前提条件と動作シーケンス（**図 7**）を以下に示す．

（前提条件）IC カード内の利用者属性管理には，“ISP X の会員” という利用者属性が，無線 LAN アクセス制御装置内の資源属性管理部には，“A 社のアクセスポイント” という資源属性が格納されている．また，IC カード内の利用権管理には，“ISP X の会員が A 社のアクセスポイントを利用する場合は 60 分利用可能，それ以外の場合は，30 分利用可能” という利用権（**図 8**）が格納されている．

（動作シーケンス）

① 資源利用要求が判定ハンドラ部に送信されると，利用権管理，利用者属性管理と PDP，PIP の間で相互認証後，セキュアチャネルが構築され，アクセス許可証の検証結果に基づいて，利用権と利用者属性が判定ハンドラ部に送信される．その後，それぞれ署名検証により情報の正しさを確認する．さらに，判定ハンドラ部は，資源属性管理部から資源属性を取得し，署名検証により情報の正しさを確認する．

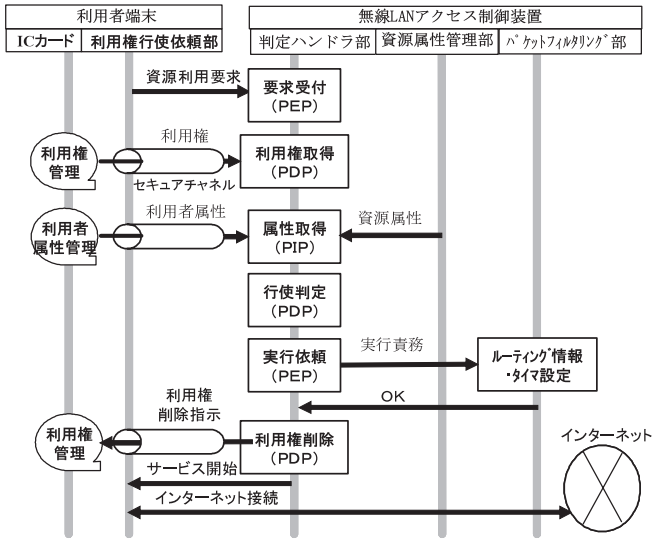

図 7　公衆無線 LAN 一時利用動作シーケンス
Fig. 7　Process flow of public wireless LAN.

② 判定ハンドラ部は，得られた利用権と利用者属性，資源属性から行使判定を行う．この場合前提条件から，1 時間利用可能と判定され，それが実行に対する責務（obligation）として，パケットフィルタリング部に通知される．

③ パケットフィルタリング部は，得られた obligation に基づいてルーティング情報とタイマを設定し，結果を判定ハンドラ部に通知する．

④ 判定ハンドラ部は，利用権を削除（回数券的利用権の場合は，価値減算処理）するとともにサービス開始を通知する．

⑤ 利用者端末からインターネット接続が可能になり，一時間経過後，接続が切断される．

①〜④で示した動作処理時間を測定した（**図 9**）．利用者が無線 LAN の一時利用を要求してから実際に利用開始されるまで，約 8 秒を要することが分かった．また，ログ出力モードにより，処理単位ごとの動作時間を測定したところ，①の処理が全体の約 80%を占めており，その中でも利用者属性や利用権の取得・検証処理が①の処理全体の約 96%を占めていることが分かった．利用者属性や利用権の取得・検証処理は相互認証により IC カードア

© 2008 Information Processing Society of Japan

```
<?xml version="1.0" encoding="UTF-8" ?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xacml-      context="urn:oasis:names:tc:xacml:1.0:context"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:xacml:1.0:policy cs-xacml-schema-
policy-01.xsd" PolicySetId="urn:oasis:names:tc:xacml:1.0:conformance-test:IID005:policyset"
PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable">
<Description> ISP Xの会員かつA社のアクセスポイントなら60分間、それ以外は30分間利用可能</Description>
・・・(省略)・・・
<Policy PolicyId="urn:pflab:urap:demo1.1:policy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
・・・(省略)・・・
 <Rule RuleId="urn:pflab:urap:demo1.1:rule" Effect="Permit">
  <Description>ISP Xの会員かつA社のアクセスポイントなら60分間利用可能</Description>
  ・・・(省略)・・・
  <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:and"> (条件をXACML記法に従って記述)
      "無線LANｱｸｾｽﾎﾟｲﾝﾄ事業者名"      equal    "A社"
       and
      "利用者ISP会員種別"              equal    "X社"
  </Condition>
 </Rule>
- <Obligations>   (条件にマッチした場合のサービス実行パラメータをXACML記法に従って記述)
      "利用可能時間"                   equal    "60分"
 </Obligations>
</Policy>
<Policy PolicyId="urn:pflab:urap:demo1.1:policy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-
overrides">
・・・(省略)・・・
- <Rule RuleId="urn:pflab:urap:demo1.1:rule" Effect="Permit">
  <Description>それ以外なら30分間利用可能</Description>
  ・・・(省略)・・・
 </Rule>
- <Obligations>  (条件にマッチした場合のサービス実行パラメータをXACML記法に従って記述)
      "利用可能時間"                   equal    "30分"
 </Obligations>
</Policy>
</PolicySet>
```

図 8　XACML による利用権記述例
Fig. 8　XACML description example.

プリケーションと判定ハンドラ部との間でセキュアチャネルを構築する処理と，アクセス許可証によるアクセス制御に基づいて属性情報・利用権を判定ハンドラ部へ送信する処理が含まれるが，それぞれの処理の内訳は，約 9 : 1 の割合であった．今回のプロトタイプにおける利用者属性とアクセス許可証は，それぞれ約 150 byte であった．また，XACML で記述した利用権（図 8）は，実際には，GZIP により圧縮して IC カードに格納する方式としたが，その場合のデータ容量は，約 660 byte であった．この程度の情報量をセキュアチャネルにより送受信する場合，情報自体の転送や検証処理時間よりもセキュアチャネル構築のオーバヘッドの方が大きいことが分かった．

これまで無線 LAN セキュリティの標準化技術として，LAN 接続時に使用する利用者認証規格である IEEE 802.1x[13] や，802.1x による認証強化と暗号化方式の強化をあわせ持つ Wi-Fi Alliance が策定した WPA（Wi-Fi Protected Access）[14]，WPA にさらに強固な暗号アルゴリズムである AES（Advanced Encrypted Technology）を追加した IEEE 802.11i[4] が提案されている．これらの標準化技術は，無線 LAN 利用時の利用者認証と暗号化通信を強化することで無線 LAN のセキュリティ強度をあげることを目的としている．標準化技術では，無線 LAN アクセスポイントは，接続要求を出した利用者端末と ESS-ID によるアソシエーション後，認証サーバに認証要求を出し，認証された場合，当該利用者端末のネットワーク接続を許可する仕組みとなっている．今回開発したプロトタイプでは，無線 LAN アクセスポイントに該当する無線 LAN アクセス制御装置が利用者端末と ESS-ID によるアソシエーション後に，認証サーバに認証要求を出すのではなく，上述した①，②の動作シーケンスにより無線 LAN アクセス制御装置のみでサービス認可判定を実施するという点が従来の標準化技術と異なる点である．また，暗号化通信に関しては，今回のプロトタイプでは，WEP キーによる暗号化のみの実装となっているため，暗号鍵を一定時間ごとに自動的に更新する TKIP（Temporal Key integrity Protocol）などの WPA や 802.11 i で採用されている方式への対応が実用化に向けた課題である．

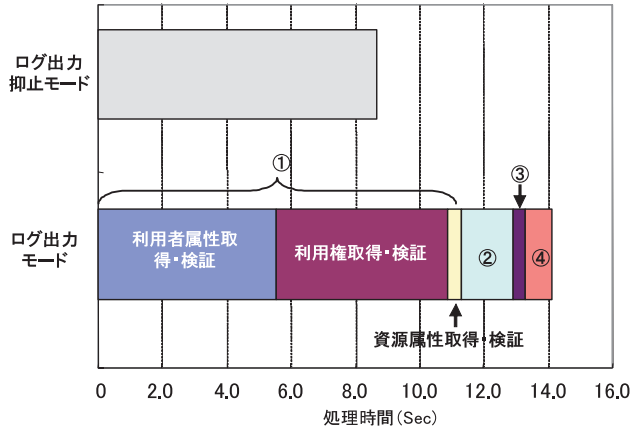

図 9　処理フェーズごとの動作時間
Fig. 9　Turnaround time.

© 2008 Information Processing Society of Japan

6. 議　　論

6.1 要求条件の達成度

5 章で示した実験結果を基に，2 章で示した要求条件の達成度や実用化に向けた今後の課題を議論する．

(1) 要件 1：一時利用者からも確実にサービス対価が受け取れること

提案した基本モデル（図 1）では，利用権取得時に対価の支払いを行うこととしている．今回実装したプロトタイプでは，利用者の IC カードに対する利用権の発行機能のみを実装したが，実用化にあたっては，この部分に課金機能を組み合わせることや発行済利用権の譲渡などの利用権を安全に流通させる仕組みの検討が必要である．電子権利流通基盤に関する研究については，たとえば，FlexToken[15] で提案されており，これらの既存研究結果を参考にすることで，改良することが可能と考える．

(2) 要件 2：利用者や資源の属性に合わせてサービスレベルを変えられること

5.2 節で示したように，実装したプロトタイプでは，自律的資源利用認証フレームワークに基づいて “ISP X の会員”であるという利用者属性と “A 社のアクセスポイント” であるという資源属性によって，無線 LAN の利用時間を正しく可変にできることが確認できた．しかし，今回実装したプロトタイプでは，無線 LAN アクセス制御装置内の判定ハンドラ部や資源属性管理部は，耐タンパデバイス上に実装していない．実用化にあたっては，より安全性を高め，資源への組み込みを容易にするために，これらの機能を IC チップなどの耐タンパデバイス上に実装することなどが考えられるが，そのためには，資源属性が格納された耐タンパデバイスを正しい資源に埋め込むなどの実用化に向けた運用方式の検討が必要である．高橋ら[16] は，VPN ルータに耐タンパデバイスが搭載されていることを想定し，機器の製造段階から，それらの機器に安全に VPN 鍵を配送するまでのフレームワークを提案している．このフレームワークはオンデマンドに VPN を構成するためのものであるが，この考えを自律的資源利用認証へ拡張することでこの課題を解決できる可能性がある．また，IC カードへの利用者属性の登録・更新・失効などの具体的な運用方式については未検討であり，今後の課題である．

(3) 要件 3：ネットワーク化されていない資源であってもサービス認可が可能であること

5.1 節で示したように，無線 LAN のサービス認可を行う無線 LAN アクセス制御装置は，利用者が無線 LAN を一時利用する際に，利用者の IC カードから利用権，利用者属性を取得し，自らの資源属性管理部から資源属性を取得することで，サービス認可が可能であった．このように提案した方式は，かならずしもネットワーク化されていない資源にも適用できることから，環境に偏在する資源に対するアクセス認証方式として適しているといえる．

6.2 安　全　性

提案方式の安全性を議論するために，情報セキュリティに関して ISO/IEC27001[5] で定義されている「機密性」「完全性」「可用性」のぞれぞれの観点においてセキュリティ脅威を明らかにすることで，提案方式における安全性を議論する．

(1) 機密性

「機密性」に対する脅威としては，

- 利用権の不正利用
- 利用者属性漏洩によるプライバシ侵害

が考えられる.「利用権の不正利用」に関しては，利用権発行時や行使判定時に正当でない利用者や資源に利用権を渡してしまうケース，サービス提供者装置—IC カード間，IC カード—資源間の通信路上からの漏洩によるケース，サービス提供者装置や IC カード，資源などの装置から漏洩するケースが考えられる．本論文の提案方式では，利用権発行時や行使判定時にサービス提供者装置—IC カード間，IC カード—資源間で自律的資源利用認証フレームワークに基づいた相互認証実施後，セキュアチャネルを構成することとしている．これによりフレームワークでその正当性が保証されていない利用者や資源を排除することが可能であり，通信路からの漏洩も防止可能である．ただし，6.1 節 (1) に示したように，今回のプロトタイプでは，課金機能との連動や発行済利用権の流通に関する機能は実装していない．そのため実用化にあたっては，たとえシステム障害や通信障害が起こっても，課金処理が完了した利用者のみに利用権を発行する利用権発行プロセスの実装や既存研究を参考にした安全な利用権流通のためのプロセスの実装が必要である．利用権が各種装置から漏洩するケースに関しては，該当装置として，サービス提供者装置，IC カード，資源がある．今回のプロトタイプでは，IC カード以外は耐タンパ性を有していない．そのため，装置の盗難などによる利用権漏洩を防止するためには，利用権を格納する装置として耐タンパ性を有したものを利用する必要がある．特に，公共環境に偏在することを前提としている資源については，盗難の危険性が高いので，6.1 節 (2) でも述べたように，対処が必要である．

© 2008 Information Processing Society of Japan

「利用者属性漏洩」に関しては，行使判定時に正当でない資源に利用者属性を提示してしまうケース，IC カード—資源間の通信路上からの漏洩によるケース，IC カードや資源などの装置から漏洩するケースが考えられる．行使判定時の利用者属性の資源への開示にあたっては，自律的資源利用認証フレームワークによる資源の正当性確認だけではなく，利用者属性管理者が信頼したサービス提供者のみに発行するアクセス許可証によるアクセス制御という 2 重のガードを施している．これにより，利用権と比較してより慎重であるべき利用者属性というプライバシ情報の開示制御を実現している．ただし，個人情報の防御に関しては，関連研究でも検討がなされているため次章で再度議論する．IC カード—資源間の通信路は，利用権のケースと同様にセキュアチャネルによって防御されている．また，同様に資源からの情報漏洩を防御するために，耐タンパ性を有したものを利用する必要がある．

「機密性」に対する脅威対策の 1 つとして，利用権や利用者属性の流通時にセキュアチャネルを構成することとしたが，5.2 節で述べたようにセキュアチャネル構築が行使判定全体処理シーケンスの中で，性能ネックになっていることが分かった．今回は公開鍵暗号として RSA を用いたが，今後はより高速な楕円暗号の適用やセキュアチャネル構築シーケンスの見直しなどによるさらなる性能向上が課題である．

(2)　完全性

「完全性」に対する脅威としては，利用権，利用者属性，資源属性，アクセス許可証などの自律的資源利用認証を実現するうえで必要な情報の改ざんである．これらの情報には，自律的資源利用認証フレームワークで定義した各管理主体により電子署名が施されており，改ざんは不可能である．

(3)　可用性

「可用性」に対する脅威としては，利用権発行時や行使判定時にサービス提供者装置や資源が故障などにより利用できないケースである．この脅威に対しては，複数のサービス提供者装置や資源を用意することで対応可能である．特に資源については，もともと本研究で対象としているものが公共環境に遍在していることを前提としており，さらにそれらは，自律的に利用権の行使判定が可能であるため，仮に 1 つの資源が故障したとしても，最寄りの他の資源を代替利用することで可用性をあげることができる．

7. 関 連 研 究

事前契約を前提としないネットワーク資源の一時利用に関する研究として，和泉らは，“ユビキタス環境におけるネットワーク資源提供のためのサービスモデル”[17] を提案している．このモデルでは，利用者が自分のホーム環境で定義された個人証明書を携帯し，移動先にその証明書を提示することで，移動先のサービス提供を要求する．各移動先のサービスドメイン内では，定義された運用またはセキュリティポリシと提示された証明書の情報を対応づけることで，テンポラリな属性証明書を発行する．各サービスドメイン内では，この属性証明書を用いて，アクセス制御や権限委譲などの処理を行い，未知の利用者に対する一時的なサービス提供を行う．また，本城らは，“プライバシに配慮した WWW における個人属性認証・アクセス制御システム”[18] を提案している．このシステムでは，ブラウザから WWW にアクセス時に，個人情報登録サーバ・チケット発行サーバからオンデマンドで個人情報が含まれるチケットを入手し，それを WWW に提示し，WWW 側で管理されているアクセス制御ポリシと突き合わせることで，個人情報に基づいたアクセス制御を実現している．これらの既存研究では，利用者の属性情報とポリシを基に資源の利用可否を決定しており，我々の研究のアプローチと同一であるが，ポリシの管理方法，プライバシ情報である利用者属性の提示方法に違いがある．

既存研究では，ポリシはサービス提供資源内にクローズドに管理されている．そのため，ネットワーク資源の一時利用を可能にするためには，利用者の属性に応じて，事前に資源内のポリシを変更する必要があり，あらかじめ参加者の属性の予測が可能な各種会議や研究会などの一時的なネットワーク資源利用には適しているが，我々が想定している不特定多数の利用者を対象とした必ずしもネットワーク化されていない資源の一時利用には適用できない．一方，我々の提案するモデルでは，資源の属性と利用に関するポリシを分離させ，資源属性は資源に格納し，利用条件として記述されたポリシは，利用権という利用者が取得できる形にして，それぞれ独立したプレーヤがその正当性を保証するモデルとしている．そのため，一時利用の際には，事前に資源内のポリシを変更する必要がなく，ネットワーク化されていない資源に対しても適用可能で，さらに資源の属性に応じた資源の行使判定を可能にしているという点において優位性がある．

利用者属性の提示方法については，和泉らの方式では，移動先サービスドメインに対する個人証明書の開示制御は考慮されていない．また，本城らは，WWW へのアクセス要求時に，個人情報登録サーバ・チケット発行サーバにより，オンデマンドで必要最小限の個人情

© 2008 Information Processing Society of Japan

報を開示する仕組みを提供しているが，ネットワーク上というオンラインを前提としている．一方，我々の方式は，利用者属性管理者がサービス提供者に発行したアクセス許可証を，行使判定時に IC カード内アプリケーションがオフラインで検証することで，利用者属性管理者が認めたサービス提供者以外への情報漏洩を防止する方式としているため，必ずしもネットワーク化されていない資源の自律的な利用認証に適している．ただし，認められたサービス提供者の資源には，不必要な個人情報も提供される可能性があるため，オフラインであっても本城らの方式のように，必要な情報のみを開示するような仕組みの検討が必要である．

8. ま と め

環境に偏在する資源の一時利用を可能とする自律的資源利用認証方式を提案し，その方式を公衆無線 LAN に適用したプロトタイプを開発した．プロトタイプの評価により提案した方式は，これまで障害となっていた一時利用者を対象とすることによるサービス提供者のリスクと利用者の安全性やサービスレベルに対する不安という問題を解決するだけでなく，不特定多数の利用者の属性や対象資源の属性によって柔軟で多様なサービスの提供が可能であることが確かめられた．さらに，提案した方式は，既存の関連研究と異なり必ずしもネットワーク化されていない資源に対しても適用可能であるなど拡張性が高いことが確かめられた．

一方，実用化に向けては，利用権の譲渡などの利用権を安全に流通させる基盤の実装や判定ハンドラ部と資源属性管理部の耐タンパデバイス上への実装と正しい資源への埋め込みのための運用方式，IC カードへの利用者属性の登録・更新・失効などの運用方式の確立などが課題であることを明らかにした．また，個人情報の防御手法についてもさらに検討を加える必要がある．今後は，これらの課題解決に向けて検討を進める予定である．

参 考 文 献

1) 岩本健嗣，徳田英幸：PMAA（Personalized Media Access Architecture）：ユビキタス環境におけるメディアアクセスアーキテクチャ，情報処理学会論文誌，Vol.43, No.3, pp.848–856 (2002).
2) 永田智大，西尾信彦，徳田英幸：ASAMA：適応的なサービス利用管理機構，情報処理学会論文誌，Vol.42, No.6, pp.1557–1569 (2001).
3) 笠井裕之，菊田洋子，川崎紀宏，山崎憲一：端末間サービス移動のためのシームレスサービス環境プラットフォーム，電子情報通信学会論文誌（B），Vol.J86-B, No.8, pp.1389–1403 (2003).
4) IEEEE 802.11 (online). available from http://www.ieee802.org/11/ (accessed 2008-03-24).
5) International Organization for Standardization (online). available from http://www.iso.org/iso/home.htm (accessed 2008-03-24).
6) 永井靖浩，大谷佳光，吉澤正浩，伊達　滋：IC カードシステム技術，NTT 技術ジャーナル，Vol.13, No.12, pp.19–23 (2001).
7) Yoshizawa, M., Unno, H., Fukunaga, T., et al.: ELWISE—a super multi-purpose smart card, *NTT REVIEW*, Vol.14, No.1, pp.23–27 (2002).
8) NICSS（次世代 IC カードシステム研究会（オンライン）．入手先 http://www.nicss.or.jp/（参照 2008-03-24）．
9) OASIS (online). available from http://www.oasis-open.org/home/index.php (accessed 2007-10-02).
10) Toji, R., Wada, Y., Hirata, S., et al.: A network-based platform for multi-Application smart cards, *Proc. 5th IEEE International Enterprise Distributed Object Computing Conference*, Seattle, USA. pp.34–45 (2001).
11) 山本修一郎，田路龍太郎，平田真一ほか：IC カード情報流通プラットフォーム：NICE, NTT 技術ジャーナル，Vol.13, No.12, pp.14–18 (2001).
12) 吉田芳浩，竹内宏典：情報セキュリティ技術，NTT 技術ジャーナル，Vol.14, No.8, pp.16–19 (2002).
13) IEEE 802.1X (online). available from http://www.ieee802.org/1/pages/802.1x.html (accessed 2008-03-24).
14) Wi-Fi Alliance (online). available from http://www.wi-fi.org/ (accessed 2008-03-24).
15) 寺田雅之，花舘蔵之，藤村　考ほか：電子権利流通基盤のための汎用的な原本性保証方式，情報処理学会論文誌，Vol.42, No.8, pp.2017–2029 (2001).
16) 高橋成文，東川淳紀，山本修一郎ほか：2 階層 PKI を用いたオンデマンド VPN システム，情報処理学会論文誌，Vol.46, No.5, pp.1129–1136 (2005).
17) 和泉順子，森島直人，砂原秀樹：ユビキタス環境におけるネットワーク資源提供のためのサービスモデルの提案，電子情報通信学会論文誌（D-I），Vol.J88-D-I, No.5, pp.940–948 (2005).
18) 本城信輔，洲崎誠一，斉藤　司ほか：プライバシに配慮した WWW における個人属性認証・アクセス制御システム，情報処理学会論文誌，Vol.43, No.8, pp.2573–2585 (2002).

(平成 19 年 10 月 29 日受付)
(平成 20 年 7 月 1 日採録)

© 2008 Information Processing Society of Japan

小林　　透

1985 年東北大学工学部精密機械工学科卒業．1987 年同大学大学院工学研究科修士課程修了．同年日本電信電話株式会社入社．以来，ソフトウェア生産技術，グループウェア，IC カードをベースとしたユビキタスコンピューティングに関する研究開発に従事．2006 年から暗号応用技術に関する研究開発を経て，現在，NTT 研究企画部門，担当部長．電子情報通信学会会員．

上野　正巳（正会員）

1993 年 3 月山梨大学大学院工学研究科修士課程修了．同年日本電信電話株式会社入社．以降，要求分析手法の研究，ライツマネージメント関連の研究，課金プラットフォームの研究，ユビキタス資源の利用権による管理の研究開発に従事．現在，NTT コミュニケーションズ金融イノベーションシステム部勤務．

近藤　好次（正会員）

1983 年山梨大学工学部計算機科学科卒業．同年日本電信電話公社（現日本電信電話株式会社）入社．高度インテリジェントネットワーク技術の研究開発に従事．その後，分散処理システム，仕様記述言語の研究を経て，2003 年からはユビキタスコンピューティング技術に関する研究開発に従事．2006 年から次世代ネットワークの研究開発推進，次世代サービス共通プラットフォームの研究開発を経て，現在，NTT アドバンステクノロジ株式会社，主幹担当部長，電子情報通信学会，情報処理学会，IEEE 各会員，工学博士．

大戸　健一

1992 年 3 月早稲田大学大学院理工学研究科機械工専攻修士課程修了．同年 4 月日本電信電話株式会社交換システム研究所に入社．以降，高度インテリジェントネットワークやユビキタスサービスを実現するためのネットワークシステムの研究開発に従事．現在，NTT 西日本技術革新部研究開発センタ勤務．電子情報通信学会会員．

© 2008 Information Processing Society of Japan